Commutative Algebra

Math 225 Winter 2021

and

Homological Algebra

Math 224 Spring 2021

Eloísa Grifo
University of California, Riverside

March 9, 2021

Warning!

Proceed with caution. These notes are under construction and are 100% guaranteed to contain typos. If you find any typos or errors, I will be most grateful to you for letting me know. If you are looking for a place where to learn commutative algebra or homological algebra , I strongly recommend the following excellent resources:

- Mel Hochster's Lecture notes
- Jack Jeffries' Lecture notes (either his UMich 614 notes or his CIMAT notes)
- Atiyah and MacDonald's *Commutative Algebra* [AM69]
- Matsumura's *Commutative Ring Theory* [Mat89], or his other less known book *Commutative Algebra* [Mat80]
- Eisenbud's *Commutative Algebra with a view towards algebraic geometry* [Eis95]
- Rotman's *An introduction to homological algebra* second edition. [Rot09]

Acknowledgements

These notes are heavily based on Jack Jeffries and Alexandra Seceleanu's notes, and I thank them for sharing their notes with me. Thank you also to all the students in my commutative algebra class at UCR in Winter 2021 for their comments and questions that lead to multiple improvements, especially Brandon Massaro, Adam Richardson, Khoa Ta, and Ryan Watson, who found typos and errors.

Contents

Chapter 0

Setting the stage

In this chapter we set the stage for what's to come in the rest of the class. The definitions and facts we collect here should be somewhat familiar to you already, and so we present them in rapid fire succession. You can learn more about the basic theory of (commutative) rings and R-modules in any introductory algebra book, such as [DF04].

0.1 Basic definitions: rings and ideals

Roughly speaking, Commutative Algebra is the branch of algebra that studies commutative rings and modules over such rings. For a commutative algebraist, every ring is commutative and has a $1 \neq 0$.

Definition 0.1 (Ring)**.** A **ring** is a set R equipped with two binary operations $+$ and $\cdot$ satisfying the following properties:

1) R is an abelian group under the addition operation $+$, with additive identity 0.[1] Explicitly, this means that
   - $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$,
   - $a + b = b + a$ for all $a, b \in R$,
   - there is an element $0 \in R$ such that $0 + a = a$ for all $a \in R$, and
   - for each $a \in R$ there exists an element $-a \in R$ such that $a + (-a) = 0$.
2) R is a commutative monoid under the multiplication operation $\cdot$, with multiplicative identity 1.[2] Explicitly, this means that
   - $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$,
   - $a \cdot b = b \cdot a$ for all $a, b \in R$, and

[1] Or 0_R if we need to specify which ring we are talking about.
[2] If we need to specify the corresponding ring, we may write 1_R.

- there exists an element $1 \in R$ such that $1 \cdot a = a \cdot 1$ for all $a \in R$.

3) multiplication is distributive with respect to addition, meaning that

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

for all $a, b, c \in R$.

4) $1 \neq 0$.

We typically write ab for $a \cdot b$.

While in some branches of algebra rings might fail to be commutative, we will explicitly say we have a *noncommutative ring* if that is the case, and otherwise all rings are assumed to be commutative. There also branches of algebra where rings might be assumed to not necessarily have a multiplicative identity; we recommend [Poo19] for an excellent read on the topic of *Why rings should have a 1*.

Example 0.2. Here are some examples of the kinds of rings we will be talking about.

a) The integers $\mathbb{Z}$.

b) Any quotient of $\mathbb{Z}$, which we write compactly as $\mathbb{Z}/n$.

c) A polynomial ring. When we say polynomial ring, we typically mean $R = k[x_1, \ldots, x_n]$, a polynomial ring in finitely many variables over a field k.

d) A quotient of a polynomial ring by an ideal I, say $R = k[x_1, \ldots, x_n]/I$.

e) Rings of polynomials in infinitely many variables, $R = k[x_1, x_2, \ldots]$.

f) Power series rings $R = k[\![x_1, \ldots, x_n]\!]$. The elements are (formal) power series $\sum_{a_i \geqslant 0} c_{a_1,\ldots,a_n} x_1^{a_1} \cdots x_n^{a_n}$.

g) While any field k is a ring, we will see that fields on their own are not very exciting from the perspective of the kinds of things we will be discussing in this class.

Definition 0.3 (ring homomorphism)**.** A map $R \xrightarrow{f} S$ between rings is a **ring homomorphism** if f preserves the operations and the multiplicative identity, meaning

- $f(a + b) = f(a) + f(b)$ for all $a, b \in R$,
- $f(ab) = f(a)f(b)$ for all $a, b \in R$, and
- $f(1) = 1$.

A bijective ring homomorphism is an **isomorphism**. We should think about a ring isomorphism as a relabelling of the elements in our ring.

Definition 0.4. A subset $R \subseteq S$ of a ring S is a **subring** if R is also a ring with the structure induced by S, meaning that the each operation on R is the restrictions of the corresponding operation on S to R, and the 0 and 1 in R are the 0 and 1 in S, respectively.

Often, we care about the ideals in a ring more than we care about individual elements.

Definition 0.5 (ideal)**.** A nonempty subset I of a ring R is an **ideal** if it is closed for the addition and for multiplication by any element in R: for any $a, b \in I$ and $r \in R$, we must have $a + b \in I$ and $ra \in I$.

The **ideal generated by** $f_1, \ldots, f_n$, denoted $(f_1, \ldots, f_n)$, is the smallest ideal containing $f_1, \ldots, f_n$, or equivalently,

$$(f_1, \ldots, f_n) = \{r_1 f_1 + \cdots r_n f_n \,|\, r_i \in R\}\,.$$

Example 0.6. Every ring has always at least 2 ideals, the zero ideal $(0) = \{0\}$ and the unit ideal $(1) = R$.

We will follow the convention that when we say *ideal* we actually mean every ideal $I \neq R$.

Exercise 1. The ideals in $\mathbb{Z}$ are the sets of multiples of a fixed integer, meaning every ideal has the form (n). In particular, every ideal in $\mathbb{Z}$ can be generated by one element.

This makes $\mathbb{Z}$ the canonical example of a **principal ideal domain**.

A **domain** is a ring with no zerodivisors, meaning that $rs = 0$ implies that $r = 0$ or $s = 0$. A **principal ideal** is an ideal generated by one element. A **principal ideal domain** or **PID** is a domain where every ideal is principal.

Exercise 2. Given a field k, $R = k[x]$ is a principal ideal domain, so every ideal in R is of the form $(f) = \{fg \,|\, g \in R\}$.

Exercise 3. While $R = k[x, y]$ is a domain, it is **not** a PID. We will see later that every ideal in R is finitely generated, and yet we can construct ideals in R with arbitrarily many generators!

Example 0.7. While $\mathbb{Z}[x]$ is a domain, it is also **not** a PID. For example, $(2, x)$ is not a principal ideal.

Finally, here is an elementary fact we will need, known as the Chinese Remainder Theorem:

Theorem 0.8. *Let R be a ring and $I_1, \ldots, I_n$ be pairwise coprime ideals in R, meaning $I_i + I_j = R$ for all $i \neq j$. Then $I := I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$, and there is an isomorphism of rings*

$$R/I \xrightarrow{\cong} R/I_1 \times \cdots \times R/I_n\ .$$

$$r + I \longmapsto (r + I_1, \ldots, r + I_n)$$

0.2 Basic definitions: modules

Similarly to how linear algebra is the study of vector spaces over fields, commutative algebra often focuses on the structure of modules over a given commutative ring R. While in other branches of algebra modules might be left- or right-modules, all our modules are two sided, and we refer to them simply as modules.

Definition 0.9 (Module)**.** Given a ring R, an **R-module** $(M, +)$ is an abelian group equipped with an R-action that is compatible with the group structure. More precisely, there is an operation $\cdot : R \times M \longrightarrow M$ such that

- $r \cdot (a + b) = r \cdot a + r \cdot b$ for all $r \in R$ and $a, b \in M$,
- $(r + s) \cdot a = r \cdot a + s \cdot a$ for all $r, s \in R$ and $a \in M$,
- $(rs) \cdot a = r \cdot (s \cdot a)$ for all $r, s \in R$ and $a \in M$, and
- $1 \cdot a = a$ for all $a \in M$.

We typically write ra for $r \cdot a$. We denote the additive identity in M by 0, or 0_M if we need to distinguish it from 0_R.

The definitions of submodule, quotient of modules, and homomorphism of modules are very natural and easy to guess, but here they are.

Definition 0.10. If $N \subseteq M$ are R-modules with compatible structures, we say that M is a **submodule** of M.

A map $M \xrightarrow{f} N$ between R-modules is a **homomorphism of R-modules** if it is a homomorphism of abelian groups that preserves the R-action, meaning $f(ra) = rf(a)$ for all $r \in R$ and all $a \in M$. We sometimes refer to R-module homomorphisms as **R-module maps**, or **maps of R-modules**. An isomorphism of R-modules is a bijective homomorphism, which we really should think about as a relabeling of the elements in our module. If two modules M and N are isomorphic, we write $M \cong N$.

Given an R-module M and a submodule $N \subseteq M$, the **quotient** M/N is an R-module whose elements are the equivalence classes determined by the relation on M given by $a \sim b \Leftrightarrow a - b \in N$. One can check that this set naturally inherits an R-module structure from the R-module structure on M, and it comes equipped with a natural **canonical map** $M \longrightarrow M/N$ induced by sending 1 to its equivalence class.

Example 0.11. The modules over a field k are precisely all the k-vector spaces. Linear transformations are precisely all the k-module maps.

While vector spaces make for a great first example, be warned that many of the basic facts we are used to from linear algebra are often a little more subtle in commutative algebra. These differences are features, not bugs.

Example 0.12. The $\mathbb{Z}$-modules are precisely all the abelian groups.

Example 0.13. When we think of the ring R as a module over itself, the submodules of R are precisely the ideals of R.

Exercise 4. The kernel $\ker f$ and image $\operatorname{im} f$ of an R-module homomorphism $M \xrightarrow{f} N$ are submodules of M and N, respectively.

Theorem 0.14 (First Isomorphism Theorem)**.** *Given a homomorphism of R-modules $M \xrightarrow{f} N$, $M/\ker f \cong \operatorname{im} f$.*

The first big noticeable difference between vector spaces and more general R-modules is that while every vector space has a basis, most R-modules do not.

Definition 0.15. A subset $\Gamma \subseteq M$ of an R-module M is a **generating set**, or a **set of generators**, if every element in M can be written as a finite linear combination of elements in M with coefficients in R. A **basis** for an R-module M is a generating set Γ for M such that $\sum_i a_i\gamma_i = 0$ implies $a_i = 0$ for all i. An R-module is **free** if it has a basis.

Remark 0.16. Every vector space is a free module.

Remark 0.17. Every free R-module is isomorphic to a direct sum of copies of R. Indeed, let's construct such an isomorphism for a given free R-module M. Given a basis $\Gamma = \{\gamma_i\}_{i\in I}$ for M, let

$$\bigoplus_{i\in I} R \xrightarrow{\pi} M \quad .$$

$$(r_i)_{i\in I} \longrightarrow \sum_i r_i\gamma_i$$

The condition that Γ is a basis for M can be restated into the statement that π is an isomorphism of R-modules.

One of the key things that makes commutative algebra so rich and beautiful is that most modules are in fact *not* free. In general, every R-module has a generating set — for example, M itself. Given some generating set Γ for M, we can always repeat the idea above and write a **presentation** $\oplus_{i\in I} R \xrightarrow{\pi} M$ for M, but in general the resulting map π will have a nontrivial kernel. A nonzero kernel element $(r_i)_{i\in I} \in \ker \pi$ corresponds to a **relation** between the generators of M.

Remark 0.18. Given a set of generators for an R-module M, any homomorphism of R-modules $M \longrightarrow N$ is determined by the images of the generators.

We say that a module is **finitely generated** if we can find a finite generating set for M. The simplest finitely generated modules are the cyclic modules.

Example 0.19. An R-module is **cyclic** if it can be generated by one element. Equivalently, we can write M as a quotient of R by some ideal I. Indeed, given a generator m for M, the kernel of the map $R \xrightarrow{\pi} M$ induced by $1 \mapsto m$ is some ideal I. Since we assumed that m generates M, π is automatically surjective, and thus induces an isomorphism $R/I \cong M$.

Similarly, if an R-module has n generators, we can naturally think about it as a quotient of R^n by the submodule of relations among those n generators.

0.3 Why study commutative algebra?

There are many reasons why one would want to study commutative algebra. For starters, it's fun! Also, modern commutative algebra has connections with many fields of mathematics, including:

- Algebra Geometry
- Algebraic Topology
- Homological Algebra
- Category Theory
- Number Theory
- Arithmetic Geometry
- Combinatorics
- Invariant Theory
- Representation Theory
- Differential Algebra
- Lie Algebras
- Cluster Algebras

Part I

Commutative Algebra

Chapter 1

Finiteness conditions

1.1 Noetherian rings and modules

The most common assumption in commutative algebra is to require that our rings be Noetherian. Noetherian rings are named after Emmy Noether, who is in many ways the mother of modern commutative algebra. Many rings that one would naturally want to study are noetherian.

Definition 1.1 (Noetherian ring)**.** A ring R is *Noetherian* if every ascending chain of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

eventually stabilizes: there is some N for which $I_n = I_{n+1}$ for all $n \geqslant N$.

This condition can be restated in various equivalent forms.

Proposition 1.2. *Let R be a ring. The following are equivalent:*

1) R is a Noetherian ring.

2) Every nonempty family of ideals has a maximal element (under $\subseteq$).

3) Every ascending chain of finitely generated ideals of R stabilizes.

4) Given any generating set S for an ideal I, I is generated by a finite subset of S.

5) Every ideal of R is finitely generated.

Proof.
(1)⇒(2): We prove the contrapositive. Suppose there is a nonempty family of ideals with no maximal element. This means that we can keep inductively choosing larger ideals from this family to obtain an infinite properly ascending chain.
(2)⇒(1): An ascending chain of ideals is a family of ideals, and the maximal ideal in the family indicates where our chain stabilizes.

(1)⇒(3): Clear.

(3)⇒(4): Let's prove the contrapositive. Suppose that there is an ideal I and a generating set S for I such that no finite subset of S generates I. So for any finite $S' \subseteq S$ we have $(S') \subsetneq (S) = I$, so there is some $s \in S \smallsetminus (S')$. Thus, $(S') \subsetneq (S' \cup \{s\})$. Inductively, we can continue this process to obtain an infinite proper chain of finitely generated ideals, contradicting (3).

(4)⇒(5): Clear.

(5)⇒(1): Given an ascending chain of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

let $I = \bigcup_{n\in\mathbb{N}} I_n$. In general, the union of two ideals might fail to be an ideal, but the union of a chain of ideals is an ideal (exercise). By assumption, the ideal I is finitely generated, say $I = (a_1, \ldots, a_t)$, and since each a_i is in some I_{n_i}, there is an N such that every a_i is in I_N. But then $I_N = I$, and thus $I_n = I_{n+1}$ for all $n \geqslant N$. □

Remark 1.3. When we say that every non-empty family of ideals has a maximal element, that maximal element does not have to be unique in any way. An ideal I is maximal in the family $\mathcal{F}$ if $I \subseteq J$ for some $J \in \mathcal{F}$ implies $I = J$; we might have many incomparable maximal elements in $\mathcal{F}$. For example, every element in the family of ideals in $\mathbb{Z}$ given by

$$\mathcal{F} = \{(p) \mid p \text{ is a prime integer}\}$$

is maximal.

Remark 1.4. If R is a Noetherian ring and S is a non-empty set of ideals in R, not only does S have a maximal element, but every element in S must be contained in a maximal element of S. Given an element $I \in S$, the subset T of S of ideals in S that contain I is nonempty, and must then contain a maximal element J by Proposition 1.2. If $J \subseteq L$ for some $L \in S$, then $I \subseteq L$, so $L \in T$, and thus by maximality of J in T, we must $J = L$. This proves that J is in fact a maximal element in S, and by construction it contains I.

Example 1.5.

1) If $R = k$ is a field, the only ideals in k are (0) and $(1) = k$, so k is a Noetherian ring.

2) $\mathbb{Z}$ is a Noetherian ring. More generally, if R is a PID, then R is Noetherian. Indeed, every ideal is finitely generated!

3) As a special case of the previous example, consider the ring of germs of complex analytic functions near 0,

$$\mathbb{C}\{z\} := \{f(z) \in \mathbb{C}[\![z]\!] \mid f \text{ is analytic on a neighborhood of } z = 0\}.$$

This ring is a PID: every ideal is of the form (z^n), since any $f \in \mathbb{C}\{z\}$ can be written as $z^n g(z)$ for some $g(z) \neq 0$, and any such $g(z)$ is a unit in $\mathbb{C}\{z\}$.

4) A ring that is *not* Noetherian is a polynomial ring in infinitely many variables over a field k, $R = k[x_1, x_2, \ldots]$: the ascending chain of ideals

$$(x_1) \subseteq (x_1, x_2) \subseteq (x_1, x_2, x_3) \subseteq \cdots$$

does *not* stabilize.

5) The ring $R = K[x, x^{1/2}, x^{1/3}, x^{1/4}, x^{1/5}, \ldots]$ is also *not* Noetherian . A nice ascending chain of ideals is

$$(x) \subsetneq (x^{1/2}) \subsetneq (x^{1/3}) \subsetneq (x^{1/4}) \subsetneq \cdots .$$

6) The ring of continuous real-valued functions $\mathcal{C}(\mathbb{R}, \mathbb{R})$ is *not* Noetherian: the chain of ideals

$$I_n = \{f(x) \mid f|_{[-1/n, 1/n]} \equiv 0\}$$

is increasing and proper. The same construction shows that the ring of infinitely differentiable real functions $\mathcal{C}^\infty(\mathbb{R}, \mathbb{R})$ is not Noetherian: properness of the chain follows from, e.g., Urysohn's lemma (though it's not too hard to find functions distinguishing the ideals in the chain). Note that if we asked for analytic functions instead of infinitely-differentiable functions, every element of the chain would be the zero ideal!

Remark 1.6. If R is Noetherian, and I is an ideal of R, then R/I is Noetherian as well, since there is an order-preserving bijection

$$\{\text{ideals of } R \text{ that contain } I\} \longleftrightarrow \{\text{ideals of } R/I\}.$$

This gives us many more examples, by simply taking quotients of the examples above. We will also see huge classes of easy examples once we learn about localization.

Similarly, we can define noetherian modules.

Definition 1.7 (Noetherian module)**.** An R-module M is *Noetherian* if every ascending chain of submodules of M eventually stabilizes.

There are analogous equivalent definitions for modules as we had above for rings, so we leave the proof as an exercise.

Proposition 1.8 (Equivalence definitions for Noetherian module)**.** *Let M be an R-module. The following are equivalent:*

1) M is a Noetherian module.

2) Every nonempty family of submodules has a maximal element.

3) Every ascending chain of finitely generated submodules of M eventually stabilizes.

4) Given any generating set S for a submodule N, the submodule N is generated by a finite subset of S.

5) Every submodule of M is finitely generated.

In particular, a Noetherian module must be finitely generated.

Remark 1.9. A ring R is a Noetherian ring if and only if R is Noetherian as a module over itself. However, a Noetherian ring need not be a Noetherian module over a subring. For example, consider $\mathbb{Z} \subseteq \mathbb{Q}$. These are both Noetherian *rings*, but $\mathbb{Q}$ is not a noetherian $\mathbb{Z}$-module; for example, the following is an ascending chain of submodules which does not stabilize:

$$0 \subsetneq \frac{1}{2}\mathbb{Z} \subsetneq \frac{1}{2}\mathbb{Z} + \frac{1}{3}\mathbb{Z} \subsetneq \frac{1}{2}\mathbb{Z} + \frac{1}{3}\mathbb{Z} + \frac{1}{5}\mathbb{Z} \subsetneq \cdots .$$

Definition 1.10. An **exact sequence** of R-modules is a sequence

$$\cdots \xrightarrow{f_{n-1}} M_n \xrightarrow{f_n} M_{n+1} \xrightarrow{f_{n+1}} \cdots$$

of R-modules and R-module homomorphisms such that $\operatorname{im} f_n = \ker f_{n+1}$ for all n. An exact sequence of the form

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

is a **short exact sequence**.

Remark 1.11. The sequence

$$0 \longrightarrow M \xrightarrow{f} N$$

is exact if and only if f is injective. Similarly,

$$M \xrightarrow{f} N \longrightarrow 0$$

is exact if and only if f is surjective. So

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

is a short exact sequence if and only if

- f is injective
- g is surjective
- $\operatorname{im} f = \ker g$.

So when this is indeed a short exact sequence, we can identify A with its image $f(A)$, and $A = \ker g$. Moreover, since g is surjective, by the First Isomorphism Theorem we conclude that $C \cong B/A$, so we might abuse notation and identify C with B/A.

Lemma 1.12 (Noetherianity in exact sequences)**.** *In an exact sequence of modules*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

B is Noetherian if and only if A and C are Noetherian.

Proof. Assume B is Noetherian. Since A is a submodule of B, and its submodules are also submodules of B, A is Noetherian. Moreover, any submodule of B/A is of the form D/A for some submodule $D \supseteq A$ of B. Since every submodule of B is finitely generated, every submodule of C is also finitely generated. Therefore, C is Noetherian.

Conversely, assume that A and C are Noetherian, and let

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$$

be a chain of submodules of B. First, note that

$$M_1 \cap A \subseteq M_2 \cap A \subseteq \cdots$$

is an ascending chain of submodules of A, and thus it stabilizes. Moreover,

$$g(M_1) \subseteq g(M_2) \subseteq g(M_3) \subseteq \cdots$$

is a chain of submodules of C, and thus it also stabilizes. Pick a large enough index n such that both of these chains stabilize. We claim that $M_n = M_{n+1}$, so that the original chain stabilizes as well. To show that, take $x \in M_{n+1}$. Then

$$g(x) \in g(M_{n+1}) = g(M_n)$$

so we can choose some $y \in M_n$ such that $g(x) = g(y)$. Then $x - y \in \ker g = \operatorname{im} f = A$. Now note that $x - y \in M_{n+1}$, so

$$x - y \in M_{n+1} \cap A = M_n \cap A.$$

Then $x - y \in M_n$, and since $y \in M_n$, we must have $x \in M_n$ as well. □

Corollary 1.13. *If A and B are Noetherian R-modules, then $A \oplus B$ is a Noetherian R-module.*

Proof. Apply the previous lemma to the short exact sequence

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

Corollary 1.14. *A module M is Noetherian if and only if M^n is Noetherian for some n. In particular, if R is a Noetherian ring then R^n is a Noetherian module.*

Proof. We will do induction on n. The case $n = 1$ is a tautology. For $n > 1$, consider the short exact sequence

$$0 \longrightarrow M^{n-1} \longrightarrow M^n \longrightarrow M \longrightarrow 0$$

Lemma 1.12 and the inductive hypothesis give the desired conclusion. □

Proposition 1.15. *Let R be a Noetherian ring. Given an R-module M, M is a Noetherian R-module if and only if M is finitely generated. Consequently, any submodule of a finitely generated R-module is also finitely generated.*

Proof. If M is Noetherian, M is finitely generated by the equivalent definitions above, and so are all of its submodules.

Now let R be Noetherian and M be a finitely generated R-module. Then M is isomorphic to a quotient of R^n for some n, which is Noetherian. □

Remark 1.16. The Notherianity hypothesis is important: if M is a finitely generated R-module over a non-Noetherian ring, M might not be Noetherian. For a dramatic example, note that R itself is a finitely generated R-module, but not Noetherian.

David Hilbert had a big influence in the early years of commutative algebra, in many different ways. Emmy Noether's early work in algebra was in part inspired by some of his work, and he later invited Emmy Noether to join the Göttingen Math Department — many of her amazing contributions to algebra happened during her time in Göttingen. Unfortunately, some of the faculty was opposed to having a woman joining the department, and for her first two years in Göttingen Noether did not have an official position nor was she paid. Hilbert's contributions also include three of the most fundamental results in commutative algebra — Hilbert's Basis Theorem, the Hilbert Syzygy Theorem, and Hilbert's Nullstellensatz. We can now prove the first.

Theorem 1.17 (Hilbert's Basis Theorem)**.** *Let R be a Noetherian ring. Then the rings $R[x_1, \ldots, x_d]$ and $R[\![x_1, \ldots, x_d]\!]$ are Noetherian.*

Remark 1.18. We can rephrase this theorem in a way that can be understood by anyone with a basic high school algebra (as opposed to abstract algebra) knowledge:

> Any system of polynomial equations in finitely many variables can be written in terms of finitely many equations.

Proof. We give the proof for polynomial rings, and indicate the difference in the power series argument. By induction on d, we can reduce to the case $d = 1$. Given $I \subseteq R[x]$, let

$$J = \{a \in R \mid \text{there is some } ax^n + \text{lower order terms (wrt } x) \in I\}.$$

So $J \subseteq R$ consists of all the leading coefficients of polynomials in I. We can check (exercise) that this is an ideal of R. By our hypothesis, J is finitely generated, so let $J = (a_1, \ldots, a_t)$. Pick $f_1, \ldots, f_t \in R[x]$ such that the leading coefficient of f_i is a_i, and set $N = \max_i\{\deg f_i\}$.

Given any $f \in I$ of degree greater than N, we can cancel off the leading term of f by subtracting a suitable combination of the f_i, so any $f \in I$ can be written as $f = g + h$ where $h \in (f_1, \ldots, f_t)$ and $g \in I$ has degree at most N, so $g \in I \cap (R + Rx + \cdots + Rx^N)$. Note that since $I \cap (R + Rx + \cdots + Rx^N)$ is a submodule of the finitely generated free R-module $R + Rx + \cdots + Rx^N$, it is also finitely generated as an R-module. Given such a generating set, say $I \cap (R + Rx + \cdots + Rx^N) = (f_{t+1}, \ldots, f_s)$, we can write any such $f \in I$ as an $R[x]$-linear combination of these generators and the f_i's. Therefore, $I = (f_1, \ldots, f_t, f_{t+1}, \ldots, f_s)$ is finitely generated, and $R[x]$ is a Noetherian ring.

In the power series case, take J to be the coefficients of *lowest degree* terms. □

1.2 Algebra finite-extensions

If R is a subring of S, then S is an **algebra** over R, meaning that S is a ring with a (natural) structure of an R-module that also satisfies

$$r(s_1 s_2) = (rs_1)s_2 \text{ for all } r \in R \text{ and } s_1, s_2 \in S.$$

More generally, given any ring homomorphism $\varphi : R \to S$, we can view S as an algebra over R via φ by setting $r \cdot s = \varphi(r)s$. We may abuse notation and write $r \in S$ for its image $\varphi(r) \in S$. We will see that in a lot of situations we want to study, it is enough to consider the case when φ is injective, so this abuse of notation makes sense. Giving a ring homomorphism $R \to S$ is the same as giving an R-algebra structure to S. In particular, a ring S can have different R-algebra structures given by different homomorphisms $R \to S$.

A set of elements $\Lambda \subseteq S$ **generates** S as an R-algebra if the following equivalent conditions hold:

- The only subring of S containing $\varphi(R)$ and Λ is S itself.
- Every element of S admits a polynomial expression in Λ with coefficients in $\varphi(R)$.
- Given a polynomial ring $R[X]$ on $|\Lambda|$ indeterminates, the ring homomorphism

$$\begin{aligned} R[X] &\xrightarrow{\psi} S \\ x_i &\longmapsto \lambda_i \end{aligned}$$

  is surjective.

Let S be an R-algebra and $\Lambda \subseteq S$ be a set of algebra generators for S over R. The ideal of **relations** on the elements Λ over R is the kernel of the map $\psi : R[X] \longrightarrow S$ above. This ideal consists of the polynomial functions with R-coefficients that the elements of Λ satisfy. Given an R-algebra S with generators Λ and ideal of relations I, we have a ring isomorphism $S \cong R[X]/I$ by the First Isomorphism Theorem. If we understand the ring R and generators and relations for S over R, we can get a pretty concrete understanding of S. If a sequence of elements has no nonzero relations, we say they are *algebraically independent* over R.

Remark 1.19. If $s_1, \ldots, s_n \in S$ are algebraically independent over R, then $R[s_1, \ldots, s_n]$ is isomorphic to the polynomial ring in n variables obver R.

We say that $\varphi : R \to S$ is **algebra-finite**, or S is a **finitely generated R-algebra**, or S is of **finite type** over R, if there exists a *finite* set of elements $f_1, \ldots, f_t \in S$ that generates S as an R-algebra. A better name might be *finitely generatable*, since to say that an algebra is finitely generated does not require knowing any actual finite set of generators. From the discussion above, we conclude that S is a finitely generated

R-algebra if and only if S is a quotient of some polynomial ring $R[x_1, \ldots, x_d]$ over R in finitely many variables. If S is generated over R by $f_1, \ldots, f_d$, we will use the notation $R[f_1, \ldots, f_d]$ to denote S. Of course, for this notation to properly specify a ring, we need to understand how these generators behave under the operations. This is no problem if A and $\underline{f}$ are understood to be contained in some larger ring.

Remark 1.20. Any surjective ring homomorphism $\varphi : R \to S$ is algebra-finite, since S must then be generated over R by 1. Moreover, we can always factor φ as the surjection $R \twoheadrightarrow R/\ker(\varphi)$ followed by the inclusion $R/\ker(\varphi) \hookrightarrow S$, so to understand algebra-finiteness it suffices to restrict our attention to injective homomorphisms.

Example 1.21. Every ring is a $\mathbb{Z}$-algebra, but generally not a finitely generated one.

Remark 1.22. Let $A \subseteq B \subseteq C$ be rings. It follows from the definitions that

- $$\begin{array}{c} A \subseteq B \text{ algebra-finite} \\ \text{and} \\ B \subseteq C \text{ algebra-finite} \end{array} \qquad \Longrightarrow \qquad A \subseteq C \text{ algebra-finite}$$
- $A \subseteq C$ algebra-finite $\Longrightarrow B \subseteq C$ algebra-finite.

However, $A \subseteq C$ algebra-finite $\not\Longrightarrow$ $A \subseteq B$ algebra-finite.

Example 1.23. Let k be a field and

$$B = k[x, xy, xy^2, xy^3, \cdots] \subseteq C = k[x, y],$$

where x and y are indeterminates. While B and C are both k-algebras, C is a finitely generated k-algebra, while B is not. Indeed, any finitely generated subalgebra of B is contained in $k[x, xy, \ldots, xy^m]$ for some m, since we can write the elements in any finite generating set as polynomial expressions in finitely many of the specified generators of B. However, note that every element of $k[x, xy, \ldots, xy^m]$ is a k-linear combination of monomials with the property that the y exponent is no more than m times the x exponent, so this ring does not contain xy^{m+1}. Thus, B is not a finitely generated A-algebra.

There are many basic questions about algebra generators that are surprisingly difficult. Let $R = \mathbb{C}[x_1, \ldots, x_n]$ and $f_1, \ldots, f_n \in R$. When do $f_1, \ldots, f_n$ generate R over $\mathbb{C}$? It is not too hard to show that the Jacobian determinant

$$\det \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_n}{\partial x_1} & \cdots & \frac{\partial f_n}{\partial x_n} \end{bmatrix}$$

must be a nonzero constant. It is a big open question whether this is in fact a sufficient condition!

Finally, note that an easy corollary of the Hilbert Basis Theorem is that finitely generated algebras over noetherian rings are also noetherian.

Corollary 1.24. *If R is a Noetherian ring, then any finitely generated R-algebra is Noetherian. In particular, any finitely generated algebra over a field is Noetherian.*

Proof. By our discussion above, a finitely generated R-algebra is isomorphic to a quotient of a polynomial ring over R in finitely many variables; polynomial rings over noetherian rings are Noetherian, by Hilbert's Basis Theorem, and quotients of Noetherian rings are Noetherian. □

The converse to this statement is false: there are lots of Noetherian rings that are not finitely generated algebras over a field. For example, $\mathbb{C}\{z\}$ is not algebra-finite over $\mathbb{C}$. We will see more examples of these when we talk about local rings.

1.3 Module-finite extensions

Given a ring homomorphism $\varphi : R \to S$, saying that S acquires an R-module structure via φ by $a \cdot r = \varphi(a)r$ is a particular case of *restriction of scalars*. By restriction of scalars, we mean that any S-module M also gains a new R-module structure given by $r \cdot m = \varphi(r)m$.[1] We may write ${}_\varphi M$ for this R-module if we need to emphasize which map we are talking about.

Given an R-algebra S, we can consider the *algebra* structure of S over R, or its *module* structure over R. So instead of asking about how S is generated as an *algebra* over R, we can ask how it is generated as a *module* over R. Recall that an A-module M is generated by a set of elements $\Gamma \subseteq M$ if the following equivalent conditions hold:

- The smallest submodule of M that contains Γ is M itself.
- Every element of M can be written as an A-linear combination of elements in Γ.
- Given a free R-module on $|\Gamma|$ basis elements $R^{\oplus Y}$, the homomorphism

$$\begin{aligned} R^{\oplus Y} &\xrightarrow{\theta} M \\ y_i &\longrightarrow \gamma_i \end{aligned}$$

  is surjective.

We use the notation $M = \sum_{\gamma \in \Gamma} A\gamma$ to indicate that M is generated by Γ as a module. We say that $\varphi : A \to R$ is *module-finite* if R is a finitely-generated A-module. This is also called simply *finite* in the literature, but we'll stick with the unambiguous "module-finite."

As with algebra-finiteness, surjective maps are always module-finite in a trivial way, and it suffices to understand this notion for ring inclusions.

The notion of module-finite is much stronger than algebra-finite, since a linear combination is a very special type of polynomial expression.

[1] This gives a functor from the category of S-modules to the category of R-modules.

Example 1.25.

a) If $K \subseteq L$ are fields, saying L is module-finite over K just means that L is a finite field extension of K.

b) The Gaussian integers $\mathbb{Z}[i]$ satisfy the well-known property (or definition, depending on your source) that any element $z \in \mathbb{Z}[i]$ admits a unique expression $z = a+bi$ with $a, b \in \mathbb{Z}$. That is, $\mathbb{Z}[i]$ is generated as a $\mathbb{Z}$-module by $\{1, i\}$; moreover, they form a free module basis!

c) If R is a ring and x an indeterminate, $R \subseteq R[x]$ is not module-finite. Indeed, $R[x]$ is a free R-module on the basis $\{1, x, x^2, x^3, \dots\}$.

d) Another map that is *not* module-finite is the inclusion $k[x] \subseteq k[x, 1/x]$. First, note that any element of $k[x, 1/x]$ can be written in the form $f(x)/x^n$ for some $f \in k[x]$ and some $n \geqslant 0$. Since $k[x]$ is a Noetherian ring, $k[x, 1/x]$ is a finitely-generated $k[x]$-module if and only if it is a Noetherian $k[x]$-module. But here is an infinite chain of submodules of $k[x, \frac{1}{x}]$:

$$k[x] \cdot \frac{1}{x} \subseteq k[x] \cdot \frac{1}{x^2} \subseteq k[x] \cdot \frac{1}{x^3} \subseteq \cdots$$

Remark 1.26. If R is an A-algebra,

- $A \subseteq R$ is algebra-finite if $R = A[f_1, \dots, f_n]$ for some $f_1, \dots, f_n \in R$.
- $A \subseteq R$ is module-finite if $R = Af_1 + \cdots + f_n$ for some $f_1, \dots, f_n \in R$.

Lemma 1.27. *If $R \subseteq S$ is module-finite and N is a finitely generated S-module, then N is a finitely generated R-module by restriction of scalars. In particular, the composition of two module-finite ring maps is module-finite.*

Proof. Let $S = Ra_1 + \cdots + Ra_r$ and $N = Sb_1 + \cdots + Sb_s$. Then we claim that

$$N = \sum_{i=1}^{r} \sum_{j=1}^{s} Ra_i b_j.$$

Indeed, given $n = \sum_{j=1}^{s} s_j b_j$, rewrite each $s_j = \sum_{i=1}^{r} r_{ij} a_i$ and substitute to get

$$n = \sum_{i=1}^{r} \sum_{j=1}^{s} r_{ij} a_i b_j$$

as an R-linear combination of the $a_i b_j$. □

Remark 1.28. Let $A \subseteq B \subseteq C$ be rings. It follows from the definitions that

- $\begin{matrix} A \subseteq B \text{ module-finite} \\ \text{and} \\ B \subseteq C \text{ module-finite} \end{matrix} \implies A \subseteq C \text{ module-finite}$

- $A \subseteq C$ module-finite $\implies B \subseteq C$ module-finite.

However, $A \subseteq C$ module-finite $\not\implies A \subseteq B$ module-finite. Note that if A is Noetherian, then $A \subseteq C$ module-finite *does* in fact imply $A \subseteq B$ module-finite, so to find an example of this bad behavior we need A to be non-Noetherian. You will construct an example in the next problem set.

1.4 Integral 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 1.29 (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.

Again, we can restrict our focus to inclusion maps $A \subseteq R$.

Remark 1.30. An element $r \in R$ is integral over A if and only if r is integral over the subring $\varphi(A) \subseteq R$, so we might as well assume that φ is injective.

Definition 1.31. Given an inclusion of rings $A \subseteq R$, the **integral closure** of A in R is the set of elements in R that are integral over A. The integral closure of a domain R in its field of fractions is usually denoted by $\overline{R}$. We say A is **integrally closed** in R if A is its own integral closure in R; a **normal domain** is a domain R that is integrally closed in its field of fractions, meaning $R = \overline{R}$.

Example 1.32. The ring of integers $\mathbb{Z}$ is a normal domain, meaning its integral closure in its fraction field $\mathbb{Q}$ is $\mathbb{Z}$ itself.

Example 1.33. The ring $\mathbb{Z}[\sqrt{d}]$, where $d \in \mathbb{Z}$ is not a perfect square, is integral over $\mathbb{Z}$. Indeed, $\sqrt{d}$ satisfies the monic polynomial $r^2 - d$, and since the integral closure of $\mathbb{Z}$ is a ring containing $\mathbb{Z}$ and $\sqrt{d}$, every element in $\mathbb{Z}[\sqrt{d}]$ is integral over $\mathbb{Z}$.

Proposition 1.34. *Let $A \subseteq R$ be rings.*

1) If $r \in R$ is integral over A then $A[r]$ is module-finite over A.

2) If $r_1, \ldots, r_t \in R$ are integral over A then $A[r_1, \ldots, r_t]$ is module-finite over A.

Proof.

1) Suppose r is integral over A, and $r^n + a_{n-1}r^{n-1} + \cdots + a_1 r + a_0 = 0$. Then we claim that $A[r] = A + Ar + \cdots + Ar^{n-1}$. First, note that to show that any polynomial $p(r) \in A[r]$ is in $A + Ar + \cdots + Ar^{n-1}$, it is enough to show that $r^m \in A + Ar + \cdots + Ar^{n-1}$ for all m. Using induction on m, the base cases $1, r, \ldots, r^{n-1} \in A + Ar + \cdots + Ar^{n-1}$ are obvious. On the other hand, we can use induction to conclude that $r^m \in A + Ar + \cdots + Ar^{n-1}$ for all $m \geqslant n-1$, since we can use the equation above to rewrite r^m as

$$r^m = r^{m-n}(a_{n-1}r^{n-1} + \cdots + a_1 r + a_0),$$

which has degree $m-1$ in r.

2) Write

$$A_0 := A \subseteq A_1 := A[r_1] \subseteq A_2 := A[r_1, r_2] \subseteq \cdots \subseteq A_t := A[r_1, \ldots, r_t].$$

Note that r_i is integral over A_{i-1}, via the same monic equation of r_i over A. Then, the inclusion $A \subseteq A[r_1, \ldots, r_t]$ is a composition of module-finite maps, and thus it is also module-finite. □

The name "ring" is roughly based on this idea: in an extension as above, the powers wrap around (like a ring).

We will need a linear algebra fact. The **classical adjoint** of an $n \times n$ matrix $B = [b_{ij}]$ is the matrix $\mathrm{adj}(B)$ with entries $\mathrm{adj}(B)_{ij} = (-1)^{i+j}\det(\widehat{B_{ji}})$, where $\widehat{B_{ji}}$ is the matrix obtained from B by deleting its jth row and ith column. You may remember this matrix from linear algebra.

Lemma 1.35 (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 1.36 (Module finite implies integral)**.** *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. $\square$

Collecting the previous results, we now have a useful characterization of module-finite extensions:

Corollary 1.37 (Characterization of module-finite extensions)**.** *Let $A \subseteq R$ be rings. R is module-finite over A if and only if R is integral and algebra-finite over A.*

Proof. ($\Rightarrow$): A generating set for R as an A-module serves as a generating set as an A-algebra. The remainder of this direction comes from the previous theorem. ($\Leftarrow$): If $R = A[r_1, \ldots, r_t]$ is integral over A, so that each r_i is integral over A, then R is module-finite over A by Proposition 1.34. $\square$

Corollary 1.38. *If R is generated over A by integral elements, then R is integral. Thus, if $A \subseteq S$, the set of elements of S that are integral over A form a subring of S.*

Proof. Let $R = A[\Lambda]$, with λ integral over A for all $\lambda \in \Lambda$. Given $r \in R$, there is a finite subset $L \subseteq \Lambda$ such that $r \in A[L]$. By the theorem, $A[L]$ is module-finite over A, and $r \in A[L]$ is integral over A.

For the latter statement, the first statement implies that

$$\{\text{integral elements}\} \subseteq A[\{\text{integral elements}\}] \subseteq \{\text{integral elements}\},$$

so equality holds throughout, and {integral elements} is a ring. □

Definition 1.39. If $A \subseteq R$, the **integral closure of A in R** is the set of elements of R that are integral over A.

So the previous result says that the integral closure of A in R is a subring of R (containing A).

Example 1.40.

1) Let $R = \mathbb{C}[x, y] \subseteq S = \mathbb{C}[x, y, z]/(x^2 + y^2 + z^2)$. Then S is module-finite over R: indeed, S is generated over R as an algebra by one element, z, and z satisfies the monic equation $r^2 + x^2 + y^2 = 0$, so it is integral over R.
2) Not all integral extensions are module-finite. Consider

$$A = k[x] \subseteq R = k[x, x^{1/2}, x^{1/3}, x^{1/4}, x^{1/5}, \dots].$$

R is generated by integral elements over $k[x]$, but it is not algebra-finite over $k[x]$.

Finally, we can prove a technical sounding result that puts together all our finiteness conditions in a useful way. We will then be able to answer a classical question using this result.

Theorem 1.41 (Artin-Tate Lemma)**.** *Let $A \subseteq B \subseteq C$ be rings. Assume that*

- *A is Noetherian,*
- *C is module-finite over B, and*
- *C is algebra-finite over A.*

Then, B is algebra-finite over A.

Proof. Let $C = A[f_1, \dots, f_r]$ and $C = Bg_1 + \cdots + Bg_s$. Then,

$$f_i = \sum_j b_{ij} g_j \quad \text{and} \quad g_i g_j = \sum_k b_{ijk} g_k$$

for some $b_{ij}, b_{ijk} \in B$. Let $B_0 = A[\{b_{ij}, b_{ijk}\}] \subseteq B$. Since A is Noetherian, so is B_0.

We claim that $C = B_0\, g_1 + \cdots + B_0 g_s$. Given an element $c \in C$, write c as a polynomial expression in $f_1, \dots, f_r$, and since the f_i are linearly combinations of the g_i, we can rewrite $c \in A[\{b_{ij}\}][g_1, \dots, g_s]$. Then using the equations for $g_i g_j$ we can write c in the form required.

Now, since B_0 is Noetherian, C is a finitely generated B_0-module, and $B \subseteq C$, then B is a finitely generated B_0-module, too. In particular, $B_0 \subseteq B$ is algebra-finite. We conclude that $A \subseteq B$ is algebra-finite, as required. □

1.5 An application to invariant rings

Historically, commutative algebra has roots in classical questions of algebraic and geometric flavors, including the following natural question:

Question 1.42. Given a (finite) set of symmetries, consider the collection of polynomial functions that are fixed by all of those symmetries. Can we describe all the fixed polynomials in terms of finitely many of them?

To make this precise, let G be a group acting on a ring R, or just as well, a group of automorphisms of R. The main case we have in mind is when $R = k[x_1, \ldots, x_d]$ and k is a field. We are interested in the set of elements that are *invariant* under the action,

$$R^G := \{r \in R \mid g(r) = r \text{ for all } g \in G\}.$$

Note that R^G is a subring of R. Indeed, given $r, s \in R^G$, then

$$r + s = g(r) + g(s) = g(r + s) \quad \text{and} \quad rs = g(r)g(s) = g(rs) \qquad \text{for all } g \in G,$$

since each g is a homomorphism. Note also that if $G = \langle g_1, \ldots, g_t \rangle$, then $r \in R^G$ if and only if $g_i(r) = r$ for $i = 1, \ldots, t$. The question above can now be rephrased as follows:

Question 1.43. Given a finite group G acting on $R = k[x_1, \ldots, x_d]$, is R^G a finitely generated k-algebra?

Proposition 1.44. *Let k be a field, R be a finitely-generated k-algebra, and G a finite group of automorphisms of R that fix k. Then $R^G \subseteq R$ is module-finite.*

Proof. Since integral implies module-finite, we will show that R is algebra-finite and integral over R^G.

First, since R is generated by a finite set as a k-algebra, and $k \subseteq R^G$, it is generated by the same finite set as an R^G-algebra as well. Extend the action of G on R to $R[t]$ with G fixing t. Now, for $r \in R$, consider the polynomial $F_r(t) = \prod_{g \in G}(t - g(r)) \in R[t]$. Then G fixes $F_r(t)$, since for each $h \in G$,

$$h(F_r(t)) = h \prod_{g \in G}(t - g(r)) = \prod_{g \in G}(h \cdot t - hg(r)) = F_r(t)$$

Thus, $F_r(t) \in (R[t])^G$. Notice that $(R[t])^G = R^G[t]$, since

$g(a_n t^n + \cdots + a_0) = a_n t^n + \cdots + a_0 \implies (g \cdot a_n)t^n + \cdots + (g \cdot a_0) = a_n t^n + \cdots + a_0$.

Therefore, $F_r(t) \in R^G[t]$. The leading term (with respect to t) of $F_r(t)$ is $t^{|G|}$, so $F_r(t)$ is monic, and r is integral over R^G. Therefore, R is integral over R^G. □

Theorem 1.45 (Noether's finiteness theorem for invariants of finite groups)**.** *Let k be a field, R be a polynomial ring over k, and G be a finite group acting k-linearly on R. Then R^G is a finitely generated k-algebra.*

Proof. Observe that $k \subseteq R^G \subseteq R$, that k is Noetherian, $k \subseteq R$ is algebra-finite, and $R^G \subseteq R$ is module-finite. Thus, by the Artin-Tate Lemma, we are done! □

Chapter summary

- R is a Noetherian ring $\iff$ every ideal I in R is Noetherian
- M is a Noetherian R-module $\underset{R \text{ Noeth}}{\overset{\text{general}}{\rightleftharpoons}}$ M is a finitely generated R-module

$A \subseteq R$ extension of rings:

- $A \subseteq R$ module-finite $\iff$ $\begin{array}{c} R = Af_1 + \cdots + Af_n \\ \text{for some } f_i \in R \end{array}$ $\iff$ $\begin{array}{c} R \cong A^n/N \\ N \subseteq A^n \text{ submod} \end{array}$
- $A \subseteq R$ algebra-finite $\iff$ $\begin{array}{c} R = A[f_1, \ldots, f_n] \\ \text{for some } f_i \in R \end{array}$ $\iff$ $\begin{array}{c} R \cong A[x_1, \ldots, x_i]/I \\ x_i \text{ indeterminates} \end{array}$
  - $A \subseteq R$ algebra-finite $\iff$ $R = A[f_1, \ldots, f_n]$, $f_i \in R$
  - $A \subseteq R$ algebra-finite, A Noetherian $\implies$ R Noetherian ring
  - $A \subseteq R$ module-finite $\iff$ $\left\{ \begin{array}{c} \text{algebra-finite} \\ \text{and integral} \end{array} \right.$ $\begin{array}{c} \not\Longrightarrow \\ \not\Longrightarrow \end{array}$ module-finite

Artin-Tate Lemma: $\underbrace{\underbrace{A}_{\text{Noeth}} \subseteq \underbrace{B \subseteq C}_{\text{mod-fin}}}_{\text{alg-fin}}$

Chapter 2

Graded rings

2.1 Graded rings

When we think of a polynomial ring R, we often think of R with its graded structure, even if we have never formalized what that means. Other rings we have seen also have a graded structure, and this structure is actually very powerful.

Definition 2.1. A ring R is **$\mathbb{N}$-graded** if we can write a direct sum decomposition of R as an abelian group indexed by $\mathbb{N}$[1]

$$R = \bigoplus_{a \geqslant 0} R_a,$$

where $R_a R_b \subseteq R_{a+b}$ for every $a, b \in \mathbb{N}$, meaning that for any $r \in R_a$ and $s \in R_b$, we have $rs \in R_{a+b}$. More generally, given a monoid T. The ring R is **T-graded** if there exists a direct sum decomposition of R as an abelian group indexed by T:

$$R = \bigoplus_{a \in T} R_a$$

satisfying $R_a R_b \subseteq R_{a+b}$.

An element that lies in one of the summands R_a is said to be **homogeneous** of **degree** a; we write $|r|$ or $\deg(r)$ to denote the degree of a homogeneous element r.

By definition, an element in a graded ring is a *unique* sum of homogeneous elements, which we call its **homogeneous components** or **graded components**. One nice thing about graded rings is that many properties can usually be sufficiently checked on homogeneous elements, and these are often easier to deal with.

Remark 2.2. Note that whenever R is a graded ring, the multiplicative identity 1 must be a homogeneous element whose degree is the identity in T. In particular, if R is $\mathbb{N}$ or $\mathbb{Z}$-graded, then $1 \in R_0$ and R_0 is a subring of R.

[1] We follow the convention that 0 is a natural number.

Example 2.3.

a) Any ring R is trivially an $\mathbb{N}$-graded ring, by setting $R_0 = R$ and $R_n = 0$ for $n \neq 0$.

b) If k is a field and $R = k[x_1, \ldots, x_n]$ is a polynomial ring, there is an $\mathbb{N}$-grading on R called the *standard grading* where R_d is the k-vector space with basis given by the monomials of total degree d, meaning those of the form $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ with $\sum_i \alpha_i = d$. Of course, this is the notion of degree familiar from middle school. So $x_1^2 + x_2x_3$ is homogeneous in the standard grading, while $x_1^2 + x_2$ is not.

c) If k is a field, and $R = k[x_1, \ldots, x_n]$ is a polynomial ring, we can give different $\mathbb{N}$-gradings on R by fixing some tuple $(\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$ and letting x_i be a homogeneous element of degree β_i; we call this a grading with *weights* $(\beta_1, \ldots, \beta_n)$. For example, in $k[x_1, x_2]$, $x_1^2 + x_2^3$ is not homogeneous in the standard grading, but it is homogeneous of degree 6 under the $\mathbb{N}$-grading with weights $(3, 2)$.

d) A polynomial ring $R = k[x_1, \ldots, x_n]$ also admits a natural $\mathbb{N}^n$-grading, with $R_{(d_1,\ldots,d_n)} = k \cdot x_1^{d_1} \cdots x_n^{d_n}$. This is called the *fine grading*.

e) Let $\Gamma \subseteq \mathbb{N}^n$ be a subsemigroup of $\mathbb{N}^n$. Then

$$\bigoplus_{\gamma \in \Gamma} k \cdot \underline{x}^{\gamma} \subseteq k[\underline{x}] = k[x_1, \ldots, x_n]$$

is an $\mathbb{N}^n$-graded subring of $k[x_1, \ldots, x_n]$. Conversely, every $\mathbb{N}^n$-graded subring of $k[x_1, \ldots, x_n]$ is of this form.

f) Polynomial rings in Macaulay2 are graded with the standard grading by default. 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
```

Remark 2.4. You may have seen the term *homogeneous polynomial* used to refer to a polynomial $f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ that satisfies

$$f(\lambda x_1, \ldots, \lambda x_n) = \lambda^d f(x_1, \ldots, x_n)$$

for some d. This is equivalent to saying that all the terms in f have the same total degree, or that f is homogeneous with respect to the standard grading.

Similarly, a polynomial is *quasi-homogeneous*, or *weighted homogeneous*, if there exist integers $w_1, \ldots, w_n$ such that he sum $w = a_1 w_1 + \cdots + a_n w_n$ is the same for all monomials $x_1^{a_1} \cdots x_n^{a_n}$ appearing in f. So f satisfies

$$f(\lambda^{w_1} x_1, \ldots, \lambda^{w_n} x_n) = \lambda^w f(x_1, \ldots, x_n),$$

and $f(x_1^{w_1}, \ldots, x_n^{w_n})$ is homogeneous (in the previous sense, so with respect to the standard grading). This condition is equivalent to asking that f be homogeneous with respect to some weighted grading on $k[x_1, \ldots, x_n]$.

Definition 2.5. An ideal I in a graded ring R is called *homogeneous* if it can be generated by homogeneous elements.

Remark 2.6. Observe that an ideal is homogeneous if and only if I has the following property: for any element $f \in R$ we have $f \in I$ if and only if every homogeneous component of f lies in I. We can repackage this by saying that I is homogeneous if

$$I = \bigoplus_{a \in T} I_a,$$

where $I_a = I \cap R_a$.

Indeed, if I has this property, take a generating set $\{f_\lambda\}_\Lambda$ for I; by assumption, all of the homogeneous components of each f_λ lie in I, and since each f_λ lies in the ideal generated by these components, the set of all the components generates I, and I is homogeneous. On the other hand, if all the components of f lie in I then so does f, whether or not I is homogeneous. If I is homogeneous and $f \in I$, write f as a combination of the (homogeneous) generators of I, say $f_1, \ldots, f_n$:

$$f = r_1 f_1 + \cdots + r_n f_n.$$

Now by writing each r_i as a sum of its components, say $r_i = r_{i,1} + \cdots + r_{i,n_i}$, each $r_{i,j} f_i \in I$, and these contain all the components of f (and potentially some redundant terms).

Example 2.7. Given an $\mathbb{N}$-graded ring R, then $R_+ = \bigoplus_{d>0} R_d$ is a homogeneous ideal.

We now observe the following:

Lemma 2.8. *Let R be an T-graded ring, and I be a homogeneous ideal. Then R/I has a natural T-graded structure induced by the T-graded structure on R.*

Proof. The ideal I decomposes as the direct sum of its graded components, so we can write

$$R/I = \frac{\oplus R_a}{\oplus I_a} \cong \oplus \frac{R_a}{I_a}.$$

□

Example 2.9.

a) The ideal $I = (w^2x + wyz + z^3, x^2 + 3xy + 5xz + 7yz + 11z^2)$ in $R = k[w, x, y, z]$ is homogeneous with respect to the standard grading on R, and thus the ring R/I admits an $\mathbb{N}$-grading with $|w| = |x| = |y| = |z| = 1$.

b) In contrast, the ring $R = k[x, y, z]/(x^2 + y^3 + z^5)$ does not admit a grading with $|x| = |y| = |z| = 1$, but does admit a grading with $|x| = 15, |y| = 10, |z| = 6$.

Definition 2.10. Let R be a T-graded ring, and M an R-module. The module R is **T-graded** if there exists a direct sum decomposition of M as an abelian group indexed by T:

$$M = \bigoplus_{a \in T} M_a \text{ such that } R_a M_b \subseteq M_{a+b}$$

for all $a, b \in T$.

The notions of homogeneous element of a module and degree of a homogeneous element of a module take the obvious meanings. A notable abuse of notation: we will often talk about $\mathbb{Z}$-graded modules over $\mathbb{N}$-graded rings, and likewise.

We can also talk about graded homomorphisms.

Definition 2.11. Let R and S be T-graded rings with the same grading monoid T. A ring homomorphism $\varphi : R \to S$ is **graded** or **degree-preserving** if $\varphi(R_a) \subseteq S_a$ for all $a \in T$.

Note that our definition of ring homomorphism requires $1_R \mapsto 1_S$, and thus it does not make sense to talk about graded ring homomorphisms of degree $d \neq 0$. But we can have graded module homomorphisms of any degree.

Definition 2.12. Let M and N be $\mathbb{Z}$-graded modules over the $\mathbb{N}$-graded ring R. A homomorphism of R-modules $\varphi : R \to S$ is **graded** if $\varphi(M_a) \subseteq N_{a+d}$ for all $a \in \mathbb{Z}$ and some fixed $d \in \mathbb{Z}$, called the **degree** of φ. A graded homomorphism of degree 0 is also called **degree-preserving**.

Example 2.13.

a) Consider the ring map $k[x, y, z] \to k[s, t]$ given by $x \mapsto s^2, y \mapsto st, z \mapsto t^2$. If $k[s, t]$ has the fine grading, meaning $|s| = (1, 0)$ and $|t| = (0, 1)$, then the given map is degree preserving if and only if $k[x, y, z]$ is graded by

$$|x| = (2, 0), |y| = (1, 1), |z| = (0, 2).$$

b) Let k be a field, and let $R = k[x_1, \ldots, x_n]$ be a polynomial ring with the standard grading. Given $c \in k = R_0$, the homomorphism of R-modules $R \to R$ given by $f \mapsto cf$ is degree preserving. However, if instead we take $g \in k = R_d$ for some $d > 0$, then the map

$$\begin{aligned} R &\longrightarrow R \\ f &\longmapsto gf \end{aligned}$$

is not degree preserving, although it is a graded map of degree d. We can make this a degree-preserving map if we shift the grading on R by defining $R(-d)$ to be the R-module R but with the $\mathbb{Z}$-grading given by $R(-d)_t = R_{t-d}$. With this grading, the component of degree d of $R(-d)$ is $R(-d)_d = R_0 = k$. Now the map

$$\begin{aligned} R(-d) &\longrightarrow R \\ f &\longmapsto gf \end{aligned}$$

is degree preserving.

We observed earlier an important relationship between algebra-finiteness and Noetherianity that followed from the Hilbert basis theorem: if R is Noetherian, then any algebra-finite extension of R is also Noetherian. There isn't a converse to this in general: there are lots of algebras over fields K that are Noetherian but not algebra-finite over K. However, for graded rings, this converse relation holds.

Proposition 2.14. *Let R be an $\mathbb{N}$-graded ring, and consider homogeneous elements $f_1, \ldots, f_n \in R$ of positive degree. Then $f_1, \ldots, f_n$ generate the ideal $R_+ := \bigoplus_{d>0} R_d$ if and only if $f_1, \ldots, f_n$ generate R as an R_0-algebra.*

Therefore, an $\mathbb{N}$-graded ring R is Noetherian if and only if R_0 is Noetherian and R is algebra-finite over R_0.

Proof. If $R = R_0[f_1, \ldots, f_n]$, then any element $r \in R_+$ can be written as a polynomial expression $r = P(f_1, \ldots, f_n)$ for some $P \in R_0[\underline{x}]$ with no constant term. Each monomial of P is a multiple of some x_i, and thus $r \in (f_1, \ldots, f_n)$.

To show that $R_+ = (f_1, \ldots, f_n)$ implies $R = R_0[f_1, \ldots, f_n]$, it suffices to show that any homogeneous element $r \in R$ can be written as a polynomial expression in the f's with coefficients in R_0. We induce on the degree of r, with degree 0 as a trivial base case. For r homogeneous of positive degree, we must have $r \in R_+$, so by assumption we can write $r = a_1 f_1 + \cdots + a_n f_n$; moreover, since r and $f_1, \ldots, f_n$ are all homogeneous, we can choose each coefficient a_i to be homogeneous of degree $|r| - |f_i|$. By the induction hypothesis, each a_i is a polynomial expression in the f's, so we are done.

For the final statement, if R_0 is Noetherian and R algebra-finite over R_0, then R is Noetherian by the Hilbert Basis Theorem. If R is Noetherian, then $R_0 \cong R/R_+$ is Noetherian. Moreover, R is algebra-finite over R_0 since R_+ is generated as an ideal by finitely many homogeneous elements by Noetherianity, so by the first statement, we get a finite algebra generating set for R over R_0. □

There are many interesting examples of $\mathbb{N}$-graded algebras with $R_0 = k$; in that case, R_+ is the largest homogeneous ideal in R. In fact, R_0 is the only maximal ideal of R that is also homogeneous, so we can call it *the* **homogeneous maximal ideal**; it is sometimes also called the **irrelevant maximal ideal** of R. This ideal plays a very important role — in many ways, R and R_+ behave similarly to a local ring R and its unique maximal ideal. We will discuss this further when we learn about local rings.

2.2 Another application to invariant rings

If R is a graded ring, and G is a group acting on R by degree-preserving automorphisms, then R^G is a graded subring of R, meaning R^G is graded with respect to the same grading monoid. In particular, if G acts k-linearly on a polynomial ring over k, the invariant ring is $\mathbb{N}$-graded.

Using this perspective, we can now give a different proof of the finite generation of invariant rings that works under different hypotheses. The proof we will discuss now is essentially Hilbert's proof. To do that, we need another notion that is very useful in commutative algebra.

Definition 2.15. Let S be an R-algebra corresponding to the ring homomorphism $\varphi : R \to S$. We say that R is a **direct summand** of S if the map φ **splits** as a map of R-modules, meaning there is an R-module homomorphism

$$\begin{array}{ccc} & \overset{\pi}{\swarrow\!\!\!\!\!\!\searrow} & \\ R & \xrightarrow[\varphi]{} & S \end{array}$$

such that $\pi\varphi$ is the identity on R.

First, observe that the condition on π implies that φ must be injective, so we can assume that $R \subseteq S$, perhaps after renaming elements. Then the condition on π is that $\pi(rs) = r\pi(s)$ for all $r \in R$ and $s \in S$ and that $\pi|_R$ is the identity. We call the map π the *splitting* of the inclusion. Note that given any R-linear map $\pi : S \to R$, if $\pi(1) = 1$ then π is a splitting: indeed, $\pi(R) = \pi(r \cdot 1) = r\pi(1) = r$ for all $r \in R$.

Being a direct summand is really nice, since many good properties of S pass onto its direct summands.

Notation 2.16. Let $R \subseteq S$ be an extension of rings. Given an ideal I in S, we write $I \cap R$ for the **contraction** of R back into R, meaning the preimage of I via the inclusion map $R \subseteq S$. More generally, we may use the notation $I \cap R$ to denote the preimage of I via a given ring map $R \to S$, even if the map is not injective.

Given a ring map $R \to S$, and an ideal I in R, the **expansion** of I in S is the ideal of S generated by the image of I via the given ring map; we naturally denote this by IS.

Lemma 2.17. *Let R be a direct summand of S. Then, for any ideal $I \subseteq R$, we have $IS \cap R = I$.*

Proof. Let π be the corresponding splitting. Clearly, $I \subseteq IS \cap R$. Conversely, if $r \in IS \cap R$, we can write $r = s_1 f_1 + \cdots + s_t f_t$ for some $f_i \in I$, $s_i \in S$. Applying π, we have

$$r = \pi(r) = \pi\left(\sum_{i=1}^{t} s_i f_i\right) = \sum_{i=1}^{t} \pi\left(s_i f_i\right) = \sum_{i=1}^{t} \pi\left(s_i\right) f_i \in I.$$

□

Proposition 2.18. *Let R be a direct summand of S. If S is Noetherian, then so is R.*

Proof. Let

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

be a chain of ideals in R. The chain of ideals in S

$$I_1S \subseteq I_2S \subseteq I_3S \subseteq \cdots$$

stabilizes, so there exist J, N such that $I_nR = J$ for $n \geqslant N$. Contracting to R, we get that $I_n = I_nS \cap R = J \cap R$ for $n \geqslant N$, so the original chain also stabilizes. □

Proposition 2.19. *Let k be a field, and R be a polynomial ring over k. Let G be a finite group acting k-linearly on R. Assume that the characteristic of k does not divide $|G$. Then R^G is a direct summand of R.*

Remark 2.20. The condition that the characteristic of k does not divide the order of G is trivially satisfied if k has characteristic zero.

Proof. We consider the map $\rho : R \to R^G$ given by

$$\rho(r) = \frac{1}{|G|} \sum_{g \in G} g \cdot r.$$

First, note that the image of this map lies in R^G, since acting by g just permutes the elements in the sum, so the sum itself remains the same. We claim that this map ρ is a splitting for the inclusion $R^G \subseteq R$. To see that, let $s \in R^G$ and $r \in R$. We have

$$\rho(sr) = \frac{1}{|G|} \sum_{g \in G} g \cdot (sr) = \frac{1}{|G|} \sum_{g \in G} (g \cdot s)(g \cdot r) = \frac{1}{|G|} \sum_{g \in G} s(g \cdot r) = s \frac{1}{|G|} \sum_{g \in G} (g \cdot r) = s\rho(r),$$

so ρ is R^G-linear, and for $s \in R^G$,

$$\rho(s) = \frac{1}{|G|} \sum_{g \in G} g \cdot s = s.$$

□

Theorem 2.21 (Hilbert's finiteness theorem for invariants)**.** *Let k be a field, and R be a polynomial ring over k. Let G be a group acting k-linearly on R. Assume that G is finite and $|G|$ does not divide the characteristic of k, or more generally, that R^G is a direct summand of R. Then R^G is a finitely generated k-algebra.*

Proof. Since G acts linearly, R^G is an $\mathbb{N}$-graded subring of R with $R_0 = k$. Since R^G is a direct summand of R, R^G is Noetherian by Proposition 2.18. By our characterization of Noetherian graded rings, R^G is finitely generated over $R_0 = k$. □

One important thing about this proof is that it applies to many infinite groups. In particular, for any *linearly reductive group*, including $\mathrm{GL}_n(\mathbb{C})$, $\mathrm{SL}_n(\mathbb{C})$, and $(\mathbb{C}^\times)^n$, we can construct a splitting map ρ.

Chapter 3

Algebraic Geometry

Colloquially, we often identify systems of equations with their solution sets. We will make this correspondence more precise for systems of polynomial equations, and develop the beginning of a rich dictionary between algebraic and geometric objects.

Question 3.1. Let k be a field. To what extent is a system of polynomial equations

$$\begin{cases} f_1 = 0 \\ \quad \vdots \\ f_t = 0 \end{cases}$$

where polynomials $f_1, \ldots, f_t \in k[x_1, \ldots, x_d]$, determined by its solution set?

Let's consider one polynomial equation in one variable. Over $\mathbb{R}, \mathbb{Q}$, or other fields that are not algebraically closed, there are many polynomials with an empty solution set; for example, $z^2 + 1$ has an empty solution set over $\mathbb{R}$. On the other hand, over $\mathbb{C}$, or any algebraically closed field, if $a_1, \ldots, a_d$ are the solutions to $f(z) = 0$, we know that we can write f in the form $f(z) = \alpha(z - a_1)^{n_1} \cdots (z - a_d)^{n_d}$, so f is completely determined up to scalar multiple and repeated factors. If we insist that f have no repeated factors, then (f) is uniquely determined.

More generally, given any system of polynomial equations

$$\begin{cases} f_1 = 0 \\ \quad \vdots \\ f_t = 0 \end{cases}$$

where $f_i \in k[z]$ for some field k, notice that that $z = a$ is a solution to the system if and only if it is a solution for any polynomial $g \in (f_1, \ldots, f_t)$. But since $k[z]$ is a PID, we have $(f_1, \ldots, f_t) = (f)$, where f is a greatest common divisor of $f_1, \ldots, f_t$. Therefore, $z = a$ is a solution to the system if and only if $f(a) = 0$.

3.1 Varieties

Definition 3.2. Given a field k, the *affine d-space over k*, denoted $\mathbb{A}_k^d$, is the set

$$\mathbb{A}_k^d = \{(a_1, \ldots, a_d) \mid a_i \in k\}.$$

Definition 3.3. For a subset T of $k[x_1, \ldots, x_d]$, we define $\mathcal{Z}(T) \subseteq \mathbb{A}_k^d$ to be the set of common zeros or the *zero set* of the polynomials (equations) in T:

$$\mathcal{Z}(T) = \{(a_1, \ldots, a_d) \in \mathbb{A}_k^d \mid f(a_1, \ldots, a_d) = 0 \text{ for all } f \in T\}.$$

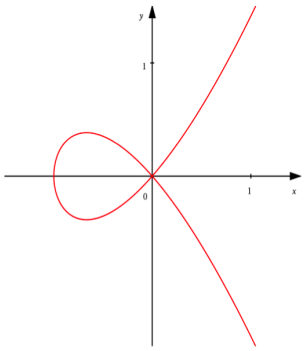
Sometimes, in order to emphasize the role of k, we will write this as $\mathcal{Z}_k(T)$.

A subset of $\mathbb{A}_k^d$ of the form $\mathcal{Z}(T)$ for some subset T is called an **algebraic subset** of $\mathbb{A}_k^d$, or an **affine algebraic variety**. So a variety $\mathbb{A}_k^d$ 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 varieties.

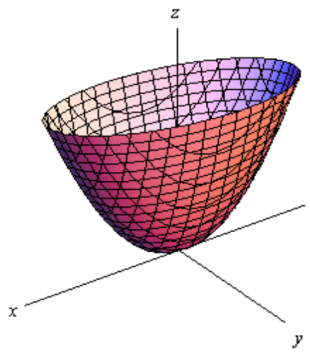
Note that some authors use the word *variety* to refer only to irreducible algebraic sets. Note also that the definitions given here are only completely standard when k is algebraically closed.

Example 3.4. Here are some simple examples of algebraic varieties:

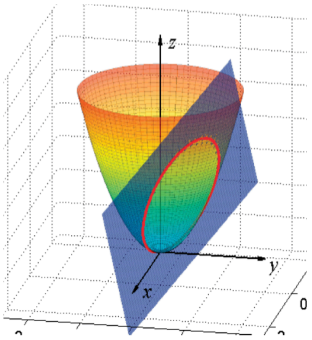
a) For $k = \mathbb{R}$ and $n = 2$, $\mathcal{Z}(y^2 + x^2(x-1))$ is a "nodal curve" in $\mathbb{A}_{\mathbb{R}}^2$, the real plane. Note that we've written x for x_1 and y for x_2 here.



b) For $k = \mathbb{R}$ and $n = 3$, $\mathcal{Z}(z - x^2 - y^2)$ is a paraboloid in $\mathbb{A}_{\mathbb{R}}^3$, real three space.



c) For $k = \mathbb{R}$ and $n = 3$, $\mathcal{Z}(z - x^2 - y^2, 3x - 2y + 7z - 7)$ is circle in $\mathbb{A}^3_{\mathbb{R}}$.



d) For $k = \mathbb{R}$, $\mathcal{Z}_{\mathbb{R}}(x^2 + y^2 + 1) = \emptyset$. Note that $\mathcal{Z}_{\mathbb{C}}(x^2 + y^2 + 1) \neq \emptyset$.

e) The subset $\mathbb{A}^2_k \setminus \{(0,0)\}$ is not an algebraic subset of $\mathbb{A}^2_k$ if k is infinite. Why?

f) The graph of the sine function is not an algebraic subset of $\mathbb{A}^2_{\mathbb{R}}$. Why not?

g) For $k = \mathbb{R}$, $\mathcal{Z}(y - x^2, xz - y^2, z - xy)$ is the so-called **twisted cubic (affine) curve**. It is the curve parametrized by (t, t^2, t^3), meaning it is the image of the map

$$\begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R}^3 \\ t & \longmapsto & (t, t^2, t^3) \end{array} .$$

We can check this with 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
```

So 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. 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 $k = \mathbb{Q}$.

h) For any field k and elements $a_1, \ldots, a_d \in k$, we have

$$\mathcal{Z}(x_1 - a_1, \ldots, x_d - a_d) = \{(a_1, \ldots, a_d)\}.$$

So, all one element subsets of $\mathbb{A}^d_k$ are algebraic subsets.

We can consider the equations that a subset of affine space satisfies.

Definition 3.5. Given any subset X of $\mathbb{A}_k^d$ for a field k, define

$$\mathcal{I}(X) = \{g(x_1, \ldots, x_d) \in k[x_1, \ldots, x_d] \mid g(a_1, \ldots, a_d) = 0 \text{ for all } (a_1, \ldots, a_d) \in X\}.$$

Exercise 5. $\mathcal{I}(X)$ is an ideal in $k[x_1, \ldots, x_d]$ for any $X \subseteq \mathbb{A}_k^d$.

Example 3.6.

a) $\mathcal{I}(\{(a_1, \ldots, a_d)\}) = (x_1 - a_1, \ldots, x_d - a_d)$, for any field k.

b) $\mathcal{I}(\text{graph of the sine function in } \mathbb{A}_{\mathbb{R}}^2) = (0)$.

Exercise 6. Here are some properties of the functions $\mathcal{Z}$ and $\mathcal{I}$:

a) For any field, we have $\mathcal{Z}(0) = \mathbb{A}_k^n$ and $\mathcal{Z}(1) = \emptyset$.

b) $\mathcal{I}(\emptyset) = (1) = k[x_1, \ldots, x_d]$ (the improper ideal).

c) $\mathcal{I}(\mathbb{A}_k^d) = (0)$ if and only if k is infinite.

d) If $I \subseteq J \subseteq k[x_1, \ldots, x_d]$ then $\mathcal{Z}(I) \supseteq \mathcal{Z}(J)$.

e) If $S \subseteq T$ are subsets of $\mathbb{A}_k^n$ then $\mathcal{I}(S) \supseteq \mathcal{I}(T)$.

f) If $I = (T)$ is the ideal generated by the elements of $T \subseteq k[x_1, \ldots, x_d]$, then $\mathcal{Z}(T) = \mathcal{Z}(I)$.

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 3.7. 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 $\mathcal{Z}(I)$ is the set of rank at most one matrices. Note that $I \subseteq (x_1, x_2, x_3) =: J$, and $\mathcal{Z}(J)$ is the set of 2×3 matrices with top row zero. The containment $\mathcal{Z}(J) \subseteq \mathcal{Z}(I)$ 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 7. Suppose that I and J are ideals in $k[x_1, \ldots, x_d]$.

a) $\mathcal{Z}(I) \cap \mathcal{Z}(J) = \mathcal{Z}(I + J)$.

b) $\mathcal{Z}(I) \cup \mathcal{Z}(J) = \mathcal{Z}(I \cap J) = \mathcal{Z}(IJ)$.

However, note that in general $IJ \neq I \cap J$.

3.2 Prime and maximal ideals

Before we talk more about geometry, let's recall some basic facts about prime and maximal ideals. As we will discover through the rest of the course, prime ideals play a very prominent role in commutative algebra.

Definition 3.8. An ideal $P \neq R$ is **prime** if $ab \in P$ implies $a \in P$ or $b \in P$.

Exercise 8. An ideal P in a ring R is prime if and only if R/P is a domain.

Example 3.9. The prime ideals in $\mathbb{Z}$ are those of the form (p) for p a prime integer, and (0).

Example 3.10. When k is a field, in $k[x]$ are easy to describe: $k[x]$ is a principal ideal domain, and $(f) \neq 0$ is prime if and only if f is an irreducible polynomial. Moreover, (0) is also a prime ideal, since $k[x]$ is a domain.

The prime ideals in $k[x_1, \ldots, x_d]$ are, however, not so easy to describe. We will see many examples throughout the course; here are some.

Example 3.11. The ideal $P = (x^3 - y^2)$ in $R = k[x, y]$ is prime; one can show that $R/P \cong k[t^2, t^3] \subseteq k[t]$, which is a domain.

Example 3.12. The k-algebra $R = k[s^3, s^2t, st^2, t^2] \subseteq k[s, t]$ is a domain, so its defining ideal I in $k[x_1, x_2, x_3, x_4]$ is prime. This is the kernel of the presentation of R sending x_1, x_2, x_3, x_4 to each of our 4 algebra generators, which we can compute with Macaulay2:

```
1 : k = QQ;

i2 : f = map(k[s,t],k[x_1 .. x_4],{s^3,s^2*t,s*t^2,t^3})
                                3   2      2   3
o2 = map(QQ[s..t],QQ[x ..x ],{s , s t, s*t , t })
                        1   4

o2 : RingMap QQ[s..t] <--- QQ[x ..x ]
                                1   4
i3 : I = ker f
             2                        2
o3 = ideal (x  - x x , x x  - x x , x  - x x )
             3    2 4   2 3    1 4   2    1 3

o3 :  Ideal of QQ[x ..x]
                   1   4
```

Later we will show that prime ideals correspond to irreducible varieties; more precisely, that X is irreducible if and only if $\mathcal{I}(X)$ is prime.

Definition 3.13 (maximal ideal)**.** An ideal $\mathfrak{m}$ in R is **maximal** if for any ideal I

$$I \supseteq \mathfrak{m} \implies I = \mathfrak{m} \text{ or } I = R.$$

Exercise 9. An ideal $\mathfrak{m}$ in R is maximal if and only if $R/\mathfrak{m}$ is a field.

Given a maximal ideal $\mathfrak{m}$ in R, the **residue field** of $\mathfrak{m}$ is the field $R/\mathfrak{m}$. A field k is a residue field of R if $k \cong R/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$.

Remark 3.14. A ring may have many different residue fields. For example, the residue fields of $\mathbb{Z}$ are all the finite fields with prime many elements, $\mathbb{F}_p \cong \mathbb{Z}/p$.

Exercise 10. Every maximal ideal is prime.

However, not every prime ideal is maximal. For example, in $\mathbb{Z}$, (0) is a prime ideal that is not maximal.

Theorem 3.15. *Given a ring R, every proper ideal $I \neq R$ is contained in some maximal ideal.*

Fun fact: this is actually *equivalent* to the Axiom of Choice. We will prove it (but not its equivalence to the Axiom of Choice!) using Zorn's Lemma, another equivalent version of the Axiom of Choice. Zorn's Lemma says that

> Every non-empty partially ordered set in which every chain (i.e., totally ordered subset) has an upper bound contains at least one maximal element.

So let's prove that every ideal is contained in some maximal ideal.

Proof. First, we will show that Zorn's Lemma applies to proper ideals in any ring R. The statement will then follow by applying Zorn's Lemma to the non-empty set of ideals $J \supseteq I$, which is partially ordered by inclusion.

So consider a chain of proper ideals in R, say $\{I_i\}_i$. Now $I = \bigcup_i I_i$ is an ideal as well, and $I \neq R$ since $1 \notin I_i$ for all i. Note that unions of ideals are not ideals in general, but a union of totally ordered ideals *is* an ideal. Then I is an upper bound for our chain $\{I_i\}_i$, and Zorn's Lemma applies to the set of proper ideals in R with inclusion $\subseteq$. □

3.3 Nullstellensatz

Lemma 3.16. *Let k be a field, and $R = k[x_1, \ldots, x_d]$ be a polynomial ring. There is a bijection*

$$\begin{array}{ccc} \mathbb{A}_k^d & \longrightarrow & \left\{ \begin{array}{c} \text{maximal ideals } \mathfrak{m} \text{ of } R \\ \text{with } R/\mathfrak{m} \cong k \end{array} \right\} \\ (a_1, \ldots, a_d) & \longmapsto & (x_1 - a_1, \ldots, x_d - a_d) \end{array}$$

Proof. Each $\mathfrak{m} = (x_1 - a_1, \ldots, x_d - a_d)$ is a maximal ideal satisfying $R/\mathfrak{m} \cong k$. Moreover, these ideals are distinct: if $x_i - a_i, x_i - a_i'$ are in the same ideal for $a_i \neq a_i'$, then the unit $a_i - a_i'$ is in the ideal, so it is not proper. Therefore, our map is injective. To see that it is surjective, let $\mathfrak{m}$ be a maximal ideal with $R/\mathfrak{m} \cong k$. Each class in $R/\mathfrak{m}$ corresponds to a unique $a \in k$, so in particular each x_i is in the class of a unique $a_i \in k$. This means that $x_i - a_i \in \mathfrak{m}$, and thus $(x_1 - a_1, \ldots, x_d - a_d) \subseteq \mathfrak{m}$. Since $(x_1 - a_i, \ldots, x_d - a_i)$ is a maximal ideal, we must have $(x_1 - a_1, \ldots, x_d - a_d) = \mathfrak{m}$. □

Example 3.17. Not all maximal ideals in $k[x_1, \ldots, x_d]$ are necessarily of this form. For example, if $k = \mathbb{R}$ and $d = 1$, the ideal $(x^2 + 1)$ is maximal, but

$$k[x]/(x^2 + 1) \cong \mathbb{C} \ncong k.$$

But this won't happen if k is algebraically closed.

Theorem 3.18 (Zariski's Lemma)**.** *Consider an extension of fields $k \subseteq L$. If L is a finitely generated k-algebra, then L is a finite dimensional k-vector space. In particular, if k is algebraically closed then $L = k$.*

This is a nice application of the Artin-Tate Lemma, together with some facts about transcendent elements. We will skip the proof, but you can find it in Jeffries' notes.

Corollary 3.19 (Nullstellensatz)**.** *Let $S = k[x_1, \ldots, x_d]$ be a polynomial ring over an algebraically closed field k. There is a bijection*

$$\begin{array}{ccc} \mathbb{A}_k^d & \longrightarrow & \{\text{maximal ideals } \mathfrak{m} \text{ of } S\} \\ (a_1, \ldots, a_d) & \longmapsto & (x_1 - a_1, \ldots, x_d - a_d) \end{array}$$

If R is a finitely generated k-algebra, we can write $R = S/I$ for a polynomial ring S, and there is an induced bijection

$$\mathcal{Z}_k(I) \subseteq \mathbb{A}_k^d \longleftrightarrow \{\text{maximal ideals } \mathfrak{m} \text{ of } R\}.$$

Proof. The first part follows immediately from Lemma 3.16 and Lemma 3.18.

To show the second statement, fix an ideal I in S, and $R = S/I$. The maximal ideal ideals in R are in bijection with the maximal ideals $\mathfrak{m}$ in S that contain I; those are the ideals of the form $(x_1 - a_1, \ldots, x_d - a_d)$ with $I \subseteq (x_1 - a_1, \ldots, x_d - a_d)$. These are in bijection with the points $(a_1, \ldots, a_d) \in \mathbb{A}_k^d$ satisfying $(a_1, \ldots, a_d) \in \mathcal{Z}_k(I)$. □

Theorem 3.20 (Weak Nullstellensatz)**.** *Let k be an algebraically closed field. If I is a proper ideal in $R = k[x_1, \ldots, x_d]$, then $\mathcal{Z}_k(I) \neq \varnothing$.*

Proof. If $I \subseteq R$ is a proper ideal, there is a maximal ideal $\mathfrak{m} \supseteq I$, so $\mathcal{Z}(\mathfrak{m}) \subseteq \mathcal{Z}(I)$. Since $\mathfrak{m} = (x_1 - a_1, \ldots, x_d - a_d)$ for some $a_i \in k$, $\mathcal{Z}(\mathfrak{m})$ is a point, and thus nonempty. □

Over an algebraically closed field, maximal ideals in $k[x_1, \ldots, x_d]$ correspond to points in $\mathbb{A}^d$. So we can start from the solution set — a point — and recover an ideal that corresponds to it. What if we start with some non-maximal ideal I, and consider its solution set $\mathcal{Z}_k(I)$ — can we recover I in some way?

Example 3.21. Many ideals define the same solution set. For example, in $R = k[x]$, the ideals $I_n = (x^n)$, for any $n \geqslant 1$, all define the same solution set $\mathcal{Z}_k(I_n) = \{0\}$.

To attack this question, we will need an observation on inequations.

Remark 3.22 (Rabinowitz's trick)**.** Observe that, if $f(\underline{x})$ is a polynomial and $\underline{a} \in \mathbb{A}^d$, $f(\underline{a}) \neq 0$ if and only if $f(\underline{a}) \in k$ is invertible; equivalently, if there is a solution $y = b \in k$ to $yf(\underline{a}) - 1 = 0$. In particular, a system of polynomial equations and inequations

$$\begin{cases} f_1(\underline{x}) = 0 \\ \vdots \\ f_m(\underline{x}) = 0 \end{cases} \text{ and } \begin{cases} g_1(\underline{x}) \neq 0 \\ \vdots \\ g_n(\underline{x}) \neq 0 \end{cases}$$

has a solution $\underline{x} = \underline{a}$ if and only if the system

$$\begin{cases} f_1(\underline{x}) = 0 \\ \vdots \\ f_m(\underline{x}) = 0 \end{cases} \text{ and } \begin{cases} y_1 g_1(\underline{x}) - 1 = 0 \\ \vdots \\ y_n g_n(\underline{x}) - 1 = 0 \end{cases}$$

has a solution $(\underline{x}, \underline{y}) = (\underline{a}, \underline{b})$. In fact, this is equivalent to a system in one extra variable:

$$\begin{cases} f_1(\underline{x}) = 0 \\ \vdots \\ f_m(\underline{x}) = 0 \\ y g_1(\underline{x}) \cdots g_n(\underline{x}) - 1 = 0 \end{cases}$$

Theorem 3.23 (Strong Nullstellensatz)**.** *Let k be an algebraically closed field, and $R = k[x_1, \ldots, x_d]$ be a polynomial ring. Let $I \subseteq R$ be an ideal. The polynomial f vanishes on $\mathcal{Z}_k(I)$ if and only if $f^n \in I$ for some $n \in \mathbb{N}$.*

Proof. Suppose that $f^n \in I$. For each $\underline{a} \in \mathcal{Z}_k(I)$, $f(\underline{a}) \in k$ satisfies $f(\underline{a})^n = 0 \in k$. Since k is a field, $f(\underline{a}) = 0$. Thus, $f \in \mathcal{Z}_k(I)$ as well.

Suppose that f vanishes along $\mathcal{Z}_k(I)$. This means that given any solution $\underline{a} \in \mathbb{A}^d$ to the system determined by I, $f(\underline{a}) = 0$. In other words, the system

$$\begin{cases} g(\underline{x}) = 0 \text{ for all } g \in I \\ f \neq 0 \end{cases}$$

has no solutions. By the discussion above, $\mathcal{Z}_k(I + (yf - 1)) = \varnothing$ in a polynomial ring in one more variable. By the Weak Nullstellensatz, we have $IR[y] + (yf - 1) = R[y]$, and equivalently $1 \in IR[y] + (yf - 1)$. Write $I = (g_1(\underline{x}), \ldots, g_m(\underline{x}))$, and

$$1 = r_0(\underline{x}, y)(1 - yf(\underline{x})) + r_1(\underline{x}, y)g_1(\underline{x}) + \cdots + r_m(\underline{x}, y)g_m(\underline{x}).$$

We can map y to $1/f$ to get

$$1 = r_1(\underline{x}, 1/f)g_1(\underline{x}) + \cdots + r_m(\underline{x}, 1/f)g_m(\underline{x})$$

in the fraction field of $R[y]$. Since each r_i is polynomial, there is a largest negative power of f occurring; say that f^n serves as a common denominator. We can multiply by f^n to obtain f^n as a polynomial combination of the g's. □

Definition 3.24. 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 $I = \sqrt{I}$.

To see that $\sqrt{I}$ is an ideal, note that if $f^m, g^n \in I$, then

$$\begin{aligned}(f+g)^{m+n-1} &= \sum_{i=0}^{m+n-1} \binom{m+n-1}{i} f^i g^{m+n-1-i} \\ &= f^m \left(f^{n-1} + \binom{m+n-1}{1} f^{n-2}g + \cdots + \binom{m+n-1}{n-1} g^{n-1} \right) \\ &\quad + g^n \left(\binom{m+n-1}{n} f^{m-1} + \binom{m+n-1}{n+1} f^{m-2}g + \cdots + g^{m-1} \right) \in I,\end{aligned}$$

and $(rf)^m = r^m f^m \in I$.

Example 3.25. Prime ideals are radical.

Exercise 11. A nonzero element $f \in R$ is **nilpotent** if $f^n = 0$ for some $n > 1$; a ring R is **reduced** if it has no nilpotent elements. If R is a ring and I an ideal, then R/I is reduced if and only if I is a radical ideal.

Using this terminology, we can rephrase the Strong Nullstellensatz: if $k = \overline{k}$, then $f \in \mathcal{I}(\mathcal{Z}_k(I))$ if and only if $f \in \sqrt{I}$. Given any ideal I in $k[x_1, \ldots, x_d]$, $\mathcal{I}(\mathcal{Z}(I)) = \sqrt{I}$.

We can now associate a ring to each subvariety of $\mathbb{A}^d$.

Definition 3.26. Let k be an algebraically closed field, and $X = \mathcal{Z}_k(I) \subseteq \mathbb{A}^d$ be a subvariety of $\mathbb{A}^d$. The **coordinate ring** of X is the ring $k[X] := k[x_1, \ldots, x_d]/\mathcal{I}(X)$.

Since $k[X]$ is obtained from the polynomial ring on the ambient $\mathbb{A}^d$ by quotienting out by exactly those polynomials that are zero on X, we interpret $k[X]$ as the ring of polynomial functions on X. Note that every reduced finitely generated k-algebra is a coordinate ring of some zero set X.

Remark 3.27. We showed before that $\mathcal{Z}(IJ) = \mathcal{Z}(I \cap J)$, despite the fact that we often have $IJ \neq I \cap J$. The Strong Nullstellensatz implies that $\sqrt{IJ} \neq \sqrt{I + J}$.

Remark 3.28. Observe that $\mathcal{Z}_k(\sqrt{J}) = \mathcal{Z}_k(J)$ whether or not k is algebraically closed, by the same proof we used above. The containment $\subseteq$ is immediate since $J \subseteq \sqrt{J}$ from the definition. Moreover, if $f^n(\underline{a}) = 0$ then $f(\underline{a}) = 0$, so if $\underline{a} \in \mathcal{Z}_k(J)$ and $f \in \sqrt{J}$ then $f(\underline{a}) = 0$, and the equality of sets follows.

What might fail when the field is not algebraically closed is that $\mathcal{I}(\mathcal{Z}(I))$ is not necessarily $\sqrt{I}$. For example, $\mathcal{Z}_{\mathbb{R}}(x^2+1) = \varnothing$, so

$$\mathcal{I}(\mathcal{Z}_{\mathbb{R}}(x^2+1)) = \mathcal{I}(\emptyset) = \mathbb{R}[x] \neq \sqrt{(x^2+1)} = (x^2+1).$$

In fact, the ingredient that is missing is precisely the fact that the Weak Nullstellensatz is not satisfied over non-algebraically closed fields. If k is not algebraically closed, there exists some irreducible polynomial $f \in k[x]$ with no roots, so $\mathcal{Z}(f) = \varnothing$.

Remark 3.29. Note that if I is a radical ideal and $I \subsetneq J$, then $\mathcal{Z}(J) \subsetneq \mathcal{Z}(I)$. Indeed, there is some $f \in J$ such that $f \notin \sqrt{I} = I$, and thus $\mathcal{Z}(I) \not\subseteq \mathcal{Z}(f)$. Since $\mathcal{Z}(J) \subseteq \mathcal{Z}(f)$, we conclude that $\mathcal{Z}(I) \not\subseteq \mathcal{Z}(J)$.

Each variety corresponds to a unique radical ideal.

Corollary 3.30. *Let k be an algebraically closed field and $R = k[x_1, \ldots, x_d]$ a polynomial ring. There is an order-reversing bijection between the collection of subvarieties of $\mathbb{A}^d_k$ and the collection of radical ideals of R:*

$$\begin{array}{ccc} \{\textit{subvarieties of } \mathbb{A}^d_k\} & \longleftrightarrow & \{\textit{radical ideals } I \subseteq R\} \\ X & \overset{\mathcal{I}}{\longmapsto} & \{f \in R \mid X \subseteq \mathcal{Z}_k(f)\} \\ \mathcal{Z}_k(I) & \overset{\mathcal{Z}}{\longmapsfrom} & I \end{array}$$

In particular, given ideals I and J, we have $\mathcal{Z}_k(I) = \mathcal{Z}_k(J)$ if and only if $\sqrt{I} = \sqrt{J}$.

Proof. The Strong Nullstellensatz says that $\mathcal{I}(\mathcal{Z}(J)) = \sqrt{J}$ for any ideal J, hence $\mathcal{I}(\mathcal{Z}(J)) = J$ for a radical ideal J. Conversely, given X we can write $X = \mathcal{Z}_k(J)$ for some ideal J, and we without loss of generality we can assume J is radical, since $\mathcal{Z}_k(J) = \mathcal{Z}_k(\sqrt{J})$. Then $\mathcal{Z}(\mathcal{I}(X)) = \mathcal{Z}(\mathcal{I}(\mathcal{Z}(J))) = \mathcal{Z}(J) = X$.

This shows that $\mathcal{I}$ and $\mathcal{Z}$ are inverse operations, and we are done. □

Under this bijection, irreducible varieties correspond to prime ideals.

Lemma 3.31. *A variety $X \subseteq \mathbb{A}^d_k$ is irreducible if and only if $\mathcal{I}(X)$ is prime.*

Proof. Suppose that X is reducible, say $X = V_1 \cup V_2$ for two varieties V_1 and V_2 such that $V_1, V_2 \subsetneq X$. Note that this implies that $\mathcal{I}(X) \subsetneq \mathcal{I}(V_1)$, $\mathcal{I}(X) \subsetneq \mathcal{I}(V_2)$, and $\mathcal{I}(X) = \mathcal{I}(V_1) \cap \mathcal{I}(V_2)$. Then we can find $f \in \mathcal{I}(V_1)$ such that $f \notin \mathcal{I}(V_2)$, and $g \in \mathcal{I}(V_2)$ such that $g \notin \mathcal{I}(V_1)$. Notice that by construction $fg \in \mathcal{I}(V_1) \cap \mathcal{I}(V_2)\mathcal{I}(X)$, while $f \notin \mathcal{I}(X)$ and $g \notin \mathcal{I}(X)$. Therefore, $\mathcal{I}(X)$ is not prime.

Now assume that $\mathcal{I}(X)$ is not prime, and fix $f, g \notin \mathcal{I}(X)$ with $fg \in \mathcal{I}(X)$. Then

$$X \subseteq \mathcal{Z}(fg) = \mathcal{Z}(f) \cup \mathcal{Z}(g).$$

The intersections

$$V_f = \mathcal{Z}(f) \cap X = \mathcal{Z}(\mathcal{I}(X) + (f))$$

and

$$V_g = \mathcal{Z}(g) \cap X = \mathcal{Z}(\mathcal{I}(X) + (g))$$

are varieties, and $X = V_f \cup V_g$. Finally, since $f \notin \mathcal{I}(X)$, then $X \not\subseteq V_f$. Similarly, $X \not\subseteq V_g$. Thus X is reducible. □

Given a variety X, we can decompose it in irreducible components by writing it as a union $X = V_1 \cup \cdots \cup V_n$. We can do this decomposition algebraically, by considering the radical ideal $I = \mathcal{I}(X)$ and writing it as an intersection of its minimal primes.

Definition 3.32. A prime P is a **minimal prime** of an ideal I if the only prime Q with $I \subseteq Q \subseteq P$ is $Q = P$. The set of minimal primes over I is denoted $\operatorname{Min}(I)$.

Soon we will show that

$$\sqrt{I} = \bigcap_{\substack{P \text{ prime} \\ P \supseteq I}} P = \bigcap_{P \in \operatorname{Min}(I)} P.$$

Later, we will prove that the set of minimal primes of an ideal in a Noetherian ring is finite, so in particular we can write $\mathcal{I}(X)$ as a finite intersection of prime ideals, say

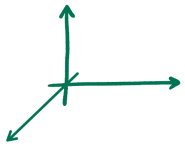
$$\mathcal{I}(X) = P_1 \cap \cdots \cap P_k.$$

Then

$$X = \mathcal{Z}(P_1) \cup \cdots \cup \mathcal{Z}(P_k)$$

is a decomposition of X into irreducible components.

Example 3.33. In $k[x, y, z]$, the radical ideal $I = (xy, xz, yz)$ corresponds to the variety X given by the union of the three coordinate axes.



Each of these axes is a variety in its own right, corresponding to the ideals (x, y), (x, z) and (y, z). The three axes are the irreducible components of X. And indeed, (x, y), (x, z) and (y, z) are the three minimal primes over I, and

$$(xy, xz, yz) = (x, y) \cap (x, z) \cap (y, z).$$

We will come back to this decomposition when we discuss primary decomposition.

In summary, Nullstellensatz gives us a dictionary between varieties and ideals:

Algebra		Geometry
algebra of ideals	$\longleftrightarrow$	geometry of varieties
algebra of $R = k[x_1, \ldots, x_d]$	$\longleftrightarrow$	geometry of $\mathbb{A}^d$
radical ideals	$\longleftrightarrow$	varieties
prime ideals	$\longleftrightarrow$	irreducible varieties
maximal ideals	$\longleftrightarrow$	points
(0)	$\longleftrightarrow$	variety $\mathbb{A}^d$
$k[x_1, \ldots, x_d]$	$\longleftrightarrow$	variety $\varnothing$
$(x_1 - a_1, \ldots, x_d - a_d)$	$\longleftrightarrow$	point $\{(a_1, \ldots, a_d)\}$
smaller ideals	$\longleftrightarrow$	larger varieties
larger ideals	$\longleftrightarrow$	smaller varieties

We now know that the subvarieties $\mathcal{Z}(I)$ of $\mathbb{A}^d$ satisfy the following properties:

- The sets $\varnothing$ and $\mathbb{A}^d$ are varieties.
- The finite union of varieties is a variety.
- The arbitrary intersection of varieties is a variety.

These are the axioms of closed sets in a topology. So there is a topology on $\mathbb{A}^d$ whose closed sets are precisely all the subvarieties $\mathcal{Z}(I)$ of $\mathbb{A}^d$. This topology is called the **Zariski topology**.

As a consequence, every variety inherits the Zariski topology, and this is the topology that algebraic geometers usually consider.

Exercise 12. A topological space X is **Noetherian** if it satisfies the descending chain condition for closed subsets: any descending chain of closed subsets

$$X_1 \supseteq X_2 \supseteq \cdots$$

stabilizes. Show that a variety with the Zariski topology is Noetherian.

Exercise 13. Show that if X is a Noetherian topological space, every open subset of X is quasicompact.

This topology is a little weird. In particular, it is *never* Hausdorff, unless the space we are considering is finite. The word *compact* is usually taken to include *Hausdorff*, so algebraic geometers say **quasicompact** to mean compact but maybe not Hausdorff.

Exercise 14. Show that $\mathbb{A}^d_{\mathbb{C}}$ with the Zariski topology is T_1 but not Hausdorff.

3.4 The prime spectrum of a ring

In modern algebraic geometry, on e often studies schemes instead of varieties. We will now introduce the simplest scheme: the spectrum $\mathrm{Spec}(R)$ of a ring R. The spectra of rings are to schemes as $\mathbb{R}^n$ is to manifolds: while a manifold is a topological space that locally looks like $\mathbb{R}^n$, a scheme is, roughly speaking, a topological space that locally looks like $\mathrm{Spec}(R)$ for some ring R.

The *maximal spectrum* of a ring R, denoted $\mathrm{mSpec}(R)$, is the set of maximal ideals of R endowed with the topology with closed sets given by

$$V_{\mathrm{Max}}(I) := \{\mathfrak{m} \in \mathrm{Max}(R) \mid \mathfrak{m} \supseteq I\}$$

as I varies over all the ideals in R. By the Nullstellensatz, for polynomial rings S over an algebraically closed field k, this space $\mathrm{mSpec}(S)$ has a natural homeomorphism to $\mathbb{A}^n$ with its Zariski topology, and for an ideal I in $S = k[x_1, \ldots, x_d]$, $\mathrm{mSpec}(S/I)$ has a natural homeomorphism to $\mathcal{Z}_k(I) \subseteq \mathbb{A}^n$ with the subspace topology coming from the Zariski topology. Moreover, this is functorial: for any map of finitely generated k-algebras, there is an induced map on maximal ideals.

This is not quite the right notion to deal with general rings, for at least two reasons. First, there are many many interesting rings with only one maximal ideal! The topological space with one element, in contrast, is not that exciting. Second, we would like to have a geometric space that is assigned *functorially* to a ring, meaning that ring homomorphisms induce continuous maps of spaces (in the other direction). For the inclusion $A = k[x, y] = k[x - 1, y]$ into $B = k(x)[y] = k(x - 1)[y]$, what maximal ideal in A would we assign to $(y) \subseteq B$? How could one of (x, y) or $(x - 1, y)$ have a better claim than the other?

Definition 3.34. Let R be a ring. The **prime spectrum**, or **spectrum** of R is the set of prime ideals of R, denoted $\mathrm{Spec}(R)$. This is naturally a poset, partially ordered by inclusion. We also endow it with the topology with closed sets

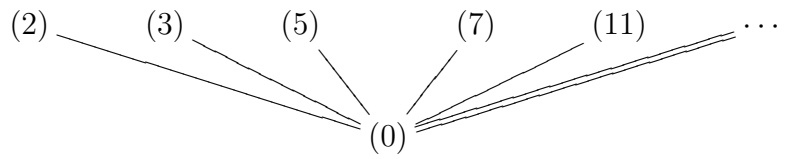
$$V(I) := \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \supseteq I\}$$

for (not necessarily proper) ideals $I \subseteq R$. In particular, $\varnothing = V(R)$ is closed.

Soon we will justify that this indeed forms a topology.

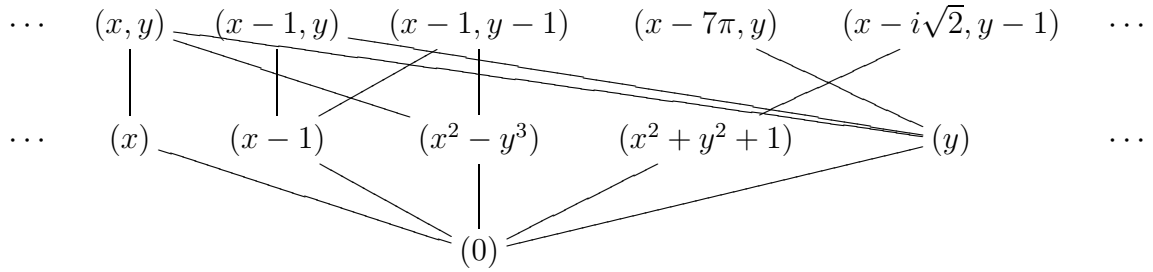
We will illustrate posets with Hasse diagrams: if an element is below something with a line connecting them, the higher element is $\geqslant$ the lower one.

Example 3.35. The spectrum of $\mathbb{Z}$ is the following poset:



The closed sets are of the form $V((n))$, which are the whole space when $n = 0$, the empty set with $n = 1$, and any finite union of things in the top row.

Example 3.36. Here are a few elements in $\mathbb{C}[x, y]$:



Note that $\mathrm{Max}(R)$ is a subspace of $\mathrm{Spec}(R)$ (that may be neither closed nor open).

Proposition 3.37. *Let R be a ring, and let I, J, and I_λ be ideals (possibly improper).*

a) If $I \subseteq J$, then $V(J) \subseteq V(I)$.

b) $V(I) \cup V(J) = V(I \cap J) = V(IJ)$.

c) $\bigcap_\lambda V(I_\lambda) = V(\sum_\lambda I_\lambda)$.

d) $\mathrm{Spec}(R)$ *has a basis given by open sets of the form*

$$D(f) := \mathrm{Spec}(R) \smallsetminus V(f) = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid f \notin \mathfrak{p}\}.$$

e) $\mathrm{Spec}(R)$ *is quasicompact.*

Proof.

a) Clear from the definition.

b) To see $V(I) \cup V(J) \subseteq V(I \cap J)$, just observe that if $\mathfrak{p} \supseteq I$ or $\mathfrak{p} \supseteq J$, then $\mathfrak{p} \supseteq I \cap J$. Since $IJ \subseteq I \cap J$, we have $V(I \cap J) \subseteq V(IJ)$. To show $V(IJ) \subseteq V(I) \cup V(J)$, if $\mathfrak{p} \not\supseteq I, J$, let $f \in I \smallsetminus \mathfrak{p}$, and $g \in J \smallsetminus \mathfrak{p}$. Then $fg \in IJ \smallsetminus \mathfrak{p}$ since $\mathfrak{p}$ is prime.

c) Ideals are closed for sums, so if $\mathfrak{p} \supseteq I_\lambda$ for all λ, then $\mathfrak{p} \supseteq \sum_\lambda I_\lambda$. Moreover, if $\mathfrak{p} \supseteq \sum_\lambda I_\lambda$, then in particular $\mathfrak{p} \supseteq I_\lambda$.

d) We can write any open set as the complement of $V(\{f_\lambda\}_\lambda) = \bigcap_\lambda V(f_\lambda)$, which is the union of $D(f_\lambda)$.

e) Given a sequence of ideals I_λ, if $\sum_\lambda I_\lambda = R$, then 1 is in the sum on the left, and thus 1 can be realized in such a sum over finitely many indices, so

$$R = \sum_\lambda I_\lambda = I_{\lambda_1} + \cdots + I_{\lambda_t}.$$

Thus, if we have a family of closed sets with empty intersection,

$$\varnothing = \bigcap_\lambda V(I_\lambda) = V\left(\sum_\lambda I_\lambda\right) = V(I_{\lambda_1} + \cdots + I_{\lambda_t}) = V(I_{\lambda_1}) \cap \cdots \cap V(I_{\lambda_t}),$$

so some finite subcollection has an empty intersection. □

Definition 3.38 (Induced map on Spec)**.** Given a homomorphism of rings $R \xrightarrow{\varphi} S$, we obtain a map on spectra

$$\begin{array}{ccc} \operatorname{Spec}(S) & \xrightarrow{\varphi^*} & \operatorname{Spec}(R) \\ \mathfrak{p} & \longrightarrow & \varphi^{-1}(\mathfrak{p}) \end{array}.$$

The key point here is that the preimage of a prime ideal is also prime. We will often write $\mathfrak{p} \cap R$ for $\varphi^{-1}(\mathfrak{p})$, even if the map is not necessarily an inclusion.

This is not only an order-preserving map, but also continuous: if $U \subseteq \operatorname{Spec}(R)$ is open, say U is the complement of $V(I)$ for some ideal I, then for a prime $\mathfrak{q}$ of S,

$$\mathfrak{q} \in (\varphi^*)^{-1}(U) \iff \mathfrak{q} \cap R \not\supseteq I \iff \mathfrak{q} \not\supseteq IS \iff \mathfrak{q} \notin V(IS).$$

So $(\varphi^*)^{-1}(U)$ is the complement of $V(IS)$, and thus open.

Example 3.39. Let $R \xrightarrow{\pi} R/I$ be the canonical projection. Then

$$\operatorname{Spec}(R/I) \xrightarrow{\pi^*} \operatorname{Spec}(R)$$

corresponds to the inclusion of $V(I)$ into $\operatorname{Spec}(R)$, since primes of R/I correspond to primes of R containing I.

We can use the spectrum of a ring to give an analogue of the strong Nullstellensatz that is valid for any ring. To prepare for this, we need a notion that we will use later.

Definition 3.40. A subset $W \subseteq R$ of a ring R is **multiplicatively closed** if $1 \in W$ and $a, b \in W \Rightarrow ab \in W$.

Lemma 3.41. *Let R be a ring, I an ideal, and W a multiplicatively closed subset. If $W \cap I = \varnothing$, then there is a prime ideal $\mathfrak{p}$ with $\mathfrak{p} \supseteq I$ and $\mathfrak{p} \cap W = \varnothing$.*

Proof. Consider the family of ideals $\mathcal{F} := \{J \mid J \supseteq I, J \cap W = \varnothing\}$ ordered with inclusion. This is nonempty, since it contains I, and any chain $J_1 \subseteq J_2 \subseteq \cdots$ has an upper bound $\cup_i J_i$. Therefore, $\mathcal{F}$ has some maximal element $\mathbb{A}$ by a basic application of Zorn's Lemma. We claim $\mathbb{A}$ is prime. Suppose $f, g \notin \mathbb{A}$. By maximality, $\mathbb{A}+(f)$ and $\mathbb{A}+(g)$ both have nonempty intersection with W, so there exist $r_1 f + a_1$, $r_2 g + a_2 \in W$, with $a_1, a_2 \in \mathbb{A}$. If $fg \in \mathbb{A}$, then

$$(\underset{\in W}{r_1 f + a_1})(\underset{\in W}{r_2 g + a_2}) = r_1 r_2 fg + r_1 \underset{\in \mathbb{A}}{f a_2} + r_2 \underset{\in \mathbb{A}}{g a_1} + \underset{\in \mathbb{A}}{a_1 a_2} \in W \cap \mathbb{A},$$

a contradiction. □

Proposition 3.42 (Spectrum analogue of strong Nullstellensatz)**.** *Let R be a ring, and I be an ideal. For $f \in R$,*

$$V(I) \subseteq V(f) \iff f \in \sqrt{I}.$$

Equivalently,

$$\bigcap_{\mathfrak{p} \in V(I)} \mathfrak{p} = \sqrt{I}.$$

Proof. First to justify the equivalence of the two statements we observe:

$$V(I) \subseteq V(f) \iff f \in \mathfrak{p} \text{ for all } \mathfrak{p} \in V(I) \iff f \in \bigcap_{\mathfrak{p} \in V(I)} \mathfrak{p}.$$

We prove that $\bigcap_{\mathfrak{p} \in V(I)} \mathfrak{p} = \sqrt{I}$.

($\supseteq$): It suffices to show that $\mathfrak{p} \supseteq I$ implies $\mathfrak{p} \supseteq \sqrt{I}$, and indeed

$$f^n \in I \subseteq \mathfrak{p} \implies f \in \mathfrak{p}.$$

($\subseteq$): If $f \notin \sqrt{I}$, consider the multiplicatively closed set $W = \{1, f, f^2, f^3, \dots\}$. We have $W \cap I = \varnothing$ by hypothesis. By the previous lemma, there is a prime $\mathfrak{p}$ in $V(I)$ that does not intersect W, and hence does not contain f. □

The following corollary follows in exactly the same way as the analogous statement for subvarieties of $\mathbb{A}^n$, Corollary 3.30.

Corollary 3.43. *Let R a ring. There is an order-reversing bijection*

$$\{\textit{closed subsets of } \operatorname{Spec}(R)\} \quad \longleftrightarrow \quad \{\textit{radical ideals } I \subseteq R\}$$

In particular, for two ideals I, J, $V(I) = V(J)$ if and only if $\sqrt{I} = \sqrt{J}$.

Chapter 4

Local Rings

The study of local rings is central to commutative algebra. As we will see, life is easier in a local ring, so much so that we often want to *localize* so we can be in a local ring. A lot of the things we will say in this chapter also apply to $\mathbb{N}$-graded k-algebras and their homogenous maximal ideal — with some appropriate changes, such as considering only homogeneous ideals.

4.1 Local rings

Definition 4.1. A ring R is a **local ring** if it has exactly one maximal ideal. We often use the notation $(R, \mathfrak{m})$ to denote R and its maximal ideal, or $(R, \mathfrak{m}, k)$ to also specify the residue field $k = R/\mathfrak{m}$. Some people reserve the term *local ring* for a Noetherian local ring, and call what we have defined a **quasilocal ring**; we will not follow this convention here.

Lemma 4.2. *A ring R is local if and only if the set of nonunits of R forms an ideal.*

Proof. If the set of nonunits is an ideal, that must be the only maximal ideal. □

Example 4.3.

a) The ring $\mathbb{Z}/(p^n)$ is local with maximal ideal (p).

b) The ring $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b \text{ when in lowest terms}\}$ is a local ring with maximal ideal (p).

c) The ring of power series $k[\![\underline{x}]\!]$ over a field k is local. Indeed, a power series has an inverse if and only if its constant term is nonzero. The complement of this set of units is the ideal $(\underline{x})$.

d) More generally, $k[\![x_1, \ldots, x_d]\!]$ is local with maximal ideal $(x_1, \ldots, x_d)$.

e) The ring of complex power series holomorphic at the origin, $\mathbb{C}\{\underline{x}\}$, is local. In the above setting, one proves that the series inverse of a holomorphic function at the origin is convergent on a neighborhood of 0.

f) A polynomial ring over a field is certainly not local; we have seen it has so many maximal ideals!

We start with a comment about the characteristic of local rings.

Definition 4.4. The **characteristic** of a ring R is, if it exists, the smallest positive integer n such that

$$\underbrace{1 + \cdots + 1}_{n \text{ times}} = 0.$$

If no such n exists, we say that R has characteristic 0. Equivalently, the characteristic of R is the integer $n \geqslant 0$ such that

$$(n) = \ker \begin{pmatrix} \mathbb{Z} \longrightarrow R \\ a \longmapsto a \cdot 1_R \end{pmatrix}.$$

Proposition 4.5. *Let $(R, \mathfrak{m}, k)$ be a local ring. Then one of the following holds:*

a) $\operatorname{char}(R) = \operatorname{char}(k) = 0$. *We say that R has* **equal characteristic zero**.

b) $\operatorname{char}(R) = 0$, $\operatorname{char}(k) = p$ *for a prime p, so R has* **mixed characteristic** $(0, p)$.

c) $\operatorname{char}(R) = \operatorname{char}(k) = p$ *for a prime p, so R has* **equal characteristic** p.

d) $\operatorname{char}(R) = p^n$, $\operatorname{char}(k) = p$ *for a prime p and an integer $n > 1$.*

If R is reduced, then one of the first three cases holds.

Proof. Since k is a quotient of R, the characteristic of R must be a multiple of the characteristic of k, since the map $\mathbb{Z} \longrightarrow k$ factors through R. We must think of 0 as a multiple of any integer for this to make sense. Now k is a field, so its characteristic is 0 or p for a prime p. If $\operatorname{char}(k) = 0$, then necessarily $\operatorname{char}(R) = 0$. If $\operatorname{char}(k) = p$, we claim that $\operatorname{char}(R)$ must be either 0 or a power of p. Indeed, if we write $\operatorname{char}(R) = p^n \cdot a$ with a coprime to p, note that $p \in \mathfrak{m}$, so if $a \in \mathfrak{m}$, we have $1 \in (p, a) \subseteq \mathfrak{m}$, which is a contradiction. Since R is local, this means that a is a unit. But then, $p^n a = 0$ implies $p^n = 0$, so the characteristic must be p^n. □

Remark 4.6. If R is an $\mathbb{N}$-graded k-algebra with $R_0 = k$, and $\mathfrak{m} = \bigoplus_{n>0} R_0$ is the homogeneous maximal ideal, R and $\mathfrak{m}$ behave a lot like a local ring and its maximal ideal, and we sometimes use the suggestive notation $(R, \mathfrak{m})$ to refer to it. Many properties of local rings also apply to the graded setting, so given a statement about local rings, you might take it as a suggestion that there might be a corresponding statement about graded rings — a statement that, nevertheless, still needs to be proved. There are usually some changes one needs to make to the statement; for example, if a theorem makes assertions about the ideals in a local ring, the corresponding graded statement will likely only apply to homogeneous ideals, and a theorem about finitely generated modules over a local ring will probably translate into a theorem about graded modules in the graded setting.

4.2 Localization

Recall that a multiplicative subset of a ring R is a set $W \ni 1$ that is closed for products. The three most important classes of multiplicative sets are the following:

Example 4.7. Let R be a ring.

a) For any $f \in R$, the set $W = \{1, f, f^2, f^3, \dots\}$ is a multiplicative set.

b) If $\mathfrak{p} \subseteq R$ is a prime ideal, the set $W = R \smallsetminus \mathfrak{p}$ is multiplicative: this is an immediate translation of the definition.

c) The set of *nonzerodivisors* in R — elements that are not zerodivisors — forms a multiplicatively closed subset.

Remark 4.8. An arbitrary intersection of multiplicatively closed subsets is multiplicatively closed. In particular, for any family of primes $\{\mathfrak{p}_\lambda\}$, the complement of $\bigcup_\lambda \mathfrak{p}_\lambda$ is multiplicatively closed.

Definition 4.9 (Localization of a ring)**.** Let R be a ring, and W be a multiplicative set with $0 \notin W$. The **localization** of R at W is the ring

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

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

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

The zero in $W^{-1}R$ is $\frac{0}{1}$ and the identity is $\frac{1}{1}$. There is a canonical ring homomorphism

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

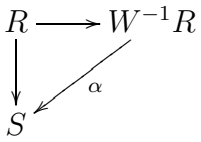
Given an ideal I in $W^{-1}R$, we write $I \cap R$ for its preimage of I in R via the canonical map $R \longrightarrow W^{-1}R$.

Note that we write elements in $W^{-1}R$ in the form $\frac{r}{w}$ even though they are equivalence classes of such expressions.

Remark 4.10. Observe that if R is a domain, the equivalence relation simplifies to $rw' = r'w$, so $R \subseteq W^{-1}R \subseteq \mathrm{Frac}(R)$, and in particular $W^{-1}R$ is a domain too. In particular, $\mathrm{Frac}(R)$ is a localization of R.

In the localization of R at W, every element of W becomes a unit. The following universal property says roughly that $W^{-1}R$ is the smallest R-algebra in which every element of W is a unit.

Proposition 4.11. *Let R be a ring, and W a multiplicative set with $0 \notin W$. Let S be an R-algebra in which every element of W is a unit. Then there is a unique homomorphism α such that the following diagram commutes:*



where the vertical map is the structure homomorphism and the horizontal map is the canonical homomorphism.

Example 4.12 (Most important localizations)**.** Let R be a ring.

a) For $f \in R$ and $W = \{1, f, f^2, f^3, \dots\}$, we usually write R_f for $W^{-1}R$.

b) For a prime ideal p in R, we generally write $R_{\mathfrak{p}}$ for $(R \smallsetminus \mathfrak{p})^{-1}R$, and call it **the localization of R at $\mathfrak{p}$**. Given an ideal I in R, we sometimes write $I_{\mathfrak{p}}$ to refer to $IR_{\mathfrak{p}}$, the image of I via the canonical map $R \to R_{\mathfrak{p}}$.

c) When W is the set of nonzerodivisors on R, we call $W^{-1}R$ the **total ring of fractions** of R. When R is a domain, this is just the fraction field of R, and in this case this coincides with the localization at the prime (0).

Remark 4.13. Notice that when we localize at a prime $\mathfrak{p}$, the resulting ring is a local ring $(R_{\mathfrak{p}}, \mathfrak{p}_{\mathfrak{p}})$. We can think of the process of localization at $\mathfrak{p}$ as *zooming in* at the prime $\mathfrak{p}$. Many properties of an ideal I can be checked *locally*, by checking them for $IR_{\mathfrak{p}}$ for each prime $\mathfrak{p} \in V(I)$.

If R is not a domain, the canonical map $R \to W^{-1}R$ is not necessarily injective.

Example 4.14. Consider $R = k[x, y]/(xy)$. The canonical maps $R \longrightarrow R_{(x)}$ and $R \longrightarrow R_y$ are not injective, since in both cases y is invertible in the localization, and thus

$$x \mapsto \frac{x}{1} = \frac{xy}{y} = \frac{0}{y} = \frac{0}{1}.$$

We can now add some more local rings to our list of examples.

Example 4.15.

a) A local ring one often encounters is $k[x_1, \dots, x_d]_{(x_1,\dots,x_d)}$. We can consider this as the ring of rational functions that in lowest terms have a denominator with nonzero constant term. Note that we can talk about lowest terms since the polynomial ring is a UFD.

b) Extending the following example, we have local rings like $(k[x_1, \ldots, x_d]/I)_{(x_1,\ldots,x_d)}$. If k is algebraically closed and I is a radical ideal, then $k[x_1, \ldots, x_d]/I = k[X]$ is the coordinate ring of some affine variety, and $(x_1, \ldots, x_d) = \mathfrak{m}_{\underline{0}}$ is the ideal defining the origin (as a point in $X \subseteq \mathbb{A}^d$). Then we call

$$k[X]_{\mathfrak{m}_{\underline{0}}} := (k[x_1, \ldots, x_d]/I)_{(x_1,\ldots,x_d)}$$

the **local ring of the point** $\underline{0} \in X$; some people write $\mathcal{O}_{X,\underline{0}}$. The radical ideals of this ring consist of radical ideals of $k[X]$ that are contained in $\mathfrak{m}_{\underline{0}}$, which by the Nullstellensatz correspond to subvarieties of X that contain $\underline{0}$. Similarly, we can define the local ring at any point $\underline{a} \in X$.

We state an analogous definition for modules, and for module homomorphisms.

Definition 4.16. Let R be a ring, W be a multiplicative set, and M an R-module. The **localization** of M at W is the $W^{-1}R$-module

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

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

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

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

We will use the notations M_f and $M_{\mathfrak{p}}$ analogously to R_f and $R_{\mathfrak{p}}$.

To understand localizations of rings and modules, we will want to understand better how they are built from R. First, we take a small detour to talk about colons and annihilators.

Definition 4.17. The **annihilator** of a module M is the ideal

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

Definition 4.18. Let I and J be ideals in a ring 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-modules A, the colon of N and M is

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

Exercise 15. 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.

Remark 4.19. If $M = Rm$ is a one-generated R-module, then $M \cong R/I$ for some ideal I. Notice that $I \cdot (R/I) = 0$, and that given an element $g \in R$, we have $g(R/I) = 0$ if and only if $g \in I$. Therefore, $M \cong R/\operatorname{ann}(M)$.

Remark 4.20. Let M be an R-module. If I is an ideal in R such that $I \subseteq \operatorname{ann}(M)$, then $IM = 0$, and thus M has is naturally an R/I-module with the *same* structure it has as an R-module, meaning

$$(r + I) \cdot m = rm$$

for each $r \in R$.

Remark 4.21. If $N \subseteq M$ are R-modules, then $\operatorname{ann}(M/N) = (N :_R M)$.

Lemma 4.22. *Let M be an R-module, and W a multiplicative set. The class*

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

Note in particular that this holds for $w = 1$.

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 4.23. It follows from this lemma that if $N \xrightarrow{\alpha} M$ is injective, then $W^{-1}\alpha$ is also injective, since

$$0 = W^{-1}\alpha\left(\frac{n}{w}\right) = \frac{\alpha(n)}{w} \Rightarrow 0 = u\alpha(n) = \alpha(un) \text{ for some } u \in W \Rightarrow un = 0 \Rightarrow \frac{n}{w} = 0.$$

We want to collect one more lemma for later.

Lemma 4.24. *Let M be a module, and $N_1, \ldots, N_t$ be a finite collection of submodules. Let W be a multiplicative set. Then,*

$$W^{-1}(N_1 \cap \cdots \cap N_t) = W^{-1}N_1 \cap \cdots \cap W^{-1}N_t \subseteq W^{-1}M.$$

Proof. The containment $W^{-1}(N_1 \cap \cdots \cap N_t) \subseteq W^{-1}N_1 \cap \cdots \cap W^{-1}N_t$ is clear. Elements of $W^{-1}N_1 \cap \cdots \cap W^{-1}N_t$ are of the form $\frac{n_1}{w_1} = \cdots = \frac{n_t}{w_t}$; we can find a common denominator to realize this in $W^{-1}(N_1 \cap \cdots \cap N_t)$. □

Later we will show that localization has good homological properties: it's an exact functor.

Theorem 4.25. *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.

Remark 4.26. Given a submodule N of M, we can apply the statement above to the short exact sequence

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

and conclude that that $W^{-1}(M/N) \cong W^{-1}M/W^{-1}N$.

Proposition 4.27. *Let W be multiplicatively closed 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 $\mathfrak{p}$ is prime and $W \cap \mathfrak{p} = \varnothing$, then $W^{-1}\mathfrak{p} = \mathfrak{p}(W^{-1}R)$ is prime.

d) The map $\operatorname{Spec}(W^{-1}R) \to \operatorname{Spec}(R)$ is injective, with image

$$\{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \cap W = \varnothing\}.$$

Proof.

a) Since $W^{-1}(R/I) \cong W^{-1}R/W^{-1}I$, we have $\ker(R \to W^{-1}(R/I)) = R \cap W^{-1}I$. The equality is then clear.

b) The containment $W^{-1}(J \cap R) \subseteq J$ holds for general reasons: given any map f, and a subset J of the target of f, $f(f^{-1}(J)) \subseteq J$. On the other hand, if $\frac{a}{w} \in J$, then $\frac{a}{1} \in J$, since its a unit multiple of an element of J, and thus $a \in J \cap R$, so $\frac{a}{w} \in W^{-1}(J \cap R)$.

c) First, since $W \cap \mathfrak{p} = \varnothing$, and $\mathfrak{p}$ is prime, no element of W kills $\bar{1} = 1 + \mathfrak{p}$ in $R/\mathfrak{p}$, so $\bar{1}/1$ is nonzero in $W^{-1}(R/\mathfrak{p})$. Thus, $W^{-1}R/W^{-1}\mathfrak{p} \cong W^{-1}(R/\mathfrak{p})$ is nonzero, and a localization of a domain, hence is a domain. Thus, $W^{-1}\mathfrak{p}$ is prime.

d) First, by part b), the map $\mathfrak{p} \mapsto W^{-1}\mathfrak{p}$, for $S = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \cap W = \varnothing\}$ sends primes to primes. We claim that

$$\begin{array}{ccc} \operatorname{Spec}(W^{-1}R) & & S \\ \mathfrak{q} & \longmapsto & \mathfrak{q} \cap R \\ W^{-1}\mathfrak{p} & \longmapsfrom & \mathfrak{p} \end{array}$$

are inverse maps.

We have already seen that $J = (J \cap R)W^{-1}R$ for any ideal J in $W^{-1}R$.

If $W \cap \mathfrak{p} = \varnothing$, then using part a) and the definition of prime, we have that

$$W^{-1}\mathfrak{p} \cap R = \{r \in R \mid rw \in \mathfrak{p} \text{ for some } w \in W\} = \{r \in R \mid r \in \mathfrak{p}\} = \mathfrak{p}. \qquad \square$$

Corollary 4.28. *Let R be a ring and $\mathfrak{p}$ be a prime ideal in R. The map on Spectra induced by the canonical map $R \to R_{\mathfrak{p}}$ corresponds to the inclusion*

$$\{\mathfrak{q} \in \operatorname{Spec}(R) \mid \mathfrak{q} \subseteq \mathfrak{p}\} \subseteq \operatorname{Spec}(R).$$

4.3 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 4.29. *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 1.35, 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 $m \in M$. $\square$

Proposition 4.30. *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 4.29, 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 $M = 0$. $\square$

Proposition 4.31. *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 4.30, $M = N$. □

Proposition 4.32. *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 4.30, $M/N = 0$ 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 4.33. Since $R/\mathfrak{m}$ is a field, $M/\mathfrak{m}M$ is a vector space over the field $R/\mathfrak{m}$.

Definition 4.34. 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 4.35. 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 4.36. *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 4.37. 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 4.38. *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 4.39. 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.

Chapter 5

Decomposing ideals

We will consider a few ways of decomposing ideals into pieces, in three ways with increasing detail. The first is the most directly geometric: for any ideal I in a Noetherian ring, we aim to write $V(I)$ as a finite union of $V(\mathfrak{p}_i)$ for prime ideals $\mathfrak{p}_i$.

5.1 Minimal primes and support

Recall the definition of minimal primes that we mentioned before.

Definition 5.1. The primes that contain I and are minimal with the property of containing I are called the **minimal primes** of I. That is, the minimal primes of I are the minimal elements of $V(I)$. We write $\mathrm{Min}(I)$ for this set.

Exercise 16. Let R be a ring, and I an ideal. Every prime $\mathfrak{p}$ that contains I contains a minimal prime of I. Consequently,

$$\sqrt{I} = \bigcap_{\mathfrak{p} \in \mathrm{Min}(I)} \mathfrak{p}.$$

Remark 5.2. If $\mathfrak{p}$ is prime, then $\mathrm{Min}(\mathfrak{p}) = \{\mathfrak{p}\}$. Also, since $V(I) = V(\sqrt{I})$, we have $\mathrm{Min}(I) = \mathrm{Min}(\sqrt{I})$.

As a special case, the nilpotent elements of a ring R are exactly the elements in every minimal prime of R, or equivalently, in every minimal prime of the ideal (0). The radical of (0) is often called the **nilradical** of R, denoted $\mathcal{N}(R)$.

Lemma 5.3. *Whenever $I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$ for some $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ for each i, j, we have $\mathrm{Min}(I) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.*

Proof. If $\mathfrak{q}$ is a prime containing I, then $\mathfrak{q} \supseteq (\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n)$. But if $\mathfrak{q} \not\supseteq \mathfrak{p}_i$ for each i, then there are elements $f_i \in \mathfrak{p}_i$ such that $f_i \notin \mathfrak{q}$, and the product $f_1 \cdots f_n \in (\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n)$ but $f_1 \cdots f_n \notin \mathfrak{q}$. Therefore, any minimal prime of I must be one of the $\mathfrak{p}_i$. Since we assumed that the $\mathfrak{p}_i$ are incomparable, they are exactly all the minimal primes of I. □

Remark 5.4. If $I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$ for some primes p_i, we can always delete unnecessary components until no component can be deleted. Therefore, $\mathrm{Min}(I) \subseteq \{\mathfrak{p}_1, \cdots, \mathfrak{p}_n\}$.

Theorem 5.5. *Let R be a Noetherian ring. Then any ideal I has finitely many minimal primes, and thus $\sqrt{I}$ is a finite intersection of primes.*

Proof. Let $S = \{\text{ideals } I \subseteq R \mid \mathrm{Min}(I) \text{ is infinite}\}$, and suppose, to obtain a contradiction, that $S \neq \varnothing$. Since R is Noetherian, S has a maximal element J, by Proposition 1.2. If J was a prime ideal, then $\mathrm{Min}(J) = \{J\}$ would be finite, by Remark 5.2, so J is not prime. However, $\mathrm{Min}(J) = \mathrm{Min}(\sqrt{J})$, and thus $\sqrt{J} \supseteq J$ is also in S, so we conclude that J is radical. Since J is not prime, we can find some $a, b \notin J$ with $ab \in J$. Then $J \subsetneq J + (a) \subseteq \sqrt{J + (a)}$ and $J \subsetneq \sqrt{J + (b)}$. Since J is maximal in S, we conclude that $\sqrt{J + (a)}$ and $\sqrt{J + (b)}$ have finitely many minimal primes, so we can write

$$J + (a) = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_a \text{ and } J + (b) = \mathfrak{p}_{a+1} \cap \cdots \cap \mathfrak{p}_b$$

for some prime ideals $\mathfrak{p}_i$. Let $f \in \sqrt{J + (a)} \cap \sqrt{J + (b)}$. Some sufficiently high power of f is in both $J + (a)$ and $J + (b)$, so there exist $n, m \geqslant 1$ such that

$$f^n = J + (a) \text{ and } f^m \in J + (b)$$

so

$$f^{n+m} \in (J + (a))(J + (b)) \subseteq J^2 + J(a) + J(b) + (\underbrace{ab}_{\in J}) \subseteq J.$$

Therefore, $f \in \sqrt{J} = J$. This shows that

$$J = (J + (a)) \cap (J + (b)) = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_a \cap \mathfrak{p}_{a+1} \cap \cdots \cap \mathfrak{p}_b.$$

By Lemma 5.3, we see that $\mathrm{Min}(J)$ must be a subset of $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_b\}$, so it is finite. □

Remark 5.6. Lemma 5.3, Theorem 5.5, and Exercise 16 imply that an ideal I is equal to a finite intersection of primes if and only if I is radical.

We now can describe the relationship between the poset structure of $\mathrm{Spec}(R)$ and the topology.

Proposition 5.7. *Let R be a ring, and $X = \mathrm{Spec}(R)$.*

a) The poset structure on X can be recovered from the topology: $\mathfrak{p} \subseteq \mathfrak{q} \Leftrightarrow \mathfrak{q} \in \overline{\{\mathfrak{p}\}}$.

b) If R is Noetherian, the topology on X can by recovered from the poset structure by the rule

$$Y \subseteq X \textit{ is closed} \Longleftrightarrow Y = \{\mathfrak{q} \in X \mid \mathfrak{p}_i \subseteq \mathfrak{q} \textit{ for some } i\} \textit{ for some } \mathfrak{p}_1, \ldots, \mathfrak{p}_n \in X.$$

Proof.

a) By definition of closure, we have

$$\overline{\{\mathfrak{p}\}} = \bigcap_{\mathfrak{p} \in V(I)} V(I).$$

If $\mathfrak{p} \in V(I)$ then $I \subseteq \mathfrak{p}$, which implies $V(\mathfrak{p}) \subseteq V(I)$. It follows that $\overline{\{\mathfrak{p}\}} = V(\mathfrak{p})$, and thus the claim.

b) If Y is closed, we have $Y = V(I) = V(\sqrt{I}) = V(\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n) = V(\mathfrak{p}_1) \cup \cdots \cup V(\mathfrak{p}_n)$. For the converse, we can work backwards. □

We now wish to understand modules in a similar way.

Definition 5.8. If M is an R-module, the **support** of M is

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

Proposition 5.9. *Given M a finitely generated R-module over a ring R,*

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

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

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

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

so

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

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

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

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

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

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 $\mathfrak{p} \in \operatorname{Supp}(M)$ if and only if $\mathfrak{p} \in \operatorname{Supp}(Rm_i)$ 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 $(R \setminus \mathfrak{p}) \cap \operatorname{ann}_R(m) \neq \varnothing$, which happens if and only if $\operatorname{ann}_R(m) \not\subseteq \mathfrak{p}$. □

The finite generating hypothesis is necessary!

Example 5.10. Let k be a field, and $R = k[x]$. Take

$$M = R_x/R = \bigoplus_{i>0} k \cdot x^{-i}.$$

With this k-vector space structure, the action is given by multiplication in the obvious way, then killing any nonnegative degree terms.

On one hand, we claim that $\operatorname{Supp}(M) = \{(x)\}$. Indeed, any element of M is killed by a large power of x, so $W^{-1}M = 0$ whenever $x \in W$, so $\operatorname{Supp}(M) \subseteq \{(x)\}$. We will soon see that the support of a nonzero module is nonempty, and thus $\operatorname{Supp}(M) = \{(x)\}$.

On the other hand, the annihilator of the class of x^{-n} is x^n, so

$$\operatorname{ann}_R(M) \subseteq \bigcap_{n \geqslant 1} (x^n) = 0.$$

In particular, $V(\operatorname{ann}_R(M)) = \operatorname{Spec}(R)$.

Example 5.11. Let $R = \mathbb{C}[x]$, and $M = \bigoplus_{n \in \mathbb{Z}} R/(x-n)$.

First, note that $M_{\mathfrak{p}} = \bigoplus_{n \in \mathbb{Z}} (R/(x-n))_{\mathfrak{p}}$, so

$$\operatorname{Supp}(M) = \bigcup_{n \in \mathbb{Z}} \operatorname{Supp}(R/(x-n)) = \bigcup_{n \in \mathbb{Z}} V((x-n)) = \{(x-n) \mid n \in \mathbb{Z}\}.$$

On the other hand,

$$\operatorname{ann}_R(M) = \bigcap_{n \in \mathbb{Z}} \operatorname{ann}_R(R/(x-n)) = \bigcap_{n \in \mathbb{Z}} (x-n) = 0.$$

Note that in this example the support is not even closed.

Lemma 5.12. *Let R be a ring, M an R-module, and $m \in M$. The following are equivalent:*

1) *$m = 0$ in M.*
2) *$\frac{m}{1} = 0$ in $M_{\mathfrak{p}}$ for all $\mathfrak{p} \in \operatorname{Spec}(R)$.*
3) *$\frac{m}{1} = 0$ in $M_{\mathfrak{p}}$ for all $\mathfrak{p} \in \operatorname{mSpec}(R)$.*

Proof. The implications 1) $\implies$ 2) $\implies$ 3) are clear. If $m \neq 0$, its annihilator is a proper ideal, which is contained in a maximal ideal, so $V(\operatorname{ann}_R m) = \operatorname{Supp}(Rm)$ contains a maximal ideal, so $\frac{m}{1} \neq 0$ in $M_{\mathfrak{p}}$ for some maximal ideal $\mathfrak{p}$. □

Lemma 5.13. *Let R be a ring, L, M, N be modules. If*

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

is exact, then $\operatorname{Supp}(L) \cup \operatorname{Supp}(N) = \operatorname{Supp}(M)$.

Proof. Localization is exact, by Theorem 4.25, so for any $\mathfrak{p}$,

$$0 \longrightarrow L_{\mathfrak{p}} \longrightarrow M_{\mathfrak{p}} \longrightarrow N_{\mathfrak{p}} \longrightarrow 0$$

is exact. If $\mathfrak{p} \in \mathrm{Supp}(L) \cup \mathrm{Supp}(N)$, then $L_{\mathfrak{p}}$ or $N_{\mathfrak{p}}$ is nonzero, so $M_{\mathfrak{p}}$ must be nonzero as well. On the other hand, if $\mathfrak{p} \notin \mathrm{Supp}(L) \cup \mathrm{Supp}(N)$, then $L_{\mathfrak{p}} = N_{\mathfrak{p}} = 0$, so $M_{\mathfrak{p}} = 0$. □

Remark 5.14. As a corollary, $\mathrm{Supp}(L) \subseteq \mathrm{Supp}(M)$ for any submodule L of M.

Corollary 5.15. *If M is a finitely generated R-module,*

1) $M = 0$.
2) $M_{\mathfrak{p}} = 0$ *in* $M_{\mathfrak{p}}$ *for all* $\mathfrak{p} \in \mathrm{Spec}(R)$.
3) $M_{\mathfrak{p}} = 0$ *in* $M_{\mathfrak{p}}$ *for all* $\mathfrak{p} \in \mathrm{mSpec}(R)$.

Proof.

The implications $\Rightarrow$ are clear. To show the last implies the first, we show the contrapositive. If $m \neq 0$, consider $Rm \subseteq M$. By Lemma 5.12, there is a maximal ideal in $\mathrm{Supp}(Rm)$, and by Lemma 5.13 applied to the inclusion $Rm \subseteq M$, this maximal ideal is in $\mathrm{Supp}(M)$ as well. □

So we conclude that $\mathrm{Supp}(M) \neq \varnothing$ for any R-module $M \neq 0$.

5.2 Associated primes

Remark 5.16. 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 $I \subseteq \mathrm{ann}(m)$.

Definition 5.17. Let R be a ring, and M a module. We say that $\mathfrak{p} \in \mathrm{Spec}(R)$ is an **associated prime** of M if $\mathfrak{p} = \mathrm{ann}_R(m)$ for some $m \in M$. Equivalently, $\mathfrak{p}$ is associated to M if there is an injective homomorphism $R/\mathfrak{p} \longrightarrow M$. We write $\mathrm{Ass}_R(M)$ for the set of associated primes of M.

If I is an ideal, by the **associated primes** of I we (almost always) mean the associated primes of R/I. To avoid confusion, we will try to write $\mathrm{Ass}_R(R/I)$.

Lemma 5.18. *Let R be a Noetherian ring and M be an R-module. A prime P is associated to M if and if and only if $P_P \in \mathrm{Ass}(M_P)$.*

Proof. Localization is exact, so any inclusion $R/P \subseteq M$ localizes to an inclusion $R_P/P_P \subseteq M_P$. Conversely, suppose that $P_P = \text{ann}(\frac{m}{w})$ for some $\frac{m}{w} \in M_P$. Let $P = (f_1, \dots, f_n)$. 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 $r \in \text{ann}(um)$, then $\frac{ru}{1} \in \text{ann}(\frac{m}{w}) = P_P$. We conclude that $ru \in P_P \cap R = P$. Since $u \notin P$, we conclude that $r \in P$. □

Lemma 5.19. *If $\mathfrak{p}$ is prime, $\text{Ass}_R(R/\mathfrak{p}) = \{\mathfrak{p}\}$.*

Proof. For any nonzero $\bar{r} \in R/\mathfrak{p}$, we have $\text{ann}_R(\bar{r}) = \{s \in R \mid rs \in \mathfrak{p}\} = \mathfrak{p}$ by definition of prime ideal. □

Let's recall the definition of zerodivisors on M.

Definition 5.20. 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 $\mathcal{Z}(M)$.

Lemma 5.21. *If R is Noetherian, and M is an arbitrary R-module, then*

1) *For any nonzero $m \in M$, $\text{ann}_R(m)$ is contained in an associated prime of M.*
2) *$\text{Ass}(M) = \varnothing \iff M = 0$, and*
3) *$\bigcup_{\mathfrak{p} \in \text{Ass}(M)} \mathfrak{p} = \mathcal{Z}(M)$.*

Additionally, if R and M are $\mathbb{Z}$-graded and $M \neq 0$, M has an associated prime that is homogeneous.

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

First, suppose that we have shown 1. If $M \neq 0$, then M contains a nonzero element m, and $\text{ann}(m)$ is contained in an associated prime of M. In particular, $\text{Ass}(M) \neq 0$, and 2 holds. Now if $r \in \mathcal{Z}(M)$, then by definition we have $r \in \text{ann}(m)$ for some nonzero $m \in M$. Since $\text{ann}(m)$ 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 $S := \{\text{ann}_R(m) \mid m \in M, m \neq 0\}$ 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 $I = \text{ann}(m)$ be any maximal element, and let $rs \in I$, $s \notin I$. We always have $\text{ann}(sm) \supseteq \text{ann}(m)$, and equality holds by the maximality of $\text{ann}(m)$ in S. Then $r(sm) = (rs)m = 0$, so $r \in \text{ann}(sm) = \text{ann}(m) = I$. We conclude that I is prime, and therefore it is an associated prime of M.

For the graded case, replace the set of zerovisisors with the annihilators of homogeneous elements. Such annihilator is homogeneous, since if m is homogeneous, and $fm = 0$, writing $f = f_{a_1} + \cdots + f_{a_b}$ as a sum of homogeneous elements of different

degrees a_i, then $0 = fm = f_{a_1}m + \cdots + f_{a_b}m$ is a sum of homogeneous elements of different degrees, so $f_{a_i}m = 0$ for each i. The same argument above works if we take $\{\text{ann}_R(m) \mid m \in M, m \neq 0 \text{ homogeneous }\}$, using the following lemma. □

Lemma 5.22. *If R is $\mathbb{Z}$-graded, an ideal with the property*

$$\textit{for any homogeneous elements } r, s \in R \quad rs \in I \Rightarrow r \in I \textit{ or } s \in I$$

is prime.

Proof. We need to show that this property implies that for any $a, b \in R$ not necessarily homogeneous, $ab \in I$ implies $a \in I$ or $b \in I$. We induce on the number of nonzero homogeneous components of a plus the number of nonzero homogeneous components of b. The base case is when this is two, which means that both a and b are homogeneous, and thus the hypotheses already gives us this case. Otherwise, write $a = a' + a_m$ and $b = b' + b_n$, where a_m, b_n are the nonzero homogeneous components of a and b of largest degree, respectively. We have $ab = (a'b' + a_m b' + b_n a') + a_m b_n$, where $a_m b_n$ is either the largest homogeneous component of ab or else it is zero. Either way, $a_m b_n \in I$, so $a_m \in I$ or $b_n \in I$; without loss of generality, we can assume $a_m \in I$. Then $ab = a'b + a_m b$, and $ab, a_m b \in I$, so $a'b \in I$, and the total number of homogeneous pieces of $a'b$ is smaller, so by induction, either $a' \in I$ so that $a \in I$, or else $b \in I$. □

Lemma 5.23. *If*

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

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

Proof. If $R/\mathfrak{p}$ includes in L, then composition with the inclusion $L \hookrightarrow M$ gives an inclusion $R/\mathfrak{p} \hookrightarrow M$. So $\text{Ass}(L) \subseteq \text{Ass}(M)$. Let $\mathfrak{p} \in \text{Ass}(M)$, say $\mathfrak{p} = \text{ann}(m)$. First, note that $\mathfrak{p} \subseteq \text{ann}(rm)$ 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 $\mathfrak{p} = \text{ann}(rm)$, and thus $\mathfrak{p} \in \text{Ass}(L)$.

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 $\mathfrak{p} = \text{ann}(m) \subseteq \text{ann}(n)$, we conclude that $\mathfrak{p} = \text{ann}(n)$. Therefore, $\mathfrak{p} \in \text{Ass}(N)$. □

Note that the inclusions in Lemma 5.23 are not necessarily equalities.

Example 5.24. If M is a module with at least two associated primes, and $\mathfrak{p}$ is an associated prime of M, then

$$0 \longrightarrow R/\mathfrak{p} \longrightarrow M$$

is exact, but $\{\mathfrak{p}\} = \text{Ass}(R/\mathfrak{p}) \subsetneq \text{Ass}(M)$.

Example 5.25. 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:

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

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

Corollary 5.26. *Let A and B be R-modules. Then* $\operatorname{Ass}(A \oplus B) = \operatorname{Ass}(A) \cup \operatorname{Ass}(B)$.

Proof. Apply Lemma 5.23 to the short exact sequence

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

We obtain $\operatorname{Ass}(A) \subseteq \operatorname{Ass}(A \oplus B) \subseteq \operatorname{Ass}(A) \cup \operatorname{Ass}(B)$. Repeat with

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

We will need a bit of notation for graded modules to help with the next statement; we saw a simple use of this notation back in Example 2.13.

Definition 5.27. Let R and M be T-graded, and $t \in T$. The **shift** of M by t is the graded R-module $M(t)$ with graded pieces $M(t)_i := M_{t+i}$. This is isomorphic to M as an R-module, when we forget about the graded structure.

Theorem 5.28. *Let R be a Noetherian ring, and M is a finitely generated module. There exists a* **filtration** *of M*

$$M = M_t \supsetneq M_{t-1} \supsetneq M_{t-2} \supsetneq \cdots \supsetneq M_1 \supsetneq M_0 = 0$$

such that $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ for primes $\mathfrak{p}_i \in \operatorname{Spec}(R)$. Such a filtration is called a **prime filtration** *of M.*

If R and M are $\mathbb{Z}$-graded, there exists a prime filtration as above where the quotients $M_i/M_{i-1} \cong (R/\mathfrak{p}_i)(t_i)$ are graded modules, the $\mathfrak{p}_i$ are homogeneous primes, and the t_i are integers.

Proof. If $M \neq 0$, then M has at least one associated prime, so there is an inclusion $R/\mathfrak{p}_1 \hookrightarrow M$. Let M_1 be the image of this inclusion. If $M/M_1 \neq 0$, it has an associated prime, so there is an $M_2 \subseteq M$ such that $R/\mathfrak{p}_2 \cong M_2/M_1 \subseteq R/M_1$. Continuing this process, we get a strictly ascending chain of submodules of M where the successive quotients are of the form $R/\mathfrak{p}_i$. If we do not have $M_t = M$ for some t, then we get an infinite strictly ascending chain of submodules of M, which contradicts that M is a Noetherian module.

In the graded case, if $\mathfrak{p}_i$ is the annihilator of an element m_i of degree t_i, we have a degree-preserving map $(R/\mathfrak{p}_i)(t_i) \cong Rm_i$ sending the class of 1 to m_i. $\square$

Prime filtrations often allow us to reduce statements about finitely generated modules to statements about quotients of R that are also domains: modules of the form $R/\mathfrak{p}$ for primes $\mathfrak{p}$.

Corollary 5.29. *If R is a Noetherian ring, and M is a finitely generated module, and*

$$M = M_t \supsetneq M_{t-1} \supsetneq M_{t-2} \supsetneq \cdots \supsetneq M_1 \supsetneq M_0 = 0$$

is a prime filtration of M with $M_i/M_{i-1} \cong R/\mathfrak{p}_i$, then

$$\operatorname{Ass}_R(M) \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}.$$

Therefore,

- *$\operatorname{Ass}_R(M)$ is finite.*
- *If M is graded, then $\operatorname{Ass}_R(M)$ is a finite set of homogeneous primes.*

Proof. For each i, we have a short exact sequence

$$0 \longrightarrow M_{i-1} \longrightarrow M_i \longrightarrow M_i/M_{i-1} \longrightarrow 0\,.$$

By Lemma 5.23, $\operatorname{Ass}(M_i) \subseteq \operatorname{Ass}(M_{i-1}) \cup \operatorname{Ass}(M_i/M_{i-1}) = \operatorname{Ass}(M_{i-1}) \cup \{\mathfrak{p}_i\}$. Inductively, we have $\operatorname{Ass}(M_i) \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_i\}$, and $\operatorname{Ass}_R(M) = \operatorname{Ass}_R(M_t) \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$. This immediately implies that $\operatorname{Ass}(M)$ is finite. In the graded case, Theorem 5.28 gives us a filtration where all the $\mathfrak{p}_i$ are homogeneous primes, and those include all the associated primes. □

Example 5.30. Any subset $X \subseteq \operatorname{Spec}(R)$ (for any R) can be realized as $\operatorname{Ass}(M)$ for some M: take $M = \bigoplus_{\mathfrak{p} \in X} R/\mathfrak{p}$. However, M is not finitely generated when X is infinite.

Example 5.31. If R is not Noetherian, then there may be modules (or ideals even) with no associated primes. Let $R = \bigcup_{n \in \mathbb{N}} \mathbb{C}[\![x^{1/n}]\!]$ be the ring of nonnegatively-valued Puiseux series. We claim that $R/(x)$ is a cyclic module with no associated primes, i.e., the ideal (x) has no associated primes. First, observe that any element of R can be written as a unit times $x^{m/n}$ for some m, n, so any associated prime of $R/(x)$ must be the annihilator of $x^{m/n} + (x)$ for some $m \leqslant n$. Hpwever, we claim that these are never prime. Indeed, we have $\operatorname{ann}(x^{m/n} + (x)) = (x^{1-m/n})$, which is not prime since $(x^{1/2-m/2n})^2 \in (x^{1-m/n})$ but $x^{1/2-m/2n} \notin (x^{1-m/n})$.

In a Noetherian ring, associated primes localize.

Theorem 5.32 (Associated primes localize in Noetherian rings)**.** *Let R be a Noetherian ring, W a multiplicative set, and M a module. Then*

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

Proof. Given $\mathfrak{p} \in \operatorname{Ass}_R(M)$ such that $\mathfrak{p} \cap W = \varnothing$, $W^{-1}\mathfrak{p}$ is a prime in $W^{-1}R$. Then $W^{-1}R/W^{-1}\mathfrak{p} \cong W^{-1}(R/\mathfrak{p}) \hookrightarrow W^{-1}M$ by exactness, so $W^{-1}\mathfrak{p}$ is an associated prime of $W^{-1}M$.

Suppose that $Q \in \operatorname{Spec}(W^{-1}R)$ is associated to $W^{-1}M$. We know this is of the form $W^{-1}\mathfrak{p}$ for some prime $\mathfrak{p}$ in R such that $\mathfrak{p} \cap W = \varnothing$. Since R is Noetherian, $\mathfrak{p}$ is finitely generated, say $\mathfrak{p} = (f_1, \ldots, f_n)$ in R, and so $Q = \left(\frac{f_1}{1}, \ldots, \frac{f_n}{1}\right)$.

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

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

Let $u = u_1 \cdots u_n \in W$. Then $u f_i r = 0$ for all i, and thus $\mathfrak{p} u r = 0$. We claim that in fact $\mathfrak{p} = \operatorname{ann}(ur)$ in R. Consider $v \in \operatorname{ann}(ur)$. Then $u(vr) = 0$, and since $u \in W$, this implies that $\frac{vr}{1} = 0$. Therefore, $\frac{v}{1} \in \operatorname{ann}(\frac{r}{1}) = W^{-1}\mathfrak{p}$, and $vw \in \mathfrak{p}$ for some $w \in W$. But $\mathfrak{p} \cap W = \varnothing$, and thus $v \in \mathfrak{p}$. Thus $\mathfrak{p} \in \operatorname{Ass}(M)$.

□

Corollary 5.33. *Let R be Noetherian, and M be an R-module.*

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

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

Proof.

a) Let $\mathfrak{p} \in \operatorname{Ass}_R(M)$ and let $\mathfrak{p} = \operatorname{ann}_R(m)$ for $m \in M$. Let $\mathfrak{q} \in V(\mathfrak{p})$, which in particular implies that $\mathfrak{q} \in \operatorname{Supp}(R/\mathfrak{p})$, by Proposition 5.9. Since $0 \to R/\mathfrak{p} \xrightarrow{m} M$ is exact, so is $0 \to (R/\mathfrak{p})_\mathfrak{q} \to M_\mathfrak{q}$. Since $(R/\mathfrak{p})_\mathfrak{q} \neq 0$, we must also have $M_\mathfrak{q} \neq 0$, and thus $\mathfrak{q} \in \operatorname{Supp}(M)$.

Suppose that $\mathfrak{q} \notin \bigcup_{\mathfrak{p} \in \operatorname{Ass}_R(M)} V(\mathfrak{p})$, so that $\mathfrak{q}$ does not contain any associated prime of M. Then there is no associated prime of M that does not intersect $R \setminus \mathfrak{q}$, so by Theorem 5.32, $\operatorname{Ass}_{R_\mathfrak{q}}(M_\mathfrak{q}) = \varnothing$. By Lemma 5.21, $M_\mathfrak{q} = 0$.

b) We have 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 5.34. 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.

5.3 Prime Avoidance

We take a quick detour to discuss an important lemma.

Lemma 5.35 (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.*

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 5.36. *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 $m \in M$.*

Proof. The assumption says that

$$I \subseteq \bigcup_{\mathfrak{p} \in \operatorname{Ass}(M)} (\mathfrak{p}).$$

By the assumptions, Corollary 5.29 applies, and it guarantees that this is a finite set of primes. By prime avoidance, $I \subseteq \mathfrak{p}$ for some $\mathfrak{p} \in \operatorname{Ass}(M)$. Equivalently, $I \subseteq \operatorname{ann}_R(m)$ for some nonzero $m \in M$. □

[1] So all the ideals are prime, except we may allow two of them to not be prime.

5.4 Primary decomposition

We refine our decomposition theory once again, and introduce primary decompositions of ideals. One of the fundamental classical results in commutative algebra is the fact that every ideal in any noetherian ring has a primary decomposition. This can be thought of as a generalization of the Fundamental Theorem of Arithmetic:

Theorem 5.37 (Fundamental Theorem of Arithmetic)**.** *Every integer $n \in \mathbb{Z}$ can be written as a product of primes: there are distinct prime integers $p_1, \ldots, p_n$ and integers $a_1, \ldots, a_n \geqslant 1$ such that*

$$n = p_1^{a_1} \cdots p_n^{a_n}.$$

Moreover, such a a product is unique up to sign and the order of the factors.

We will soon discover that such a product *is* a primary decomposition, perhaps after some light rewriting. But before we get to the *what* and the *how* of primary decomposition, it is worth discussing the *why*. If we wanted to extend the Fundamental Theorem of Arithmetic to other rings, our first attempt might involve irreducible elements. Unfortunately, we don't have to go far to find rings where we *cannot* write elements as a unique product of irreducibles up to multiplying by a unit.

Example 5.38. 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. In fact, we cannot obtain 2 or 3 by multiplying $1 + \sqrt{-5}$ or $1 + \sqrt{-5}$ by a unit.

Instead of writing *elements* as products of irreducibles, we will write *ideals* in terms of *primary ideals*.

Definition 5.39. We say that an ideal is **primary** if

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

We say that an ideal is **$\mathfrak{p}$-primary**, where $\mathfrak{p}$ is prime, if I is primary and $\sqrt{I} = \mathfrak{p}$.

Remark 5.40. Note that a primary ideal has indeed a prime radical: if Q is primary, and $xy \in \sqrt{Q}$, then $x^n y^n \in Q$ for some n. If $y \notin \sqrt{Q}$, then we must have $x^n \in Q$, so $x \in \sqrt{Q}$. Thus, every primary ideal Q is $\sqrt{Q}$-primary.

Example 5.41.

a) Any prime ideal is also 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 a prime element. Indeed, if $a = f^n$, with f irreducible, then

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

Conversely, if a is not a prime power, then $a = gh$, for some g, h nonunits with no common factor, then take $gh \in (a)$ but $g \notin a$ and $h \notin \sqrt{(a)}$.

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 is not in I.

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

Example 5.42. In $R = k[x, y, z]$, the ideal $\mathfrak{q} = (x^2, xy)$ is not primary, even though $\sqrt{\mathfrak{q}} = (x)$ is prime. The offending product is xy.

The definition of primary can be reinterpreted in many forms.

Proposition 5.43. *If R is Noetherian, the following are equivalent :*

(1) $\mathfrak{q}$ *is primary.*

(2) Every zerodivisor in $R/\mathfrak{q}$ *is nilpotent on* $R/\mathfrak{q}$.

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

(4) $\mathfrak{q}$ *has exactly one minimal prime, and no embedded primes.*

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

(6) $\sqrt{\mathfrak{q}} = \mathfrak{p}$ *is prime, and* $\mathfrak{q}R_{\mathfrak{p}} \cap R = \mathfrak{q}$.

Proof. (1) $\iff$ (2): y is a zerodivisor mod $\mathfrak{q}$ if there is some $x \notin \mathfrak{q}$ with $xy \in \mathfrak{q}$; the primary assumption translates to a power of y is in $\mathfrak{q}$.

(2) $\iff$ (3): On the one hand, (2) says that the set of zerodivisors on $R/\mathfrak{q}$ and coincide with the elements in the nilradical of $R/\mathfrak{q}$. By Lemma 5.21 and Exercise 16, respectively, these agree with the union of all the associated primes and the intersection of all the minimal primes.

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

This holds 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): We secretly already know this from the discussion on behavior of ideals in localizations, in Proposition 4.27, which says that

$$\mathfrak{q}R_{\mathfrak{p}} \cap R = \{r \in R \mid rs \in \mathfrak{q} \text{ for some } s \notin \mathfrak{p}\}.$$

□

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

Remark 5.44. 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 5.42. Moreover, even the powers of a prime ideal may fail to be primary.

Example 5.45. 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 $y \notin P$. On the one hand, $xy = z^n \in P^n$, 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.

The contraction of primary ideals is always primary.

Remark 5.46. Given any ring map $R \xrightarrow{f} S$, and a primary ideal Q in S, then the contraction of Q in R (via f) $Q \cap R$ is always primary. Indeed, if $xy \in Q \cap R$, and $x \notin Q \cap R$, then $f(x) \notin Q$, so $f(y^n) = f(y)^n \in Q$ for some n. Therefore, $y^n \in Q \cap R$, and $Q \cap R$ is indeed primary.

Lemma 5.47. *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 $\mathfrak{p}$-primary ideals is $\mathfrak{p}$-primary.

Proof. There is an inclusion $R/(I_1 \cap I_2) \subseteq R/I_1 \oplus R/I_2$. Hence, by Lemma 5.23, $\operatorname{Ass}(R/(I_1 \cap I_2)) \subseteq \operatorname{Ass}(R/I_1) \cup \operatorname{Ass}(R/I_2)$; the statement for larger t is an easy induction.

If the I_j are all $\mathfrak{p}$-primary, then

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

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 non-empty, and therefore the singleton $\{\mathfrak{p}\}$. Then $\bigcap_{j=1}^{t} I_j$ is $\mathfrak{p}$-primary by the characterization of primary in Proposition 5.43 (3) above. □

Definition 5.48 (Primary decomposition)**.** A **primary decomposition** of an ideal I is an expression of the form

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t,$$

with each $\mathfrak{q}_i$ primary. A **minimal primary decomposition** of an ideal I is a primary decomposition as above in which $\sqrt{\mathfrak{q}_i} \neq \sqrt{\mathfrak{q}_j}$ for $i \neq j$, and $\mathfrak{q}_i \not\supseteq \bigcap_{j \neq i} \mathfrak{q}_j$ for all i.[2]

[2]Some authors use the term *irredundant* instead of minimal.

Remark 5.49. By the previous lemma, we can turn any primary decomposition into a minimal one by combining the terms with the same radical, then removing redundant terms.

Example 5.50 (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 5.45 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 (which weren't called that yet at the time) by Emmy Noether in 1921 [Noe21].

Theorem 5.51 (Existence of primary decompositions)**.** *If R is Noetherian, then every ideal of R admits 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 $\mathfrak{q}$ is not primary, and take $xy \in \mathfrak{q}$ with $x \notin \mathfrak{q}$, $y \notin \sqrt{\mathfrak{q}}$. The ascending chain of ideals

$$(\mathfrak{q} : y) \subseteq (\mathfrak{q} : y^2) \subseteq (\mathfrak{q} : y^3) \subseteq \cdots$$

stabilizes for some n, since R is Noetherian. This means that $y^{n+1} f \in \mathfrak{q} \implies y^n f \in \mathfrak{q}$. We will show that

$$(\mathfrak{q} + (y^n)) \cap (\mathfrak{q} + (x)) = \mathfrak{q},$$

proving that $\mathfrak{q}$ is not irreducible.

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

$$a \in (\mathfrak{q} + (y^n)) \cap (\mathfrak{q} + (x)),$$

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

$$a \in \mathfrak{q} + (x) \implies ay \in \mathfrak{q} + (xy) = \mathfrak{q}.$$

So

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

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

Primary decompositions, even minimal ones, are not unique.

Example 5.52. Let $R = k[x, y]$, where k is a field, and $I = (x^2, xy)$. We can write

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

These are two different minimal primary decompositions of I. To check this, we just need to see that each of the ideals (x^2, xy, y^2) and (x^2, y) are primary. Observe that each has radical $\mathfrak{m} = (x, y)$, which is maximal, so by an earlier remark, these ideals are both primary. In fact, our ideal I has infinitely many minimal primary decompositions: given any $n \geqslant 1$,

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

is a minimal primary decomposition. One thing all of these have in common is the radicals of the primary components: they are always (x) and (x, y).

In the previous example, the fact that all our minimal 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 5.53 (First uniqueness theorem for primary decompositions)**.** *Suppose I is an ideal in a Noetherian ring R. Given any minimal primary decomposition of I, say*

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t,$$

we have

$$\{\sqrt{\mathfrak{q}_1}, \ldots, \sqrt{\mathfrak{q}_t}\} = \operatorname{Ass}(R/I).$$

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

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

$$\operatorname{Ass}(R/I) \subseteq \bigcup_i \operatorname{Ass}(R/\mathfrak{q}_i) = \{\sqrt{\mathfrak{q}_1}, \ldots, \sqrt{\mathfrak{q}_t}\}$$

from the lemma on intersections we proved, Lemma 5.47. We just need to show that in a minimal decomposition as above, every $\mathfrak{p}_j := \sqrt{\mathfrak{q}_j}$ is an associated prime.

So fix j, and let

$$I_j = \bigcap_{i \neq j} \mathfrak{q}_i \supseteq I.$$

Since the decomposition is minimal, the module I_j/I is nonzero, hence by Lemma 5.21 it has an associated prime $\mathfrak{a}$. Let $\mathfrak{a}$ be such an associated prime, and fix $x_j \in R$ such that $\mathfrak{a}$ is the annihilator of $\overline{x_j}$ in I_j/I. Since

$$\mathfrak{q}_j x_j \subseteq \mathfrak{q}_j \cdot \bigcap_{i \neq j} \mathfrak{q}_i \subseteq \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n = I,$$

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

We note that if we don't 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 minimal 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 a minimal decomposition.

Theorem 5.54 (Second uniqueness theorem for primary decompositions)**.** *If I is an ideal in a Noetherian ring R, then for any minimal primary decomposition of I, say $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$, the set of* minimal components $\{\mathfrak{q}_i \mid \sqrt{\mathfrak{q}_i} \in \operatorname{Min}(R/I)\}$ *is the same. Namely, $\mathfrak{q}_i = IR_{\sqrt{\mathfrak{q}_i}} \cap R$.*

Proof. We observe that a localization $\mathfrak{q}_{\mathbb{A}}$ of a $\mathfrak{p}$-primary ideal $\mathfrak{q}$ at a prime $\mathbb{A}$ is either the unit ideal (if $\mathfrak{p} \not\subseteq \mathbb{A}$), or a $\mathfrak{p}_{\mathbb{A}}$-primary ideal; this follows from the fact that the associated primes of $R/\mathfrak{q}$ localize, Theorem 5.32.

Now, since finite intersections commute with localization, then for any prime $\mathbb{A}$,

$$I_{\mathbb{A}} = (\mathfrak{q}_1)_{\mathbb{A}} \cap \cdots \cap (\mathfrak{q}_t)_{\mathbb{A}}$$

is a primary decomposition, although not necessarily minimal. In a minimal decomposition, choose a minimal prime $\mathbb{A} = \mathfrak{p}_i$. Then when we localize at $\mathbb{A}$, all the other components become the unit ideal since their radicals are not contained in $\mathfrak{p}_i$, and thus $I_{\mathfrak{p}_i} = (\mathfrak{q}_i)_{\mathfrak{p}_i}$t. We can then contract to R to get $I_{\mathfrak{p}_i} \cap R = (\mathfrak{q}_i)_{\mathfrak{p}_i} \cap R = \mathfrak{q}_i$, since $\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary. □

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

Example 5.55. If R is Noetherian, and I is a radical ideal, then we have seen that I coincides with the intersection of its minimal primes $\mathfrak{p}_i$, meaning $I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_t$. 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 $(xy, xz, yz) = (x, y) \cap (x, z) \cap (y, z)$. More generally, the radical monomial ideals are precisely those that are squarefree, and the primary components of a monomial ideal are also monomial.

Example 5.56. 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

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

So $(6) = (2) \cap (3)$, 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):

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

In fact, all of these come components are minimal, and so this primary decomposition is unique. Primary decomposition saves the day!

Finally, we note that the primary decompositions of powers of ideals are especially interesting.

Definition 5.57 (Symbolic power)**.** If $\mathfrak{p}$ is a prime ideal in a ring R, the n**th symbolic power** of $\mathfrak{p}$ is $\mathfrak{p}^{(n)} := \mathfrak{p}^n R_{\mathfrak{p}} \cap R$.

This admits equivalent characterizations.

Proposition 5.58. *Let R be Noetherian, and $\mathfrak{p}$ a prime ideal of R.*

a) $\mathfrak{p}^{(n)} = \{r \in R \mid rs \in \mathfrak{p}^n \text{ for some } s \notin \mathfrak{p}\}$.

b) $\mathfrak{p}^{(n)}$ *is the unique smallest* $\mathfrak{p}$*-primary ideal containing* $\mathfrak{p}^n$.

c) $\mathfrak{p}^{(n)}$ *is the* $\mathfrak{p}$*-primary component in any minimal primary decomposition of* $\mathfrak{p}^n$.

Proof. The first characterization follows from the definition, and the fact that expanding and contraction to/from a localization is equivalent to saturating with respect to the multiplicative set, which we proved in Proposition 4.27.

We know that $\mathfrak{p}^{(n)}$ is $\mathfrak{p}$-primary from one of the characterizations of primary we gave in Proposition 5.43. Any $\mathfrak{p}$-primary ideal satisfies $\mathfrak{q}R_{\mathfrak{p}} \cap R = \mathfrak{q}$, and if $\mathfrak{q} \supseteq \mathfrak{p}^n$, then $\mathfrak{p}^{(n)} = \mathfrak{p}^n R_{\mathfrak{p}} \cap R \subseteq \mathfrak{q}R_{\mathfrak{p}} \cap R = \mathfrak{q}$. Thus, $\mathfrak{p}^{(n)}$ is the unique smallest $\mathfrak{p}$-primary ideal containing $\mathfrak{p}^n$.

The last characterization follows from the second uniqueness theorem, Theorem 5.54. □

In particular, note that $\mathfrak{p}^n = \mathfrak{p}^{(n)}$ if and only if $\mathfrak{p}^n$ is primary.

Example 5.59.

a) In $R = k[x, y, z]$, the prime $\mathfrak{p} = (y, z)$ satisfies $\mathfrak{p}^{(n)} = \mathfrak{p}^n$ for all n. This follows along the same lines as Example 5.41 d.

b) In $R = k[x, y, z] = (xy - z^n)$, where $n \geqslant 2$, we have seen in Example 5.45 that the square of $\mathfrak{p} = (y, z)$ is not primary, and therefore $\mathfrak{p}^{(2)} \neq \mathfrak{p}^2$. Indeed, $xy = z^n \in \mathfrak{p}^2$, and $x \notin \mathfrak{p}$, so $y \in \mathfrak{p}^{(2)}$ but $y \notin \mathfrak{p}^2$.

c) Let $X = X_{3\times 3}$ be a 3×3 matrix of indeterminates, and $k[X]$ be a polynomial ring over a field k. Let $\mathfrak{p} = I_2(X)$ be the ideal generated by 2×2 minors of X. Write $\Delta_{\substack{i|k\\ j|l}}$ for the determinant of the submatrix with rows i, j and columns k, l. We find

$$\begin{aligned} x_{11}\det(X) &= x_{11}x_{31}\Delta_{\substack{1|2\\2|3}} - x_{11}x_{32}\Delta_{\substack{1|1\\2|3}} + x_{11}x_{33}\Delta_{\substack{1|1\\2|2}} \\ &= (x_{11}x_{31}\Delta_{\substack{1|2\\2|3}} - x_{11}x_{32}\Delta_{\substack{1|1\\2|3}} + x_{11}x_{33}\Delta_{\substack{1|1\\2|2}}) \\ &\quad - (x_{11}x_{31}\Delta_{\substack{1|2\\2|3}} - x_{12}x_{31}\Delta_{\substack{1|1\\2|3}} + x_{13}x_{31}\Delta_{\substack{1|1\\2|2}}) \\ &= -\Delta_{\substack{1|1\\3|2}}\Delta_{\substack{1|1\\2|3}} + \Delta_{\substack{1|1\\3|3}}\Delta_{\substack{1|1\\2|2}} \in I_2(X)^2. \end{aligned}$$

Note that in the second row, we subtracted the Laplace expansion of the determinant of the matrix with row 3 replaced by another copy of row 1. That is, we subtracted zero.

While we will not discuss symbolic powers in detail, they are ubiquitous in commutative algebra. They show up as tools to prove various important theorems of different flavors, and they are also interesting objects in their own right. In particular, symbolic powers can be interpreted from a geometric perspective, via the Zariski–Nagata Theorem [Zar49, NM91]. Roughly, this theorem says that when we consider symbolic powers of prime ideals over $\mathbb{C}[x_1, \ldots, x_d]$, the polynomials in $\mathfrak{p}^{(n)}$ are precisely the polynomials that vanish *to order* n on the variety corresponding to $\mathfrak{p}$. This result can be made sense of more generally, for any radical ideal in $\mathbb{C}[x_1, \ldots, x_d]$ over any perfect field k [EH79, FMS14], and even when $k = \mathbb{Z}$ [DSGJ].

5.5 The Krull Intersection Theorem

Lemma 5.60. *Let R be a ring. If $I \subseteq J$ are ideals, $J \subseteq \sqrt{I}$, and J is finitely generated, then there is some n with $J^n \subseteq I$. Therefore, if R is Noetherian, for every ideal I, there is some n with $\sqrt{I}^n \subseteq I$.*

Proof. Write $J = (f_1, \ldots, f_m)$. By definition, each $f_i^{a_i} \in I$ for some $a_1, \ldots, a_m$. Let $n := a_1 + \cdots + a_m + 1$. Now J^n is generated by products of the form $f_1^{b_1} \cdots f_m^{b_m}$ with $b_1 + \cdots + b_m = n$. By the Pigeonhole Principle, at least one b_i satisfies $b_i \geqslant a_i$, so $f_1^{b_1} \cdots f_m^{b_m} \in I$.

The second statement is a consequence of the first, since $\sqrt{I}$ is a finitely generated ideal with $\sqrt{I} \supseteq I$. □

Theorem 5.61 (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 Lemma 5.60. 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 4.30. □

Remark 5.62. As an easy corollary, we obtain that

$$\bigcap_{n\geqslant 1} I^n = 0$$

for any proper ideal I in a Noetherian local ring $(R, \mathfrak{m})$, since $I^n \subseteq \mathfrak{m}^n$ for all n.

In the non-local setting, it is not true in general that $\bigcap_{n\geqslant 1} I^n = 0$.

Exercise 17. Let k be a field and let $R = k \times k$ be the product of k with itself. Show that the ideal $I = \{(a, 0) \mid a \in k\}$ is **idempotent**, meaning $I^2 = I$, and thus $\bigcap_{n\geqslant 1} I^n = I \neq 0$.

But it is true if R is a domain.

Theorem 5.63 (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. Exercise. □

Chapter 6

Dimension theory

6.1 Dimension and height

Definition 6.1. A **chain of primes** of **length** n in a ring R is a chain

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n \quad \text{with } \mathfrak{p}_i \in \operatorname{Spec}(R).$$

We say a chain of primes is **saturated** if for each i, there is no $\mathfrak{q} \in \operatorname{Spec}(R)$ with $\mathfrak{p}_i \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}_{i+1}$. The **dimension** or **Krull dimension** of a ring R is the supremum of the lengths of chains of primes in R. Equivalently, it is the supremum of the lengths of saturated chains of primes in R. We denote the Krull dimension of R 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. Equivalently, it is the supremum of the lengths of saturated chains of primes in R that end in $\mathfrak{p}$. We denote the height of $\mathfrak{p}$ by $\operatorname{ht}(\mathfrak{p})$. The **height** of an ideal I is the infimum of the heights of the minimal primes of I:

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

To get a feel for these definitions, here are some easy observations.

Remark 6.2.

a) If $\mathfrak{p}$ is prime, then $\dim(R/\mathfrak{p})$ is the supremum of the lengths of (saturated) chains of primes in R

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

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

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

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

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

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

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

e) 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 (saturated) chains of primes in R

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

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

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

h) If $\mathfrak{p}$ is prime, $\dim(R/\mathfrak{p}) + \mathrm{height}(\mathfrak{p}) \leqslant \dim(R)$.

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

j) The ideal (0) has height 0.

k) A prime has height zero if and only if it is a minimal prime.

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 6.3.

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. Likewise, a principal ideal domain has dimension 1.

d) In a UFD, I is a prime of height 1 if and only if $I = (f)$ for a prime element f. 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 $(0) \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \cdots \subsetneq (x_1, \ldots, x_d)$.

We pose a related definition for modules.

Definition 6.4. 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 $\mathrm{Supp}_R(M)$.

Definition 6.5. 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, or equivalently $\dim(R/P)$ is the same finite number for every minimal prime P.

Here are some examples of what can go wrong.

Example 6.6. Consider the ring

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

We can find the minimal primes of R by computing $\operatorname{Min}((xy,xz))$ in $k[x,y,z]$: (x) and (y,z) are prime, and $(x) \cap (y,z) = (xy,xz)$. Therefore, $\operatorname{Min}(R) = \{(x),(y,z)\}$. Now, the height of $(x-1,y,z)$ 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.

Even domains may fail to be equidimensional.

Example 6.7. 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

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

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

Remark 6.8.

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 $\mathfrak{p} \in \operatorname{Min}(R)$.

Before we get too optimistic, know that there are Noetherian rings of infinite dimension, as the following example due to Nagata [Nag62, Appendix, Example 1] shows.

Example 6.9. The ring $R = k[x_1, x_2, \dots]$ is infinite-dimensional. Let

$$W = R \setminus ((x_1) \cup (x_2, x_3) \cup (x_4, x_5, x_6) \cdots)$$

and $S = W^{-1}R$. This ring has primes of arbitrarily large height, given by the images of those primes we cut out from W. Thus, it has infinite dimension. The work is to show that this ring is Noetherian. We omit this argument here.

Note also that a ring might have finite dimension but not be Noetherian.

Example 6.10. Let $R = k[x_1, x_2, \dots]/(x_1^2, x_2^2, \dots)$. On the one hand, R is not Noetherian, since

$$(x_1) \subseteq (x_1, x_2) \subseteq (x_1, x_2, x_3) \subseteq \cdots$$

is an infinite ascending chain of ideals. On the other hand, R has only one prime ideal, and thus $\dim(R) = 0$.

6.2 Artinian rings

To prepare for our next big theorems in dimension theory, we need to understand the structure of zero-dimensional Noetherian rings. In order to do that, we will take a theorem on primary decomposition for certain ideals in not necessarily Noetherian rings.

Theorem 6.11. *Let R be a ring, not necessarily Noetherian. Let I be an ideal such that $V(I) = \{\mathfrak{m}_1, \dots, \mathfrak{m}_t\}$ is a finite set of maximal ideals. There is a primary decomposition $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$, and moreover $I = \mathfrak{q}_1 \cdots \mathfrak{q}_t$ and $R/I \cong R/\mathfrak{q}_1 \times \cdots \times R/\mathfrak{q}_t$.*

Proof. First, we claim that $IR_{\mathfrak{m}_i}$ is $\mathfrak{m}_i R_{\mathfrak{m}_i}$-primary. The local ring $(R/I)_{\mathfrak{m}_i} = R_{\mathfrak{m}_i}/IR_{\mathfrak{m}_i}$ has a unique maximal ideal $\mathfrak{m}_i R_{\mathfrak{m}_i}/IR_{\mathfrak{m}_i}$, so if $x, y \in R_{\mathfrak{m}_i}$ are such that $xy \in IR_{\mathfrak{m}_i}$, and $x \notin \mathfrak{m}_i R_{\mathfrak{m}_i}$, then x is a unit modulo $I_{\mathfrak{m}_i}$, so $y \in IR_{\mathfrak{m}_i}$. Now the contraction of a primary ideal is primary, by Remark 5.46, so $\mathfrak{q}_i = IR_{\mathfrak{m}_i} \cap R$ is $\mathfrak{m}_i$-primary, and $I \subseteq \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$.

On the other hand, equality of these modules is a local property, so let's check it at each prime. When $\mathfrak{p} \notin V(I)$, then both I and $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$ are the unit ideal in $R_{\mathfrak{p}}$. On the other hand, for each $\mathfrak{m}_i \in V(I)$, $I_{\mathfrak{m}_i} = (\mathfrak{q}_i)_{\mathfrak{m}_i}$ in $R_{\mathfrak{m}_i}$. Therefore, $I = \mathfrak{q}_1 \cdots \mathfrak{q}_t$, and this is a primary decomposition, since each $\mathfrak{q}_i$ is $\mathfrak{m}_i$-primary.

Now notice that $\mathfrak{q}_i + \mathfrak{q}_j = R$ for each pair $\mathfrak{q}_i \neq \mathfrak{q}_j$, so Theorem 0.8 applies. Therefore, we obtain the fact that our intersection is a product and the quotient ring is a direct product as a consequence of Theorem 0.8. □

Definition 6.12. A module $M \neq 0$ is **simple** if its only submodules are (0) and M.

Remark 6.13. If $\mathfrak{m}$ is a maximal ideal in R, then $R/\mathfrak{m}$ is a simple R-module. On the other hand, if M is any cyclic R-module, then given any nonzero element $m \in M$, Rm is a nonzero submodule of M, and thus it must be all of M. Therefore, any simple module must be cyclic. If I is a proper ideal contained in some maximal ideal $\mathfrak{m} \supsetneq I$, then $\mathfrak{m}/I$ is a proper nonzero submodule of R/I. Therefore, the simple modules of any ring R are precisely those that are isomorphic to $R/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$.

In particular, if R is a local, then R has only one simple module up to isomorphism: the residue field.

Definition 6.14. A module M has **finite length** if it has a filtration of the form

$$0 = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n = M$$

with M_{i+1}/M_i simple for each i; such a filtration is called a **composition series** of **length** n. We say a composition series is **strict** if $M_i \neq M_{i+1}$ for all i. Two composition series are **equivalent** if the collections of composition factors M_{i+1}/M_i are the same up to reordering. The **length** of a finite length module M, denoted $\ell(M)$, is the minimum of the lengths of a composition series of M. If M has does not have finite length, we say that M has infinite length, or $\ell(M) = \infty$.

You may have seen the Jordan–Holder theorem in the context of groups:

Theorem 6.15 (Jordan–Holder theorem)**.** *Let M be a module of finite length.*

1) Any proper submodule N of M has $\ell(N) < \ell(M)$.

2) Any filtration of M can be refined to a composition series.

3) All strict composition series for M are equivalent, and hence have the same length.

Proof. If $n := \ell(M)$, consider a strict composition series of M of length n, say

$$0 = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n = M.$$

1) Given a submodule N of M, consider the filtration

$$0 = M_0 \cap N \subseteq M_1 \cap N \subseteq M_2 \cap N \subseteq \cdots \subseteq M_n \cap N = N.$$

By the Second Isomorphism Theorem, its composition factors satisfy

$$(M_{i+1} \cap N)/(M_i \cap N) \cong (M_{i+1} \cap N + M_i)/M_i.$$

This is a submodule of M_{i+1}/M_i, which by assumption is simple. Then either

$$(M_{i+1} \cap N + M_i)/M_i = 0 \quad \text{or} \quad (M_{i+1} \cap N + M_i)/M_i = M_{i+1}/M_i.$$

The quotients that are zero correspond to terms that we can delete; the remaining ones are simple modules. The resulting filtration is a strict composition series for N, so this shows that $\ell(N) \leqslant n$. Moreover, if there are no zero coefficients to delete, then

$$(M_{i+1} \cap N + M_i)/M_i = M_{i+1}/M_i$$

for all i, and in particular when we take $i + 1 = n$ we obtain

$$N + M_{n-1} = M_n \cap N + M_{n-1} = M_n = M,$$

Since M/M_{n-1} is simple by assumption, we must have $N = M$. If N is a proper submodule, this cannot happen, and thus at least one of the terms can be deleted, so $\ell(N) < n$.

2) Let us use induction on n to show that any chain of submodules of M, say

$$N_0 \subsetneq N_1 \subseteq M_2 \subsetneq \cdots \subsetneq N_k,$$

has length at most n. If $n = 0$, then $M = 0$ and there is nothing to prove. Now assume that $n \geqslant 1$ and that the statement holds for modules of length $< n$. Since N_{k-1} must be a proper submodule of N, 1) tells us that $\ell(N_{k-1}) < n$, and thus $k - 1 \leqslant n - 1$. Therefore, $k \leqslant n$. This shows our claim that all chains of submodules of M have length at most n.

Now notice that if we are given a chain of submodules of length $< n$, then it cannot be a compositions series, since by definition the smallest composition series has length n. That means that some of the quotients are not simple, so we can extend the chain by adding a term, as follows: if N_{i+1}/N_i is not simple, and N'/N_i is a.proper nonzero submodule, then $N_i \subseteq N_{i+1}$ can be extended $N_i \subseteq N \subseteq N_{i+1}$. Therefore, every chain of submodules can be extended to a composition series.

3) Suppose that

$$0 = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_k = M$$

is a strict composition series of $M \neq 0$. Since $\ell(M)$ is the smallest possible length of a composition series, we have $\ell(M) \leqslant k$. Moreover, notice that for each $i \geqslant 1$, N_i is a proper submodule of N_{i+1}, and thus by 1) we have

$$\ell(M) > \ell(N_{k-1}) > \ell(N_{k-1}) > \cdots > \ell(N_1) > 0.$$

Therefore, $\ell(M) \geqslant k$, so we must have $\ell(M) = \ell(k)$. □

Let's collect some basic consequences of this theorem.

Lemma 6.16. *Length is associative on short exact sequences, that is, if*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

is a short exact sequence of R-modules, then $\ell(B) = \ell(A) + \ell(B)$.

Proof. Given filtrations of lengths a and c for A and C, respectively, we can construct a filtration for B of length $a + c$, so $\ell(B) \geqslant \ell(A) + \ell(C)$. On the other hand, if

$$0 = B_0 \subseteq B_1 \subseteq B_2 \subseteq \cdots \subseteq B_n = B$$

is a filtration for B, then $B_i \cap A$ and $g(B_i)$ are filtrations for A and C, respectively. Suppose that both $g(B_i) = g(B_{i+1}$ and $B_i \cap A = B_{i+1} \cap A$, and let $b \in B_{i+1}$. Then $g(b) \in g(B_i)$, so there is $b' \in B_i$ such that $b - b' \in \ker g = \operatorname{im} f$. Since b and b' are both in B_{i+1}, we conclude that $b - b' \in B_{i+1} \cap A = B_i \cap A$. But $b' \in B_i$, so we conclude that $b \in B_i$. Therefore, $B_i = B_{i+1}$. This shows that sum of the lengths of the filtrations $B_i \cap A$ and $g(B_i)$ is at most the length of the filtration B_i. We conclude that $\ell(B) \leqslant \ell(A) + \ell(C)$. □

Using an homological trick we haven't seen yet, one can actually show that if

$$0 \longrightarrow A_1 \longrightarrow \cdots \longrightarrow A_n \longrightarrow 0\ ,$$

is an exact sequence, then $\sum_{i=1}^{n} \ell(A_i) = 0$.

Remark 6.17.

a) Given a chain of submodules $0 = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n = M$,

$$\ell(M) = \sum_{i=0}^{n-1} \ell(M_{i+1}/M_i).$$

b) If $M \subseteq N$, then $\ell(M) \leqslant \ell(N)$, with equality only when $M = N$.

Remark 6.18. If M is annihilated by a maximal ideal $\mathfrak{m}$, so that M is an $R/\mathfrak{m}$-module, then $\ell(M) = \dim_{R/\mathfrak{m}}(M/\mathfrak{m}M)$.

Example 6.19. Let $R = \mathbb{R}[x, y]_{(x,y)}$. Then $M = R/\mathfrak{m}^2$ has length 3, since we have a composition series $0 \subseteq xM \subseteq (x, y)M \subseteq M$. However, M is not an $R/\mathfrak{m}$-vector space.

Back when we discussed Noetherian rings, we could have also considered the dual notion of Artinian rings. The reason we have waited so long to do so is that as we will soon show, Artinian rings are just Noetherian rings of dimension 0.

Definition 6.20. A ring is **Artinian** if every descending chain of ideals eventually stabilizes. A module is **Artinian** if every descending chain of submodules eventually stabilizes.

Adapting the proofs of the analogous statements for Noetherian rings and modules, one can easily show the following:

Exercise 18.

a) If R is an Artinian ring, then R/I is Artinian for any ideal I of R.

b) If R is an Artinian ring, then any nonempty family of ideals has a minimal element.

c) If M is an Artinian module, and $N \subseteq M$, then N and M/N are Artinian.

Lemma 6.21. *A module M has finite length if and only if it is both Noetherian and Artinian.*

Proof. If M has finite length, then all chains of submodules of M must have length at most $\ell(M)$, and thus in particular all ascending and descending chains of submodules must stabilize.

On the other hand, suppose that M is both Noetherian and Artinian. If $M = 0$, there is nothing to show, so we might as well assume $M \neq 0$. The set of proper submodules of M is then be nonempty, and thus it has a maximal element M_1 by Noetherianity. This forces M/M_1 to be simple, so we can start constructing a composition series for M by taking $M \supseteq M_1$. At each step, if we have constructed modules

$$M_0 = M \supseteq M_1 \supseteq M_2 \supseteq \cdots \supseteq M_k$$

such that M_i/M_{i+1} is simple, either $M_k = 0$ and we can stop, or $M_k \neq 0$ and it has a proper submodule. Repeating the initial construction for M_k, which is again Noetherian, we can continue to build a descending chain of submodules of M. But M is Artinian, and thus this process must eventually stop, since M is Artinian. □

Lemma 6.22. *Let R be a Noetherian ring. An R-module M has finite length if and only if M is finitely generated and* $\dim(M) = \dim(R/\operatorname{ann}(M)) = 0$.

Proof. Suppose M has finite length. Then M is Noetherian, by Lemma 6.21, and in particular finitely generated. Moreover, consider a composition series

$$0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_n = M$$

for M. For each $i \geqslant 1$, $M_i/M_{i-1} \cong R/\mathfrak{m}_i$ for some maximal ideal $\mathfrak{m}_i$. Also, our composition series breaks into short exact sequences

$$0 \longrightarrow M_i \longrightarrow M_{i+1} \longrightarrow M_{i+1}/M_i \longrightarrow 0\,.$$

When $i = 1$, $M_1 \cong M_1/M_0 \cong R/\mathfrak{m}_1$. Using Lemma 5.23 repeatedly, we conclude that $\operatorname{Ass}(M_i) \subseteq \{\mathfrak{m}_1, \ldots, \mathfrak{m}_i\}$ for each i, and in particular $\operatorname{Ass}(M) \subseteq \{\mathfrak{m}_1, \ldots, \mathfrak{m}_i\}$. So all the minimal primes over $\operatorname{ann}(M)$ are maximal, and $\dim(R/\operatorname{ann}(M)) = 0$.

Now suppose that M is finitely generated and $\dim(R/\operatorname{ann}(M)) = 0$. Since M is finitely generated over a Noetherian ring, by Theorem 5.28 there exists a filtration of M

$$M = M_t \supsetneq M_{t-1} \supsetneq M_{t-2} \supsetneq \cdots \supsetneq M_1 \supsetneq M_0 = 0$$

such that $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ for primes $\mathfrak{p}_i \in \operatorname{Spec}(R)$. For each i,

$$\operatorname{ann}(M)M_i = 0 \subseteq M_{i-1} \implies \operatorname{ann}(M) \subseteq (M_{i-1} :_R M_i) = \mathfrak{p}_i.$$

Since $\dim(R/\operatorname{ann}(M)) = 0$, all the primes containing $\operatorname{ann}(M)$ must be maximal, and thus the $\mathfrak{p}_i$ are all maximal ideals. So our prime filtration is a composition series, and M has finite length. □

Equivalently, an R-module M over a Noetherian ring has finite length if and only if it is finitely generated and all of its associated primes are maximal ideals of R.

Exercise 19. Let $(R, \mathfrak{m})$ be a Noetherian local ring. An R-module M has finite length if and only if M is finitely generated and $\mathfrak{m}^n M = 0$ for some n.

Example 6.23. Let $(R, \mathfrak{m})$ be a local ring. Then $M = (R/\mathfrak{m})^n$ is a finite length module for any $n \geqslant 1$. Note that $\ell(M) = \dim_{R/\mathfrak{m}}((R/m)^n) = n$, while $\mathfrak{m}M = 0$.

Finally, we can show that Artinian rings are just zero-dimensional Noetherian rings.

Theorem 6.24. *The following are equivalent:*

a) R is Noetherian of dimension zero.

b) R is a finite product of local Noetherian rings of dimension zero.

c) R has finite length as an R-module.

d) R is Artinian.

Proof. (1)⇒(2): Since R is Noetherian of dimension zero, every prime is maximal and minimal. Since there are finitely many minimal primes in R, by Theorem 5.5, there are finitely many primes in R. By Theorem 6.11, R decomposes as a direct product of Noetherian local rings, which all must have dimension zero.

(2)⇒(3): It suffices to deal with the case when $(R, \mathfrak{m})$ is a local Noetherian ring of dimension 0. In this case, the maximal ideal is the unique minimal prime, so $\mathfrak{m} = \sqrt{(0)}$. Since R is Noetherian, Lemma 5.60 yields $\mathfrak{m}^n = 0$ for some n. Then R has finite length by Exercise 19.

(3)⇒(4): This follows by Lemma 6.21, noting that R is an Artinian R-module if and only if R is an Artinian ring.

(4)⇒(1):

First we show that R has dimension zero. If $\mathfrak{p}$ is any prime, then $R/\mathfrak{p}$ is Artinian, since the ideals of $R/\mathfrak{p}$ are in bijection with the ideals of R containing $\mathfrak{p}$. Pick $a \in R/\mathfrak{p}$ some nonzero element. The ideals

$$(a) \supseteq (a^2) \supseteq (a^3) \supseteq \cdots$$

stabilize, so $a^n = a^{n+1}b$ for some b. Since $R/\mathfrak{p}$ is a domain, $ab = 1$ in A, so a is a unit. Thus, $R/\mathfrak{p}$ is a field, so every prime is maximal. In particular, $\dim(R) = 0$.

Second, note that there are only finitely many maximal ideals. Otherwise, of $\mathfrak{m}_i$ are distinct primes for all $i \geqslant 1$, consider the chain

$$\mathfrak{m}_1 \supseteq \mathfrak{m}_1 \cap \mathfrak{m}_2 \supseteq \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \mathfrak{m}_3 \supseteq \cdots .$$

This stabilizes, since R is Artinian, so $\mathfrak{m}_{n+1} \supseteq \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n \supseteq \mathfrak{m}_1 \cdots \mathfrak{m}_n$. Since $\mathfrak{m}_{n+1}$ is prime, $\mathfrak{m}_{n+1} \supseteq \mathfrak{m}_i$ for some $i \leqslant n$, and since $\mathfrak{m}_i$ is maximal, we conclude that $\mathfrak{m}_i = \mathfrak{m}_{n+1}$. This contradicts the hypothesis that the $\mathfrak{m}_i$ are all distinct maximal ideals, so we conclude that R has finitely many primes, all maximal. Now, we apply Theorem 6.11 to conclude that R is a finite direct product of local rings of dimension zero. Each of the factors is a quotient of R, and thus each is Artinian. It suffices to show that each factor is Noetherian. So our proof will be complete if we show that any Artinian local ring $(R, \mathfrak{m})$ with only one prime must be a Noetherian ring.

The chain $\mathfrak{m} \supseteq \mathfrak{m}^2 \supseteq \mathfrak{m}^3 \supseteq \cdots$ stabilizes, so that $\mathfrak{m}^n = \mathfrak{m}^{n+1}$. Notice that we cannot apply NAK yet, since we don't know $\mathfrak{m}^n$ is finitely generated. If $\mathfrak{m}^n \neq 0$, consider the family S of ideals $I \subseteq \mathfrak{m}$ such that $I\mathfrak{m}^n \neq 0$. This family contains $\mathfrak{m}$, so in particular it is nonempty, and thus it must have a minimal element since R is Artinian. Take J minimal in S. For some $x \in J$, $x\mathfrak{m}^n \neq 0$, and $(x) \subseteq J \subseteq \mathfrak{m}$, so $J = (x)$ is principal by minimality. Now, $((x)\mathfrak{m}) \cdot \mathfrak{m}^n = (x)\mathfrak{m}^{n+1} = (x)\mathfrak{m}^n \neq 0$, so $(x)\mathfrak{m} \subseteq (x)$ is in S, and by minimality, $(x) = \mathfrak{m}(x)$. Now we can apply NAK 4.30, so $(x) = (0)$, contradicting that $\mathfrak{m}^n \neq 0$. Therefore,

$$0 = \mathfrak{m}^n \subseteq \mathfrak{m}^{n-1} \subseteq \cdots \subseteq \mathfrak{m} \subseteq R.$$

In particular, R has finite length as an R-module, so R is a Noetherian R-module by Lemma 6.21. We conclude that R is also a Noetherian ring. □

Example 6.25. Some Artinian local rings include $k[x,y]/(x^2, y^2)$, $k[x,y]/(x^2, xy, y^2)$, and $\mathbb{Z}/(p^n)$.

Note that $\dim(R) = 0$ does not imply R Artinian unless R is also Noetherian.

Example 6.26. As we saw in Example 6.10, there are rings of dimension 0 that are not Noetherian, and thus also not Artinian. In Example 6.10 we considered the ring $k[x_1, x_2, \ldots]/(x_1^2, x_2^2, \ldots)$, which in fact has only one prime ideal. Note however that

$$(x_1, x_2, \ldots) \supseteq (x_2, x_3, \ldots) \supseteq (x_3, x_4, \ldots) \supseteq \cdots$$

is an infinite descending chain.

Even though every Artinian ring is Noetherian and has finite length, it is not true that Artinian modules are always Noetherian or of finite length.

Example 6.27. Let $R = \mathbb{C}[\![x]\!]$, and $M = R[1/x]/R$. Note that $R[1/x]$ is the ring of Laurent series, so M is the module of "tails" of these functions. This module does not have finite length; it is not even finitely generated! Observe that any submodule N of M either contains $1/x^n$ for all n, or else there is a largest n for which $1/x^n \in N$, and $N = R \cdot 1/x^n$ for this n. The module $R \cdot 1/x^n \subseteq M$ has length n, so it is Artinian, Then every proper submodule of M is Artinian, and thus M itself is Artinian.

Definition 6.28. If $(R, \mathfrak{m}, k)$ is local, a **coefficient field** for R is a subfield $K \subseteq R$ such that the map $K \to R \to R/\mathfrak{m} \cong k$ is an isomorphism.

Rings like $K[\underline{x}]_{(\underline{x})}/I$ have coefficient fields: the copy of K. Some rings without coefficient fields are $\mathbb{Z}_{(p)}$ and $\mathbb{R}[x]_{(x^2+1)}$. Other rings have lots of coefficient fields: $\mathbb{C}[x,y]_{(x)}$ contains $\mathbb{C}(y)$ and $\mathbb{C}(x+y)$, which both are coefficient fields!

Remark 6.29. If $(R, \mathfrak{m}, k)$ is local with coefficient field K, then a finite length R-module M may not be a k-module (it may not be killed by $\mathfrak{m}$), but it is a K-vector space by restriction of scalars, and $\ell(M) = \dim_K(M)$.

6.3 Height and number of generators

Theorem 6.30 (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). 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 4.30, $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)}$ 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 the Krull intersection theorem 5.61. 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. ∎

We want to generalize this, but 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 6.31. *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 the principal ideal theorem 6.30, 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 6.32 (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 6.30.

Let $I = (f_1, \dots, f_n)$ 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 $(f_2, \dots, f_n)\overline{R}$. 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 $f_1 \in \mathfrak{p}_1$. □

Example 6.33.

a) The bound is certainly sharp: an ideal generated by n variables $(x_1, x_2, \dots, x_n)$ in a polynomial ring has height n. There are many other such ideals. For example, $(u^3 - xyz, x^2 + 2xz - 6y^5, vx + 7vy) \in k[u, v, w, x, y, z]$. An ideal of height n generated by n elements is called a **complete intersection**.

b) The ideal (xy, xz) in $k[x, y, z]$ has minimal primes of heights 1 and 2.

c) 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).

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

e) 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 in R, and moreover $\mathfrak{m} = (x, xy, xy^2, \dots) \subseteq \sqrt{(x)}$. 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 $\operatorname{ht}(\mathfrak{m}) > 1$.

Lemma 6.34. *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 6.32, the height of $\mathfrak{q}$ is then exactly $m + 1$. □

Theorem 6.35. *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) If I is any ideal in R, then there are (at most) $d + 1$ elements $f_1, \dots, f_{d+1} \in I$ such that $\sqrt{I} = \sqrt{(f_1, \dots, f_{d+1})}$.

c) 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 $J_i = (f_1, \dots, f_i)$

$$\mathfrak{p} \not\subseteq \bigcup_{\substack{\mathfrak{a} \in \operatorname{Min}(J_i) \\ \mathfrak{a} \notin V(I)}} \mathfrak{a}$$

for $i = 0, \dots, h-1$. As long as the set on the right is nonempty,

$$(f_1, \dots, f_i) \subseteq \bigcup_{\substack{\mathfrak{a} \in \operatorname{Min}(J_i) \\ \mathfrak{a} \notin V(I)}} \mathfrak{a},$$

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 6.32 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

$$\mathfrak{p} \not\subseteq \bigcup_{\substack{\mathfrak{a} \in \operatorname{Min}(f_1, \dots, f_i) \\ \mathfrak{a} \notin V(I)}} \mathfrak{a} = \bigcup_{\mathfrak{a} \in \operatorname{Min}(f_1, \dots, f_i)} \mathfrak{a}$$

This is immediate by prime avoidance 5.35, 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) Again, we use the recipe from Lemma 6.34. We again need to see that we can do this. Inductively, we will choose elements inside of I, so each J_i is contained in I, and $V(I) \subseteq V(J_i)$. We start with $J_0 = (0)$.

If for some i we have $\operatorname{Min}(J_i) \smallsetminus V(I) = \varnothing$, then each minimal prime of J_i lies in $V(I)$, so $V(J_i) \subseteq V(I)$. Then $V(J_i) = V(I)$, so $\sqrt{J_i} = \sqrt{I}$. If $\operatorname{Min}(J_i) \smallsetminus V(I) \neq \varnothing$, then $I \not\subseteq \mathfrak{q}$ for any $\mathfrak{q} \in \operatorname{Min}(J_i) \smallsetminus V(I)$, and $I \not\subseteq \bigcup_{\operatorname{Min}(J_i) \smallsetminus V(I)} \mathfrak{q}$ by prime avoidance 5.35, so we can choose elements as in the lemma.

If $\sqrt{(f_1, \dots, f_i)} = \sqrt{I}$ for $i \leqslant d$, we are done. Suppose not. Then we get elements $(f_1, \dots, f_{d+1}) = J_{d+1} \subseteq I$ such that the minimal primes of J_{d+1} either contain I or have height at least $d+1$. By the assumption that $\dim(R) = d$, no prime has height $d+1$, so all the minimal primes of J_{d+1} must contain I. Since $J_{d+1} \subseteq I$, any minimal prime of J_{d+1} must also be minimal over I. Thus, $\operatorname{Min}(J_{d+1}) \subseteq \operatorname{Min}(I)$, so $V(J_{d+1}) \subseteq V(I)$, and equality holds, so the radicals are equal.

c) 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. □

Corollary 6.36. *Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring. Then*

$$\dim(R) = \min\{n \mid \sqrt{(f_1, \dots, f_n)} = \mathfrak{m} \text{ for some } f_1, \dots, f_n\} \leqslant \mu(\mathfrak{m}).$$

In particular, a Noetherian local ring has finite dimension.

Proof. The dimension of a local ring is the height of its maximal ideal. Thus, by Krull's Height Theorem 6.32, the minimum n in the middle is at least $\dim(R)$, and Theorem 6.35 gives the other direction. Since $\mathfrak{m}$ is generated by $\mu(\mathfrak{m})$ elements, there are in particular $\mu(\mathfrak{m})$ elements whose radical is $\mathfrak{m}$. □

Definition 6.37. 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.

So Corollary 6.36 can be restated as $\dim(R) \leqslant \operatorname{embdim}(R)$.

Corollary 6.38. *Let k be a field and $R = k[\![x_1, \ldots, x_d]\!]$. Then $\dim(R) = d$.*

Proof. Let $\mathfrak{m} = (x_1, \ldots, x_d)$. The strict chain of primes

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

shows that $\dim(R) \leqslant d$. On the other hand, the images of $x_1, \ldots, x_d$ in $\mathfrak{m}/\mathfrak{m}^2$ are linearly independent, so $\mu(\mathfrak{m}) = d$. By Corollary 6.36, $\dim(R) = d$. □

Rings whose dimension and embedding dimension agree are very nicely behaved.

Definition 6.39. A local ring $(R, \mathfrak{m})$ is **regular** if $\dim(R) = \operatorname{embdim}(R)$.

So we just showed that power series rings $k[\![x_1, \ldots, x_d]\!]$ are regular local rings.

In general, a ring is regular if all its localizations are regular local rings. In order for this definition to make sense, we need to first make sure that regularity localizes, meaning that if $(R, \mathfrak{m})$ is a regular local ring, then R_P is also regular for all primes P. But to do that, we need some homological algebra. However (spoiler alert!), things do work out alright, and as you might expect, polynomial rings over fields are also regular.

Chapter 7

Dimension theory II

7.1 Over, up and down

Given a ring homomorphism $R \xrightarrow{\varphi} S$, we want to study the behavior of chains of primes under φ, meaning how chains in R behave under expansion to S or chains in S behave under contraction to R.

First, we need a technical definition.

Definition 7.1. Let $R \xrightarrow{\varphi} S$ be a ring homomorphism, and consider a prime $\mathfrak{p}$ in R. The ring

$$\kappa_\phi(\mathfrak{p}) := (R \smallsetminus \mathfrak{p})^{-1}(S/\mathfrak{p}S)$$

is the *fiber ring* of ϕ over $\mathfrak{p}$. As a special case, we write $\kappa(\mathfrak{p})$ for the fiber of the identity map; this is $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$, the residue field of the local ring $R_\mathfrak{p}$.

The point of this definition is that the primes ideals in this ring correspond to the primes in S that contract to $\mathfrak{p}$.

Lemma 7.2. *Let $R \xrightarrow{\varphi} S$ be a ring homomorphism, and $\mathfrak{p} \in \operatorname{Spec}(R)$. The set of primes in S that contract to $\mathfrak{p}$ correspond to the primes in $\kappa_\phi(\mathfrak{p})$. More precisely, $\operatorname{Spec}(\kappa_\phi(\mathfrak{p})) \cong (\varphi^*)^{-1}(\mathfrak{p})$.*

Proof. Consider the maps $S \xrightarrow{\pi} S/\mathfrak{p}S \xrightarrow{g} (R \smallsetminus \mathfrak{p})^{-1}(S/\mathfrak{p}S)$. In Example 3.39 we saw that the map on spectra induced by π can be identified with the inclusion of $V(\mathfrak{p}S)$ into $\operatorname{Spec}(S)$. For the second map, g, we saw in Proposition 4.27 that the map on spectra can be identified with the inclusion of the set of primes that do not intersect $R \smallsetminus \mathfrak{p}$, i.e., those whose contraction is contained in $\mathfrak{p}$. Together, these say $(g \circ \pi)^*$ is an inclusion, whose image is the set of primes in S that contract to $\mathfrak{p}$. □

We have seen that taking $IS \cap R$ does not always recover the ideal I. When I is a prime ideal, we can characterize this in terms of the induced map on Spec.

Lemma 7.3 (Image criterion)**.** *Let* $R \xrightarrow{\varphi} S$ *be a ring homomorphism. For any* $\mathfrak{p} \in \operatorname{Spec}(R)$*,* $\mathfrak{p} \in \operatorname{im}(\varphi^*)$ *if and only if* $\mathfrak{p}S \cap R = \mathfrak{p}$*.*

Proof. If $\mathfrak{p}S \cap R = \mathfrak{p}$, then

$$\frac{R}{\mathfrak{p}} = \frac{R}{\mathfrak{p}S \cap R} \hookrightarrow \frac{S}{\mathfrak{p}S},$$

so localizing at $(R \smallsetminus \mathfrak{p})$, we get an inclusion $\kappa(\mathfrak{p}) \subseteq \kappa_\varphi(\mathfrak{p})$. Since $\kappa(\mathfrak{p})$ is nonzero, so is $\kappa_\varphi(\mathfrak{p})$, and thus its spectrum is nonempty. By Lemma 7.2, there is a prime mapping to $\mathfrak{p}$.

If $\mathfrak{p}S \cap R \neq \mathfrak{p}$, then $\mathfrak{p}S \cap R \supsetneq \mathfrak{p}$. If $\mathfrak{q} \cap R = \mathfrak{p}$, then $\mathfrak{q} \supseteq \mathfrak{p}S$, so $\mathfrak{q} \cap R \supsetneq \mathfrak{p}$. So no prime contracts to $\mathfrak{p}$. □

Note that $\mathfrak{p}S$ may not be prime, in general.

Example 7.4. Let $R = \mathbb{C}[x^n] \subseteq S = \mathbb{C}[x]$. The ideal $(x^n - 1)R$ is prime. On the other hand, if ζ is a primitive nth root of unity, then

$$(x^n - 1)S = \left(\prod_{i=0}^{n-1} x - \zeta^i \right) S,$$

which is not prime. However, each of its minimal primes $(x-\zeta^i)S$ contracts to $(x^n-1)R$, so $(x^n - 1)S \cap R = (x^n - 1)R$. Similarly, the ideal $x^n R$ is prime, while $x^n S$ is not even radical.

Example 7.5. Consider the inclusion $R := k[xy, xz, yz] \xhookrightarrow{\varphi} S := k[x, y, z]$ and the prime $\mathfrak{p} = (xy)$ in R. Notice that $(xz)(yz) \in \mathfrak{p}S \cap R$, but *not* in $\mathfrak{p}$, so $\mathfrak{p}S \cap R \supsetneq \mathfrak{p}$, and thus $\mathfrak{p} \notin \operatorname{im}(\varphi^*)$. We can check this more directly, by noting that any prime Q in S contracting to $\mathfrak{p}$ would contain $\mathfrak{p}S = (x) \cap (y)$, so $Q \supseteq (x)$ or $Q \supseteq (y)$. But $(x) \cap R = (xy, xz) \supsetneq \mathfrak{p}$ and $(y) \cap R = (xy, yz) \supsetneq \mathfrak{p}$, so no prime in S contracts to $\mathfrak{p}$.

Corollary 7.6. *If* $R \subseteq S$ *is a direct summand, then* $\operatorname{Spec}(S) \to \operatorname{Spec}(R)$ *is surjective, so Lemma 7.3 says the map on Spec is surjective.*

Proof. By Lemma 2.17, we know $IS \cap R = I$ for all ideals in this case. □

We want to extend the idea of the last corollary to work for all integral extensions.

Definition 7.7. Let R be a ring, S an R-algebra, and I an ideal. An element r of R is **integral** over I if it satisfies an equation of the form

$$r^n + a_1 r^{n-1} + \cdots + a_{n-1} r + a_n = 0 \qquad \text{with } a_i \in I^i \text{ for all } i.$$

An element of S is **integral** over I if

$$s^n + a_1 s^{n-1} + \cdots + a_{n-1} s + a_n = 0 \qquad \text{with } a_i \in I^i \text{ for all } i.$$

The **integral closure** of I in R is the set of elements of R that are integral over I, denoted $\overline{I}$. Similarly, we write $\overline{I}^S$ for the integral closure of I in S.

The convention is that $I^0 = R$ for any ideal I of R.

Remark 7.8. Notice that $\overline{I}^S \cap R = \overline{I}$ is immediate from the definition.

Exercise 20. Let $R \subseteq S$, I be an ideal of S, and t be an indeterminate. Consider the rings $R[It] \subseteq R[t] \subseteq S[t]$. Here $R[It]$ is the subalgebra of $R[t]$ generated by elements of the form at for all $a \in I$. Notice that we can give this a structure of a graded ring by setting all elements in R to have degree 0 and t to have degree 1, so

$$R[It] = \bigoplus_{n \geqslant 0} I^n t^n.$$

This is usually called the **Rees algebra** of I.

a) $\overline{I}^S = \{s \in S \mid st \in S[t] \text{ is integral over the ring } R[It]\}$.

b) $\overline{I}^S$ is an ideal of S.

In older texts and papers (e.g., Atiyah–Macdonald [AM69] and [Kun69]) a different definition is given for integral closure of an ideal. The one we use here is now the more universally used notion.

Lemma 7.9 (Extension–contraction lemma for integral extensions)**.** *Let $R \subseteq S$ be integral, and I be an ideal of R. Then $IS \subseteq \overline{I}^S$, and hence $IS \cap R \subseteq \overline{I}$.*

Proof. Let $x \in IS$. We can write $x = a_1 s_1 + \cdots + a_t s_t$ for some $a_i \in I$. Moreover, taking $S' = R[s_1, \ldots, s_t]$, we also have $x \in IS'$. We will show that $x \in \overline{I}^{S'}$, so $x \in \overline{I}^S$ follows as a corollary. So we might as well replace S with S', so that $R \subseteq S$ is also integral and module-finite. By Corollary 1.37, the extension is also module-finite.

Let $S = Rb_1 + \cdots + Rb_n$. We can write

$$xb_i = \left(\sum_{k=1}^{t} a_k s_k\right) b_i = \sum_j a_{ij} b_j$$

with $a_{ij} \in I$. We can write these equations in the form $xv = Av$, where $v = (b_1, \ldots, b_u)$, and $A = [a_{ij}]$. By the determinantal trick, Lemma 1.35, we have $\det(xI - A)v = 0$. Since we can assume $b_1 = 1$, we have $\det(xI - A) = 0$. The fact that this is the type of equation we want follows from the monomial expansion of the determinant: any monomial is a product of n terms where some of them are copies of x, and the rest are elements of I. Since this is a product of n terms, a term in x^i has a coefficient coming from a product of $n - i$ elements of I.

So this shows that $IS \subseteq \overline{I}^S$. Now notice that $\overline{I}^S \cap R = \overline{I}$ is immediate from the definition, as noted in Remark 7.8. □

Theorem 7.10 (Lying over)**.** *If $R \subseteq S$ is an integral extension, then $\mathfrak{p}S \cap R = \mathfrak{p}$ for every $\mathfrak{p} \in \operatorname{Spec}(R)$, so the induced map $\operatorname{Spec}(S) \longrightarrow \operatorname{Spec}(R)$ is surjective.*

Proof. We claim that $\overline{I} \subseteq \sqrt{I}$. Indeed, if $r \in \overline{I}$, then

$$r^n + a_1 r^{n-1} + \cdots + a_{n-1} r + a_n = 0$$

for some n and some $a_i \in I^i$ for all i, so

$$r^n = -a_1 r^{n-1} - \cdots - a_{n-1} r - a_n \in I.$$

Therefore, if $\mathfrak{p}$ is a prime in R, by Lemma 7.9 we have $\mathfrak{p}S \cap R \subseteq \overline{\mathfrak{p}}$, and

$$\mathfrak{p}S \cap R \subseteq \overline{\mathfrak{p}} \subseteq \sqrt{\mathfrak{p}} = \mathfrak{p}.$$

Then $\mathfrak{p}S \cap R = \mathfrak{p}$, and by Lemma 7.3 we conclude that $\mathfrak{p}$ is in the image of the map on Spec. □

Example 7.11. We saw in **??????** that the map induced on Spec by the inclusion $k[xy, xz, yz] \subseteq k[x, y, z]$ is not surjective. So Theorem 7.10 does not apply — indeed, this inclusion is not module-finite, and thus it is not integral. For example, the infinite set $\{1, x^n, y^n, z^n \mid n \geqslant 1\}$ is a minimal generating set for $k[x, y, z]$ over $k[xy, xz, yz]$

Both assumptions that the extension is integral and that it is an inclusion are needed in Theorem 7.10.

Example 7.12.

a) Suppose f is a regular element on R, but not a unit. Since f is regular, the map $R \longrightarrow R_f$ is an inclusion, but we claim it is not integral. If $\frac{1}{f}$ was integral over R, there would be $a_i \in R$ such that

$$\frac{1}{f^n} + \frac{a_{n-1}}{f^{n-1}} + \cdots + \frac{a_1}{f} + a_0 = 0.$$

After multiplying by f^n all terms are of the form $\frac{r}{1}$, and thus in R, since the localization map is injective. So

$$1 = a_{n-1} f + \cdots + a_1 f^{n-1} + a_0 f^n \in (f),$$

and f must be a unit.

So $R \longrightarrow R_f$ is an example of an inclusion that is not integral. Note that the image of the map on Spec is the complement of $V(f)$, so in particular the map is not surjective.

b) In contrast, the map $R \longrightarrow R/(f)$ is integral, but it is not an inclusion. The map on Spec is again not surjective: its image is $V(f)$.

Remark 7.13. Let I be an ideal in S. Suppose $R \longrightarrow S$ is an integral extension. There is an induced map $R/(I \cap R) \longrightarrow S/I$, and that map is integral: an equation of integral dependance for $s \in S$ over R give an equation for integral dependance of its class in S/I over $R/(I \cap R)$.

Lemma 7.14. *If $R \xrightarrow{\varphi} S$ is integral, $Q \cap R$ is maximal if and only if Q is maximal in S. If $R \subseteq S$ is an integral extension of domains, R is a field if and only S is a field.*

Proof. By Remark 7.13, the induced map $R/(Q \cap R) \subseteq S/Q$ is an integral extension of domains, and Q (respectively, $Q \cap R$) is maximal if and only if S/Q (respectively, $R/(Q \cap R)$) is a field. So it is sufficient to show the second statement, about inclusions of domains.

Now suppose $R \subseteq S$ is an integral extension of domains. Assume R is a field, and take any nonzero $s \in S$. Consider some 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. □

Theorem 7.15 (Incomparability)**.** *If $R \longrightarrow S$ is integral and $P \subseteq Q$ are such that $P \cap R = Q \cap R$, then $P = Q$.*

Proof. Since the map on spectra induced by $R \longrightarrow R/\ker(R)$ is injective, we can replace R by the quotient and assume φ is an integral inclusion.

So suppose $R \subseteq S$ is integral, and let $\mathfrak{p} = P \cap R = Q \cap R$. We claim that localizing at $(R \smallsetminus P)$ preserves integrality: if $x \in S$ and $w \in R \smallsetminus \mathfrak{p}$, then we have equations of the form

$$x^n + r_1 x^{n-1} + \cdots + r_n = 0 \implies \left(\frac{x}{w}\right)^n + \frac{r_1}{w}\left(\frac{x}{w}\right)^{n-1} + \cdots + \frac{r_n}{w^n} = 0.$$

By localizing R at $(R \smallsetminus \mathfrak{p})$, the image of $\mathfrak{p}$ is a maximal ideal. So we reduced to the situation where $R \cap P = R \cap Q$ is a maximal ideal. By Lemma 7.14, $P \subseteq Q$ are both maximal ideals. Therefore, $P = Q$. □

Corollary 7.16. *Suppose $R \longrightarrow S$ is integral and that S is Noetherian. If S is Noetherian, then only finitely many primes contract to each $\mathfrak{p} \in \operatorname{Spec}(R)$.*

Proof. If $P \in \operatorname{Spec}(S)$ contracts to $\mathfrak{p}$, then $P \supseteq \mathfrak{p}S$, so in particular P contains some prime Q minimal over $\mathfrak{p}S$. Then

$$\mathfrak{p}S \subseteq Q \subseteq P \implies \mathfrak{p} \subseteq Q \cap R \subseteq P \cap R = \mathfrak{p},$$

so $Q \cap R = P \cap R$. By Theorem 7.15, $Q = P$. So all the primes contracting to $\mathfrak{p}$ are in $\operatorname{Min}(\mathfrak{p}S)$, which is a finite set since R is Noetherian. □

Corollary 7.17. *If $R \longrightarrow S$ is integral, then $\operatorname{ht}(\mathfrak{q}) \leqslant \operatorname{ht}(\mathfrak{q} \cap R)$ for any $\mathfrak{q} \in \operatorname{Spec}(S)$. In particular, $\dim(S) \leqslant \dim(R)$.*

Proof. Given a chain of primes $\mathfrak{a}_0 \subsetneq \cdots \subsetneq \mathfrak{a}_n = \mathfrak{q}$ in $\operatorname{Spec}(S)$, we can contract to R, and by Theorem 7.15 we get a chain of distinct primes in $\operatorname{Spec}(R)$. □

Theorem 7.18 (Going up)**.** *If $R \longrightarrow S$ is integral, then for every $\mathfrak{p} \subsetneq \mathfrak{q}$ in $\operatorname{Spec}(R)$ and $P \in \operatorname{Spec}(S)$ with $P \cap R = \mathfrak{p}$, there is some $Q \in \operatorname{Spec}(S)$ with $P \subsetneq Q$ and $Q \cap R = \mathfrak{q}$.*

The picture looks something like this:

$$\begin{array}{ccc} P & & P \subseteq Q \\ \subseteq & \overset{\exists Q}{\rightsquigarrow} & \subseteq \quad \subseteq \\ \mathfrak{p} \subseteq \mathfrak{q} & & \mathfrak{p} \subseteq \mathfrak{q} \end{array}$$

Proof. Consider the map $R/\mathfrak{p} \longrightarrow S/\mathfrak{p}S \longrightarrow S/P$. This is integral, as we observed in Remark 7.13. It is also injective, so Lying Over, Theorem 7.10, applies. Thus, there is a prime $\mathfrak{a}$ of S/P that contracts to the prime $\mathfrak{q}/\mathfrak{p}$ in $\operatorname{Spec}(R/\mathfrak{p})$. We can write $\mathfrak{a} = Q/P$ for some $Q \in \operatorname{Spec}(S)$, and we must have that Q contracts to $\mathfrak{q}$. □

Corollary 7.19. *If $R \subseteq S$ is integral, then $\dim(R) = \dim(S)$.*

Proof. We have already shown that $\dim(S) \leqslant \dim(R)$ in Corollary 7.17, so we just need to show that $\dim(R) \leqslant \dim(S)$. Fix a chain of primes $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ in $\operatorname{Spec}(R)$. By Lying Over, Theorem 7.10, there is a prime $\mathfrak{q}_0 \in \operatorname{Spec}(S)$ contracting to $\mathfrak{p}_0$. Then by Going up, Theorem 7.18, we have $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1$ with $\mathfrak{q}_1 \cap R = \mathfrak{p}_1$. Continuing, we can build a chain of distinct primes in S of length n. So $\dim(R) \leqslant \dim(S)$, and equality follows. □

Recall that a domain is normal if it is integrally closed in its field of fractions. In a previous problem set, you showed that $\mathbb{Z}$ is normal; we now extend that result to any unique factorization domain.

Lemma 7.20. *A unique factorization domain is normal. In particular, a polynomial ring over a field is normal.*

Proof. Let R be a UFD, and $\frac{r}{s} \in \text{frac}(R)$ be integral over R. We can assume that r and s have no common factor. Then we have some $a_i \in R$ such that

$$\frac{r^n}{s^n} + a_1 \frac{r^{n-1}}{s^{n-1}} + \cdots + a_n = 0 \quad \Longrightarrow \quad r^n = -(a_1 r^{n-1} s + \cdots + a_n s^n).$$

Any irreducible factor of s must then divide r^n, and hence divide r. If s is not a unit in R, then this contradicts that there is no common factor. Therefore, $r/s \in R$. □

Lemma 7.21. *Let R be a normal domain, x be an element integral over R in some larger domain. Let k be the fraction field of R, and $f(t) \in k[t]$ be the minimal polynomial of x over k.*

a) If x is integral over R, then $f(t) \in R[t] \subseteq k[t]$.

b) If x is integral over a prime $\mathfrak{p}$, then $f(t)$ has all of its nonleading coefficients in $\mathfrak{p}$.

Proof. Let x be integral over R. Fix an algebraic closure of k containing x, and let $x_1 = x, x_2, \ldots, x_u$ be the roots of f. Since $f(t)$ divides any polynomial with coefficients in k that x satisfies, it also divides a monic equation of integral dependance for x over R. Therefore, each x_i is a solution to such an equation of integral dependence, and thus must be integral over R.

Let $S = R[x_1, \ldots, x_u] \subseteq \overline{k}$. This is a module-finite extension of R, so all of its elements are integral over R. The leading coefficient of $f(t)$ is 1, and the remaining coefficients of $f(t)$ are polynomials in the x_i, hence they lie in S. On the other hand, R is normal, so $S \cap k = R$. We conclude that all the coefficients of f are in R, and $f \in R[t]$.

Now let x be integral over $\mathfrak{p}$. By the same argument as above, all of the x_i are integral over $\mathfrak{p}$. Since each $x_i \in \overline{\mathfrak{p}}^S$, any polynomial in the x_i lies in $\overline{\mathfrak{p}}^S$. So the nonleading coefficients of f lie in $\overline{\mathfrak{p}}^S \cap R = \mathfrak{p}$, by Theorem 7.10. □

Theorem 7.22 (Going down)**.** *Suppose that R is a normal domain, S is a domain, and $R \subseteq S$ is integral. Then, for every $\mathfrak{p} \subsetneq \mathfrak{q}$ in $\text{Spec}(R)$ and Q in $\text{Spec}(S)$ with $Q \cap R = \mathfrak{q}$, there is some $P \in \text{Spec}(S)$ with $P \subsetneq Q$ and $P \cap R = \mathfrak{p}$.*

The picture looks like

$$\begin{array}{rcl} Q & & P \subseteq Q \\ \subseteq & \rightsquigarrow^{\exists P} & \subseteq \quad \subseteq \\ \mathfrak{p} \subseteq \mathfrak{q} & & \mathfrak{p} \subseteq \mathfrak{q} \end{array}$$

Proof. As before, we can replace R and S by their localizations at the multiplicatively closed set $R \setminus \mathfrak{q}$ without loss of generality, since that extension is still integral. So now $\mathfrak{q}$ is the unique maximal ideal in R, and want to show that $\mathfrak{p}$ is the contraction of some prime ideal $P \subseteq Q$, so it suffices to find some prime ideal in S_Q. Se we can further compose with the localization of S at Q, and as before $R \longrightarrow S_Q$ is still an integrally

closed extension. We have thus reduced to the case when $(R, \mathfrak{q})$ and (S, Q) are local. By Lemma 7.3, it suffices to show that $\mathfrak{p}S \cap R = \mathfrak{p}$.

Let $r \in \mathfrak{p}S \cap R$. Then $r = s_1a_1 + \cdots, +s_na_n$ for some $s_i \in S$ and $a_i \in \mathfrak{p}$, so $r \in R[s_1, \ldots, s_n]$.

Let $W = (S \smallsetminus Q)(R \smallsetminus \mathfrak{p})$ be the multiplicative set in S consisting of products of elements in $S \smallsetminus Q$ and $R \smallsetminus \mathfrak{p}$. Note that each of these sets contains 1, so each set is contained in W, the product of the two. We will show that $W \cap \mathfrak{p}S$ is empty. Once we do that, it will follow from Lemma 3.41 that there is a prime ideal P in S containing $\mathfrak{p}S$ such that $W \cap P$ is empty. Notice that such a prime is necessarily contained in Q, since $S \smallsetminus Q \subseteq W$. Moreover, $R \setminus \mathfrak{p} \subseteq W$, so $(Q \cap R) \cap (R \setminus \mathfrak{p})$ is empty, or equivalently, $Q \cap R \subseteq \mathfrak{p}$. We conclude that $Q \cap R = \mathfrak{p}$.

So our goal is to show that $W \cap \mathfrak{p}S$ is empty. We proceed by contradiction, and assume there is some $x \in \mathfrak{p}S \cap W$. We can write $x = rs$ for some $r \in R \smallsetminus \mathfrak{p}$ and $s \in S \smallsetminus Q$. Moreover, since $x \in \mathfrak{p}S$, x is integral over $\mathfrak{p}$, by Lemma 7.9.

Consider the minimal polynomial of x over $\operatorname{frac}(R)$, say

$$h(x) = x^n + a_1x^{n-1} + \cdots + a_n = 0.$$

By Lemma 7.21, each $a_i \in \mathfrak{q} \subseteq R$. Then substituting $x = rs$ in $\operatorname{frac}(R)$ and dividing by r^n yields

$$g(s) = s^n + \frac{a_1}{r}s^{n-1} + \cdots + \frac{a_n}{r^n} = 0.$$

We claim that this is the minimal polynomial of s. If s satisfied a monic polynomial of degree $d < n$, multiplying by r^d would give us a polynomial of degree d that x satisfies, which is impossible. So indeed, this is the minimal polynomial of s.

Since $s \in S$, and thus integral over R, Lemma 7.21 says that each $\frac{a_i}{r^i} =: v_i \in R$. Since $r \notin \mathfrak{p}$ and $r^iv_i = a_i \in \mathfrak{p}$, we must have $v_i \in \mathfrak{p}$. The equation $g(s) = 0$ then shows that $s \in \sqrt{\mathfrak{p}S}$. Since $Q \in \operatorname{Spec}(S)$ contains $\mathfrak{q}S$ and hence $\mathfrak{p}S$, we have $s \in \sqrt{\mathfrak{p}S} \subseteq Q$. This is the desired contradiction. □

Corollary 7.23. *If R is a normal domain, S is a domain, and $R \subseteq S$ is integral, then* $\operatorname{ht}(\mathfrak{q}) = \operatorname{ht}(\mathfrak{q} \cap R)$ *for any* $\mathfrak{q} \in \operatorname{Spec}(S)$.

Proof. We already know from Corollary 7.17 that $\operatorname{ht}(\mathfrak{q}) \leqslant \operatorname{ht}(\mathfrak{q} \cap R)$. Given a saturated chain up to $\mathfrak{q} \cap R$, we can apply Going Down, Theorem 7.22 to get a chain just as long that goes up to $\mathfrak{q}$. □

7.2 Noether normalization and dimension of affine rings

Lemma 7.24 (Making a pure-power leading term)**.**

a) Let A be a domain, and $f \in R = A[x_1, \ldots, x_n]$ be a (not necessarily homogeneous) polynomial of degree at most N. The A-algebra automorphism of R given by

$\phi(x_i) = x_i + x_n^{N^{n-i}}$ for $i < n$ and $\phi(x_n) = x_n$ maps f to a polynomial that, viewed as a polynomial in x_n with coefficients in $A[x_1, \ldots, x_{n-1}]$, has leading term dx_n^a for some $d \in A$ and $a \in \mathbb{N}$.

b) Let k be an infinite field, and let $R = k[x_1, \ldots, x_n]$ be standard graded, meaning $\deg(x_i) = 1$. Let $f \in R$ be a homogeneous polynomial of degree N. There is a degree-preserving k-algebra automorphism of R given by $\phi(x_i) = x_i + a_i x_n$ for $i < n$ and $\phi(x_n) = x_n$ that maps f to a polynomial that viewed as a polynomial in x_n with coefficients in $k[x_1, \ldots, x_{n-1}]$, has leading term ax_n^N for some (nonzero) $a \in k$.

Proof.

a) The map ϕ sends a monomial term $dx_1^{a_1} \cdots x_n^{a_n}$ to a polynomial with unique highest degree term $dx_n^{a_1 N^{n-1} + a_2 N^{n-2} + \cdots + a_{n-1} N + a_n}$. For each of the monomials $dx_1^{a_1} \cdots x_n^{a_n}$ in f with nonzero coefficient $d \neq 0$, we must have each $a_i \leqslant N$, so the map $(a_1, \ldots, a_n) \mapsto a_1 N^{n-1} + a_2 N^{n-2} + \cdots + a_{n-1} N + a_n$ is injective when restricted to the set of exponent tuples of f. Therefore, none of the terms can cancel. We find that the leading term is of the promised form.

b) We just need to show that the x^N coefficient of $\phi(f)$ is nonzero for some choice of a_i. One can check that the coefficient of the x^N term is $f(-a_1, \ldots, -a_{n-1}, 1)$. But $f(-a_1, \ldots, -a_{n-1}, 1)$, when thought of as a polynomial in the a_i, is identically zero, then f must be the zero polynomial. □

Theorem 7.25 (Noether Normalization)**.** *Let A be a domain, and R be a finitely generated A-algebra. There is some nonzero $a \in A$ and $x_1, \ldots, x_t \in R$ algebraically independent over A such that R_a is module-finite over $A_a[x_1, \ldots, x_t]$. In particular, if $A = k$ is a field, then R is module-finite over $k[x_1, \ldots, x_t]$.*

Proof. We proceed by induction on the number of generators n of R over A. There is nothing to prove in the case when $n = 0$.

Now suppose that we know the result holds for A-algebras generated by at most $n - 1$ elements, and let $R = A[r_1, \ldots, r_n]$. If $r_1, \ldots, r_n$ are algebraically independent over A, we are done. If not, there is some $f(x_1, \ldots, x_n) \in A[x_1, \ldots, x_n]$ such that $f(r_1, \ldots, r_n) = 0$. After possibly applying Lemma 7.24 to change our choice of algebra generators, we can assume that f has leading term ax_n^N for some a. Then f is monic in x_n after inverting a, so R_a is module-finite over $A_a[r_1, \ldots, r_{n-1}]$. By hypothesis, $A_{ab}[r_1, \ldots, r_{n-1}]$ is module-finite over $A_{ab}[x_1, \ldots, x_s]$ for some $b \in A$ and $x_1, \ldots, x_s$ that are algebraically independent over A. Since R_{ab} is module-finite over $A_{ab}[r_1, \ldots, r_{n-1}]$, R_{ab} must also be module-finite over $A_{ab}[x_1, \ldots, x_s]$, and we are done. □

Theorem 7.26 (Graded Noether Normalization)**.** *Let k be an infinite field, and R be a finitely generated $\mathbb{N}$-graded k-algebra with $R_0 = k$ and $R = k[R_1]$. There are homogeneous elements $x_1, \ldots, x_t \in R_1$ algebraically independent over k such that R is module-finite over $k[x_1, \ldots, x_t]$.*

Proof. We repeat the proof of Theorem 7.25 but use Lemma 7.24 (2), the graded version. □

Remark 7.27. There also exist Noether normalizations for quotients of power series rings over fields: after a change of coordinates, one can rewrite any nonzero power series in $k[\![x_1, \ldots, x_n]\!]$ as a series of the form $u(x_n^d + a_{d-1}x_n^{d-1} + \cdots + a_0)$ for a unit u and $a_0, \ldots, a_{d-1} \in k[\![x_1, \ldots, x_{n-1}]\!]$. This is called *Weierstrass preparation*. The proof of the Noether normalization theorem proceeds in essentially the same way. Thus, given $k[\![x_1, \ldots, x_n]\!]/I$, we have some module-finite inclusion of another power series ring $k[\![z_1, \ldots, z_d]\!] \subseteq k[\![x_1, \ldots, x_n]\!]/I$.

Theorem 7.28. *Let R be a domain that is a finitely generated algebra over a field k, or a quotient of a power series ring over a field. Let $k[z_1, \ldots, z_d]$ be any Noether normalization for R. For any maximal ideal $\mathfrak{m}$ of R, the length of any saturated chain of primes from 0 to $\mathfrak{m}$ is d. In particular,* $\dim(R) = d$.

Proof. We will show the proof in the case when R is a finitely generated domain over a field k; the power series case is similar, and left as an exercise. We prove by induction on d that for any finitely generated domain with a Noether normalization with d algebraically independent elements, any saturated chain of primes ending in a maximal ideal has length d.

When $d = 0$, R is a domain that is integral over a field, hence R is a field by Lemma 7.14. So suppose the statement holds for $d-1$, and let R be a finitely generated domain over some field k with Noether normalization $k[z_1, \ldots, z_d]$. Consider a maximal ideal $\mathfrak{m}$ of R, and a saturated chain

$$0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_k = \mathfrak{m}.$$

Consider the contraction of this chain to $A = k[z_1, \ldots, z_d]$, which by Theorem 7.15 are distinct primes in R:

$$0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_k.$$

Our assumption that the original chain is saturated implies that $\mathfrak{q}_1$ has height 1. If $\mathfrak{p}_1$ had height 2 or more, then by Going Down, Theorem 7.22, so would $\mathfrak{q}_1$, so $\mathfrak{p}_1$ has height 1 as well. Since $k[z_1, \ldots, z_d]$ is a UFD, $\mathfrak{p}_1 = (f)$ for some prime element f, by Example 6.3 d. After a change of variables, as in Lemma 7.24, we can assume that f is monic in z_d with coefficients in $k[z_1, \ldots, z_{d-1}]$. So $k[z_1, \ldots, z_{d-1}] \subseteq A/(f) \subseteq R/\mathfrak{q}_1$ are module-finite, and the induction hypothesis applies to $R/\mathfrak{q}_1$. Now

$$0 = \mathfrak{q}_1/\mathfrak{q}_1 \subsetneq \mathfrak{q}_2/\mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_k/\mathfrak{q}_1 = \mathfrak{m}/\mathfrak{q}_1$$

is a saturated chain in the affine domain $R/\mathfrak{q}_1$ going up to the maximal ideal $\mathfrak{m}/\mathfrak{q}_1$. The induction hypothesis then says that this chain has length $d-1$, so $k-1 = d-1$, and $k = d$. □

Corollary 7.29. *The dimension of the polynomial ring $k[x_1, \ldots, x_d]$ is d.*

Proof. The polynomial ring $k[x_1, \ldots, x_d]$ is a Noether normalization of itself, and Theorem 7.28 says that it must have dimension d. □

This matches our geometric intuition: $k[x_1, \ldots, x_d]$ corresponds to $\mathbb{A}^d_k$, and we are used to thinking of $\mathbb{A}^d_k$ as a d-dimensional space. Moreover, if R is a finitely generated k-algebra, then R is a quotient of $k[x_1, \ldots, x_d]$, where d is the number of generators of R as a k-algebra. Therefore, $\dim(R) \leqslant d$.

Corollary 7.30. *If R is a k-algebra, the dimension of R is less than or equal to the minimal size of an algebra generating set for R over k. If $R = k[f_1, \ldots, f_d]$ and $\dim(R) = d$, then R is isomorphic to a polynomial ring over k, and the generators f_i are algebraically independent.*

Proof. The first statement is trivial unless R is finitely generated, in which case we can write $R = k[f_1, \ldots, f_s] \cong k[x_1, \ldots, x_s]/I$ for some ideal I, so

$$\dim(R) \leqslant \dim(k[x_1, \ldots, x_s]) = d.$$

Suppose we chose s to be minimal. If $I \neq 0$, then $\dim(R) < s$, since the zero ideal is not contained in I. □

Corollary 7.31. *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) $\mathrm{ht}(I) = \dim(R) - \dim(R/I)$ for all ideals I.

Proof.

1) Let $\mathfrak{p} \subseteq \mathfrak{q}$ be primes in R. We can quotient out by $\mathfrak{p}$, and assume that R is a domain and $\mathfrak{p} = 0$. Fix a saturated chain C from $\mathfrak{q}$ to a maximal ideal $\mathfrak{m}$. Given two saturated chains C', C'' from 0 to $\mathfrak{q}$, the concatenations $C'|C$ and $C''|C$ are saturated chains from 0 to $\mathfrak{m}$, so by Theorem 7.28 they must have the same length. It follows that C' and C'' have the same length.
2) Equidimensionality is immediate from Theorem 7.28.
3) We have
$$\mathrm{ht}(I) = \min\{\mathrm{ht}(\mathfrak{p}) \mid \mathfrak{p} \in \mathrm{Min}(I)\}$$
and
$$\dim(R/I) = \max\{\dim(R/\mathfrak{p}) \mid \mathfrak{p} \in \mathrm{Min}(I)\}.$$
Therefore, it suffices to show the equality for prime ideals, since if $\mathfrak{p} \in \mathrm{Min}(I)$ attains the minimal $\mathrm{ht}(\mathfrak{p})$, then it also attains the maximal $\dim(R/\mathfrak{p})$. Now, take a saturated chain of primes C from 0 to $\mathfrak{p}$, and a saturated chain C' from $\mathfrak{p}$ to a maximal ideal $\mathfrak{m}$. Since R is catenary, C has length $\mathrm{ht}(\mathfrak{p})$. Moreover, C' has length $\dim(R/\mathfrak{p})$ by Theorem 7.28, and $C|C'$ has length $\dim(R)$ by Theorem 7.28.

□

Example 7.32. Let's use our dimension theorems to give a few different proofs that $R = k[x, y, z]/(y^2 - xz)$ has dimension 2 for any field K.

1) $k[x, z]$ is a Noether normalization for R, so the dimension is 2.
2) We observe that $y^2 - xz$ is irreducible, e.g., by thinking of it as a polynomial in y and applying Eisenstein's criterion. Then $(y^2 - xz)$ is a prime of height one, so the dimension of R is $\dim(k[x, y, z]) - \mathrm{ht}((y^2 - xz)) = 3 - 1 = 2$.

Chapter 8

Hilbert functions

8.1 Hilbert functions of graded rings

We now introduce a useful combinatorial book keeping tool for the vector space dimensions of the graded components of a finitely generated k-algebra.

Definition 8.1. Let k be a field. If R is an $\mathbb{N}$-graded k-algebra, the **Hilbert function**[1] of R is the function $H_R\colon \mathbb{Z} \longrightarrow \mathbb{N} \cup \infty$ defined by

$$H_R(t) := \dim_k(R_t)$$

Similarly, if M is a $\mathbb{Z}$-graded R-module, the Hilbert function of M is the function $H_R\colon \mathbb{Z} \longrightarrow \mathbb{N} \cup \infty$ defined by

$$H_M(t) := \dim_k(M_t).$$

We may write $H_R^k(t)$ or $H_M^k(t)$ if we want to emphasize what field k we are considering.

Sometimes it's useful to collect the values of the Hilbert function in the form of a power series.

Definition 8.2. If R is $\mathbb{Z}$-graded or $\mathbb{N}$-graded we define the **Hilbert series** of R or of a graded R-module M by $h_R(z) = \sum_{i\in\mathbb{Z}} H_R(i)z^i$ and $h_M(z) = \sum_{i\in\mathbb{Z}} H_M(i)z^i$.

Example 8.3. Consider the standard graded ring

$$R = k[x,y]/(x^2,y^3) = \underbrace{k}_{R_0} \bigoplus \underbrace{(k\,x \oplus k\,y)}_{R_1} \bigoplus \underbrace{(k\,xy \oplus k\,y^2)}_{R_2} \bigoplus \underbrace{k\,xy^2}_{R_3}.$$

Then $H_R(t) = \begin{cases} 1 & \text{if } t = 0 \\ 2 & \text{if } t = 1,2 \\ 1 & \text{if } t = 3 \\ 0 & \text{if } t \geqslant 4 \end{cases}$ and $h_R(z) = 1 + 2z + 2z^2 + z^3$.

[1] Some authors call the Hilbert series the Poicaré series, but in modern terminology that means something else.

Notice that in this example $H_R(t)$ is eventually the zero function, which we will take by convention to have degree -1 as a polynomial. Note also that R is a finite dimensional k-algebra, hence Artinian. So $\dim(R) = 0$.

The key example of a Hilbert function is what happens in the case of a polynomial ring.

Example 8.4. Let k be a field, and $R = k[x_1, \ldots, x_d]$ be a polynomial ring with the standard grading, meaning $\deg x_i = 1$ for each i. To compute the Hilbert function of R, we need to compute the size of a k-basis for $H_R(t)$ for each t. Such a basis is given by all the monomials in $x_1, \ldots, x_d$ of degree t:

$$R_t = \bigoplus_{a_1+\cdots+a_d=t} k \cdot x_1^{a_1} \cdots x_d^{a_d}.$$

We can easily count the number of monomials of degree t using elementary combinatorics, and we find that

$$H_R(t) = \binom{t+d-1}{d-1} = \binom{t+d-1}{t} \quad \text{for } t \geqslant 0.$$

We claim that the binomial function here can be expressed as a polynomial in t for $t \geqslant 0$. Consider

$$P_d(t) = \frac{(t+d-1)(t+d-2)\cdots(t+1)}{(d-1)!} \in \mathbb{Q}[t].$$

Observe that $P_n(t)$ has $-1, -2, \ldots, -(d-1)$ as roots. Then

$$H_R(t) = \begin{cases} P_d(t) & \text{if } t > -d \\ 0 & \text{if } t < 0. \end{cases}$$

Note that the two cases overlap for $-(d-1) \leqslant t \leqslant -1$.

Notice that in this example the Hilbert function is eventually (for $t \geqslant -d$) equal to a polynomial of degree $d-1$. Moreover, recall that $\dim(R) = d$.

To compute the Hilbert series, notice that the number of monomials of degree t is equal to the number of ordered tuples $(a_1, \ldots, a_d)$ with $a_1 + \cdots + a_d = t$. This is the coefficient of z^t in the product

$$(1 + z + z^2 + \cdots + z^{a_1} + \cdots)(1 + z + z^2 + \cdots + z^{a_2} + \cdots) \cdots (1 + z + z^2 + \cdots + z^{a_d} + \cdots)$$

hence

$$h_R(z) = (1 + z + z^2 + \cdots + z^i + \cdots)^d = \frac{1}{(1-z)^n}.$$

While the Hilbert function is a polynomial for any $n \in \mathbb{N}$ in this example, this is not always the case. Here's a cheap example:

Example 8.5. Let k be a field, and $R = k[x_1, \ldots, x_n]$ a polynomial ring with the standard grading $|x_i| = 1$ for each i as in the previous example and let d be an integer. Then

$$H_{R(-d)}(t) = \dim_k(R(-d)_t) = \dim_k(R(-d)_{t-d}) = H_R(t-d)$$

and $h_{R(-d)}(z) = z^d h_R(z)$. In particular, we see that $H_{R(-d)(t)} = P_n(t-d)$ for $t-d > -n$, can be expressed as a polynomial in t when $t - d > -n$, so for $t > d - n$. This Hilbert function is no longer a polynomial for all nonnegative integers, but it is a polynomial for high enough values of t.

To compute more sophisticated examples, we use short exact sequences. Unsurprisingly, Hilbert polynomials behave well with respect to short exact sequences.

Lemma 8.6. *Let R be a graded ring, and*

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

be a degree-preserving short exact sequence of graded R-modules. Then $H_M = H_L + H_N$.

Proof. In each degree t we get short exact sequences of vector spaces

$$0 \longrightarrow L_t \xrightarrow{f} M_t \xrightarrow{g} N_t \longrightarrow 0\,.$$

The claim follows from the Rank–Nullity Theorem from Linear Algebra:

$$\dim(M_t) = \dim(\operatorname{im} g) + \dim(\ker f) = \dim(\operatorname{im} g) + \dim(\operatorname{im} g) = \dim(N_t) + \dim(L_t).$$

□

We can now compute a more sophisticated example.

Example 8.7. Let f be a homogeneous element of degree d in a $\mathbb{Z}$-graded ring R. We have the short exact sequence

$$0 \longrightarrow R(-d) \longrightarrow R \longrightarrow R/(f) \longrightarrow 0\,.$$

By Lemma 8.6 and the definition of shift, this gives

$$H_R = H_{R(-d)} + H_{R/(f)} \implies H_{R/(f)}(t) = H_R(t) - H_{R(-d)}(t) = H_R(t) - H_R(t-d)$$

and

$$h_R = h_{R(-d)} + h_{R/(f)} \implies h_{R/(f)}(z) = h_R(z) - h_{R(-d)}(z) = h_R(z) - z^d h_R(z).$$

Then

$$H_{R/(f)}(t) = H_R(t) - H_R(t-d)$$

and

$$h_{R/(f)}(z) = (1 - z^d) h_R(z).$$

When $R = k[x_1, \dots, x_n]$, we saw in Example 8.4 that $H_R(t) = P_n(t)$ is a polynomial for $t > -n$. If $d < n$, then $t - d > -n$ for all $t \geqslant 0$, so

$$H_{R/(f)}(t) = P_n(t) - P_n(t-d) = \binom{t+n-1}{t} - \binom{t-d+n-1}{t}$$

is still given by a polynomial. When $d > n$, $H_{R/(f)}(t)$ still agrees with a polynomial *eventually*: for all $t \geqslant d - n$.

We can now show that Hilbert function is always eventually equal to a polynomial, as in Example 8.7.

Theorem 8.8. *Let k be a field, and R be a finitely graded k-algebra such that $R_0 = k$ and R is generated by elements of degree one. Let M be a finitely generated graded R-module.*[2] *There is a polynomial $P_M(t) \in \mathbb{Q}[t]$ and some $n \in \mathbb{N}$ such that $H_M(t) = P_M(t)$ for $t \geqslant n$. Moreover, $\deg(P_M) = \dim(M) - 1$, and we can write*

$$P_M(t) = \frac{e}{(\dim(M)-1)!} t^{\dim(M)-1} + \text{ lower order terms}$$

for some positive integer e. Finally, if $\dim(M) = 0$ then $P_M = 0$.

Proof. We will use induction on the dimension of M.

If $\dim(M) = 0$, then M has finite length by Lemma 6.22. In particular, it must be finite dimensional as a k-vector space, so only finitely many graded pieces can be nonzero. So for $t \gg 0$, $H_M(t) = 0$, which is a polynomial of degree -1, by our convention.

Now suppose that the theorem holds for every ring R satisfying our hypotheses and for every R-module of dimension $n-1$. Assume M has dimension n, and take a homogeneous prime filtration of M, which we constructed in Theorem 5.28. Say this prime filtration is

$$M = M_m \supsetneq M_{m-1} \supsetneq M_{m-2} \supsetneq \cdots \supsetneq M_1 \supsetneq M_0 = 0$$

with $M_i/M_{i-1} \cong R/\mathfrak{p}_i(d_i)$ for some homogeneous primes $\mathfrak{p}_i$ and integers d_i. This breaks into short exact sequences

$$0 \longrightarrow M_i \longrightarrow M_{i+1} \longrightarrow M_{i+1}/M_i \longrightarrow 0\,.$$

Using Lemma 8.6 inductively on i, we get that $H_M(t) = H_{R/\mathfrak{p}_1(d_1)}(t) + \cdots + H_{R/\mathfrak{p}_m(d_m)}(t)$. Observe that $H_{R/\mathfrak{p}_i(d_i)}(t) = H_{R/\mathfrak{p}_i}(t + d_i)$ for each i. Since the associated primes of M are contained in $V(\operatorname{ann}_R(M))$, we have $\dim(R/\mathfrak{p}_i) \leqslant \dim(M)$. Moreover, there must be some $\mathfrak{p}_i$ for which equality occurs, since every associated prime of M occurs among the $\mathfrak{p}_i$, so in particular all the minimal primes of $\operatorname{ann}_R(M)$ are among the $\mathfrak{p}_i$. If we can show that each module of the form $R/\mathfrak{p}_i$ verifies the conclusion of the theorem, then we

[2] Recall that the dimension of a module M is the dimension of $R/\operatorname{ann}_R(M)$.

are done: all of the claims of polynomiality, degree, and positivity of leading term pass to $H_M(t)$ by the equality above, as the shifting does not change degree or the leading term, $\dim(M) = \max\{\dim(R/\mathfrak{p}_i)\}$, and the leading term satisfies the hypotheses again.

If $M = R/\mathfrak{p}_i$, then take a homogeneous Noether normalization A for this k-algebra M, and consider a homogeneous prime filtration for M as an A-module. Every factor is either a shift of A, or else has dimension less than $a := \dim(A) = \dim(M)$, since A is a domain. Applying the induction hypothesis and the formula

$$H_M(t) = H_{R/\mathfrak{p}_1(d_1)}(t) + \cdots + H_{R/\mathfrak{p}_m(d_m)}(t)$$

from above to this context, we find that $H_M(t)$ is a sum of shifts of the polynomial $P_a(t)$ from Example 8.4, plus polynomials of lower degree. Notice that

$$P_a(t) = \frac{(t+a-1)(t+a-2)\cdots(t+1)}{(a-1)!} = \frac{1}{(a-1)!}t^{a-1} + \text{ lower degree terms.}$$

Thus, the claims hold for M. □

Definition 8.9. The **Hilbert polynomial** of a graded module is the polynomial $P_M(t)$ that agrees with $H_M(t)$ for $t \gg 0$. The **multiplicity** of an R-module $M \neq 0$ is the positive integer $e(M)$ such that

$$P_M(t) = \frac{e(M)}{(\dim(M)-1)!}t^{\dim(M)-1} + \text{ lower order terms.}$$

Example 8.10. The multiplicity of a standard graded ring is $e(k[x_1, \ldots, x_n]) = 1$.

Proposition 8.11. *Let k be a field, and R be a finitely graded k-algebra such that $R_0 = k$ and R is generated by elements of degree one. Let*

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

be a short exact sequence of graded R-modules. Then $P_M(t) = P_L(t) + P_N(t)$. If $\dim(L) = \dim(M) = \dim(N)$, then $e(M) = e(L) + e(N)$.

Proof. Both claims follow immediately from the fact that Hilbert functions are additive on short exact sequences, Lemma 8.6. □

Example 8.12. If R is a polynomial ring, then $e(R) = 1$. If $R = S/fS$ for a polynomial ring S and a homogeneous element f of degree d, then $e(R) = d$.

Example 8.13. If $k[x_1, \ldots, x_n]$ is a standard $\mathbb{N}$-graded ring and f is a homogeneous element of degree d, then $R = k[x_1, \ldots, x_n]/(f)$ satisfies $e(R) = d$. We can compute this using Example 8.7.

We can use Theorem 8.8 something about the Hilbert series as well, thanks to the following lemma.

Lemma 8.14. *Let $\phi\colon \mathbb{N} \to \mathbb{N}$, and consider its generating function $g(z) = \sum_{i=0}^{\infty} \phi(i) z^i$. The following are equivalent:*

a) there is a polynomial $P \in \mathbb{Q}[t]$ of degree $d-1$ such that $\phi(n) = P(n)$ for $n \gg 0$

b) $g(z) = \dfrac{q(z)}{(1-z)^d}$ for some $q \in \mathbb{Z}[z]$ such that $q(1) \neq 0$ and $d \geqslant 0$.

Proof sketch. Use the "negative binomial" formula

$$\frac{1}{(1-z)^d} = \sum_{i=0}^{\infty} \binom{i+d-1}{d-1} z^i. \qquad \square$$

Corollary 8.15. *Let k be a field, and R be a finitely graded k-algebra such that $R_0 = k$ and R is generated by elements of degree one. Let M be a finitely generated graded R-module. Then the Hilbert series of M is of the form*

$$h_M(z) = \frac{q(z)}{(1-z)^d},$$

for some $q \in \mathbb{Z}[z]$, where $d = \dim(M)$.

Proof. Immediate from Theorem 8.8 and Lemma 8.14. $\square$

We have now given many different characterizations for the dimension for a finitely generated graded k-algebra. Here's a summary:

Theorem 8.16 (The dimension theorem - graded version)**.** *Let K be a field, and R be a finitely generated graded K-algebra such that $R_0 = K$ and R is generated by elements of degree one i.e. $R = R_0[R_1]$. The following numbers are equal:*

a) The Krull dimension of R.

b) The smallest d such that $\sqrt{(x_1, \ldots, x_d)} = R_+$ for some homogeneous $x_1, \ldots, x_d$.

c) $1 + \deg(P_R)$, where P_R is the Hilbert polynomial of R.

d) The order of pole of the Hilbert series of R at 1, that is, the number d such that $h_R(z) = \frac{q(z)}{(1-z)^d}$ and this fraction is in lowest terms, i.e. $q(1) \neq 0$.

Finally, we also want to consider the case when the ring is not necessarily generated in degree one. The key fact we will need is the following:

Exercise 21. Let k be a field, and R be a finitely generated positively graded k-algebra with $R_0 = k$. There is some $d \in \mathbb{N}$ such that the subring $R^{(d)} = \bigoplus_{i \geqslant 0} R_{id}$ is generated as a k-algebra by R_d.

The Hilbert function of a non-standard graded k-algebra is no longer eventually a polynomial. But it is eventually a *quasipolynomial*.

Definition 8.17. A function $f\colon \mathbb{Z} \longrightarrow \mathbb{R}$ is a **quasipolynomial** if there exists an integer b and polynomials $p_0, \ldots, p_{b-1} \in \mathbb{R}[t]$ such that $f(n) = p_c(n)$ for $c \equiv n \bmod b$ for each $n \in \mathbb{Z}$.

So a quasipolynomial alternates between various polynomials.

Theorem 8.18. *Let k be a field, and R be a finitely graded k-algebra such that $R_0 = k$. Let M be a finitely generated graded R-module. Then there is a quasipolynomial with rational coefficients $P_M(t)$ such that $H_M(t) = P_M(t)$ for $t \gg 0$.*

Proof. Let d be such that $R^{(d)}$ is generated by R_d, which exists by Exercise 21. We can think of $R^{(d)}$ as a standard graded k-algebra, where we consider the elements of R_{id} to have degree i. Since R is finitely generated as a k-algebra, it is also a finitely generated $R^{(d)}$-algebra. Moreover, any homogeneous element $x \in R$ satisfies a monic equation of the form $t^d - x^d \in R^{(d)}[t]$, so R is integral over $R^{(d)}$. By Corollary 1.37, R is module-finite over $R^{(d)}$. So M is a finitely generated $R^{(d)}$-module. However, its grading over R is not consistent with the grading of $R^{(d)}$. We can decompose M as an $R^{(d)}$-module as

$$M = N_0 \oplus N_1 \oplus \cdots \oplus N_{d-1}, \quad \text{where } N_j = \bigoplus_{i \in \mathbb{N}} M_{j+id}.$$

Set $[N_j]_i := M_{j+id}$. This gives us a grading on each N_j that is compatible with $R^{(d)}$. Note also that each N_j is a submodule of a finitely generated module over a Noetherian ring, so is also finitely generated. Therefore, each N_j admits its own Hilbert polynomial. Taking each of these, we obtain a quasipolynomial that agrees with the Hilbert function for large values. □

One can then show (see [Mat89, Theorem 13.2]) that the Hilbert series of a finitely generated graded module over a non-standard graded k-algebra with $R_0 = k$ is of the form

$$\frac{q(t)}{(1-t)^{d_1} \cdots (1-t)^{d_n}},$$

where the integers d_i are the degrees of the algebra generators of R.

8.2 Associated graded rings and Hilbert functions for local rings

We next wish to give a version of the dimension theorem from the previous section in the local case. For this, we need a notion of Hilbert function that applies to local rings. We get this by associating a graded ring to each local ring.

Definition 8.19. The **associated graded ring** of an ideal I in a ring R is the ring

$$\mathrm{gr}_I(R) := \bigoplus_{n\geqslant 0} I^n/I^{n+1}$$

with n-th graded piece I^n/I^{n+1} and multiplication

$$(a+I^{n+1})(b+I^{m+1}) = ab + I^{m+n+1} \text{ for } a\in I^n,\ b\in I^m.$$

If $(R,\mathfrak{m})$ is local, then $\mathrm{gr}(R) := \mathrm{gr}_{\mathfrak{m}}(R)$ will be called the associated graded ring of R.

Note that the multiplication is well-defined.

Remark 8.20. If $a\in I^n$, $b\in I^m$, $u\in I^{n+1}$, $v\in I^{m+1}$, that is, $a+u\in a+I^{n+1}$ and $b+v\in b+I^{m+1}$ then

$$(a+u)(b+v) = ab = av+bu+uv \in ab + I^{m+n+1}.$$

So the multiplication on the associated graded ring is indeed well-defined.

Remark 8.21.

a) $[\mathrm{gr}_I(R)]_0 = R/I$, so if $(R,\mathfrak{m},k)$ is local then $[\mathrm{gr}(R)]_0 = R/\mathfrak{m} = k$.

b) Each graded piece $[\mathrm{gr}(R)]_n = I^n/I^{n+1}$ is an R-module annihilated by I, so it is an R/I-module. If $(R,\mathfrak{m},k)$ is local then $[\mathrm{gr}(R)]_n$ is a k-vector space.

c) Let R be Noetherian and $I=(f_1,\ldots,f_n)$. Then $f_1+I^2,\ldots,f_n+I^2\in[\mathrm{gr}_I(R)]_1$ and $\mathrm{gr}_I(R) = (R/I)[f_1,\ldots,f_n]$ is finitely generated as a $[\mathrm{gr}(R)]_0$-algebra by elements of degree one. If $(R,\mathfrak{m},k)$ is Noetherian and local, then by NAK Proposition 4.32 a basis for $[\mathrm{gr}(R)]_n$ corresponds to a minimal set of generators for $\mathfrak{m}^n$, and in particular $\dim_k[\mathrm{gr}(R)]_n = \mu(\mathfrak{m}^n) < \infty$.

Example 8.22. Take $R=k[x,y]$ and $I=(x,y)$. Then

$$\mathrm{gr}_I(R) = R/I \oplus I/I^2 \oplus I^2/I^3 \oplus \cdots = k \oplus (k\,x \oplus k\,y) \oplus (k\,x^2 \oplus k\,xy \oplus k\,y^2) \oplus \cdots$$

so we see that in fact $\mathrm{gr}_{(x,y)}(k[x,y]) = k[x,y]$. Similarly, for any graded k-algebra generated in degree 1, $\mathrm{gr}_{R_+}(R) = R$.

Example 8.23. Let $R = k[x,y]_{(x,y)}$.

a) Let $I=(x,y)$. The same computation as above applies to show

$$\mathrm{gr}_{(x,y)}\, k[x,y]_{(x,y)} = k[x,y].$$

b) Now take $I=(x^2,y^2)$. Then

$$\mathrm{gr}_I(R) = R/I \oplus (x^2R/I \oplus y^2R/I) \oplus (x^2R/I \oplus x^2y^2R/I \oplus y^2R/I) \oplus \cdots$$

so we get

$$\mathrm{gr}_I(R) = (R/I)[x^2,y^2]$$

with $\deg(x^2) = \deg(y^2) = 1$ and $\deg(r+I) = 0$ for all $r\in R$. In this case the R/I-algebra generators for $\mathrm{gr}_I(R)$ are algebraically independent.

c) Finally take $I = (x^2, xy)$. Then

$$\mathrm{gr}_I(R) = (R/I)[x^2, xy],$$

with $\deg(x^2) = \deg(xy) = 1$ and $\deg(r + I) = 0$ for all $r \in R$. However, in this case the algebra generators x^2, xy are not algebraically independent over R/I. For example, $\overline{y}x^2 - \overline{x}xy = 0$.

Definition 8.24. Let $(R, \mathfrak{m})$ be a local ring. The **Hilbert function** of R is

$$H_R(t) := H_{\mathrm{gr}(R)}(t).$$

and **Hilbert series** of R is

$$h_R(t) := h_{\mathrm{gr}(R)}(t).$$

Example 8.25. When $R = k[x, y]_{(x,y)}$,

$$H_R(t) = H_{k[x,y]}(t) = t + 1.$$

More generally, if $R = k[x_1, \ldots, x_n]_{(x_1,\ldots,x_n)}$ then

$$H_R(t) = H_{k[x_1,\ldots,x_n]}(t) = P_n(t)$$

as in Example 8.4.

To get a completely satisfactory analogue of the Hilbert function theory in this setting, we would like to understand the dimension of the associated graded ring. To understand this, we use the following related object.

Definition 8.26. Let R be a ring, and I an ideal. Recall that the **Rees algebra** of I is the $\mathbb{N}$-graded ring

$$R[It] = \bigoplus_{n \geqslant 1} I^n t^n = R \oplus It \oplus I^2t^2 \oplus \cdots \subseteq R[t],$$

The **extended Rees algebra** of I is the $\mathbb{Z}$-graded ring

$$R[It, t^{-1}] = \cdots \oplus Rt^{-2} \oplus Rt^{-1} \oplus R \oplus It \oplus I^2t^2 \oplus \cdots . \subseteq R[t, t^{-1}].$$

In both cases, the grading is given by setting $\deg t = 1$, and $\deg r = 0$ for all $r \in R$.

Note that $t \notin R[It, t^{-1}]$ since $1 \notin I$, so t^{-1} is not a unit, even though it looks like one.

Example 8.27. If $R = k[x, y]$ and $I = (x^2, y^2)$ then $R[It, t^{-1}] = R[x^2t, y^2t, t^{-1}]$. Think about t as being a constant which is allowed to vary in k. Then the extended Rees algebra of I can be viewed as a family of R-algebras, one for each value of t^{-1}. Let's explore some of the algebras in this family by plugging in values for t^{-1}:

- if $t^{-1} = 0$, which is ok to do since t^{-1} is not actually a unit, then we get

$$R[It, t^{-1}]|_{t^{-1}=0} = R[x^2t, y^2t] \cong \mathrm{gr}_I[t].$$

- If $t^{-1} = 1$ then we get $x^2t = x^2t \cdot 1 = x^2tt^{-1} = x^2 \in R$ and similarly $y^2t = y^2 \in R$ so

$$R[It, t^{-1}]|_{t^{-1}=1} = R[x_R^2, y_R^2] \cong R.$$

  In fact the same is true for every value $t^{-1} \in k^\times$.

The following lemma makes these observations rigorous.

Lemma 8.28. *There are isomorphisms*

$$R[It, t^{-1}]/(t^{-1}) \cong \mathrm{gr}_I(R) \qquad \text{and} \qquad R[It, t^{-1}]/(t^{-1} - 1) \cong R.$$

Proof. For the first isomorphism, since t is homogeneous, we can use the graded structure. We have

$$t^{-1}R[It, t^{-1}] = \cdots \oplus Rt^{-2} \oplus Rt^{-1} \oplus I \oplus I^2t \oplus I^3t^2 \oplus \cdots,$$

so matching the graded pieces, we see that

$$R[It, t^{-1}]/(t^{-1}) = \frac{\cdots \oplus Rt^{-2} \oplus Rt^{-1} \oplus R \oplus It \oplus I^2t^2 \oplus \cdots}{\cdots \oplus Rt^{-2} \oplus Rt^{-1} \oplus I \oplus I^2t \oplus I^3t^2 \oplus \cdots}$$

$$\begin{aligned} &\cong R/I \oplus I/I^2 \oplus I^2/I^3 \oplus \cdots \\ &= \mathrm{gr}_I(R). \end{aligned}$$

For the second isomorphism, we consider the map $R[It, t^{-1}] \longrightarrow R$ given by sending $t \mapsto 1$. This is surjective, and the kernel is the set of elements $a_mt^m + \cdots + a_nt^n$ such that $a_m + \cdots + a_n = 0$. We claim that this ideal is generated by $(t^{-1} - 1)$. We proceed by induction on $n - m$. The case $n - m = 0$ corresponds to there being at most one nonzero term, say at^m, in which case at^m is in the kernel if and only if $a = 0$. In $n - m = 1$, we have an element of the form $at^{n-1} - at^n$ for some a, which is of the form $(at^n)(t^{-1} - 1)$. For the inductive step, if $a_m + \cdots + a_n = 0$, write

$$a_mt^m + \cdots + a_nt^n = (a_mt^m + \cdots + (a_{n-1} + a_n)t^{n-1}) + (-a_nt^{n-1} + a_nt^n).$$

Observe that $-a_nt^{n-1}+a_nt^n \mapsto -a_n+a_n = 0$, and thus $a_mt^m+\cdots+(a_{n-1}+a_n)t^{n-1}$ must also be in the kernel. The induction hypothesis now applies to both $-a_nt^{n-1} + a_nt^n$ and $a_mt^m + \cdots + (a_{n-1} + a_n)t^{n-1}$, which must then be in $(t^{-1} - 1)$. Therefore, so is $a_mt^m + \cdots + a_nt^n$, and we are done. □

Lemma 8.29. *Let R be a Noetherian ring, and I an ideal in R. The minimal primes of $R[It, t^{-1}]$ are exactly the primes of the form $\mathfrak{p}R[t, t^{-1}] \cap R[It, t^{-1}]$ for $\mathfrak{p} \in \mathrm{Min}(R)$.*

Proof. Let $(0) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$ be a minimal primary decomposition of (0) in R, and $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$. One can check (exercise!) that $\mathfrak{q}_i R[t]$ is primary with radical $\mathfrak{p}_i R[t]$. Then the same is true in $R[t, t^{-1}]$, by localizing at $\{1, t, t^2, \ldots\}$. Contracting to $R[It, t^{-1}]$, we get primary ideals that intersect to (0); none is contained in the intersection of the others, since this is the case after contracting to R, and likewise the radicals are distinct since they contract to different primes in R.

Therefore, setting $\mathfrak{q}_i' = \mathfrak{q}_i R[t, t^{-1}] \cap R[It, t^{-1}]$, $\mathfrak{q}_1' \cap \cdots \cap \mathfrak{q}_t'$ is a minimal primary decomposition of (0) in $R[It, t^{-1}]$, and thus the minimal primes in $R[It, t^{-1}]$ are $\mathfrak{p}_i R[t, t^{-1}] \cap R[It, t^{-1}]$ □

Theorem 8.30. *Let $(R, \mathfrak{m})$ be a Noetherian local ring, and $I \subseteq \mathfrak{m}$ an ideal. Then*

$$\dim(R) = \dim(R[It, t^{-1}]) - 1 = \dim(\mathrm{gr}_I(R)).$$

Proof. First, let's show $\dim(R) = \dim(R[It, t^{-1}]) - 1$. By Lemma 8.29, we can reduce to the case when R is a domain by localizing at each of the minimal primes of R. In particular, $R[It, t^{-1}]$ is also a domain.

By Lemma 8.28, $R[It, t^{-1}]/(t^{-1} - 1) \cong R$, so $\dim(R[It, t^{-1}]) \geqslant \dim(R)$. Also, since $(t^{-1} - 1)$ is principal, $\mathrm{ht}(t^{-1} - 1) \leqslant 1$, by Theorem 6.32. But $R[It, t^{-1}]$ is a domain, so $\mathrm{ht}(t^{-1} - 1) = 1$. By Corollary 7.31,

$$\dim R = \dim(R[It, t^{-1}]) - \mathrm{ht}(t^{-1} - 1) = \dim(R[It, t^{-1}]) - 1.$$

Now, we claim that

$$Q = \cdots \oplus Rt^{-2} \oplus Rt^{-1} \oplus \mathfrak{m} \oplus It \oplus I^2t^2 \oplus \cdots = (\mathfrak{m}, It, t^{-1})R[It, t^{-1}]$$

is a maximal ideal of height $\dim(R) + 1$ in $R[It, t^{-1}]$. The quotient ring is $R/\mathfrak{m}$, so it is clearly maximal. Given a chain $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_h = \mathfrak{m}$ of length $h = \dim(R)$, let $\mathfrak{q}_i = \mathfrak{p}_i R[t, t^{-1}] \cap R[It, t^{-1}]$. Since $\mathfrak{q}_i \cap R = \mathfrak{p}_i[t, t^{-1}] \cap R = \mathfrak{p}_i$, this is a proper chain of primes in $R[It, t^{-1}]$. We have

$$\mathfrak{q}_h = \cdots \oplus \mathfrak{m}t^{-2} \oplus \mathfrak{m}t^{-1} \oplus \mathfrak{m} \oplus It \oplus I^2t^2 \oplus \cdots = (\mathfrak{m}, It)R[It, t^{-1}] \subsetneq Q$$

so the height of Q is at least $\dim(R) + 1$, and hence equal to $\dim(R) + 1$ using the previous upper bound on the dimension.

For the last equality, since t^{-1} is a nonzerodivisor on $R[It, t^{-1}]$, we have

$$\dim(\mathrm{gr}_I(R)) \leqslant \dim(R[It, t^{-1}]) - 1.$$

For the other inequality, let $\overline{Q} = Q/(t^{-1})$. Then

$$\begin{aligned} \dim(\mathrm{gr}_I(R)) &\geqslant \dim(\mathrm{gr}_I(R)_{\overline{Q}}) = \dim(R[It, t^{-1}]_Q/(t^{-1})) \\ &\geqslant \dim(R[It, t^{-1}]_Q) - 1 \\ &= \mathrm{height}(Q) - 1 \\ &= \dim(R). \end{aligned}$$

□

Theorem 8.31. . *Let $(R, \mathfrak{m}, k)$ be a local ring. Then there is a polynomial $P_R(t) \in \mathbb{Q}[t]$ of degree equal to $\dim(R) - 1$ such that $H_R(t) = P_R(t)$ for $t \gg 0$. Moreover, if $\dim(R) > 0$ then*

$$P + R(t) = \frac{e}{(\dim(R) - 1)!} t^{\dim(R)-1} + \text{ lower order terms.}$$

.

Proof. Because $H_R(t) = H_{\mathrm{gr}(R)}(t)$, we already know by Theorem 8.8 that $H_R(t)$ is eventually equal to a polynomial of degree $\dim(\mathrm{gr}(R)) - 1$ and that $(\dim(\mathrm{gr}(R)) - 1)!$ times the leading coefficient is positive. So the theorem follows as long as $\dim(R) = \dim(\mathrm{gr}(R)))$. □

Definition 8.32. The **Hilbert polynomial** of a local ring R is the polynomial $P_R(t)$ that agrees with $H_R(t)$ for $t \gg 0$. The **multiplicity** of R is the positive integer $e(R)$ such that

$$P_R(t) = \frac{e(R)}{(\dim(R) - 1)!} t^{\dim(M)-1} + \text{ lower order terms.}$$

This gives an analogue of the dimension theorem in the local case:

Theorem 8.33 (The dimension theorem — local version)**.** *Let $(R, \mathfrak{m}, k)$ be a Noetherian ring. The following numbers are equal:*

a) the Krull dimension of R.

b) the smallest number d so that $x_1, \ldots, x_d$ is a system of parameters for R, that is $\sqrt{x_1, \ldots, x_d} = R_+$.

c) $1 + \deg(P_R)$, where P_R is the Hilbert polynomial of R (and $\mathrm{gr}(R)$).

d) The order of pole of the Hilbert series of R (really, of $\mathrm{gr}(R)$) at 1, that is, the number d such that

$$h_R(z) = \frac{q(z)}{(1 - z)^d}$$

and this fraction is in lowest terms with $q(1) \neq 0$.

Part II

Homological Algebra

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. Lines indicated with as in, where n is some integer, are input lines, whereas lines with an on indicate output lines.

We can now do all sorts of computations over our ring R. We can define ideals in R, and use them to either define a quotient ring S of R or an R-module M, as follows:

```
i3 : I = ideal(x^2,y^2,x*y)

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

o3 : Ideal of R

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

$$R^3 \xrightarrow{\begin{bmatrix} x^2 & y^2 & xy \end{bmatrix}} R\,.$$

Note also that there is an alternative syntax to write our ideal I from above, as follows:

```
i15 : I = ideal"x2,xy,y2"

               2        2
o15 = ideal (x , x*y, y )

o15 : Ideal of 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 S`.

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 2nd 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:

```
i11 : U = k[a,b,c]

o11 = U

o11 : PolynomialRing

i12 : f = map(R,U,{x^2,x*y,y^2})
                2        2
o12 = map(R,U,{x , x*y, y })

o12 : RingMap R <--- U

i13 : J = ker f

             2
o13 = ideal(b  - a*c)
```

```
o13 : Ideal of U

i14 : T = U/J

o14 = T

o14 : QuotientRing
```

Our ring T at the end is isomorphic to the 2nd Veronese of R, which is the ring we wanted.

A.2 Basic commands

Many Macaulay2 commands are easy to guess, and named exactly what you would expect them to be named. If you are not sure how to use a certain command, you can run `viewHelp` followed by the command you want to ask about; this will open an html file with the documentation for the method you asked about. Often, googling "Macaulay2" followed by 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.
- `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

$$A = \begin{pmatrix} a_{1,1} & \ldots & a_{1,n} \\ & \ddots & \\ a_{m,1} & \ldots & a_{m,n} \end{pmatrix}$$

Index

Bibliography

[AM69] Michael F. Atiyah and Ian G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[DF04] David S. Dummit and Richard M. Foote. *Abstract algebra*. Wiley, 3rd ed edition, 2004.

[DSGJ] Alessandro De Stefani, Eloísa Grifo, and Jack Jeffries. A Zariski-Nagata theorem for smooth $\mathbb{Z}$-algebras. *To appear in J. Reine Angew. Math.*

[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.

[Eis95] David Eisenbud. *Commutative algebra with a view toward algebraic geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[FMS14] Christopher A Francisco, Jeffrey Mermin, and Jay Schweig. A survey of stanley–reisner theory. In *Connections Between Algebra, Combinatorics, and Geometry*, pages 209–234. Springer, 2014.

[Kun69] Ernst Kunz. Characterizations of regular local rings for characteristic p. *Amer. J. Math.*, 91:772–784, 1969.

[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.

[Nag62] Masayoshi Nagata. *Local rings*. Interscience, 1962.

[NM91] Luis Narváez-Macarro. A note on the behaviour under a ground field extension of quasicoefficient fields. *J. London Math. Soc. (2)*, 43(1):12–22, 1991.

[Noe21] Emmy Noether. Idealtheorie in ringbereichen. *Mathematische Annalen*, 83(1):24–66, 1921.

[Poo19] Bjorn Poonen. Why all rings should have a 1. *Mathematics Magazine*, 92(1):58–62, 2019.

[Rot09] Joseph J. Rotman. *An introduction to homological algebra*. Universitext. Springer, New York, second edition, 2009.

[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.