Monomial Ideals and Their Decompositions

W. Frank Moore

Mark Rogers

Sean Sather-Wagstaff

Department of Mathematics, Manchester Hall, Wake Forest University, Winston-Salem, NC, 27106
E-mail address: moorewf@wfu.edu
URL: http://users.wfu.edu/~moorewf

Mathematics Department, Missouri State University, Cheek Hall Room 45M, 901 South National Avenue, Springfield, MO 65897, USA
E-mail address: markrogers@missouristate.edu
URL: http://math.missouristate.edu/43628.htm

Mathematics Department, North Dakota State University Department # 2750, PO Box 6050, Fargo, ND 58108-6050, USA
E-mail address: Sean.Sather-Wagstaff@ndsu.edu
URL: http://www.ndsu.edu/pubweb/~ssatherw/

January 15, 2015.

Contents

Introduction

What Is This Book About?

A fundamental fact in arithmetic states that every integer $n \geqslant 2$ factors into a product of prime numbers in an essentially unique way. In algebra class, one learns a similar factorization result for polynomials in one variable with real number coefficients: every non-constant polynomial factors into a product of linear polynomials and irreducible quadratic polynomials in an essentially unique way. These examples share some obvious common ideas.

First, in each case we have a set of objects (in the first example, the set of integers; in the second example, the set of polynomials with real number coefficients) that can be added, subtracted, and multiplied in pairs so that the resulting sums, differences, and products are in the same set. (We say that the sets are "closed" under these operations.) Furthermore, addition and multiplication satisfy certain rules (or axioms) that make them "nice": they are commutative and associative, they have identities and additive inverses, and they interact coherently together via the distributive law. In other words, each of these sets is a *commutative ring with identity*. Note that we do not consider division in this setting because, for instance, the quotient of two non-zero integers need not be an integer. Commutative rings with identity arise in many areas of mathematics, e.g., in combinatorics, geometry, graph theory, and number theory.

Second, each example deals with factorization of certain elements into finite products of "irreducible" elements, that is, elements that cannot themselves be factored in a nontrivial manner. In general, given a commutative ring R with identity, the fact that elements can be multiplied implies that elements can be factored. One way to study R is to investigate how well its factorizations behave. For instance, one can ask whether the elements of R can be factored into a finite product of irreducible elements. (There are non-trivial examples where this fails.) Assuming that the elements of R can be factored into a finite product of irreducible elements, one can ask whether the factorizations are unique. The first example one might see where this fails is the ring $\mathbb{Z}[\sqrt{-5}]$ consisting of all complex numbers $a + b\sqrt{-5}$ such that a and b are integers. In this ring, we have $(2)(3) = 6 = (1+\sqrt{-5})(1-\sqrt{-5})$, and these two factorizations of 6 are fundamentally different.

In the 1800's, Ernst Kummer and Richard Dedekind recognized that this problem can be remedied, essentially by factoring elements into products of sets. More specifically, one replaces the element r to be factored with the set rR of all multiples of that element, and one factors this set into a product $rR = I_1 I_2 \cdots I_n$ of similar sets. (We are being intentionally vague here. For some technical details, see Chapter A.) The "similar sets" are called *ideals* because they are, in a sense, idealized versions of numbers. In the ring $R = \mathbb{Z}[\sqrt{-5}]$, the pathological factorizations of 6 yield a factorization $6R = J_1 J_2$ that is unique up to re-ordering the factors.

In many settings, factorizations into products of ideals are not as well behaved as one might like. In the 1900's Emanuel Lasker and Emmy Noether recognized that it is better in some ways to consider intersections instead of products. The idea is the same, except that factorizations are replaced by decompositions into finite intersections of irreducible ideals, i.e., ideals that cannot themselves be written as a non-trivial intersection of two ideals. In some cases (e.g., in $\mathbb{Z}[\sqrt{-5}]$) these are the same, but it can be shown that decompositions exist in many rings where nice factorizations do not.

In this book, we study ideals in the polynomial ring $R = A[X_1, \ldots, X_d]$ with coefficients in a commutative ring A over the variables $X_1, \ldots, X_d$. Specifically, we focus on monomial ideals, that is, ideals that are generated by monomials $X_1^{n_1} \cdots X_d^{n_d}$. We show that every monomial ideal in R can be written as an intersection of "m-irreducible" monomial ideals, that is, monomial ideals that cannot themselves be written as a non-trivial intersection of two monomial ideals. Such an intersection is called an "m-irreducible decomposition." We explicitly characterize the m-irreducible monomial ideals as those ideals generated by "pure powers" $X_{i_1}^{m_1}, \ldots, X_{i_n}^{m_n}$ of some of the variables. For certain classes of ideals, we provide explicit algorithms for computing m-irreducible decompositions. We focus on monomial ideals for several reasons.

First, monomial ideals are the simplest ideals, in a sense, since the generators have only one term each. Accordingly, this makes monomial ideals optimal objects of study for students with little background in abstract algebra. Indeed, students begin studying polynomials in middle school, and they have seen polynomials in several variables in calculus, so these are familiar objects that are not as intimidating as arbitrary elements of an arbitrary commutative ring. In other words, students feel more comfortable with the process of formally manipulating polynomials because they feel more concrete. When one restricts to ideals generated by monomials, the ideas become even more concrete. In the process of teaching the students about abstract algebra via monomial ideals, we find that the concreteness of these ideals makes it easier for students to grasp more the general concept of ideals. In addition, the material is not terribly difficult, but students will learn a non-trivial amount of mathematics in the process of working through it.

Second, monomial ideals have incredible connections to other areas of mathematics. For instance, one can use monomial ideals to study certain objects in combinatorics, geometry, graph theory, and topology. Reciprocally, one can study a monomial ideal using ideas from combinatorics, geometry, graph theory, and/or topology. For instance, we use some of these techniques explicitly in our algorithms for computing m-irreducible decompositions.

Who Is the Audience for This Book?

This book is written for mathematics students (in the broadest sense) who have taken an undergraduate course in abstract algebra. It is appropriate for a course for advanced undergraduates and/or graduate students. We have used preliminary versions of this text for traditional courses, for individual reading courses, and as a starting point for research projects, each with undergraduate and graduate students.

There are several excellent texts available for students and researchers who are interested in learning about monomial ideals, for instance, Herzog and Hibi [**19**], Hibi [**20**], Miller and Sturmfels [**30**], and Stanley [**39**]. The topic also receives significant attention in the books of Bruns and Herzog [**4**], and Villarreal [**42**]. However, each of these books is geared toward advanced graduate students (and higher). We think of our book as a gentle introduction to the subject that provides partial preparation for students interested in these other texts but without the necessary background. The level of this book is similar to that of the text by Cox, Little, and O'Shea [**6**]. However, the material covered in that text is very different from ours.

A Summary of the Contents

The book is divided topically into four parts. Part 1 of the text sets the stage with a general treatment of monomial ideals divided into three chapters. Chapter 1 deals with the fundamental properties of monomial ideals in the polynomial ring $A[X_1, \ldots, X_d]$ for use in the rest of the text. It is worth noting that we do not require A to be a field for most of the text, unlike many treatments of monomial ideals. We are able to do this because, unlike other treatments, we focus almost exclusively on the decompositions of these ideals, not on properties of their quotient rings.

Chapter 2 addresses ways of modifying monomial ideals to create new monomial ideals. For instance, we show that the intersection of monomial ideals is a monomial ideal, a fundamental fact for proving that every monomial ideal can be decomposed as an intersection of other monomial ideals.

Chapter 3 gets to the issue of m-irreducibility and m-irreducible decompositions for monomial ideals. The characterization of m-irreducibility is explicit, as we noted above. However, the proof of the existence of m-irreducible decompositions is not constructive. Some may view this as a defect, but we feel that it is an important demonstration of the power of abstraction.

Part 2 of the text describes connections between the realm of monomial ideals and other areas of mathematics and even other disciplines. Chapter 4 is devoted to certain connections with combinatorics. It discusses a case of ideals where m-irreducible decompositions can be described explicitly using combinatorial data. These are the square-free monomial ideals, that is, the ideals generated by monomials of the form $X_{i_1} \cdots X_{i_m}$ with strictly increasing subscripts. The algebraic properties of these ideals are completely determined by the combinatorial properties of an associated simplicial complex, and we show how the simplicial complex provides the m-irreducible decomposition of the ideal. The chapter begins with the special case of square-free monomial ideals generated by monomials of the form X_iX_j, whose decompositions can be described in terms of "vertex covers" of an associated simple graph.

Chapter 5 treats some interactions with other areas. For instance, we describe connections with electrical engineering, via the PMU Placement Problem. This uses graphs and edge ideals to understand properties of graphs that arise as models of electrical power systems. Connections to topology, geometry, and homological algebra are also highlighted here. It is worth noting that this chapter is quite colloquial in nature. In contrast to the other chapters, this one omits proofs of some results because they are outside the scope of this text. The idea here is to give a taste of these areas as they connect with monomial ideals. We include many references for readers looking for more information on any of these topics.

Part 3 of the text deals with the problem of computing m-irreducible decompositions explicitly. Chapter 6 deals with another case of ideals where m-irreducible decompositions can be described explicitly. These are the ideals that contain a power of each one of the variables. This condition means that there are only finitely many monomials that are not in the ideal, and there is an algorithm using these excluded monomials to find the decompositions. In this case, we call the decompositions "parametric decompositions."

Chapter 7 deals with some cases where we can describe the behavior of the m-irreducible decompositions when one modifies the ideals using the operations from Chapter 2. As a consequence, it contains an algorithm for computing m-irreducible decompositions in general.

Part 4 of the text consists of two appendices. Appendix A serves as a review of (or introduction to) the fundamentals of commutative algebra. Much of the material therein may have been covered in a course on abstract algebra. Accordingly, much of this material may be skipped, though it cannot be ignored entirely as it contains many of the definitions and notations used in the rest of the text.

Appendix B is an introduction to the computer algebra system Macaulay2 [**13**] which is available from the website `http://www.math.uiuc.edu/Macaulay2/` for free download. While it is not essential for a reader to use Macaulay2 to get a lot from the book, a certain amount of insight can be gained by working on these ideas with a computer algebra system. For instance, one can perform many computations in a short time period allowing one to formulate conjectures based on empirical data. Moreover, readers not familiar with Macaulay2 will want to work through much of this appendix if they hope to work through the computer portions of the main text found at the ends of the sections. On the other hand, some readers may prefer to use other programs like CoCoA [**5**] or Singular [**14**]. However, such readers will necessarily have to translate our code to their chosen system.

Most of the computer subsections in the text have two parts. The first part is a tutorial that introduces relevant Macaulay2 commands for the section, discussing how to format the input and how to interpret the output. The second part contains exercises to work through to practice the ideas from the tutorial. We do not include instructions for installing Macaulay2, referring the interested reader to the website `http://www.math.uiuc.edu/Macaulay2/Downloads/` for instructions. Note that the website `http://www.math.uiuc.edu/Macaulay2/GettingStarted/` contains tutorials, so the interested reader can get started there if he or she plans to skip most of Appendix A.

The reader may also notice that most chapters end with an "exploration" or two. These sections consist of exercise sets, with no lecture material, where students investigate a particular aspect of the ideas from the section. The philosophy behind these sections is that students often learn best by doing instead of reading or listening to lecture. We have had some success using these sections as extended writing projects. We have also devoted time in class to brainstorming with students about how to approach these exercises, to give them further insight into the process of problem solving around new concepts. The non-exploration sections are almost entirely independent of the explorations, and of each other. Exceptions to this are the following: Section 1.6 depends on 1.5, Section 6.6 depends on 3.5, and 7.6

depends on 2.6. In addition, Sections 3.5 and 6.6 provide many good examples for later use.

The reader should further notice that most chapters contain a few sections labeled as "optional." These sections contain fundamental results and ideas that are motivated by the work on monomial ideals, but are not necessary if one is exclusively focused on monomial ideals. For instance, in Section 1.1 one encounters the cancellation law for monomials: If f, g, and h are monomials such that $fg = fh$, then $g = h$. It is well known that the cancellation law does not hold in most rings. For instance, in $\mathbb{Z}_6$, we have $(2)(3) = 0 = (2)(0)$, but $3 \neq 0$. However, the cancellation law does hold in an integral domain, so we devote Section 1.2 to integral domains, though it is not needed for the remaining non-optional sections. We expect that students who encounter these sections will understand that certain properties of monomial ideals do not hold for arbitrary monomial ideals. Furthermore, we hope that these sections will compel students to delve more deeply into the subject of abstract algebra. Note that the optional sections depend on each other more than the explorations do. For instance, Section 3.2 uses material from 1.2, and Section 3.4 relies on 1.2, 1.4, and 3.2.

Lastly, we point out that this text contains over 200 exercises, most of which have multiple parts. Around 30 of these exercises are used in later sections; these are identified with an asterisk (see, e.g., Exercise A.1.24) and contain references to the place(s) where they are used. In addition, several proofs and parts of proofs are left as exercises for the reader. Finally, many examples, facts, remarks, and proofs omit details. In most places, this is intentional, and we encourage students to read the text critically. If a particular detail seems unjustified, work out the details with a pencil and paper.

Possible Course Outlines

One can use this text in several different ways, as we have done. Obviously, one can start at the beginning and work through as much material as one has time for. Another approach is to ignore the optional sections, leaving them as possible reading exercises for motivated students. Similar comments hold for the exploration sections, though we do encourage discussions of Sections 3.5 and 6.6, and for the sections that are not as central and do not feed much into the other sections; for example, Sections 2.5 and 7.2.

Another option is to pick a particular goal and work toward it, covering only the material needed for that goal. A couple of outlines for such course are as follows:

(1) Goal: Decompositions of edge ideals, face ideals and facet ideals. Cover Chapter A, as much as is needed. (Section A.5 is not needed.) Cover Sections 1.1, 1.3, 2.1, 2.3, 3.1, 3.3, and 3.5, then Chapter 4.

(2) Goal: parametric decompositions. Cover Chapter A, as much as is needed. (Note that Section A.5 *is* needed.) Cover Sections 1.1, 1.3, 2.1, 2.4, 2.3, 3.1, 3.3, and 3.5, then Chapter 6. If there is time, the material from Sections 7.3 and 7.5 give a nice ending to the course. Note that the proof of Theorem 7.5.3 uses Lemma 7.3.3, so Section 7.3 is needed for 7.5.

Depending on the pace, these course outlines may leave some time at the end of the term for other topics to be discussed.

Acknowledgments

We would like to express our thanks to the Mathematics Department at the University of Nebraska-Lincoln for its hospitality and generosity during the 2006 IMMERSE program (Intensive Mathematics: a Mentoring, Education and Research Summer Experience) when we taught the pilot version of this course. Specific thanks are due to the program's staff Allan Donsig and Marilyn Johnson, and to the other graduate student mentors Jen Everson, Martha Gregg, Kris Lund, Lori McDonnell, Jeremy Parrott, Emily Price, and Mark Stigge.

We are grateful to the students who have worked so enthusiastically through the various versions of these notes: Hannah Altmann, Zechariah Andersen, Ben Anderson, Katie Ansaldi, Pye Aung, Cheryl Balm, Debbie Berg, Stefan Bock, Sam Cash, Jacqueline Dresch, Sarah Gilles, Chad Haugen, Colleen Hughes, Dan Ingebretson, Erik Insko, Nick Johnson, Samuel Kolins, Alexis Krier, Bethany Kubik, Maxx Kureczko, Jeff Langford, David Lovit, Chelsey Morrow, Benjamin Noteboom, Chelsey Paulsen, Trevor Potter, Becky Price, Rebecca Ramos, Tyler Seacrest, Kelly Smith, Sarah Tekansik, Jon Totushek, and Rich Wicklein.

We are also grateful to William Heinzer, Louis J. Ratliff, Jr., and Kishor Shah whose paper [**18**] provided the initial motivation for this project. We are also grateful to Rajesh Kavasseri for introducing us to the topic of PMU placement, to Irena Swanson for invaluable help with the computer algebra system Macaulay2, to Jon Totushek for producing our simplicial complexes with TikZ, and to Carolyn Yackel for helping to make the book more readable (though she should not be blamed if it is not readable).

We are also pleased to acknowledge the financial support of the National Science Foundation (NSF grant NSF 0354281) and the National Security Agency. This material is based on work supported by North Dakota EPSCoR and National Science Foundation Grant EPS-0814442.

Notation

$\mathbb{N}$ is the set of nonnegative integers.
$\mathbb{Z}$ is the set of all integers.
$\mathbb{Q}$ is the set of rational numbers.
$\mathbb{R}$ is the set of real numbers.
$\mathbb{C}$ is the set of complex numbers.
$A \times B$ is the Cartesian product of two sets A and B.
$\mathbb{N}^d = \mathbb{N} \times \mathbb{N} \times \cdots \times \mathbb{N}$ with d factors.
$A[X]$ is the polynomial ring in one variable with coefficients in A.
$A[X, Y]$ is the polynomial ring in two variables with coefficients in A.
$A[X, Y, Z]$ is the polynomial ring in three variables with coefficients in A.
$A[X_1, \ldots, X_d]$ is the polynomial ring in d variables with coefficients in A.
$\mathfrak{X}$ is the ideal $(X_1, \ldots, X_d)R$ in the ring $R = A[X_1, \ldots, X_d]$.
S_n is the symmetric group on n letters.
$P(n)$ hold for $n \gg 0$ when there is an integer N such that $P(n)$ holds for all $n \geqslant N$.

Part 1

Monomial Ideals

In this part of the text, we explore the algebra of monomial ideals, that is, ideals in a polynomial ring that are generated by sets of monomials. In particular, the results of this part open the door to the connections to combinatorics and other areas described in Part 2.

Chapter 1 sets the stage with important basic properties of monomial ideals. Section 1.1 discusses the relation between a monomial ideal I and the set $[\![I]\!]$ of monomials in I. This includes a simple but important criterion for checking when a given monomial is in I. Some of the basic properties of monomials lead naturally to a discussion of integral domains, which is the subject of the optional Section 1.2. Section 1.3 is about generators of monomial ideals, and includes the fact that every monomial ideal is finitely generated. This is closely related to the noetherian property, which we treat in the optional Section 1.4. This chapter ends with two explorations: Section 1.5 shows how binomial coefficients arise in problems of counting monomials, and Section 1.6 introduces the related problem of determining numbers of generators of monomial ideals.

Chapter 2 looks at the behavior of monomial ideals under certain operations. We start with intersections in Section 2.1, which form the framework for our decomposition results. Since we use least common multiples to describe generating sets of intersections, we follow this with the optional Section 2.2 on unique factorization domains. Next comes Section 2.3, dealing with monomial radicals (a monomial version of the radical of an ideal), which are very important for the study of square-free monomial ideals in Chapter 4. Similarly, Section 2.3 is all about colon ideals, which are crucial for our treatment of parametric decompositions in Chapter 6. Bracket powers, related to the Frobenius endomorphism in characteristic p, are the next topic, in Section 2.5, and a souped-up version of this notion is treated in the exploration Section 2.6.

This part culminates in Chapter 3, which is an existential chapter about decompositions of monomial ideals. This chapter begins with Section 3.1 on m-irreducible monomial ideals. These are the analogs of prime numbers in our decomposition results, and we characterize them explicitly here. When working over a field, the m-irreducible monomial ideals are also irreducible, as we prove in the optional Section 3.2. The main point of this part of the text is the existence and uniqueness of m-irreducible decompositions, which we establish in Section 3.3. The related (but optional) topic of irreducible decompositions is treated in Section 3.4. While most of this chapter is existential in nature, Section 3.5 gives a first taste of how to actually compute these decompositions. This subjects is explored further in Chapter 4 and Part 3.

CHAPTER 1

Basic Properties of Monomial Ideals

In this chapter, we develop the fundamental tools for working with monomial ideals. Section 1.1 introduces the main players. Motivated by some properties from this section, Section 1.2 contains a brief discussion of integral domains. Section 1.3 deals with some aspects of generating sets for monomial ideals. The optional Section 1.4 on noetherian rings is a natural follow-up. The chapter concludes with an exploration of some numerical aspects of monomial ideals in Section 1.6.

1.1. Monomial Ideals

In this section, A is a non-zero commutative ring with identity.

Without further ado, we introduce the main objects of study in this text. For an introductory treatment of ideals and generators, see Section A.3.

DEFINITION 1.1.1. Set $R = A[X_1, \ldots, X_d]$. A *monomial ideal* in R is an ideal of R that can be generated by monomials in $X_1, \ldots, X_d$; see Definition A.1.11.

For example, consider the polynomial ring $R = A[X, Y]$. The ideal $I = (X^2, Y^3)R$ is a monomial ideal. Note that I contains the polynomial $X^2 - Y^3$, so monomial ideals may contain more than monomials. The ideal $J = (Y^2 - X^3, X^3)R$ is a monomial ideal because $J = (Y^2, X^3)R$. The trivial ideals 0 and R are monomial ideals since $0 = (\emptyset)R$ and $R = 1_R R = X_1^0 \cdots X_d^0 R$.

The following notation is non-standard but quite useful, so we use it frequently.

DEFINITION 1.1.2. Set $R = A[X_1, \ldots, X_d]$. For each monomial ideal $I \subseteq R$, let $[\![I]\!]$ denote the set of all monomials contained in I.

It is important to not that for each non-zero monomial ideal $I \subseteq R$, the set $[\![I]\!] \subset R$ is an infinite set that is not an ideal. Also, by definition, we have the useful equality $[\![I]\!] = I \bigcap [\![R]\!]$. The next lemma shows how this set is a natural generating set for I.

LEMMA 1.1.3. *Set $R = A[X_1, \ldots, X_d]$. For each monomial ideal $I \subseteq R$, we have $I = ([\![I]\!])R$.*

PROOF. Let S be a set of monomials generating I. It follows that $S \subseteq [\![I]\!] \subseteq I$, so $I = (S)R \subseteq ([\![I]\!])R \subseteq I$. This implies the desired equality. $\square$

The next criterion for containment and equality of monomial ideals is straightforward to prove, but it is incredibly useful.

PROPOSITION 1.1.4. *Set $R = A[X_1, \ldots, X_d]$. Let I and J be monomial ideals of R.*

(a) *We have $I \subseteq J$ if and only if $[\![I]\!] \subseteq [\![J]\!]$.*

(b) *We have* $I = J$ *if and only if* $[\![I]\!] = [\![J]\!]$.

PROOF. (a) If $I \subseteq J$, then $[\![I]\!] = I \bigcap [\![R]\!] \subseteq J \bigcap [\![R]\!] = [\![J]\!]$. Conversely, if $[\![I]\!] \subseteq [\![J]\!]$, then Lemma 1.1.3 implies that $I = ([\![I]\!])R \subseteq ([\![J]\!])R = J$.

Part (b) follows directly from (a). □

DEFINITION 1.1.5. Set $R = A[X_1, \ldots, X_d]$.

(a) Let f and g be monomials in R. Then f is a *monomial multiple* of g if there is a monomial $h \in R$ such that $f = gh$.
(b) For a monomial $f = \underline{X}^{\underline{n}} \in R$, the d-tuple $\underline{n} \in \mathbb{N}^d$ is the *exponent vector* of f.

Because the monomials in $R = A[X_1, \ldots, X_d]$ are linearly independent over A, the exponent vector of each monomial $f \in R$ is well-defined. In particular, for $\underline{m}, \underline{n} \in \mathbb{N}^d$, we have $\underline{X}^{\underline{m}} = \underline{X}^{\underline{n}}$ if and only if $\underline{m} = \underline{n}$.

In words, the next result says that a the product of a monomial and a non-monomial is not a monomial. While this may be intuitively clear, we include a proof for completeness. The main point is the linear independence of the monomials in $A[X_1, \ldots, X_d]$. The relation $\succcurlyeq$ is from Definition A.7.8.

LEMMA 1.1.6. *Set* $R = A[X_1, \ldots, X_d]$. *Let* $f = \underline{X}^{\underline{m}}$ *and* $g = \underline{X}^{\underline{n}}$ *be monomials in* R. *If* h *is a polynomial in* R *such that* $f = gh$, *then* $\underline{m} \succcurlyeq \underline{n}$ *and* h *is the monomial* $h = \underline{X}^{\underline{p}}$ *where* $p_i = m_i - n_i$.

PROOF. Assume that $f = gh$ where $h = \sum_{\underline{p} \in \Lambda} a_{\underline{p}} \underline{X}^{\underline{p}} \in R$ and $\Lambda \subset \mathbb{N}^d$ is a finite subset such that $a_{\underline{p}} \neq 0_A$ for each $\underline{p} \in \Lambda$. The equation $f = gh$ then reads

$$\underline{X}^{\underline{m}} = \underline{X}^{\underline{n}} \sum_{\underline{p} \in \Lambda} a_{\underline{p}} \underline{X}^{\underline{p}} = \sum_{\underline{p} \in \Lambda} a_{\underline{p}} \underline{X}^{\underline{n}+\underline{p}}.$$

The linear independence of the monomials in R implies that

$$a_{\underline{p}} = \begin{cases} 0_A & \text{when } \underline{n} + \underline{p} \neq \underline{m} \\ 1_A & \text{when } \underline{n} + \underline{p} = \underline{m}. \end{cases}$$

Since we have assumed that each of the coefficients $a_{\underline{p}}$ is non-zero, this implies that the only possible non-zero term in h is $a_{\underline{p}} \underline{X}^{\underline{p}}$ when $\underline{n} + \underline{p} = \underline{m}$; in other words, the set Λ consists of a single element $\Lambda = \{\underline{p}\}$. The coefficient $a_{\underline{p}} = 1_A$ then implies that $h = \underline{X}^{\underline{p}}$, so the equation $f = gh$ implies that f is a monomial multiple of g by definition, as desired. □

The next lemma builds from the previous one. For our purposes, the main point is the equivalence of conditions (i) and (iv) which gives a numerical/combinatorial criterion for a monomial f to be in the ideal generated by another monomial g. This is significantly enhanced in Theorem 1.1.8 and Exercise 1.1.11. See Definition A.7.10 for an explanation of the notation.

LEMMA 1.1.7. *Set* $R = A[X_1, \ldots, X_d]$. *Let* $f = \underline{X}^{\underline{m}}$ *and* $g = \underline{X}^{\underline{n}}$ *be monomials in* R. *The following conditions are equivalent:*

(i) *we have* $f \in gR$;
(ii) *the element* f *is a multiple of* g;
(iii) *the element* f *is a monomial multiple of* g;
(iv) *we have* $\underline{m} \succcurlyeq \underline{n}$; *and*
(v) *we have* $\underline{m} \in [\underline{n}]$.

PROOF. The equivalences (i) $\iff$ (ii) and (iv) $\iff$ (v) hold by definition, and the implication (iii) $\implies$ (ii) is by definition. The implication (ii) $\implies$ (iii) follows from Lemma 1.1.6.

(iii) $\implies$ (iv): Assume that $f = gh$ where $h = \underline{X}^{\underline{p}}$. It follows that

$$\underline{X}^{\underline{m}} = \underline{X}^{\underline{n}}\underline{X}^{\underline{p}} = \underline{X}^{\underline{n}+\underline{p}}.$$

The well-definedness of the exponent vector for a monomial implies that $\underline{m} = \underline{n}+\underline{p}$, i.e., that $m_i = n_i+p_i$ for $i = 1,\ldots,d$. Since each $p_i \geqslant 0$, this implies $m_i = n_i+p_i \geqslant n_i$ for each i, so $\underline{m} \succcurlyeq \underline{n}$ by definition, as desired.

(iv) $\implies$ (iii): Assume that $\underline{m} \succcurlyeq \underline{n}$. By definition, this implies that $m_i - n_i \geqslant 0$ for each i. Setting $p_i = m_i - n_i$, we have $\underline{p} \in \mathbb{N}^d$ and, as above, it follows that $f = gh$ where $h = \underline{X}^{\underline{p}}$. This says that f is a monomial multiple of g, as desired. □

Note that the previous result shows that the "divisibility order" on the monomial set $[\![R]\!]$ is a partial order. Indeed, the order $\succcurlyeq$ on $\mathbb{N}^d$ is a partial order by Exercise A.7.12. Thus, the desired conclusion follows from Lemma 1.1.7 since (a) the monomials in $[\![R]\!]$ are in bijection with the elements of $\mathbb{N}^d$, and (b) Lemma 1.1.7 implies that $\underline{X}^{\underline{m}} \succcurlyeq \underline{X}^{\underline{n}}$ if and only if $\underline{m} \succcurlyeq \underline{n}$.

The next result provides a criterion for detecting membership of a monomial in a monomial ideal. Note that it assumes that the ideal is generated by a finite set of monomials. We show in Theorem 1.3.1 that every monomial ideal is generated by a finite list of monomials, so this result applies to every monomial ideal. See also Exercise 1.1.11. It is worth noting that the non-trivial implication of Theorem 1.1.8 can fail if the f_i are not monomials; see Exercise A.3.19(a).

THEOREM 1.1.8. *Set $R = A[X_1,\ldots,X_d]$. Let $f, f_1,\ldots,f_m$ be monomials in R. Then $f \in (f_1,\ldots,f_m)R$ if and only if $f \in f_iR$ for some i.*

PROOF. $\Longleftarrow$: Since $f_i \in \{f_1,\ldots,f_m\}$, we have $f_iR = (f_i)R \subseteq (f_1,\ldots,f_m)R$.

$\Longrightarrow$: Assume that $f \in (f_1,\ldots,f_m)R$ and write $f = \sum_{i=1}^m f_ig_i$ with elements $g_i \in R$. By assumption, we have $f = \underline{X}^{\underline{n}}$ and $f_i = \underline{X}^{\underline{n}_i}$ for some $\underline{n},\underline{n}_1,\ldots,\underline{n}_m \in \mathbb{N}^d$. By definition, we can write each $g_i = \sum_{\underline{p}\in\mathbb{N}^d}^{\text{finite}} a_{i,\underline{p}}\underline{X}^{\underline{p}}$ where each $a_{i,\underline{p}} \in A$, so

$$\underline{X}^{\underline{n}} = f = \sum_{i=1}^m f_ig_i = \sum_{i=1}^m \underline{X}^{\underline{n}_i}\left(\sum_{\underline{p}\in\mathbb{N}^d}^{\text{finite}} a_{i,\underline{p}}\underline{X}^{\underline{p}}\right) = \sum_{i=1}^m \sum_{\underline{p}\in\mathbb{N}^d}^{\text{finite}} a_{i,\underline{p}}\underline{X}^{\underline{n}_i+\underline{p}}.$$

Since the monomials in R are linearly independent over A, the monomial $\underline{X}^{\underline{n}}$ must occur in the right-most sum in this display. (Note that we are not suggesting that the monomials occurring in the right-most sum are distinct. Hence, the monomial $\underline{X}^{\underline{n}}$ it may occur more than once in this expression.) In other words, we have $\underline{X}^{\underline{n}} = \underline{X}^{\underline{n}_i+\underline{p}}$ for some i and some $\underline{p}$. It follows that

$$f = \underline{X}^{\underline{n}} = \underline{X}^{\underline{n}_i+\underline{p}} = \underline{X}^{\underline{n}_i}\underline{X}^{\underline{p}} = f_i\underline{X}^{\underline{p}} \in f_iR$$

for some i, as desired. □

The next construction allows us to visualize monomial ideals, at least in two variables, which is very useful for building intuition.

DEFINITION 1.1.9. Set $R = A[X_1,\ldots,X_d]$. The *graph* of a monomial ideal I is

$$\Gamma(I) = \{\underline{n} \in \mathbb{N}^d \mid \underline{X}^{\underline{n}} \in I\}.$$

The next result explains the connection between generators of monomial ideals and some basic subsets of $\mathbb{N}^d$. It simplifies the work involved in identifying $\Gamma(I)$.

Theorem 1.1.10. *Set $R = A[X_1, \ldots, X_d]$. If $I = (\underline{X}^{\underline{n}_1}, \ldots, \underline{X}^{\underline{n}_m})R$, then $\Gamma(I) = [\underline{n}_1] \cup \cdots \cup [\underline{n}_m]$.*

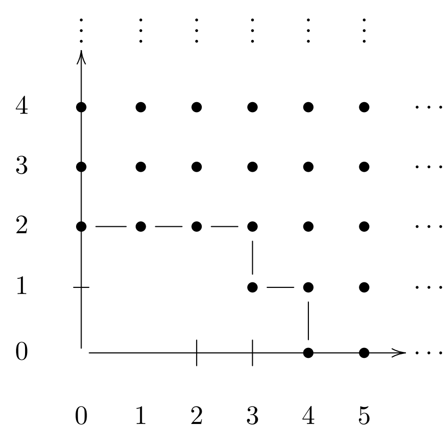
Proof. $\supseteq$: Let $\underline{m} \in [\underline{n}_1] \cup \cdots \cup [\underline{n}_m]$. Then we have $\underline{m} \in [\underline{n}_i]$ for some i, and so $\underline{m} \succcurlyeq \underline{n}_i$. Lemma 1.1.7 implies that

$$\underline{X}^{\underline{m}} \in \underline{X}^{\underline{n}_i}R \subseteq (\underline{X}^{\underline{n}_1}, \ldots, \underline{X}^{\underline{n}_m})R = I$$

and it follows by definition that $\underline{m} \in \Gamma(I)$.

$\subseteq$: Assume that $\underline{p} \in \Gamma(I)$. Then $\underline{X}^{\underline{p}} \in I = (\underline{X}^{\underline{n}_1}, \ldots, \underline{X}^{\underline{n}_m})R$, so Theorem 1.1.8 implies that $\underline{X}^{\underline{p}} \in \underline{X}^{\underline{n}_j}R$ for some j. From Lemma 1.1.7 we conclude that $\underline{p} \in [\underline{n}_j] \subseteq [\underline{n}_1] \cup \cdots \cup [\underline{n}_m]$, as desired. $\square$

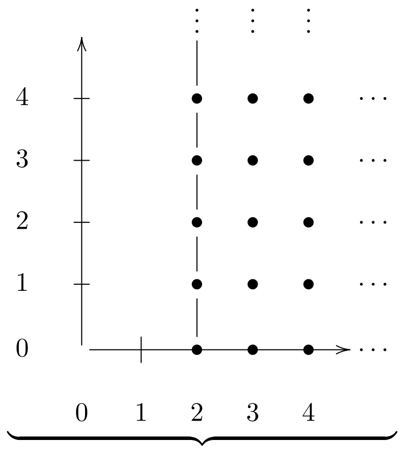
We consider a couple of examples in $R = A[X, Y]$. For $I = (X^4, X^3Y, Y^2)R$, we have $\Gamma(I) = [(4, 0)] \cup [(3, 1)] \cup [(0, 2)] \subseteq \mathbb{N}^2$, represented in the next diagram.



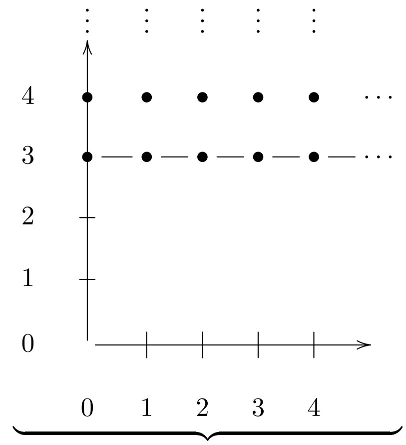
Next, consider the ideals $J = (X^2)R$ and $K = (Y^3)R$. Then $J + K = (X^2, Y^3)R$. Theorem 1.1.10 shows that $\Gamma(J) = [(2, 0)]$, $\Gamma(K) = [(0, 3)]$ and

$$\Gamma(J + K) = [(2, 0)] \cup [(0, 3)] = \Gamma(J) \cup \Gamma(K).$$

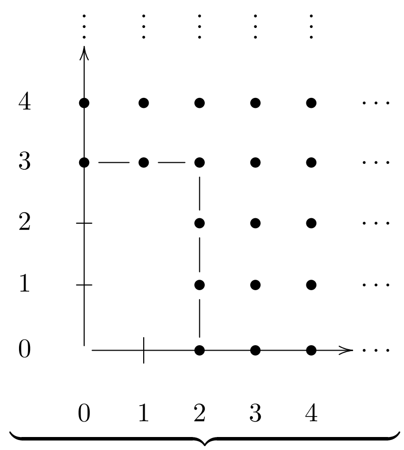
Graphically, we have the following:



$\Gamma(J)$



$\Gamma(K)$

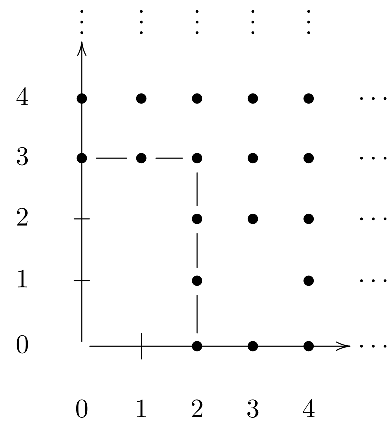


$\Gamma(J+K)=\Gamma(J)\cup\Gamma(K)$

More generally, in Exercise 1.3.11(e) we see that if $I_1, \ldots, I_n$ are monomial ideals in $A[X_1, \ldots, X_d]$, then $\Gamma(\sum_{j=1}^n I_j) = \cup_{j=1}^n \Gamma(I_j)$.

It is straightforward to identify the subsets of $\mathbb{N}^d$ that occur as graphs of monomial ideals: a nonempty subset $\Gamma \subseteq \mathbb{N}^d$ is of the form $\gamma = \Gamma(I)$ for some monomial ideal $I \subseteq A[X_1, \ldots, X_d]$ if and only if for each $\underline{m} \in \Gamma$ and each $\underline{n} \in \mathbb{N}^d$ one has

$\underline{m} + \underline{n} \in \Gamma$. For instance, the following is not of the form $\gamma = \Gamma(I)$:



Exercises.

EXERCISE 1.1.11. Set $R = A[X_1, \ldots, X_d]$. Let f be a monomial in R, and let S be a set of monomials in R. Prove that $f \in (S)R$ if and only if $f \in sR$ for some $s \in S$.

EXERCISE 1.1.12. Set $R = A[X_1, \ldots, X_d]$. Set $\mathfrak{X} = (X_1, \ldots, X_d)R$ and let I be a monomial ideal. Prove that $I \neq R$ if and only if $I \subseteq \mathfrak{X}$.

EXERCISE 1.1.13. Set $R = A[X_1, \ldots, X_d]$. Set $\mathfrak{X} = (X_1, \ldots, X_d)R$. Prove that if I is a monomial ideal such that $I \neq R$, then $\operatorname{rad}(I) = \operatorname{rad}(\mathfrak{X})$ if and only if for each $i = 1, \ldots, d$ there exists an integer $n_i > 0$ such that $X_i^{n_i} \in I$.

*EXERCISE 1.1.14. Set $R = A[X_1, \ldots, X_d]$. Set $\mathfrak{X} = (X_1, \ldots, X_d)R$ and let I be a monomial ideal. Prove that if $\operatorname{rad}(I) \subseteq \operatorname{rad}(\mathfrak{X})$, then $I \subseteq \mathfrak{X} \subsetneq R$. (This exercise is used in the proof of Lemma 2.4.3.)

EXERCISE 1.1.15. Set $R = A[X_1, \ldots, X_d]$. Prove that for monomials $f, g \in [\![R]\!]$, one has $(f)R = (g)R$ if and only if $f = g$.

*EXERCISE 1.1.16. Set $R = A[X_1, \ldots, X_d]$. Let I be an ideal of R. Prove that the following conditions are equivalent.

(i) I is a monomial ideal; and
(ii) for each $f \in I$ each monomial occurring in f is in I.

(This exercise is used in the proofs of Theorems 2.1.1, 2.4.1, and 3.2.4.)

EXERCISE 1.1.17. Set $R = A[X_1, \ldots, X_d]$. Let I and J be monomial ideals in R. Prove that $I = J$ if and only if $\Gamma(I) = \Gamma(J)$.

EXERCISE 1.1.18. Set $R = A[X_1, \ldots, X_d]$. Prove that if I is a monomial ideal in R such that $I \neq R$, then $I \bigcap A = 0$.

EXERCISE 1.1.19. Set $R = A[X_1, \ldots, X_d]$. Let f, g, h be monomials in R.

(a) Prove that if $fh = gh$, then $f = g$.
(b) Prove that if $fX_i = gX_j$ for some $i \neq j$, then $f \in (X_j)R$ and $g \in (X_i)R$.
(c) Prove that $\deg(fg) = \deg(f) + \deg(g)$.

EXERCISE 1.1.20. Set $R = A[X, Y]$. Find $\Gamma(I)$ for the following ideals and justify your answers:

(a) $I = (X^5, Y^4)R$.
(b) $I = (X^5, XY^2, Y^4)R$.
(c) $I = (X^5Y, X^2Y^2, XY^4)R$.

*EXERCISE 1.1.21. Set $R = A[X_1, \ldots, X_d]$. Let $\mathfrak{X} = (X_1, \ldots, X_d)R$. Let I be a monomial ideal in R, and let S denote the set of monomials in $R \smallsetminus I$. Prove that S is a finite set if and only if $\operatorname{rad}(I) \supseteq \operatorname{rad}(\mathfrak{X})$. (This exercise is used in the proofs of Propositions 6.3.4 and 6.5.1.)

Monomial Ideals in Macaulay2.

In this tutorial, we show how to use the `exponents` command to work with exponent vectors of monomials. Exponent vectors can be subtracted, and then the function `all` can be used to test whether all elements of the resulting list satisfy a given condition (in this case, we test for positivity). We also see how the command `->` is used to create a function, and how the command `first` gives the first element of a list. Note that this method of exponent vectors is not the quickest way to use Macaulay2 to decide if one monomial divides another; you may wish to choose an easier method for the exercises that follow.

```
i1 : R = ZZ/101[x, y, z]

o1 = R

o1 : PolynomialRing

i2 : exponents(x^3*y) -- the exponent vector, with redundant braces

o2 = {{3, 1, 0}}

o2 : List

i3 : f = i -> i^2 -- the squaring function, for example

o3 = f

o3 : FunctionClosure

i4 : f(3)

o4 = 9

i5 : f = i -> (i > 0) -- but we need a function to test positivity

o5 = f

o5 : FunctionClosure

i6 : f(-1) -- testing; should be false since -1 is not positive
```

```
o6 = false

i7 : exponents(x^3*y) - exponents(x^2*y*2*z^3)

o7 = {{1, 0, -3}}

o7 : List

i8 : first oo -- grab first element to get rid of extra braces

o8 = {1, 0, -3}

o8 : List

i9 : all(oo, f) -- test to see if all entries are positive

o9 = false
```

Exercises.

Exercise 1.1.22. Set $R = \mathbb{Z}_{101}[X, Y]$.

(a) Use Macaulay2 to verify that $X^2 - Y^3 \in (X^2, Y^3)R$.
(b) Use Macaulay2 to verify that $(Y^2 - X^3, X^3)R = (Y^2, X^3)R$.

Exercise 1.1.23. Set $R = \mathbb{Z}_{101}[X, Y]$.

(a) Use Macaulay2 to verify that $X^2Y \nmid XY^7$ and $X^2Y \big| X^2Y^7$.
(b) Use Macaulay2 to verify that $XY^7 \notin (X^2Y)R$ and $X^2Y^7 \in (X^2Y)R$.

Exercise 1.1.24. Set $R = \mathbb{Z}_{101}[X, Y]$ and $J = (Y^2 - X^3, X^3)R = (Y^2, X^3)R$.

(a) Use Macaulay2 to verify that $Y^2 \in J$ and $Y^2 - X^3 \nmid Y^2$ and $X^3 \nmid Y^2$.
(b) Use Macaulay2 to verify that $X^2 \notin J$ and $Y^2 \nmid X^2$ and $X^3 \nmid X^2$.

Exercise 1.1.25. Set $R = \mathbb{Z}_{101}[X, Y]$. Choose two monomials $f, g \in R$ and use Macaulay2 to verify that $\deg(fg) = \deg(f) + \deg(g)$.

1.2. Integral Domains (optional)

Given polynomials $f, g \in A[X]$ one may have $\deg(fg) = \deg(f) + \deg(g)$ or $\deg(fg) < \deg(f) + \deg(g)$. For monomials, we have seen that the equality always holds. This is, in many regards, the nicest situation. This section focuses on rings for which this equality always holds.

Definition 1.2.1. An *integral domain* is a commutative ring R with identity such that $1_R \neq 0_R$ and such that for all $r, s \in R$ if $r, s \neq 0_R$, then $rs \neq 0_R$.

For example, the rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{Z}$ are integral domains. The ring $\mathbb{Z}_n$ is an integral domain if and only if n is prime. For instance, the ring $\mathbb{Z}_6$ is not an integral domain because $2, 3 \neq 0$ in $\mathbb{Z}_6$, but $2 \cdot 3 = 0$ in $\mathbb{Z}_6$.

The next proposition shows that every field is an integral domain; for a treatment of the converse, see Exercise 1.2.7.

Proposition 1.2.2. *If R is a field, then R is an integral domain.*

PROOF. Assume that R is a field, and let $r, s \in R$ such that $rs = 0_R$. We need to show that $r = 0_R$ or $s = 0_R$. Assume that $r \neq 0_R$. Since R is a field, we have

$$s = 1_R s = (r^{-1}r)s = r^{-1}(rs) = r^{-1}0_R = 0_R$$

as desired. $\square$

In many respects, the next result contains the most important property of integral domains. Compare it with Exercise 1.1.19(a). See also Exercise 1.2.10 for the converse.

PROPOSITION 1.2.3 (cancellation). *Let R be an integral domain. If $r, s, t \in R$ such that $r \neq 0_R$ and $rs = rt$, then $s = t$.*

PROOF. Given that $rs = rt$, we have $r(s - t) = 0_R$. Since R is an integral domain and $r \neq 0_R$, it follows that $s - t = 0_R$, that is, that $s = t$. $\square$

Next we present the result described in the introduction to this section. See Exercise 1.2.8 for a counterexample when A is not an integral domain. Exercises 1.2.9 and 1.2.11 contain related results.

PROPOSITION 1.2.4. *Let A be an integral domain.*

(a) *Given non-zero polynomials $f, g \in A[X]$, one has $\deg(fg) = \deg(f) + \deg(g)$, and the leading coefficient of fg is the product of the leading coefficients of f and g.*
(b) *The ring $A[X]$ is an integral domain.*

PROOF. (a) Write $f = \sum_{i=0}^{m} a_i X^i$ and $g = \sum_{i=0}^{n} b_i X^i$ with $m = \deg(f)$ and $n = \deg(g)$. It follows that we have

$$fg = a_0b_0 + (a_1b_0 + a_0b_1)X + \cdots + (a_mb_{n-1} + a_{m-1}b_n)X^{m+n-1} + a_mb_nX^{m+n}.$$

Since R is an integral domain and $a_m, b_n \neq 0_R$, it follows that $a_mb_n \neq 0_R$, and hence the desired properties.

(b) Part (a) shows that the product of two non-zero polynomials in $A[X]$ is non-zero. Since $1_{A[X]} = 0_A \neq 1_A = 1_{A[X]}$, it follows that $A[X]$ is an integral domain. $\square$

COROLLARY 1.2.5. *If A is an integral domain, then so is $A[X_1, \ldots, X_d]$.*

PROOF. Argue by induction on d, using Proposition 1.2.4(b). $\square$

Exercises.

EXERCISE 1.2.6. Prove that $\mathbb{Z}_n$ is an integral domain if and only if n is prime.

EXERCISE 1.2.7. Find an example of an integral domain that is not a field.

EXERCISE 1.2.8. Find two nonzero polynomials f and g in $\mathbb{Z}_4[x]$ such that $\deg(fg) \neq \deg(f) + \deg(g)$.

EXERCISE 1.2.9. Let A be a commutative ring with identity.

(a) Prove that if A is a subring of an integral domain, then A is an integral domain.
(b) Prove that if the polynomial ring $A[X_1, \ldots, X_d]$ in d variables is an integral domain for some $d \geqslant 1$, then A is an integral domain.

Exercise 1.2.10. Let R be a commutative ring with identity such that $1_R \neq 0_R$. Assume that for all $r, s, t \in R$ if $r \neq 0_R$ and $rs = rt$, then $s = t$ Prove that R is an integral domain.

Exercise 1.2.11. Let A be a commutative ring with identity such that $1_A \neq 0_A$. Assume that for all non-zero polynomials $f, g \in A[X]$ in one variable, one has $\deg(fg) = \deg(f) + \deg(g)$. Prove that A is an integral domain.

Exercise 1.2.12. Prove or disprove the following: If A is an integral domain, then $A[X_1, X_2, \ldots]$ is an integral domain. Does the converse hold? Justify your answers.

Integral Domains in Macaulay2: Exercises.

Exercise 1.2.13. Set $A = \mathbb{Z}_{101}[Y, Z]$. Choose two polynomials $f, g \in A[X]$ and use Macaulay2 to verify that $\deg(fg) = \deg(f) + \deg(g)$.

1.3. Generators of Monomial Ideals

In this section, A is a non-zero commutative ring with identity.

Theorem 1.1.10 is only stated for a monomial ideal I that is generated by a finite number of monomials. The next result shows that this condition is automatic for all monomial ideals. We call it the "Monomial Hilbert Basis Theorem," after David Hilbert; compare to the usual Hilbert Basis Theorem 1.4.5. Notice that we do not impose any extra restrictions on the ring A.

Theorem 1.3.1. *Set $R = A[X_1, \ldots, X_d]$. Then every monomial ideal of R is finitely generated; moreover, it is generated by a finite set of monomials.*

Proof. Let $I \subseteq R$ be a monomial ideal, and assume without loss of generality that $I \neq 0$. We proceed by induction on the number of variables d.

Base case: $d = 1$. For this case, we write $R = A[X]$. Let

$$r = \min\{e \geqslant 0 \mid X^e \in I\}.$$

Then $X^r \in I$ and so $X^r R \subseteq I$. We will be done with this case once we show that $X^r R \supseteq I$. Since I is generated by its monomials, it suffices to show that $X^r R \supseteq [\![I]\!]$. For this, note that if $X^s \in I$, then $s \geqslant r$ and so $X^s \in X^r R$ by Lemma 1.1.7.

Induction step: Assume that $d \geqslant 2$ and assume that every monomial ideal of the ring $R' = A[X_1, \ldots, X_{d-1}]$ is finitely generated. Given a monomial ideal I, set

$$S = \{\text{monomials } z \in R' \mid zX_d^e \in I \text{ for some } e \geqslant 0\}$$

and $J = (S)R'$. By definition J is a monomial ideal in R', so our induction hypothesis implies that it is finitely generated, say $J = (z_1, \ldots, z_n)R'$ where $z_1, \ldots, z_n \in S$; see Proposition A.3.11(d). For $i = 1, \ldots, n$ there exists an integer $e_i \geqslant 0$ such that $z_i X_d^{e_i} \in I$. With $e = \max\{e_1, \ldots, e_n\}$, it follows that $z_i X_d^e \in I$ for $i = 1, \ldots, n$.

For $m = 0, \ldots, e - 1$ we set

$$S_m = \{\text{monomials } w \in R' \mid wX_d^m \in I\}$$

and $J_m = (S_m)R'$. By definition J_m is a monomial ideal in R', so our induction hypothesis implies that it is finitely generated, say $J_m = (w_{m,1}, \ldots, w_{m,n_m})R'$ where $w_{m,1}, \ldots, w_{m,n_m} \in S_m$.

Let I' be the ideal of R generated by the $z_iX_d^e$ and the $w_{m,i}X_d^m$:

$$I' = (\{z_iX_d^e \mid i = 1, \ldots, n\} \cup \{w_{m,i}X_d^m \mid m = 0, \ldots, e-1; i = 1, \ldots, n_m\})R.$$

By construction I' is a finitely generated monomial ideal of R. By definition, each $z_iX_d^e, w_{m,i}X_d^m \in I$, so we have $I' \subseteq I$.

Claim: $I' = I$. (Once the claim is established, we conclude that I is generated by a finite set of its monomials, completing the proof.) It suffices to show that $I' \supseteq I$. Since I is generated by its monomials, it suffices to show that $I' \supseteq [\![I]\!]$, so let $\underline{X}^{\underline{p}} = X_1^{p_1} \cdots X_{d-1}^{p_{d-1}} X_d^{p_d} \in [\![I]\!]$.

Case 1: $p_d \geqslant e$. We have $X_1^{p_1} \cdots X_{d-1}^{p_{d-1}} \in S \subseteq J = (z_1, \ldots, z_n)R'$. Thus, we have $X_1^{p_1} \cdots X_{d-1}^{p_{d-1}} \in z_iR'$ for some i, by Theorem 1.1.8. Writing $X_1^{p_1} \cdots X_{d-1}^{p_{d-1}} = z_iz$ for some $z \in R'$, we have

$$\underline{X}^{\underline{p}} = X_1^{p_1} \cdots X_{d-1}^{p_{d-1}} X_d^{p_d} = z_izX_d^eX_d^{p_d-e} = (z_iX_d^e)(zX_d^{p_d-e}) \in (z_iX^e)R \subseteq I'$$

as desired.

Case 2: $p_d < e$. The monomial $X_1^{p_1} \cdots X_{d-1}^{p_{d-1}}$ is in the set $S_{p_d} \subseteq J_{p_d} = (w_{p_d,1}, \ldots, w_{p_d,n_{p_d}})R'$. Theorem 1.1.8 implies that $X_1^{p_1} \cdots X_{d-1}^{p_{d-1}} \in w_{p_d,i}R'$ for some i. Writing $X_1^{p_1} \cdots X_{d-1}^{p_{d-1}} = w_{p_d,i}w$ for some $w \in R'$, we have

$$\underline{X}^{\underline{p}} = X_1^{p_1} \cdots X_{d-1}^{p_{d-1}} X_d^{p_d} = w_{p_d,i}wX_d^{p_d} = (w_{p_d,i}X_d^{p_d})(w) \in (w_{p_d,i}X_d^{p_d})R \subseteq I'$$

as desired. □

Corollary 1.3.2. *Set $R = A[X_1, \ldots, X_d]$. Let $S \subseteq [\![R]\!]$ and set $I = (S)R$. Then there is a finite sequence $s_1, \ldots, s_n \in S$ such that $I = (s_1, \ldots, s_n)R$.*

Proof. Theorem 1.3.1 implies that I is finitely generated, so the desired conclusion follows from Proposition A.3.11(d). □

Part (a) of the next result says that the polynomial ring $R = A[X_1, \ldots, X_d]$ satisfies the *ascending chain condition for monomial ideals*. Part (b) says that every nonempty set Σ of monomial ideals in R has a *maximal element*, and that every element of Σ is contained in a maximal element of Σ. While this result may seem esoteric, it is quite useful. For instance, it is the key to the main result of this part of the text in Section 3.3.

Theorem 1.3.3. *Set $R = A[X_1, \ldots, X_d]$.*

(a) *Given a chain $I_1 \subseteq I_2 \subseteq \cdots$ of monomial ideals in R, there is an integer $N \geqslant 1$ such that $I_N = I_{N+1} = \cdots$.*

(b) *Given a nonempty set Σ of monomial ideals in R, there is an ideal $I \in \Sigma$ such that for all $J \in \Sigma$, if $I \subseteq J$, then $I = J$. Moreover, for each $K \in \Sigma$, there is an ideal $I \in \Sigma$ such that $K \subseteq I$ and such that for all $J \in \Sigma$, if $I \subseteq J$, then $I = J$.*

Proof. (a) Consider a chain $I_1 \subseteq I_2 \subseteq \cdots$ of monomial ideals in R. Then the ideal $J = \sum_{j=1}^\infty I_j = \cup_{j=1}^\infty I_j$ is a monomial ideal in R; see Fact A.4.6(c) and Exercise 1.3.11(a). Theorem 1.3.1 implies that J is generated by a finite list of monomials $f_1, \ldots, f_m \in [\![J]\!]$. Since $J = \cup_{j=1}^\infty I_j$, for $i = 1, \ldots, m$ there is an index j_i such that $f_i \in I_{j_i}$. The condition $I_1 \subseteq I_2 \subseteq \cdots$ implies that there is an index N such that $f_i \in I_N$ for $i = 1, \ldots, m$. It follows that

$$J = (f_1, \ldots, f_m)R \subseteq I_N \subseteq I_{N+1} \subseteq I_{N+2} \subseteq \cdots \subseteq J.$$

Thus, we have equality at each step, as desired.

(b) Let Σ be a nonempty set of monomial ideals in R, and let $K \in \Sigma$. Suppose by way of contradiction that K is not contained in a maximal element of Σ. In particular, K is not a maximal element of Σ, so there is an element $I_1 \in \Sigma$ such that $K \subsetneq I_1$. Since K is not contained in a maximal element of Σ, it follows that I_1 is not a maximal element of Σ. Thus, there is an element $I_2 \in \Sigma$ such that $K \subsetneq I_1 \subsetneq I_2$. Continue this process inductively to construct a chain $K \subsetneq I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$ of elements of Σ. The existence of this chain contradicts part (a). $\square$

Definition 1.3.4. Set $R = A[X_1, \ldots, X_d]$. Let I be a monomial ideal of R. Let $z_1, \ldots, z_m \in [\![I]\!]$ such that $I = (z_1, \ldots, z_m)R$. The list $z_1, \ldots, z_m$ is an *irredundant monomial generating sequence* for I if z_i is not a monomial multiple of z_j whenever $i \neq j$. The list is a *redundant monomial generating sequence* for I if it is not irredundant.

For an example, we work in $R = A[X, Y]$. The sequence X^3, X^2Y, X^2Y^2, Y^5 is a redundant generating sequence for $(X^3, X^2Y, X^2Y^2, Y^5)R$ because $X^2Y \big| X^2Y^2$. The sequence X^3, X^2Y, XY^2, Y^3 is an irredundant monomial generating sequence for $(X^3, X^2Y, XY^2, Y^3)R$ because none of the monomials X^3, X^2Y, XY^2, Y^3 is a multiple of the other; verify this using exponent vectors and Lemma 1.1.7.

Our next result contains a practical criterion for checking whether a given monomial generating sequence is irredundant.

Proposition 1.3.5. *Set $R = A[X_1, \ldots, X_d]$. Let I be a monomial ideal of R, and let $z_1, \ldots, z_m \in [\![I]\!]$ such that $I = (z_1, \ldots, z_m)R$. The following conditions are equivalent:*

(i) *the generating sequence $z_1, \ldots, z_m$ is irredundant;*
(ii) *for $i = 1, \ldots, m$ we have $z_i \notin (z_1, \ldots, z_{i-1}, z_{i+1}, \ldots, z_m)R$; and*
(iii) *for $i = 1, \ldots, m$ we have $(z_1, \ldots, z_{i-1}, z_{i+1}, \ldots, z_m)R \subsetneq I$.*

Proof. (i) $\Longrightarrow$ (ii): Assume that the generating sequence $z_1, \ldots, z_m$ is irredundant. If $z_i \in (z_1, \ldots, z_{i-1}, z_{i+1}, \ldots, z_m)R$, then Theorem 1.1.8 implies that $z_i \in z_jR$ for some $j \neq i$; Lemma 1.1.7 then implies that z_i is a monomial multiple of z_j; this contradicts the irredundancy of the generating sequence.

(ii) $\Longrightarrow$ (iii): If $z_i \notin (z_1, \ldots, z_{i-1}, z_{i+1}, \ldots, z_m)R$, then z_i is in I and is not in $(z_1, \ldots, z_{i-1}, z_{i+1}, \ldots, z_m)R$ so $(z_1, \ldots, z_{i-1}, z_{i+1}, \ldots, z_m)R \subsetneq I$.

(iii) $\Longrightarrow$ (i): Assume that $(z_1, \ldots, z_{i-1}, z_{i+1}, \ldots, z_m)R \subsetneq I$ for $i = 1, \ldots, m$. Suppose that the sequence $z_1, \ldots, z_m$ is redundant and fix indices i, j such that $i \neq j$ and z_i is a monomial multiple of z_j. Then $z_i \in z_jR \subseteq (z_1, \ldots, z_{i-1}, z_{i+1}, \ldots, z_m)R$. It follows that

$$I = (z_1, \ldots, z_{i-1}, z_i, z_{i+1}, \ldots, z_m)R \subseteq (z_1, \ldots, z_{i-1}, z_{i+1}, \ldots, z_m)R$$

which contradicts our assumption. $\square$

The previous result does not assume (or conclude) that the ideal I has an irredundant monomial generating sequence. This is dealt with in the next result.

Theorem 1.3.6. *Set $R = A[X_1, \ldots, X_d]$. Let I be a monomial ideal of R.*

(a) *Every monomial generating set for I contains an irredundant monomial generating sequence for I.*
(b) *The ideal I has an irredundant monomial generating sequence.*
(c) *Irredundant monomial generating sequences are unique up to re-ordering.*

PROOF. (a) Assume without loss of generality that $S \neq 0$. Corollary 1.3.2 implies that I can be generated by a finite list of monomials $z_1, \ldots, z_m \in S$. If the sequence is redundant, then Proposition 1.3.5 provides an index i such that $(z_1, \ldots, z_{i-1}, z_{i+1}, \ldots, z_m)R = I$; hence, the shorter list $z_1, \ldots, z_{i-1}, z_{i+1}, \ldots, z_m$ of monomials generates I. Repeat this process with the new list, removing elements from the list until the remaining elements form an irredundant monomial generating sequence for I. The process will terminate in finitely many steps as the original list is finite.

(b) The ideal I has a monomial generating set by definition, so the desired conclusion follows from part (a).

(c) Assume that $z_1, \ldots, z_m$ and $w_1, \ldots, w_n$ are two irredundant monomial generating sequences. We show that $m = n$ and that there is a permutation $\sigma \in S_n$ such that $z_i = w_{\sigma(i)}$ for $i = 1, \ldots, n$.

Fix an index i. Since z_i is in $I = (w_1, \ldots, w_n)R$, Theorem 1.1.8 implies that z_i is a monomial multiple of w_j for some index j. Similarly, there is an index k such that w_j is a monomial multiple of z_k. The transitivity of the divisibility order on the monomial set $[\![R]\!]$ implies that z_i is a multiple of z_k; that is, z_i is a monomial multiple of z_k. Since the generating sequence $z_1, \ldots, z_m$ is irredundant, it follows that $i = k$. It follows that $z_i \big| w_j$ and $w_j \big| z_i$. The fact that the divisibility order on $[\![R]\!]$ is antisymmetric implies $z_i = w_j$.

In summary, we see that for each index $i = 1, \ldots, m$ there exists an index $j = \sigma(i)$ such that $z_i = w_j = w_{\sigma(i)}$. Since the z_i are distinct and the w_j are distinct, we conclude that the function $\sigma\colon \{1, \ldots, m\} \to \{1, \ldots, n\}$ is 1-1. By symmetry, there is a 1-1 function $\delta\colon \{1, \ldots, n\} \to \{1, \ldots, m\}$ such that $w_i = z_{\delta(i)}$ for $i = 1, \ldots, n$. It follows that $m \leqslant n \leqslant m$ and so $m = n$. Furthermore, since σ is 1-1 and $m = n$, the pigeon-hole principle implies that σ is also onto. This is the desired conclusion. $\square$

Here is an algorithm for finding an irredundant monomial generating sequence.

ALGORITHM 1.3.7. Set $R = A[X_1, \ldots, X_d]$. Fix monomials $z_1, \ldots, z_m \in [\![R]\!]$ and set $J = (z_1, \ldots, z_m)R$. We assume that $m \geqslant 1$.

Step 1. Check whether the generating sequence $z_1, \ldots, z_m$ is irredundant using the definition.

Step 1a. If, for all indices i and j such that $i \neq j$, we have $z_j \notin (z_i)R$, then the generating sequence is irredundant; in this case, the algorithm terminates.

Step 1b. If there exist indices i and j such that $i \neq j$ and $z_j \in (z_i)R$, then the generating sequence is redundant; in this case, continue to Step 2.

Step 2. Reduce the generating sequence by removing the generator that causes the redundancy in the generating sequence. By assumption, there exist indices i and j such that $i \neq j$ and $z_j \in (z_i)R$. Reorder the indices to assume without loss of generality that $j = m$. Thus, we have $i < m$ and $z_m \in (z_i)R$. It follows that $J = (z_1, \ldots, z_m)R = (z_1, \ldots, z_{m-1})R$. Now apply Step 1 to the new list of monomials $z_1, \ldots, z_{m-1}$.

The algorithm will terminate in at most $m - 1$ steps because one can remove at most $m - 1$ monomials from the list and still form a non-zero ideal.

EXAMPLE 1.3.8. Set $R = A[X, Y]$. Using Algorithm 1.3.7, one finds that the sequence X^3, X^2Y, Y^5 is an irredundant monomial generating sequence for the ideal $(X^3, X^2Y, X^2Y^2, Y^5)R$.

Here is a proposition that shows how to find an irredundant monomial generating sequence in one shot.

PROPOSITION 1.3.9. *Set* $R = A[X_1, \ldots, X_d]$. *Fix a non-empty set of monomials* $S \subseteq [\![R]\!]$ *and set* $J = (S)R$. *For each* $z \in S$, *write* $z = \underline{X}^{\underline{n}_z}$ *with* $\underline{n}_z \in \mathbb{N}^d$. *Set* $\Delta = \{\underline{n}_z \mid z \in S\} \subseteq \mathbb{N}^d$ *and consider the order* $\succcurlyeq$ *on* $\mathbb{N}^d$ *from Definition A.7.8. Let* Δ' *denote the set of minimal elements of* Δ *under this order.*

(a) *Then* $S' = \{z \mid \underline{n}_z \in \Delta'\}$ *is an irredundant monomial generating set for* J.
(b) *The set* Δ' *is finite.*

PROOF. Note: the set Δ has minimal elements by the Well-Ordering Axiom.

(a) The minimality of the elements of Δ' implies that for each $\underline{n}_z \in \Delta$, there is an element $\underline{n}_w \in \Delta'$ such that $\underline{n}_z \succcurlyeq \underline{n}_w$; it follows that $z \in (w)R$. From this, we conclude that

$$J = (S)R \subseteq (\{w \in S \mid \underline{n}_w \in \Delta'\})R \subseteq (S)R = J$$

so $J = (\{w \in S \mid \underline{n}_w \in \Delta'\})R = (S')R$.

For distinct elements $w, z \in S'$ we have $\underline{n}_w \not\succcurlyeq \underline{n}_z$ since $\underline{n}_w$ and $\underline{n}_z$ are both minimal among the elements of Δ and they are distinct. It follows that $w \notin (z)R$.

Theorem 1.3.6(a) implies that S' contains an irredundant monomial generating sequence $s_1, \ldots, s_n \in S'$ for J. We claim that $S' = \{s_1, \ldots, s_n\}$. (From this, it follows that S' is an irredundant monomial generating set for J.) We know that $\{s_1, \ldots, s_n\} \subseteq S'$, so suppose by way of contradiction that $\{s_1, \ldots, s_n\} \subsetneq S'$, and let $s \in S' \smallsetminus \{s_1, \ldots, s_n\}$. It follows that $s \in J = (s_1, \ldots, s_n)R$ so $s \in (s_i)R$ for some i by Theorem 1.1.8. The previous paragraph implies that $s = s_i \in \{s_1, \ldots, s_n\}$, a contradiction.

(b) The set Δ' is in bijection with S', which is finite. □

Exercises.

*EXERCISE 1.3.10. Set $R = A[X_1, \ldots, X_d]$. Let $I_1, \ldots, I_n$ be monomial ideals in R and set $\mathfrak{X} = (X_1, \ldots, X_d)R$.

(a) Prove that the product $I_1 \cdots I_n$ is a monomial ideal.
(b) Prove that if $\operatorname{rad}(I_j) = \operatorname{rad}(\mathfrak{X})$ for $j = 1, \ldots, n$, then $\operatorname{rad}(I_1 \cdots I_n) = \operatorname{rad}(\mathfrak{X})$.
(c) Prove that if $I_j \neq R$ for $j = 1, \ldots, n$ and $\operatorname{rad}(I_1 \cdots I_n) = \operatorname{rad}(\mathfrak{X})$, then $\operatorname{rad}(I_j) = \operatorname{rad}(\mathfrak{X})$ for $j = 1, \ldots, n$.
(d) Prove that $[\![I_1 \cdots I_n]\!] = \{z_1 \cdots z_n \mid z_1 \in [\![I_1]\!], \ldots, z_n \in [\![I_n]\!]\}$.

(This exercise is used in the proof of Theorem 6.2.1.)

*EXERCISE 1.3.11. Set $R = A[X_1, \ldots, X_d]$. Let $I_1, \ldots, I_n$ be monomial ideals in R and set $\mathfrak{X} = (X_1, \ldots, X_d)R$.

(a) Prove that the sum $I_1 + \cdots + I_n$ is a monomial ideal.
(b) Prove that if $\operatorname{rad}(I_j) = \operatorname{rad}(\mathfrak{X})$ for $j = 1, \ldots, n$, then $\operatorname{rad}(I_1 + \cdots + I_n) = \operatorname{rad}(\mathfrak{X})$.
(c) Prove or give a counter-example for the following: if $\operatorname{rad}(I_1 + \cdots + I_n) = \operatorname{rad}(\mathfrak{X})$, then $\operatorname{rad}(I_j) = \operatorname{rad}(\mathfrak{X})$ for $j = 1, \ldots, n$.
(d) Prove that $[\![I_1 + \cdots + I_n]\!] = [\![I_1]\!] \cup \cdots \cup [\![I_n]\!]$.
(e) Prove that $\Gamma(I_1 + \cdots + I_n) = \Gamma(I_1) \cup \cdots \cup \Gamma(I_n)$.

(This exercise is used in a number of proofs.)

EXERCISE 1.3.12. Set $R = A[X_1, \dots, X_d]$. Find irredundant monomial generating sequences for the following monomial ideals and justify your answers:

(a) $I = (X_1^5, X_1X_2, X_1^2X_2^3, X_2^3)R$
(b) $I = (X_1X_2^2X_3^3, X_1X_3, X_2X_4, X_1^3X_2^2X_4X_5)R$

EXERCISE 1.3.13. Set $R = A[X_1, \dots, X_d]$. Let I be a monomial ideal of R, and set $\mathfrak{X} = (X_1, \dots, X_d)R$. Prove that $\operatorname{rad}(I) = \operatorname{rad}(\mathfrak{X})$ if and only if an irredundant monomial generating sequence for I contains a positive power of each variable.

Generators of Monomial Ideals in Macaulay2.

In this tutorial, we show how to find an irredundant generating sequence for a monomial ideal. The commands are `trim`, `mingens`, and `first entries mingens`, depending on the output desired. The command `trim` outputs the same ideal, but generated by an irredundant generating sequence. The command `mingens` outputs an irredundant generating sequence as a matrix. And `first entries mingens` outputs an irredundant generating sequence as a list; one can also use the command `_*` here.

```
i1 : R=ZZ/101[x,y,z]

o1 = R

o1 : PolynomialRing

i2 : I=ideal(x,y,z,x^2*y,y^2*z)

                          2    2
o2 = ideal (x, y, z, x y, y z)

o2 : Ideal of R

i3 : trim I

o3 = ideal (z, y, x)

o3 : Ideal of R

i4 : mingens I

o4 = | z y x |

              1       3
o4 : Matrix R  <--- R

i5 : first entries mingens I

o5 = {z, y, x}

o5 : List
```

```
i6 : I_*

                 2    2
o6 = {x, y, z, x y, y z}

o6 : List

i7 : (trim I)_*

o7 = {z, y, x}

o7 : List
```

Exercises.

EXERCISE 1.3.14. Set $R = \mathbb{Z}_{101}[X_1, \ldots, X_5]$, and use Macaulay2 to find irredundant generating sequences for the ideals in Example 1.3.8 and Exercise 1.3.12.

EXERCISE 1.3.15. Set $R = \mathbb{Z}_{101}[X_1, \ldots, X_5]$ and $I = (X_1^5, X_1X_2, X_1^2X_2^3, X_2^3)R$ and $I = (X_1X_2^2X_3^3, X_1X_3, X_2X_4, X_1^3X_2^2X_4X_5)R$.

(a) Use Macaulay2 to find irredundant generating sequences for $I + J$, IJ and I^3.
(b) Use Macaulay2 to show that $I \bigcap J$, $(R :_I J)$ and $\operatorname{rad}(I)$ are monomial ideals.

1.4. Noetherian Rings (optional)

In this section, R is a non-zero commutative ring with identity.

In the previous section, we saw that every monomial ideal in the polynomial ring $A[X_1, \ldots, X_d]$ is finitely generated. This condition can fail for more general ideals. Specifically, there exist rings with ideals that are not finitely generated; see Example 1.4.4(d). This motivates the study of noetherian rings, which are defined after Theorem 1.4.2. We begin with a definition that echoes Theorem 1.3.3(a).

DEFINITION 1.4.1. We say that an ascending chain $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ of ideals in R *stabilizes* if there is a positive integer n such that $I_n = I_{n+1} = I_{n+2} = \cdots$. The ring R satisfies the *ascending chain condition* (sometimes abbreviated ACC) for ideals if every ascending chain of ideals in R stabilizes.

Compare the next result with Theorems 1.3.1 and 1.3.3.

THEOREM 1.4.2. *The following conditions are equivalent:*

(i) *every ideal of R is finitely generated;*
(ii) *every non-empty set of ideals of R contains a maximal element; and*
(iii) *R satisfies the ascending chain condition for ideals.*

PROOF. (iii) $\Longrightarrow$ (ii): We argue by contradiction. Assume that R satisfies the ascending chain condition for ideals, and suppose that R admits a non-empty set Σ of ideals with no maximal element. Let $I_1 \in \Sigma$. Since Σ has no maximal element, there is an element $I_2 \in \Sigma$ such that $I_1 \subsetneq I_2$. Since Σ has no maximal element, there is an element $I_3 \in \Sigma$ such that $I_2 \subsetneq I_3$. Inductively, this process yields an ascending chain $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$. By construction, this chain does not stabilize;

this contradicts the assumption that R satisfies the ascending chain condition for ideals.

(ii) $\Longrightarrow$ (i): Assume that every non-empty set of ideals of R contains a maximal element. Let I be an ideal of R, and let

$$\Sigma = \{\text{finitely generated ideals } J \subseteq R \mid J \subseteq I\}.$$

Note that $\Sigma \neq \emptyset$ since $0 = (0_R)R \in \Sigma$. By assumption, the set Σ has a maximal element J. Then $J \subseteq I$ and J is finitely generated.

We claim that $J = I$. By way of contradiction, suppose that $J \subsetneq I$ and let $a \in I \smallsetminus J$. Since J is finitely generated, so is $J + aR$. Furthermore, since $a \in I$, we have $aR \subseteq I$, so the assumption $J \subseteq I$ implies that $J + aR \subseteq I$. Furthermore, we have $a \in aR \subseteq J + aR$, so the condition $a \notin J$ implies that $J + aR$ is an ideal in Σ that properly contains J. This contradicts the maximality of J. Hence, we have $J = I$ and so I is finitely generated.

(i) $\Longrightarrow$ (iii): Assume that every ideal of R is finitely generated. Consider an ascending chain $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ of ideals in R, and set $I = \cup_{j=1}^{\infty} I_j$. Fact A.3.4(c) implies that I is an ideal of R. Our assumption implies that $I = (r_1, \ldots, r_k)R$ for some elements $r_i \in R$. For $i = 1, \ldots, k$ we have $r_i \in I = \cup_{j=1}^{\infty} I_j$, and so there exists a positive integer n_i such that $r_i \in I_{n_i}$. With $n = \max\{n_1, \ldots, n_k\}$ we have $r_i \in I_{n_i} \subseteq I_n$ and so $I = (r_1, \ldots, r_k)R \subseteq I_n$. Hence, for each $m \geqslant 0$, we have

$$I_{n+m} \subseteq I \subseteq I_n \subseteq I_{n+m}$$

and so $I_{n+m} = I_n$. That is, the chain stabilizes, as desired. $\square$

Definition 1.4.3. The ring R is *noetherian* if it satisfies the equivalent conditions of Theorem 1.4.2.

Example 1.4.4. (a) The ring $\mathbb{Z}$ is noetherian because every ideal is principal; see Exercise A.3.16.

(b) Every finite ring is noetherian. In particular, the ring $\mathbb{Z}_n$ is noetherian.

(c) Every field k is noetherian since its only ideals are $0 = 0k$ and $k = 1_k k$. In particular, the rings $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are noetherian.

(d) Given a non-zero commutative ring A with identity, the polynomial ring $R = A[X_1, X_2, X_3, \ldots]$ in infinitely many variables is not noetherian, since the ideal $(X_1, X_2, X_3, \ldots)R$ is not finitely generated. Also, the chain of ideals $(X_1)R \subsetneq (X_1, X_2)R \subsetneq (X_1, X_2, X_3)R \subsetneq \cdots$ never stabilizes.

(e) The ring $R = \mathrm{C}(\mathbb{R})$ of continuous functions is not noetherian. Indeed, for each $n \in \mathbb{N}$ define

$$I_n = \{f \in R \mid f(m) = 0 \text{ for all } k \in \mathbb{N} \text{ such that } k \geqslant n\}.$$

Then the chain of ideals $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots$ never stabilizes.

Here is the Hilbert Basis Theorem. Compare it with Theorem 1.3.1. In the language of the 1890's, the conclusion of this result says that every ideal of $A[X]$ has a finite basis, hence the name Hilbert Basis Theorem. In today's language, we say "finite generating set" instead of "finite basis".

Theorem 1.4.5 (Hilbert Basis Theorem). *Let A be a commutative ring with identity. If A is noetherian, then so is $A[X]$.*

Proof. Let I be an ideal of $A[X]$. We need to show that I is finitely generated. Assume without loss of generality that $I \neq 0$. Let

$$J = \{a \in A \mid a \text{ is the leading coefficient of some } f \in I\} \cup \{0_A\}.$$

The set J is an ideal of A. The fact that A is noetherian implies that there exist $a_1, \ldots, a_n \in J$ such that $J = (a_1, \ldots, a_n)A$. Assume without loss of generality that each a_i is non-zero. By definition, for each $i = 1, \ldots, n$ there is a polynomial $f_i \in I$ such that a_i is the leading coefficient of f_i. By multiplying each polynomial f_i by a power of X, we may assume that the polynomials $f_1, \ldots, f_n$ have the same degree; let N denote this common degree.

For $d = 0, 1, \ldots, N-1$ let

$$J_d = \{a \in A \mid a \text{ is the leading coefficient of some } f \in I \text{ of degree } d\} \cup \{0_A\}.$$

The set J_d is an ideal of A. The fact that A is noetherian implies that there exist $b_{d,1}, \ldots, b_{d,n_d} \in J_d$ such that $J = (b_{d,1}, \ldots, b_{d,n_d})A$. For each d such that $J_d \neq 0$, we assume without loss of generality that each $b_{d,i}$ is non-zero. By definition, for each d such that $J_d \neq 0$ and for each $i = 1, \ldots, n_d$ there is a polynomial $g_{d,i} \in I$ such that $b_{d,i}$ is the leading coefficient of $g_{d,i}$. For each d such that $J_d = 0$, we set $n_d = 1$ and $b_{d,1} = 0 = g_{d,1}$.

Let I' be the ideal of $A[X]$ generated by the polynomials f_i and $g_{d,i}$:

$$I' = (\{f_i \mid i = 1, \ldots, n\} \cup \{g_{d,i} \mid d = 0, \ldots, N-1; i = 1, \ldots, n_d\})\, A[X].$$

By construction I' is a finitely generated ideal of $A[X]$. Since each $f_i, g_{d,i} \in I$, we have $I' \subseteq I$.

Claim: $I' = I$. (Once the claim is established, we conclude that I is finitely generated, completing the proof.) Suppose by way of contradiction that $I' \subsetneq I$ Let f be a polynomial of minimal degree in the compliment $I \smallsetminus I'$, Let e denote the degree of f and let a be the leading coefficient of f.

Suppose that $e \geqslant N$. Since $f \in I$, we have $a \in J$, and so there exist elements $r_1, \ldots, r_n \in A$ such that $a = \sum_{i=1}^n r_i a_i$. For $i = 1, \ldots, n$ the polynomial $r_i X^{e-N} f_i$ is an element of I' with degree at most e. Also, the coefficient of X^e in the polynomial $r_i X^{e-N} f_i$ is $r_i a_i$. Since each polynomial $r_i X^{e-N} f_i$ is in I', we have $\sum_{i=1}^n r_i X^{e-N} f_i \in I'$. Exercise A.2.13 implies that $\sum_{i=1}^n r_i X^{e-N} f_i$ has degree e and leading coefficient $\sum_{i=1}^n r_i a_i$. Fact A.3.2 implies that $f - \sum_{i=1}^n r_i X^{e-N} f_i$ is in $I \smallsetminus I'$. Furthermore, the polynomial $f - \sum_{i=1}^n r_i X^{e-N} f_i$ has degree strictly less than e. This contradicts the minimality of e.

Hence, we have $e < N$. It follows that $a \in J_e$ and so there exist elements $s_1, \ldots, s_{n_e}$ such that $a = \sum_{i=1}^{n_e} s_i b_{e,i}$. The polynomial $f - \sum_{i=1}^{n_e} s_i g_{e,i}$ is in $I \smallsetminus I'$ and has degree strictly less than e. Again, this contradicts the minimality of e. It follows that $I' = I$, as claimed. □

Corollary 1.4.6. *Let A be a commutative ring with identity. If A is noetherian, then so is $A[X_1, \ldots, X_d]$.*

Proof. Argue by induction on d using Theorem 1.4.5. □

Exercises.

Exercise 1.4.7. Let I be an ideal of R, generated by a set $S \subset R$. Prove that if R is noetherian, then I is generated by a finite subset of elements of S.

EXERCISE 1.4.8. Let A be a commutative ring with identity. Prove that the following conditions are equivalent:

(i) the ring A is noetherian;
(ii) for each integer $d \geqslant 1$ the polynomial ring $A[X_1, \ldots, X_d]$ in d variables is noetherian; and
(iii) there is an integer $d \geqslant 1$ such that the polynomial ring $A[X_1, \ldots, X_d]$ in d variables is noetherian.

EXERCISE 1.4.9. Set $R = \{a_0 + Xf(X,Y) \in \mathbb{Q}[X,Y] \mid f(X,Y) \in \mathbb{Q}[X,Y]\}$ and $I = \{Xf(X,Y) \in R \mid f(X,Y) \in \mathbb{Q}[X,Y]\}$.

(a) Prove that R is a commutative ring with identity under the usual polynomial addition and multiplication. (That is, prove that R is a subring of $\mathbb{Q}[X,Y]$.)
(b) Prove that I is an ideal of R.
(c) Prove that R is not noetherian by showing that the ideal I is not finitely generated.

1.5. Exploration: Counting Monomials

In this section, A is a commutative ring with identity.

Here we outline some fundamental combinatorial aspects of monomials in polynomial rings.

EXERCISE 1.5.1. Set $R = A[X]$.

(a) For each integer $n \geqslant 0$, how many monomials of degree n are in R?
(b) For each integer $n \geqslant 0$, how many monomials of degree at most n are in R?

EXERCISE 1.5.2. Set $R = A[X,Y]$.

(a) For each integer $n \geqslant 0$, how many monomials of degree n are in R? (Hint: Write down how many there are for n =0–3. Make an educated guess about the formula for arbitrary n, then prove it.)
(b) Compare the answer from part (a) with the answer to Exercise 1.5.1(b). Explain the similarity.
(c) For each integer $n \geqslant 0$, how many monomials of degree at most n are in R? Interpret your answer as a binomial coefficient.

EXERCISE 1.5.3. Repeat Exercise 1.5.2 for the ring $R = A[X,Y,Z]$, interpreting each of your answers as a binomial coefficient.

EXERCISE 1.5.4. Given your answers to Exercises 1.5.1–1.5.3, make a conjecture (that is, an educated guess) about the number of monomials of degree n in the ring $R = A[X_1, \ldots, X_d]$. Make a conjecture about the number of monomials of degree at most n in R. Prove your conjectures by induction on d.

EXERCISE 1.5.5. Here is another way to prove one of the formulas from Exercise 1.5.4. Set $R = A[X_1, \ldots, X_d]$. Each monomial $X_1^{a_1} \cdots X_d^{a_d} \in R$ of degree k corresponds to a binary number with exactly k ones and $d-1$ zeroes:

$$\underbrace{1\,1\,1\,\ldots\,1}_{a_1 \text{ ones}}0\underbrace{1\,1\,1\,\ldots\,1}_{a_2 \text{ ones}}0\cdots0\underbrace{1\,1\,1\,\ldots\,1}_{a_d \text{ ones}}.$$

(a) How many digits does each of these binary numbers have?

(b) Each of these binary numbers is determined by the placement of the $d - 1$ zeroes. Use this to count the total number of these binary numbers.
(c) Use part (b) to count the number of monomials of degree n in R.
(d) Can you find a similar argument for counting the number of monomials of degree at most n in R?

Counting Monomials in Macaulay2.

In this tutorial, we show how to use the `basis` command to find the numbers of monomials of a certain degree, or range of degrees. We also introduce the command `numgens`, which gives the number of generators of an ideal. We make use of the last output command `oo`, and introduce comments in the Macaulay2 code using `--`.

```
i1 : R = ZZ/41[x, y, z]

o1 = R

o1 : PolynomialRing

i2 : basis(2, R) -- Gives degree 2 monomials, in matrix form

o2 = | x2 xy xz y2 yz z2 |

             1       6
o2 : Matrix R  <--- R

i3 : ideal oo -- Convert the image of the matrix to an ideal

             2              2        2
o3 = ideal (x , x*y, x*z, y , y*z, z )

o3 : Ideal of R

i4 : numgens oo -- Count the number of generators

o4 = 6

i5 : basis(1, 3, R)

o5 = |x x2 x3 x2y x2z xy xy2 xyz xz xz2 y y2 y3 y2z yz yz2 z z2 z3|

             1       19
o5 : Matrix R  <--- R

i6 : numgens ideal basis(1, R) +
     numgens ideal basis(2, R) +
     numgens ideal basis(3, R) ==
     numgens ideal basis(1, 3, R) -- Testing a basic equality

o6 = true
```

Exercises.

EXERCISE 1.5.6. With $A = \mathbb{Z}_{41}$, use Macaulay2 to test your formulas from the exercises above for a few values of n. Be sure to use the `binomial` command as well as the equality test `==`.

1.6. Exploration: Numbers of Generators

In this section, A is a non-zero commutative ring with identity.

This section presents a guided tour of some of the numerical properties of irredundant generating sequences.

DEFINITION 1.6.1. Set $R = A[X_1, \ldots, X_d]$. For each monomial ideal $I \subseteq R$, let $\nu_R(J)$ denote the number of elements in an irredundant monomial generating sequence for I.

EXAMPLE 1.6.2. Set $R = A[X, Y]$. Example 1.3.8 shows that X^3, X^2Y, Y^5 is an irredundant monomial generating sequence for $I = (X^3, X^2Y, X^2Y^2, Y^5)R$, so we have $\nu_R(I) = 3$.

Exercises.

EXERCISE 1.6.3. Compute $\nu_R(I)$ for the monomial ideals from Exercise 1.3.12.

EXERCISE 1.6.4. Set $R = A[X_1, \ldots, X_d]$ and $\mathfrak{X} = (X_1, \ldots, X_d)R$. Compute $\nu_R(\mathfrak{X}^n)$ for each integer $n \geqslant 0$. (Hint: Exercise 1.5.4 or 1.5.5 may be helpful.)

EXERCISE 1.6.5. Set $R = A[X_1, \ldots, X_d]$ and consider $I = (X_{i_1}, \ldots, X_{i_t})R$ where $1 \leqslant t \leqslant d$ and $1 \leqslant i_1 < \cdots < i_t \leqslant d$. Compute $\nu_R(I^n)$ for each integer $n \geqslant 0$.

EXERCISE 1.6.6. Set $R = A[X_1, \ldots, X_d]$ and $J = (X_{i_1}^{e_1}, \ldots, X_{i_t}^{e_t})R$ where $1 \leqslant t \leqslant d$ and $1 \leqslant i_1 < \cdots < i_t \leqslant d$ and $e_1, \ldots, e_t \geqslant 1$. Compute $\nu_R(J^n)$ for each integer $n \geqslant 0$.

EXERCISE 1.6.7. Set $R = A[X_1, \ldots, X_d]$. Fix monomials $f_1, \ldots, f_t \in [\![R]\!]$, and consider the ideal $K = (f_1, \ldots, f_t)R$. Compute an upper bound for $\nu_R(K^n)$ in terms of n and t. (Hint: The computation from Exercise 1.6.5 may be helpful.)

Numbers of Generators in Macaulay2.
In this tutorial, we show how to compute $\nu_R(I)$ where I is a monomial ideal. The relevant command is `numgens` with the help of `trim`. Note that the command `numgens I` does not give $\nu_R(I)$ unless I has been trimmed.

```
i1 : R=ZZ/101[x,y,z]

o1 = R

o1 : PolynomialRing

i2 : I=ideal(x,y,z,x*y,y*z)

o2 = ideal (x, y, z, x*y, y*z)
```

```
o2 : Ideal of R

i3 : numgens I

o3 = 5

i4 : numgens trim I

o4 = 3

i5 : J=trim I

o5 = ideal (z, y, x)

o5 : Ideal of R

i6 : numgens J

o6 = 3
```

Exercises.

EXERCISE 1.6.8. Set $A = \mathbb{Z}_{101}$, and use Macaulay2 to compute $\nu_R(I)$ for the ideals in Example 1.6.2 and Exercise 1.3.12.

EXERCISE 1.6.9. Set $A = \mathbb{Z}_{101}$, and use Macaulay2 to verify your answer to Exercise 1.6.4 in the following cases:
(a) $d = 2$ and $n = 1, \ldots, 5$, and
(b) $d = 3$ and $n = 1, \ldots, 5$.

EXERCISE 1.6.10. Set $R = \mathbb{Z}_{101}[X_1, \ldots, X_d]$ and $K = \mathfrak{X}^2$ where $\mathfrak{X}$ is the ideal $(X_1, \ldots, X_d)R$. Use Macaulay2 to calculate $\nu_R(I^n)$ in the following cases:
(a) $d = 2$ and $n = 1, \ldots, 5$, and
(b) $d = 3$ and $n = 1, \ldots, 5$.
How close are these values to the upper bound you found in Exercise 1.6.7?

Conclusion

Include some history here. Talk about some of the literature from this area. Who is Noether?

"This is not mathematics, it is theology." This quote is attributed to the mathematician Paul Gordan, circa 1890, in response to Hilbert's proof of Theorem 1.4.5. Gordan was apparently dismayed by the non-constructive nature of the proof. (The authors of this text do not necessarily agree with Gordan's assessment.)

CHAPTER 2

Operations on Monomial Ideals

In this chapter we apply some of the operations of Chapter A to monomial ideals. We have already seen this theme for sums and products in Exercises 1.3.10 and 1.3.11. In Sections 2.1 and 2.4 we show, for instance, that intersections and colons of monomial ideals are monomial ideals. Since we are interested in decomposing monomial ideals into intersections, it is important to know that the class of monomial ideals is closed under intersections.

On the other hand, the radical of a monomial ideal need not be a monomial ideal, so we remedy this by introducing the monomial radical of a monomial ideal in Section 2.3. Other constructions we consider are bracket powers and generalized bracket powers of monomial ideals, in Sections 2.5 and 2.6. We show that generating sequences for intersections of monomial ideals are described using least common multiples. This motivates Section 2.2 on unique factorization domains, which are rings where least common multiples are guaranteed to exist.

2.1. Intersections of Monomial Ideals

In this section, A is a non-zero commutative ring with identity.

Given set of ideals in a commutative ring R, Fact A.3.4(a) show that their intersection is also an ideal of R. In other words, the set of ideals of R is closed under intersections. In the next result, we show that the same is true of the set of monomial ideals in a polynomial ring over A. Following this, we show how generators of the ideals being intersected yield generators of the intersection.

THEOREM 2.1.1. *Set $R = A[X_1, \ldots, X_d]$. If $I_1, \ldots, I_n$ are monomial ideals of R, then the intersection $I_1 \bigcap \cdots \bigcap I_n$ is generated by the set of monomials in $I_1 \bigcap \cdots \bigcap I_n$. In particular, the ideal $I_1 \bigcap \cdots \bigcap I_n$ is a monomial ideal of R and $[\![I_1 \bigcap \cdots \bigcap I_n]\!] = [\![I_1]\!] \bigcap \cdots \bigcap [\![I_n]\!]$.*

PROOF. Let S denote the set of monomials $\bigcap_{j=1}^n [\![I_j]\!]$ and set $J = (S)R$. By construction J is a monomial ideal such that $J \subseteq \bigcap_{j=1}^n I_j$, since $S \subseteq \bigcap_{j=1}^n I_j$. We claim that $J = \bigcap_{j=1}^n I_j$. To show this, fix an element $f \in \bigcap_{j=1}^n I_j$ and write $f = \sum_{\underline{n}\in\mathbb{N}^d}^{\text{finite}} a_{\underline{n}} \underline{X}^{\underline{n}}$. For $j = 1, \ldots, n$ we have $f \in I_j$. Hence, Exercise 1.1.16 implies that if $a_{\underline{n}} \neq 0$, then $\underline{X}^{\underline{n}} \in [\![I_j]\!]$ for each j, that is, if $a_{\underline{n}} \neq 0$, then $\underline{X}^{\underline{n}} \in \bigcap_{j=1}^n [\![I_j]\!] = S$. Hence, we have $f \in (S)R = J$, as desired.

The previous paragraph shows that $I_1 \bigcap \cdots \bigcap I_n$ is a monomial ideal of R and is generated by the monomial set $\bigcap_{j=1}^n [\![I_j]\!]$. We complete the proof with the following computation:

$$[\![\bigcap_{j=1}^{n} I_j]\!] = \left(\bigcap_{j=1}^{n} I_j\right) \bigcap [\![R]\!] = \bigcap_{j=1}^{n} (I_j \bigcap [\![R]\!]) = \bigcap_{j=1}^{n} [\![I_j]\!]. \quad \square$$

REMARK 2.1.2. Set $R = A[X_1, \ldots, X_d]$. Let $I_1, \ldots, I_n$ be monomial ideals of R. The fact that the intersection $I_1 \bigcap \cdots \bigcap I_n$ is a monomial ideal such that $[\![I_1 \bigcap \cdots \bigcap I_n]\!] = [\![I_1]\!] \bigcap \cdots \bigcap [\![I_n]\!]$ implies $\Gamma(I_1 \bigcap \cdots \bigcap I_n) = \Gamma(I_1) \bigcap \cdots \bigcap \Gamma(I_n)$.

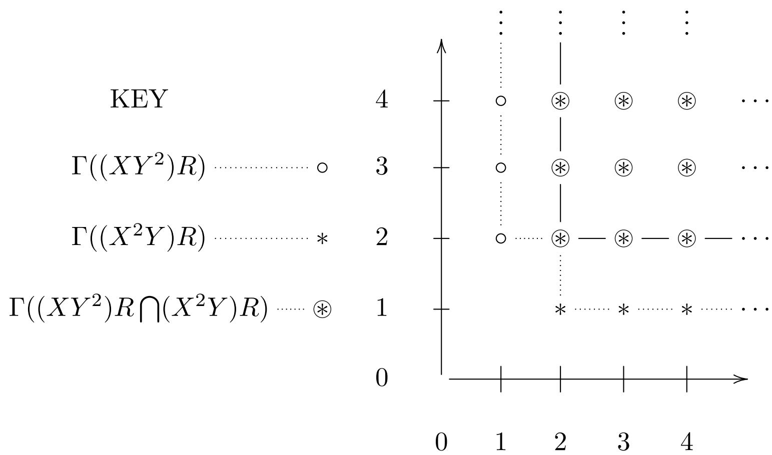
Next we show how to find a monomial generating sequence for an intersection of monomial ideals.

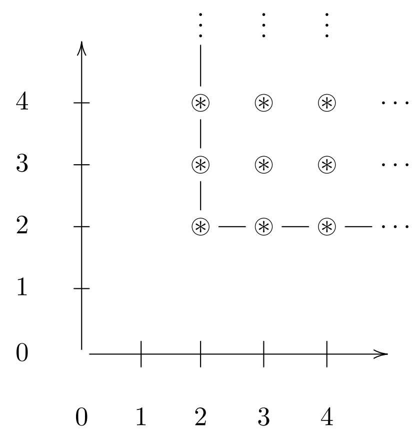
DEFINITION 2.1.3. Set $R = A[X_1, \ldots, X_d]$. Let $f = \underline{X}^{\underline{m}}$ and $g = \underline{X}^{\underline{n}}$ for some $\underline{m}, \underline{n} \in \mathbb{N}^d$. For $i = 1, \ldots, d$ set $p_i = \max\{m_i, n_i\}$. Define the *least common multiple* of f and g to be the monomial $\operatorname{lcm}(f, g) = \underline{X}^{\underline{p}}$.

For example, consider $R = A[X, Y, Z]$. We compute the least common multiple of $f = XY^4Z^8$ and $g = X^3Z^5$. In the notation of Definition 2.1.3, we have $\underline{m} = (1, 4, 8)$ and $\underline{n} = (3, 0, 5)$, and thus $\underline{p} = (3, 4, 8)$. This yields $\operatorname{lcm}(XY^4Z^8, X^3Z^5) = X^3Y^4Z^8$.

Next, we work in $R = A[X, Y]$ to motivate the connection between intersections of monomial ideals and least common multiples. We compute the ideal

$(XY^2)R\bigcap(X^2Y)R$. Because of Theorem 2.1.1 and Remark 2.1.2, we need to compute the intersection $\Gamma((XY^2)R\bigcap(X^2Y)R) = \Gamma((XY^2)R)\bigcap\Gamma((X^2Y)R)$.





From this, we see that $(XY^2)R\bigcap(X^2Y)R = (X^2Y^2)R = (\mathrm{lcm}(XY^2, X^2Y))R$. In words, the intersection of the principal ideals generated by XY^2 and X^2Y is principal and is generated by $\mathrm{lcm}(XY^2, X^2Y)$. The next result shows that this is true for any two principal monomial ideals. The subsequent proposition deals with the non-principal case.

Lemma 2.1.4. *Set $R = A[X_1, \ldots, X_d]$. For monomials $f, g \in [\![R]\!]$, there is an equality $(f)R\bigcap(g)R = (\mathrm{lcm}(f,g))R$.*

Proof. Exercise. Hint: apply Lemma 1.1.7 repeatedly. □

Proposition 2.1.5. *Set $R = A[X_1, \ldots, X_d]$. Suppose I is generated by the set of monomials $\{f_1, \ldots, f_m\}$ and J is generated by the set of monomials $\{g_1, \ldots, g_n\}$. Then $I\bigcap J$ is generated by the set of monomials*

$$\{\mathrm{lcm}(f_i, g_j) \mid 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n\}.$$

Proof. We begin by setting

$$K = (\{\mathrm{lcm}(f_i, g_j) \mid 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n\})R.$$

This is a monomial ideal in R since each element $\operatorname{lcm}(f_i, g_j)$ is a monomial in R.

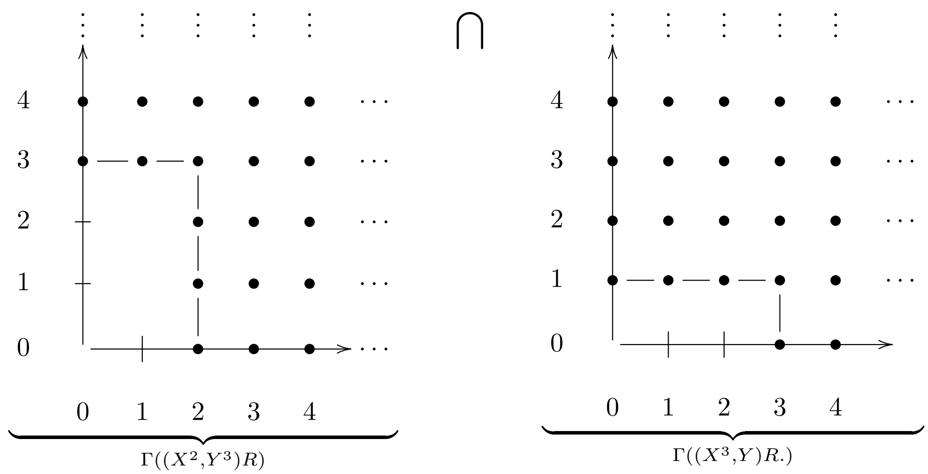
For the containment $I \bigcap J \subseteq K$, it suffices to show that every monomial $z \in [\![I \bigcap J]\!]$ is in K. The element z is a monomial in $I = (f_1, \ldots, f_m)R$ so Theorem 1.1.8 implies that $z \in (f_i)R$ for some index i. Similarly, the condition $z \in J = (g_1, \ldots, g_n)R$ implies that $z \in (g_j)R$ for some index j. Hence, Lemma 2.1.4 yields $z \in (f_i)R \bigcap (g_j)R = (\operatorname{lcm}(f_i, g_j))R \subseteq K$ as desired.

For the containment $I \bigcap J \supseteq K$, it suffices to show that each monomial generator $\operatorname{lcm}(f_i, g_j)$ of K is in $I \bigcap J$. Theorem 1.1.8 implies the equality in the next sequence

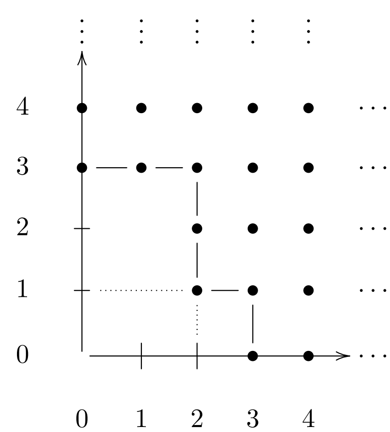
$$\operatorname{lcm}(f_i, g_j) \in (\operatorname{lcm}(f_i, g_j))R = (f_i)R \bigcap (g_j)R \subseteq I \bigcap J$$

while the rest of the sequence are standard. This gives the desired conclusion. $\square$

EXAMPLE 2.1.6. Set $R = A[X, Y]$. We compute a generating sequence for the ideal $I = (X^2, Y^3)R \bigcap (X^3, Y)R$:



Theorem 2.1.1 implies that $[\![I]\!] = [\![(X^2, Y^3)R]\!] \bigcap [\![(X^3, Y)R]\!]$, so the graph of I is the following.



Using Proposition 1.3.9 and a visual inspection of the graph, we conclude that an irredundant monomial generating sequence for I is Y^3, X^2Y, X^3.

We now use Proposition 2.1.5 and Algorithm 1.3.7 to find an irredundant monomial generating sequence for I. In the notation of Proposition 2.1.5, we have $f_1 = X^2$, $f_2 = Y^3$, $g_1 = X^3$ and $g_2 = Y$. We compute the relevant LCM's:

$$\begin{aligned} \operatorname{lcm}(f_1, g_1) &= X^3 & \qquad \operatorname{lcm}(f_2, g_1) &= X^3Y^3 \\ \operatorname{lcm}(f_1, g_2) &= X^2Y & \qquad \operatorname{lcm}(f_2, g_2) &= Y^3. \end{aligned}$$

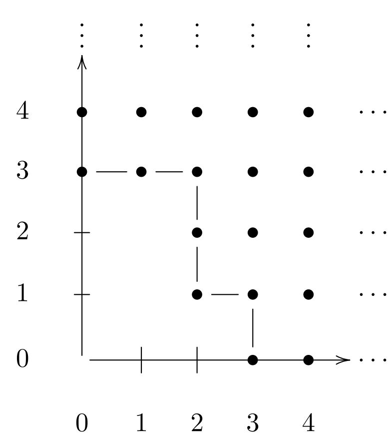
Proposition 2.1.5 implies that the sequence X^3, X^3Y^3, X^2Y, Y^3 generates I.

Now we use Algorithm 1.3.7 to find an irredundant monomial generating sequence for this ideal. The list of z_i's to consider is X^3, X^3Y^3, X^2Y, Y^3.

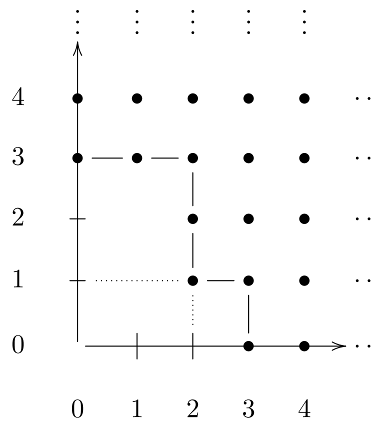
The monomial X^3Y^3 is a multiple of X^3, so we remove X^3Y^3 from the list. The new list of z_i's to consider is X^3, X^2Y, Y^3. No monomial in this list is a multiple of another since the exponent vectors $(3, 0)$, $(2, 1)$, and $(0, 3)$ are incomparable. Hence, the list X^3, X^2Y, Y^3 is an irredundant monomial generating sequence for J.

Let I be a monomial ideal of R. One goal of this text is the following: given a monomial ideal I, to find simpler monomial ideals $I_1, \ldots, I_n \subseteq R$ such that $I = I_1 \bigcap \cdots \bigcap I_n$. A hint as to how this might be done is found in the previous example, as we discuss next.

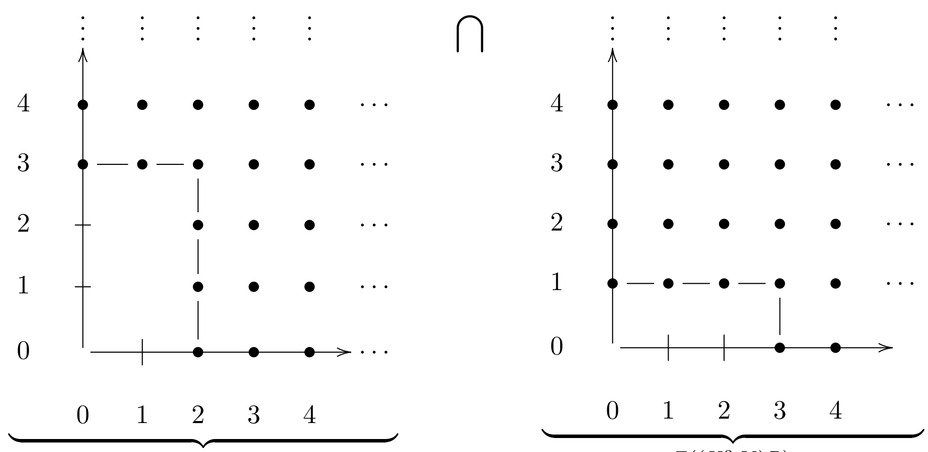
EXAMPLE 2.1.7. Set $R = A[X, Y]$ and $I = (X^3, X^2Y, Y^3)R$. The graph $\Gamma(I)$ has the following form.



The two corners of the form ⌝ break the "negative space" into two pieces



and suggest the following decomposition.



$\Gamma((X^2,Y^3)R)$ $\bigcap$ $\Gamma((X^3,Y)R)$

We conclude this section by noting that the methods from Proposition 2.1.5 and Example 2.1.6 can be extended to intersections of three or more monomial ideals inductively, simply by repeating the process. For instance, to find a monomial generating sequence for $I\bigcap J\bigcap K$, first find a monomial generating sequence for $I\bigcap J$, then find one for $(I\bigcap J)\bigcap K$. See also Exercise 2.1.15.

Exercises.

Exercise 2.1.8. Set $R = A[X,Y]$. Find irredundant generating sequences for the ideals $I = (X,Y^5)R\bigcap(X^4,Y)R$ and $J = (X^4,X^3Y^2,Y^3)R\bigcap(X^3,Y^5)R$.

Exercise 2.1.9. Set $R = A[X_1,\ldots,X_d]$. Prove that if $\{I_\lambda\}_{\lambda\in\Lambda}$ is a (possibly infinite) set of monomial ideals in R, then $\bigcap_{\lambda\in\Lambda} I_\lambda$ is a monomial ideal with $[\![\bigcap_{\lambda\in\Lambda} I_\lambda]\!] = \bigcap_{\lambda\in\Lambda}[\![I_\lambda]\!]$.

Exercise 2.1.10. Prove Lemma 2.1.4.

Exercise 2.1.11. Set $R = A[X_1,\ldots,X_d]$. Assume that I is generated by the set of monomials S and that J is generated by the set of monomials T. Prove or disprove the following: The ideal $I \bigcap J$ is generated by the set of monomials $L = \{\mathrm{lcm}(f, g) \mid f \in S \text{ and } g \in T\}$.

*Exercise 2.1.12. Set $R = A[X_1, \dots, X_d]$.

(a) Let $I_1, \dots, I_k$, and J be monomial ideals in R. Prove that $(I_1 + \cdots + I_k) \bigcap J = (I_1 \bigcap J) + \cdots + (I_k \bigcap J)$.
(b) Give an example (where $d = 2$) to show that this is not true without the assumption that each of the ideals I_1, I_2, and J are monomial ideals; justify your answer.

(This exercise is used in the proof of Lemma 7.5.1.)

Exercise 2.1.13. Set $R = A[X_1, \dots, X_d]$. Let $f = \underline{X}^{\underline{m}}$, $g = \underline{X}^{\underline{n}}$, and $w = \underline{X}^{\underline{p}}$ be monomials in R. Prove that the following conditions are equivalent.

(i) $w = \mathrm{lcm}(f, g)$;
(ii) w is a common multiple of f and g, and if $h \in R$ is a common multiple of f and g, then h is a multiple of w (note that we have not assumed that h is a monomial); and
(iii) we have $\underline{m} \leqslant \underline{p}$ and $\underline{n} \leqslant \underline{p}$, and if $\underline{e} \in \mathbb{N}^d$ is such that $\underline{m} \leqslant \underline{e}$ and $\underline{n} \leqslant \underline{e}$, then $\underline{p} \leqslant \underline{e}$.

Exercise 2.1.14. Set $R = A[X_1, \dots, X_d]$. Let $f = \underline{X}^{\underline{m}}$ and $g = \underline{X}^{\underline{n}}$ for some $\underline{m}, \underline{n} \in \mathbb{N}^d$. For $i = 1, \dots, d$ set $q_i = \min\{m_i, n_i\}$. Define the *greatest common divisor* of f and g to be the monomial $\gcd(f, g) = \underline{X}^{\underline{q}}$. Prove that $\mathrm{lcm}(f, g) \gcd(f, g) = fg$.

*Exercise 2.1.15. Set $R = A[X_1, \dots, X_d]$. Let $f = \underline{X}^{\underline{m}}$ and $g = \underline{X}^{\underline{n}}$ and $h = \underline{X}^{\underline{p}}$ for some $\underline{m}, \underline{n}, \underline{p} \in \mathbb{N}^d$. For $i = 1, \dots, d$ set $q_i = \max\{m_i, n_i, p_i\}$. Define the *least common multiple* of f, g, and h to be the monomial $\mathrm{lcm}(f, g, h) = \underline{X}^{\underline{q}}$.

(a) Prove that $\mathrm{lcm}(\mathrm{lcm}(f, g), h) = \mathrm{lcm}(f, g, h) = \mathrm{lcm}(f, \mathrm{lcm}(g, h))$.
(b) Prove that $(f)R \bigcap (g)R \bigcap (h)R = (\mathrm{lcm}(f, g, h))R$.
(c) Assume that I is generated by the set of monomials $\{f_1, \dots, f_m\}$ and that J is generated by the set of monomials $\{g_1, \dots, g_n\}$ and K is generated by the set of monomials $\{h_1, \dots, h_p\}$. Prove that $I \bigcap J \bigcap K$ is generated by the set of monomials $L = \{\mathrm{lcm}(f_i, g_j, h_k) \mid 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n, 1 \leqslant k \leqslant p\}$.
(d) For a sequence $z_1, \dots, z_a \in [\![R]\!]$, propose a definition of the term "least common multiple of $z_1, \dots, z_a$. State and prove the versions of parts (a)–(c) for your definition.

(This exercise is used in the proof of Theorem 6.2.4.)

*Exercise 2.1.16. Let K be a field, and let I be a monomial ideal in the polynomial ring $R = K[X_1, \dots, X_d]$ in d variables.

(a) Prove that $\mathrm{rad}\,(I)$ is a monomial ideal.
(b) Describe $[\![\mathrm{rad}\,(I)]\!]$ and $\Gamma(\mathrm{rad}\,(I))$ in terms of $[\![I]\!]$ and $\Gamma(I)$.

(This exercise is used in the proof of Proposition 2.3.2 and in Exercise 2.3.9.)

Exercise 2.1.17. Give an example of a commutative ring A with identity that satisfies the following property: there exists a monomial ideal I in the polynomial ring $R = A[x, y]$ in two variables such that $\mathrm{rad}\,(I)$ is not a monomial ideal; justify your answer.

Exercise 2.1.18. An element $a \in A$ is *nilpotent* if there exists $n \geqslant 0$ such that $a^n = 0_A$. The *nilradical* of A is

$$\mathrm{N}(A) = \{\text{nilpotent elements of } A\}.$$

The ring A is *reduced* if $\mathrm{N}(A) = 0$.

(a) Prove that $\mathrm{N}(A) = \mathrm{rad}\,(0)$; conclude that $\mathrm{N}(A)$ is an ideal of A.
(b) Prove that if $a \in A$ and $n \geqslant 0$ such that $a^n \in \mathrm{N}(A)$, then $a \in \mathrm{N}(A)$.
(c) Prove that if R is an integral domain, then R is reduced.

*Exercise 2.1.19. Set $R = A[X_1, \ldots, X_d]$. Prove that the following conditions are equivalent:

(i) the ring A is reduced;
(ii) for every monomial ideal $I \subset R$, the ideal $\mathrm{rad}\,(I)$ is a monomial ideal; and
(iii) there exists a monomial ideal $I \subset R$ such that $\mathrm{rad}\,(I)$ is a monomial ideal.

(This exercise is used in Exercise 2.3.9.)

Intersections of Monomial Ideals in Macaulay2: Exercises.

Exercise 2.1.20. Set $R = \mathbb{Z}_{101}[X, Y]$. Use Macaulay2 to verify the equalities $(XY^2)R \bigcap (X^2Y)R = (X^2Y^2)R$ and $(X^2, Y^3)R \bigcap (X^3, Y)R = (X^3, X^2Y, Y^3)R$.

Exercise 2.1.21. Set $R = \mathbb{Z}_{101}[X, Y]$. Use Macaulay2 to compute irredundant generating sequences for the intersection ideals $I = (X, Y^5)R \bigcap (X^4, Y)R$ and $J = (X^4, X^3Y^2, Y^3)R \bigcap (X^3, Y^5)R$.

Exercise 2.1.22. Set $R = \mathbb{Z}_{101}[X, Y]$, and consider the ideals $I = (X^2, Y^5)R$, $J = (X^4, Y)R$, and $K = (X^3, XY, Y^5)R$.

(a) Use Macaulay2 to verify that $(I + J) \bigcap K = (I \bigcap K) + (J \bigcap K)$.
(b) Use Macaulay2 to verify your answer to Exercise 2.1.12(b).

Exercise 2.1.23. Set $R = \mathbb{Z}_{101}[X, Y, Z]$ and $I = (X^2Y, YZ, Z^5)R$. Work with Macaulay2 to verify that $\mathrm{rad}\,(I)$ is a monomial ideal.

2.2. Unique Factorization Domains (optional)

In this section, R is an integral domain.

In a polynomial ring $A[X_1, \ldots, X_d]$, each monomial $\underline{X}^{\underline{n}}$ has a factorization as a product of powers of the variables X_i. This is similar to the *Fundamental Theorem of Arithmetic* which states that every positive integer has a unique factorization as a product of powers of prime numbers. This section deals with classes of rings with similar properties. The definition is in 2.2.4; it needs the following prerequisites.

Definition 2.2.1. Two elements $r, s \in R$ are *associates* if $(r)R = (s)R$.

A non-zero non-unit $t \in R$ is *irreducible* if it admits no non-trivial factorization, i.e., if for every $a, b \in R$ such that $t = ab$ either a is a unit or b is a unit.

A non-zero non-unit $p \in R$ is *prime* if for every $a, b \in R$ such that $p \big| ab$ either $p \big| a$ or $p \big| b$.

For example, a non-zero positive integer is irreducible in $\mathbb{Z}$ if and only if it is a prime number, that is, if and only if it is a prime element in the terminology of Definition 2.2.1. Also, two integers m and n are associates in $\mathbb{Z}$ if and only if $m = \pm n$. This corresponds to the fact that for elements $r, s \in R$ the following conditions are equivalent:

(i) r and s are associates;
(ii) $r\big|s$ and $s\big|r$;
(iii) $r \in (s)R$ and $s \in (r)R$; and
(iv) there is a unit $u \in R$ such that $r = us$.

Many other familiar factorization facts from $\mathbb{Z}$ and $A[X]$ hold in arbitrary integral domains. Some of these are described in the following facts, whose proofs are left as exercises.

FACT 2.2.2. Let $r, r', s, u \in R$.

(a) If $u \in R$ is a unit and $r \in R$, then $r\big|u$ if and only if r is a unit.
(b) If r and r' are associates, then $r\big|s$ if and only if $r'\big|s$.

FACT 2.2.3. Let p and q be non-zero non-units in R, and let $a_1, \ldots, a_n \in R$.

(a) If p is prime and $p\big|a_1 \cdots a_n$, then there is an index i such that $p\big|a_i$.
(b) If p is prime, then p is irreducible.
(c) The converse to part (b) can fail in general. See however Lemma 2.2.6.
(d) If p and q are prime and $p\big|q$, then p and q are associates.

Now we are in position to give the main definition of this section, based on the standard factorization properties of $\mathbb{Z}$.

DEFINITION 2.2.4. The integral domain R is a *unique factorization domain* provided that every non-zero non-unit of R can be factored as a product of irreducible elements in an essentially unique way, that is:

(1) for every non-zero non-unit $r \in R$ there are (not necessarily distinct) irreducible elements $s_1, \ldots, s_m \in R$ such that $r = s_1 \cdots s_m$; and
(2) for all irreducible elements $s_1, \ldots, s_m, t_1, \ldots, t_n$ if $s_1 \cdots s_m = t_1 \cdots t_n$, then $m = n$ and there is a permutation σ of the integers $1, \ldots, m$ such that s_i and $t_{\sigma(i)}$ are associates for $i = 1, \ldots, m$.

The term "unique factorization domain" is frequently abbreviated as "UFD".

The Fundamental Theorem of Arithmetic states that the ring $\mathbb{Z}$ is a unique factorization domain. Every field is (vacuously) a unique factorization domain. The ring of Gaussian integers

$$\mathbb{Z}[i] = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$$

is a unique factorization domain. The ring

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \in \mathbb{R} \mid a, b \in \mathbb{Z}\}$$

is not a unique factorization domain; see [**22**, Sec. III.3].

FACT 2.2.5. If A is a unique factorization domain, then so is the polynomial ring $A[X_1, \ldots, X_d]$ in d variables for each d. In particular, if k is a field, then $k[X_1, \ldots, X_d]$ is a unique factorization domain. See, e.g., [**22**, Thm. III.6.12].

In the next result, the unique factorization assumption is essential. For instance, it explains why we do not distinguish between prime elements and irreducible elements in $\mathbb{Z}$.

LEMMA 2.2.6. *Let R be a unique factorization domain. An element $p \in R$ is irreducible if and only if it is prime.*

PROOF. One implication is in Fact 2.2.3(b).

For the converse, assume that p is irreducible in R. To show that p is prime, let $a, b \in R$ and assume that $p\big|ab$. We need to prove that $p\big|a$ or $p\big|b$. Then there is an element $c \in R$ such that $ab = pc$. If $a = 0$, then $p\big|a$ because $a = 0 = 0 \cdot p$, and we are done. If a is a unit, then $b = a^{-1}pc$, so we have $p\big|b$ and we are done. Similarly, if $b = 0$ or if b is a unit, then we are done. So, we may assume that a and b are non-zero non-units. In particular, the equation $pc = ab$ implies that $c \neq 0$.

Assume that c is not a unit. (The case where c is a unit is handled similarly.) Since R is a unique factorization domain, there are irreducible elements $a_1, \ldots, a_k, b_1, \ldots, b_m, c_1, \ldots c_n \in R$ such that $a = a_1 \cdots a_k$ and $b = b_1 \cdots b_m$ and $c = c_1 \cdots c_n$. The equation $pc = ab$ then reads

$$pc_1 \cdots c_n = a_1 \cdots a_k b_1 \cdots b_m.$$

The uniqueness of factorizations in R implies that p is associate to one of the factors on the right-hand side. (Here is where we use the fact that p is irreducible.) If p and a_i are associates, then $p\big|a_1$, so p divides $a_1 \cdots a_k = a$, as desired. Similarly, if p and b_j are associates, then $p\big|b$. Thus p is prime. $\square$

The next two lemmas treat useful bookkeeping notions for factorizations over UFDs that should be familiar over $\mathbb{Z}$.

LEMMA 2.2.7. *Let R be a unique factorization domain, and let $r \in R$ be a non-zero non-unit. There exist irreducible elements $p_1, \ldots, p_m \in R$, a unit $u \in R$, and integers $e_1, \ldots, e_m \geqslant 1$ such that*

(1) *$r = up_1^{e_1} \cdots p_m^{e_m}$, and*
(2) *for all $i, j \in \{1, \ldots, m\}$ such that $i \neq j$, the elements p_i and p_j are not associates.*

PROOF. By definition there are (not necessarily distinct) irreducible elements $s_1, \ldots, s_k \in R$ such that $r = s_1 \cdots s_k$. Re-order the s_i so that they are grouped by associates. That is, re-order the s_i to assume that there are integers $i_0 = 0 < 1 = i_1 < i_2 < \cdots < i_m < i_{m+1} = k + 1$ such that

(1) for $j = 1, \ldots, m$ and $l = i_j, \ldots, i_{j+1} - 1$ the elements s_l and s_{i_j} are associates, and
(2) for $j = 1, \ldots, m$ if $1 \leqslant l < i_j \leqslant h$ the s_l and s_h are not associates.

For $j = 1, \ldots, n$ set $p_j = s_{i_j}$ and $e_j = i_j - i_{j-1} \geqslant 1$. For $l = i_j, \ldots, i_{j+1} - 1$ fix units $u_l \in R$ such that $s_l = u_l s_{i_j} = u_l p_j$. Note that $u_{i_j} = 1_R$ for $j = 1, \ldots, n$.

For $j = 1, \ldots, n$ set $v_j = u_{i_j} \cdots u_{i_{j+1}-1}$. This yields

$$s_{i_j} s_{i_j+1} \cdots s_{i_{j+1}-1} = p_j(u_{i_j+1}p_j) \cdots (u_{i_{j+1}-1}p_j) = v_j p_j^{e_j}.$$

With $u = \prod_{j=1}^n v_j = \prod_{l=1}^k u_l$, it follows that we have

$$\begin{aligned} r &= s_1 \cdots s_k \\ &= [s_{i_1} \cdots s_{i_2-1}][s_{i_2} \cdots s_{i_3-1}] \cdots [s_{i_m} \cdots s_{i_{m+1}-1}] \\ &= [v_1 p_1^{e_1}][v_2 p_2^{e_2}] \cdots [v_n p_n^{e_n}] \\ &= up_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}. \end{aligned}$$

This is the desired factorization. $\square$

LEMMA 2.2.8. *Let R be a unique factorization domain, and let $r, s \in R$ be non-zero non-units. There exist irreducible elements $p_1, \ldots, p_n \in R$, units $u, v \in R$, and integers $e_1, \ldots, e_n, f_1, \ldots, f_n \geqslant 0$ such that*

(1) $r = up_1^{e_1} \cdots p_n^{e_n}$ *and* $s = vp_1^{f_1} \cdots p_n^{f_n}$*, and*
(2) *for all $i, j \in \{1, \ldots, n\}$ such that $i \neq j$, the elements p_i and p_j are not associates.*

PROOF. Lemma 2.2.7 yields irreducible elements $p_1, \ldots, p_m, p'_1, \ldots, p'_{m'} \in R$, integers $e_1, \ldots, e_m, e'_1, \ldots, e'_{m'} \geqslant 1$, and units $u, u' \in R$ such that

(1) $r = up_1^{e_1} \cdots p_m^{e_m}$ and $s = u'(p'_1)^{e'_1} \cdots (p'_{m'})^{e'_m}$,
(2) for all $i, j \in \{1, \ldots, m\}$ such that $i \neq j$, the elements p_i and p_j are not associates, and
(3) for all $i, j \in \{1, \ldots, m'\}$ such that $i \neq j$, the elements p'_i and p'_j are not associates.

Re-order the p'_i if necessary to assume that there is an integer $\mu \geqslant 1$ such that

(4) for $1 \leqslant i < \mu$ the elements p_i and p'_i are associates, and
(5) for $\mu \leqslant i \leqslant m$ and $\mu \leqslant i' \leqslant m'$ the elements p_i and $p'_{i'}$ are not associates.

Set $n = m + (m' - \mu + 1)$. For $i = m+1, \ldots, n$ set $p_i = p'_{\mu-m-1+i}$ and $e_i = 0$. Then one has

$$r = up_1^{e_1} \cdots p_m^{e_m} = up_1^{e_1} \cdots p_m^{e_m} p_{m+1}^0 \cdots p_n^0 = up_1^{e_1} \cdots p_n^{e_n}$$

For $i = 1, \ldots, \mu-1$ set $f_i = e'_i$ and fix a unit x_i such that $p'_i = x_i p_i$. For $i = \mu, \ldots, m$ set $f_i = 0$. For $i = m+1, \ldots, n$ set $f_i = e'_{\mu-m-1+i}$. Then one has

$$\begin{aligned} s &= u'(p'_1)^{e'_1} \cdots (p'_{m'})^{e'_m} \\ &= u'(x_1p_1)^{e'_1} \cdots (x_\mu p_\mu)^{e'_\mu} p_{\mu+1}^0 \cdots p_m^0 (x_{m+1}p_{m+1})^{e'_{\mu+1}} \cdots (x_n p_n)^{e'_n} \\ &= vp_1^{f_1} \cdots p_n^{f_n} \end{aligned}$$

where $v = u' x_1^{e'_1} \cdots x_{m'}^{e'_m}$. □

Again, the next few lemmas should be familiar in the context of the integers. We use them below in our treatment of greatest common divisors and least common multiples in unique factorization domains. The first one characterizes divisibility by a prime element.

LEMMA 2.2.9. *Let R be a unique factorization domain, and let $r \in R$ be a non-zero non-unit. Fix irreducible elements $p_1, \ldots, p_n \in R$, integers $e_1, \ldots, e_n \geqslant 0$, and a unit $u \in R$ such that $r = up_1^{e_1} \cdots p_n^{e_n}$, and for all $i, j \in \{1, \ldots, n\}$ such that $i \neq j$, the elements p_i and p_j are not associates. Given a prime element $p \in R$, one has $p \big| r$ if and only if there is an index i such that p and p_i are associates and $e_i \geqslant 1$.*

PROOF. First, assume that there is an index i such that $e_i \geqslant 1$ and the elements p and p_i are associates. Then $p \big| p_i$, and hence $p \big| up_1^{e_1} \cdots p_i^{e_i} \cdots p_n^{e_n} = r$.

Conversely, assume that $p \big| r = up_1^{e_1} \cdots p_n^{e_n}$. Fact 2.2.3(a) implies that either $p \big| u$ or $p \big| p_i^{e_i}$ for some index i. Since p is not a unit and u is a unit, Fact 2.2.2(a) implies that $p \nmid u$. Thus, we have $p \big| p_i^{e_i}$ for some index i. If $e_i = 0$ then $p \big| p_i^0 = 1$, which is impossible, again because p is not a unit. It follows that $e_i \geqslant 1$ and $p \big| p_i \cdots p_i$. Another application of Fact 2.2.3(a) shows that $p \big| p_i$. We conclude from Fact 2.2.3(d) that p and p_i are associates. □

The next two results characterize divisibility in a UFD in terms of prime factorizations. Lemma 1.1.7 is a similar result for monomials. This similarity is one of our main motivations for discussing UFD's.

LEMMA 2.2.10. *Let R be a unique factorization domain, and let $r, s \in R$ be non-zero non-units. Given irreducible elements $p_1, \ldots, p_n \in R$, units $u, v \in R$, and integers $e_1, \ldots, e_n, f_1, \ldots, f_n \geqslant 0$ as in Lemma 2.2.8, one has $r \big| s$ if and only if $e_i \leqslant f_i$ for $i = 1, \ldots, n$.*

PROOF. Assume first that $e_i \leqslant f_i$ for $i = 1, \ldots, n$ and consider the element $x = vu^{-1} p_1^{f_1 - e_1} \cdots p_n^{f_n - e_n}$. It is straightforward to show that $rx = s$, so $r \big| s$.

Assume now that $r \big| s$, and fix an element $t \in R$ such that $s = rt$. Our assumptions imply that

$$vp_1^{f_1} \cdots p_n^{f_n} = up_1^{e_1} \cdots p_n^{e_n} t. \tag{2.2.10.1}$$

We prove that $f_i \geqslant e_i$ by induction on $e = e_1 + \cdots + e_n$.

Base case: $e = 0$. In this case, each $e_i = 0$, so we have $f_i \geqslant 0 = e_i$ for each i.

Induction step: Assume that $e \geqslant 1$ and that the result holds for elements of the form $r' = up_1^{e'_1} \cdots p_n^{e'_n}$ where $e'_1 + \cdots e'_n = e - 1$. Since $e \geqslant 1$, we have $e_i \geqslant 1$ for some index i. It follows that $p_i \big| up_1^{e_1} \cdots p_n^{e_n} t = vp_1^{f_1} \cdots p_n^{f_n}$. Lemma 2.2.9 implies that there is an index j such that p_i and p_j are associates and $f_j \geqslant 1$. It follows that $i = j$, so we have $f_i \geqslant 1$. Equation (2.2.10.1) now reads as

$$p_i(vp_1^{f_1} \cdots p_i^{f_i - 1} \cdots p_n^{f_n}) = p_i(up_1^{e_1} \cdots p_i^{e_i - 1} \cdots p_n^{e_n} t).$$

Since R is an integral domain, the cancellation property 1.2.3 implies that

$$vp_1^{f_1} \cdots p_i^{f_i - 1} \cdots p_n^{f_n} = up_1^{e_1} \cdots p_i^{e_i - 1} \cdots p_n^{e_n} t.$$

The sum of the exponents on the right-hand side of this equation is $e - 1$, so the induction hypothesis implies that $f_j \geqslant e_j$ for each $j \neq i$, and $f_i - 1 \geqslant e_i - 1$ so $f_i \geqslant e_i$, as desired. $\square$

LEMMA 2.2.11. *Let R be a unique factorization domain, and let $r \in R$ be a non-zero non-unit. Fix irreducible elements $p_1, \ldots, p_n \in R$, integers $e_1, \ldots, e_n \geqslant 0$, and a unit $u \in R$ such that $r = up_1^{e_1} \cdots p_n^{e_n}$, and for all $i, j \in \{1, \ldots, n\}$ such that $i \neq j$, the elements p_i and p_j are not associates. Given a non-zero element $t \in R$, one has $t \big| r$ if and only if there exist integers $l_1, \ldots, l_n$, and a unit $w \in R$ such that $t = wp_1^{l_1} \cdots p_n^{l_n}$ and $0 \leqslant l_i \leqslant e_i$ for $i = 1, \ldots, n$.*

PROOF. One implication follows from Lemma 2.2.10.

For the converse, assume that $t \big| r$. If t is a unit, then the integers $l_1 = \cdots = l_n = 0$ and the unit $w = t$ satisfy the desired conclusions. Assume that t is not a unit. Since t is also non-zero, it has a prime factor, say p. Since $t \big| r$, we have $p \big| r$, so Lemma 2.2.9 provides an index i such that p and p_i are associates and $e_i \geqslant 1$. Thus, Fact 2.2.2(b) implies that p_i is a prime factor of t. In other words, in a prime factorization of t, the element p can be replaced with p_i. This implies that there exist integers $l_1, \ldots, l_n \geqslant 0$, and a unit $w \in R$ such that $t = wp_1^{l_1} \cdots p_n^{l_n}$. Since $t \big| r$, Lemma 2.2.10 implies that $l_i \leqslant e_i$ for $i = 1, \ldots, n$. $\square$

Other familiar notions from the integers are GCD's and LCM's. Again, these notions extend to general UFD's and compare directly to the notions we have introduced for monomial ideals; see Exercises 2.1.13 and 2.1.14.

DEFINITION 2.2.12. Let $r, s \in R$.

(a) An element $g \in R$ is a *greatest common divisor* for r and s if
   (1) one has $g \big| r$ and $g \big| s$; and
   (2) for all $h \in R$ such that $h \big| r$ and $h \big| s$, one has $h \big| g$.

(b) An element $l \in R$ is a *least common multiple* for r and s if
   (1) one has $r \big| l$ and $s \big| l$; and
   (2) for all $m \in R$ such that $r \big| m$ and $s \big| m$, one has $l \big| m$.

Given elements $r, s \in R$, one can show that GCD's and LCM's are "unique up to associates". That is, if $g \in R$ is a greatest common divisor for r and s, then $g' \in R$ is a greatest common divisor for r and s if and only if g and g' are associates. Also, if $l \in R$ is a least common multiple for r and s, then $l' \in R$ is a least common multiple for r and s if and only if l and l' are associates.

The next result shows how to compute GCD's in terms of prime factorizations, just like in $\mathbb{Z}$. Compare it to the corresponding fact for monomial GCD's in Exercise 2.1.13.

THEOREM 2.2.13. *Let R be a unique factorization domain, and let $r, s \in R$ be non-zero non-units. Then R contains a greatest common divisor and a least common multiple for r and s. Specifically, fix irreducible elements $p_1, \ldots, p_n \in R$, integers $e_1, \ldots, e_n, f_1, \ldots, f_n \geqslant 0$, and units $u, v \in R$ as in Lemma 2.2.8. For $i = 1, \ldots, n$ let $m_i = \min\{e_i, f_i\}$ and $M_i = \max\{e_i, f_i\}$. Then $g = p_1^{m_1} \cdots p_n^{m_n}$ is a greatest common divisor for r and s, and $l = p_1^{M_1} \cdots p_n^{M_n}$ is a least common multiple for r and s.*

PROOF. We prove that g is a greatest common divisor for r and s. The proof that l is a least common multiple for r and s is left as an exercise.

Lemma 2.2.10 shows that $g \big| r$ and $g \big| s$, since $m_i \leqslant e_i$ and $m_i \leqslant f_i$. Now, assume that $h \in R$ such that $h \big| r$ and $h \big| s$; we need to show that $h \big| g$. Since $h \big| r$, Lemma 2.2.11 provides integers $l_1, \ldots, l_n$, and a unit $w \in R$ such that $h = wp_1^{l_1} \cdots p_n^{l_n}$ and $0 \leqslant l_i \leqslant e_i$ for $i = 1, \ldots, n$. Since $h \big| s$, Lemma 2.2.10 implies that $l_i \leqslant f_i$ for $i = 1, \ldots, n$ so we have $l_i \leqslant \min\{e_i, f_i\} = m_i$ for $i = 1, \ldots, n$. Another application of Lemma 2.2.10 implies that $h \big| g$, as desired. □

Exercises.

EXERCISE 2.2.14. Prove Facts 2.2.2 and 2.2.3

EXERCISE 2.2.15. Let R be a unique factorization domain, and let $r, s \in R$.

(a) Prove that $(r)R \bigcap (s)R = (\mathrm{lcm}(r, s))R$.
(b) Prove or disprove the following: $(r)R + (s)R = (\gcd(r, s))R$. (Hint: Feel free to use Fact 2.2.5.)

EXERCISE 2.2.16. Let R be a unique factorization domain, and let $r, s \in R$ be non-zero non-units. Let $g \in R$ be a greatest common divisor for r and s, and let $l \in R$ be a least common multiple for r and s. Prove that there is a unit $w \in R$ such that $gl = wrs$. (Compare this with the corresponding result for monomials in Exercise 2.1.14.)

2.3. Monomial Radicals

In this section, A is a non-zero commutative ring with identity.

This section focuses on the following version of the radical for monomial ideals. (See Section B.5 for an introduction to radicals.) To motivate it, note that the radical of a monomial ideal need not be a monomial ideal. Indeed, in the polynomial ring $R = \mathbb{Z}_4[X]$ in one variable, the ideal $J = (X)R$ is a monomial ideal, but the ideal $\operatorname{rad}(J) = (2, X)R$ is not a monomial ideal. See Exercises 2.1.16–2.1.19 for more details about this phenomenon.

DEFINITION 2.3.1. Set $R = A[X_1, \ldots, X_d]$. Let J be a monomial ideal in R. The *monomial radical* of J is the monomial ideal $\text{m-rad}(J) = (S)R$ where

$$S = \operatorname{rad}(J) \bigcap [\![R]\!] = \{z \in [\![R]\!] \mid z^n \in J \text{ for some } n \geqslant 1\}.$$

For instance, in the ring $R = A[X, Y]$, we have $\text{m-rad}\big((X^3, Y^2)R\big) = (X, Y)R$ and $\text{m-rad}\big((X^3Y^2)R\big) = (XY)R$. (This can be verified directly, or using Theorem 2.3.7.) The example preceding Definition 2.3.1 shows that one has $\text{m-rad}(J) \neq \operatorname{rad}(J)$ in general. The next result gives more information about the relation between $\operatorname{rad}(J)$ and $\text{m-rad}(J)$. Note that the equality $\text{m-rad}(J) = \operatorname{rad}(J)$ in part (c) holds more generally when R is reduced, e.g., an integral domain; see Exercise 2.3.9.

PROPOSITION 2.3.2. *Set $R = A[X_1, \ldots, X_d]$. Let J be a monomial ideal in R.*
(a) *One has* $\text{m-rad}(J) \subseteq \operatorname{rad}(J)$.
(b) *One has* $\text{m-rad}(J) = \operatorname{rad}(J)$ *if and only if* $\operatorname{rad}(J)$ *is a monomial ideal.*
(c) *If A is a field, then* $\text{m-rad}(J) = \operatorname{rad}(J)$.

PROOF. (a) The ideal $\text{m-rad}(J)$ is generated by the set $S = \operatorname{rad}(J) \bigcap [\![R]\!] \subseteq \operatorname{rad}(J)$, so we have $\text{m-rad}(J) \subseteq \operatorname{rad}(J)$.

(b) If $\operatorname{rad}(J)$ is a monomial ideal, then

$$\operatorname{rad}(J) = ([\![\operatorname{rad}(J)]\!])R = (S)R = \text{m-rad}(J).$$

Conversely, if $\operatorname{rad}(J) = \text{m-rad}(J)$, then the fact that $\text{m-rad}(J)$ is a monomial ideal implies that $\operatorname{rad}(J)$ is a monomial ideal.

(c) Assuming that R is a field, Exercise 2.1.16 shows that $\operatorname{rad}(J)$ is a monomial ideal, part (b) implies that $\text{m-rad}(J) = \operatorname{rad}(J)$. □

The next result contains some fundamental properties of the monomial radical. It compares to Proposition A.6.3.

PROPOSITION 2.3.3. *Set $R = A[X_1, \ldots, X_d]$. Let J be a monomial ideal in R.*
(a) *There is a containment* $J \subseteq \text{m-rad}(J)$.
(b) *One has* $[\![\text{m-rad}(J)]\!] = \operatorname{rad}(J) \bigcap [\![R]\!]$.
(c) *If $I \subseteq J$, then* $\text{m-rad}(I) \subseteq \text{m-rad}(J)$.
(d) *There is an equality* $\text{m-rad}(J) = \text{m-rad}(\text{m-rad}(J))$.
(e) *One has* $\text{m-rad}(J) = R$ *if and only if* $J = R$.
(f) *One has* $\text{m-rad}(J) = 0$ *if and only if* $J = 0$.
(g) *For each integer $n \geqslant 1$, one has* $\text{m-rad}(J) = \text{m-rad}(J^n)$.

PROOF. (a) The set $S = \operatorname{rad}(J) \bigcap [\![R]\!] \supseteq J \bigcap [\![R]\!] = [\![J]\!]$ generates $\text{m-rad}(J)$, so we have $\text{m-rad}(J) = (S)R \supseteq ([\![J]\!])R = J$.

(b) Since $S = \operatorname{rad}(J) \bigcap [\![R]\!]$ is a monomial generating set for $\text{m-rad}(J)$, we have $[\![\text{m-rad}(J)]\!] \supseteq \operatorname{rad}(J) \bigcap [\![R]\!]$. For the reverse containment, the condition $\text{m-rad}(J) \subseteq \operatorname{rad}(J)$ implies that $[\![\text{m-rad}(J)]\!] = \text{m-rad}(J) \bigcap [\![R]\!] \subseteq \operatorname{rad}(J) \bigcap [\![R]\!]$.

(c) Assume that $I \subseteq J$. The containment $\operatorname{rad}(I) \subseteq \operatorname{rad}(J)$ is from Proposition A.6.3(c), so we have $\operatorname{rad}(I) \bigcap [\![R]\!] \subseteq \operatorname{rad}(J) \bigcap [\![R]\!]$ and

$$\text{m-rad}(I) = (\operatorname{rad}(I) \bigcap [\![R]\!])R \subseteq (\operatorname{rad}(J) \bigcap [\![R]\!])R = \text{m-rad}(J)\,.$$

(d) The containment $\text{m-rad}(J) \subseteq \text{m-rad}(\text{m-rad}(J))$ follows from part (a). For the reverse containment, is suffices to show that $[\![\text{m-rad}(J)]\!] \supseteq [\![\text{m-rad}(\text{m-rad}(J))]\!]$. Let $f \in [\![\text{m-rad}(\text{m-rad}(J))]\!] = \operatorname{rad}(\text{m-rad}(J)) \bigcap [\![R]\!]$, and fix an exponent $n \geqslant 1$ such that $f^n \in \text{m-rad}(J)$. Then

$$f^n \in \text{m-rad}(J) \bigcap [\![R]\!] = [\![\text{m-rad}(J)]\!] = \operatorname{rad}(J) \bigcap [\![R]\!]$$

so there is an exponenet $m \geqslant 1$ such that $f^{mn} = (f^n)^m \in J$. This shows that $f \in \operatorname{rad}(J) \bigcap [\![R]\!] = [\![\text{m-rad}(J)]\!]$, as desired.

The proofs of parts (e)–(g) are left as exercises. $\square$

The next result describes some of the behavior between monomial radicals and other operations on ideals. It compares to Proposition A.6.5. However, the properties in parts (c) and (d) show that the monomial radical is somewhat better behaved than the regular radical; see Example A.6.6.

PROPOSITION 2.3.4. *Set $R = A[X_1, \ldots, X_d]$. Let n be a positive integer, and let $I, J, I_1, I_2, \ldots, I_n$ be monomial ideals of R.*

(a) *There are equalities* $\text{m-rad}(IJ) = \text{m-rad}(I \bigcap J) = \text{m-rad}(I) \bigcap \text{m-rad}(J)$.

(b) *There are equalities*

$$\text{m-rad}(I_1 I_2 \cdots I_n) = \text{m-rad}\left(\bigcap_{j=1}^{n} I_j\right) = \bigcap_{j=1}^{n} \text{m-rad}(I_j)\,.$$

(c) *There is an equality* $\text{m-rad}(I + J) = \text{m-rad}(I) + \text{m-rad}(J)$.

(d) *There is an equality* $\text{m-rad}\left(\sum_{j=1}^{n} I_j\right) = \sum_{j=1}^{n} \text{m-rad}(I_j)$.

PROOF. (a) As in the proof of Proposition A.6.5(a), we have $\text{m-rad}(IJ) \subseteq \text{m-rad}(I \bigcap J) \subseteq \text{m-rad}(I) \bigcap \text{m-rad}(J)$ by Proposition 2.3.3(c). For the containment $\text{m-rad}(I) \bigcap \text{m-rad}(J) \subseteq \text{m-rad}(IJ)$, it suffices to show that $[\![\text{m-rad}(IJ)]\!] = [\![\text{m-rad}(I) \bigcap \text{m-rad}(J)]\!]$. We compute:

$$\begin{aligned}
[\![\text{m-rad}(I) \textstyle\bigcap \text{m-rad}(J)]\!] &= [\![\text{m-rad}(I)]\!] \textstyle\bigcap [\![\text{m-rad}(J)]\!] \\
&= (\operatorname{rad}(I) \textstyle\bigcap [\![R]\!]) \textstyle\bigcap (\operatorname{rad}(J) \textstyle\bigcap [\![R]\!]) \\
&= (\operatorname{rad}(I) \textstyle\bigcap \operatorname{rad}(J)) \textstyle\bigcap [\![R]\!] \\
&= \operatorname{rad}(IJ) \textstyle\bigcap [\![R]\!] \\
&= [\![\text{m-rad}(IJ)]\!].
\end{aligned}$$

The first step in this sequence is from Theorem 2.1.1. The second and fifth steps are from Proposition 2.3.3(b). The third step is routine, and the fourth step is from Proposition A.6.5(a).

(c) We first show that

$$\operatorname{rad}(I + J) \bigcap [\![R]\!] = (\operatorname{rad}(I) \bigcap [\![R]\!]) \cup (\operatorname{rad}(J) \bigcap [\![R]\!]). \tag{2.3.4.1}$$

For the containment "$\subseteq$", let $f \in \operatorname{rad}(I+J) \bigcap [\![R]\!]$ and fix an integer $n \geqslant 1$ such that $f^n \in I+J$. Since f^n is a monomial, Exercise 1.3.11(b) implies that $f^n \in I \cup J$. If $f^n \in I$, then $f \in \operatorname{rad}(I) \bigcap [\![R]\!]$. If $f^n \in J$, then $f \in \operatorname{rad}(J) \bigcap [\![R]\!]$. So, we conclude that $f \in (\operatorname{rad}(I) \bigcap [\![R]\!]) \cup (\operatorname{rad}(J) \bigcap [\![R]\!])$. For the reverse containment, we compute:

$$\begin{aligned}
(\operatorname{rad}(I) \textstyle\bigcap [\![R]\!]) \cup (\operatorname{rad}(J) \textstyle\bigcap [\![R]\!]) &= (\operatorname{rad}(I) \cup \operatorname{rad}(J)) \textstyle\bigcap [\![R]\!] \\
&\subseteq (\operatorname{rad}(I) + \operatorname{rad}(J)) \textstyle\bigcap [\![R]\!] \\
&\subseteq \operatorname{rad}(\operatorname{rad}(I) + \operatorname{rad}(J)) \textstyle\bigcap [\![R]\!] \\
&= \operatorname{rad}(I+J) \textstyle\bigcap [\![R]\!].
\end{aligned}$$

The first step is routine, and the second step is from the containment $\operatorname{rad}(I) \cup \operatorname{rad}(J) \subseteq \operatorname{rad}(I) + \operatorname{rad}(J)$. The remaining steps are from Propositions A.6.3(b) and A.6.5(c).

In the next sequence, the second step is from equation (2.3.4.1):

$$\begin{aligned}
[\![\text{m-rad}(I+J)]\!] &= \operatorname{rad}(I+J) \textstyle\bigcap [\![R]\!] \\
&= (\operatorname{rad}(I) \textstyle\bigcap [\![R]\!]) \cup (\operatorname{rad}(J) \textstyle\bigcap [\![R]\!]) \\
&= [\![\text{m-rad}(I)]\!] \cup [\![\text{m-rad}(J)]\!] \\
&= [\![\text{m-rad}(I) + \text{m-rad}(J)]\!].
\end{aligned}$$

The first and third steps are from Proposition 2.3.3(b), and the fourth step is from Exercise 1.3.11(b).

The proofs of the remaining statements follow by induction and are left as exercises. □

Our next goal is to find monomial generating sequences for m-rad(J) in terms of the generators of J. This is accomplished in Theorem 2.3.7, which is based on the following constructions.

DEFINITION 2.3.5. Set $R = A[X_1, \ldots, X_d]$. The *support* of a monomial $f = \underline{X}^{\underline{n}} \in [\![R]\!]$ is the set

$$\operatorname{Supp}(f) = \{i \in \mathbb{N} \mid 1 \leqslant i \leqslant d \text{ and } n_i \neq 0\}.$$

The *reduction* of f is the monomial

$$\operatorname{red}(f) = \prod_{i \in \operatorname{Supp}(f)} X_i.$$

In words, the support of a monomial $f \in [\![R]\!]$ is the set of indices i such that $X_i \big| f$. The reduction of f is the product of the variables dividing f:

$$\operatorname{red}(f) = \prod_{X_i | f} X_i.$$

For instance, in the ring $R = A[X_1, X_2, X_3]$, we have $\operatorname{Supp}(X_1^2 X_3^5) = \{1, 3\}$ and $\operatorname{red}(X_1^2 X_3^5) = X_1 X_3$.

In general in $R = A[X_1, \ldots, X_d]$, for each integer $n \geqslant 1$ and each monomial $f \in [\![R]\!]$, we have $\operatorname{Supp}(f^n) = \operatorname{Supp}(f) = \operatorname{Supp}(\operatorname{red}(f))$ and $\operatorname{red}(f^n) = \operatorname{red}(f)$ and $\operatorname{red}(f) \big| f$. For monomials $f, g \in [\![R]\!]$, one has $\operatorname{Supp}(f) \subseteq \operatorname{Supp}(g)$ if and only if $\operatorname{red}(f) \big| \operatorname{red}(g)$. Also, if $f \big| g$, then $\operatorname{Supp}(f) \subseteq \operatorname{Supp}(g)$ and $\operatorname{red}(f) \big| \operatorname{red}(g)$. The next lemma contains similar properties that are used in our description of the generators of $\text{m-rad}\,(J)$ in Theorem 2.3.7.

LEMMA 2.3.6. *Set $R = A[X_1, \ldots, X_d]$. Let J be a monomial ideal in R, and let $f \in [\![R]\!]$.*

(a) *There is an integer $n \geqslant 1$ such that $\text{red}(f)^n \in (f)R$.*

(b) *If $f \in J$, then $\text{red}(f) \in \text{m-rad}\,(J)$.*

PROOF. (a) Let $\text{Supp}(f) = \{i_1, \ldots, i_k\}$ with $1 \leqslant i_1 < \cdots < i_k \leqslant d$. It follows that $\text{red}(f) = X_{i_1} \cdots X_{i_k}$. Write $f = \underline{X}^{\underline{m}}$ and let $n = \max\{m_1, \ldots, m_d\}$. Then $f = X_{i_1}^{m_{i_1}} \cdots X_{i_k}^{m_{i_k}}$. Since $n \geqslant m_i$ for $i = 1, \ldots, d$ we have

$$f = X_{i_1}^{m_{i_1}} \cdots X_{i_k}^{m_{i_k}} \big| X_{i_1}^{n} \cdots X_{i_k}^{n} = \text{red}(f)^n$$

so $\text{red}(f)^n \in (f)R$, as desired.

(b) Assume that $f \in J$. Part (a) yields an integer $n \geqslant 1$ such that $\text{red}(f)^n \in (f)R \subseteq J$. Hence $\text{red}(f) \in \text{m-rad}\,(J)$. $\square$

Now we are in a position to describe the generators of $\text{m-rad}\,(J)$ in terms of the reduced versions of the generators of J.

THEOREM 2.3.7. *Set $R = A[X_1, \ldots, X_d]$. Let $S \subseteq [\![R]\!]$ and set $J = (S)R$. Then one has $\text{m-rad}\,(J) = (\{\text{red}(f) \mid f \in S\})R$.*

PROOF. Set $T = \{\text{red}(f) \mid f \in S\}$ and $K = (T)R$.

For each $f \in S \subseteq [\![J]\!]$, we have $\text{red}(f) \in \text{m-rad}\,(J)$ by Lemma 2.3.6(b). This explains the containment $\text{m-rad}\,(J) \supseteq T$, hence $\text{m-rad}\,(J) \supseteq K$.

For the reverse containment, let $g \in [\![\text{m-rad}\,(J)]\!] = \text{rad}\,(J) \bigcap [\![R]\!]$. Then there is an integer $n \geqslant 1$ such that $g^n \in [\![J]\!]$. It follows that there is a monomial $f \in S$ such that $f \big| g^n$. It follows that $\text{red}(f) \big| \text{red}(g^n) = \text{red}(g) \big| g$, so we have $g \in (\text{red}(f))R \subseteq (T)R = K$. It follows that $\text{m-rad}\,(J) = (\text{m-rad}\,(J))R \subseteq K$. $\square$

In the notation of Theorem 2.3.7, if the generating sequence $f_1, \ldots, f_n$ is irredundant, then the generating sequence $\text{red}(f_1), \ldots, \text{red}(f_n)$ of $\text{m-rad}\,(J)$ may be redundant. Indeed, in the ring $R = A[X, Y]$, the sequence X^2Y, XY^2 is an irredundant monomial generating sequence for the ideal $J = (X^2Y, XY^2)R$. However, we have $\text{red}(X^2Y) = XY = \text{red}(XY^2)$, so the generating sequence XY, XY of $\text{m-rad}\,(J)$ from Theorem 2.3.7 is redundant.

We end this section with an important special case of Theorem 2.3.7.

COROLLARY 2.3.8. *Set $R = A[X_1, \ldots, X_d]$ and set $J = (X_{t_1}^{e_1}, \ldots, X_{t_k}^{e_k})R$ where $k, t_1, \ldots, t_k, e_1, \ldots, e_k \geqslant 1$ are such that $1 \leqslant t_1 < \cdots < t_k \leqslant d$. Then $\text{m-rad}\,(J) = (X_{t_1}, \ldots, X_{t_k})R$*

PROOF. For $i = 1, \ldots, k$ we have $\text{red}(X_{t_i}^{e_i}) = X_{t_i}$, so the result follows from Theorem 2.3.7. $\square$

Exercises.

EXERCISE 2.3.9. Set $R = A[X_1, \ldots, X_d]$. Let J be a monomial ideal in R.

(a) Prove that if A is an integral domain, then $\text{m-rad}\,(J) = \text{rad}\,(J)$.

(b) Prove that if A is reduced, then $\text{m-rad}\,(J) = \text{rad}\,(J)$.

(c) Prove that if $J \neq R$ and $\text{m-rad}\,(J) = \text{rad}\,(J)$, then A is reduced.

See Exercises 2.1.16–2.1.19.

EXERCISE 2.3.10. Set $R = A[X,Y,Z]$, and consider the monomial ideals $I = (X^3, Y^2Z^4)R$ and $J = (X^4Y, Y^3, X^2Y^3Z^2, Z^9)R$. Compute irredundant monomial generating sequences for $\text{m-rad}\,(I)$ and $\text{m-rad}\,(J)$. Justify your answers.

EXERCISE 2.3.11. Set $R = A[X_1, \ldots, X_d]$. Let $f_1, \ldots, f_s, g_1, \ldots, g_t \in [\![R]\!]$, and set $I = (f_1, \ldots, f_s)R$ and $J = (g_1, \ldots, g_t)R$.

(a) Prove that $\text{m-rad}\,(I) \subseteq \text{m-rad}\,(J)$ if and only if for each $i = 1, 2, \ldots, s$ there exists a positive integer n_i such that $f_i^{n_i} \in J$.
(b) Prove that $\text{m-rad}\,(I) = \text{m-rad}\,(J)$ if and only if for each $i = 1, 2, \ldots, s$ there exists a positive integer n_i such that $f_i^{n_i} \in J$, and for each $j = 1, 2, \ldots, t$ there exists a positive integer m_j such that $g_j^{m_j} \in I$.
(c) Assume that $I \subseteq J$. Prove that $\text{m-rad}\,(I) = \text{m-rad}\,(J)$ if and only if for each $j = 1, 2, \ldots, t$ there exists an integer m_j such that $g_j^{m_j} \in I$.

Compare these properties with Fact A.6.7.

EXERCISE 2.3.12. Set $R = A[X_1, \ldots, X_d]$. Let I, J be monomial ideals in R.

(a) Prove that $\text{m-rad}\,(I) \subseteq \text{m-rad}\,(J)$ if and only if $\text{rad}\,(I) \subseteq \text{rad}\,(J)$.
(b) Prove that $\text{m-rad}\,(I) = \text{m-rad}\,(J)$ if and only if $\text{rad}\,(I) = \text{rad}\,(J)$.

*EXERCISE 2.3.13. Set $R = A[X_1, \ldots, X_d]$, and $\mathfrak{X} = (X_1, \ldots, X_d)R$. Let I be a monomial ideal such that $I \neq R$. Prove that the following conditions are equivalent:

(i) $\text{m-rad}\,(I) = \mathfrak{X}$;
(ii) $\text{rad}\,(I) = \text{rad}\,(\mathfrak{X})$;
(iii) an irredundant monomial generating sequence for I contains a power of each variable;
(iv) for each $i = 1, \ldots, d$ there exists an integer $n_i > 0$ such that $X_i^{n_i} \in I$; and
(v) the set $[\![R]\!] \smallsetminus [\![I]\!]$ is finite.

In particular, we have $\text{m-rad}\,(\mathfrak{X}) = \mathfrak{X}$. (This exercise is used in the proof of Proposition 6.1.7.)

*EXERCISE 2.3.14. Set $R = A[X_1, \ldots, X_d]$ and $\mathfrak{X} = (X_1, \ldots, X_d)R$. Consider monomial ideals $I_1, \ldots, I_n$ of R such that $I_j \neq R$ for $j = 1, \ldots, n$. Prove that the following conditions are equivalent:

(i) $\text{m-rad}\,(I_j) = \mathfrak{X}$ for $j = 1, \ldots, n$;
(ii) $\text{m-rad}\,(I_1 \cdots I_n) = \mathfrak{X}$; and
(iii) $\text{m-rad}\,(I_1 \bigcap \cdots \bigcap I_n) = \mathfrak{X}$.

(This exercise is used in the proof of Theorem 6.1.8.)

EXERCISE 2.3.15. Set $R = A[X_1, \ldots, X_d]$. Let $I_1, \ldots, I_n$ be monomial ideals in R and set $\mathfrak{X} = (X_1, \ldots, X_d)R$.

(a) Prove that if $\text{m-rad}\,(I_j) = \mathfrak{X}$ for $j = 1, \ldots, n$, then $\text{m-rad}\,(I_1 + \cdots + I_n) = \mathfrak{X}$.
(b) Prove or give a counter-example for the following: if $\text{m-rad}\,(I_1 + \cdots + I_n) = \mathfrak{X}$, then $\text{m-rad}\,(I_j) = \mathfrak{X}$ for $j = 1, \ldots, n$.

EXERCISE 2.3.16. Set $R = A[X_1, \ldots, X_d]$. Set $\mathfrak{X} = (X_1, \ldots, X_d)R$, and let I and J be monomial ideals of R. Prove that if $I \subseteq \mathfrak{X}$ and $\text{m-rad}\,(J) = \mathfrak{X}$, then $(J :_R I) \supsetneq J$.

Monomial Radicals in Macaulay2.

Exercises.

2.4. Colons of Monomial Ideals

In this section, A is a non-zero commutative ring with identity.

This section focuses on the colon ideal of two monomial ideals. (See Section A.5 for an introduction to colons.) Similarly to the previous section, we begin by showing that the set of monomial ideals is closed under taking colons.

Theorem 2.4.1. *Set $R = A[X_1, \ldots, X_d]$. If I and J are monomial ideals of R, then the colon ideal $(J :_R I)$ is a monomial ideal of R.*

Proof. Case 1: $I = zR$ for some monomial $z = \underline{X}^{\underline{m}} \in R$. Let S denote the set of monomials in $(J :_R I) = (J :_R zR)$ and set $K = (S)R$. By construction K is a monomial ideal such that $K \subseteq (J :_R I)$, since $S \subseteq (J :_R I)$. We claim that $K = (J :_R I)$. To show this, fix an element $f \in (J :_R I)$ and write $f = \sum_{\underline{n} \in \mathbb{N}^d}^{\text{finite}} a_{\underline{n}} \underline{X}^{\underline{n}}$. Then $fz = \sum_{\underline{n} \in \mathbb{N}^d}^{\text{finite}} a_{\underline{n}} \underline{X}^{\underline{n}+\underline{m}} \in J$. By Exercise 1.1.16 we know that if $a_{\underline{n}} \neq 0$, then $\underline{X}^{\underline{n}+\underline{m}} \in J$, since J is a monomial ideal. So, if $a_{\underline{n}} \neq 0$, then $z\underline{X}^{\underline{n}} = \underline{X}^{\underline{n}+\underline{m}} \in J$. In other words, if $a_{\underline{n}} \neq 0$, then $\underline{X}^{\underline{n}} \in (J :_R zR) = (J :_R I)$, and so $\underline{X}^{\underline{n}} \in S \subseteq (S)R = K$. It follows that $f = \sum_{\underline{n} \in \mathbb{N}^d}^{\text{finite}} a_{\underline{n}} \underline{X}^{\underline{n}} \in K$, as desired.

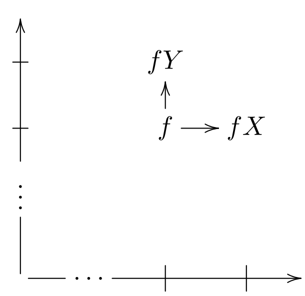
Case 2: The general case. The ideal I is generated by a finite list of monomials $z_1, \ldots, z_n$. It follows that

$$(J :_R I) = (J :_R (z_1, \ldots, z_n)R) = \bigcap_{i=1}^{n} (J :_R z_i R).$$

Thus, the ideal $(J :_R I)$ is a finite intersection of monomial ideals. By Theorem 2.1.1, it follows that $(J :_R I)$ is a monomial ideal. $\square$

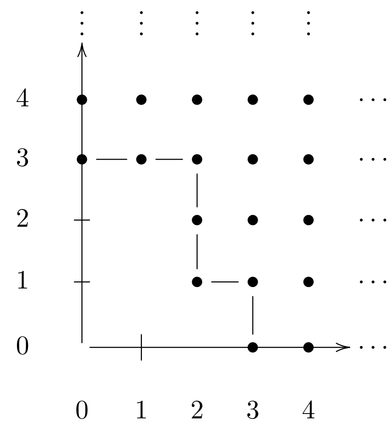
Given monomial ideals I and J of the polynomial ring $R = A[X_1, \ldots, X_d]$, it is difficult in general to identify the monomial set $[\![(J :_R I)]\!]$ in terms of $[\![I]\!]$ and $[\![J]\!]$. Of course, we have $J \subseteq (J :_R I)$, so $[\![J]\!] \subseteq [\![(J :_R I)]\!]$. Sometimes these containments are proper, and sometimes they are not proper. For Chapter 6, we are interested in the special case $I = \mathfrak{X} = (X_1, \ldots, X_d)R$. A hint as to how we might find monomials in $(J :_R \mathfrak{X}) \smallsetminus J$ is found in the graph $\Gamma(I)$, as we see in the next examples in $R = A[X, Y]$.

Let I be a monomial ideal in R and set $\mathfrak{X} = (X, Y)R$. A monomial $f \in R$ is in $(I :_R \mathfrak{X})$ if and only if $fX, fY \in I$; see Proposition A.5.3(b). The elements f, fX and fY relate to each graphically as follows.

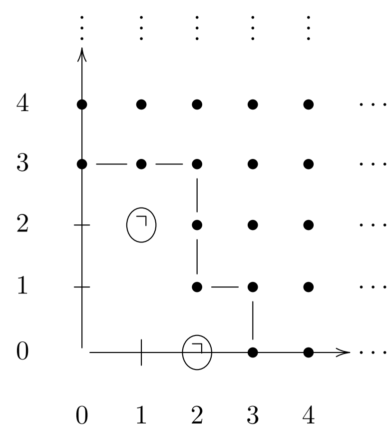


Thus, the point $(a, b) \in \mathbb{N}^2$ represents a point in $(I :_R \mathfrak{X})$ if and only if the ordered pairs $(a + 1, b)$ and $(a, b + 1)$ are in the graph $\Gamma(I)$.

For instance, consider the ideal $I = (X^3, X^2Y, Y^3)R$. The graph $\Gamma(I)$ has the following form.

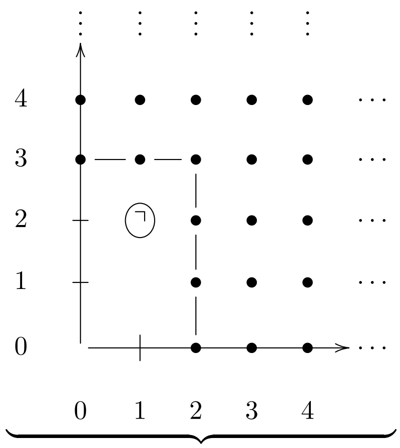


The two corners of the form $\urcorner$ show us where to find elements of $(I :_R \mathfrak{X}) \smallsetminus I$.

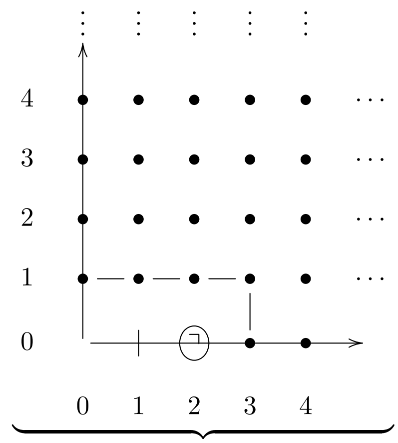


It is not difficult to show that the monomials X^2 and XY^2 are precisely the monomials in $(I :_R \mathfrak{X}) \smallsetminus I$; see Exercise 2.4.6. Note that these "corners" correspond to the "corners" in the ideals $(X^2, Y^3)R$ and $(X^3, Y)R$ in the decomposition

$I = (X^2, Y^3)R \bigcap (X^3, Y)R$; see Examples 2.1.6 and 2.1.7.



$\Gamma((X^2,Y^3)R)$



$\Gamma((X^3,Y)R)$

One point of Chapter 6 is that the "corner elements" of certain monomial ideals $J \subseteq R$ give rise to the decomposition of J as an intersection of monomial ideals of the form $(X^a, Y^b)R$.

Our next concern for Chapter 6 is the question of when $(I :_R \mathfrak{X}) \supsetneq I$.

DEFINITION 2.4.2. Set $R = A[X_1, \ldots, X_d]$. Let I be a monomial ideal of R. The monomial ideal I is *non-degenerate* if any irredundant monomial generating sequence $z_1, \ldots, z_m$ satisfies the following property: for each $i = 1, \ldots, d$ there exists an index j such that z_j is a monomial multiple of X_i; in other words, if each variable X_i is a factor of some generator z_j. The monomial ideal I is *degenerate* if it is not non-degenerate, i.e., if there is an index i between 1 and d such that for each $j = 1, \ldots, m$ the monomial z_j is not a multiple of X_i; in other words, there is a variable X_i that is not a factor of any z_j.

For example, in $R = A[X, Y]$, the ideal $(X^3)R$ is degenerate because X^3 is an irredundant monomial generating sequence, and the variable Y is not a factor of X^3. The ideal $(X^2Y^2)R$ is non-degenerate because X and Y both occur in an irredundant monomial generating sequence X^2Y^2.

In general in the ring $R = A[X_1, \ldots, X_d]$, set $\mathfrak{X} = (X_1, \ldots, X_d)R$, and let I be a non-degenerate monomial ideal of R. Then $I \subseteq \mathfrak{X}$. Indeed, if not, then we have $I = R$ by Exercise 1.1.12, so an irredundant monomial generating sequence for I is 1, which is not a multiple of any of the variables.

The next lemma says that each monomial ideal I such that $\operatorname{rad}(I) = \operatorname{rad}(\mathfrak{X})$ is non-degenerate. The condition $\operatorname{rad}(I) = \operatorname{rad}(\mathfrak{X})$ is paramount for Chapter 6. This condition is investigated in Exercises 2.3.13–2.3.16.

LEMMA 2.4.3. *Set $R = A[X_1, \ldots, X_d]$. Set $\mathfrak{X} = (X_1, \ldots, X_d)R$, and let I be a monomial ideal of R such that* $\operatorname{rad}(I) = \operatorname{rad}(\mathfrak{X})$. *Let $z_1, \ldots, z_m \in [\![I]\!]$ be an irredundant monomial generating sequence for I. Then for $i = 1, \ldots, d$ there exists $n_i \geqslant 1$ and there exists j such that $z_j = X_i^{n_i}$. In particular, the ideal I is non-degenerate.*

PROOF. First, note that the condition $\operatorname{rad}(I) = \operatorname{rad}(\mathfrak{X})$ implies that $I \subseteq \mathfrak{X} \subsetneq R$ by Exercise 1.1.14.

For $j = 1, \ldots, m$ write $z_i = \underline{X}^{\underline{n}_i}$ where $\underline{n}_i = (n_{i,1}, \ldots, n_{i,d}) \in \mathbb{N}^d$. Fix an index i such that $1 \leqslant i \leqslant d$. The condition $\operatorname{rad}(I) = \operatorname{rad}(\mathfrak{X})$ implies that $X_i^{m_i} \in I = (z_1, \ldots, z_m)R$ for some $m_i \geqslant 1$, and so $X_i^{m_i}$ is a monomial multiple of $z_j = \underline{X}^{\underline{n}_j}$ for some index j. Lemma 1.1.7 implies that $m_i \geqslant n_{j,i}$ and, for $k \neq i$ we have $0 \geqslant n_{j,k} \geqslant 0$. It follows that $n_{j,k} = 0$ whenever $k \neq i$ and so $z_j = X_i^{n_{j,i}}$. It also follows that $n_{j,i} \geqslant 1$ since, otherwise we have $n_{j,i} = 0$ so $1 = X_i^{n_{j,i}} \in I$; this contradicts the condition $I \subsetneq R$.

From this we conclude that I is non-degenerate because the variable X_i is a factor of the generator $z_j = X_i^{n_{j,i}}$. $\square$

The next theorem and its corollary give conditions on monomial ideals I and J guaranteeing that the containment $(J :_R I) \supseteq J$ is proper.

Theorem 2.4.4. *Set $R = A[X_1, \ldots, X_d]$. Let I and J be monomial ideals of R such that $I \subsetneq R$. Assume that J is non-degenerate and that $(X_2, \ldots, X_d)R \subseteq \operatorname{rad}(J)$. Then $(J :_R I) \supsetneq J$.*

Proof. We know that $(J :_R I) \supseteq J$, so we need to show that $(J :_R I) \not\subseteq J$. Let $z_1, \ldots, z_n \in [\![J]\!]$ be an irredundant monomial generating sequence for J. Since J is non-degenerate, for each index i there exists an index j such that z_j is a monomial multiple of X_i. Reorder the generators $z_1, \ldots, z_n$ to assume that z_1 is a monomial multiple of X_1, and fix a monomial $w_1 \in [\![R]\!]$ such that $z_1 = X_1 w_1$. Exercise 2.4.8 implies that $w_1 \notin J$.

Claim: For $j = 1, \ldots, d$ there exists a monomial $w_j \in [\![R]\!]$ such that $w_j \notin J$ and $X_1 w_j, \ldots, X_j w_j \in J$. We prove the claim by induction on j. The base case $j = 1$ is established in the previous paragraph.

Induction step, assume that $j > 1$ and that there is a monomial $w_{j-1} \in [\![R]\!]$ such that $w_{j-1} \notin J$ and $X_1 w_{j-1}, \ldots, X_{j-1} w_{j-1} \in J$. The assumption $(X_2, \ldots, X_d)R \subseteq \operatorname{rad}(J)$ implies that there is an integer $m_j \geqslant 1$ such that $X_j^{m_j} \in J$. It follows that $X_j^{m_j} w_{j-1} \in J$, so the set

$$K_j = \{m \geqslant 1 \mid X_j^m w_{j-1} \in J\}$$

is a non-empty set of positive integers. The Well-Ordering Axiom implies that K_j has a unique minimal element $k_j = \min(K_j)$. Set $w_j = X_j^{k_j - 1} w_{j-1}$. By the definition of k_j we have $w_j \notin J$ and $X_j w_j \in J$. Furthermore, for $i = 1, \ldots, j-1$ we have $X_i w_j = (X_i w_{j-1}) X_j^{k_j - 1} \in J$. This establishes the claim.

The monomial w_d is not in J and satisfies $X_1 w_d, \ldots, X_d w_d \in J$. It follows that w_d is in $(J :_R \mathfrak{X}) \subseteq (J :_R I)$, so $(J :_R I) \not\subseteq J$. $\square$

Corollary 2.4.5. *Set $R = A[X_1, \ldots, X_d]$. Set $\mathfrak{X} = (X_1, \ldots, X_d)R$, and let J be a monomial ideal of R. If $\operatorname{rad}(J) = \operatorname{rad}(\mathfrak{X})$, then $(J :_R \mathfrak{X}) \supsetneq J$.*

Proof. The assumption $\operatorname{rad}(J) = \operatorname{rad}(\mathfrak{X})$ implies that

$$(X_2, \ldots, X_d)R \subseteq \operatorname{rad}(\mathfrak{X}) = \operatorname{rad}(J).$$

Lemma 2.4.3 implies that J is non-degenerate. Hence, the hypotheses of Theorem 2.4.4 are satisfied with the ideal $I = \mathfrak{X}$. $\square$

Exercises.

Exercise 2.4.6. Set $R = A[X, Y]$. Set $J = (X^3, X^2Y, Y^3)R$ and $\mathfrak{X} = (X, Y)R$. Verify that the monomials in $(J :_R \mathfrak{X}) \smallsetminus J$ are XY^2 and X^2.

EXERCISE 2.4.7. Set $R = A[X,Y]$ and $\mathfrak{X} = (X,Y)R$, and find a monomial ideal I in R such that $(I :_R \mathfrak{X}) = I$; justify your answer.

*EXERCISE 2.4.8. Set $R = A[X_1,\ldots,X_d]$. Let $J \subseteq R$ be a monomial ideal, and let $z_1,\ldots,z_n \in [\![J]\!]$ be an irredundant monomial generating sequence for J. Let $f,g \in R$ be monomials such that $f \neq 1_A$ and $z_1 = fg$. Then $g \notin J$. (This exercise is used in the proof of Theorem 2.4.4.)

EXERCISE 2.4.9. Set $R = A[X,Y]$. In this exercise you are asked to work through the proof of Theorem 2.4.4 with $I = (X,Y)R$ and $J = (X^3,X^2Y^2,Y^4)R$.

(a) Prove that the hypotheses of Theorem 2.4.4 are satisfied for this ideal J.
(b) Start with $z_1 = X^3$ and follow the proof to find an element $w_2 \in (J :_R I) \smallsetminus J$; show your steps. Graph z_1, w_2, and J on the same set of coordinate axes.
(c) Start with $z_1 = X^2Y^2$ and follow the proof to find an element $w_2 \in (J :_R I) \setminus J$; show your steps. Graph z_1, w_2, and J on the same set of coordinate axes.

CHALLENGE EXERCISE 2.4.10. Set $R = A[X,Y]$ and $\mathfrak{X} = (X,Y)R$, and let I be a monomial ideal in R. Give a necessary and sufficient condition for the strictness of the containment $(I :_R \mathfrak{X}) \supseteq I$; prove this result. Do the same for an arbitrary monomial ideal in $A[X_1,\ldots,X_d]$.

Colons of Monomial Ideals in Macaulay2: Exercises.

EXERCISE 2.4.11. Set $R = \mathbb{Z}_{101}[X,Y]$, and use the ideals $J = (X^3,X^2Y,Y^3)R$ and $\mathfrak{X} = (X,Y)R$.

(a) Use Macaulay2 to verify that $(J :_R \mathfrak{X})$ is a monomial ideal where $(J :_R \mathfrak{X}) = J + (X^2,XY^2)R$ and $(J :_R \mathfrak{X}) \supsetneq J$.
(b) Use Macaulay2 to verify your answer to Exercise 2.4.7.

EXERCISE 2.4.12. Set $A = \mathbb{Z}_{101}$. Use Macaulay2 to verify that $w_2 \in (J :_R I) \smallsetminus J$ in Exercise 2.4.9(b)–(c).

2.5. Bracket Powers of Monomial Ideals

In this section, A is a non-zero commutative ring with identity.

As we mention in Section A.4, the power I^n is not generated by the powers of the generators of I. This section investigates the ideal that *is* generated by powers of the generators of I. The notation $J^{[k]}$ is used to suggest the "Frobenius powers" of an ideal when A is a field of positive characteristic.

DEFINITION 2.5.1. Set $R = A[X_1,\ldots,X_d]$. Let J be a monomial ideal of R. For $k = 1,2,\ldots$ we set $J^{[k]} = (T_k)R$ where $T_k = \{f^k \mid f \in [\![J]\!]\}$.

By definition, the ideal $J^{[k]}$ is a monomial ideal for each $k = 1,2,\ldots$. The next lemma helps us find generating sets for $J^{[k]}$; this is made explicit in Propositions 2.5.3 and 2.5.5.

LEMMA 2.5.2. *Set $R = A[X_1,\ldots,X_d]$. Consider a set of monomials $S \subseteq [\![R]\!]$ and an integer $k \geqslant 1$. Set $J = (S)R$ and $I = (\{f^k \mid f \in S\})R$. For each monomial $g \in [\![R]\!]$ we have $g \in J$ if and only if $g^k \in I$.*

PROOF. For the forward implication, we assume that $g \in J$. The ideal J is a monomial ideal, so Theorem 1.3.1 implies that there is a finite subset $S' \subseteq S$ such that $J = (S')R$. Theorem 1.1.8 implies that $g \in (f)R$ for some $f \in S'$, and it follows that $g^k \in (f^k)R \subseteq I$.

For the converse, assume that $g^k \in I$. The set $S_k = \{f^k \mid f \in S\}$ is a monomial generating set for I. Hence, there is a finite subset $S'_k \subseteq S_k$ such that $I = (S'_k)R$. Theorem 1.1.8 implies that $g^k \in (f^k)R$ for some $f^k \in S'_k$. Note that $f \in S$ by definition. Write $f = \underline{X}^{\underline{m}}$ and $g = \underline{X}^{\underline{n}}$ with $\underline{m}, \underline{n} \in \mathbb{N}^d$. Then $f^k = \underline{X}^{k\underline{m}}$ and $g^k = \underline{X}^{k\underline{n}}$, so Lemma 1.1.7 implies that $k\underline{m} \preccurlyeq k\underline{n}$. It follows readily that $\underline{m} \preccurlyeq \underline{n}$, so $g = \underline{X}^{\underline{n}} \in (\underline{X}^{\underline{m}})R = (f)R \subseteq J$. $\square$

PROPOSITION 2.5.3. *Set $R = A[X_1, \ldots, X_d]$. Let J be a monomial ideal in R.*

(a) *If S is a monomial generating set for J, then the set $S_k = \{f^k \mid f \in S\}$ is a monomial generating set for $J^{[k]}$.*
(b) *If $f_1, \ldots, f_n \in [\![J]\!]$ is a monomial generating sequence for J, then $J^{[k]} = (f_1^k, \ldots, f_n^k)R$.*

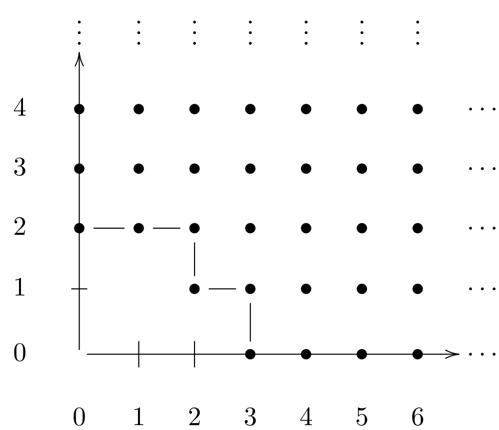
PROOF. (a) Let $T_k = \{f^k \mid f \in [\![J]\!]\}$. By definition, we have $J^{[k]} = (T_k)R$, so we need to show that $(S_k)R = (T_k)R$.

To verify the containment $(S_k)R \subseteq (T_k)R$, we need to show that $S_k \subseteq (T_k)R$. An arbitrary element of S_k has the form f^k for some $f \in S$. By definition, we have $f^k \in T_k \subseteq (T_k)R$, so $S_k \subseteq (T_k)R$, as desired.

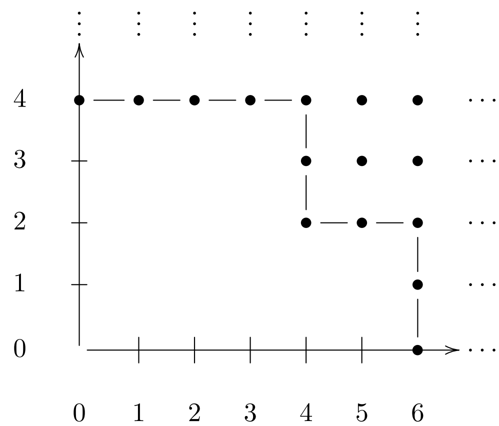
To verify the containment $(S_k)R \supseteq (T_k)R$, we need to show that $T_k \subseteq (S_k)R$. An arbitrary element of T_k has the form f^k for some $f \in [\![J]\!]$. Lemma 2.5.2 implies that $f^k \in (S_k)R$, so $T_k \subseteq (S_k)R$, as desired.

(b) This is the special case of part (a) with $S = \{f_1, \ldots, f_n\}$. $\square$

For example, in $R = A[X, Y]$, consider the ideal $J = (X^3, X^2Y, Y^2)R$ which has the following graph.



We have $J^{[2]} = (X^6, X^4Y^2, Y^4)R$ which has the following graph.



Notice that the graph of $J^{[2]}$ is essentially a scale model of the graph of J.

The next result is a useful combination of Lemma 2.5.2 Proposition 2.5.3(a). Note that it does *not* imply that $[\![J^{[k]}]\!] = \{h^k \mid h \in [\![J]\!]\}$; see Exercise 2.5.8.

LEMMA 2.5.4. *Set $R = A[X_1, \ldots, X_d]$. Let J be a monomial ideal of R, and let $g \in [\![R]\!]$ be a monomial in R. For $k = 1, 2, \ldots$ we have $g \in J$ if and only if $g^k \in J^{[k]}$.*

The next result augments Proposition 2.5.3 by showing how to find an *irredundant* monomial generating sequence for bracket powers of monomial ideals.

PROPOSITION 2.5.5. *Set $R = A[X_1, \ldots, X_d]$. Let J be a monomial ideal of R and let $f_1, \ldots, f_n \in [\![J]\!]$ be an irredundant monomial generating sequence for J. For $k = 1, 2, \ldots$ an irredundant monomial generating sequence for $J^{[k]}$ is $f_1^k, \ldots, f_n^k$.*

PROOF. By Proposition 2.5.3(b), the sequence $f_1^k, \ldots, f_n^k$ is a monomial generating sequence for $J^{[k]}$, so it suffices to show irredundancy. Suppose that the sequence is redundant. Then there are indices i, j such that $i \neq j$ and $f_i^k \in (f_j^k)R = ((f_j)R)^{[k]}$. Then Lemma 2.5.4 implies that $f_i \in (f_j)R$, contradicting the irredundancy of the original generating sequence. $\square$

The next result provides a useful criterion for checking containment and equality of bracket powers. A first application can be found in the subsequent Proposition 2.5.7.

LEMMA 2.5.6. *Set $R = A[X_1, \ldots, X_d]$. Let I and J be monomial ideals in R and fix an integer $k \geqslant 1$.*

(a) *$I \subseteq J$ if and only if $I^{[k]} \subseteq J^{[k]}$.*
(b) *$I = J$ if and only if $I^{[k]} = J^{[k]}$.*

PROOF. (a) Let $f_1, \ldots, f_m \in [\![I]\!]$ be a monomial generating sequence for I, and let $g_1, \ldots, g_n \in [\![J]\!]$ be a monomial generating sequence for J.

For the forward implication, we assume that $I \subseteq J$, and we show that $I^{[k]} \subseteq J^{[k]}$. It suffices to show that each generator $f_i^k \in I^{[k]}$ is in $J^{[k]}$. By assumption, we have $f_i \in I \subseteq J$. Lemma 2.5.4 implies that $f_i^k \in J^{[k]}$.

For the converse, we assume that $I^{[k]} \subseteq J^{[k]}$, and we show that $I \subseteq J$. For $i = 1, \ldots, m$ we have $f_i^k \in I^{[k]} \subseteq J^{[k]}$ so Lemma 2.5.4 implies that $f_i \in J$. It follows that $I = (f_1, \ldots, f_m)R \subseteq J$, as desired.

(b) We have $I = J$ if and only if $I \subseteq J$ and $J \subseteq I$. By part (a), we have ($I \subseteq J$ and $J \subseteq I$) if and only if ($I^{[k]} \subseteq J^{[k]}$ and $J^{[k]} \subseteq J^{[k]}$), that is, if and only if $I^{[k]} = J^{[k]}$. $\square$

The next result shows that the bracket power operation commutes with intersections. For this, recall that the intersection of monomial ideals is a monomial ideal by Theorem 2.1.1. Hence, the ideal $(\bigcap_{i=1}^n J_i)^{[k]}$ is defined, and it is a monomial ideal. Similarly, the ideal $\bigcap_{i=1}^n {J_i}^{[k]}$ is also a monomial ideal.

PROPOSITION 2.5.7. *Set $R = A[X_1, \ldots, X_d]$. Let $J_1, \ldots, J_n$ be monomial ideals in R. For each integer $k \geqslant 1$, we have $(\bigcap_{i=1}^n J_i)^{[k]} = \bigcap_{i=1}^n {J_i}^{[k]}$.*

PROOF. We proceed by induction on n, the number of ideals.

Base case: $n = 2$. Let $f_1, \ldots, f_m \in [\![J_1]\!]$ be a monomial generating sequence for J_1. Let $g_1, \ldots, g_n \in [\![J_2]\!]$ be a monomial generating sequence for J_2.

For the containment $(J_1 \bigcap J_2)^{[k]} \subseteq {J_1}^{[k]} \bigcap {J_2}^{[k]}$, observe that $J_1 \bigcap J_2 \subseteq J_1$, so Lemma 2.5.6(a) implies that $(J_1 \bigcap J_2)^{[k]} \subseteq {J_1}^{[k]}$. Similarly, we have $(J_1 \bigcap J_2)^{[k]} \subseteq {J_2}^{[k]}$, and hence $(J_1 \bigcap J_2)^{[k]} \subseteq {J_1}^{[k]} \bigcap {J_2}^{[k]}$.

For the containment $(J_1 \bigcap J_2)^{[k]} \supseteq {J_1}^{[k]} \bigcap {J_2}^{[k]}$, we need only show that every monomial $z \in [\![{J_1}^{[k]} \bigcap {J_2}^{[k]}]\!] = [\![{J_1}^{[k]}]\!] \bigcap [\![{J_2}^{[k]}]\!]$ is in $(J_1 \bigcap J_2)^{[k]}$. The condition $z \in [\![{J_1}^{[k]}]\!] = [\![(f_1^k, \ldots, f_m^k)R]\!]$ implies that $z \in (f_i^k)R$ for some index i. Similarly, the condition $z \in [\![{J_2}^{[k]}]\!] = [\![(g_1^k, \ldots, g_n^k)R]\!]$ implies that $z \in (g_j^k)R$ for some index j. Write $f_i = \underline{X}^{\underline{m}}$ and $g_j = \underline{X}^{\underline{n}}$, so we have $f_i^k = \underline{X}^{k\underline{m}}$ and $g_j^k = \underline{X}^{k\underline{n}}$. For $l = 1, \ldots, d$ set $p_l = \max\{m_l, n_l\}$. It is straightforward to show that $kp_l = \max\{km_l, kn_l\}$, so Lemma 2.1.4 yields the first and third equalities in the next sequence

$$z \in (f_i^k)R \bigcap (g_j^k)R = (\underline{X}^{k\underline{p}})R = ((\underline{X}^{\underline{p}})R)^{[k]} = \left((f_i)R \bigcap (g_j)R\right)^{[k]} \subseteq \left(J_1 \bigcap J_2\right)^{[k]}.$$

The second equality is by definition. The containment at the end of the sequence follows from Lemma 2.5.6(a) since $(f_i)R \bigcap (g_j)R \subseteq J_1 \bigcap J_2$.

Induction step: Exercise. $\square$

Exercises.

EXERCISE 2.5.8. Set $R = A[X_1, \ldots, X_d]$. Let J be a non-zero monomial ideal in R. Prove that for each integer $k \geqslant 2$, we have $[\![J^{[k]}]\!] \supsetneq \{h^k \mid h \in [\![J]\!]\}$.

EXERCISE 2.5.9. Set $R = A[X_1, \ldots, X_d]$. Let J be a monomial ideal in R with monomial generating sequence $f_1, \ldots, f_n$. Fix an integer $k \geqslant 1$, and show that $f_1, \ldots, f_n$ is an irredundant monomial generating sequence for J if and only if $f_1^k, \ldots, f_n^k$ is an irredundant monomial generating sequence for $J^{[k]}$.

EXERCISE 2.5.10. Set $R = A[X_1, \ldots, X_d]$. Let J be a monomial ideal of R. Prove that for $k = 1, 2, \ldots$ we have $J^{[k]} \subseteq J$ and $\operatorname{rad}\left(J^{[k]}\right) = \operatorname{rad}(J)$.

EXERCISE 2.5.11. Complete the induction step of Proposition 2.5.7.

EXERCISE 2.5.12. Set $R = A[X_1, \ldots, X_d]$, and let J be a monomial ideal in R. Prove that for each integer $n \geqslant 1$, one has $\operatorname{m-rad}(J) = \operatorname{m-rad}\left(J^{[n]}\right)$.

EXERCISE 2.5.13. Let p be a prime number and set $R = \mathbb{Z}_p[X_1, \ldots, X_d]$. Let $f_1, \ldots, f_n \in R$ and set $I = (f_1, \ldots, f_n)R$. (Note that the f_i need not be monomials.) For each integer $e \geqslant 1$, set $I^{[p^e]} = (T_{p^e})R$ where $T_{p^e} = \{f^{p^e} \mid f \in I\}$. Prove that $I^{[p^e]} = (f_1^{p^e}, \ldots, f_n^{p^e})R$. Show that the analogous result for $I^{[k]}$ need not hold when k is not a power of p.

EXERCISE 2.5.14. Set $R = A[X_1, \ldots, X_d]$. Prove or disprove the following: If I and J are monomial ideals in R, then $(IJ)^{[n]} = I^{[n]}J^{[n]}$ for each integer $n \geqslant 1$.

Bracket Powers of Monomial Ideals in Macaulay2.

In this tutorial, we show how to compute bracket powers of monomial ideals. Line `i3` contains the command used to compute the bracket power $I^{[3]}$. Note that line `i1` combines two commands in one, using the semicolon `;`. The semicolon also suppresses part of the output.

```
i1 : R=ZZ/101[x,y,z]; I=ideal(x^2,y^3,z^4,x*y,y*z);

o2 : Ideal of R

i3 : ideal apply(numgens I, i -> I_i^(3))

              6   9   12   3 3   3 3
o3 = ideal (x , y , z  , x y , y z )

o3 : Ideal of R
```

Exercises.

EXERCISE 2.5.15. Set $R = \mathbb{Z}_{101}[X, Y, Z]$, and consider the ideals $J = (XY, Z)$ and $I = (X^2Y, YZ, Z^5)R$.

(a) Use Macaulay2 to compute the ideal $I^{[4]}$.
(b) Use Macaulay2 to verify that $Y^2Z \in I$, $(Y^2Z)^5 \in I^{[5]}$, $XY \notin I$, and $(XY)^5 \notin I^{[5]}$.
(c) Use Macaulay2 to verify that $I^{[4]} \subseteq I$ and $\operatorname{rad}\left(I^{[4]}\right) = \operatorname{rad}(I)$.
(d) Use Macaulay2 to verify that $I \subseteq J$, $I^{[3]} \subseteq J^{[3]}$, $J \not\subseteq I$, and $J^{[3]} \not\subseteq I^{[3]}$.
(e) Use Macaulay2 to verify that $(I \bigcap J^{[2]})^{[3]} = I^{[3]} \bigcap (J^{[2]})^{[3]} = I^{[3]} \bigcap J^{[6]}$.
(f) Use Macaulay2 to check whether or not that $(IJ)^{[3]} = I^{[3]}J^{[3]}$.

2.6. Exploration: Generalized Bracket Powers

In this section, A is a non-zero commutative ring with identity. Set $R = A[X_1, \ldots, X_d]$, and fix a d-tuple $\underline{e} \in \mathbb{N}^d$ such that $e_1, \ldots, e_d \geqslant 1$. For a monomial $z = \underline{X}^{\underline{n}}$, set $z^{\underline{e}} = (\underline{X}^{\underline{n}})^{\underline{e}} = X_1^{n_1e_1} \cdots X_d^{n_de_d}$. Let $f, f_1, \ldots, f_m, g_1, \ldots, g_n$ be monomials in R.

In this section, we generalize the notions from Section 2.5.

EXERCISE 2.6.1. Prove that one has $f^{\underline{e}} \in (f_1^{\underline{e}}, \ldots, f_m^{\underline{e}})R$ if and only if $f \in (f_1, \ldots, f_m)R$.

EXERCISE 2.6.2. Prove that we have $(f_1,\ldots,f_m)R \subseteq (g_1,\ldots,g_n)R$ if and only if $(f_1^{\underline{e}},\ldots,f_m^{\underline{e}})R \subseteq (g_1^{\underline{e}},\ldots,g_n^{\underline{e}})R$.

EXERCISE 2.6.3. Prove that we have $(f_1,\ldots,f_m)R = (g_1,\ldots,g_n)R$ if and only if $(f_1^{\underline{e}},\ldots,f_m^{\underline{e}})R = (g_1^{\underline{e}},\ldots,g_n^{\underline{e}})R$.

DEFINITION 2.6.4. If $I = (f_1,\ldots,f_m)R$, define

$$I^{[\underline{e}]} = (f_1^{\underline{e}},\ldots,f_m^{\underline{e}})R.$$

EXERCISE 2.6.5. Prove that $I^{[\underline{e}]}$ is independent of the choice of monomial generating sequence for I.

EXERCISE 2.6.6. Prove that $I^{[\underline{e}]} \subseteq I$ and $\operatorname{rad}\left(I^{[\underline{e}]}\right) = \operatorname{rad}(I)$ and $\text{m-rad}\left(I^{[\underline{e}]}\right) = \text{m-rad}(I)$.

EXERCISE 2.6.7. Prove that $f_1,\ldots,f_n$ is an irredundant monomial generating sequence for I if and only if $f_1^{\underline{e}},\ldots,f_n^{\underline{e}}$ is an irredundant monomial generating sequence for $I^{[\underline{e}]}$.

EXERCISE 2.6.8. Let $R = A[X,Y]$ and set $I = (X^2, XY^2, Y^3)R$ and $\underline{e} = (2,3)$. Write out an irredundant monomial generating sequence for $I^{[\underline{e}]}$. Sketch the graphs $\Gamma(I)$ and $\Gamma(I^{[\underline{e}]})$, indicating the generators in each case.

EXERCISE 2.6.9. Let $J_1,\ldots,J_n$ be monomial ideals in R, and set $J = \bigcap_{i=1}^n J_i$. Prove that $J^{[\underline{e}]} = \bigcap_{i=1}^n J_i{}^{[\underline{e}]}$.

Generalized Bracket Powers in Macaulay2.

Exercises.

Conclusion

Include some history here. Talk about some of the literature from this area. Include Frobenius powers.

CHAPTER 3

M-Irreducible Ideals and Decompositions

M-irreducible ideals are, in a sense, the simplest monomial ideals, in that they cannot be written as non-trivial intersections of monomial ideals. We study these ideals in Section 3.1. In many texts, these notions are only considered when the ground ring A is a field. In this setting, the m-irreducible ideals are actually irreducible, meaning that they cannot be written as non-trivial intersections of any ideals. This is the topic of Section 3.2.

One of the main points of this book is (1) to show that every monomial ideal can be written as a finite intersection of m-irreducible monomial ideals, and (2) to show how, given a monomial ideal J to find m-irreducible ideals $J_1, \ldots, J_n$ such that $J = \bigcap_{i=1}^n J_i$. The first of these goals is accomplished in Section 3.2. The second goal is dealt with, for important special cases in Chapters 4, 6, and 7. The general case of irreducible decompositions is treated in Section 3.4. The chapter concludes with Section 3.5, which is an exploration of m-irreducible decompositions in two variables. Even though this section is optional, it is very useful for computing examples.

3.1. M-Irreducible Monomial Ideals

In this section, A is a non-zero commutative ring with identity.

We are now ready to introduce the building blocks of our decompositions. Note that our assumption $A \neq 0$ is crucial here because if $A = 0$, then $R = A[X_1, \ldots, X_d] = 0$, and it follows that every ideal $J \subseteq R$ satisfies $J = 0 = R$.

Definition 3.1.1. Set $R = A[X_1, \ldots, X_d]$. A monomial ideal $J \subsetneq R$ is *m-reducible* if there are monomial ideals $J_1, J_2 \neq J$ such that $J = J_1 \bigcap J_2$. A monomial ideal $J \subsetneq R$ is *m-irreducible* if it is not m-reducible.

By definition, a monomial ideal $J \subseteq R$ is m-irreducible if and only if it $J \neq R$ and, given two monomial ideals J_1, J_2 such that $J = J_1 \bigcap J_2$, either $J_1 = J$ or $J_2 = J$. Inductively, if J is m-irreducible and $J_1, \ldots, J_n$ are monomial ideals (with $n \geqslant 2$) such that $J = \bigcap_{i=1}^n J_i$, then $J = J_i$ for some index i.

Example 3.1.2. Set $R = A[X, Y]$. The monomial ideal $J = (X^3, X^2Y, Y^3)R$ is m-reducible. Indeed, we have

$$J = (X^2, Y^3)R \bigcap (X^3, Y)R$$

by Example 2.1.6. Also, we have $X^2 \in (X^2, Y^3)R \smallsetminus J$ so $J \neq (X^2, Y^3)R$. Also $Y \in (X^3, Y)R \smallsetminus J$, so $J \neq (X^3, Y)R$.

On the other hand, the ideals $(X^2, Y^3)R$ and $(X^3, Y)R$ are m-irreducible. This can be verified directly, or by appealing to Theorem 3.1.3.

The next theorem is the main result of this section. It characterizes the non-zero m-irreducible monomial ideals as the ideals generated by "pure powers" of the variables. See Exercise 3.1.5 for information about the zero ideal.

THEOREM 3.1.3. *Set $R = A[X_1, \ldots, X_d]$, and let J be a non-zero monomial ideal of R. The ideal J is m-irreducible if and only if there exist positive integers $k, t_1, \ldots, t_k, e_1, \ldots, e_k$ such that $1 \leqslant t_1 < \cdots < t_k \leqslant d$ and $J = (X_{t_1}^{e_1}, \ldots, X_{t_k}^{e_k})R$.*

PROOF. Assume that there are integers $k, t_1, \ldots, t_k, e_1, \ldots, e_k \geqslant 1$ such that $t_1 < \cdots < t_k \leqslant d$ and $J = (X_{t_1}^{e_1}, \ldots, X_{t_k}^{e_k})R$. Note that $J \subseteq (X_{t_i}, \ldots, X_{t_k})R \subseteq (X_1, \ldots, X_d)R$, so $J \neq R$.

Fix monomial ideals J_1, J_2 in R such that $J = J_1 \bigcap J_2$. Suppose that $J \subsetneq J_i$ for $i = 1, 2$ and fix a monomial $f_i \in [\![J_i]\!] \smallsetminus [\![J]\!]$. Write $f_1 = \underline{X}^{\underline{m}}$ and $f_2 = \underline{X}^{\underline{n}}$. For $i = 1, \ldots, d$ set $p_i = \max\{m_i, n_i\}$.

For $i = 1, \ldots, k$ we have $m_{t_i} < e_i$: otherwise, we have $m_i \geqslant e_i$ for some i, so a comparison of exponent vectors shows that $f_1 \in (X_{t_i}^{e_i})R \subseteq J$, a contradiction. Similarly, for $i = 1, \ldots, k$ we have $n_i < e_i$, and hence $p_i = \max\{m_i, n_i\} < e_i$. A similar argument shows that $\operatorname{lcm}(f_1, f_2) = \underline{X}^{\underline{p}} \notin J$. However, we have $\operatorname{lcm}(f_1, f_2) \in J_1 \bigcap J_2 = J$, a contradiction.

For the converse, assume that J is m-irreducible. Let $f_1, \ldots, f_k$ be an irredundant monomial generating sequence for J. It suffices to show that each f_i is of the form $X_{t_i}^{e_i}$. Suppose by way of contradiction that one of the f_i is not of this form. Re-order the f_j if necessary to assume that f_k is not of the form $X_{t_i}^{e_i}$. This means that we can write $f_k = X_{t_i}^{e_i} g$ where $e_i \geqslant 1$ and $X_{t_i} \nmid g$ and $g \neq 1$. Re-order the variables if necessary to assume that $f_k = X_1^e g$ where $e \geqslant 1$ and $X_1 \nmid g$ and $g \neq 1$. Set $I = (f_1, \ldots, f_{k-1}, X_1^e)R$ and $I' = (f_1, \ldots, f_{k-1}, g)R$.

Claim: $J = I \bigcap I'$. For this, we use Proposition 2.1.5 to conclude that the following sequence generated $I \bigcap I'$:

$$f_1, \ldots, f_{n-1}, \underbrace{\operatorname{lcm}(f_1, X_1^e), \operatorname{lcm}(f_1, g)}_{\in (f_1)R}, \ldots, \underbrace{\operatorname{lcm}(f_{n-1}1, X_1^e), \operatorname{lcm}(f_{n-1}, g)}_{\in (f_{n-1})R}, \underbrace{\operatorname{lcm}(X_1^e, g)}_{= f_n}.$$

Removing redundancies from this list (by Algorithm 1.3.7) we see that $I \bigcap I'$ is generated by $f_1, \ldots, f_{n-1}, f_n$. As this sequence generates J, we have the desired equality.

Claim: $J \subsetneq I$. To show that $J \subseteq I$, it suffices to show that $f_1, \ldots, f_n \in I$. The elements $f_1, \ldots, f_{n-1}$ are generators for I, by definition. Also, the element X_1^e is a generator for I, so we have $f_n = X_1^e g \in I$. To show that $J \neq I$, we need to show that $X_1^e \notin J$. Suppose by way of contradiction that $X_1^e \in J$. Then $f_i \big| X_1^e$ for some index i. Since $X_1^e \big| f_k$, this implies that $f_i \big| f_k$. The sequence $f_1, \ldots, f_k$ is irredundant, so we have $f_i = f_k$. Thus, we have $f_k = X_1^e g \big| X_1^e$. By comparing exponent vectors, we conclude that $g = 1$, a contradiction.

Similarly, we have $J \subsetneq I'$. In short, we have $J = I \bigcap I'$ and $J \subsetneq I$ and $J \subsetneq I'$. This contradicts the assumption that J is m-irreducible, completing the proof. $\square$

The next result is useful for removing redundancies from m-irreducible decompositions; see Proposition 3.3.7. Note that the conclusion is a souped up version of the definition of m-irreducible.

LEMMA 3.1.4. *Set $R = A[X_1, \ldots, X_d]$. Let $I, J_1, \ldots, J_n$ be monomial ideals in R such that I is m-irreducible. If $\bigcap_{i=1}^n J_i \subseteq I$, then there is an index j such that $J_j \subseteq I$.*

PROOF. If $I = 0$, then the condition $\bigcap_{i=1}^n J_i \subseteq I = 0$ implies that $\bigcap_{i=1}^n J_i = 0$; it is straightforward to show that this implies that $J_i = 0 = I$ for some index i. Thus, we assume that $I \neq 0$. Also, the case $n = 1$ is routine, so we assume that $n \geqslant 2$. Theorem 3.1.3 provides positive integers $k, t_1, \ldots, t_k, e_1, \ldots, e_k$ such that $1 \leqslant t_1 < \cdots < t_k \leqslant d$ such that $I = (X_{t_1}^{e_1}, \ldots, X_{t_k}^{e_k})R$.

We proceed by induction on n.

Base case: $n = 2$. Assume that $J_1 \bigcap J_2 \subseteq I$. Suppose by way of contradiction that $J_1 \not\subseteq I$ and $J_2 \not\subseteq I$. This implies that $[\![J_1]\!] \not\subseteq [\![I]\!]$ and $[\![J_2]\!] \not\subseteq [\![I]\!]$, so there are monomials $f_1 \in J_1 \smallsetminus I$ and $f_2 \in J_2 \smallsetminus I$. Write $f_1 = \underline{X}^{\underline{m}}$ and $f_2 = \underline{X}^{\underline{n}}$. For $i = 1, \ldots, d$ set $p_i = \max\{m_i, n_i\}$ so we have

$$\underline{X}^{\underline{p}} = \operatorname{lcm}(f_1, f_2) \in J_1 \bigcap J_2 \subseteq I = (X_{t_1}^{e_1}, \ldots, X_{t_k}^{e_k})R.$$

It follows that there is an index j such that $X_{t_j}^{e_j} \big| \underline{X}^{\underline{p}}$. Comparing exponent vectors, we find that $e_j \leqslant p_{t_j} = \max\{m_{t_j}, n_{t_j}\}$. It follows that either $e_j \leqslant m_{t_j}$ or $e_j \leqslant n_{t_j}$. If $e_j \leqslant m_{t_j}$, then another comparison of exponent vectors implies that $X_{t_j}^{e_j} \big| \underline{X}^{\underline{m}} = f_1$, so $f_1 \in (X_{t_j}^{e_j})R \subseteq I$, a contradiction. Similarly, if $e_j \leqslant n_{t_j}$, we conclude that $f_2 \in I$, a contradiction. This concludes the proof of the base case.

Induction step: Exercise. $\square$

Exercises.

*EXERCISE 3.1.5. Set $R = A[X_1, \ldots, X_d]$. Prove that 0 is m-irreducible. (This exercise is used in the proof of Theorem 3.3.3.)

*EXERCISE 3.1.6. Set $R = A[X_1, \ldots, X_d]$. Let J be a monomial ideal in R.

(a) Prove that if J is non-zero and m-irreducible, then there are positive integers $n, t_1, \ldots, t_n$ such that $\text{m-rad}\,(J) = (X_{t_1}, \ldots, X_{t_n})R$.
(b) Prove that if J is m-irreducible, then $\text{m-rad}\,(J)$ is m-irreducible.
(c) Prove or disprove the following: if $\text{m-rad}\,(J)$ is m-irreducible, then J is m-irreducible.

(This exercise is used in the proof of Proposition 7.1.1.)

EXERCISE 3.1.7. Set $R = A[X]$. Prove that every monomial ideal in R is m-irreducible.

*EXERCISE 3.1.8. Set $R = A[X_1, \ldots, X_d]$. Let $k, t_1, \ldots, t_k, e_1, \ldots, e_k \geqslant 1$ be integers such that $1 \leqslant t_1 < \cdots < t_k \leqslant d$, and set $J = (X_{t_1}^{e_1}, \ldots, X_{t_k}^{e_k})R$. Prove that the monomial $X_{t_1}^{e_1-1} \cdots X_{t_k}^{e_k-1}$ is not in J. (This exercise is used in the proof of Theorem 3.2.4.)

EXERCISE 3.1.9. Set $R = A[X_1, \ldots, X_d]$. Let J be a non-zero m-irreducible monomial ideal in R. Prove or disprove the following: If $\{I_\lambda\}_{\lambda \in \Lambda}$ is a (possibly infinite) set of monomial ideals in R such that $J = \bigcap_{\lambda \in \Lambda} I_\lambda$, then there is an index $\lambda \in \Lambda$ such that $J = I_\lambda$.

EXERCISE 3.1.10. Set $R = A[X_1, \ldots, X_d]$. Let J be a monomial ideal in R such that $J \neq R$. Prove that the following conditions are equivalent:

(i) J is m-irreducible;
(ii) for all monomial ideal J_1, J_2 if $J_1 \bigcap J_2 \subseteq J$, then either $J_1 \subseteq J$ or $J_2 \subseteq J$; and
(iii) for all monomials $f, g \in [\![R]\!]$ if $\operatorname{lcm}(f, g) \in J$, then either $f \in J$ or $g \in J$.

EXERCISE 3.1.11. Complete the induction step of Lemma 3.1.4.

EXERCISE 3.1.12. Set $R = A[X_1, \ldots, X_d]$, and consider a chain $J_1 \supseteq J_2 \supseteq J_3 \supseteq \cdots$ of m-irreducible monomial ideals of R. Prove that $\bigcap_{i=1}^{\infty} J_i$ is m-irreducible.

M-Irreducible Monomial Ideals in Macaulay2.

Exercises.

3.2. Irreducible Ideals (optional)

In this section, A is a non-zero commutative ring with identity.

The notion of m-irreducibility for monomial ideals is derived from the notion of irreducibility for arbitrary ideals, which is the focus of this section. In words, an ideal is irreducible if it cannot be written as a non-trivial intersection of two ideals.

DEFINITION 3.2.1. An ideal $J \subsetneq A$ is *reducible* if there are ideals $J_1, J_2 \neq J$ such that $J = J_1 \bigcap J_2$. An ideal $J \subsetneq A$ is *irreducible* if it is not reducible.

By definition, an ideal $J \subseteq A$ is irreducible if and only if $J \neq A$, and given two ideals J_1, J_2 such that $J = J_1 \bigcap J_2$, either $J_1 = J$ or $J_2 = J$. Inductively, if J is irreducible and $J_1, \ldots, J_n$ are ideals (with $n \geqslant 2$) such that $J = \bigcap_{i=1}^{n} J_i$, then $J = J_i$ for some index i.

For example, the ideal $0 \subseteq \mathbb{Z}$ is irreducible. If p is a prime number and n is a positive integer, then the ideal $p^n\mathbb{Z} \subseteq \mathbb{Z}$ is irreducible. These are the only irreducible ideals of $\mathbb{Z}$; for instance, we have $6\mathbb{Z} = 3\mathbb{Z} \bigcap 2\mathbb{Z}$. In the ring $\mathbb{Z}_6$, the ideal 0 is reducible since $2\mathbb{Z}_6 \bigcap 3\mathbb{Z}_6 = 0$. In the ring $\mathbb{Z}_4$, the ideal 0 is irreducible since the only ideals in $\mathbb{Z}_4$ are 0, $2\mathbb{Z}_4$ and $\mathbb{Z}_4$.

Let k be a field and let R be the polynomial ring $R = k[X]$ in one variable. For each $a \in k$ and each positive integer n, the ideal $(X - a)^n R \subseteq R$ is irreducible.

The main result of this section is Theorem 3.2.4. It shows that, when A is an integral domain, every m-irreducible monomial ideal is also irreducible. It's proof uses the following notion.

DEFINITION 3.2.2. Set $R = A[X_1, \ldots, X_d]$. For each $f = \sum_{\underline{n}\in\mathbb{N}^d}^{\text{finite}} a_{\underline{n}} \underline{X}^{\underline{n}} \in R$, the *support* of f is the set $\gamma(f) = \{\underline{n} \in \mathbb{N}^d \mid a_{\underline{n}} \neq 0\}$.

For instance, the support of the polynomial $f = X^2 + XY + X^2Z^3 - XY^2Z^3$ in $A[X, Y, Z]$ is the set $\gamma(f) = \{(2, 0, 0), (1, 1, 0), (2, 0, 3), (1, 2, 3)\} \subseteq \mathbb{N}^3$. In general, $\gamma(f)$ is a finite set such that $f = \sum_{\underline{n}\in\gamma(f)} a_{\underline{n}} \underline{X}^{\underline{n}}$. Furthermore, we have $\gamma(f) = \emptyset$ if and only if $f = 0$.

The following technical lemma is included for the proof of Theorem 3.2.4.

LEMMA 3.2.3. *Set $R = A[X_1, \ldots, X_d]$. Fix positive integers $k, e_1, \ldots, e_k$ and set $J = (X_1^{e_1}, \ldots, X_k^{e_k})R$. Let I be an ideal of R such that $J \subsetneq I$. Then there is a polynomial*

$$h_k = z\widehat{h}(X_{k+1}, \ldots, X_d)$$

in $I \smallsetminus J$ where $z = X_1^{e_1-1} \cdots X_k^{e_k-1}$.

PROOF. Fix a polynomial $h \in I \smallsetminus J$. Then we have

$$h = \sum_{\underline{n}\in\gamma(h)} a_{\underline{n}} \underline{X}^{\underline{n}} = \sum_{\substack{\underline{n}\in\gamma(h)\\ \underline{n}\notin\Gamma(J)}} a_{\underline{n}} \underline{X}^{\underline{n}} + \sum_{\substack{\underline{n}\in\gamma(h)\\ \underline{n}\in\Gamma(J)}} a_{\underline{n}} \underline{X}^{\underline{n}} = f + g$$

where

$$f = \sum_{\substack{\underline{n}\in\gamma(h)\\ \underline{n}\notin\Gamma(J)}} a_{\underline{n}}\underline{X}^{\underline{n}} \qquad \text{and} \qquad g = \sum_{\substack{\underline{n}\in\gamma(h)\\ \underline{n}\in\Gamma(J)}} a_{\underline{n}}\underline{X}^{\underline{n}}.$$

By construction, every monomial occuring in g is in J, so $g \in J$. On the other hand, since $h \notin J$ and $g \in J$, we have $f = h - g \notin J$. In particular, we have $f \neq 0$. Also, we have $h \in I$ by assumption, so the condition $g \in J \subseteq I$ implies that $f = h - g \in I$.

Furthermore, we have

$$\gamma(f) = \{\underline{n} \in \gamma(h) \mid \underline{n} \notin \Gamma(J)\}$$

so for each $\underline{n} \in \gamma(f)$ and for $i = 1, \ldots, k$, we have $n_i < e_i$. Indeed, if $n_i \geqslant e_i$, then $\underline{X}^{\underline{n}} \in (X_i^{e_i})R \subseteq J$, contradicting the condition $\underline{n} \notin \Gamma(J)$.

(In a sense, the existence of f is stronger than the existence of h. Not only is f in I and not in J, but also no monomial occurring in f is in P. For this reason, we turn our attention from h to f.)

Claim: For $j = 1, \ldots, k$ there exists a polynomial $h_j \in I \smallsetminus J$ such that for each $\underline{n} \in \gamma(h_j)$, we have $n_i = e_i - 1$ when $1 \leqslant i \leqslant j$ and we have $n_i \leqslant e_i$ when $j + 1 \leqslant i \leqslant k$. We prove the claim by induction on j.

Base case: $j = 1$. Consider the powers of X_1 appearing in the monomials of f, and set

$$r_1 = \min\{n_1 \in \mathbb{N} \mid \underline{n} \in \gamma(f)\}$$

which is the smallest of these powers. It follows that $r_1 < e_1$ since, if not, then every monomial occurring in f would be in $(X_1^{e_1})R \subseteq J$; this would imply that $f \in J$, a contradiction. This implies that $e_1 - r_1 > 0$, that is, that $e_1 - r_1 \geqslant 1$.

Write

$$f = \sum_{\substack{\underline{n}\in\gamma(f)\\ n_1=r_1}} a_{\underline{n}}\underline{X}^{\underline{n}} + \sum_{\substack{\underline{n}\in\gamma(f)\\ n_1>r_1}} a_{\underline{n}}\underline{X}^{\underline{n}} = f_1 + g_1$$

where

$$f_1 = \sum_{\substack{\underline{n}\in\gamma(f)\\ n_1=r_1}} a_{\underline{n}}\underline{X}^{\underline{n}} \qquad \text{and} \qquad g = \sum_{\substack{\underline{n}\in\gamma(f)\\ n_1>r_1}} a_{\underline{n}}\underline{X}^{\underline{n}}$$

and note that

$$\gamma(f_1) = \{\underline{n} \in \gamma(f) \mid n_1 = r_1\} \neq \emptyset$$
$$\gamma(g_1) = \{\underline{n} \in \gamma(f) \mid n_1 \geqslant r_1 + 1\}.$$

We set $h_1 = X_1^{e_1 - r_1 - 1} f_1 \neq 0$.

To show that h_1 has the desired properties, we first show that $X_1^{e_1-r_1-1}g_1 \in J \subseteq I$. For each d-tuple $\underline{n} \in \gamma(g_1)$ we have $n_1 \geqslant r_1 + 1$. By construction, we have

$$X_1^{e_1-r_1-1}g_1 = X_1^{e_1-r_1-1}\sum_{\underline{n}\in\gamma(g_1)} a_{\underline{n}}\underline{X}^{\underline{n}} = \sum_{\underline{n}\in\gamma(g_1)} a_{\underline{n}}X_1^{e_1-r_1-1}\underline{X}^{\underline{n}}.$$

It follows that every d-tuple $\underline{m} \in \gamma(X_1^{p_1-r_1}g_1)$ satisfies

$$m_1 = (e_1 - r_1 - 1) + n_1 \geqslant (e_1 - r_1 - 1) + r_1 + 1 = e_1$$

so $X_1^{e_1-r_1-1}g_1 \in (X_1^{e_1})R \subseteq J$.

Since $f \in I$, it follows that

$$h_1 = X_1^{e_1-r_1-1}f_1 = X_1^{e_1-r_1-1}f - X_1^{e_1-r_1-1}g_1 \in I.$$

Each monomial occurring in h_1 has the form $\underline{X}^{\underline{m}} = X_1^{e_1-r_1-1}\underline{X}^{\underline{n}}$ for some $\underline{n} \in \gamma(f_1)$. The condition $\underline{n} \in \gamma(f_1)$ implies that $n_1 = r_1$ so

$$m_1 = e_1 - r_1 - 1 + n_1 = e_1 - r_1 + r_1 - 1 = e_1 - 1.$$

Furthermore, for $i \geqslant 2$, the condition $\underline{n} \in \gamma(f_1) \subset \gamma(f)$ implies that $n_i < e_i$, that is $n_i \leqslant e_i - 1$, so $m_i = n_i \leqslant e_i - 1$.

To complete the proof of the base case, we need to show that $h_1 \notin J$. Since J is a monomial ideal, it suffices to show that no monomial $\underline{X}^{\underline{m}}$ occurring in h_1 is in J. Again write $\underline{X}^{\underline{m}} = X_1^{p_1-r_1}\underline{X}^{\underline{n}}$ for some $\underline{n} \in \gamma(f_1)$, and suppose that $\underline{X}^{\underline{m}} \in J = (X_1^{e_1}, \ldots, X_k^{e_k})R$. Theorem 1.1.8 implies $\underline{X}^{\underline{m}} \in (X_i^{e_i})R$ for some $i \leqslant k$, so $m_i \geqslant e_i$ by Lemma 1.1.7. This contradicts the condition $m_i \leqslant e_i - 1$, which has already been shown for each i.

This completes the proof of the base case of our induction. The induction step is left as an exercise. This step is quite similar to the base case. Here are some hints. Assume that $1 \leqslant j \leqslant d-1$ and that h_j has been constructed. We want to construct h_{j+1}. Set

$$r_{j+1} = \min\{n_{j+1} \in \mathbb{N} \mid \underline{n} \in \gamma(h_j)\}$$

and show that $r_{j+1} \leqslant p_{j+1}$. Then write

$$h_j = \sum_{\substack{\underline{n}\in\gamma(h_n)\\ n_{j+1}=r_{j+1}}} a_{\underline{n}}\underline{X}^{\underline{n}} + \sum_{\substack{\underline{n}\in\gamma(h_n)\\ n_{j+1}=r_{j+1}}} a_{\underline{n}}\underline{X}^{\underline{n}} = f_{j+1} + g_{j+1}.$$

Set $h_{j+1} = X_{j+1}^{p_{j+1}-r_{j+1}} f_{j+1}$ and show that this polynomial satisfies the desired properties.

It follows that there is a polynomial $h_k \in I \smallsetminus J$ such that for each $\underline{n} \in \gamma(h_k)$, we have $n_i = e_i - 1$ when $1 \leqslant i \leqslant k$. In other words, every monomial occurring in h_k has the form zw where w is a monomial in $X_{k+1}, \ldots, X_d$. This implies that there is a polynomial $\widehat{h}(X_{k+1}, \ldots, X_d)$ such that $h_k = z\widehat{h}(X_{k+1}, \ldots, X_d)$, as desired. □

The next theorem is the main result of this section. Note that Exercises 3.2.6, 3.2.9, and 3.2.10 show why the integral domain assumption is essential. Also, not every irreducible ideal in a polynomial ring over an integral domain is a monomial ideal. For instance, let k be a field and let R denote the polynomial ring $R = k[X]$ in one variable. Then the ideal $(X+1)R$ is irreducible.

THEOREM 3.2.4. *Let A be an integral domain, and set $R = A[X_1, \ldots, X_d]$. A non-zero monomial ideal $J \subseteq R$ is irreducible if and only if it is m-irreducible.*

PROOF. The forward implication is straightforward: if J cannot be written as a non-trivial intersection of any two ideals, it cannot be written as a non-trivial intersection of two monomial ideals.

For the converse, assume that J is m-irreducible. Theorem 3.1.3, yields positive integers $k, t_1, \ldots, t_k, e_1, \ldots, e_k$ such that $1 \leqslant t_1 < \cdots < t_k \leqslant d$ such that $J = (X_{t_1}^{e_1}, \ldots, X_{t_k}^{e_k})R$. By re-ordering the variables if necessary, we may assume without loss of generality that $J = (X_1^{e_1}, \ldots, X_k^{e_k})R$. Set $z = X_1^{e_1-1} \cdots X_n^{e_n-1}$, and note that Exercise 3.1.8 implies that $z \notin J$.

By way of contradiction, suppose that there are ideals $I, K \subseteq R$ such that $J = I \bigcap K$ and $J \subsetneq I$ and $J \subsetneq K$. Lemma 3.2.3 provides polynomials

$$f_k = z\widehat{f}(X_{k+1}, \ldots, X_d) \in I \smallsetminus J$$
$$g_k = z\widehat{g}(X_{k+1}, \ldots, X_d) \in K \smallsetminus J.$$

Write $\widehat{f} = \widehat{f}(X_{k+1}, \ldots, X_d)$ and $\widehat{g} = \widehat{g}(X_{k+1}, \ldots, X_d)$. Since $f_k \in I$, we have $z\widehat{f}\widehat{g} = f_k\widehat{g} \in I$. Similarly, the condition $g_k \in K$ implies that $z\widehat{f}\widehat{g} \in K$, hence $z\widehat{f}\widehat{g} \in I \bigcap K = J$.

Because of the conditions $\widehat{f} = \widehat{f}(X_{k+1}, \ldots, X_d)$ and $\widehat{g} = \widehat{g}(X_{k+1}, \ldots, X_d)$, every monomial occurring in $z\widehat{f}\widehat{g}$ has the form

$$w = zv = X_1^{e_1-1} \cdots X_n^{e_n-1} X_{n+1}^{m_{n+1}} \cdots X_d^{m_d}.$$

Since J is a monomial ideal, every monomial occurring in $z\widehat{f}\widehat{g}$ is in J; see Exercise 1.1.16. The condition $w \in J$ implies that there is an index j such that $1 \leqslant j \leqslant k$ and $X_j^{e_j} \big| w$. By comparing exponent vectors, we deduce that $e_j \leqslant e_j - 1$, which is impossible.

We conclude that the polynomial $z\widehat{f}\widehat{g}$ does not have any monomials, that is, we have $z\widehat{f}\widehat{g} = 0$. Since R is an integral domain and z is a monomial, it follows that either $\widehat{f} = 0$ or $\widehat{g} = 0$. If $\widehat{f} = 0$, then $0 = z\widehat{f} = f_k \notin J$, which is impossible. A similar contradiction arises if $\widehat{g} = 0$. Thus, the ideal J is irreducible, as desired. $\square$

Exercises.

EXERCISE 3.2.5. Prove that if A is an integral domain, then 0 is irreducible in A.

EXERCISE 3.2.6. Set $R = A[X_1, \ldots, X_d]$.

(a) Prove that the ideal 0 is irreducible in R if and only if it is irreducible in A.
(b) Prove that if A is a field, then 0 is irreducible in R.
(c) Prove that if A is an integral domain, then 0 is irreducible in R.

EXERCISE 3.2.7. Let $I \subseteq A$ be an ideal.

(a) Assume that I has the following property: there exists an element $f \in R$ such that f is not in I, but $f \in J$ for every ideal J of R that properly contains I. Prove that I is irreducible.
(b) Does the converse of part (a) hold? That is, if I is irreducible, must there exist an element $f \in R$ such that f is not in I, but $f \in J$ for every ideal J of R that properly contains I?

EXERCISE 3.2.8. Set $R = \mathbb{Q}[X, Y, Z]$. Set $J = (X^4, Y^5, Z^3)R$ and

$$h = 2X^2Y + 3X^2YZ^2 + 5X^2Y^2 + 2X^2Y^4Z + X^3Y^2 + 9X^4Y^2 + 6XY^4Z^4 + 11Y^3Z^5 + Y^6$$

and suppose that I is an ideal of R that contains h. Work through the proof of Lemma 3.2.3 in this special case by completing the following steps.

(a) Prove that $h \notin J$.
(b) List the elements in the set $\gamma(h)$.
(c) What is $a_{(4,2,0)}$?
(d) Find f and g.
(e) Find r_1. Is $r_1 \leqslant 3$?
(f) Find f_1 and g_1.

(g) Find h_1. Does h_1 have the property that X appears raised to the power 3 in each monomial of h_1, while Y appears raised to a power of at most 4 and Z appears raised to a power of at most 2?
(h) Find r_2. Is $r_2 \leqslant 4$?
(i) Find f_2 and g_2.
(j) Find h_2. Does h_2 have the property that X appears raised to the power 3 in each monomial of h_2, while Y appears raised to a power of at most 4 and Z appears raised to a power of at most 2?
(k) Find r_3. Is $r_3 \leqslant 2$?
(l) Find f_3 and g_3.
(m) Find h_3. Does h_3 have the property that X appears raised to the power 3 in each monomial of h_3, while Y appears raised to a power of at most 4 and Z appears raised to a power of at most 2?
(n) What is $\widehat{h}$? What is z? Is it true that $h_3 = z\widehat{h}$?

EXERCISE 3.2.9. Find an example of a commutative ring A with identity such that the ideal $(X_1, \ldots, X_d)R$ in the polynomial ring $R = A[X_1, \ldots, X_d]$ is reducible.

EXERCISE 3.2.10. Set $R = A[X_1, \ldots, X_d]$. Prove that the following conditions are equivalent:
(a) the ideal 0 is irreducible in A;
(b) R has an irreducible monomial ideal; and
(c) every non-zero m-irreducible monomial ideal $J \subsetneq R$ is irreducible.

EXERCISE 3.2.11. Let J be a non-zero irreducible ideal in A. Prove or disprove the following: If $\{I_\lambda\}_{\lambda \in \Lambda}$ is a (possibly infinite) set of ideals in A such that $J = \bigcap_{\lambda \in \Lambda} I_\lambda$, then there is an index $\lambda \in \Lambda$ such that $J = I_\lambda$.

EXERCISE 3.2.12. We say that an ideal J in A is *prime* if it satisfies the following condition: for all $f, g \in A$ if $fg \in J$, then either $f \in J$ or $g \in J$.
(a) Prove that 0 is prime if and only if A is an integral domain.
(b) Prove that the non-zero prime ideals of $\mathbb{Z}$ are the ideals of the form $p\mathbb{Z}$ where p is a prime number. (This is where the name "prime ideal" comes from.)
(c) Let n be an integer such that $n \geqslant 2$. Prove that the prime ideals of $\mathbb{Z}_n$ are the ideals $p\mathbb{Z}_n$ such that p is a prime integer such that $p \big| n$.
(d) Let k be a field and set $R = k[X_1, \ldots, X_d]$. Prove that each ideal of the form $(X_{i_1}, \ldots, X_{i_n})R$ is prime. (It can be shown that R has infinitely many prime ideals, once one knows Gauss' Theorem which states that R is a unique factorization domain.)
(e) Prove that the following conditions are equivalent:
    (i) J is prime;
    (ii) for all ideals I and K if $IK \subseteq J$, then either $I \subseteq J$ or $K \subseteq J$; and
    (iii) J is irreducible and $\operatorname{rad}(J) = J$.
    (Here is an outline for the proof of (iii) $\Longrightarrow$ (i). Assume that J is irreducible and $\operatorname{rad}(J) = J$, and suppose that J is not prime. Then there exist $f, g \in A \smallsetminus J$ such that $fg \in J$. Set $I = J + fA$ and $K = J + gA$. The containments $IK \subseteq J \subseteq I \bigcap K$ imply that $J = \operatorname{rad}(J) = \operatorname{rad}(I \bigcap K) = \operatorname{rad}(I) \bigcap \operatorname{rad}(K)$. Since J is irreducible, we have $J = \operatorname{rad}(I)$ or $J = \operatorname{rad}(K)$. The fact that $f \in I \subseteq \operatorname{rad}(I)$ and $g \in K \subseteq \operatorname{rad}(K)$ yield a contradiction.)

Irreducible Ideals in Macaulay2.

Exercises.

3.3. M-Irreducible Decompositions

In this section, A is a non-zero commutative ring with identity.

Section 3.1 characterizes the monomial ideals that cannot be decomposed as non-trivial intersections of two monomial ideals. The next step is to show that every monomial ideal can be decomposed in terms of these ideals.

DEFINITION 3.3.1. Set $R = A[X_1, \ldots, X_d]$. Let $J \subsetneq R$ be a monomial ideal. An *m-irreducible decomposition* of J is an expression $J = \bigcap_{i=1}^{n} J_i$ where each J_i is m-irreducible.

EXAMPLE 3.3.2. Set $R = A[X, Y]$. An m-irreducible decomposition of the monomial ideal $J = (X^3, X^2Y, Y^3)R$ is

$$J = (X^2, Y^3)R \bigcap (X^3, Y)R.$$

See Example 3.1.2 and Theorem 3.1.3.

The next result accomplishes goal (1) from the introduction of this chapter by showing that every monomial ideal admits an m-irreducible decomposition. The proof is essentially due to Emmy Noether. Below, we discuss conditions guaranteeing that such decompositions are unique.

THEOREM 3.3.3. *Set $R = A[X_1, \ldots, X_d]$. If $J \subsetneq R$ is a monomial ideal, then there are m-irreducible monomial ideals $J_1, \ldots, J_n$ of R such that $J = \bigcap_{i=1}^{n} J_i$.*

PROOF. If $J = 0$, then J is m-irreducible by Exercise 3.1.5, so it is an intersection of one m-irreducible monomial ideal.

Suppose that there is a non-zero monomial ideal $J \subsetneq R$ that is not an intersection of finitely many m-irreducible monomial ideals of R. Then the set

$$\Sigma = \{\text{non-zero monomial ideals } J \subsetneq R \mid J \text{ is not an intersection of finitely many m-irreducible monomial ideals of } R\}$$

is a non-empty set of monomial ideals of R. Theorem 1.3.3(b) implies that Σ has a maximal element J. In particular J is not m-irreducible, so there exist monomial ideals $I, K \subseteq R$ such that $J = I \bigcap K$ and $J \subsetneq I, K$. In particular, we have $0 \neq I \neq R$ and $0 \neq K \neq R$. Since J is maximal in Σ, we have $I, K \notin \Sigma$. Hence, there are m-irreducible monomial ideals $I_1, \ldots, I_m, K_1, \ldots, K_n$ such that $I = \bigcap_{j=1}^{m} I_j$ and $K = \bigcap_{i=1}^{n} K_i$. It follows that

$$J = I \bigcap K = \left(\bigcap_{j=1}^{m} I_j \right) \bigcap \left(\bigcap_{i=1}^{n} K_i \right)$$

so J is a finite intersection of m-irreducible monomial ideals, a contradiction. $\square$

As with monomial generating sequences, we are interested in finding and understanding m-irreducible decompositions that are as efficient as possible. An added benefit of such decompositions is that they are unique, as we show below.

DEFINITION 3.3.4. Set $R = A[X_1, \ldots, X_d]$. Let $J \subsetneq R$ be a monomial ideal. An m-irreducible decomposition $J = \bigcap_{i=1}^n J_i$ is *redundant* if there exist indices $i \neq i'$ such that $J_i \subseteq J_{i'}$. An m-irreducible decomposition $J = \bigcap_{i=1}^n J_i$ is *irredundant* if if it is not redundant, that is if for all indices $i \neq i'$ one has $J_i \not\subseteq J_{i'}$.

For example, consider the monomial ideal $J = (X^3, X^2Y, Y^3)R$ in $R = A[X, Y]$. The m-irreducible decomposition of J from Example 3.3.2

$$J = (X^2, Y^3)R \bigcap (X^3, Y)R$$

is irredundant. Indeed, we have $X^2 \in (X^2, Y^3)R \smallsetminus (X^3, Y)R$ so $(X^2, Y^3)R \not\subseteq (X^3, Y)R$. Also, we have $Y \in (X^3, Y)R \smallsetminus (X^2, Y^3)R$ so $(X^3, Y)R \not\subseteq (X^2, Y^3)R$.

On the other hand, the m-irreducible decomposition

$$J = (X^2, Y^3)R \bigcap (X^3, Y)R \bigcap (X, Y)R$$

is redundant because $(X^2, Y^3)R \subseteq (X, Y)R$. This shows that m-irreducible decompositions are not unique in general. However, we show below that *irredundant* m-irreducible decompositions are unique. First, we show that every m-irreducible decomposition can be transformed into an irredundant one by removing redundancies.

ALGORITHM 3.3.5. Set $R = A[X_1, \ldots, X_d]$. Let J be a monomial ideal with m-irreducible decomposition $J = \bigcap_{i=1}^n J_i$. Note that $n \geqslant 1$.

Step 1. Check whether the intersection $J = \bigcap_{i=1}^n J_i$ is irredundant.

Step 1a. If, for all indices j and j' such that $j \neq j'$, we have $J_j \not\subseteq J_{j'}$, then the intersection is irredundant; in this case, the algorithm terminates.

Step 1b. If there exist indices j and j' such that $j \neq j'$ and $J_j \subseteq J_{j'}$, then the intersection is redundant; in this case, continue to Step 2.

Step 2. Reduce the intersection by removing the ideal that causes the redundancy in the intersection. By assumption, there exist indices j and j' such that $j \neq j'$ and $J_j \subseteq J_{j'}$. Reorder the indices to assume without loss of generality that $j' = n$. Thus, we have $j < n$ and $J_j \subseteq J_n$. It follows that $J = \bigcap_{i=1}^n J_i = \bigcap_{i=1}^{n-1} J_i$.

Step 3: Apply Step 1 to the new decomposition $J = \bigcap_{i=1}^{n-1} J_i$.

The algorithm will terminate in at most $n - 1$ steps because one can remove at most $n - 1$ monomials from the list and still form an ideal that is a non-empty intersection of parameter ideals.

COROLLARY 3.3.6. *Set $R = A[X_1, \ldots, X_d]$. Every monomial ideal $J \subsetneq R$ has an irredundant m-irreducible decomposition.*

PROOF. Theorem 3.3.3 and Algorithm 3.3.5. □

The next result explains the our use of the term "redundant" for m-irreducible decompositions.

PROPOSITION 3.3.7. *Set $R = A[X_1, \ldots, X_d]$. Let J be a monomial ideal in R with m-irreducible decomposition $J = \bigcap_{i=1}^n J_i$. Then the following conditions are equivalent:*

(i) *the decomposition $J = \bigcap_{i=1}^n J_i$ is redundant; and*
(ii) *there is an index j such that $J = \bigcap_{i \neq j} J_i$.*

PROOF. (i) $\Longrightarrow$ (ii) Assume that the decomposition $J = \bigcap_{i=1}^n J_i$ is redundant. This implies that there are indices $j \neq j'$ such that $J_j \subseteq J_{j'}$, and it follows that $J = \bigcap_{i \neq j'} J_i$.

(ii) $\Longrightarrow$ (i) Assume that there is an index j such that $J = \bigcap_{i \neq j} J_i$. (This implies that $n \geqslant 2$.) Then we have $\bigcap_{i \neq j} J_i = J = \bigcap_{i=1}^n J_i \subseteq J_j$. Lemma 3.1.4 implies that there is an index j' such that $J_{j'} \subseteq J_j$, so the intersection is redundant. $\square$

The next result shows that irredundant m-irreducible decompositions are unique up to re-ordering the terms. Given the similarities between m-irreducible decompositions of monomial ideals and prime factorizations of integers, this result compares to the uniqueness theorem for prime factorizations.

THEOREM 3.3.8. *Set $R = A[X_1, \ldots, X_d]$. Let J be a monomial ideal in R with irredundant m-irreducible decompositions $J = \bigcap_{i=1}^n J_i = \bigcap_{h=1}^m I_h$. Then $m = n$ and there is a permutation $\sigma \in S_n$ such that $J_t = I_{\sigma(t)}$ for $t = 1, \ldots, n$.*

PROOF. Claim 1: For $t = 1, \ldots, n$ there is an index u such that $I_u = J_t$. To show this, we compute:

$$\bigcap_{h=1}^m I_h = J = \bigcap_{i=1}^n J_i \subseteq J_t.$$

Lemma 3.1.4 implies that there is an index u such that $I_u \subseteq J_t$. Similarly, we have

$$\bigcap_{i=1}^n J_i = J = \bigcap_{h=1}^m I_h \subseteq I_u$$

so Lemma 3.1.4 implies that there is an index v such that $J_v \subseteq I_u \subseteq J_t$. Since the decomposition $\bigcap_{i=1}^n J_i$ is irredundant, the containment $J_v \subseteq J_t$ implies that $v = t$, so we have $J_t \subseteq I_u \subseteq J_t$, that is $I_u = J_t$.

Claim 2: For $t = 1, \ldots, n$ there is a unique index u such that $I_u = J_t$. Indeed, if $I_u = J_t = I_{u'}$, then the irredundancy of the intersection $\bigcap_{h=1}^m I_h$ implies that $u = u'$.

Define the function $\sigma\colon \{1, \ldots, n\} \to \{1, \ldots, m\}$ by letting $\sigma(t)$ be the unique index u such that $I_u = J_t$.

The same reasoning shows the following: For $u = 1, \ldots, m$ there is a unique index t such that $I_u = J_t$. Define the function $\omega\colon \{1, \ldots, m\} \to \{1, \ldots, n\}$ by letting $\omega(u)$ be the unique index t such that $I_u = J_t$. By construction, the function ω is a two-sided inverse function for σ, hence the desired conclusions. $\square$

Exercises.

M-Irreducible Decompositions in Macaulay2.

Exercises.

3.4. Irreducible Decompositions (optional)

In this section, A is a non-zero commutative ring with identity.

This section treats decompositions of non-monomial ideals of A in terms of the irreducible ideals of Section 3.2. Such decompositions are guaranteed to exist when A is noetherian; see Theorem 3.4.2. We also explore irredundancy of such decompositions, which are not in general unique. This gives yet another indication of how special monomial ideals are.

Definition 3.4.1. Let $J \subsetneq A$ be an ideal. An *irreducible decomposition* of J is an expression $J = \bigcap_{i=1}^{n} J_i$ where each J_i is irreducible.

The next decomposition result akin to Theorem 3.3.3. Its proof is due to Emmy Noether. Note that Theorem 3.2.4 shows that, over an integral domain, m-irreducible decompositions of monomial ideals are also irreducible decompositions.

Theorem 3.4.2. *If A is noetherian and $J \subsetneq A$ is an ideal, then there are irreducible ideals $J_1, \ldots, J_n$ of A such that $J = \bigcap_{i=1}^{n} J_i$.*

Proof. Suppose that there is an ideal $J \subsetneq A$ that is not an intersection of finitely many irreducible monomial ideals of A. Then the set

$$\Sigma = \{\text{ideals } J \subsetneq A \mid A \text{ is not an intersection of finitely many irreducible ideals of } A\}$$

is a non-empty set of ideals of A. Since A is noetherian, the set Σ has a maximal element J. In particular J is not irreducible, so there exist ideals $I, K \subseteq A$ such that $J = I \bigcap K$ and $J \subsetneq I, K$. In particular, we have $I \neq A$ and $K \neq A$. Since J is maximal in Σ, we have $I, K \notin \Sigma$. Hence, there are irreducible ideals $I_1, \ldots, I_m, K_1, \ldots, K_n$ such that $I = \bigcap_{j=1}^{m} I_j$ and $K = \bigcap_{i=1}^{n} K_i$. It follows that

$$J = I \bigcap K = \left(\bigcap_{j=1}^{m} I_j\right) \bigcap \left(\bigcap_{i=1}^{n} K_i\right)$$

so J is a finite intersection of irreducible ideals, a contradiction. $\square$

For instance, let n be an integer such that $n \geqslant 2$. The Fundamental Theorem of Arithmetic says that n has a factorization $n = p_1^{e_1} \cdots p_m^{e_m}$ where the p_i are distinct prime numbers and each e_i is a positive integer. It follows that $n\mathbb{Z} = p_1^{e_1}\mathbb{Z} \bigcap \cdots \bigcap p_m^{e_m}\mathbb{Z}$ is an irredundant irreducible decomposition.

Next, let R be the polynomial ring $R = \mathbb{C}[X]$ in one variable, and let f be a non-constant polynomial in R. The Fundamental Theorem of Algebra says that f has a factorization $f = c(X - a_1)^{e_1} \cdots (X - a_m)^{e_m}$ where the a_i are distinct complex numbers, each e_i is a positive integer, and c is the leading coefficient of f. It follows that $fR = (X - a_1)^{e_1} R \bigcap \cdots \bigcap (X - a_m)^{e_m} R$ is an irredundant irreducible decomposition.

In the ring $\mathrm{C}(\mathbb{R})$ of continuous functions, the ideal

$$I = \{f \in \mathrm{C}(\mathbb{R}) \mid f(n) = 0 \text{ for all } n \in \mathbb{N}\}$$

does not have an irreducible decomposition. For an indication of why this is true, note that $I = \bigcap_{n \in \mathbb{Z}} I_n$ where

$$I_n = \{f \in \mathrm{C}(\mathbb{R}) \mid f(n) = 0\}.$$

Each ideal is irreducible since it is prime (see Exercise 3.2.12) but there is no finite sequence $n_1, \ldots, n_t$ such that $I = I_{n_1} \bigcap \cdots \bigcap I_{n_t}$.

Example 3.4.3. Let k be an integral domain, and set $A = k[X, Y]$. An irreducible decomposition of the ideal $J = (X^3, X^2Y, Y^3)A$ is

$$J = (X^2, Y^3)A \bigcap (X^3, Y)A.$$

See Example 3.1.2 and Theorem 3.2.4.

We next explore the notion of irredundancy for irreducible decompositions.

DEFINITION 3.4.4. Let $J \subsetneq A$ be an ideal. An irreducible decomposition $J = \bigcap_{i=1}^{n} J_i$ is *redundant* if if there exists an index i' such that $J = \bigcap_{i \neq i'} J_i$. An irreducible decomposition $J = \bigcap_{i=1}^{n} J_i$ is *irredundant* if if it is not redundant, that is if for all indices i' one has $J \neq \bigcap_{i \neq i'} J_i$.

For example, let k be an integral domain, and let A be the polynomial ring $A = k[X, Y]$ in 2 variables. Set $J = (X^3, X^2Y, Y^3)A$. The irreducible decomposition of J from Example 3.4.3

$$J = (X^2, Y^3)A \bigcap (X^3, Y)A$$

is irredundant. Indeed, we have $X^2 \in (X^2, Y^3)A \smallsetminus J$ so $J \neq (X^3, Y)A$. Also, we have $Y \in (X^3, Y)A \smallsetminus J$ so $J \neq (X^2, Y^3)A$. On the other hand, the irreducible decomposition

$$J = (X^2, Y^3)A \bigcap (X^3, Y)A \bigcap (X, Y)A$$

is redundant because $J = (X^2, Y^3)A \bigcap (X^3, Y)A$.

This example shows that irreducible decompositions are not unique in general. The situation is even worse, however, as the next example shows that even irredundant irreducible decompositions are not unique in general. Contrast this with the situation of m-irreducible decompositions. See Exercise 3.4.11 for a weak uniqueness statement.

EXAMPLE 3.4.5. Let k be an integral domain, and set $A = k[X, Y]$. The following ideals are irreducible and pair-wise distinct:

$$(X, Y^2)A \qquad (X^2, Y)A \qquad (X^2, X+Y)A \qquad (X, (X+Y)^2)A.$$

Furthermore, one has

$$(X, Y^2)A \bigcap (X^2, Y)A = (X^2, XY, Y^2)A = (X^2, X+Y)A \bigcap (X, (X+Y)^2)A.$$

The following procedure shows how to pare down an arbitrary irreducible decomposition to an irredundant one. It compares to Algorithm 3.3.5.

ALGORITHM 3.4.6. Let J be an ideal of A with irreducible decomposition $J = \bigcap_{i=1}^{n} J_i$. Note that $n \geqslant 1$.

Step 1. Check whether the intersection $J = \bigcap_{i=1}^{n} J_i$ is irredundant.

Step 1a. If, for all indices j and j' such that $j \neq j'$, we have $J_j \not\subseteq J_{j'}$, then the intersection is irredundant; in this case, the algorithm terminates.

Step 1b. If there exist indices j and j' such that $j \neq j'$ and $J_j \subseteq J_{j'}$, then the intersection is redundant; in this case, continue to Step 2.

Step 2. Reduce the intersection by removing the ideal that causes the redundancy in the intersection. By assumption, there exist indices j and j' such that $j \neq j'$ and $J_j \subseteq J_{j'}$. Reorder the indices to assume without loss of generality that $j' = n$. Thus, we have $j < n$ and $J_j \subseteq J_n$. It follows that $J = \bigcap_{i=1}^{n} J_i = \bigcap_{i=1}^{n-1} J_i$.

Step 3: Apply Step 1 to the new decomposition $J = \bigcap_{i=1}^{n-1} J_i$.

The algorithm will terminate in at most $n - 1$ steps because one can remove at most $n - 1$ monomials from the list and still form an ideal that is a non-empty intersection of parameter ideals.

COROLLARY 3.4.7. *If A is noetherian, then every ideal in A has an irredundant irreducible decomposition.*

PROOF. Theorem 3.4.2 and Algorithm 3.4.6. □

The next result give a criterion for detecting whether a given irreducible decomposition is redundant. It corresponds to one implication of Theorem 3.3.8.

PROPOSITION 3.4.8. *Let J be an ideal in A with irreducible decomposition $J = \bigcap_{i=1}^n J_i$. If there are indices $j \neq j'$ such that $J_j \subseteq J_{j'}$, then the decomposition $J = \bigcap_{i=1}^n J_i$ is redundant.*

PROOF. If there are indices $j \neq j'$ such that $J_j \subseteq J_{j'}$, then $J = \bigcap_{i \neq j'} J_i$. □

It is worth noting that the converse of the previous result fails in general. (Contrast this with the situation for monomial ideals from Theorem 3.3.8.) For instance, let k be an integral domain, and set $A = k[X, Y]$. We consider the irreducible decompositions

$$(X, Y^2)A \bigcap (X^2, Y)A = (X^2, XY, Y^2)A = (X^2, X + Y)A \bigcap (X, (X + Y)^2)A$$

from Example 3.4.5. It follows that the decomposition

$$(X^2, XY, Y^2)A = (X, Y^2)A \bigcap (X^2, Y)A \bigcap (X^2, X + Y)A$$

is redundant; however, there are no containment relations between the three ideals in this decomposition. Thus, the converse of Proposition 3.4.8 fails in general.

Also, we have

$$(X, Y^2)A \bigcap (X^2, Y)A = (X^2, XY, Y^2)A \subseteq (X^2, X + Y)A$$

even though $(X, Y^2)A \not\subseteq (X^2, X+Y)A$ and $(X^2, Y)A \not\subseteq (X^2, X+Y)A$. This shows that the version of Lemma 3.1.4 fails in this setting.

We end this section by formally addressing the existence of irreducible decompositions of monomial ideals. Note that this results does not assume that A is noetherian, so it does not follow from Corollary 3.4.7.

COROLLARY 3.4.9. *Let A be an integral domain, and set $R = A[X_1, \ldots, X_d]$. Every non-zero monomial ideal in R has an irredundant irreducible decomposition.*

PROOF. Apply Corollary 3.3.6 and Theorem 3.2.4. □

Exercises.

EXERCISE 3.4.10. Let J be an ideal in A with irredundant irreducible decomposition $J = \bigcap_{i=1}^n J_i$.

(a) Assume that for $i = 1, \ldots, n$ one has $\operatorname{rad}(J_i) = J_i$. Prove that $J = \operatorname{rad}(J)$.
(b) Prove or disprove the following: If $J = \operatorname{rad}(J)$, then $\operatorname{rad}(J_i) = J_i$ for $i = 1, \ldots, n$.

EXERCISE 3.4.11. Let J be an ideal in A with irredundant irreducible decompositions $J = \bigcap_{i=1}^n J_i = \bigcap_{h=1}^m I_h$. Then $m = n$ and there is a permutation $\sigma \in S_n$ such that $\operatorname{rad}(J_t) = \operatorname{rad}\left(I_{\sigma(t)}\right)$ for $t = 1, \ldots, n$. (Hint: Show that for $i = 1, \ldots, m$ there is an index j such that $J = J_1 \bigcap \cdots \bigcap J_{i-1} \bigcap I_j \bigcap J_{i+1} \bigcap \cdots \bigcap J_n$.)

Irreducible Decompositions in Macaulay2.

Exercises.

3.5. Exploration: Decompositions in Two Variables, I

In this section, A is a non-zero commutative ring with identity and $R = A[X,Y]$.

Exercise 3.1.7 shows how to compute m-irreducible decompositions in $A[X]$. Here we focus on the case of two variables, building from Example 3.3.2. The idea is to factor the generators of the form X^mY^n, one at a time.

Exercise 3.5.1. Set $I = (X^a, X^bY^c, Y^d)R$ where $a > b \geqslant 1$ and $d > c \geqslant 1$.

(a) Prove that X^a, X^bY^c, Y^d is an irredundant monomial generating sequence for I.
(b) Prove that $I = (X^b, Y^d)R \bigcap (X^a, Y^c)R$ is an irredundant m-irreducible decomposition.

Exercise 3.5.2. Set $J = (X^a, X^bY^c, X^dY^e, Y^f)R$ where $a > b > d \geqslant 1$ and $f > e > c \geqslant 1$.

(a) Prove that X^a, X^bY^c, X^dY^e, Y^f is an irredundant monomial generating sequence for J.
(b) Prove that $J = (X^b, X^dY^e, Y^f)R \bigcap (X^a, Y^c)R$.
(c) Prove that the expression $J = (X^d, Y^f)R \bigcap (X^b, Y^e)R \bigcap (X^a, Y^c)R$ is an irredundant m-irreducible decomposition.

Exercise 3.5.3. Repeat Exercise 3.5.2 for the ideal

$$K = (X^{a_1}, X^{a_2}Y^{b_2}, X^{a_3}Y^{b_3}, X^{a_4}Y^{b_4}, Y^{b_5})R$$

where $a_1 > a_2 > a_3 > a_4 \geqslant 1$ and $b_5 > b_4 > b_3 > b_2 \geqslant 1$.

Exercise 3.5.4. Use induction to repeat Exercise 3.5.3 for the ideal

$$L = (X^{a_1}, X^{a_2}Y^{b_2}, X^{a_3}Y^{b_3}, \ldots, X^{a_{m-1}}Y^{b_{m-1}}, Y^{b_m})R$$

where $a_1 > a_2 > a_3 > \cdots > a_{m-1} \geqslant 1$ and $b_m > b_{m-1} > \cdots > b_3 > b_2 \geqslant 1$.

Decompositions in Two Variables in Macaulay 2.

Exercises.

Conclusion

Include some history here. Talk about some of the literature from this area.

Part 2

Monomial Ideals and Other Areas

CHAPTER 4

Connections with Combinatorics

This chapter investigates three special cases of monomial ideals that are important for graph theory and combinatorics: the edge ideal of a simple graph, and the face and facet ideals of a simplicial complex. Each of these cases is a monomial ideal that is "square free." These ideals are treated in general in Section 4.1. Graphs and their edge ideals (as devised by Villarreal [**41**]) are introduced in Section 4.2, and the decompositions of edge ideals are described in Section 4.3. This includes, as a consequence, a method for finding decompositions of quadratic square-free monomial ideals. Simplicial complexes and their face ideals (as introduced by Hochster [**21**] and Reisner [**36**]) are presented in Section 4.4, and the decompositions of face ideals are described in Section 4.5. This includes, as a consequence, a method for finding decompositions of arbitrary square-free monomial ideals. Section 4.6 treats the facet ideals of Faridi [**9**] associated to a simplicial complexes, and their m-irreducible decompositions. The chapter ends in Section 4.7 with an exploration of Alexander duality, a process that transforms monomial generating sequences to m-irreducible decompositions, and vice versa. In our context, the notion of Alexander duality goes back at least to Hochster [**21**].

4.1. Square-Free Monomial Ideals

In this section, A is a non-zero commutative ring with identity.

The following notion of "square-free" monomials compares directly to the same notion for integers. The main point of this section is to characterize the square-free monomial ideals in terms of their monomial radicals.

Definition 4.1.1. Set $R = A[X_1, \ldots, X_d]$. A monomial $\underline{X}^{\underline{n}} \in [\![R]\!]$ is *square-free* if, for $i = 1, \ldots, d$ one has $n_i \in \{0, 1\}$. A monomial ideal $J \subseteq R$ is *square-free* if it is generated by square-free monomials.

For instance, the square-free monomials in $R = A[X, Y, Z]$ are

$$1, X, Y, Z, XY, XZ, YZ, XYZ.$$

The ideal $(XY, YZ)R$ is square-free. The ideal $(X^2Y, YZ^2)R$ is not square-free.

More generally, a monomial $f \in [\![R]\!] = A[X_1, \ldots, X_d]$ is square-free if and only if it has no factor of the form X_i^2, i.e., if and only if $f = \mathrm{red}(f)$. (In particular, the monomial $\mathrm{red}(f)$ is square-free.) Thus, the term "square-free" refers to the fact that it is free of square factors.

Proposition 4.1.2. *Set $R = A[X_1, \ldots, X_d]$. A monomial ideal $J \subseteq R$ is square-free if and only if* $\text{m-rad}(J) = J$. *In particular, the ideal* $\text{m-rad}(J)$ *is square-free.*

PROOF. Let $f_1, \ldots, f_n \in [\![J]\!]$ be an irredundant monomial generating sequence for J.

Assume first that J is square-free; we show that $\text{m-rad}\,(J) = J$. The ideal J has a square-free monomial generating sequence, and Theorem 1.3.6 shows that this sequence contains the f_i's. Thus, each monomial f_i is square-free, so $f_i = \text{red}(f_i)$ for $i = 1, \ldots, n$. Thus, Theorem 2.3.7 implies that

$$\text{m-rad}\,(J) = (\text{red}(f_1), \ldots, \text{red}(f_n))R = (f_1, \ldots, f_n)R = J$$

as desired.

Assume next that $\text{m-rad}\,(J) = J$. To show that J is square-free, we need to show that each f_i is square-free, that is, that $f_i = \text{red}(f_i)$ for $i = 1, \ldots, n$. Theorem 2.3.7 implies that

$$J = \text{m-rad}\,(J) = (\text{red}(f_1), \ldots, \text{red}(f_n))R$$

so an irredundant monomial generating sequence for J is a sequence of the form $\text{red}(f_{i_1}), \ldots, \text{red}(f_{i_k})$. The uniqueness of irredundant monomial generating sequences implies that $k = n$, so an irredundant monomial generating sequence for J is $\text{red}(f_1), \ldots, \text{red}(f_n)$, and further that $\{f_1, \ldots, f_n\} = \{\text{red}(f_1), \ldots, \text{red}(f_n)\}$. Thus, for $i = 1, \ldots, n$ there is an index j_i such that $f_i = \text{red}(f_{j_i})$. It follows that $\text{red}(f_{j_i}) \big| f_{j_i}$, so we have $f_i \big| f_{j_i}$. The irredundancy of the sequence $f_1, \ldots, f_n$ implies that $j_i = i$, so $f_i = \text{red}(f_i)$.

Finally, if J is an arbitrary monomial ideal, then we have $\text{m-rad}\,(\text{m-rad}\,(J)) = \text{m-rad}\,(J)$ by Proposition 2.3.3(d), so the previous paragraph shows that $\text{m-rad}\,(J)$ is square-free. $\square$

We end this section with the following useful characterization of square-free m-irreducible monomial ideals.

PROPOSITION 4.1.3. *Set $R = A[X_1, \ldots, X_d]$. A monomial ideal $J \subseteq R$ is square-free and m-irreducible if and only if there exist positive integers $k, t_1, \ldots, t_k$ such that $1 \leqslant t_1 < \cdots < t_k \leqslant d$ and $J = (X_{t_1}, \ldots, X_{t_k})R$.*

PROOF. For the forward implication, assume that J is square-free and m-irreducible. Let $f_1, \ldots, f_n$ be a square-free monomial generating sequence for J. Theorem 3.1.3 implies that there are positive integers $k, t_1, \ldots, t_k, e_1, \ldots, e_k$ such that $1 \leqslant t_1 < \cdots < t_k \leqslant d$ and $J = (X_{t_1}^{e_1}, \ldots, X_{t_k}^{e_k})R$. The generating sequence $X_{t_1}^{e_1}, \ldots, X_{t_k}^{e_k}$ is irredundant, so Theorem 1.3.6 shows that the sequence of f_i's contains the sequence of $X_{t_j}^{e_j}$'s. Thus, each monomial $X_{t_j}^{e_j}$ is square-free, that is, we have $e_j = 1$ for $j = 1, \ldots, k$. The desired conclusion $J = (X_{t_1}, \ldots, X_{t_k})R$ follows directly.

Conversely, if we have $J = (X_{t_1}, \ldots, X_{t_k})R$, then J is m-irreducible by Theorem 3.1.3, and it is square-free by definition. $\square$

Exercises.

*EXERCISE 4.1.4. Set $R = A[X_1, \ldots, X_d]$. Let J be a monomial ideal in R with m-irreducible decomposition $J = \bigcap_{i=1}^n J_i$.

(a) Assume that for $i = 1, \ldots, n$ the ideal J_i is square-free. Prove that J is square-free.

(b) Prove that if J is square-free and the decomposition $J = \bigcap_{i=1}^n J_i$ is irredundant, then each ideal J_i is square-free.

(This exercise is used in the proof of Proposition 4.3.3.)

EXERCISE 4.1.5. Set $R = A[X_1, \ldots, X_d]$. We say that a monomial ideal J in R is *m-prime* if it satisfies the following condition: for all monomials $f, g \in [\![R]\!]$ if $fg \in J$, then either $f \in J$ or $g \in J$.

(a) Prove that 0 is m-prime.
(b) Prove that the following conditions are equivalent when $J \neq 0$:
   (i) J is m-prime;
   (ii) for all non-zero monomial ideals I and K, if $IK \subseteq J$, then either $I \subseteq J$ or $K \subseteq J$;
   (iii) J is m-irreducible and square-free; and
   (iv) there are positive integers $k, t_1, \ldots, t_k$ such that $J = (X_{t_1}, \ldots, X_{t_k})R$.

EXERCISE 4.1.6. Set $R = A[X_1, \ldots, X_d]$; let I and J be monomial ideals of R.

(a) Prove or disprove: If I is square-free then so is $(I :_R J)$.
(b) Prove or disprove: If J is square-free then so is $(I :_R J)$.
(c) Prove or disprove: If $(I :_R J)$ is square-free then so is I.
(d) Prove or disprove: If $(I :_R J)$ is square-free then so is J.

Square-Free Monomial Ideals in Macaulay2.

Here we use the Macaulay2 command `isSquareFree` to determine whether a monomial ideal is square-free. This command only works for monomial ideals, so we also introduce the command `monomialIdeal`, which can be used in place of `ideal` when defining a monomial ideal.

```
i1 : R = ZZ/101[x, y, z]

o1 = R

o1 : PolynomialRing

i2 : I = monomialIdeal(x^2, x*y, y*z)

                         2
o2 = monomialIdeal (x , x*y, y*z)

o2 : MonomialIdeal of R

i3 : isSquareFree I

o3 = false

i4 : J = monomialIdeal(x*y, y*z)

o4 = monomialIdeal (x*y, y*z)

o4 : MonomialIdeal of R

i5 : isSquareFree J

o5 = true
```

Exercises.

EXERCISE 4.1.7. Use Macaulay2 to test any counterexamples you gave in Exercise 4.1.6.

4.2. Graphs and Edge Ideals

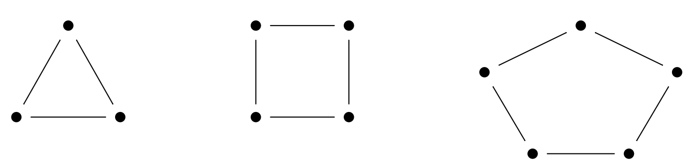
In this section, A is a non-zero commutative ring with identity.

Geometrically, a graph consists of a set of points (called "vertices") and a set of lines or arcs (called "edges") connecting pairs of vertices. (For us, the term "graph" is short for "finite simple graph".) We will take the more combinatorial approach (as opposed to the geometric approach) to the study of graphs. Our treatment of graph theory is brief, but self-contained. However, the interested reader may wish to consult the text of Diestel [**7**] as a reference.

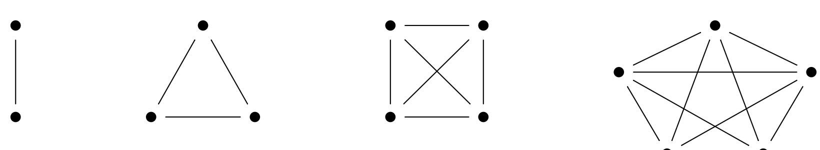
DEFINITION 4.2.1. Let $V = \{v_1, \ldots, v_d\}$ be a finite set. A *graph* with *vertex set* V is an ordered pair $G = (V, E)$ where E is a set of un-ordered pairs v_iv_j with $v_i \neq v_j$. (Since the pairs are un-ordered, we have $v_iv_j = v_jv_i$.) An element $v_i \in V$ is a *vertex* of G. (The plural of vertex is "vertices".) The set E is the *edge set* of G. Given an edge $e = v_iv_j$, the *endpoints* of e are the vertices v_i and v_j. Two vertices $v_i, v_j \in V$ are *adjacent* if there is an edge $e \in E$ with endpoints v_i and v_j, that is, if $v_iv_j \in E$.

Our definition implies that our graphs are finite (i.e., have finite vertex sets) and are simple (i.e., have no loops and no multiple edges). Some standard examples of graphs are as follows.

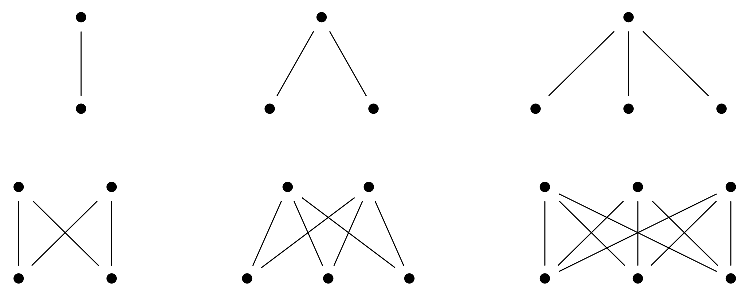
For each $d \geqslant 3$, the *d-cycle* is the graph C_d with vertex set $\{v_1, v_2, \ldots, v_d\}$ and edge set $\{v_1v_2, v_2v_3, \ldots, v_{d-1}v_d, v_dv_1\}$. Geometric versions of C_3, C_4, and C_5 are as follows:



For each $d \geqslant 2$, the *complete graph on d vertices* is the graph K_d with vertex set $\{v_1, \ldots, v_d\}$ and edge set $\{v_iv_j \mid 1 \leqslant i < j \leqslant d\}$. Geometric versions of K_2, K_3, K_4, and K_5 are as follows:



Given $m, n > 1$, the *complete bipartite graph* $B_{m,n}$ is the graph with vertex set $\{u_1, \ldots, u_m, v_1, \ldots, v_n\}$ and edge set $\{u_iv_j \mid 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n\}$. Geometric versions of $B_{1,1}$, $B_{1,2}$, $B_{1,3}$, $B_{2,2}$, $B_{2,3}$, and $B_{3,3}$ are as follows:



The next definition shows how to use a graph to construct a monomial ideal.

Definition 4.2.2. Let G be a graph with vertex set $V = \{v_1, \ldots, v_d\}$. The *edge ideal* associated to G is the ideal $I_G \subseteq R = A[X_1, \ldots, X_d]$ that is "generated by the edges of G":

$$I_G = (\{X_i X_j \mid v_i v_j \text{ is an edge in } G\})R.$$

By definition, the edge ideal I_G is square-free.

For example, the edge ideals associated to C_3, C_4, and C_5 are

$$\begin{aligned} I_{C_3} &= (X_1X_2, X_2X_3, X_1X_3) \subseteq A[X_1, X_2, X_3] \\ I_{C_4} &= (X_1X_2, X_2X_3, X_3X_4, X_1X_4) \subseteq A[X_1, X_2, X_3, X_4] \\ I_{C_5} &= (X_1X_2, X_2X_3, X_3X_4, X_4X_5, X_1X_5) \subseteq A[X_1, X_2, X_3, X_4, X_5]. \end{aligned}$$

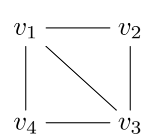
The edge ideals associated to K_2, K_3, and K_4 are

$$\begin{aligned} I_{K_2} &= (X_1X_2) \subseteq A[X_1, X_2] \\ I_{K_3} &= (X_1X_2, X_1X_3, X_2X_3) \subseteq A[X_1, X_2, X_3] \\ I_{K_4} &= (X_1X_2, X_1X_3, X_1X_4, X_2X_3, X_2X_4, X_3X_4) \subseteq A[X_1, X_2, X_3, X_4]. \end{aligned}$$

The edge ideals associated to some bipartite graphs are

$$\begin{aligned} I_{B_{1,1}} &= (X_1Y_1) \subseteq A[X_1, Y_1] \\ I_{B_{1,2}} &= (X_1Y_1, X_1Y_2) \subseteq A[X_1, Y_1, Y_2] \\ I_{B_{1,3}} &= (X_1Y_1, X_1Y_2, X_1Y_3) \subseteq A[X_1, Y_1, Y_2, Y_3] \\ I_{B_{2,2}} &= (X_1Y_1, X_1Y_2, X_2Y_1, X_2Y_2) \subseteq A[X_1, X_2, Y_1, Y_2] \\ I_{B_{2,3}} &= (X_1Y_1, X_1Y_2, X_1Y_3, X_2Y_1, X_2Y_2, X_2Y_3) \subseteq A[X_1, X_2, Y_1, Y_2, Y_3]. \end{aligned}$$

The edge ideal of the graph



is $(X_1X_2, X_1X_3, X_1X_4, X_2X_3, X_3X_4) \subseteq A[X_1, X_2, X_3, X_4]$.

Exercises.

EXERCISE 4.2.3. Let G be a graph with vertex set $\{v_1, \ldots, v_d\}$. Prove that the set $\{X_iX_j \mid v_iv_j \text{ is an edge in } G\}$ is an irredundant generating sequence for I_G.

EXERCISE 4.2.4. Let G and G' be graphs with vertex sets $\{v_1, \ldots, v_d\}$.

(a) Prove that $G \subseteq G'$ if and only if $I_G \subseteq I_{G'}$.
(b) Prove that $I_G \subseteq I_{K_d}$.

Graphs and Edge Ideals in Macaulay2.

Exercises.

4.3. Decompositions of Edge Ideals

In this section, A is a non-zero commutative ring with identity.

Our goal for this section is to characterize the m-irreducible decompositions of edge ideals. These are given in terms of the graph's vertex covers. One consequence is a method for finding m-irreducible decompositions of quadratic square-free monomial ideals. We begin with some notation for the relevant m-irreducible monomial ideals.

DEFINITION 4.3.1. Let $V = \{v_1, \ldots, v_d\}$, and set $R = A[X_1, \ldots, X_d]$. For each subset $V' \subseteq V$, let $P_{V'} \subseteq R$ be the ideal "generated by the elements of V'":

$$P_{V'} = (\{X_i \mid v_i \in V'\})R.$$

For instance, with $V = \{v_1, \ldots, v_d\}$ and $R = A[X_1, \ldots, X_d]$, we have

$$P_\emptyset = 0 \qquad P_{\{v_1,v_3\}} = (X_1, X_3)R \qquad P_V = (X_1, \ldots, X_d)R$$

and so on.

FACT 4.3.2. Let $V = \{v_1, \ldots, v_d\}$ be a finite set, and set $R = A[X_1, \ldots, X_d]$.

(a) Given subsets $V', V'' \subseteq V$, one has $P_{V'} \subseteq P_{V''}$ if and only if $V' \subseteq V''$.
(b) A monomial ideal $J \subseteq R$ is square-free and m-irreducible if and only if there exists a subset $V' \subseteq V$ such that $J = P_{V'}$; see Proposition 4.1.3.

The next result gives a first indication about how we will find m-irreducible decompositions for square-free monomial ideals, in particular, for edge ideals.

PROPOSITION 4.3.3. *Let $V = \{v_1, \ldots, v_d\}$, and set $R = A[X_1, \ldots, X_d]$. A monomial ideal $J \subsetneq R$ is square-free if and only if there are subsets $V_1, \ldots, V_n \subseteq V$ such that $J = \bigcap_{i=1}^n P_{V_i}$.*

PROOF. First, assume that J is square-free. Theorem 3.3.3 implies that J has an irredundant m-irreducible decomposition $J = \bigcap_{i=1}^n J_i$, and Exercise 4.1.4(b) implies that each J_i is square-free. We conclude from Fact 4.3.2(b) that there exist subsets $V_1, \ldots, V_n \subseteq V$ such that for $i = 1, \ldots, n$ we have $J_i = P_{V_i}$, so $J = \bigcap_{i=1}^n P_{V_i}$.

Conversely, if $J = \bigcap_{i=1}^n P_{V_i}$ for some subsets $V_1, \ldots, V_n \subseteq V$. Fact 4.3.2(b) implies that each P_{V_i} is square-free, so J is square-free by Exercise 4.1.4(a). $\square$

The following notions are used to identify which ideals $P_{V'}$ occur in an (irredundant) m-irreducible decomposition of an edge ideal.

Definition 4.3.4. Let G be a graph with vertex set $V = \{v_1, \ldots, v_d\}$. A *vertex cover* of G is a subset $V' \subseteq V$ such that for each edge v_iv_j in G either $v_i \in V'$ or $v_j \in V'$. A vertex cover V' is *minimal* if it does not properly contain another vertex cover of G.

For instance, the vertex set V is a vertex cover of G. In particular, G has a vertex cover. The next fact states that the set of vertex covers of G is closed under supersets, and that every graph has a minimal vertex cover.

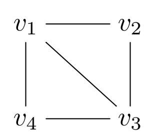
Fact 4.3.5. Let G be a graph with vertex set V.

(a) If $V' \subseteq V$ is a vertex cover of G and $V' \subseteq V'' \subseteq V$, then V'' is a vertex cover of G.

(b) Since V is finite, every vertex cover of G contains a minimal vertex cover of G.

The next example shows that a given graph can have several distinct vertex covers. Moreover, it has have vertex covers of differing sizes.

Example 4.3.6. We compute the vertex covers of the following graph G:



In light of Fact 4.3.5, parts (a) and (b), we really only need to find the *minimal* vertex covers of G.

First, we find the minimal vertex covers containing v_1. If $v_1 \in V'$, then the edges v_1v_2, v_1v_3, and v_1v_4 are "covered". This leaves only the edges v_2v_3, and v_3v_4 "uncovered". These edges can be covered either by adding v_3 or by adding v_2, v_4. Thus, the minimal vertex covers containing v_1 are $\{v_1, v_3\}$ and $\{v_1, v_2, v_4\}$.

Next, we find the minimal vertex covers that do not contain v_1. If $v_1 \notin V'$, we must have $v_2, v_3, v_4 \in V'$ in order to cover the edges v_1v_2, v_1v_3, and v_1v_4. It is straightforward to show that the set $\{v_2, v_3, v_4\}$ is a minimal vertex cover of G.

The connection between vertex covers and m-irreducible decompositions begins with the next result.

Lemma 4.3.7. *Let G be a graph with vertex set $V = \{v_1, \ldots, v_d\}$, and let $V' \subseteq V$. Set $R = A[X_1, \ldots, X_d]$. Then $I_G \subseteq P_{V'}$ if and only if V' is a vertex cover of G.*

Proof. Write $V' = \{v_{i_1}, \ldots, v_{i_n}\}$, so that $P_{V'} = (X_{i_1}, \ldots, X_{i_n})R$.

For the forward implication, assume that $I_G \subseteq P_{V'}$. We show that V' is a vertex cover of G. Let v_jv_k be an edge in G. Then we have $X_jX_k \in I_G \subseteq P_{V'} = (X_{i_1}, \ldots, X_{i_n})R$. It follows that $X_jX_k \in (X_{i_m})R$ for some index m. A comparison of exponent vectors shows that either $j = i_m$ or $k = i_m$, that is, either $v_j = v_{i_m} \in V'$ or $v_k = v_{i_m} \in V'$. Thus V' is a vertex cover of G.

For the reverse implication, assume that V' is a vertex cover of G. To show that $I_G \subseteq P_{V'}$, we need to show that each generator of I_G is in $P_{V'}$. To this end, fix a generator $X_iX_j \in I_G$, corresponding to an edge v_iv_j in G. Since V' is a vertex cover of G, either $v_i \in V'$ or $v_j \in V'$. It follows that either $X_i \in P_{V'}$ or $X_j \in P_{V'}$, so $X_iX_j \in P_{V'}$. $\square$

Without further ado, here is the decomposition theorem for edge ideals. It shows explicitly how the combinatorial properties of a graph inform some algebraic properties of its edge ideal. The subsequent discussion explains the reciprocal relation of how the algebraic properties of the edge ideal inform some combinatorial properties of the graph.

THEOREM 4.3.8. *Let G be a graph with vertex set $V = \{v_1, \ldots, v_d\}$, and set $R = A[X_1, \ldots, X_d]$. Then the edge ideal $I_G \subseteq R$ has the following m-irreducible decompositions*

$$I_G = \bigcap_{V'} P_{V'} = \bigcap_{V' \ \mathit{min.}} P_{V'}$$

where the first intersection is taken over all vertex covers of G, and the second intersection is taken over all minimal vertex covers of G. The second intersection is irredundant.

PROOF. Fact 4.3.2(a) shows that the second intersection is irredundant. The containment $\bigcap_{V'} P_{V'} \subseteq \bigcap_{V' \text{ min.}} P_{V'}$ is straightforward. The reverse containment $\bigcap_{V'} P_{V'} \supseteq \bigcap_{V' \text{ min.}} P_{V'}$ follows from the fact that every vertex cover V' contains a minimal vertex cover V''; see Facts 4.3.2(a) and 4.3.5(b). The containment $I_G \subseteq \bigcap_{V'} P_{V'}$ is from Lemma 4.3.7.

For the final containment $I_G \supseteq \bigcap_{V'} P_{V'}$ recall that I_G is square-free. Hence, Proposition 4.3.3 provides subsets $V_1, \ldots, V_n$ such that $I_G = \bigcap_{j=1}^{n} P_{V_j}$. For each index j, we then have $I_G \subseteq P_{V_j}$, so Lemma 4.3.7 implies that V_j is a vertex cover of G. It follows that $I_G = \bigcap_{j=1}^{n} P_{V_j} \supseteq \bigcap_{V'} P_{V'}$, as desired. $\square$

EXAMPLE 4.3.9. We compute an irredundant m-irreducible decomposition of the ideal I_G where G is the graph from Example 4.3.6. Using Theorem 4.3.8, this can be read from the list of minimal vertex covers that we computed:

$$I_G = (X_1, X_3)R \bigcap (X_1, X_2, X_4)R \bigcap (X_2, X_3, X_4)R.$$

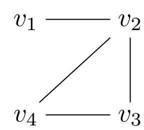
In general, given an irredundant m-irreducible decomposition $I_G = \bigcap_{i=1}^{n} P_{V_i}$ as in Proposition 4.3.3, one concludes the minimal vertex covers of G are precisely $V_1, \ldots, V_n$. Indeed, Theorem 4.3.8 gives an irredundant m-irreducible decomposition $I_G = \bigcap_{V' \text{ min.}} P_{V'}$, so the uniqueness of such decompositions from Theorem 3.3.8 provides the desired conclusion.

It is straightforward to identify the monomial ideals $J \subseteq R = A[X_1, \ldots, X_d]$ that are of the form I_G for some graph G with vertex set $V = \{v_1, \ldots, v_d\}$: they are precisely the ideals whose irredundant monomial generating sequences contain only elements of the form X_iX_j with $i \neq j$. (In other words, they are precisely the square-free "quadratic" monomial ideals of R.) Thus, we can use the techniques of this section to find m-irreducible decompositions of such ideals, as in the following example.

EXAMPLE 4.3.10. Set $R = A[X_1, X_2, X_3, X_4]$. We compute an irredundant m-irreducible decomposition of the ideal

$$J = (X_1X_2, X_2X_3, X_2X_4, X_3X_4)R.$$

First, we find a graph G with vertex set $V = \{v_1, v_2, v_3, v_4\}$ such that $J = I_G$ by adding an edge for each generator:



Next, we find the minimal vertex covers for G:

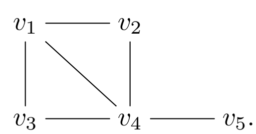
$$\{v_1, v_3, v_4\} \qquad \{v_2, v_3\} \qquad \{v_2, v_4\}.$$

Finally, we read off the decomposition using Theorem 4.3.8:

$$J = I_G = (X_1, X_3, X_4)R \bigcap (X_2, X_3)R \bigcap (X_2, X_4)R.$$

Exercises.

EXERCISE 4.3.11. Set $R = A[X_1, \ldots, X_5]$, and let G be the graph represented by the following sketch:



(a) Find an irredundant monomial generating sequence for I_G.
(b) Find all minimal vertex covers of G.
(c) Use Theorem 4.3.8 to find an irredundant m-irreducible decomposition of I_G.
(d) Verify the decomposition $I_G = \bigcap_{V'} P_{V'}$ from part (c) by computing the generators for $\bigcap_{V'} P_{V'}$ using least common multiples and comparing to the list of generators found in part (a).

Justify your answers.

EXERCISE 4.3.12. Verify the decomposition

$$I_G = (X_1, X_3)R \bigcap (X_1, X_2, X_4)R \bigcap (X_2, X_3, X_4)R$$

from Example 4.3.9 as in Exercise 4.3.11(d).

EXERCISE 4.3.13. Verify the decomposition

$$I_G = (X_1, X_3, X_4)R \bigcap (X_2, X_3)R \bigcap (X_2, X_4)R$$

from Example 4.3.10 as in Exercise 4.3.11(d).

EXERCISE 4.3.14. Set $R = A[X_1, \ldots, X_5]$ and compute an irredundant m-irreducible decomposition of $J = (X_1X_2, X_1X_4, X_1X_5, X_2X_3, X_2X_5, X_3X_4, X_4X_5)R$ as in Example 4.3.10. Check your decomposition as in Exercise 4.3.11(d). Justify your answers.

EXERCISE 4.3.15. Let G be a graph with vertex set $\{v_1, \ldots, v_d\}$, and set $R = A[X_1, \ldots, X_d]$ and $\mathfrak{X} = (X_1, \ldots, X_d)R$.

(a) Prove that for $i = 1, \ldots, d$ the set $V \smallsetminus \{v_i\} = \{v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_d\}$ is a vertex cover of G.
(b) Let $I_G = \bigcap_{i=1}^n J_i$ be an irredundant m-irreducible decomposition of the edge ideal I_G. Prove that for $i = 1, \ldots, n$ we have $J_i \neq \mathfrak{X}$.

EXERCISE 4.3.16. Let $d \geqslant 3$.

(a) Prove that the minimal vertex covers of the complete graph K_d are the sets $V \smallsetminus \{v_i\} = \{v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_d\}$.
(b) Find an irredundant m-irreducible decomposition of I_{K_d}. Justify your answer.

EXERCISE 4.3.17. Let $m, n \geqslant 1$.

(a) Prove that the minimal vertex covers of the complete bipartite graph $B_{m,n}$ are the sets $\{u_1, \ldots, u_m\}$ and $\{v_1, \ldots, v_n\}$.
(b) Find an irredundant m-irreducible decomposition of $I_{B_{m,n}}$. Justify your answer.

EXERCISE 4.3.18. Let $d \geqslant 3$. Find the minimal vertex covers of the d-cycle C_d, and find an irredundant m-irreducible decomposition of I_{C_d}. Justify your answer.

EXERCISE 4.3.19. Let $V = \{v_1, \ldots, v_d\}$ and $R = A[X_1, \ldots, X_d]$. Prove that the association $G \mapsto I_G$ describes a bijection between the set of graphs with vertex set V and the set of square-free "quadratic" monomial ideals of R.

Decompositions of Edge Ideals in Macaulay2.

Exercises.

4.4. Simplicial Complexes and Face Ideals

In this section, A is a non-zero commutative ring with identity.

The previous section gave a method for computing m-irreducible decompositions for quadratic square-free monomial ideals. The next section introduces some tools to accomplish this for arbitrary square-free monomial ideals. This uses the notion of a simplicial complex, defined next. One often thinks of this as a higher dimensional graph. not only does it have vertices and edges, but it also can have shaded triangles, solid tetrahedra, and so on. Again, we take a purely combinatorial approach here.

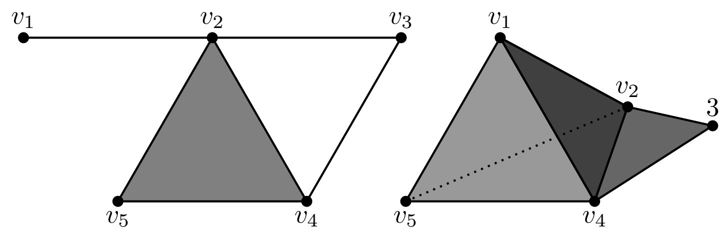
DEFINITION 4.4.1. Let $V = \{v_1, \ldots, v_d\}$ be a finite set. A *simplicial complex* on V is a non-empty collection Δ of subsets of V that is closed under subsets, that is, such that for all subsets $F, G \subseteq V$, if $F \subseteq G$ and $G \in \Delta$, then $F \in \Delta$. An element of Δ is called a *face* of Δ. A face of the form $\{v_i\}$ is called a *vertex* of Δ. A face of the form $\{v_j, v_k\}$ is called an *edge* of Δ. A maximal element of Δ with respect to containment is a *facet* of Δ.

By definition, a simplicial complex Δ on $V = \{v_1, \ldots, v_d\}$ is a subset of the power set $\mathsf{P}(V)$. Note that we do not assume that each singleton $\{v_i\}$ is in Δ. This differs slightly from some definitions. However, this convention allows for some added flexibility.

Since V is finite, every face of Δ is contained in a facet of Δ. In particular, since Δ is non-empty, it has at least one facet. Since Δ is non-empty and closed under subsets, we have $\emptyset \in \Delta$, that is, $\emptyset$ is a face of Δ.

Every graph G with vertex set $V = \{v_1, \ldots, v_d\}$ gives rise to a simplicial complex, namely the complex that contains $\emptyset$ along with every singleton $\{v_i\}$ and every pair $\{v_j, v_k\}$ such that $v_j v_k$ is an edge in G. As with graphs, it can be helpful to sketch the "geometric realization" of a simplicial complex. We will not give a technical definition of this here. The idea is the following: every vertex corresponds to a point; every edge corresponds to a line between two vertices; every face of the form $\{v_1, v_2, v_3\}$ corresponds to a shaded triangle with vertices v_1, v_2, and v_3; every face of the form $\{v_1, v_2, v_3, v_4\}$ corresponds to a solid tetrahedron with vertices v_1, v_2, v_3, and v_4; et cetera. We demonstrate this in the next example.

EXAMPLE 4.4.2. Here are some sketches of simplicial complexes:



The first one Δ consists of an edge, a shaded triangle, and an unshaded triangle. This is the simplicial complex with the following faces:

$$\begin{aligned}
\text{trivial:}\quad & \emptyset \\
\text{vertices:}\quad & \{v_1\}, \{v_2\}, \{v_3\}, \{v_4\}, \{v_5\} \\
\text{edges:}\quad & \{v_1, v_2\}, \{v_2, v_3\}, \{v_2, v_4\}, \{v_2, v_5\}, \{v_3, v_4\}, \{v_4, v_5\} \\
\text{shaded triangle:}\quad & \{v_2, v_4, v_5\} \\
\text{facets:}\quad & \{v_1, v_2\}, \{v_2, v_3\}, \{v_3, v_4\}, \{v_2, v_4, v_5\}.
\end{aligned}$$

The second sketched simplicial complex Δ' consists of a solid tetrahedron and a shaded triangle. With the same vertex-labelling protocol as above, this is the simplicial complex with the following faces:

$$\begin{aligned}
\text{trivial:}\quad & \emptyset \\
\text{vertices:}\quad & \{v_1\}, \{v_2\}, \{v_3\}, \{v_4\}, \{v_5\} \\
\text{edges:}\quad & \{v_1, v_2\}, \{v_1, v_4\}, \{v_1, v_5\}, \{v_2, v_3\}, \\
& \{v_2, v_4\}, \{v_2, v_5\}, \{v_3, v_4\}, \{v_4, v_5\} \\
\text{shaded triangles:}\quad & \{v_1, v_2, v_4\}, \{v_1, v_2, v_5\}, \{v_1, v_4, v_5\}, \{v_2, v_3, v_4\}, \{v_2, v_4, v_5\} \\
\text{solid tetrahedron:}\quad & \{v_1, v_2, v_4, v_5\} \\
\text{facets:}\quad & \{v_2, v_3, v_4\}, \{v_1, v_2, v_4, v_5\}.
\end{aligned}$$

The next definition shows how to use a simplicial complex to construct a monomial ideal.

DEFINITION 4.4.3. Let Δ be a simplicial complex on $V = \{v_1, \ldots, v_d\}$, and set $R = A[X_1, \ldots, X_d]$. The *face ideal* of R associated to Δ is the ideal "generated by the non-faces of Δ":

$$J_\Delta = (X_{i_1} \cdots X_{i_s} \mid 1 \leqslant i_1 < \cdots < i_s \leqslant d \text{ and } \{v_{i_1}, \ldots, v_{i_n}\} \notin \Delta)R.$$

By definition, the face ideal J_Δ is square-free. Next, we compute this ideal for our previous examples.

EXAMPLE 4.4.4. Consider the simplicial complexes from Example 4.4.2. The "non-faces" of Δ are

$$\{v_1,v_3\} \quad \{v_1,v_4\} \quad \{v_1,v_5\} \quad \{v_3,v_5\} \quad \{v_1,v_2,v_3\} \quad \{v_1,v_2,v_4\} \quad \{v_1,v_2,v_5\}$$
$$\{v_1,v_3,v_4\} \quad \{v_1,v_3,v_5\} \quad \{v_1,v_4,v_5\} \quad \{v_2,v_3,v_4\} \quad \{v_2,v_3,v_5\} \quad \{v_3,v_4,v_5\}$$
$$\{v_1,v_2,v_3,v_4\} \quad \{v_1,v_2,v_3,v_5\} \quad \{v_1,v_2,v_4,v_5\} \quad \{v_1,v_3,v_4,v_5\} \quad \{v_2,v_3,v_4,v_5\}$$
$$\{v_1,v_2,v_3,v_4,v_5\}.$$

It follows that the generators for J_Δ are

$$X_1X_3 \quad X_1X_4 \quad X_1X_5 \quad X_3X_5 \quad X_1X_2X_3 \quad X_1X_2X_4 \quad X_1X_2X_5 \quad X_1X_3X_4$$
$$X_1X_3X_5 \quad X_1X_4X_5 \quad X_2X_3X_4 \quad X_2X_3X_5 \quad X_3X_4X_5 \quad X_1X_2X_3X_4 \quad X_1X_2X_3X_5$$
$$X_1X_2X_4X_5 \quad X_1X_3X_4X_5 \quad X_2X_3X_4X_5 \quad X_1X_2X_3X_4X_5$$

Removing redundancies, we have

$$J_\Delta = (X_1X_3, X_1X_4, X_1X_5, X_3X_5, X_2X_3X_4)R.$$

Similarly, for Δ' we have

$$J_{\Delta'} = (X_1X_3, X_3X_5)R = (X_3)R \bigcap (X_1, X_5)R.$$

The following notions are for use in Chapter 5. In particular, the dimension of a simplicial complex gives a measure of its size.

DEFINITION 4.4.5. Let Δ be a simplicial complex on $V = \{v_1, \ldots, v_d\}$. The *dimension* of a face $F \in \Delta$ is $|F| - 1$. The *dimension* of Δ, denoted $\dim(\Delta)$, is the maximal dimension of a face of Δ. The simplicial complex Δ is *pure* if every facet of Δ has the same dimension.

For $i = -1, 0, \ldots, \dim(\Delta)$, let $f_i(\Delta)$ denote the number of i-dimensional faces of Δ. The *f-vector* of Δ is the vector $f(\Delta) = (f_0(\Delta), f_1(\Delta), \ldots, f_{\dim(\Delta)}(\Delta))$.

By definition, and as one might expect, vertices have dimension 0, edges have dimension 1, and so on. Thus, the dimension of a graph is 1. Since the facets of Δ are its maximal faces, one can compute $\dim(\Delta)$ as the maximal dimension of a facet of Δ. For example, for the simplicial complexes from Example 4.4.2, we have

$$\dim(\Delta) = 2 \qquad\qquad f(\Delta) = (5, 6, 1)$$
$$\dim(\Delta') = 3 \qquad\qquad f(\Delta') = (5, 8, 5, 1)$$

Exercises.

EXERCISE 4.4.6. Sketch the geometric realizations of all simplicial complexes on d vertices for $d = 1, 2, 3, 4$. (Do not forget to include complexes with vertices that are not connected to other vertices.)

EXERCISE 4.4.7. Let Δ and Δ' be simplicial complexes on $V = \{v_1, \ldots, v_d\}$, and set $R = A[X_1, \ldots, X_d]$.

(a) Prove that $\Delta \subseteq \Delta'$ if and only if $J_{\Delta'} \subseteq J_\Delta$.
(b) Prove that $\Delta = \Delta'$ if and only if $J_{\Delta'} = J_\Delta$.
(c) Prove that $\Delta = \mathsf{P}(V)$ if and only if $J_\Delta = 0$.
(d) Prove that $\Delta = \{\emptyset\}$ if and only if $J_\Delta = (X_1, \ldots, X_d)R$.

Simplicial Complexes and Face Ideals in Macaulay2.

Exercises.

4.5. Decompositions of Face Ideals

In this section, A is a non-zero commutative ring with identity.

This section gives a method for computing m-irreducible decompositions for face ideals of simplicial complexes. As for edge ideals, this decomposition is given in terms of combinatorial information about the simplicial complex, namely its facets. Moreover, we show how to use this to find m-irreducible decompositions for arbitrary square-free monomial ideals. We begin with some notation for the relevant m-irreducible monomial ideals.

Definition 4.5.1. Let $V = \{v_1, \ldots, v_d\}$, and set $R = A[X_1, \ldots, X_d]$. For each subset $F \subseteq V$, let $Q_F \subseteq R$ be the ideal "generated by the non-elements of F":

$$Q_F = (\{X_i \mid v_i \notin F\})R.$$

For instance, in the ring $R = A[X_1, \ldots, X_5]$ with $V = \{v_1, \ldots, v_5\}$, we have

$$Q_\emptyset = (X_1, \ldots, X_5)R \qquad Q_{\{v_1,v_3\}} = (X_2, X_4, X_5)R \qquad Q_V = 0$$

and so on. In general, given a subset $F \subseteq V$, one has $Q_F = P_{V \smallsetminus F}$ by definition. And a monomial ideal $J \subseteq R$ is square-free and m-irreducible if and only if there exists a subset $F \subseteq V$ such that $J = Q_F$, by Proposition 4.1.3.

Fact 4.5.2. Let $V = \{v_1, \ldots, v_d\}$ be a finite set, and set $R = A[X_1, \ldots, X_d]$.

(a) Given subsets $F, G \subseteq V$, one has $Q_F \subseteq Q_G$ if and only if $G \subseteq F$.
(b) A monomial ideal $J \subsetneq R$ is square-free if and only if there exist subsets $F_1, \ldots, F_n \subseteq V$ such that $J = \bigcap_{i=1}^n Q_{F_i}$; see Proposition 4.3.3.

Like Lemma 4.3.7, the connection between faces and m-irreducible decompositions begins with the next result.

Lemma 4.5.3. *Let Δ be a simplicial complex on $V = \{v_1, \ldots, v_d\}$, and let $F \subseteq V$. Set $R = A[X_1, \ldots, X_d]$. Then $J_\Delta \subseteq Q_F$ if and only if F is a face of Δ.*

Proof. Write $F = \{v_{i_1}, \ldots, v_{i_n}\}$ and $V \smallsetminus F = \{v_{j_1}, \ldots, v_{j_p}\}$, so that $Q_F = (X_{j_1}, \ldots, X_{j_p})R$.

For the forward implication, assume that $J_\Delta \subseteq Q_F$. By way of contradiction, suppose that F is not a face of Δ, that is, $F \notin \Delta$. By definition, this implies that $X_{i_1} \cdots X_{i_n} \in J_\Delta \subseteq Q_F$. It follows that there is an index k such that $X_{i_1} \cdots X_{i_n} \in (X_{j_k})R$. An inspection of exponent vectors shows that there is an index l such that $j_k = i_l$. This says that $F \bigcap (V \smallsetminus F) \neq \emptyset$, a contradiction.

For the reverse implication, assume that $F \in \Delta$. To show that $J_\Delta \subseteq Q_F$, we need to show that each generator of J_Δ is in Q_F. To this end, fix a generator $X_{r_1} \cdots X_{r_q} \in J_\Delta$, corresponding to a "non-face" $V' = \{v_{r_1}, \ldots, v_{r_q}\} \notin \Delta$. Since $F \in \Delta$, the defining condition for a simplicial complex shows that $V' \not\subseteq F$. It follows that there is an index s such that $v_{r_s} \in V' \smallsetminus F$, so $X_{r_s} \in Q_F$. We conclude that the generator $X_{r_1} \cdots X_{r_q}$ is in $(X_{r_s})R \subseteq Q_F$, as desired. $\square$

Next, we present the decomposition theorem for face ideals. As with the corresponding result for edge ideals, it shows how the combinatorial properties of a simplicial complex determine algebraic properties of its face ideal. Remark 4.5.6 shows how this applies to the study of arbitrary square-free monomial ideals.

THEOREM 4.5.4. *Let Δ be a simplicial complex on $V = \{v_1, \ldots, v_d\}$, and set $R = A[X_1, \ldots, X_d]$. Then the ideal $J_\Delta \subseteq R$ has the following m-irreducible decompositions*

$$J_\Delta = \bigcap_{F \in \Delta} Q_F = \bigcap_{F \text{ facet}} Q_F$$

where the first intersection is taken over all faces of Δ, and the second intersection is taken over all facets of Δ. The second intersection is irredundant.

PROOF. Fact 4.5.2(a) shows that the second intersection is irredundant. The containment $\bigcap_{F\in\Delta} Q_F \subseteq \bigcap_{F \text{ facet}} Q_F$ is straightforward. The reverse containment $\bigcap_{F\in\Delta} Q_F \supseteq \bigcap_{F \text{ facet}} Q_F$ follows from the fact that every face of Δ is contained in a facet, along with Fact 4.5.2(a). The containment $J_\Delta \subseteq \bigcap_{F\in\Delta} Q_F$ is from Lemma 4.5.3.

For the final containment $J_\Delta \subseteq \bigcap_{F\in\Delta} Q_F$ recall that J_Δ is square-free. Hence, Fact 4.5.2(b) provides subsets $F_1, \ldots, F_n$ such that $J_\Delta = \bigcap_{j=1}^n Q_{F_j}$. For each index j, we then have $J_\Delta \subseteq Q_{F_j}$, so Lemma 4.5.3 implies that F_j is a face of Δ. It follows that $J_\Delta = \bigcap_{j=1}^n Q_{F_j} \supseteq \bigcap_{F\in\Delta} Q_F$, as desired. $\square$

EXAMPLE 4.5.5. We compute an irredundant m-irreducible decomposition of the ideals J_Δ and $J_{\Delta'}$ from Example 4.4.4. Using Theorem 4.5.4, this can be read from the lists of facets that we computed in Example 4.4.2:

$$\begin{aligned} J_\Delta &= (X_2, X_4, X_5)R \bigcap (X_2, X_3, X_5)R \bigcap (X_2, X_3, X_4)R \\ &\quad \bigcap (X_1, X_2, X_4)R \bigcap (X_1, X_5)R \\ J_{\Delta'} &= (X_1, X_5)R \bigcap (X_3)R. \end{aligned}$$

Notice that this second computation agrees with the decomposition of $J_{\Delta'}$ from Example 4.4.4.

REMARK 4.5.6. Set $V = \{v_1, \ldots, v_d\}$ and $R = A[X_1, \ldots, X_d]$. It is straightforward to identify the monomial ideals $J \subseteq R$ that are of the form J_Δ for some simplicial complex Δ on V: they are precisely the square-free monomial ideals $I \subsetneq R$. Thus, we can use the techniques of this section to find m-irreducible decompositions of such ideals, as in the following example.

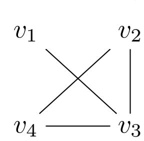
EXAMPLE 4.5.7. We compute an irredundant m-irreducible decomposition of the ideal

$$J = (X_1X_2, X_2X_3X_4, X_1X_4)R \subseteq R = A[X_1, X_2, X_3, X_4].$$

First, we find a simplicial complex Δ on $V = \{v_1, v_2, v_3, v_4\}$ such that $J = J_\Delta$. To do this, we need to add a face for every square-free monomial that is not in J:

$$\Delta = \{\emptyset, \{v_1\}, \{v_2\}, \{v_3\}, \{v_4\}, \{v_1, v_3\}, \{v_2, v_3\}, \{v_2, v_4\}, \{v_3, v_4\}\}.$$

The geometric realization of Δ is the following graph:



Next, we list the facets of Δ:

$$\{v_1, v_3\} \qquad \{v_2, v_3\} \qquad \{v_2, v_4\} \qquad \{v_3, v_4\}.$$

Finally, we read off the decomposition using Theorem 4.5.4:

$$J = J_\Delta = (X_2, X_4)R \bigcap (X_1, X_4)R \bigcap (X_1, X_3)R \bigcap (X_1, X_2)R.$$

Given a graph G with vertex set V, Remark 4.5.6 implies that the edge ideal I_G is of the form J_{Δ_G} for some simplicial complex Δ_G on V. We conclude this section by identifying and investigating Δ_G.

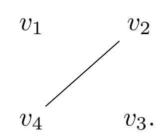
Definition 4.5.8. Let G be a graph with vertex set $V = \{v_1, \ldots, v_d\}$ and edge set E. A subset $F \subseteq V$ is *independent in* G if none of the vertices in F are adjacent in G. An independent subset in G is *maximal* if it is maximal with respect to containment. Let Δ_G denote the set of independent subsets of G.

For instance, every singleton $\{v_i\} \subseteq V$ is independent in G, as is the empty set $\emptyset \subset V$. Furthermore, every subset of an independent set in G is also independent in G, so Δ_G is a simplicial complex on V. Here is a concrete example of this construction.

Example 4.5.9. Consider the graph G from Example 4.3.6. The independent subsets in G are exactly the following:

$$\emptyset \qquad \{v_1\} \qquad \{v_2\} \qquad \{v_3\} \qquad \{v_4\} \qquad \{v_2, v_4\}.$$

That is, the geometric realization of Δ_G is as follows:



The maximal independent subsets in G are $\{v_1\}$, $\{v_3\}$, and $\{v_2, v_4\}$.

The next result shows that the faces of Δ_G are in bijection with the vertex covers of G, and the facets of Δ_G are in bijection with the minimal vertex covers of G.

Lemma 4.5.10. *Let G be a graph with vertex set V.*

(a) *A subset $F \subseteq V$ is independent in G if and only if $V \smallsetminus F$ is a vertex cover of G.*
(b) *An independent subset $F \subseteq V$ in G is maximal if and only if the vertex cover $V \smallsetminus F$ of G is minimal.*

Proof. Exercise. $\square$

The next result makes explicit the algebraic connection between a given graph G and the simplicial complex Δ_G.

Theorem 4.5.11. *Let G be a graph with vertex set $V = \{v_1, \ldots, v_d\}$ and edge set E. Set $R = A[X_1, \ldots, X_d]$. Then we have $I_G = J_{\Delta_G}$.*

Proof. For the containment $I_G \subseteq J_{\Delta_G}$, consider an arbitrary generator X_iX_j of I_G, given by the edge $v_iv_j \in E$. It follows that the set $\{v_i, v_j\}$ is not independent in G, so it is a non-face of Δ_G by definition. It follows that we have $X_iX_j \in \Delta_G$.

For the reverse containment $I_G \supseteq J_{\Delta_G}$, consider a generator $X_{i_1} \cdots X_{i_n}$ of J_{Δ_G}, given by the non-face $\{v_{i_1}, \ldots, v_{i_n}\} \notin \Delta_G$. By definition, this means that the set $\{v_{i_1}, \ldots, v_{i_n}\}$ is not independent in G, so it must contain a pair of adjacent vertices v_{i_k}, v_{i_m}. It follows that $X_{i_k}X_{i_m}$ is a generator of I_G. Thus, we have $X_{i_1} \cdots X_{i_n} \in (X_{i_k}X_{i_m})R \subseteq I_G$, as desired. $\square$

For example, consider the graph G from Example 4.3.6, with Δ_G identified in Example 4.5.9. The non-faces of Δ_G are exactly the following subsets of $V = \{v_1, v_2, v_3, v_4\}$:

$$\begin{array}{ccccc} \{v_1, v_2\} & \{v_1, v_3\} & \{v_1, v_4\} & \{v_2, v_3\} & \{v_3, v_4\} \\ \{v_1, v_2, v_3\} & \{v_1, v_2, v_4\} & \{v_1, v_3, v_4\} & \{v_2, v_3, v_4\} & \{v_1, v_2, v_3, v_4\}. \end{array}$$

Thus, the ideal J_{Δ_G} is generated by the following list of monomials: X_1X_2, X_1X_3, X_1X_4, X_2X_3, X_3X_4, $X_1X_2X_3$, $X_1X_2X_4$, $X_1X_3X_4$, $X_2X_3X_4$, $X_1X_2X_3X_4$. Removing redundancies from this list, we see that

$$J_{\Delta_G} = (X_1X_2, X_1X_3, X_1X_4, X_2X_3, X_3X_4)R = I_G$$

as in Theorem 4.5.11.

The next result shows how one can use this construction to find m-irreducible decompositions of edge ideals of graphs.

THEOREM 4.5.12. *Let G be a graph with vertex set $V = \{v_1, \ldots, v_d\}$ and edge set E. Set $R = A[X_1, \ldots, X_d]$. Then the ideal $I_G \subseteq R$ has the following m-irreducible decompositions*

$$J_\Delta = \bigcap_{F \text{ indep.}} Q_F = \bigcap_{F \text{ max. indep.}} Q_F$$

where the first intersection is taken over all independent subsets in G, and the second intersection is taken over all maximal independent subsets in G. The second intersection is irredundant.

PROOF. By definition, the independent subsets in G are the faces of Δ_G, and the maximal independent subsets in G are the facets of Δ_G. Thus, the result follows from Theorem 4.5.4. (Alternately, one can combine Theorem 4.5.4 and Lemma 4.5.10.) $\square$

For instance, consider the graph G from Example 4.3.6, with maximal independent sets identified in Example 4.5.9. Theorem 4.5.12 implies that the irredundant m-irreducible decomposition of I_G is

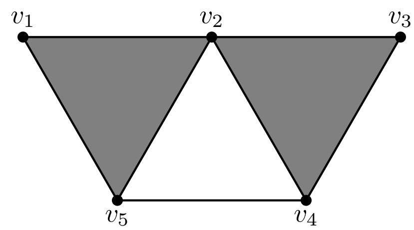
$$I_G = Q_{\{v_1\}} \bigcap Q_{\{v_3\}} \bigcap Q_{\{v_2,v_4\}} = (X_2, X_3, X_4)R \bigcap (X_1, X_2, X_4)R \bigcap (X_1, X_3)R.$$

Compare to Example 4.3.9.

In general, given an irredundant m-irreducible decomposition $I_G = \bigcap_{i=1}^n P_{V_i}$ as in Proposition 4.3.3, one concludes that the maximal independent subsets in G are precisely $V \smallsetminus V_1, \ldots, V \smallsetminus V_n$. Indeed, Theorem 4.5.12 gives an irredundant m-irreducible decomposition $I_G = \bigcap_{F \text{ max. indep.}} Q_F$, so the uniqueness of such decompositions from Theorem 3.3.8 provides the desired conclusion.

Exercises.

EXERCISE 4.5.13. Set $R = A[X_1, \ldots, X_5]$, and let Δ be the simplicial complex represented by the following sketch:



(a) Find $\dim(\Delta)$ and $f(\Delta)$.
(b) Find an irredundant monomial generating sequence for J_Δ.
(c) Find all facets of Δ.
(d) Use Theorem 4.5.4 to find an irredundant m-irreducible decomposition of J_Δ.
(e) Verify the decomposition $J_\Delta = \bigcap_F Q_F$ from part (d) as in Exercise 4.3.11(d).

Justify your answers.

Exercise 4.5.14. Verify the following decomposition

$$J_\Delta$$
$$= (X_2, X_4, X_5)R \bigcap (X_2, X_3, X_5)R \bigcap (X_2, X_3, X_4)R \bigcap (X_1, X_2, X_4)R \bigcap (X_1, X_5)R$$

from Example 4.5.5 as in Exercise 4.3.11(d).

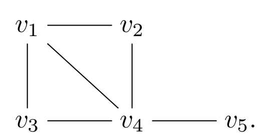
Exercise 4.5.15. Verify the decomposition

$$J = (X_2, X_4)R \bigcap (X_1, X_4)R \bigcap (X_1, X_3)R \bigcap (X_1, X_2)R$$

from Example 4.5.7 as in Exercise 4.3.11(d).

Exercise 4.5.16. Set $R = A[X_1, \ldots, X_4]$ and find an irredundant m-irreducible decomposition of the ideal $J = (X_1X_2X_3, X_1X_2X_4, X_1X_3X_4, X_2X_3X_4)R$ as in Example 4.5.7. Verify that your decomposition is correct as in Exercise 4.3.11(d). Justify your answer.

Exercise 4.5.17. Set $R = A[X_1, \ldots, X_5]$, and let G be the graph represented by the following sketch:



(a) Find the independent subsets in G and the maximal independent subsets in G. Sketch the geometric realization of Δ_G.
(b) Find $\dim(\Delta_G)$ and $f(\Delta_G)$.
(c) Compute an irredundant monomial generating sequence for J_{Δ_G}, and compare it to the generating sequence from Exercise 4.3.11(a).
(d) Use Theorem 4.5.12 to find an irredundant m-irreducible decomposition of I_G, and compare it to the decomposition from Exercise 4.3.11(c).

Justify your answers.

Exercise 4.5.18. Prove Lemma 4.5.10.

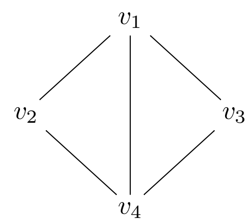
Exercise 4.5.19. Fix a partially ordered set $\Pi = (V, \leqslant)$ with $V = \{v_1, \ldots, v_d\}$. The *order complex* associated to Π is the set of all chains in Π:

$$\Delta(\Pi) = \{\{v_{i_1}, \ldots, v_{i_n}\} \subseteq V \mid n \geqslant 0 \text{ and } v_{i_1} \leqslant \cdots \leqslant v_{i_n}\}.$$

Set $R = A[X_1, \ldots, X_d]$.

(a) Prove that the order complex associated to Π is a simplicial complex on V.

(b) Sketch the geometric realization of the order complex $\Delta(\Pi)$ associated to the following partially ordered set:



Here the order is represented "vertically" by the graph structure. For instance, we have $v_4 < v_2 < v_1$, hence $v_4 < v_1$, and so on.

(c) Prove that the face ideal $J_{\Delta(\Pi)}$ is "generated by the pairs of incomparable elements":

$$J_{\Delta(\Pi)} = (X_iX_j \mid v_i \not\leqslant v_j \text{ and } v_j \not\leqslant v_i)R.$$

(d) Prove that $J_{\Delta(\Pi)}$ can be decomposed in terms of the chains in Π:

$$J_{\Delta(\Pi)} = \bigcap_{v_{i_1} < \cdots < v_{i_n}} Q_{\{v_{i_1}, \cdots, v_{i_n}\}} = \bigcap_{\substack{v_{i_1} < \cdots < v_{i_n} \\ \text{max.}}} Q_{\{v_{i_1}, \cdots, v_{i_n}\}}.$$

Here the first intersection is taken over all chains $v_{i_1} < \cdots < v_{i_n}$ in Π, and the second intersection is taken over all maximal chains $v_{i_1} < \cdots < v_{i_n}$ in Π. Prove that the second decomposition is irredundant.

(e) Use part (d) to find an irredundant m-irreducible decomposition of the face ideal $J_{\Delta(\Pi)}$ where Π is the partially ordered set from part (b). Justify your answer.

(f) Verify that your decomposition from part (e) is correct as in Exercise 4.3.11(d).

EXERCISE 4.5.20. Let G be a graph with vertex set $V = \{v_1, \ldots, v_d\}$ and edge set E. Identify G with its associated simplicial complex. Set $R = A[X_1, \ldots, X_d]$.

(a) Prove that the face ideal J_G is "generated by the non-edges of G along with all the closed triangles":

$$J_G = (\{X_iX_j \mid v_iv_j \text{ is not an edge in } G\} \cup \{X_iX_jX_k \mid 1 \leqslant i < j < k \leqslant d\})R.$$

(b) Prove that J_G can be decomposed in terms of the edges in G:

$$\begin{aligned} J_G &= \left(\bigcap_{v_i \in V} Q_{\{v_i\}} \right) \bigcap \left(\bigcap_{v_iv_j \in E} Q_{\{v_i, v_j\}} \right) \\ &= \left(\bigcap_{\substack{v_i \in V \\ \text{isolated}}} Q_{\{v_i\}} \right) \bigcap \left(\bigcap_{v_iv_j \in E} Q_{\{v_i, v_j\}} \right). \end{aligned}$$

Here the first intersection is taken over all vertices of G, and the third intersection is taken over all isolated vertices of G. The second and fourth intersections are taken over all edges v_iv_j in G. Prove that the second decomposition is irredundant.

(c) Use part (b) to find an irredundant m-irreducible decomposition of the face ideal J_G where G is the graph from Exercise 4.3.11. Justify your answer.

(d) Verify that your decomposition from part (c) is correct as in Exercise 4.3.11(d).

EXERCISE 4.5.21. Let $V = \{v_1, \ldots, v_d\}$ and $R = A[X_1, \ldots, X_d]$. Prove that the association $\Delta \mapsto J_\Delta$ describes a bijection between the set of simplicial complexes on V and the set of square-free monomial ideals of R.

Decompositions of Face Ideals in Macaulay2.

Exercises.

4.6. Facet Ideals and Their Decompositions

In this section, we investigate a version of the edge ideal for simplicial complexes (instead of just for graphs). It gives another algebraic construction defined in terms of some combinatorial data from a simplicial complex, and we show how other combinatorial information provides m-irreducible decompositions.

DEFINITION 4.6.1. Let Δ be a simplicial complex on $V = \{v_1, \ldots, v_d\}$, and set $R = A[X_1, \ldots, X_d]$. The *facet ideal* of R associated to Δ is the ideal "generated by the facets of Δ":

$$K_\Delta = (X_{i_1} \cdots X_{i_s} \mid 1 \leqslant i_1 < \cdots < i_s \leqslant d \text{ and } \{v_{i_1}, \ldots, v_{i_n}\} \text{ is a facet in } \Delta)R.$$

For example, we consider the simplicial complexes from Example 4.4.2. The facets of Δ are $\{v_1, v_2\}$, $\{v_2, v_3\}$, $\{v_3, v_4\}$, $\{v_2, v_4, v_5\}$. It follows that we have $K_\Delta = (X_1X_2, X_2X_3, X_3X_4, X_2X_4X_5)$R. Similarly, for the complex Δ' we have $K_{\Delta'} = (X_2X_3X_4, X_1X_2X_4X_5)R$.

In general, the facet ideal K_Δ is square-free, by definition. Moreover, since the facets of Δ are incomparable with respect to containment, they generate K_Δ irredundantly, that is, the set

$$\{X_{i_1} \cdots X_{i_s} \mid 1 \leqslant i_1 < \cdots < i_s \leqslant d \text{ and } \{v_{i_1}, \ldots, v_{i_n}\} \text{ is a facet in } \Delta\}$$

describes an irredundant monomial generating sequence for K_Δ.

The following notions are used to identify which ideals $P_{V'}$ occur in an (irredundant) m-irreducible decomposition of a facet ideal.

DEFINITION 4.6.2. Let Δ be a simplicial complex on $V = \{v_1, \ldots, v_d\}$. A *vertex cover* of Δ is a subset $V' \subseteq V$ such that for each facet F in Δ there is a vertex $v_i \in F \bigcap V'$. A vertex cover V' is *minimal* if it does not properly contain another vertex cover of Δ.

As with a graph, the vertex set V is a vertex cover of Δ. In particular, Δ has a vertex cover. Also, the set of vertex covers of Δ is closed under subsets: if $V' \subseteq V$ is a vertex cover of Δ and $V' \subseteq V'' \subseteq V$, then V'' is a vertex cover of Δ. Since V is finite, every vertex cover of Δ contains a minimal vertex cover of Δ.

EXAMPLE 4.6.3. We compute the minimal vertex covers of the simplicial complexes from Example 4.4.2.

First, we find the minimal vertex covers of Δ containing v_2. If $v_2 \in V'$, then the facets $\{v_1, v_2\}$, $\{v_2, v_3\}$, and $\{v_2, v_4, v_5\}$ are "covered". This leaves only the facet v_3v_4 "uncovered". This facet can be covered either by adding v_3 or by adding v_4. Thus, the minimal vertex covers containing v_2 are $\{v_2, v_3\}$ and $\{v_2, v_4\}$.

Next, we find the minimal vertex covers of Δ that do not contain v_2. If $v_2 \notin V'$, we must have $v_1, v_3 \in V'$ in order to cover the facets $\{v_1, v_2\}$ and $\{v_2, v_3\}$. Moreover, to cover the facet $\{v_2, v_4, v_5\}$, we must add either v_4 or v_5. It is straightforward to show that the sets $\{v_1, v_3, v_4\}$ and $\{v_1, v_3, v_5\}$ are minimal vertex covers of Δ.

A similar argument shows that the minimal vertex covers of Δ' are $\{v_2\}$, $\{v_4\}$, $\{v_1, v_3\}$, and $\{v_3, v_5\}$.

Similarly to previous constructions in this chapter, t he connection between vertex covers and m-irreducible decompositions begins with the next result. It uses the notation from Definition 4.3.1.

LEMMA 4.6.4. *Let Δ be a simplicial complex on $V = \{v_1, \ldots, v_d\}$, and let $V' \subseteq V$. Set $R = A[X_1, \ldots, X_d]$. Then $K_\Delta \subseteq P_{V'}$ if and only if V' is a vertex cover of Δ.*

PROOF. Write $V' = \{v_{i_1}, \ldots, v_{i_n}\}$, so that $P_{V'} = (X_{i_1}, \ldots, X_{i_n})R$.

For the forward implication, assume that $K_\Delta \subseteq P_{V'}$. We show that V' is a vertex cover of G. Let $\{v_{j_1}, \ldots, v_{j_k}\}$ be a facet of Δ. Then we have $X_{j_1} \cdots X_{j_k} \in K_\Delta \subseteq P_{V'} = (X_{i_1}, \ldots, X_{i_n})R$. It follows that $X_{j_1} \cdots X_{j_k} \in (X_{i_m})R$ for some index m. A comparison of exponent vectors shows that $j_l = i_m$ for some l, that is, that $v_{j_l} = v_{i_m} \in V'$. Thus V' is a vertex cover of Δ.

For the reverse implication, assume that V' is a vertex cover of Δ. To show that $K_\Delta \subseteq P_{V'}$, we need to show that each generator of K_Δ is in $P_{V'}$. To this end, fix a generator $X_{j_1} \cdots X_{j_k} \in K_\Delta$, corresponding to a facet $\{v_{j_1}, \ldots, v_{j_k}\}$ in Δ. Since V' is a vertex cover of Δ, we have $v_{j_l} \in V'$ for some index l. It follows that $X_{j_l} \in P_{V'}$, so $X_{j_1} \cdots X_{j_k} \in P_{V'}$. $\square$

Here is the decomposition theorem for facet ideals. As in previous results, it shows how combinatorial information from a given simplicial complex informs algebraic properties of its facet ideal. Again, the subsequent remark shows how this applies to arbitrary square-free monomial ideals.

THEOREM 4.6.5. *Let Δ be a simplicial complex on $V = \{v_1, \ldots, v_d\}$, and set $R = A[X_1, \ldots, X_d]$. Then the facet ideal $K_\Delta \subseteq R$ has the following m-irreducible decompositions*

$$K_\Delta = \bigcap_{V'} P_{V'} = \bigcap_{V' \ min.} P_{V'}$$

where the first intersection is taken over all vertex covers of Δ, and the second intersection is taken over all minimal vertex covers of Δ. The second intersection is irredundant.

PROOF. Exercise. Argue as in the proof of Theorem 4.3.8. $\square$

EXAMPLE 4.6.6. We compute an irredundant m-irreducible decomposition of the ideals K_Δ and $K_{\Delta'}$ where Δ and Δ' are the simplicial complexes from Example 4.4.2. Using Theorem 4.3.8, this can be read from the list of minimal vertex covers that we computed in Example 4.6.3:

$$K_\Delta = (X_2, X_3)R \bigcap (X_2, X_4)R \bigcap (X_1, X_3, X_4)R \bigcap (X_1, X_3, X_5)R$$
$$K_{\Delta'} = (X_2)R \bigcap (X_4)R \bigcap (X_1, X_5)R \bigcap (X_3, X_5)R.$$

In general, given an irredundant m-irreducible decomposition $K_\Delta = \bigcap_{i=1}^n P_{V_i}$ as in Proposition 4.3.3, one concludes the the minimal vertex covers of Δ are precisely $V_1, \ldots, V_n$. Indeed, Theorem 4.6.5 gives an irredundant m-irreducible decomposition $K_\Delta = \bigcap_{V' \text{ min.}} P_{V'}$, so the uniqueness of such decompositions from Theorem 3.3.8 provides the desired conclusion.

Set $V = \{v_1, \ldots, v_d\}$ and $R = A[X_1, \ldots, X_d]$. It is straightforward to identify the monomial ideals $J \subseteq R$ that are of the form K_Δ for some simplicial complex Δ on V: they are precisely the square-free monomial ideals $I \subsetneq R$. Thus, we can use the techniques of this section to find m-irreducible decompositions of such ideals, as in the following example.

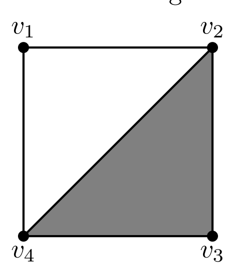
Example 4.6.7. We compute an irredundant m-irreducible decomposition of the ideal

$$J = (X_1X_2, X_2X_3X_4, X_1X_4)R \subseteq R = A[X_1, X_2, X_3, X_4].$$

First, we find a simplicial complex Δ on $V = \{v_1, v_2, v_3, v_4\}$ such that $J = K_\Delta$. To do this, we need to add a facet for every monomial in the irredundant generating sequence of J; the faces of Δ are then the subsets of these facets:

$$\begin{aligned} \text{facets:} \quad & \{v_1, v_2\}, \{v_2, v_3, v_4\}, \{v_1, v_4\} \\ \text{trivial face:} \quad & \emptyset \\ \text{vertices:} \quad & \{v_1\}, \{v_2\}, \{v_3\}, \{v_4\} \\ \text{edges:} \quad & \{v_1, v_2\}, \{v_2, v_3\}, \{v_2, v_4\}, \{v_3, v_4\}, \{v_1, v_4\} \\ \text{shaded triangles:} \quad & \{v_2, v_3, v_4\} \end{aligned}$$

The geometric realization of Δ is the following:



Next, we list the minimal vertex covers of Δ:

$$\{v_1, v_2\} \qquad \{v_1, v_3\} \qquad \{v_1, v_4\} \qquad \{v_2, v_4\}.$$

Finally, we read off the decomposition using Theorem 4.5.4:

$$J = J_\Delta = (X_1, X_2)R \bigcap (X_1, X_3)R \bigcap (X_1, X_4)R \bigcap (X_2, X_4)R.$$

Compare this to the decomposition from Example 4.5.7.

Exercises.

Exercise 4.6.8. Set $R = A[X_1, \ldots, X_5]$, and let Δ be the simplicial complex from Exercise 4.5.13.

(a) Find an irredundant monomial generating sequence for K_Δ.
(b) Find all minimal vertex covers of Δ.
(c) Use Theorem 4.6.5 to find an irredundant m-irreducible decomposition of K_Δ.
(d) Verify the decomposition $K_\Delta = \bigcap_{V'} P_{V'}$ from part (c) as in Exercise 4.3.11(d).

Justify your answers.

EXERCISE 4.6.9. Verify the following decompositions

$$K_\Delta = (X_2, X_3)R \bigcap (X_2, X_4)R \bigcap (X_1, X_3, X_4)R \bigcap (X_1, X_3, X_5)R$$
$$K_{\Delta'} = (X_2)R \bigcap (X_4)R \bigcap (X_1, X_5)R \bigcap (X_3, X_5)R.$$

from Example 4.6.6 as in Exercise 4.3.11(d).

EXERCISE 4.6.10. Prove Theorem 4.6.5.

EXERCISE 4.6.11. Set $R = A[X_1, \ldots, X_4]$ and find an irredundant m-irreducible decomposition of the ideal $J = (X_1X_2X_3, X_1X_2X_4, X_1X_3X_4, X_2X_3X_4)R$ as in Example 4.6.7. Verify that your decomposition is correct as in Exercise 4.3.11(d). Justify your answer.

EXERCISE 4.6.12. Let $V = \{v_1, \ldots, v_d\}$ and $R = A[X_1, \ldots, X_d]$. Prove that the association $\Delta \mapsto K_\Delta$ describes a bijection between the set of simplicial complexes on V and the set of square-free monomial ideals of R.

EXERCISE 4.6.13. Let $V = \{v_1, \ldots, v_d\}$ and $R = A[X_1, \ldots, X_d]$. Let Δ be a simplicial complex on V. The facet ideal K_Δ is a square-free monomial ideal of R, so there is a simplicial complex $\Lambda(\Delta)$ such that $K_\Delta = J_{\Lambda(\Delta)}$. Describe $\Lambda(\Delta)$ in terms of Δ. Justify your answer.

4.7. Exploration: Alexander Duality

In this section, A is a non-zero commutative ring with identity.

This section explores the connection between monomial generating sequences and m-irreducible decompositions of square-free monomial ideals that manifests as Alexander duality.

DEFINITION 4.7.1. Set $V = \{v_1, \ldots, v_d\}$ and $R = A[X_1, \ldots, X_d]$. For each $V' \subseteq V$, set $\underline{n}(V') = (n_1, \ldots, n_d)$ where

$$n_i = \begin{cases} 0 & \text{if } v_i \notin V' \\ 1 & \text{if } v_i \in V' \end{cases}$$

and set $\underline{X}^{V'} = \underline{X}^{\underline{n}(V')}$.

For example, consider $V = \{v_1, v_2, v_3, v_4\}$ and $R = A[X_1, X_2, X_3, X_4]$. Then

$$\underline{n}(\emptyset) = (0,0,0,0) \qquad \underline{n}(\{v_1, v_4\}) = (1,0,0,1) \qquad \underline{n}(V) = (1,1,1,1)$$

and

$$\underline{X}^{\emptyset} = 1 \qquad \underline{X}^{\{v_1,v_4\}} = X_1X_4 \qquad \underline{X}^{V} = X_1X_2X_3X_4.$$

In general, for each $V' \subseteq V$, the monomial $\underline{X}^{V'}$ is square-free. On the other hand, every square-free monomial in R is of the form $\underline{X}^{V'}$ for some $V' \subseteq V$.

EXERCISE 4.7.2. Set $V = \{v_1, \ldots, v_d\}$ and $R = A[X_1, \ldots, X_d]$. Prove that, given subsets $V', V'' \subseteq V$ one has $P_{V'} \subseteq P_{V''}$ if and only if $\underline{X}^{V''} \in (\underline{X}^{V'})R$.

DEFINITION 4.7.3. Set $V = \{v_1, \ldots, v_d\}$ and $R = A[X_1, \ldots, X_d]$. Given a square-free monomial ideal $I \subseteq R$ define the $*$-*dual* of I to be the ideal

$$I^* = \bigcap_{\underline{X}^{V'} \in I} P_{V'} = \bigcap_{\underline{X}^{V'} \in I} Q_{V \smallsetminus V'}$$

where each intersection is taken over the set of all subsets $V' \subseteq V$ such that $\underline{X}^{V'} \in I$; define $I^{**} = (I^*)^*$.

EXERCISE 4.7.4. Set $V = \{v_1, \ldots, v_d\}$ and $R = A[X_1, \ldots, X_d]$. Let I be a square-free monomial ideal of R with monomial generating sequence $\underline{X}^{V_1}, \ldots, \underline{X}^{V_n}$.

(a) Prove that I^* is square-free. (In particular, the definition of I^{**} makes sense.)
(b) Prove that $I^* = \bigcap_{i=1}^n P_{V_i}$.
(c) Prove that the generating sequence $\underline{X}^{V_1}, \ldots, \underline{X}^{V_n}$ is irredundant if and only if the intersection $\bigcap_{i=1}^n P_{V_i}$ is irredundant.

EXERCISE 4.7.5. Set $V = \{v_1, \ldots, v_d\}$ and $R = A[X_1, \ldots, X_d]$. Prove that $R^* = 0$ and $0^* = R$. For each $V' \subseteq V$, find $(P_{V'})^*$ and prove that $(P_{V'})^{**} = P_{V'}$.

EXERCISE 4.7.6. Let I, J be square-free monomial ideals in $R = A[X_1, \ldots, X_d]$, and set $V = \{v_1, \ldots, v_d\}$.

(a) Prove that $I \subseteq J$ if and only if every square-free monomial in I is in J.
(b) Prove that $I \subseteq J$ if and only if for every $V' \subseteq V$ such that $J \subseteq P_{V'}$ we have $I \subseteq P_{V'}$.
(c) Prove that $I \subseteq J$ if and only if $J^* \subseteq I^*$.
(d) Prove that $I = J$ if and only if $J^* = I^*$.

DEFINITION 4.7.7. Set $V = \{v_1, \ldots, v_d\}$ and $R = A[X_1, \ldots, X_d]$. Fix a square-free monomial ideal $I \subsetneq R$ with irredundant m-irreducible decomposition $I = \bigcap_{i=1}^n P_{V_i}$ where $V_1, \ldots, V_n$ are subsets of V. (See Proposition 4.3.3.) Define the $\vee$-*dual* of I to be the ideal

$$I^\vee = (\underline{X}^{V_1}, \ldots, \underline{X}^{V_n})R.$$

When $I \neq 0$, set $I^{\vee\vee} = (I^\vee)^\vee$.

EXERCISE 4.7.8. Set $V = \{v_1, \ldots, v_d\}$ and $R = A[X_1, \ldots, X_d]$. Let $I \subsetneq R$ be a square-free monomial ideal with irredundant m-irreducible decomposition $I = \bigcap_{i=1}^n P_{V_i}$ where $V_1, \ldots, V_n$ are subsets of V.

(a) Prove that $I^\vee$ is square-free.
(b) Prove that, if $I \neq 0$, then $I^\vee \neq R$. (In particular, the definition of $I^{\vee\vee}$ makes sense.)
(c) Prove that the monomial generating sequence $\underline{X}^{V_1}, \ldots, \underline{X}^{V_n}$ is irredundant.
(d) Prove that if $I = \bigcap_{j=1}^m P_{W_j}$ where $W_1, \ldots, W_m$ are subsets of V, then $I^\vee = (\underline{X}^{W_1}, \ldots, \underline{X}^{W_m})R$.

EXERCISE 4.7.9. Set $V = \{v_1, \ldots, v_d\}$ and $R = A[X_1, \ldots, X_d]$. Prove that $0^\vee = R$. For each $V' \subseteq V$, compute $(P_{V'})^\vee$ and prove that $(P_{V'})^{\vee\vee} = P_{V'}$.

EXERCISE 4.7.10. Let $I, J \subsetneq R = A[X_1, \ldots, X_d]$ be square-free monomial ideals.

(a) Prove that $I \subseteq J$ if and only if $J^\vee \subseteq I^\vee$.
(b) Prove that $I = J$ if and only if $J^\vee = I^\vee$.

EXERCISE 4.7.11. Set $R = A[X_1, \ldots, X_d]$, and let I be a square-free monomial ideal of R.

(a) Prove that if $I \neq R$, then $I^{\vee *} = I$.
(b) Prove that if $I \neq 0$, then $I^{* \vee} = I$.

The goal of the remainder of this section is to prove that if $I \neq R$, then $I^\vee = I^*$. This is done using simplicial complexes.

DEFINITION 4.7.12. Let Δ be a simplicial complex on $V = \{v_1, \ldots, v_d\}$. The *Alexander dual* of Δ is the set of all compliments of the "non-faces" of Δ:

$$\Delta^\vee = \{V \smallsetminus F \mid F \subset V \text{ and } F \notin \Delta\}.$$

When $\Delta \neq \mathsf{P}(V)$, set $\Delta^{\vee\vee} = (\Delta^\vee)^\vee$.

EXERCISE 4.7.13. Sketch the geometric realization of the Alexander dual of the simplicial complex Δ from Exercise 4.5.13.

EXERCISE 4.7.14. Let Δ and Δ' be simplicial complexes on $V = \{v_1, \ldots, v_d\}$.

(a) Prove that $\Delta' \subseteq \Delta$ if and only if $\Delta^\vee \subseteq \Delta'^\vee$.
(b) Prove that $\Delta' = \Delta$ if and only if $\Delta^\vee = \Delta'^\vee$.

EXERCISE 4.7.15. Let Δ be a simplicial complex on $V = \{v_1, \ldots, v_d\}$.

(a) Prove that $\mathsf{P}(V)^\vee = \emptyset$.
(b) Prove that, if $\Delta \neq \mathsf{P}(V)$, then $\Delta^\vee$ is a simplicial complex on V. (In particular, the definition of $\Delta^{\vee\vee}$ makes sense.)
(c) Prove that $\Delta^\vee \neq \mathsf{P}(V)$.

EXERCISE 4.7.16. Set $R = A[X_1, \ldots, X_d]$, and let I be a square-free monomial ideal of R such that $0 \neq I \neq R$. Let Δ be a simplicial complex on $V = \{v_1, \ldots, v_d\}$ such that $I = J_\Delta$.

(a) Prove that $J_{\Delta^\vee} = (J_\Delta)^*$.
(b) Prove that $J_{\Delta^\vee} = (J_\Delta)^\vee$.
(c) Prove that $I^\vee = I^*$.
(d) Prove that $I^{\vee\vee} = I$.
(e) Prove that $I^{**} = I$.

Facet Ideals and Their Decompositions in Macaulay2.

Exercises.

Conclusion

Include some history here. Talk about some of the literature from this area. Talk about topological Alexander duality here.

CHAPTER 5

Connections with Other Areas

This chapter deals with other areas of mathematics and engineering intersect with the notions we have already discussed. We omit many details in the Chapter. The point is to give big-picture ideas about other realms where these notions arise. Our purpose here is to give some big-picture idea of the significance of these notions. The interested reader should consult, e.g., [**1, 8, 26**] for much more information about this.

5.1. Vertex Covers and Phasor Measurement Unit (PMU) Placement

One problem in electrical engineering involves finding optimal placements of sensors (called "phasor measurement units" or "PMUs") in an electrical power system to monitor the substations and the transmission lines between the substations. Effective placement of PMUs in a system ensure the secure operation of the power system, and optimal placement helps reduce the cost of running the system. The problem of finding the smallest number of PMUs needed to monitor the entire system (and the placements of the PMUs) is the "PMU Placement Problem". Techniques to attack this optimization problem (which has been shown to be NP-complete) include integer linear programming, genetic algorithms, Gröbner bases, and graph theory.

In this section, we discuss how this problem relates to one that we have already seen: the problem of finding minimal vertex covers of graphs. (Recall from Section 4.3 that these were the keys to finding m-irreducible decompositions of edge ideals.) We begin with some basic notions from electrical engineering.

Definition 5.1.1. In an electrical power system, a *bus* is a substation where *transmission lines* meet. (The term "transmission line" is frequently shortened to "line".) Each line connects two buses.

In practice, electrical power systems are represented by diagrams of varying complexity, depending on how much information about the systems is being tracked. Here we are only interested in illustrating the buses and lines, so we model the systems with graphs where the vertices represent buses and the edges represent transmission lines. For instance, the next graph

$$\begin{tikzcd} v_1 \arrow[r, dash] \arrow[d, dash] \arrow[dr, dash] & v_2 \arrow[d, dash] \\ v_4 \arrow[r, dash] & v_3 \end{tikzcd}$$

represents a power system with four buses and five lines.

In the next definition, the term "phasor measurement unit" indicates that each PMU is a unit or device that tracks the voltage phasor (magnitude and phase) at a bus and similarly for the current phasor in the lines.

DEFINITION 5.1.2. In an electrical power system, a *phasor measurement unit* or *PMU* is a device placed at a bus to monitor the voltage at the bus and the current in all lines that connect to that bus. A *PMU placement* is a set of buses where PMUs are placed.

A bus in the system is *observable* if its voltage is known, e.g., by the placement of one or more PMUs. The power system is *observable* if every bus is observable.

The placement of a PMU at a bus makes that bus observable; it also makes every bus adjacent to that one observable because the PMU monitors the current between the two buses. For example, in the power system represented by the graph above, a PMU placed at the bus v_1 observes itself and every other bus in the system. On the other hand, a PMU placed at the bus v_2 observes all buses except v_4. This is illustrated in the following diagrams where observable buses are in boxes, buses with PMUs are labeled "PMU", and other observable buses and observable lines are labeled "obs".

Thus, given a PMU placement Π, the power system is observable if and only if each bus either has a PMU or is adjacent to a bus with a PMU. In other words, if the power system is represented as a graph G, then Π makes the power system observable if and only if Π is a vertex cover of G. This explains the first term in the next definition.

DEFINITION 5.1.3. A *PMU cover* of an electrical power system is a PMU placement that observes the entire system. A PMU cover is *minimum* if it has the smallest size among all PMU covers of the system.

It is important to note that the term "minimum PMU cover" is not synonymous with "minimal vertex cover". Indeed, as we have seen, a given graph can have minimal vertex covers of different size. The graph we have been considering has this property: the sets $\{v_1\}$ and $\{v_2, v_4\}$ are minimal vertex covers of different size. Thus, the first one represents a minimum PMU cover: the system requires at least one PMU to be observable, and this PMU cover has exactly one PMU. However, the second vertex cover does not represent a minimum PMU cover because it has more that one PMU. One reason for this difference in terminology is the expense involved in placing PMUs at buses. Engineers are interested in minimizing the cost of observing the system, by minimizing the number of PMUs.

This difference relates to an important concept in algebra, which we discuss next.

DEFINITION 5.1.4. Let R be a commutative ring with identity.

An ideal $I \subseteq R$ is *prime* if $I \neq R$ and the compliment $R \smallsetminus I$ is closed under multiplication, i.e., for all $a, b \in R$ if $ab \in I$, then either $a \in I$ or $b \in I$.

The *Krull dimension*, denoted $\dim(R)$, is the supremum of the lengths of chains of prime ideals in R. In symbols, we have

$$\dim(R) = \sup\{n \geqslant 0 \mid \text{there is a chain of prime ideals } \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n \text{ in } R\}.$$

The term "Krull dimension" is frequently shortened to "dimension".

For instance, if A is a field, then the dimension of the polynomial ring $R = A[X_1, \ldots, X_d]$ is exactly d; the inequality $\dim(R) \geqslant n$ is straightforward to verify because of the chain of prime ideals

$$0 \subsetneq (X_1)R \subsetneq (X_1, X_2)R \subsetneq \cdots \subsetneq (X_1, \ldots, X_d)R$$

but the reverse inequality takes more work. It is worth noting that the Krull dimension of a ring need not be finite, hence the supremum in the definition. However, if there is a bound on the lengths of the chains of prime ideals in the ring, then the supremum is the same as the maximum.

The dimension of a ring R is an important measure of its size. While the definition is purely algebraic, it has significant geometric content. For instance, the polynomial ring $\mathbb{R}[X]$ in one variable, which has Krull dimension 1, represents the real line (the X-axis, if you like), which is a 1-dimensional geometric object. Similarly, the polynomial ring $\mathbb{R}[X, Y]$ in two variables has Krull dimension 2 and represents the XY-plane, which is a 2-dimensional geometric object. It turns out that the quotient ring $\mathbb{R}[X, Y]/(Y - X^2)$ has Krull dimension 1 and represents the parabola $Y = X^2$, a 1-dimensional geometric object.

The connection between Krull dimension and minimum PMU covers is in the following theorem. It says that, if the graph G represents a power system with d buses, and n is the size of a minimum PMU cover, then $\dim(R/I_G) = d - n$. (See Section B.7 for background on ideal quotients like R/I_G.)

THEOREM 5.1.5. *Let G be a graph with vertex set $V = \{v_1, \ldots, v_d\}$. Let A be a field, and set $R = A[X_1, \ldots, X_d]$. If n is the size of the smallest vertex cover of G, then* $\dim(R/I_G) = d - n$.

SKETCH OF PROOF. Let V' be a vertex cover of G such that $|V'| = n$. Relabel the vertices if necessary to assume that $V' = \{v_1, \ldots, v_n\}$. Since A is a field, the ideal $P_{V'} = (X_1, \ldots, X_n)R \subset R$ is prime and contains the edge ideal I_G. Thus, it corresponds to a prime ideal in the quotient ring R/I_G. Similarly, the following chain of prime ideals of length $d - n$

$$(X_1, \ldots, X_n)R \subsetneq (X_1, \ldots, X_n, X_{n+1})R \subsetneq \cdots \subsetneq (X_1, \ldots, X_n, \ldots, X_d)R$$

corresponds to a chain $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{d-n}$ of prime ideals in R/I_G. This explains the inequality $\dim(R/I_G) \geqslant d - n$.

The reverse inequality requires techniques beyond the scope of this text, but here is the idea. Suppose by way of contradiction that there were a chain of prime ideals in R/I_G of length $d - n + 1$. This would imply the existence of an ideal $(X_{i_1}, \ldots, X_{i_{n-1}})R$ in R that contains I_G. Lemma 4.3.7 implies that the set $\{v_{i_1}, \ldots, v_{i_{n-1}}\} \subset V$ is a vertex cover of G of size $n-1$, contradicting the minimality of n. $\square$

Arguing similarly, one can show that if A is a field and Δ is a simplicial complex on a vertex set of size d, then $\dim(A[X_1, \ldots, X_d]/J_\Delta) = \dim(\Delta) + 1$.

As we mention above, a question in electrical engineering asks, given a power system, how to find a minimum PMU cover for it? Engineers have applied many mathematical techniques to answering this question. For instance, considering the problem from a graph-theoretical standpoint, Brueni and Heath [**3**] prove the following result. Note that $\lfloor d/3 \rfloor$ is the "floor" or "round-down" of $d/3$.

THEOREM 5.1.6 ([**3**, Theorem 6]). *Given an electrical power system G with $d \geqslant 3$ buses, there is a PMU cover Π of G such that $|\Pi| \leqslant \lfloor d/3 \rfloor$.*

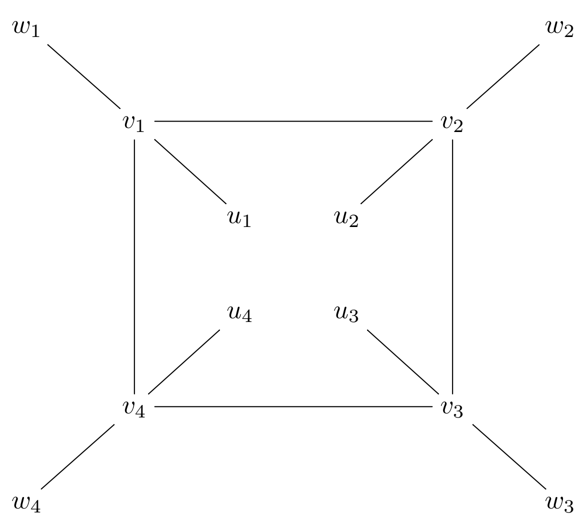
The proof of this theorem is quite technical, so we omit it here. However, we note the following surprising algebraic consequence.

COROLLARY 5.1.7. *Let G be a graph with vertex set $V = \{v_1, \dots, v_d\}$ such that $d \geqslant 3$. Let A be a field, and set $R = A[X_1, \dots, X_d]$. Then one has* $\dim(R/I_G) \geqslant d - \lfloor d/3 \rfloor = \lceil 2d/3 \rceil$.

PROOF. Let n be the size of the smallest vertex cover of G. Theorem 5.1.6 implies that $n \leqslant \lfloor d/3 \rfloor$, so we conclude from Theorem 5.1.5 that $\dim(R/I_G) = d - n \geqslant d - \lfloor d/3 \rfloor = \lceil 2d/3 \rceil$, as desired. $\square$

Brueni and Heath [**3**] also use the following example to show that the bound in Theorem 5.1.6 is sharp.

EXAMPLE 5.1.8 ([**3**, special case of Theorem 7]). Fix an integer $\ell \geqslant 3$. We build a graph G_ℓ with 3ℓ vertices such that each minimum PMU cover Π of G has $|\Pi| = \ell = \lfloor 3\ell/3 \rfloor$. Start with the ℓ-cycle C_ℓ with vertex set $\{v_1, \dots, v_\ell\}$. For $i = 1, \dots, \ell$ add two vertices u_i and w_i, and add edges $u_i v_i$ and $v_i w_i$. In [**3**], the resulting graph is denoted $B_{\ell,2}$. For the sake of simplicity and to avoid confusion with the complete bipartite graph also denoted $B_{\ell,2}$, we denote this new graph G_ℓ. For instance, the graph G_4 is sketched next.



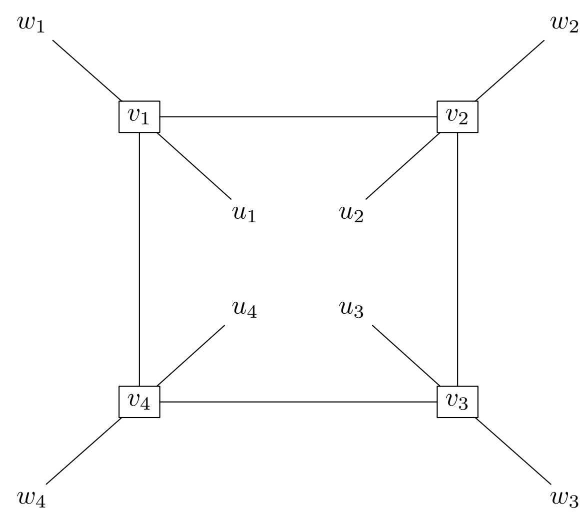
Technically, the graph G_ℓ has vertex set

$$V = \{v_1, \dots, v_\ell, u_1, \dots, u_\ell, w_1, \dots, w_\ell\}$$

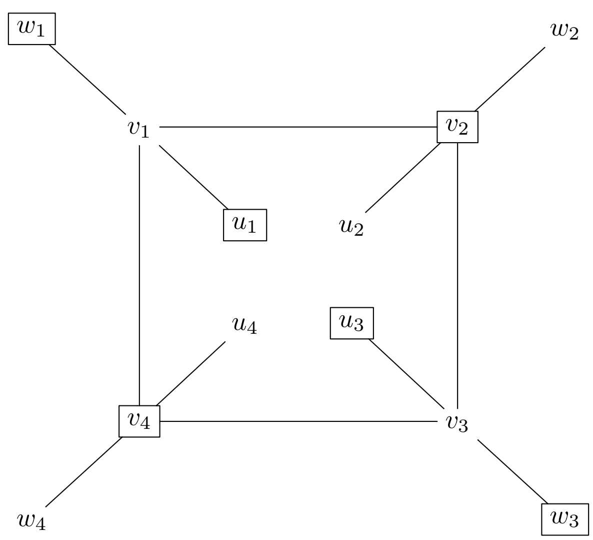
and edge set

$$E = \{u_1 v_1, \dots, u_\ell v_\ell, v_1 w_1, \dots, v_\ell w_\ell\} \cup \{v_1 v_2, v_2 v_3, \dots, v_{\ell-1} v_\ell, v_\ell v_1\}.$$

In particular, G_ℓ has 3ℓ vertices. The set $V' = \{v_1, \ldots, v_\ell\}$ is a minimum PMU cover of G_ℓ with size $\ell = 3\ell/3 = d/3 = \lfloor d/3 \rfloor$. (This takes some work to show.) For instance, the case $\ell = 4$ is illustrated next.



Note that G_ℓ has minimal vertex covers that have more than ℓ elements. For instance, here is one for the case $\ell = 4$.



See Exercise 5.1.10 for more about G_ℓ.

Exercises.

EXERCISE 5.1.9. Let G be a graph with vertex set $V = \{v_1, \ldots, v_d\}$ where $d \leqslant 2$. Find all minimum PMU covers of G. Justify your answer.

EXERCISE 5.1.10. Fix and integer $\ell \geqslant 3$, and consider the graph G_ℓ from Example 5.1.8.

(a) Prove that $V' = \{v_1, \ldots, v_\ell\}$ is the unique minimum PMU cover of G_ℓ.

(b) Find all minimal vertex covers of G_ℓ. Show that G_ℓ has minimal vertex covers of size $m > \ell$.
(c) Write out an irredundant monomial generating sequence and an irredundant m-irreducible decomposition for I_{G_ℓ}.

Justify your answers.

Exercise 5.1.11. The graph G_ℓ from Example 5.1.8 has vertex set of size $d = 3\ell \geqslant 9$. Are there connected graphs with $d = 3, 4, \ldots, 8$ such that the bound in Theorem 5.1.6 is sharp? (A graph G is *connected* if, for all distinct vertices v_i and v_j, there is a path of edges in G from v_i to v_j.) Justify your answer.

Vertex Covers and Phasor Measurement Unit (PMU) Placement in Macaulay2.

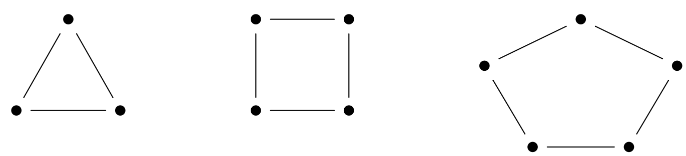
Exercises.

5.2. Cohen-Macaulayness and the Upper Bound Theorem

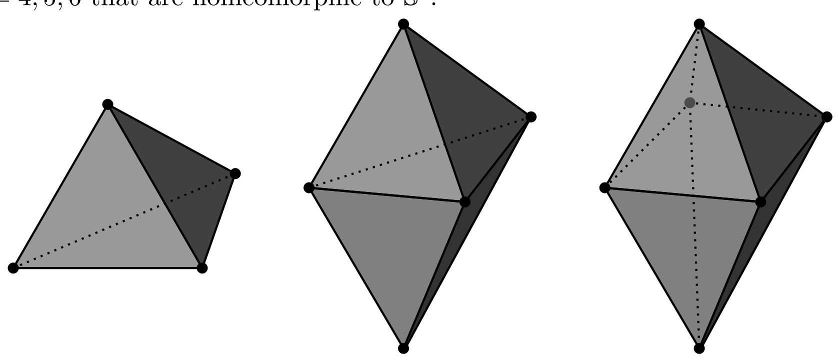
In this section, we discuss a powerful application of monomial ideals to topology. (For basic notions from topology, we refer the reader to any standard textbook, e.g., Munkres [**33**].) To get started, we need the following definition.

Definition 5.2.1. A *simplicial sphere* is a a simplicial complex whose geometric realization is homeomorphic to a sphere $\mathbb{S}^{n-1}$ in $\mathbb{R}^n$.

For instance, the d-cycle C_d (illustrated here for $d = 3, 4, 5$)



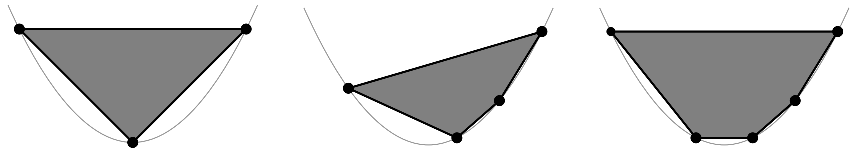
is a simplicial sphere with $n = 2$. With $n = 3$, here are sketches of examples with $d = 4, 5, 6$ that are homeomorphic to $\mathbb{S}^2$.



To state the Upper Bound Conjecture (UBC) for simplicial spheres, we need the next definition.

Definition 5.2.2. Let n and d be positive integers such that $d > n$, and consider the curve $X_n := \{(t, t^2, t^3, \ldots, t^n) \mid t \in \mathbb{R}\}$ in $\mathbb{R}^n$. Choose d distinct points in X_n and let $C(d, n)$ denote the convex hull of these points.

For example, the curve X_2 is the parabola $y = x^2$ in $\mathbb{R}^2$. Some examples of $C(d, 2)$ for $d = 3, 4, 5$ are sketched next.



In general, the object $C(d,n)$ is homeomorphic to an n-dimensional ball in $\mathbb{R}^n$, and its boundary $\Delta(d,n) := \partial C(d,n)$ is homeomorphic to $\mathbb{S}^{n-1}$. (This depends on the condition $d > n$.) Moreover, $C(d,n)$ and $\Delta(d,n)$ are geometric realizations of simplicial complexes, which we also denote $C(d,n)$ and $\Delta(d,n)$. These simplicial complexes are independent of the choice of points in X_n, only depending on d and n, up to re-labeling the vertices. This allows us to state the following:

Conjecture 5.2.3 (UBC for simplicial spheres). Let Δ be a simplicial complex on a set of d vertices whose geometric realization is homeomorphic to a sphere $\mathbb{S}^{n-1}$ in $\mathbb{R}^n$. Then we have $f_i(\Delta) \leqslant f_i(C(d,n))$ for $i = 0, \ldots, n-1$.

Motzkin [**32**] first formulated this conjecture for the special case of convex simplicial polytopes, and it was proved in this case by McMullen [**27**]. The general form stated here was formulated by Klee and proved by Stanley [**38**] using the notion of "Cohen-Macaulayness" from commutative algebra (via monomial ideals) which we outline next.

To motivate the following definition, let $R = A[X_1, \ldots, X_d]$ for some non-zero commutative ring A with identity. Every square-free monomial ideal $J \subsetneq R$ has an irredundant m-irreducible decomposition $J = \bigcap_{i=1}^p P_{V_i}$ by Proposition 4.3.3 and Algorithm 3.3.5. Also, Theorem 3.3.8 implies that this decomposition is unique up to re-ordering the V_i's. In particular, the list of V_i's is unique up to re-ordering. We have seen several examples where all the V_i's all have the same size, and other examples show that the V_i's can have different sizes. In the first of these cases, J is nicer than in the other case, and we identify this with the following definition.

Definition 5.2.4. Let A be a non-zero commutative ring with identity, and set $R = A[X_1, \ldots, X_d]$. Consider a monomial ideal $J \subsetneq R$ with irredundant m-irreducible decomposition $J = \bigcap_{i=1}^p Q_i$. For $i = 1, \ldots, p$ we have $\text{m-rad}\,(Q_i) = P_{V_i}$ for some set $V_i \subseteq \{v_1, \ldots, v_d\}$. Then J is *m-unmixed* if $|V_i| = |V_j|$ for all $i \neq j$. We say that J is *m-mixed* if it is not m-unmixed, that is, if there are indices $i \neq j$ such that $|V_i| \neq |V_j|$.

For instance, the ideal I_G from Example 4.3.9 is m-mixed, as is the ideal J from Example 4.3.10. On the other hand, the ideal from Example 4.5.7 is m-unmixed. For a graph G, Theorem 4.3.8 tells us that the edge ideal I_G is m-unmixed if and only if every minimal vertex cover of G has the same cardinality. (In the language of Section 5.1, this means that every minimal vertex cover of G is a minimum PMU cover of the associated electrical power system.) For a simplicial complex Δ, Theorem 4.6.5 tells us that the face ideal J_Δ is m-unmixed if and only if it is pure; see Definition 4.4.5.

The notion of Cohen-Macaulayness is a souped-up version of unmixedness; see Theorem 5.2.15(a). Outside of commutative algebra, it is incredibly important in areas like algebraic geometry that heavily rely on techniques from commutative algebra. One outcome of Stanley's proof of the UBC for simplicial spheres is that this notion has also become important in topology and combinatorics.

DEFINITION 5.2.5. Let R be a non-zero commutative ring with identity, and let $g \in R$. Then g is *R-regular* if the map $R \xrightarrow{g} R$ given by $p \mapsto gp$ is 1-1 and not onto. More generally, given an ideal $I \subsetneq R$, the element $g \in R$ is *regular for R/I* if the map $R/I \xrightarrow{g} R/I$ given by $p + I \mapsto (gp) + I$ is 1-1 and not onto.

For instance, if $R = A[X_1, \ldots, X_d]$ where A is a field and g is a non-constant polynomial in R, then g is R-regular. (More generally, if R is an integral domain and g is a non-zero non-unit of R, then g is R-regular.) Here is another example for later use.

EXAMPLE 5.2.6. Let A be a field, set $R = A[X_1, X_2, X_3]$, and consider the ideal $I = (X_1X_2X_3)R$. The element X_1 is not regular for R/I because we have $0 + I = 0 \neq X_2X_3 + I \in R/I$ and $X_1 \cdot 0 + I = 0 = X_1 \cdot X_2X_3 + I \in R/I$. On the other hand, the element $X_3 - X_2$ is regular on R/I. To see this, let $p, q \in R$ such that $(X_3 - X_2)p + I = (X_3 - X_2)q + I$ in R/I. We need to show that $p + I = q + I$ in R/I. The condition $(X_3 - X_2)p + I = (X_3 - X_2)q + I$ implies that $(X_3 - X_2)(p - q) \in I = (X_1X_2X_3)R$. From the unique factorization property in R (this uses the assumption that A is a field) it follows that $p - q \in (X_1X_2X_3)R = I$, so we have $p + I = q + I$ in R/I, as desired.

For future reference, note that modding out by $X_3 - X_2$ is tantamount to setting X_3 equal to X_2. Thus, we have

$$R/(I + (X_3 - X_2)R) = A[X_1, X_2, X_3]/(X_1X_2X_3, X_3 - X_2)R \cong A[X_1, X_2]/(X_1X_2^2).$$

Similar reasoning as above shows that $X_2 - X_1$ is regular for $R/(I + (X_3 - X_2)R)$ and that we have

$$R/((I + (X_3 - X_2)R) + (X_2 - X_1)R) \cong A[X_1, X_2]/(X_1X_2^2, X_2 - X_1) \cong A[X_1]/(X_1^3).$$

Regular elements for R are important in commutative algebra because they allow for effective transmission of certain important properties between R and $R/(g)R$. Geometrically, if g is regular for R/I, then the intersection between the zero-locus of g and the zero-locus of I (in A^d) is sufficiently nice as to allow similar transfer between the zero-loci of I and $I + (g)R$. A hint of this can be seen in the following result which says that modding out by a regular element causes the Krull dimension to drop by exactly 1.

FACT 5.2.7. Let A be a field, and set $R = A[X_1, \ldots, X_d]$. Consider an ideal $I \subsetneq R$ generated by homogeneous polynomials, and let g be a non-constant homogeneous polynomial in R that is regular for R/I. Then $\dim(R/(I + (g)R)) = \dim(R/I) - 1$.

EXAMPLE 5.2.8. Continue with the notation of Example 5.2.6. Since A is a field, the ring $R = A[X_1, X_2, X_3]$ has Krull dimension 3. According to the paragraph preceding Example 5.2.6, the element $X_1X_2X_3$ is R-regular, so $\dim(R/I) = 2$, by Fact 5.2.7. Similarly, the ring $R/(I + (X_3 - X_2)R) \cong A[X_1, X_2]/(X_1X_2^2)$ has Krull dimension 1, and the ring $R/((I + (X_3 - X_2)R) + (X_2 - X_1)R) \cong A[X_1]/(X_1^3)$ has Krull dimension 0.

The following extension of regularity to sequences with more than one element is key to defining the Cohen-Macaulay property.

DEFINITION 5.2.9. Let A be a field, and set $R = A[X_1, \ldots, X_d]$. Consider an ideal $I \subsetneq R$. Then a sequence $g_1, \ldots, g_m \in R$ is *regular for R/I* if it satisfies the following conditions:

(1) the polynomial g_1 is regular for R/I, and
(2) for $i = 2, \ldots, m$ the polynomial g_i is regular for $R/(I + (g_1, \ldots, g_{i-1})R)$.

EXAMPLE 5.2.10. From Example 5.2.8, the sequence $X_3 - X_2, X_2 - X_1$ is regular for $A[X_1, X_2, X_3]/(X_1X_2X_3)R$.

An important consequence of Fact 5.2.7 is the following.

LEMMA 5.2.11. *Let A be a field, and set $R = A[X_1, \ldots, X_d]$. Consider an ideal $I \subsetneq R$ generated by homogeneous polynomials, and let $g_1, \ldots, g_m$ be non-constant homogeneous polynomials in R. If this sequence is regular for R/I, then $m \leqslant \dim(R/I)$.*

PROOF. Exercise. $\square$

We are finally prepared to define the Cohen-Macaulay property.

DEFINITION 5.2.12. Let A be a field, and set $R = A[X_1, \ldots, X_d]$. Consider an ideal $I \subsetneq R$ generated by homogeneous polynomials. The quotient R/I is *Cohen-Macaulay* if it has a homogeneous regular sequence $g_1, \ldots, g_m$ such that $m = \dim(R/I)$.

EXAMPLE 5.2.13. When A is a field, the quotient $A[X_1, X_2, X_3]/(X_1X_2X_3)R$ is Cohen-Macaulay, by Examples 5.2.8 and 5.2.10.

Before we return to the UBC for simplicial spheres, we need to discuss how the notion of Cohen-Macaulayness applies to simplicial complexes.

DEFINITION 5.2.14. Let A be a field, and set $R = A[X_1, \ldots, X_d]$. A simplicial complex Δ with vertex set $\{v_1, \ldots, v_d\}$ is *Cohen-Macaulay* over A if the quotient R/J_Δ is Cohen-Macaulay. A graph G with vertex set $\{v_1, \ldots, v_d\}$ is *Cohen-Macaulay* over A if the quotient R/I_G is Cohen-Macaulay.

In general, a simplicial complex Δ is *Cohen-Macaulay* if it is Cohen-Macaulay over every field A. A graph G with vertex set $\{v_1, \ldots, v_d\}$ is *Cohen-Macaulay* if it is Cohen-Macaulay over every field A.

For instance, Example 5.2.13 shows that the shaded triangle Δ on three vertices is Cohen-Macaulay because we have $R/J_\Delta = A[X_1, X_2, X_3]/(X_1X_2X_3)R$.

The next result contains an important test for Cohen-Macaulayness. The proof of part (a) is beyond the scope of this text. However, we show how it implies parts (b) and (c). It is worth noting that the hypotheses of parts (b) and (c) are independent of the field A; it follows that the conclusions of these parts are also independent of the choice of A.

THEOREM 5.2.15. *Let A be a field, and set $R = A[X_1, \ldots, X_d]$.*
(a) *Let I is a square-free monomial ideal in R. If R/I is Cohen-Macaulay, then I is m-unmixed.*
(b) *Let Δ be a simplicial complex with vertex set $\{v_1, \ldots, v_d\}$. If Δ is not pure, then it is not Cohen-Macaulay over A.*
(c) *Let G be a graph with vertex set $\{v_1, \ldots, v_d\}$. If G has minimal vertex covers of different sizes, then G is not Cohen-Macaulay A.*

PROOF. (b) We prove the contrapositive. Assume that Δ is Cohen-Macaulay over A. Part (a) implies that J_Δ is m-unmixed, so Theorem 4.6.5 tells us that Δ is pure; see also the discussion following Definition 5.2.4.

(c) This follows like part (b), using Theorem 4.3.8. $\square$

Finally, we are in position to sketch sketch Stanley's proof of the UBC for simplicial spheres, now known as the "Upper Bound Theorem".

THEOREM 5.2.16. *The Upper Bound Conjecture for simplicial spheres holds.*

SKETCH OF PROOF. Stanley shows that a result of Munkres [**34**] implies that simplicial spheres are Cohen-Macaulay. He uses this, with a result of McMullen [**27**] to show that the desired bounds from Conjecture 5.2.3 hold. For more details, see [**4, 38, 39**]. □

Exercises.

EXERCISE 5.2.17. Let R be a non-zero commutative ring with identity.

(a) Prove that an element $g \in R$ is R-regular if and only if g is a non-unit in R such that $(0 :_R g) = 0$.
(b) Fix an ideal $I \subsetneq R$. Prove that an element $g \in R$ is regular for R/I if and only if $I + (g)R \neq R$ and $(I :_R g) = I$.

EXERCISE 5.2.18. Prove Lemma 5.2.11. (Hint: Use Fact 5.2.7.)

EXERCISE 5.2.19. Let A be a field. Prove that $A[X_1, \ldots, X_d]/(X_1 \cdots X_d)$ is Cohen-Macaulay. Conclude that the "d-simplex" Δ_d, defined to be the power set $\mathsf{P}(\{v_1, \ldots, v_d\})$, is Cohen-Macaulay over A. (Note that this is the simplest case of Stanley's observation that simplicial spheres are Cohen-Macaulay.)

EXERCISE 5.2.20. Decide whether the simplicial complexes from Example 4.4.2 and Exercise 4.5.13 are Cohen Macaulay. Do the same for the simplicial complexes following Definitions 5.2.1 and 5.2.2.

Cohen-Macaulayness and the Upper Bound Theorem in Macaulay2.

Exercises.

5.3. Hilbert Functions and Initial Ideals

In this section, A is a field

One of the amazing things about monomial ideals is that they have the power to give us information about other ideals. In short, given an ideal I generated by homogeneous polynomials over A, one can find a monomial ideal $\mathrm{in}(I)$ in the polynomial ring R with many of the same properties as I. The ideal $\mathrm{in}(I)$ is called the "initial ideal" of I. It depends on the choice of an ordering on the set of monomials $[\![R]\!]$, so in fact there are potentially several monomial ideals with this property. In principle, this allows one to transfer problems for arbitrary ideals in R, which can be quite messy, to similar problems for monomial ideals. One can then apply, e.g., combinatorial techniques to the monomial ideal in addition to purely algebraic techniques, as we have already seen.

In this section, we focus on the "Hilbert function" of R/I, which is the same as that of $R/\in I$; see Theorem 5.3.8. Hilbert functions are another extremely important tool in commutative algebra and algebraic geometry. For instance, they are crucial for Stanley's proof of the UBC outlined in Section 5.2. However, our treatment here only scratches the surface. It is also worth noting that the ideas in this section form the stating point for the study of "Gröbner bases" which have applications in many areas including, surprisingly, the study of electrical power systems; see Kavasseri and Nag [**23**].

DEFINITION 5.3.1. Set $R = A[X_1, \ldots, X_d]$, and consider an ideal $I \subsetneq R$ generated by homogeneous polynomials. For each $i \in \mathbb{N}$, we consider the finite-dimensional A-vector space

$$(R/I)_i = \{f + I \in R/I \mid f \in R \text{ is homogeneous of degree } i\} \cup \{0 + I\}$$

and its vector space dimension

$$h_{R/I}(i) = \dim_A((R/I)_i).$$

The function $h_{R/I} \colon \mathbb{N} \to \mathbb{N}$ is the *Hilbert function* of R/I.

It is worth noting that the fact that there are only finitely many monomials of a fixed degree i in $A[X_1, \ldots, X_d]$ implies that $\dim_A((R/I)_i) < \infty$.

One reason for the importance of Hilbert functions comes from the following result of Hilbert which shows that these functions encode surprising algebraic and geometric data.

THEOREM 5.3.2. *Set $R = A[X_1, \ldots, X_d]$, and consider an ideal $I \subsetneq R$ generated by homogeneous polynomials. There is a polynomial $p_{R/I}$ in one variable over $\mathbb{Q}$ such that $h_{R/I}(i) = p_{R/I}(i)$ for $i \gg 0$. Moreover, $p_{R/I}$ has degree equal to $\dim(R/I) - 1$ and is of the form*

$$p_{R/I}(i) = \frac{e(R/I)}{(\dim(R/I) - 1)!} i^{\dim(R/I)-1} + \textit{lower degree terms}$$

where $e(R/I)$ is a positive integer. Here $\dim(R/I)$ is the Krull dimension of R/I. In the case $\dim(R/I) = 0$, the degree of $p_{R/I}$ is -1, which we interpret as $p_{R/I} = 0$.

DEFINITION 5.3.3. Set $R = A[X_1, \ldots, X_d]$, and consider an ideal $I \subsetneq R$ generated by homogeneous polynomials. The polynomial $p_{R/I}$ from Theorem 5.3.2 is the *Hilbert polynomial* of R/I. When $\dim(R/I) \geqslant 1$, the integer $e(R/I)$ is the *multiplicity* of R/I.

Section 1.5 contains an exploration of the case where $I = 0$, where one shows the first step in the following sequence.

$$\begin{aligned} h_{R/0}(i) &= \binom{i+d-1}{d-1} \\ &= \frac{(i+d-1)!}{(d-1)!i!} \\ &= \frac{(i+d-1)(i+d-2)\cdots(i+1)}{(d-1)!} \\ &= \frac{1}{(d-1)!} i^{d-1} + \text{lower degree terms} \end{aligned}$$

Thus, Theorem 5.3.2 gives another method for verifying that R has Krull dimension d, and we see that the multiplicity of R is 1.

As we have already remarked, the Krull dimension of R/I is a measure of the size of R/I. Similarly, the multiplicity of R/I is a measure of the complexity of R/I. For instance, given a simplicial complex Δ, the multiplicity of R/J_Δ equals the number of facets of Δ that have maximal dimension. Similarly, given a graph G, the multiplicity of R/I_G equals the number of minimal vertex covers of G of minimal size, i.e., the number of minimum PMU covers of G.

The previous paragraph indicates how some information about the Hilbert polynomial $p_{R/I}$ can be obtained combinatorially in the case where I is a square-free monomial ideal. (This is due to the fact such and ideal I is of the form J_Δ, by Remark 4.5.6.) The next result shows that, in fact, the entire Hilbert function can be gotten from combinatorial data in this case.

THEOREM 5.3.4. *Let Δ be a simplicial complex of dimension n on a vertex set of size d, and assume that each singleton $\{v_i\}$ is in Δ. Set $R = A[X_1, \ldots, X_d]$.. Then we have*

$$h_{R/J_\Delta}(i) = \begin{cases} 1 & \text{if } i = 0 \\ \sum_{j=0}^{n} f_j(\Delta)\binom{i-1}{j} & \text{if } i \geqslant 1 \end{cases}$$

For instance, if Δ is the 3-cycle C_3, then we have $f(\Delta) = (3, 3)$ and $n = 1$. Theorem 5.3.4 tells us that for $i \geqslant 1$ we have the following.

$$h_{R/J_\Delta}(i) = \sum_{j=0}^{n} f_j(\Delta)\binom{i-1}{j} = 3\binom{i-1}{0} + 3\binom{i-1}{1} = 3(1) + 3(i-1) = 3i$$

Note that we can see that the Hilbert polynomial of R/J_Δ is $p_{R/J_\Delta}(i) = 3i$ and that we have $p_{R/J_\Delta}(i) = h_{R/J_\Delta}(i)$ for all $i \geqslant 1$. This has the form predicted by Theorem 5.3.2 since

(1) the degree of $p_{R/J_\Delta}(i)$ is $\dim(R/J_\Delta) - 1 = \dim(\Delta) = 1$, by the discussion following Theorem 5.1.5, and
(2) the leading coefficient of p_{R/J_Δ} is $\frac{e(R/J_\Delta)}{(\dim(R/J_\Delta)-1)!} = \frac{3}{0!} = \frac{3}{1} = 3$, by the discussion following Definition 5.3.3.

In order to describe how monomial ideals can give information about Hilbert functions for non-monomial ideals, we need to describe how one transforms a general ideal I in a polynomial ring into the monomial ideal $\mathrm{in}(I)$. The first step is to specify an ordering on the monomials with certain properties.

DEFINITION 5.3.5. Set $R = A[X_1, \ldots, X_d]$. A *monomial order* on the set $[\![R]\!]$ of monomials of R is a total order $\leqslant$ on $[\![R]\!]$ satisfying the following conditions.

(1) For every $f \in [\![R]\!]$, we have $1 \geqslant f$.
(2) For all $f, g, h \in [\![R]\!]$, if $f \leqslant g$, then $fh \leqslant gh$.

As usual, we write $f < g$ when $f \leqslant g$ and $f \neq g$.

Note that the divisibility order (given by $f \leqslant g$ if and only if g divides f) is not a monomial order, unless $d = 1$, since it is not a total order. We have already seen a special case of an important example of a monomial order, in Section 6.4, in the special case $d = 2$: the lexicographical order. (The general case is treated briefly in Exercise 6.4.11.) Again, the terminology comes from the fact that it is modeled on the ordering of words in a dictionary. We describe this in general and a related order next.

DEFINITION 5.3.6. Set $R = A[X_1, \ldots, X_d]$, and fix monomials $\underline{X}^{\underline{m}}, \underline{X}^{\underline{n}} \in [\![R]\!]$.

(1) Write $\underline{X}^{\underline{m}} <_{\mathrm{lex}} \underline{X}^{\underline{n}}$ when, for some i, we have $m_j = n_j$ for $j = 1, \ldots, i$ and $m_{i+1} < n_{i+1}$. This is the *lexicographical order* on $[\![R]\!]$ (or *lex order*).
(2) Write $\underline{X}^{\underline{m}} <_{\mathrm{revlex}} \underline{X}^{\underline{n}}$ when, for some i, we have $m_j = n_j$ for $j = 1, \ldots, i$ and $m_{i+1} > n_{i+1}$. This is the *reverse lexicographical order* on $[\![R]\!]$ (or *revlex order*).

For example, when $d = 3$, we have $X_1^2X_2^3X_3^6 <_{\text{lex}} X_1^2X_2^4X_3^2$, and we have $X_1^2X_2^4X_3^2 <_{\text{revlex}} X_1^2X_2^3X_3^6$.

The idea behind constructing the initial ideal of an ideal I is to throw away all but the "leading terms" of the elements of I, as described next.

DEFINITION 5.3.7. Set $R = A[X_1, \ldots, X_d]$, and fix a monomial order $\leqslant$ on $[\![R]\!]$.

For each non-zero polynomial $f \in R$, write $f = \sum_{i=1}^p a_i\underline{X}^{\underline{n}_i}$ where we have $0 \neq a_i \in A$ and $\underline{n}_i \in \mathbb{N}^d$ such that $\underline{X}^{\underline{n}_1} < \cdots < \underline{X}^{\underline{n}_p}$. The *leading term* of f is $\mathrm{lt}(f) := \underline{X}^{\underline{n}_p}$.

Let I be a non-zero ideal of R. The *initial ideal* of I with respect to $<$ is the monomial ideal generated by the leading terms of the non-zero polynomials in I:

$$\mathrm{in}_<(I) := (\mathrm{lt}_<(f) \mid 0 \neq f \in I)R.$$

Also, we set $\mathrm{in}_<(0) := 0$. Often, one writes $\mathrm{lt}(f)$ and $\mathrm{in}(I)$ when the order $<$ is understood.

For example, the leading term of a monomial f is just f itself. It follows that the initial ideal of a monomial ideal I is just I; see Exercise 5.3.12. In the polynomial $X^3 - Y^3$ in $R = A[X, Y]$, we have

$$\mathrm{lt}_{<_{\text{lex}}}(X^3 - Y^3) = X^3 \qquad\qquad \mathrm{lt}_{<_{\text{revlex}}}(X^3 - Y^3) = Y^3$$

because $Y^3 <_{\text{lex}} X^3$ and $X^3 <_{\text{revlex}} Y^3$. From this, one can show that

$$\mathrm{in}_{<_{\text{lex}}}((X^3 - Y^3)R) = (X^3)R \qquad \mathrm{in}_{<_{\text{revlex}}}((X^3 - Y^3)R) = (Y^3)R.$$

More generally, see Exercise 5.3.13. Do be careful, though, trying to use generators of an ideal to find generators of an initial ideal. If $I = (f_1, \ldots, f_m)R$, then one always has

$$\mathrm{in}_<(I) \supseteq (\mathrm{lt}_<(f_1), \ldots, \mathrm{lt}_<(f_m))R$$

but this containment may be strict; see Exercise 5.3.15.

The next result, due to Macaulay, is the one we have been building up to. It provides the connection between the Hilbert functions of homogeneous ideals and their initial ideals.

THEOREM 5.3.8. *Set $R = A[X_1, \ldots, X_d]$. Consider an ideal $I \subsetneq R$ generated by homogeneous polynomials, and fix a monomial order $<$. Then the rings R/I and $R/\mathrm{in}_<(I)$ have the same Hilbert functions, Hilbert polynomials, Krull dimensions, and multiplicities.*

For example, one can apply this to the ideal $I = (X^3 - Y^3)R$ where $R = A[X, Y]$. As we have seen, one has $\mathrm{in}_{<_{\text{lex}}}(I) = (X^3)R$ and $\mathrm{in}_{<_{\text{revlex}}}(I) = (Y^3)R$. In some ways, the Hilbert function of these initial ideals is simpler to compute than that of I itself:

$$h_{R/I}(i) = h_{R/\mathrm{in}(I)}(i) = \begin{cases} i+1 & \text{if } 0 \leqslant i \leqslant 2 \\ 3 & \text{if } i \geqslant 2. \end{cases}$$

Note that the example $J = (X^2 - Y^3)R$ shows that the homogeneous assumption in Theorem 5.3.8 is crucial since we have

$$\mathrm{in}_{<_{\text{lex}}}((X^2 - Y^3)R) = (X^2)R \qquad \mathrm{in}_{<_{\text{revlex}}}((X^3 - Y^3)R) = (Y^3)R$$

and these ideals do not have the same Hilbert functions.

Exercises.

EXERCISE 5.3.9. Set $R = A[X_1, \ldots, X_d]$, and let I be a monomial ideal of R.

(a) Prove that for $i = 0, 1, 2, \ldots$, the following set is a basis for $(R/I)_i$.
$$\{\underline{X}^{\underline{n}} + I \mid \underline{X}^{\underline{n}} \text{ is a monomial of degree } i \text{ in } R \smallsetminus I\}$$
It follows that $h_{R/I}(i) = |\{\underline{X}^{\underline{n}} \mid \underline{X}^{\underline{n}} \text{ is a monomial of degree } i \text{ in } R \smallsetminus I\}|$.

(b) Let $d = 1$. Fix a monomial $\underline{X}^{\underline{m}} \in [\![R]\!]$ of degree e, and set $I = (\underline{X}^{\underline{m}})R$. Show that
$$h_{R/I}(i) = \begin{cases} 1 & \text{if } 0 \leqslant i < e \\ 0 & \text{if } i \geqslant e. \end{cases}$$
Conclude that R/I has dimension e as a vector space over A.

(c) Let $d = 2$. Fix a monomial $\underline{X}^{\underline{m}} \in [\![R]\!]$ of degree e, and set $I = (\underline{X}^{\underline{m}})R$. Show that
$$h_{R/I}(i) = \begin{cases} i+1 & \text{if } 0 \leqslant i < e \\ e & \text{if } i \geqslant e. \end{cases}$$
Conclude that R/I has multiplicity e.

(d) Extend parts (b) and (c) to the case $d \geqslant 3$.

EXERCISE 5.3.10. Use Theorem 5.3.4 to compute the Hilbert function for R/J_δ where Δ is the simplicial complex from Example 4.4.2.

EXERCISE 5.3.11. Prove that $<_{\text{lex}}$ and $<_{\text{revlex}}$ are monomial orders for $R = A[X_1, \ldots, X_d]$.

EXERCISE 5.3.12. Set $R = A[X_1, \ldots, X_d]$ and let I be an ideal in R. Prove that I is a monomial ideal if and only if it is equal to all (equivalently, at least one) of its initial ideals.

EXERCISE 5.3.13. Set $R = A[X_1, \ldots, X_d]$, and fix a monomial order $<$ for R.

(a) Prove that for non-zero polynomials $f, g \in R$, we have $\mathrm{lt}_<(fg) = \mathrm{lt}_<(f)\,\mathrm{lt}_<(g)$.

(b) Let f be a non-zero polynomial in R, and prove that $\mathrm{in}_<((f)R) = (\mathrm{lt}_<(f))R$.

EXERCISE 5.3.14. Set $R = A[X, Y]$, and let f be a non-zero homogeneous polynomial in R of degree d. Use Theorem 5.3.8 and Exercise 5.3.9 to find the Hilbert function, Hilbert polynomial, and multiplicity of $R/(f)R$.

EXERCISE 5.3.15. Set $R = A[X, Y]$ and $I = (X^3 - Y^3, Y^3)R$.

(a) Prove that $(\mathrm{lt}_{<_{\text{lex}}}(X^3 - Y^3), \mathrm{lt}_{<_{\text{lex}}}(Y^3))R = (Y^3)R$.

(b) Prove that $X^3 \in \mathrm{in}_{<_{\text{lex}}}(I)$.

(c) Conclude that $\mathrm{in}_{<_{\text{lex}}}((X^3 - Y^3, Y^3)R) \supsetneq (\mathrm{lt}_{<_{\text{lex}}}(X^3 - Y^3), \mathrm{lt}_{<_{\text{lex}}}(Y^3))R$.

Hilbert Functions and Initial Ideals in Macaulay2.

Exercises.

5.4. Resolutions of Monomial Ideals

In this section, A is a field.

In this section, we explore some basic aspects of homological algebra as they relate to monomial ideals. The starting point in this area is the following: a list of polynomials $f_1, \ldots, f_n \in R = A[X_1, \ldots, X_d]$ with $m \geqslant 2$ can be linearly independent over A, but it will not be linearly independent over R. This is because we always have the commutativity relation $f_i f_j - f_j f_i = 0$. For an arbitrary list of polynomials, it is difficult to write down all such relations. However, for monomials, one can use combinatorial data to find all such relations with relative ease. The case $d = 1$ is easy since all monomials are of the form X_1^i, so we begin by discussing the case $d = 2$.

EXAMPLE 5.4.1. Set $R = A[X, Y]$, and let $I \subseteq R$ be a monomial ideal with irredundant monomial generating sequence $f_1, \ldots, f_n$. Assume that $n \geqslant 2$ and that $f_1 <_{\text{lex}} \cdots <_{\text{lex}} f_n$. Then we have $f_i = X^{a_i} Y^{b_i}$ such that $a_1 < \cdots < a_n$ and $b_1 > \cdots > b_n$. From this, one sees the relations

$$\begin{aligned} X^{a_{i+1}-a_i} f_i - Y^{b_i - b_{i+1}} f_{i+1} &= X^{a_{i+1}-a_i} X^{a_i} Y^{b_i} - Y^{b_i - b_{i+1}} X^{a_{i+1}} Y^{b_{i+1}} \\ &= X^{a_{i+1}} Y^{b_i} - X^{a_{i+1}} Y^{b_i} \\ &= 0. \end{aligned}$$

We can construct other relations from these in straightforward ways. For instance, for each $g \in R$, we have

$$(gX^{a_{i+1}-a_i}) f_i - (gY^{b_i - b_{i+1}}) f_{i+1} = g(X^{a_{i+1}-a_i} f_i - Y^{b_i - b_{i+1}} f_{i+1}) = 0.$$

More generally, for $g_1, \ldots, g_{n-1} \in R$ we have

$$\sum_{i=1}^{n-1} [(g_i X^{a_{i+1}-a_i}) f_i - (g_i Y^{b_i - b_{i+1}}) f_{i+1}] = \sum_{i=1}^{n-1} g_i (X^{a_{i+1}-a_i} f_i - Y^{b_i - b_{i+1}} f_{i+1}) = 0.$$

It is not difficult to show that these are the only relations possible between the f_i; see Exercise 5.4.7. For instance, for $i < j$, we have the relations

$$X^{a_j - a_i} f_i - Y^{b_i - b_j} f_j = X^{a_j - a_i} X^{a_i} Y^{b_i} - Y^{b_i - b_j} X^{a_j} Y^{b_{i+1}} = X^{a_j} Y^{b_i} - X^{a_j} Y^{b_i} = 0.$$

These can be re-written in the above form. For example, with $j = i + 2$ we have the following:

$$\begin{aligned} 0 &= X^{a_{i+2}-a_i} f_i - Y^{b_i - b_{i+2}} f_{i+2} \\ &= X^{a_{i+2}-a_i} X^{a_i} Y^{b_i} - Y^{b_i - b_{i+2}} X^{a_{i+2}} Y^{b_{i+2}} \\ &= X^{a_{i+2}-a_i} X^{a_i} Y^{b_i} - X^{a_{i+2}-a_{i+1}} Y^{b_i - b_{i+1}} X^{a_{i+1}} Y^{b_{i+1}} \\ &\quad + X^{a_{i+2}-a_{i+1}} Y^{b_i - b_{i+1}} X^{a_{i+1}} Y^{b_{i+1}} - Y^{b_i - b_{i+2}} X^{a_{i+2}} Y^{b_{i+2}} \\ &= X^{a_{i+2}-a_{i+1}} X^{a_{i+1}-a_i} X^{a_i} Y^{b_i} - X^{a_{i+2}-a_{i+1}} Y^{b_i - b_{i+1}} X^{a_{i+1}} Y^{b_{i+1}} \\ &\quad + X^{a_{i+2}-a_{i+1}} Y^{b_i - b_{i+1}} X^{a_{i+1}} Y^{b_{i+1}} - Y^{b_i - b_{i+1}} Y^{b_{i+1} - b_{i+2}} X^{a_{i+2}} Y^{b_{i+2}} \\ &= X^{a_{i+2}-a_{i+1}} \big(X^{a_{i+1}-a_i} X^{a_i} Y^{b_i} - Y^{b_i - b_{i+1}} X^{a_{i+1}} Y^{b_{i+1}} \big) \\ &\quad + Y^{b_i - b_{i+1}} \big(X^{a_{i+2}-a_{i+1}} X^{a_{i+1}} Y^{b_{i+1}} - Y^{b_{i+1} - b_{i+2}} X^{a_{i+2}} Y^{b_{i+2}} \big) \\ &= X^{a_{i+2}-a_{i+1}} \big(X^{a_{i+1}-a_i} f_i - Y^{b_i - b_{i+1}} f_{i+1} \big) \\ &\quad + Y^{b_i - b_{i+1}} \big(X^{a_{i+2}-a_{i+1}} f_{i+1} - Y^{b_{i+1} - b_{i+2}} f_{i+2} \big). \end{aligned}$$

Moreover, one can show readily that the relations $X^{a_{i+1}-a_i} f_i - Y^{b_i - b_{i+1}} f_{i+1} = 0$ are minimal in the sense none of them can be re-written in terms of the others. We formalize this as follows.

Consider the set R^n of column vectors of size n with entries in R.

$$R^n = \left\{ \begin{pmatrix} g_1 \\ g_2 \\ \vdots \\ g_n \end{pmatrix} \middle| \, g_1, \ldots, g_n \in R \right\}$$

Each relation of the form $\sum_{i=1}^n g_i f_i = 0$ determines a column vector $\begin{pmatrix} g_1 \\ \vdots \\ g_n \end{pmatrix} \in R^n$ such that

$$\begin{pmatrix} f_1 & \cdots & f_n \end{pmatrix} \begin{pmatrix} g_1 \\ \vdots \\ g_n \end{pmatrix} = \left(\sum_{i=1}^n f_i g_i \right) = 0. \tag{5.4.1.1}$$

(Here we use the usual multiplication of matrices.) Moreover, a column vector $\begin{pmatrix} g_1 \\ \vdots \\ g_n \end{pmatrix} \in R^n$ satisfies equation (5.4.1.1) if and only if it determines such a relation. For instance, the relation $X^{a_{i+1}-a_i} f_i - Y^{b_i - b_{i+1}} f_{i+1} = 0$ determines the following column vector where the non-zero entries are in the ith and $(i+1)$st slots.

$$v_i := \begin{pmatrix} 0 \\ \vdots \\ 0 \\ X^{a_{i+1}-a_i} \\ -Y^{b_i - b_{i+1}} \\ 0 \\ \vdots \\ 0 \end{pmatrix} \tag{5.4.1.2}$$

Using this notation, the given relations are minimal in that one cannot write the vector v_i as a linear combination over R of the remaining v_j's. To see this, suppose that $v_i = \sum_{j \neq i} g_j v_j$ for some polynomials $g_j \in R$. Setting $g_i = -1$ this yields an equations $\sum_{j=1}^{n-1} g_j v_j = 0$. Writing out the column vectors, we have

$$\begin{pmatrix}0\\0\\0\\0\\\vdots\\0\end{pmatrix} = g_1\begin{pmatrix}X^{a_2-a_1}\\-Y^{b_1-b_2}\\0\\0\\\vdots\\0\end{pmatrix} + g_2\begin{pmatrix}0\\X^{a_3-a_2}\\-Y^{b_2-b_3}\\0\\\vdots\\0\end{pmatrix} + \cdots + g_{n-1}\begin{pmatrix}0\\0\\\vdots\\0\\X^{a_n-a_{n-1}}\\-Y^{b_{n-1}-b_n}\end{pmatrix}$$

$$\begin{pmatrix}0\\0\\0\\0\\\vdots\\0\end{pmatrix} = \begin{pmatrix}g_1X^{a_2-a_1}\\-g_1Y^{b_1-b_2}\\0\\0\\\vdots\\0\end{pmatrix} + \begin{pmatrix}0\\g_2X^{a_3-a_2}\\-g_2Y^{b_2-b_3}\\0\\\vdots\\0\end{pmatrix} + \cdots + \begin{pmatrix}0\\0\\\vdots\\0\\g_{n-1}X^{a_n-a_{n-1}}\\-g_{n-1}Y^{b_{n-1}-b_n}\end{pmatrix}$$

$$\begin{pmatrix}0\\0\\0\\0\\\vdots\\0\end{pmatrix} = \begin{pmatrix}g_1X^{a_2-a_1}\\-g_1Y^{b_1-b_2}+g_2X^{a_3-a_2}\\-g_2Y^{b_2-b_3}+g_3X^{a_4-a_3}\\-g_3Y^{b_3-b_4}+g_4X^{a_5-a_4}\\\vdots\\-g_{n-1}Y^{b_{n-1}-b_n}\end{pmatrix}$$

Equating the first entries here, we have $0 = g_1X^{a_2-a_1}$, which implies that $g_1 = 0$ since A is a field. Equating the second entries, we have $0 = -g_1Y^{b_1-b_2}+g_2X^{a_3-a_2} = g_2X^{a_3-a_2}$, so we have $g_2 = 0$. Continuing in this way, we have $g_j = 0$ for $j = 1, \ldots, n-1$. In particular, this implies that $-1 = g_i = 0$, contradicting the fact that A is a field.

The case of monomial ideals in more than two variables is a bit more subtle. One can easily get a list of relations satisfied by a generating sequence $f_1, \ldots, f_n \in [\![R]\!]$ of a monomial ideal I, as follows. Begin by observing the commutativity relations $f_if_j - f_jf_i = 0$, which yield relations of the form $\sum_{i<j} g_{i,j}(f_if_j - f_jf_i) = 0$. In general, there are more relations, though, because f_i and f_j need not be relatively prime. For instance, given $f_1 = X_1^2X_2$ and $f_2 = X_1X_2^2$, we have the relation

$$(X_1^2X_2)(X_1X_2^2) - (X_1X_2^2)(X_1^2X_2) = 0$$

but we can also divide by the greatest common divisor of $X_1^2X_2$ and $X_1X_2^2$ (see Exercise 2.1.14) to obtain the relation

$$(X_1)(X_1X_2^2) - (X_2)(X_1^2X_2) = 0.$$

This leads to the following result.

THEOREM 5.4.2. *Set $R = A[X_1, \ldots, X_d]$, and let $I \subseteq R$ be a monomial ideal with monomial generating sequence $f_1, \ldots, f_n$. Assume that $n \geqslant 2$. Then every relation $\sum_{i=1}^n g_if_i = 0$ with $g_i \in R$ can be re-written in the form*

$$\sum_{i<j} h_{i,j}\left(\frac{f_i}{\gcd(f_i,f_j)}f_j - \frac{f_j}{\gcd(f_i,f_j)}f_i\right) = 0$$

for some polynomials $h_{i,j} \in R$.

PROOF. In this proof, we use the following modification of the notation of Example 5.4.1. Let R^n denote the set of column vectors of size n with entries from R. For $i = 1, \ldots, n$ let $\underline{e}_i \in R^n$ denote the ith standard basis vector

$$\underline{e}_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

where the 1 occurs in the ith position. Then each relation $\sum_{i=1}^n g_i f_i = 0$ is equivalent to a vector $\sum_{i=1}^n g_i \underline{e}_i$ in R^n such that $\begin{pmatrix} f_1 & \cdots & f_n \end{pmatrix} (\sum_{i=1}^n g_i \underline{e}_i) = (\sum_{i=1}^n f_i g_i) = 0$. (Here we use the usual multiplication of matrices.) Using this notation, when we say that a relation $\sum_{i=1}^n g_i f_i = 0$ with $g_i \in R$ can be re-written in the form

$$\sum_{i<j} h_{i,j} \left(\frac{f_i}{\gcd(f_i, f_j)} f_j - \frac{f_j}{\gcd(f_i, f_j)} f_i \right) = 0$$

for some polynomials $h_{i,j} \in R$, we mean that the corresponding vector $\sum_{i=1}^n g_i \underline{e}_i = 0$ can be re-written in the form

$$\sum_{i<j} h_{i,j} \left(\frac{f_i}{\gcd(f_i, f_j)} \underline{e}_j - \frac{f_j}{\gcd(f_i, f_j)} \underline{e}_i \right) = 0.$$

Write $f_i = \underline{X}^{\underline{c}_i}$ for $i = 1, \ldots, n$.

Let $g_1, \ldots, g_n \in R$ be such that $\sum_{i=1}^n g_i f_i = 0$. Note that if $g_i = 0$ for all i, then we can re-write the given relation in the desired form using $h_{i,j} = 0$ for all i, j. Thus, we assume that at least one of the g_i's is non-zero. Note that it follows that at least two of the g_i's are non-zero. Indeed, if g_k is the only non-zero element in the list of g_i's, then we have $0 = \sum_i g_i f_i = g_k f_k$. Since A is a field, the fact that g_k and f_k are non-zero implies that their product $g_k f_k$ is also non-zero, contradiction.

Case 1: For $i = 1, \ldots, n$ there are monomials $\underline{X}^{\underline{m}_i} \in [\![R]\!]$ and coefficients $a_i \in A$ such that $g_i = a_i \underline{X}^{\underline{m}_i}$. We argue by induction on the number p of non-zero g_i's.

Base case: $p = 2$. To simplify matters, re-order the f_i's if necessary to assume that $g_i \neq 0$ for $i = 1, 2$ and $g_i = 0$ for $i > 2$. For $l = 1, \ldots, d$ set $q_l = \min(e_{1,l}, e_{2,l})$. Then we have $\gcd(f_1, f_2) = \underline{X}^{\underline{q}}$. In this case, we have $0 = g_1 f_1 + g_2 f_2 = a_1 \underline{X}^{\underline{m}_1} f_1 + a_2 \underline{X}^{\underline{m}_2} f_2$. Since $a_1 \neq 0 \neq a_2$, the linear independence of the monomials of R implies that $a_2 = -a_1$ and $\underline{X}^{\underline{m}_1} f_1 = \underline{X}^{\underline{m}_2} f_2$. Thus, we have

$$\underline{X}^{\underline{m}_1 + \underline{c}_1} = \underline{X}^{\underline{m}_1} \underline{X}^{\underline{c}_1} = \underline{X}^{\underline{m}_1} f_1 = \underline{X}^{\underline{m}_2} f_2 = \underline{X}^{\underline{m}_2} \underline{X}^{\underline{c}_2} = \underline{X}^{\underline{m}_2 + \underline{c}_2}.$$

We conclude that

$$\underline{m}_1 + \underline{c}_1 = \underline{m}_2 + \underline{c}_2 \tag{5.4.2.1}$$

in $\mathbb{N}^d$.

We claim that $\underline{m}_1 \succcurlyeq \underline{c}_2 - \underline{q}$. To see this, use the definition $q_l = \min(e_{1,l}, e_{2,l})$ to analyze two cases. If $q_l = e_{1,l} \leqslant e_{2,l}$, then equation (5.4.2.1) implies that $m_{1,l} = m_{2,l} + e_{2,l} - e_{1,l} = m_{2,l} + e_{2,l} - q_l \geqslant e_{2,l} - q_l$. On the other hand, if $q_l = e_{2,l} \leqslant e_{1,l}$, then $m_{1,l} \geqslant 0 = e_{2,l} - q_l$. This establishes the claim.

It follows that the expression $\underline{X}^{\underline{m}_1-(\underline{c}_2-\underline{q})} = \underline{X}^{\underline{m}_1}/\underline{X}^{\underline{c}_2-\underline{q}}$ describes a valid monomial in R. Similarly, we have $\underline{m}_2 \succcurlyeq \underline{c}_1 - \underline{q}$, so the expression $\underline{X}^{\underline{m}_2-(\underline{c}_1-\underline{q})} = \underline{X}^{\underline{m}_2}/\underline{X}^{\underline{c}_1-\underline{q}}$ describes a valid monomial in R. Moreover, equation (5.4.2.1) implies that $\underline{m}_2 + \underline{c}_2 - \underline{q} = \underline{m}_1 + \underline{c}_1 - \underline{q}$, so we have

$$\underline{X}^{\underline{m}_1-(\underline{c}_2-\underline{q})} = \frac{\underline{X}^{\underline{m}_1}}{\underline{X}^{\underline{c}_2-\underline{q}}} = \frac{\underline{X}^{\underline{m}_2}}{\underline{X}^{\underline{c}_1-\underline{q}}} = \underline{X}^{\underline{m}_2-(\underline{c}_1-\underline{q})} \tag{5.4.2.2}$$

in R. Set $h_{1,2} = a_2\underline{X}^{\underline{m}_2-(\underline{c}_1-\underline{q})}$. The given relation $0 = g_1 f_1 + g_2 f_2$ determines the vector $g_1\underline{e}_1 + g_2\underline{e}_2 \in R^n$, which we re-write as follows:

$$\begin{aligned}
0 &= a_1\underline{X}^{\underline{m}_1}\underline{e}_1 + a_2\underline{X}^{\underline{m}_2}\underline{e}_2 \\
&= -a_2\underline{X}^{\underline{m}_1}\underline{e}_1 + a_2\underline{X}^{\underline{m}_2}\underline{e}_2 \\
&= a_2(-\underline{X}^{\underline{m}_1}\underline{e}_1 + \underline{X}^{\underline{m}_2}\underline{e}_2) \\
&= a_2\left(-\underline{X}^{\underline{m}_1-(\underline{c}_2-\underline{q})}\underline{X}^{\underline{c}_2-\underline{q}}\underline{e}_1 + \underline{X}^{\underline{m}_2-(\underline{c}_1-\underline{q})}\underline{X}^{\underline{c}_1-\underline{q}}\underline{e}_2\right) \\
&= a_2\left(-\underline{X}^{\underline{m}_2-(\underline{c}_1-\underline{q})}\underline{X}^{\underline{c}_2-\underline{q}}\underline{e}_1 + \underline{X}^{\underline{m}_2-(\underline{c}_1-\underline{q})}\underline{X}^{\underline{c}_1-\underline{q}}\underline{e}_2\right) \\
&= a_2\underline{X}^{\underline{m}_2-(\underline{c}_1-\underline{q})}\left(-\underline{X}^{\underline{c}_2-\underline{q}}\underline{e}_1 + \underline{X}^{\underline{c}_1-\underline{q}}\underline{e}_2\right) \\
&= h_{1,2}\left(-\frac{\underline{X}^{\underline{c}_2}}{\underline{X}^{\underline{q}}}\underline{e}_1 + \frac{\underline{X}^{\underline{c}_1}}{\underline{X}^{\underline{q}}}\underline{e}_2\right) \\
&= h_{1,2}\left(-\frac{f_2}{\gcd(f_1,f_2)}\underline{e}_1 + \frac{f_1}{\gcd(f_1,f_2)}\underline{e}_2\right).
\end{aligned}$$

Thus, the given relation can be re-written in the desired form.

Induction step. Assume that $p > 2$ and that every relation $\sum_{i=1}^n \tilde{g}_i f_i = 0$ with $\tilde{g}_i = \tilde{a}_i\underline{X}^{\underline{m}_i}$ such that at most $p-1$ of the $\tilde{g}_i$'s are non-zero can be re-written in the desired form. Consider the relation $\sum_{i=1}^n g_i f_i = 0$ with $g_i = a_i\underline{X}^{\underline{m}_i}$ such that p of the g_i's are non-zero. To simplify matters, re-order the f_i's if necessary to assume that $g_i \neq 0$ for $i = 1, \ldots, p$ and $g_i = 0$ for $i > p$. Thus, we have

$$0 = \sum_{i=1}^p g_i f_i = \sum_{i=1}^p a_i\underline{X}^{\underline{m}_i}\underline{X}^{\underline{c}_i} = \sum_{i=1}^p a_i\underline{X}^{\underline{m}_i+\underline{c}_i}.$$

Since $a_p \neq 0$, linear independence of the monomials implies that the monomial $\underline{X}^{\underline{m}_p+\underline{c}_p}$ must occur in the shorter sum $\sum_{i=1}^{p-1} a_i\underline{X}^{\underline{m}_i+\underline{c}_i}$. Re-order the f_i's if necessary to assume that $\underline{X}^{\underline{m}_p+\underline{c}_p} = \underline{X}^{\underline{m}_{p-1}+\underline{c}_{p-1}}$. Arguing as in the base case, there is a monomial $\underline{X}^{\underline{b}}$ such that

$$\underline{X}^{\underline{b}}\frac{f_p}{\gcd(f_{p-1},f_p)}f_{p-1} = \underline{X}^{\underline{m}_p+\underline{c}_p} = \underline{X}^{\underline{m}_{p-1}+\underline{c}_{p-1}} = \underline{X}^{\underline{b}}\frac{f_{p-1}}{\gcd(f_{p-1},f_p)}f_p.$$

Set $h_{p-1,p} = a_p\underline{X}^{\underline{b}}$, and note that $a_p\underline{X}^{\underline{b}}\frac{f_{p-1}}{\gcd(f_{p-1},f_p)} = a_p\underline{X}^{\underline{m}_p} = g_p$. Set $\tilde{g}_{p-1} = (a_{p-1}+a_p)\underline{X}^{\underline{m}_{p-1}}$, and consider the relation

$$\begin{aligned}
0 &= \left(\sum_{i=1}^{p} g_i f_i\right) - h_{p-1,p}\left(\frac{f_{p-1}}{\gcd(f_{p-1},f_p)}f_p - \frac{f_p}{\gcd(f_{p-1},f_p)}f_{p-1}\right)\\
&= \left(\sum_{i=1}^{p} g_i f_i\right) - a_p\underline{X}^{\underline{b}}\left(\frac{f_{p-1}}{\gcd(f_{p-1},f_p)}f_p - \frac{f_p}{\gcd(f_{p-1},f_p)}f_{p-1}\right)\\
&= \left(\sum_{i=1}^{p} g_i f_i\right) - a_p\underline{X}^{\underline{b}}\frac{f_{p-1}}{\gcd(f_{p-1},f_p)}f_p + a_p\underline{X}^{\underline{b}}\frac{f_p}{\gcd(f_{p-1},f_p)}f_{p-1}\\
&= \left(\sum_{i=1}^{p} g_i f_i\right) - g_p f_p + a_p\underline{X}^{\underline{m}_{p-1}}f_{p-1}\\
&= \left(\sum_{i=1}^{p-2} g_i f_i\right) + \tilde{g}_{p-1}f_{p-1}.
\end{aligned}$$

The final expression in this display is one where our induction hypothesis applies. Thus, the vector $(\sum_{i=1}^{p} g_i\underline{e}_i) - h_{p-1,p}\left(\frac{f_{p-1}}{\gcd(f_{p-1},f_p)}\underline{e}_p - \frac{f_p}{\gcd(f_{p-1},f_p)}\underline{e}_{p-1}\right)$ can be re-written in the form $\sum_{i<j}\tilde{h}_{i,j}\left(\frac{f_i}{\gcd(f_i,f_j)}\underline{e}_j - \frac{f_j}{\gcd(f_i,f_j)}\underline{e}_i\right) = 0$. By adding the vector $h_{p-1,p}\left(\frac{f_{p-1}}{\gcd(f_{p-1},f_p)}\underline{e}_p - \frac{f_p}{\gcd(f_{p-1},f_p)}\underline{e}_{p-1}\right)$, we conclude that the original vector $\sum_{i=1}^{p} g_i\underline{e}_i = 0$ can be re-written in the desired form. This concludes the proof in case 1.

Case 2: The general case. Write each g_i as a linear combination of monomials. Then rewrite the relation $\sum_{i=1}^{n} g_i f_i = 0$ in terms of the monomials occurring in the g_i's. Use the linear independence of the monomials in R to obtain relations $\sum_{i=1}^{n} g_{i,\underline{m}} f_i = 0$ where $\underline{m} \in \mathbb{N}^d$ and each $g_{i,\underline{m}}$ is of the form $a_{i,\underline{m}}\underline{X}^{\underline{p}_i}$ for some $\underline{p}_i \in \mathbb{N}^d$ such that $g_{i,\underline{m}} f_i = a_i\underline{X}^{\underline{m}}$. Apply Case 1 to each of the relations $\sum_{i=1}^{n} g_{i,\underline{m}} f_i = 0$, and add the results to re-write the general relation $\sum_{i=1}^{n} g_i f_i = 0$ in the desired form. □

Note that Theorem 5.4.2 does not give a minimal set of relations between the f_i in general. Indeed, consider the case $d = 2$ and $n > 2$. For $i = 1, \ldots, n-1$, the relation $\frac{f_i}{\gcd(f_i,f_{i+1})}f_{i+1} - \frac{f_{i+1}}{\gcd(f_i,f_{i+1})}f_i$ is equivalent to the relation given at the beginning of Example 5.4.1. In particular, the list of relations in Theorem 5.4.2 is not minimal because it consists of $\binom{n}{2}$ many relations, and it contains the list of $n - 1 < \binom{n}{2}$ relations in Example 5.4.1.

Note also that each quotient $f_i/\gcd(f_i,f_j)$ can be re-written as $\operatorname{lcm}(f_i,f_j)/f_j$, by Exercise 2.1.14. The lcm-formulation of this expression is more convenient for the work that follows.

Part of the discussion of Example 5.4.1 shows that the vectors $v_1, \ldots, v_{n-1}$ are linearly independent. In other words, in this case, there are no relations between the relations on the f_i. This is not true in general, though. One of the insights of homological algebra is that there is value in understanding the relations between the relations on the f_i in general, and the relations between the relations between the relations, and so on. For arbitrary ideals, this is an extremely difficult problem. However, for monomial ideals the "Taylor resolution" solves this problem. Note that is uses the relations from Theorem 5.4.2 as a starting point, so it is not minimal in general. However, it gives very useful information about monomial ideals. Moreover, given a non-monomial ideal I one can use the Taylor resolution of the initial ideal $\mathrm{in}(I)$ to get useful information about the original ideal I.

As a motivation for the general construction, we first identify the relations between the relations from Theorem 5.4.2 for a specific example. We use the notation R^n and $\underline{e}_i$ from the proof of Theorem 5.4.2.

Example 5.4.3. Set $R = A[X, Y, Z]$, and consider the ideal $(X^3, Y^5, Z^4)R$. In R^3, we have the following relations from Theorem 5.4.2.

$$X^3\underline{e}_2 - Y^5\underline{e}_1 \qquad X^3\underline{e}_3 - Z^4\underline{e}_1 \qquad Y^5\underline{e}_3 - Z^4\underline{e}_2.$$

A relation between these relations is an equation of the form

$$g_{1,2}(X^3\underline{e}_2 - Y^5\underline{e}_1) + g_{1,3}(X^3\underline{e}_3 - Z^4\underline{e}_1) + g_{2,3}(Y^5\underline{e}_3 - Z^4\underline{e}_2) = 0. \tag{5.4.3.1}$$

For instance, we have

$$Z^4(X^3\underline{e}_2 - Y^5\underline{e}_1) - Y^5(X^3\underline{e}_3 - Z^4\underline{e}_1) + X^3(Y^5\underline{e}_3 - Z^4\underline{e}_2) = 0. \tag{5.4.3.2}$$

In fact, we can check that every relation of the form (5.4.3.1) can be re-written as a multiple of the one given in (5.4.3.2). Indeed, combining like terms in (5.4.3.1) yields the following.

$$0 = -(g_{1,2}Y^5 + g_{1,3}Z^4)\underline{e}_1 + (g_{1,2}X^3 - g_{2,3}Z^4)\underline{e}_2 + (g_{1,3}X^3 + g_{2,3}Y^5)\underline{e}_3.$$

It follows that we have

$$0 = g_{1,2}Y^5 + g_{1,3}Z^4 \tag{5.4.3.3}$$

$$0 = g_{1,2}X^3 - g_{2,3}Z^4 \tag{5.4.3.4}$$

$$0 = g_{1,3}X^3 + g_{2,3}Y^5. \tag{5.4.3.5}$$

From equation (5.4.3.3), we have $g_{1,3}Z^4 = -g_{1,2}Y^5$. Since R is a unique factorization domain and $\gcd(Y^5, Z^4) = 1$, we conclude that $Y^5 \big| g_{1,3}$ and $Z^4 \big| g_{1,2}$. Thus, there are polynomials $\tilde{g}_{1,2}, \tilde{g}_{1,3} \in R$ such that $g_{1,2} = Z^4\tilde{g}_{1,2}$ and $g_{1,3} = Y^5\tilde{g}_{1,3}$. Substituting into the equation (5.4.3.3), we have

$$0 = Z^4\tilde{g}_{1,2}Y^5 + Y^5\tilde{g}_{1,2}Z^4 = Y^5Z^4(\tilde{g}_{1,2} + \tilde{g}_{1,3})$$

and we conclude that $\tilde{g}_{1,3} = -\tilde{g}_{1,2}$. Thus, we have $g_{1,3} = -Y^5\tilde{g}_{1,2}$. Similarly, equation (5.4.3.4) implies that $g_{2,3} = X^3\tilde{g}_{1,2}$. It follows that equation (5.4.3.1) can be re-written in the following form.

$$\begin{aligned} 0 &= Z^4\tilde{g}_{1,2}(X^3\underline{e}_2 - Y^5\underline{e}_1) - Y^5\tilde{g}_{1,2}(X^3\underline{e}_3 - Z^4\underline{e}_1) + X^3\tilde{g}_{1,2}(Y^5\underline{e}_3 - Z^4\underline{e}_2) \\ &= \tilde{g}_{1,2}[Z^4(X^3\underline{e}_2 - Y^5\underline{e}_1) - Y^5(X^3\underline{e}_3 - Z^4\underline{e}_1) + X^3(Y^5\underline{e}_3 - Z^4\underline{e}_2)] \end{aligned}$$

As claimed, this is a multiple of the relation given in (5.4.3.2).

As in Example 5.4.1, we need to make this slightly more formal. Consider a new copy of R^3. Each column vector

$$\underline{v} = \begin{pmatrix} g_{1,2} \\ g_{1,3} \\ g_{2,3} \end{pmatrix}$$

has the potential to determine a relation as in equation (5.4.3.1). For instance, the relation (5.4.3.2) determines the following column vector.

$$\underline{w} = \begin{pmatrix} Z^4 \\ -Y^5 \\ X^3 \end{pmatrix}$$

What we have shown implies that the vector $\underline{v}$ determines a relation as in equation (5.4.3.1) if and only if there is a polynomial h such that $\underline{v} = h\underline{w}$. See Exercise 5.4.8 and Theorem 5.4.4.

The next results give general versions of the previous example. The first one uses our intuitive formulation of the notion of "re-writing the relations". See Example 5.4.1 and Theorem 5.4.2 for explanations of the notations R^n and $\underline{e}_i$.

THEOREM 5.4.4. *Set $R = A[X_1, \ldots, X_d]$, and let $I \subseteq R$ be a monomial ideal with monomial generating sequence $f_1, \ldots, f_n$. Assume that $n \geqslant 2$. For all i, j with $1 \leqslant i < j \leqslant n$, consider the following vector in R^n.*

$$w_{i,j} := \frac{f_i}{\gcd(f_i, f_j)}\underline{e}_j - \frac{f_j}{\gcd(f_i, f_j)}\underline{e}_i = \frac{\operatorname{lcm}(f_i, f_j)}{f_j}\underline{e}_j - \frac{\operatorname{lcm}(f_i, f_j)}{f_i}\underline{e}_i.$$

Then each relation $\sum_{i<j} g_{i,j} w_{i,j} = 0$ with $g_{i,j} \in R$ can be re-written in the form

$$\sum_{i<j<k} h_{i,j,k} \left(\frac{\operatorname{lcm}(f_i, f_j, f_k)}{\operatorname{lcm}(f_j, f_k)} w_{j,k} - \frac{\operatorname{lcm}(f_i, f_j, f_k)}{\operatorname{lcm}(f_i, f_k)} w_{i,k} + \frac{\operatorname{lcm}(f_i, f_j, f_k)}{\operatorname{lcm}(f_i, f_j)} w_{i,j} \right) = 0$$

for some polynomials $h_{i,j,k} \in R$.

THEOREM 5.4.5. *Set $R = A[X_1, \ldots, X_d]$, and let $I \subseteq R$ be a monomial ideal with monomial generating sequence $f_1, \ldots, f_n$. Assume that $n \geqslant 2$. For all i, j with $1 \leqslant i < j \leqslant n$, consider the following vector in R^n.*

$$w_{i,j} := \frac{f_i}{\gcd(f_i, f_j)}\underline{e}_j - \frac{f_j}{\gcd(f_i, f_j)}\underline{e}_i = \frac{\operatorname{lcm}(f_i, f_j)}{f_j}\underline{e}_j - \frac{\operatorname{lcm}(f_i, f_j)}{f_i}\underline{e}_i.$$

Now, consider the set $R^{\binom{n}{2}}$ of column vectors of R of size $\binom{n}{2}$. Denote the standard basis vectors in $R^{\binom{n}{2}}$ as $\underline{e}_{1,2}, \ldots, \underline{e}_{1,n}, \underline{e}_{2,3}, \ldots, \underline{e}_{2,n}, \ldots, \underline{e}_{n-1,n}$. Then a vector

$$\begin{pmatrix} g_{1,2} \\ \vdots \\ g_{n-1,n} \end{pmatrix} = \sum_{i<j} g_{i,j}\underline{e}_{i,j} \in R^{\binom{n}{2}}$$

determines a relation $\sum_{i<j} g_{i,j} w_{i,j} = 0$ in R^n if and only if it can be re-written in the form

$$\sum_{i<j<k} h_{i,j,k} \left(\frac{\operatorname{lcm}(f_i, f_j, f_k)}{\operatorname{lcm}(f_j, f_k)} \underline{e}_{j,k} - \frac{\operatorname{lcm}(f_i, f_j, f_k)}{\operatorname{lcm}(f_i, f_k)} \underline{e}_{i,k} + \frac{\operatorname{lcm}(f_i, f_j, f_k)}{\operatorname{lcm}(f_i, f_j)} \underline{e}_{i,j} \right)$$

for some polynomials $h_{i,j,k} \in R$.

As one may imagine, one can continue along these lines. For instance, if we consider the vector

$$w_{i,j,k} = \frac{\operatorname{lcm}(f_i, f_j, f_k)}{\operatorname{lcm}(f_j, f_k)} \underline{e}_{j,k} - \frac{\operatorname{lcm}(f_i, f_j, f_k)}{\operatorname{lcm}(f_i, f_k)} \underline{e}_{i,k} + \frac{\operatorname{lcm}(f_i, f_j, f_k)}{\operatorname{lcm}(f_i, f_j)} \underline{e}_{i,j}$$

in $R^{\binom{n}{2}}$, we can ask what all the relations between the $w_{i,j,k}$ look like. It turns out that they look similar to the $w_{i,j,k}$ themselves, just like the relations between the w_i look similar to the w_i. This is formalized, as follows.

For $t = 1, \ldots, n$ consider the set $R^{\binom{n}{t}}$ of column vectors of R of size $\binom{n}{t}$. Denote the standard basis vectors in $R^{\binom{n}{t}}$ as $\underline{e}_{F_1}, \ldots, \underline{e}_{F_{\binom{n}{t}}}$ where $F_1, \ldots, F_{\binom{n}{t}}$ are the distinct subsets of $\{1, \ldots, n\}$ of size t. (In other words, the F_i are the distinct $t-1$-dimensional faces of the $(n-1)$-simplex Δ_{n-1}.) For each $F_i = \{j_1, \ldots, j_t\}$ with $j_1 < \cdots < j_t$, consider the following vector in $R^{\binom{n}{t-1}}$.

$$w_{F_i} := \sum_{p=1}^{t} (-1)^{p-1} \frac{\operatorname{lcm}(f_{j_1}, \ldots, f_{j_t})}{\operatorname{lcm}(f_{j_1}, \ldots, f_{j_{p-1}}, f_{j_{p+1}}, \ldots, f_{j_t})} \underline{e}_{\{j_1, \ldots, j_{p-1}, j_{p+1}, \ldots, j_t\}}$$

Then we have the following generalization of Theorem 5.4.5.

THEOREM 5.4.6. *With the above notation, a vector*

$$\begin{pmatrix} g_{F_1} \\ \vdots \\ g_{F_{\binom{n}{t}}} \end{pmatrix} = \sum_{i=1}^{\binom{n}{t}} g_{F_i} \underline{e}_{F_i} \in R^{\binom{n}{t}}$$

determines a relation $\sum_{i=1}^{\binom{n}{t}} g_{F_i} w_{F_i} = 0$ *in* $R^{\binom{n}{t-1}}$ *if and only if it can be re-written in the form*

$$\sum_{i=1}^{\binom{n}{t}} g_{F_i} \underline{e}_{F_i} = \sum_{q=1}^{\binom{n}{t+1}} h_{F_q} w_{F_q}$$

for some polynomials $h_{F_q} \in R$.

One translates this into the language of homological algebra as follows. Let $\partial_t \colon R^{\binom{n}{t}} \to R^{\binom{n}{t-1}}$ denote the function given by the rule

$$\partial_t \left(\sum_{i=1}^{\binom{n}{t}} g_{F_i} \underline{e}_{F_i} \right) = \sum_{i=1}^{\binom{n}{t}} g_{F_i} w_{F_i}.$$

In other words, using the standard correspondence between linear transformations and matrices (remembering that elements of $R^{\binom{n}{t}}$ are column vectors) ∂_t is represented by the matrix δ_t whose ith column is w_{F_i}. Each map ∂_t is R-*linear*, meaning that one has $\partial_t(rv + sw) = r\partial_t(v) + s\partial_t(w)$ for all $r, s \in R$ and all $v, w \in R^{\binom{n}{t}}$. (One also says that ∂_t is an R-*module homomorphism*.) The *image* of ∂_t is the set of all outputs of ∂_t

$$\operatorname{Im}(\partial_t) = \left\{ \partial_t(v) \mid v \in R^{\binom{n}{t}} \right\}$$

and the *kernel* of ∂_t is

$$\operatorname{Ker}(\partial_t) = \left\{ v \in R^{\binom{n}{t}} \mid \partial_t(v) = 0 \right\}.$$

In linear algebra terms, these correspond to the column space and the null space of the matrix δ_t, respectively.

In this language, Theorem 5.4.6 says that for $t = 1, \ldots, n$ we have

$$\mathrm{Im}(\partial_{t+1}) = \mathrm{Ker}(\partial_t).$$

When $t = n$, this means that $\mathrm{Ker}(\partial_n) = 0$.

In the language of homological algebra, we say that the following sequence

$$0 \to R^{\binom{n}{n}} \xrightarrow{\partial_n} R^{\binom{n}{n-1}} \xrightarrow{\partial_{n-1}} \cdots \xrightarrow{\partial_2} R^{\binom{n}{1}} \xrightarrow{\partial_1} R^{\binom{n}{0}} \xrightarrow{\tau} R/I \to 0$$

is *exact*, where τ is the function $\tau(r) = r + I$. Such a sequence is called a *free resolution* of R/I. This notion is the starting point of homological algebra, in many ways. For instance, one uses free resolutions to construct the cohomology module $\mathrm{Ext}^i_R(R/I, A)$. This is a finite-dimensional vector space over A whose dimension is the ith *Betti number* of R/I, an important invariant used to study I. On the other hand, one can use the cohomology module $\mathrm{Ext}^i_R(A, R/I)$ to decide when R/I is Cohen-Macaulay. These ideas have far-reaching applications to many, many areas of mathematics and science.

Exercises.

EXERCISE 5.4.7. Assume that R, I, and $f_1, \ldots, f_n$ are as in Example 5.4.1.

(a) Let $h_i, h_{i+1} \in [\![R]\!]$ be such that $h_i f_i - h_{i+1} f_{i+1} = 0$. Prove that there exists $g \in [\![R]\!]$ such that $h_i = gX^{a_{i+1}-a_i}$ and $h_{i+1} = g_i Y^{b_i - b_{i+1}}$. (Hint: g is an appropriate GCD of h_i and h_{i+1}.)

(b) Let $h_i, h_j \in [\![R]\!]$ and $c_i, c_j \in A$ be such that $i < j$ and $c_i h_i f_i + c_j h_j f_j = 0$. Prove that $c_j = -c_i$ and that there exist $g_i, \ldots, g_{j-1} \in [\![R]\!]$ such that $h_i = g_i X^{a_{i+1}-a_i}$ and $h_j = g_{j-1} Y^{b_{j-1}-b_j}$ and such that the relation $c_i h_i f_i + c_j h_j f_j = 0$ can be re-written in the form

$$\sum_{p=i}^{j-1} [(c_p g_p X^{a_{p+1}-a_p}) f_p - (c_p g_p Y^{b_p - b_{p+1}}) f_{p+1}] = 0.$$

(Hint: Argue by induction on $j - i$.)

(c) Let $h_1, \ldots, h_n \in [\![R]\!]$ be such that $\sum_{i=1}^n h_i f_i = 0$. Prove that this relation can be re-written in the form

$$\sum_{i=1}^{n-1} [(g_i X^{a_{i+1}-a_i}) f_i - (g_i Y^{b_i - b_{i+1}}) f_{i+1}] = 0$$

for suitable choices of $g_1, \ldots, g_{n-1}$. (Hint: Rewrite each h_i as a linear combination of monomials, and collect like terms.)

EXERCISE 5.4.8. In the notation of Example 5.4.3, prove that the vector $\underline{v}$ determines a relation as in equation (5.4.3.1) if and only if there is a polynomial h such that $\underline{v} = h\underline{w}$.

EXERCISE 5.4.9. Set $R = A[X, Y]$, and consider the monomial ideal $I = (X^5, X^4Y^2, X^2Y^3)R$.

(a) Write out the minimal relations between the generators of I, as in Example 5.4.1.

(b) Write out the relations between the generators of I, as in Theorem 5.4.2, and the relations between the relations (etc.) as in Theorems 5.4.4, 5.4.5, and 5.4.6.

(c) Repeat part (b) for the ideal $J = (X^3, Y^2, Z^2, XYZ) \subseteq A[X, Y, Z]$.

Resolutions of Monomial Ideals in Macaulay2.

Exercises.

Conclusion

Include some history here. E.g., who are Cohen and Macaulay? (Point out the connection to Macaulay2.) Talk about some of the literature from this area. Our treatment of the PMU Placement Problem in Section 5.1 is motivated largely by [**3**]. Our treatment of the Upper Bound Theorem in Section 5.2 comes mostly from [**4, 39**]. Our treatment of initial ideals in Section 5.3 comes mostly from [**42**]. Hilbert functions are from [**4**]. Our treatment of resolutions in Section 5.4 comes mostly from [**30**].

Other references on the PMU Placement Problem in Section 5.1 include [**2, 24, 35**]. Other references on the Upper Bound Theorem in Section 5.2 include the original source [**38**]. Further references on Hilbert functions, Gröbner bases, initial ideals; include basics like [**1, 4, 8, 26, 39**]. Also, include weighted edge ideals, path ideals, and weighted path ideals.

Part 3

Decomposing Monomial Ideals

CHAPTER 6

Parametric Decompositions of Monomial Ideals

This chapter deals with another case of monomial ideals where there is a reasonable algorithm for computing m-irreducible decompositions. These are the monomial ideals I such that its monomial radical $\text{m-rad}\,(I)$ is the ideal $\mathfrak{X}$ generated by all the variables in R. See Section 2.3 for properties of the monomial radical; the exercises of that section are particularly relevant.

This chapter begins with Section 6.1, discussing properties of the m-irreducible ideals that arise in the decompositions of these ideals. These ideals are called "parameter ideals," and they determine "parametric decompositions." This section explicitly characterizes the monomial ideals that admit parametric decompositions as those monomial ideals I such that $\text{m-rad}\,(I) = \mathfrak{X}$. The rest of the chapter focuses on techniques for computing parametric decompositions. Section 6.2 contains an in-depth treatment of the special case where $I = \mathfrak{X}^n$. This motivates the use of "corner elements," and it is shown in Section 6.3 how these elements determine irredundant parametric decompositions in general. Sections 6.4 and 6.5 deal with the problem of finding the corner elements of a given ideal, first in two variables, then in general. Finally, Section 6.6 contains an exploration of the process of using parametric decompositions in two variables to find m-irreducible decompositions in two variables for ideals that do not necessarily have parametric decompositions.

6.1. Parameter Ideals

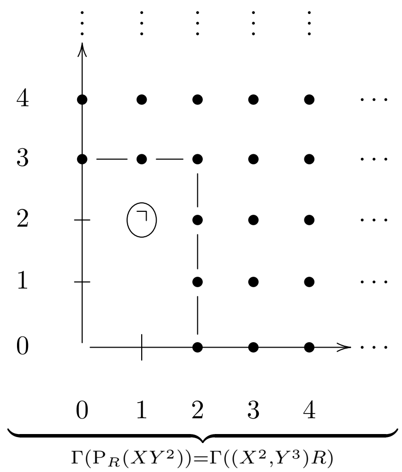
In this section, A is a non-zero commutative ring with identity.

This section deals with special cases of m-irreducible monomial ideals. In the following definition, the "P" stands for "parameter". The term "parameter ideal" comes from the idea that each power of each variable is a parameter, so these ideals are generated by a complete sequence of parameters.

Definition 6.1.1. Set $R = A[X_1, \ldots, X_d]$. A *parameter ideal* in R is an ideal of the form $(X_1^{a_1}, \ldots, X_d^{a_d})R$ with $a_1, \ldots, a_d \geqslant 1$. If $f = \underline{X}^{\underline{n}}$ with $\underline{n} \in \mathbb{N}^d$, then set

$$\mathrm{P}_R(f) = (X_1^{n_1+1}, \ldots, X_d^{n_d+1})R.$$

EXAMPLE 6.1.2. Set $R = A[X,Y]$. Then $\mathrm{P}_R(XY^2) = (X^2,Y^3)R$. One can see from the graph



that the "corner" in the graph of $\mathrm{P}_R(XY^2)$ corresponds exactly to the monomial XY^2. (See also Corollary 6.3.7 below.) This partially explains why this ideal is denoted $\mathrm{P}_R(XY^2)$ instead of $\mathrm{P}_R(f)$ for some different monomial f.

Other computations in this situation include $\mathrm{P}_R(1) = (X,Y)R$ and $\mathrm{P}_R(X) = (X^2,Y)R$ and $\mathrm{P}_R(Y) = (X,Y^2)R$.

The next lemma is particularly useful for working with parameter ideals.

LEMMA 6.1.3. *Set $R = A[X_1,\ldots,X_d]$. Let f and g be monomials in R.*

(a) *We have $f \notin \mathrm{P}_R(f)$.*
(b) *We have $g \in \mathrm{P}_R(f)$ if and only if $f \notin (g)R$.*

PROOF. Write $f = \underline{X}^{\underline{m}}$ and $g = \underline{X}^{\underline{n}}$.

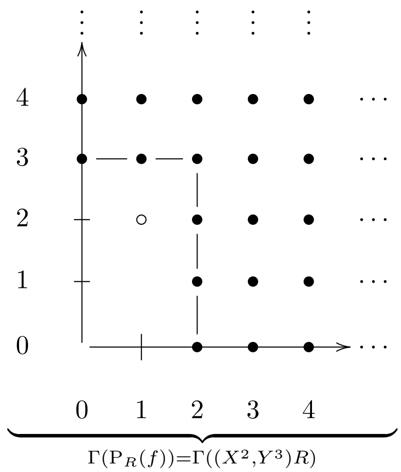
(a) We have $\mathrm{P}_R(f) = (X_1^{m_1+1},\ldots,X_d^{m_d+1})R$. Suppose that $f \in \mathrm{P}_R(f)$. Theorem 1.1.8 implies that f is a monomial multiple of some $X_i^{m_i+1}$, and it follows from Lemma 1.1.7 that $m_i \geqslant m_i+1$, which is impossible.

(b) $\Longrightarrow$: Assume that $g \in \mathrm{P}_R(f)$ and suppose that $f \in (g)R$. The condition $g \in \mathrm{P}_R(f)$ implies $f \in (g)R \subseteq \mathrm{P}_R(f)$, which contradicts part (a).

$\Longleftarrow$: Assume that $g \notin \mathrm{P}_R(f)$. Since $\mathrm{P}_R(f)$ is generated by $X_1^{m_1+1},\ldots,X_d^{m_d+1}$ this implies that $g \notin (X_i^{m_i+1})R$ for $i = 1,\ldots,d$. Lemma 1.1.7 implies that either $n_j < 0$ for some $j \neq i$ or $n_i < m_i+1$. Since we have $n_j \geqslant 0$ for all j, this implies that $n_i < m_i+1$, that is, that $n_i \leqslant m_i$. This is true for each index i, so $\underline{m} \succcurlyeq \underline{n}$. This implies that $f \in (g)R$ by Lemma 1.1.7. $\square$

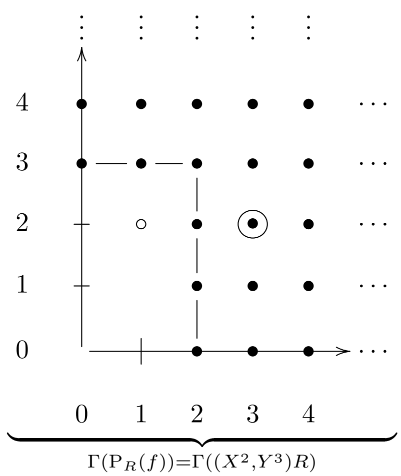
The next example contains a graphical explanation of the previous lemma.

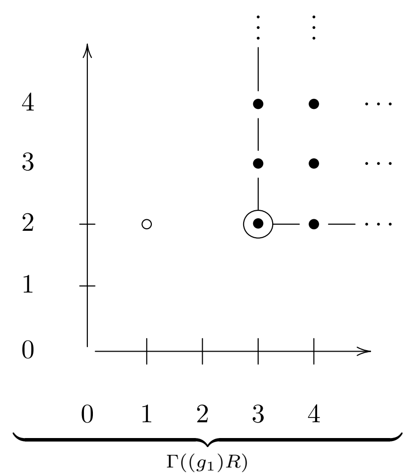
EXAMPLE 6.1.4. Set $R = A[X,Y]$. Then $\mathrm{P}_R(XY^2) = (X^2, Y^3)R$. For part (a) one can see from the graph



that $f = XY^2 \notin \mathrm{P}_R(XY^2)$. (The monomial XY^2 is represented by $\circ$ in this graph.)

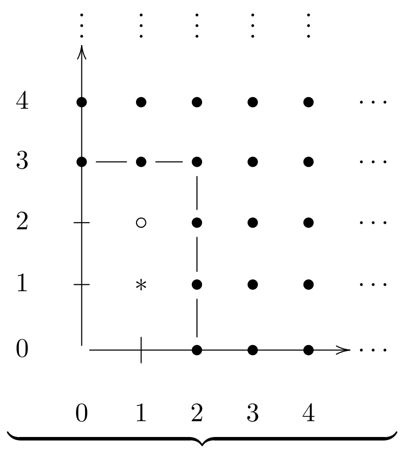
For part (b) we look at two examples. In the first example, the monomial $g_1 = X^3Y^2 \in \mathrm{P}_R(f)$ is circled



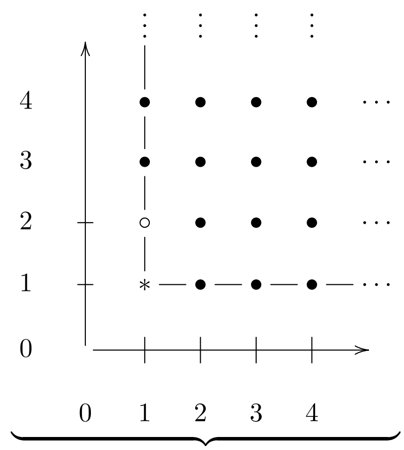


and we have $g_1 \in \mathrm{P}_R(f)$ and $f \notin g_1R$.

In the second example, the monomial $g_2 = XY \notin \mathrm{P}_R(f)$ designated with an asterisk $*$



$\Gamma(\mathrm{P}_R(f))=\Gamma((X^2,Y^3)R)$



$\Gamma((g_2)R)$

and we have $g_2 \notin \mathrm{P}_R(f)$ and $f \in g_1R$.

The decompositions of interest for this chapter are defined next.

DEFINITION 6.1.5. Set $R = A[X_1,\ldots,X_d]$. Let J be a monomial ideal of R. A *parametric decomposition* of J is a decomposition of J of the form $J = \bigcap_{i=1}^n \mathrm{P}_R(z_i)$. A parametric decomposition $J = \bigcap_{i=1}^n \mathrm{P}_R(z_i)$ is *redundant* if if there exists indices $j \neq j'$ such that $\mathrm{P}_R(z_j) \subseteq \mathrm{P}_R(z_{j'})$. A parametric decomposition $J = \bigcap_{i=1}^n \mathrm{P}_R(z_i)$ is *irredundant* if if it is not redundant, that is if for all indices $j \neq j'$ one has $\mathrm{P}_R(z_j) \not\subseteq \mathrm{P}_R(z_{j'})$.

REMARK 6.1.6. Set $R = A[X_1,\ldots,X_d]$. Let J be a monomial ideal of R.

The monomial J may or may not have a parametric decomposition. In fact, we shall see in Theorem 6.1.8 that J has a parametric decomposition if and only if $\text{m-rad}\,(J) = (X_1,\ldots,X_d)R$.

Theorem 3.1.3 implies that every parameter ideal in R is m-irreducible. Hence, each parametric decomposition of J is an m-irreducible decomposition; also, such a decomposition is (ir)redundant as a parametric decomposition if and only if it is (ir)redundant as an m-irreducible decomposition. Furthermore, any parametric decomposition can be reduced to an irredundant parametric decomposition, and irredundant parametric decompositions are unique up to re-ordering; see Algorithm 3.3.5 and Theorem 3.3.8.

The next result contains the first step toward characterizing the monomial ideals that admit parametric decompositions.

PROPOSITION 6.1.7. *Set $R = A[X_1,\ldots,X_d]$ and $\mathfrak{X} = (X_1,\ldots,X_d)R$. A monomial ideal $J \subseteq R$ is a parameter ideal if and only if J is m-irreducible and* $\text{m-rad}\,(J) = \mathfrak{X}$.

PROOF. If J is a parameter ideal, then J is m-irreducible by Theorem 3.1.3, and Exercise 2.3.13 implies that $\text{m-rad}\,(J) = \mathfrak{X}$.

Conversely, assume that J is m-irreducible and $\text{m-rad}\,(J) = \mathfrak{X}$. The condition $\text{m-rad}\,(J) = \mathfrak{X}$ implies that $J \neq 0$, so Theorem 3.1.3 provides positive integers

$k, t_1, \ldots, t_k, e_1, \ldots, e_k$ such that $1 \leqslant t_1 < \cdots < t_k \leqslant d$ and $J = (X_{t_1}^{e_1}, \ldots, X_{t_k}^{e_k})R$. By Exercise 2.3.13, the irredundant monomial generating sequence $X_{t_1}^{e_1}, \ldots, X_{t_k}^{e_k}$ for J contains a power of each variable X_i. That is, we have $J = (X_1^{e_1}, \ldots, X_d^{e_d})R$, so J is a parameter ideal. $\square$

THEOREM 6.1.8. *Set $R = A[X_1, \ldots, X_d]$ and $\mathfrak{X} = (X_1, \ldots, X_d)R$. Let J be a monomial ideal of R. Then J has a parametric decomposition if and only if* $\text{m-rad}\,(J) = \mathfrak{X}$.

PROOF. $\Longrightarrow$: If J has a parametric decomposition $J = \bigcap_{i=1}^n \mathrm{P}_R(z_i)$, then

$$\text{m-rad}\,(J) = \text{m-rad}\left(\bigcap_{i=1}^n \mathrm{P}_R(z_i)\right) = \bigcap_{i=1}^n \text{m-rad}\,(\mathrm{P}_R(z_i)) = \bigcap_{i=1}^n \mathfrak{X} = \mathfrak{X}.$$

See Propositions 2.3.4(b) and 6.1.7.

$\Longleftarrow$: Assume that $\text{m-rad}\,(J) = \mathfrak{X}$. The monomial ideal J has an m-irreducible decomposition $J = \bigcap_{i=1}^n J_i$ by Corollary 3.3.6. Exercise 2.3.14 implies that $\text{m-rad}\,(J_i) = \mathfrak{X}$ for each index i, so each J_i is a parameter ideal by Proposition 6.1.7. Thus, the intersection $\bigcap_{i=1}^n J_i$ is a parametric decomposition of J. $\square$

Exercises.

EXERCISE 6.1.9. Set $R = A[X_1, \ldots, X_d]$. Compute $\mathrm{P}_R(1)$ and $\mathrm{P}_R(X_i)$ for $i = 1, \ldots, d$. What are the generators for these ideals?

EXERCISE 6.1.10. Set $R = A[X_1, \ldots, X_d]$. Let f, g be monomials in $[\![R]\!]$.

(a) Prove that $\mathrm{P}_R(fg) \subseteq \mathrm{P}_R(f) \bigcap \mathrm{P}_R(g)$.
(b) Prove or disprove: $\mathrm{P}_R(fg) = \mathrm{P}_R(f) \bigcap \mathrm{P}_R(g)$.
(c) Prove or disprove: $\mathrm{P}_R(fg) \subseteq \mathrm{P}_R(f)\mathrm{P}_R(g)$.
(d) Prove or disprove: $\mathrm{P}_R(fg) = \mathrm{P}_R(f)\mathrm{P}_R(g)$.
(e) Prove that the following conditions are equivalent.
 (i) $\mathrm{P}_R(fg) = \mathrm{P}_R(f)$;
 (ii) $fg = f$; and
 (iii) $g = 1_R$.

EXERCISE 6.1.11. Set $R = A[X_1, \ldots, X_d]$. Set $\mathfrak{X} = (X_1, \ldots, X_d)R$. Prove that the following conditions are equivalent.

(i) A is reduced;
(ii) for every monomial $z \in R$, one has $\mathrm{rad}\,(\mathrm{P}_R(z)) = \mathfrak{X}$; and
(iii) there exists a monomial $z \in R$ such that $\mathrm{rad}\,(\mathrm{P}_R(z)) = \mathfrak{X}$.

EXERCISE 6.1.12. Set $R = A[X_1, \ldots, X_d]$. For a monomial $z \in [\![R]\!]$, prove that $z \notin I$ if and only if $I \subseteq \mathrm{P}_R(z)$.

*EXERCISE 6.1.13. Set $R = A[X_1, \ldots, X_d]$. Let w, z be monomials in R. Prove that the following conditions are equivalent:

(i) $z \in (w)R$;
(ii) $w \notin \mathrm{P}_R(z)$;
(iii) $\mathrm{P}_R(z) \subseteq \mathrm{P}_R(w)$; and
(iv) $(\mathrm{P}_R(z) :_R w) \neq R$.

(This exercise is used in several places.)

EXERCISE 6.1.14. Set $R = A[X_1, \ldots, X_d]$ with $d \geqslant 2$. Let I be a monomial ideal in R. If f and w are monomials in R, show that $(\mathrm{P}_R(fw) :_R fR) = \mathrm{P}_R(w)$.

Parameter Ideals in Macaulay2.

Exercises.

6.2. An Example

In this section, A is a non-zero commutative ring with identity.

For the ideal $\mathfrak{X} = (X_1, \ldots, X_d)R$ in the ring $R = A[X_1, \ldots, X_d]$, we have m-rad$(\mathfrak{X}^n) = \mathfrak{X}$. Hence, Theorem 6.1.8 implies that $\mathfrak{X}^n$ has a parametric decomposition. The next theorem explicitly describes this decomposition.

Theorem 6.2.1. *Set $R = A[X_1, \ldots, X_d]$ and $\mathfrak{X} = (X_1, \ldots, X_d)R$. For each integer $n \geqslant 1$, we have*

$$\mathfrak{X}^n = \bigcap_{\deg(f)=n-1} \mathrm{P}_R(f)$$

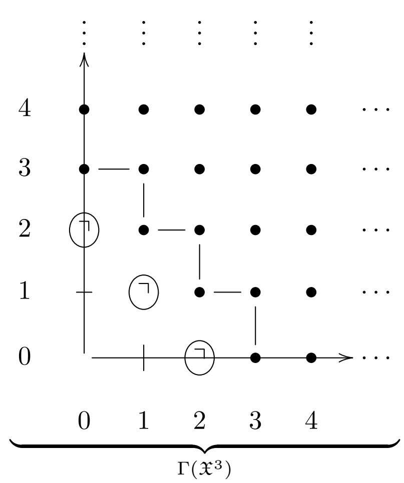
where the intersection runs over all monomials $f \in [\![R]\!]$ such that $\deg(f) = n - 1$. *Furthermore, this intersection is irredundant.*

Before proving this result, we give a specific example.

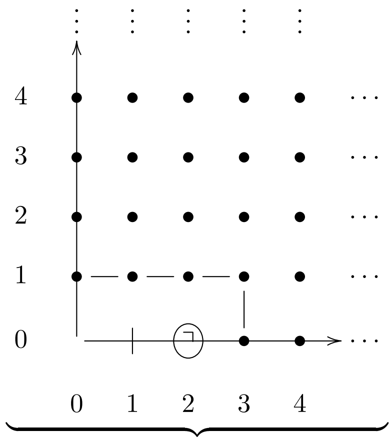
Example 6.2.2. Set $R = A[X, Y]$ and $\mathfrak{X} = (X, Y)R$. Then we have $\mathfrak{X}^3 = (X^3, X^2Y, XY^2, Y^3)R$. The monomials of total degree 2 in R are X^2, XY, Y^2. Theorem 6.2.1 says that we have

$$\mathfrak{X}^3 = \mathrm{P}_R(X^2) \bigcap \mathrm{P}_R(XY) \bigcap \mathrm{P}_R(Y^2) = (X^3, Y)R \bigcap (X^2, Y^2)R \bigcap (X, Y^3)R.$$

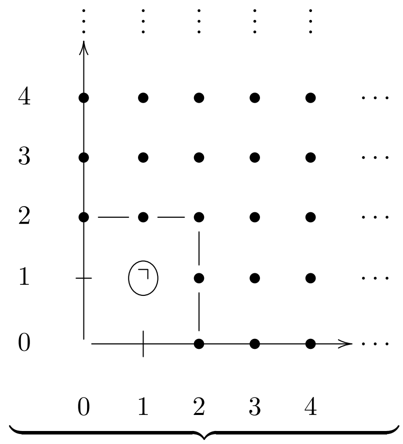
Graphically, we are decomposing the graph $\Gamma(\mathfrak{X}^3)$



according to the monomials in the "corners".

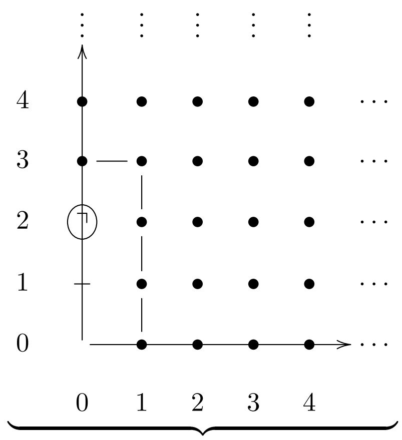


$\Gamma(\mathrm{P}_R(X^2)){=}\Gamma((X^3,Y)R)$



$\Gamma(\mathrm{P}_R(XY)){=}\Gamma((X^2,Y^2)R)$

and



$\Gamma(\mathrm{P}_R(Y^2)){=}\Gamma((X,Y^3)R)$

One can check easily that this decomposition is irredundant. For instance, the monomial X^2 is in $\mathrm{P}_R(XY) \smallsetminus \mathrm{P}_R(X^2)$. See also Exercise 6.1.13, and compare with the results from Section 3.5.

Proof of Theorem 6.2.1. Set $J = \bigcap_{\deg(f)=n-1} \mathrm{P}_R(f)$ where the intersection runs over all monomials $f \in [\![R]\!]$ such that $\deg(f) = n-1$. We show that $J = \mathfrak{X}^n$. Since each ideal $\mathrm{P}_R(f)$ is a monomial ideal, Theorem 2.1.1 implies that J is a monomial ideal. Thus, in order to show that $J = \mathfrak{X}^n$, it suffices to show that $[\![J]\!] = [\![\mathfrak{X}^n]\!]$; see Proposition 1.1.4(b).

To this end, let g be a monomial in $[\![R]\!]$. We show that $g \notin J$ if and only if $g \notin \mathfrak{X}^n$. We have $g \notin J$ if and only if there exists a monomial $f \in [\![R]\!]$ of total degree $n-1$ such that $g \notin \mathrm{P}_R(f)$, by the definition of J, that is, if and only if there exists a monomial $f \in [\![R]\!]$ of total degree $n-1$ such that $f \in (g)R$; see Lemma 6.1.3(b). Exercise 6.2.7 shows that this condition occurs if and only if $\deg(g) < n$, and this is so if and only if $g \notin \mathfrak{X}^n$; see Exercises 1.3.10(d) and A.4.18. It follows that $J = \mathfrak{X}^n$.

To see that the intersection is irredundant, let f and g be distinct monomials with $\deg(f) = n-1 = \deg(g)$. Exercise 6.2.6(d) shows that $f \in \mathrm{P}_R(g)$, so we have $\mathrm{P}_R(g) \not\subseteq \mathrm{P}_R(f)$ by Exercise 6.1.13. $\square$

REMARK 6.2.3. Exercise 1.6.4 shows that the number of monomials in $[\![R]\!]$ of degree $n-1$ is precisely $\binom{d+(n-1)-1}{d-1} = \binom{d+n-2}{d-1}$. This is the number of ideals occurring in the decomposition of $\mathfrak{X}^n$.

Here is a souped up version of Theorem 6.2.1.

THEOREM 6.2.4. *Set $R = A[X_1, \ldots, X_d]$. Fix positive integers $n, t_1, \ldots, t_n$ and set $I = (X_{t_1}, \ldots, X_{t_n})R$. For each $k \geqslant 1$, we have*

$$I^k = \bigcap_{e_1+\cdots+e_n=k+n-1} (X_{t_1}^{e_1}, \ldots, X_{t_n}^{e_n})R$$

where the intersection runs over all sequences $e_1, \ldots, e_n$ of positive integers such that $e_1 + \cdots + e_n = k+n-1$. Furthermore, this intersection is irredundant.

PROOF. Re-order the variables if necessary to assume that $I = (X_1, \ldots, X_n)R$. For simplicity, write $\underline{e} = (e_1, \ldots, e_n)$ and $I_{\underline{e}} = (X_1^{e_1}, \ldots, X_n^{e_n})R$.

First, we verify that $I^k \subseteq \bigcap_{|\underline{e}|=k+n-1} I_{\underline{e}}$. The ideal I^k is generated by monomials of the form $f = X_1^{m_1} \cdots X_n^{m_n}$ such that $m_1 + \cdots + m_n = k$; we need to show that this generator is in each ideal $I_{\underline{e}}$ such that $|\underline{e}| = k+n-1$. Suppose that $f \notin I_{\underline{e}}$. Then we have $e_i > m_i$ for all $i = 1, \ldots, n$. That is, we have $e_i \geqslant m_i + 1$, so

$$k+n-1 = \sum_{i=1}^n e_i \geqslant \sum_{i=1}^n (m_i+1) = \left(\sum_{i=1}^n m_i\right) + n = k+n.$$

This is a contradiction.

Next, we verify the containment $I^k \supseteq \bigcap_{|\underline{e}|=k+n-1} I_{\underline{e}}$. Set $R' = A[X_1, \ldots, X_n] \subseteq R$ and $I' = (X_1, \ldots, X_n)R'$. For each n-tuple $\underline{e}$ such that $|\underline{e}| = k+n-1$, set $I'_{\underline{e}} = (X_1^{e_1}, \ldots, X_n^{e_n})R'$. Let p be the number of n-tuples $\underline{e}$ such that $|\underline{e}| = k+n-1$. (Using Exercise 1.6.4, one can conclude that $p = \binom{k+n-2}{n-1}$.) Let $I_1, \ldots, I_p$ be the distinct ideals of the form $I_{\underline{e}}$, and let $I'_1, \ldots, I'_p$ be the distinct ideals of the form $I'_{\underline{e}}$.

Using an induction argument based on Proposition 2.1.5, one can show that the ideals $\bigcap_{|\underline{e}|=k+n-1} I_{\underline{e}} = \bigcap_{j=1}^p I_j$ and $\bigcap_{|\underline{e}|=k+n-1} I'_{\underline{e}} = \bigcap_{j=1}^p I'_j$ have the same generating sets, namely, the set of all monomials of the form $\operatorname{lcm}(f_1, \ldots, f_p)$ where each f_j is a generator of I_j; see Exercise 2.1.15. Theorem 6.2.1 shows that each of these generators is in $(I')^k \subseteq I^k$, as desired.

Finally, we prove that this intersection $\bigcap_{|\underline{e}|=k+n-1} I_{\underline{e}}$ is irredundant. By way of contradiction, suppose that the intersection is redundant. Then there are n-tuples $\underline{e} \neq \underline{e}'$ such that $I_{\underline{e}} \subseteq I_{\underline{e}'}$. This implies that each generator of $I_{\underline{e}}$ is in $I_{\underline{e}'}$. A comparison of exponent vectors shows that this implies that $e_i \geqslant e'_i$ for $i = 1, \ldots, n$. The assumption that $\underline{e} \neq \underline{e}'$ then implies that we have $e_i > e'_i$ for some i, so

$$k+n-1 = |\underline{e}| > |\underline{e}'| = k+n-1$$

a contradiction. $\square$

Exercises.

EXERCISE 6.2.5. Set $R = A[X, Y, Z]$. Use Theorem 6.2.1 to find an irredundant parametric decomposition of $((X,Y,Z)R)^4$. Justify your answer.

*EXERCISE 6.2.6. Set $R = A[X_1, \ldots, X_d]$. Let f and g be monomials in R.

(a) Prove that if $f \in (g)R$, then $\deg(f) \geqslant \deg(g)$.
(b) Prove or disprove: If $\deg(f) \geqslant \deg(g)$, then $f \in (g)R$.
(c) Prove that if $\deg(f) = \deg(g)$ and $g \in (f)R$, then $g = f$.
(d) Prove that if $\deg(f) = \deg(g)$ and $f \neq g$, then $f \in \mathrm{P}_R(g)$.

(This exercise is used in the proof of Theorem 6.2.1.)

*EXERCISE 6.2.7. Set $R = A[X_1, \ldots, X_d]$. Let f be a monomial in R and let n be an integer such that $n \geqslant 1$. Prove that $\deg(f) < n$ if and only if there exists a monomial g of degree $n-1$ such that $g \in (f)R$. (This exercise is used in the proof of Theorem 6.2.1.)

EXERCISE 6.2.8. Set $R = A[X_1, \ldots, X_d]$, and let $f = \underline{X}^{\underline{a}} \in \llbracket R \rrbracket$.

(a) Prove that for each integer $n \geqslant 1$, we have
$$\mathrm{P}_R(f)^n = \bigcap_{|\underline{m}|=n-1} \mathrm{P}_R(X_1^{a_1 m_1 + a_1 + m_1} \cdots X_d^{a_d m_d + a_d + m_d})$$
where the intersection runs over all d-tuples $\underline{m} \in \mathbb{N}^d$ such that $+\underline{m}| = n - 1$.
(b) Prove that this intersection is irredundant.
(c) Set $R = A[X, Y]$ and $I = (X^2, Y^3)R$. Use parts (a)–(b) to find an irredundant m-irreducible decomposition of the ideal I^3. Justify your answer.
(d) Verify that your decomposition from part (c) is correct as in Exercise 4.3.11(d).

EXERCISE 6.2.9. Set $R = A[X_1, \ldots, X_d]$. Fix integers $n, t_1, \ldots, t_n, e_1, \ldots, e_n \geqslant 1$, and set $I = (X_{t_1}^{e_1}, \ldots, X_{t_n}^{e_n})R$.

(a) Describe an irredundant m-irreducible decomposition of I^k. Justify your answer. (Hint: Mimic the proof of Theorem 6.2.4, using Exercise 6.2.8 in place of Theorem 6.2.1.)
(b) Set $R = A[X, Y, Z]$ and $I = (X^2, Z^3)R$. Use part (a) to find an irredundant m-irreducible decomposition of the ideal I^3. Justify your answer.
(c) Verify that your decomposition from part (b) is correct as in Exercise 4.3.11(d).

An Example in Macaulay2.

Exercises.

6.3. Corner Elements

In this section, A is a non-zero commutative ring with identity.

This section contains an explicit formula for computing irredundant parametric decomposition; see Theorem 6.3.5. The formula uses the next definition.

DEFINITION 6.3.1. Set $R = A[X_1, \ldots, X_d]$. Let J be a monomial ideal in R. A monomial $z \in \llbracket R \rrbracket$ is a *J-corner element* if $z \notin J$ and $X_1 z, \ldots, X_d z \in J$. The set of J-corner elements of J in $\llbracket R \rrbracket$ is denoted $\mathrm{C}_R(J)$.

The next three results contain tools for the proof of Theorem 6.3.5.

PROPOSITION 6.3.2. *Set $R = A[X_1, \ldots, X_d]$. Set $\mathfrak{X} = (X_1, \ldots, X_d)R$ and let J be a monomial ideal in R.*

(a) *The J-corner elements are precisely the monomials in $(J :_R \mathfrak{X}) \smallsetminus J$, in other words, we have $\mathrm{C}_R(J) = \llbracket (J :_R \mathfrak{X}) \rrbracket \smallsetminus \llbracket J \rrbracket$.*

(b) *If z and z' are distinct J-corner elements, then $z \notin (z')R$ and $z' \notin (z)R$.*
(c) *The set $\mathrm{C}_R(J)$ is finite.*

PROOF. (a) This follows from Proposition A.5.3(b).

(b) Assume that z and z' are distinct J-corner elements and suppose that $z \in (z')R$. It follows that there is a monomial $f \in [\![R]\!]$ such that $z = fz'$. Since $z \neq z'$, we conclude that $f \neq 1$. Since f is a monomial, it follows that $f \in \mathfrak{X}$. By part (a), we have $z' \in (J :_R \mathfrak{X})$, so the condition $f \in \mathfrak{X}$ implies that $z = fz' \in J$. This contradicts the condition $z \in \mathrm{C}_R(J)$, and so the condition $z \in (z')R$ must be false. Similarly, we conclude that $z' \notin (z)R$ as desired.

(c) The ideal $K = (\mathrm{C}_R(J))R$ is a monomial ideal, so Theorem 1.3.1 implies that K is generated by a finite list of monomials $z_1, \ldots, z_n \in \mathrm{C}_R(J)$. We claim that $\{z_1, \ldots, z_n\} = \mathrm{C}_R(J)$. The containment $\{z_1, \ldots, z_n\} \subseteq \mathrm{C}_R(J)$ holds by assumption. For the reverse containment, let $z' \in \mathrm{C}_R(J)$. Then we have $z' \in \mathrm{C}_R(J) \subseteq K = (z_1, \ldots, z_n)R$, so z' is a monomial multiple of z_j for some index j. Part (b) implies $z' = z_j$, as desired. $\square$

COROLLARY 6.3.3. *Set $R = A[X_1, \ldots, X_d]$. Set $\mathfrak{X} = (X_1, \ldots, X_d)R$ and let J be a monomial ideal in R. Let $z_1, \ldots, z_m$ be the distinct J-corner elements and set $J' = \mathrm{P}_R(z_1) \bigcap \cdots \bigcap \mathrm{P}_R(z_m)$.*
(a) *For $i = 1, \ldots, m$ we have $(z_1, \ldots, z_{i-1}, z_{i+1}, \ldots, z_m)R \subseteq \mathrm{P}_R(z_i)$ and $z_i \notin \mathrm{P}_R(z_i)$ and $z_i \notin J'$.*
(b) *The intersection $J' = \bigcap_{i=1}^m \mathrm{P}_R(z_i)$ is irredundant.*
(c) *There is a containment $J \subseteq J'$.*

PROOF. (a) The condition $z_i \notin \mathrm{P}_R(z_i)$ is from Lemma 6.1.3(b). From this, the special case $m = 1$ is straightforward, so we assume that $m \geqslant 2$. For indices i and j such that $j \neq i$, we have $z_i \neq z_j$, so $z_i \notin (z_j)R$ by Proposition 6.3.2(b); it follows that $z_j \in \mathrm{P}_R(z_i)$ by Lemma 6.1.3(b). We conclude that $z_1, \ldots, z_{i-1}, z_{i+1}, \ldots, z_m \in \mathrm{P}_R(z_i)$ so $(z_1, \ldots, z_{i-1}, z_{i+1}, \ldots, z_m)R \subseteq \mathrm{P}_R(z_i)$.

The condition $z_i \notin J'$ follows because $J' \subseteq \mathrm{P}_R(z_i)$.

(b) This follows from part (a) because $z_i \in \bigcap_{j \neq i} \mathrm{P}_R(z_j)$ and $z_i \notin \mathrm{P}_R(z_i)$.

(c) Exercise 6.3.17(c). $\square$

PROPOSITION 6.3.4. *Set $R = A[X_1, \ldots, X_d]$. Set $\mathfrak{X} = (X_1, \ldots, X_d)R$, and let I be a monomial ideal in R such that* $\text{m-rad}\,(I) = \mathfrak{X}$.
(a) *If $f \in [\![R]\!] \smallsetminus [\![I]\!]$, then there is a monomial $g \in [\![R]\!]$ such that $fg \in \mathrm{C}_R(I)$.*
(b) *$\mathrm{C}_R(I) \neq \emptyset$.*
(c) *Given a monomial ideal $J \subseteq R$ such that $J \not\subseteq I$ one has $\mathrm{C}_R(I) \bigcap J \neq \emptyset$.*

PROOF. (a) Set $S = [\![R]\!] \smallsetminus [\![I]\!]$ which is a finite set by Exercise 1.1.21. Set

$$T = \{g \in [\![R]\!] \mid fg \notin I\}.$$

If $g \in T$, then $g \notin I$ since $fg \notin I$ and I is an ideal. It follows that $T \subseteq S$, so T is a finite set. Let g be a monomial in T with maximal degree. By the maximality of $\deg(g)$, we have $X_i g \notin T$ for $i = 1, \ldots, d$. In other words, we have $X_i fg \in I$ for $i = 1, \ldots, d$. This says that $fg \in (I :_R \mathfrak{X})$, so the condition $fg \notin I$ implies that $fg \in \mathrm{C}_R(I)$, as desired.

(b) Since $\text{m-rad}\,(I) = \mathfrak{X}$, we have $I \neq R$ by Exercise A.4.18 and Proposition 2.3.3(2.3.3). In particular, $f = 1 \in [\![R]\!] \smallsetminus [\![I]\!]$ so part (a) provides a monomial $g \in [\![R]\!]$ such that $g = 1g \in \mathrm{C}_R(I)$.

(c) Fix a monomial $f \in [\![J]\!] \smallsetminus [\![I]\!]$. Part (a) implies that there is a monomial $g \in [\![R]\!]$ such that $fg \in \mathrm{C}_R(I)$. Since J is an ideal and $f \in J$, we have $fg \in J$, and so $fg \in \mathrm{C}_R(I) \bigcap J$. $\square$

Now we are ready to describe irredundant parametric decompositions in terms of corner elements.

THEOREM 6.3.5. *Set $R = A[X_1, \ldots, X_d]$. Set $\mathfrak{X} = (X_1, \ldots, X_d)R$ and let J be a monomial ideal of R such that* m-rad$(J) = \mathfrak{X}$. *If the distinct J-corner elements are $z_1, \ldots, z_m$ then $J = \bigcap_{j=1}^m \mathrm{P}_R(z_j)$ is an irredundant parametric decomposition of J.*

PROOF. Note first that Proposition 6.3.4 shows that J has a corner element. Set $J' = \bigcap_{j=1}^m \mathrm{P}_R(z_j)$. Corollary 6.3.3 implies that this intersection is irredundant and that $J' \subseteq J$. Thus, it remains to show that $J' \supseteq J$. Since each $\mathrm{P}_R(z_j)$ is a monomial ideal, Theorem 2.1.1 implies that J' is a monomial ideal. Suppose by way of contradiction that $J' \subsetneq J$. Proposition 6.3.4(c) implies that J' contains an J-corner element, say $z_i \in J'$. This implies that $z_i \in \mathrm{P}_R(z_i)$, which contradicts Lemma 6.1.3(a). $\square$

Theorem 6.3.5 shows that the J-corner elements determine an irredundant parametric decomposition of J. The next result is the reverse: an irredundant parametric decomposition of J determines the J-corner elements.

PROPOSITION 6.3.6. *Set $R = A[X_1, \ldots, X_d]$. Fix monomials $z_1, \ldots, z_m \in [\![R]\!]$ and assume that $J = \bigcap_{j=1}^m \mathrm{P}_R(z_j)$ is an irredundant parametric decomposition of J. Then the distinct J-corner elements are $z_1, \ldots, z_m$.*

PROOF. Claim 1: Each z_i is a J-corner element. First, note that $z_i \notin \mathrm{P}_R(z_i)$ by Lemma 6.1.3(a); it follows that $z_i \notin J$ since $J = \bigcap_{j=1}^m \mathrm{P}_R(z_j) \subseteq \mathrm{P}_R(z_i)$. To complete the proof of the claim, we need to show that $X_j z_i \in J$ for each j. By way of contradiction, suppose that $X_j z_i \notin J$. It follows that $X_j z_i \notin \mathrm{P}_R(z_k)$ for some k. Lemma 6.1.3(b) implies that $z_k \in (X_j z_i)R \subseteq (z_i)R$. Exercise 6.1.13 implies that $\mathrm{P}_R(z_k) \subseteq \mathrm{P}_R(z_i)$. The irredundancy of the intersection implies that $\mathrm{P}_R(z_k) = \mathrm{P}_R(z_i)$, so $i = k$. The condition $z_k \in (X_j z_i)R$ then reads as $z_k \in (X_j z_k)R$. A degree argument shows that this is impossible. Thus we must have $X_j z_i \in J$ for each i and j, so each $z_i \in \mathrm{C}_R(J)$, as claimed.

Claim 2: The elements $z_1, \ldots, z_m$ are distinct. Indeed, if $z_i = z_j$, then $\mathrm{P}_R(z_i) = \mathrm{P}_R(z_j)$, so the irreduncancy of the intersection implies that $i = j$.

Claim 3: $\mathrm{C}_R(J) \subseteq \{z_1, \ldots, z_m\}$. (Once this claim is established, the proof is complete.) Let $z \in \mathrm{C}_R(J)$. This implies that $z \notin J$, and so there is an index k such that $z \notin \mathrm{P}_R(z_k)$. Lemma 6.1.3(b) implies that $z_k \in (z)R$, so Proposition 6.3.2(b) says that $z = z_k$. This establishes the claim. $\square$

The next result says that the only m-irreducible monomial ideals with monomial radical equal to $\mathfrak{X}$ are the parameter ideals.

COROLLARY 6.3.7. *Set $R = A[X_1, \ldots, X_d]$. Set $\mathfrak{X} = (X_1, \ldots, X_d)R$ and let J be a monomial ideal in R such that* m-rad$(J) = \mathfrak{X}$.

(a) *For each monomial $z \in [\![R]\!]$ we have $\mathrm{C}_R(\mathrm{P}_R(z)) = \{z\}$.*
(b) *The following conditions are equivalent:*
   (i) *the ideal J is m-irreducible;*

(ii) *the ideal J is a parameter ideal; and*
(iii) *there is precisely one J-corner element.*

PROOF. (a) The trivial intersection $J = \mathrm{P}_R(z)$ is an irredundant parametric decomposition, so Proposition 6.3.6 implies that $\mathrm{C}_R(\mathrm{P}_R(z)) = \mathrm{C}_R(J) = \{z\}$.

(b) The equivalence (i) $\iff$ (ii) is from Proposition 6.1.7. The implication (ii) $\Longrightarrow$ (iii) follows from part (a).

(iii) $\Longrightarrow$ (ii): Assume that there is precisely one J-corner element w. Then the decomposition $J = \bigcap_{z \in \mathrm{C}_R(J)} \mathrm{P}_R(z)$ from Theorem 6.3.5 reads as $J = \mathrm{P}_R(w)$, so J is a parameter ideal. □

Checking that a given parametric decomposition is irredundant can be tedious. Imagine how it goes in three or more variables when there is no good visual to help guide you. The next proposition makes it a lot easier.

PROPOSITION 6.3.8. *Set $R = A[X_1, \ldots, X_d]$. Fix monomials $z_1, \ldots, z_m \in [\![R]\!]$ and set $I = \bigcap_{j=1}^m \mathrm{P}_R(z_j)$. The following conditions are equivalent:*

(i) *the intersection $\bigcap_{j=1}^m \mathrm{P}_R(z_j)$ is irredundant; and*
(ii) *for all indices i and j, if $i \neq j$, then $z_i \notin (z_j)R$.*

PROOF. Exercise 6.1.13. □

EXAMPLE 6.3.9. Set $R = A[X, Y]$ and

$$\begin{aligned} J &= (X^3, Y^6)R \bigcap (X^4, Y^4)R \bigcap (X^5, Y^2)R \\ &= \mathrm{P}_R(X^2Y^5) \bigcap \mathrm{P}_R(X^3Y^3) \bigcap \mathrm{P}_R(X^4Y). \end{aligned}$$

To show that the intersection is irredundant, it suffices (by Proposition 6.3.8) to observe that no monomial in the list X^2Y^5, X^3Y^3, X^4Y is a monomial multiple of any other monomial in this list.

Proposition 6.3.8 and Exercise 6.1.13 combine to give the following algorithm for transforming redundant parametric intersections into irredundant parametric intersections.

ALGORITHM 6.3.10. Set $R = A[X_1, \ldots, X_d]$. Fix monomials $z_1, \ldots, z_m \in [\![R]\!]$ and set $I = \bigcap_{j=1}^m \mathrm{P}_R(z_j)$. We assume that $m \geqslant 1$.

Step 1. Check whether the intersection $\bigcap_{j=1}^m \mathrm{P}_R(z_j)$ is irredundant using Proposition 6.3.8.

Step 1a. If, for all indices i and j such that $i \neq j$, we have $z_j \notin (z_i)R$, then the intersection is irredundant; in this case, the algorithm terminates.

Step 1b. If there exist indices i and j such that $i \neq j$ and $z_j \in (z_i)R$, then the intersection is redundant; in this case, continue to Step 2.

Step 2. Reduce the intersection by removing the parameter ideal which causes the redundancy in the intersection. By assumption, there exist indices i and j such that $i \neq j$ and $z_j \in (z_i)R$. Reorder the indices to assume without loss of generality that $i = m$. Thus, we have $j < m$ and $z_j \in (z_m)R$. Exercise 6.1.13 implies that $\mathrm{P}_R(z_j) \subseteq \mathrm{P}_R(z_m)$, and it follows that $I = \bigcap_{j=1}^m \mathrm{P}_R(z_j) = \bigcap_{j=1}^{m-1} \mathrm{P}_R(z_j)$. Now apply Step 1 to the new list of monomials $z_1, \ldots, z_{m-1}$.

The algorithm will terminate in at most $m - 1$ steps because one can remove at most $m - 1$ monomials from the list and still form an ideal that is a non-empty intersection of parameter ideals.

EXAMPLE 6.3.11. Set $R = A[X, Y]$ and

$$\begin{aligned} J &= (X, Y^5)R \bigcap (X^2, Y^3)R \bigcap (X^4, Y^4)R \bigcap (X^3, Y)R \bigcap (X^5, Y^2)R \\ &= \mathrm{P}_R(Y^4) \bigcap \mathrm{P}_R(XY^2) \bigcap \mathrm{P}_R(X^3Y^3) \bigcap \mathrm{P}_R(X^2) \bigcap \mathrm{P}_R(X^4Y). \end{aligned}$$

The list of z_i's to consider is $Y^4, XY^2, X^3Y^3, X^2, X^4Y$.

The monomial X^3Y^3 is a multiple of XY^2, so we remove XY^2 from the list.

The new list of z_i's to consider is Y^4, X^3Y^3, X^2, X^4Y.

The monomial X^4Y is a multiple of X^2, so we remove X^2 from the list.

The new list of z_i's to consider is Y^4, X^3Y^3, X^4Y. No monomial in the list is a multiple of another since the exponent vectors $(0, 4)$, $(3, 3)$ and $(4, 1)$ are incomparable. Hence, the intersection

$$J = \mathrm{P}_R(Y^4) \bigcap \mathrm{P}_R(X^3Y^3) \bigcap \mathrm{P}_R(X^4Y) = (X, Y^5)R \bigcap (X^4, Y^4)R \bigcap (X^5, Y^2)R.$$

is an irredundant parametric decomposition of J.

Here is a one-step procedure for transforming redundant parametric intersections into irredundant parametric intersections.

PROPOSITION 6.3.12. *Set $R = A[X_1, \ldots, X_d]$, and let $m \geqslant 1$. Fix distinct monomials $z_1, \ldots, z_m \in [\![R]\!]$, and set $I = \bigcap_{j=1}^m \mathrm{P}_R(z_j)$. For $j = 1, \ldots, m$ write $z_j = \underline{X}^{\underline{n}_j}$ with $\underline{n}_j \in \mathbb{N}^d$. Set $\Delta = \{\underline{n}_1, \ldots, \underline{n}_m\} \subseteq \mathbb{N}^d$ and consider the order $\succcurlyeq$ on $\mathbb{N}^d$ from Definition A.7.8. Let Δ' denote the set of maximal elements of Δ under this order. Then $I = \bigcap_{\underline{n}_j \in \Delta'} \mathrm{P}_R(z_j)$ is an irredundant parametric decomposition of I and $\mathrm{C}_R(I) = \{z_j \mid \underline{n}_j \in \Delta'\} \subseteq \{z_1, \ldots, z_n\}$.*

PROOF. Note that the set Δ has maximal elements since Δ is finite; see Proposition 6.3.2(c).

The maximality of the elements of Δ' implies that for each $\underline{n}_i \in \Delta$, there is an element $\underline{n}_j \in \Delta'$ such that $\underline{n}_j \succcurlyeq \underline{n}_i$. It follows that $z_j \in (z_i)R$ and so Exercise 6.1.13 implies that $\mathrm{P}_R(z_j) \subseteq \mathrm{P}_R(z_i)$. From this, we conclude that $I = \bigcap_{\underline{n}_j \in \Delta'} \mathrm{P}_R(z_j)$. (Note that we are using the following straightforward fact from set-theory: If $S_1, \ldots, S_n$ are subsets of a fixed set T, and i, j are indices such that $i \neq j$ and $S_i \subseteq S_j$, then $\bigcap_{k=1}^n S_k = \bigcap_{k \neq j} S_k$.)

For each $\underline{n}_j, \underline{n}_k \in \Delta'$ such that $j \neq k$, we have $\underline{n}_j \not\succcurlyeq \underline{n}_k$ since $\underline{n}_j$ and $\underline{n}_k$ are both maximal among the elements of Δ and they are distinct. It follows that $z_j \notin (z_k)R$ and so $\mathrm{P}_R(z_k) \not\subseteq \mathrm{P}_R(z_j)$. Proposition 6.3.8 then implies that the intersection $I = \bigcap_{\underline{n}_j \in \Delta'} \mathrm{P}_R(z_j)$ is irredundant, and the equality $\mathrm{C}_R(I) = \{z_j \mid \underline{n}_j \in \Delta'\}$ comes from Proposition 6.3.6. □

EXAMPLE 6.3.13. Set $R = A[X, Y]$. Set

$$\begin{aligned} J &= (X, Y^5)R \bigcap (X^2, Y^3)R \bigcap (X^4, Y^4)R \bigcap (X^3, Y)R \bigcap (X^5, Y^2)R \\ &= \mathrm{P}_R(Y^4) \bigcap \mathrm{P}_R(XY^2) \bigcap \mathrm{P}_R(X^3Y^3) \bigcap \mathrm{P}_R(X^2) \bigcap \mathrm{P}_R(X^4Y). \end{aligned}$$

The list of exponent vectors is $\Delta = \{(0, 4), (1, 2), (3, 3), (2, 0), (4, 1)\}$. The list of maximal elements in Δ is $\Delta' = \{(0, 4), (3, 3), (4, 1)\}$. Hence, the intersection

$$J = \mathrm{P}_R(Y^4) \bigcap \mathrm{P}_R(X^3Y^3) \bigcap \mathrm{P}_R(X^4Y) = (X, Y^5)R \bigcap (X^4, Y^4)R \bigcap (X^5, Y^2)R.$$

is an irredundant parametric decomposition of J. Compare this to Example 6.3.11.

Exercises.

EXERCISE 6.3.14. Set $R = A[X_1, \ldots, X_d]$ with $d \geqslant 2$. Let f be a monomial in $[\![R]\!]$ and prove that $\mathrm{C}_R((f)R) = \emptyset$.

EXERCISE 6.3.15. Set $R = A[X_1, \ldots, X_d]$ and $\mathfrak{X} = (X_1, \ldots, X_d)R$. Let J be a monomial ideal in R, and prove that the following conditions are equivalent:

(i) $1 \in \mathrm{C}_R(J)$;
(ii) $J = \mathfrak{X}$; and
(iii) $\mathrm{C}_R(J) = \{1\}$.

EXERCISE 6.3.16. Set $R = A[X_1, \ldots, X_d]$. Let J be a monomial ideal in R, and fix a monomial $f = \underline{X}^{\underline{n}} \in [\![R]\!]$. For $i = 1, \ldots, d$ set $\underline{e_i} = (0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{N}^d$ where the 1 occurs in the ith position. Prove that f is a J-corner element if and only if $\underline{n} \notin \Gamma(J)$ and $\underline{n} + \underline{e_i} \in \Gamma(J)$ for each $i = 1, \ldots, d$.

*EXERCISE 6.3.17. Set $R = A[X_1, \ldots, X_d]$. Let J be a monomial ideal in R, and fix a monomial $w \in [\![R]\!]$.

(a) Prove that if $w \notin J$, then $J \subseteq \mathrm{P}_R(w)$.
(b) Prove that if w is a J-corner element, then $J \subsetneq \mathrm{P}_R(w)$.
(c) In the notation of Corollary 6.3.3, prove that $J \subseteq J'$.

(This exercise is used in the proof of Corollary 6.3.3.)

EXERCISE 6.3.18. Set $R = A[X, Y]$ and $\mathfrak{X} = (X, Y)R$. Find monomial ideals I and J in R such that $\mathrm{rad}\,(I) = \mathrm{rad}\,(\mathfrak{X}) = \mathrm{rad}\,(J)$ and $I \subseteq J$ and $\mathrm{C}_R(I) \bigcap \mathrm{C}_R(J) = \emptyset$; in particular, such an example has $\mathrm{C}_R(I) \not\subseteq \mathrm{C}_R(J)$ and $\mathrm{C}_R(I) \not\supseteq \mathrm{C}_R(J)$.

EXERCISE 6.3.19. Set $R = A[X, Y, Z]$. Consider the monomial ideal

$$J = (Z^4, Y^2Z^3, Y^3, XYZ, XY^2, X^2)R$$

and set $f = X$. Show that $f \notin J$ and find a monomial g such that $fg \in \mathrm{C}_R(I)$. (See Proposition 6.3.4(c).) Justify your answer.

EXERCISE 6.3.20. Set $R = A[X_1, \ldots, X_d]$ and $\mathfrak{X} = (X_1, \ldots, X_d)R$. Let I be a monomial ideal in R. Prove that if $I \subsetneq \mathfrak{X}$, then $\mathrm{C}_R(I) \subseteq \text{m-rad}\,(I)$.

EXERCISE 6.3.21. Set $R = A[X, Y, Z]$. Set

$$I = (X^2, Y, Z)R \bigcap (X, Y^2, Z)R \bigcap (X^3, Y, Z^2)R \bigcap (X, Y^2, Z^3)R \bigcap (X^2, Y^2, Z^2)R.$$

(a) Find a finite set $\{z_1, \ldots, z_m\}$ of monomials such that
$$I = \mathrm{P}_R(z_1) \bigcap \cdots \bigcap \mathrm{P}_R(z_m).$$
(b) Find an irredundant parametric decomposition for I and list the I-corner elements using:
   (1) Algorithm 6.3.10.
   (2) Proposition 6.3.12.

Justify your answers.

*EXERCISE 6.3.22. Set $R = A[X_1, \ldots, X_d]$. Set $\mathfrak{X} = (X_1, \ldots, X_d)R$ and let J be a monomial ideal in R such that $J \subseteq \mathfrak{X}$. Let $z_1, \ldots, z_m$ be the distinct J-corner elements. Prove that $(J :_R \mathfrak{X}) = (z_1, \ldots, z_m)R + J$. (This exercise is used in the proof of Lemma 7.4.6.)

*EXERCISE 6.3.23. Set $R = A[X_1, \ldots, X_d]$ and $\mathfrak{X} = (X_1, \ldots, X_d)R = \mathrm{P}_R(1)$.

(a) Prove that $\mathrm{C}_R(\mathfrak{X}^n) = \mathfrak{X}^{n-1} \smallsetminus \mathfrak{X}^n$ for each integer $n \geqslant 1$.

(b) For each monomial $f \in [\![R]\!]$ and each integer $n \geqslant 1$, explicitly describe the set $\mathrm{C}_R(\mathrm{P}_R(f)^n)$ as in part (a). Justify your answer.

(This exercise is used in Example 7.5.6.)

Corner Elements in Macaulay2.

Exercises.

6.4. Finding Corner Elements in Two Variables

In this section, A is a non-zero commutative ring with identity.

In this section we show how to find corner elements, and hence irredundant m-irreducible decompositions, for monomial ideals in two variables. The outcomes are the same as for Section 3.5, but with different proofs. The results are based on the following order.

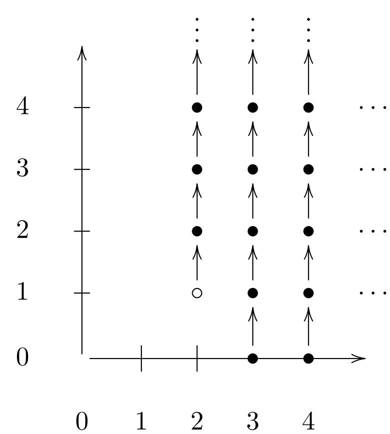
DEFINITION 6.4.1. Set $R = A[X, Y]$. We define the *lexicographical order* on the set of monomials $[\![R]\!]$ as follows: For monomials $f = X^aY^b$ and $g = X^cY^d$ write $f <_{\mathrm{lex}} g$ if either $(a < c)$ or $(a = c$ and $b < d)$. We also write $f \leqslant_{\mathrm{lex}} g$ if either $f <_{\mathrm{lex}} g$ or $f = g$.

REMARK 6.4.2. Set $R = A[X, Y]$. The order $<_{\mathrm{lex}}$ is called "lexicographical" because it is modeled on the order of words in the dictionary. (The word "lexicon" means "dictionary".)

EXAMPLE 6.4.3. Set $R = A[X, Y]$. We have $X^2Y^3 <_{\mathrm{lex}} X^3Y^2$ because of the X-exponents. We also have $X^2Y^3 <_{\mathrm{lex}} X^2Y^5$. The monomials in $[\![R]\!]$ can be listed in order as follows:

$$1 <_{\mathrm{lex}} Y <_{\mathrm{lex}} Y^2 <_{\mathrm{lex}} Y^3 <_{\mathrm{lex}} \cdots X <_{\mathrm{lex}} XY <_{\mathrm{lex}} XY^2 <_{\mathrm{lex}} XY^3 <_{\mathrm{lex}} \cdots .$$

We can visualize this order graphically as follows. Given a monomial $f \in [\![R]\!]$, the monomials $g \in [\![R]\!]$ such that $f <_{\mathrm{lex}} g$ are exactly the monomials represented by points that are to the right of f or directly above f.



In the graph, we have represented the order with sequential vertical arrows.

FACT 6.4.4. Set $R = A[X,Y]$. The lexicographical order $\leqslant_{\text{lex}}$ on $[\![R]\!]$ is a total order; see Definition A.7.6. Moreover, it is a well-order, that is, a total order such that every non-empty subset of $[\![R]\!]$ has a unique minimal element. Also, given monomials $f, g \in [\![R]\!]$ we have $f <_{\text{lex}} g$ if and only if $f \leqslant_{\text{lex}} g$ and $f \neq g$. In particular, for each monomial $f \in [\![R]\!]$ we have $f \not<_{\text{lex}} f$.

The idea for finding parametric decompositions in two variables is to determine the corner elements for a monomial ideal in terms of its generators using the lexicographical order. The next lemma is key for this idea, as we see in the subsequent example and theorem.

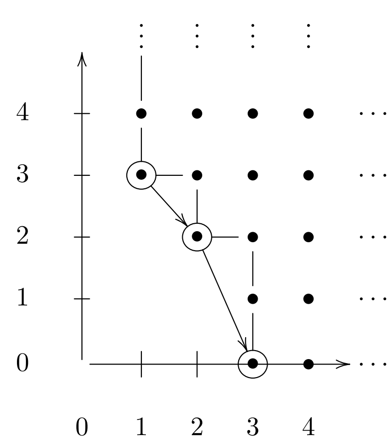
LEMMA 6.4.5. *Set $R = A[X,Y]$. Let J be a non-zero monomial ideal in R and let $f_1, \ldots, f_n \in [\![J]\!]$ be an irredundant monomial generating sequence for J, and assume that $n \geqslant 2$. For $i = 1, \ldots, n$ we write $f_i = X^{a_i}Y^{b_i}$. If $f_i <_{lex} f_j$, then $a_i < a_j$ and $b_i > b_j$.*

PROOF. By definition, the inequality $f_i <_{\text{lex}} f_j$ translates to either $(a_i < a_j)$ or $(a_i = a_j$ and $b_i < b_j)$.

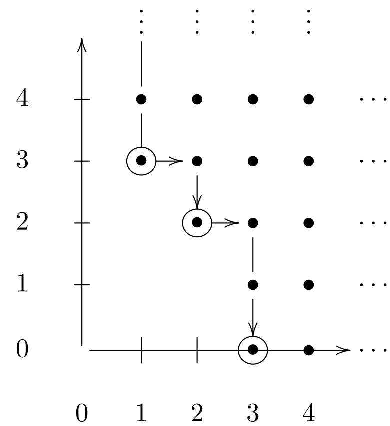
Suppose first that $a_i \geqslant a_j$. The previous paragraph shows that this implies that $a_i = a_j$ and $b_i < b_j$. In other words, in the order on $\mathbb{N}^2$ we have $(a_j, b_j) \succcurlyeq (a_i, b_i)$. It follows that f_j is a monomial multiple of f_i, contradicting the irredundancy of the generating sequence.

Suppose next that $b_i \leqslant b_j$. The condition $a_i < a_j$ that we have already established then implies $(a_j, b_j) \succcurlyeq (a_i, b_i)$, and this again contradicts the irredundancy of the generating sequence. $\square$

EXAMPLE 6.4.6. Set $R = A[X,Y]$, and let J be a monomial ideal in R. Graphically, the previous lemma says that, when the monomials of an irredundant monomial generating sequence for J are arranged in lexicographical order, they form a strictly descending sequence



or, if you like, a strictly descending staircase pattern.



Here is our characterization of the corner elements for a monomial ideal in two variables. Note that the case $n = 1$ is handled in Exercise 6.3.14.

THEOREM 6.4.7. *Set $R = A[X, Y]$. Let J be a non-zero monomial ideal in R and let $f_1, \ldots, f_n \in [\![J]\!]$ be an irredundant monomial generating sequence for J with $n \geqslant 2$. Assume that $f_1 <_{lex} f_2 <_{lex} \cdots <_{lex} f_n$, and for $i = 1, \ldots, n$ write $f_i = X^{a_i}Y^{b_i}$. For $i = 1, \ldots, n-1$ set $z_i = X^{a_{i+1}-1}Y^{b_i-1}$. Then the monomials $z_1, \ldots, z_{n-1}$ are the distinct J-corner elements. Hence J has exactly $n - 1$ corner elements.*

PROOF. First, we note that, since the generating sequence $f_1, \ldots, f_n$ is irredundant, we have $f_i \neq f_j$ whenever $i \neq j$. It follows from Fact 6.4.4 that we have either $f_i <_{\text{lex}} f_j$ or $f_j <_{\text{lex}} f_i$ whenever $i \neq j$. Thus, we may always re-order the list $f_1, \ldots, f_n$ to assume that $f_1 <_{\text{lex}} f_2 <_{\text{lex}} \cdots <_{\text{lex}} f_n$.

By Lemma 6.4.5, the inequality $f_i <_{\text{lex}} f_j$ for $i < j$ implies that

$$(6.4.7.1) \qquad a_i < a_j \qquad \text{and} \qquad b_i > b_j \qquad \text{when } i < j.$$

In particular, the inequalities $0 \leqslant a_1 < a_j$ for $j \geqslant 2$ imply that $1 \leqslant a_j$ when $j \geqslant 2$, and the inequalities $0 \leqslant b_n < b_i$ for $i < n$ imply that $1 \leqslant b_i$ when $i < n$.

Claim 1: For $i = 1, \ldots, n-1$ we have $z_i \notin J$. Suppose by way of contradiction that $z_i \in J$. Theorem 1.1.8 then implies that z_i is a monomial multiple of f_j for some j. Comparing exponents, we have $a_{i+1} - 1 \geqslant a_j$ and $b_i - 1 \geqslant b_j$. If $j \leqslant i$, then this implies the first inequality in the following sequence

$$b_i - 1 \geqslant b_j \geqslant b_i$$

while the second inequality is from (6.4.7.1); this is impossible. If $j > i$, then we have $j \geqslant i + 1$, so similar reasoning explains the sequence

$$a_{i+1} - 1 \geqslant a_j \geqslant a_{i+1}$$

which is also impossible. This establishes the claim.

Claim 2: For $i = 1, \ldots, n-1$ we have $z_i \in \mathrm{C}_R(J)$. Since we have already seen that $z_i \notin J$, it suffices to show that $Xz_i, Yz_i \in J$. By construction, we have

$$\begin{aligned} Xz_i &= XX^{a_{i+1}-1}Y^{b_i-1} = X^{a_{i+1}}Y^{b_i-1} = X^{a_{i+1}}Y^{b_{i+1}}Y^{b_i-1-b_{i+1}} \\ &= f_{i+1}Y^{b_i-1-b_{i+1}} \in (f_{i+1})R \subseteq J. \end{aligned}$$

Note that the element $Y^{b_i-1-b_{i+1}}$ is a bona fide element of R because the condition $b_i > b_{i+1}$ implies that $b_i - 1 - b_{i+1} \geqslant 0$. Similarly, we have

$$\begin{aligned} Yz_i &= YX^{a_{i+1}-1}Y^{b_i-1} = X^{a_{i+1}-1}Y^{b_i} = X^{a_i}Y^{b_i}X^{a_{i+1}-1-a_i} \\ &= f_iX^{a_{i+1}-1-a_i} \in (f_i)R \subseteq J. \end{aligned}$$

This establishes the claim.

Claim 3: For indices i, j such that $i \neq j$ we have $z_i \neq z_j$. This comes from a direct comparison of X-exponents when $i < j$: the inequailty $a_i < a_j$ implies that $a_i - 1 < a_j - 1$, so $z_i <_{\text{lex}} z_j$.

Claim 4: For each J-corner element $z \in \mathrm{C}_R(J)$, there is an index i such that $z = z_i$. (Once this claim is established, the proof will be complete.) Write $z = X^aY^b$. We have $z \notin J$ by assumption, and $Xz, Yz \in J$. Suppose by way of contradiction that $z \neq z_i$ for $i = 1, \ldots, n-1$. Since the lexicographical order on $[\![R]\!]$ is a total order, we know that one of the following three cases must occur: $z <_{\text{lex}} z_1$ or $z_i <_{\text{lex}} z <_{\text{lex}} z_{i+1}$ for some $i = 1, \ldots, n-1$ or $z_{n-1} <_{\text{lex}} z$.

Case 1: $z <_{\text{lex}} z_1$. By definition, this condition implies that either $(a < a_2 - 1)$ or $(a = a_2 - 1$ and $b < b_1 - 1)$.

If $a < a_2 - 1$, then $a + 1 < a_2 \leqslant a_i$ for all $i \geqslant 2$. It follows that Xz is not a monomial multiple of f_i for all $i \geqslant 2$. Hence, the condition $Xz \in J$ implies that Xz is a monomial multiple of f_1. This implies that $a_1 \leqslant a + 1$ and $b_1 \leqslant b$. However, since $z \notin J$, we know that z is not a monomial multiple of f_1, and so either $a_1 > a$ or $b_1 > b$. The condition $b_1 \leqslant b$ implies that $b_1 \not> b$, so we must have $a_1 > a$. Hence, we have $a < a_1 \leqslant a + 1$, and so $a_1 = a + 1$. This implies that $a = a_1 - 1 < a_1 \leqslant a_i$ for all $i \geqslant 1$. Comparing X-exponents, we conclude that Yz is not a monomial multiple of any f_i, so $Yz \notin J$, a contradiction.

It follows that we must have $a = a_2 - 1$ and $b < b_1 - 1$. In this case, the Y-exponent of Yz is $b + 1 < b_1$ which shows that Yz is not a monomial multiple of f_1. The X-exponent of Yz is $a_2 - 1 < a_i$ for all $i \geqslant 2$, and this shows that Yz is not a monomial multiple of f_i for $i = 2, \ldots, n$. This shows that $Yz \notin J$, a contradiction. This shows that the condition $z <_{\text{lex}} z_1$ is impossible.

The remaining cases (Case 2: $z_i <_{\text{lex}} z <_{\text{lex}} z_{i+1}$ for some $i = 1, \ldots, n-1$; Case 3: $z_{n-1} <_{\text{lex}} z$) similarly result in contradictions. Thus, the supposition $z \neq z_i$ for $i = 1, \ldots, n-1$ is false. This establishes the claim and completes the proof. $\square$

Example 6.4.8. Set $R = A[X, Y]$. We compute an irredundant parametric decomposition of the monomial ideal $J = (X^6, X^4Y, X^3Y^2, Y^6)R$. The distinct J-corner elements are X^2Y^5, X^3Y, X^5, by Theorem 6.4.7. So, Theorem 6.3.5 yields

$$J = \mathrm{P}_R(X^2Y^5) \bigcap \mathrm{P}_R(X^3Y) \bigcap \mathrm{P}_R(X^5) = (X^3, Y^6)R \bigcap (X^4, Y^2)R \bigcap (X^6, Y)R.$$

Exercises.

Exercise 6.4.9. Verify the decomposition

$$J = (X^3, Y^6)R \bigcap (X^4, Y^2)R \bigcap (X^6, Y)R$$

from Example 6.4.8 as in Exercise 4.3.11(d).

Exercise 6.4.10. Set $R = A[X, Y]$ and $J = (Y^9, XY^7, X^3Y^4, X^5Y^2, X^{11})R$.

(a) Use Theorem 6.4.7 to find the corner elements of J.
(b) Sketch the graph of J and check that your answer from part (a) agrees with the graph.

(c) Use Theorem 6.3.5 to find an irredundant parametric decomposition of J.
(d) Verify that your decomposition from part (c) is correct as in Exercise 4.3.11(d).

Justify your answers.

Exercise 6.4.11. Define a lexicographical order on the monomials $[\![R]\!]$ in the polynomial ring $R = A[X_1, \ldots, X_d]$ in d variables. Prove that this order is a total order. Is it a well-order? Justify your answer.

Finding Corner Elements in Two Variables in Macaulay2.

Exercises.

6.5. Finding Corner Elements in General

In this section, A is a non-zero commutative ring with identity.

The algorithm from the previous extension does not generalize easily to the case of three or more variables. However, the next result covers the case of any number of variables.

Proposition 6.5.1. *Set $R = A[X_1, \ldots, X_d]$. Set $\mathfrak{X} = (X_1, \ldots, X_d)R$, and let I be a monomial ideal in R such that* m-rad$(I) = \mathfrak{X}$. *Set $S = [\![R]\!] \smallsetminus [\![I]\!]$, the set of monomials in R that are not in I, and set $w = \max\{\deg(f) \mid f \in S\}$. For $j = 0, \ldots, w$ set $D_j = \{f \in S \mid \deg(f) = j\}$. For $j = 0, \ldots, w-1$ set*

$$C_j = \{f \in D_j \mid \textit{for } i = 1, \ldots, d \textit{ we have } X_i f \notin D_{j+1}\}$$

and set $C_w = D_w$. Then $\mathrm{C}_R(I)$ is the disjoint union $\mathrm{C}_R(I) = \cup_{j=0}^{w} C_j$.

Proof. Note that $\mathrm{C}_R(I) \neq \emptyset$ by Proposition 6.3.4. Also, the set S is finite by Exercise 1.1.21. In particular, the number w is well-defined as it is the maximum element of a finite set of natural numbers. Also, for $i \neq j$ we have $C_i \bigcap C_j = \emptyset$ because the elements of C_i have different degrees from the elements of C_j.

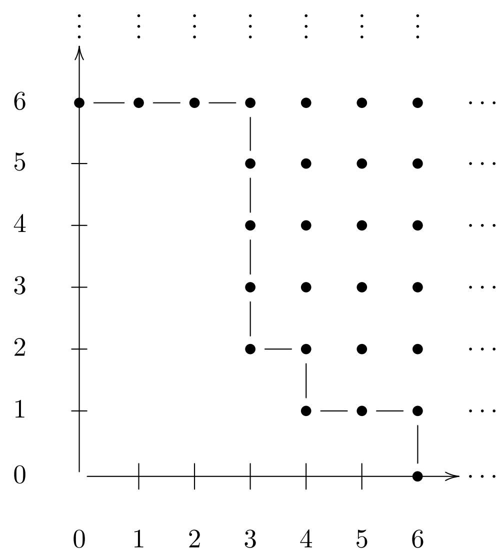
Claim 1: $\cup_{j=0}^{w} C_j \subseteq \mathrm{C}_R(I)$. To verify this containment, we fix a monomial $f \in C_j$ for some j and show that $f \in \mathrm{C}_R(I)$. The containments $C_j \subseteq D_j \subseteq S \subseteq R \smallsetminus I$ show that $f \notin I$. Since $\deg(f) = j$ by definition, we have $\deg(X_i f) = j + 1$ for $i = 1, \ldots, d$.

If $j = w$, then $f \in C_w = D_w$, and so the condition $\deg(X_i f) = j + 1 = w + 1 > w = \max\{\deg(g) \mid g \in S\}$ implies that $X_i f \notin S$ for $i = 1, \ldots, d$. On the other hand, if $j < w$, then $X_i f \notin D_{j+1}$ by definition of C_j, and so the definition of D_{j+1} implies that $X_i f \notin S$. In either case, the elements $X_1 f, \ldots, X_d f$ are monomials of R that are not in $S = [\![R]\!] \smallsetminus [\![I]\!]$. It follows that $X_1 f, \ldots, X_d f \in I$ and so $f \in \mathrm{C}_R(I)$. This establishes the claim.

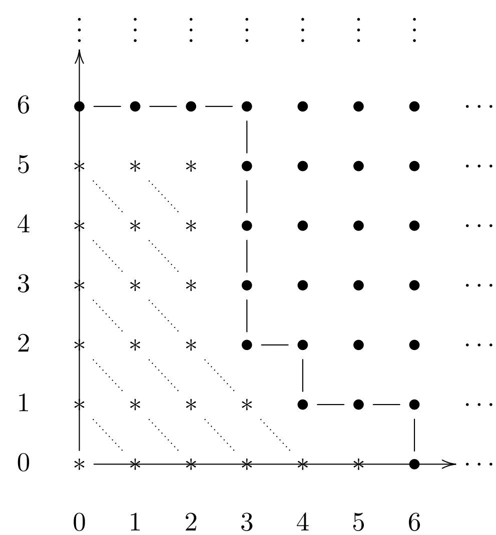
Claim 2: $\cup_{j=0}^{w} C_j \supseteq \mathrm{C}_R(I)$. To verify this containment, we fix a monomial $g \in \mathrm{C}_R(I)$ and set $j = \deg(g)$; we show that $g \in C_j$. The assumption $g \in \mathrm{C}_R(I)$ implies that g is a monomial in R that is not in I, and so $g \in S$. By definition, we have $g \in D_j$. When $j = w$, this implies $g \in C_j$, so we assume that $j < w$. For $i = 1, \ldots, d$ we have $X_i g \in I$ and so $X_i g \notin S$. It follows that $X_i g$ cannot be in D_{j+1}. This shows that $g \in C_j$, thus completing the proof of the claim and the proof of the proposition. □

Here is an example of Proposition 6.5.1 in action.

EXAMPLE 6.5.2. Set $R = A[X, Y]$. Let $J = (X^6, X^4Y, X^3Y^2, Y^6)R$ which has the following graph.



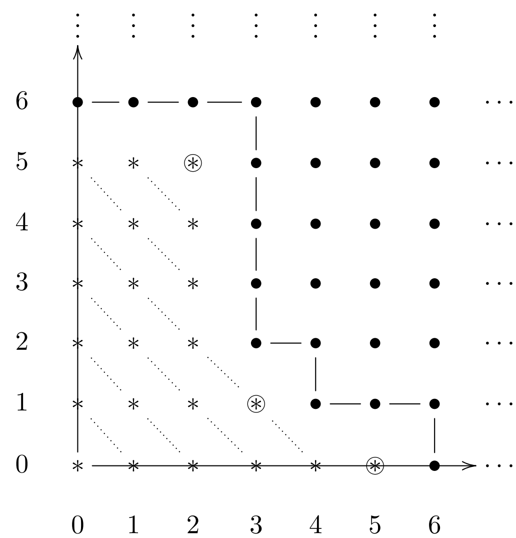
The monomials in the set S are designated with $*$'s, and the elements of D_j are the represented by the $*$'s on the diagonal line of slope -1 and Y-intercept j.



In this example, the set S contains 22 monomials, and the largest degree occurring is $w = 7$. The sets D_j are

$$D_0 = \{1\} \qquad D_1 = \{X, Y\}$$
$$D_2 = \{X^2, XY, Y^2\} \qquad D_3 = \{X^3, X^2Y, XY^2, Y^3\}$$
$$D_4 = \{X^4, X^3Y, X^2Y^2, XY^3, Y^4\} \qquad D_5 = \{X^5, X^2Y^3, XY^4, Y^5\}$$
$$D_6 = \{X^2Y^4, XY^5\} \qquad D_7 = \{X^2Y^5\}.$$

It follows that $C_7 = D_7 = \{X^2Y^5\}$. For $j < w = 7$, the elements of C_j are the monomials of degree j represented by $*$'s such that (a) the point one unit to the right is a $\bullet$, and (b) the point one unit up is a $\bullet$. Such points are designated in the next graph as $\circledast$'s



and so we have

$$\begin{array}{llll} C_0 = \emptyset & C_1 = \emptyset & C_2 = \emptyset & C_3 = \emptyset \\ C_4 = \{X^3Y\} & C_5 = \{X^5\} & C_6 = \emptyset & C_7 = \{X^2Y^5\}. \end{array}$$

It follows that $\mathrm{C}_R(J) = \{X^3Y, X^5, X^2Y^5\}$, so Theorem 6.3.5 yields the following irredundant m-irreducible decomposition

$$J = \mathrm{P}_R(X^3Y) \bigcap \mathrm{P}_R(X^5) \bigcap \mathrm{P}_R(X^2Y^5) = (X^4, Y^2)R \bigcap (X^6, Y)R \bigcap (X^3, Y^6)R.$$

While this gives us a longer algorithm for finding corner elements in the case of two variables, it also works in more than two variables.

Exercises.

Exercise 6.5.3. Verify the decomposition

$$J = (X^4, Y^2)R \bigcap (X^6, Y)R \bigcap (X^3, Y^6)R$$

from Example 6.5.2 as in Exercise 4.3.11(d).

Exercise 6.5.4. Set $R = A[X, Y, Z]$ and

$$J = (Z^4, Y^2Z^3, Y^3, XYZ, XY^2, X^2)R.$$

Use Proposition 6.5.1 to find the J-corner-elements. State the value of w and list the elements in each C_i and D_i. Use Theorem 6.3.5 to find an irredundant parametric decomposition of J. Justify your answers.

Exercise 6.5.5. Set $R = A[U, X, Y, Z]$. Set

$$J = (Z^5, YZ^4, Y^2Z^2, Y^3, XZ^2, XYZ, X^3Z, X^3Y^2, X^4, U)R.$$

Use Proposition 6.5.1 to find the J-corner-elements. State the value of w and list the elements in each C_i and D_i. Use Theorem 6.3.5 to find an irredundant parametric decomposition of J. Justify your answers.

EXERCISE 6.5.6. Set $R = A[U, X, Y, Z]$. Set

$$J = (Z^d, Y^c, X^b, UXYZ, U^a)R$$

where a, b, c, and d are integers that are greater than 1. Use Proposition 6.5.1 to find the J-corner-elements. State the value of w and list the elements in each C_i and D_i. Use Theorem 6.3.5 to find an irredundant parametric decomposition of J. Justify your answers.

Finding Corner Elements in General.

Exercises.

6.6. Exploration: Decompositions in Two Variables, II

In this section, A is a non-zero commutative ring with identity and $R = A[X, Y]$.

This section outlines how to find m-irreducible decompositions for arbitrary monomial ideals in two variables, using the parametric decompositions from Section 6.4.

EXERCISE 6.6.1. Fix a monomial $f = X^a Y^b \in [\![(X, Y)R]\!]$.

(a) Prove that $(f)R = (X^a)R \bigcap (Y^b)R$. This is an m-irreducible decomposition of $(f)R$.
(b) Prove that if $a, b \geqslant 1$, then the decomposition from part (a) is irredundant.
(c) Prove that if $a = 0$ or $b = 0$, then $(f)R$ is m-irreducible, so the trivial intersection $(f)R$ is an irredundant m-irreducible decomposition of $(f)R$.

EXERCISE 6.6.2. Let J be a monomial ideal of R such that $0 \neq J \neq R$, and let $f_1, \ldots, f_n \in [\![J]\!]$ be an irredundant monomial generating sequence for J. Assume that $n \geqslant 2$ and $f_1 <_{\text{lex}} f_2 <_{\text{lex}} \cdots <_{\text{lex}} f_n$. For $i = 1, \ldots, n$ write $f_i = X^{a_i} Y^{b_i}$. For $i = 1, \ldots, n-1$ set $z_i = X^{a_{i+1}-1} Y^{b_i - 1}$; see Theorem 6.4.7.

(a) Compare the graphs of the ideals J and $\bigcap_{i=1}^{n-1} \mathrm{P}_R(z_i)$ in some special cases.
(b) Use part (a) to make a conjecture about an irredundant monomial generating sequence for $\bigcap_{i=1}^{n-1} \mathrm{P}_R(z_i)$. Prove your conjecture. (If you need some help, see Section 3.5.)
(c) Prove that $J = (X^{a_1})R \bigcap (Y^{b_n})R \bigcap \mathrm{P}_R(z_1) \bigcap \cdots \bigcap \mathrm{P}_R(z_{n-1})$. This is an m-irreducible decomposition of J.
(d) Prove that if $a_1, b_n \geqslant 1$, then the decomposition from part (c) is irredundant.
(e) If $a_1 = 0$ or $b_n = 0$, find an irredundant m-irreducible decomposition of J. Justify your answer.

Decompositions in Two Variables in Macaulay2.

Exercises.

Conclusion

Include some history here. Talk about some of the literature from this area.

CHAPTER 7

Computing M-Irreducible Decompositions

The third section of this chapter contains two algorithms for computing m-irreducible decompositions for arbitrary monomial ideals. The remaining sections deal with the following theme: Given monomial ideals I and J, use m-irreducible decompositions $I = \bigcap_{j=1}^n I_j$ and $J = \bigcap_{i=1}^m J_i$ to find m-irreducible decompositions of other ideals obtained from I and J. For instance, the monomial ideal $I \bigcap J$ has m-irreducible decomposition $I \bigcap J = (\bigcap_{j=1}^n I_j) \bigcap (\bigcap_{i=1}^m J_i)$. (Of course, this also works for intersections of more than two ideals.) Note that this decomposition may be redundant, even when the original decompositions are irredundant.

7.1. M-Irreducible Decompositions of Monomial Radicals

In this section, A is a non-zero commutative ring with identity.

Here we show how to use an m-irreducible decomposition of J to find an m-irreducible decomposition of $\text{m-rad}\,(J)$.

PROPOSITION 7.1.1. *Set $R = A[X_1, \ldots, X_d]$. Let I be a monomial ideal of R with m-irreducible decomposition $I = \bigcap_{j=1}^n I_j$.*

(a) *Each ideal* $\text{m-rad}\,(I_j)$ *is m-irreducible.*
(b) *An m-irreducible decomposition of* $\text{m-rad}\,(I)$ *is* $\text{m-rad}\,(I) = \bigcap_{j=1}^n \text{m-rad}\,(I_j)$.
(c) *If the decomposition $I = \bigcap_{j=1}^n I_j$ is redundant, then so is the decomposition* $\text{m-rad}\,(I) = \bigcap_{j=1}^n \text{m-rad}\,(I_j)$.

PROOF. (a) Exercise 3.1.6(a).

(b) The first step in the next sequence is by assumption:

$$\text{m-rad}\,(I) = \text{m-rad}\left(\bigcap_{j=1}^n I_j\right) = \bigcap_{j=1}^n \text{m-rad}\,(I_j)\,.$$

The second step is from Proposition 2.3.4(b). Part (a) shows that each ideal $\text{m-rad}\,(I_j)$ is m-irreducible, so this is an m-irreducible decomposition.

(c) Assume that the decomposition $I = \bigcap_{j=1}^n I_j$ is redundant. Then there are indices $j \neq j'$ such that $I_j \subseteq I_{j'}$. Proposition 2.3.3(c) implies that $\text{m-rad}\,(I_j) \subseteq \text{m-rad}\,(I_{j'})$, so the decomposition $\text{m-rad}\,(I) = \bigcap_{j=1}^n \text{m-rad}\,(I_j)$ is redundant. □

EXAMPLE 7.1.2. Set $R = A[X, Y, Z]$. The ideal $J = (X^2Z^2, Y^4, Y^3Z^2)R = (X^2, Y^3)R \bigcap (Y^4, Z^2)R$ has $\text{m-rad}\,(J) = (XZ, Y)R$ with m-irreducible decomposition $\text{m-rad}\,(J) = (X, Y)R \bigcap (Y, Z)R$. See Theorem 2.3.7 and Proposition 7.1.1.

Exercises.

EXERCISE 7.1.3. Set $R = A[X, Y, Z]$, and consider the monomial ideal

$$J = (X^3Y^4, X^2Y^4Z^3, X^2Z^5, Y^4Z^3, Y^3Z^5)R.$$

(a) Find an irredundant m-irreducible decomposition of m-rad (J). (Hint: Use Proposition 2.1.5 to show that $J = (X^2, Y^3)R \bigcap (X^3, Z^3)R \bigcap (Y^4, Z^5)R$.)
(b) Use Theorem 2.3.7 to find an irredundant monomial generating sequence for m-rad (J), and verify that your decomposition from part (a) is correct as in Exercise 4.3.11(d).

Justify your answers.

EXERCISE 7.1.4. Set $R = A[X, Y]$. Find a non-zero monomial ideal $I, J \subsetneq R$ with irredundant m-irreducible decomposition $I = \bigcap_{j=1}^n I_j$ such that the decomposition m-rad $(I) = \bigcap_{j=1}^n$ m-rad (I_j) is redundant. Can this be done in one variable? Justify your answers.

EXERCISE 7.1.5. Set $R = A[X, Y]$. Find non-zero monomial ideals $I, J \subsetneq R$ with irredundant m-irreducible decompositions $I = \bigcap_{j=1}^n I_j$ and $J = \bigcap_{i=1}^m J_i$ such that the decomposition $I \bigcap J = (\bigcap_{j=1}^n I_j) \bigcap (\bigcap_{i=1}^m J_i)$ is redundant. Can this be done for monomial ideals in 1 variable? Justify your answers.

EXERCISE 7.1.6. Set $R = A[X_1, \ldots, X_d]$, and let J be a monomial ideal of R that has a parametric decomposition. Prove that $\mathrm{C}_R(\text{m-rad}\,(J)) = \{1\}$.

M-Irreducible Decompositions of Monomial Radicals in Macaulay2.

Exercises.

7.2. M-Irreducible Decompositions of Bracket Powers

In this section, A is a non-zero commutative ring with identity.

In this section, we consider bracket powers of monomial ideals, as discussed in Section 2.5.

PROPOSITION 7.2.1. *Set $R = A[X_1, \ldots, X_d]$. Let I be a monomial ideal of R with m-irreducible decomposition $I = \bigcap_{j=1}^n I_j$, and let k be a positive integer.*

(a) *The ideal I is m-irreducible if and only if $I^{[k]}$ is m-irreducible.*
(b) *An m-irreducible decomposition of $I^{[k]}$ is $I^{[k]} = \bigcap_{j=1}^n I_j{}^{[k]}$.*
(c) *The decomposition $I = \bigcap_{j=1}^n I_j$ is irredundant if and only if the decomposition $I^{[k]} = \bigcap_{j=1}^n I_j{}^{[k]}$ is irredundant.*

PROOF. (a) $\Longrightarrow$: Assume that I is m-irreducible. If $I = 0$, then $I^{[k]} = 0$, which is m-irreducible. So, assume that $I \neq 0$. Theorem 3.1.3 provides positive integers $m, t_1, \ldots, t_m, e_1, \ldots, e_m$ such that $1 \leqslant t_1 < \cdots < t_m \leqslant d$ such that $I = (X_{t_1}^{e_1}, \ldots, X_{t_m}^{e_m})R$. From Proposition 2.5.5, we have $I^{[k]} = (X_{t_1}^{ke_1}, \ldots, X_{t_m}^{ke_m})R$ so Theorem 3.1.3 implies that $I^{[k]}$ is m-irreducible.

$\Longleftarrow$: Assume that $I^{[k]}$ is m-irreducible. As in the previous paragraph, assume without loss of generality that $I \neq 0$. Let $f_1, \ldots, f_m$ be an irredundant monomial generating sequence for I. Then an irredundant monomial generating sequence for $I^{[k]}$ is $f_1^k, \ldots, f_m^k$ by Proposition 2.5.5. Since $I^{[k]}$ is m-irreducible, Theorem 3.1.3

implies that for $i = 1, \ldots, m$ there is an index j_i and an exponent e_i such that $f_i^k = X_{j_i}^{e_i}$. A comparison of exponent vectors shows that this implies that for $i = 1, \ldots, m$ there is an exponent a_i such that $e_i = ka_i$ and $f_i = X_{j_i}^{a_i}$. It follows from Theorem 3.1.3 that I is m-irreducible.

(b) Proposition 2.5.7 shows that $I^{[k]} = \bigcap_{j=1}^n I_j{}^{[k]}$, and part (a) shows that each ideal $I_j{}^{[k]}$ is m-irreducible.

(c) "$\Longleftarrow$": If the decomposition $I = \bigcap_{j=1}^n I_j$ is redundant, then there are indices $i \neq i'$ such that $I_i \subseteq I_{i'}$. Lemma 2.5.6(a) implies that $I_i{}^{[k]} \subseteq I_{i'}{}^{[k]}$, so the decomposition $I^{[k]} = \bigcap_{j=1}^n I_j{}^{[k]}$ is redundant.

"$\Longrightarrow$": If the decomposition $I^{[k]} = \bigcap_{j=1}^n I_j{}^{[k]}$ is redundant, then there are indices $i \neq i'$ such that $I_i{}^{[k]} \subseteq I_{i'}{}^{[k]}$. Lemma 2.5.6(a) implies that $I_i \subseteq I_{i'}$, so the decomposition $I = \bigcap_{j=1}^n I_j$ is redundant. $\square$

Example 7.2.2. Set $R = A[X, Y, Z]$, and consider the monomial ideal

$$\begin{aligned} J &= (X^3Y^4, X^2Y^4Z^3, X^2Z^5, Y^4Z^3, Y^3Z^5)R \\ &= (X^2, Y^3)R \bigcap (X^3, Z^3)R \bigcap (Y^4, Z^5)R. \end{aligned}$$

See Exercise 7.1.3. This is an irredundant m-irreducible decomposition of J. Then we have the following irredundant m-irreducible decomposition of $J^{[k]}$:

$$\begin{aligned} J^{[3]} &= (X^9Y^{12}, X^6Y^{12}Z^9, X^6Z^{15}, Y^{12}Z^9, Y^9Z^{15})R \\ &= (X^2, Y^3)R^{[k]} \bigcap (X^3, Z^3)R^{[k]} \bigcap (Y^4, Z^5)R^{[3]} \\ &= (X^6, Y^9)R \bigcap (X^9, Z^9)R \bigcap (Y^{12}, Z^{15})R. \end{aligned}$$

Exercises.

Exercise 7.2.3. Set $R = A[X, Y]$ and $J = (X^3, X^2Y, Y^3)R$.

(a) Find the J-corner elements and use them to compute an irredundant parametric decomposition of J.
(b) Use Proposition 7.2.1 with your answer from part (a) to find an irredundant parametric decomposition of $J^{[3]}$.
(c) Use Proposition 2.5.5 to find an irredundant monomial generating sequence for $J^{[3]}$, and verify that your decomposition from part (b) is correct as in Exercise 4.3.11(d).

Justify your answers.

Exercise 7.2.4. Set $R = A[X_1, \ldots, X_d]$. Let I be a monomial ideal of R, and let k be a positive integer.

(a) Prove that I is a parameter ideal if and only if $I^{[k]}$ is a parameter ideal.
(b) Prove that if I has a parametric decomposition $I = \bigcap_{j=1}^n I_j$, then $I^{[k]} = \bigcap_{j=1}^n I_j{}^{[k]}$ is a parametric decomposition of $I^{[k]}$.
(c) Prove that I has a parametric decomposition if and only if $I^{[k]}$ has a parametric decomposition

Exercise 7.2.5. Set $R = A[X_1, \ldots, X_d]$. Let I be a monomial ideal of R, and let k be a positive integer. For each monomial $f = X_1^{n_1} \cdots X_d^{n_d}$ in R, set

$$f^{(k)} = X_1^{k(n_1+1)-1} \cdots X_d^{k(n_d+1)-1}.$$

(a) Prove that $\mathrm{C}_R(I^{[k]}) = \{f^{(k)} \mid f \in \mathrm{C}_R(I)\}$.
(b) Use part (a) to compute the $J^{[3]}$-corner elements for the ideal from Exercise 7.2.3.
(c) Verify your answer from part (b) using the decomposition of $J^{[3]}$ from Exercise 7.2.3(b).

M-Irreducible Decompositions of Bracket Powers in Macaulay2.

Exercises.

7.3. M-Irreducible Decompositions of Sums

In this section, A is a non-zero commutative ring with identity.

Next, we look at sums of monomial ideals. Recall that Exercise 1.3.11 shows that each sum of monomial ideals is a monomial ideal. We begin by showing that each sum of m-irreducible monomial ideals is m-irreducible.

PROPOSITION 7.3.1. *Set $R = A[X_1, \ldots, X_d]$. If $J_1, \ldots, J_n$ are m-irreducible monomial ideals of R, then the sum $J_1 + \cdots + J_n$ is m-irreducible.*

PROOF. We prove the result by induction on n. The case $n = 1$ is evident.

Base case: $n = 2$. Assume that I and J are m-irreducible monomial ideals; we show that $I + J$ is m-irreducible. If $I = 0$, then $I + J = 0 + J = J$ which is m-irreducible. Similarly, if $J = 0$, then we are done, so we assume that I and J are both non-zero. Theorem 3.1.3 shows that there are positive integers $j, k, s_1, \ldots, s_j, t_1, \ldots, t_k, d_1, \ldots, d_j, e_1, \ldots, e_k$ such that $1 \leqslant s_1 < \cdots < s_j \leqslant d$ and $1 \leqslant t_1 < \cdots < t_k \leqslant d$ and $I = (X_{s_1}^{d_1}, \ldots, X_{s_j}^{d_j})R$ and $J = (X_{t_1}^{e_1}, \ldots, X_{t_k}^{e_k})R$. Fact A.4.8(a) implies that

$$I + J = (X_{s_1}^{d_1}, \ldots, X_{s_j}^{d_j}, X_{t_1}^{e_1}, \ldots, X_{t_k}^{e_k})R.$$

It is straightforward but tedious to show that it follows that $I+J = (X_{u_1}^{f_1}, \ldots, X_{u_l}^{f_l})R$ for appropriate positive integers $l, u_1, \ldots, u_l, f_1, \ldots, f_l$. Theorem 3.1.3 implies that this ideal is m-irreducible.

Induction step: Exercise. $\square$

EXAMPLE 7.3.2. In the ring $R = A[X, Y, Z]$, one has

$$(X^2, Y^3)R + (X^3, Z^3)R = (X^2, Y^3, Z^3)R.$$

The next result is a distributive law for intersections and sums of monomial ideals, based on the corresponding distributive law for intersections and unions.

LEMMA 7.3.3. *Set $R = A[X_1, \ldots, X_d]$. Given monomial ideals $I_1, \ldots, I_n$ and $J_1, \ldots, J_m$ of R, one has*

$$(\bigcap_{j=1}^{n} I_j) + (\bigcap_{i=1}^{m} J_i) = \bigcap_{j=1}^{n} \bigcap_{i=1}^{m} (I_j + J_i).$$

PROOF. The ideals $(\bigcap_{j=1}^{n} I_j) + (\bigcap_{i=1}^{m} J_i)$ and $\bigcap_{j=1}^{n} \bigcap_{i=1}^{m} (I_j + J_i)$ are monomial ideals, so we need only show that the sets of monomials in each ideals are the same.

To this end, The first and fourth steps below are from Exercise 1.3.11(d).

$$\begin{aligned}
[\![(\bigcap_{j=1}^{n} I_j) + (\bigcap_{i=1}^{m} J_i)]\!] &= [\![\bigcap_{j=1}^{n} I_j]\!] \cup [\![\bigcap_{i=1}^{m} J_i]\!] \\
&= (\bigcap_{j=1}^{n} [\![I_j]\!]) \cup (\bigcap_{i=1}^{m} [\![J_i]\!]) \\
&= \bigcap_{j=1}^{n} \bigcap_{i=1}^{m} ([\![I_j]\!] \cup [\![J_i]\!]) \\
&= \bigcap_{j=1}^{n} \bigcap_{i=1}^{m} [\![I_j + J_i]\!] \\
&= [\![\bigcap_{j=1}^{n} \bigcap_{i=1}^{m} (I_j + J_i)]\!].
\end{aligned}$$

The second and fifth steps are from Theorem 2.1.1. The third step is from the distributive laws for intersections and unions. □

The next result shows how to build m-irreducible decompositions for sums of monomial ideals.

THEOREM 7.3.4. *Set $R = A[X_1, \ldots, X_d]$. Let I and J be monomial ideals of R with m-irreducible decompositions $I = \bigcap_{j=1}^{n} I_j$ and $J = \bigcap_{i=1}^{m} J_i$. Then an m-irreducible decomposition of $I + J$ is*

$$I + J = \bigcap_{j=1}^{n} \bigcap_{i=1}^{m} (I_j + J_i).$$

PROOF. From Lemma 7.3.3 we have

$$I + J = (\bigcap_{j=1}^{n} I_j) + (\bigcap_{i=1}^{m} J_i) = \bigcap_{j=1}^{n} \bigcap_{i=1}^{m} (I_j + J_i)$$

and Proposition 7.3.1 shows that each ideal $I_j + J_i$ is m-irreducible. □

EXAMPLE 7.3.5. Set $R = A[X, Y, Z]$, and consider the monomial ideals

$$\begin{aligned}
I &= (X^3, X^2Z^3, X^3Y^3, Y^3Z^3)R = (X^2, Y^3)R \bigcap (X^3, Z^3)R \\
J &= (Y^4, Z^5)R.
\end{aligned}$$

Then we have the following irredundant m-irreducible decomposition of $I + J$:

$$\begin{aligned}
I + J &= (X^3, X^2Z^3, X^3Y^3, Y^3Z^3, Y^4, Z^5)R \\
&= ((X^2, Y^3)R + (Y^4, Z^5)R) \bigcap ((X^3, Z^3)R(Y^4, Z^5)R) \\
&= (X^2, Y^3, Z^5)R \bigcap (X^3, Y^4, Z^3)R.
\end{aligned}$$

Exercises.

EXERCISE 7.3.6. Complete the induction step of Proposition 7.3.1.

EXERCISE 7.3.7. Verify that the decomposition from Example 7.3.5 is correct as in Exercise 4.3.11(d).

EXERCISE 7.3.8. Set $R = A[X_1, \ldots, X_d]$. Prove that if $J_1, \ldots, J_n$ are parameter ideals of R, then the sum $J_1 + \cdots + J_n$ is a parameter ideal.

EXERCISE 7.3.9. Set $R = A[X_1, \ldots, X_d]$. Let I and J be monomial ideals of R with parametric decompositions $I = \bigcap_{j=1}^n I_j$ and $J = \bigcap_{i=1}^m J_i$. Prove that a parametric decomposition of $I + J$ is $I + J = \bigcap_{j=1}^n \bigcap_{i=1}^m (I_j + J_i)$.

EXERCISE 7.3.10. Set $R = A[X_1, \ldots, X_d]$. Prove or disprove the following: if $J_1, \ldots, J_n$ are monomial ideals of R such that the sum $J_1 + \cdots + J_n$ is an m-irreducible monomial ideal, then J_i is m-irreducible for $j = 1, \ldots, n$.

EXERCISE 7.3.11. Set $R = A[X, Y]$. Use Theorem 7.3.4 to find an irredundant m-irreducible decomposition of the ideal $I + J$ where $I = (X^3, XY^2, Y^3)R$ and $J = (X^3, X^2Y, Y^3)R$. Verify that your decomposition is correct as in Exercise 4.3.11(d). Justify your answer.

EXERCISE 7.3.12. Set $R = A[X, Y]$. Find non-zero monomial ideals $I, J \subsetneq R$ with irredundant m-irreducible decompositions $I = \bigcap_{j=1}^n I_j$ and $J = \bigcap_{i=1}^m J_i$ such that the decomposition $I + J = \bigcap_{j=1}^n \bigcap_{i=1}^m (I_j + J_i)$ is redundant. Can this be done for monomial ideals in 1 variable? Justify your answers.

*EXERCISE 7.3.13. Let $K_1, \ldots, K_p \subsetneq R$ be monomial ideals of R. For $i = 1, \ldots, p$ fix an m-irreducible decomposition $K_i = \bigcap_{j=1}^{s_i} K_{i,j}$. Prove that

$$K_1 + \cdots + K_p = \bigcap_{l_1=1}^{s_1} \cdots \bigcap_{l_p=1}^{s_p} (K_{1,l_1} + \cdots + K_{p,l_p})$$

and prove that this is an m-irreducible decomposition. (This exercise is used in several places.)

EXERCISE 7.3.14. Set $R = A[X, Y]$. Use Exercise 7.3.13 to find an m-irreducible decomposition of $(X^2, XY^5, Y^6)R + (X^4, X^3Y^3, Y^5)R + (X^7, X^3Y^2, Y^3)R$. Verify that your decomposition is correct as in Exercise 4.3.11(d). Justify your answer.

EXERCISE 7.3.15. Set $R = A[X_1, \ldots, X_d]$.

(a) Prove that if $f, g \in [\![R]\!]$, then $\mathrm{P}_R(f) + \mathrm{P}_R(g) = \mathrm{P}_R(\gcd(f, g))$. (See Exercise 2.1.14 for the definition of $\gcd(f, g)$.)
(b) Let I and J be monomial ideals of R with parametric decompositions. Prove that $\mathrm{C}_R(I + J) \subseteq \{\gcd(f, g) \mid f \in \mathrm{C}_R(I) \text{ and } g \in \mathrm{C}_R(J)\}$.
(c) Find monomial ideals I and J of R with parametric decompositions such that $\mathrm{C}_R(I + J) \subsetneq \{\gcd(f, g) \mid f \in \mathrm{C}_R(I) \text{ and } g \in \mathrm{C}_R(J)\}$. Justify your answer.
(d) Does the containment in part (b) hold if I or J does not have a parametric decomposition? Justify your answer.

M-Irreducible Decompositions of Sums in Macaulay2.

Exercises.

7.4. M-Irreducible Decompositions of Colon Ideals

In this section, A is a non-zero commutative ring with identity.

Next, we look at colon ideals of monomial ideals. Recall that Theorem 2.4.1 implies that the colon ideal of two monomial ideals is a monomial ideal. As in the proof of that result, the general case follows from the following special case where the second ideal is principal.

PROPOSITION 7.4.1. *Set $R = A[X_1, \ldots, X_d]$. Let $k, t_1, \ldots, t_k, e_{t_1}, \ldots, e_{t_k}$ be positive integers, and set $J = (X_{t_1}^{e_{t_1}}, \ldots, X_{t_k}^{e_{t_k}})R$. Given a monomial $f = \underline{X}^{\underline{n}} \in [\![R]\!]$, we have*

$$\begin{aligned}(J :_R f) &= \begin{cases} R & \text{if there is an index } i \text{ such that } n_{t_i} \geqslant e_{t_i} \\ (X_{t_1}^{e_{t_1}-n_{t_1}}, \ldots, X_{t_k}^{e_{t_k}-n_{t_k}})R & \text{if for } i = 1, \ldots, k \text{ we have } n_{t_i} < e_{t_i} \end{cases} \\ &= \begin{cases} R & \text{if } f \in J \\ (X_{t_1}^{e_{t_1}-n_{t_1}}, \ldots, X_{t_k}^{e_{t_k}-n_{t_k}})R & \text{if } f \notin J. \end{cases}\end{aligned}$$

PROOF. We know that $f \in J$ if and only if if there is an index i such that $f \in (X_{t_i}^{e_{t_i}})R$. By comparing exponent vectors, this says that $f \in J$ if and only if there is an index i such that $n_{t_i} \geqslant e_{t_i}$.

If there is an index i such that $n_{t_i} \geqslant e_{t_i}$, then $f \in J$, so $(J :_R f) = R$ by Proposition A.5.3(c).

Assume now that for $i = 1, \ldots, k$ we have $n_{t_i} < e_{t_i}$. For $i = 1, \ldots, k$ the monomial $X_{t_i}^{e_{t_i}-n_{t_i}}$ is in $(J :_R f)$ because

$$X_{t_i}^{e_{t_i}-n_{t_i}} f = X_1^{n_1} \cdots X_{t_i}^{e_{t_i}-n_{t_i}+n_{t_i}} \cdots X_d^{n_d} \in (X_{t_i}^{e_{t_i}})R \subseteq J.$$

To complete the proof, we need to fix a monomial $g \in (J :_R f)$ and show that $g \in (X_{t_i}^{e_{t_i}-n_{t_i}})R$ for some index i. (This uses the fact that $(J :_R f)$ is a monomial ideal; see Theorem 2.4.1.) Let $g = \underline{X}^{\underline{m}} \in [\![(J :_R f)]\!]$. Then $fg \in J$, so there is an index i such that $1 \leqslant i \leqslant n$ and $fg \in (X_{t_i}^{e_{t_i}})R$. A comparison of exponent vectors shows that this implies that $n_{t_i} + m_{t_i} \geqslant e_{t_i}$, so $m_{t_i} \geqslant e_{t_i} - n_{t_i}$. Another comparison of exponent vectors implies that $g \in (X_{t_i}^{e_{t_i}-n_{t_i}})R$ as desired. □

COROLLARY 7.4.2. *Set $R = A[X_1, \ldots, X_d]$, and let J be an m-irreducible monomial ideal of R. Given a monomial $f \in [\![R]\!]$, either the ideal $(J :_R f)$ is m-irreducible or $(J :_R f) = R$. The ideal $(J :_R f)$ is m-irreducible if and only if $f \notin J$.*

PROOF. If $J = 0$, then $(J :_R f) = 0$ which is m-irreducible. If $J \neq 0$, then the result follows from Theorem 3.1.3 and Proposition 7.4.1. □

EXAMPLE 7.4.3. Set $R = A[X, Y, Z]$ and $J = (X^2, Z^3)R$. Proposition 7.4.1 provides the following:

$$(J :_R XY) = (X, Z^3)R \qquad\qquad (J :_R XYZ^4) = R.$$

THEOREM 7.4.4. *Set $R = A[X_1, \ldots, X_d]$. Let I be a monomial ideal of R with monomial generating sequence $f_1, \ldots, f_t$. Let J be a monomial ideal of R with m-irreducible decomposition $J = \bigcap_{i=1}^m J_i$. Assume that $I \not\subseteq J$. Then an m-irreducible decomposition of $(J :_R I)$ is*

$$(J :_R I) = \bigcap_{f_j \notin J_i} (J_i :_R f_j)$$

where the intersection is taken over the set of all ordered pairs (i, j) such that $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant t$ and $f_j \notin J_i$.

PROOF. The first and third equalities below are by assumption:

$$\begin{aligned}(J :_R I) &= (J :_R (f_1, \ldots, f_t)R)\\ &= \bigcap_{j=1}^{t}(J :_R f_j)\\ &= \bigcap_{j=1}^{t}(\bigcap_{i=1}^{m} J_i :_R f_j)\\ &= \bigcap_{j=1}^{t}\bigcap_{i=1}^{m}(J_i :_R f_j)\\ &= \bigcap_{(i,j)\in S}(J_i :_R f_j).\end{aligned}$$

The second equality is from Proposition A.5.3(b), and the fourth equality is from Proposition A.5.4(b). The fifth equality is from Corollary 7.4.2. Another application of Corollary 7.4.2 shows that when $f_j \notin J_i$, the ideal $(J_i :_R f_j)$ is m-irreducible. $\square$

EXAMPLE 7.4.5. Set $R = A[X, Y, Z]$, and consider the monomial ideals

$$\begin{aligned}I &= (Y^4, Z^5)R\\ J &= (X^3, X^2Z^3, X^3Y^3, Y^3Z^3)R = (X^2, Y^3)R\bigcap(X^3, Z^3)R.\end{aligned}$$

In the notation of Theorem 7.4.4, we have $f_1 = Y^4$, $f_2 = Z^5$, $J_1 = (X^2, Y^3)R$, and $J_2 = (X^3, Z^3)R$. To find an m-irreducible decomposition of $(J :_R I)$, we first find the ordered pairs (i, j) such that $f_j \notin J_i$: $f_1 \in J_1$, $f_1 \notin J_2$, $f_2 \notin J_1$, and $f_2 \in J_2$. Thus, the first step in the next sequence is from Theorem 7.4.4:

$$(J :_R I) = (J_2 :_R f_1)\bigcap(J_1 :_R f_2) = (X^2, Y^3)R\bigcap(X^3, Z^3)R = J.$$

The second step is from Proposition 7.4.1.

LEMMA 7.4.6. *Set $R = A[X_1, \ldots, X_d]$ and $\mathfrak{X} = (X_1, \ldots, X_d)R$. Let J be an m-irreducible monomial ideal of R.*

(a) *If* m-rad $(J) \neq \mathfrak{X}$*, then* $(J :_R \mathfrak{X}) = J$ *and* $\mathrm{C}_R(J) = \emptyset$.
(b) *If* m-rad $(J) = \mathfrak{X}$*, then J is a parameter ideal, say $J = \mathrm{P}_R(z)$, and we have* $(J :_R \mathfrak{X}) = J + (z)R$ *and* $\mathrm{C}_R(J) = \{z\}$.

PROOF. If $J = 0$, then the result is straightforward. Thus, we assume that $J \neq 0$. Theorem 3.1.3 provides positive integers $k, t_1, \ldots, t_k, e_1, \ldots, e_k$ such that $J = (X_{t_1}^{e_1}, \ldots, X_{t_k}^{e_k})R$.

(a) Assume that m-rad $(J) \neq \mathfrak{X}$. By Exercise 6.3.22, it suffices to show that $\mathrm{C}_R(J) = \emptyset$. By definition, we have $\mathrm{C}_R(J) = [\![(J :_R \mathfrak{X})]\!] \smallsetminus [\![J]\!]$, so we need to show that $[\![(J :_R \mathfrak{X})]\!] \subseteq J$. Fix a monomial $f = \underline{X}^{\underline{m}} \in [\![(J :_R \mathfrak{X})]\!]$.

The assumption m-rad $(J) \neq \mathfrak{X}$. provides an index j such that $X_j \notin$ m-rad (J). Since $f \in (J :_R \mathfrak{X})$, we have $X_jf \in J$. Theorem 1.1.8 implies that there is an index p such that $X_jf \in (X_{t_p}^{e_p})R$. Since $X_j \notin$ m-rad (J), we have $X_j \neq X_{t_p}$. Thus, a comparison of exponent vectors shows that we have $m_{t_p} \geqslant e_p$, and it follows that $f = \underline{X}^{\underline{m}} \in (X_{t_p}^{e_p})R \subseteq J$. Thus, we have $(J :_R \mathfrak{X}) = J$.

(b) Assume that $\text{m-rad}\,(J) = \mathfrak{X}$. Then Corollary 2.3.8 shows that J is a parameter ideal, say $J = \mathrm{P}_R(z)$. Corollary 6.3.7(a) implies that $\mathrm{C}_R(J) = \{z\}$, and it follows from Exercise 6.3.22 that $(J :_R \mathfrak{X}) = J + (z)R$. $\square$

To conclude this section, we address the question of which monomial ideals admit a corner element.

Proposition 7.4.7. *Set $R = A[X_1, \ldots, X_d]$ and $\mathfrak{X} = (X_1, \ldots, X_d)R$. Let J be a monomial ideal of R with irredundant m-irreducible decomposition $J = \bigcap_{i=1}^m J_i$ with $m \geqslant 1$. Assume that the ideals J_i are ordered so that* $\text{m-rad}\,(J_i) = \mathfrak{X}$ *when $1 \leqslant i \leqslant n$ and* $\text{m-rad}\,(J_i) \neq \mathfrak{X}$ *when $n < i \leqslant m$. Then $\mathrm{C}_R(J) = \cup_{i=1}^n \mathrm{C}_R(J_i)$. In other words, if $J_i = \mathrm{P}_R(z_i)$ for $i = 1, \ldots, n$ then the distinct J-corner elements are $z_1, \ldots, z_n$.*

Proof. The case where J is m-irreducible is covered by Lemma 7.4.6. Thus, we assume without loss of generality that J is not m-irreducible, that is, that $m \geqslant 2$.

The irredundancy of the intersection $\bigcap_{i=1}^m J_i$ implies that for indices $i \neq j$ we have $J_j \not\subseteq J_i$. When $1 \leqslant i \leqslant n$, we have $\text{m-rad}\,(J_i) = \mathfrak{X}$, so Proposition 6.3.4(c) implies that $\mathrm{C}_R(J_i) \bigcap J_j \neq \emptyset$. Since $\mathrm{C}_R(J_i) = \{z_i\}$, this means that $z_i \in J_j$.

Claim: For $i = 1, \ldots, n$ we have $z_i \in \mathrm{C}_R(J)$. Since $z_i \notin J_i$ and $J \subseteq J_i$, we have $z_i \notin J$. Thus, we need only show that $X_k z_i \in J$ for $k = 1, \ldots, d$. Since $J = \bigcap_{j=1}^m J_j$, it suffices to show that $X_k z_i \in J_j$ for $j = 1, \ldots, m$. When $j \neq i$, this follows from the condition $z_i \in J_j$ established in the previous paragraph. When $j = i$, this follows from the fact that $z_i \in \mathrm{C}_R(J_i)$.

Claim: We have $\mathrm{C}_R(J) \subseteq \{z_1, \ldots, z_n\}$. The first equality in the next sequence is by assumption:

$$(J :_R \mathfrak{X}) = (\bigcap_{i=1}^n J_i :_R \mathfrak{X}) = \bigcap_{i=1}^n (J_i :_R \mathfrak{X}) = [\bigcap_{i=1}^n [J_i + (z_i)R]] \bigcap [\bigcap_{j=n+1}^m J_j].$$

The second equality is by Proposition A.5.4(b), and the third one is by Lemma 7.4.6. This explains the first equality in the next sequence:

$$\begin{aligned}
[\![(J :_R \mathfrak{X})]\!] &= [\![\bigcap_{i=1}^n [J_i + (z_i)R]] \bigcap [\bigcap_{j=n+1}^m J_j]]\!] \\
&= [\bigcap_{i=1}^n [\![J_i + (z_i)R]\!]] \bigcap [\bigcap_{j=n+1}^m [\![J_j]\!]] \\
&= [\bigcap_{i=1}^n [\![J_i]\!] \cup \{z_i\}] \bigcap [\bigcap_{j=n+1}^m [\![J_j]\!]].
\end{aligned}$$

The second equality is from Theorem 2.1.1. For the third equality, use the fact that $\{z_i\} = \mathrm{C}_R(J_i) = [\![(J_i :_R \mathfrak{X})]\!] \smallsetminus [\![J_i]\!]$ to conclude that $[\![J_i + (z_i)R]\!] = [\![J_i]\!] \cup \{z_i\}$.

Given an element $z \in \mathrm{C}_R(J) \subseteq [\![(J :_R \mathfrak{X})]\!]$, we conclude from the previous displayed sequence that $z \in [\![J_i]\!] \cup \{z_i\}$ for $i = 1, \ldots, n$ and that $z \in [\![J_j]\!]$ for $j = n+1, \ldots, m$. On the other hand, since $z \notin [\![J]\!]$, the sequence

$$[\![J]\!] = [\![\bigcap_{i=1}^m J_i]\!] = \bigcap_{i=1}^m [\![J_i]\!]$$

shows that there is an index i' such that $z \notin [\![J_{i'}]\!]$. Since we have $z \in [\![J_j]\!]$ for $j = n+1, \ldots, m$ it follows that $i' \leqslant n$, that is, we have $z \in ([\![J_{i'}]\!] \cup \{z_i\}) \smallsetminus [\![J_{i'}]\!] = \{z_{i'}\}$. We conclude that $z = z_{i'}$, as desired. $\square$

COROLLARY 7.4.8. *Set $R = A[X_1, \ldots, X_d]$ and $\mathfrak{X} = (X_1, \ldots, X_d)R$. Let J be a monomial ideal of R with irredundant m-irreducible decomposition $J = \bigcap_{i=1}^m J_i$ with $m \geqslant 1$. Then J has a corner element if and only if there is an index i such that* m-rad$(J_i) = \mathfrak{X}$.

PROOF. In the notation of Proposition 7.4.7, there is a J-corner element if and only if $n \geqslant 1$, that is, if and only if there is an index i such that m-rad$(J_i) = \mathfrak{X}$. $\square$

EXAMPLE 7.4.9. Set $R = A[X, Y]$ and $J = (XY, XZ, YZ)R$. We show that $\mathrm{C}_R(J) = \emptyset$. Example 7.5.6 provides an irredundant m-irreducible decomposition.

$$J = (Y, Z)R \bigcap (X, Z)R \bigcap (X, Y)R.$$

As this decomposition has no parameter ideals, Corollary 7.4.8 says that $\mathrm{C}_R(J) = \emptyset$.

Exercises.

EXERCISE 7.4.10. Verify directly the equalities in Example 7.4.3. Justify your answers.

EXERCISE 7.4.11. Verify directly the equality $(J :_R I) = J$ in Example 7.4.5. Justify your answer.

EXERCISE 7.4.12. Verify directly the equality $\mathrm{C}_R(J) = \emptyset$ in Example 7.4.9. Justify your answer.

EXERCISE 7.4.13. Set $R = A[X, Y]$. Use Proposition 7.4.1 to identify the ideals $(J :_R f)$ and $(J :_R g)$ where $J = (X^3, X^2Y, Y^3)R$, $f = XY^2$, and $g = X^2Y^2$. Justify your answer.

EXERCISE 7.4.14. Set $R = A[X_1, \ldots, X_d]$. Let J be a monomial ideal of R, and let $f \in [\![R]\!]$. If $(J :_R f)$ is m-irreducible, must J be m-irreducible? Justify your answer.

EXERCISE 7.4.15. Set $R = A[X_1, \ldots, X_d]$, and let J be a parameter ideal of R. Fix a monomial $f \in [\![R]\!]$.

(a) Prove that either $(J :_R f)$ is a parameter ideal or $(J :_R f) = R$.
(b) Prove that $(J :_R f)$ is a parameter ideal if and only if $f \notin J$.
(c) Prove that if $f = \underline{X}^{\underline{m}}$ and $g = \underline{X}^{\underline{n}}$, then $(\mathrm{P}_R(g) :_R f) = \mathrm{P}_R(\underline{X}^{\underline{p}})$ where $p_i = m_i - n_i$ for $i = 1, \ldots, d$.

EXERCISE 7.4.16. Set $R = A[X, Y]$, and use the ideals $I = (X^3, XY^2, Y^3)R$ and $J = (X^3, X^2Y, Y^3)R$.

(a) Use Theorem 7.4.4 to find an irredundant m-irreducible decomposition $\bigcap_{i=1}^m J_i$ of the ideal $(J :_R I)$.
(b) Compute directly a monomial generating sequence for $(J :_R I)$. and verify the decomposition $(J :_R I) = \bigcap_{i=1}^m J_i$ from part (a) by computing the generators for $\bigcap_{i=1}^m J_i$ using least common multiples.

Justify your answers.

Exercise 7.4.17. Set $R = A[X, Y]$. Find non-zero monomial ideals $I, J \subsetneq R$ such that the decomposition $(J :_R I) = \bigcap_{f_j \notin J_i} (J_i :_R f_j)$ from Theorem 7.4.4 is redundant. Can this be done for monomial ideals in 1 variable? Justify your answers.

Exercise 7.4.18. Set $R = A[X_1, \ldots, X_d]$, and let I and J be monomial ideals of R. Assume that J has a parametric decomposition $J = \bigcap_{i=1}^{m} \mathrm{P}_R(z_i)$ and that $I \not\subseteq J$.

(a) Prove that the decomposition of $(J :_R I)$ from Theorem 7.4.4 is a parametric decomposition.
(b) Let $f_1, \ldots, f_n$ be a monomial generating sequence of I, and for $j = 1, \ldots, n$ write $f_j = \underline{X}^{\underline{n}_j}$ where $\underline{n}_j = (n_{j,1}, \ldots, n_{j,d}) \in \mathbb{N}^d$. For $i = 1, \ldots, m$ write $z_i = \underline{X}^{\underline{m}_i}$ where $\underline{m}_i = (m_{i,1}, \ldots, m_{i,d}) \in \mathbb{N}^d$. When $f_j \notin \mathrm{P}_R(z_i)$, write $g_{i,j} = \underline{X}^{\underline{p}}$ where $p_i = m_i - n_i$. Prove that $\mathrm{C}_R((J :_R I)) \subseteq \{g_{i,j} \mid f_j \notin \mathrm{P}_R(z_i)\}$.
(c) Find ideals I and J such that $\mathrm{C}_R((J :_R I)) \subsetneq \{g_{i,j} \mid f_j \notin \mathrm{P}_R(z_i)\}$.
(d) Does the containment in part (b) hold if J does not have a parametric decomposition?

Justify your answers.

Exercise 7.4.19. Set $R = A[X, Y, Z]$ and $J = (X^2Y, Y^2Z, XZ^2, XYZ)R$. Use Corollary 7.4.8 to show that $\mathrm{C}_R(J) = \emptyset$.

Exercise 7.4.20. Set $R = A[X_1, \ldots, X_d]$, and let J be a monomial ideal of R with irredundant monomial generating sequence $f_1, \ldots, f_t$. Prove that if J has a corner element, then $t \geqslant d$.

M-Irreducible Decompositions of Colon Ideals in Macaulay2.

Exercises.

7.5. Methods for Computing General M-Irreducible Decompositions

In this section, A is a non-zero commutative ring with identity.

We learned of the algorithms in this section from Jung-Chen Liu [**25**]. This section is based on lectures she gave. Other algorithms can be found, e.g., in [**11, 37**]. We begin with another distributive law. Recall that the definitions of lcm and support are in 2.2.12 and 2.3.5.

Lemma 7.5.1. *Set $R = A[X_1, \ldots, X_d]$, and let J be a monomial ideal of R. Given monomials $f, g \in [\![R]\!]$, one has*

$$[J + (f)R] \bigcap [J + (g)R] = J + [(f)R \bigcap (g)R] = J + (\mathrm{lcm}(f, g))R.$$

In particular, if $\mathrm{Supp}(f) \bigcap \mathrm{Supp}(g) = \emptyset$, then $[J + (f)R] \bigcap [J + (g)R] = J + (fg)R$.

Proof. Exercise 2.1.12(a) explains the first two steps in the next sequence:

$$\begin{aligned}
[J + (f)R] \bigcap [J + (g)R] &= (J \bigcap [J + (g)R]) + [(f)R \bigcap [J + (g)R]] \\
&= (J \bigcap J) + [J \bigcap (g)R] + [(f)R \bigcap J] + [(f)R \bigcap (g)R] \\
&= J + [J \bigcap (g)R] + [(f)R \bigcap J] + [(f)R \bigcap (g)R)] \\
&\subseteq J + [(f)R \bigcap (g)R] \\
&\subseteq [J + (f)R] \bigcap [J + (g)R].
\end{aligned}$$

The third step is from the equality $J \bigcap J = J$, and the fourth step follows from the containments $J \bigcap (f)R \subseteq J$ and $J \bigcap (g)R \subseteq J$. The fifth step follows from the containments $J + [(f)R \bigcap (g)R] \subseteq J + (f)R$ and $J + [(f)R \bigcap (g)R] \subseteq J + (g)R$. This explains the equation $[J + (f)R] \bigcap [J + (g)R] = J + [(f)R \bigcap (g)R]$, and the equality $J + [(f)R \bigcap (g)R] = J + (\mathrm{lcm}(f,g))R$ follows from Lemma 2.1.4.

Assume that $\mathrm{Supp}(f) \bigcap \mathrm{Supp}(g) = \emptyset$. It follows that $\mathrm{lcm}(f,g) = fg$, hence the equality $[J + (f)R] \bigcap [J + (g)R] = J + (fg)R$ follows. $\square$

LEMMA 7.5.2. *Set $R = A[X_1, \ldots, X_d]$, and let J be a monomial ideal of R. Fix positive integers $m, i_1, \ldots, i_m, a_1, \ldots, a_m$ such that $1 < m \leqslant d$ and $1 \leqslant i_1 < \cdots < i_m \leqslant d$. Then one has*

$$J + (X_{i_1}^{a_1} \cdots X_{i_m}^{a_m})R = \bigcap_{j=1}^{m} [J + (X_{i_j}^{a_j})R].$$

PROOF. Proceed by induction on m. The base case $m = 2$ follows from Lemma 7.5.1. The induction step is an exercise. $\square$

The next result provides our first method for finding m-irreducible decompositions of arbitrary monomial ideals.

THEOREM 7.5.3. *Set $R = A[X_1, \ldots, X_d]$, and let I be a monomial ideal of R with monomial generating sequence $f_1, \ldots, f_t$. For $i = 1, \ldots, t$ write $f_i = \underline{X}^{\underline{a}_i}$ where $\underline{a}_i = (a_{i,1}, \ldots, a_{i,d}) \in \mathbb{N}^d$. Then we have*

$$I = \bigcap_{i_1=1}^{d} \cdots \bigcap_{i_t=1}^{d} (X_{i_1}^{a_{1,i_1}}, \ldots, X_{i_t}^{a_{t,i_t}})R.$$

Before proving this result, we give an example.

EXAMPLE 7.5.4. Set $R = A[X,Y,Z]$ and $I = (X^1Y^3Z^5, X^6Y^4Z^2)R$. From Theorem 7.5.3 we have the first step in the next sequence:

$$\begin{aligned}
I &= (X^1, X^6)R \bigcap (X^1, Y^4)R \bigcap (X^1, Z^2)R \\
&\quad \bigcap (Y^3, X^6)R \bigcap (Y^3, Y^4)R \bigcap (Y^3, Z^2)R \\
&\quad \bigcap (Z^5, X^6)R \bigcap (Z^5, Y^4)R \bigcap (Z^5, Z^2)R \\
&= (X^1)R \bigcap (X^1, Y^4)R \bigcap (X^1, Z^2)R \\
&\quad \bigcap (X^6, Y^3)R \bigcap (Y^3)R \bigcap (Y^3, Z^2)R \\
&\quad \bigcap (X^6, Z^5)R \bigcap (Y^4, Z^5)R \bigcap (Z^2)R \\
&= (X^1)R \bigcap (Y^3)R \bigcap (X^6, Z^5)R \bigcap (Y^4, Z^5)R \bigcap (Z^2)R.
\end{aligned}$$

The second step is obtained by simplifying each ideal in the first intersection. The third step follows by removing redundancies from the second intersection.

PROOF OF THEOREM 7.5.3. We proceed by induction on t.

Base case: $t = 1$. In this case, we have

$$I = (f_1)R = (X_1^{a_{1,1}} \cdots X_d^{a_{1,d}})R = (X_1^{a_{1,1}})R \bigcap \cdots \bigcap (X_d^{a_{d,1}})R = \bigcap_{i_1=1}^{d} (X_{i_1}^{a_{i_1,1}})R$$

by Lemma 2.1.4. This is the desired formula.

Induction step: Assume that $t \geqslant 2$ and that the result holds for monomial ideals generated by $t-1$ monomials. Set $J = (f_2, \ldots, f_t)R$. By the induction hypothesis, we have

$$J = \bigcap_{i_2=1}^{d} \cdots \bigcap_{i_t=1}^{d} (X_{i_2}^{a_{2,i_2}}, \ldots, X_{i_t}^{a_{t,i_t}})R$$

and this explains the fourth step in the next sequence:

$$\begin{aligned}
I &= J + (f_1)R \\
&= J + (X_1^{a_{1,1}} \cdots X_d^{a_{1,d}})R \\
&= \bigcap_{i_1=1}^{d} [J + (X_{i_1}^{a_{1,i_1}})R] \\
&= \bigcap_{i_1=1}^{d} [[\bigcap_{i_2=1}^{d} \cdots \bigcap_{i_t=1}^{d} (X_{i_2}^{a_{2,i_2}}, \ldots, X_{i_t}^{a_{t,i_t}})R] + (X_{i_1}^{a_{1,i_1}})R] \\
&= \bigcap_{i_1=1}^{d} [\bigcap_{i_2=1}^{d} \cdots \bigcap_{i_t=1}^{d} [(X_{i_2}^{a_{2,i_2}}, \ldots, X_{i_t}^{a_{t,i_t}})R + (X_{i_1}^{a_{1,i_1}})R]] \\
&= \bigcap_{i_1=1}^{d} \cdots \bigcap_{i_t=1}^{d} (X_{i_1}^{a_{1,i_1}}, \ldots, X_{i_t}^{a_{t,i_t}})R.
\end{aligned}$$

The first step is from Fact A.4.8(a), and the second step is by assumption. The third step is from Lemma 7.5.2, and the fifth step follows from Lemma 7.3.3. The final step if by the associativity of intersection. $\square$

Here is another method for computing m-irreducible decompositions in general.

THEOREM 7.5.5. *Set $R = A[X_1, \ldots, X_d]$, and let I be a monomial ideal of R with monomial generating sequence $f_1, \ldots, f_t$. For $i = 1, \ldots, t$ write $f_i = \underline{X}^{\underline{a}_i}$ where $\underline{a}_i = (a_{i,1}, \ldots, a_{i,d}) \in \mathbb{N}^d$. Fix an integer*

$$n > \max\{a_{j,i} \mid i = 1, \ldots, d \text{ and } j = 1, \ldots, t\}.$$

Set $J = (X_1^n, \ldots, X_d^n)R + I$, and let $J = \bigcap_{i=1}^{l} Q_i$ be an irredundant parametric decomposition of J. For $i = 1, \ldots, l$ let Q_i' be the m-irreducible ideal obtained by removing $X_1^n, \ldots, X_d^n$ from the generators of Q_i. Then $I = \bigcap_{i=1}^{l} Q_i'$ is an irredundant m-irreducible decomposition of I.

Before proving this result, we present an example.

EXAMPLE 7.5.6. Set $R = A[X, Y, Z]$ and $I = (XY, XZ, YZ)R$. Following the notation of Theorem 7.5.5, we may set $n = 2$ and

$$J = (XY, XZ, YZ)R + (X^2, Y^2, Z^2)R = (XY, XZ, YZ, X^2, Y^2, Z^2)R\mathfrak{X}^2$$

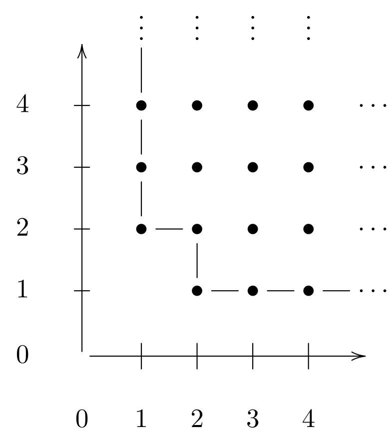
where $\mathfrak{X} = (X, Y, Z)R$. Exercise 6.3.23(a) shows that the J-corner elements are X, Y, Z and Theorem 6.2.1 yields the decomposition

$$J = \mathrm{P}_R(X) \bigcap \mathrm{P}_R(Y) \bigcap \mathrm{P}_R(Z) = (X^2, Y, Z)R \bigcap (X, Y^2, Z)R \bigcap (X, Y, Z^2)R.$$

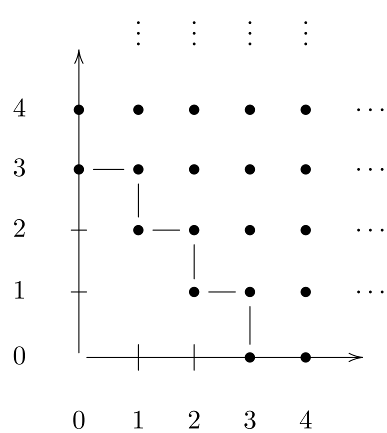
We remove the monomials X^2, Y^2, Z^2 from these ideals to obtain

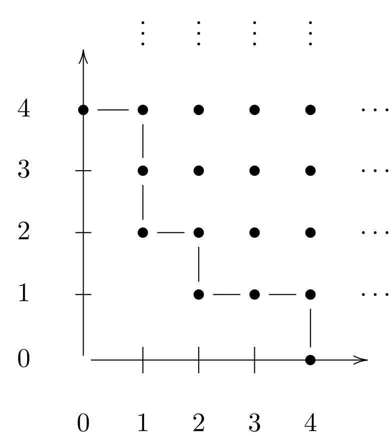
$$I = (Y,Z)R \bigcap (X,Z)R \bigcap (X,Y)R.$$

REMARK 7.5.7. Graphically, the idea behind Theorem 7.5.5 is as follows. Set $R = A[X,Y]$ and consider the ideal $(X^2Y, XY^2)R$.

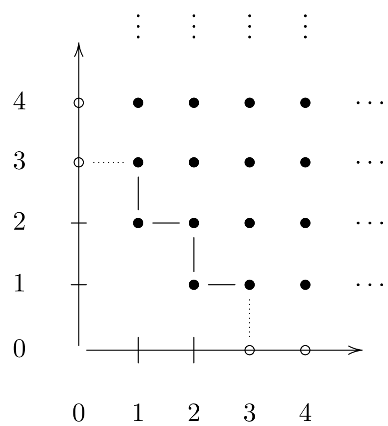


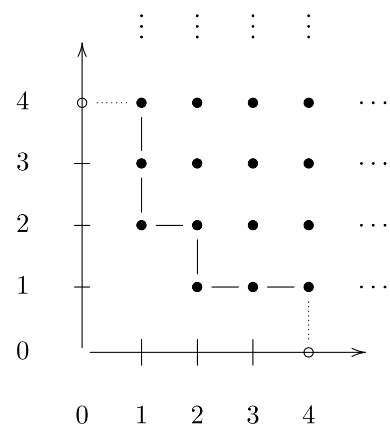
Following the notation of Theorem 7.5.5, we may choose any value $n \geqslant 3$. The next two graphs exhibit the ideal $I + (X^n, Y^n)R$ for the values $n = 3, 4$.





The point is that the ideal I can be seen as the part of J obtained by removing the generators X^n, Y^n.





Proof of Theorem 7.5.5. Recall that $I = (f_1, \ldots, f_t)R$ with $f_i = \underline{X}^{\underline{a}_i}$ for $i = 1, \ldots, t$. Given an integer $n > \max\{a_{j,i} \mid i = 1, \ldots, d \text{ and } j = 1, \ldots, t\}$, set

$$J = (X_1^n, \ldots, X_d^n)R + I = (X_1^n, \ldots, X_d^n, f_1, \ldots, f_t)R;$$

see Fact A.4.8(a). For each t-tuple $\underline{i} = (i_1, \ldots, i_t)$ such that $1 \leqslant i_k \leqslant d$, set

$$Q_{\underline{i}} = (X_1^n, \ldots, X_d^n, X_{i_1}^{a_{1,i_1}}, \ldots, X_{i_t}^{a_{t,i_t}})R$$
$$Q'_{\underline{i}} = (X_{i_1}^{a_{1,i_1}}, \ldots, X_{i_t}^{a_{t,i_t}})R.$$

Applying Theorem 7.5.3, we have

$$J = \bigcap_{i_1=1}^{d} \cdots \bigcap_{i_t=1}^{d} (X_1^n, \ldots, X_d^n, X_{i_1}^{a_{1,i_1}}, \ldots, X_{i_t}^{a_{t,i_t}})R = \bigcap_{\underline{i}} Q_{\underline{i}} \tag{7.5.7.1}$$

$$I = \bigcap_{i_1=1}^{d} \cdots \bigcap_{i_t=1}^{d} (X_{i_1}^{a_{1,i_1}}, \ldots, X_{i_t}^{a_{t,i_t}})R = \bigcap_{\underline{i}} Q'_{\underline{i}}. \tag{7.5.7.2}$$

Fact A.4.8(a) implies that $Q_{\underline{i}} = (X_1^n, \ldots, X_d^n)R + Q_{\underline{i}}$. Furthermore, since $n > a_{j,i_j}$, the ideal $Q'_{\underline{i}}$ is obtained by removing $X_1^n, \ldots, X_d^n$ from the generators of $Q_{\underline{i}}$, as in the statement of the theorem.

Claim: Given t-tuples $\underline{i}$ and $\underline{j}$, one has $Q'_{\underline{i}} \subseteq Q'_{\underline{j}}$ if and only if $Q_{\underline{i}} \subseteq Q_{\underline{j}}$. For the forward implication, if $Q'_{\underline{i}} \subseteq Q'_{\underline{j}}$, then

$$Q_{\underline{i}} = (X_1^n, \ldots, X_d^n)R + Q'_{\underline{i}} \subseteq (X_1^n, \ldots, X_d^n)R + Q'_{\underline{j}} = Q_{\underline{j}}.$$

For the converse, assume that $Q_{\underline{i}} \subseteq Q_{\underline{j}}$. Since each monomial $X_{i_p}^{a_{p,i_p}}$ is in $Q_{\underline{i}}$, it follows that $X_{i_p}^{a_{p,i_p}} \in Q_{\underline{j}}$. To prove that $Q'_{\underline{i}} \subseteq Q'_{\underline{j}}$, it suffices to show that $X_{i_p}^{a_{p,i_p}} \in Q'_{\underline{j}}$. Theorem 1.1.8 implies that $X_{i_p}^{a_{p,i_p}}$ is in the ideal generated by one of the monomials from the list $X_1^n, \ldots, X_d^n, X_{j_1}^{a_{1,j_1}}, \ldots, X_{j_t}^{a_{t,j_t}}$ of generators of $Q_{\underline{j}}$. Since $n > a_{p,i_p}$, a comparison of exponent vectors shows that $X_{i_p}^{a_{p,i_p}} \notin (X_k^n)R$ for $k = 1, \ldots, n$. Thus, there is an index q such that $X_{i_p}^{a_{p,i_p}} \in (X_{j_q}^{a_{q,j_q}})R \subseteq Q'_{\underline{j}}$

Recall that an irredundant m-irreducible decomposition of I can be obtained from (7.5.7.2) by removing the ideals $Q'_{\underline{j}}$ such that there is an ideal $Q'_{\underline{i}}$ contained in $Q'_{\underline{j}}$. Similarly, an irredundant m-irreducible decomposition of J can be obtained from (7.5.7.1) by removing the ideals $Q_{\underline{j}}$ such that there is an ideal $Q_{\underline{i}}$ contained in $Q_{\underline{j}}$. From the above claim, we see that the ideals $Q_{\underline{i}}$ removed from the decomposition (7.5.7.1) are in 1-1 correspondence with the ideals $Q'_{\underline{i}}$ removed from the decomposition (7.5.7.2). In summary, if S is a set such that $J = \bigcap_{\underline{i} \in S} Q_{\underline{i}}$ is an irredundant m-irreducible decomposition of J, then $I = \bigcap_{\underline{i} \in S} Q'_{\underline{i}}$ is an irredundant m-irreducible decomposition of I. This establishes the theorem. $\square$

Exercises.

EXERCISE 7.5.8. Verify the decomposition in Example 7.5.4 by computing the generators for $(X^1)R \bigcap (Y^3)R \bigcap (X^6, Z^5)R \bigcap (Y^4, Z^5)R \bigcap (Z^2)R$ using least common multiples and comparing to the list of generators given in Example 7.5.4. Justify your answer.

EXERCISE 7.5.9. Set $R = A[X, Y, Z]$ and $I = (X^1Y^5Z^8, X^2Y^3Z^7, X^4Y^9Z^6)R$. Use Theorem 7.5.3 as in Example 7.5.4 to find an irredundant m-irreducible decomposition of I. Verify that your decomposition is correct as in Exercise 7.5.8. Justify your answer.

EXERCISE 7.5.10. Set $R = A[X_1, \ldots, X_d]$, and let J be a non-zero monomial ideal of R with irredundant m-irreducible decomposition $J = \bigcap_{i=1}^m J_i$. Let $f_1, \ldots, f_t$ be a monomial generating sequence for J. Use Theorem 7.5.3 to prove that each ideal J_i has a generating sequence consisting of t monomials.

EXERCISE 7.5.11. Verify the decomposition $I = (Y, Z)R \bigcap (X, Z)R \bigcap (X, Y)R$ of Example 7.5.6 as in Exercise 7.5.8. Justify your answer.

EXERCISE 7.5.12. Set $R = A[X, Y, Z]$ and $I = (X^2YZ, XY^2Z, XYZ^2)R$. Use Theorem 7.5.5 as in Example 7.5.6 to find an irredundant m-irreducible decomposition of I. Verify that your decomposition is correct as in Exercise 7.5.8. Justify your answers.

EXERCISE 7.5.13. Set $R = A[X_1, \ldots, X_d]$, and let I be a monomial ideal of R with monomial generating sequence $f_1, \ldots, f_t$. For $i = 1, \ldots, t$ write $f_i = \underline{X}^{\underline{a}_i}$ where $\underline{a}_i = (a_{i,1}, \ldots, a_{i,d}) \in \mathbb{N}^d$. For $i = 1, \ldots, d$ let $a_i > \max\{a_{1,i}, \ldots, a_{t,i}\}$. Set $J = (X_1^{a_1}, \ldots, X_d^{a_d})R + I$, and let $z_1, \ldots, z_l$ be the distinct J-corner elements. For $i = 1, \ldots, l$ set $Q_i = \mathrm{P}_R(z_i)$, and let Q'_i be the m-irreducible ideal obtained by removing $X_1^{a_1}, \ldots, X_d^{a_d}$ from the generators of Q_i. Prove that $I = \bigcap_{i=1}^l Q'_i$ is an irredundant m-irreducible decomposition of I.

Methods for Computing General M-Irreducible Decompositions in Macaulay2.

Exercises.

7.6. Exploration: Decompositions of Generalized Bracket Powers

In this section, A is a non-zero commutative ring with identity. Set $R = A[X_1, \ldots, X_d]$, and fix a d-tuple $\underline{e} \in \mathbb{N}^d$ such that $e_1, \ldots, e_d \geqslant 1$. For the basic properties of generalized bracket powers of monomial ideals, see Section 2.6.

EXERCISE 7.6.1. Let I be a monomial ideal of R with m-irreducible decomposition $I = \bigcap_{j=1}^{n} I_j$.

(a) Prove that the ideal I is m-irreducible if and only if $I^{[\underline{e}]}$ is m-irreducible.
(b) Prove that an m-irreducible decomposition of $I^{[\underline{e}]}$ is $I^{[\underline{e}]} = \bigcap_{j=1}^{n} I_j{}^{[\underline{e}]}$.
(c) Prove that the decomposition $I = \bigcap_{j=1}^{n} I_j$ is irredundant if and only if the decomposition $I^{[\underline{e}]} = \bigcap_{j=1}^{n} I_j{}^{[\underline{e}]}$ is irredundant.

EXERCISE 7.6.2. Set $R = A[X,Y]$ and $\underline{e} = (2,3)$. Set $J = (X^3, X^2Y, Y^3)R$, and use Exercise 7.6.1 to find an irredundant m-irreducible decomposition of the ideal $J^{[\underline{e}]}$. Justify your answer.

EXERCISE 7.6.3. Let I be a monomial ideal of R.

(a) Prove that I is a parameter ideal if and only if $I^{[\underline{e}]}$ is a parameter ideal.
(b) Prove that if I has a parametric decomposition $I = \bigcap_{j=1}^{n} I_j$, then $I^{[\underline{e}]} = \bigcap_{j=1}^{n} I_j{}^{[\underline{e}]}$ is a parametric decomposition of $I^{[\underline{e}]}$.
(c) Prove that I has a parametric decomposition if and only if $I^{[\underline{e}]}$ has a parametric decomposition

EXERCISE 7.6.4. Let I be a monomial ideal of R. For each monomial $f = \underline{X}^{\underline{n}}$ in R, set $f^{(\underline{e})} = X_1^{e_1(n_1+1)-1} \cdots X_d^{e_d(n_d+1)-1}$. Prove that $\mathrm{C}_R(I^{[\underline{e}]}) = \{f^{(\underline{e})} \mid f \in \mathrm{C}_R(I)\}$.

Decompositions of Generalized Bracket Powers in Macaulay2.

Exercises.

7.7. Exploration: Decompositions of Products of Monomial Ideals

In this section, A is a non-zero commutative ring with identity.

The final section of this chapter investigates the problem of finding m-irreducible decompositions of products of monomial ideals. We provide an algorithm for computing such decompositions, but it is highly redundant; see Example 7.7.5.

EXERCISE 7.7.1. Let $J_1, \ldots, J_n$ be monomial ideals of R, and let $f \in [\![R]\!]$.

(a) Prove that $f(\bigcap_{i=1}^{n} J_i) = \bigcap_{i=1}^{n}(fJ_i)$.
(b) If I is a monomial ideal of R, must one have $I(\bigcap_{i=1}^{n} J_i) = \bigcap_{i=1}^{n}(IJ_i)$? Justify your answer.

EXERCISE 7.7.2. Fix positive integers $k, t_1, \ldots, t_k, e_1, \ldots, e_k$ such that $1 \leqslant t_1 < \cdots < t_k \leqslant d$, and set $J = (X_{t_i}^{e_1}, \ldots, X_{t_k}^{e_k})R$. Let $f = \underline{X}^{\underline{a}} \in [\![R]\!]$, and set $J' = (X_{t_1}^{e_1+a_{t_1}}, \ldots, X_{t_k}^{e_k+a_{t_k}})R$. Prove that $fJ = (f)R \bigcap J'$. (Hint: Use lcm's to compute a monomial generating sequence for $(f)R \bigcap J'$.)

EXERCISE 7.7.3. Set $R = A[X,Y,Z]$. In the notation of Exercise 7.7.2, compute J' where $J = (X^2, Z^3)R$ and $f = Y^3Z^2$.

EXERCISE 7.7.4. Let I and J be non-zero monomial ideals in R such that $J \neq R$. Here is an algorithm for computing an m-irreducible decomposition of the product IJ. It combines a monomial generating sequence for I with an m-irreducible decomposition of J.

Step 1. Let $f_1,\ldots,f_m$ be a monomial generating sequence for I. Note that Fact A.4.8(b) implies that $I=\sum_{j=1}^m (f_j)$.

Step 2. For $j=1,\ldots,m$ write $f_j=\underline{X}^{\underline{a}_j}\in [\![R]\!]$ where $\underline{a}_j=(a_{j,1},\ldots,a_{j_d})\in\mathbb{N}^d$.

Step 3. Write each f_j in terms of positive exponents: For $j=1,\ldots,m$ fix positive integers $l_j,s_{j,1},\ldots,s_{j,l_j}$ such that the exponents $a_{s_{j,1}},\ldots,a_{s_{j,l_j}}$ are positive and $f=X_{s_{j,1}}^{a_{s_{j,1}}}\cdots X_{s_{j,l_j}}^{a_{s_{j,l_j}}}$. Note that Proposition 2.1.5 and Theorem 3.1.3 imply that $(f_j)R=\bigcap_{p=1}^{l_j}(X_{s_{j,p}}^{a_{s_{j,p}}})R$ is an irredundant m-irreducible decomposition.

Step 4. Fix an m-irreducible decomposition $J=\bigcap_{i=1}^n J_i$. Fix positive integers $k_i,t_{i,1},\ldots,t_{i,k_i},e_{i,1},\ldots,e_{i,k_i}$ such that $1\leqslant t_{i,1}<\cdots<t_{i,k_i}\leqslant d$ and $J_i=(X_{t_{i,1}}^{e_{i,1}},\ldots,X_{t_{i,k_i}}^{e_{i,k_i}})R$. Set $J_{i,j}=(X_{t_{i,1}}^{e_{i,1}+a_{j,t_{i,1}}},\ldots,X_{t_{i,k_i}}^{e_{i,k_i}+a_{j,t_{i,k_i}}})R$.

Step 5. Decompose IJ as follows:

$$
\begin{aligned}
IJ &= \left(\textstyle\sum_{j=1}^m (f_j)R\right)(\textstyle\bigcap_{i=1}^n J_i) && \text{by assumption (see Step 1)}\\
&= \textstyle\sum_{j=1}^m (f_j(\bigcap_{i=1}^n J_i)) && \text{Fact A.4.12(d)}\\
&= \textstyle\sum_{j=1}^m \bigcap_{i=1}^n (f_jJ_i) && \text{Exercise 7.7.1(a)}\\
&= \textstyle\sum_{j=1}^m \bigcap_{i=1}^n ((f_j)R\bigcap J_{i,j}) && \text{Exercise 7.7.2}\\
&= \textstyle\sum_{j=1}^m ((f_j)R\bigcap(\bigcap_{i=1}^n J_{i,j})) && \text{basic properties of intersections}\\
&= \textstyle\sum_{j=1}^m ((\bigcap_{p=1}^{l_j}(X_{s_{j,p}}^{a_{s_{j,p}}})R)\bigcap(\bigcap_{i=1}^n J_{i,j})) && \text{Step 3}
\end{aligned}
$$

Step 6. Use Exercise 7.3.13 to find an m-irreducible decomposition of the ideal $IJ=\sum_{j=1}^m((\bigcap_{p=1}^{l_j}(X_{s_{j,p}}^{a_{s_{j,p}}})R)\bigcap(\bigcap_{i=1}^n J_{i,j}))$.

Example 7.7.5. Set $R=A[X,Y]$. We use Exercise 7.7.4 to find an m-irreducible decomposition of the ideal IJ where $I=(X,Y)R$ and $J=(X^2,XY,Y^2)R$. We use the monomial generating sequence X,Y for I, and the m-irreducible decomposition $J=(X^2,Y)R\bigcap(X,Y^2)R$. In the following computation, the equalities

(1)–(5) follow the sequence of equalities in Exercise 7.7.4:

$$
\begin{aligned}
IJ &\overset{(1)}{=} [(X)R + (Y)R][(X^2, Y)R \bigcap (X, Y^2)R] \\
&\overset{(2)}{=} X[(X^2, Y)R \bigcap (X, Y^2)R] \\
&\quad + Y[(X^2, Y)R \bigcap (X, Y^2)R] \\
&\overset{(3)}{=} [X(X^2, Y)R \bigcap X(X, Y^2)R] \\
&\quad + [Y(X^2, Y)R \bigcap Y(X, Y^2)R] \\
&\overset{(4)}{=} [(X)R \bigcap (X^3, Y)R \bigcap (X)R \bigcap (X^2, Y^2)R] \\
&\quad + [(Y)R \bigcap (X^2, Y^2)R \bigcap (Y)R \bigcap (X, Y^3)R] \\
&\overset{(5)}{=} [(X)R \bigcap (X^3, Y)R \bigcap (X^2, Y^2)R] \\
&\quad + [(Y)R \bigcap (X^2, Y^2)R \bigcap (X, Y^3)R] \\
&\overset{(6)}{=} [(X)R + (Y)R] \bigcap [(X)R + (X^2, Y^2)R] \bigcap [(X)R + (X, Y^3)R] \\
&\bigcap [(X^3, Y)R + (Y)R] \bigcap [(X^3, Y)R + (X^2, Y^2)R] \bigcap [(X^3, Y)R + (X, Y^3)R] \\
&\bigcap [(X^2, Y^2)R + (Y)R] \bigcap [(X^2, Y^2)R + (X^2, Y^2)R] \bigcap [(X^2, Y^2)R + (X, Y^3)R] \\
&\overset{(7)}{=} (X, Y)R \bigcap (X, Y^2)R \bigcap (X, Y^3)R \\
&\quad \bigcap (X^3, Y)R \bigcap (X^2, Y)R \bigcap (X, Y)R \\
&\quad \bigcap (X^2, Y)R \bigcap (X^2, Y^2)R \bigcap (X, Y^2)R \\
&\overset{(8)}{=} (X, Y^3)R \bigcap (X^3, Y)R \bigcap (X^2, Y^2)R
\end{aligned}
$$

The equality (6) is from Exercise 7.3.13, and (7) is from Fact A.4.8(b). The equality (8) follows from an application of Algorithm 3.3.5.

(Note that $IJ = \mathfrak{X}^3$ where $\mathfrak{X} = (X, Y)R = I$, and this decomposition agrees with the one obtained in Example 6.2.2.)

EXERCISE 7.7.6. Set $R = A[X, Y]$, and use Exercise 7.7.4 to find an m-irreducible decomposition of the ideal IJ in each of the following cases:

(a) $I = (X, Y)R$ and $J = (X^3, XY, Y^2)R$.
(b) $I = (X^2, XY, Y^2)R = J$.

Decompositions of Products of Monomial Ideals in Macaulay2.

Exercises.

Part 4

Commutative Algebra and Macaulay2

APPENDIX A

Foundational Concepts

This chapter contains a review of certain fundamental concepts in abstract algebra for use throughout the text. Section A.1 deals with the basic properties of commutative rings with identity, and Section A.2 focuses on polynomial rings. Section A.3 introduces ideals, while Sections A.4 and B.5 investigate several methods for building new ideals from old ones. The chapter ends with Section A.7, dealing with relations on sets, and Section 1.5 which is a combinatorial exploration.

A.1. Rings

The following term was coined by David Hilbert. The axiomatic description was formalized by Emmy Noether.

Definition A.1.1. A *commutative ring with identity* is a set R equipped with two binary operations (addition and multiplication) satisfying the following axioms:

(1) (closure under addition) for all $r, s \in R$ we have $r + s \in R$;
(2) (associativity of addition) for all $r, s, t \in R$ we have $(r + s) + t = r + (s + t)$;
(3) (commutativity of addition) for all $r, s \in R$ we have $r + s = s + r$;
(4) (additive identity) there exists an element $z \in R$ such that for all $r \in R$, we have $z + r = r$;
(5) (additive inverse) for each $r \in R$ there exists an element $s \in R$ such that $r + s = z$ where z is the additive identity;
(6) (closure under multiplication) for all $r, s \in R$ we have $rs \in R$;
(7) (associativity of multiplication) for all $r, s, t \in R$ we have $(rs)t = r(st)$;
(8) (commutativity of multiplication) for all $r, s \in R$ we have $rs = sr$;
(9) (multiplicative identity) there exists an element $m \in R$ such that for all $r \in R$, we have $mr = r$;
(10) (distributivity) for all $r, s, t \in R$, we have $r(s + t) = rs + rt$.

We include the following examples for the sake of thoroughness, and in order to specify some notation.

Example A.1.2. Here are some examples.

(a) The set of integers $\mathbb{Z}$ with the usual addition and multiplication, and with identities $z = 0$ and $m = 1$, is a commutative ring with identity.
(b) The set of rational numbers $\mathbb{Q}$ with the usual addition and multiplication, and with $z = 0$ and $m = 1$, is a commutative ring with identity.
(c) The set of real numbers $\mathbb{R}$ with the usual addition and multiplication, and with $z = 0$ and $m = 1$, is a commutative ring with identity.
(d) The set of complex numbers $\mathbb{C}$ with the usual addition and multiplication, and with $z = 0$ and $m = 1$, is a commutative ring with identity.

(e) The set of natural numbers $\mathbb{N} = \{n \in \mathbb{Z} \mid n \geqslant 0\}$ with the usual addition and multiplication is not a commutative ring with identity because it does not have additive inverses.
(f) The set of even integers $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$ with the usual addition and multiplication is not a commutative ring with identity because it does not have a multiplicative identity.
(g) The set $\mathrm{M}_2(\mathbb{R})$ of 2×2 matrices with entries in $\mathbb{R}$, with the usual addition and multiplication is not a commutative ring with identity because multiplication is not commutative.
(h) Fix an integer $n \geqslant 2$ and let $\mathbb{Z}_n = \{m \in \mathbb{Z} \mid 0 \leqslant m < n\}$. For $r, s \in \mathbb{Z}_n$ we define operations on $\mathbb{Z}_n$ by the following formulas:

$$r \oplus s := \text{the remainder after } r + s \text{ is divided by } n$$
$$r \odot s := \text{the remainder after } rs \text{ is divided by } n.$$

With $z = 0$ and $m = 1$, this makes $\mathbb{Z}_n$ into a commutative ring with identity. Note that when $0 < m < n$, the additive inverse of m in $\mathbb{Z}_n$ is $n - m$.
(i) The set $\mathrm{C}(\mathbb{R})$ of continuous functions $f \colon \mathbb{R} \to \mathbb{R}$, with pointwise addition and multiplication, and with the constant functions $z = 0$ and $m = 1$, is a commutative ring with identity.
(j) The set $\mathrm{D}(\mathbb{R})$ of differentiable functions $f \colon \mathbb{R} \to \mathbb{R}$, with pointwise addition and multiplication, and with the constant functions $z = 0$ and $m = 1$, is a commutative ring with identity.

Most of the facts in this section are routine exercises showing that arithmetic in a commutative ring with identity is very similar to arithmetic in $\mathbb{Z}$.

Fact A.1.3. Let R be a commutative ring with identity.
(a) The additive and multiplicative identities for R are unique; we denote them 0_R and 1_R, respectively, or 0 and 1 when the context is clear.
(b) For each $r \in R$, the additive inverse of r in R is unique; we denote it $-r$.
(c) (cancellation) Let $r, s, t \in R$. If $r + s = r + t$, then $s = t$. If $r + s = t + s$, then $r = t$.

Fact A.1.4. Let R be a commutative ring with identity.
(a) For all $r \in R$, we have $0_R r = 0_R$.
(b) For all $r, s \in R$, we have $(-r)s = -(rs) = r(-s)$.
(c) For all $r \in R$, we have $-r = (-1_R)r$. This implies that $-0_R = 0_R$.
(d) For all $r \in R$, we have $-(-r) = r$. This implies that for all $r, s \in R$, we have $(-r)(-s) = rs$.

Definition A.1.5. Let R be a commutative ring with identity For all $r, s \in R$ we set $r - s = r + (-s)$.

Fact A.1.6. Let R be a commutative ring with identity.
(a) (closure under subtraction) For all $r, s \in R$ we have $r - s \in R$.
(b) For all $r, s, t \in R$ we have $r(s - t) = rs - rt$.
(c) For all $r, s \in R$ we have $-(r - s) = s - r$.
(d) For all $r \in R$ we have $r - r = 0_R$.

Here is a formal definition of nr and r^n where $n \in \mathbb{N}$.

Definition A.1.7. Let R be a commutative ring with identity and let $r \in R$.

(a) Set $0r = 0_R$ and $1r = r$. Inductively, for each $n \in \mathbb{N}$, define $(n+1)r = r + (nr)$.
(b) Set $(-1)r = -r$. Inductively, for each $n \in \mathbb{N}$ with, define $(-n-1)r = (-n)r - r$.
(c) Set $r^0 = 1_R$ and $r^1 = r$. Inductively, for each $n \in \mathbb{N}$ with, define $r^{n+1} = r^n r$.

FACT A.1.8. Let R be a commutative ring with identity.
(a) For all $r, s \in R$ and $n \in \mathbb{Z}$ we have $(nr)s = n(rs) = r(ns)$.
(b) For all $r \in R$ and $m, n \in \mathbb{Z}$ we have $(m+n)r = mr + nr$ and $(mn)r = m(nr)$.
(c) For all $r, s \in R$ and $n \in \mathbb{N}$ we have $(rs)^n = r^n s^n$.
(d) For all $r \in R$ and $m, n \in \mathbb{N}$ we have $r^m r^n = r^{m+n}$ and $(r^m)^n = r^{mn}$.

DEFINITION A.1.9. Let R be a commutative ring with identity. Let $n \geqslant 1$ be an integer, and let $r_1, \ldots, r_n \in R$.

We define the sum $\sum_{i=1}^n r_i = r_1 + \cdots + r_n$ inductively. For $n = 1, 2$ we have $\sum_{i=1}^1 r_i = r_1$ and $\sum_{i=1}^2 r_i = r_1 + r_2$. For $n \geqslant 3$, we define $\sum_{i=1}^n r_i = (\sum_{i=1}^{n-1} r_i) + r_n$.

We define the product $\prod_{i=1}^n r_i = r_1 \cdots r_n$ inductively. For $n = 1, 2$ we have $\prod_{i=1}^1 r_i = r_1$ and $\prod_{i=1}^2 r_i = r_1 r_2$. For $n \geqslant 3$, we define $\prod_{i=1}^n r_i = (\prod_{i=1}^{n-1} r_i) r_n$.

FACT A.1.10. Let R be a commutative ring with identity. Let $n \geqslant 1$ be an integer, and let $r_1, \ldots, r_n, s_1, \ldots, s_n \in R$.
(a) (generalized closure laws) We have $\sum_{i=1}^n r_i \in R$ and $\prod_{i=1}^n r_i \in R$.
(b) (generalized associative laws) Any two "meaningful sums" of the elements $r_1, \ldots, r_n$ in this order are equal. For instance, we have $((r+s)+t)+u = (r+s)+(t+u) = r+((s+t)+u)$ for all $r, s, t, u \in R$. Any two "meaningful products" of the elements $r_1, \ldots, r_n$ in this order are equal.
(c) (generalized commutative law) Given any permutation $i_1, \ldots, i_n$ of the numbers $1, \ldots, n$ we have $r_1 + \cdots + r_n = r_{i_1} + \cdots + r_{i_n}$ and $r_1 \cdots r_n = r_{i_1} \cdots r_{i_n}$.
(d) (generalized distributive law) For all sequences $r_1, \ldots, r_m, s_1, \ldots, s_n \in R$ we have $(\sum_{i=1}^m r_i)(\sum_{j=1}^n s_j) = \sum_{i=1}^m \sum_{j=1}^n r_i s_j$. (There are more general generalized distributive laws for products of more than two sums. One verifies them by induction on the number of sums.)

(If you find parts (b) and (c) to be difficult, consult [**22**, I.1.6–7].)

The next notation is fundamental for this text.

DEFINITION A.1.11. Let R be a commutative ring with identity. A *monomial* in the elements $X_1, \ldots, X_d \in R$ is an element of the form $X_1^{n_1} \cdots X_d^{n_d} \in R$ where $n_1, \ldots, n_d \in \mathbb{N}$. For short, we write $\underline{n} = (n_1, \ldots, n_d) \in \mathbb{N}^d$ and $\underline{X}^{\underline{n}} = X_1^{n_1} \cdots X_d^{n_d}$. Define addition and scalar multiplication in $\mathbb{N}^d$ coordinate-wise: for $\underline{m} = (m_1, \ldots, m_d) \in \mathbb{N}^d$ and $p \in \mathbb{N}$, set $\underline{m} + \underline{n} = (m_1 + n_1, \ldots, m_d + n_d) \in \mathbb{N}^d$ and $p\underline{n} = (pn_1, \ldots, pn_d) \in \mathbb{N}^d$.

FACT A.1.12. Let R be a commutative ring with identity, and let $X_1, \ldots, X_d \in R$. For all $\underline{m}, \underline{n} \in \mathbb{N}^d$ and $p \in \mathbb{N}$ we have $\underline{X}^{\underline{m}} \underline{X}^{\underline{n}} = \underline{X}^{\underline{m}+\underline{n}}$ and $(\underline{X}^{\underline{m}})^p = \underline{X}^{p\underline{m}}$.

DEFINITION A.1.13. Let R be a commutative ring with identity. An element $r \in R$ is a *unit* in R if there exists an element $s \in R$ such that $sr = 1_R$; such an element s is a *multiplicative inverse* for r.

EXAMPLE A.1.14. Here is what happens for some basic rings.
(a) An integer m is a unit in $\mathbb{Z}$ if and only if $m = \pm 1$.
(b) Let $n \in \mathbb{Z}$ with $n \geqslant 2$, and let $m \in \mathbb{Z}_n$. Then m is a unit in $\mathbb{Z}_n$ if and only if $\gcd(m, n) = 1$.

FACT A.1.15. Let R be a commutative ring with identity.

(a) If r is a unit in R then it has a unique multiplicative inverse; we denote the multiplicative inverse of r by r^{-1}.
(b) If $1_R \neq 0_R$ and r is a unit in R, then $r \neq 0$.

DEFINITION A.1.16. Let R be a commutative ring with identity. Then R is a *field* if $1_R \neq 0_R$ and every non-zero element of R is a unit in R.

EXAMPLE A.1.17. Here is what happens for the standard rings.

(a) The rings $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields.
(b) The ring $\mathbb{Z}$ is not a field.
(c) Let $n \in \mathbb{Z}$ with $n \geqslant 1$. The ring $\mathbb{Z}_n$ is a field if and only if n is prime.

DEFINITION A.1.18. Let R be a commutative ring with identity. A subset $S \subseteq R$ is a *subring* of R provided that it is a commutative ring under the operations of R with identity $1_S = 1_R$.

EXAMPLE A.1.19. The ring $\mathbb{Z}$ is a subring of $\mathbb{Q}$, and $\mathbb{Q}$ is a subring of $\mathbb{R}$.

FACT A.1.20. Let R be a commutative ring with identity, and let $S \subseteq R$ be a subring. Then $0_S = 0_R$.

The next example shows that the condition $1_S = 1_R$ is not automatic.

EXAMPLE A.1.21. Let $R = \{\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) \mid a, b \in \mathbb{R}\}$ and $S = \{\left(\begin{smallmatrix} a & 0 \\ 0 & 0 \end{smallmatrix}\right) \mid a \in \mathbb{R}\}$. Then R and S are commutative rings with identity, under the standard addition and multiplication of matrices. However, we have $1_R = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $1_S = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, so we have $1_R \neq 1_S$.

The notion of divisibility plays a crucial role in the rest of this text.

DEFINITION A.1.22. Let R be a commutative ring with identity, and let $r, s \in R$. We say that r *divides* s when there is an element $t \in R$ such that $s = rt$. When r divides s, we write $r \big| s$.

Exercises.

EXERCISE A.1.23. Let R be a commutative ring with identity. If n is a positive integer, define $n1_R$ to be the n-fold sum $n1_R = 1_R + \cdots + 1_R$. If n is a negative integer, define $n1_R = -((-n)1_R) = (-1_R) + \cdots + (-1_R)$. For $n = 0$, define $01_R = 0_R$. Define $F_R \colon \mathbb{Z} \to R$ by the formula $F_R(n) = n1_R$. Show that for all $m, n \in \mathbb{Z}$ we have $F_R(m+n) = F_R(m) + F_R(n)$ and $F_R(mn) = F_R(m)F_R(n)$.

*EXERCISE A.1.24. (binomial theorem) Let R be a commutative ring with identity and let $r, s \in R$. Prove that for each positive integer n, there is an equality $(r+s)^n = \sum_{i=0}^{n} \binom{n}{i} r^i s^{n-i}$. (This exercise is used in the proof of Proposition A.6.3.)

EXERCISE A.1.25. Let f, g, h be elements of a ring R. Prove or disprove the following: If $h \neq 0_R$ and $fh = gh$, then $f = g$.

A.2. Polynomial Rings

In this section, A is a commutative ring with identity.

This section introduces, the main rings of study in this text: polynomial rings.

THEOREM A.2.1. *There exists a commutative ring with identity $A[X]$ with the following properties:*

(1) *The ring A is a subring of $A[X]$.*
(2) *There is an element $X \in A[X] \smallsetminus A$ such that for every $f \in A[X]$, there exist $n \in \mathbb{N}$ and $a_0, a_1 \ldots, a_n \in A$ such that $f = a_0 + a_1X + \cdots + a_nX^n$;*
(3) *The elements $1_A, X, X^2, X^3, \ldots$ are linearly independent over A, that is, we have $a_0 + a_1X + \cdots + a_nX^n = 0_A$ if and only if $a_0 = a_1 = \cdots = a_n = 0_A$.*

SKETCH OF PROOF. Set $A[X]$ equal to the set of sequences in A which are eventually zero:

$$A[X] = \{(a_0, a_1, a_2, \ldots) \mid a_0, a_1, a_2, \ldots \in A \text{ and } a_i = 0_A \text{ for all } i \gg 0\}.$$

We define addition and multiplication as follows:

$$(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots)$$
$$(a_0, a_1, a_2, \ldots)(b_0, b_1, b_2, \ldots) = (c_0, c_1, c_2, \ldots)$$

where $c_n = \sum_{i=0}^{n} a_i b_{n-i}$. It is straightforward to show that the axioms for a commutative ring with identity are satisfied with $0_{A[X]} = (0_A, 0_A, 0_A, \ldots)$ and $1_{A[X]} = (1_A, 0_A, 0_A, \ldots)$.

For each $a \in A$, we identify a with the sequence $(a, 0_A, 0_A, \ldots)$. This identification makes A into a subset of $A[X]$. It is straightforward to show that the addition and multiplication are compatible under this identification.

Set $X = (0_A, 1_A, 0_A, 0_A, \ldots)$ and note that

$$X^n = (\underbrace{0_A, 0_A, \ldots, 0_A}_{n \text{ terms}}, 1_A, 0_A, 0_A, \ldots).$$

It is straightforward to show that properties (2) and (3) are satisfied. □

DEFINITION A.2.2. The ring $A[X]$ is the *polynomial ring* in one variable with coefficients in A. An element $f \in A[X]$ is a *polynomial* in one variable with coefficients in A. The (unique) elements $a_0, a_1 \ldots, a_n \in A$ such that $f = a_0 + a_1X + \cdots + a_nX^n$ are the *coefficients* of f. The element $X \in A[X]$ is the *variable* or *indeterminate*. If $0 \neq f \in A[X]$, then the smallest $n \in \mathbb{N}$ such that f can be written in the form $f = a_0 + a_1X + \cdots + a_nX^n$ is the *degree* of f; the corresponding coefficient a_n is the *leading coefficient* of f. If the leading coefficient of f is 1_A, then f is *monic*. The coefficient a_0 is the *constant term* of f. Elements of A are sometimes called *constant polynomials*. We often employ the notation $f = \sum_{i \in \mathbb{N}}^{\text{finite}} a_i X^i$ for elements $f \in A[X]$.

REMARK A.2.3. (a) The constant polynomial $0_A \in A[X]$ does not have a well-defined degree.

(b) Theorem A.2.1(3) implies that if $a_0 + a_1X + \cdots + a_mX^m = b_0 + b_1X + \cdots + b_nX^n$ in $A[X]$ and $m \leqslant n$, then $a_i = b_i$ for $i = 0, \ldots, m$ and $b_i = 0_A$ for $i = m + 1, \ldots, n$.
(c) The ring A is identified with the set of constant polynomials in $A[X]$:

$$A = \{a + 0_AX + 0_AX^2 + \cdots \mid a \in A\}.$$

REMARK A.2.4. A polynomial $f = a_0 + a_1X + \cdots + a_nX^n \in A[X]$ gives rise to a well-defined function $f \colon A \to A$ by the rule $f(b) = a_0 + a_1b + \cdots + a_nb^n$.

For the next definition, see A.1.11 for the notation $\underline{X}^{\underline{n}}$.

Definition A.2.5. (a) Inductively, for $d \geqslant 2$, the *polynomial ring* in d variables $X_1, \ldots, X_d$ with coefficients in A is $A[X_1, \ldots, X_d] = A[X_1, \ldots, X_{d-1}][X_d]$. For a small number of variables, we sometimes write $A[X, Y]$ and $A[X, Y, Z]$.

(b) The *polynomial ring* in infinitely many variables $X_1, X_2, X_3, \ldots$ with coefficients in A is $A[X_1, X_2, X_3, \ldots] = \cup_{d=1}^{\infty} A[X_1, \ldots, X_d]$.

(c) The *(total) degree* of a monomial $f = \underline{X}^{\underline{n}}$ is $\deg(f) = |\underline{n}| = n_1 + \ldots + n_d$.

Corollary A.2.6. *The set $A[X_1, \ldots, X_d]$ is a commutative ring with identity satisfying the following properties:*

(a) *The ring A is a subring of $A[X_1, \ldots, X_d]$.*

(b) *For every $f \in A[X_1, \ldots, X_d]$, there is a finite collection of indices $\underline{n} \in \mathbb{N}^d$ and elements $a_{\underline{n}} \in A$ such that*

$$f = \sum_{\underline{n} \in \mathbb{N}^d}^{\text{finite}} a_{\underline{n}} \underline{X}^{\underline{n}} = \sum_{n_1, \ldots, n_d \in \mathbb{N}}^{\text{finite}} a_{n_1, \ldots, n_d} X_1^{n_1} \cdots X_d^{n_d}.$$

(c) *The set of monomials $\{\underline{X}^{\underline{n}} \mid \underline{n} \in \mathbb{N}^d\}$ is linearly independent over A, that is, we have $\sum_{\underline{n} \in \mathbb{N}^d}^{\text{finite}} a_{\underline{n}} \underline{X}^{\underline{n}} = 0_A$ if and only if each $a_{\underline{n}} = 0_A$.*

Proof. By induction on d. The base case $d = 1$ is in Theorem A.2.1. $\square$

Definition A.2.7. For a polynomial $f \in A[X_1, \ldots, X_d]$, we say that a monomial $\underline{X}^{\underline{n}}$ *occurs* in f if the corresponding coefficient $a_{\underline{n}}$ is non-zero. The polynomial f is *homogeneous* if every monomial occurring in f has the same degree.

Example A.2.8. In the ring $R = \mathbb{Z}[X, Y, Z]$, the monomials occurring in the polynomial $3XY - 7X^2Z^3$ are XY and X^2Z^3. this polynomial is not homogeneous because monomials of degree 2 and 5 occur in it. On the other hand, the polynomial $X^2Y^2 + XYZ^2$ is homogeneous of degree 4.

Remark A.2.9. A polynomial $f = \sum_{\underline{n} \in \mathbb{N}^d}^{\text{finite}} a_{\underline{n}} \underline{X}^{\underline{n}} \in A[\underline{X}]$ gives rise to a well-defined function $f \colon A^d \to A$ by the rule $f(\underline{x}) = \sum_{\underline{n} \in \mathbb{N}^d}^{\text{finite}} a_{\underline{n}} \underline{x}^{\underline{n}}$.

Exercises.

Exercise A.2.10. Perform the following polynomial computations, showing your steps and simplifying your answers.

(a) In $\mathbb{Q}[X, Y, Z]$: $(3XY + 7Z^2 - XY^2Z + 5)(X + Z - Y^2 + X^3Y^2Z)$

(b) In $\mathbb{Z}_4[X]$: $(2X^2 + 2)^2$. This shows that one can have $f^n = 0$ even when $f \neq 0$.

(c) In $\mathbb{Z}_4[X]$: $(2X^2 + 1)^2$. This shows that $\deg(f^n)$ can be strictly smaller than $n \deg(f)$.

Exercise A.2.11. Under what conditions can $A[X]$ be a field? Justify your answer with a proof.

Exercise A.2.12. Find a commutative ring with identity A and a non-zero polynomial $f \in A[X]$ such that the induced function $f \colon A \to A$ is the zero function. Justify your answer.

*Exercise A.2.13. Consider polynomials $f_1, \ldots, f_n \in A[X]$. Assume that each polynomial has degree at most N, that is, we have $f_i = a_{i,0} + a_{i,1}X + \cdots + a_{i,N}X^N$ for $i = 1, \ldots, N$. Prove that if $\sum_{i=1}^n a_{i,N} \neq 0_A$, then $\sum_{i=1}^n f_i$ has degree N and leading coefficient $\sum_{i=1}^n a_{i,N}$. (This exercise is used in the proof of Theorem 1.4.5.)

EXERCISE A.2.14. Let p be a prime number and set $R = \mathbb{Z}_p[X_1, \ldots, X_d]$. Let $f, g \in R$. Prove that for each integer $e \geqslant 1$ one has $(f+g)^{p^e} = f^{p^e} + g^{p^e}$. Show that the analogous result for $(f+g)^k$ need not hold when k is not a power of p.

EXERCISE A.2.15. Determine whether the following polynomials in $\mathbb{Q}[X, Y, Z]$ are homogeneous: $3XY + 7Z^2 - XY^2Z + 5$ and $XZ^5 + Y^5Z - XY^2Z^2 + X^3Y^2Z$. Justify your answers.

EXERCISE A.2.16. Prove that any product of two homogeneous polynomials in $A[X_1, \ldots, X_d]$ is homogeneous.

A.3. Ideals and Generators

In this section, R is a commutative ring with identity.

The following definition was first made by Richard Dedekind, as a generalization of Ernst Kummer's "ideal numbers". The definition extends the well-known properties of even integers under addition and multiplication, namely that the sum of two even integers is even, and the product of an integer and an even integer is again even.

DEFINITION A.3.1. An *ideal* of R is a subset $I \subseteq R$ satisfying the following axioms:
(1) $I \neq \emptyset$;
(2) (closure under addition) for all $a, b \in I$ we have $a + b \in I$;
(3) (closure under external multiplication) for all $r \in R$ and $a \in I$ we have $ra \in I$.

FACT A.3.2. Let $I \subseteq R$ be an ideal.
(a) We have $0_R \in I$.
(b) (closure under additive inverses) If $a \in I$, then $-a \in I$.
(c) (closure under subtraction) For all $a, b \in I$ we have $a - b \in I$.
(d) For all $r \in R$ and all $a \in I$ we have $r + a \in I$ if and only if $r \in I$.
(e) (generalized closure law) For all $r_1, \ldots, r_n \in I$ we have $\sum_{i=1}^n r_i \in I$.
(f) We have $I = R$ if and only if $1_R \in I$.

EXAMPLE A.3.3. (a) For each $n \in \mathbb{Z}$, the set $n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$. For instance, if $n = 2$, then we have the set of even integers $2\mathbb{Z}$, which is an ideal of $\mathbb{Z}$. On the other hand, the set of odd integers is not an ideal of $\mathbb{Z}$ because it is not closed under addition.
(b) If R is a commutative ring with identity, then the sets $\{0_R\}$ and R are ideals of R. Moreover $\{0_R\}$ is the unique smallest ideal of R and R is the unique largest ideal of R. For obvious reasons, we often write 0 for the ideal $\{0_R\}$.
(c) The ring $\mathbb{Q}$ has precisely two ideals: 0 and $\mathbb{Q}$. Similar statements hold for $\mathbb{R}$ and $\mathbb{C}$.
(d) The set $\{f \in \mathrm{C}(\mathbb{R}) \mid f(2) = 0\}$ is an ideal of $\mathrm{C}(\mathbb{R})$. On the other hand, the set $\{f \in \mathrm{C}(\mathbb{R}) \mid f(2) = 1\}$ is not an ideal of $\mathrm{C}(\mathbb{R})$ because it is not closed under addition.

FACT A.3.4. (a) If $\{I_\lambda\}_{\lambda \in \Lambda}$ is a set of ideals of R, then $\bigcap_{\lambda \in \Lambda} I_\lambda$ is an ideal of R.
(b) If $\{I_\lambda\}_{\lambda \in \Lambda}$ is a set of ideals of R, then $\cup_{\lambda \in \Lambda} I_\lambda$ need not be an ideal of R. For instance, if I and J are ideals of R, then $I \cup J$ is an ideal of R if and only if either $I \subseteq J$ or $J \subseteq I$.

(c) If $\{I_\lambda\}_{\lambda\in\Lambda}$ is a chain of ideals of R, then $\cup_{\lambda\in\Lambda} I_\lambda$ is an ideal of R. (Recall that the set of ideals $\{I_\lambda\}_{\lambda\in\Lambda}$ is a *chain* if, for every $\lambda, \mu \in \Lambda$ we have either $I_\lambda \subseteq I_\mu$ or $I_\mu \subseteq I_\lambda$.)

In the following definition, part (a) is a special case of part (b), and part (b) is a special case of part (c).

Definition A.3.5. (a) Given an element $s \in R$, the *ideal generated by s* is the set

$$(s)R = sR = \{sr \in R \mid r \in R\}.$$

An ideal is *principal* if it can be generated by a single element.

(b) For each sequence $s_1, \ldots, s_n \in R$, the *ideal generated by $s_1, \ldots, s_n$* is the set

$$(s_1, \ldots, s_n)R = \{\textstyle\sum_{i=1}^n s_i r_i \in R \mid r_1, \ldots, r_n \in R\}.$$

An ideal is *finitely generated* if it can be generated by a finite list of elements.

(c) For each subset $S \subseteq R$, the *ideal generated by S* is the set

$$(S)R = \{\textstyle\sum_{i=1}^n s_i r_i \in R \mid n \geqslant 0 \text{ and } s_1, \ldots, s_n \in S \text{ and } r_1, \ldots, r_n \in R\}.$$

The subset $S \subseteq R$ is a *generating set* for an ideal $I \subseteq R$ when $I = (S)R$.

Remark A.3.6. For each sequence $s_1, \ldots, s_n \in R$ we have $0_R \in (s_1, \ldots, s_n)R$ because $0_R = \sum_{i=1}^n s_i 0_R$. Tacitly, we are assuming that $n \geqslant 1$. In the case $n = 0$ (that is, when we are considering the empty sequence) we have $0_R \in (\emptyset)R$ because the empty sum $\sum_{i=1}^0 s_i r_i$ is 0_R by convention. Similarly, the empty product $\prod_{i=1}^0 r_i$ is 1_R by convention.

Remark A.3.7. Let $r, s \in R$. We have $r \in (s)R$ if and only if $s\big|r$.

Example A.3.8. One has $R = (1_R)R$ and $(0_R)R = \{0_R\} = (\emptyset)R$.

Remark A.3.9. Let $S, T \subseteq R$ be subsets. If $S \subseteq T$, then $(S)R \subseteq (T)R$.

The following notation is non-standard, but we use it frequently.

Remark A.3.10. Let $S \subseteq R$ be a subset. We will often find it convenient to use the notation $\sum_{s\in S}^{\text{finite}} sr_s$ for elements of $(S)R$. Here, the elements r_s are in R, and the superscript "finite" signifies that we are assuming that all but finitely many of the r_s are equal to 0_R.

Note that in part (c) of the next result, we are not claiming that every ideal has a finite generating set.

Proposition A.3.11. *Let $S \subseteq R$.*

(a) *The set $(S)R$ is the unique smallest ideal of R such that $S \subseteq (S)R$. In particular, the set $(S)R$ is an ideal of R and, for each ideal $I \subseteq R$, we have $S \subseteq I$ if and only if $(S)R \subseteq I$.*
(b) *The ideal $(S)R$ is the intersection of all the ideals of R containing S.*
(c) *If I is an ideal, then $(I)R = I$. In particular, every ideal has a generating set.*
(d) *If $I = (S)R$ is finitely generated, then there exist elements $s_1, \ldots, s_n \in S$ such that $I = (s_1, \ldots, s_n)R$.*

Proof. We verify part (a); parts (b)–(d) are left as exercises.

We first show that $(S)R$ is an ideal of R. To this end, we assume that $S \neq \emptyset$, since this case is covered in Example A.3.8. Using the reasoning of Remark A.3.6, we conclude that $0_R \in (S)R$, and so $(S)R \neq \emptyset$. To show that $(S)R$ is closed under addition and external multiplication, fix elements $a, b \in (S)R$ and $r \in R$. Write $a = \sum_{s\in S}^{\text{finite}} st_s$ and $b = \sum_{s\in S}^{\text{finite}} su_s$ for elements $t_s, u_s \in R$. Then, we have

$$a + b = (\textstyle\sum_{s\in S}^{\text{finite}} st_s) + (\sum_{s\in S}^{\text{finite}} su_s) = \sum_{s\in S}^{\text{finite}} s(t_s + u_s) \in (S)R$$

and

$$ra = r(\textstyle\sum_{s\in S}^{\text{finite}} st_s) = \sum_{s\in S}^{\text{finite}} s(rt_s) \in (S)R.$$

Hence the set $(S)R$ is an ideal of R.

Next, we observe that $S \subseteq (S)R$. For this, fix an element $s_0 \in S$ and set

$$r_s = \begin{cases} 1_R & \text{when } s = s_0 \\ 0_R & \text{when } s \neq s_0. \end{cases}$$

With these choices, it follows directly that $s_0 = \sum_{s\in S}^{\text{finite}} sr_s \in (S)R$, as desired.

Next, let $I \subseteq R$ be an ideal; we show that $S \subset I$ if and only if $(S)R \subseteq I$. One implication is straightforward: if $(S)R \subseteq I$, then the previous paragraph implies that $S \subseteq (S)R \subseteq I$. For the converse, assume that $S \subseteq I$. Since I is closed under external multiplication, we conclude that $sr_s \in I$ for all $s \in S$ and all $r_s \in R$. Since I is closed under finite sums, it follows that $\sum_{s\in S}^{\text{finite}} sr_s \in I$ for all $s \in S$ and all $r_s \in R$. That is, every element of $(S)R$ is in I, as desired.

It now follows directly that $(S)R$ is the unique smallest ideal of R such that $S \subseteq (S)R$. □

Exercises.

EXERCISE A.3.12. Let $R = \mathbb{Z}[X]$. Prove or disprove:

(a) The set K of all constant polynomials in R is an ideal of R.
(b) The set I of all polynomials in R with even constant terms is an ideal of R.

EXERCISE A.3.13. Verify the following equalities for ideals in $R = \mathbb{Q}[X, Y]$:

(a) $(X + Y, X - Y)R = (X, Y)R$.
(b) $(X + XY, Y + XY, X^2, Y^2)R = (X, Y)R$.
(c) $(2X^2 + 3Y^2 - 11, X^2 - Y^2 - 3)R = (X^2 - 4, Y^2 - 1)R$.

This shows that the same ideal can have many different generating sets and that different generating sets may have different numbers of elements.

EXERCISE A.3.14. For each of the sets in Exercise A.3.12 that is an ideal, find a finite generating set. Prove that the set actually generates the ideal.

EXERCISE A.3.15. Let A be a commutative ring with identity. Let $R = A[X, Y]$ and show that the ideal $(X, Y)R$ is not principal.

*EXERCISE A.3.16. If $I \subseteq \mathbb{Z}$ is an ideal, then there exists an integer $m \in \mathbb{Z}$ such that $I = m\mathbb{Z}$. (Hint: If $I = 0$ then $m = 0$, so you may assume that $I \neq 0$. In this case, show that I has a smallest positive element m; then use the Division Algorithm to show that $I = m\mathbb{Z}$.) (This exercise is used in Example 1.4.4.)

EXERCISE A.3.17. Given integers m, n that are not both zero, prove that the ideal $(m, n)\mathbb{Z}$ is generated by $\gcd(m, n)$.

EXERCISE A.3.18. Prove the following:

(a) An element $r \in R$ is a unit in R if and only if $rR = R$.
(b) Let $I \subseteq R$ be an ideal. Then $I = R$ if and only if I contains a unit. (For this reason, the ideal $R = (1_R)R$ is often called the *unit ideal*.)
(c) If $1_R \neq 0_R$, then R is a field if and only if the only ideals of R are 0 and R.

Exercise A.3.19. Let $f, g, f_1, \ldots, f_n \in R$. Prove or disprove each of the following:

(a) If $f \in (f_1, \ldots, f_n)R$, then $f \in (f_i)R$ for some $i = 1, \ldots, n$.
(b) If $f \in (f_i)R$ for some $i = 1, \ldots, n$, then $f \in (f_1, \ldots, f_n)R$
(c) If $ff_j = gf_i$ and $f_i \neq f_j$, then $f \in (f_i)R$ and $g \in (f_j)R$.

Exercise A.3.20. Prove or disprove the following: Fix $f_1, \ldots, f_m, g_1, \ldots, g_n \in R$ and a positive integer k. If $(f_1, \ldots, f_m)R = (g_1, \ldots, g_n)R$, then $(f_1^k, \ldots, f_m^k)R = (g_1^k, \ldots, g_n^k)R$.

A.4. Sums, Products, and Powers of Ideals

In this section, R is a commutative ring with identity.

We have seen in Fact A.3.4(a) that intersections of ideals are themselves ideals. This section deals with other methods of combining ideals to form new ideals. Given that the notion of an ideal generalizes the notion of a number, these constructions generalize familiar constructions for numbers, though not necessarily in the way one might expect. For instance, the sum of two ideals, introduced next, generalizes the greatest common divisor of two integers.

Sums of Ideals. In the following definition, part (a) is a special case of part (b), and part (b) is a special case of part (c).

Definition A.4.1. (a) Let I and J be ideals of R. The *sum* of I and J is

$$I + J = \{a + b \mid a \in I, b \in J\}.$$

(b) Let n be a positive integer and let $I_1, I_2, \ldots, I_n$ be ideals of R. The *sum* of the ideals $I_1, I_2, \ldots, I_n$ is

$$\textstyle\sum_{j=1}^n I_j = I_1 + I_2 + \cdots + I_n = \{\sum_{i=1}^n a_i \mid a_i \in I_i \text{ for } i = 1, 2, \ldots, n\}.$$

(c) Let $\{I_\lambda\}_{\lambda\in\Lambda}$ be a (possibly uncountably infinite) collection of ideals of R. The *sum* of the ideals in this collection to be the set $\sum_{\lambda\in\Lambda} I_\lambda$ consisting of all sums of the form $\sum_{\lambda\in\Lambda} a_\lambda$, where $a_\lambda \in I_\lambda$ for all $\lambda \in \Lambda$ and all but a finite number of the a_λ are zero (in other words, finite sums). In symbols, we write

$$\textstyle\sum_{\lambda\in\Lambda} I_\lambda = \{\sum_{\lambda\in\Lambda}^{\text{finite}} a_\lambda \mid a_\lambda \in I_\lambda\}.$$

Example A.4.2. If m and n are integers that are not both zero, then $m\mathbb{Z}+n\mathbb{Z} = \gcd(m, n)\mathbb{Z}$.

Theorem A.4.3. *Let $\{I_\lambda\}_{\lambda\in\Lambda}$ be a collection of ideals of R.*

(a) *The set $\sum_{\lambda\in\Lambda} I_\lambda$ is an ideal; more specifically, we have $\sum_{\lambda\in\Lambda} I_\lambda = (\cup_{\lambda\in\Lambda} I_\lambda)R$.*
(b) *$\sum_{\lambda\in\Lambda} I_\lambda$ is the unique smallest ideal of R containing $\cup_{\lambda\in\Lambda} I_\lambda$.*
(c) *$\sum_{\lambda\in\Lambda} I_\lambda$ is the intersection of all the ideals of R containing $\cup_{\lambda\in\Lambda} I_\lambda$.*
(d) *For each ideal $K \subseteq R$, we have $\sum_{\lambda\in\Lambda} I_\lambda \subseteq K$ if and only if $\cup_{\lambda\in\Lambda} I_\lambda \subseteq K$.*

PROOF. (a) The proof that $\sum_{\lambda\in\Lambda} I_\lambda$ is an ideal of R is similar to the proof that $(S)R$ is an ideal in Proposition A.3.11(a); we leave this as an exercise. The containment $\sum_{\lambda\in\Lambda} I_\lambda \subseteq (\cup_{\lambda\in\Lambda} I_\lambda)R$ is a direct consequence of the definitions, because R has a multiplicative identity. For the reverse containment, use the fact that $0_R \in I_\lambda$ for each $\lambda \in \Lambda$ to conclude that $I_\lambda \subseteq \sum_{\lambda\in\Lambda} I_\lambda$. It follows that $\cup_{\lambda\in\Lambda} I_\lambda \subseteq \sum_{\lambda\in\Lambda} I_\lambda$, so $(\cup_{\lambda\in\Lambda} I_\lambda) \subseteq \sum_{\lambda\in\Lambda} I_\lambda$ by Proposition A.3.11(a).

Parts (b)–(d) follow from Proposition A.3.11. □

The next two results are special cases of Theorem A.4.3. We include them for ease of reference.

COROLLARY A.4.4. *Let n be a positive integer and let $I_1, I_2, \ldots, I_n$ be ideals of R.*

(a) *The set $\sum_{j=1}^n I_j$ is an ideal; more specifically, we have $\sum_{j=1}^n I_j = (\cup_{j=1}^n I_j)R$.*
(b) *$\sum_{j=1}^n I_j$ is the unique smallest ideal of R containing $\cup_{j=1}^n I_j$.*
(c) *$\sum_{j=1}^n I_j$ is the intersection of all the ideals of R containing $\cup_{j=1}^n I_j$.*
(d) *For each ideal $K \subseteq R$, we have $\sum_{j=1}^n I_j \subseteq K$ if and only if $\cup_{j=1}^n I_j \subseteq K$.* □

COROLLARY A.4.5. *Let I and J be ideals of R.*

(a) *The set $I + J$ is an ideal; more specifically, we have $I + J = (I \cup J)R$.*
(b) *$I + J$ is the unique smallest ideal of R containing $I \cup J$.*
(c) *$I + J$ is the intersection of all the ideals of R containing $I \cup J$.*
(d) *For each ideal $K \subseteq R$, we have $I + J \subseteq K$ if and only if $I \cup J \subseteq K$.* □

FACT A.4.6. (a) Let I and J be ideals of R. Then $I + J = J$ if and only if $I \subseteq J$.
(b) Let n be a positive integer and let $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n$ be ideals of R. Then $\sum_{j=1}^n I_j = I_n$.
(c) Let $\{I_\lambda\}_{\lambda\in\Lambda}$ be a chain of ideals of R. Then $\sum_{\lambda\in\Lambda} I_\lambda = \cup_{\lambda\in\Lambda} I_\lambda$.

FACT A.4.7. (a) (0 and 1) If I is an ideal in R, then $0 + I = I$ and $R + I = R$.
(b) (commutative law) If I and J are ideals of R, then $I + J = J + I$. More generally, if $\{I_\lambda\}_{\lambda\in\Lambda}$ is a collection of ideals of R and $f\colon \Lambda \to \Lambda$ is a bijection, then $\sum_{\lambda\in\Lambda} I_\lambda = \sum_{\lambda\in\Lambda} I_{f(\lambda)}$.
(c) (associative law) If I, J and K are ideals of R, then $(I+J)+K = I+J+K = I+(J+K)$. (More general associative laws, using more than three ideals, hold by induction on the number of ideals.)

FACT A.4.8. (a) Let $I = (f_1, \ldots, f_n)R$ and let $J = (g_1, \ldots, g_m)R$. Then $I + J$ is generated by the set $\{f_1, \ldots, f_n, g_1, \ldots, g_m\}$.
(b) Let n be a positive integer and let $S_1, S_2, \ldots, S_n$ be subsets of R. Then $\sum_{j=1}^n (S_j)R = (\cup_{j=1}^n S_j)R$.
(c) If $\{S_\lambda\}_{\lambda\in\Lambda}$ is a collection of subsets of R, then $\sum_{\lambda\in\Lambda}(S_\lambda)R = (\cup_{\lambda\in\Lambda} S_\lambda)R$.

Products and Powers of Ideals.

DEFINITION A.4.9. Let I and J be ideals of R. Define the *product* of I and J to be the ideal IJ generated by all products xy, where $x \in I$ and $y \in J$:

$$IJ = (\{xy \mid x \in I, y \in J\})R.$$

Similarly, we define the product of any finite family of ideals $I_1, \ldots, I_n$ of R to be the ideal $I_1 I_2 \cdots I_n$ generated by all products $x_1 x_2 \cdots x_n$, where $x_i \in I_i$ for $i = 1, 2, \ldots, n$:

$$I_1 I_2 \cdots I_n = (\{x_1 x_2 \cdots x_n \mid x_i \in I_i \text{ for } i = 1, 2, \ldots, n\})R.$$

Given an ideal I of R and a positive integer n, we define

$$I^n = \underbrace{II \cdots I}_{n \text{ factors}}$$

that is, I^n is the ideal $I_1 I_2 \cdots I_n$, where $I_i = I$ for each $i = 1, 2, \ldots, n$. When $I \neq 0$, we define $I^0 = R$. We leave 0^0 undefined.

EXAMPLE A.4.10. If m and n are integers, then $(m\mathbb{Z})(n\mathbb{Z}) = (mn)\mathbb{Z}$.

FACT A.4.11. Let $I, J, I_1, \ldots, I_n$ be ideals of R.

(a) The product ideal IJ is the unique smallest ideal of R that contains the set $\{ab \mid a \in I \text{ and } b \in J\}$. In particular, an ideal K contains the product IJ if and only if it contains each product of the form ab where $a \in I$ and $b \in J$.

(b) The product $I_1 \cdots I_n$ is the unique smallest ideal of R containing the set $\{a_1 \cdots a_n \mid a_j \in I_j \text{ for } j = 1, \ldots, n\}$. In particular, an ideal K contains the product $I_1 \cdots I_n$ if and only if it contains each product of the form $a_1 \cdots a_n$ where $a_j \in I_j$ for $j = 1, \ldots, n$.

(c) There are equalities $IJ = \{\sum_k^{\text{finite}} a_k b_k \mid a_k \in I \text{ and } b_k \in J \text{ for each } k\}$ and $I_1 \cdots I_n = \{\sum_k^{\text{finite}} a_{1,k} \cdots a_{n,k} \mid a_{j,k} \in I_j \text{ for each } j \text{ and each } k\}$.

(d) There are containments $IJ \subseteq I \bigcap J$ and $I_1 \cdots I_n \subseteq I_1 \bigcap \cdots \bigcap I_n$ and $I^n \subseteq I$. These containments may be proper or not.

Even though the notation for the nth power of an ideal is the same as the notation for the n-fold Cartesian product of I with itself, these objects are not the same. We expect that it will be clear from the context which construction we mean at a given location.

FACT A.4.12. (a) (0 and 1) If I is an ideal of R, then $RI = I$ and $0I = 0$.

(b) (commutative law) If I and J are ideals of R, then $IJ = JI$. Moreover, if $I_1, \ldots, I_n$ are ideals of R and $i_1, \ldots, i_n$ is a permutation of the numbers $1, \ldots, n$, then $I_1 \cdots I_n = I_{i_1} \cdots I_{i_n}$.

(c) (associative law) If I, J and K are ideals of R, then $(IJ)K = IJK = I(JK)$. (More general associative laws hold by induction on the number of ideals.)

(d) (distributive law) If I, J and K are ideals of R, then $(I + J)K = IK + JK = K(I + J)$. (More general distributive laws hold by induction on the number of ideals involved.)

The next fact provides generating sets for products and powers.

FACT A.4.13. (a) If $I = (f_1, \ldots, f_n)R$ and $J = (g_1, \ldots, g_m)R$, then

$$IJ = (\{f_i g_j \mid 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m\})R.$$

(b) If $I_j = (S_j)R$ for $j = 1, \ldots, n$ then

$$I_1 \cdots I_n = (\{s_1 \cdots s_n \mid s_i \in S_i \text{ for } i = 1, \ldots, n\})R.$$

(c) If n is a positive integer and $I = (f_1, \ldots, f_m)R$, then

$$I^n = (\{f_{i_1} \cdots f_{i_n} \mid 1 \leqslant i_j \leqslant m \text{ for } j = 1, \ldots, n\})R.$$

Remark A.4.14. Let I be an ideal of R. In general, the ideal I^n is not generated by the nth powers of elements of I, that is $I^n \supsetneq (\{f^n \mid f \in I\})R$. For instance, if $R = \mathbb{Z}_2[X,Y]$ and $I = (X,Y)R$, then

$$I^2 = (X^2, XY, Y^2)R \supsetneq (X^2, Y^2)R = (\{f^2 \mid f \in I\})R.$$

The inequalities are straightforward, as is the containment. For the inequality $(X^2, XY, Y^2)R \neq (X^2, Y^2)R$, note that $XY \in (X^2, XY, Y^2)R \smallsetminus (X^2, Y^2)R$.

Definition A.4.15. Let J be an ideal of R. For each $r \in R$, we set $rJ = \{rb \in R \mid b \in J\}$.

Fact A.4.16. If J is an ideal of R and r is an element of R, then $rJ = (rR)J$. In particular, the set rJ is an ideal of R such that $rJ \subseteq J$. Note that we can have $rJ \subsetneq J$.

Exercises.

Exercise A.4.17. Let I and J be ideals of R. Set $K = \{ab \mid a \in I, b \in J\}$. Prove or disprove: K is an ideal of R.

*Exercise A.4.18. Let A denote a commutative ring with identity, and set $R = A[X_1, \ldots, X_d]$ and $\mathfrak{X} = (X_1, \ldots, X_d)R$. Prove that if $f \in R$, then $f \in \mathfrak{X}^n$ if and only if each monomial occurring in f has degree at least n. Prove that $\mathfrak{X} \neq R$. (This exercise is used in the proofs of Theorem 6.2.1 and Proposition 6.3.4.)

A.5. Colon Ideals

In this section, R is a commutative ring with identity.

This section deals with a constructions of ideals that may be less familiar, namely colon ideals.

Definition A.5.1. Let S be a subset of R, and let I be an ideal of R. For each element $r \in R$, set $rS = \{rs \mid s \in S\}$. The *colon ideal* of I with S is defined as

$$(I :_R S) = \{r \in R \mid rS \subseteq I\} = \{r \in R \mid rs \in I \text{ for all } s \in S\}.$$

For each $s \in R$, we set $(I :_R s) = (I :_R \{s\})$.

Example A.5.2. We have $(6\mathbb{Z} :_{\mathbb{Z}} 15) = (6\mathbb{Z} :_{\mathbb{Z}} 15\mathbb{Z}) = 2\mathbb{Z}$.

The basic properties of colon ideals are contained in the next two results.

Proposition A.5.3. *Let I, J, and K be ideals of R, and let S, T be subsets of R.*

(a) *The set $(I :_R S)$ is an ideal of R.*
(b) *We have $(I :_R (S)R) = (I :_R S) = \bigcap_{s \in S}(I :_R s)$.*
(c) *We have $(I :_R S) = R$ if and only if $S \subseteq I$.*
(d) *There are containments $J(I :_R J) \subseteq I \subseteq (I :_R S)$.*
(e) *If $I \subseteq J$, then $(I :_R S) \subseteq (J :_R S)$.*
(f) *If $S \subseteq T$, then $(I :_R S) \supseteq (I :_R T)$.*

Proof. (a) For every $s \in S$, we have $0s = 0 \in I$; it follows that $0 \in (I :_R S)$ and so $(I :_R S) \neq \emptyset$.

To show that $(I :_R S)$ is closed under addition, let $r, r' \in (I :_R S)$. For all $s \in S$ we then have $rs, r's \in I$. The distributive law combines with the fact that I

is closed under addition to show that $(r+r')s = rs+r's \in I$, and so $r+r' \in (I :_R S)$, as desired.

To show that $(I :_R S)$ is closed under external multiplication, let $r \in (I :_R S)$ and $t \in R$. For all $s \in S$ we then have $rs \in I$. The associative law combines with the fact that I is closed under external multiplication to show that $(tr)s = t(rs) \in I$, and so $tr \in (I :_R S)$, as desired.

(c) For the forward implication, assume that $(I :_R S) = R$. It follows that $1_R \in (I :_R S)$, and so $S = 1_R S \subseteq I$.

For the converse, assume that $S \subseteq I$. It follows that $1_R \in (I :_R S)$. Since $(I :_R S)$ is an ideal in R, it follows from Fact A.3.2(f) that $(I :_R S) = R$.

The proofs of the remaining statements are left as exercises. □

PROPOSITION A.5.4. *Let I, J, and K be ideals of R, and let S be a subset of R. Let $\{I_\lambda\}_{\lambda\in\Lambda}$ be a collection of ideals of R, and let $\{S_\lambda\}_{\lambda\in\Lambda}$ be a collection of subsets of R.*

(a) *There are equalities $((I :_R J) :_R K) = (I :_R JK) = ((I :_R K) :_R J)$.*
(b) *There is an equality $(\bigcap_{\lambda\in\Lambda} I_\lambda :_R S) = \bigcap_{\lambda\in\Lambda}(I_\lambda :_R S)$.*
(c) *There is an equality $(J :_R \cup_{\lambda\in\Lambda} S_\lambda) = \bigcap_{\lambda\in\Lambda}(J :_R S_\lambda)$.*
(d) *There is an equality $(J :_R \sum_{\lambda\in\Lambda} I_\lambda) = \bigcap_{\lambda\in\Lambda}(J :_R I_\lambda)$.*

PROOF. (a) We first show that $((I :_R K) :_R J) \subseteq (I :_R JK)$. Fix elements $r \in ((I :_R K) :_R J)$ and $x \in JK$. It follows that there are elements $b_1, \ldots, b_n \in J$ and $c_1, \ldots, c_n \in K$ such that $x = \sum_{i=1}^n b_i c_i$. Since $r \in ((I :_R K) :_R J)$ and $b_i \in J$, we have $rb_i \in (I :_R K)$. The fact that $c_i \in K$ implies that $rb_ic_i \in I$. It follows that

$$rx = r\sum_{i=1}^n b_ic_i = \sum_{i=1}^n rb_ic_i \in I$$

because I is an ideal, so $rx \in (I :_R JK)$, as desired.

We next show that $((I :_R K) :_R J) \supseteq (I :_R JK)$. Let $s \in (I :_R JK)$ and $b \in J$. To show that $s \in ((I :_R K) :_R J)$, it suffices to show that $sb \in (I :_R K)$. Let $c \in K$. One needs to show that $(sb)c \in I$. The conditions $b \in J$ and $c \in K$ imply $bc \in JK$. Hence, the assumption $s \in (I :_R JK)$ implies $(sb)c = s(bc) \in I$, as desired.

The other equality follows from the next sequence

$$((I :_R K) :_R J) = (I :_R JK) = (I :_R KJ) = ((I :_R J) :_R K).$$

The proofs of the remaining statements are left as exercises. □

Exercises.

EXERCISE A.5.5. Let I be an ideal of R, and let S and T be subsets of R. Prove that $((I :_R S) :_R T) = ((I :_R T) :_R S)$.

EXERCISE A.5.6. Let $m, n \in \mathbb{Z}$ and compute $(m\mathbb{Z} :_{\mathbb{Z}} n\mathbb{Z})$ and $\operatorname{rad}(n\mathbb{Z})$; justify your answer.

EXERCISE A.5.7. Let A be a commutative ring with identity. Consider the ring $R = A[X_1, \ldots, X_d]$ and the ideal $\mathfrak{X} = (X_1, \ldots, X_d)R$.

(a) Prove that $(\mathfrak{X}^n : \mathfrak{X}) = \mathfrak{X}^{n-1}$.
(b) List the monomials in $\mathfrak{X}^{n-1} \smallsetminus \mathfrak{X}^n$; justify your answer.

A.6. Radicals of Ideals

In this section, R is a commutative ring with identity.

This section deals with another construction of ideals that may be less familiar, namely radicals. Given an ideal I, the radical of I is the set of "nth roots" of elements of I, hence the name.

DEFINITION A.6.1. Let I be an ideal of R. The *radical* of I is the set

$$\mathrm{rad}\,(I) = \{x \in R \mid x^n \in I \text{ for some } n \geqslant 1\}.$$

Other common notations include $\sqrt{I}$ and $\mathrm{r}(I)$.

EXAMPLE A.6.2. In the ring $\mathbb{Z}$ we have $\mathrm{rad}\,(12\mathbb{Z}) = 6\mathbb{Z}$.
In the ring $\mathbb{Z}_8$ we have $\mathrm{rad}\,(0\mathbb{Z}_8) = \mathrm{rad}\,(4\mathbb{Z}_8) = 2\mathbb{Z}_8$.

PROPOSITION A.6.3. *Let I be an ideal of R.*

(a) *The set* $\mathrm{rad}\,(I)$ *is an ideal of R.*
(b) *There is a containment* $I \subseteq \mathrm{rad}\,(I)$.
(c) *If $I \subseteq J$, then* $\mathrm{rad}\,(I) \subseteq \mathrm{rad}\,(J)$.
(d) *There is an equality* $\mathrm{rad}\,(I) = \mathrm{rad}\,(\mathrm{rad}\,(I))$.
(e) *We have* $\mathrm{rad}\,(I) = R$ *if and only if* $I = R$.
(f) *For each integer $n \geqslant 1$, there is an equality* $\mathrm{rad}\,(I^n) = \mathrm{rad}\,(I)$.

PROOF. (a) We have $0^1 = 0 \in I$; it follows that $0 \in \mathrm{rad}\,(I)$, so $\mathrm{rad}\,(I) \neq \emptyset$.

To show that $\mathrm{rad}\,(I)$ is closed under addition, let $r, s \in \mathrm{rad}\,(I)$. There are integers $m, n \geqslant 1$ such that $r^m, s^n \in I$. The binomial theorem A.1.24 implies that

$$(r+s)^{m+n} = \textstyle\sum_{i=0}^{m+n} \binom{m+n}{i} r^i s^{m+n-i}.$$

Note that for each $i = 0, \ldots, m+n$ we have either $i \geqslant m$ or $m+n-i \geqslant n$. It follows that each term $\binom{m+n}{i} r^i s^{m+n-i}$ is in I. This implies that $(r+s)^{m+n} \in I$, so $r+s \in \mathrm{rad}\,(I)$.

To show that $\mathrm{rad}\,(I)$ is closed under external multiplication, let $r \in \mathrm{rad}\,(I)$ and $t \in R$, and let n be a positive integer such that $r^n \in I$. It follows that $(rt)^n = r^n t^n \in I$, so $rt \in \mathrm{rad}\,(I)$.

(c) Assume that $I \subseteq J$ and let $r \in \mathrm{rad}\,(I)$. There is an integer $m \geqslant 1$ such that $r^m \in I \subseteq J$, so $r \in \mathrm{rad}\,(J)$.

(e) For the forward implication, assume that $\mathrm{rad}\,(I) = R$. It follows that there exists a positive integer n such that $1_R^n \in I$. The equality $1_R^n = 1_R$ implies that $1_R \in I$, so $I = R$.

For the reverse implication, assume that $I = R$. Part (b) explains the second step in the sequence $R = I \subseteq \mathrm{rad}\,(I) \subseteq R$, so $\mathrm{rad}\,(I) = R$.

The proofs of the remaining statements are left as exercises. $\square$

The next example shows that, without the commutative hypothesis, the set $\mathrm{rad}\,(I)$ need not be an ideal.

EXAMPLE A.6.4. Let $\mathrm{M}_2(\mathbb{R})$ denote the set of all 2×2 matrices with entries in $\mathbb{R}$. This is a non-commutative ring with identity under the standard definitions of matrix addition and matrix multiplication. The set $\mathrm{rad}\,(0)$ is not an ideal because it is not closed under addition. Indeed, we have $M = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) \in \mathrm{rad}\,(0)$ because $M^2 = 0$. Similarly, we have $N = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{rad}\,(0)$, but $M + N = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \notin \mathrm{rad}\,(0)$

because $M+N$ is invertible. Also, we have $MN = \left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right) \notin \operatorname{rad}(0)$ so $\operatorname{rad}(0)$ is not closed under external multiplication. (Moreover, it is not even closed under internal multiplication.)

PROPOSITION A.6.5. *Let n be a positive integer, and let $I, J, I_1, I_2, \ldots, I_n$ be ideals of R.*

(a) *There are equalities* $\operatorname{rad}(IJ) = \operatorname{rad}(I \bigcap J) = \operatorname{rad}(I) \bigcap \operatorname{rad}(J)$.
(b) *There are equalities*

$$\begin{aligned}\operatorname{rad}(I_1 I_2 \cdots I_n) &= \operatorname{rad}\left(I_1 \bigcap I_2 \bigcap \cdots \bigcap I_n\right) \\ &= \operatorname{rad}(I_1) \bigcap \operatorname{rad}(I_2) \bigcap \cdots \bigcap \operatorname{rad}(I_n).\end{aligned}$$

(c) $\operatorname{rad}(I+J) = \operatorname{rad}(\operatorname{rad}(I) + \operatorname{rad}(J))$.
(d) $\operatorname{rad}(I_1 + I_2 + \cdots + I_n) = \operatorname{rad}(\operatorname{rad}(I_1) + \operatorname{rad}(I_2) + \cdots + \operatorname{rad}(I_n))$.

PROOF. (a) We show that

$$\operatorname{rad}(IJ) \subseteq \operatorname{rad}\left(I \bigcap J\right) \subseteq \operatorname{rad}(I) \bigcap \operatorname{rad}(J) \subseteq \operatorname{rad}(IJ).$$

The containment $\operatorname{rad}(IJ) \subseteq \operatorname{rad}(I \bigcap J)$ follows from Proposition A.6.3(c) since $IJ \subseteq I \bigcap J$. The containment $\operatorname{rad}(I \bigcap J) \subseteq \operatorname{rad}(I) \bigcap \operatorname{rad}(J)$ also follows from Proposition A.6.3(c): the containments $I \bigcap J \subseteq I$ and $I \bigcap J \subseteq J$ imply that $\operatorname{rad}(I) \bigcap \operatorname{rad}(J) \subseteq \operatorname{rad}(I)$ and $\operatorname{rad}(I) \bigcap \operatorname{rad}(J) \subseteq \operatorname{rad}(J)$ For the containment $\operatorname{rad}(I) \bigcap \operatorname{rad}(J) \subseteq \operatorname{rad}(IJ)$, let $r \in \operatorname{rad}(I) \bigcap \operatorname{rad}(J)$. There are integers $l, m \geqslant 1$ such that $r^l \in I$ and $r^m \in J$, so $r^{l+m} = r^l r^m \in IJ$. It follows that $r \in \operatorname{rad}(IJ)$, as desired.

(b) The case $n = 2$ follows from part (a); the remaining cases are proved by induction on n.

The proofs of the remaining statements are left as exercises. $\square$

The following example shows that we may have $\operatorname{rad}(I+J) \neq \operatorname{rad}(I) + \operatorname{rad}(J)$; compare to Proposition A.6.5(c).

EXAMPLE A.6.6. Set $R = \mathbb{C}[X,Y]$, and let $I = (X^2+Y^2)R$ and $J = (X)R$. Then $\operatorname{rad}(I) = I$ and $\operatorname{rad}(J) = J$, so $\operatorname{rad}(I) + \operatorname{rad}(J) = I + J = (X, Y^2)R$. On the other hand, we have $\operatorname{rad}(I+J) = \operatorname{rad}\big((X,Y^2)R\big) = (X,Y)R$, so $X \in \operatorname{rad}(I+J) \smallsetminus \operatorname{rad}(I) + \operatorname{rad}(J)$.

The next fact provides handy criteria for verifying containments and equalities of radicals.

FACT A.6.7. Let I and J be ideals of R.

(a) Assume that $I = (f_1, \ldots, f_s)R$ with $s \geqslant 1$. Then $\operatorname{rad}(I) \subseteq \operatorname{rad}(J)$ if and only if for each $i = 1, 2, \ldots, s$ there exists a positive integer n_i such that $f_i^{n_i} \in J$.
(b) Assume that $I = (f_1, \ldots, f_s)R$ and $J = (g_1, \ldots, g_t)R$ with $s, t \geqslant 1$. Then $\operatorname{rad}(I) = \operatorname{rad}(J)$ if and only if for each $i = 1, 2, \ldots, s$ there exists a positive integer n_i such that $f_i^{n_i} \in J$, and for each $j = 1, 2, \ldots, t$ there exists a positive integer m_j such that $g_j^{m_j} \in I$.
(c) Suppose $I \subseteq J$ and that $J = (g_1, \ldots, g_t)R$. Then $\operatorname{rad}(I) = \operatorname{rad}(J)$ if and only if for each $j = 1, 2, \ldots, t$ there exists an integer m_j such that $g_j^{m_j} \in I$.

Exercises.

Exercise A.6.8. Let I and J be ideals of R. Prove or disprove: If $\operatorname{rad}(I) \subseteq \operatorname{rad}(J)$, then $I \subseteq J$.

Exercise A.6.9. Let A be a commutative ring with identity. Set $R = A[X, Y]$ and $I = (X^3, Y^4)R$ and $J = (XY^2, X^2Y)R$.

(a) Use Fact A.6.7 to prove that $\operatorname{rad}(I) \supsetneq \operatorname{rad}(J)$.
(b) Assume that A is a field. Prove that $\operatorname{rad}(I) = (X, Y)R$ and $\operatorname{rad}(J) = (XY)R$. Use this to give another proof that $\operatorname{rad}(I) \supsetneq \operatorname{rad}(J)$.

A.7. Relations

This section contains a brief review of the notion of relations, culminating in a particular relation that is very useful for the study of monomial ideals.

Definition A.7.1. Let A be a set. A *relation* on A is a subset $\sim \subseteq A \times A$. If $\sim \subseteq A \times A$ is a relation, then we write "$a \sim b$" instead of "$(a, b) \in \sim$".

Remark A.7.2. More generally, one can define a relation on the cartesian product $A \times B$ of two sets A and B as a subset $\sim \subseteq A \times B$. Our definition is the special case $A = B$. We will not need the more general version.

Example A.7.3. Every equivalence relation on a set A is a relation on A.

Definition A.7.4. Let A be a non-empty set and let $\geqslant$ be a relation on A. The relation $\geqslant$ is a *partial order* on A if it satisfies the following properties:

(a) (reflexivity) For all $a \in A$ we have $a \geqslant a$;
(b) (transitivity) For all $a, b, c \in A$, if $a \geqslant b$ and $b \geqslant c$, then $a \geqslant c$;
(c) (antisymmetry) For all $a, b \in A$, if $a \geqslant b$ and $b \geqslant a$, then $a = b$.

The negation of "$a \geqslant b$" is written "$a \ngeqslant b$".

Example A.7.5. The usual orders $\geqslant$ on the sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ are partial orders. The "divisibility relation" on the set of positive integers $\mathbb{N}_+$, given by $n \geqslant_{\text{div}} m$ when $m \big| n$, is a partial order on $\mathbb{N}$. The obvious divisibility relation on $\mathbb{Z}$ is not a partial order on $\mathbb{Z}$ because it is not antisymmetric: We have $1 \big| -1$ and $-1 \big| 1$, but $1 \neq -1$.

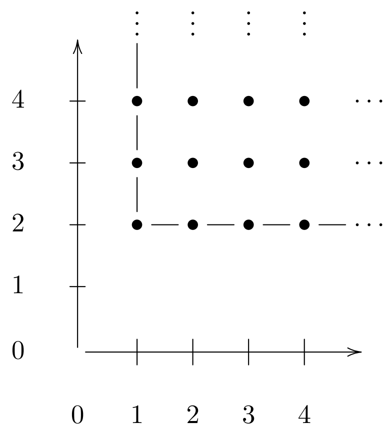
Definition A.7.6. Let A be a set with a partial order $\geqslant$. Two elements $a, b \in A$ are *comparable* if either $a \geqslant b$ or $b \geqslant a$. The partial order $\geqslant$ is a *total order* if every $a, b \in A$ are comparable.

Remark A.7.7. Sets with partial orders are often called "partially ordered sets", or "posets" for short. The adjective "partial" is used for these relations because there is no guarantee it is a total order. For instance, the divisibility order on the set of positive integers $\mathbb{N}_+$ is not a total order because $2 \nmid 3$ and $3 \nmid 2$.

Here is the main example for this text, though we will encounter another important example later.

Definition A.7.8. Let d be a positive integer and define a relation $\succcurlyeq$ on $\mathbb{N}^d$ as follows: $(a_1, \ldots, a_d) \succcurlyeq (b_1, \ldots, b_d)$ when, for $i = 1, \ldots, d$ we have $a_i \geqslant b_i$ in the usual order on $\mathbb{N}$.

Example A.7.9. When $d = 2$, we graph the set $\{\underline{n} \in \mathbb{N}^2 \mid \underline{n} \succcurlyeq (1,2)\}$ as follows.

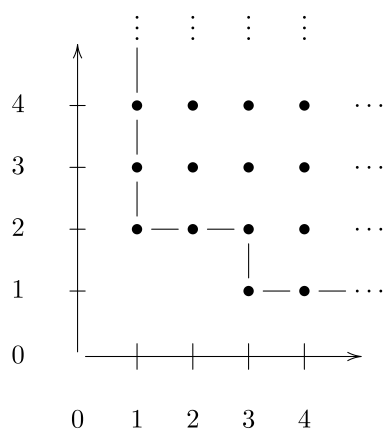


This set can be described as the "translate" $(1,2) + \mathbb{N}^2$.

Definition A.7.10. Let d be a positive integer. For each $\underline{n} \in \mathbb{N}^d$, set

$$[\underline{n}] = \{\underline{m} \in \mathbb{N}^d \mid \underline{m} \succcurlyeq \underline{n}\} = \underline{n} + \mathbb{N}^d.$$

Example A.7.11. When $d = 2$, the graph of $[(1,2)] \cup [(3,1)]$ is the following.



Exercises.

Exercise A.7.12. Prove that the relation from Definition A.7.8 is a partial order. Prove that it is a total order if and only if $d = 1$.

Exercise A.7.13. Let R be a commutative ring with identity. Prove that the divisibility order on R is reflexive and transitive.

APPENDIX B

Introduction to Macaulay2

B.1. Rings

In this tutorial, we show how to declare rings and perform basic computations in Macaulay2. Below is the annotated output of a Macaulay2 session. To begin, type `M2` in a command line, which will produce some initial output, ending with the input prompt:

```
i1 :
```

Now perform some integer arithmetic:

```
i1 : 1+2*3^2

o1 = 19
```

The second line here is the output. Note that Macaulay 2 uses the standard order of operations, so that `1+2*3^2` is `1+2*(3^2)`, not `1+(2*3)^2`. You can refer to previous lines of output using `o1`, `o2`, etc. Also, you can refer to the last output as `oo`, the next to the last output as `ooo`, and the third to the last output as `oooo`.

```
i2 : 1+o1

o2 = 20

i3 : 1/3

      1
o3 = -
      3

o3 : QQ
```

The second line of output `o3` indicates that you are now working in the field $\mathbb{Q}$, represented as `QQ`. To switch back to integer arithmetic, simply type `ZZ`.

```
i4 : ZZ

o4 = ZZ
```

```
o4 : Ring
```

We can also work in the ring $\mathbb{Z}_p$ for any prime p up to 32749:

```
i5 : R=ZZ/37

o5 = R

o5 : QuotientRing
```

Note that $\mathbb{Z}_n$ is not allowed when n is composite. To perform arithmetic in this ring, use `_R`:

```
i6 : 12_R^2

o6 = -4

o6 : R

i7 : 11_R/12_R

o7 = 4

o7 : R
```

For integers, the operators `//` and `%` compute integer quotients and remainders, respectively, as in the division algorithm:

```
i8 : ZZ

o8 = ZZ

o8 : Ring

i9 : 7//4

o9 = 1

i10 : 7%4

o10 = 3
```

Exercises.

EXERCISE B.1.1. Work with Macaulay2 to perform some calculations in $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{Z}_p$ for your favorite prime number p.

EXERCISE B.1.2. Using the Macaulay2 documentation, learn how to calculate binomial coefficients $\binom{n}{m}$ and factorials $n!$ in $\mathbb{Z}$. (Search for `binomial` and `!`.)

B.2. Polynomial Rings

In this tutorial, we show how to declare polynomial rings and perform basic computations with polynomials in Macaulay2. These are done, as one would expect, first in one variable:

```
i1 : A=ZZ/7[x]

o1 = A

o1 : PolynomialRing
```

Notice that the output specifies the name of the ring and the type of ring. Similarly, with computations, the output not only simplifies for you, but also gives the name of the ring:

```
i2 : (x+1)^3

      3     2
o2 = x  + 3x  + 3x + 1

o2 : A

i3 : (x+1)^7

      7
o3 = x  + 1

o3 : A
```

For multiplication, you need to use `*`. For instance, in the next computation, if you were to type `(x+1)(x+2)`, you would receive an error:

```
i4 : (x+1)*(x+2)

      2
o4 = x  + 3x + 2

o4 : A
```

As with integers, the operators `//` and `%` compute quotients and remainders, respectively, as in the division algorithm:

```
i5 : (x^2+x+1)//(x+1)
```

```
o5 = x

o5 : A

i6 : (x^2+x+1)%(x+1)

o6 = 1

o6 : A
```

It is similarly easy to work in several variables:

```
i7 : B=ZZ/11[y,z]

o7 = B

o7 : PolynomialRing

i8 : (3*y+7*z)^2*(y+z)-(y-z)^3

         3    2      3
o8 = - 3y  - y z - 5z

o8 : B
```

Note that coefficient multiplication requires the * in the input.

Exercises.

Exercise B.2.1. Use Macaulay2 to perform some calculations in $\mathbb{Z}_p[x, y, z]$ for your favorite prime number p.

Exercise B.2.2. Using the Macaulay2 documentation, learn how to compute the degree of a polynomial in one variable and the degree of a monomial in several variables. (Search for `degree`.)

Exercise B.2.3. Using the Macaulay2 documentation, learn how to define and evaluate functions from a ring to itself. (Search for `->`.)

B.3. Ideals and Generators

In this tutorial, we show how to declare ideals and perform basic computations with ideals in Macaulay2. We begin with ideals in $\mathbb{Z}$, defined using the function `ideal` with a generating sequence:

```
i1 : I=ideal(3)

o1 = ideal 3

o1 : Ideal of ZZ
```

```
i2 : J=ideal(4)

o2 = ideal 4

o2 : Ideal of ZZ
```

The command `intersect` is used to intersect ideals.

```
i3 : K=intersect(I,J)

o3 = ideal(-12)

o3 : Ideal of ZZ
```

Notice that the output is given using the same format as one would use to define the ideal. The commands `isSubset` and `==` test whether ideals are contained in one another and if they are equal.

```
i4 : isSubset(I,J)

o4 = false

i5 : isSubset(K,I)

o5 = true

i6 : I==K

o6 = false
```

Longer lists of generators can also be used for ideals, though Macaulay2 does not automatically reduce the generating list to a minimal one.

```
i7 : L=ideal(6,9)

o7 = ideal (6, 9)

o7 : Ideal of ZZ

i8 : I==L

o8 = true
```

Ideals are handled similarly in polynomial rings. Note how we declare the variables in this example:

```
i9 : R=ZZ/7[x_1..x_4]
```

```
o9 = R

o9 : PolynomialRing

i10 : I=ideal(x_1*x_2,x_2*x_3)

o10 = ideal (x x , x x )
              1 2   2 3

o10 : Ideal of R

i11 : J=ideal(x_2*x_3^2,x_3*x_4)

                2
o11 = ideal (x x , x x )
              2 3   3 4

o11 : Ideal of R

i12 : K=intersect(I,J)

                        2
o12 = ideal (x x x , x x )
              2 3 4   2 3

o12 : Ideal of R
```

In this setting, one can reduce modulo an ideal, using the `%` operator

```
i13 : x_1*x_2 % J

o13 = x x
       1 2

o13 : R

i14 : x_1*x_2 % I

o14 = 0

o14 : R
```

The output `o14 = 0` tells us that $x_1x_2 \in I$. The output `o13 = x_1x_2` suggests that $x_1x_2 \notin J$. To check this, we use the operator `==`:

```
i15 : x_1*x_2 % J == 0
```

```
o15 = false
```

This is a handy way to check if a given polynomial is in a particular ideal.

Exercises.

EXERCISE B.3.1. Use Macaulay2 to verify the following equalities for ideals in $R = \mathbb{Z}_{41}[X, Y]$:

(a) $(X + Y, X - Y)R = (X, Y)R$.
(b) $(X + XY, Y + XY, X^2, Y^2)R = (X, Y)R$.
(c) $(2X^2 + 3Y^2 - 11, X^2 - Y^2 - 3)R = (X^2 - 4, Y^2 - 1)R$. Use Macaulay2 to determine whether the same equalities hold in $\mathbb{Z}_2[X, Y]$. In cases where the ideals are not equal, determine if one of the ideals is contained in the other.

EXERCISE B.3.2. Use Macaulay2 to find a generating sequence for the ideal $I = (X^2, Y^3, Z^4)R \bigcap (X^4, Y, Z^2)R \bigcap (X^3, Y^2, Z^5)R$ in $R = \mathbb{Z}_{53}[X, Y, Z]$. Is either of the polynomials X^2YZ and X^2Y^2Z in this ideal?

B.4. Sums, Products, and Powers of Ideals

In this tutorial, we show how to work with sums, products, and powers of ideals in Macaulay2. The command for summing two ideals is +.

```
i1 : R=ZZ/41[x_1..x_4]

o1 = R

o1 : PolynomialRing

i2 : I=ideal(x_1*x_2,x_2*x_3)

o2 = ideal (x x , x x )
             1 2   2 3

o2 : Ideal of R

i3 : J=ideal(x_2*x_3^2,x_3*x_4)

                2
o3 = ideal (x x , x x )
             2 3   3 4

o3 : Ideal of R

i4 : K=I+J

                               2
o4 = ideal (x x , x x , x x , x x )
             1 2   2 3   2 3   3 4
```

```
o4 : Ideal of R
```

Notice that the generating sequence Macaulay2 produces is somewhat redundant: since x_2x_3 divides $x_2x_3^2$, the generator $x_2x_3^2$ is unnecessary. The commands `mingens` and `trim` remove the redundancies. (Note that these commands only work for ideals generated by homogeneous polynomials.) See Section 1.3 for more information about redundant and irredundant generating sequences.

```
i5 : mingens K

o5 = | x_3x_4 x_2x_3 x_1x_2 |

             1       3
o5 : Matrix R  <--- R

i6 : trim K

o6 = ideal (x x , x x , x x )
             3 4   2 3   1 2

o6 : Ideal of R
```

Similarly, products and powers of ideals are built using `*` and `^`, respectively.

```
i7 : I*J

               2 2              2 3     2
o7 = ideal (x x x , x x x x , x x , x x x )
             1 2 3   1 2 3 4   2 3   2 3 4

o7 : Ideal of R

i8 : I^3

             3 3   2 3       3 2   3 3
o8 = ideal (x x , x x x , x x x , x x )
             1 2   1 2 3   1 2 3   2 3

o8 : Ideal of R
```

As in Section B.3, one can use the commands `isSubset` and `==` to compare products and intersections.

```
i12 : isSubset(I*J,intersect(I,J))

o12 = true
```

```
i13 : I*J == intersect(I,J)

o13 = false
```

Exercises.

EXERCISE B.4.1. Consider the next ideals in $R = \mathbb{Z}_{41}[X,Y]$: $I = (X^3, Y)R$, $J = (X^2, XY, Y^2)R$, and $K = (X, Y^4)R$.

(a) Use Macaulay2 to verify the proper containments $IJ \subsetneq I \bigcap J \subsetneq I \subsetneq I + J$.

(b) Use Macaulay2 to verify the equalities $I+J = J+I$, $(I+J)+K = I+(J+K)$, $IJ = JI$, $(IJ)K = I(JK)$, and $I(J+K) = IJ + IK$.

B.5. Colon Ideals

In this tutorial, we show how to work with colon ideals in Macaulay2. The command is `:`.

```
i1 : R=ZZ/41[x_1..x_4]

o1 = R

o1 : PolynomialRing

i2 : I=ideal(x_1*x_2,x_2*x_3)

o2 = ideal (x x , x x )
             1 2   2 3

o2 : Ideal of R

i3 : J=ideal(x_2*x_3^2,x_3*x_4)

                2
o3 = ideal (x x , x x )
             2 3   3 4

o3 : Ideal of R

i4 : I:J

o4 = ideal(x )
            2

o4 : Ideal of R

i5 : J:I

                    2
o5 = ideal (x x , x )
```

```
           3 4   3

o5 : Ideal of R
```

Exercises.

EXERCISE B.5.1. Consider the next ideals in $R = \mathbb{Z}_{41}[X, Y]$: $I = (X^3, Y)R$, $J = (X^2, XY, Y^2)R$, and $K = (X, Y^4)R$.

(a) Use Macaulay2 to verify the containments $J(I :_R J) \subseteq I \subseteq (I :_R J)$. Does equality hold in either containment?

(b) Use Macaulay2 to verify the equalities

$$((I :_R J) :_R K) = (I :_R JK) = ((I :_R K) :_R J)$$
$$(I \bigcap J :_R K) = (I :_R K) \bigcap (J :_R K)$$
$$(I :_R J + K) = (I :_R J) \bigcap (I :_R K)$$

B.6. Radicals of Ideals

In this tutorial, we show how to work with radicals of ideals in Macaulay2. The command is `radical`.

```
i1 : R=ZZ/41[x_1..x_4]

o1 = R

o1 : PolynomialRing

i2 : I=ideal(x_1*x_2,x_2*x_3)

o2 = ideal (x x , x x )
             1 2   2 3

o2 : Ideal of R

i3 : J=ideal(x_2*x_3^2,x_3*x_4)

                2
o3 = ideal (x x , x x )
             2 3   3 4

o3 : Ideal of R

i4 : radical I

o4 = monomialIdeal (x x , x x )
                     1 2   2 3

o4 : MonomialIdeal of R
```

```
i5 : radical J

o5 = monomialIdeal (x x , x x )
                     2 3   3 4

o5 : MonomialIdeal of R
```

Exercises.

EXERCISE B.6.1. Consider the next ideals in $R = \mathbb{Z}_{41}[X, Y]$: $I = (X^3, Y)R$, $J = (X^2, XY, Y^2)R$, and $K = (X, Y^4)R$.

(a) Use Macaulay2 to verify the containment $I \subseteq \operatorname{rad}(I)$. Does equality hold?

(b) Use Macaulay2 to verify the equalities

$$\operatorname{rad}(\operatorname{rad}(I)) = \operatorname{rad}(I)$$
$$\operatorname{rad}\left(I^3\right) = \operatorname{rad}(I)$$
$$\operatorname{rad}(IJ) = \operatorname{rad}\left(I \bigcap J\right) = \operatorname{rad}(I) \bigcap \operatorname{rad}(J)$$
$$\operatorname{rad}(I + J) = \operatorname{rad}(\operatorname{rad}(I) + \operatorname{rad}(J)) = \operatorname{rad}(I) + \operatorname{rad}(J).$$

Note that the last equality is not predicted by Proposition A.6.5(c).

B.7. Ideal Quotients

Conclusion

Include some history here. Talk about some of the literature from this area.

Further Reading

For more information about algorithms for computing m-irreducible decompositions of monomial ideals, we recommend the articles of Gao and Zhu [**11**], Liu [**25**], and Roune [**37**].

We know of several fine graduate texts that are devoted (wholly or partially) to the subject of monomial ideals. The texts of Herzog and Hibi [**19**], Hibi [**20**], Miller and Sturmfels [**30**], and Stanley [**39**] are devoted to the study of monomial ideals. Also, the texts of Bruns and Herzog [**4**], and Villarreal [**42**] contain significant material about monomial ideals. It should be noted that these books are more advanced than the current text; for instance, each one uses the notion of Cohen-Macaulyness for quotients of polynomial rings. On the other hand, these techniques allow for more significant applications, including Stanley's proof [**38**] of the upper bound conjecture for simplicial spheres.

The original source for edge ideals of simple graphs is the article of Villarreal [**41**]. This notion has been generalized to edge ideals of "clutters" and "hypergraphs" by Faridi [**10**], Gitler, Valencia, and Villarreal [**12**], and Hà and Van Tuyl [**16**]. The original source for facet ideals of a simplicial complexes, is the article of Faridi [**9**]. Excellent surveys of this area are given by Hà and Van Tuyl [**15**] and Morey and Villarreal [**31**]. Each of these contains an extensive bibliography for the subject.

The use of monomial ideals to study simplicial complexes was pioneered by Hochster [**21**] and Reisner [**36**]. Stanley's proof of the upper bound conjecture, mentioned above, is one of the most important applications of this idea. Accordingly, these ideals are often called "Stanley-Reisner ideals" in the literature. The best surveys of this material we know of are in the texts [**4, 19, 30, 39**] mentioned above. We learned about Alexander duality from Miller, whose papers [**29, 28**] treat (and generalize) some aspects of the subject.

Lastly, the papers of Heinzer, Ratliff, and Shah [**18, 17**] treat monomial ideals determined by "regular sequences," based in part on the dissertation of Taylor [**40**]. The article [**18**] holds a special place in our heart, as we began our work on this text because of it.

Bibliography

1. M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969. MR 0242802 (39 #4129)
2. T. L. Baldwin, L. Mili, M. B. Boisen, and R. Adapa, *Power system observability with minimal phasor measurement placement*, IEEE Trans. Power Systems **8** (1993), no. 2, 707–715.
3. D. J. Brueni and L. S. Heath, *The PMU placement problem*, SIAM J. Discrete Math. **19** (2005), no. 3, 744–761.
4. W. Bruns and J. Herzog, *Cohen-Macaulay rings*, revised ed., Studies in Advanced Mathematics, vol. 39, University Press, Cambridge, 1998. MR 1251956 (95h:13020)
5. CoCoATeam, CoCoA*: a system for doing Computations in Commutative Algebra*, Available at `http://cocoa.dima.unige.it`.
6. D. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms*, third ed., Undergraduate Texts in Mathematics, Springer, New York, 2007, An introduction to computational algebraic geometry and commutative algebra. MR 2290010 (2007h:13036)
7. R. Diestel, *Graph theory*, fourth ed., Graduate Texts in Mathematics, vol. 173, Springer, Heidelberg, 2010. MR 2744811
8. D. Eisenbud, *Commutative algebra*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995, With a view toward algebraic geometry. MR 1322960 (97a:13001)
9. S. Faridi, *The facet ideal of a simplicial complex*, Manuscripta Math. **109** (2002), no. 2, 159–174. MR 1935027 (2003k:13027)
10. ———, *Simplicial trees are sequentially Cohen-Macaulay*, J. Pure Appl. Algebra **190** (2004), no. 1-3, 121–136. MR 2043324 (2004m:13058)
11. S. Gao and M. Zhu, *Computing irreducible decomposition of monomial ideals*, preprint (2008), `arXiv:0811.3425v1`.
12. I. Gitler, C. E. Valencia, and R. H. Villarreal, *A note on Rees algebras and the MFMC property*, Beiträge Algebra Geom. **48** (2007), no. 1, 141–150. MR 2326406 (2008f:13004)
13. D. R. Grayson and M. E. Stillman, *Macaulay 2, a software system for research in algebraic geometry*, Available at http://www.math.uiuc.edu/Macaulay2/.
14. G.-M. Greuel, G. Pfister, and H. Schönemann, *Symbolic computation and automated reasoning, the calculemus-2000 symposium*, ch. SINGULAR 3.0 — A computer algebra system for polynomial computations, pp. 227–233, A. K. Peters, Ltd., Natick, MA, USA, 2001.
15. H. T. Hà and A. Van Tuyl, *Resolutions of square-free monomial ideals via facet ideals: a survey*, Algebra, geometry and their interactions, Contemp. Math., vol. 448, Amer. Math. Soc., Providence, RI, 2007, pp. 91–117. MR 2389237 (2009b:13032)
16. ———, *Monomial ideals, edge ideals of hypergraphs, and their graded Betti numbers*, J. Algebraic Combin. **27** (2008), no. 2, 215–245. MR 2375493 (2009a:05145)
17. W. Heinzer, A. Mirbagheri, L. J. Ratliff, Jr., and K. Shah, *Parametric decomposition of monomial ideals. II*, J. Algebra **187** (1997), no. 1, 120–149. MR 1425562 (97k:13001)
18. W. Heinzer, L. J. Ratliff, Jr., and K. Shah, *Parametric decomposition of monomial ideals. I*, Houston J. Math. **21** (1995), no. 1, 29–52. MR 1331242 (96c:13002)
19. J. Herzog and T. Hibi, *Monomial ideals*, Graduate Texts in Mathematics, vol. 260, Springer-Verlag London Ltd., London, 2011. MR 2724673
20. T. Hibi, *Algebraic combinatorics on convex polytopes*, Carslaw Publications, 1992.
21. M. Hochster, *Cohen-Macaulay rings, combinatorics, and simplicial complexes*, Ring theory, II (Proc. Second Conf., Univ. Oklahoma, Norman, Okla., 1975), Dekker, New York, 1977, pp. 171–223. Lecture Notes in Pure and Appl. Math., Vol. 26. MR 0441987 (56 #376)
22. T. W. Hungerford, *Algebra*, Graduate Texts in Mathematics, vol. 73, Springer-Verlag, New York, 1980, Reprint of the 1974 original. MR 600654 (82a:00006)

23. R. Kavasseri and P. Nag, *An algebraic geometric approach to analyze static voltage collapse in a simple power system model*, Proceedings of the Fifteenth National Power Systems Conference (NPSC) 2008 (Mumbai, India), IIT Bombay, 2008, pp. 482–487.
24. R. Kavasseri and S. K. Srinivasan, *Joint placement of phasor and conventional measurements for observability of power systems*, IET-Gener. Transm. Distrib. **5** (2011), no. 10, 1019–1024.
25. J.-C. Liu, *Algorithms on parametric decomposition of monomial ideals*, Comm. Algebra **30** (2002), no. 7, 3435–3456. MR 1915006 (2003e:13031)
26. H. Matsumura, *Commutative ring theory*, second ed., Studies in Advanced Mathematics, vol. 8, University Press, Cambridge, 1989. MR 90i:13001
27. P. McMullen, *The maximum numbers of faces of a convex polytope*, Mathematika **17** (1970), 179–184. MR 0283691 (44 #921)
28. E. Miller, *The Alexander duality functors and local duality with monomial support*, J. Algebra **231** (2000), no. 1, 180–234. MR 1779598 (2001k:13028)
29. E. Miller, *Alexander duality for monomial ideals and their resolutions*, Rejecta Mathematica **1** (2009), no. 1, 18–57.
30. E. Miller and B. Sturmfels, *Combinatorial commutative algebra*, Graduate Texts in Mathematics, vol. 227, Springer-Verlag, New York, 2005. MR 2110098 (2006d:13001)
31. S. Morey and R. H. Villarreal, *Edge ideals: algebraic and combinatorial properties*, Progress in commutative algebra 1, de Gruyter, Berlin, 2012, pp. 85–126. MR 2932582
32. T. S. Motzkin, *Comonotone curves and polyhedra*, Bull. Amre. Math. Soc. **63** (1957), no. 1, 35, abstract for talk.
33. J. R. Munkres, *Topology: a first course*, Prentice-Hall, Inc., Englewood Cliffs, N.J., 1975. MR 0464128 (57 #4063)
34. ———, *Topological results in combinatorics*, Michigan Math. J. **31** (1984), no. 1, 113–128. MR 736476 (85k:13022)
35. A. G. Phadke, *Synchronized phasor measurements in power systems*, IEEE Comp. Appl. in Power Systems **6** (1993), no. 2, 10–15.
36. G. A. Reisner, *Cohen-Macaulay quotients of polynomial rings*, Advances in Math. **21** (1976), no. 1, 30–49. MR 0407036 (53 #10819)
37. B. H. Roune, *The slice algorithm for irreducible decomposition of monomial ideals*, J. Symbolic Comput. **44** (2009), no. 4, 358–381. MR 2494980 (2009m:13031)
38. R. P. Stanley, *The upper bound conjecture and Cohen-Macaulay rings*, Studies in Appl. Math. **54** (1975), no. 2, 135–142. MR 0458437 (56 #16640)
39. ———, *Combinatorics and commutative algebra*, second ed., Progress in Mathematics, vol. 41, Birkhäuser Boston Inc., Boston, MA, 1996. MR 1453579 (98h:05001)
40. D. K. Taylor, *Ideals generated by monomials in an r-sequence*, ProQuest LLC, Ann Arbor, MI, 1966, Thesis (Ph.D.)–The University of Chicago. MR 2611561
41. R. H. Villarreal, *Cohen-Macaulay graphs*, Manuscripta Math. **66** (1990), no. 3, 277–293. MR 1031197 (91b:13031)
42. ———, *Monomial algebras*, Monographs and Textbooks in Pure and Applied Mathematics, vol. 238, Marcel Dekker Inc., New York, 2001. MR 1800904 (2002c:13001)

Index