Symbolic powers

Eloísa Grifo
University of Nebraska – Lincoln

March 10, 2022

Contents

1 Primary Decomposition **2**
- 1.1 Minimal primes . . . 2
- 1.2 Localization . . . 5
- 1.3 Associated primes . . . 8
- 1.4 Primary Ideals . . . 14
- 1.5 Primary decomposition . . . 17
- 1.6 Computing primary decompositions . . . 21

2 Symbolic powers **23**
- 2.1 What are symbolic powers? . . . 23
- 2.2 Homogeneous ideals . . . 29
- 2.3 Computing symbolic powers . . . 31
- 2.4 Where are we going? . . . 32

3 Sharpening our tools **35**
- 3.1 Dimension and height . . . 35
- 3.2 The Koszul complex . . . 41
- 3.3 Regular sequences . . . 47
- 3.4 Free resolutions . . . 51
- 3.5 Regular rings . . . 56
- 3.6 Depth . . . 59
- 3.7 Cohen-Macaulay rings . . . 66
- 3.8 A few direct applications to symbolic powers . . . 74

4 A geometric perspective **77**
- 4.1 Affine varieties . . . 77
- 4.2 Projective varieties . . . 83
- 4.3 Zariski–Nagata . . . 88
- 4.4 Mixed characteristic . . . 96

A Macaulay2 **98**
- A.1 Getting started . . . 98
- A.2 Asking Macaulay2 for help . . . 101
- A.3 Basic commands . . . 102
- A.4 Graded rings . . . 103

A.5 Complexes and homology in Macaulay2 . . . 104
A.5.1 Chain Complexes . . . 104
A.5.2 The Complexes package . . . 107
A.5.3 Maps of complexes . . . 108

B Commutative algebra background **112**
B.1 Prime Avoidance . . . 112
B.2 NAK . . . 113
B.3 Krull's Intersection Theorem . . . 116
B.4 Ring extensions . . . 116

Index **119**

Bibliography **121**

Warning!

These are notes for a topics course on symbolic powers I am teaching at the University of Nebraska — Lincoln in Spring 2022. These are under construction and are guaranteed to contain typos. Please let me know if you find any typos or errors, no matter how small.

Assumptions

Throughout, all rings are commutative with identity. Moreover, we will almost always assume our rings are Noetherian, so we settle on the convention that rings are Noetherian unless we say otherwise.

We will assume the reader has some knowledge of elementary commutative algebra, as in [AM69], [Mat80], [Mat89], [BH93], or [Eis95]. Any elementary commutative algebra details or proofs we skip can be found in the references above.

Chapter 1

Primary Decomposition

One of the first theorems one learns in abstract algebra is the Fundamental Theorem of Arithmetic:

Theorem 1.1. *Every integer can be written as a product of primes, which is unique up to sign and the order of the factors. More precisely, for every $n \in \mathbb{Z}$ there exist primes $p_1, \ldots, p_k \in \mathbb{Z}$ and integers $a_1, \ldots, a_k > 0$ such that*

$$n = \pm p_1^{a_1} \cdots p_k^{a_k}.$$

Under the philosophy that general rings are modeled after the integers, we might expect such a theorem in any ring. But what would a general version of this theorem look like? A first guess would perhaps be that every element in any reasonable ring should be a product of irreducible elements, unique up to the order of the factors and up to multiplication by a unit. But this fails easily.

Example 1.2. In $\mathbb{Z}[\sqrt{-5}]$,

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

are two *different* ways to write 6 as a product of irreducible elements: there is no way to obtain 2 or 3 from $1 + \sqrt{-5}$ or $1 - \sqrt{-5}$ by multiplying by a unit.

The problem here is that we are focusing on *elements* when we ought to focus on *ideals*. Instead of writing *elements* as products of irreducibles, we will write *ideals* in terms of *primary ideals*.

But before we discuss primary decomposition, we will need to recall some elementary facts about minimal primes and associated primes; the details and proofs we skip can be found in any standard introduction to commutative algebra, such as [Eis95], [AM69], or [BH93].

1.1 Minimal primes

Definition 1.3. Given a ring R, the set of prime ideals in R is denoted $\mathrm{Spec}(R)$, and called the **spectrum** of R. Given an ideal I, the set of all primes that contain I is denoted $V(I)$.

Definition 1.4. Let I be an ideal in a ring R. A **minimal prime** of I is a minimal element (with respect to containment) in $V(I)$. More precisely, P is a minimal prime of I if the following hold:

- P is a prime ideal,
- $P \supseteq I$, and
- if Q is also a prime ideal and $I \subseteq Q \subseteq P$, then $Q = P$.

The set of minimal primes of I is denoted $\operatorname{Min}(I)$.

Example 1.5. Let k be a field and $R = k[x, y]$. Every prime containing $I = (x^2, xy)$ must contain x^2, and thus x. On the other hand, (x) is a prime ideal containing I. Therefore, I has a unique minimal prime, and $\operatorname{Min}(I) = \{(x)\}$.

Remark 1.6. If $\mathfrak{p}$ is prime, then $\operatorname{Min}(\mathfrak{p}) = \{\mathfrak{p}\}$.

Minimal primes are closely associated to radicals.

Definition 1.7. The **radical** of an ideal I in a ring R is the ideal

$$\sqrt{I} := \{f \in R \mid f^n \in I \text{ for some } n\}.$$

An ideal is a **radical ideal** if $I = \sqrt{I}$.

Macaulay2. Given an ideal I, `radical I` returns the radical of I.

Example 1.8. Prime ideals are radical.

Example 1.9. The ideal $I = (x^2, xy)$ in the ring $R = k[x, y]$ from Example 1.5 is not radical, since it contains x^2 but not x.

Theorem 1.10. *Let R be a ring, and I be an ideal. Then*

$$\sqrt{I} = \bigcap_{P \in V(I)} P = \bigcap_{P \in \operatorname{Min}(I)} P.$$

Example 1.11. The radical of the ideal $I = (x^2, xy)$ in the ring $R = k[x, y]$ from Example 1.5 is $\sqrt{I} = (x)$. We saw before that $\operatorname{Min}(I) = \{(x)\}$.

Example 1.12. In $R = k[x, y]$, the ideal $I = (xy, xz) = (x) \cap (y, z)$ is radical, and its minimal primes are (x) and (y, z).

Over a noetherian ring, we can realize every radical ideal as the intersection of finitely many primes.

Theorem 1.13. *Over any noetherian ring, any ideal I has finitely many minimal primes, and thus $\sqrt{I}$ is a finite intersection of primes.*

Macaulay2. The method `minimalPrimes` receives an ideal and returns a list of its minimal primes.

Example 1.14. The nilpotent elements of a ring R are exactly the elements in the radical of (0). By Theorem 1.10, $\sqrt{(0)}$ is the intersection of the minimal primes of (0), or equivalently, the intersection of the minimal elements among all the primes in R. The radical of (0) is often called the **nilradical** of R, denoted $\mathcal{N}(R)$.

Example 1.15. Let k be a field. The nilradical of $R = k[x, y]/(x^2, xy)$ corresponds to the radical of (x^2, xy) is $k[x, y]$, so it is the ideal $(x)/(x^2, xy)$.

Remark 1.16. Since $I \subseteq \sqrt{I}$, any prime containing $\sqrt{I}$ must also contain I. On the other hand, if P is a prime containing I, and $f \in \sqrt{I}$, then for some n we have $f^n \in I \subseteq P$, and since P is prime we must have $f \in P$. This shows that $V(I) = V(\sqrt{I})$, and therefore $\operatorname{Min}(I) = \operatorname{Min}(\sqrt{I})$.

Lemma 1.17. *If* $\operatorname{Min}(I) = \{P_1, \ldots, P_n\}$*, no* P_i *can be deleted in the intersection* $P_1 \cap \cdots \cap P_n$*.*

Proof. Suppose that we can delete P_i, meaning that

$$\bigcap_{j=1}^{n} P_j = \bigcap_{j \neq i} P_j.$$

Then

$$P_i \supseteq \bigcap_{j=1}^{n} P_j = \bigcap_{j \neq i} P_j \supseteq \prod_{j \neq i} P_j.$$

Since P_i is prime, this implies that $P_i \supseteq P_j$ for some $j \neq i$, but this contradicts the assumption that the primes are incomparable. □

Lemma 1.18. *Let* I *be an ideal in* R*. If* $I = P_1 \cap \cdots \cap P_n$ *where each* P_i *is prime and* $P_i \not\subseteq P_j$ *for each* $i \neq j$*, then* $\operatorname{Min}(I) = \{P_1, \ldots, P_n\}$*. Moreover,* I *must be radical.*

Proof. If Q is a prime containing I, then $Q \supseteq (P_1 \cap \cdots \cap P_n)$. We claim that Q must contain of the P_i. Indeed, if $Q \not\supseteq P_i$ for all i, then there are elements $f_i \in P_i$ such that $f_i \notin Q$, so their product satisfies $f_1 \cdots f_n \in (P_1 \cap \cdots \cap P_n)$ but $f_1 \cdots f_n \notin Q$. This is a contradiction, so indeed any prime containing I must contain some P_i. Therefore, any minimal prime of I must be one of the P_i. Since we assumed that the P_i are incomparable, these are exactly all the minimal primes of I.

By assumption, I coincides with the intersection of its minimal primes, and by Theorem 1.10 this intersection is $\sqrt{I}$. Therefore, $I = \sqrt{I}$. □

Remark 1.19. If $I = P_1 \cap \cdots \cap P_n$ for some primes P_i, we can always delete unnecessary components until no component can be deleted. Therefore, $\operatorname{Min}(I) \subseteq \{P_1, \ldots, P_n\}$.

As a consequence of Lemma 1.17 and Lemma 1.18, if I is a radical ideal, there is a unique way to write I as a finite intersection of incomparable prime ideals. Moreover, any ideal that can be written as a finite intersection of prime ideals is radical.

1.2 Localization

Definition 1.20. A **multiplicative closed** set W in a ring R is a subset $W \subseteq R$ containing 1 and closed for products, meaning $a, b \in W \implies ab \in W$.

Given a multiplicative closed subset W, we can form a new ring, the **localization** of R at W, which is a ring with elements

$$W^{-1}R := \left\{ \frac{r}{w} \;\middle|\; r \in R, w \in W \right\} / \sim$$

where $\sim$ is the equivalence relation

$$\frac{r}{w} \sim \frac{r'}{w'} \text{ if there exists } u \in W : u(rw' - r'w) = 0.$$

The operations are given by

$$\frac{r}{v} + \frac{s}{w} = \frac{rw + sv}{vw} \qquad \text{and} \qquad \frac{r}{v}\frac{s}{w} = \frac{rs}{vw}.$$

We write elements in $W^{-1}R$ in the form $\frac{r}{w}$, though they are equivalence classes of such expressions. The zero in $W^{-1}R$ is $\frac{0}{1}$ and the identity is $\frac{1}{1}$. There is a canonical ring homomorphism

$$\begin{aligned} R &\longrightarrow W^{-1}R\,. \\ r &\longmapsto \tfrac{r}{1} \end{aligned}$$

We can also localize modules. Given a module M, the **localization** of M at W is a module over the ring $W^{-1}R$, given by

$$W^{-1}M := \left\{ \frac{m}{w} \;\middle|\; m \in M, w \in W \right\} / \sim$$

where $\sim$ is the equivalence relation $\dfrac{m}{w} \sim \dfrac{m'}{w'}$ if $u(mw' - m'w) = 0$ for some $u \in W$. The operations are given by

$$\frac{m}{v} + \frac{n}{w} = \frac{mw + nv}{vw} \qquad \text{and} \qquad \frac{r}{v}\frac{m}{w} = \frac{rm}{vw}.$$

Remark 1.21. If $\alpha : M \to N$ is an R-module homomorphism, then there is a $W^{-1}R$-module homomorphism $W^{-1}\alpha : W^{-1}M \to W^{-1}N$ given by the rule $W^{-1}\alpha(\frac{m}{w}) = \frac{\alpha(m)}{w}$.

One thing to keep in mind is that things might unexpectedly become zero in a localization.

Definition 1.22. The **annihilator** of an R-module M is the ideal

$$\operatorname{ann}(M) := \{r \in R \mid rm = 0 \text{ for all } m \in M\}.$$

Given ideals I and J in R, the **colon** of I and J is the ideal

$$(J : I) := \{r \in R \mid rI \subseteq J\}.$$

More generally, if M and N are submodules of some R-module A, the colon of N and M is

$$(N :_R M) := \{r \in R \mid rM \subseteq N\}.$$

The annihilator of M is an ideal in R, and $\operatorname{ann}(M) = (0 :_R M)$. Moreover, any colon $(N :_R M)$ is an ideal in R.

Macaulay2. The methods `ann` and `annihilator` are equivalent, and both receive a module M or an element f in a module M and returns $\operatorname{ann}(M)$ or $\operatorname{ann}(f)$. Given two R-modules M and N or two ideals I and J in R, `M : N` and `I : J` return the corresponding colon ideals.

Remark 1.23. Given ideals I and J in R, $(I : J) = R$ if and only if $J \subseteq I$. Moreover, note that we always have $(I : J) \supseteq I$.

Lemma 1.24. *Given an R-module M,*

$$\frac{m}{w} \in W^{-1}M \text{ is zero} \iff vm = 0 \text{ for some } v \in W \iff \operatorname{ann}_R(m) \cap W \neq \varnothing.$$

Proof. For the first equivalence, we use the equivalence relation defining $W^{-1}R$ to note that $\frac{m}{w} = \frac{0}{1}$ in $W^{-1}M$ if and only if there exists some $v \in W$ such that $0 = v(1m - 0w) = vm$. The second equivalence just comes from the definition of the annihilator. □

Remark 1.25. As a corollary to Lemma 1.24, we obtain that if W is a multiplicatively closed set in R and W does not contain any zerodivisors, then the localization map $R \to W^{-1}R$ is injective, since no element in W can be in the annihilator of a nonzero element.

Notation 1.26. Let $f : R \to S$ be a ring homomorphism. Given an ideal I in R, the **expansion** of I to S is the ideal of S generated by $f(I)$, and we denote it by IS. Given an ideal J of S, the contractionx of J to R is the preimage of J via f, which we denote by $J \cap R$:

$$J \cap R := f^{-1}(J) = \{r \in R \mid f(r) \in J\}.$$

There is much to say about expansion and contraction of ideals, the details of which can be found in any standard commutative algebra reference such as [Mat89] or [AM69]. Later on, it it will be helpful to know the following facts:

- For any ideals I in R and J in S, we have $(IS \cap R)S = IS$ and $(J \cap R)S \cap R = J \cap R$.
- The contraction of a prime ideal is prime.
- The expansion of a prime ideal might fail to be prime.
- A prime ideal P in R is the contraction of a prime in S if and only if $PS \cap R = P$.

We will see contractions of ideals most often when talking about localizations. Given a multiplicatively closed set W in a ring R and an ideal I in $W^{-1}R$, we write $I \cap R$ for the **contraction** of I into R, which is the preimage of I in R via the canonical map $R \to W^{-1}R$. More precisely,

$$I \cap R = \left\{ r \in R \,\middle|\, \frac{r}{1} \in I \right\}.$$

Theorem 1.27. *Let R be a ring and W be a multiplicatively closed set in R.*

a) If I is an ideal in R, then $W^{-1}I \cap R = \{r \in R \mid wr \in I \text{ for some } w \in W\}$.

b) If J is an ideal in $W^{-1}R$, then $W^{-1}(J \cap R) = J$.

c) If P is a prime ideal and $W \cap P = \varnothing$, then $W^{-1}P = P(W^{-1}R)$ is prime.

d) The set of prime ideals in $W^{-1}R$ is in bijection with

$$\{P \in \mathrm{Spec}(R) \mid P \cap W = \varnothing\}.$$

Theorem 1.28. *Localization is exact: given a short exact sequence of R-modules*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

and a multiplicative set W, the sequence

$$0 \longrightarrow W^{-1}A \longrightarrow W^{-1}B \longrightarrow W^{-1}C \longrightarrow 0$$

is also exact.

The most important multiplicatively closed sets we will do localization on are the complements of prime ideals. As an immediate consequence of the definition of prime ideal, we get that $W = R \setminus P$ is a multiplicatively closed set.

Definition 1.29. Let R be a ring and P be a prime ideal in R. We write R_P for the localization $(R \setminus P)^{-1}R$, and call it the **localization of R at P**. Given an ideal I in R, we write I_P instead of $(R \setminus P)^{-1}I$, the ideal in R_P generated by all the images of elements in I. This ideal I_P is the same as IR_P, the expansion of I to R_P.

The ring R_P is a local ring with unique maximal ideal P_P. The proper ideals in R_P are of the form I_P, where $I \subseteq P$ is an ideal in R, and the primes in R_P are precisely the ideals of the form Q_P with $Q \subseteq P$ prime.

We can also localize at the complement of a union of primes.

Remark 1.30. Let A be a finite set of prime ideals in a noetherian ring R, and consider the set

$$W := \{r \in R \mid r \notin \bigcup_{P \in A} P\}.$$

If $x, y \in W$, then $x, y \notin P$ for any of the primes $P \in A$, and thus $xy \in W$. Moreover, $1 \notin P$ for any $P \in A$, so $1 \in W$. We conclude that W is a multiplicatively closed set. The localization $W^{-1}R$ is now a semilocal ring, which means it has only finitely many maximal ideals — the maximal elements in A.

Definition 1.31. If M is an R-module, the **support** of M is

$$\mathrm{Supp}(M) := \{\mathfrak{p} \in \mathrm{Spec}(R) \mid M_\mathfrak{p} \neq 0\}.$$

Example 1.32. If $M = R/I$, then $\mathrm{Supp}(M) = V(I)$. Indeed, $M_\mathfrak{p}$ is generated by the image of 1, so $M_\mathfrak{p} = 0$ iff the image of 1 is zero in the localization. But this happens if and only if

$$\exists w \notin \mathfrak{p} : w \cdot 1 = 0 \text{ in } R/I \Leftrightarrow \exists w \notin \mathfrak{p}, w \in I \Leftrightarrow \mathfrak{p} \not\supseteq I.$$

Proposition 1.33. *Given M a finitely generated R-module over a ring R,*

$$\mathrm{Supp}(M) = V(\mathrm{ann}_R(M)).$$

In particular, $\mathrm{Supp}(R/I) = V(I)$.

Proof. Let $M = Rm_i + \cdots + Rm_n$. We have

$$\mathrm{ann}_R(M) = \bigcap_{i=1}^{n} \mathrm{ann}_R(m_i),$$

so

$$V(\mathrm{ann}_R(M)) = \bigcup_{i=1}^{n} V(\mathrm{ann}_R(m_i)).$$

Notice that we need finiteness here. Also, we claim that

$$\mathrm{Supp}(M) = \bigcup_{i=1}^{n} \mathrm{Supp}(Rm_i).$$

To show $(\supseteq)$, notice that $(Rm_i)_\mathfrak{p} \subseteq M_\mathfrak{p}$, so

$$\mathfrak{p} \in \mathrm{Supp}(Rm_i) \implies 0 \neq (Rm_i)_\mathfrak{p} \subseteq M_\mathfrak{p} \implies \mathfrak{p} \in \mathrm{Supp}(M).$$

On the other hand, the images of $m_1, \ldots, m_n$ in $M_\mathfrak{p}$ generate $M_\mathfrak{p}$ for each $\mathfrak{p}$, so $\mathfrak{p} \in \mathrm{Supp}(M)$ if and only if $\mathfrak{p} \in \mathrm{Supp}(Rm_i)$ for some m_i. Thus, we can reduce to the case of a cyclic module Rm. Now $\frac{m}{1} = 0$ in $M_\mathfrak{p}$ if and only if $(R \setminus \mathfrak{p}) \cap \mathrm{ann}_R(m) \neq \varnothing$, which happens if and only if $\mathrm{ann}_R(m) \not\subseteq \mathfrak{p}$. □

1.3 Associated primes

Remark 1.34. Let R be a ring, I be an ideal in R, and M be an R-module. To give an R-module homomorphism $R \longrightarrow M$ is the same as choosing an element m of M (the image of 1 via our map) or equivalently, to choose a cyclic submodule of M (the submodule generated by m).

To give an R-module homomorphism $R/I \longrightarrow M$ is the same as giving an R-module homomorphism $R \longrightarrow M$ whose image is killed by I. Thus giving an R-module homomorphism $R/I \longrightarrow M$ is to choose an element $m \in M$ that is killed by I, meaning $I \subseteq \mathrm{ann}(m)$. The kernel of the map $R \to M$ given by $1 \mapsto m$ is precisely $\mathrm{ann}(m)$, so a well-defined map $R/I \to M$ given by $1 \mapsto m$ is injective if and only if $I = \mathrm{ann}(m)$.

Definition 1.35. Let R be a ring, and M a module. We say that $P \in \mathrm{Spec}(R)$ is an **associated prime** of M if $P = \mathrm{ann}_R(m)$ for some $m \in M$. Equivalently, P is associated to M if there is an injective homomorphism $R/P \longrightarrow M$. We write $\mathrm{Ass}_R(M)$ for the set of associated primes of M.

We will be primarily interested in the associated primes of R/I, where I is an ideal in R. We will abuse notation and call these the **associated primes of** I, and even write $\mathrm{Ass}_R(I)$.

Lemma 1.36. *Let R be a noetherian ring and M be an R-module. A prime P is associated to M if and only if $P_P \in \mathrm{Ass}(M_P)$.*

Proof. By Theorem 1.28, localization is exact, so any inclusion $R/P \subseteq M$ gives an inclusion $R_P/P_P \subseteq M_P$. Conversely, let $P_P = \mathrm{ann}(\frac{m}{w})$ for some $\frac{m}{w} \in M_P$. Let $P = (f_1, \ldots, f_n)$. Since $\frac{f_i}{1}\frac{m}{r} = \frac{0}{1}$, there exists $u_i \notin P$ such that $u_i f_i m = 0$. Then $u = u_1 \cdots u_n$ is not in P, since P is prime, and $u f_i m = 0$ for all i. Since the f_i generate P, we have $P(um) = 0$. On the other hand, if $r \in \mathrm{ann}(um)$, then $\frac{ru}{1} \in \mathrm{ann}(\frac{m}{w}) = P_P$. We conclude that $ru \in P_P \cap R = P$. Since $u \notin P$, we conclude that $r \in P$. □

Lemma 1.37. *If P is prime, then $\mathrm{Ass}_R(R/P) = \{P\}$.*

Proof. An element $r + P \in R/P$ is nonzero if and only if $r \notin P$. Given any nonzero $r + P \in R/P$ we have $\mathrm{ann}_R(r + P) = \{s \in R \mid rs \in P\} = P$ by definition of prime ideal. □

Soon we will see that the converse does not hold.

Definition 1.38. Let M be an R-module. An element $r \in R$ is a **zerodivisor** on M if $rm = 0$ for some $m \in M$. We sometimes write the set of zerodivisors of M as $\mathcal{Z}(M)$.

Theorem 1.39. *If R is Noetherian, and M is an arbitrary R-module, then the following hold:*

1) For any nonzero $m \in M$, $\mathrm{ann}_R(m)$ is contained in an associated prime of M.

2) $\mathrm{Ass}(M) = \varnothing \iff M = 0$.

3) $\bigcup_{\mathfrak{p} \in \mathrm{Ass}(M)} \mathfrak{p} = \mathcal{Z}(M)$.

Proof. Even if R is not Noetherian, $M = 0$ implies $\mathrm{Ass}(M) = \varnothing$ by definition. So we focus on the case when $M \neq 0$.

First, we are going to show that 1) implies 2) and 3). To do that, let's suppose that we have shown 1). If $M \neq 0$, then M contains a nonzero element m, and $\mathrm{ann}(m)$ is contained in an associated prime of M. In particular, $\mathrm{Ass}(M) \neq 0$, and 2) holds. Now if $r \in \mathcal{Z}(M)$, then by definition we have $r \in \mathrm{ann}(m)$ for some nonzero $m \in M$. Since $\mathrm{ann}(m)$ is contained in some associated prime of M, so is r. On the other hand, if $\mathfrak{p}$ is an associated prime of M, then by definition all elements in $\mathfrak{p}$ are zerodivisors on M. This shows that 3) holds. So all that is left is to prove 1).

Now we show 1) for any $M \neq 0$. The set of ideals $S := \{\mathrm{ann}_R(m) \mid m \in M, m \neq 0\}$ is nonempty, and any element in S is contained in a maximal element, by Noetherianity. Note in fact that any element in S must be contained in a maximal element of S. Let $I = \mathrm{ann}(m)$ be any maximal element, and let $rs \in I$, $s \notin I$. We always have $\mathrm{ann}(sm) \supseteq \mathrm{ann}(m)$, and equality holds by the maximality of $\mathrm{ann}(m)$ in S. Then $r(sm) = (rs)m = 0$, so $r \in \mathrm{ann}(sm) = \mathrm{ann}(m) = I$. We conclude that I is prime, and therefore it is an associated prime of M. □

Lemma 1.40. *If*

$$0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$$

is an exact sequence of R-modules, then $\mathrm{Ass}(L) \subseteq \mathrm{Ass}(M) \subseteq \mathrm{Ass}(L) \cup \mathrm{Ass}(N)$.

Proof. If R/P includes in L, then composition with the inclusion $L \hookrightarrow M$ gives an inclusion $R/P \hookrightarrow M$. This shows that $\mathrm{Ass}(L) \subseteq \mathrm{Ass}(M)$.

Now let $\mathfrak{p} \in \mathrm{Ass}(M)$, and let $m \in M$ be such that $\mathfrak{p} = \mathrm{ann}(m)$. First, note that $\mathfrak{p} \subseteq \mathrm{ann}(rm)$ for all $r \in R$.

Thinking of L as a submodule of N, suppose that there exists $r \notin \mathfrak{p}$ such that $rm \in L$. Then

$$s(rm) = 0 \iff (sr)m = 0 \implies sr \in \mathfrak{p} \implies s \in p.$$

So $\mathfrak{p} = \mathrm{ann}(rm)$, and thus $\mathfrak{p} \in \mathrm{Ass}(L)$.

If $rm \notin L$ for all $r \notin \mathfrak{p}$, let n be the image of m in N. Thinking of N as M/L, if $rn = 0$, then we must have $rm \in L$, and by assumption this implies $r \in \mathfrak{p}$. Since $\mathfrak{p} = \mathrm{ann}(m) \subseteq \mathrm{ann}(n)$, we conclude that $\mathfrak{p} = \mathrm{ann}(n)$. Therefore, $\mathfrak{p} \in \mathrm{Ass}(N)$. □

Note that the inclusions in Lemma 1.40 are not necessarily equalities.

Example 1.41. If M is a module with at least two associated primes, and P is an associated prime of M, then

$$0 \longrightarrow R/P \longrightarrow M$$

is exact, but $\{P\} = \mathrm{Ass}(R/P) \subsetneq \mathrm{Ass}(M)$.

Example 1.42. Let $R = k[x]$, where k is a field, and consider the short exact sequence of R-modules

$$0 \longrightarrow (x) \longrightarrow R \longrightarrow R/(x) \longrightarrow 0\,.$$

Then one can check that:

- $\mathrm{Ass}(R/(x)) = \mathrm{Ass}(k) = \{(x)\}$.
- $\mathrm{Ass}(R) = \mathrm{Ass}((x)) = \{(0)\}$.

In particular, $\mathrm{Ass}(R) \subsetneq \mathrm{Ass}(R/(x)) \cup \mathrm{Ass}((x))$.

Corollary 1.43. *Let A and B be R-modules. Then $\mathrm{Ass}(A \oplus B) = \mathrm{Ass}(A) \cup \mathrm{Ass}(B)$.*

Proof. Apply Lemma 1.40 to the short exact sequence

$$0 \longrightarrow A \longrightarrow A \oplus B \longrightarrow B \longrightarrow 0\,.$$

This gives us $\mathrm{Ass}(A) \subseteq \mathrm{Ass}(A \oplus B) \subseteq \mathrm{Ass}(A) \cup \mathrm{Ass}(B)$. Repeating with

$$0 \longrightarrow B \longrightarrow A \oplus B \longrightarrow A \longrightarrow 0\,,$$

we conclude that $\mathrm{Ass}(B) \subseteq \mathrm{Ass}(A \oplus B)$. So we have shown both $\mathrm{Ass}(A) \subseteq \mathrm{Ass}(A \oplus B)$ and $\mathrm{Ass}(B) \subseteq \mathrm{Ass}(A \oplus B)$, so $\mathrm{Ass}(A) \cup \mathrm{Ass}(B) \subseteq \mathrm{Ass}(A \oplus B)$. Since we have also already shown $\mathrm{Ass}(A \oplus B) \subseteq \mathrm{Ass}(A) \cup \mathrm{Ass}(B)$, we must have $\mathrm{Ass}(A \oplus B) = \mathrm{Ass}(A) \cup \mathrm{Ass}(B)$. □

Theorem 1.44. *If R is a noetherian ring, and M is a finitely generated R-module, then $\mathrm{Ass}_R(M)$ is finite. Moreover, if R and M are graded, then $\mathrm{Ass}_R(M)$ is a finite set of homogeneous primes.*

In a Noetherian ring, associated primes localize.

Theorem 1.45. *Let R be a Noetherian ring, W a multiplicative set, and M a module. Then*

$$\mathrm{Ass}_{W^{-1}R}(W^{-1}M) = \{W^{-1}P \mid P \in \mathrm{Ass}_R(M),\ P \cap W = \varnothing\}.$$

Proof. Given $P \in \mathrm{Ass}_R(M)$ such that $P \cap W = \varnothing$, Theorem 1.27 says that $W^{-1}P$ is a prime in $W^{-1}R$. Since $P \in \mathrm{Ass}(M)$, we have an inclusion map $R/P \subseteq M$. Localization is exact, by Theorem 1.28, so we get an inclusion $W^{-1}R/W^{-1}P \cong W^{-1}(R/P) \subseteq W^{-1}M$, which says that $W^{-1}P$ is an associated prime of $W^{-1}M$.

Now suppose that $Q \in \mathrm{Spec}(W^{-1}R)$ is associated to $W^{-1}M$. By Theorem 1.27, we know this is of the form $W^{-1}P$ for some prime P in R such that $P \cap W = \varnothing$, so we just need to prove that $P \in \mathrm{Ass}(M)$. Since R is noetherian, P is finitely generated, say $P = (f_1, \ldots, f_n)$ in R, and so $Q = \left(\frac{f_1}{1}, \ldots, \frac{f_n}{1}\right)$.

By assumption, $Q = \mathrm{ann}(\frac{m}{w})$ for some $m \in M$, $w \in W$. Since w is a unit in $W^{-1}R$, we can also write $Q = \mathrm{ann}(\frac{m}{1})$. By definition, this means that for each i

$$\frac{f_i}{1}\frac{m}{1} = \frac{0}{1} \iff u_i f_i m = 0 \text{ for some } u_i \in W.$$

Let $u = u_1 \cdots u_n \in W$. Then $u f_i m = 0$ for all i, and thus $Pum = 0$. We claim that in fact $P = \mathrm{ann}(um)$ in R. Given any $v \in \mathrm{ann}(um)$, we have $u(vm) = v(um) = 0$, and since $u \in W$, this implies that $\frac{vm}{1} = 0$. Therefore, $\frac{v}{1} \in \mathrm{ann}(\frac{m}{1}) = W^{-1}\mathfrak{p}$, and $vw \in P$ for some $w \in W$. But $P \cap W = \varnothing$, and thus $v \in P$. Thus $P \in \mathrm{Ass}(M)$. □

Theorem 1.46. *Let R be Noetherian, and M be an R-module.*

a) $\mathrm{Supp}_R(M) = \bigcup_{\mathfrak{p} \in \mathrm{Ass}_R(M)} V(\mathfrak{p})$.

b) If M is a finitely generated R-module, then $\mathrm{Min}(\mathrm{ann}_R(M)) \subseteq \mathrm{Ass}_R(M)$. *In particular,* $\mathrm{Min}(I) \subseteq \mathrm{Ass}_R(R/I)$.

Proof.

a) Let $P \in \mathrm{Ass}_R(M)$, and fix $m \in M$ such that $P = \mathrm{ann}_R(m)$. Let $Q \in V(P)$. By Proposition 1.33, $Q \in \mathrm{Supp}(R/P)$. Since $0 \to R/\mathfrak{p} \xrightarrow{m} M$ is exact and localization is exact, by Theorem 1.28, $0 \to (R/P)_Q \to M_Q$ is also exact. Since $(R/P)_Q \neq 0$, we must also have $M_Q \neq 0$, and thus $Q \in \mathrm{Supp}(M)$. This shows $\mathrm{Supp}_R(M) \supseteq \bigcup_{\mathfrak{p} \in \mathrm{Ass}_R(M)} V(\mathfrak{p})$.

Now let Q be a prime ideal and suppose that

$$Q \notin \bigcup_{\mathfrak{p} \in \mathrm{Ass}_R(M)} V(\mathfrak{p}).$$

In particular, Q does not contain any associated prime of M. Then there is no associated prime of M that does not intersect $R \setminus Q$, so by Theorem 1.45, $\mathrm{Ass}_{R_Q}(M_Q) = \varnothing$. By Theorem 1.39, $M_Q = 0$.

b) We have shown that

$$V(\operatorname{ann}_R(M)) = \operatorname{Supp}_R(M) = \bigcup_{\mathfrak{p} \in \operatorname{Ass}_R(M)} V(\mathfrak{p}),$$

so the minimal elements of both sets agree. In particular, the right hand side has the minimal primes of $\operatorname{ann}_R(M)$ as minimal elements, and they must be associated primes of M, or else this would contradict minimality. □

So the minimal primes of a module M are all associated to M, and they are precisely the minimal elements in the support of M.

Definition 1.47. If I is an ideal, then an associated prime of I that is not a minimal prime of I is called an **embedded prime** of I.

Macaulay2. Given an R-module M, `associatedPrimes M` will return a list, the list of all the primes in $\operatorname{Ass}_R(M)$. If I is an ideal in R, Macaulay2 follows the same convention we do: `associatedPrimes I` will return $\operatorname{Ass}(I)$, the associated primes of the module R/I.

Example 1.48. Let's get back to the ideal $I = (x^2, xy)$ in $R = k[x, y]$ from Example 1.5. We saw before that this ideal has only one minimal prime, (x). We claim it also has an embedded prime: $\mathfrak{m} = (x, y)$. Indeed, $x + I$ is a nonzero element in R/I killed by $\mathfrak{m}$, and since $\mathfrak{m}$ is a maximal ideal and $x + I \neq 0$, we must have $\operatorname{ann}(x + I) = \mathfrak{m}$. We can also rewrite all this as $\mathfrak{m} = (I : x)$. This shows that indeed $\mathfrak{m}$ is an associated prime of I.

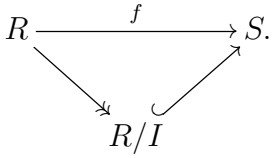
We can use Macaulay2 to check that these are all the associated primes of I for some choice of k.

```
i1 : R = QQ[x,y];

i2 : I = ideal"x2,xy";

i3 : associatedPrimes I

o3 = {ideal x, ideal (y, x)}

o3 : List
```

Theorem 1.49. *Let $f : R \to S$ be a ring homomorphism and let M be a finitely generated S-module. Then*

$$\operatorname{Ass}_R(M) = \{P \cap R \mid P \in \operatorname{Ass}_S(M)\}.$$

Proof. First let's reduce to the case when $R \subseteq S$ is an inclusion of noetherian rings. Setting $I = \ker f$, we can factor f as follows:



Given any S-module M, when we view it as an R-module via restriction of scalars we must have $I \subseteq \operatorname{ann}(M)$, so M is an R/I-module with the exact same structure it has as an R-module. In particular, we see that a prime P in R is in $\operatorname{Ass}_R(M)$ if and only if $P/I \in \operatorname{Ass}_{R/I}(M)$. Moreover, given any prime P in S, if its contraction to R or R/I is prime, and if Q is a prime ideal in R such that $Q/I = P \cap R/I$, then $Q = P \cap R$. This shows that it is sufficient to consider the case when f is injective.

Given an element $m \in M$, an element $r \in R$ acts on m by $r \cdot m = f(r)m$, so

$$r \in (0 :_R m) \Leftrightarrow r \cdot m = 0 \Leftrightarrow f(r)m = 0 \Leftrightarrow f(r) \in (0 :_S m).$$

Therefore, $\operatorname{ann}_R(m) = \operatorname{ann}_S(m) \cap R$. In particular, if a prime P in S is associated to M, then $P = \operatorname{ann}_S(m)$ for some m, and $P \cap R = \operatorname{ann}_R(m)$. Since the contraction of a prime is prime, $P \cap R \in \operatorname{Ass}_R(M)$.

Now let $Q \in \operatorname{Ass}_R(M)$, and let $m \in M$ be such that $Q = \operatorname{ann}_R(m)$. Then $I := \operatorname{ann}_S(m)$ satisfies $I \cap R = Q$. We want to find a prime ideal P in S such that $P \cap R = Q$. First, note that since $I = \operatorname{ann}_S(m)$, the map $S \to M$ determined by sending 1 to m has kernel I, so we have an inclusion $S/I \hookrightarrow M$. By Lemma 1.40, $\operatorname{Ass}_S(S/I) \subseteq \operatorname{Ass}_S(M)$. So if we find a prime $P \in \operatorname{Ass}_S(S/I)$ such that $P \cap R = Q$, this P will be an element of $\operatorname{Ass}_S(M)$, and we will be done.

Since $I \cap R = Q$, we have an inclusion $R/Q \to S/I$. Write $\overline{R} := R/Q$ and $\overline{S} := S/I$. Since $\overline{R}$ is a domain, the zero ideal J in $\overline{R}$ is prime. On the other hand, $J\overline{S}$ is the zero ideal in $\overline{S}$, so $J\overline{S} \cap \overline{R} = J$. Any prime ideal J satisfying $J\overline{S} \cap \overline{R} = J$ is the contraction of a prime, so let P be a prime ideal in S whose image in $\overline{S}$ contracts to $J = (0)$ in $\overline{R}$. Lifting to R and S, this prime ideal P in S must contract to Q. Moreover, we can take this P to be minimal over I: if P is not minimal over I, then it contains a minimal prime P' of I, and $Q = P \cap R \supseteq P' \cap R \supseteq I \cap R = Q$, so we can ultimately replace P with P'.

We found a prime ideal P in S with $P \cap R = Q$. By construction, this prime P is a minimal prime of I, and thus by Theorem 1.46, $P \in \operatorname{Ass}_S(R/I) \subseteq \operatorname{Ass}_S(M)$. □

Finally, we record a lemma we will use later about the associated primes over R and R/I.

Lemma 1.50. *Given an ideal I in a noetherian ring R, and let P be a prime ideal in R. If M is a finitely generated R-module with $I \subseteq \operatorname{ann}(M)$, then*

$$P \in \operatorname{Ass}_R(M) \text{ if and only if } P/I \in \operatorname{Ass}_{R/I}(M).$$

Proof. Since $I \subseteq \operatorname{ann}(M)$, M has a structure of an R/I-module that is compatible with its R-module structure; these two structures are essentially the same.

If $P \in \operatorname{Ass}_R(M)$, there exists $a \in M$ such that

$$P = \operatorname{ann}_R(m) = \{r \in R \mid ra = 0\}.$$

Then

$$P/I = \{r + I \mid ra = 0\} = \operatorname{ann}_{R/I}(m).$$

On the other hand, all primes in R/I are of the form P/I for some prime ideal $P \supseteq I$ in R, so if $P/I = ann_{R/I}(m)$ for some $m \in M$, then

$$P/I = \{r + I \mid ra = 0\} = \{r + I \mid (r + I)a = 0\},$$

and thus $P \subseteq \operatorname{ann}_R(m)$. Moreover, if $r \in R$ satisfies $ra = 0$, then $(r + I)a = ra = 0$, so $r + I \in \operatorname{ann}_{R/I}(m) = P/I$. Since $P \supseteq I$, we conclude that $r \in P$. □

1.4 Primary Ideals

Definition 1.51. We say that an ideal I is **primary** if

$$xy \in I \implies x \in I \text{ or } y \in \sqrt{I}.$$

We say that an ideal I is P**-primary** if I is primary and $\sqrt{I} = P$.

Remark 1.52. Suppose that Q is primary and $xy \in \sqrt{Q}$. Then $x^n y^n \in Q$ for some n. If $y \notin \sqrt{Q}$, then $y^n \notin \sqrt{Q}$. Since Q is primary, we must have $x^n \in Q$, so $x \in \sqrt{Q}$. Therefore, the radical of a primary ideal is always prime, so every primary ideal Q is $\sqrt{Q}$-primary.

Example 1.53. a) Any prime ideal is primary.

b) If R is a UFD, we claim that a principal ideal is primary if and only if it is generated by a power of an irreducible element. If $f \in R$ is an irreducible element, then

$$xy \in (f^n) \iff f^n | xy.$$

Since f is irreducible and every element in R can be written as a unique product of irreducibles, if f^n divides xy but f^n does not divide x, then f must divide y. So

$$f^n | x \text{ or } f | y \iff x \in (f^n) \text{ or } y \in \sqrt{(f^n)} = (f).$$

We conclude that (f^n) is indeed primary. Conversely, if a is not a prime power, then $a = gh$, for some g, h nonunits with no common factor, so we can take $gh \in (a)$ but $g \notin a$ and $h \notin \sqrt{(a)}$. This shows that (a) is not primary.

c) As a particular case of the previous example, the nonzero primary ideals in $\mathbb{Z}$ are of the form (p^n) for some prime p and some $n \geqslant 1$. This example is a bit misleading, as it suggests that primary ideals are the same as powers of primes. We will soon see that it not the case.

d) In $R = k[x, y, z]$, the ideal $I = (y^2, yz, z^2)$ is primary. Give R the grading with weights $|y| = |z| = 1$, and $|x| = 0$. If $g \notin \sqrt{I} = (y, z)$, then g has a degree zero term. If $f \notin I$, then f has a term of degree zero or one. The product fg has a term of degree zero or one, so it is not in I.

If the radical of an ideal is prime, that does not imply that ideal is primary.

Example 1.54. In $R = k[x, y, z]$, the ideal $Q = (x^2, xy)$ is not primary, even though $\sqrt{Q} = (x)$ is prime. The offending product is xy: $x \notin Q$ and $y \notin Q$.

The definition of primary can be reinterpreted in many ways.

Proposition 1.55. *If R is noetherian, the following are equivalent:*

(1) Q is primary.

(2) Every zerodivisor in R/Q is nilpotent on R/Q.

(3) $\operatorname{Ass}(R/Q)$ *is a singleton.*

(4) Q *has exactly one minimal prime, and no embedded primes.*

(5) $\sqrt{Q} = P$ *is prime and for all* $r, w \in R$ *with* $w \notin P$, $rw \in Q$ *implies* $r \in Q$.

(6) $\sqrt{Q} = P$ *is prime, and* $QR_P \cap R = Q$.

Proof. (1) $\iff$ (2): y is a zerodivisor modulo Q if there is some $x \notin Q$ with $xy \in Q$; the primary assumption translates to saying that a power of y is in Q.

(2) $\iff$ (3): On the one hand, (2) says that the set of zerodivisors on R/Q coincides with the elements in the nilradical of R/Q. In general, the set of zerodivisors is the union of all the associated primes, while the nilradical is the intersection of all the minimal primes. Now notice that the associated primes of R/Q are the associated primes of the ideal Q, while the minimal primes of R/Q are the minimal primes of Q. So we always have

$$\bigcup_{\mathfrak{p}\in\operatorname{Ass}(Q)} \mathfrak{p} = \mathcal{Z}(R/Q) \supseteq \{r \in R \mid r + Q \in \mathcal{N}(R/\mathfrak{q})\} = \bigcap_{\mathfrak{p}\in\operatorname{Min}(Q)} \mathfrak{p} = \bigcap_{\mathfrak{p}\in\operatorname{Ass}(Q)} \mathfrak{p}.$$

The rest of the proof is elementary set theory: the intersection and union of a collection of sets agree if and only if there is only one set. More precisely, we have equality above if and only if there is only one associated prime.

(3) $\iff$ (4) is clear, since each statement is just a restatement of the other one.

(1) $\iff$ (5): Given the observation that the radical of a primary ideal is prime, this is just a rewording of the definition.

(5) $\iff$ (6): This is immediate from the following characterization:

$$\begin{aligned} QR_P \cap R &= \left\{ r \in R \mid \frac{r}{1} \in QR_P \right\} \\ &= \left\{ r \in R \mid \frac{r}{1} = \frac{a}{w} \text{ for some } a \in Q, w \notin P \right\} \end{aligned}$$

The equality $\frac{r}{1} = \frac{a}{w}$ is equivalent to $u(wr - a)$ for some $a \in Q$ and $u, w \notin P$, so equivalently $s := uw \in W$ satisfies $sr = ua \in Q$. Therefore,

$$QR_P \cap R = \{r \in R \mid sr \in Q \text{ for some } s \notin P\}$$ □

If the radical of an ideal is maximal, that *does* imply the ideal is primary.

Remark 1.56. Let I be an ideal with $\sqrt{I} = \mathfrak{m}$ a maximal ideal. If R is noetherian, then $\operatorname{Ass}_R(R/I)$ is nonempty and contained in $\operatorname{Supp}(R/I) = V(I) = \{\mathfrak{m}\}$, so $\operatorname{Ass}_R(R/I) = \{\mathfrak{m}\}$, and hence I is primary.

Note that the assumption that $\mathfrak{m}$ is maximal was necessary here. Indeed, having a prime radical does not guarantee an ideal is primary, as we saw in Example 1.54. Moreover, even the powers of a prime ideal may fail to be primary.

Example 1.57. Let $R = k[x, y, z]/(xy - z^n)$, where k is a field and $n \geqslant 2$ is an integer. Consider the prime ideal $P = (x, z)$ in R, and note that $y \notin P$. We have $xy = z^n \in P^n$, while $x \notin P^n$ and $y \notin \sqrt{P^n} = P$. Therefore, P^n is not a primary ideal, even though its radical is the prime P.

Lemma 1.58. *Let P be a prime ideal in a noetherian ring R. If $Q \subseteq P$ is a primary ideal, then Q_P is a primary ideal in R_P, even if Q is not P-primary.*

Proof. Since $Q \subseteq P$ and P is prime, we must have $\sqrt{Q} \subseteq P$, so $Q_P = QR_P$ and $\sqrt{Q}R_P$ are proper ideals of R_P with $\sqrt{Q}R_P$ prime. Since $\operatorname{Ass}(Q) = \{\sqrt{Q}\}$, by Theorem 1.45 we have $\operatorname{Ass}(Q_P) = \{\sqrt{Q}R_P\}$. By Proposition 1.55, Q_P is a primary ideal. □

The contraction of primary ideals is always primary.

Lemma 1.59. *Let $f : R \to S$ be a ring homomorphism. If Q is a primary ideal in S, then $Q \cap R$ is a primary ideal in R. In particular, given any multiplicatively closed set W in R, and a primary ideal Q in $W^{-1}R$, $Q \cap R$ is a primary ideal in R.*

Proof. If $xy \in Q \cap R$ and $x \notin Q \cap R$, then $f(x) \notin Q$. But $f(x)f(y) = f(xy) \in Q$, and since Q is primary, so we must have $f(y^n) = f(y)^n \in Q$ for some n. Therefore, $y^n \in Q \cap R$, and $Q \cap R$ is indeed primary. □

Lemma 1.60. *Let Q be a primary ideal in a noetherian ring R. If P is a prime ideal containing Q, then $QR_P \cap R = Q$.*

Proof. By Lemma 1.58, QR_P is a primary ideal in R_P. By Lemma 1.59, $QR_P \cap R$ is also primary.

$$Q = QR_{\sqrt{Q}} \cap R = \left\{ r \in R \mid sr \in Q \text{ for some } s \notin \sqrt{Q} \right\}$$

Since P is prime and $P \supseteq Q$, then $P \supseteq \sqrt{Q}$. Therefore, the complement of $\sqrt{Q}$ contains the complement of P, and

$$\left\{ r \in R \mid sr \in Q \text{ for some } s \notin \sqrt{Q} \right\} \supseteq \{ r \in R \mid sr \in Q \text{ for some } s \notin P \} = QR_P \cap R.$$

Therefore, $Q \supseteq QR_P \cap R$. But by elementary set theory, $Q \subseteq QR_P \cap R$, so we must have $Q = QR_P \cap R$. □

The intersection of primary ideals is also primary.

Lemma 1.61. *If $I_1, \ldots, I_t$ are ideals, then*

$$\operatorname{Ass}\left(R/\bigcap_{j=1}^{t} I_j \right) \subseteq \bigcup_{j=i}^{t} \operatorname{Ass}(R/I_j).$$

In particular, a finite intersection of P-primary ideals is P-primary.

Proof. The map $R \to R/I_1 \oplus R/I_2$ given by $r \mapsto (r + I_1, r + I_2)$ has kernel $I_1 \cap I_2$, so there is an inclusion $R/(I_1 \cap I_2) \subseteq R/I_1 \oplus R/I_2$. Hence, by Lemma 1.40 we have

$$\operatorname{Ass}(R/(I_1 \cap I_2)) \subseteq \operatorname{Ass}(R/I_1) \cup \operatorname{Ass}(R/I_2).$$

For $t \geqslant 3$,

$$\operatorname{Ass}\left(R/\bigcap_{j=1}^{t} I_j \right) \subseteq \bigcup_{j=i}^{t} \operatorname{Ass}(R/I_j)$$

can be shown by an easy induction.

Now suppose all the I_j are all P-primary. Then

$$\operatorname{Ass}\left(R/\bigcap_{j=1}^{t} I_j\right) \subseteq \bigcup_{j=i}^{t} \operatorname{Ass}(R/I_j) = \{P\}.$$

On the other hand, $\bigcap_{j=1}^{t} I_j \subseteq I_1 \neq R$, so $R/(\bigcap_{j=1}^{t} I_j) \neq 0$. Thus $\operatorname{Ass}(R/(\bigcap_{j=1}^{t} I_j))$ is nonempty, by Theorem 1.39, and therefore it must be the singleton $\{P\}$. Then $\bigcap_{j=1}^{t} I_j$ is P-primary by the characterization of primary in Proposition 1.55 (3). □

1.5 Primary decomposition

Definition 1.62 (Primary decomposition)**.** A **primary decomposition** of an ideal I is an expression of the form

$$I = Q_1 \cap \cdots \cap Q_t,$$

with each $\mathfrak{q}_i$ primary. An **irredundant primary decomposition** of an ideal I is a primary decomposition as above in which $\sqrt{Q_i} \neq \sqrt{Q_j}$ for $i \neq j$, and $Q_i \not\supseteq \bigcap_{j \neq i} Q_j$ for all i.

Remark 1.63. By Lemma 1.61, we can turn any primary decomposition into an irredundant one by combining the terms with the same radical, then removing redundant terms.

Example 1.64 (Primary decomposition in $\mathbb{Z}$)**.** Given a decomposition of $n \in \mathbb{Z}$ as a product of distinct primes, say $n = p_1^{a_1} \cdots p_k^{a_k}$, then the primary decomposition of the ideal (n) is $(n) = (p_1^{a_1}) \cap \cdots \cap (p_k^{a_k})$. However, this example can be deceiving, in that it suggests that primary ideals are just powers of primes; as we saw in Example 1.57, they are not!

The existence of primary decompositions was first shown by Emanuel Lasker (yes, the chess champion!) for polynomial rings and power series rings in 1905 [Las05], and then extended to noetherian rings (in the same paper where she introduced noetherian rings – though not by that name) by Emmy Noether in 1921 [Noe21].

Theorem 1.65 (Existence of primary decompositions)**.** *Every ideal in a noetherian ring has a primary decomposition.*

Proof. We will say that an ideal is irreducible if it cannot be written as a proper intersection of larger ideals. If R is Noetherian, we claim that any ideal of R can be expressed as a finite intersection of irreducible ideals. If the set of ideals that are not a finite intersection of irreducibles were non-empty, then by Noetherianity there would be an ideal maximal with the property of not being an intersection of irreducible ideals. Such a maximal element must be an intersection of two larger ideals, each of which are finite intersections of irreducibles, giving a contradiction.

Next, we claim that every irreducible ideal is primary. To prove the contrapositive, suppose that Q is not primary, and take $xy \in Q$ with $x \notin Q$, $y \notin \sqrt{Q}$. The ascending chain of ideals

$$(Q : y) \subseteq (Q : y^2) \subseteq (Q : y^3) \subseteq \cdots$$

stabilizes for some n, since R is Noetherian. It will soon be helpful to realize that this means that for any element $f \in R$, $y^{n+1}f \in Q \implies y^n f \in Q$. Using this, we will show that

$$(Q + (y^n)) \cap (Q + (x)) = Q,$$

proving that Q is not irreducible.

The containment $Q \subseteq (Q + (y^n)) \cap (Q + (x))$ is clear. On the other hand, if

$$a \in (Q + (y^n)) \cap (Q + (x)),$$

we can write $a = q + by^n$ for some $q \in Q$, and

$$a \in Q + (x) \implies ay \in Q + (xy) = Q.$$

So

$$by^{n+1} = ay - aq \in Q \implies b \in (Q : y^{n+1}) = (Q : y^n).$$

By definition, this means that $by^n \in Q$, and thus $a = q + by^n \in Q$. This shows that Q is not irreducible, concluding the proof. □

Primary decompositions, even irredundant ones, are not unique.

Example 1.66. Let $R = k[x, y]$, where k is a field, and $I = (x^2, xy)$. We can write

$$I = (x) \cap (x^2, xy, y^2) = (x) \cap (x^2, y).$$

The ideals (x^2, xy, y^2) and (x^2, y) are primary, since each has radical $\mathfrak{m} = (x, y)$, which is maximal, and by Remark 1.56 any ideal whose radical is maximal must be primary. In fact, our ideal I has infinitely many irredundant primary decompositions: given any $n \geqslant 1$,

$$I = (x) \cap (x^2, xy, y^n)$$

is a irredundant primary decomposition. One thing all of these have in common is the radicals of the primary components: they are always (x) and (x, y). Indeed, we saw in Example 1.48 that these are the associated primes of I.

In the previous example, the fact that all our irredundant primary decompositions had primary components always with the same radical was not an accident. Indeed, there are some aspects of primary decompositions that are unique, and this is one of them.

Theorem 1.67 (First uniqueness theorem for primary decompositions)**.** *Suppose I is an ideal in a noetherian ring R. Given any irredundant primary decomposition of I, say*

$$I = Q_1 \cap \cdots \cap Q_t,$$

we have

$$\{\sqrt{Q_1}, \ldots, \sqrt{Q_t}\} = \operatorname{Ass}(R/I).$$

In particular, this set is the same for all irredundant primary decompositions of I.

Proof. For any primary decomposition, irredundant or not, we have

$$\operatorname{Ass}(I) \subseteq \bigcup_i \operatorname{Ass}(Q_i) = \{\sqrt{Q_1}, \ldots, \sqrt{Q_t}\}$$

by Lemma 1.61. We just need to show that in an irredundant decomposition as above, every $P_j := \sqrt{Q_j}$ is indeed an associated prime of I.

So fix j, and let

$$I_j = \bigcap_{i \neq j} Q_i \supseteq I.$$

Since the decomposition is irredundant, the module I_j/I is nonzero, hence by Theorem 1.39 it has an associated prime, say $\mathfrak{a}$. Fix $x_j \in R$ such that $\mathfrak{a}$ is the annihilator of $\overline{x_j}$ in I_j/I. Since

$$Q_j x_j \subseteq Q_j \cdot \bigcap_{i \neq j} Q_i \subseteq Q_1 \cap \cdots \cap Q_n = I,$$

we conclude that Q_j is contained in the annihilator of $\overline{x_j}$, meaning $Q_j \subseteq \mathfrak{a}$. Since P_j is the unique minimal prime of Q_j and $\mathfrak{a}$ is a prime containing Q_j, we must have $P_j \subseteq \mathfrak{a}$. On the other hand, if $r \in \mathfrak{a}$, we have $rx_j \in I \subseteq Q_j$, and since $x_j \notin Q_j$, we must have $r \in \sqrt{Q_j} = P_j$ by the definition of primary ideal. Thus $\mathfrak{a} \subseteq P_j$, so we can now conclude that $\mathfrak{a} = P_j$. This shows that P_j is an associated prime of R/I. □

If we do not assume that R is noetherian, we may or may not have a primary decomposition for a given ideal. It is true that if an ideal I in a general ring has a primary decomposition, then the primes occurring are the same in any irredundant decomposition. However, they are not the associated primes of I in general; rather, they are the primes that occur as radicals of annihilators of elements.

There is also a partial uniqueness result for the actual primary ideals that occur in an irredundant decomposition.

Theorem 1.68 (Second uniqueness theorem for primary decompositions)**.** *If I is an ideal in a noetherian ring R, then the minimal components in any irredundant primary decomposition of I are unique. More precisely, if*

$$I = Q_1 \cap \cdots \cap Q_t$$

is an irredundant primary decomposition, and $\sqrt{Q_i} \in \operatorname{Min}(I)$, then Q_i is given by the formula

$$Q_i = IR_{\sqrt{Q_i}} \cap R,$$

which does not depend on our choice of irredundant decomposition.

Proof. Let Q be a primary ideal, and let P be any prime. The localization Q_P is either:

- the unit ideal, if $Q \not\subseteq P$, or
- a P-primary ideal, if $Q \subseteq P$.

This follows from Theorem 1.45, the fact that the associated primes of Q localize, since $Q \subseteq P$ implies $\sqrt{Q} \subseteq P$, and Q_P will still have a unique associated prime.

Finite intersections commute with localization, so for any prime P,

$$I_P = (Q_1)_P \cap \cdots \cap (Q_t)_P$$

is a primary decomposition, although not necessarily irredundant. Fix a minimal prime $P = P_i$ of I, and let $Q = Q_i$. When we localize at P, all the other components become the unit ideal, since their radicals are not contained in P, and thus $I_P = Q_P$. We can then contract to R to get $I_P \cap R = (Q_i)_{P_i} \cap R = Q_i$, since Q_i is P_i-primary and we can then apply Proposition 1.55 (6). □

We saw in Example 1.66 that the components associated to embedded primes are not necessarily unique. One might be tempted to think that the formula above, $IR_P \cap R$, still gives a P-primary component for I for any associated prime; unfortunately, that is *always* false when P is embedded.

Remark 1.69. If P is an embedded prime of I, we claim that $IR_P \cap R$ is not primary. Let $P_1, \ldots, P_k$ be all the associated primes of I that are contained in P, and let $Q_1, \ldots, Q_k$ be the P_i-primary components and Q be the P-primary component in an irredundant primary decomposition of I. Since $Q_i \subseteq P_i \subseteq P$, by Lemma 1.60 we have $Q_i R_P \cap R = Q_i$. On the other hand, if $\mathfrak{q}$ is another primary component of I but with $\sqrt{\mathfrak{q}} \nsubseteq P$, then $\mathfrak{q}R_P = R_P$, and $\mathfrak{q}R_P \cap R = R$.

Finally, localization commutes with intersections, so we conclude that

$$IR_P \cap R = (Q_1 R_P \cap R) \cap \cdots \cap (Q_k R_P \cap R) = Q_1 \cap \cdots \cap Q_k.$$

This says $IR_P \cap R$ collects *all* the primary components of I corresponding to primes contained in P. If P is an embedded prime of I, there are at least two such components, and thus this ideal is not primary.

This does show, however, that if $\mathrm{mAss}(I)$ denotes the set of maximal elements in $\mathrm{Ass}(I)$, then

$$I = \bigcap_{P \in \mathrm{Ass}(I)} IR_P \cap R = \bigcap_{P \in \mathrm{mAss}(I)} IR_P \cap R,$$

since each $IR_P \cap R$ is the intersection of all the primary components associated to elements in $\mathrm{Ass}(I)$ that are contained in P.

Remark 1.70. Fix an ideal I and suppose that A is a finite set of primes that contains every associated prime of I. By Remark 1.30, $W = R \setminus \bigcup_{P \in A} P$ is a multiplicatively closed set, so we can consider the localization ring $W^{-1}R$. For each associated prime P of I, $R \setminus P \supseteq W$, so if

$$r \in W^{-1}I \cap R \implies sr \in I \text{ for some } s \in W \implies sr \in I \text{ for some } s \notin P \implies r \in IR_P \cap R.$$

Therefore,

$$I \subseteq W^{-1}I \cap R \subseteq \bigcap_{P \in \mathrm{Ass}(I)} IR_P \cap R = I,$$

where the last equality was discussed in Remark 1.69. We conclude that $W^{-1}I \cap R = I$.

It is relatively easy to give a primary decomposition for a radical ideal:

Example 1.71. If R is noetherian, and I is a radical ideal, then we have seen that I coincides with the intersection of its minimal primes, say $I = P_1 \cap \cdots \cap P_t$. This is the *only* primary decomposition of a radical ideal.

For a more concrete example, take the ideal $I = (xy, xz, yz)$ in $k[x, y, z]$. This ideal is radical, so we just need to find its minimal primes. And indeed, one can check that $(xy, xz, yz) = (x, y) \cap (x, z) \cap (y, z)$.

Example 1.72. Let's get back to our motivating example in $\mathbb{Z}[\sqrt{-5}]$, where some elements can be written as products of irreducible elements in more than one way. For example, we saw that

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

In fact, $(6) = (2) \cap (3)$, but while (2) is primary, (3) is not. In fact, (3) has two distinct minimal primes, and the following is a minimal primary decomposition for (6):

$$(6) = (2) \cap (3, 1 + \sqrt{-5}) \cap (3, 1 - \sqrt{-5}).$$

1.6 Computing primary decompositions

> Providing efficient algorithms for primary decomposition of an ideal [...] is [...] still one of the big challenges for computational algebra and computational algebraic geometry.
>
> (Decker, Greuel, and Pfister write in [DGP99])

Computing primary decompositions is a computationally difficult problem. This is true in a formal sense: even if one restricts to ideals monomial in a polynomial ring over a field, the problem of finding a primary decompositions is NP-complete [HS02].

The method `primaryDecomposition` in Macaulay2 computes primary decompositions using several strategies: there are special algorithms for monomial and binomial ideals, which we will discuss later, an algorithm of Shimoyama and Yokoyama [SY96] for ideals in polynomial rings, and an algorithm by Eisenbud, Huneke, and Vasconcelos [EHV92], and a hybrid of the last two. The user can force Macaulay2 to choose a particular strategy using the command `Strategy`. Here's an example from the Macaulay2 documentation:

```
i2 : Q = QQ[a..d];

i3 : I = ideal(a^2*b,a*c^2,b*d,c*d^2);

o3 : Ideal of Q

i4 : primaryDecomposition(I, Strategy => Monomial)
                                                    2              2   2
o4 = {ideal (d, a), ideal (c, b), ideal (b, a, d ), ideal (d, c , a ),
```

```
-----------------------------------------------------------------------
           2   2
ideal (b, d , c )}

o4 : List
```

To compute a primary decomposition of I, we want to isolate the components with a particular radical, which can be done via saturations.

Definition 1.73. Let I and J be ideals in a ring R. The **saturation of I with respect to J** is the ideal

$$(I : J^\infty) := \bigcup_{n \geqslant 1} (I : J^n) = \{r \in R \mid rJ^n \subseteq I \text{ for some } n\}.$$

Given an element $x \in R$, we write $(I : x^\infty)$ instead of $(I : (x)^\infty)$. Some authors drop the parenthesis altogether, and write simply $I : J^\infty$.

We leave the following basic properties of saturations as an exercise.

Exercise 1. Let I, J, and L be ideals in a noetherian ring R.

a) There exists n such that $(I : J^\infty) = (I : J^n)$.

b) If Q is a P-primary ideal, then

$$(Q : J^\infty) = \begin{cases} Q & \text{if } J \nsubseteq P \\ R & \text{if } J \subseteq P \end{cases}.$$

c) $(I \cap J : L^\infty) = (I : L^\infty) \cap (J : L^\infty)$.

d) Given a primary decomposition $I = Q_1 \cap \cdots \cap Q_k$,

$$(I : J^\infty) = \bigcap_{J \nsubseteq \sqrt{Q_i}} Q_i.$$

e) If $\operatorname{Ass}(I) = \operatorname{Min}(I) = \{P_1, \ldots, P_k\}$, then for each i there exists an element $x_i \in R$ such that the P_i-primary component of I is given by $(I : x_i^\infty)$.

Chapter 2

Symbolic powers

Given an ideal I, its n**th power** is the ideal

$$I^n := (f_1 \cdots f_n \mid f_i \in I).$$

By convention, we set $I^0 = R$. While $\sqrt{I^n} = \sqrt{I}$ and the minimal primes of I^n are the same as the minimal primes of R, I^n might have new, exciting embedded primes. This is the beginning of a beautiful friendship.

2.1 What are symbolic powers?

Definition 2.1. Let I be an ideal in a noetherian ring R and fix an integer $n \geqslant 1$. The n**th symbolic power** of I is the ideal

$$I^{(n)} := \bigcap_{P \in \operatorname{Ass}(I)} I^n R_P \cap R.$$

Our main focus will be on symbolic powers of ideals I with no embedded primes. In that case, $\operatorname{Ass}(I) = \operatorname{Min}(I)$, and since $\operatorname{Min}(I^n) = \operatorname{Min}(I)$, the nth symbolic power of I is the ideal

$$I^{(n)} = \bigcap_{P \in \operatorname{Ass}(I)} I^n R_P \cap R = \bigcap_{P \in \operatorname{Min}(I)} I^n R_P \cap R = \bigcap_{P \in \operatorname{Min}(I^n)} I^n R_P \cap R.$$

For each minimal prime P of I^n, $I^n R_P \cap R$ is the P-primary component of I^n. The nth symbolic power of I is thus obtained by computing a primary decomposition for I^n, collecting the minimal components, and discarding the embedded ones.

When I does have embedded primes, the two ideals

$$\bigcap_{P \in \operatorname{Ass}(I)} I^n R_P \cap R \quad \text{and} \quad \bigcap_{P \in \operatorname{Min}(I)} I^n R_P \cap R$$

are necessarily distinct. Both appear in the literature as definitions for symbolic powers, and the ambiguity only arises when one considers ideals with embedded components. While we will briefly discuss the advantages and disadvantages of each definition, our main focus will be the situation where I has no embedded primes and there is no ambiguity to worry about. In fact, even the study of symbolic powers of primes is interesting enough to keep us busy all semester, and so focusing on ideals with no embedded primes is not a big concession.

Lemma 2.2. *Let P be a prime ideal in a noetherian ring R.*

(1) $P^{(n)} = P^n R_P \cap P$.

(2) $P^{(n)} = \{r \in R \mid sr \in P^n \text{ for some } s \notin P\}$.

(3) $P^{(n)}$ *is the unique P-primary component in a primary decomposition of* P^n.

(4) $P^{(n)}$ *is the smallest P-primary ideal containing* P^n.

Moreover, $P^n = P^{(n)}$ *if and only if* P^n *is primary.*

Proof. Prime ideals are primary, and $\operatorname{Ass}(P) = \{P\}$, so (1) is immediate. The characterization in (2) follows from (1) and the definition of R_P. Theorem 1.68 says that $P^n R_P \cap R$ is the unique minimal (P-primary) component in a primary decomposition of P^n, which is (3).

So $P^{(n)}$ is a P-primary ideal containing P^n. To show it is the smallest such ideal, consider any other P-primary ideal Q containing P^n. Since images and preimages preserve containments, $P^n R_P \cap R \subseteq Q R_P \cap R$. Since Q is P-primary, the characterization of primary ideals in Proposition 1.55 says that $Q R_P \cap R = Q$. We conclude that

$$P^{(n)} = P^n R_P \cap R \subseteq Q R_P \cap R = Q,$$

and $P^{(n)}$ is the smallest P-primary ideal containing P^n, which is (4).

The final statement is now immediate from (4). □

The symbolic powers of a prime ideal do not necessarily coincide with its powers.

Example 2.3. Fix $n \geqslant 2$. Let k be a field, $R = k[x, y, z]/(xy - z^n)$, and consider the prime ideal $P = (x, z)$ in R. While $y \notin P$, $xy = z^n \in P^n$, so $x \in P^{(n)}$.

In fact, the symbolic powers of a prime ideal might not coincide with its powers even over a polynomial ring.

Example 2.4. Fix a field k, and let $R = k[x, y, z]$. Consider the ideal P given by

$$P = \left(\underbrace{x^3 - yz}_{f}, \underbrace{y^2 - xz}_{g}, \underbrace{z^2 - x^2 y}_{h} \right).$$

We will show that the ring homomorphism

$$\begin{aligned} \tfrac{k[x,y,z]}{P} &\xrightarrow{\ \pi\ } k[t^3, t^4, t^5] \\ (x, y, z) &\longmapsto (t^3, t^4, t^5) \end{aligned}$$

is an isomorphism. First, note that it is immediately surjective by construction, so we just need to prove it is injective. If we set $\deg(x) = 3, \deg(y) = 4, \deg(z) = 5, \deg(t) = 1$, π is a graded homomorphism of graded rings, whose kernel is homogeneous. Since $[k[t^3, t^4, t^5]]_n$ is a 1-dimensional vector space generated by t^n for all $n \geqslant 3$ (and zero in degrees 1 and 2), it suffices to show that $\dim([\frac{k[x,y,z]}{P}]_n) = 1$ for all $n \leqslant 3$ (and zero in degrees 1 and 2).

Given any monomial in $\frac{k[x,y,z]}{P}$, we can use the relations $y^2 - xz$, $z^2 - x^2y$, and $yz - x^3$ to obtain an equivalent monomial where the sum of the y and z exponents is smaller until we get a monomial of the form x^a, x^ay, or x^az. If $n = 1, 2$, there is no such monomial; if $n \geqslant 3$, there is exactly one, namely,

$$\begin{cases} x^{n/3} & \text{if } n \equiv 0 \mod 3 \\ x^{(n-4)/3}y & \text{if } n \equiv 1 \mod 3 \\ x^{(n-5)/3}y & \text{if } n \equiv 2 \mod 3 \end{cases}$$

This shows that P is the kernel of the map

$$\begin{aligned} k[x, y, z] &\longrightarrow k[t^3, t^4, t^5] \, . \\ (x, y, z) &\longmapsto (t^3, t^4, t^5) \end{aligned}$$

Since $k[t^3, t^4, t^5] \subseteq k[t]$ is a domain, we conclude that P is a prime ideal. In fact, P is a homogeneous ideal with the grading we considered above: our generators f, g, and h are now homogeneous, with $\deg(f) = 9$, $\deg(g) = 8$, and $\deg(h) = 10$. We claim that $P^{(2)} \neq P^2$.

Consider the homogeneous element $fg - h^2 \in (x)$, which has degree 18, and let q be such that $fg = qx$. Since $x \notin P$ and $xq = fg - h^2 \in P^2$, we conclude that $q \in P^{(2)}$. However, since $\deg(x) = 3$ and $\deg(fg) = 18$, q must be a homogeneous element of degree 15, but the smallest degree of any element in P^2 is $2 \times 8 = 16$, so $q \notin P^2$.

The symbolic powers of an ideal do sometimes coincide with its ordinary powers.

Lemma 2.5. *Let k be a field and consider a polynomial ring $R = k[x_1, \ldots, x_d]$. If I is an ideal generated by some of the variables, then $I^{(n)} = I^n$ for all $n \geqslant 1$.*

Proof. Since I is a prime ideal, we want to show that I^n is primary for all n. Without loss of generality, assume $I = (x_1, \ldots, x_t)$ for some $t \leqslant d$. Give R the grading with weights $|x_1| = \cdots = |x_t| = 1$, and $|x_{t+1}| = \cdots = |x_n| = 0$. With this grading, I is a homogeneous ideal, and the nonzero homogeneous elements in I are precisely the homogeneous elements of positive degree. Similarly, the nonzero homogeneous elements in I^n are the homogeneous elements in R of degree at least n. If $g \notin \sqrt{I^n} = I$, then g has a term of degree zero. If $f \notin I$, then f has a term of degree strictly smaller than n. The product fg must then have a term of degree strictly smaller than n, so it is not in I^n. We conclude that I^n is primary. □

Lemma 2.6. *If $\mathfrak{m}$ is a maximal ideal in a noetherian ring R, then $\mathfrak{m}^n = \mathfrak{m}^{(n)}$ for all n.*

Proof. We just need to show that $\mathfrak{m}^n$ is primary. But $\mathfrak{m}$ is the only prime containing $\mathfrak{m}^n$, so we necessarily have $\operatorname{Ass}(\mathfrak{m}^n) \subseteq \{\mathfrak{m}\}$. By Theorem 1.39 Item 3, $\operatorname{Ass}(\mathfrak{m}^n) \neq \varnothing$, so $\operatorname{Ass}(\mathfrak{m}^n) = \{\mathfrak{m}\}$. □

Now we are ready to discuss the general case. When I is an ideal with no embedded primes, the symbolic powers of I are given by

$$I^{(n)} = \bigcap_{P \in \operatorname{Ass}(I)} I^n R_P \cap R = \bigcap_{P \in \operatorname{Min}(I)} I^n R_P \cap R.$$

This is a primary decomposition of $I^{(n)}$: the associated primes of $I^{(n)}$ are precisely the minimal primes of I, and for each $P \in \operatorname{Min}(I)$ the P-primary component of $I^{(n)}$ is given by $I^n R_P \cap R$.

Lemma 2.7. *Let I be an ideal with no embedded primes in a noetherian ring R.*

(1) $I^n = I^{(n)}$ if and only if I^n has no embedded primes.

(2) $\operatorname{Ass}(I^{(n)}) = \operatorname{Ass}(I) = \operatorname{Min}(I) = \operatorname{Min}(I^n)$.

Proof.

(1) Since $\sqrt{I^n} = \sqrt{I}$, the minimal primes of I^n coincide with those of I. Therefore, an irredundant primary decomposition of I^n consists of

$$I^n = I^{(n)} \cap Q_1 \cap \cdots \cap Q_k,$$

where $Q_1, \ldots, Q_k$ are primary components corresponding to embedded primes of I^n. There are no such components precisely when $I^n = I^{(n)}$.

(2) Saying I has no embedded primes is the same as saying that $\operatorname{Ass}(I) = \operatorname{Min}(I)$, and $\operatorname{Min}(I) = \operatorname{Min}(I^n)$ always holds. For each $P \in \operatorname{Ass}(I) = \operatorname{Min}(I) = \operatorname{Min}(I^n)$, $I^n R_P \cap R$ is a P-primary ideal, so

$$\bigcap_{P \in \operatorname{Ass}(I)} I^n R_P \cap R$$

is an intersection of primary ideals with distinct, incomparable radicals. This must then be a primary decomposition of $I^{(n)}$, and the corresponding primes are the associated primes of $I^{(n)}$. □

We can write $I^{(n)}$ more directly as the elements that live in I^n up to multiplication by an element not in any associated prime of I.

Remark 2.8. Let I be an ideal in a noetherian ring R. Setting

$$W := R \setminus \bigcup_{P \in \operatorname{Ass}(I)} P$$

we claim that

$$I^{(n)} = W^{-1} I^n \cap R = \{r \in R \mid sr \in I^n \text{ for some } s \in W\}.$$

If $a \in I^{(n)}$, then $a \in I^n R_P \cap R$ for each $P \in \operatorname{Min}(I)$, so for each such P there exists an element $s \notin P$ with $sa \in I^n$. Therefore, $(I^n : a)$ is not contained in any $P \in \operatorname{Ass}(I)$. There are finitely many such primes, by Theorem 1.44, so by Prime Avoidance

$$(I^n : a) \nsubseteq \bigcup_{P \in \operatorname{Ass}(I)} P.$$

Therefore, there exists $s \in W$ such that $sa \in I^n$. Now assume $s \in W$ and $a \in R$ satisfy $sa \in I^n$. For each $P \in \operatorname{Ass}(I)$, $s \notin P$, so $sa \in I^n$ gives $a \in I^n R_P \cap R$. Therefore, $a \in I^{(n)}$.

Lemma 2.9. *Let I be an ideal in a noetherian ring R.*

(1) For all $n \geqslant 1$, $I^n \subseteq I^{(n)}$.

(2) If I has no embedded primes, then $I^{(1)} = I$.

(3) If R is a domain and I is a nonzero ideal, then $I^a \subseteq I^{(b)}$ implies $a \geqslant b$.

(4) If $a \geqslant b$, then $I^{(a)} \subseteq I^{(b)}$.

(5) For all $a, b \geqslant 1$, $I^{(a)} I^{(b)} \subseteq I^{(a+b)}$.

Proof.

(1) This is a set-theoretic statement: any set is contained in the preimage of its own image by any map. In particular, for all associated primes P of I, $I^n \subseteq I^n R_P \cap R$.

(2) By Theorem 1.68, the minimal primary components of I^n are unique, and the component associated to each $P \in \operatorname{Min}(I^n) = \operatorname{Min}(I) = \operatorname{Ass}(I)$ is given by $IR_P \cap R$. Since all the associated primes of I are minimal,

$$I \quad = \bigcap_{P \in \operatorname{Min}(I)} (IR_P \cap R) = \bigcap_{P \in \operatorname{Ass}(I)} (IR_P \cap R) = I^{(1)}.$$

(3) Suppose $I^a \subseteq I^{(b)}$, and let P be an associated prime of I. We have

$$(I_P)^a = (I^a)_P \subseteq \left(I^{(b)}\right)_P = (I_P)^b.$$

Write $J = I_P$, and note that J is contained in the unique maximal ideal of R_P. If $a < b$, it would follow that $J^a = J^b$, which by NAK implies $J = 0$. Since R is a domain, the localization map is injective, and thus $J = 0$ happens only if $I = 0$.

(4) Since $a \geqslant b$, $I^a \subseteq I^b$, so $I^a R_P \subseteq I^b R_P$ for any prime ideal P. Since taking preimages preserves inclusions, we conclude that $I^a R_P \cap R \subseteq I^b R_P \cap R$, and thus $I^{(a)} \subseteq I^{(b)}$.

(5) Let $P \in \operatorname{Ass}(I)$ and let π be the canonical homomorphism $R \to R_P$. Given $x \in I^{(a)}$ and $y \in I^{(b)}$, $\pi(xy) = \pi(x)\pi(y) \in I^a I^b R_P$. Now notice that $I^a I^b = I^{a+b}$, so $\pi(xy) \in I^{a+b} R_P$, and $xy \in I^{a+b} R_P \cap R$. Since this holds for all $P \in \operatorname{Ass}(I)$, we conclude that $xy \in I^{(a+b)}$. □

Remark 2.10. Let I be a radical ideal with minimal primes $P_1, \ldots, P_s$, so $I = P_1 \cap \cdots \cap P_s$. As we discussed in the proof of Theorem 1.68, $IR_{P_i} = P_i R_{P_i}$. Since localization commutes with powers, we conclude that $I^n R_{P_i} = P_i^n R_{P_i}$, and thus

$$I^{(n)} = P_1^{(n)} \cap \cdots P_s^{(n)}.$$

Example 2.11. Consider the radical ideal $I = (xy, xz, yz) = (x, y) \cap (x, z) \cap (y, z)$. As in Remark 2.10, its symbolic powers are given by

$$I^{(n)} = (x, y)^{(n)} \cap (x, z)^{(n)} \cap (y, z)^{(n)},$$

which by Lemma 2.5 can be simplified to

$$I^{(n)} = (x, y)^n \cap (x, z)^n \cap (y, z)^n.$$

Now $xyz \in I^{(2)}$ but $xyz \notin I^2$, since I^2 is generated by homogeneous elements of degree 2.

Just because $I^{(n)} = I^n$ for some $n > 1$, that does not mean that $I^{(m)} = I^m$ for other values of m. Here is an example by Susan Morey [Mor96].

Example 2.12 (Morey)**.** Let k be a field, $R = k[x_1, x_2, x_3, x_4]$, and consider the matrix

$$M = \begin{pmatrix} 0 & -x_1 & -x_3 & x_2 & -x_1 & x_4 & -x_3 \\ x_1 & 0 & -x_3 & x_2 & x_1 & -x_4 & -x_1 \\ x_3 & x_3 & 0 & 0 & -x_3 & x_1 & x_4 \\ -x_2 & -x_2 & 0 & 0 & -x_4 & x_2 & 0 \\ x_1 & -x_1 & x_3 & x_4 & 0 & -x_3 & x_1 \\ -x_4 & x_4 & -x_1 & -x_2 & x_3 & 0 & x_2 \\ x_3 & x_1 & x_4 & 0 & -x_1 & x_2 & 0 \end{pmatrix}.$$

This a skew-symmetric matrix, meaning that $M_{ij} = -M_{ji}$ for all i, j. The even sized minors of such a matrix turn out to be squares, so we can consider polynomials f such that f^2 is an even-sized minor of M. The ideal generated by the $2t$-sized minors of a skew-symmetric matrix is called the **ideal of** $2t \times 2t$ **pfaffians** of M.

The ideal I of 6×6 pfaffians of M is an example of an ideal that satisfies $I^{(2)} = I^2$ but $I^{(3)} \neq I^3$, which one can check with Macaulay2.

While most of the ideals we will be interested in will be radical, here are some comments on the symbolic powers of a general ideal.

Remark 2.13. Let I be any ideal and consider a prime $P \supseteq I$. By Remark 1.69, $IR_P \cap P$ is the intersection of all the primary components of I that are contained in P. Therefore, if $Q \subseteq P$, $I^n R_Q \cap R \subseteq I^n R_P \cap R$. As in Remark 1.69, $\operatorname{mAss}(I)$ denotes the set of primes in $\operatorname{Ass}(I)$ that are maximal with respect to inclusion. Then

$$I^{(n)} = \bigcap_{P \in \operatorname{Ass}(I)} I^n R_P \cap R = \bigcap_{P \in \operatorname{mAss}(I)} I^n R_P \cap R.$$

Now fix $P \in \operatorname{Ass}(I)$ and let $J = IR_P \cap R$, which is the intersection of the P-primary components of I contained in P — which is by construction a primary decomposition of J. Therefore, $\operatorname{Ass}(J) = \{Q \in \operatorname{Ass}(I) \mid Q \subseteq P\}$. In particular, $JR_P = IR_P$, and since powers commute with localization, $J^n R_P = I^n R_P$ for all n. Therefore, $J^{(n)} = I^n R_P \cap R$, and

$$I^{(n)} = \bigcap_{P \in \operatorname{mAss}(I)} (IR_P \cap R)^{(n)}$$

where $IR_P \cap R$ is the intersection of the primary components of I contained in P.

2.2 Homogeneous ideals

We have already seen a few examples of symbolic powers of homogeneous ideals where we took advantage of being able to look at degrees of homogeneous elements. And indeed, the symbolic powers of a homogeneous ideal are also homogeneous.

Theorem 2.14. *Let R be a noetherian graded ring. If I is a homogeneous ideal, then its symbolic powers $I^{(n)}$ are homogeneous for all $n \geqslant 1$.*

Proof. By Theorem 1.44, the associated primes of I are all homogeneous. Fix a homogeneous prime $P \in \operatorname{Ass}(I)$, and $n \geqslant 1$. The localization R_P is still a graded ring, with grading

$$\deg\left(\frac{r}{w}\right) = \deg(r) - \deg(w),$$

and the canonical map $R \to R_P$ is graded. The image and contraction of a homogeneous ideal by a graded map is homogeneous, so since I is homogeneous, so is $IR_P \cap R$. This shows that all the minimal primary components of I are homogeneous. Similarly, if I^n is homogeneous, then so is $I^n R_P \cap R$. The intersection of homogeneous ideals is homogeneous, and thus $I^{(n)}$ is homogeneous for all n. □

We have seen several examples of homogeneous ideals whose symbolic powers do not coincide with the powers because they have elements in *wrong* degrees. This is a very common phenomenon. In the examples we saw before, we had elements of degrees that were too small.

Definition 2.15. If I is a homogeneous ideal in an $\mathbb{N}$-graded ring R, then

$$\alpha(I) := \min\{\deg(f) \mid 0 \neq f \in I \text{ is a homogeneous element}\}.$$

So $\alpha(I)$ is the smallest degree of a homogeneous generator for I.

Example 2.16. Consider a 3×3 matrix of variables,

$$X = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 \\ x_7 & x_8 & x_9 \end{pmatrix}.$$

Given a field k, we write $R = k[X]$ for the polynomial ring $R = k[x_1, \ldots, x_9]$, and $I_t(X)$ for the ideal in R generated by the t-minors of X. Let $I = I_2(X)$, which is a homogeneous ideal generated in degree 2. It is a nontrivial fact (which we won't prove) that this ideal is in fact prime. We claim $I^{(2)} \neq I^2$, and once more we will use a degree argument. To see this, consider the element $\det(X)$, which we can write for example using cofactor expansion on the first row:

$$\det(X) = x_1 \begin{vmatrix} x_5 & x_6 \\ x_8 & x_9 \end{vmatrix} - x_2 \begin{vmatrix} x_4 & x_6 \\ x_7 & x_9 \end{vmatrix} + x_3 \begin{vmatrix} x_4 & x_5 \\ x_7 & x_8 \end{vmatrix}.$$

This is clearly an element in I, since we wrote it as a linear combination of elements in I. On the other hand, this is *not* an element in I^2, since it has degree 3 and $\alpha(I^2) = 4$. On the other hand, with a few careful computations one can see that

$$x_1 \det(X) = \begin{vmatrix} x_1 & x_3 \\ x_7 & x_9 \end{vmatrix} \begin{vmatrix} x_1 & x_2 \\ x_4 & x_5 \end{vmatrix} - \begin{vmatrix} x_1 & x_2 \\ x_7 & x_8 \end{vmatrix} \begin{vmatrix} x_1 & x_3 \\ x_4 & x_6 \end{vmatrix} \in I^2,$$

and since $x_1 \notin I$, we conclude that $\det(X) \in I^{(2)}$. So we have shown that $I^2 \neq I^{(2)}$.

In Example 2.16, Example 2.4 and Example 2.11, we found a homogeneous element in $I^{(n)}$ of degree smaller than $\alpha(I^n)$. The existence of such elements is not necessary for $I^n \neq I^{(n)}$.

Example 2.17. Let $R = \mathbb{Q}[x, y, z]$, and let P be the defining ideal of the curve parametrized by (t^9, t^{11}, t^{14}). Here are some Macaulay2 computations.

```
i1 : k = QQ;

i2 : a = 9; b = 11; c = 14;

i6 : R = k[x,y,z, Degrees => {a,b,c}];

i7 : P = ker map(QQ[t],R,{t^a,t^b,t^c})

             4    2      3    3   5    3 2
o7 = ideal (x  - y z, x*y  - z , y  - x z )

o7 : Ideal of R

i8 : associatedPrimes(P^2)
              4    2      3    3   5    3 2
o8 = {ideal (x  - y z, x*y  - z , y  - x z ), ideal (x, y, z)}

o8 : List

i9 : symbolic2 = (select(primaryDecomposition(P^2), Q -> radical(Q) == P))_0
             8     4 2     4 2   5 3      5     4 3    2 4   2 6       3 3    6
o9 = ideal (x  - 2x y z + y z , x y  - x*y z - x z  + y z , x y  - 2x*y z  + z ,
     ------------------------------------------------------------------------
      8    7        3 3 2    2 5   4 5    7     7 2    3 2 3
     y  + x y*z - 3x y z  + x z , x y  - y z - x z  + x y z )

o9 : Ideal of R

i10 : degrees symbolic2

o10 = {{72}, {78}, {84}, {88}, {91}}

o10 : List

i11 : degrees (P^2)

o11 = {{72}, {78}, {91}, {84}, {97}, {110}}

o11 : List
```

In line i8 we learned that P^2 has one embedded prime, the homogeneous maximal ideal. This automatically tells us that $P^2 \neq P^{(2)}$. We computed $P^{(2)}$ and called it `symbolic2` by simply taking a primary decomposition of P^2 and selecting the P-primary component. Since both P^2 and $P^{(2)}$ are homogeneous ideals, we then asked Macaulay2 for the degrees of the generators using the command `degrees`, and found two interesting things:

- $\alpha(P^2) = \alpha(P^{(2)})$, despite the fact that $P^2 \neq P^{(2)}$.
- $P^{(2)}$ has a minimal generator of degree 84, while P^2 does not.

We can ask Macaulay2 to help us identify this generator of $P^{(2)}$ of degree 84:

```
i14 : select(flatten entries mingens (symbolic2), f -> degree(f) == {88})
        8    7        3 3 2    2 5
o14 = {y  + x y*z - 3x y z  + x z }

o14 : List
```

We can do even more, and find all the generators of $P^{(2)}$ in our generating set that are not in P^2.

```
i19 : select(flatten entries mingens (symbolic2), f -> f%(P^2) != 0)
        8    7        3 3 2    2 5
o19 = {y  + x y*z - 3x y z  + x z }

o19 : List

i20 : f = oo_0
       8    7        3 3 2    2 5
o20 = y  + x y*z - 3x y z  + x z

o20 : R

i21 : P^2 + ideal(f) == symbolic2

o21 = true
```

This last computation tells us that this element $f = y^8 + x^7yz - 3x^3y^3z^2 + x^2z^5$ of degree 88 satisfies $P^{(2)} = P^2 + (f)$.

2.3 Computing symbolic powers

From what we have seen so far, it appears that to compute the symbolic powers of a given ideal we need only to find a primary decomposition of I^n, and then collec the appropriate components. In practice, that would be a terrible idea: as we briefly discussed in the previous chapter, computing primary decompositions is a computationally difficult problem, and to add to that, the number of calculations involved in computing powers of ideals grows

very fast. One of the problems we will study is how to find effective and practical ways to compute the symbolic powers of an ideal — and most importantly, to avoid computing primary decompositions.

We saw in Exercise 1 that we can compute the minimal primary components of any ideal via saturation, so we can now put the same trick to use to compute symbolic powers. More interestingly, given an ideal I with no embedded primes, we can construct an ideal J such that $I^{(n)} = (I^n : J^\infty)$ for all n. Saturations are computationally simple, so the difficult task is only to find the appropriate ideal to saturate with.

To show that we can compute the symbolic powers of I by saturating with a fixed J, we will use the beautiful and extraordinary fact that the there are only finitely many primes that are associated to some power of I. Unfortunately, we will have to establish a bit more background before we can prove this.

Theorem 2.18 (Ratliff, 1976 [Rat76], Brodmann, 1979 [Bro79])**.** *If I is an ideal in a noetherian ring R, then $\operatorname{Ass}(I^n)$ stabilizes, meaning that there exists N such that $\operatorname{Ass}(I^n)$ is independent of $n \geqslant N$. In particular,*

$$\bigcup_{n \geqslant 1} \operatorname{Ass}(I^n)$$

is finite.

Notation 2.19. We denote the set of all primes that are associated to some power of I by

$$\mathcal{A}(I) := \bigcup_{n \geqslant 1} \operatorname{Ass}(I^n).$$

This will allow us to show that to compute the symbolic powers of an ideal I, we can now take saturations with respect to a fixed ideal; in fact, we can take saturations with respect to a fixed principal ideal. To do that, however, we will need to use prime avoidance.

Exercise 2. Let I be an ideal with no embedded primes in a noetherian ring R. There exists an ideal J, which we can take to be principal, such that $I^{(n)} = (I^n : J^\infty)$ for all $n \geqslant 1$.

The hard part, of course, is constructing this ideal explicitly and in a computationally efficient way.

2.4 Where are we going?

In order to understand symbolic powers better, we will need to first take a short detour to develop a few more fundamental commutative algebra tools. Here are some of the main questions that will motivate our study:

Computing symbolic powers

As we saw in the previous section, we need only to find an appropriate element x such that $I^{(n)} = (I^n : J^\infty)$. We have discussed how to find this element in theory, but our description

appears to require knowledge of all the associated primes of all the powers of I. This is of course unreasonable, and our goal is to find more effective ways to find such an x.

We will also discuss how to find symbolic powers via other methods for some special classes of ideals. To do this, we will use all sorts of different tools. For example, we will discuss how to apply combinatorics to study the symbolic powers of monomial ideals.

Equality

Computing symbolic powers would be an easy problem if $I^{(n)} = I^n$. So when does this hold? What are some sufficient or necessary conditions for this to hold for some fixed n, or for all n? Can we test the equality $I^{(n)} = I^n$ for all n by doing only finitely many tests?

Minimal degrees

When I is a homogeneous ideal, $I^{(n)}$ is also homogeneous, but its elements may have unexpected degrees. We have briefly discussed some of the behavior we may find, but we would like to explore this further. Will keep a special eye towards lower bounds on $\alpha(I^{(n)})$, since $n\alpha(I) = \alpha(I^n)$ is the obvious upper bound.

Finite generation of symbolic Rees algebras

In Lemma 2.9 we showed that $I^{(a)}I^{(b)} \subseteq I^{(a+b)}$. So as we compute higher and higher symbolic powers of I, we can think of all the elements in

$$\sum_{a_1+\cdots+a_{n-1}=n} I^{a_1} \cdots \left(I^{(n-1)}\right)^{a_{n-1}} \subseteq I^{(n)}$$

as *expected*, and any other element in $I^{(n)}$ as *unexpected*. Roughly speaking, we want to understand whether we will see unexpected elements in $I^{(n)}$ for arbitrarily large n, or whether there is a finite set of symbolic powers which describe all the remaining ones. We will make this problem precise when we study the symbolic Rees algebra of I, which is a graded algebra we construct from the symbolic powers of I. In a surprising twist, these algebras will sometimes be NOT noetherian.

Comparing powers and symbolic powers of ideals

While the symbolic and ordinary powers of an ideal are not necessarily equal, they are of course related. How different are I^n and $I^{(n)}$, really? And how can we formalize this question? One way is of course by studying $\alpha(I^{(n)})$ and comparing it to $\alpha(I^n)$, but there are other ways to formalize this comparison. One in particular we will discuss is known as the Containment Problem, which is the question of when $I^{(a)} \subseteq I^b$. Another way we can formalize this question is to ask whether $I^{(n+1)}$ contains any minimal generator of $I^{(n)}$, which is roughly speaking the content of an open problem known as the Eisenbud-Mazur conjecture.

A geometric perspective

Over a polynomial ring over a perfect field, there is a geometric interpretation for the symbolic powers of a radical ideal. We will discuss this, and take it in part as a motivation to study symbolic powers.

But before we do any of this, it's time for a short detour through some classical commutative algebra topics that algebraist should keep in their back pocket.

Chapter 3

Sharpening our tools

3.1 Dimension and height

Definition 3.1. A **chain of prime ideals**

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$$

has **length** n. We say a chain of primes is **saturated** if for each i there is no prime $\mathfrak{q}$ with $\mathfrak{p}_i \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}_{i+1}$. The **Krull dimension** of a ring R is the supremum of the lengths of chains of primes in R, and we denote it by $\dim(R)$. The **height** of a prime $\mathfrak{p}$ is the supremum of the lengths of chains of primes in R that end in $\mathfrak{p}$, i.e., with $\mathfrak{p} = \mathfrak{p}_n$ above, and we denote it by $\mathrm{ht}(\mathfrak{p})$. The **height** of an ideal I is given by

$$\mathrm{ht}(I) := \inf \{\mathrm{ht}(\mathfrak{p}) \mid \mathfrak{p} \in \mathrm{Min}(I)\}$$

Macaulay2. We can compute the dimension of a ring using `dim`. To compute the height of an ideal I, we use the method `codim`.

Definition 3.2. The **dimension** of an R-module M is defined as $\dim(R/\operatorname{ann}_R(M))$.

Note that if M is finitely generated, $\dim(M)$ is the same as the supremum of the lengths of chains of primes in $\mathrm{Supp}_R(M)$.

Remark 3.3.

1) If I is an ideal, then $\dim(R/I)$ is the supremum of the lengths of chains of primes in R

$$\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_n$$

with each $\mathfrak{q}_i \in V(I)$.

2) If W is a multiplicative set, then $\dim(W^{-1}R) \leqslant \dim(R)$.

3) If $\mathfrak{p}$ is prime, then $\dim(R_\mathfrak{p}) = \mathrm{ht}(\mathfrak{p})$.

4) If $\mathfrak{q} \supseteq \mathfrak{p}$ are primes, then $\dim(R_\mathfrak{q}/\mathfrak{p}R_\mathfrak{q})$ is the supremum of the lengths of all chains of primes in R of the form

$$\mathfrak{p} = \mathfrak{a}_0 \subsetneq \mathfrak{a}_1 \subsetneq \cdots \subsetneq \mathfrak{a}_n = \mathfrak{q}.$$

5) $\dim(R) = \sup\{\mathrm{ht}(\mathfrak{m}) \mid \mathfrak{m} \in \mathrm{mSpec}(R)\}$.

6) $\dim(R) = \sup\{\dim(R/\mathfrak{p}) \mid \mathfrak{p} \in \mathrm{Min}(R)\}$.

7) If I is an ideal, $\dim(R/I) + \mathrm{ht}(I) \leqslant \dim(R)$.

8) The ideal (0) has height 0.

9) A prime ideal has height zero if and only if it is a minimal prime of R.

We will need a few theorems before we compute the height and dimension of many examples, but we can handle a few basic cases.

Example 3.4.

a) The dimension of a field is zero.

b) A ring is zero-dimensional if and only if every minimal prime is maximal.

c) The ring of integers $\mathbb{Z}$ has dimension 1: there is one minimal prime (0) and every other prime is maximal. More generally, any principal ideal domain has dimension 1.

d) In a UFD, we claim that I is a prime of height 1 if and only if $I = (f)$ with f prime element.

   To see this, note that if $I = (f)$ with f irreducible, and $0 \subsetneq \mathfrak{p} \subseteq I$, then $\mathfrak{p}$ contains some nonzero multiple of f, say af^n with a and f coprime. Since $a \notin I$, $a \notin \mathfrak{p}$, so we must have $f \in \mathfrak{p}$, so $\mathfrak{p} = (f)$. Thus, I has height one. On the other hand, if I is a prime of height one, we claim I contains an irreducible element. Indeed, I is nonzero, so it contains some $f \neq 0$, and primeness implies one of the prime factors of f is contained in I. Thus, any nonzero prime contains a prime ideal of the form (f), so a height one prime must be of this form.

e) If k is a field, then $\dim(k[x_1, \ldots, x_d]) \geqslant d$, since there is a saturated chain of primes $(0) \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \cdots \subsetneq (x_1, \ldots, x_d)$.

Definition 3.5. A ring is **catenary** if for every pair of primes $\mathfrak{q} \supseteq \mathfrak{p}$ in R, every saturated chain of primes

$$\mathfrak{p} = P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n = \mathfrak{q}$$

has the same length. A ring is **equidimensional** if every maximal ideal has the same finite height and $\dim(R/P)$ is the same finite number for every minimal prime P.

Here are some examples of what can go wrong.

Example 3.6. We can find the minimal primes of the ring

$$R = \frac{k[x, y, z]}{(xy, xz)}$$

by computing $\mathrm{Min}((xy, xz))$ in $k[x, y, z]$. As we saw in Example 1.12, the primes (x) and (y, z) are incomparable, and $(x) \cap (y, z) = (xy, xz)$, so $\mathrm{Min}(R) = \{(x), (y, z)\}$. We claim that

the height of $(x-1,y,z)$ in R is one: it contains the minimal prime (y,z), and any saturated chain from (y,z) to $(x-1,y,z)$ corresponds to a saturated chain from (0) to $(x-1)$ in $k[x]$, which must have length 1 since this is a PID. The height of $(x,y-1,z)$ is at least 2, as witnessed by the chain $(x) \subseteq (x,y-1) \subseteq (x,y-1,z)$. So R is not equidimensional. One can also show that the minimal primes of (xy,xz) in $k[x,y,z]$ have different heights: the prime (x) has height 1, which (y,z) has height at least 2, since $(0) \subsetneq (y) \subsetneq (y,z)$. In fact, we will soon see that any ideal generated by 2 elements must have height at most 2, and thus (y,z) has height exactly 2.

While the previous example is not a domain, even domains may fail to be equidimensional.

Example 3.7. The ring $\mathbb{Z}_{(2)}[x]$ is a domain that is not equidimensional. On the one hand, the maximal ideal $(2,x)$ has height at least two, which we see from the chain

$$(0) \subsetneq (x) \subseteq (x,2).$$

On the other hand, the ideal $(2x-1)$ has height 1, and it is maximal since the quotient is $\mathbb{Q}$.

Remark 3.8.

a) If R is a finite dimensional domain, and $f \neq 0$, then $\dim(R/(f)) < \dim(R)$.

b) If R is equidimensional, then $\dim(R/(f)) < \dim(R)$ if and only if $f \notin \bigcup_{\mathfrak{p} \in \operatorname{Min}(R)} \mathfrak{p}$.

c) In general, $\dim(R/(f)) < \dim(R)$ if and only if $f \notin \bigcup_{\substack{\mathfrak{p} \in \operatorname{Min}(R) \\ \dim(R/\mathfrak{p}) = \dim(R)}} \mathfrak{p}$.

d) $f \notin \bigcup_{\mathfrak{p} \in \operatorname{Min}(R)} \mathfrak{p}$ if and only if $\dim(R/(\mathfrak{p}+(f))) < \dim(R/\mathfrak{p})$ for all $\mathfrak{p} \in \operatorname{Min}(R)$.

Krull's Height Theorem, which we will now prove, gives us the most elementary and important connection between height and number of generators. This is also an excellent example of a theorem in elementary commutative algebra that we can prove using symbolic powers.

Theorem 3.9 (Krull's Principal Ideal theorem)**.** *Let R be a Noetherian ring, and $f \in R$. Then, every minimal prime of (f) has height at most one.*

Note that this is stronger than the statement that the height of (f) is at most one: that would only mean that some minimal prime of (f) has height at most one.

Proof. Suppose the theorem is false, so that there is some ring R, a prime $\mathfrak{p}$, and an element f such that $\mathfrak{p}$ is minimal over (f) and $\operatorname{ht}(\mathfrak{p}) > 1$. If we localize at $\mathfrak{p}$ and then mod out by an appropriate minimal prime, we obtain a Noetherian local domain $(R,\mathfrak{m})$ of dimension at least two in which $\mathfrak{m}$ is the unique minimal prime of (f), so let's work over that Noetherian local domain $(R,\mathfrak{m})$. Note that $\overline{R} = R/(f)$ is zero-dimensional, since $\mathfrak{m}$ is the only minimal prime over (f). Back in R, let $\mathfrak{q}$ be a prime strictly in between (0) and $\mathfrak{m}$, and notice that we necessarily have $f \notin \mathfrak{q}$.

Consider the symbolic powers $\mathfrak{q}^{(n)}$ of $\mathfrak{q}$. We will show that these stabilize in R. Since $\overline{R} = R/(f)$ is Artinian, the descending chain of ideals

$$\mathfrak{q}\overline{R} \supseteq \mathfrak{q}^{(2)}\overline{R} \supseteq \mathfrak{q}^{(3)}\overline{R} \supseteq \cdots$$

stabilizes. We then have some n such that $\mathfrak{q}^{(n)}\overline{R} = \mathfrak{q}^{(m)}\overline{R}$ for all $m \geqslant n$, and in particular, $\mathfrak{q}^{(n)}\overline{R} = \mathfrak{q}^{(n+1)}\overline{R}$. Pulling back to R, we get $\mathfrak{q}^{(n)} \subseteq \mathfrak{q}^{(n+1)} + (f)$. Then any element $a \in \mathfrak{q}^{(n)}$ can be written as $a = b + fr$, where $b \in \mathfrak{q}^{(n+1)} \subseteq \mathfrak{q}^{(n)}$ and $r \in R$. Notice that this implies that $fr \in \mathfrak{q}^{(n)}$. Since $f \notin \mathfrak{q}$, we must have $r \in \mathfrak{q}^{(n)}$. This yields $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)} + f\mathfrak{q}^{(n)}$. Thus, $\mathfrak{q}^{(n)}/\mathfrak{q}^{(n+1)} = f(\mathfrak{q}^{(n)}/\mathfrak{q}^{(n+1)})$, so $\mathfrak{q}^{(n)}/\mathfrak{q}^{(n+1)} = \mathfrak{m}(\mathfrak{q}^{(n)}/\mathfrak{q}^{(n+1)})$. By NAK, $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)}$ in R. Similarly, we obtain $\mathfrak{q}^{(n)} = \mathfrak{q}^{(m)}$ for all $m \geqslant n$.

Now, if $a \in \mathfrak{q}$ is nonzero, we have $a^n \in \mathfrak{q}^n \subseteq \mathfrak{q}^{(n)} = \mathfrak{q}^{(m)}$ for all m, so

$$\bigcap_{m \geqslant 1} \mathfrak{q}^{(m)} = \bigcap_{m \geqslant n} \mathfrak{q}^{(m)} = \mathfrak{q}^{(n)}.$$

Notice that $\mathfrak{q}^n \neq 0$ because R is a domain, and so $\mathfrak{q}^{(n)} \supseteq \mathfrak{q}^n$ is also nonzero. So

$$\bigcap_{m \geqslant 1} \mathfrak{q}^{(m)} = \mathfrak{q}^{(n)} \neq 0.$$

On the other hand, $\mathfrak{q}^{(m)} = \mathfrak{q}^m R_{\mathfrak{q}} \cap R$ for all m, and

$$\bigcap_{m \geqslant 1} \mathfrak{q}^{(m)} R_{\mathfrak{q}} \subseteq \bigcap_{m \geqslant 1} \mathfrak{q}^m R_{\mathfrak{q}} = \bigcap_{m \geqslant 1} (\mathfrak{q}R_{\mathfrak{q}})^m = 0$$

by Krull's Intersection theorem. Since R is a domain, the contraction of (0) in $R_{\mathfrak{q}}$ back in R is (0). This is the contradiction we seek. So no such $\mathfrak{q}$ exists, so that R has dimension 1, and in the original ring, all the minimal primes over f must have height at most 1. □

To generalize this to ideals generated by n elements, it is not so straightforward to run an induction. We will need a lemma that allows us to control the chains of primes we get.

Lemma 3.10. *Let R be Noetherian, $\mathfrak{p} \subsetneq \mathfrak{q} \subsetneq \mathfrak{a}$ be primes, and $f \in \mathfrak{a}$. Then there is some $\mathfrak{q}'$ with $\mathfrak{p} \subsetneq \mathfrak{q}' \subsetneq \mathfrak{a}$ and $f \in \mathfrak{q}'$.*

Proof. If $f \in \mathfrak{p}$, there is nothing to prove, since we can simply take $\mathfrak{q}' = \mathfrak{q}$. Suppose $f \notin \mathfrak{p}$. After we quotient out by $\mathfrak{p}$ and localize at $\mathfrak{a}$, we may assume that $\mathfrak{a}$ is the maximal ideal. We want to find a nonzero prime $\mathfrak{q}' \subsetneq \mathfrak{a}$. Our assumption implies that $f \neq 0$, and then by Theorem 3.9, minimal primes of (f) have height one, hence are not $\mathfrak{a}$ nor $\mathfrak{p}$. We can take $\mathfrak{q}'$ to be one of the minimal primes of f. □

Theorem 3.11 (Krull's Height Theorem)**.** *Let R be a Noetherian ring. If I is an ideal generated by n elements, then every minimal prime of I has height at most n.*

Proof. By induction on n. The case $n = 1$ is the Principal Ideal Theorem.

Let $I = (f_1, \ldots, f_n)$ be an ideal, $\mathfrak{p}$ a minimal prime of I, and $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_h = \mathfrak{p}$ be a saturated chain of length h ending at $\mathfrak{p}$. If $f_1 \in \mathfrak{p}_1$, then we can apply the induction hypothesis to the ring $\overline{R} = R/((f_1) + \mathfrak{p}_0)$ and the ideal $(f_2, \ldots, f_n)\overline{R}$. Then by induction

hypothesis, the chain $\mathfrak{p}_1\overline{R} \subsetneq \cdots \subsetneq \mathfrak{p}_h\overline{R}$ has length at most $n-1$, so $h-1 \leqslant n-1$ and $\mathfrak{p}$ has height at most n.

If $f_1 \notin \mathfrak{p}_1$, we use the previous lemma to replace our given chain with a chain of the same length but such that $f_1 \in \mathfrak{p}_1$. To do this, note that $f_1 \in \mathfrak{p}_i$ for some i; after all, $f_1 \in I \subseteq \mathfrak{p}$. So in the given chain, suppose that $f_1 \in \mathfrak{p}_{i+1}$ but $f_1 \notin \mathfrak{p}_i$. If $i > 0$, apply the previous lemma with $\mathfrak{a} = \mathfrak{p}_{i+1}$, $\mathfrak{q} = \mathfrak{p}_i$, and $\mathfrak{p} = \mathfrak{p}_{i-1}$ to find $\mathfrak{q}_i$ such that $f_1 \in \mathfrak{q}_i$. Replace the chain with

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{i-1} \subsetneq \mathfrak{q}_i \subsetneq \mathfrak{p}_i \subsetneq \cdots \subsetneq \mathfrak{p}_h = \mathfrak{p}.$$

Repeat until $f_1 \in \mathfrak{p}_1$. □

The bound given by Krull's Height Theorem is sharp:

Example 3.12. Any ideal generated by n variables in a polynomial ring has height n. The ideal $(u^3 - xyz, x^2 + 2xz - 6y^5, vx + 7vy)$ in $k[u, v, w, x, y, z]$ has height 3.

Definition 3.13. An ideal of height n generated by n elements is a **complete intersection**.

Here are some other examples.

Example 3.14.

a) As we saw in Example 3.6, the ideal (xy, xz) in $k[x, y, z]$ has minimal primes of heights 1 and 2. Its height is 1, though its minimal number of generators is 2.

b) It is possible to have associated primes of height greater than the number of generators. For a cheap example, in $R = k[x, y]/(x^2, xy)$, the ideal generated by zero elements (the zero ideal) has an associated prime of height two, namely (x, y).

c) The same phenomenon can happen even in a nice polynomial ring. For example, consider the ideal $I = (x^3, y^3, x^2u + xyv + y^2w)$ in $R = k[u, v, w, x, y]$. The element $x^2y^2 \notin I$ has $(u, v, w, x, y) = (I : x^2y^2)$, so I has an associated prime of height 5.

d) Noetherianity is necessary. Let $R = k[x, xy, xy^2, \dots] \subseteq k[x, y]$. For all $a \geqslant 1$, $xy^a \notin (x)$, since $y^a \notin R$, but $(xy^a)^2 = x \cdot xy^{2a} \in (x)$. Then (x) is not prime, and $\mathfrak{m} = (x, xy, xy^2, \dots) \subseteq \sqrt{(x)}$. Since $\mathfrak{m}$ is a maximal ideal, we have equality, so $\operatorname{Min}(x) = \{\mathfrak{m}\}$. However, $\mathfrak{p} = (xy, xy^2, xy^3, \dots) = (y)k[x, y] \cap R$ is prime, and the chain $(0) \subsetneq \mathfrak{p} \subsetneq \mathfrak{m}$ shows that $\operatorname{ht}(\mathfrak{m}) > 1$.

Corollary 3.15. *Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring. Then*

$$\dim(R) \leqslant \mu(\mathfrak{m}).$$

In particular, a Noetherian local ring has finite dimension.

Proof. The dimension of a local ring is the height of its unique maximal ideal, so this is just Krull's Height Theorem applied to $\mathfrak{m}$. If R is noetherian, then $\mu(\mathfrak{m})$ is finite, so $\dim(R)$ must also be finite. □

Definition 3.16. The **embedding dimension** of a local ring $(R, \mathfrak{m})$ is the minimal number of generators of $\mathfrak{m}$, $\mu(\mathfrak{m})$. We write $\operatorname{embdim}(R) := \mu(\mathfrak{m})$ for the embedding dimension of R.

Macaulay2. The minimal number of generators of an ideal or module can be computed via the method `numgens`. We can also find a particular minimal generating set with `mingens`. Unfortunately, these computations are not reliable if the ideal is not homogeneous.

So Corollary 3.15 can be restated as $\dim(R) \leqslant \operatorname{embdim}(R)$. Rings whose dimension and embedding dimension agree are very nicely behaved.

Definition 3.17. A Noetherian local ring $(R, \mathfrak{m})$ is **regular** if $\dim(R) = \operatorname{embdim}(R)$.

Corollary 3.18. *Let k be a field. The power series ring $R = k[\![x_1, \ldots, x_d]\!]$ is a regular local ring. Then $\dim(R) = d$ and R is a regular local ring.*

Proof. Let $\mathfrak{m} = (x_1, \ldots, x_d)$. The images of $x_1, \ldots, x_d$ in $\mathfrak{m}/\mathfrak{m}^2$ are linearly independent, so $\mu(\mathfrak{m}) = d$. To show that R is regular, we need to show that $\dim(R) = d$. The strict chain of primes

$$(0) \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \cdots \subsetneq (x_1, \ldots, x_d)$$

shows that $\dim(R) \geqslant d$. By Corollary 3.15, $\dim(R) = d$. □

But before we can say more about regular rings, we will need to discuss regular sequences. We record here a few results one would cover in a first course in commutative algebra that we will not prove, but that we will want to use later.

Theorem 3.19. *If a domain R is a finitely generated algebra over a field k, or a quotient of a power series ring over a field, then all the maximal ideals of R have the same finite height. Moreover, $\dim(k[x_1, \ldots, x_d]) = d$.*

Theorem 3.20. *Let R be a finitely generated algebra or a quotient of a power series ring over a field.*

1) R is catenary.

If additionally R is a domain, then

2) R is equidimensional, and

2) $\operatorname{ht}(I) = \dim(R) - \dim(R/I)$ for all ideals I.

Definition 3.21. Let $K \subseteq L$ be an extension of fields. A **transcendence basis** for L over K is a maximal algebraically independent subset of L. The **transcendence degree** of a field extension L over K is the common size of any transcendence basis for the extension.

Definition 3.22. For a prime P in a ring R, we denote the residue field of R_P by $\kappa(P)$. Equivalently, $\kappa(P)$ is the field of fractions of R/P.

Theorem 3.23 (Dimension inequality)**.** *Let $R \subseteq S$ be an inclusion of domains with R noetherian. Let $\mathfrak{q} \in \operatorname{Spec}(S)$ and $\mathfrak{p} = \mathfrak{q} \cap R \in \operatorname{Spec}(R)$. Then*

$$\operatorname{height}(\mathfrak{q}) + \operatorname{trdeg}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})) \leqslant \operatorname{height}(\mathfrak{p}) + \operatorname{trdeg}(\operatorname{frac}(S)/\operatorname{frac}(R)).$$

3.2 The Koszul complex

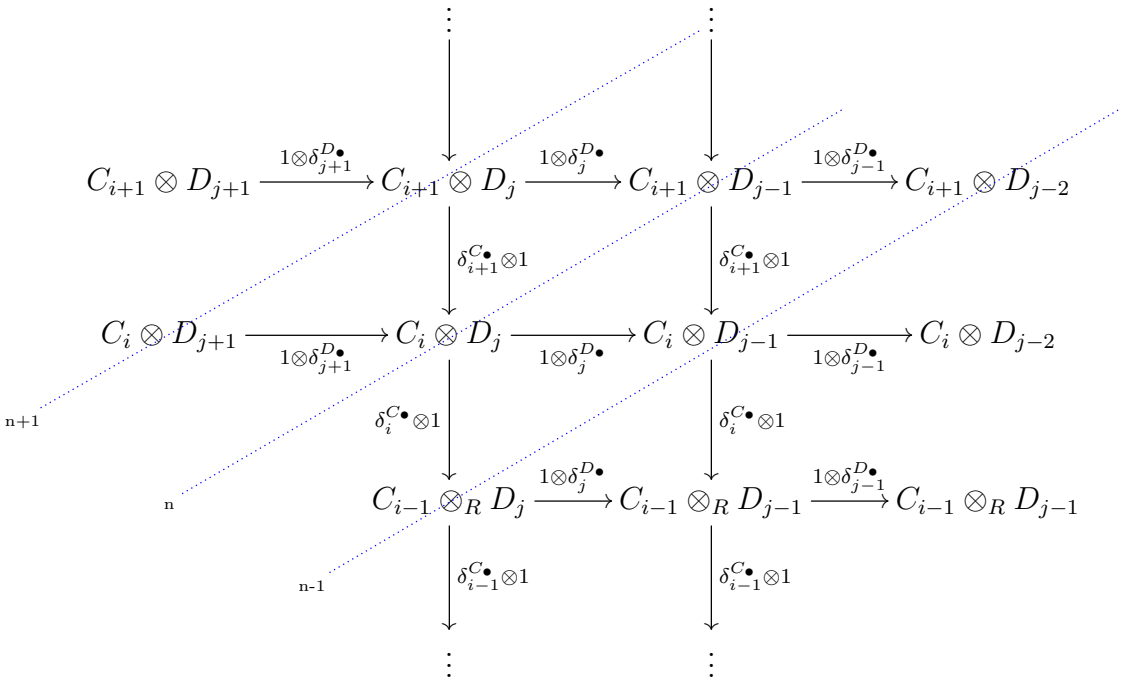
The Koszul complex is arguably the most important complex in commutative algebra (and beyond). It appears everywhere, and it is a very powerful yet elementary tool any homological algebraist needs in their toolbox. Every sequence of elements $x_1, \dots, x_n$ in any ring R gives rise to a Koszul complex.

Definition 3.24. The tensor product of two complexes of R-modules $C_\bullet$ and $D_\bullet$ is the complex $C_\bullet \otimes_R D_\bullet$ with

$$(C_\bullet \otimes_R D_\bullet)_n = \bigoplus_{i+j=n} C_i \otimes_R D_j,$$

and with differential δ_n defined on simple tensors $x \otimes y \in C_i \otimes_R D_j$ by

$$\delta_n(x \otimes y) = \delta_i^{C_\bullet}(x) \otimes y + (-1)^i x \otimes \delta_i^{D_\bullet}(y).$$



Definition 3.25. The **Koszul complex** on $r \in R$ is the complex

$$K(r) := \; 0 \longrightarrow R \xrightarrow{r} \underset{0}{R} \longrightarrow 0.$$

More generally, the **Koszul complex** on the R-module M with respect to $r \in R$ is

$$K(r; M) = K(r) \otimes_R M = \; 0 \longrightarrow M \xrightarrow{r} M \longrightarrow 0.$$

Finally, given $x_1, \dots, x_n \in R$, the **Koszul complex** on M with respect to $x_1, \dots, x_n$ is the complex $K(x_1, \dots, x_n)$ defined inductively as

$$K(x_1, \dots, x_n; M) = K(x_1, \dots, x_{n-1}; M) \otimes_R K(x_n).$$

You will find different sign conventions for the Koszul complex in the literature, but at the end of the day they all lead to isomorphic complexes.

Example 3.26. The Koszul complex on $f, g \in R$ is given by

$$K_\bullet(f,g) \quad = \quad \begin{array}{ccccccc} & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & R & \xrightarrow{-g} & R & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f} & & \\ 0 & \longrightarrow & R & \xrightarrow[g]{} & R & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & \end{array} \quad = \quad 0 \longrightarrow R \xrightarrow{\binom{-g}{f}} R^2 \xrightarrow{(f \quad g)} R \longrightarrow 0$$

Example 3.27. $K_\bullet(f,g,h) = \; 0 \longrightarrow R \xrightarrow{\begin{pmatrix} f \\ -g \\ h \end{pmatrix}} R^3 \xrightarrow{\begin{pmatrix} 0 & -h & -g \\ -h & 0 & f \\ g & f & 0 \end{pmatrix}} R^3 \xrightarrow{\begin{pmatrix} f & g & h \end{pmatrix}} R \longrightarrow 0\,.$

Remark 3.28. Easy induction arguments show that when $\underline{f} = f_1, \ldots, f_n$:

- $K_i(\underline{f}) \cong R^{\binom{n}{i}}$, with a basis naturally indexed by the subsets of $I \subseteq [n]$ with i elements; we write Re_I for the corresponding free summand.
- The component of the map $K_i(\underline{f}) \to K_{i-1}(\underline{f})$ from $Re_I \to Re_J$ is zero if $J \not\subseteq I$, and is $\pm f_i$ if $I = J \cup \{i\}$.

Definition 3.29. If M is an R-module and $\underline{f} = f_1, \ldots, f_n$, then

$$K_\bullet(\underline{f}; M) := K_\bullet(\underline{f}) \otimes M \text{ and } K^\bullet(\underline{f}; M) := \mathrm{Hom}_R(K_\bullet(\underline{f}), M).$$

Another easy induction shows that $K_\bullet(\underline{f}; M) \cong K^{n-\bullet}(\underline{f}; M)$.

The Koszul complex has more structure than simply being a complex: it is an example of a differentially graded algebra, or DG algebra for short, meaning it has an algebra structure on it as well. We will briefly describe how to construct the Koszul complex in such a way, but emphasize that this is only the beginning of a beautiful story about DG algebras.

In a rare moment on non-commutativity, we will need to consider exterior algebras. The **exterior algebra** $\bigwedge M$ on an R-module M is obtained by taking the the free R-algebra $R \oplus M \oplus (M \otimes M) \oplus (M \otimes M \otimes M) \oplus \cdots$ modulo the relations $x \otimes y = -y \otimes x$ and $x \otimes x = 0$ for all $x, y \in N$. We again denote the product on $\bigwedge M$ by $a \wedge b$, and see $\bigwedge M$ as a graded algebra where the homogeneous elements in degree d are those in the image of $N^{\otimes n}$. This is a **skew commutative** algebra, since

$$a \wedge b = (-1)^{\deg(a)\deg(b)} b \wedge a$$

for any homogeneous elements a and b. We denote the homogeneous elements of degree n by $\bigwedge^n M$. Note also that this construction is functorial: a map $M \xrightarrow{f} N$ of R-modules induces a map $\bigwedge M \xrightarrow{\wedge f} \bigwedge N$ given by $m_1 \wedge \cdots \wedge m_s \mapsto f(m_1) \wedge \cdots \wedge f(m_s)$.

We will use this construction in the case of free modules. When $M = R^n$ with basis $e_1, \ldots, e_n$, $\wedge^k M \cong R^{\binom{n}{k}}$, with basis $e_{i_1} \wedge \cdots \wedge e_{i_s}$ ranging over $i_1 < i_2 < \cdots < i_s$, $s = \binom{n}{k}$.

Definition 3.30. Let $x_1, \ldots, x_n$ be elements in R. The **Koszul complex** on $x_1, \ldots, x_n$ is the complex

$$K(x_1, \ldots, x_n) := \; 0 \longrightarrow \bigwedge^n R^n \longrightarrow \bigwedge^{n-1} R^n \longrightarrow \cdots \longrightarrow \bigwedge^1 R^n \longrightarrow R \longrightarrow 0$$

with differential given by

$$d(e_{i_1} \wedge \cdots \wedge e_{i_s}) = \sum_{1 \leqslant p \leqslant s} (-1)^{p+1} x_{i_p} e_{i_1} \wedge \cdots \wedge \widehat{e_{i_p}} \wedge \cdots \wedge e_{i_s}.$$

More generally, given an R-module M, the Koszul complex on M with respect to $x_1, \ldots, x_n$ is $K(x_1, \ldots, x_n; M) := K(x_1, \ldots, x_n) \otimes_R M$.

Exercise 3. Show that d as defined above is indeed a differential, meaning $d^2 = 0$.

Exercise 4. Check that our two definitions of the Koszul complex coincide.

Example 3.31. Let's compute the Koszul complex on 2 elements x_1, x_2 via this second definition. The complex looks like

$$K_\bullet(x_1, x_2) := \; 0 \longrightarrow \bigwedge^2 R^2 \longrightarrow \bigwedge^1 R^2 \longrightarrow R \longrightarrow 0 \; = \; 0 \longrightarrow R^1 \longrightarrow R^2 \longrightarrow R \longrightarrow 0\,.$$

The differential in degree 1 is given by

$$d(e_1) = x_1 \text{ and } d(e_2) = x_2$$

while the differential in degree 2 is

$$d(e_1 \wedge e_2) = x_1 e_2 - x_2 e_1,$$

so the Koszul complex is

$$K_\bullet(x_1, x_2) = \; 0 \longrightarrow R \xrightarrow{\binom{-x_2}{x_1}} R^2 \xrightarrow{(x_1 \quad x_2)} R \longrightarrow 0\,.$$

Remark 3.32. The Koszul complex $K(\underline{x}; M)$ looks like

$$0 \longrightarrow M \longrightarrow M^n \longrightarrow \cdots \longrightarrow M^n \longrightarrow M \longrightarrow 0$$

where the map in degree n is a column with entries $\pm x_i$, which after reordering looks like

$$\begin{pmatrix} x_1 \\ -x_2 \\ x_3 \\ \vdots \\ (-1)^{n+1} x_n \end{pmatrix}$$

and the map in degree 0 is

$$\begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_n \end{pmatrix}.$$

The homology of the Koszul complex has nice properties.

Definition 3.33. Let M be an R-module and $x_1, \ldots, x_n \in R$. The i**th Koszul homology** module of M with respect to $x_1, \ldots, x_d$ is

$$\mathrm{H}_i(x_1, \ldots, x_d; M) := \mathrm{H}_i(K(x_1, \ldots, x_d; M)).$$

Example 3.34. In $R = k[x, y]$,

$$\mathrm{H}_1(x, y; R) = \text{ homology of } R \xrightarrow{\begin{pmatrix} -y \\ x \end{pmatrix}} R^2 \xrightarrow{\begin{pmatrix} x \\ y \end{pmatrix}} R = 0.$$

Example 3.35. In $R = k[x, y, u, v]/(xu - yv)$,

$$\mathrm{H}_1(x, y; R) = \frac{\left\langle \binom{-y}{x}, \binom{u}{-v} \right\rangle}{\left\langle \binom{-y}{x} \right\rangle}.$$

Note that

$$x\begin{pmatrix} u \\ -v \end{pmatrix} = \begin{pmatrix} xu \\ -xv \end{pmatrix} = \begin{pmatrix} yv \\ -xv \end{pmatrix} = -v\begin{pmatrix} -y \\ x \end{pmatrix} = 0 \text{ in } \mathrm{H}_1(x, y; R).$$

Proposition 3.36. *Let R be a ring, $\underline{x} = x_1, \ldots, x_n \in R$, and $I = (x_1, \ldots, x_n)$.*

a) $\mathrm{H}_i(\underline{x}; M) = 0$ *whenever* $i < 0$ *or* $i > n$.

b) $\mathrm{H}_0(\underline{x}; M) = M/IM$.

c) $\mathrm{H}_n(\underline{x}; M) = (0 :_M I) = \mathrm{ann}_M(I)$.

d) Every Koszul homology module $\mathrm{H}_i(\underline{x}; M)$ *is killed by* $\mathrm{ann}_R(M)$.

e) Every Koszul homology module $\mathrm{H}_i(\underline{x}; M)$ *is killed by* I.

f) If M is a Noetherian R-module, so is $\mathrm{H}_i(\underline{x}; M)$ *for every i.*

g) For every i, $\mathrm{H}_i(\underline{x}; -)$ *is a covariant additive functor R-**mod** $\longrightarrow$ R-**mod**.*

h) Every short exact sequence of R-modules

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

gives rise to a long exact sequence on Koszul homology,

$$\cdots \longrightarrow \mathrm{H}_1(\underline{x}; C) \longrightarrow \mathrm{H}_0(\underline{x}; A) \longrightarrow \mathrm{H}_0(\underline{x}; B) \longrightarrow \mathrm{H}_0(\underline{x}; C) \longrightarrow 0.$$

Proof.

a) Immediate from the definition, since the Koszul complex is only nonzero in homological degrees 0 through n.

b) The comment above tells us that

$$\mathrm{H}_n(\underline{x}; M) = \mathrm{coker}\begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_n \end{pmatrix} = M/IM.$$

c) The comment above tells us that

$$\begin{aligned}\mathrm{H}_n(\underline{x}; M) &= \ker(\ M \xrightarrow{\begin{pmatrix} x_1 & -x_2 & x_3 & \cdots & (-1)^{n+1}x_n \end{pmatrix}^T} M\ ) \\ &= \{m \in M \mid rx_1 = rx_2 = \cdots = rx_n = 0\} = (0 :_M I).\end{aligned}$$

d) In each homological degree, the Koszul complex is simply a direct sum of copies of M. So the modules in $K(\underline{x}; M)$ in each degree are themselves already killed by $\mathrm{ann}_I(M)$.

e) We are going to show something stronger: that for every $a \in I$, multiplication by a on $K(\underline{x}; M)$ is nullhomotopic, which proves that a kills the homology of $K(\underline{x}; M)$. It is in fact sufficient to show that multiplication by a is nullhomotopic on $K(\underline{x})$, since additive functors preserve the homotopy relation. To do this, we will explicitly use the multiplicative structure of the Koszul complex, and think of our description of the Koszul complex via exterior powers. Given $a \in I = (x_1, \ldots, x_n)$, write $a = a_1x_1 + \cdots + a_nx_n$. Consider the map $s_a : K(\underline{x}) \longrightarrow \Sigma^{-}1K(\underline{x})$ given by multiplication by $a_1e_1 \wedge \cdots a_ne_n$, meaning

$$s_a(e_{i_1} \wedge \cdots \wedge e_{i_t}) = \sum_{j=1}^{n} a_j e_j \wedge e_{i_1} \wedge \cdots \wedge e_{i_t}.$$

Now we claim this map s_a is a nullhomotopy for the map of complexes $K(\underline{x}) \longrightarrow K(\underline{x})$ given by multiplication by a in every component. To check that, it is sufficient to check that

$$s_a d\,(e_{i_1} \wedge \cdots \wedge e_{i_t}) + d s_a\,(e_{i_1} \wedge \cdots \wedge e_{i_t}) = a e_{i_1} \wedge \cdots \wedge e_{i_t}.$$

We have

$$\begin{aligned}s_a d\,(e_{i_1} \wedge \cdots \wedge e_{i_t}) &= s_a\left(\sum_{k=1}^{t} (-1)^{k+1} x_k e_{i_1} \wedge \cdots \wedge \widehat{e_{j_k}} \wedge \cdots \wedge e_{i_t}\right) \\ &= \sum_{j=1}^{n}\sum_{k=1}^{t} (-1)^{k+1} a_j x_k e_j \wedge e_{i_1} \wedge \cdots \wedge \widehat{e_{j_k}} \wedge \cdots \wedge e_{i_t}\end{aligned}$$

and

$$\begin{aligned}d s_a\,(e_{i_1} \wedge \cdots \wedge e_{i_t}) &= d\left(\sum_{j=1}^{n} a_j e_j \wedge e_{i_1} \wedge \cdots \wedge e_{i_t}\right) \\ &= \sum_{j=1}^{n}\sum_{k=1}^{t} (-1)^{k+2} a_j e_j \wedge e_{j_1} \wedge \cdots \wedge \widehat{e_{i_k}} \wedge \cdots \wedge e_{i_s} + \sum_{j=1}^{n} a_j x_j e_{i_1} \wedge \cdots \wedge e_{i_t} \\ &= -s_a d\,(e_{i_1} \wedge \cdots \wedge e_{i_t}) + \sum_{j=1}^{n} a_j x_j e_{i_1} \wedge \cdots \wedge e_{i_t}\end{aligned}$$

and since $\sum_{j=1}^{n} a_j x_j = a$, we conclude that

$$(s_a d + d s_a)\left(e_{i_1} \wedge \cdots \wedge e_{i_t}\right) = a e_{i_1} \wedge \cdots \wedge e_{i_t}.$$

f) If M is Noetherian, then so is M^k for any k, as well as any submodules of M^k and any of their quotients. Each $\mathrm{H}_i(\underline{x}; M)$ is a subquotient of a direct sum of copies of M, so it must be Noetherian.

g) An R-module homomorphism $M \xrightarrow{f} N$ induces map $K(f)\colon K(\underline{x}; M) \longrightarrow K(\underline{x}; N)$ given by $K(\underline{x}) \otimes f$, so $\mathrm{H}_i(\underline{x}; f) = \mathrm{H}_i(K(\underline{x}) \otimes f)$.

h) In each homological degree, $K(\underline{x})$ has a free module, so $K(\underline{x}) \otimes_R -$ is exact. We conclude that

$$0 \longrightarrow K(\underline{x}) \otimes_R A \longrightarrow K(\underline{x}) \otimes_R B \longrightarrow K(\underline{x}) \otimes_R C \longrightarrow 0$$

is a short exact sequence of complexes, and the long exact sequence we want is precisely resulting the long exact sequence in homology. □

Remark 3.37. If $C_\bullet$ is a complex, there exists a short exact sequence of complexes

$$0 \longrightarrow C_\bullet \longrightarrow C_\bullet \otimes K_\bullet(f) \longrightarrow C_\bullet(-1) \longrightarrow 0 \qquad \text{given by}$$

$$0 \longrightarrow C_n \xrightarrow{\begin{pmatrix} 1 \\ 0 \end{pmatrix}} C_n \oplus C'_{n-1} \xrightarrow{\begin{pmatrix} 0 & (-1)^{n-1} \end{pmatrix}} C'_{n-1} \longrightarrow 0$$

where $C'_i \cong C_i$, and the $'$ indicates that this is the copy tensored with $K_1(f)$. Indeed, these are clearly exact, and we only need to check that these give maps of complexes; i.e., that the maps above commute with the differentials. An element $\nu \in C_n$ maps to $(\nu, 0)$ in $C_n \oplus C'_{n-1}$, which maps to $(\delta(\nu), 0)$ by the differential on $C_\bullet \otimes K_\bullet(f)$, so the map $C_\bullet \to C_\bullet \otimes K_\bullet(f)$ is a map of complexes. Likewise, an element (ν, μ) in $C_n \oplus C'_{n-1}$ maps to an element with second component $\delta(\mu)$ by the differential on $C_\bullet \otimes K_\bullet(f)$, so the map $C_\bullet \otimes K_\bullet(f) \to C_\bullet(-1)$ is a map of complexes as well.

The corresponding long exact sequence in homology is

$$\cdots \longrightarrow \mathrm{H}_n(C_\bullet) \longrightarrow \mathrm{H}_n(C_\bullet \otimes K_\bullet(f)) \longrightarrow \mathrm{H}_n(C'_\bullet(-1)) \xrightarrow{\delta} \cdots .$$
$$\wr \| \wr$$
$$\mathrm{H}_{n-1}(C_\bullet)$$

We claim that the connecting homomorphism δ agrees with multiplication by f. Indeed, for $[\eta] \in H_i(C'_\bullet)$, one has that $(0, [\eta]) \in H_i(C_\bullet \otimes K_\bullet(f)) \mapsto [\eta] \in H_i(C'_\bullet)$. Applying the differential yields $([f\eta], [\delta(g)]) = ([f\eta], 0) \in H_{i-1}(C_\bullet \otimes K_\bullet(f))$, and $[f\eta] \in H_{i-1}(C_\bullet) \mapsto ([f\eta], 0) \in H_{i-1}(C_\bullet \otimes K_\bullet(f))$.

Thus, the long exact sequence breaks into short exact sequences

$$0 \longrightarrow \tfrac{\mathrm{H}_n(C_\bullet)}{f\,\mathrm{H}_n(C_\bullet)} \longrightarrow \mathrm{H}_n(C_\bullet \otimes K_\bullet(f)) \longrightarrow \operatorname{ann}_{\mathrm{H}_{n-1}(C_\bullet)}(f) \longrightarrow 0\,.$$

In particular, if $\underline{x}, y$ is a sequence of elements of R, and M is an R-module, then

$$0 \longrightarrow \tfrac{\mathrm{H}_n(\underline{x}; M)}{y\,\mathrm{H}_n(\underline{x}; M)} \longrightarrow \mathrm{H}_n(\underline{x}, y; M) \longrightarrow \operatorname{ann}_{\mathrm{H}_{n-1}(\underline{x})}(y) \longrightarrow 0$$

3.3 Regular sequences

Definition 3.38. Let R be a ring and M be an R-module. An element $r \in R$ is **regular** (or a nonzerodivisor) on an R-module M if

$$rm = 0 \implies m = 0$$

for any $m \in M$. More generally, a sequence of elements $x_1, \dots, x_n$ is a **regular sequence on** M if

- $(x_1, \dots, x_n)M \neq M$, and
- for each i, x_i is regular on $M/(x_1, \dots, x_{i-1})M$.

Remark 3.39. Requiring that x_i is regular on $M/(x_1, \dots, x_{i-1})M$ is equivalent to asking that $((x_1, \dots, x_{i-1})M :_M x_i) = (x_1, \dots, x_{i-1})M$.

Example 3.40.

a) Consider the polynomial ring $R = k[x_1, \dots, x_n]$ in n variables over a field k. The variables $x_1, \dots, x_n$ for a regular sequence on R.

b) Let k be a field and $R = k[x, y, z]$. The sequence xy, xz is not regular on R, since xz is kills y on $R/(xy)$.

The order we write the elements in is important.

Example 3.41. Let k be a filed and $R = k[x, y, z]$. The sequence $x, (x-1)y, (x-1)z$ is regular, while $(x-1)y, (x-1)z, x$ is not.

Remark 3.42. An element r is regular on M if and only if $\mathrm{H}_1(K(r; M)) = 0$. Indeed,

$$\mathrm{H}_1(K(r; M)) = \ker(\ M \xrightarrow{r} M\ ) = (0 :_M r),$$

and by definition, r is regular on M if and only if $(0 :_M r) = 0$.

The Koszul complex on a regular sequence is exact in all positive degrees.

Theorem 3.43. *If $\underline{x} = x_1, \dots, x_n \in R$ is a regular sequence on the R-module M, then $\mathrm{H}_i(\underline{x}; M) = 0$ for all $i > 0$.*

Proof. We proceed by induction on the length of the sequence, noting that the case $n = 1$ is Remark 3.42. Now suppose that $\mathrm{H}_j(x_1, \dots, x_i; M) = 0$ for all $j > 0$. The long exact sequence

$$\cdots \longrightarrow \mathrm{H}_n(x_1, \dots, x_{i+1}; M) \longrightarrow \mathrm{H}_{n-1}(x_1, \dots, x_i; M) \xrightarrow{x_{i+1}} \mathrm{H}_{n-1}(x_1, \dots, x_i; M) \longrightarrow \cdots$$

we discussed in Remark 3.37 forces $\mathrm{H}_j(x_1, \dots, x_{i+1}; M) = 0$ for all $j > 1$. Moreover, Remark 3.37 also gave us the short exact sequence

$$0 \longrightarrow \frac{\mathrm{H}_1(x_1, \dots, x_i; M)}{x_{i+1} \cdot \mathrm{H}_1(x_1, \dots, x_i; M)} \longrightarrow \mathrm{H}_1(x_1, \dots, x_{i+1}; M) \longrightarrow \mathrm{ann}_{\mathrm{H}_0(x_1, \dots, x_i; M)}(x_{i+1}) \longrightarrow 0.$$

Since x_{i+1} is regular on $M/(x_1,\dots,x_i)M = \mathrm{H}_0(x_1,\dots,x_i;M)$, $\operatorname{ann}_{\mathrm{H}_0(x_1,\dots,x_i;M)}(x_{i+1}) = 0$. Moreover, $\mathrm{H}_1(x_1,\dots,x_i;M) = 0$ by hypothesis. Therefore, the short exact sequence above gives us $\mathrm{H}_1(x_1,\dots,x_{i+1};M) = 0$.

□

It is natural to ask if Theorem 3.43 has a converse; over a nice enough ring, the answer is yes: the vanishing of Koszul homology does characterize regular sequences.

Theorem 3.44. *Let $(R,\mathfrak{m},k)$ is either a Noetherian local ring or an $\mathbb{N}$-graded algebra over a field k with $R_0 = k$ and homogeneous maximal ideal $\mathfrak{m} = R_+$. Let $M \neq 0$ be a finitely generated R-module, and consider $\underline{x} = x_1,\dots,x_n \in \mathfrak{m}$. In the graded case, we assume that M is graded and $x_1,\dots,x_n$ are all homogeneous. If $\mathrm{H}_i(\underline{x};M) = 0$ for all $i \geqslant 1$, then $x_1,\dots,x_n$ is a regular sequence on R.*

Proof. We proceed by induction on n, noting that the case $n = 1$ is simply Remark 3.42. Now let $n > 1$ and suppose that the statement holds for all sequences of $n-1$ elements. By Remark 3.37, we have short exact sequences

$$0 \longrightarrow \frac{\mathrm{H}_i(x_1,\dots,x_{n-1};M)}{x_n\cdot\mathrm{H}_i(x_1,\dots,x_n;M)} \longrightarrow \mathrm{H}_i(x_1,\dots,x_n;M) \longrightarrow \operatorname{ann}_{\mathrm{H}_{i-1}(x_1,\dots,x_{n-1};M)}(x_n) \longrightarrow 0,$$

and since the middle term is 0 for all $i \geqslant 1$, we conclude that

- $\frac{\mathrm{H}_i(x_1,\dots,x_{n-1};M)}{x_n\cdot\mathrm{H}_i(x_1,\dots,x_n;M)} = 0$ for all $i \geqslant 1$, and
- $\operatorname{ann}_{\mathrm{H}_0(x_1,\dots,x_{n-1};M)}(x_n) = 0$, so x_n is regular on $\mathrm{H}_0(x_1,\dots,x_{n-1};M) = M/(x_1,\dots,x_{n-1})M$.

By Proposition 3.36, $\mathrm{H}_i(x_1,\dots,x_{n-1};M)$ is a finitely generated R-module for all i. Since $x_n \in \mathfrak{m}$ and $x_n\,\mathrm{H}_i(x_1,\dots,x_{n-1};M) = \mathrm{H}_i(x_1,\dots,x_{n-1};M)$, NAK (or Proposition B.11 in the graded case) implies that $\mathrm{H}_i(x_1,\dots,x_{n-1};M) = 0$ for all $i \geqslant 1$. By induction hypothesis, $x_1,\dots,x_{n-1}$ is a regular sequence. We conclude that $x_1,\dots,x_n$ is a regular sequence. □

A corollary of Theorem 3.44 is that in a regular ring, the order of the elements in a regular sequence does not matter.

Corollary 3.45. *Let $(R,\mathfrak{m},k)$ is either a noetherian local ring or a finitely generated $\mathbb{N}$-graded algebra over a field k with $R_0 = k$ and homogeneous maximal ideal $\mathfrak{m} = R_+$. Let M be a finitely generated R-module, and consider $\underline{x} = x_1,\dots,x_n \in \mathfrak{m}$. In the graded case, we assume that M is graded and $x_1,\dots,x_n$ are all homogeneous. If the sequence $\underline{x}$ is regular on M, then so is any of its permutations.*

Proof. If $x_1,\dots,x_n$ is a regular sequence, then $\mathrm{H}_i(x_1,\dots,x_n;M) = 0$ for all $i > 0$, by Proposition 3.36. The Koszul homology on $\underline{x}$ agrees with the Koszul homology on any permutation of $\underline{x}$, which must then also vanish. By Theorem 3.44, any permutation of $\underline{x}$ is a regular sequence. □

In fact, we can extend this to any ring and any module under a reasonable assumption.

Lemma 3.46. *Let R be a ring and M an R-module. If x,y is a regular sequence on M and y is regular on M, then y,x is a regular sequence on M.*

Proof. Suppose that $xm = yn$ for some $m, n \in M$. Since x, y is a regular sequence on M and $yn \in (x)M$, we must have $n \in (x)M$, so there exists some $w \in M$ such that $n = xw$. But then $xm = yn = xyw$. Since x is regular on M, we conclude that $m = yw$, so $m \in (y)M$. In particular, this shows that x is regular on $M/(y)M$. □

Lemma 3.47. *Let $(R, \mathfrak{m}, k)$ is either a Noetherian local ring or an $\mathbb{N}$-graded algebra over a field k with $R_0 = k$ and homogeneous maximal ideal $\mathfrak{m} = R_+$. Let $M \neq 0$ be a finitely generated R-module, and consider $\underline{x} = x_1, \ldots, x_n \in \mathfrak{m}$. In the graded case, we assume that M is graded and $x_1, \ldots, x_n$ are all homogeneous.*

If $x_1, \ldots, x_n$ is a regular sequence on M, then so is $x_1^{a_1}, \ldots, x_n^{a_n}$ for any integers $a_i > 0$.

Proof. By Corollary 3.45, we are allowed to permute the elements in our sequence. Let's use this fact to reduce our proof to the case $n = 1$. If the case $n = 1$ holds, since x_n is a regular sequence on $M/(x_1, \ldots, x_{n-1})$ we can now say $x_n^{a_n}$ is regular on $M/(x_1, \ldots, x_{n-1})$. Therefore, $x_1, \ldots, x_{n-1}, x_n^{a_n}$ is regular on M. Now switch the order and repeat the argument with each x_i, until we conclude that $x_1^{a_1}, \ldots, x_n^{a_n}$ is also regular on M.

Finally, we give a proof when $n = 1$. Now if x is a regular element on M, if $x^a \neq 0$, then $x^a m = 0 \implies x x^{a-1} m = 0$, and since x is regular we must have $x^{a-1}m = 0$. Repeating this $a - 1$ times, we conclude that $xm = 0$, and $m = 0$. □

There is a connection between regular sequences and height.

Theorem 3.48. *If $x_1, \ldots, x_n$ is a regular sequence on R, then* $\operatorname{ht}(x_1, \ldots, x_n) = n$.

Proof. We use induction on n. When $n = 1$, x_1 is regular if and only if x_1 is not in the set of zero divisors of R. By Theorem 1.39, this means x_1 is not in any associated prime of R, and in particular, x_1 is not in any of the minimal primes of R. Therefore, any prime containing x_1 must have height at least 1. By Theorem 3.11, $\operatorname{ht}(x_1) \leqslant 1$, so $\operatorname{ht}(x_1) = 1$. When $n > 1$, x_n is regular on $R/(x_1, \ldots, x_{n-1})$, so by case $n = 1$, $(x_1, \ldots, x_n)/(x_1, \ldots, x_{n-1})$ has height 1 on $R/(x_1, \ldots, x_{n-1})$. By induction hypothesis, $\operatorname{ht}(x_1, \ldots, x_{n-1}) = n - 1$. We conclude that $\operatorname{ht}(x_1, \ldots, x_n) = n$. □

We now record some useful facts about regular sequences we will need when we get back to talking about symbolic powers.

Lemma 3.49. *Let $x_1, \ldots, x_t$ be a regular sequence on R. If $r_1, \ldots, r_t \in R$ are such that $r_1 x_1 + \cdots + r_t x_t = 0$, then $r_1, \ldots, r_t \in (x_1, \ldots, x_t)$.*

Proof. We will do induction on t. When $t = 1$, x_1 is a regular element on R, so $r_1 x_1 = 0$ implies $r_1 = 0 \in (x_1)$.

Now suppose the claim holds for all regular sequences of length $t - 1$ for some $t - 1 \geqslant 1$. Since x_t is regular on $R/(x_1, \ldots, x_{t-1})$, the fact that $r_t x_t = -(r_1 x_1 + \cdots + r_{t-1} x_{t-1}) \in (x_1, \ldots, x_{t-1})$ implies that $r_t \in (x_1, \ldots, x_{t-1})$. Rewriting $r_t = s_1 x_1 + \cdots + s_{t-1} x_{t-1}$, our assumption is that

$$0 = r_1 x_1 + \cdots + r_t x_t = (r_1 + s_1 x_t) x_1 + \cdots (r_{t-1} + s_{t-1} x_t) x_{t-1}.$$

By induction hypothesis, we must have $r_1 + s_1 x_t, \ldots, r_{t-1} + s_{t-1} x_t \in (x_1, \ldots, x_{t-1})$, and thus $r_1, \ldots, r_{t-1} \in (x_1, \ldots, x_t)$. □

Theorem 3.50. *Let R be a ring and consider $I = (a_1, \dots, a_t)$, where $a_1, \dots, a_t$ is a regular sequence on R. Given a homogeneous polynomial $F \in R[x_1, \dots, x_t]$ of degree $n \geqslant 1$, if $F(a_1, \dots, a_t) \in I^{n+1}$, then the coefficients of F must all be in I.*

Proof. Fix nonnegative integers $c_1, \dots, c_t$ with $c_1 + \cdots + c_t = n$, and let u be the coefficient of F in $x_1^{c_1} \cdots x_t^{c_t}$. Since F is homogeneous, all the remaining monomials in F have a factor of at least one of the terms $x_1^{c_1+1}, \dots, x_t^{c_t+1}$. So we can write

$$F(a_1, \dots, a_t) = u a_1^{c_1} \cdots a_t^{c_t} + \sum_{j=1}^{t} a_j^{c_j+1} v_j$$

for some $v_j \in R$. The ideal I^{n+1} is generated by all $a_1^{d_1} \cdots a_t^{d_t}$ with $d_1 + \cdots + d_t = n+1$. For each of these generators, we must have $d_i \geqslant c_i + 1$ for some i, since $c_1 + \cdots + c_t = n$, and thus $I^{n+1} \subseteq \left(a_1^{c_1+1}, \dots, a_t^{c_t+1}\right)$. Since $F(a_1, \dots, a_t) \in I^{n+1}$, we can now find $b_j \in R$ such that

$$u a_1^{c_1} \cdots a_t^{c_t} = \sum_{j=1}^{t} a_j^{c_j+1} b_j.$$

We will show that this implies that $u \in I$, and since we chose $c_1, \dots, c_t$ to be arbitrary, we will then be able to conclude that all the coefficients of F are in I. To do that, we will do induction on the number of nonzero c_j. If all the c_j are 0, then the assumption is that $u = \sum_{j=1}^{t} a_j b_j$, so $u \in I = (a_1, \dots, a_t)$. For the induction step, set

$$y := \prod_{j \neq i} a_j^{c_j}.$$

Now the equality for $u a_1^{c_1} \cdots a_t^{c_t}$ above can be rewritten as

$$\sum_{j \neq i} a_j^{c_j+1} b_j - a_i^{c_i}(uy - a_i b_i) = 0.$$

By Lemma 3.47, $a_1^{c_1+1}, \dots, a_{i-1}^{c_{i-1}+1}, a_i^{c_i}, a_{i+1}^{c_{i+1}+1}, \dots, a_t^{c_t+1}$ is also a regular sequence, so

$$\sum_{j \neq i} a_j^{c_j+1} b_j - a_i^{c_i}(uy - a_i b_i)$$

is a linear combination of the elements in a regular sequence. By Lemma 3.49, all the coefficients must be in the ideal generated by this regular sequence. Therefore,

$$uy - a_i b_i \in (a_i^{c_i}) + \left(a_j^{c_j+1} \mid j \neq i\right) \implies uy \in (a_i) + \left(a_j^{c_j+1} \mid j \neq i\right).$$

Now

$$uy = u \prod_{j \neq i} a_j^{c_j} = u a_1^{c_1} \cdots a_{i-1}^{c_{i-1}} a_i^0 a_{i+1}^{c_{i+1}} \cdots a_t^{c_t} = b_i' a_i^{0+1} + \sum_{j \neq i} d_j a_j^{c_j+1}$$

has one fewer nonzero exponent than our original $u a_1^{c_1} \cdots a_t^{c_t}$, and it is of the form

$$uy = u a_1^{d_1} \cdot \cdots \cdot a_t^{d_t} = \sum_{j=1}^{t} e_j a_j^{d_j+1}$$

with $d_i = 0$ and $d_j = c_j$ for $j \neq i$, and some $e_j \in R$. Therefore, the induction hypothesis applies, and thus $u \in (a_1, \dots, a_t)$. □

3.4 Free resolutions

Definition 3.51. Let M be an R-module. A **free resolution** is a complex

$$F_\bullet = \cdots \longrightarrow F_n \xrightarrow[n]{} \cdots \longrightarrow F_1 \xrightarrow[1]{} F_0 \xrightarrow[0]{} 0$$

where all the F_i are free R-modules, $\mathrm{H}_0(F) = M$, and $\mathrm{H}_i(F) = 0$ for all $i \neq 0$. We may also write a free resolution for M as an exact sequence free modules F_i of the form

$$\cdots \longrightarrow F_n \xrightarrow[n]{} \cdots \longrightarrow F_1 \xrightarrow[1]{} F_0 \xrightarrow[0]{} M \longrightarrow 0\,.$$

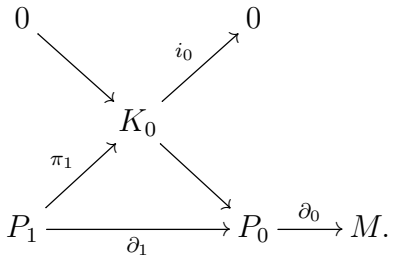
You will find both these definitions in the literature, often indicating the second option as an abuse of notation. We will be a bit sloppy and consider both equivalently, since at the end of the day they contain the same information.

Theorem 3.52. *Every R-module has a free resolution.*

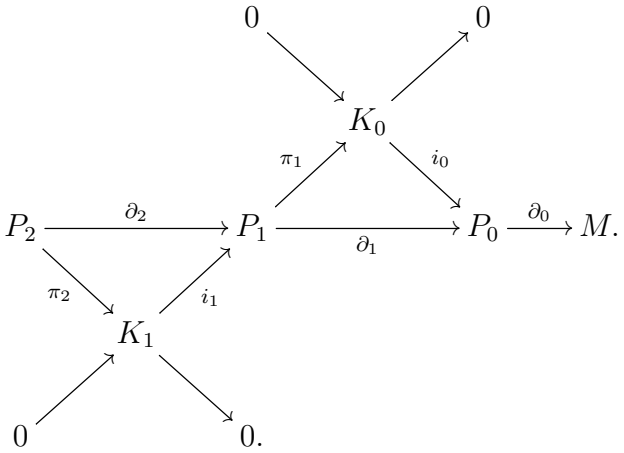
Proof. Let M be an R-module. We are going to construct a free resolution quite explicitly. The first step is to find a free module surjecting onto M, which we can do by taking a free module on any set of generators for M. Now consider the kernel of that projection, say

$$0 \longrightarrow K_0 \xrightarrow{i_0} P_0 \xrightarrow{\pi_0} M \longrightarrow 0.$$

Set $\partial_0 := \pi_0$. There exists a free module P_1 surjecting onto K_0. Now the map $\partial_1 = i_0\pi_1$ satisfies $\operatorname{im}\partial_1 = K_0 = \ker\partial_0$.



Now the process continues analougously. We find a free module P_2 surjecting onto $K_1 := \ker\partial_1$, and set



At each stage, $\pi_i \colon P_i \longrightarrow K_{i-1}$ is a surjective map, $K_i := \ker \partial_i$, i_i is the inclusion of the kernel of ∂_i into P_i, and we get short exact sequences

$$0 \longrightarrow K_{n+1} \xrightarrow{i_{n+1}} P_{n+1} \xrightarrow{\pi_{n+1}} K_n \longrightarrow 0.$$

In fact, $\operatorname{im}(i_{n+1}) = \ker \partial_{n+1} = \ker(i_n \pi_{n+1}) = \ker \pi_{n+1}$. We can continue this process indefinitely for as long as $P_n \neq 0$, and the resulting sequence will be a projective resolution for M. □

We can think of a free resolution

$$\cdots \longrightarrow F_2 \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M$$

as giving a detailed description of our module M. The first free module, F_0, gives us generators for M. The second free module, F_1, gives us generators for all the relations among our generators for M. The next module describes the relations among the relations among our generators. And so on.

Definition 3.53. Let $(R, \mathfrak{m}, k)$ is either a noetherian local ring or a finitely generated $\mathbb{N}$-graded algebra over a field k with $R_0 = k$ and homogeneous maximal ideal $\mathfrak{m} = R_+$. Let M be a finitely generated R-module, which we assume to be graded in the case when R is graded. The **projective dimension** of M is

$$\operatorname{pdim}_R(M) := \inf \left\{ c \mid 0 \longrightarrow P_c \longrightarrow \cdots \longrightarrow P_0 \longrightarrow 0 \text{ is a free resolution for } M \right\}.$$

The projective dimension of a finitely generated module can be infinite.

Example 3.54. Let k be a field and $R = k[x]/(x^2)$, which is a local ring with maximal ideal $\mathfrak{m} = (x)$. The residue field $k = R/\mathfrak{m}$ has infinite projective dimension:

$$\cdots \longrightarrow R \xrightarrow{x} R \xrightarrow{x} R \xrightarrow{x} R \longrightarrow k \longrightarrow 0.$$

So even cyclic modules can have infinite projective dimension.

When $(R, \mathfrak{m})$ is either a local ring or an $\mathbb{N}$-graded graded k-algebra with $R_0 = k$ and homogeneous maximal ideal $\mathfrak{m} = R_+$, we can talk about **minimal** free resolutions. To construct a minimal free resolution of M, we simply take as few generators as possible in each step. This is equivalent to having a **minimal complex** F, meaning that the differential ∂ satisfies $\operatorname{im}(\partial^F) \subseteq \mathfrak{m}F$. If we find basis for each free module F_i, and write the differentials as matrices in those basis, the entries in every differential matrix are all in $\mathfrak{m}$. Ultimately, we can talk about *the* minimal free resolution of M, since all minimal free resolutions are isomorphic. While we will not discuss the details here, here are some examples.

Definition 3.55. Let $(R, \mathfrak{m})$ be either a local ring or an $\mathbb{N}$-graded graded k-algebra with $R_0 = k$ and homogeneous maximal ideal $\mathfrak{m} = R_+$. Let F be a minimal free resolution for the finitely generated (graded) R-module M. The nth betti number of M is

$$\beta_i(M) := \operatorname{rank} F_i = \mu(F_i).$$

In the graded case, the (i,j)th betti number of M, $\beta_{ij}(M)$, counts the number of generators of F_i in degree j. We often collect the betti numbers of a module in its **betti table**:

$\beta(M)$	0	1	2	$\cdots$
0	$\beta_{00}(M)$	$\beta_{11}(M)$	$\beta_{22}(M)$	
1	$\beta_{01}(M)$	$\beta_{12}(M)$	$\beta_{23}(M)$	
2	$\beta_{02}(M)$	$\beta_{13}(M)$		
$\vdots$			$\ddots$	

By convention, the entry corresponding to (i,j) in the betti table of M contains $\beta_{i,i+j}(M)$, and *not* $\beta_{ij}(M)$. This is how Macaulay2 displays betti tables as well, using the command `betti`.

Example 3.56. Suppose that $R = k[x,y,z]$ and that $M = R/(xy, xz, yz)$ corresponds to the variety defining the union of the three coordinate lines in $\mathbb{A}^3_k$. This variety has dimension 1 and degree 3. The minimal free resolution for M is

$$0 \longrightarrow R^2 \xrightarrow{\begin{pmatrix} z & 0 \\ -y & y \\ 0 & -x \end{pmatrix}} R^3 \xrightarrow{\begin{pmatrix} xy & xz & yz \end{pmatrix}} R \longrightarrow M.$$

From this minimal resolution, we can read the betti numbers of M:

- $\beta_0(M) = 1$, since M is a cyclic module;
- $\beta_1(M) = 3$, and these three quadratic generators live in degree 2;
- $\beta_2(M) = 2$, and these represent linear syzygies on quadrics, and thus live in degree 3.

Here is the graded free resolution of M:

$$0 \longrightarrow R(-3)^2 \xrightarrow{\begin{pmatrix} z & 0 \\ -y & y \\ 0 & -x \end{pmatrix}} R(-2)^3 \xrightarrow{\begin{pmatrix} xy & xz & yz \end{pmatrix}} R \longrightarrow M.$$

Notice that the graded shifts in lower homological degrees affect all the higher homological degrees as well. For example, when we write the map in degree 2, we only need to shift the degree of each generator by 1, but since our map now lands on $R(-2)^3$, we have to bump up degrees from 2 to 3, and write $R(-3)^2$. The graded betti number $\beta_{ij}(M)$ of M counts the number of copies of $R(-j)$ in homological degree i in our resolution. So we have

$$\beta_{00} = 1, \beta_{12} = 3, \text{and } \beta_{23} = 2.$$

We can collect the graded betti numbers of M in what is called a *betti table*:

$\beta(M)$	0	1	2
0	1	–	–
1	–	3	2

.

Example 3.57. Let k be a field, $R = k[x, y]$, and consider the ideal

$$I = (x^2, xy, y^3)$$

which has two generators of degree 2 and one of degree 3, so there are graded betti numbers β_{12} and β_{13}. The minimal free resolution for R/I is

$$0 \longrightarrow \begin{matrix} R(-3)^1 \\ \bigoplus \\ R(-4)^1 \end{matrix} \xrightarrow{\begin{pmatrix} y & 0 \\ -x & y^2 \\ 0 & -x \end{pmatrix}} \begin{matrix} R(-2)^2 \\ \bigoplus \\ R(-3)^1 \end{matrix} \xrightarrow{\begin{pmatrix} x^2 & xy & y^3 \end{pmatrix}} R \longrightarrow R/I.$$

$$\begin{matrix} \beta_{23}(R/I) = 1 \\ \beta_{24}(R/I) = 1 \end{matrix} \qquad \begin{matrix} \beta_{12}(R/I) = 2 \\ \beta_{13}(R/I) = 1 \end{matrix}$$

So the betti table of R/I is

$\beta(M)$	0	1	2
0	1	–	–
1	–	2	1
2	–	1	1

These invariants can give us some information about Ext and Tor, and vice-versa.

Remark 3.58. If $\operatorname{pdim}_R(M) = n$ is finite, then we can take a free resolution of M with length n to compute $\operatorname{Tor}_i^R(M, -)$, and thus $\operatorname{Tor}_i^R(M, -) = 0$ for all $i > n$. For the same reason, $\operatorname{Ext}_R^i(M, -) = 0$ for all $i > n$.

Remark 3.59. Let $(R, \mathfrak{m}, k)$ be either a local ring or an $\mathbb{N}$-graded k-algebra, where k is a field, with $R_0 = k$ and homogeneous maximal ideal $\mathfrak{m} = R_+$, and M a finitely generated (graded) R-module. The homomorphisms of R-modules $R \longrightarrow R$ are precisely the multiplication maps by each fixed $r \in R$. The map $(r \cdot -) \otimes_R k$ is simply multiplication by the image of r in $k = R/\mathfrak{m}$ on k. More generally, a homomorphism of R-modules $R^n \xrightarrow{f} R^m$ can be represented by an $m \times n$ matrix A with entries in R after we fix bases for R^n and R^m, and the matrix representing $f \otimes_R k$ in the corresponding bases for k^m and k^n is the matrix obtained from A by considering the images of the entries in k.

Given any $g \in \operatorname{Hom}_R(R, k)$, the composition of f with multiplication by r is the map $g(r \cdot -) = rg(-)$. So $\operatorname{Hom}_R(r \cdot -, k)$ is multiplication by the image of r in k. More generally, if A is an $m \times n$ matrix representing $R^n \xrightarrow{f} R^m$, the map $\operatorname{Hom}_R(f, k)$ is represented in the corresponding bases for k^n and k^m by the transpose of A, where the entries are now replaced by their images in $k = R/\mathfrak{m}$.

Theorem 3.60. *Let $(R, \mathfrak{m}, k)$ be either a Noetherian local ring or an $\mathbb{N}$-graded k-algebra, where k is a field, with $R_0 = k$ and homogeneous maximal ideal $\mathfrak{m} = R_+$, and M a finitely generated (graded) R-module. Then*

$$\beta_i(M) = \dim_k(\operatorname{Tor}_i^R(M, k)) = \dim_k(\operatorname{Ext}_R^i(M, k)).$$

Proof. Let F be a minimal free resolution for M. The module in degree i in the complex $F \otimes_R k$ is

$$F_i \otimes_R k = R^{\beta_i(M)} \otimes_R k = k^{\beta_i(M)}.$$

Minimal free resolutions are minimal complexes, so $\operatorname{im}(\partial^F) \subseteq \mathfrak{m}F$, and thus $\partial \otimes_R k = 0$. So

$$F \otimes_R k = \cdots \longrightarrow k^{\beta_i(M)} \longrightarrow k^{\beta_{i-1}(M)} \longrightarrow \cdots \longrightarrow k^{\beta_1(M)} \longrightarrow k^{\beta_0} \longrightarrow 0.$$

Therefore,

$$\operatorname{Tor}_i^R(M,k) = \operatorname{H}_i(F \otimes_R k) = k^{\beta_i(M)}.$$

The module in degree i in the complex $\operatorname{Hom}_R(F,k)$ is

$$\operatorname{Hom}_R(F_i,k) = \operatorname{Hom}_R(R^{\beta_i(M)},k) = k^{\beta_i(M)}.$$

Following the discussion in Remark 3.59, the fact that $\partial(F) \subseteq \mathfrak{m}F$ implies $\operatorname{Hom}_R(\partial^F,k) = 0$. Therefore,

$$\operatorname{Hom}_R(F,k) = 0 \longrightarrow k^{\beta_0(M)} \xrightarrow{0} k^{\beta_1(M)} \longrightarrow \cdots \longrightarrow k^{\beta_i(M)} \longrightarrow \cdots$$

so

$$\operatorname{Ext}_R^i(M,k) = \operatorname{H}^i(\operatorname{Hom}_R(F,k)) = k^{\beta_i(M)}. \qquad \square$$

Corollary 3.61. *Let $(R,\mathfrak{m},k)$ be either a local ring or an $\mathbb{N}$-graded k-algebra, where k is a field, with $R_0 = k$ and homogeneous maximal ideal $\mathfrak{m} = R_+$. For every finitely generated (graded) R-module M, $\operatorname{pdim}_R(M) \leqslant \operatorname{pdim}_R(k)$.*

Proof. When $i > \operatorname{pdim}_R(k)$, $\operatorname{Tor}_i^R(M,k) = 0$, so $\beta_i(M) = 0$ by Theorem 3.60. $\square$

Remark 3.62. Also as a consequence of Theorem 3.60, we learn that

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

We can extend this to graded betti numbers once we realize that Tor and Ext of graded modules can also be given graded structures.

Exercise 5. Let $(R,\mathfrak{m},k)$ be an $\mathbb{N}$-graded k-algebra, where k is a field, with $R_0 = k$ and homogeneous maximal ideal $\mathfrak{m} = R_+$, and M a finitely generated graded R-module. Fix a graded minimal free resolution F of M. Then

$$\beta_{i,j}(M) = \text{number of copies of } R(-j) \text{ in } F_i = \dim_k(\operatorname{Tor}_i^R(M,k)_j) = \dim_k(\operatorname{Ext}_R^i(M,k)_j).$$

If only we had an explicit minimal free resolution of k, maybe we could use it to say something about the minimal free resolutions of other finitely generated R-modules. With that goal in mind, we return to regular sequences.

Corollary 3.63. *If $x_1,\dots x_n$ is a regular sequence on R, then the Koszul complex on $x_1,\dots,x_n$ is a free resolution for $R/(x_1,\dots,x_n)$. Moreover, if $(R,\mathfrak{m},k)$ is either a local ring or an $\mathbb{N}$-graded algebra over a field k with $R_0 = k$ and homogeneous maximal ideal $\mathfrak{m} = R_+$, then the Koszul complex $K_\bullet(x_1,\dots,x_n)$ is a minimal free resolution for $R/(x_1,\dots,x_n)$.*

Proof. By Theorem 3.43, the Koszul complex $P = K_\bullet(x_1, \dots, x_n)$ has $\mathrm{H}_i(P) = 0$ for all $i > 0$. This is a complex of free modules, and thus a free resolution of $\mathrm{H}_0(P)$, which by Proposition 3.36 is $R/(x_1, \dots, x_n)$. □

Theorem 3.64 (Hilbert Syzygy Theorem)**.** *Every finitely generated graded module M over a polynomial ring $R = k[x_1, \dots, x_n]$ over a field k has finite projective dimension. In fact,* $\operatorname{pdim}(M) \leqslant n$.

Proof. By Corollary 3.63, the Koszul complex on the regular sequence $x_1, \dots, x_d$ is a minimal free resolution for $k = R/(x_1, \dots, x_n)$, so $\operatorname{pdim}_R k = n$. But $\beta_i(M) = \dim_k \operatorname{Tor}_R^i(M, k)$ by Theorem 3.60, and since $\operatorname{Tor}_i^R(M, k) = 0$ for all $i > n = \operatorname{pdim}_R(k)$, $\operatorname{pdim}_R(M) \leqslant n$. □

3.5 Regular rings

Regular rings are the nicest possible kinds of rings. A **regular local ring** $(R, \mathfrak{m}, k)$ is a finite dimensional Noetherian ring of dimension d whose maximal ideal $\mathfrak{m}$ is generated by d elements. When we discussed height and dimension, we saw that this is in fact the smallest possible value for the minimal number of generators of $\mathfrak{m}$; in general, $\mu(\mathfrak{m}) \geqslant d$. We are now ready to give a completely homological characterization of regular local rings. This characterization, first proved by Auslander and Buchsbaum and independently by Serre, solved a famous open problem called the Localization Problem.

Problem 3.65 (Localization Problem)**.** *If R is a regular local ring, must R_P be regular for every prime P in R?*

This is asking if being regular is a local property. A positive answer allows for a simple global definition of regularity:

Definition 3.66. A ring R is **regular** if R_P is a regular local ring for all prime ideals P.

Before we can get to this famous homological characterization of regular local rings, and the solution to the localization problem, we will need to sharpen our tools a bit.

Theorem 3.67 (Serre)**.** *Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring. Moreover, if $\mu(\mathfrak{m}) = s$, then*

$$\dim_k(\operatorname{Tor}_i^R(k, k)) \geqslant \binom{s}{i}.$$

Replacing k by M in the previous result leads to a famous open question.

Conjecture 3.68 (Buchsbaum—Eisenbud, Horrocks)**.** *Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring of dimension d and M a finitely generated Artinian R-module of finite projective dimension. Then*

$$\beta_i(M) = \dim_k(\operatorname{Tor}_i^R(M, k)) \geqslant \binom{d}{i}.$$

While this remains an open question, there is much evidence to support it. For example, the conjecture predicts that

$$\sum_i \beta_i(M) \geqslant \sum_i \binom{d}{i} = 2^d.$$

This is known as the Total Rank Conjecture, and it was recently shown by Walker in almost all cases.

Theorem 3.69 (Walker, 2017)**.** *Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring of dimension d and characteristic not 2, $M \neq 0$ a finitely generated R-module of finite projective dimension, and $c = \operatorname{ht}(\operatorname{ann}(M))$. Then*

$$\sum_i \beta_i(M) \geqslant 2^c.$$

The famous homological characterization of regular rings that solved the localization problem is the following:

Theorem 3.70 (Auslander–Buchsbaum, Serre)**.** *Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring of dimension d. The following are equivalent:*

a) The residue field k has finite projective dimension.

b) Every finitely generated R-module has finite projective dimension.

c) The maximal ideal $\mathfrak{m}$ is generated by a regular sequence.

d) The maximal ideal $\mathfrak{m}$ is generated by d elements.

Proof. The implication b $\implies$ a is obvious: just take $M = k$. The proof of a $\implies$ b is essentially the same as Hilbert's Syzygy Theorem: $\beta_i(M) = \dim_k \operatorname{Tor}_i^k(M, k)$ for all i, and $\operatorname{Tor}_i^k(M, k) = 0$ for all $i > \operatorname{pdim}_R(k)$.

If $\mathfrak{m}$ is generated by a regular sequence, then the Koszul complex on that regular sequence is a minimal free resolution of k, by Corollary 3.63, so k has projective dimension d. This is c $\implies$ a.

Let's now show that d $\implies$ c. Set $\mathfrak{m} = (x_1, \dots, x_d)$. In fact, we will show something stronger: that $(0), (x_1), (x_1, x_2), \dots, (x_1, \dots, x_d)$ are distinct prime ideals in R. Notice in particular that this implies that $x_1, \dots, x_d$ form a regular sequence.

If $d = 0$, then $\mathfrak{m} = (\{\}) = (0)$, and there is nothing to prove. We proceed by induction on d, assuming that $d > 0$ and that we have shown that whenever $\mathfrak{m}$ is generated by $d - 1$ elements, $x_1, \dots, x_{d-1}$, the ideals $(0), (x_1), (x_1, x_2), \dots, (x_1, \dots, x_{d-1})$ are distinct prime ideals in R.

When $d > 0$, $\mathfrak{m}$ is not a minimal prime. By Prime Avoidance,

$$\mathfrak{m} \not\subseteq \bigcup_{P \in \operatorname{Min}(R)} P,$$

and using Theorem B.3 we can find an element

$$y_1 = x_1 + r_2 x_2 + \cdots + r_d x_d \notin \bigcup_{P \in \operatorname{Min}(R)} P.$$

Now we can replace x_1 by y_1, since $\mathfrak{m} = (y_1, x_2, \ldots, x_d)$, so we can assume that x_1 is not in any minimal prime. By Krull's Height Theorem 3.11, $\mathrm{ht}(x_1) \leqslant 1$, so $\dim(R/(x_1)) = \mathrm{ht}(\mathfrak{m}/(x_1)) \geqslant d-1$. By construction, $\mathfrak{m}/(x_1)$ is generated by $d-1$ elements, so again by Krull's Height Theorem, $\dim(R/(x_1)) = \mathrm{ht}(\mathfrak{m}/(x_1)) \leqslant d-1$. We conclude that $\dim(R/(x_1)) = d-1$. By induction hypothesis, $(x_1)/(x_1), \ldots, (x_1, \ldots, x_d)/(x_1)$ are distinct prime ideals in $R/(x_1)$. Therefore, $(x_1), (x_1, x_2), \ldots, (x_1, \ldots, x_d)$ are distinct prime ideals in R.

Now we claim that R is a domain, which will show that $(0) \subsetneq (x_1)$ is also a prime ideal. First, note that x_1 is not contained in any minimal prime, but (x_1) is a prime ideal, so there exists some minimal prime $P \subsetneq (x_1)$. Given any $y \in P \subseteq (x_1)$, we can write $y = rx_1$ for some r. By constrution, $x_1 \notin P$, so we must have $r \in P$. But we just showed that every element in P is of the form rx_1, so $P = x_1 P$. By NAK, $P = (0)$. We conclude that R is a domain, and this finishes the proof of d $\implies$ c.

Finally, all that's left to show is a $\implies$ d. We claim that $\mathrm{pdim}_R(k) < \infty$ implies $\mathrm{pdim}_R(k) \leqslant \dim(R) = d$. If the claim holds, then Theorem 3.67 and Theorem 3.60 say that

$$\beta_i(k) = \dim_k(\mathrm{Tor}_i^R(k,k)) \geqslant \binom{\mu(\mathfrak{m})}{i}$$

for all i. Since $\beta_i(k) = 0$ for all $i > \mathrm{pdim}_R(k)$, we must have

$$\mu(\mathfrak{m}) \leqslant \mathrm{pdim}_R(k) \leqslant \dim(R) = d.$$

But $\mathrm{ht}(\mathfrak{m}) = \dim(R) = d$, so by Theorem 3.11, $\mu(\mathfrak{m}) \geqslant d$. We conclude that $\mathfrak{m}$ is generated by exactly d elements, which is precisely d. So all we have left to do is to prove the claim that $\mathrm{pdim}_R(k) < \infty$ implies $\mathrm{pdim}_R(k) \leqslant \dim(R) = d$.

By contradiction, suppose $\mathrm{pdim}_R(k) > d$ but $\mathrm{pdim}_R(k) < \infty$. Choose a maximal regular sequence $y_1, \ldots, y_t \in \mathfrak{m}$. By Theorem 3.48, $t \leqslant d$.

Since our regular sequence $y_1, \ldots, y_t$ was chosen to be maximal inside $\mathfrak{m}$, every element in $\mathfrak{m}$ is a zerodivisor on $R/(y_1, \ldots, y_t)$, or else we could increase our regular sequence. So $\mathfrak{m}$ is contained in the union of the zerodivisors on $R/(y_1, \ldots, y_t)$, which by Theorem 1.39 is the same as the union of the associated primes of $R/(y_1, \ldots, y_t)$. By Prime Avoidance, $\mathfrak{m}$ must be contained in some associated prime of $R/(y_1, \ldots, y_t)$. But $\mathfrak{m}$ is maximal, so $\mathfrak{m}$ *is* an associated prime of $R/(y_1, \ldots, y_t)$. Equivalently, $k = R/\mathfrak{m}$ embeds into $R/(y_1, \ldots, y_t)$. This gives us some short exact sequence

$$0 \longrightarrow k \longrightarrow R/(y_1, \ldots, y_t) \longrightarrow M \longrightarrow 0.$$

The corresponding long exact sequence for Tor is

$$\cdots \longrightarrow \mathrm{Tor}_{i+1}^R(M,k) \longrightarrow \mathrm{Tor}_i^R(k,k) \longrightarrow \mathrm{Tor}_i^R(R/(y_1, \ldots, y_t), k) \longrightarrow \cdots.$$

We know $t = \mathrm{pdim}_R(R/(y_1, \ldots, y_t))$, by Corollary 3.63, so $\mathrm{Tor}_i^R(R/(y_1, \ldots, y_t), k) = 0$ for $i > t$. But $t \leqslant d < \mathrm{pdim}_R(k)$, so in particular $\mathrm{Tor}_i^R(R/(y_1, \ldots, y_t), k) = 0$ for $i = \mathrm{pdim}_R(k)$.

Moreover, Corollary 3.61 says that $\mathrm{pdim}_R(M) \leqslant \mathrm{pdim}_R(k)$ for any finitely generated R-module M, so in particular $\mathrm{Tor}_{i+1}^R(M,k) = 0$ for $i = \mathrm{pdim}_R(k)$. But this is impossible: our long exact sequence would then have $\mathrm{Tor}_{\mathrm{pdim}_R(k)}^R(k,k) \neq 0$ sandwiched between two zero modules. $\square$

Our proof also showed the following:

Corollary 3.71. *Every regular local ring is a domain.*

Corollary 3.72. *Every regular local ring* $(R, \mathfrak{m}, k)$ *has* $\operatorname{pdim}_R(k) = \dim R$.

Now we can solve the localization problem very easily.

Exercise 6. If R is a regular local ring, then R_P is a regular local ring for every prime P.

Remark 3.73. If we want to show that a particular ring (not necessarily local) is regular, it is sufficient to show that $R_{\mathfrak{m}}$ is a regular local ring for every maximal ideal $\mathfrak{m}$ — this will imply that R_P is a localization of a regular local ring for every prime P.

Exercise 7. Show that every principal ideal domain is a regular ring.

We have shown that finitely generated *graded* modules over a polynomial ring $k[x_1, \dots, x_d]$ have finite projective dimension, but this is not quite enough to conclude that polynomial rings are regular.

Theorem 3.74. *Every polynomial ring* $R = k[x_1, \dots, x_d]$ *over a field* k *is a regular ring.*

We have seen that regular rings are very nice. Modulo some technical conditions, it turns out that *every* noetherian local ring is a quotient of a regular ring. More precisely, every *complete* local ring is a quotient of a regular local ring. If a local ring R is not complete, we can always take its *completion*, which is now a quotient of a regular local ring. This very important fact is the Cohen Structure Theorem.[1] When our local ring R contains a field k, the Cohen Structure Theorem actually says that R is a quotient of $k[\![x_1, \dots, x_d]\!]$ for some d.

The nice things we proved about regular local rings have analogues in any regular ring, not necessarily local. For example, when R is a regular ring of dimension d, then it is still true that every finitely generated R-module has projective dimension at most d, even if R is not local; if R is not regular, then it has finitely generated modules with infinite projective dimension.

3.6 Depth

We now get back to regular sequences to talk about their length.

Definition 3.75. Let I be an ideal in a ring R and M be an R-module. The **I-depth** of M is the maximal length of a regular sequence on M consisting of elements in I, denoted $\operatorname{depth}_I(M)$. When $(R, \mathfrak{m})$ is a local ring, we write $\operatorname{depth}(M)$ for $\operatorname{depth}_{\mathfrak{m}}(M)$, and call it the **depth** of M.

While it is not yet clear that all maximal regular sequences on M inside an ideal I have the same length, we already have an upper bound for depth.

Remark 3.76. If $x_1, \dots, x_n$ is a regular sequence on R inside I, we saw in Theorem 3.48 that $\operatorname{ht}(x_1, \dots, x_n) = n$, so $\operatorname{depth}_I(R) \leqslant \operatorname{ht}(I)$. In particular, $\operatorname{depth}(R) \leqslant \dim(R)$.

[1] In fact, this amazing theorem was I. S. Cohen's PhD thesis!

We can construct maximal regular sequences explicitly.

Construction 3.77. Let R be a Noetherian ring, I be an ideal in R, and $M \neq 0$ be a finitely generated R-module. To construct a regular sequence on M inside I, we start by finding a regular element on M inside I. Either I is contained in some associated prime of M, in which case every element in I is a zerodivisor on M, or there exists an element x_1 in I not in any associated prime of M, by Prime Avoidance. Such an element is regular on M, since the union of the associated primes of M is precisely the set of zerodiviors, by Theorem 1.39.

Now we repeat the process: either I is contained in some associated prime of $M/(x_1)M$, in which case there are no regular elements on $M/(x_1)M$ inside I, or we can find $x_2 \in I$ not in any associated prime of $M/(x_1)M$, which is necessarily regular on $M/(x_1)M$. At each step, $(x_1, \ldots, x_i)M \subsetneq (x_1, \ldots, x_{i+1})M$, and since M is Noetherian, the process must stop.

In fact, we get such an increasing sequence given any regular sequence on M inside of I, so all such sequences are finite. We will now show that all maximal regular sequences on M inside I have the same length, which proves that $\operatorname{depth}_I(M)$ is finite. First, we need a few lemmas.

Lemma 3.78. *Let R be a Noetherian ring, I be an ideal in R, and $M \neq 0$ be a finitely generated R-module. There exists $r \in I$ which is regular on M if and only if $I \not\subseteq P$ for all $P \in \operatorname{Ass}(M)$. In particular, if $(R, \mathfrak{m})$ is a noetherian local ring, $\mathfrak{m} \in \operatorname{Ass}(M)$ if and only if there are no regular elements on M.*

Proof. If $r \in I$ is regular on M, then r is not a zerodivisor on M, so r is not in the union of the associated primes of M, by Theorem 1.39. As a consequence, I cannot be contained in any associated prime of M.

Conversely, recall that M has finitely many associated primes, by Theorem 1.44. If I is not contained in any associated prime of M, then by Prime Avoidance B.1 it also cannot be contained in the union of the associated primes of M. Recall Theorem 1.39, which says that the union of the associated primes is the set of zero divisors. We conclude that I contains some regular element on M.

The final statement now follows once we note that the fact that $\mathfrak{m}$ is a maximal ideal implies that $\mathfrak{m}$ *in* $\operatorname{Ass}(M)$ if and only if $\mathfrak{m}$ is contained in some associated prime of M. □

Lemma 3.79. *Let R be a noetherian ring and M and N be finitely generated R-modules. If $a \in \operatorname{ann}_R(M)$, then $a \operatorname{Ext}^i_R(M, N) = 0$ for all i. Moreover, if $b \in \operatorname{ann}_R(N)$, then $b \operatorname{Ext}^i_R(M, N) = 0$ for all i.*

Proof. When $i = 0$, we want to show that $a \in \operatorname{ann}(\operatorname{Hom}_R(M, N)$ and $b \in \operatorname{ann}(\operatorname{Hom}_R(M, N)$. Given any $f \in \operatorname{Hom}_R(M, N)$ and any $m \in M$,

$$af(m) = f(am) = f(0) = 0,$$

so $af = 0$. Moreover, b kills every element in N, so $bf = 0$. Now let $P \longrightarrow M$ be a projective resolution on M, and $N \longrightarrow E$ be an injective resolution of N. Then

$$\begin{aligned}\operatorname{Ext}^i_R(M, N) &= \mathrm{H}^i\left(0 \longrightarrow \operatorname{Hom}_R(P_0, N) \longrightarrow \operatorname{Hom}_R(P_1, N) \longrightarrow \operatorname{Hom}_R(P_2, N) \longrightarrow \cdots\right) \\ &= \mathrm{H}^i\left(0 \longrightarrow \operatorname{Hom}_R(M, E^0) \longrightarrow \operatorname{Hom}_R(M, E^1) \longrightarrow \operatorname{Hom}_R(M, E^2) \longrightarrow \cdots\right),\end{aligned}$$

so $\operatorname{Ext}^i_R(M,N)$ is a subquotient of both $\operatorname{Hom}_R(P_i,N)$ and $\operatorname{Hom}_R(M,E^i)$. We conclude that a and b both kill $\operatorname{Ext}^i_R(M,N)$. □

Theorem 3.80. *Let R be a Noetherian ring, I be an ideal in R, and $M \neq 0$ be a finitely generated R-module with $M \neq IM$. Then all maximal regular sequences on M inside I have the same length.*

Proof. Let $x_1,\dots,x_n \in I$ and $y_1,\dots,y_\ell \in I$ both be maximal regular sequences on M, and assume $n \leqslant \ell$.

When $n = 0$, every element in I is a zerodivisor on M, so $\ell = 0$. When $n = 1$, every element in I is a zerodivisor on $M/(x_1)M$, so $I \subseteq P$ for some $P \in \operatorname{Ass}(M/(x_1)M)$. In particular, there exists some $m \in M$, $m \notin (x_1)M$, such that $I \subseteq ((x_1)M :_R m)$, so $Im \in (x_1)M$. In particular, $y_1 m = x_1 a$ for some $a \in M$. If $a \in (y_1)M$, then we would have $y_1 m = x_1 a \in (x_1y_1)M$, and since y_1 is regular on M, that would imply $m \in (x_1)M$, which is a contradiction. Thus $a \notin (y_1)M$. Moreover,

$$(x_1)Ia = Ix_1a = Iy_1m = y_1(Im) \subseteq (x_1)(y_1)M,$$

and since x_1 is a regular element on M, we must have $Ia \subseteq (y_1)M$. Therefore, $a \in M$ is an element that both satisfies $a \notin (y_1)M$ and $Ia \subseteq (y_1)M$, so every element in I kills a in $M/(y_1)M$, and is thus a zerodivisor on $M/(y_1)M$. This proves that $\ell = 1$.

We proceed by induction on n. Now assume that $n > 1$ and $\ell > n$. In particular, I contains a regular element on $M/(x_1,\dots,x_i)$ for all $i < n$ and a regular element on $M/(y_1,\dots,y_j)$ for all $j < \ell$, so by Prime Avoidance we can pick $c \in I$ that avoids both all the (finitely many) associated primes of $M/(x_1,\dots,x_i)M$ for all $i < n$ and $M/(y_1,\dots,y_j)M$ for all $j < \ell$. In particular, $x_1,\dots,x_{n-1},c$ and $y_1,\dots,y_n,c$ are both regular sequences on M. Now x_n and c are both regular sequences on $M/(x_1,\dots,x_{n-1})$, so the case $n = 1$ says $x_1,\dots,x_{n-1},c$ is also a maximal regular sequence on M. Now by Lemma 3.46, $x_1,\dots,c,x_{n-1}$ is also a regular sequence on M, since c is also regular on $M/(x_1,\dots,x_{n-2}$, and so on, until we conclude that $c,x_1,\dots,x_{n-1}$ is a regular sequence on M. Similarly, $c,y_1,\dots,y_n$ is a regular sequence on M. Notice in fact that $c,x_1,\dots,x_{n-1}$ is maximal inside I, or else we could increase its size, move c back to after x_{n-1}, and obtain a contradiction. Therefore, $x_1,\dots,x_{n-1}$ and $c,y_1,\dots,y_n$ are both regular sequences on $M/(c)M$, and $x_1,\dots,x_{n-1}$ is maximal. But by induction hypothesis, all maximal regular sequences on $M/(c)M$ inside I have the same length, which would say that the length of $y_1,\dots,y_n$, n, is at most $n-1$. This is a contradiction, and we conclude that $\ell = n$. □

It turns out that depth can be described in a purely homological way.

Theorem 3.81. *Let R be a Noetherian ring and M a finitely generated R-module. Then*

$$\operatorname{depth}_I(M) = \min\{i \mid \operatorname{Ext}^i_R(R/I,M) \neq 0\}.$$

Proof. When $\operatorname{depth}_I(M) = 0$, there is no regular sequence on M inside I. By Lemma 3.78, $I \subseteq P$ for some $P \in \operatorname{Ass}(M)$. We have an inclusion $R/P \hookrightarrow M$, so consider the composition

$$R/I \twoheadrightarrow R/P \hookrightarrow M.$$

This is a nonzero map, so $\mathrm{Ext}^0(R/I, M) = \mathrm{Hom}(R/I, M) \neq 0$. On the other hand, if $\mathrm{Hom}_R(R/I, M) = \mathrm{Ext}^0(R/I, M) \neq 0$, there exists a nonzero R-module homomorphism $R/I \longrightarrow M$. But to choose an R-module homomorphism $R/I \longrightarrow M$ is the same as choosing an element in M that is killed by I, so I contains no nonzero divisors on M and $\mathrm{depth}_I(M) = 0$.

We proceed by induction on $\mathrm{depth}_I(M) = n$, assuming we have proved the statement whenever $\mathrm{depth}_I(M) < n$. Suppose that $x_1, \ldots, x_n$ is a maximal regular sequence on M inside I. Then $x_2, \ldots, x_n$ is a maximal regular sequence on M/x_1M, so by induction we know $n-1 = \min\{i \mid \mathrm{Ext}^i_R(R/I, M/x_1M) \neq 0\}$. Applying $\mathrm{Hom}_R(R/I, -)$ to the short exact sequence

$$0 \longrightarrow M \xrightarrow{\cdot x_1} M \longrightarrow M/x_1M \longrightarrow 0$$

we get a long exact sequence

$$\cdots \longrightarrow \mathrm{Ext}^{i-1}_R(R/I, M/x_1M) \longrightarrow \mathrm{Ext}^i_R(R/I, M) \xrightarrow{x_1} \mathrm{Ext}^i_R(R/I, M) \longrightarrow \cdots .$$

We know that $\mathrm{Ext}^{n-1}_R(R/I, M/x_1M) \neq 0$ and that $\mathrm{Ext}^i_R(R/I, M/x_1M) = 0$ for all $i < n-1$. Therefore, whenever $i < n-1$,

$$\mathrm{Ext}^i_R(R/I, M) \xrightarrow{x_1} \mathrm{Ext}^i_R(R/I, M)$$

is an isomorphism. However, $x_1 \in I = \mathrm{ann}(R/I)$, so $\mathrm{ann}(R/I) \subseteq \mathrm{ann}(\mathrm{Ext}^i_R(R/I, M))$ by Lemma 3.79. Therefore, $\mathrm{Ext}^i_R(R/I, M) = 0$ for all $i < n-1$. Moreover, multiplication by x_1 is the zero map on $\mathrm{Ext}^i_R(R/I, M)$ for any i, also by Lemma 3.79. Finally, we have an exact sequence

$$\mathrm{Ext}^{n-1}_R(R/I, M) \xrightarrow{x_1} \mathrm{Ext}^{n-1}_R(R/I, M) \longrightarrow \mathrm{Ext}^{n-1}_R(R/I, M/x_1M) \longrightarrow \cdots .$$

where the multiplication by x_1 maps are 0, so our exact sequence is

$$0 \longrightarrow \mathrm{Ext}^{n-1}_R(R/I, M) \xrightarrow{0} \mathrm{Ext}^{n-1}_R(R/I, M) \longrightarrow \underbrace{\mathrm{Ext}^{n-1}_R(R/I, M/x_1M)}_{\neq 0} \longrightarrow \mathrm{Ext}^n_R(R/I, M) \xrightarrow{0} \cdots .$$

In particular, $\mathrm{Ext}^{n-1}(R/I, M) = 0$ and $\mathrm{Ext}^n(R/I, M) \neq 0$. We conclude that

$$\mathrm{depth}_I(M) = n = \min\{i \mid \mathrm{Ext}^i_R(R/I, M) \neq 0\}. \qquad \square$$

For yet another homological characterization of depth, we turn to Koszul homology.

Theorem 3.82 (Depth sensitivity of the Koszul complex)**.** *Let R be a Noetherian ring and M be finitely generated R-module. Given any $\underline{x} = x_1, \ldots, x_n$ such that $(\underline{x})M \neq M$,*

$$\mathrm{depth}_{(\underline{x})}(M) = \max\{r \mid \mathrm{H}^i(\underline{x}; M) = 0 \text{ for all } i > n - r\}.$$

So we can measure $\mathrm{depth}_I(M)$ by looking at the first nonzero Koszul homology we see when we start counting *from the top*.

$$\begin{array}{ll} K(\underline{x}; M) & 0 \to M \to \cdots \to M^{\binom{n}{n-r+1}} \to M^{\binom{n}{n-r}} \to \cdots \to M \to 0 \\ \mathrm{H}(\underline{x}; M) & \qquad 0 \qquad \cdots \qquad 0 \qquad \neq 0 \end{array}$$

Proof. We are going to show that if $I = (\underline{x})$ contains a regular sequence $y_1, \dots, y_m$ on M, then $\mathrm{H}_{n-i+1}(\underline{x}; M) = 0$ for all $i = 1, \dots, m$, and $\mathrm{H}_{n-m}(\underline{x}; M) \cong \mathrm{Ext}^m_R(R/I, M)$. This will prove the theorem, since depth is the largest possible m we could take, and Theorem 3.81 says $\mathrm{Ext}^{\mathrm{depth}}_R(R/I, M) \neq 0$.

We proceed by induction on m. When $m = 0$, Proposition 3.36 c says that

$$\mathrm{H}_n(\underline{x}; M) \cong (0 :_M I) \cong \mathrm{Hom}_R(R/I, M),$$

and we are done. When $m > 0$, the short exact sequence

$$0 \longrightarrow M \xrightarrow{y_1} M \longrightarrow M/(y_1)M \longrightarrow 0$$

induces a long exact sequence in koszul homology (see Proposition 3.36 h)

$$\cdots \longrightarrow \mathrm{H}_{i+1}(\underline{x}; M/(y_1)M) \longrightarrow \mathrm{H}_i(\underline{x}; M) \xrightarrow{y_1} \mathrm{H}_i(\underline{x}; M) \longrightarrow \mathrm{H}_i(\underline{x}; M/(y_1)M) \longrightarrow \cdots.$$

Now by Proposition 3.36 e, I kills $\mathrm{H}_i(\underline{x}; M)$, so the multiplication by y_1 map is zero in the long exact sequence above, which must then break into short exact sequences

$$0 \longrightarrow \mathrm{H}_i(\underline{x}; M) \longrightarrow \mathrm{H}_i(\underline{x}; M/(y_1)M) \longrightarrow \mathrm{H}_{i-1}(\underline{x}; M) \longrightarrow 0.$$

We have an exact sequence $y_2, \dots, y_m$ of $m-1$ elements on M inside $(\underline{x})$, so by induction hypothesis

$$\mathrm{H}_{n-i+1}(\underline{x}; M/(y_1)M) = 0 \text{ for all } i = 1, \dots, m-1$$

and

$$\mathrm{H}_{n-m+1}(\underline{x}; M/(y_1)M) \cong \mathrm{Ext}^{m-1}_R(R/I, M/y_1M).$$

Therefore, for all $i \leqslant m-1$,

$$0 \longrightarrow \mathrm{H}_{n-i+1}(\underline{x}; M) \longrightarrow \underbrace{\mathrm{H}_{n-i+1}(\underline{x}; M/(y_1)M)}_{0} \longrightarrow \mathrm{H}_{n-i}(\underline{x}; M) \longrightarrow 0.$$

This implies $\mathrm{H}_{n-i+1}(\underline{x}; M) = 0$ for all $i = 1, \dots, m$. Moreover, we have a short exact sequence

$$0 \longrightarrow \underbrace{\mathrm{H}_{n-m+1}(\underline{x}; M)}_{0} \longrightarrow \mathrm{H}_{n-m+1}(\underline{x}; M/(y_1)M) \longrightarrow \mathrm{H}_{n-m}(\underline{x}; M) \longrightarrow 0.$$

so

$$\mathrm{H}_{n-m}(\underline{x}; M) \cong \mathrm{H}_{n-m+1}(\underline{x}; M/(y_1)M) \cong \mathrm{Ext}^{m-1}_R(R/I, M/y_1M).$$

Finally, we claim that $\mathrm{Ext}^m_R(R/I, M) \cong \mathrm{Ext}^{m-1}_R(R/I, M/(y_1)M)$. For that purpose, consider the long exact sequence on $\mathrm{Ext}^i_R(R/I, -)$ induced by the short exact sequence

$$0 \longrightarrow M \xrightarrow{y_1} M \longrightarrow M/(y_1)M \longrightarrow 0,$$

which looks like

$$\cdots \longrightarrow \mathrm{Ext}^i_R(R/I, M) \xrightarrow{y_1} \mathrm{Ext}^i_R(R/I, M) \longrightarrow \mathrm{Ext}^i_R(R/I, M/(y_1)M) \longrightarrow \cdots.$$

We do have a regular sequence on M of length m inside I, so $\operatorname{depth}_I(M) \geqslant m$. Therefore, $\operatorname{Ext}_R^{m-1}(R/I, M) = 0$ by Theorem 3.81. By Lemma 3.79, multiplication by y_1 on $\operatorname{Ext}_R^i(R/I, M)$ is the zero map, since $y_1 \in I$, so we get an exact sequence

$$0 \longrightarrow \operatorname{Ext}_R^{m-1}(R/I, M/(y_1)M) \longrightarrow \operatorname{Ext}_R^m(R/I, M) \longrightarrow 0.$$

Therefore,

$$\operatorname{Ext}_R^m(R/I, M) \cong \operatorname{Ext}_R^{m-1}(R/I, M/(y_1)M),$$

which finishes our proof. □

Remark 3.83. If $I = (x_1, \ldots, x_n)$ and $\operatorname{depth}_I(M) = n$, then by Theorem 3.82 the Koszul complex $K(\underline{x}; M)$ must be exact. This does not necessarily say that $\underline{x}$ is a regular sequence, only that there exists some regular sequence on M of length n inside I. However, that implication does hold in the local or graded setting, by Theorem 3.44.

We now have all the tools we need to prove a very useful formula relating depth and projective dimension.

Theorem 3.84 (Auslander—Buchsbaum Formula)**.** *Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring and $M \neq 0$ a finitely generated R-module of finite projective dimension. Then*

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

Proof. Suppose $\operatorname{depth}(R) = 0$. In that case, the claim is that $\operatorname{pdim}_R(M) = \operatorname{depth}(M) = 0$. First, note that the fact that $\operatorname{depth}(R) = 0$ implies immediately that $\mathfrak{m} \in \operatorname{Ass}(R)$, by Lemma 3.78, so $\mathfrak{m}$ kills some nonzero $r \in R$. Consider a minimal free resolution for M, say

$$0 \longrightarrow F_n \xrightarrow{\varphi_n} F_{n-1} \xrightarrow{\varphi_{n-1}} \cdots \longrightarrow F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0.$$

Suppose $n > 0$, so that $\varphi_n \neq 0$. By minimality, $\varphi_n(F_n) \subseteq \mathfrak{m}F_{n-1}$, so $\varphi_n(r, 0, \cdots, 0) = r\varphi_n(1, 0, \cdots, 0) \in r\mathfrak{m} = 0$, so φ_n is not injective. This is a contradiction, so we must have $n = 0$, and M is free, say $M \cong R^n$. Therefore, $\operatorname{pdim}_R(M) = 0$ and $\operatorname{depth}(M) = \operatorname{depth}(R^n) = \operatorname{depth}(R) = 0$.

Now assume that $\operatorname{depth}(M) = 0$. Set $t := \operatorname{depth}(R)$, and fix a maximal regular sequence $x_1, \ldots, x_t \in \mathfrak{m}$. By Corollary 3.63, $\operatorname{pdim}_R(R/(x_1, \ldots, x_t)) = t$. Our goal is to show that that $n := \operatorname{pdim}_R(M) = \operatorname{depth}(R) = t$. Notice that $\operatorname{Tor}_i^R(R/(x_1, \ldots, x_t), M)$ can be computed via minimal free resolutions for either M or $R/(x_1, \ldots, x_t)$, so it vanishes for $i > \min\{t, n\}$. We are going to show that both $\operatorname{Tor}_t^R(R/(x_1, \ldots, x_t), M) \neq 0$ and $\operatorname{Tor}_n^R(R/(x_1, \ldots, x_t), M) \neq 0$, which proves that $\operatorname{depth}(R) = t = n = \operatorname{pdim}_R(M)$.

The Koszul complex is a minimal free resolution for $R/(x_1, \ldots, x_t)$, by Corollary 3.63, so the last map in the minimal free resolution looks like

$$0 \longrightarrow R \xrightarrow{\begin{pmatrix} x_1 & -x_2 & x_3 & \cdots & (-1)^{n+1}x_n \end{pmatrix}^T} R^t$$

so applying $- \otimes_R M$ gives

$$0 \longrightarrow M \xrightarrow{\begin{pmatrix} x_1 & -x_2 & x_3 & \cdots & (-1)^{n+1}x_n \end{pmatrix}^T} M^t.$$

Therefore,

$$\operatorname{Tor}_t^R(R/(x_1,\dots,x_t),M) = \bigcap_{i=1}^{t} \ker(M \xrightarrow{\pm x_i} M).$$

Our assumption that $\operatorname{depth}(M) = 0$ says that there are no regular elements on M, so by Lemma 3.78, $\mathfrak{m} \in \operatorname{Ass}(M)$. Therefore, there exists a nonzero element $m \in M$ such that $\operatorname{ann}(m) = \mathfrak{m} \supseteq (x_1,\dots,x_t)$, so $\operatorname{Tor}_t^R(R/(x_1,\dots,x_t),M) \neq 0$.

On the other hand, to compute $\operatorname{Tor}_n^R(R/(x_1,\dots,x_t),M)$ we can take a minimal free resolution of M, say

$$0 \longrightarrow R^{\beta_n} \xrightarrow{\varphi_n} R^{\beta_{n-1}} \xrightarrow{\varphi_{n-1}} \cdots \longrightarrow R^{\beta_1} \xrightarrow{\varphi_1} R^{\beta_0} \xrightarrow{\varphi_0} M \longrightarrow 0,$$

and apply $- \otimes_R M$, so that $\operatorname{Tor}_n^R(R/(x_1,\dots,x_t),M)$ is the kernel of

$$(R/(x_1,\dots,x_t))^{\beta_n} \longrightarrow (R/(x_1,\dots,x_t))^{\beta_{n-1}}.$$

Our assumption that $x_1,\dots,x_t$ is a maximal regular sequence on R implies that any other element in R is a zerodivisor on $R/(x_1,\dots,x_t)$, and $\operatorname{depth}(R/(x_1,\dots,x_t)) = 0$. In particular, $\mathfrak{m} \in \operatorname{Ass}(R/(x_1,\dots,x_t))$, so there exists some $r \notin (x_1,\dots,x_t)$ such that $\mathfrak{m}r \subseteq (x_1,\dots,x_t)$. The map

$$(R/(x_1,\dots,x_t))^{\beta_n} \longrightarrow (R/(x_1,\dots,x_t))^{\beta_{n-1}}$$

is given by multiplication by a matrix whose entries are all in $\mathfrak{m}$, so its kernel is nonzero, meaning $\operatorname{Tor}_n^R(R/(x_1,\dots,x_t),M) \neq 0$.

So we have shown the theorem holds in two situations: when $\operatorname{depth}(R) = 0$ and when $\operatorname{depth}(M) = 0$. So now we assume that both $t := \operatorname{depth}(R) > 0$ and $n := \operatorname{depth}(M) > 0$, and assume we have shown the theorem holds when $\operatorname{depth}(R) \leqslant t-1$ and $\operatorname{depth}(M) \leqslant n-1$.

By Prime Avoidance, Theorem B.1, we can find $r \in \mathfrak{m}$ that avoids both the associated primes of M and R, so r is both regular on M and on R. In particular, $\operatorname{pdim}_R(R/(x)) = 1$, by Corollary 3.63, so $\operatorname{Tor}_i^R(R/(x),M) = 0$ for all $i \geqslant 2$. Let

$$0 \longrightarrow R^{\beta_n} \xrightarrow{\varphi_n} R^{\beta_{n-1}} \xrightarrow{\varphi_{n-1}} \cdots \longrightarrow R^{\beta_1} \xrightarrow{\varphi_1} R^{\beta_0} \xrightarrow{\varphi_0} M \longrightarrow 0$$

be a minimal free resolution for M. In particular, if we choose basis for each R^{β_i}, the entries in the matrices representing φ_i are all in $\mathfrak{m}$. Applying $- \otimes_R R/(x)$, we get a complex

$$0 \longrightarrow (R/(x))^{\beta_n} \longrightarrow (R/(x))^{\beta_{n-1}} \longrightarrow \cdots \longrightarrow (R/(x))^{\beta_0} \longrightarrow M/xM \longrightarrow 0$$

which is exact at $M \otimes_R R/(x) \cong M/xM$, since tensor is right exact, and whose homology is otherwise given by $\operatorname{Tor}_i^R(R/(x),M)$. In particular, our complex is exact for all $i \geqslant 2$, since we have seen that $\operatorname{Tor}_i^R(R/(x),M) = 0$ for all $i \geqslant 2$. The only remaining possibly interesting homology is given by

$$\operatorname{Tor}_1^R(R/(x),M) = \operatorname{H}_1(M \otimes (0 \to R \xrightarrow{x} R \to 0)) = \operatorname{H}_1(0 \to M \xrightarrow{x} M \to 0) = (0 :_M x).$$

By assumption, x is regular on M, so $\operatorname{Tor}_1^R(R/(x),M) = (0 :_M x) = 0$. So the complex above is exact, and thus a free resolution for M/xM over $R/(x)$. In fact, the maps in this is free

resolution for M/xM were obtained by tensoring φ with $R/(x)$, so we can obtain matrices representing each map by taking the matrix representing φ_i and setting all the entries in (x) equal to 0. In particular, all the entries are still in $\mathfrak{m}/(x)$, and our resolution for M/xM over $R/(x)$ is minimal. This shows that $\operatorname{pdim}_{R/(x)}(M/xM) = \operatorname{pdim}_R(M)$.

Now notice that we picked x to be regular on M, so that $\operatorname{depth}(M/xM) = \operatorname{depth}(M) - 1$. Similarly, x is regular on R, so $\operatorname{depth}(R/(x)) = \operatorname{depth}(R) - 1$. Using our assumption, we conclude that

$$\begin{aligned} &\operatorname{depth}(M/x) + \operatorname{pdim}_{R/(x)}(M/xM) = \operatorname{depth}(R/(x)) \\ \Leftrightarrow\ &\operatorname{depth}(M) - 1 + \operatorname{pdim}_R(M) = \operatorname{depth}(R) - 1 \\ \Leftrightarrow\ &\operatorname{depth}(M) + \operatorname{pdim}_R(M) = \operatorname{depth}(R). \end{aligned}$$

□

This formula is very useful. For example, when doing explicit computations, it is often easier to compute a minimal free resolution for M than to compute its depth. If we happen to know $\operatorname{depth}(R)$, one can deduce $\operatorname{depth}(M)$ by computing $\operatorname{pdim}_R(M)$.

Remark 3.85. One of the consequences of Theorem 3.84 is that if a finitely generated R-module M has finite projective dimension, then $\operatorname{pdim}_R(M) \leqslant \operatorname{depth}(R) \leqslant \dim R$.

We close this section with an easy fact about depth.

Lemma 3.86. *Let $(R, \mathfrak{m})$ be a Noetherian local ring and M a finitely generated R-module. Given any ideal I in R, $\operatorname{depth}_I(M) = \operatorname{depth}_{\sqrt{I}}(M)$.*

Proof. On the one hand, $I \subseteq \sqrt{I}$, so $\operatorname{depth}_I(M) \leqslant \operatorname{depth}_{\sqrt{I}}(M)$. On the other hand, if $x_1, \ldots, x_n$ is a maximal regular sequence on M inside $\sqrt{I}$, then there exists $a_1, \ldots, a_n > 0$ such that $x_1^{a_1}, \ldots, x_n^{a_n} \in I$, but by Lemma 3.47 $x_1^{a_1}, \ldots, x_n^{a_n}$ is a regular sequence on M. □

3.7 Cohen-Macaulay rings

> Life is really worth living in a Noetherian ring R when all the local rings have the property that every system of parameters is an R-sequence. Such a ring is called Cohen-Macaulay (C-M for short).
>
> (Mel Hochster, page 887 of [Hoc78])

Cohen-Macaulay rings, named after Irvin Cohen and Francis Macaulay, two big influences in the early days of commutative algebra, are by some measure the largest class of nice rings commutative algebraists study. They are on the border of being just nice enough to make life is easier, and just broad enough to contain many interesting examples. One of the main reference books in any commutative algebraist's shelf is dedicated to Cohen-Macaulay rings specifically [BH93]. In this section, we will see some of the reasons why life really is worth living in a Cohen-Macaulay ring.

Given a local ring R,

$$\operatorname{depth}(R) \leqslant \dim(R) \leqslant \operatorname{embdim}(R).$$

When the second inequality is an equality, we have a regular ring. When the first inequality is an equality, our ring is Cohen-Macaulay.

Definition 3.87. A Noetherian local ring R is **Cohen-Macaulay** if $\operatorname{depth}(R) = \dim(R)$. More generally, an R-module M is **Cohen-Macaulay** if $\operatorname{depth}(M) = \dim(M)$. A Noetherian ring R is **Cohen-Macaulay** if $R_{\mathfrak{m}}$ is Cohen-Macaulay for every maximal ideal $\mathfrak{m}$.

Example 3.88.

a) Every regular ring is Cohen-Macaulay, since our homological characterization of regular local rings, Theorem 3.70, says that the maximal ideal is generated by a regular sequence of dimension many elements.

b) Every Artinian ring is Cohen-Macaulay: since we always have $\dim(R) \geqslant \operatorname{depth}(R)$, having $\dim(R) = 0$ automatically implies $\operatorname{depth}(R) = 0$.

c) Every 1-dimensional domain is Cohen-Macaulay, since any nonzero nonunit is a regular element.

d) The ring $k[x]/(x^2)$ is Cohen-Macaulay because it has dimension 0, but it is not regular, since 0-dimensional regular rings must be fields; in fact, the embedding dimension of $k[x]/(x^2)$ is 1.

e) We claim that the local ring $R = k[\![x, y, z]\!]/(xy, xz)$ is not Cohen-Macaulay. First, we compute its dimension: since (x) is the unique minimal prime over (xy, xz) in $k[\![x, y, z]\!]$, by Theorem 3.20 we have $\dim(R) = \dim(k[\![x, y, z]\!]) - \operatorname{ht}(xy, xz) = 3 - 1 = 2$. So for R to be Cohen-Macaulay, we must be able to find a regular sequence of length 2 in R. To find one regular element, we need to find an element in R that is not a unit and not in any associated prime of R: the associated primes of (xy, xz) in $k[\![x, y, z]\!]$ are (x) and (y, z), so we can take for example $x - y$. Now $R/(x - y) \cong k[\![x, z]\!]/(x^2, xz)$, and the unique maximal ideal (x, y, z) of R is associated to $R/(x - y)$: it is the annihilator of x, since $x^2 = 0$, $xz = 0$, and $yx = x^2 = 0$. As we saw in Lemma 3.78, this means that there are no elements on R that are regular on $R/(x - y)$, so we conclude that $x - y$ is a maximal regular sequence on R, and $\operatorname{depth}(R) = 1$. Since R is 2-dimensional, R is not Cohen-Macaulay.

   We could have concluded this ring is not Cohen-Macaulay by noting that it is not equidimensional, which as we will see is a property shared by all Cohen-Macaulay rings.

Many rings with *nice* singularities are Cohen-Macaulay. For example, Hochster and Roberts famously showed [HR74] that the ring of invariants of any finite group G over a field k of characteristic not dividing $|G|$ is Cohen-Macaulay. Their proof used prime characteristic techniques, introducing what is now a very important class of characteristic p singularities, and are essentially homological in nature.

Remark 3.89. Given a Noetherian local ring $(R, \mathfrak{m})$, we can decide whether R is Cohen-Macaulay by computing $\dim(R)$ and $\operatorname{depth}(R)$. By Theorem 3.81, we can compute $\operatorname{depth}(R)$ by finding the smallest i such that $\operatorname{Ext}^i_R(R/\mathfrak{m}, R) \neq 0$. On the other hand, if R can easily be seen to be regular, then we can immediately conclude R is Cohen-Macaulay. The easiest way to decide whether a given regular local ring is regular is by finding $\mu(\mathfrak{m})$ and to compare its size to $\dim(R)$.

To compute the depth of a finitely generated R-module M over a Cohen-Macaulay local ring $(R, \mathfrak{m})$, we can start by computing a minimal free resolution of M. If $\operatorname{pdim}_R(M) < \infty$, then the Auslander–Buchsbaum formula tells us that

$$\operatorname{depth}(M) = \operatorname{depth}(R) - \operatorname{pdim}_R(M) = \dim(R) - \operatorname{pdim}_R(M).$$

If R is not Cohen-Macaulay, we need to also compute $\operatorname{depth}(R)$, which we can do for example by finding the smallest i such that $\operatorname{Ext}^i_R(R/\mathfrak{m}, R) \neq 0$, or by explicitly constructing a maximal regular sequence as in Construction 3.77. If $\operatorname{pdim}_R(M) = \infty$, then Theorem 3.84 does not apply, and we need to explicitly find $\operatorname{depth}(M)$, for example by finding the smallest i such that $\operatorname{Ext}^i_R(R/\mathfrak{m}, M) \neq 0$, or by explicitly constructing a maximal regular sequence as in Construction 3.77.

Hochster's quote in the beginning of this section pointed us to an equivalent characterization of Cohen-Macaulayness, for which we will need to recall the notion of a system of parameters.

Definition 3.90. A sequence of d elements $x_1, \dots, x_d$ in a d-dimensional noetherian local ring $(R, \mathfrak{m})$ is a **system of parameters** or **SOP** if $\sqrt{(x_1, \dots, x_d)} = \mathfrak{m}$. If k is a field, a sequence of d homogeneous elements $x_1, \dots, x_d$ in a d-dimensional $\mathbb{N}$-graded finitely generated k-algebra R, with $R_0 = k$, is a *homogeneous system of parameters* if $\sqrt{(x_1, \dots, x_d)} = R_+$.

We say that elements $x_1, \dots, x_t$ are **parameters** if they are part of a system of parameters; this is a property of the set, not just the elements.

Lemma 3.91. *Let R be a Noetherian ring, and I be an ideal. Let $f_1, \dots, f_t \in I$, and $J_i = (f_1, \dots, f_i)$ for each i. Suppose that for each i,*

$$f_i \notin \bigcup_{\substack{\mathfrak{a} \in \operatorname{Min}(J_{i-1}) \\ \mathfrak{a} \notin V(I)}} \mathfrak{a}.$$

Then any minimal prime of J_i either contains I or has height i.

Proof. We use induction on i. For $i = 0$, $J_0 = (0)$, and every minimal prime has height zero. Suppose know the statement holds for $i = m$, and consider a minimal prime $\mathfrak{q}$ of J_{m+1}. Since $J_m \subseteq J_{m+1}$, $\mathfrak{q}$ must contain some minimal prime of J_m, say $\mathfrak{p}$. If $\mathfrak{p} \supseteq I$, then $\mathfrak{q} \supseteq I$. If $\mathfrak{q}$ does not contain I, then neither does $\mathfrak{p}$. On the one hand, $f_{m+1} \in J_{m+1} \subseteq \mathfrak{q}$. On the other hand, since $\mathfrak{p} \in \operatorname{Min}(J_m)$ and $\mathfrak{p} \notin V(I)$, our assumption implies that $f_{m+1} \notin \mathfrak{p}$. In particular, $\mathfrak{p} \subsetneq \mathfrak{q}$. By the induction hypothesys, $\mathfrak{p}$ has height m, and thus the height of $\mathfrak{q}$ is at least $m + 1$. But J_{m+1} is generated by $m + 1$ elements, so by the Krull Height Theorem 3.11, the height of $\mathfrak{q}$ is then exactly $m + 1$. □

Theorem 3.92. *Let R be a Noetherian ring of dimension d.*

a) If $\mathfrak{p}$ is a prime of height h, then there are h elements $f_1, \dots, f_h \in \mathfrak{p}$ such that $\mathfrak{p}$ is a minimal prime of $(f_1, \dots, f_h)$.

b) Suppose that R is either a local ring or an $\mathbb{N}$-graded ring with R_0 a field. Let I is an ideal in R, homogeneous in the graded case. There are d elements, which can be chosen to be homogeneous in the graded case, say $f_1, \dots, f_d \in I$, such that $\sqrt{I} = \sqrt{(f_1, \dots, f_d)}$.

Proof. We will use the notation from the previous lemma.

a) If $\mathfrak{p}$ is a minimal prime in R, then $\mathfrak{p}$ is minimal over the ideal generated by 0 elements, (0). Otherwise, we will use the recipe from the lemma above with $I = \mathfrak{p}$. First, we need to show that we can choose h elements satisfying the hypotheses. So we will show that starting from $J_0 = (0)$, we can find elements $f_1, \dots, f_h \in p$ such that $J_i = (f_1, \dots, f_i)$

$$\mathfrak{p} \not\subseteq \bigcup_{\substack{\mathfrak{a} \in \operatorname{Min}(J_i) \\ \mathfrak{a} \not\in V(I)}} \mathfrak{a}$$

for $i = 0, \dots, h-1$. As long as the set on the right is nonempty,

$$(f_1, \dots, f_i) \subseteq \bigcup_{\substack{\mathfrak{a} \in \operatorname{Min}(J_i) \\ \mathfrak{a} \not\in V(I)}} \mathfrak{a},$$

so the previous statement allows us to choose f_{i+1} as in the Lemma. So fix any $i \leqslant h-1$, and suppose we have constructed J_i. The Krull Height Theorem 3.11 implies that all the elements in $\operatorname{Min}(J_i)$ have height strictly less than h. Since $\mathfrak{p}$ has height h, that implies that the sets $\operatorname{Min}(J_i)$ and $V(\mathfrak{p})$ are disjoint. So we want to show that

$$\mathfrak{p} \not\subseteq \bigcup_{\substack{\mathfrak{a} \in \operatorname{Min}(f_1, \dots, f_i) \\ \mathfrak{a} \not\in V(I)}} \mathfrak{a} = \bigcup_{\mathfrak{a} \in \operatorname{Min}(f_1, \dots, f_i)} \mathfrak{a}$$

This is immediate by prime avoidance B.1, again because $\mathfrak{p}$ is not contained in a minimal prime of $(f_1, \dots, f_i)$. Thus, we can choose $(f_1, \dots, f_h) \subseteq \mathfrak{p}$ as in the lemma, and by the lemma its minimal primes either have height h or contain $\mathfrak{p}$. Since $(f_1, \dots, f_h) \subseteq \mathfrak{p}$, some minimal prime $\mathfrak{q}$ of J_h is contained in $\mathfrak{p}$. We know that this $\mathfrak{q}$ either contains $\mathfrak{p}$, and hence is $\mathfrak{p}$, or else is contained in and has the same height as $\mathfrak{p}$, so again must be equal to $\mathfrak{p}$. Therefore, $\mathfrak{p}$ is a minimal prime of $(f_1, \dots, f_h)$.

b) We again run the same argument, using homogeneous prime avoidance in the graded case. The point is that the only (homogeneous, in the graded case) ideal of height d already contains I. □

By Theorem 3.92, every local (or graded) ring admits a system of parameters, and these can be useful in characterizing the dimension of a local Noetherian ring, or the height of a prime in a Noetherian ring. Moreover, we can characterize Cohen-Macaulayness in terms of sops.

Theorem 3.93. *The following are equivalent for any Notherian local ring* $(R, \mathfrak{m})$*:*

a) R is Cohen-Macaulay.

b) Some system of parameters in R is a regular sequence on R.

c) Every system of parameters in R is a regular sequence on R.

Proof. Clearly, c $\Rightarrow$ b $\Rightarrow$ a. Suppose R is Cohen-Macaulay and let $\underline{x} = x_1, \ldots, x_d$ be a system of parameters on R, meaning $\sqrt{(\underline{x})} = \mathfrak{m}$. By Lemma 3.86, $\operatorname{depth}_{(\underline{x})}(R) = \operatorname{depth}_{\mathfrak{m}}(R) = d$. By Theorem 3.82, $K(\underline{x})$ is exact, and by Theorem 3.44, this implies that $\underline{x}$ is a regular sequence. □

To prove some other nice properties of Cohen-Macaulay rings, we will need the following technical looking result.

Theorem 3.94. *Let $(R, \mathfrak{m})$ be a Noetherian local ring and M and N finitely generated R-modules. Then $\operatorname{Ext}^i_R(M, N) = 0$ for all $i < \operatorname{depth}(N) - \dim(M)$.*

Proof. First, we reduce to the case when $M = R/P$ for some prime ideal P. To do that, fix a prime filtration of M; such a filtration is well-known to exist. More precisely, this is an ascending chain of submodules

$$0 = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n = M$$

such that $M_i/M_{i-1} \cong R/P_i$ for some primes P. First, we claim that we can reduce the problem to showing $\operatorname{Ext}^j_R(R/P_i, N) = 0$ for all $j < \operatorname{depth}(N) - \dim(M)$ and all i.

Break this filtration into short exact sequences

$$0 \longrightarrow M_{i-1} \longrightarrow M_i \longrightarrow R/P_i \longrightarrow 0$$

and look at the long exact sequence we get when we apply $\operatorname{Hom}_R(-, N)$:

$$\cdots \longrightarrow \operatorname{Ext}^j_R(R/P_i, N) \longrightarrow \operatorname{Ext}^j_R(M_i, N) \longrightarrow \operatorname{Ext}^j_R(M_{i-1}, N) \longrightarrow \cdots .$$

If $\operatorname{Ext}^j_R(R/P_i, N) = 0$ for all i, then we must have $\operatorname{Ext}^j_R(M_i, N) = 0$ for all i, and therefore $\operatorname{Ext}^j_R(M, N) = 0$.

So we have reduced the problem to showing that $\operatorname{Ext}^j_R(R/P_i, N) = 0$ for all i and all $j < \operatorname{depth}(N) - \dim(M)$. Notice also that by the construction of the prime filtration, all the P_i contain $\operatorname{ann}(M)$, so $\dim(R/P_i) \leqslant \dim(M)$. Therefore, it is sufficient to show that if P is prime, then $\operatorname{Ext}^i_R(R/P, N) = 0$ for all $i < \operatorname{depth}(N) - \dim(R/P)$.

We proceed by induction on $\dim(R/P)$. If $\dim(R/P) = 0$, then $P = \mathfrak{m}$, so by Theorem 3.81 we have $\operatorname{Ext}^i_R(R/\mathfrak{m}, N) = 0$ for all $i < \operatorname{depth}(N) = \operatorname{depth}(N) - \dim(R/P)$. If $\dim(R/P) > 0$, the $P \neq \mathfrak{m}$, so pick $x \in \mathfrak{m}$ but $x \notin P$. The short exact sequence

$$0 \longrightarrow R/P \xrightarrow{x} R/P \longrightarrow R/P + (x) \longrightarrow 0$$

gives rise to the long exact sequence

$$\cdots \longrightarrow \operatorname{Ext}^i_R(R/P + (x), N) \longrightarrow \operatorname{Ext}^i_R(R/P, N) \xrightarrow{x} \operatorname{Ext}^i_R(R/P, N) \longrightarrow \operatorname{Ext}^i_R(R/P + (x), N) \longrightarrow \cdots .$$

Since $x \notin P$, we necessarily have $\dim(R/P + (x)) < \dim(R/P)$, so by induction hypothesis we have $\operatorname{Ext}^i_R(R/P + (x), N) = 0$ for all

$$i < \operatorname{depth}(N) - \dim(R/P + (x)) = \operatorname{depth}(N) - \dim(R/P) + 1.$$

Therefore, for all $i < \operatorname{depth}(N) - \dim(R/P)$,

$$\operatorname{Ext}^i_R(R/P, N) \xrightarrow{x} \operatorname{Ext}^i_R(R/P, N)$$

is an isomorphism. In particular, $\operatorname{Ext}^i_R(R/P, N) = x \cdot \operatorname{Ext}^i_R(R/P, N)$, so $\operatorname{Ext}^i_R(R/P, N) = 0$ by NAK, where we used that $\operatorname{Ext}^i_R(R/P, N)$ is finitely generated.

It remains to show that $\operatorname{Ext}^i_R(R/P, N) = 0$ when $i < \operatorname{depth}(N) - \dim(R/P)$. □

Corollary 3.95. *Let $(R, \mathfrak{m})$ be a Noetherian local ring and M be a finitely generated R-module. For every associated prime of M, $\operatorname{depth}(M) \leqslant \dim(R/P)$.*

Proof. By Theorem 3.94, $\operatorname{Ext}^i_R(R/P, M) = 0$ for all $i < \operatorname{depth}(M) - \dim(R/P)$. But every element in P is a zerodivisor on M, so $\operatorname{depth}_P(M) = 0$, and by Theorem 3.81, $\operatorname{Ext}^0_R(R/P, M) \neq 0$. We conclude that $\operatorname{depth}(M) \leqslant \dim(R/P)$. □

One of the nicest properties all Cohen-Macaulay rings have is called unmixedness.

Theorem 3.96 (Unmixedness theorem)**.** *Let R be a Noetherian local ring. If M is a Cohen-Macaulay R-module, then*

$$\operatorname{depth}(M) = \dim(R/\mathfrak{p})$$

for every $\mathfrak{p} \in \operatorname{Ass}(M)$. In particular, if R is a Cohen-Macaulay ring, then R has no embedded primes, and $\dim(R/\mathfrak{p}) = \dim(R)$ for each $\mathfrak{p} \in \operatorname{Min}(R)$.

Proof. This follows from the inequality on depth and dimension of associated primes from Corollary 3.95:

$$\dim(M) = \max\{\dim(R/\mathfrak{p}) \mid \mathfrak{p} \in \operatorname{Ass}(M)\} \geqslant \min\{\dim(R/\mathfrak{p}) \mid \mathfrak{p} \in \operatorname{Ass}(M)\} \geqslant \operatorname{depth}(M).$$

Since M is Cohen-Macaulay, equality holds throughout, and that implies in fact that equality holds for each $\dim(R/\mathfrak{p})$ with $\mathfrak{p} \in \operatorname{Ass}(M)$. □

The Cohen-Macaulay property localizes.

Theorem 3.97. *Let $(R, \mathfrak{m})$ be a Cohen-Macaulay local ring and P be a prime ideal in R. Then R_P is a Cohen-Macaulay local ring.*

Proof. We claim that there is a regular sequence contained in R of length equal to the height of P. If P is minimal, there is nothing to show. If P is not minimal, it is not contained in the union of the minimal primes, hence not in the union of the associated primes of R by Theorem 3.96. Thus, there is a nonzerodivisor in P. We can mod out by this to get a Cohen-Macaulay ring of lower dimension, and inductively, the claim follows. Now localizing at P this stays a regular sequence that is a system of parameters for R_P. □

Theorem 3.98 (Dimension formula)**.** *Let R be a Cohen-Macaulay ring, and $\mathfrak{p} \subseteq \mathfrak{q}$ be primes. Then*

$$\operatorname{ht}(\mathfrak{q}) - \operatorname{ht}(\mathfrak{p}) = \dim(R_{\mathfrak{q}}/\mathfrak{p}R_{\mathfrak{q}}).$$

In particular, if $(R, \mathfrak{m})$ is a Cohen-Macaulay local ring, then $\dim(R) - \operatorname{height}(\mathfrak{p}) = \dim(R/\mathfrak{p})$.

Proof. Cohen-Macaulayness localizes, by Theorem 3.97, so $R_{\mathfrak{q}}$ is a Cohen-Macaulay local ring of dimension $\operatorname{ht}(\mathfrak{q})$. Pick $h = \operatorname{ht}(\mathfrak{p})$ elements $r_1, \ldots, r_h \in \mathfrak{p}$ that form a regular sequence. Now $R_{\mathfrak{q}}/(r_1, \ldots, r_h)R_{\mathfrak{q}}$ is Cohen-Macaulay, and $\dim(R_{\mathfrak{q}}/(r_1, \ldots, r_h)R_{\mathfrak{q}}) = \dim(R_{\mathfrak{q}}/\mathfrak{p}R_{\mathfrak{q}})$, since $r_1, \ldots, r_h$ is a maximal regular sequence in $\mathfrak{p}$, so $\mathfrak{p}R_{\mathfrak{q}} \in \operatorname{Ass}(R_{\mathfrak{q}}/(r_1, \ldots, r_h)R_{\mathfrak{q}})$. On the other hand, $\dim(R_{\mathfrak{q}}/(r_1, \ldots, r_h)R_{\mathfrak{q}}) = \dim(R_{\mathfrak{q}}) - h$. The equality follows. □

Remark 3.99. If $(R, \mathfrak{m})$ is Cohen-Macaulay and $x_1, \ldots, x_a$ is a regular sequence on R, then we claim that $R/(x_1, \ldots, x_a)$ is also Cohen-Macaulay. On the one hand, $\operatorname{ht}(x_1, \ldots, x_a) = a$ by Theorem 3.48. On the other hand, by Theorem 3.11 all the minimal primes of $R/(x_1, \ldots, x_a)$ have height at most a, so we conclude that all the minimal primes of $R/(x_1, \ldots, x_a)$ have the same height a. By Theorem 3.98, $\dim(R/(x_1, \ldots, x_a)) = \dim(R) - a$. On the other hand, going modulo each x_i decreases the depth by 1, so $\operatorname{depth}(R/(x_1, \ldots, x_a) = \operatorname{depth}(R) - a = \dim(R) - a$.

To help characterize systems of parameters, we we will use the following definition:

Definition 3.100. Let R be a Noetherian ring. A prime $\mathfrak{p}$ of R is *absolutely minimal* if $\dim(R) = \dim(R/\mathfrak{p})$.

An absolutely minimal prime is minimal, since $\dim(R) \geqslant \dim(R/\mathfrak{p}) + \operatorname{height}(\mathfrak{p})$.

Theorem 3.101. *Let $(R, \mathfrak{m})$ be a Noetherian local ring, and $x_1, \ldots, x_t \in \mathfrak{m}$.*

1) $\dim(R/(x_1, \ldots, x_t)) \geqslant \dim(R) - t$.

2) $x_1, \ldots, x_t$ are parameters if and only if $\dim(R/(x_1, \ldots, x_t)) = \dim(R) - t$.

3) $x_1, \ldots, x_t$ are parameters if and only if x_1 is not in any absolutely minimal prime of R and x_i is not contained in any absolutely minimal prime of $R/(x_1, \ldots, x_{i-1})$ for each $i = 2, \ldots, t$.

Proof.

1) If $\dim(R/(x_1, \ldots, x_t)) = s$, then take a system of parameters $y_1, \ldots, y_s$ for $R/(x_1, \ldots, x_t)$, and pull back to R to get $x_1, \ldots, x_t, y_1', \ldots, y_s'$ in R such that the quotient of R modulo the ideal generated by these elements has dimension zero. By Krull's Height Theorem, we get that $t + s \geqslant \dim(R)$.

2) Let $d = \dim(R)$. Suppose first that $\dim(R/(x_1, \ldots, x_t)) = d - t$. Then, there is a SOP $y_1, \ldots, y_{d-t}$ for $R/(x_1, \ldots, x_t)$; lift back to R to get a sequence of d elements $x_1, \ldots, x_t, y_1, \ldots, y_{d-t}$ that generate an $\mathfrak{m}$-primary ideal. This is a SOP, so $x_1, \ldots, x_t$ are parameters.

   On the other hand, if $x_1, \ldots, x_t$, are parameters, extend to a SOP $x_1, \ldots, x_d$. If I is the image of $(x_{t+1}, \ldots, x_d)$ in $R' = R/(x_1, \ldots, x_t)$, we have R'/I is zero-dimensional, hence

has finite length, so $\mathrm{Ass}_{R'}(R'/I) = \{\mathfrak{m}\}$, and I is $\mathfrak{m}$-primary in R'. Thus, $\dim(R')$ is equal to the height of I, which is then $\leqslant d - t$ by Krull height. That is, $\dim(R') \leqslant d - t$, and using the first statement, we have equality.

3) This follows from the previous statement and the observation that $\dim(S/(f)) \lneqq \dim(S)$ if and only if f is not in any absolutely minimal prime of S. □

Lemma 3.102. *Given a Cohen-Macaulay ring R and a regular sequence $x_1, \ldots, x_n$, every associated prime of $(x_1, \ldots, x_n)$ must have height n.*

Proof. We can reduce to the local case, since associated primes localize, $\frac{x_1}{1}, \ldots, \frac{x_n}{1}$ must also be regular on R_P for each $P \in \mathrm{Ass}(x_1, \ldots, x_n)$, and $\mathrm{ht}(P) = \mathrm{ht}(P_P)$.

Now note that $\dim(R/(x_1, \ldots, x_n)) = \dim(R) - n$, by Remark 3.99, so $x_1, \ldots, x_n$ form part of a system of parameters by Theorem 3.101. Let P be an associated prime of $(x_1, \ldots, x_n)$. Then P_P is an associated prime of $(x_1, \ldots, x_n)_P$, by Theorem 1.45, and R_P is Cohen-Macaulay by Theorem 3.97. The images of $x_1, \ldots, x_n$ can be extended to a system of parameters, which by Theorem 3.93 must be a maximal regular sequence. However, every element in P_P is a zerodivisor on $R_P/(x_1, \ldots, x_n)_P$, since P_P is associated to $x_1, \ldots, x_n$, so $x_1, \ldots, x_n$ cannot be extended inside P_P. Thus $\mathrm{depth}(R_P/(x_1, \ldots, x_n)_P) = 0$. By Remark 3.99, $R_P/(x_1, \ldots, x_n)_P$ is Cohen-Macaulay, so it must have dimension 0. Therefore, P is minimal over $(x_1, \ldots, x_n)$.

By Theorem 3.11, $\mathrm{ht}\, P \leqslant n$. By Theorem 3.48, $\mathrm{ht}(P) \leqslant n$, so $\mathrm{ht}(P) = n$. □

Theorem 3.103. *Let R be a Noetherian ring. The following are equivalent:*

1) R is Cohen-Macaulay.

2) Every ideal I in R contains a regular sequence of length $\mathrm{ht}(I)$.

3) Every maximal regular sequence inside I has length $\mathrm{ht}(I)$.

Proof. Notice that 3) ⇒ 2) is obvious, and 2) ⇒ 1) is clear once we take I to be equal to each maximal ideal in R. To show 1) ⇒ 2), let $x_1, \ldots, x_n$ be a maximal regular sequence inside I. The elements of I must all be zerodivisors on $R/(x_1, \ldots, x_n)$, by maximality, so by Lemma 3.78 we must have I contained in some associated prime P of $R/(x_1, \ldots, x_n)$. By Lemma 3.102, P has height n, so $\mathrm{ht}(I) \leqslant \mathrm{ht}(P) = n$. But $I \supseteq (x_1, \ldots, x_n)$ and $\mathrm{ht}(x_1, \ldots, x_n) = n$ by Theorem 3.48, so $\mathrm{ht}(I) = n$. □

Remark 3.104. Let I be an ideal in a Cohen-Macaulay ring R. If I is generated by a regular sequence, then that regular sequence must have length $\mathrm{ht}(I)$, so I must be generated by exactly $\mathrm{ht}(I)$ elements. If R is a local ring and $\mu(I) > \mathrm{ht}(I)$, then I is not generated by a regular sequence.

The most important classes of rings we will consider are

$$\text{Regular rings} \subseteq \text{complete intersections} \subseteq \text{Cohen-Macaulay rings.}$$

We will unfortunately not have a chance to discuss Gorenstein rings, which are a special subclass of Cohen-Macaulay rings that contain all complete intersections.

3.8 A few direct applications to symbolic powers

We now collect some immediate applications of the tools we developed in the remainder of the chapter to associated primes and symbolic powers.

Theorem 3.105. *Let I be an ideal in a noetherian ring R. A prime P is associated to I if and only if* $\operatorname{depth}(R_P/I_P) = 0$. *In particular, if $(R, \mathfrak{m})$ is a local ring, then $\mathfrak{m} \in \operatorname{Ass}(I)$ if and only if* $\operatorname{depth}(R/I) = 0$.

Proof. By Lemma 1.36, $P \in \operatorname{Ass}(I)$ if and only if $P_P \in \operatorname{Ass}_{R_P}(I_P)$. This means we can reduce to the local case, and that it is enough to show that in a local ring $(R, \mathfrak{m})$, $\mathfrak{m} \in \operatorname{Ass}(I)$ if and only if $\operatorname{depth}(R/I) = 0$. If $\mathfrak{m}$ is associated to I, then every element in $\mathfrak{m}$ is a zerodivisor on R/I, so there are no regular elements on R/I, and $\operatorname{depth}(R/I) = 0$. If $\operatorname{depth}(R/I) = 0$, then every element in $\mathfrak{m}$ must be a zerodivisor on R/I, so $\mathfrak{m}$ is contained in the zerodivisors of R/I. By Theorem 1.39, this means that

$$\mathfrak{m} \subseteq \bigcup_{P \in \operatorname{Ass}(I)} P.$$

By Theorem 1.44, this is a union of finitely many primes, so by Prime Avoidance $\mathfrak{m}$ must be contained in some associated prime of I. But $\mathfrak{m}$ is already maximal, so $\mathfrak{m}$ is an associated prime of I. □

Lemma 3.106. *Let $(R, \mathfrak{m})$ be a local ring or an $\mathbb{N}$-graded algebra over a field k with $R_0 \cong k$. Given an ideal I in R, which is homogeneous in the graded setting, if all the associated primes of I have height* $\dim(R) - 1$ *then*

$$I^{(n)} = I^n \text{ if and only if } \operatorname{depth}(R/I^n) > 0$$

for all $n \geqslant 1$.

For example, this applies if I is a prime of height $\dim(R) - 1$.

Proof. In the graded case, recall that all the associated primes of I must be homogeneous, by Theorem 1.44. Since all the associated primes of I have height $\dim(R) - 1$, $\mathfrak{m}$ is the only possible embedded prime of I^n for any n. By Theorem 3.105, $\mathfrak{m}$ is associated to I if and only if $\operatorname{depth}(R/I^n) = 0$. □

And finally, here is a large class of ideals I satisfying $I^{(n)} = I^n$ for all n.

Theorem 3.107. *Let R be a noetherian ring and consider an ideal I. If I is generated by a regular sequence, then $\operatorname{Ass}(I^n) = \operatorname{Ass}(I)$ for all $n \geqslant 1$, and thus $I^{(n)} = I^n$.*

Proof. We will construct a descending chain of ideals

$$I = I_0 \supseteq I_1 \supseteq I_2 \supseteq \cdots$$

containing all the powers of I and such that

$$I_{n+1}/I_n \cong R/I$$

for all n. Given this sequence, the quotient maps

$$R/I_{n+1} \twoheadrightarrow R/I_n$$

all have kernel R/I, giving us short exact sequences

$$0 \longrightarrow R/I \longrightarrow R/I_{n+1} \longrightarrow R/I_n \longrightarrow 0\,.$$

By Lemma 1.40,

$$\operatorname{Ass}(I) \subseteq \operatorname{Ass}(I_{n+1}) \subseteq \operatorname{Ass}(I) \cup \operatorname{Ass}(I_n).$$

When $n = 0$, $I_n = I$, so

$$\operatorname{Ass}(I) \subseteq \operatorname{Ass}(I_1) \subseteq \operatorname{Ass}(I) \cup \operatorname{Ass}(I) \implies \operatorname{Ass}(I_1) = \operatorname{Ass}(I).$$

Proceeding inductively, this shows that $\operatorname{Ass}(I_n) = \operatorname{Ass}(I)$ for all n. In particular, all the powers I^n satisfy $\operatorname{Ass}(I^n) = \operatorname{Ass}(I)$.

So all that remains is to show the key technical point of the proof: the construction of the promised sequence. Let $I = (f_1, \ldots, f_t)$, where $f_1, \ldots, f_t$ is a regular sequence. First, for each n we fix an order for the generators $f_1^{a_1} \cdots f_t^{a_t}$ of I^n; for example, consider the lexicographical order

$$f_{n,0} = f_1^n,\ f_{n,1} = f_1^{n-1} f_2, \cdots, f_{n,t-1} = f_1^{n-1} f_t,\ f_{n,t} = f_1^{n-2} f_2^2, \cdots, f_{n,\binom{n+t-1}{t-1}} = f_t^n.$$

For each $n \geqslant 0$ and $0 \leqslant m \leqslant \binom{n+t-1}{t-1}$, set

$$I_{n,m} := I^{n+1} + (f_{n,k} \mid 0 \leqslant k \leqslant m)\,.$$

By construction, $I_{0,0} = I$, $I_{n,m} \subseteq I_{n,m+1}$, and

$$I_{n,\binom{n+t-1}{t-1}} = I^{n+1} + I^n = I^n = I_{n-1,0}.$$

So these give us a descending chain of ideals

$$I = I_{0,0} = I_{1,t} \supseteq I_{1,t-1} \supseteq \cdots \supseteq I_{1,0} = I^2 = I_{2,\binom{n+1}{t-1}} \supseteq \cdots\,.$$

If we can show that all the successive quotients are isomorphic to R/I, this chain of ideals will have all the promised features. To do that, it's sufficient to show that for all $n \geqslant 1$ and $0 \leqslant m < \binom{n+t-1}{t-1}$,

$$I_{n,m+1}/I_{n,m} \cong R/I.$$

By construction, the quotient $I_{n,m+1}/I_{n,m}$ is a cyclic module, so

$$I_{n,m+1}/I_{n,m} \cong R/(I_{n,m} : I_{n,m+1}).$$

So all that remains to be shown is that $(I_{n,m} : I_{n,m+1}) = I$. One containment is immediate from the construction: since $I_{n,m+1} \subseteq I^{n+1} + I^n$, then

$$I \cdot I_{n,m+1} \subseteq I(I^{n+1} + I^n) \subseteq I^{n+2} + I^{n+1} \subseteq I^{n+1} \subseteq I_{n,m}.$$

Now suppose that $g \in R$ satisfies $gI_{n,m+1} \subseteq I_{n,m}$. This is equivalent to the statement that

$$gf_{n,m+1} \subseteq I_{n,m} = I^{n+1} + (f_{n,k} \mid 0 \leqslant k \leqslant m)\,.$$

Therefore, there exist $r_0, \ldots, r_m \in R$ such that

$$gf_{n,m+1} + r_0 f_{n,0} + \cdots + r_m f_{n,m} \in I^{n+1}.$$

The elements $f_{n,0}, \ldots, f_{n,m+1}$ are distinct monomials in $f_1, \ldots, f_t$ of degree n, so

$$gf_{n,m+1} + r_0 f_{n,0} + \cdots + r_m f_{n,m} = F(f_1, \ldots, f_t)$$

for some homogeneous polynomial of degree n. By Theorem 3.50, the coefficients of F must be in I, so in particular $g \in I$. Since we took g to be any element in $(I_{n,m} : I_{n,m+1})$, we conclude that $(I_{n,m} : I_{n,m+1}) = I$. □

Remark 3.108. What we showed in Theorem 3.107 is that $\operatorname{Ass}(I^n) = \operatorname{Ass}(I)$ for all $n \geqslant 1$ whenever I is generated by a regular sequence. With our definition of symbolic powers, this gives the equality $I^n = I^{(n)}$. Notice, however, that if we choose the other definition of symbolic powers — meaning, by taking $I^n R_P \cap R$ with P ranging over $\operatorname{Min}(I)$ instead of $\operatorname{Ass}(I)$ — we only obtain $I^n = I^{(n)}$ in Cohen-Macaulay rings, since all complete intersections are unmixed in a Cohen-Macaulay ring. If R is not Cohen-Macaulay, we can still say that $I^n = I^{(n)}$ whenever I is a complete intersection with no embedded primes.

Chapter 4

A geometric perspective

The symbolic powers of a radical ideal in $k[x_1, \ldots, x_d]$ have a geometric meaning. To explain that meaning, we will start with a brief recap of affine and projective varieties. For a nice and thorough computationally minded introduction to affine and projective varieties, see [CLO92].

4.1 Affine varieties

Definition 4.1. Given a field k, the **affine d-space over** k, denoted $\mathbb{A}_k^d$, is given by

$$\mathbb{A}_k^d := \{(a_1, \ldots, a_d) \mid a_i \in k\}.$$

For a subset T of $k[x_1, \ldots, x_d]$, we define $\mathbb{V}(T) \subseteq \mathbb{A}_k^d$ to be the set of common zeros or the *zero set* of the polynomials (equations) in T:

$$\mathbb{V}(T) = \{(a_1, \ldots, a_d) \in \mathbb{A}_k^d \mid f(a_1, \ldots, a_d) = 0 \text{ for all } f \in T\}.$$

Whenever we want to emphasize the role of k, we will write this as $\mathbb{V}_k(T)$.

A subset of $\mathbb{A}_k^d$ of the form $\mathbb{V}(T)$ for some subset T is called an **algebraic subset** of $\mathbb{A}_k^d$, or an **affine algebraic variety**. So a variety in $\mathbb{A}_k^d$ is the set of common solutions of some (possibly infinite) collection of polynomial equations. A variety is **irreducible** if it cannot be written as the union of two proper subvarieties.

Note that some authors use the word *variety* to refer only to irreducible algebraic sets; it is always wise to check what definition of variety is being considered. Note also that the definitions given here are only completely standard when k is algebraically closed.

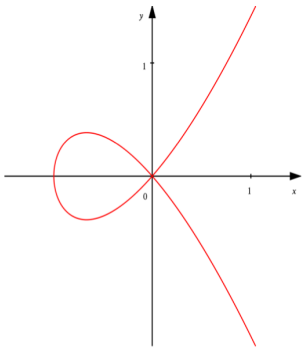
Example 4.2. Here are some simple examples of algebraic varieties:

a) For any field k and elements $a_1, \ldots, a_d \in k$, we have

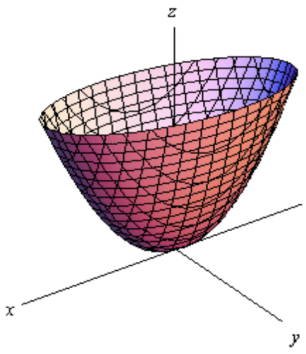
$$\mathbb{V}(x_1 - a_1, \ldots, x_d - a_d) = \{(a_1, \ldots, a_d)\}.$$

So, all one element subsets of $\mathbb{A}_k^d$ are varieties.

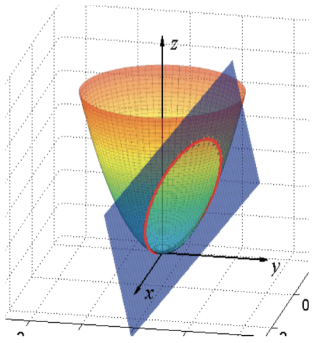
b) For $k = \mathbb{R}$ and $n = 2$, $\mathbb{V}(y^2 + x^2(x-1))$ is a "nodal curve" in $\mathbb{A}^2_{\mathbb{R}}$, the real plane. Note that we have written x for x_1 and y for x_2 here.



c) For $k = \mathbb{R}$ and $n = 3$, $\mathbb{V}(z - x^2 - y^2)$ is a paraboloid in $\mathbb{A}^3_{\mathbb{R}}$, real three space.



d) For $k = \mathbb{R}$ and $n = 3$, $\mathbb{V}(z - x^2 - y^2, 3x - 2y + 7z - 7)$ is a circle in $\mathbb{A}^3_{\mathbb{R}}$.



e) For $k = \mathbb{R}$, $\mathbb{V}_{\mathbb{R}}(x^2 + y^2 + 1) = \emptyset$. Note that $\mathbb{V}_{\mathbb{C}}(x^2 + y^2 + 1) \neq \emptyset$.

We can consider the equations that a subset of affine space satisfies.

Definition 4.3. Given any subset X of $\mathbb{A}_k^d$ for a field k, define

$$\mathbf{I}(X) = \{g(x_1, \ldots, x_d) \in k[x_1, \ldots, x_d] \mid g(a_1, \ldots, a_d) = 0 \text{ for all } (a_1, \ldots, a_d) \in X\}.$$

Exercise 8. $\mathbf{I}(X)$ is an ideal in $k[x_1, \ldots, x_d]$ for any $X \subseteq \mathbb{A}_k^d$.

Remark 4.4. If I is an ideal in $k[x_1, \ldots, x_d]$, $\mathbf{I}(\mathbb{V}(I)) \supseteq I$, but we do not necessarily have equality. For example, when $I = (x^2)$ in $k[x]$, $\mathbb{V}(I) = \{0\}$, and thus $\mathbf{I}(\mathbb{V}(I)) = (x)$.

Example 4.5. The **twisted cubic (affine) curve** is the curve C parametrized by (t, t^2, t^3), meaning it is the image of the map

$$\begin{aligned} \mathbb{R} &\longrightarrow \mathbb{R}^3. \\ t &\longmapsto (t, t^2, t^3) \end{aligned}$$

Consider the ideal $I = (x^2 - y, x^3 - z)$. It is clear that $C \subseteq \mathbb{V}(I)$. On the other hand, given a point $(a, b, c) \in \mathbb{A}_{\mathbb{R}}^3$ in $\mathbb{V}(I)$, it must satisfy $b = a^2$ and $c = a^3$, so $(a, b, c) = (a, a^2, a^3) \in C$. Therefore, C is a variety. To find $\mathbf{I}(C)$, we can get help from Macaulay2:

```
i1 : k = RR;

i2 : R = k[x,y,z];

i3 : f = map(k[t],R,{t,t^2,t^3});

i4 : ker f
              2                   2
o4 = ideal (y  - x*z, x*y - z, x  - y)

o4 : Ideal of R
```

In our computation above, f sets $x = t$, $y = t^2$, and $z = t^3$, and its kernel consists precisely of the polynomials that vanish at every point of this form. We conclude that $\mathbf{I}(C) = (y - x^2, xz - y^2, z - xy)$. Note that computations over the reals in Macaulay2 are experimental, and yet we obtain the correct answer; we can also run the same computation over $k = \mathbb{Q}$.

Exercise 9. Here are some properties of the functions $\mathbb{V}$ and $\mathbf{I}$:

a) For any field, we have $\mathbb{V}(0) = \mathbb{A}_k^n$ and $\mathbb{V}(1) = \emptyset$.

b) $\mathbf{I}(\emptyset) = (1) = k[x_1, \ldots, x_d]$ (the improper ideal).

c) $\mathbf{I}(\mathbb{A}_k^d) = (0)$ if and only if k is infinite.

d) If $I \subseteq J \subseteq k[x_1, \ldots, x_d]$ then $\mathbb{V}(I) \supseteq \mathbb{V}(J)$.

e) If $S \subseteq T$ are subsets of $\mathbb{A}_k^n$ then $\mathbf{I}(S) \supseteq \mathbf{I}(T)$.

f) If $I = (T)$ is the ideal generated by the elements of $T \subseteq k[x_1, \ldots, x_d]$, then $\mathbb{V}(T) = \mathbb{V}(I)$.

So we will talk about the solution set of an ideal, rather than of an arbitrary set. Hilbert's Basis Theorem implies that every ideal in $k[x_1, \ldots, x_d]$ is finitely generated, so any system of equations in $k[x_1, \ldots, x_d]$ can be replaced with a system of *finitely many* equations.

Example 4.6. Let

$$X = \begin{bmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{bmatrix}$$

be a 2×3 matrix of variables — we usually call these *generic* matrices — and let

$$R = k[X] = k\begin{bmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{bmatrix}.$$

Let $\Delta_1, \Delta_2, \Delta_3$ the 2×2-minors of X. Consider the ideal $I = (\Delta_1, \Delta_2, \Delta_3)$. Thinking of these generators as equations, a solution to the system corresponds to a choice of 2×3 matrix whose 2×2 minors all vanish — that is, a matrix of rank at most one. So $\mathbb{V}(I)$ is the set of rank at most one matrices. Note that $I \subseteq (x_1, x_2, x_3) =: J$, and $\mathbb{V}(J)$ is the set of 2×3 matrices with top row zero. The containment $\mathbb{V}(J) \subseteq \mathbb{V}(I)$ we obtain from $I \subseteq J$ translates to the fact that a 2×3 matrix with a zero row has rank at most 1.

Finally, the union and intersection of varieties is also a variety.

Exercise 10. Suppose that I and J are ideals in $k[x_1, \ldots, x_d]$.

a) $\mathbb{V}(I) \cap \mathbb{V}(J) = \mathbb{V}(I + J)$.

b) $\mathbb{V}(I) \cup \mathbb{V}(J) = \mathbb{V}(I \cap J) = \mathbb{V}(IJ)$.

However, note that in general $IJ \neq I \cap J$.

Remark 4.7. We noted in Example 4.2 that a point is a variety. By Exercise 10, the finite union of varieties is a variety, so we conclude that any finite set of points is a variety.

Theorem 4.8 (Weak Nullstellensatz)**.** *Let k be an algebraically closed field. If I is a proper ideal in $R = k[x_1, \ldots, x_d]$, then $\mathbb{V}_k(I) \neq \varnothing$.*

Theorem 4.9 (Strong Nullstellensatz)**.** *Let k be an algebraically closed field, and consider a polynomial ring $R = k[x_1, \ldots, x_d]$. Let $I \subseteq R$ be an ideal. The polynomial f vanishes on $\mathbb{V}_k(I)$ if and only if $f^n \in I$ for some n. Therefore, $\mathbf{I}(\mathbb{V}(I)) = \sqrt{I}$.*

This gives us a bijection between radical ideals and varieties. Given a variety V, $\mathbf{I}(V)$ is the unique radical ideal that determines V.

Definition 4.10. Given a variety $X \subseteq \mathbb{A}^d_k$, the **coordinate ring** of X is the ring

$$k[X] := k[x_1, \ldots, x_d]/\mathbf{I}(X).$$

Theorem 4.11. *Given an an algebraically closed field k, $\mathbf{I}$ and $\mathbb{V}$ induce order-reversing bijections*

$$\begin{array}{cc} \underline{\text{in } K[x_1,\ldots,x_n]} & \underline{\text{in } \mathbb{A}^n_K} \\ \{\text{radical ideals}\} & \{\text{varieties}\} \\ \{\text{prime ideals}\} & \{\text{irreducible varieties}\} \\ \{\text{maximal ideals}\} & \{\text{points}\}. \end{array}$$

In particular, given ideals I and J, we have $\mathbb{V}(I) = \mathbb{V}(J)$ if and only if $\sqrt{I} = \sqrt{J}$. Likewise, for any variety X over an algebraically closed field, we have order-reversing bijections

$$\begin{array}{cc} \underline{\text{in } k[X]} & \underline{\text{in } X} \\ \{\text{radical ideals}\} & \{\text{subvarieties}\} \\ \{\text{prime ideals}\} & \{\text{irreducible subvarieties}\} \\ \{\text{maximal ideals}\} & \{\text{points}\}. \end{array}$$

Example 4.12. In Example 2.4, we showed that the kernel of the map

$$\begin{aligned} \mathbb{C}[x,y,z] &\longrightarrow \mathbb{C}[t^3,t^4,t^5] \\ (x,y,z) &\longmapsto (t^3,t^4,t^5) \end{aligned}$$

is the ideal

$$P = \left(x^3 - yz, y^2 - xz, z^2 - x^2y\right).$$

As a consequence, the set of points

$$X = \left\{(t^3,t^4,t^5) \in \mathbb{A}^3_{\mathbb{C}} \mid t \in \mathbb{C}\right\}$$

satisfies $\mathbf{I}(X) = P$. In fact, we claim that for $k = \mathbb{R}$ or $\mathbb{C}$, the set

$$X = \{(t^3,t^4,t^5) \mid t \in k\}$$

is an algebraic variety, though again it needs justification. Consider $Y = \mathbb{V}(y^3 - x^4, z^3 - x^5)$; clearly, $X \subseteq Y$. Over $\mathbb{R}$, for $(a,b,c) \in Y$, take $t = \sqrt[3]{a}$; then $a = t^3$, $b^3 = a^4$ means $b = \sqrt[3]{a}^4$, so $b = t^4$, and similarly $c = t^5$, so $X = Y$. We were using uniqueness of cube roots in this argument though, so we need to reconsider over $\mathbb{C}$. Indeed, if ω is a cube root of unity, then $(\omega,1,1) \in Y \smallsetminus X$, so we need to do better. Let's try $Z = \mathbb{V}(y^3 - x^4, z^3 - x^5, z^4 - y^5)$. Again, $X \subseteq Z$. Say that $(a,b,c) \in \mathbb{A}^3_{\mathbb{C}}$ are in Z, and let s be a cube root of a. Then $b^3 = a^4 = (s^4)^3$ implies that $b = \omega s^4$ for some cube root of unity ω' (maybe 1, maybe not). Similarly $c^3 = a^4 = (s^5)^3$ implies that $c = \omega'' s^5$ for some cube root of unity ω'' (maybe 1, maybe ω', maybe not). So at least $(a,b,c) = (s^3, \omega' s^4, \omega'' s^5)$. Let $t = \omega' s$. Then $(s^3, \omega' s^4, \omega'' s^5) = (t^3, t^4, \omega s^5)$, where $\omega = (\omega')^2 \omega''$ is again some cube root of unity. The

equation $b^5 = c^4$ shows that $t^{20} = \omega^4 t^{20}$. If $t \neq 0$, this shows $\omega = 1$, so $(a, b, c) = (t^3, t^4, t^5)$; if $t = 0$, then $(a, b, c) = (0, 0, 0) = (0^3, 0^4, 0^5)$. Thus, $X = Z$.

We have shown in particular that

$$X = \{(t^3, t^4, t^5) \mid t \in \mathbb{C}\}$$

is a variety, and that $\mathbf{I}(X) = P$. As we already saw in Example 2.4, P is a prime ideal, since $\mathbb{C}[x, y, z]/P \cong \mathbb{C}[t^3, t^4, t^5] \subseteq \mathbb{C}[t]$ is a domain. Since P is prime, by **??** the variety X is irreducible.

Every radical ideal can be written as the intersection of its finitely many minimal primes, so in particular we can write I uniquely as

$$I = P_1 \cap \cdots \cap P_n$$

where each P_i is a prime ideal and $P_i \nsubseteq P_j$ for each $i \neq j$. In fact, as we discussed in Remark 1.19, this is the unique way to write I as an intersection of finitely many incomparable primes. Translating this into the world of varieties, we obtain the following:

Theorem 4.13. *Every affine variety $V \subseteq \mathbb{A}^d_k$ can be written uniquely as a finite union of irreducible affine varieties $V = V_1 \cup \cdots \cup V_n$ with $V_i \nsubseteq V_j$ for each $i \neq j$,s.*

In summary, over an algebraically closed field, we have the following dictionary between algebra and geometry:

Algebra	$\longleftrightarrow$	Geometry
radical ideals	$\longleftrightarrow$	varieties
prime ideals	$\longleftrightarrow$	irreducible varieties
maximal ideals	$\longleftrightarrow$	points
$(x_1 - a_1, \ldots, x_d - a_d)$	$\longleftrightarrow$	point $\{(a_1, \ldots, a_d)\}$
(0)	$\longleftrightarrow$	variety $\mathbb{A}^d$
$k[x_1, \ldots, x_d]$	$\longleftrightarrow$	variety $\varnothing$
smaller ideals	$\longleftrightarrow$	larger varieties
larger ideals	$\longleftrightarrow$	smaller varieties
sum of ideals	$\longleftrightarrow$	intersection of varieties
intersection of ideals	$\longleftrightarrow$	union of varieties
$I = P_1 \cap \cdots \cap P_k$ unique decomposition into incomparable primes	$\longleftrightarrow$	$V = V_1 \cup \cdots \cup V_k$ unique decomposition into irreducible components

4.2 Projective varieties

Definition 4.14. Given a field k and $d \geqslant 0$, consider the equivalence relation $\sim$ on k^{d+1} given by

$$(a_0, \ldots, a_d) \sim (b_0, \ldots, b_d) \text{ if there exists some } 0 \neq \lambda \in k \text{ such that } b_i = \lambda b_i \text{ for every } i.$$

The **projective d-space over k**, denoted $\mathbb{P}^d_k$, is given by

$$\mathbb{P}^d_k := k^{d+1} / \sim .$$

The class of $(a_0, \ldots, a_d)$ in $\mathbb{P}^d_k$ is denoted $(a_0 : \cdots : a_d)$, and we call it a **point** in $\mathbb{P}^d$. Notice each point in $\mathbb{P}^d_k$ can be represented by many different tuples in k^{d+1}; given a point P in $\mathbb{P}^d_k$, any $(a_0, \ldots, a_d) \in k^{d+1}$ (which we can also think of as a point in $\mathbb{A}^{d+1}_k$) such that $P = (a_0 : \cdots : a_d)$ is a set of **homogeneous coordinates** for P.

Remark 4.15. There is a one to one correspondence between $\mathbb{P}^d_k$ and the set of lines through the origin in k^{n+1}.

Remark 4.16. Here is a typical trick one uses often. Given a point $P = (a_0 : \cdots : a_d)$, we know that at least one of the coordinates a_i must be nonzero, so

$$P = (a_0 : \cdots : a_d) = \left(\frac{a_0}{a_i} : \cdots : \frac{a_i}{a_i} : \cdots : \frac{a_d}{a_i} \right) = \left(\frac{a_0}{a_i} : \cdots : 1 : \cdots : \frac{a_d}{a_i} \right).$$

Therefore, we can always assume that $P = \left(b_0 : \cdots : b_{i-1} : 1 : b_{i+1} : \cdots : \frac{a_d}{a_i} \right)$.

Lemma 4.17. *Let k be a field and $f \in k[x_0, \ldots, x_d]$ be a homogeneous polynomial. Given any nonzero $(a_0, \ldots, a_d) \in k^{d+1}$, if $f(a_0, \ldots, a_d) = 0$ then $f(\lambda a_0, \ldots, \lambda a_d) = 0$ for all nonzero $\lambda \in k$. In particular, the set*

$$V(f) = \left\{ p \in \mathbb{P}^d_k \mid f(p) = 0 \right\}$$

is a well-defined subset of $\mathbb{P}^d_k$.

Proof. If f is homogeneous of degree $d = n$, we can write f as

$$f = \sum_{b_0 + \cdots + b_d = n} c_b x_0^{b_0} \cdots x_d^{b_d}$$

for some $c_b \in k$. Then

$$f(\lambda a_0, \ldots, \lambda a_d) = \sum_{b_0 + \cdots + b_d = n} c_b (\lambda a_0)^{b_0} \cdots (\lambda a_d)^{b_d} = \sum_{b_0 + \cdots + b_d = n} c_b \lambda^n a_0^{b_0} \cdots a_d^{b_d} = \lambda^n f(a_0, \ldots, a_d)$$

so $f(a_0, \ldots, a_d) = 0$ if and only if $f(\lambda a_0, \ldots, \lambda a_d) = 0$ for all λ. □

In contrast, if f is not homogeneous, then the equation $f(p) = 0$ does not make sense in $\mathbb{P}^d_k$.

Definition 4.18. Let $f_1, \ldots, f_n$ be homogeneous polynomials in $R = k[x_0, \ldots, x_d]$, where k is a field. The **projective variety** defined by $f_1, \ldots, f_n$ is

$$\mathbb{V}(f_1, \ldots, f_n) := \{a \in \mathbb{P}^n_k \mid f_i(a) = 0 \text{ for all } 1 \leqslant i \leqslant n\}.$$

A **projective variety** if any subset $V \subseteq \mathbb{P}^d_k$ which can be realized as $V = V(f_1, \ldots, f_n)$ for some $f_1, \ldots, f_n$.

Notation 4.19. If I is a homogeneous ideal in R, we set

$$\mathbb{V}(I) := \left\{p \in \mathbb{P}^d_k \mid f(p) = 0 \text{ for all } f \in I\right\}.$$

We will use the same notation for affine and projective varieties, hoping the distinction is clear from context.

Remark 4.20. Whenever I is a homogeneous ideal in R, I is generated by homogeneous elements, say $f_1, \ldots, f_n$. We claim that $V(I) = V(f_1, \ldots, f_n)$. On the one hand, if $p \in V(I)$ then in particular $f_i(p) = 0$ for all i, so $p \in V(f_1, \ldots, f_n)$. On the other hand, any element $f \in I$ is of the form $f = g_1 f_1 + \cdots g_n f_n$, so if $p \in V(f_1, \ldots, f_n)$ then

$$f(p) = g_1(p)\underbrace{f_1(p)}_{0} + \cdots g_n(p)\underbrace{f_n(p)}_{0} = 0.$$

Therefore, $V(I)$ is a projective variety.

Definition 4.21. Given a projective variety $V \subseteq \mathbb{P}^d_k$,

$$\mathbf{I}(V) := \{f \in k[x_0, \ldots, x_d] \mid f(p) = 0 \text{ for all } p \in V\}.$$

Exercise 11. Let V be a projective variety in $\mathbb{P}^d_k$. If k is infinite, then $\mathbf{I}(V)$ is a homogeneous ideal.

Remark 4.22. When k is finite, there are certain polynomials that are in $\mathbf{I}(V)$ for every variety V. Over $\mathbb{F}_p$, Fermat's Little Theorem implies that $x_0^p - x_0, \ldots, x_d^p - x_d$ vanish at every point in $\mathbb{P}^d_{\mathbb{F}_p}$, but these are not homogeneous polynomials.

Exercise 12.

a) If $I \subseteq J \subseteq k[x_0, \ldots, x_d]$ are homogeneous ideals then $\mathbb{V}(I) \supseteq \mathbb{V}(J)$.

b) If $S \subseteq T$ are subsets of $\mathbb{P}^d_k$ then $\mathbf{I}(S) \supseteq \mathbf{I}(T)$.

Exercise 13. If I is a homogeneous ideal, then $\sqrt{I}$ is also homogeneous.

Remark 4.23. A homogeneous ideal I in $R = k[x_0, \ldots, x_d]$ gives us the projective variety $V = \mathbb{V}(I) \subseteq \mathbb{P}^d_k$, but it also determines the affine variety

$$A = \left\{a \in \mathbb{A}^{d+1}_k \mid f(a) = 0 \text{ for all } f \in I\right\} \subseteq \mathbb{A}^{d+1}_k.$$

If we think of each point in V as corresponding to a line through the origin in affine space, then A is the union of those lines; notice that A includes the origin. In particular, for every point $a = (a_0 : \cdots : a_d) \in V$, whatever the choice of homogeneous coordinates $a_0, \ldots, a_d$, we always have $(a_0, \ldots, a_d) \in A$. This affine variety A is the **affine cone** of V.

Since a lot of the theory of projective varieties appears to be parallel to the theory of affine varieties, we might be expecting a projective version of Nullstellensatz. However, the details are a bit more complicated.

Remark 4.24. Not all homogeneous proper ideals in $k[x_0, \ldots, x_d]$ give rise to non-empty projective varieties. For example, the homogeneous maximal ideal $(x_0, \ldots, x_d)$ in $k[x_0, \ldots, x_d]$ determines an empty variety in $\mathbb{P}_k^d$. Why? One simple way to explain this is to note that the affine variety $\mathbb{V}(x_0, \ldots, x_d)$ is the origin.

Since $(x_0, \ldots, x_d)$ is essentially irrelevant from the perspective of projective varieties, we call it the **irrelevant (maximal) ideal** of $k[x_0, \ldots, x_d]$.

Theorem 4.25 (Projective Weak Nullstellensatz)**.** *Let k be an algebraically closed field and let I be a homogeneous ideal in $R = k[x_0, \ldots, x_d]$. Let $\mathfrak{m}$ denote the irrelevant maximal ideal of R. The variety $\mathbb{V}(I)$ is empty if and only if $(I : \mathfrak{m}^\infty) = R$.*

Proof. As described in Remark 4.23, we will consider two varieties: the projective variety $V = \mathbb{V}(I) \subseteq \mathbb{P}_k^d$ and its affine cone, the affine variety

$$A = \left\{ a \in \mathbb{A}_k^{d+1} \mid f(a) = 0 \text{ for all } f \in I \right\} \subseteq \mathbb{A}_k^{d+1}.$$

Since 0 does not determine a point in projective space, V is empty if and only if $A \subseteq \{0\}$. In affine space, we know that $A = \{0\}$ if and only if $\sqrt{I} = \mathfrak{m}$, and in that case $(I : \mathfrak{m}^\infty) = R$ by Exercise 1. Similarly, A is empty if and only if $I = R$, and in that case $(I : \mathfrak{m}^\infty) = R$ is immediate. Conversely, by Exercise 1 the saturation $(I : \mathfrak{m}^\infty)$ returns the intersection of primary components of I whose radicals do not contain $\mathfrak{m}$. If $(I : \mathfrak{m}^\infty) = R$, then all the associated primes of I contain $\mathfrak{m}$, so either $I = R$ or $\sqrt{I} = \mathfrak{m}$. In both these cases, $A \subseteq \{0\}$ and V is empty. □

As in the affine setting, a projective variety is irreducible if it cannot be decomposed as a finite union of proper subvarieties.

Exercise 14. A projective variety $V \subseteq \mathbb{P}_k^d$ is irreducible if and only if $\mathbf{I}(V)$ is a homogeneous prime ideal.

Remark 4.26. Let $\mathfrak{m}$ be the irrelevant ideal in $R = k[x_0, \ldots, x_d]$, where k is an algebraically closed field. If $P \neq \mathfrak{m}$ is a homogeneous prime ideal, then by Exercise 1 we know that $(P : \mathfrak{m}^\infty) = P$, since P has no $\mathfrak{m}$-primary components, so by Theorem 4.25 the variety $\mathbb{V}(P)$ is nonempty. Therefore, we have a bijective correspondence between homogeneous prime ideals $P \neq \mathfrak{m}$ and nonempty irreducible projective varieties.

Theorem 4.27 (Projective Strong Nullstellensatz)**.** *Let k be an algebraically closed field and let I be a homogeneous ideal in $R = k[x_0, \ldots, x_d]$. If $V = \mathbb{V}(I)$ is a nonempty projective variety, then*

$$\mathbf{I}(\mathbb{V}(I)) = \sqrt{I}.$$

Proof. We will again consider projective variety $V = \mathbb{V}(I) \subseteq \mathbb{P}_k^d$ and its affine cone

$$A = \left\{ a \in \mathbb{A}_k^{d+1} \mid f(a) = 0 \text{ for all } f \in I \right\} \subseteq \mathbb{A}_k^{d+1}.$$

First, we claim that $\mathbf{I}(A) = \mathbf{I}(V)$. For each point $P \in V$, any choice of homogeneous coordinates $(a_0 : \cdots : a_d)$ for P must satisfy $(a_0, \ldots, a_d) \in A$. Therefore, if $f \in \mathbf{I}(A)$ then $f(a_0, \ldots, a_d) = 0$ for all homogeneous coordinates $(a_0, \ldots, a_d)$ for P, and thus $f(P) = 0$. This shows that $\mathbf{I}(A) \subseteq \mathbf{I}(V)$. Conversely, let $f \in \mathbf{I}(V)$. Any nonzero point in A gives homogeneous coordinates for some $P \in V$, and since f vanishes at V, we conclude that f vanishes at every nonzero point in A. To show that $f(0) = 0$, notice that $f(0) = f_0$ is the homogeneous piece of f of degree 0. Since $\mathbf{I}(V)$ is a homogeneous ideal and $f \in \mathbf{I}(V)$, $f_0 \in \mathbf{I}(V)$. Now f_0 is a constant and V is nonempty, so we must have $f_0 = 0$. Therefore, $f(0) = f_0 = 0$.

We have shown that $\mathbf{I}(A) = \mathbf{I}(V)$. By Theorem 4.9, $\mathbf{I}(A) = \sqrt{I}$. Therefore,

$$\mathbf{I}(\mathbb{V}(I)) = \mathbf{I}(V) = \mathbf{I}(A) = \sqrt{I}. \qquad \square$$

In summary, over an algebraically closed field, we have the following dictionary:

Algebra of $k[x_0, \ldots, x_d]$	$\longleftrightarrow$	Geometry of $\mathbb{P}^d_k$
radical homogeneous ideals properly contained in $(x_0, \ldots, x_d)$	$\longleftrightarrow$	nonempty projective varieties
homogeneous prime ideals $P \neq (x_0, \ldots, x_d)$	$\longleftrightarrow$	irreducible nonempty projective varieties
$(a_i x_j - a_j x_i \mid i, j)$	$\longleftrightarrow$	point $\{(a_0 : \cdots : a_d)\}$
(0)	$\longleftrightarrow$	variety $\mathbb{P}^d$
sum of ideals	$\longleftrightarrow$	intersection of varieties
intersection of ideals	$\longleftrightarrow$	union of varieties

We close this section with a comment about finite sets of points in projective space.

Remark 4.28. In the affine setting, the ideal corresponding to the point $(a_1, \ldots, a_d)$ is $(x_1 - a_1, \ldots, x_d - a_d)$. In projective space, the ideal corresponding $P = (a_0 : \cdots : a_d)$ is

$$I(P) = (a_i x_j - a_j x_i \mid 0 \leqslant i \leqslant j \leqslant d).$$

A point is of course irreducible, so $I(P)$ is a homogeneous prime ideal by Exercise 14.

As described in Remark 4.16, we can assume that $a_i = 1$ for some i. We claim that the set of d elements

$$\{x_j - a_j x_i \mid j \neq i\}$$

generate $I(P)$. And indeed, for each $j, k \neq i$,

$$a_k x_j - a_j x_k = a_k(x_j - a_j x_i) - a_j(x_k - a_j x_i).$$

Notice that these d elements $x_j - a_j x_i$ with $j \neq i$ each involve a different variable that does not appear in the remaining ones, so they are linearly independent, and thus they form a regular sequence. This shows that the ideal $I(P)$ is generated by a regular sequence of d elements, and thus by Theorem 3.48, $\operatorname{ht}(I(P)) = d$.

The expression *ideal of points* is often used to refer to the radical ideal $I(V)$ corresponding to a finite set of points $V \subseteq \mathbb{P}^n$. Given $\{P_1, \ldots, P_n\} \subseteq \mathbb{P}^d$, the corresponding ideal of points is the ideal

$$I = \bigcap_{i=1}^{n} I(P_i)$$

of all polynomials that vanish at all the points $P_1, \ldots, P_n$.

Remark 4.29. Let $X = \{P_1, \ldots, P_s\}$ be a finite set of points in $\mathbb{P}^d_k$, where k is any field. The ideal $I = \mathbf{I}(X)$ can be written as

$$I = \mathbf{I}(X) = \bigcap_{i=1}^{s} \mathbf{I}(P_i).$$

By Remark 4.28, each $\mathbf{I}(P_i)$ is a prime ideal of height d. Therefore, the $\mathbf{I}(P_i)$ are the minimal primes of I, so

$$I^{(n)} = \bigcap_{i=1}^{s} \mathbf{I}(P_i)^{(n)}.$$

Also by Remark 4.28, each $\mathbf{I}(P_i)$ is generated by a regular sequence, so by Theorem 3.107 we know that $\mathbf{I}(P_i)^{(n)} = \mathbf{I}(P_i)^n$. We conclude that

$$I^{(n)} = \bigcap_{i=1}^{s} \mathbf{I}(P_i)^n.$$

We can interpret this as saying that the symbolic powers of an ideal of points is the set of polynomials that vanish to order n at each point. Since a polynomial in $R = k[x_0, \ldots, x_d]$ determines a hypersurface in $\mathbb{P}^d$, we can think of the nth symbolic power of an ideal of points as corresponding to all the hypersurfaces that pass through our given points with multiplicity n.

Example 4.30. Consider the points $\{(1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1)\} \subseteq \mathbb{P}^2$, which correspond to the homogeneous radical ideal

$$I = (x, y) \cap (y, z) \cap (x, z) = (xy, xz, yz)$$

in $R = k[x, y, z]$. The polynomials that vanish to order 2 at these points are

$$I^{(2)} = (x, y)^2 \cap (y, z)^2 \cap (x, z)^2,$$

which in particular contain $xyz \notin I^2$.

In the next section, we will show a much more general version of this: that in general, if k is an algebraically closed field and I is a radical ideal in $k[x_1, \ldots, x_d]$, then $I^{(n)}$ is the set of polynomials that vanish to order n along the variety determined by I.

4.3 Zariski–Nagata

The affine Nullstellensatz tells us that over an algebraically closed field k, a radical ideal I in $R = k[x_1, \ldots, x_d]$ is the set of polynomials that vanish at every point in $\mathbb{V}(I)$, and that the polynomials that vanish at the point $(a_1, \ldots, a_d)$ are those in the ideal $(x_1 - a_1, \ldots, x_d - a_d)$. Therefore, every radical ideal I satisfies

$$I = \bigcap_{a \in \mathbb{V}(I)} (x_1 - a_1, \ldots, x_d - a_d).$$

Moreover, Nullstellensatz tells us that all the maximal ideals $\mathfrak{m}$ in R correspond to a point in $\mathbb{A}^d$, and so they are all of this form, and that $I \subseteq \mathfrak{m}$ if and only if the point $\mathbb{V}(\mathfrak{m})$ is in $\mathbb{V}(I)$. Therefore, every radical ideal I satisfies

$$I = \bigcap_{\substack{\mathfrak{m} \supseteq I \\ \mathfrak{m} \text{ maximal}}} \mathfrak{m}.$$

The fact that this holds for all radical ideals I says that $R = k[x_1, \ldots, x_d]$ is a **Jacobson ring**. It turns out that all polynomial rings over a field are Jacobson rings, even if the field is not algebraically closed.

Theorem 4.31. *Let R be a finitely generated k-algebra over any field k. If I is a radical ideal in R, then*

$$I = \bigcap_{\substack{\mathfrak{m} \supseteq I \\ \mathfrak{m} \text{ maximal}}} \mathfrak{m}.$$

Proof. The containment

$$I \subseteq \bigcap_{\substack{\mathfrak{m} \supseteq I \\ \mathfrak{m} \text{ maximal}}} \mathfrak{m}$$

is obvious. For the other containment, we need to show that for any $f \notin I$ we can find a maximal ideal $\mathfrak{m}$ containing I such that $f \notin \mathfrak{m}$. In order to do that, fix $f \in I$. In the ring $(R/I)_f$, we claim that $1 \neq 0$. Indeed, $1 = 0$ would say that $f^n + I = 0$ for some n, or equivalently that $f^n \in I$, but I is radical and $f \notin I$, so no such n exists. Therefore, $(R/I)_f$ is a nonzero ring, and thus it has a maximal ideal J. Let $\mathfrak{m}$ be an ideal in R whose image in $(R/I)_f$ is our chosen maximal ideal; we can obtain $\mathfrak{m}$ by considering the ideal $J \cap (R/I)$ in R/I, which must necessarily be of the form $\mathfrak{m}/I$ for some ideal $\mathfrak{m}$ in I. Since the contraction of a prime is a prime, and the primes in R/I are of the form P/I with P prime in R, our chosen ideal $\mathfrak{m}$ must be prime. By construction, $\mathfrak{m}$ contains I and $\mathfrak{m}/I$ becomes a maximal ideal when localizing at f, which means that $f \notin \mathfrak{m}$. We will show that $\mathfrak{m}$ is a maximal ideal, which will finish the proof.

First, note that $\mathfrak{m} \neq R$, so $\mathfrak{m}$ does not contain any element of k. Therefore, the quotient map $R \to R/\mathfrak{m}$ induces an inclusion $k \subseteq R/\mathfrak{m}$ by restriction. Let's write $S = (R/I)_f$, and recall that $J = (\mathfrak{m}/I)_f$. Now consider the localization map

$$R/\mathfrak{m} \cong \frac{R/I}{\mathfrak{m}/I} \longrightarrow \left(\frac{R/I}{\mathfrak{m}/I}\right)_f \cong \frac{(R/I)_f}{(\mathfrak{m}/I)_f} = S/J.$$

Since $\mathfrak{m}$ is prime, $R/\mathfrak{m}$ is a domain. Therefore, the localization at f is injective. We now have inclusions

$$k \subseteq R/\mathfrak{m} \subseteq S/J.$$

Notice that $S/J \cong (R/\mathfrak{m})_f \cong R/\mathfrak{m}[s]/(sf-1)$ is algebra-finite over $R/\mathfrak{m}$. Since R is a finitely generated k-algebra, then the field extension $k \subseteq S/J$ is algebra-finite. By Zariski's Lemma, which is the key ingredient in proving Nullstellensatz, the field extension $k \subseteq R/\mathfrak{m} \subseteq S/J$ must be module-finite. Therefore, the extension of domains $k \subseteq R/\mathfrak{m}$ must also be module-finite, and thus integral, by Theorem B.19. By Lemma B.20, $R/\mathfrak{m}$ must be a field, so $\mathfrak{m}$ is a maximal ideal. □

The Zariski–Nagata theorem is a higher order version of this result, which roughly speaking says that the symbolic powers of a radical ideal are the sets of polynomials that vanish up to order n on the corresponding variety. There are actually a few different results known as Zariski–Nagata; the first one is a theorem of Nagata's [Nag62]. To prove this theorem, we will need a few fundamental facts about Hilbert-Samuel multiplicity.

Definition 4.32. Let $(R, \mathfrak{m})$ be a noetherian local ring with dimension d. Let $\lambda(M)$ denote the length of the module M. The **Hilbert-Samuel multiplicity** of R is

$$e(R) := \lim_{n\to\infty} \frac{d!\lambda(R/\mathfrak{m}^n)}{n^d}.$$

The Hilbert-Samuel multiplicity is an important invariant which detects and measures singularities. The defining limit exists, and can also be described in terms of the Hilbert function of $\mathfrak{m}$: the Hilbert function is eventually a polynomial, and $e(R)$ is essentially the coefficient of the highest order term in that polynomial (after some appropriate rescaling). We will need a few facts about $e(R)$, which we will not prove for now:

- If $(R, \mathfrak{m})$ is a regular local ring and $f \in \mathfrak{m}$, then $e(R) = \operatorname{ord}(f) := \max\{t \mid f \in \mathfrak{m}^t\}$.
- Under mild assumptions, $e(R) \geqslant e(R_P)$.

Using these two facts, we can now prove Nagata's version [Nag62] of the Zariski–Nagata theorem:

Theorem 4.33 (Local Zariski—Nagata)**.** *Let $(R, \mathfrak{m})$ be a regular local ring. For every prime ideal P and every $n \geqslant 1$,*

$$P^{(n)} \subseteq \mathfrak{m}^n.$$

Proof. Fix a prime ideal P and an element $f \in \mathfrak{m}$. First, note that R_P is also regular, and that $f \in P^{(t)}$ if and only if $\frac{f}{1} \in P^t R_P$, so by the properties above,

$$\max\{t \mid f \in P^{(t)}\} = \max\{t \mid \frac{f}{1} \in P^t R_P\} = e((R/f)_P) \leqslant e(R/f) = \max\{t \mid f \in \mathfrak{m}^t\}.$$

So if $f \in P^{(n)}$, then we must have $f \in \mathfrak{m}^n$, showing that $P^{(n)} \subseteq \mathfrak{m}^n$. □

The assumption that R is regular is necessary: we cannot extend this result to any noetherian local ring.

Example 4.34. As in Example 1.54, when $R = k[\![x, y, z]\!]/(xy - z^c)$ and $c \geqslant 2$, the prime $P = (x, z)$ satisfies $x \in P^{(c)}$, so in particular $P^{(c)} \nsubseteq \mathfrak{m}^c$. One can show that $P^{(cn)} = (x^n)$, so in fact $P^{(cn)} \subseteq \mathfrak{m}^n$ for all $n \geqslant 1$.

This is a more general phenomenon.

Theorem 4.35 (Huneke–Katz–Validashti, 2009 [HKV09])**.** *Let $(R, \mathfrak{m})$ be a complete local domain. There exists a constant c such that for all primes P and all $n \geqslant 1$,*

$$P^{(cn)} \subseteq \mathfrak{m}^n.$$

Finding effective bounds for this constant c is a difficult problem, and in general it is wide open; such bounds are known in the graded setting when k is a field [DDSG+18, Theorem 3.27] or a DVR with uniformizer $p \in \mathbb{Z}$ [SGJ21] and $R = k[f_1, \ldots, f_n] \subseteq k[x_1, \ldots, x_d]$ generated by homogeneous elements f_i and such that the inclusion of R into $k[x_1, \ldots, x_d]$ splits. In that case, one can take $c = \max\{\deg(f_i)\}$.

The theorem most commonly known as Zariski–Nagata is a result about polynomial rings, which we will prove via yet another version of the theorem, in terms of differential operators.

Definition 4.36 (Differential operators)**.** Given a finitely generated k-algebra R, the k-linear differential operators on R of order n, $D^n_R \subseteq \mathrm{Hom}_k(R, R)$, are defined as follows:

- The differential operators of order zero are the k-linear maps which are also R-linear:

$$D^0_{R|k} := \mathrm{Hom}_R(R, R) \cong R.$$

- We say that $\delta \in \mathrm{Hom}_k(R, R)$ is an operator of order up to n, meaning $\delta \in D^n_R$, if

$$[\delta, r] = \delta r - r\delta$$

  is an operator of order up to $n - 1$ for all $r \in D^0_R$.

The **ring of k-linear differential operators** is the subring of $\mathrm{Hom}_k(R, R)$ defined by

$$D_{R|k} := \bigcup_{n \in \mathbb{N}} D^n_{R|k}.$$

In particular, the multiplication on $D_{R|k}$ just composition.

If R or k are clear from the context, we may drop one of the subscripts, or both. Notice that $D_{R|k}$ is almost always a noncommutative ring!

Example 4.37. Let k be a field and $R = k[x_1, \ldots, x_d]$ or $R = k[\![x_1, \ldots, x_d]\!]$. When k is a field of characteristic 0,

$$D^n_R = \bigoplus_{\alpha_1 + \ldots + \alpha_d \leqslant n} R \cdot \frac{\partial^{\alpha_1}}{\partial x_1^{\alpha_1}} \cdots \frac{\partial^{\alpha_d}}{\partial x_d^{\alpha_d}} \quad \text{and} \quad D_{R|k} = R\left\langle \frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_d} \right\rangle.$$

When k has prime characteristic p, things are a little more complicated; notice that over $R = k[x]$, $\frac{\partial^p}{\partial x^p}(x^n) = 0$ for any n, but there are indeed nonzero differential operators of order p. To give a correct description of our differential operators on $R = k[x_1, \ldots, x_d]$ over any field k of any characteristic, we consider

$$D_\alpha := \frac{1}{\alpha_1!}\frac{\partial^{\alpha_1}}{\partial x_1^{\alpha_1}} \cdots \frac{1}{\alpha_d!}\frac{\partial^{\alpha_d}}{\partial x_d^{\alpha_d}}, \qquad \text{where} \quad D_\alpha(x^\beta) = \begin{cases} \binom{\alpha}{\beta} x^{\alpha-\beta} & \text{if } \alpha_i \geqslant \beta_i \text{ for all } i \\ 0 & \text{otherwise.} \end{cases}$$

and now we have

$$D_R^n = \bigoplus_{\alpha_1+\cdots+\alpha_d \leqslant n} D_\alpha.$$

For example, when $R = \mathbb{F}_3[x]$, $D_3(x^5) = \binom{5}{3}x^{5-3}$; since $\binom{5}{3} = \frac{5!}{3!2!} = \frac{5\cdot 4}{2} = 10$, and $10 = 1$ in $\mathbb{F}_3$, this means that $D_3(x^5) = x^2$. On the other hand, notice that $\frac{\partial^3}{\partial x^3}(x^5) = 5 \cdot 4 \cdot 3 \cdot x^2 = 0$.

Definition 4.38. Let R be a finitely generated k-algebra, I an ideal of R, and n be a positive integer. The nth k-linear **differential power** of I is given by

$$I^{\langle n \rangle} = \{f \in R \,|\, \delta(f) \in I \text{ for all } \delta \in D_R^{n-1}\}.$$

Exercise 15. Let $\{I_\alpha\}_{\alpha \in A}$ be an indexed family of ideals. For every $n \geqslant 0$ we have

$$\bigcap_{\alpha \in A} I_\alpha^{\langle n \rangle} = \left(\bigcap_{\alpha \in A} I_\alpha\right)^{\langle n \rangle}.$$

We will also use the fact that containments are local.

Exercise 16. (Containments are local statements) Given ideals I and J in a noetherian ring R, the following are equivalent:

(a) $I \subseteq J$;

(b) $I_P \subseteq J_P$ for all primes $P \in \operatorname{Supp}(R/J)$;

(c) $I_P \subseteq J_P$ for all primes $P \in \operatorname{Ass}(R/J)$.

We note that in what follows and up to Proposition 4.42, k can be any ring.

Remark 4.39. Since $D_R^{n-1} \subseteq D_R^n$, it follows that $I^{\langle n+1 \rangle} \subseteq I^{\langle n \rangle}$. Moreover, given any ideals $I \subseteq J$, we have $I^{\langle n \rangle} \subseteq J^{\langle n \rangle}$ for every $n \geqslant 1$.

Lemma 4.40. *Let R be a finitely generated k-algebra, I be an ideal of R, and n be a positive integer. The set $I^{\langle n \rangle}$ is an ideal.*

Proof. Every $f \in \operatorname{Hom}_k(R, R)$ must satisfy $f(0) = 0$, and since $D_{R|k} \subseteq Hom_k(R, R)$, we conclude that $D_{R|k} \cdot 0 = 0$. In particular, $0 \in I^{\langle n \rangle}$ for all ideals I and all n.

If $f, g \in I^{\langle n \rangle}$ then $f + g \in I^{\langle n \rangle}$, since for any $\delta \in D_R^{n-1}$,

$$\delta(f + g) = \underbrace{\delta(f)}_{\in I} + \underbrace{\delta(g)}_{\in I} \in I.$$

Now we need to show that $rf \in I^{\langle n \rangle}$ for any $r \in R$ and $f \in I^{\langle n \rangle}$. For any $\delta \in D^{n-1}$, note that $f \in I^{\langle n \rangle} \subseteq I^{\langle n-1 \rangle}$, $[\delta, r] \in D^{n-2}$, and $\delta(f) \in I$, so

$$\delta(rf) = \underbrace{\underbrace{[\delta, r]}_{\in D^{n-2}} \big(\underbrace{f}_{\in I^{\langle n-1 \rangle}} \big)}_{\in I} + r\underbrace{\delta(f)}_{\in I} \in I.$$

We conclude that $\delta(rf) \in I$. Hence, $rf \in I^{\langle n \rangle}$. □

Proposition 4.41. *Let R be a finitely generated k-algebra. If P is a prime ideal, then $P^{\langle n \rangle}$ is P-primary for all $n \geqslant 1$.*

Proposition 4.42. *Let R be a finitely generated k-algebra, I be an ideal of R, and $n \geqslant 1$. Then $I^n \subseteq I^{\langle n \rangle}$.*

Proof. Induction on n. The base case is straightforward: $I = I^{\langle 1 \rangle}$ because $D^0 = R$.

Suppose that $I^n \subseteq I^{\langle n \rangle}$. Notice that I^n is generated by the elements of the form fg where $f \in I$, $g \in I^n$. In order to show that $I^{n+1} \subseteq I^{\langle n+1 \rangle}$, it is enough to show that $fg \in I^{\langle n+1 \rangle}$ for any such f and g.

To do that, we consider any $\delta \in D^n$, and we will show that $\delta(fg) \in I$. And in fact, since by induction hypothesis $g \in I^n \subseteq I^{\langle n \rangle}$, then

$$\delta(fg) = \underbrace{\underbrace{[\delta, f]}_{\in D^{n-1}} \big(\underbrace{g}_{\in I^{\langle n \rangle}} \big)}_{\in I} + \underbrace{f}_{\in I} \delta(g) \in I.$$

Notice here we used the fact that $\delta f = [\delta, f] + f\delta$. We conclude that $I^{n+1} \subseteq I^{\langle n+1 \rangle}$. □

Lemma 4.43. *For any radical ideal I and prime ideal P in a k-algebra R, $(I_P)^{\langle n \rangle} = \left(I^{\langle n \rangle}\right)_P$.*

A lot more is true: taking differential powers commutes with localization at any multiplicative set W [BJNB19, Lemma 3.9]. The main technical point is that any k-linear differential operator of order n on R can be extended to a k-linear differential operator of order n on R_P, and that every k-linear differential operator on R_P can be obtained from a differential operator on R. We skip the proof to avoid a lengthier discussion on these technical details, but it can be found in [BJNB19, Lemma 3.9].

Remark 4.44. Let k be a field, $R = k[x_1, \ldots, x_d]$ or $R = k[\![x_1, \ldots, x_d]\!]$, and $\mathfrak{m} = (x_1, \ldots, x_d)$. In this case,

$$D_R^n = R\left\langle \frac{1}{\alpha_1!}\frac{\partial^{\alpha_1}}{\partial x_1^{\alpha_1}} \cdots \frac{1}{\alpha_d!}\frac{\partial^{\alpha_d}}{\partial x_d^{\alpha_d}} \;\middle|\; \alpha_1 + \ldots + \alpha_d \leqslant n \right\rangle.$$

If $f \notin \mathfrak{m}^n$, then f has a monomial of the form $x_1^{\alpha_1} \cdots x_d^{\alpha_d}$ with nonzero coefficient $\lambda \in k$ for some $\alpha_1 + \cdots + \alpha_d < n$. Fix such a monomial which is minimal among all monomials appearing in f under the graded lexicographical order. Applying the differential operator $\frac{1}{\alpha_1!}\frac{\partial^{\alpha_1}}{\partial x_1^{\alpha_1}} \cdots \frac{1}{\alpha_d!}\frac{\partial^{\alpha_d}}{\partial x_d^{\alpha_d}}$ maps $\lambda x_1^{\alpha_1} \cdots x_d^{\alpha_d}$ to the nonzero element $\lambda \in k$, and any other monomial appearing in f either to a nonconstant monomial or to zero. Consequently, $f \notin \mathfrak{m}^{\langle n \rangle}$. Hence, $\mathfrak{m}^{\langle n \rangle} \subseteq \mathfrak{m}^n$. Since $\mathfrak{m}^n \subseteq \mathfrak{m}^{\langle n \rangle}$ by Proposition 4.42, we conclude that $\mathfrak{m}^{\langle n \rangle} = \mathfrak{m}^n$.

There is a more technical version of this idea that proves that if we assume that k is perfect, and $\mathfrak{m}$ is any maximal ideal in R a regular algebra essentially of finite type over k, then we still have $\mathfrak{m}^n = \mathfrak{m}^{\langle n \rangle}$. This technical point, however, is difficult – this is the subtle part of the proof. For a complete proof, see [DSGJ20, Theorem 3.6].

Definition 4.45. A field k of prime characteristic p is **perfect** if every element of k is a pth power. More generally, a field k is **perfect** if k has characteristic 0 or k is a perfect field of characteristic p.

Example 4.46.

1) Every finite field is perfect, thanks to Fermat's Little Theorem.

2) If k is an algebraically closed field of characteristic p, then $x^p - a$ has a root for every $a \in k$, which means that k is perfect. Therefore, every algebraically closed field is perfect.

3) For an example of an imperfect field, take $\mathbb{F}_p(t)$, where t does not have a pth root.

Theorem 4.47. *Let k be a perfect field and let $S = k[x_1, \ldots, x_d]$. If $(R, \mathfrak{m})$ is a localization of S at a prime ideal, then $\mathfrak{m}^n = \mathfrak{m}^{\langle n \rangle}$ for all $n \geqslant 1$.*

A detailed proof can be found in [DSGJ20, Theorem 3.6]. More surprisingly, this condition characterizes regularity, as shown by Brenner, Jeffries, and Núnez Betancourt [BJNB19, Theorem 10.2].

Theorem 4.48 (Differential version of Zariski–Nagata, see [DDSG+18])**.** *Let $R = k[x_1, \ldots, x_d]$, where k is a perfect field, and let I be a radical ideal. For all $n \geqslant 1$,*

$$I^{(n)} = I^{\langle n \rangle}.$$

Proof. First, let $I = P$ be a prime ideal.

1) $P^{\langle n \rangle}$ is a P-primary ideal. (Lemma 4.40 and Proposition 4.41)

2) $P^n \subseteq P^{\langle n \rangle}$. (Proposition 4.42)

3) $\left(P^{\langle n \rangle}\right)_P = (P_P)^{\langle n \rangle}$. (Lemma 4.43)

Now 1) and 2) together imply $P^{(n)} \subseteq P^{\langle n \rangle}$, since $P^{(n)}$ is the smallest P-primary ideal containing P^n. To show $P^{\langle n \rangle} \subseteq P^{(n)}$, we only need to show the containment holds after localizing at P, which is the only associated prime of $P^{(n)}$, by Exercise 16. But 3) says differential powers commute with localization, and after localization P becomes the maximal ideal; so Theorem 4.47 completes the proof that $P^{\langle n \rangle} \subseteq P^{(n)}$ for a prime ideal P.

Now if we take any radical ideal I, we can write I as the intersection of finitely many primes, say

$$I = P_1 \cap \cdots \cap P_r.$$

Then

$$I^{(n)} = P_1^{(n)} \cap \cdots \cap P_r^{(n)} = P_1^{\langle n \rangle} \cap \cdots \cap P_r^{\langle n \rangle} = (P_1 \cap \cdots \cap P_r)^{\langle n \rangle} = I^{\langle n \rangle}. \qquad \square$$

In Theorem 4.48, we cannot replace $k[x_1, \ldots, x_d]$ with a finitely generated k-algebra.

Example 4.49. Let k be any field, $R = k[x, y, z]/(xy - z^2)$, $\mathfrak{m} = (x, y, z)$, and $P = (x, z)$. By Example 1.54, $x \in P^{(2)}$, so $P^{(2)} \nsubseteq \mathfrak{m}^2$. On the other hand, it follows immediately from the definition that $P^{\langle 2 \rangle} \subseteq \mathfrak{m}^{\langle 2 \rangle}$. Thus $x \in P^{(2)} \subseteq P^{\langle 2 \rangle} \subseteq \mathfrak{m}^{\langle 2 \rangle}$, but since $\mathfrak{m}$ is maximal, $\mathfrak{m}^2 = \mathfrak{m}^{(2)}$, so we can conclude that $\mathfrak{m}^{\langle 2 \rangle} \neq m^{(2)}$.

We also cannot substitute k by any field.

Example 4.50. Let $k = \mathbb{F}_p(t)$, with p prime, and consider the ring $R = k[x]$ and the prime ideal $P = (x^p - t)$. As we described in Example 4.37, $D^1_{R|k} = R \oplus R\frac{\partial}{\partial x}$, and $\frac{\partial}{\partial x}(x^p - t) = 0 \in P$. Therefore, $P^{\langle 2 \rangle} = P$. On the other hand, P is a principal ideal in a domain, so its symbolic powers are the powers; in particular, $P^{(2)} = P^2 \neq P^{\langle 2 \rangle}$.

Theorem 4.51 (Zariski–Nagata Theorem for polynomial rings [Zar49])**.** *Let k be a perfect field and $R = k[x_1, \ldots, x_d]$. For any radical ideal I, we have*

$$I^{(n)} = \bigcap_{\substack{\mathfrak{m} \supseteq I \\ \mathfrak{m} \in \mathrm{mSpec}(R)}} \mathfrak{m}^n.$$

Proof. On the one hand,

$$I^{(n)} \underset{4.41}{\subseteq} I^{\langle n \rangle} \underset{4.39}{\subseteq} \mathfrak{m}^{\langle n \rangle} \underset{4.44}{=} \mathfrak{m}^n.$$

For the converse, take $f \in \mathfrak{m}^n$ for all the maximal ideals $\mathfrak{m} \supseteq I$. For each maximal ideal $\mathfrak{m}$ containing I, we have $f \in \mathfrak{m}^{\langle n \rangle}$ by Remark 4.44, so for every $\delta \in D^{n-1}$, $\delta(f) \in \mathfrak{m}$. But by Theorem 4.31, every radical ideal in R is an intersection of maximal ideals:

$$I = \bigcap_{\substack{\mathfrak{m} \supseteq I \\ \mathfrak{m} \in \text{ maximal ideal}}} \mathfrak{m}.$$

Thus $\partial(f) \in I$ for every $\delta \in D^{n-1}$, so $f \in I^{\langle n \rangle}$. By Theorem 4.48, $I^{\langle n \rangle} = I^{(n)}$. □

Over $\mathbb{C}$ or any perfect field, the polynomials in $\mathfrak{m}^n$ are those that vanish to order n at the point corresponding to $\mathfrak{m}$. So Zariski–Nagata says that $I^{(n)}$ is the set of polynomials that vanish to order n along the variety $\mathbb{V}(I)$.

We can also give such an interpretation to the symbolic powers of ideals corresponding to finite sets of points in projective space. We have seen that the polynomials that vanish to order n on a finite set of points X in $\mathbb{P}^d$ are precisely the polynomials in $\mathbf{I}(X)^{(n)}$. More generally, this also holds for any projective variety.

Theorem 4.52. *Let k be an algebraically closed field, and let $X \subseteq \mathbb{P}^d_k$ be a non-empty projective variety with corresponding ideal $I = \mathbb{I}(X) \subseteq k[x_1, \ldots, x_d]$. For all $n \geqslant 1$,*

$$I^{(n)} = \bigcap_{P \in X} I(P)^n.$$

Proof. Let C be the cone of X, meaning that C is the union of the lines through the origin of $\mathbb{A}_k^{d+1}$ that correspond to points in X. First, we claim that

$$\mathcal{N} := \{\mathfrak{m} \in \operatorname{mSpec}(R) \mid \mathfrak{m} \supseteq I\} = \{\mathfrak{m} \in \operatorname{mSpec}(R) \mid \mathfrak{m} \supseteq I(P) \text{ for some } P \in X\}.$$

Since k is algebraically closed, the affine Nullstellensatz tells us that the maximal ideals containing I are precisely the maximal ideals corresponding to points in C. For each $P \in X$, consider the cone of P in $\mathbb{A}_k^{d+1}$, meaning the line L through the origin of $\mathbb{A}_k^{d+1}$ that corresponds to P. Since k is algebraically closed, a maximal ideal $\mathfrak{m}$ contains $I(P)$ if and only if $\mathfrak{m}$ corresponds to a point on the line L. Since C is the union of all such lines, this proves our claim.

Now by Theorem 4.31,

$$I(P) = \bigcap_{\substack{\mathfrak{m} \in \operatorname{mSpec}(R) \\ \mathfrak{m} \supseteq I(P)}} \mathfrak{m}, \quad \text{so} \quad \bigcap_{P \in X} I(P) = \bigcap_{\mathfrak{m} \in \mathcal{N}} \mathfrak{m}.$$

Also by Theorem 4.31,

$$I = \bigcap_{\substack{\mathfrak{m} \in \operatorname{mSpec}(R) \\ \mathfrak{m} \supseteq I}} \mathfrak{m} = \bigcap_{\mathfrak{m} \in \mathcal{N}} \mathfrak{m}.$$

Now fix $n \geqslant 1$. By Theorem 4.51,

$$I^{(n)} = \bigcap_{\mathfrak{m} \in \mathcal{N}} \mathfrak{m}^n,$$

and for each $P \in X$,

$$I(P)^{(n)} = \bigcap_{\substack{\mathfrak{m} \in \operatorname{mSpec}(R) \\ \mathfrak{m} \supseteq I(P)}} \mathfrak{m}^n.$$

By Remark 4.29, $I(P)^{(n)} = I(P)^n$. By definition of $\mathcal{N}$,

$$\bigcap_{P \in X} I(P)^n = \bigcap_{P \in X} I(P)^{(n)} = \bigcap_{\mathfrak{m} \in \mathcal{N}} \mathfrak{m}^n.$$

We conclude that

$$I^{(n)} = \bigcap_{P \in X} I(P)^{(n)}.$$

□

There are several extensions of Zariski–Nagata. In 1979, Eisenbud and Hochster [EH79] gave a more general version of Theorem 4.51; Zariski's original result [Zar49] then follows as a corollary. As for the differential operators version of the theorem, Yairon Cid Ruiz [CR21] recently gave a more general version of the theorem for finitely generated k-algebras, which uses differential operators that are k-linear maps from R to R/P. In the next section, we will briefly discuss a version of the differential version of Zariski–Nagata when we replace k by $\mathbb{Z}$ or a DVR.

4.4 Mixed characteristic

As to the differential operators description of symbolic powers, if we replace k by $\mathbb{Z}$ or some other ring of mixed characteristic, this description no longer holds; roughly speaking, the differential operators cannot see what happens in the arithmetic direction.

Example 4.53. In $R = \mathbb{Z}[x]$, the symbolic powers of the maximal ideal $\mathfrak{m} = (2, x)$ coincide with its powers, so $2 \notin \mathfrak{m}^n$ for any $n > 1$. However, any differential operator $\partial \in D^n_{R|\mathbb{Z}}$ of any order is $\mathbb{Z}$-linear, so $\partial(2) = 2 \cdot \partial(1) \in \mathfrak{m}$.

To describe symbolic powers in mixed characteristic, we need to consider differential operators together with p-derivations, a tool from arithmetic geometry introduced independently in [Joy85] and [Bui95]; for a thorough development of the theory of p-derivations, see [Bui05].

Definition 4.54 (p-derivation)**.** Fix a prime $p \in \mathbb{Z}$, and let S be a ring on which p is a nonzerodivisor. A set-theoretic map $\delta : R \to R$ is a **p-derivation** if $\phi_p(x) := x^p + p\delta(x)$ is a ring homomorphism. Equivalently, δ is a p-derivation if $\delta(1) = 0$ and δ satisfies the following identities for all $x, y \in R$:

1) $\delta(xy) = x^p\delta(y) + y^p\delta(x) + p\delta(x)\delta(y)$,

2) $\delta(x + y) = \delta(x) + \delta(y) + \mathcal{C}_p(x, y)$

where $\mathcal{C}_p(X, Y) = \frac{X^p+Y^p-(X+Y)^p}{p} \in \mathbb{Z}[X, Y]$. If δ is a p-derivation, we set δ^a to be the a-fold self-composition of δ; in particular, δ^0 is the identity.

These are very non-intuitive maps; for example, they are not even additive!

Example 4.55. Let $R = \mathbb{Z}$ and fix a prime p. To give a p-derivation is the same as finding a lift Φ of the Frobenius map on R/p to R: the p-derivation δ satisfies $\Phi(n) = n^p + p\delta(n)$. But the Frobenius map on $\mathbb{Z}/p$ is the identity, by Fermat's Little Theorem, so a p-derivation δ_p must satisfy $n^p + p\delta_p(n) = n$. Again by Fermat's Little Theorem $x^p - x$ is always divisible by p for any integer x, so $\delta_p(n) = \frac{n-n^p}{p}$. In particular, there is a unique p-derivation on $\mathbb{Z}$.

Example 4.56. If S is a ring with a p-derivation δ, then $R = S[x]$ also has p-derivations, but infinitely many: we can extend δ to R by setting $\delta(x)$ to be any element in S, and this always determines a unique p-derivation on S for each choice of $\delta(x)$.

Roughly speaking, a p-derivation and its powers play the role of differential operators in the arithmetic direction. The following theorem applies, for example, when $R = \mathbb{Z}[x_1, \ldots, x_d]$.

Theorem 4.57 (De Stefani – Grifo – Jeffries, 2020 [DSGJ20])**.** *Let p be a prime. Let $A = \mathbb{Z}$ or a DVR with uniformizer p. Let R be an essentially smooth A-algebra that has a p-derivation δ. Let Q be a prime ideal of R that contains p, and assume that A/pA is perfect, or more generally that the field extension $A/pA \subseteq R_Q/QR_Q$ is separable. Then*

$$Q^{(n)} = \{f \in S \mid (\delta^s \circ \partial)(f) \in I \text{ for all } \partial \in D^t_{R|A} \text{ with } s + t \leqslant n - 1\}.$$

For prime ideals that do not contain p, the usual description using only differential operators, as in Theorem 4.48, still holds [DSGJ20, Theorem 3.9].

Example 4.58. The maximal ideal $\mathfrak{m} = (2, x)$ in $R = \mathbb{Z}[x]$ contains the prime 2, so to describe its symbolic powers we need to consider a 2-derivation. The map $\delta_2 \colon R \to R$

$$\delta_2(f(x)) = \frac{f(x^2) - f(x)^2}{2}$$

is a 2-derivation on R. By Theorem 4.57, the symbolic powers of $\mathfrak{m} = (2, x)$ are given by

$$\mathfrak{m}^{(n)} = \left\{ f \in \mathbb{Z}[x] \mid \delta_2^a \left(\frac{\partial^b f}{\partial x^b} \right) \in (2, x), \text{ for } a + b \leqslant n - 1 \right\}.$$

In particular, we can now see that $2 \notin \mathfrak{m}^{(2)}$, since

$$\delta_2(2) = \frac{2 - 2^2}{2} = -1 \notin \mathfrak{m},$$

while as we saw in Example 4.53 there are no $\mathbb{Z}$-linear differential operators ∂ of order up to 1 (or even any order!) satisfying $\partial(2) \notin \mathfrak{m}$.

Appendix A

Macaulay2

There are several computer algebra systems dedicated to algebraic geometry and commutative algebra computations, such as Singular (more popular among algebraic geometers), CoCoA (which is more popular with european commutative algebraists, having originated in Genova, Italy), and Macaulay2. There are many computations you could run on any of these systems (and others), but we will focus on Macaulay2 since it's the most popular computer algebra system among US based commutative algebraists.

Macaulay2, as the name suggests, is a successor of a previous computer algebra system named Macaulay. Macaulay was first developed in 1983 by Dave Bayer and Mike Stillman, and while some still use it today, the system has not been updated since its final release in 2000. In 1993, Daniel Grayson and Mike Stillman released the first version of Macaulay2, and the current stable version if Macaulay2 1.16.

Macaulay2, or M2 for short, is an open-source project, with many contributors writing packages that are then released with the newest Macaulay2 version. Journals like the *Journal of Software for Algebra and Geometry* publish peer-refereed short articles that describe and explain the functionality of new packages, with the package source code being peer reviewed as well.

The National Science Foundation has funded Macaulay2 since 1992. Besides funding the project through direct grants, the NSF has also funded several Macaulay2 workshops — conferences where Macaulay2 package developers gather to work on new packages, and to share updates to the Macaulay2 core code and recent packages.

A.1 Getting started

A Macaulay2 session often starts with defining some ambient ring we will be doing computations over. Common rings such as the rationals and the integers can be defined using the commands `QQ` and `ZZ`; one can easily take quotients or build polynomial rings (in finitely many variables) over these. For example,

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

o1 = R
```

```
o1 : PolynomialRing
```

and

```
i1 : k = ZZ/101;

i2 : R = k[x,y];
```

both store the ring $\mathbb{Z}/101$ as R, with the small difference that in the second example Macaulay2 has named the coefficient field k. One quirk that might make a difference later is that if we use the first option and later set k to be the field $\mathbb{Z}/101$, our ring R is *not* a polynomial ring over k. Also, in the second example we ended each line with a `;`, which tells Macaulay2 to run the command but not display the result of the computation — which is in this case was simply an assignment, so the result is not relevant.

We can now do all sorts of computations over our ring R. For example, we can define an ideal in R, as follows:

```
i3 : I = ideal(x^2,y^2,x*y)

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

o3 : Ideal of R
```

Above we have set I to be the ideal in R that is generated by x^2, y^2, xy. The notation `ideal( )` requires the usage of `^` for powers and $*$ for products; alternatively, we can define the exact same ideal with the notation `ideal" "`, as follows:

```
i3 : I = ideal"x2,y2,xy"

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

o3 : Ideal of R
```

Now we can use this ideal I to either define a quotient ring $S = R/I$ or the R-module $M = R/I$, as follows:

```
i4 : M = R^1/I

o4 = cokernel | x2 y2 xy |
                          1
o4 : R-module, quotient of R

i5 : S = R/I

o5 = S

o5 : QuotientRing
```

It's important to note that while R is a ring, R^1 is the R-module R — this is a very important difference for Macaulay2, since these two objects have different types. So S defined above is a ring, while M is a module. Notice that Macaulay2 stored the module M as the cokernel of the map

$$R^3 \xrightarrow{\begin{bmatrix} x^2 & y^2 & xy \end{bmatrix}} R\,.$$

When you make a new definition in Macaulay2, you might want to pay attention to what ring your new object is defined over. For example, now that we defined this ring S, Macaulay2 has automatically taken S to be our current ambient ring, and any calculation or definition we run next will be considered over S and not R. If you want to return to the original ring R, you must first run the command `use R`.

If you want to work over a finitely generated algebra over one of the basic rings you can define in Macaulay2, and your ring is not a quotient of a polynomial ring, you want to rewrite this algebra as a quotient of a polynomial ring. For example, suppose you want to work over the second Veronese in 2 variables over our field k from before, meaning the algebra $k[x^2, xy, y^2]$. We need 3 algebra generators, which we will call a, b, c, corresponding to x^2, xy, and y^2:

```
i6 : U = k[a,b,c]

o6 = U

o6 : PolynomialRing

i7 : f = map(R,U,{x^2,x*y,y^2})
                 2        2
o7 = map(R,U,{x , x*y, y })

o7 : RingMap R <--- U

i8 : J = ker f
             2
o8 = ideal(b  - a*c)

o8 : Ideal of U

i9 : T = U/J

o9 = T

o9 : QuotientRing
```

Our ring T at the end is isomorphic to the 2nd Veronese of R, which is the ring we wanted. Note the syntax order in `map`: first target, then source, then a list with the images of each algebra generator.

A.2 Asking Macaulay2 for help

As you're learning how to use Macaulay2, you will often find yourself needing some help. Luckily, Macaulay2 can help you directly! For example, suppose you know the name of a command, but do not remember the syntax to use it. You can ask `?command`, and Macaulay2 will show you the different usages of the command you want to know about.

```
i10 : ?primaryDecomposition

primaryDecomposition -- irredundant primary decomposition of an ideal

  * Usage:
        primaryDecomposition I
  * Inputs:
      * I, an ideal, in a (quotient of a) polynomial ring R
  * Optional inputs:
      * MinimalGenerators => a Boolean value, default value true, if false, the
        components will not be minimalized
      * Strategy => ..., default value null,
  * Outputs:
      * a list, containing a minimal list of primary ideals whose intersection
        is I

Ways to use primaryDecomposition :
==================================

  * "primaryDecomposition(Ideal)" -- see "primaryDecomposition" -- irredundant
    primary decomposition of an ideal
  * "primaryDecomposition(Module)" -- irredundant primary decomposition of a
    module
  * "primaryDecomposition(Ring)" -- see "primaryDecomposition(Module)" --
    irredundant primary decomposition of a module

For the programmer
==================

The object "primaryDecomposition" is a method function with options.
```

If instead you'd rather read the complete Macaulay2 documentation on the command you are interested in, you can use the `viewHelp` command, which will open an html page with the documentation you asked for. So running

```
i11 : viewHelp "primaryDecomposition"
```

will open an html page dedicate to the method `primaryDecomposition`, which includes examples and links to related methods.

A.3 Basic commands

Many Macaulay2 commands are easy to guess, and named exactly what you would expect them to be named. Often, googling "Macaulay2" followed by a few descriptive words will easily land you on the documentation for whatever you are trying to do.

Here are some basic commands you will likely use:

- `ideal`$(f_1, \ldots, f_n)$ will return the ideal generated by $f_1, \ldots, f_n$. Here products should be indicated by $*$, and powers with $\widehat{}$. If you'd rather not use $\widehat{}$ (this might be nice if you have lots of powers), you can write `ideal`$(f_1, \ldots, f_n)$ instead.
- `map`$(S, R, f_1, \ldots, f_n)$ gives a ring map $R \to S$ if R and S are rings, and R is a quotient of $k[x_1, \ldots, x_n]$. The resulting ring map will send $x_i \mapsto f_i$. There are many variations of `map` — for example, you can use it to define R-module homomorphisms — but you should carefully input the information in the required format. Try `viewHelp map` in Macaulay2 for more details
- `ker`(f) returns the kernel of the map f.
- `I + J` and `I*J` return the sum and product of the ideals I and J, respectively.
- `A = matrix`$\{\{a_{1,1}, \ldots, a_{1,n}\}, \ldots, \{a_{m,1}, \ldots, a_{m,n}\}\}$ returns the matrix

$$A = \begin{pmatrix} a_{1,1} & \ldots & a_{1,n} \\ & \ddots & \\ a_{m,1} & \ldots & a_{m,n} \end{pmatrix}$$

If you are familiar with any other programming language, many of the basics are still the same. For example, some of the commands we will use return lists, and we might often need to do operations on lists. As with many other programming languages, a list is indicated by { } with the elements separated by commas.

```
i6 : w = {ZZ, 3, ideal"xy3"}
                          3
o6 = {ZZ, 3, ideal(x*y )}

o6 : List
```

As in most programming languages, Macaulay2 follows the convention that the first position in a list is the 0th position.

The method `primaryDecomposition` returns a list of primary ideals whose intersection is the input ideal, and `associatedPrimes` returns the list of associated primes of the given ideal or module. Operations on lists are often intuitive. For example, let's say we want to find the primary component of an ideal with a particular radical.

```
i1 : R = QQ[x,y];

i2 : I = ideal"x2,xy";

o2 : Ideal of R

i3 : prim = primaryDecomposition I
                              2
o3 = {ideal x, ideal (y, x )}

o3 : List

i4 : L = select(prim, Q -> radical(Q) == ideal"x,y")
                   2
o4 = {ideal (y, x )}

o4 : List
```

The method `select` returns a list of all the elements in our list with the required properties. In this case, if we actually want the primary ideal we just selected, as opposed to a list containing it, we need to extract the first component of our list L.

```
i5 : L_0
                  2
o5 = ideal (y, x )

o5 : Ideal of R
```

A.4 Graded rings

Polynomial rings in Macaulay2 are graded with the standard grading by default, meaning that all the variables have degree 1. To define a different grading, we give Macaulay2 a list with the grading of each of the variables:

```
i1 : R = ZZ/101[a,b,c,Degrees=>{{1,2},{2,1},{1,0}}];
```

We can check whether an element of R `isHomogeneous`, and the function `degree` applied to an element of R returns the least upper bound of the degrees of its monomials:

```
i2 : degree (a+b)
o2 = {2, 2}
o2 : List

i3 : isHomogeneous(a+b)
o3 = false
```

A.5 Complexes and homology in Macaulay2

There are two different ways to do computations involving complexes in Macaulay2: using `ChainComplexes`, or the new (and still under construction) `Complexes` package. To use `Complexes`, you must first load the `Complexes` package, while the `ChainComplexes` methods are automatically loaded with Macaulay2.

A.5.1 Chain Complexes

To create a new chain complex by hand, we start by setting up R-module maps.

```
i1 : R = QQ[a,b];

i2 : d1 = map(R^1, R^2, {{a,b}})

o2 = | a b |
             1       2
o2 : Matrix R  <--- R

i3 : d2 = map(R^2, R^1, {{-b},{a}})

o3 = | -b |
     | a  |
             2       1
o3 : Matrix R  <--- R
```

Keep in mind that the syntax of map is a bit funny: we write `map(target,source,matrix)`. To make sure we set up the next map in a way that is composable with d_1, we can use the methods `source` and `target`:

```
i3 : d1 = map(source d0, R^1, {{-b},{a}})

o3 = | -b |
     | a  |
             2       1
o3 : Matrix R  <--- R
```

We can also double check our maps do indeed map a complex, by checking the composition $d_1 \circ d_2$:

```
i4 : d1 * d2 == 0

o4 = true
```

So now we are ready to set up our new chain complex.

```
i5 : C = new ChainComplex

o5 = 0

o5 : ChainComplex

i6 : C#0 = target d1

      1
o6 = R

o6 : R-module, free

i7 : C#1 = target d2

      2
o7 = R

o7 : R-module, free

i8 : C#2 = source d2

      1
o8 = R

o8 : R-module, free
```

Given a chain complex `C`, we can ask Macaulay2 what our complex is by simply running the name of the complex:

```
i9 : C

      1      2      1
o9 = R  <-- R  <-- R

     0      1      2

o9 : ChainComplex
```

Or we can ask for a better visual description of the maps, using `C.dd`:

```
i10 : C.dd

            1         2
o10 = 0 : R  <----- R  : 1
                 0
```

```
           2         1
      1 : R  <----- R  : 2
                0

o10 : ChainComplexMap
```

We can also set up the same complex in a more compact way, by simply feeding the maps we want in order. Macaulay2 will automatically place the first map with the target in homological degree 0 and the source in degree 1.

```
11 : D = chainComplex(d1,d2)

       1      2      1
o11 = R  <-- R  <-- R

      0      1      2

o11 : ChainComplex
```

Notice this is indeed the same complex.

```
i12 : D.dd

           1               2
o12 = 0 : R  <----------- R  : 1
                | a b |

           2              1
      1 : R  <---------- R  : 2
                | -b |
                | a  |

o12 : ChainComplexMap
```

We can also ask Macaulay2 to compute the homology of our complex:

```
i13 : HH D

o13 = 0 : cokernel | a b |

      1 : subquotient (| b  |, | -b |)
                      | -a |  | a  |
      2 : image 0

o13 : GradedModule
```

Or we could simply ask for the homology in a specific degree:

```
i14 : HH_0 D

o14 = cokernel | a b |
                                1
o14 : R-module, quotient of R
```

A.5.2 The Complexes package

To use this functionality, you must first load the `Complexes` package.

```
i15 : needsPackage "Complexes";

o15 = Complexes

o15 : Package
```

We can use our maps from above to set up a complex with the same maps. We feed a list of the maps we want to use to the method `complex`.

```
i16 : F = complex({d1,d2})

       1      2      1
o16 = R  <-- R  <-- R

      0      1      2

o16 : Complex
```

We cam read off the maps and the homology in our complex using the same commands as we use with `chainComplexes`, although the information returned gets presented in a slightly different fashion.

```
i17 : HH F

o17 = cokernel | a b | <-- subquotient (| b  |, | -b |) <-- image 0
                                        | -a |  | a  |
      0                                                        2
                              1

o17 : Complex

i18 : F.dd

           1               2
```

```
o18 = 0 : R  <----------- R  : 1
                | a b |

            2              1
      1 : R  <---------- R  : 2
                | -b |
                | a  |

o18 : ComplexMap
```

If we want to set up our complex starting in a different homological degree, we can do the following:

```
i19 : G = complex({d1,d2}, Base => 7)

       1      2      1
o19 = R  <-- R  <-- R

      7      8      9

o19 : Complex

i20 : H = complex({d1,d2}, Base => -13)

       1       2       1
o20 = R   <-- R   <-- R

      -13     -12     -11

o20 : Complex
```

A.5.3 Maps of complexes

Suppose we are given two complexes `C` and `D` and a map of complexes `f : C` $\longrightarrow$ `D`. The routine `map` can be used to define f using `chainComplexes`: it receives the target `D`, the source `D`, and a function `f` that returns f_i when we compute `f(i)`.

```
i1 : R = QQ[a,b];

i2 : c1 = map(R^0,R^1,0);

                    1
o2 : Matrix 0 <--- R

i3 : c2 = map(R^1, R^2, {{a,b}});
```

```
             1       2
o3 : Matrix R  <--- R

i4 : c3 = map(R^2, R^1, {{-b},{a}});

             2       1
o4 : Matrix R  <--- R

i5 : c4 = map(R^1, R^0, 0);

             1
o5 : Matrix R  <--- 0

i6 : C = chainComplex(c1,c2,c3,c4);

i7 :
     d1 = map(R^0,R^1,0);

                    1
o7 : Matrix 0 <--- R

i8 : d2 = id_(R^1);

             1       1
o8 : Matrix R  <--- R

i9 : d3 = map(R^1, R^0, 0);

             1
o9 : Matrix R  <--- 0

i10 : d4 = map(R^0, R^0, 0);

o10 : Matrix 0 <--- 0

i11 : D = chainComplex(d1,d2,d3,d4)

             1      1
o11 = 0 <-- R  <-- R  <-- 0 <-- 0

      0     1      2      3     4

o11 : ChainComplex

i12 :
```

```
      f0 = map(R^0, R^0, 0);

o12 : Matrix 0 <--- 0

i13 : f1 = map(R^1, R^1, matrix{{0_R}});

              1       1
o13 : Matrix R  <--- R

i14 : f2 = map(R^2, R^1, {{b},{-a}});

              2       1
o14 : Matrix R  <--- R

i15 : f3 = map(R^1, R^0, 0);

              1
o15 : Matrix R  <--- 0

i16 : f4 = map(R^0, R^0, 0);

o16 : Matrix 0 <--- 0

i17 : f = map(C,D,i -> if i==0 then f0 else(
      if i==1 then f1 else (
      if i==2 then f2 else (
      if i == 3 then f3 else (
      if i==4 then f4)))))

o17 = 0 : 0 <----- 0 : 0
               0

           1         1
      1 : R  <----- R  : 1
                0

           2              1
      2 : R  <---------- R  : 2
                | b  |
                | -a |
           1
      3 : R  <----- 0 : 3
                0

      4 : 0 <----- 0 : 4
```

```
              0

o17 : ChainComplexMap
```

Here's what we can do if we prefer to write a list with the maps in `f`:

```
i18 : f = map(C,D,i -> {f0,f1,f2,f3,f4}_i)

o18 = 0 : 0 <----- 0 : 0
              0

           1         1
      1 : R  <----- R  : 1
                0

           2              1
      2 : R  <---------- R  : 2
                | b  |
                | -a |

           1
      3 : R  <----- 0 : 3
                0

      4 : 0 <----- 0 : 4
              0

o18 : ChainComplexMap
```

If we prefer to do the same with the `Complexes` package, one advantage is that `map` *does* receive `(target, source, list of maps)`.

```
i42 : C = complex({c1,c2,c3,c4});

i43 : D = complex({d1,d2,d3,d4});

i44 : f = map(C,D,{f0,f1,f2,f3,f4})

           2              1
o44 = 2 : R  <---------- R  : 2
                | b  |
                | -a |

o44 : ComplexMap
```

Appendix B

Commutative algebra background

B.1 Prime Avoidance

Theorem B.1 (Prime avoidance)**.** *Let R be a ring, $I_1, \dots, I_n, J$ be ideals, and suppose that I_i is prime for $i > 2$.*[1] *If $J \not\subseteq I_i$ for all i, then $J \not\subseteq \bigcup_i I_i$. Equivalently, if $J \subseteq \bigcup_i I_i$, then $J \subseteq I_i$ for some i. So if $J \not\subseteq I_i$ for all i, then we can find an element $x \in J$ such that $x \notin I_i$ for all i.*

Moreover, if R is $\mathbb{N}$-graded, and all of the ideals are homogeneous, all I_i are prime, and $J \not\subseteq I_i$ for all i, then there is a homogeneous element in J that is not in $\bigcup_i I_i$.

Proof. We proceed by induction on n. If $n = 1$, there is nothing to show.

By induction hypothesis, we can find elements a_i such that

$$a_i \notin \bigcup_{j \neq i} I_j \text{ and } a_i \in J$$

for each i. If some $a_i \notin I_i$, we are done, so let's assume that $a_i \in I_i$ for each i. Consider $a = a_n + a_1 \cdots a_{n-1} \in J$. Notice that $a_1 \cdots a_{n-1} = a_i(a_1 \cdots \widehat{a_i} \cdots a_{n-1}) \in I_i$. If $a \in I_i$ for $i < n$, then we also have $a_n \in I_i$, a contradiction. If $a \in I_n$, then we also have $a_1 \cdots a_{n-1} = a - a_n \in I_n$, since $a_n \in I_n$. If $n = 2$, this says $a_1 \in I_2$, a contradiction. If $n > 2$, our assumption is that I_n is prime, so one of $a_1, \dots, a_{n-1} \in I_n$, which is a contradiction. So a is the element we were searching for, meaning $a \notin I_i$ for all i.

If all I_i are homogeneous and prime, then we proceed as above but replacing a_n and $a_1, \dots, a_{n-1}$ with suitable powers so that $a_n + a_1 \cdots a_{n-1}$ is homogeneous. For example, we could take

$$a := a_n^{\deg(a_1) + \cdots \deg(a_{n-1})} + (a_1 \cdots a_{n-1})^{\deg(a_n)}.$$

The primeness assumption guarantees that noncontainments in ideals is preserved. □

Corollary B.2. *Let I be an ideal and M a finitely generated module over a Noetherian ring R. If I consists of zerodivisors on M, then $Im = 0$ for some nonzero $m \in M$.*

[1] So all the ideals are prime, except we may allow two of them to not be prime.

Proof. The assumption says that

$$I \subseteq \bigcup_{\mathfrak{p} \in \mathrm{Ass}(M)} (\mathfrak{p}).$$

By the assumptions, Theorem 1.44 applies, and it guarantees that this is a finite set of primes. By Prime Avoidance, $I \subseteq \mathfrak{p}$ for some $\mathfrak{p} \in \mathrm{Ass}(M)$. Equivalently, $I \subseteq \mathrm{ann}_R(m)$ for some nonzero $m \in M$. □

Later on, we will also need a slightly stronger version of Prime Avoidance, so we record it now.

Theorem B.3. *Let R be a ring, $P_1, \ldots, P_n$ prime ideals, $x \in R$ and I be an ideal in R. If $(x) + I \not\subseteq P_i$ for each i, then there exists $y \in J$ such that*

$$x + y \notin \bigcup_{i=1}^{n} P_i.$$

Proof. We proceed by induction on n. When $n = 1$, if every element of the form $x + y$ with $y \in R$ is in $P = P_1$, then multiplying by $r \in R$ we conclude that every $rx + y \in P$, meaning $(x) + I \subseteq P$.

Now suppose $n > 1$ and that we have shown the statement for $n - 1$ primes. If $P_i \subseteq P_j$ for some $i \neq j$, then we might as well exclude P_i from our list of primes, and the statement follows by induction. So assume that all our primes P_i are incomparable.

If $x \notin P_i$ for all i, we are done, since we can take $x + 0$ for the element we are searching for. So suppose x is in some P_i, which we assume without loss of generality to be P_n. Our induction hypothesis says that we can find $y \in I$ such that $x + y \notin P_1 \cup \cdots \cup P_{n-1}$. If $x + y \notin P_n$, we are done, so suppose $x + y \in P_n$. Since we assumed $x \in P_n$, we must have $I \not\subseteq P_n$, or else we would have had $(x) + I \subseteq P_n$. Now P_n is a prime ideal that does not contain $P_1, \ldots, P_{n-1}$, nor I, so

$$P \not\supseteq IP_1 \cdots P_{n-1}.$$

Choose $z \in IP_1 \cdots P_{n-1}$ not in P_n. Then $x + y + z \notin P_n$, since $z \notin P_n$ but $x + y \in P_n$. Moreover, for all $i < n$ we have $x + y + z \notin P_i$, since $z \in P_i$ and $x + y \notin P_i$. □

B.2 NAK

We will now show a very simple but extremely useful result known as Nakayama's Lemma. As noted in [Mat89, page 8], Nakayama himself claimed that this should be attributed to Krull and Azumaya, but it's not clear which of the three actually had the commutative ring statement first. So some authors (eg, Matsumura) prefer to refer to it as NAK. There are actually a range of statements, rather than just one, that go under the banner of Nakayama's Lemma a.k.a. NAK.

Proposition B.4. *Let R be a ring, I an ideal, and M a finitely generated R-module. If $IM = M$, then*

a) there is an element $r \in 1 + I$ such that $rM = 0$, and

b) there is an element $a \in I$ such that $am = m$ for all $m \in M$.

Proof. Let $M = Rm_1 + \cdots + Rm_s$. By assumption, we have equations

$$m_1 = a_{11}m_1 + \cdots + a_{1s}m_s \ , \ \ldots \ , \ m_s = a_{s1}m_1 + \cdots + a_{ss}m_s,$$

with $a_{ij} \in I$. Setting $A = [a_{ij}]$ and $v = [x_i]$ we have a matrix equations $Av = v$. By the determinantal trick, Lemma B.18, the element $\det(I_{s\times s} - A) \in R$ kills each m_i, and hence M. Since $\det(I_{s\times s} - A) \equiv \det(I_{s\times s}) \equiv 1 \bmod I$, this determinant is the element r we seek for the first statement.

For the latter statement, set $a = 1 - r$; this is in I and satisfies $am = m - rm = m$ for all $m \in M$. □

Proposition B.5. *Let $(R, \mathfrak{m}, k)$ be a local ring, and M be a finitely generated module. If $M = \mathfrak{m}M$, then $M = 0$.*

Proof. By the Proposition B.4, there exists an element $r \in 1 + \mathfrak{m}$ that annihilates M. Notice that $1 \notin \mathfrak{m}$, so any such r must be outside of $\mathfrak{m}$, and thus a unit. Multiplying by its inverse, we conclude that 1 annihilates M, or equivalently, that $M = 0$. □

Proposition B.6. *Let $(R, \mathfrak{m}, k)$ be a local ring, and M be a finitely generated module, and N a submodule of M. If $M = N + \mathfrak{m}M$, then $M = N$.*

Proof. By taking the quotient by N, we see that

$$M/N = (N + \mathfrak{m}M)/N = \mathfrak{m}\,(M/N)\,.$$

By Proposition B.5, $M = N$. □

Proposition B.7. *Let $(R, \mathfrak{m}, k)$ be a local ring, and M be a finitely generated module. For $m_1, \ldots, m_s \in M$,*

$$m_1, \ldots, m_s \text{ generate } M \iff \overline{m_1}, \ldots, \overline{m_s} \text{ generate } M/\mathfrak{m}M.$$

Thus, any generating set for M consists of at least $\dim_k(M/\mathfrak{m}M)$ elements.

Proof. The implication ($\Rightarrow$) is clear. If $m_1, \ldots, m_s \in M$ are such that $\overline{m_1}, \ldots, \overline{m_s}$ generate $M/\mathfrak{m}M$, let $N = Rm_1 + \cdots + Rm_s \subseteq M$. By Proposition B.5, $M/N = 0$ if and only if $M/N = \mathfrak{m}(M/N)$. The latter statement is equivalent to $M = \mathfrak{m}M + N$, which is equivalent to saying that $M/\mathfrak{m}M$ is generated by the image of N. □

Remark B.8. Since $R/\mathfrak{m}$ is a field, $M/\mathfrak{m}M$ is a vector space over the field $R/\mathfrak{m}$.

Definition B.9. Let $(R, \mathfrak{m})$ be a local ring, and M a finitely generated module. A set of elements $\{m_1, \ldots, m_t\}$ is a **minimal generating set** of M if the images of $m_1, \ldots, m_t$ form a basis for the $R/\mathfrak{m}$ vector space $M/\mathfrak{m}M$.

As a consequence of basic facts about basis for vector spaces, we conclude that any generating set for M contains a minimal generating set, and that every minimal generating set has the same cardinality.

Definition B.10. Let $(R, \mathfrak{m})$ be a local ring, and N an R-module. The **minimal number of generators** of M is

$$\mu(M) := \dim_{R/\mathfrak{m}} (M/\mathfrak{m}M) .$$

Equivalently, this is the number of elements in a minimal generating set for M.

We commented before that graded rings behave a lot like local rings, so now we want to give graded analogues for the results above.

Proposition B.11. *Let R be an $\mathbb{N}$-graded ring, and M a $\mathbb{Z}$-graded module such that $M_{<a} = 0$ for some a. If $M = (R_+)M$, then $M = 0$.*

Proof. On the one hand, the homogeneous elements in M live in degrees at least a, but $(R_+)M$ lives in degrees strictly bigger than a. If M has a nonzero element, it has a nonzero homogeneous element, and we obtain a contradiction. □

This condition includes all finitely generated $\mathbb{Z}$-graded R-modules.

Remark B.12. If M is finitely generated, then it can be generated by finitely many homogeneous elements, the homogeneous components of some finite generating set. If a is the smallest degree of a homogeneous element in a homogeneous generating set, since R lives only in positive degrees we must have $M \subseteq RM_{\geqslant a} \subseteq M_{\geqslant a}$, so $M_{<a} = 0$.

Just as above, we obtain the following:

Proposition B.13. *Let R be an $\mathbb{N}$-graded ring, with R_0 a field, and M a $\mathbb{Z}$-graded module such that $M_{<a} = 0$ for some degree a. A set of elements of M generates M if and only if their images in $M/(R_+)M$ spans as a vector space. Since M and $(R_+)M$ are graded, $M/(R_+)M$ admits a basis of homogeneous elements.*

In particular, if k is a field, R is a positively graded k-algebra, and I is a homogeneous ideal, then I has a minimal generating set by homogeneous elements, and this set is unique up to k-linear combinations.

Definition B.14. Let R be an $\mathbb{N}$-graded ring with R_0 a field, and M a finitely generated $\mathbb{Z}$-graded R-module. The **minimal number of generators** of M is

$$\mu(M) := \dim_{R/R_+} (M/R_+M) .$$

We can use Macaulay2 to compute (the) minimal (number of) generators of graded modules over graded k-algebras, using the commands `mingens` and `numgens`.

Note that we can use NAK to prove that certain modules are finitely generated in the graded case; in the local case, we cannot.

B.3 Krull's Intersection Theorem

Theorem B.15 (Krull intersection theorem)**.** *Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring. Then*

$$\bigcap_{n \geqslant 1} \mathfrak{m}^n = 0.$$

Proof. Let $J = \bigcap_{n \in \mathbb{N}} \mathfrak{m}^n$. First, we claim that $J \subseteq \mathfrak{m}J$.

Let $\mathfrak{m}J = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$ be a primary decomposition. To show that $J \subseteq \mathfrak{m}J$, it is sufficient to prove that $J \subseteq \mathfrak{q}_i$ for each i. If $\sqrt{\mathfrak{q}_i} \neq \mathfrak{m}$, pick $x \in \mathfrak{m}$ such that $x \notin \sqrt{\mathfrak{q}_i}$. Then $xJ \subseteq \mathfrak{m}J \subseteq \mathfrak{q}_i$, but $x \notin \sqrt{\mathfrak{q}_i}$, so $J \subseteq \mathfrak{q}_i$ by definition of primary. If instead $\sqrt{\mathfrak{q}_i} = \mathfrak{m}$, there is some N with $\mathfrak{m}^N \subseteq \mathfrak{q}_i$ by **??**. By definition of J, we have $J \subseteq \mathfrak{m}^N \subseteq \mathfrak{q}_i$, and we are done.

We showed that $J \subseteq \mathfrak{m}J$, hence $J = \mathfrak{m}J$, and thus $J = 0$ by NAK. □

This also holds over any domain without the local assumption.

Theorem B.16 (Krull Intersection Theorem for domains)**.** *If R is a domain, then*

$$\bigcap_{n \geqslant 1} I^n = 0.$$

for any proper ideal I in R.

Proof. Let $\mathfrak{m}$ be a maximal ideal in R. The only minimal prime over $\mathfrak{m}^n$ is $\mathfrak{m}$, so the powers of $\mathfrak{m}$ have no embedded primes and must then all be $\mathfrak{m}$-primary. In particular, $\mathfrak{m}^n = \mathfrak{m}^n R_{\mathfrak{m}} \cap R$. Notice that taking pre-images commutes with taking intersections, so

$$\bigcap_{n \geqslant 1} \mathfrak{m}^n = \bigcap_{n \geqslant 1} (\mathfrak{m}^n R_{\mathfrak{m}} \cap R) = \left(\bigcap_{n \geqslant 1} \mathfrak{m}^n R_{\mathfrak{m}} \right) \cap R = \left(\bigcap_{n \geqslant 1} \mathfrak{m}_{\mathfrak{m}}^n \right) \cap R.$$

By Theorem B.15, $\bigcap_{n \geqslant 1} \mathfrak{m}_{\mathfrak{m}}^n = 0$. Since R is a domain, the localization map is injective, and we conclude that

$$\bigcap_{n \geqslant 1} \mathfrak{m}^n = 0.$$

Now if I is any proper ideal in R, $I \subseteq \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$, and

$$\bigcap_{n \geqslant 1} I^n = \bigcap_{n \geqslant 1} \mathfrak{m}^n = 0.$$ □

B.4 Ring extensions

In field theory, there is a close relationship between (vector space-)finite field extensions and algebraic equations. The situation for rings is similar.

Definition B.17 (Integral element/extension)**.** Let R be an A-algebra. The element $r \in R$ is **integral** over A if there are elements $a_0, \ldots, a_{n-1} \in A$ such that

$$r^n + a_{n-1}r^{n-1} + \cdots + a_1 r + a_0 = 0;$$

i.e., r satisfies an **equation of integral dependence** over A. We say that R is **integral over** A if every $r \in R$ is integral over A.

Integral automatically implies algebraic, but the condition that there exists an equation of algebraic dependence that is *monic* is stronger in the setting of rings.

Lemma B.18 (Determinantal trick)**.** *Let R be a ring, $B \in M_{n\times n}(R)$, $v \in R^{\oplus n}$, and $r \in R$.*

1) $\mathrm{adj}(B)B = \det(B)I_{n\times n}$.

2) If $Bv = rv$, *then* $\det(rI_{n\times n} - B)v = 0$.

Proof.

1) When R is a field, this is a basic linear algebra fact. We deduce the case of a general ring from the field case.

   The ring R is a $\mathbb{Z}$-algebra, so we can write R as a quotient of some polynomial ring $\mathbb{Z}[X]$. Let $\psi : \mathbb{Z}[X] \twoheadrightarrow R$ be a surjection, $a_{ij} \in \mathbb{Z}[X]$ be such that $\psi(a_{ij}) = b_{ij}$, and let $A = [a_{ij}]$. Note that

   $$\psi(\mathrm{adj}(A)_{ij}) = \mathrm{adj}(B)_{ij} \quad \text{and} \quad \psi((\mathrm{adj}(A)A)_{ij}) = (\mathrm{adj}(B)B)_{ij},$$

   since ψ is a homomorphism, and the entries are the same polynomial functions of the entries of the matrices A and B, respectively. Thus, it suffices to establish

   $$\mathrm{adj}(B)B = \det(B)I_{n\times n}$$

   in the case when $R = \mathbb{Z}[X]$, and we can do this entry by entry. Now, $R = \mathbb{Z}[X]$ is an integral domain, hence a subring of a field (its fraction field). Since both sides of the equation

   $$(\mathrm{adj}(B)B)_{ij} = (\det(B)I_{n\times n})_{ij}$$

   live in R and are equal in the fraction field (by linear algebra) they are equal in R. This holds for all i, j, and thus 1) holds.

2) We have $(rI_{n\times n} - B)v = 0$, so by part 1)

   $$\det(rI_{n\times n} - B)v = \mathrm{adj}(rI_{n\times n} - B)(rI_{n\times n} - B)v = 0. \qquad \square$$

Theorem B.19. *Let $A \subseteq R$ be module-finite. Then R is integral over A.*

Proof. Given $r \in R$, we want to show that r is integral over A. The idea is to show that multiplication by r, realized as a linear transformation over A, satisfies the characteristic polynomial of that linear transformation.

Write $R = Ar_1 + \cdots Ar_t$. We may assume that $r_1 = 1$, perhaps by adding module generators. By assumption, we can find $a_{ij} \in A$ such that

$$rr_i = \sum_{j=1}^{t} a_{ij} r_j$$

for each i. Let $C = [a_{ij}]$, and v be the column vector $(r_1, \ldots, r_t)$. We have $rv = Cv$, so by the determinant trick, $\det(rI_{n\times n} - C)v = 0$. Since we chose one of the entries of v to be 1, we have in particular that $\det(rI_{n\times n} - C) = 0$. Expanding this determinant as a polynomial in r, this is a monic equation with coefficients in A. □

Lemma B.20. *If $R \subseteq S$ is an integral extension of domains, R is a field if and only S is a field.*

Proof. Take any nonzero $s \in S$, and consider an equation of integral dependance of s over R, say

$$s^n + a_{n-1}s^{n-1} + \cdots + a_1 s + a_0 = 0.$$

Since a_0 is a unit in $R \subseteq S$, we can divide by a_0, so that

$$-s(s^{n-1} + a_{n-1}s^{n-2} + \cdots + a_1) = 1.$$

The s is a unit, and S is a field.

If S is a field, and $r \in R$ is nonzero, then there exists an inverse s for r in S, which is integral over R. Then

$$s^n + a_{n-1}s^{n-1} + \cdots + a_1 s + a_0 = 0$$

for some $a_i \in R$, and multiplying through by r^{n-1} gives

$$s = -(a_{n-1} + a_{n-2}r \cdots + a_1 r^{n-2} + a_0 r^{n-1}) \in R.$$

Then R is a field. □

Index

$(I : J^\infty)$, 22
$I \cap R$, 6
I-depth, 59
IS, 6
I^n, 23
$K(r)$, 41
$K^\bullet(f_1, \ldots, f_n; M)$, 42
$K_\bullet(f_1, \ldots, f_n; M)$, 42
P-primary ideal, 14
$V(I)$, 2
$W^{-1}M$, 5
$W^{-1}\alpha$, 5
$\mathrm{Ass}_R(M)$, 8
$\mathrm{H}_i(x_1, \ldots, x_d; M)$, 44
$\mathrm{Min}(I)$, 3
$\mathrm{Spec}(R)$, 2
$\mathrm{Supp}(M)$, 7
$\alpha(I)$, 29
$\mathrm{ann}(M)$, 5
$\mathrm{depth}(M)$, 59
$\mathrm{depth}_I(M)$, 59
$\dim(R)$, 35
$\mathbb{V}(X)$, 77
$\mathbf{I}(V)$, 84
$\mathcal{A}$, 32
$\mathcal{N}(R)$, 4
$\mathcal{Z}(M)$, 9
$\mathrm{pdim}_R(M)$, 52
$\sqrt{I}$, 3
$\mathrm{embdim}(R)$, 40

absolutely minimal prime, 72
affine algebraic variety, 77
affine cone of a projective variety, 84
affine space, 77
algebraic set, 77
algebraic variety, 77
annihilator, 5
associated prime, 8
associated primes of an ideal, 8
Auslander—Buchsbaum formula, 64

betti numbers, 52

catenary ring, 36
chain of primes, 35
Cohen-Macaulay, 67
Cohen-Macaulay ring, 67
colon, 5
complete intersection, 39
contraction, 6
coordinate ring of a variety, 80

depth, 59
determinantal trick, 117
differential power, 91
dimension of a module, 35
dimension of a ring, 35

embedded prime, 12
embedding dimension, 40
equation of integral dependence, 117
equidimensional ring, 36
expansion of an ideal, 6

free resolution, 51

height, 35
height of a prime, 35
height of an ideal, 35
homogeneous coordinates, 83
homogeneous system of parameters, 68

ideal of points, 87

integral element, 117
integral over A, 117
irreducible ideal, 17
irredundant primary decomposition, 17
irrelevant maximal ideal, 85

Jacobson ring, 88

Koszul complex, 41, 43
Koszul complex of a module, 42
Koszul homology, 44
Krull dimension, 35
Krull Intersection Theorem, 116
Krull's Height Theorem, 38
Krull's Principal Ideal Theorem, 37

length of a chain of primes, 35
localization, 5
localization at a prime, 7
localization of a module, 5
localization of a ring, 5

minimal complex, 52
minimal free resolution, 52
minimal generating set, 114
minimal generators, 114
minimal number of generators, 115
minimal prime, 3

nilradical, 4
nonzerodivisor, 47

parameters, 68
perfect field, 93
primary decomposition, 17
primary ideal, 14
Prime avoidance, 112
projective dimension, 52
projective space, 83
projective variety, 84

radical ideal, 3
radical of an ideal, 3
regular element, 47
regular local ring, 40, 56
regular ring, 56
ring of differential operators, 90

saturated chain of primes, 35
saturation, 22
SOP, 68
spectrum of a ring, 2
support, 7
system of parameters, 68

tensor product of complexes, 41
transcendence basis, 40
transcendence degree, 40

variety, 77

zerodivisors, 9

Bibliography

[AM69] Michael F. Atiyah and Ian G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[BH93] Winfried Bruns and Jürgen Herzog. *Cohen-Macaulay rings*, volume 39 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1993.

[BJNB19] Holger Brenner, Jack Jeffries, and Luis Núñez-Betancourt. Quantifying singularities with differential operators. *Advances in Mathematics*, 358:106843, 2019.

[Bro79] Markus P. Brodmann. Asymptotic stability of $\mathrm{Ass}(M/I^nM)$. *Proc. Amer. Math. Soc.*, 74(1):16–18, 1979.

[Bui95] Alexandru Buium. Differential characters of abelian varieties over p-adic fields. *Inventiones mathematicae*, 122(2):309–340, 1995.

[Bui05] Alexandru Buium. *Arithmetic differential equations*, volume 118 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2005.

[CLO92] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992. An introduction to computational algebraic geometry and commutative algebra.

[CR21] Yairon Cid-Ruiz. Noetherian operators, primary submodules and symbolic powers. *Collect. Math.*, 72(1):175–202, 2021.

[DDSG+18] Hailong Dao, Alessandro De Stefani, Eloísa Grifo, Craig Huneke, and Luis Núñez Betancourt. Symbolic powers of ideals. In *Singularities and foliations. geometry, topology and applications*, volume 222 of *Springer Proc. Math. Stat.*, pages 387–432. Springer, Cham, 2018.

[DGP99] Wolfram Decker, Gert-Martin Greuel, and Gerhard Pfister. Primary decomposition: algorithms and comparisons. In *Algorithmic algebra and number theory (Heidelberg, 1997)*, pages 187–220. Springer, Berlin, 1999.

[DSGJ20] Alessandro De Stefani, Eloísa Grifo, and Jack Jeffries. A Zariski-Nagata theorem for smooth $\mathbb{Z}$-algebras. *J. Reine Angew. Math.*, 761:123–140, 2020.

[EH79] David Eisenbud and Melvin Hochster. A Nullstellensatz with nilpotents and Zariski's main lemma on holomorphic functions. *J. Algebra*, 58(1):157–161, 1979.

[EHV92] David Eisenbud, Craig Huneke, and Wolmer Vasconcelos. Direct methods for primary decomposition. *Invent. Math.*, 110(1):207–235, 1992.

[Eis95] David Eisenbud. *Commutative algebra with a view toward algebraic geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[HKV09] Craig Huneke, Daniel Katz, and Javid Validashti. Uniform Equivalente of Symbolic and Adic Topologies. *Illinois Journal of Mathematics*, 53(1):325–338, 2009.

[Hoc78] Melvin Hochster. Some applications of the Frobenius in characteristic 0. *Bulletin of the American Mathematical Society*, 84(5):886 – 912, 1978.

[HR74] Melvin Hochster and Joel L. Roberts. Rings of invariants of reductive groups acting on regular rings are Cohen-Macaulay. *Advances in Math.*, 13:115–175, 1974.

[HS02] Serkan Hoşten and Gregory G. Smith. Monomial ideals. In *Computations in algebraic geometry with Macaulay 2*, volume 8 of *Algorithms Comput. Math.*, pages 73–100. Springer, Berlin, 2002.

[Joy85] A. Joyal. δ-anneaux et vecteurs de Witt. *C.R. Acad. Sci. Canada*, VII(3):177–182, 1985.

[Las05] Emanuel Lasker. Zur theorie der moduln und ideale. *Mathematische Annalen*, 60:20–116, 1905.

[Mat80] Hideyuki Matsumura. *Commutative algebra*, volume 56 of *Mathematics Lecture Note Series*. Benjamin/Cummings Publishing Co., Inc., Reading, Mass., second edition, 1980.

[Mat89] Hideyuki Matsumura. *Commutative ring theory*, volume 8 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1989. Translated from the Japanese by M. Reid.

[Mor96] Susan Morey. Equations of blowups of ideals of codimension two and three. *J. Pure Appl. Algebra*, 109(2):197–211, 1996.

[Nag62] Masayoshi Nagata. *Local rings*. Interscience, 1962.

[Noe21] Emmy Noether. Idealtheorie in ringbereichen. *Mathematische Annalen*, 83(1):24–66, 1921.

[Rat76] Louis J. Ratliff. On prime divisors of I^n, n large. *Michigan Math. J.*, 23(4):337–352, 1976.

[SGJ21] Alessandro De Stefani, Eloísa Grifo, and Jack Jeffries. A uniform chevalley theorem for direct summands of polynomial rings in mixed characteristic, 2021.

[SY96] Takeshi Shimoyama and Kazuhiro Yokoyama. Localization and primary decomposition of polynomial ideals. *J. Symbolic Comput.*, 22(3):247–277, 1996.

[Zar49] Oscar Zariski. A fundamental lemma from the theory of holomorphic functions on an algebraic variety. *Ann. Mat. Pura Appl. (4)*, 29:187–198, 1949.