Commutative Algebra 1

Math 905 Fall 2022

Eloísa Grifo
University of Nebraska-Lincoln

November 6, 2023

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, I strongly recommend the following excellent resources:

- Mel Hochster's Lecture notes
- Jack Jeffries' Lecture notes (either his notes from UMich 614, CIMAT, or UNL)
- 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]

Acknowledgements

These notes have evolved from the notes I wrote for my commutative algebra class at the University of California, Riverside, in Winter 2021, which were in turn heavily based on Jack Jeffries and Alexandra Seceleanu's notes. I am very thankful to Jack and Alexandra for sharing their notes with me. I am also deeply thankful to all the students who have found typos and asked questions that lead to many improvements: Brandon Massaro, Rahul Rajkumar, Adam Richardson, Khoa Ta, Ryan Watson, Noble Williamson, Jordan Barrett, Julie Geraci, Sabrina Klement, Sam Macdonald, Jorge Gaspar Lara, Mikkel Munkholm, Robert Thompson, Sara Mueller, Shalom Echalaz Alvarez.

Contents

Chapter 0

Setting the stage

Here are some elementary definitions and facts we will assume you have already seen before. For more details, see any introductory algebra book, such as [DF04].

0.1 Basic definitions: rings and ideals

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, or 0_R if we need to specify which ring we are talking about. 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_R or simply 1. 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
   - there exists an element $1 \in R$ such that $1 \cdot a = a \cdot 1$ for all $a \in R$.

   We typically write ab for $a \cdot b$.
3) multiplication is distributive with respect to addition, meaning that for all $a, b, c \in R$ we have
$$a \cdot (b + c) = a \cdot b + a \cdot c.$$
4) $1 \neq 0$.

In this class, **all rings are commutative**. In other branches of algebra rings might fail to be commutative, but we will explicitly say *noncommutative ring* if that is the case. There also branches of algebra where rings are allowed to not 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 $\mathbb{Z}$, or any quotient of $\mathbb{Z}$, which we write compactly as $\mathbb{Z}/n$.

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

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

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

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

f) 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)**.** Given rings R and S, a function $R \xrightarrow{f} S$ 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,

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

Example 0.6. Every ring has always at least two 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 an 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**.

Definition 0.7. 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 $(f) = \{fg \mid g \in R\}$.

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 0.8. The ring $\mathbb{Z}[x]$ is a domain but **not** a PID. For example, $(2, x)$ is not principal.

Theorem 0.9 (CRT)**.** *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*

$$\begin{aligned} R/I &\xrightarrow{\cong} R/I_1 \times \cdots \times R/I_n \ . \\ r + I &\longmapsto (r + I_1, \ldots, r + I_n) \end{aligned}$$

0.2 Basic definitions: modules

Just like linear algebra is the study of vector spaces over fields, commutative algebra often focuses on the structure of modules over commutative rings. While in other branches of algebra modules might be left- or right-modules, our modules are usually two sided, and we refer to them simply as modules.

Definition 0.10 (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 $r \cdot a$, and 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 0.11. If $N \subseteq M$ are R-modules with compatible structures, we say that N 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 module** M/N is an R-module whose elements are the equivalence classes under 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 0.12. The modules over a field k are precisely all the k-vector spaces. Linear transformations are precisely all the k-module maps.

Example 0.13. The $\mathbb{Z}$-modules are precisely all the abelian groups.

Example 0.14. 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 0.15 (First Isomorphism Theorem)**.** *If $M \xrightarrow{f} N$ is a homomorphism of R-modules, then $M/\ker f \cong \operatorname{im} f$.*

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

Chapter 1

Finiteness conditions

We start our study of commutative algebra by discussing modules and algebras, the most important structures over a given ring. We will discuss module-finite versus algebra-finite ring extensions, the relationship between the two concepts, and how they relate to integral extensions. We will then be ready to discuss noetherian rings; most of the rings we will be interested in are noetherian, as it often happens in commutative algebra.

1.1 Modules

In many ways, commutative algebra is the study of finitely generated modules. While vector spaces make for a great first example of modules, 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. The first big noticeable difference between vector spaces and general modules is that while every vector space has a basis, most modules do not.

Definition 1.1. Let M be an R-module and $\Gamma \subseteq M$. The **submodule** of M **generated by** Γ, denoted $\sum_{m \in \Gamma} Rm$, is the smallest (with respect to containment) submodule of M containing Γ. We say Γ **generates** M, or is a **set of generators** for M, if $\sum_{m \in \Gamma} Rm = M$, meaning that every element in M can be written as a finite linear combination of elements in Γ. 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.

Example 1.2. Every vector space over a field k is a free k-module.

Remark 1.3. Every free R-module is isomorphic to a direct sum of copies of R. To construct such an isomorphism for the free R-module M, take a basis $\Gamma = \{\gamma_i\}_{i \in I}$ for M and let

$$\begin{aligned} \oplus_{i \in I} R &\xrightarrow{\pi} M \\ (r_i)_{i \in I} &\longrightarrow \sum_i r_i \gamma_i. \end{aligned}$$

The condition that Γ is a basis for M is equivalent to π being 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 write a **presentation**

$$\begin{aligned} \oplus_{i\in I} R &\xrightarrow{\pi} M \\ (r_i)_{i\in I} &\longrightarrow \sum_i r_i\gamma_i. \end{aligned}$$

for M, but in general 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 1.4. A homomorphism of R-modules $M \longrightarrow N$ is completely determined by the images of the elements on any given set of generators for M.

Lemma 1.5. *The following are equivalent:*

1) Γ *generates* M *as an* R*-module.*

2) Every element of M *can be written as a finite linear combination of the elements of* Γ *with coefficients in* R*.*

3) The homomorphism $\theta\colon R^{\oplus Y} \to M$*, where* $R^{\oplus Y}$ *is a free* R*-module with basis* Y *in bijection with* Γ *via* $\theta(y_i) = \gamma_i$*, is surjective.*

Remark 1.6. The equivalence between 1) and 2) in Lemma 1.5 says that the submodule generated by Γ is exactly the set of all finite linear combinations of elements in Γ with coefficients in R, which explains the notation $\sum_{m\in\Gamma} Rm$.

Definition 1.7. We say that a module M is **finitely generated** if we can find a finite generating set for M.

A better name might be *finitely generatable*, since we do not need to know an actual finite set of generators to say that a module is finitely generated. The simplest finitely generated modules are the cyclic modules.

Example 1.8. 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 $R/I \cong M$.

Remark 1.9. More generally, 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. More precisely, if M is generated by $m_1, \dots, m_n \in M$, then the homomorphism of R-modules

$$\begin{aligned} R^n &\xrightarrow{\quad\pi\quad} M \\ (r_1, \dots, r_n) &\longrightarrow r_1m_1 + \cdots + r_nm_n \end{aligned}$$

that sends each of the canonical generators e_i of R^n to m_i is surjective; more precisely, this is a presentation for M. By the First Isomorphism Theorem, $M \cong R^n/\ker\pi$.

Macaulay2. Defining free modules in Macaulay2 is easy:

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

i2 : M = R^3
       3
o2 = R

o2 : R-module, free
```

Note that from now on and until we reset Macaulay2, whenever you write `R` it will be read as a ring, not a module; if instead you want to refer to the module R, you can write it as `R^1`. Alternatively, you can also use the command `module` and write `module R`. If you do calculations that require a module and not a ring, it is important to be careful about whether you write `R` or `R^1`; this is an easy way to get an error message.

If we want to define a module that happens to be an ideal, but we want to think about it as a module, we can simply use the command `module` to turn the ideal into a module:

```
i3 : I = ideal"xy,yz"

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

o3 : Ideal of R

i4 : N = module I

o4 = image | xy yz |
                                      1
o4 : R-module, submodule of R
```

If we forget that this is actually an ideal, and simply think about as a submodule of the module R, we can also view this module as the image of a map, as we described in Remark 1.9: if a submodule of R^m has n generators, we can view it as the the image of the map $R^n \to R^m$ that sends each of the canonical generators of R^n to the generators we chose for our module. In our example, our module is the image of the following map from R^2 to R:

```
i5 : phi = map(R^1,R^2,{{x*y,y*z}})

o5 = | xy yz |
                  1       2
o5 : Matrix R  <--- R

i6 : L = image phi

o6 = image | xy yz |
                                      1
o6 : R-module, submodule of R
```

Note that above, when we first defined the module N, Macaulay2 immediately stored that information in this exact way, as the image of the same map we just defined. This is useful to keep in mind when you see the results for a computation: if a module is given to us as the image of a matrix, then we are being told that our module is a submodule of some free module. If the matrix has n rows, then that means our module is a submodule of R^n. Each column corresponds to a generator of our module (as a submodule of R^n).

Of course that the modules M, N, and L we have defined are all the same module: the ideal (xy, yz). It is our job to know that; depending on how you ask the question, Macaulay2 might not be able to identify this. Finally, we can also describe this module by saying that it has two generators, say f and g, and there is a unique relation between them:

$$-zf + yg = 0.$$

This means that our module is the quotient of R^2 by the submodule generated by the relation $(-z, y)$. We can write this as the quotient of R^2 by the image of a map landing in R^2, meaning it is the cokernel of a map.

```
i7 : psi = map(R^2,R^1,{{-z},{y}})

o7 = | -z |
     | y  |

                2       1
o7 : Matrix R  <--- R

i8 : K = coker psi

o8 = cokernel | -z |
              | y  |

                             2
o8 : R-module, quotient of R
```

When a module is given to us in this format, as the cokernel of some matrix, we are essentially being given a presentation: the number of rows is the number of generators, while each column corresponds to a relation among those generators. If one the vector $(r_1, \ldots, r_n)$ appears in a column of the matrix, that means that the generators $m_1, \ldots, m_n$ satisfy the relation

$$r_1 m_1 + \cdots + r_n m_n = 0.$$

Keep in mind that when you do a calculation and the result is a module given to you in this format, Macaulay2 will not necessarily respond with a *minimal* presentation: one of the generators given might actually be a linear combination of the remaining ones, so there might be more generators than necessary, and there might be superfluous relations which follow as linear combinations of the others. You might be able to get rid of some superfluous generators and relations using the command `prune`. We will discuss this in more detail when we talk about local rings.

1.2 Algebras

Definition 1.10 (Algebra)**.** Given a ring R, an R-**algebra** is a ring S equipped with a ring homomorphism $\phi : R \to S$. This defines an R-module structure on S given by **restriction of scalars**: for each $r \in R$ and $s \in S$, $rs := \phi(r)s$. This R-module structure on S is compatible with the internal multiplication of S i.e.,

$$r(st) = (rs)t = s(rt) \text{ for all } r \in R, s, t \in S.$$

We will call ϕ the **structure homomorphism** of the R-algebra S.

Example 1.11.

1) If A is a ring and $x_1, \dots, x_n$ are indeterminates, the inclusion map $A \hookrightarrow A[x_1, \dots, x_n]$ makes the polynomial ring into an A-algebra.

2) More generally, any inclusion map $R \subseteq S$ gives S an R-algebra structure. In this case the R-module multiplication coincides with the internal (ring) multiplication on S.

3) Any ring comes with a unique structure as a $\mathbb{Z}$-algebra, since there is a unique ring homomorphism $\mathbb{Z} \to R$: the one given by $n \mapsto n \cdot 1_R$.

Definition 1.12 (algebra generation)**.** Let S be an R-algebra with structure homomorphism φ and let $\Lambda \subseteq S$ be a set. The R-**algebra generated by** a subset Λ of S, denoted $R[\Lambda]$, is the smallest (with respect to containment) subring of S containing Λ and $\varphi(R)$. A set of elements $\Lambda \subseteq S$ **generates** S as an R-algebra if $S = R[\Lambda]$.

Note that there are two different meanings for the notation $R[S]$ for a ring R and set S: one calls for a polynomial ring, and the other calls for a subring of something. If S is a subset of elements of some other larger ring which is clear from context, then we are talking about the algebra generated by S; in contrast, if S is just a set of indeterminates, then we are talking about a polynomial ring in those variables.

This can be unpackaged more concretely in a number of equivalent ways:

Lemma 1.13. *The following are equivalent:*

1) Λ generates S as an R-algebra.

2) Every element in S admits a polynomial expression in Λ with coefficients in $\phi(R)$, i.e.

$$S = \left\{ \sum_{\text{finite}} \phi(r_{i_1,\dots,i_n}) \lambda_1^{i_1} \cdots \lambda_n^{i_n} \mid r_l \in R, \lambda_j \in \Lambda, i_j \geqslant 0 \right\}.$$

3) If $R[X]$ is a polynomial ring on a set of indeterminates X in bijection with Λ, then the R-algebra homomorphism

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

is surjective.

Proof. Let $S = \left\{\sum_{\text{finite}} \phi(a)\lambda_1^{i_1}\cdots\lambda_n^{i_n} \mid a \in A, \lambda_j \in \Lambda, i_j \in \mathbb{N}\right\}$. For the equivalence between 2) and 3), we note that S is the image of π. In particular, S is a subring of R. It then follows from the definition that 1) implies 2). Conversely, any subring of R containing $\phi(A)$ and Λ certainly must contain S, so 2) implies 1). □

Let S be an R-algebra generated by Λ, let π be the surjective map in part 3) of Lemma 1.13, and let $I := \ker \pi$. By the First Isomorphism Theorem, we have a ring isomorphism $S \cong R[X]/I$. The elements of I are the **relations** among the generators in Λ. If we understand the ring R and generators and relations for S over R, we can get a pretty concrete understanding of S.

Note that the homomorphism π need not be injective. If the homomorphism π is injective (and thus an isomorphism) we say that S is a **free algebra**; a free algebra on R is isomorphic to a polynomial ring on R. The ideal $I = \ker(\pi)$ measures how far R is from being a free R-algebra and is called the set of **relations** on Λ.

Example 1.14. You may have seen this used in $\mathbb{Z}[\sqrt{d}]$ for some $d \in \mathbb{Z}$ to describe the ring

$$\{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}.$$

The $\mathbb{Z}$-algebra generated by $\sqrt{d}$ in the most natural place, the algebraic closure of $\mathbb{Q}$, is exactly the set above. The point is that for any power $(\sqrt{d})^n$, we can always write $n = 2q+r$ with $r \in \{0,1\}$, so $(\sqrt{d})^n = d^q(\sqrt{d})^r$ is in the algebra generated by $\mathbb{Z}$ and $\sqrt{d}$.

We can also write the one-generated $\mathbb{Z}$-algebra $\mathbb{Z}[\sqrt{d}]$ as a quotient of a polynomial ring in one variable: if d is not a perfect square, the map π in part 3) of Lemma 1.13 is

$$\begin{aligned} \mathbb{Z}[x] &\xrightarrow{\pi} \mathbb{Z}[\sqrt{d}] \\ x &\longmapsto \sqrt{d} \end{aligned}$$

and its kernel is generated by $x^2 - d$, so $\mathbb{Z}[\sqrt{d}] \cong \mathbb{Z}[x]/(x^2 - d)$.

Similarly, the ring $\mathbb{Z}[\sqrt[3]{d}]$ can be written as

$$\mathbb{Z}[\sqrt[3]{d}] = \{a + b\sqrt[3]{d} + c\sqrt[3]{d^2} \mid a, b, c \in \mathbb{Z}\},$$

which is a quotient of $\mathbb{Z}[x, y]$, and the map π in part 3) of Lemma 1.13 is

$$\begin{aligned} \mathbb{Z}[x,y] &\xrightarrow{\pi} \mathbb{Z}[\sqrt[3]{d}] \\ x &\longmapsto \sqrt[3]{d} \\ y &\longmapsto \sqrt[3]{d^2}. \end{aligned}$$

Macaulay2. Unfortunately, Macaulay2 does not understand subalgebras directly, only quotient rings. But as we have discussed, any R-algebra can be thought of as a quotient of a polynomial ring over R. For example, the Veronese algebra $V = \mathbb{Q}[x^2, xy, xz, y^2, yz, z^2]$ is a quotient of a polynomial ring over $\mathbb{Q}$ in 6 variables, since it has 6 algebra generators. More precisely, V is the image of the map

$$\begin{aligned} \mathbb{Q}[w_1, \ldots, w_6] &\xrightarrow{\quad\pi\quad} R \\ (w_1, \ldots, w_6) &\longmapsto (x^2, xy, xz, y^2, yz, z^2) \end{aligned}$$

so by the First Isomorphism Theorem, $V \cong \mathbb{Q}[w_1, \ldots, w_6]/\ker \pi$.

```
i4 : use R;

i5 : aux = QQ[w_1 .. w_6]

o5 = aux

o5 : PolynomialRing

i6 : p = map(R,aux,{x^2,x*y,x*z,y^2,y*z,z^2})
                    2              2       2
o6 = map (R, aux, {x , x*y, x*z, y , y*z, z })

o6 : RingMap R <--- aux

i7 : V = aux/ker p

o7 = V

o7 : QuotientRing
```

To do calculations with V, note that w_1 is actually x^2, w_2 is xy, and so on.

Definition 1.15. 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 $f_1, \dots, f_t \in S$ that generates S as an R-algebra.

A better name might be *finitely generatable*, since we do not need to know an actual finite set of generators to say that an algebra is finitely generated. 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 $R[x_1, \dots, x_d]$ over R in finitely many variables. If S is generated over R by $f_1, \dots, f_d$, we will use the notation $R[f_1, \dots, f_d]$ 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 R and $\underline{f}$ are understood to be contained in some larger ring.

There are many basic questions about algebra generators that are surprisingly difficult. Let $R = \mathbb{C}[x_1, \dots, x_n]$ and $f_1, \dots, f_n \in R$. When do $f_1, \dots, f_n$ 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!

1.3 Algebra-finite versus module-finite

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. We say S is **module-finite** over R if it is finitely generated as an R-module, and **algebra-finite** over R if it is finitely generated as an R-algebra. The notion of module-finite is much stronger than algebra-finite, since a linear combination is a very special type of polynomial expression.

Lemma 1.16.

- *If M is a finitely generated R-module, then any generating set for M as an R-module contains a finite subset that generates M.*
- *If the ring S is algebra-finite over R, then any generating set for S as an R-algebra contains a finite subset that also generates S as an R-algebra.*

Proof. Let Γ be a generating set for M as an R-module. If M is a finitely generated R-module, then we can find elements $f_1 \ldots, f_r$ that generate M as an R-module. Since Γ generates M, for each i we can find finitely many elements $\gamma_{i,1}, \ldots, \gamma_{i,n_i} \in \Gamma$ and R-coefficients $r_{i,1}, \ldots, r_{i,n_i}$ such

$$f_i = r_{i,1}\gamma_{i,1} + \cdots + r_{i,n_i}\gamma_{i,n_i}.$$

The submodule N of M generated by all the $\gamma_{i,j}$ contains the elements $f_1, \ldots, f_n$, but since $M = Rf_1 + \cdots + f_n$, we conclude that M is generated by those finitely many $\gamma_{i,j}$, and thus by a finite subset of Γ.

The other proof is essentially the same, with the appropriate replacements: whenever we talk about a set that generates M as an R-module, we should instead consider a set that generates S as an R-algebra, and instead of taking linear combinations of elements we should consider polynomials in those elements with R-coefficients. □

Remark 1.17. If S is an R-algebra,

- $R \subseteq S$ is algebra-finite if $S = R[f_1, \ldots, f_n]$ for some $f_1, \ldots, f_n \in S$.
- $R \subseteq S$ is module-finite if $S = Rf_1 + \cdots + Rf_n$ for some $f_1, \ldots, f_n \in S$.

Algebra generating sets can be very different from module generating sets.

Example 1.18. Given $n \geqslant 2$, the $\mathbb{Q}$-algebra $S = \mathbb{Q}[x]/(x^n)$ is generated as an algebra by the element x. Note, however, that this is not a free $\mathbb{Q}$-algebra: x satisfies the algebra relation $x^n = 0$. When we think about it as a $\mathbb{Q}$-module, x does not generate S, since we are no longer allowed to take products of x by itself. The set $\{1, x, \ldots x^n\}$ is a generating set for S as a module; this is of course the same as asking for a basis for the $\mathbb{Q}$-vector space S.

Lemma 1.19. *If S is a module-finite R-algebra, then it is also algebra-finite.*

Proof. Let $S = Rf_1 + \cdots + Rf_n$, meaning that $f_1, \ldots, f_n$ is a set of module generators for S over R. Note that every R-linear combination of $f_1, \ldots, f_n$ is also an element of $R[f_1, \ldots, f_n]$, and thus S is a subalgebra of $R[f_1, \ldots, f_n]$. On the other hand, since $f_1, \ldots, f_n \in S$ and S is an R-algebra, every polynomial in $f_1, \ldots, f_n$ with coefficients in R is also in S, and thus $S = R[f_1, \ldots, f_n]$, so that S is algebra-finite over R. □

The converse, however, is false: it is *harder* to be module-finite than algebra-finite.

Example 1.20.

a) 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, $\{1, i\}$ is a free module basis! As a $\mathbb{Z}$-algebra, $\mathbb{Z}[i]$ is generated by i, but it is not a free $\mathbb{Z}$-algebra, since $i^2 - 1 = 0$.

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

c) Another map that is *not* module-finite is the inclusion $R := k[x] \subseteq k[x, \frac{1}{x}] =: S$. First, note that any element of $k[x, \frac{1}{x}]$ can be written in the form $\frac{f(x)}{x^n}$ for some $f \in k[x]$ and some $n \geqslant 0$. Now any finitely generated R-submodule of S is of the form

$$M = \sum_i R \cdot \frac{f_i(x)}{x^{n_i}} = \sum_i k[x] \cdot \frac{f_i(x)}{x^{n_i}}.$$

If $n := \max\{n_i\}_i$, then $M \subseteq \frac{1}{x^n} k[x] \neq k[x, \frac{1}{x}] = S$.

d) Even innocent looking examples can be quite complicated. For example, we claim that the extension $\mathbb{Z} \subseteq \mathbb{Q}$ is neither module-finite nor algebra-finite. To see that, we first claim that the set

$$P = \left\{ \frac{1}{p} \mid p \text{ prime integer} \right\}$$

generates $\mathbb{Q}$ as a $\mathbb{Z}$-algebra. The key point here is the Fundamental Theorem of Arithmetic: since any positive integer n can be written as a product $n = p_1^{a_1} \cdots p_s^{a_s}$ where the p_i are all prime and the $a_i \geqslant 0$ are nonnegative integers, we see that the rational number $\frac{m}{n} \neq 0$ can be written as

$$\frac{m}{n} = m \left(\frac{1}{p_1}\right)^{a_1} \cdots \left(\frac{1}{p_s}\right)^{a_s} \in \mathbb{Z}\left[\frac{1}{p_1}, \ldots, \frac{1}{p_s}\right] \subseteq \mathbb{Z}[P].$$

On the other hand, note that any finite subset of P is contained in

$$\left\{ \frac{1}{p} \mid p \leqslant q \text{ prime integer} \right\}$$

for some fixed prime q, and that

$$\mathbb{Z}\left[\frac{1}{p} \mid p \leqslant q \text{ is prime} \right]$$

contains only rational numbers whose denominator is a product of primes smaller than q. But there are infinitely many primes, and thus this cannot be all of $\mathbb{Q}$. By Lemma 1.16, we can conclude that $\mathbb{Q}$ is not a algebra-finite over $\mathbb{Z}$. But then $\mathbb{Q}$ cannot be module-finite over $\mathbb{Z}$, by Lemma 1.19.

Lemma 1.21. *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 1.22. Let $A \subseteq B \subseteq C$ be rings. It follows from the definitions that

- $A \subseteq B$ algebra-finite and $B \subseteq C$ algebra-finite $\Longrightarrow$ $A \subseteq C$ 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. To see this, first note by Lemma 1.16 it is sufficient to show that no finite subset of $\{xy^n \mid n \geqslant 1\}$ generates B over k. Since any such subset is contained in $\{xy^n \mid 1 \leqslant n \leqslant m\}$ for some fixed m, it is sufficient to show that B is not $k[x, xy, \ldots, xy^m]$ for any m. Now note that every element of $k[x, xy, \ldots, xy^m]$ is a k-linear combination of monomials $x^i y^j$ with $j \leqslant mi$, so this ring does not contain xy^{m+1}. Therefore, B is not a finitely generated A-algebra.

Remark 1.24. Let $A \subseteq B \subseteq C$ be rings. It follows from the definitions that

- $A \subseteq B$ module-finite and $B \subseteq C$ module-finite $\Longrightarrow$ $A \subseteq C$ module-finite
- $A \subseteq C$ module-finite $\Longrightarrow B \subseteq C$ module-finite.

However, we will see that $A \subseteq C$ module-finite $\not\Longrightarrow$ $A \subseteq B$ module-finite. This construction is a bit more involved, so we will leave it for the problem sets.

Remark 1.25. Any surjective ring homomorphism $\varphi \colon R \to S$ is both algebra-finite and module-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 or module-finiteness it suffices to restrict our attention to injective homomorphisms.

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, but much more subtle.

Definition 1.26 (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

$$r^n + a_{n-1}r^{n-1} + \cdots + a_1 r + a_0 = 0,$$

we say that 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. This is very different to what happens over fields, where algebraic and integral are equivalent conditions.

Example 1.27. Let's see some examples of elements that are integral over $\mathbb{Z}$, and others that are not. First, consider the $\mathbb{Z}$-algebra $R = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. The element $\sqrt{2}$ is integral over $\mathbb{Z}$, since it satisfies the equation of integral dependence $x^2 - 2 = 0$.

On the other hand, $\frac{1}{2} \in \mathbb{Q}$ is not integral over $\mathbb{Z}$: if $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ are such that

$$\left(\frac{1}{2}\right)^n + a_{n-1}\left(\frac{1}{2}\right)^{n-1} + \cdots + a_0 = 0,$$

then multiplying by 2^n gives

$$1 + 2a_{n-1} + \cdots + 2^n a_0 = 0,$$

which is impossible for parity reasons (the left hand-side is odd!). Notice, in contrast, that $\frac{1}{2}$ is algebraic over $\mathbb{Z}$, since it satisfies $2x - 1 = 0$.

Definition 1.28. Consider an 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. We say A is **integrally closed** in R if A is its own integral closure in R. The integral closure of a domain R in its field of fractions is usually denoted by $\overline{R}$. A **normal domain** is a domain R that is integrally closed in its field of fractions, meaning $R = \overline{R}$.

Example 1.29. The ring of integers $\mathbb{Z}$ is a normal domain, meaning its integral closure in its fraction field $\mathbb{Q}$ is $\mathbb{Z}$ itself. The key idea to show this is similar to the argument we used in Example 1.27 to show that $\frac{1}{2}$ is not integral over $\mathbb{Z}$.

In fact, this is a special case of the fact that every UFD is normal.

Exercise 5. Show that every unique factorization domain is normal.

Remark 1.30. We cannot talk about the integral closure of a ring R without specifying in what extension; the integral closures of R in different extension can be very different. In Example 1.27, we saw that the integral closure of $\mathbb{Z}$ in $\mathbb{Z}[\sqrt{2}]$ contains at least $\mathbb{Z}$ and $\sqrt{2}$, while Example 1.29 says that the integral closure of $\mathbb{Z}$ in $\mathbb{Q}$ is $\mathbb{Z}$.

When R is a domain, if we ever refer to *the* integral closure of R, it is understood that we mean the integral closure of R in its field of fractions, $\overline{R}$.

When we study integral extensions, we can restrict our focus to inclusion maps $A \subseteq R$, just like we did with module-finite and algebra-finite extensions.

Remark 1.31. 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.

Proposition 1.32. *Consider a ring extension $A \subseteq R$.*

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) Let r be integral over A, with $r^n + a_{n-1}r^{n-1} + \cdots + a_1 r + a_0 = 0$ for some $a_i \in A$. We claim that $A[r] = A + Ar + \cdots + Ar^{n-1}$. Since $A[r]$ is generated by all the powers r^m of r as an A-module, 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. For the induction step, we need to show that $r^m \in A + Ar + \cdots + Ar^{n-1}$ for all $m \geqslant n-1$; we can do this by induction because we can use the equation above to rewrite r^m as

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

which is a linear combination of powers of r of degree up to $m-1$.

2) Write
$$A_0 := A \subseteq A_1 := A[r_1] \subseteq A_2 := A[r_1, r_2] \subseteq \cdots \subseteq A_t := A[r_1, \ldots, r_t].$$
Since r_i is integral over A, it is also integral over A_{i-1}, via the same monic equation that r_i satisfies over A. By part 1), we conclude that the each extension $A_{i-1} \subseteq A_i$ is module-finite. Thus the inclusion $A \subseteq A[r_1, \ldots, r_t]$ is a composition of module-finite maps, and thus by Remark 1.24 it is also module-finite. □

In what follows, we will need the following elementary linear algebra fact, which is actually very useful in various contexts within commutative algebra. In fact, later in this class we will use this useful fact again, perhaps when you least expect it. This is a nice example of an algebra fact that holds over any ring that we can actually reduce to the case of fields.

Definition 1.33. The **classical adjoint** of an $n \times n$ matrix $B = [b_{ij}]$ is the matrix $\operatorname{adj}(B)$ with entries $\operatorname{adj}(B)_{ij} = (-1)^{i+j} \det(\widehat{B_{ji}})$, where $\widehat{B_{ji}}$ is the matrix obtained from B by deleting its jth row and ith column.

Lemma 1.34 (Determinantal trick)**.** *Let R be a ring, $B \in M_{n\times n}(R)$, $v \in R^n$, and $r \in R$.*

1) $\operatorname{adj}(B)B = \det(B)I_{n\times n}$.

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 will 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

$$\psi(\operatorname{adj}(A)_{ij}) = \operatorname{adj}(B)_{ij} \quad \text{and} \quad \psi((\operatorname{adj}(A)A)_{ij}) = (\operatorname{adj}(B)B)_{ij},$$

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

$$\operatorname{adj}(B)B = \det(B)I_{n\times n}$$

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

$$(\operatorname{adj}(B)B)_{ij} = (\det(B)I_{n\times n})_{ij}$$

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) By assumption, we have $(rI_{n\times n} - B)v = 0$, so by part 1)

$$\det(rI_{n\times n} - B)v = \operatorname{adj}(rI_{n\times n} - B)(rI_{n\times n} - B)v = 0. \qquad \square$$

Theorem 1.35 (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.

Suppose that $R = Af_1 + \cdots + Af_n$. We may assume that $f_1 = 1$, perhaps by adding a module generator. Since every element in R is an A-linear combination of $f_1, \dots, f_n$, this is in particular true for the elements $rf_1, \dots, rf_n$. Thus we can find $a_{ij} \in A$ such that

$$rf_i = \sum_{j=1}^{t} a_{ij} f_j$$

for each i. Consider the matrix $C = [a_{ij}]$ and the column vector $v = (f_1, \dots, f_n)$. We can now write the equalities above more compactly as $rv = Cv$. By the determinantal 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. $\square$

We are now ready to show the following important characterization of module-finite extensions, which tells us exactly what we need besides algebra-finite to force an extension to be module-finite:

Corollary 1.36. *An A-algebra R is module-finite over A if and only if R is integral and algebra-finite over A.*

Proof. ($\Rightarrow$): Module-finite implies integral by Theorem 1.35, and algebra-finite by Lemma 1.19. ($\Leftarrow$): If $R = A[r_1, \ldots, r_t]$ is integral over A, then each r_i is integral over A, and this implies R is module-finite over A by Proposition 1.32,. $\square$

Corollary 1.37. *If R is generated as an algebra over A by integral elements, then R is integral over A.*

Proof. Let $R = A[\Lambda]$, with λ integral over A for all $\lambda \in \Lambda$. Given $r \in R$, we need to show that r is integral over A. There is a finite subset $L \subseteq \Lambda$ such that $r \in A[L]$. This $A[L]$ is now a finitely-generated algebra generated by integral elements, and thus by Proposition 1.32 it must be module-finite over A. By Theorem 1.35, module-finite implies integral, and thus $A[L]$ is an integral extension of A. In particular, $r \in A[L]$ is integral over A. $\square$

Corollary 1.38. *Given any ring extension $A \subseteq R$, the set of elements of R that are integral over A form a subring of R.*

Proof. By Corollary 1.37, the A-subalgebra of R generated by all elements in R that are integral over A is integral over A, so it is contained in the set of all elements that are integral over A: this means that

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

so equality holds throughout, and $\{\text{integral elements}\}$ is a ring. $\square$

In other words, the integral closure of A in R is a subring of R containing A.

Example 1.39.

1) 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 $x^2 - d$, and since the integral closure of $\mathbb{Z}$ is a ring containing $\mathbb{Z}$ and $\sqrt{d}$, and $\mathbb{Z}[\sqrt{d}]$ is the smallest such ring, we conclude that every element in $\mathbb{Z}[\sqrt{d}]$ is integral over $\mathbb{Z}$.

2) Let $R = \mathbb{C}[x, y] \subseteq S = \mathbb{C}[x, y, z]/(x^2 + y^2 + z^2)$. Then we claim that S is module-finite over R, though to see this we first need to realize R as a subring of S. To do that, consider the $\mathbb{C}$-algebra homomorphism

$$\begin{aligned} R &\xrightarrow{\varphi} S \\ (x, y) &\longmapsto (x, y). \end{aligned}$$

The kernel of φ consists of the polynomials in x and y that are multiples of $x^2 + y^2 + z^2$, but any nonzero multiple of $x^2 + y^2 + z^2$ in $\mathbb{C}[x, y, z] = R[z]$ must have z-degree at least 2, which implies it involves z and thus it is not in $\mathbb{C}[x, y]$. We conclude that φ is injective, and thus $R \subseteq S$.

Now S is generated over R as an algebra by one element, z, and z satisfies the monic equation $t^2 + (x^2 + y^2) = 0$, so S is integral over R.

Note, however, that not all integral extensions are module-finite.

Example 1.40. Let k be a field, and consider the $k[x]$-algebra R given by

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

Note that $x^{1/n}$ satisfies the monic polynomial $t^n - x$, and thus it is integral over $k[x]$. Since R is generated by elements that are integral over $k[x]$, by Corollary 1.37 it must be an integral extension of A. However, $k[x] \subseteq R$ is not algebra-finite, and thus it is also not module-finite.

Exercise 6. Given ring extensions $A \subseteq B \subseteq C$, the extensions $A \subseteq B$ and $B \subseteq C$ are integral if and only if $A \subseteq C$ is integral.

Finally, here is a useful fact about integral extensions that we will use multiple times.

Theorem 1.41. *If $R \subseteq S$ is an integral extension of domains, then R is a field if and only if S is a field.*

Proof. Suppose that R is a field, and let $s \in S$ be a nonzero element, which is necessarily integral over R. The ring $R[s]$ is algebra-finite over R by construction, and integral over R by Corollary 1.37. Since $R \subseteq R[s]$ is integral and algebra-finite, it must also be module-finite by Corollary 1.36. Since R is a field, this means that $R[s]$ is a finite-dimensional vector space over R. Since $R[s] \subseteq S$ is a domain, the map $R[s] \xrightarrow{s} R[s]$ is injective. Notice that this is a map of finite-dimensional R-vector spaces, and thus it must also be surjective. In particular, there exists an element $t \in R[s]$ such that $st = 1$, and thus s is invertible. We conclude that S must be a field.

Now suppose that S is a field, and let $r \in R$. Since $r \in R \subseteq S$, there exists an inverse r^{-1} for r in S, which must be integral over R. Given any equation of integral dependence for r^{-1} over R, say

$$(r^{-1})^n + a_{n-1}(r^{-1})^{n-1} + \cdots + a_0 = 0$$

with $a_i \in R$, we can multiply by r^{n-1} to obtain

$$r^{-1} = -a_{n-1} - \cdots - a_0 r^{n-1} \in R.$$

Therefore, r is invertible in R, and R is a field. □

Before we move on from algebra-finite and module-finite extensions, we should remark on what the situation looks like over fields. First, note that over a field, module-finite just means finite dimensional vector space. While over a general ring the notions of algebra-finite and module-finite are quite different, they are actually equivalent over a field. This is a very deep fact, and we will unfortunately skip its proof — since it is a key ingredient in proving a fundamental result in algebraic geometry, we will leave it for the algebraic geometry class next semester. This is a nice application of the Artin-Tate Lemma, which we are going to discuss shortly, together with some facts about transcendent elements. We will skip the proof, but you can find it in Jeffries' notes.

Theorem 1.42 (Zariski's Lemma)**.** *A field extension $k \subseteq L$ is algebra-finite if and only if it is module-finite.*

The following corollary follows immediately from what we proved in this section:

Corollary 1.43. *Let k be an algebraically closed field. If the field extension $k \subseteq L$ is algebra-finite, then $k = L$.*

Proof. By Theorem 1.42, $k \subseteq L$ must be module-finite. By Theorem 1.35, any module-finite extension must be integral. When we are over a field, integral is the same as algebraic, but integrally closed fields have no nontrivial algebraic extensions. □

We have shown the following about ring extensions:

$$\begin{tikzcd} & \text{module-finite} \arrow[dl, Rightarrow] \arrow[dr, Rightarrow] & \\ \text{algebra-finite} & & \text{integral} \end{tikzcd}$$

The remaining implications are all false:

- Given an indeterminate x, the extension $R \subseteq R[x]$ is algebra-finite but not module finite nor integral.
- Example 1.40 is an example of an integral extension that is not module-finite nor algebra-finite.

1.5 We interrupt this broadcast for a very short introduction to exact sequences

Homological techniques play a central role in commutative algebra. Ideally, our study of commutative algebra would start with a semester long course on homological algebra; but we are not assuming any homological algebra background, and thus we need to introduce some elementary homological algebra tools.

Definition 1.44. 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 called a **short exact sequence**.

Example 1.45. Let $R = k[x]/(x^2)$, where k is any field. The $R \xrightarrow{x} R$ has image and kernel (x), so the following is an exact sequence:

$$\cdots \longrightarrow R \xrightarrow{x} R \xrightarrow{x} R \longrightarrow \cdots$$

Remark 1.46. 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. As a consequence, we see that
$$0 \longrightarrow M \xrightarrow{f} N \longrightarrow 0$$
is exact if and only if f is an isomorphism. Moreover,
$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$
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 $f(A)$, which makes $A = \ker g$. 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. In particular, note that $C = \operatorname{coker} f$.

In summary, any short exact sequence encodes an inclusion and its cokernel, or equivalently a surjection on its kernel. To give a short exact sequence
$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$
is the same as giving an inclusion of modules $A \subseteq B$ and the corresponding quotient module B/A.

Example 1.47. The following is a short exact sequence of $\mathbb{Z}$-modules:
$$0 \longrightarrow \mathbb{Z} \xrightarrow{2} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0.$$
Indeed, multiplication by 2 on $\mathbb{Z}$ is injective, and its cokernel is $\mathbb{Z}/2\mathbb{Z}$. Another way to look at this is to notice that the kernel of the canonical projection map $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ is the ideal generated by 2, which is a free $\mathbb{Z}$-module with 1 generator. The map $\mathbb{Z} \xrightarrow{2} \mathbb{Z}$ corresponds to the inclusion of that module in $\mathbb{Z}$.

Remark 1.48. Suppose that
$$0 \longrightarrow M \longrightarrow 0$$
is an exact sequence. This means that the image of the zero map to M, which is the zero module, is the same as the kernel of the zero map from M, which is all of M. Thus saying that
$$0 \longrightarrow M \longrightarrow 0$$
is exact is equivalent to saying that $M = 0$.

1.6 Noetherian rings

Most rings that commutative algebraists naturally want to study are noetherian. Noetherian rings are named after Emmy Noether, who is in many ways the mother of modern commutative algebra.

Definition 1.49 (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 1.50. *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)$\Rightarrow$(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, so R is not noetherian.

(2)$\Rightarrow$(1): An ascending chain of ideals is a family of ideals, and the maximal ideal in the family indicates where our chain stabilizes.

(1)$\Rightarrow$(3): Clear, since (3) is a special case of (1).

(3)$\Rightarrow$(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 $s \in S \setminus (S')$. Thus, $(S') \subsetneq (S' \cup \{s\})$. Inductively, we can continue this process to obtain an infinite proper chain of finitely generated ideals, so (3) does not hold.

(4)$\Rightarrow$(5): Clear.

(5)$\Rightarrow$(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 $I = (a_1, \ldots, a_t)$. Now since each a_i is in I, it must be in some I_{n_i}, by definition. Thus for any $N \geqslant \max n_i$, we have $a_1, \ldots, a_t \in I_N$. But then $I_N = I$, and thus $I_n = I_{n+1}$ for all $n \geqslant N$. Thus the original chain stabilizes, and R is noetherian. ☐

Remark 1.51. 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 $I = J$. However, 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 1.52. 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 1.50. 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 1.53.

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, since all ideals are principal. 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) If k is a field, 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

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

   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!

Lemma 1.54. *Let R be a ring and I an ideal in R. If R is noetherian, then so is R/I.*

Proof. There is an order preserving bijection

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

that sends the ideal $J \supseteq I$ to J/I; its inverse is the map that sends each ideal in R/I to its preimage. Given this bijection, chains of ideals in R/I come from chains of ideals in R that contain J. This implies that if R is noetherian, then R/I is noetherian as well. □

This gives us many more examples of noetherian rings, by simply taking quotients of the examples above. We will soon show that any polynomial ring over a noetherian ring is also noetherian; as a consequence, we obtain that any quotient of a polynomial ring over a field is noetherian. This is the content of Hilbert's Basis Theorem.

But first, we need to talk about noetherian modules.

Definition 1.55 (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; the proof is analogous, so we leave it as an exercise.

Proposition 1.56 (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 1.57. The submodules of a ring are its ideals. Thus 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:

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

A module B is noetherian if and only if it has a submodule A such that both A and B/A are noetherian.

Lemma 1.58 (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 $y \in M_n \subseteq M_{n+1}$, so $x - y \in M_{n+1}$, and thus

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

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

Corollary 1.59. *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

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

$\square$

Corollary 1.60. *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 1.58 and the inductive hypothesis give the desired conclusion. $\square$

Proposition 1.61. *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 by Corollary 1.60 and Lemma 1.54. □

Remark 1.62. The notherianity hypothesis is important: if R is a non-noetherian ring and M is a finitely generated R-module, M might not be noetherian. For a dramatic example, note that R itself is a finitely generated R-module, but not noetherian.

Now we are ready to prove Hilbert's Basis Theorem. David Hilbert was 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 her to join the Göttingen Math Department — many of her amazing contributions to algebra happened during her time in Göttingen. Unfortunately, some of the faculty opposed 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.

Theorem 1.63 (Hilbert's Basis Theorem)**.** *If R is a noetherian ring, then the polynomial rings $R[x_1, \dots, x_d]$ and $R[\![x_1, \dots, x_d]\!]$ are noetherian for any $d \geqslant 1$.*

Proof. We will give the proof for polynomial rings, and at the end we will indicate what the difference is in the argument for the power series ring case. First, note that by induction on d, we can reduce to the case $d = 1$.

Given an ideal $I \subseteq R[x]$, consider the set of leading coefficients of all polynomials in I,

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

We can check (exercise!) that this is an ideal of R. Since R is noetherian, Proposition 1.50 says that J is finitely generated, so let $J = (a_1, \dots, a_t)$. Pick $f_1, \dots, f_t \in R[x]$ such that the leading coefficient of f_i is a_i, and set $N = \max_i \{\deg f_i\}$.

Let $f \in I$. The leading coefficient of f is an R-linear combination of $a_1, \dots, a_t$. If f has degree greater than N, then we can cancel off the leading term of f by subtracting a suitable combination of the f_i. Therefore, any $f \in I$ can be written as $f = g + h$ for some $h \in (f_1, \dots, f_t)$ and $g \in I$ with degree at most N. In particular, note that $g \in I \cap (R + Rx + \cdots + Rx^N)$. Since $I \cap (R + Rx + \cdots + Rx^N)$ is a submodule of the finitely generated free R-module $R + Rx + \cdots + Rx^N$, it must also be finitely generated as an R-module. Given such a generating set, say $I \cap (R + Rx + \cdots + Rx^N) = (f_{t+1}, \dots, f_s)$, we can write any element $f \in I$ as an $R[x]$-linear combination of these generators $f_{t+1}, \dots, f_s$ and the original $f_1, \dots, f_t$. Therefore, $I = (f_1, \dots, f_t, f_{t+1}, \dots, f_s)$ is finitely generated as an ideal in $R[x]$, and $R[x]$ is a noetherian ring.

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

Remark 1.64. We can rephrase Hilbert's Basis 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.

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

Corollary 1.65. *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. Any 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.

Finally, we can now prove a technical sounding result that puts together all our finiteness conditions in a useful way.

Theorem 1.66 (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 $C = A[f_1, \ldots, f_r]$ 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 $B_0 = A[\{b_{ij}, b_{ijk}\}] \subseteq B$. This is a finitely generated A-algebra; by Corollary 1.65, 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 $f_1, \ldots, f_r$. Since the f_i are linear combinations of the g_i with coefficients in the b_{ij}, we have $c \in A[\{b_{ij}\}][g_1, \ldots, g_s]$. Then using the equations for $g_i g_j$ repeatedly, we can rewrite c as a linear combination of the g_i with coefficients in B_0.

Since B_0 is noetherian and C is a finitely generated B_0-module, C is a noetherian B_0-module, by Proposition 1.61. Since $B \subseteq C$, then B is also a finitely generated B_0-module. In particular, $B_0 \subseteq B$ is algebra-finite. Since $A \subseteq B_0$ is algebra-finite, we conclude that $A \subseteq B$ is algebra-finite, as required. □

1.7 An application to invariant rings

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

Question 1.67. 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. The main case we have in mind is when $R = k[x_1, \ldots, x_d]$ and k is a field; we let G act trivially on k, and the action respects the sum and product in the ring:

$$g \cdot \left(\sum_a c_a x_1^{a_1} \cdots x_d^{a_d} \right) = \sum_a c_a (g \cdot x_1)^{a_1} \cdots (g \cdot x_d)^{a_d}.$$

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

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

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

Note that R^G is a k-subalgebra of R. Even though R is a finitely generated k-algebra, this does not guarantee a priori that R^G is a finitely generated k-algebra — recall Example 1.23, where we saw a subalgebra of a finitely generated algebra which is nevertheless not finitely generated.

Example 1.69. Consider the group with two elements $G = \{e, g\}$. To define an action of G on $R = k[x]$, we need only to define $g \cdot x$, since e is the identity and g acts linearly. Consider the action of G on $R = k[x]$ given by $g \cdot x = -x$, so $g \cdot f(x) = f(-x)$. Suppose that the characteristic of k is not 2, so $-1 \neq 1$. Write $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$. We have $g \cdot x^i = (-x)^i = (-1)^i x^i$, so

$$g \cdot f = (-1)^n a_n x^n + (-1)^{n-1} a_{n-1} x^{n-1} + \cdots + a_0,$$

which differs from f unless for each odd i, $a_i = 0$. That is,

$$R^G = \{ f \in R \mid \text{every term of } f \text{ has even degree} \}.$$

Any such f is a polynomial in x^2, so we have

$$R^G = k[x^2].$$

In particular, R^G is a finitely generated k-algebra.

Exercise 7. Generalize the last example as follows: let k be a field with a primitive dth root of unity ζ, and let $G = \langle g \rangle \cong C_d$ act on $R = k[x_1, \ldots, x_n]$ via $g \cdot x_i = \zeta x_i$ for all i. Then

$$R^G = \{f \in R \mid \text{every term of } f \text{ has degree a multiple of } d\} = k[\{\text{monomials of degree d}\}].$$

This what is known as the Veronese subring of R of degree d.

Example 1.70 (Standard representation of the symmetric group)**.** Let S_n be the symmetric group on n letters acting on $R = k[x_1, \ldots, x_n]$ via $\sigma(x_i) = x_{\sigma(i)}$. For example, if $n = 3$, then $f = x_1^2 + x_2^2 + x_3^2$ is invariant, while $g = x_1^2 + x_1x_2 + x_2^2 + x_3^2$ is not, since swapping 1 with 3 gives a different polynomial.

You may recall the Fundamental Theorem of Symmetric Polynomials says that every element of R^{S_n} can be written as polynomial expression in the elementary symmetric polynomials

$$\begin{aligned} e_1 &= x_1 + \cdots + x_n \\ e_2 &= \sum x_i x_j \\ &\vdots \\ e_n &= x_1 x_2 \cdots x_n. \end{aligned}$$

More precisely, $R^{S_n} = k[e_1, \ldots, e_n]$. For example, f above is $e_1^2 - 2e_2$. In fact, any symmetric polynomial can be written like so in a *unique* way, so R^{S_n} is a free k-algebra. So even though we have infinitely many invariant polynomials, we can understand them in terms of only finitely many of them, which are *fundamental* invariants.

Proposition 1.71. *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. By Corollary 1.36, integral and algebra-finite implies module-finite, so we will show that R is algebra-finite and integral over R^G.

First, since $k \subseteq R^G$ and R is generated finitely generated k-algebra, it is generated by the same finite set as an R^G-algebra as well. Thus $R^G \subseteq R$ is algebra-finite.

To show that $R^G \subseteq R$ is integral, let us first extend the action of G on R to $R[t]$ trivially, meaning that we will let G fix t. Given $r \in R$, consider the polynomial

$$F_r(t) := \prod_{g \in G} (t - g \cdot r) \in R[t].$$

Now G fixes $F_r(t)$, since for each $h \in G$,

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

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. On the other hand, one of the factors of $F_r(t)$ is $(t - r)$, so $F_r(r) = 0$. Therefore, r satisfies a monic polynomial with coefficients in R^G, and thus R is integral over R^G. $\square$

Theorem 1.72 (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. The desired result is now a corollary of the Artin-Tate Lemma. □

Chapter summary

- R is a noetherian ring $\iff$ every ideal I in R is noetherian
- M is a noetherian R-module $\underset{R \text{ Noeth}}{\overset{\text{general}}{\rightleftarrows}}$ 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 $\iff$ $\left\{ \begin{array}{c} \text{algebra-finite} \\ \text{and integral} \end{array} \right.$ $\begin{array}{c} \not\Rightarrow \\ \not\Rightarrow \end{array}$ module-finite

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

Chapter 2

Graded rings

The main purpose of this chapter is to set up some background and notation we will use throughout the rest of the course.

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. Let T be a monoid; in many examples we will take $T = \mathbb{N}$, which is a monoid since we follow the convention that 0 is a natural number. A ring R is T**-graded** if we can write a direct sum decomposition of R as an abelian group indexed by T,

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

such that

$$R_a R_b \subseteq R_{a+b} \qquad \text{for every } a, b \in T.$$

This means that for all $r \in R_a$ and $s \in R_b$, we have $rs \in R_{a+b}$.

An element 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 checked on homogeneous elements, and these are often easier to deal with.

Lemma 2.2. *Let R be a T-graded ring.*

a) 1 is homogeneous of degree $0 \in T$ (the identity of T).

b) R_0 is a subring of R.

c) Each R_a is an R_0-module.

Proof.

a) Write $1 = \sum_a r_a$ with r_a homogeneous of degree a. Then $r_0 = r_0(\sum_a r_a) = \sum_a r_0 r_a$ implies $r_0 r_a = 0$ for $a \neq 0$. Similarly, for any other a we have $r_a = r_a(\sum_b r_b)$, and thus $r_a = r_a r_0$ (here is where we use the cancellative assumption). Thus $r_a = 0$ for $a \neq 0$, so $1 \in R_0$.

b) We have shown that $1 \in R_0$. Moreover, R_0 is a subgroup under addition, and $r, s \in R_0$ implies $rs \in R_0$.

c) By assumption, R_a is a subgroup under addition. Given $r \in R_0$ and $s \in R_a$ we must have $rs \in R_a$. □

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 $R = k[x_1, \dots, x_n]$ 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 $\sum_i \alpha_i = d$. For example, $x_1^2 + x_2 x_3$ is homogeneous in the standard grading, while $x_1^2 + x_2$ is not.

c) If k is a field, and $R = k[x_1, \dots, x_n]$ is a polynomial ring, we can give different $\mathbb{N}$-gradings on R by fixing some tuple $(\beta_1, \dots, \beta_n) \in \mathbb{N}^n$ and letting x_i be a homogeneous element of degree β_i; we call this a grading with *weights* $(\beta_1, \dots, \beta_n)$.

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

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

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

   is an $\mathbb{N}^n$-graded subring of $k[x_1, \dots, x_n]$ with the fine grading. Moreover, every $\mathbb{N}^n$-graded subring of $k[x_1, \dots, x_n]$ is of this form.

Macaulay2. 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 $f(x_1,\dots,x_n)\in k[x_1,\dots,x_n]$ that satisfies

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

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

Similarly, a polynomial is *quasi-homogeneous*, or *weighted homogeneous*, if there exist integers $w_1,\dots,w_n$ such that the sum $d=a_1w_1+\cdots+a_nw_n$ is the same for all monomials $x_1^{a_1}\cdots x_n^{a_n}$ appearing in f. So f satisfies

$$f(\lambda^{w_1}x_1,\dots,\lambda^{w_n}x_n)=\lambda^d f(x_1,\dots,x_n),$$

for all $\lambda\in k$ and $f(x_1^{w_1},\dots,x_n^{w_n})$ 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 $k[x_1,\dots,x_n]$.

Example 2.5. In $k[x,y,z]$, the element $x^2+y^3+z^5$ is not homogeneous in the standard grading, but it is homogeneous (of degree 30) if we set $\deg(x)=15$, $\deg(y)=10$, and $\deg(z)=6$. This tells us that $x^2+y^3+z^5$ is quasi-homogeneous; it is homogeneous with respect to the weights $(15,10,6)$. Indeed,

$$(\lambda^{15}x)^2+(\lambda^{10}y)^3+(\lambda^6z)^5=\lambda^{30}(x^2+y^3+z^5).$$

Definition 2.6. An ideal I in a graded ring R is called **homogeneous** if it can be generated by homogeneous elements.

Lemma 2.7. *Let I be an ideal in a graded ring R. The following are equivalent:*

(1) I is homogeneous.

(2) For any element $f\in R$ we have $f\in I$ if and only if every homogeneous component of f lies in I.

(3) $I=\bigoplus_{a\in T}I_a$, where $I_a=I\cap R_a$.

Proof. (1) $\Rightarrow$ (2): Let $f_1,\dots,f_n$ be homogeneous generators for I. If $f\in I$, we can write f as

$$f=r_1f_1+\cdots+r_nf_n.$$

We can also write each r_i as a sum of its components, say $r_i=[r_i]_{d_{i,1}}+\cdots+[r_i]_{d_{i,m_i}}$. Then, after substituting and collecting,

$$f=\sum_d\left([r_1]_{d-|f_1|}f_1+\cdots+[r_n]_{d-|f_n|}f_n\right)$$

expresses f as a sum of homogeneous elements of different degrees, so

$$f_d = [r_1]_{d-|f_1|} f_1 + \cdots + [r_n]_{d-|f_n|} f_n \in I.$$

(2) $\Rightarrow$ (1): Any element of I is a sum of its homogeneous components. Thus, in this case, the set of homogeneous elements in I is a generating set for I.

(2) $\Rightarrow$ (3): As above, I is generated by the collection of additive subgroups $\{I_a\}$ in this case; the sum is direct as there is no nontrivial $\mathbb{Z}$-linear combination of elements of different degrees.

(3) $\Rightarrow$ (2): We can take generators for each abelian group $I \cap R_a$, and the collection of all of them is a generating set for I. ☐

Example 2.8. Given an $\mathbb{N}$-graded ring R, then $R_+ = \bigoplus_{d>0} R_d$ is a homogeneous ideal.

We now observe the following:

Lemma 2.9. *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

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

It's elementary to check that this direct sum decomposition satisfies the desired properties.

Example 2.10.

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) The ring $R = k[x,y,z]/(x^2 + y^3 + z^5)$ does not admit a grading with $|x| = |y| = |z| = 1$, but by Example 2.5 it does admit a grading with $|x| = 15, |y| = 10, |z| = 6$.

Definition 2.11. Let R be a T-graded ring and M an R-module. An R-module M 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 2.12. 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 2.13. Let M and N be T-graded modules over the T-graded ring R. A homomorphism of R-modules $\varphi\colon M \to N$ is **graded** of **degree** d if $\varphi(M_a) \subseteq N_{a+d}$ for all $a \in T$. A graded homomorphism of degree 0 is also called **degree-preserving**.

Example 2.14.

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 $R = k[x_1, \dots, x_n]$ 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 $g \in R_d$ 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.

2.2 Finiteness conditions for graded algebras

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

Proof. Suppose $R = R_0[f_1, \ldots, f_n]$. Any element $r \in R_+$ can be written as a polynomial expression $r = P(f_1, \ldots, f_n)$ for some $P \in R_0[x_1, \ldots, x_n]$ with no constant term. Each monomial of P is a multiple of some x_i, and thus each term in $r = P(f_1, \ldots, f_n)$ is a multiple of f_i. Thus $r \in Rf_1 + \cdots + Rf_n = (f_1, \ldots, f_n)$.

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 $f_1, \ldots, f_n$ with coefficients in R_0. We will use induction 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 $f_1, \ldots, f_n$, so we are done. □

This leads to the following characterization of noetherian $\mathbb{N}$-graded rings:

Corollary 2.16. *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_0 is noetherian and R is algebra-finite over R_0, then R is noetherian by the Hilbert Basis Theorem. On the other hand, if R is noetherian then any quotient of R is also noetherian, by Lemma 1.54, and in particular $R_0 \cong R/R_+$ is noetherian. Moreover, R_+ is generated as an ideal by finitely many homogeneous elements by noetherianity; by Proposition 2.15, 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.

2.3 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 2.17. Let $\varphi : R \to S$ be a ring homomorphism. 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

$$\begin{tikzcd} R \arrow[r, "\varphi"'] & S \arrow[l, bend right, dashed, "\rho"'] \end{tikzcd}$$

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

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

Remark 2.18. The subring R of S is a direct summand of S if and only if there exists an R-submodule of S such that $S = R \oplus M$. In the language above, $M = \ker \rho$. Conversely, given a direct sum decomposition $S = R \oplus M$, the quotient map onto the first component is a splitting.

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

Notation 2.19. Let $\varphi\colon R \to S$ be a ring homomorphism. 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 φ. In particular, if $R \subseteq S$ is a ring extension, then $I \cap R$ denotes the preimage of I via the inclusion map $R \subseteq S$. 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 2.20. *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 2.21. *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

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

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

Example 2.22. Notice in general a subring of a noetherian ring does not have to be noetherian. For example, if k is a field, $S = k[x, y]$ is noetherian by Hilbert's Basis Theorem, but we claim that the subring

$$R = k[xy, xy^2, xy^3, \ldots]$$

of $S = k[x,y]$ is not noetherian. Indeed,

$$(xy) \subseteq (xy, xy^2) \subseteq (xy, xy^2, xy^3) \subseteq \cdots$$

is an ascending chain of ideals of R that does not stabilize. Notice that if we considered the same chain of ideals in S, then it does stabilize, and in fact it is the constant chain (xy).

Proposition 2.23. *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 2.24. 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 $\rho \colon R \to R^G$ 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 $s \in R^G$,

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

$\square$

Theorem 2.25 (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 that the characteristic of k does not divide $|G|$, 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 on R, 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 2.21. By our characterization of noetherian graded rings in Corollary 2.16, R^G is finitely generated over $R_0 = k$. $\square$

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

Primes

3.1 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 3.1. 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. In particular, (0) is a prime ideal if and only if R is a domain.

Example 3.2. The prime ideals in $\mathbb{Z}$ are those of the form (p) for p a prime integer, and (0).

Example 3.3. When k is a field, prime ideals 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 3.4. Let k be a field. 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 3.5. The k-algebra $R = k[t^3, t^4, t^5] \subseteq k[t]$ is a domain, so its defining ideal P in $k[x, y, z]$ is prime. This is the kernel of the presentation of R sending x, y, z to each of our 3 algebra generators, which we can compute with Macaulay2:

```
i1 : k = QQ

o1 = QQ

o1 : Ring

i2 : f = map(k[t],k[x,y,z],{t^3,t^4,t^5})
                                 3   4   5
o2 = map (QQ[t], QQ[x..z], {t , t , t })
```

```
o2 : RingMap QQ[t] <--- QQ[x..z]

i3 : P = ker f
              2          2     2   3
o3 = ideal (y  - x*z, x y - z , x  - y*z)

o3 : Ideal of QQ[x..z]
```

Definition 3.6 (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 3.7. A ring may have many different residue fields. For example, the residue fields of $\mathbb{Z}$ are all the finite fields with a prime numbers of 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 3.8. *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 is a statement about partially ordered sets. Given a partially ordered set S, a chain in S is a totally ordered subset of S.

Theorem 3.9 (Zorn's Lemma)**.** *Let S be a nonempty partially ordered set S such that every chain in S has an upper bound in S. Then S contains at least one maximal element.*

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

Proof. Fix a ring R and a proper ideal I. Let S be the set of all proper ideals J in R such that $J \supseteq I$, which is partially ordered with the inclusion order $\subseteq$. We claim that Zorn's Lemma applies to S. First, S is nonempty, since it contains I. Now consider a chain of proper ideals in R, say $\{J_i\}_i$, all of which contain I. Notice that $J := \bigcup_i J_i$ is an ideal as well (exercise!), and moreover $J \neq R$ since $1 \notin J_i$ for all i.[1] Since each $J_i \supseteq I$, we conclude that $J \supseteq I$. Thus we have checked that $J \in S$. Now this ideal $J \in S$ is an upper bound for our chain $\{J_i\}_i$, and thus Zorn's Lemma applies to S. We conclude that S has a maximal element.

There is a subtle point missing: we have shown that there is a maximal element M in S containing I, but we have yet to show that this maximal element is a maximal ideal of R. Finally, suppose that L is an ideal in R with $L \supseteq M$. Since M contains J, so does L. If $L \in S$, by the maximality of M we must have $L = M$. Since L already satisfies $L \supseteq J$, if $L \notin S$ then we must have $L = R$. $\square$

[1] Note that unions of ideals are not ideals in general, but a union of totally ordered ideals *is* an ideal.

3.2 The spectrum of a ring

Definition 3.10. Let R be a ring. The **prime spectrum** of R, denoted $\operatorname{Spec}(R)$, is the set of prime ideals of R.

Definition 3.11. For a ring R and an ideal I, we set

$$V(I) := \{P \in \operatorname{Spec}(R) \mid P \supseteq I\}.$$

Proposition 3.12. *Let R be a ring, and I_λ, J be ideals, not necessarily proper.*

(0) $V(R) = \varnothing$ and $V(0) = \operatorname{Spec}(R)$.

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

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

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

Proof. Both (0) and (1) are straightforward, so we just prove (2).

To see $V(I) \cup V(J) \subseteq V(I \cap J)$, just observe that if $P \supseteq I$ or $P \supseteq J$, then $P \supseteq I \cap J$. 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 P is a prime and $P \notin V(I) \cup V(J)$, then $P \not\supseteq I, P \not\supseteq J$. Thus we can find $f \in I$, and $g \in J$ such that $f, g \notin P$. Since P is prime, $fg \notin P$, while also $fg \in IJ$. Therefore, $P \not\supseteq IJ$.

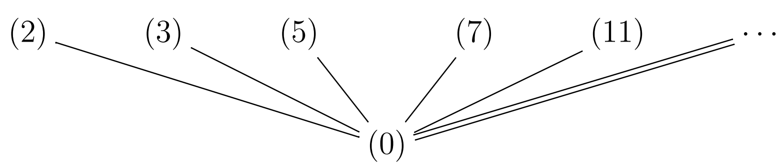
To show (3), since ideals are closed for sums, if $P \supseteq I_\lambda$ for all λ, then $P \supseteq \sum_\lambda I_\lambda$. Moreover, if $P \supseteq \sum_\lambda I_\lambda$, then in particular $P \supseteq I_\lambda$. $\square$

It follows that $\operatorname{Spec}(R)$ obtains a topology by setting the closed sets to be all sets of the form $V(I)$; this is the **Zariski topology** on $\operatorname{Spec}(R)$.

Exercise 11. Note that $\operatorname{Spec}(R)$ is also a poset under inclusion. Show that the poset structure of $\operatorname{Spec}(R)$ can be recovered from the topology as follows:

$$P \subseteq Q \quad \Leftrightarrow \quad Q \in \overline{\{P\}}.$$

Example 3.13. The spectrum of $\mathbb{Z}$ is, as a poset:



The closed sets are of the form $V((n))$, which are the whole space when $n = 0$, the empty set when $n = 1$, and any finite union of things in the top row. Any closed set that contains (0) must be all of $\operatorname{Spec}(\mathbb{Z})$.

Definition 3.14. 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 $I = \sqrt{I}$.

Remark 3.15. To see that $\sqrt{I}$ is an ideal, note that if $f^m, g^n \in I$, then

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

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

Definition 3.16. A ring R is **reduced** if it has no nonzero nilpotents.

Remark 3.17. An ideal I in R is radical if and only if R/I is reduced.

Lemma 3.18. *Let R be a ring. For any ideal I, $V(I) = V(\sqrt{I})$.*

Proof. The containment $I \subseteq \sqrt{I}$ is immediate from the definition of radical, and thus by Proposition 3.12 we have $V(I) \supseteq V(\sqrt{I})$. Now let $P \supseteq I$ be a prime ideal, and let $f \in \sqrt{I}$. By definition, there exists some n such that $f^n \in I \subseteq P$, but since P is prime, we conclude that $f \in P$. Therefore, $V(I) \subseteq V(\sqrt{I})$, and we are done. □

Lemma 3.19. *Let $R \xrightarrow{\varphi} S$ be a ring homomorphism and $P \subset S$ be a prime ideal. Then $P \cap R$ is also prime.*

Proof. Let P be a prime ideal in S. Given elements $f, g \in R$ such that $fg \in P \cap R$, then $\varphi(f)\varphi(g) = \varphi(fg) \in P$, and since P is prime, we conclude that $\varphi(f) \in P$ or $\varphi(g) \in P$. Therefore, $f \in P \cap R$ or $g \in P \cap R$. □

Definition 3.20 (Induced map on Spec)**.** Each ring homomorphism $\varphi \colon R \to S$ induces a map on spectra $\varphi^* \colon \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ given by $\varphi^*(P) = \varphi^{-1}(P) = P \cap R$.

The key point is that the preimage of a prime ideal is also prime, which we showed in Lemma 3.19.

Remark 3.21. We observe that this is not only an order-preserving map, but also it is continuous: if $U \subseteq \mathrm{Spec}(R)$ is open, we have $U = \mathrm{Spec}(R) \setminus V(I)$ for some ideal I; then for a prime Q of S,

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

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

Definition 3.22. Let I be an ideal in a ring R. A prime P is a **minimal prime** of I if P is minimal in $V(I)$. A **minimal prime of** R is a minimal element in $\mathrm{Spec}(R)$.

Lemma 3.23. *Let R be a ring, and I an ideal. Every prime P that contains I contains a minimal prime of I.*

Proof. Fix an ideal I and a prime $P \supseteq I$, and consider the set

$$S = \{Q \in V(I) \mid P \supseteq Q\},$$

which is partially ordered with $\supseteq$. On the one hand, $P \in S$, so S is nonempty. On the other hand, given any chain $\{Q_i\}_i$ in S, $Q := \bigcap_i Q_i$ is a prime ideal in R (exercise!). Moreover, Q contains I, since every Q_i contain I, and Q is contained in P, since every $Q_i \subseteq P$. Therefore, $Q \in S$, and Zorn's Lemma applies to S. By Zorn's lemma, S contains a maximal element for $\supseteq$, say Q.

Notice that Q is equivalently a minimal element for $\subseteq$. Now if Q' is a prime ideal with $I \subseteq Q' \subseteq Q$, then $Q' \subseteq Q \subseteq P$, and thus $Q' \in S$. Therefore, we must have $Q' = Q$, by maximality of Q with respect to $\supseteq$. We conclude that Q is a minimal prime of I, and by definition Q is contained in P. $\square$

Definition 3.24. 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 3.25. *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 P with $P \supseteq I$ and $P \cap W = \varnothing$.*

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

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

a contradiction. $\square$

Theorem 3.26 (Spectrum analogue of strong Nullstellensatz)**.** *Let R be a ring, and I be an ideal. For $f \in R$,*

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

Moreover

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

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

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

Now we will show that $\displaystyle\bigcap_{P \in V(I)} P = \sqrt{I}$:

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

$$f \in \sqrt{I} \implies f^n \in I \subseteq P \implies f \in P.$$

($\subseteq$): If $f \notin \sqrt{I}$, consider the multiplicatively closed set $W = \{1, f, f^2, f^3, \ldots\}$. We have $W \cap I = \varnothing$ by hypothesis. By Lemma 3.25, there is a prime P in $V(I)$ that does not intersect W, and hence P does not contain f.

Finally, $\operatorname{Min}(I) \subseteq V(I)$, and since by Lemma 3.23 every prime in $V(I)$ contains a minimal prime of I, we conclude that

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

Example 3.27. Let k be a field, $R = k[x]$, and $I = (x^2)$. On the one hand, it is immediate from the definition that $x \in \sqrt{I}$, and thus $(x) \subseteq \sqrt{I}$. On the other hand, (x) is a prime ideal that contains I, and thus by Theorem 3.26 we must have $\sqrt{I} = (x)$.

Corollary 3.28. *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 and J, we have $V(I) = V(J)$ if and only if $\sqrt{I} = \sqrt{J}$.

Proof. The closed sets of $\operatorname{Spec}(R)$ are precisely the sets of the form $V(I)$ for some ideal I. By Lemma 3.18, $V(I) = V(\sqrt{I})$, so the closed sets of $\operatorname{Spec}(R)$ are given by $V(I)$ where I ranges over all radical ideals. We showed in Proposition 3.12 that the map

$$V : \{\text{radical ideals } I \subseteq R\} \longrightarrow \{\text{closed subsets of } \operatorname{Spec}(R)\}$$

is order-reversing. Finally, suppose that I and J are ideals such that $V(I) = V(J)$. By Theorem 3.26,

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

Conversely, suppose that $\sqrt{I} = \sqrt{J}$. Given a prime $P \in V(I)$, we also have $P \in V(\sqrt{I})$, by Lemma 3.18, and thus

$$P \supseteq \sqrt{I} = \sqrt{J} \supseteq J,$$

so $P \in V(J)$. Since the same argument applies to show that $V(J) \supseteq V(I)$, we conclude that $V(I) = V(J)$. $\square$

Exercise 12. Let I and J be ideals in a ring R.

a) Show that $\sqrt{\sqrt{I}} = \sqrt{I}$.

b) Show that if $I \subseteq J$, then $\sqrt{I} \subseteq \sqrt{J}$.

c) Show that $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

d) Show that $\sqrt{I^n} = \sqrt{I}$ for all $n \geqslant 1$.

e) Show that if P is a prime ideal, then $\sqrt{P^n} = P$ for all $n \geqslant 1$.

3.3 Prime Avoidance

We will now discuss an important lemma known as Prime Avoidance. This is an elementary fact, but it is very helpful. Prime Avoidance says that if an ideal I is not contained in any of the primes $P_1, \dots, P_n$, then I cannot be contained in their union. Set-theoretically this is possible, of course; but if the ideals $P_1, \dots, P_n$ are all prime, then it is actually not possible for $I \subseteq P_1 \cup \cdots \cup P_n$ unless I is contained in one of the P_i. In fact, for this to work we can even allow two of the P_i to be just any ideals, as long as the remaining P_i are prime.

Lemma 3.29 (Prime avoidance)**.** *Let R be a ring, $I_1, \dots, I_n, J$ be ideals, and suppose that I_i is prime for $i > 2$. If $J \nsubseteq I_i$ for all i, then $J \nsubseteq \bigcup_i I_i$. 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 $J \nsubseteq I_i$ 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. When $n = 2$, we have two ideals I_1 and I_2 and an ideal J such that $J \nsubseteq I_1$ and $J \nsubseteq I_2$, and we want to show that $J \nsubseteq I_1 \cup I_2$. By assumption, there exist elements $a_1, a_2 \in J$ with $a_1 \notin I_1$ and $a_2 \notin I_2$. If $a_2 \notin I_1$ or $a_1 \notin I_2$, then we have an element that is not in $I_1 \cup I_2$, and we are done. On the other hand, if $a_2 \in I_1$ and $a_1 \in I_2$, then consider $c = a_1 + a_2 \in J$. Since $a_1 \in I_1$ but $a_2 \notin I_1$, then $c \notin I_1$. Similarly, $c \notin I_2$. Therefore, $c \notin I_1 \cup I_2$.

Now suppose that the statement holds for some $n - 1 \geqslant 2$, and consider ideals $I_1, \dots, I_n$ with I_i prime for all $i \geqslant 3$ such that $J \nsubseteq I_i$ for any i. By induction hypothesis, for each i we have

$$J \nsubseteq \bigcup_{j \neq i} I_j,$$

so we can find elements a_i such that

$$a_i \notin \bigcup_{j \neq i} I_j \text{ and } a_i \in J.$$

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 $a_n \in I_n$. Since $n > 2$, 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 $a \notin I_i$ for all i, and thus a is the element we were searching for.

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. $\square$

We will also need a slightly stronger version of Prime Avoidance.

Theorem 3.30. *Let R be a ring, $P_1, \ldots, P_n$ prime ideals, $x \in R$ and I be an ideal in R. If $(x) + I \nsubseteq P_i$ for each i, then there exists $y \in J$ such that*

$$x + y \notin \bigcup_{i=1}^{n} P_i.$$

Proof. We proceed by induction on n. When $n = 1$, if every element of the form $x + y$ with $y \in R$ is in $P = P_1$, then multiplying by $r \in R$ we conclude that every $rx + y \in P$, meaning $(x) + I \subseteq P$.

Now suppose $n > 1$ and that we have shown the statement for $n - 1$ primes. If $P_i \subseteq P_j$ for some $i \neq j$, then we might as well exclude P_i from our list of primes, and the statement follows by induction. So assume that all our primes P_i are incomparable.

If $x \notin P_i$ for all i, we are done, since we can take $x + 0$ for the element we are searching for. So suppose x is in some P_i, which we assume without loss of generality to be P_n. Our induction hypothesis says that we can find $y \in I$ such that $x + y \notin P_1 \cup \cdots \cup P_{n-1}$. If $x + y \notin P_n$, we are done, so suppose $x + y \in P_n$. Since we assumed $x \in P_n$, we must have $I \nsubseteq P_n$, or else we would have had $(x) + I \subseteq P_n$. Now P_n is a prime ideal that does not contain $P_1, \ldots, P_{n-1}$, nor I, so

$$P \nsupseteq IP_1 \cdots P_{n-1}.$$

Choose $z \in IP_1 \cdots P_{n-1}$ not in P_n. Then $x + y + z \notin P_n$, since $z \notin P_n$ but $x + y \in P_n$. Moreover, for all $i < n$ we have $x + y + z \notin P_i$, since $z \in P_i$ and $x + y \notin P_i$. $\square$

Chapter 4

Affine varieties

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

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

with $f_1, \dots, f_t \in k[x_1, \dots, x_d]$ determined by its solution set?

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 $a_1, \dots, a_d$ are the solutions to $f(z) = 0$, then 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 $g \in (f_1, \dots, f_t)$. But since $k[z]$ is a PID, we have $(f_1, \dots, f_t) = (f)$, where f is a greatest common divisor of $f_1, \dots, f_t$. Therefore, $z = a$ is a solution to the system if and only if $f(a) = 0$.

4.1 Varieties

Definition 4.2. Given a field k, the **affine d-space over k**, denoted $\mathbb{A}^d_k$, is the set

$$\mathbb{A}^d_k := \{(a_1, \dots, a_d) \mid a_i \in k\}.$$

A variety in $\mathbb{A}_k^d$ is the set of common solutions of some (possibly infinite) collection of polynomial equations.

Definition 4.3. 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:

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

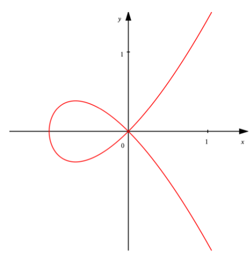
A subset of $\mathbb{A}_k^d$ of the form $\mathcal{Z}(T)$ for some subset T is called an **algebraic subset** of $\mathbb{A}_k^d$, or an **affine algebraic variety**. A variety is **irreducible** if it cannot be written as the union of two proper subvarieties.

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.

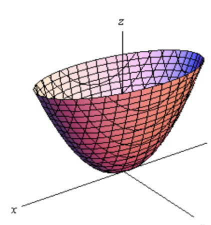
Remark 4.4. Note that if $L \supseteq k$ are both fields, any polynomial $f \in k[x_1, \ldots, x_n]$ is also an element of $L[x_1, \ldots, x_n]$, and we can evaluate it at any point in $\mathbb{A}_L^n$. Thus, we may write $\mathcal{Z}_k(T)$ or $\mathcal{Z}_L(T)$ to distinguish between the zero sets over different fields.

Example 4.5. Here are some simple examples of algebraic varieties:

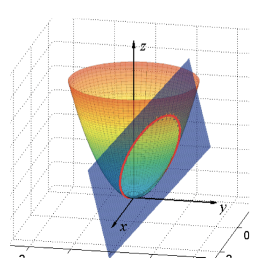
1) For $k = \mathbb{R}$ and $n = 2$, $\mathcal{Z}(y^2 - x^2(x+1))$ is a "nodal curve" in $\mathbb{A}_{\mathbb{R}}^2$, the real plane. Note that we have written x for x_1 and y for x_2 here, which is a common choice.



2) 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.



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



4) For $k = \mathbb{R}$ and $n = 3$, $\mathcal{Z}(xy, xz)$ is a line and a plane that cross transversely.

5) Over an arbitrary field k, a linear subspace of $\mathbb{A}^n_k = k^n$ is a subvariety: such a subset is defined by some linear equations.

6) For $k = \mathbb{R}$, $\mathcal{Z}_{\mathbb{R}}(x^2 + y^2 + 1) = \emptyset$. Note that $\mathcal{Z}_{\mathbb{C}}(x^2 + y^2 + 1) \neq \emptyset$, since it contains $(i, 0)$.

7) For $k = \mathbb{R}$, $\mathcal{Z}_{\mathbb{R}}(x^2 + y^2) = \{(0,0)\}$. On the other hand, $\mathcal{Z}_{\mathbb{C}}(x^2 + y^2)$ is a union of two lines in $\mathbb{C}^2$ (or two planes, in the real sense), given by the equations $x + iy = 0$ and $x - iy = 0$.

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

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

10) For $k = \mathbb{R}$ or $\mathbb{C}$, the set
$$X = \{(t, t^2, t^3) \mid t \in k\}$$
is an algebraic variety, though it is not clear from this description that that is the case. In fact, $X = \mathcal{Z}(y - x^2, z - x^3)$. To see the containment $(\subseteq)$, for $(t, t^2, t^3) \in X$, we have $t^2 - t^2 = 0$ and $t^3 - t^3 = 0$. For the containment $(\supseteq)$, let $(a, b, c) \in \mathcal{Z}(y - x^2, z - x^3)$, so $b = a^2$ and $c = a^3$. Setting $t = a$, we get that $(a, b, c) = (t, t^2, t^3) \in X$. The same argument works over $\mathbb{C}$.

11) For $k = \mathbb{R}$ or $\mathbb{C}$, we claim that the set
$$X := \{(t^3, t^4, t^5) \mid t \in \mathbb{R}\}$$
is an algebraic variety. Consider $Y = \mathcal{Z}(y^3 - x^4, z^3 - x^5)$. It is easy to see that $X \subseteq Y$. Over $\mathbb{R}$, for $(a, b, c) \in Y$, take $t = \sqrt[3]{a}$; then $a = t^3$, $b^3 = a^4$ means $b = \sqrt[3]{a}^4$, so $b = t^4$, and similarly $c = t^5$, so $X = Y$. We used uniqueness of cube roots in this argument though, so we need to reconsider over $\mathbb{C}$. Indeed, if ω is a cube root of unity, then $(1, 1, \omega) \in Y \setminus X$, so we need to do better. Let's try $Z = \mathcal{Z}(y^3 - x^4, z^3 - x^5, z^4 - y^5)$. Again, $X \subseteq Z$. Say that $(a, b, c) \in \mathbb{A}^3_{\mathbb{C}}$ are in Z, and let s be a cube root of a. Then $b^3 = a^4 = (s^4)^3$ implies that $b = \omega s^4$ for some cube root of unity ω' (maybe 1, maybe not). Similarly $c^3 = a^4 = (s^5)^3$ implies that $c = \omega'' s^5$ for some cube root of unity ω'' (maybe 1, maybe ω', maybe not). So at least $(a, b, c) = (s^3, \omega' s^4, \omega'' s^5)$. Let $t = \omega' s$. Then $(s^3, \omega' s^4, \omega'' s^5) = (t^3, t^4, \omega s^5)$, where $\omega = (\omega')^2 \omega''$ is again some cube root of unity. The equation $b^5 = c^4$ shows that $t^2 0 = \omega^5 t^2 0$. If $t \neq 0$, this shows $\omega = 1$, so $(a, b, c) = (t^3, t^4, t^5)$; if $t = 0$, then $(a, b, c) = (0, 0, 0) = (0^3, 0^4, 0^5)$. Thus, $X = Z$.

12) For any field k and elements $a_1, \dots, a_d \in k$, we have
$$\mathcal{Z}(x_1 - a_1, \dots, x_d - a_d) = \{(a_1, \dots, a_d)\}.$$
So, all one element subsets of $\mathbb{A}^d_k$ are algebraic subsets.

13) Here is an example from linear algebra. Fix a field k and consider the set of pairs (A, v) of 2×2 matrices and 2×1 vectors over k. We can again identify this with $\mathbb{A}^6_k$; let's call our variables $x_{11}, x_{12}, x_{21}, x_{22}, y_1, y_2$, where we are thinking of

$$A = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} \text{ and } v = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}.$$

The set $X := \{(A, v) \mid Av = 0\}$ is a subvariety of $\mathbb{A}^6_k$:

$$X = \mathcal{Z}(x_{11}y_1 + x_{12}y_2, x_{21}y_1 + x_{22}y_2).$$

14) Let us take another linear algebra example. We can identify the set of 2×3 matrices over a field k with $\mathbb{A}^6_k$. To make this line up a little more naturally, label our variables as $x_{11}, x_{12}, x_{13}, x_{21}, x_{22}, x_{23}$. We claim that the set X of matrices of rank strictly less than 2 is a subvariety of $\mathbb{A}^6_k$. To see this, we need to find equations.

For a 2×3 matrix A to have rank strictly less than 2, it is necessary and sufficient that each 2×2 submatrix have rank strictly less than 2, which is equivalent to each of the 2×2 minors (subdeterminants) of the matrix to be zero. Thus, if we use variables

$$\begin{bmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \end{bmatrix},$$

our variety is

$$X = \mathcal{Z}\left(x_{11}x_{22} - x_{12}x_{21}, x_{11}x_{23} - x_{13}x_{21}, x_{12}x_{23} - x_{13}x_{22}\right).$$

Proposition 4.6. *Let k be a field and $R = k[x_1, \dots, x_n]$. Let $S, T \subseteq R$ be arbitrary subsets.*

(1) If $S \subseteq T$, then $\mathcal{Z}(S) \supseteq \mathcal{Z}(T)$.

(2) If $I = (S)$ is the ideal generated by S, then $\mathcal{Z}(S) = \mathcal{Z}(I)$.

Proof. First, note that imposing more equations can only lead to a smaller the solution set, which gives (1). For (2), we have $\mathcal{Z}(I) \subseteq \mathcal{Z}(S)$ by (1). On the other hand, if $f_1, \dots, f_m \in S$ and $r_1, \dots, r_m \in R$, and $(a_1, \dots, a_n) \in \mathcal{Z}(S)$, then $f_i(a_1, \dots, a_n) = 0$ for all i. Therefore,

$$\left(\sum_i r_i f_i\right)(a_1, \dots, a_n) = \sum_i r_i(a_1, \dots, a_n) f_i(a_1, \dots, a_n) = 0,$$

so $(a_1, \dots, a_n) \in \mathcal{Z}(\sum_i r_i f_i)$. Thus, $(a_1, \dots, a_n) \in \mathcal{Z}(I)$. That is, $\mathcal{Z}(S) \subseteq \mathcal{Z}(I)$. $\square$

Given Proposition 4.6, it is sufficient to consider $\mathcal{Z}(I)$ with I varying over all ideals in $R = k[x_1, \dots, x_n]$. In other words, we will talk about the solution set of an ideal, rather than of an arbitrary set.

Notice that different ideals can determine the same variety.

Example 4.7. Let k be a field and $R = k[x]$. The varieties $\mathcal{Z}(x)$ and $\mathcal{Z}(x^2)$ are both the singleton given by the origin $\{0\}$ of $\mathbb{A}^1_k$, even though the ideals (x) and (x^2) are distinct.

Proposition 4.8. *Let k be a field and $R = k[x_1, \dots, x_n]$. Let $I, I_\lambda, J \subseteq R$ be ideals in R.*

(1) $\mathcal{Z}(R) = \mathcal{Z}(1) = \varnothing$ *and* $\mathcal{Z}(0) = \mathbb{A}^n_k$.

(2) $\bigcap_{\lambda\in\Lambda} \mathcal{Z}(I_\lambda) = \mathcal{Z}(\sum\limits_{\lambda\in\Lambda} I_\lambda)$.

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

Proof. (1) is clear, since 1 is never equal to zero and 0 is always zero.

Let's now show (2). Given sets $S_\lambda \subseteq T$, a point is a solution to all of the equations in each set S_λ if and only if it is a solution of each set of equations S_λ. Therefore,

$$\mathcal{Z}(\bigcup_{\lambda\in\Lambda} S_\lambda) = \bigcap_{\lambda\in\Lambda} \mathcal{Z}(S_\lambda).$$

Given ideals I_λ, $\sum_{\lambda\in\Lambda} I_\lambda$ is the ideal generated by $\bigcup_{\lambda\in\Lambda} I_\lambda$, and thus

$$\mathcal{Z}(\sum_{\lambda\in\Lambda} I_\lambda) = \mathcal{Z}(\bigcup_{\lambda\in\Lambda} I_\lambda) = \bigcap_{\lambda\in\Lambda} \mathcal{Z}(I_\lambda).$$

To show (3), first consider subsets $S, T \subseteq R$. We claim that

$$\mathcal{Z}(S) \cup \mathcal{Z}(T) \subseteq \mathcal{Z}(\{fg \mid f \in S, g \in T\}).$$

Indeed, $f(a_1, \dots, a_n) = 0$ for all $f \in S$ implies $f(a_1, \dots, a_n)g(a_1, \dots, a_n) = 0$ for all $f \in S$ and all $g \in T$. On the other hand, if $(a_1, \dots, a_n) \notin \mathcal{Z}(S) \cup \mathcal{Z}(T)$, then there is some $f \in S$ and some $g \in T$ with $f(a_1, \dots, a_n) \neq 0$ and $g(a_1, \dots, a_n) \neq 0$, so $f(a_1, \dots, a_n)g(a_1, \dots, a_n) \neq 0$. Therefore,

$$\mathcal{Z}(S) \cup \mathcal{Z}(T) \subseteq \mathcal{Z}(\{fg \mid f \in S, g \in T\}).$$

Now given ideals I and J, since $IJ \subseteq I \cap J \subseteq I$ and $I \cap J \subseteq J$, by (1) we get

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

On the other hand, by (2) and (4) we get

$$\mathcal{Z}(IJ) \subseteq \mathcal{Z}(\{fg \mid f \in I, g \in J\}) = \mathcal{Z}(I) \cup \mathcal{Z}(J),$$

so the equalities hold throughout. □

Proposition 4.8 allows us to define a topology on $\mathbb{A}^n_k$.

Definition 4.9. Let k be a field. The collection of subvarieties $X \subseteq \mathbb{A}^n_k$ is the collection of closed subsets in a topology on $\mathbb{A}^n_k$. This is called the **Zariski topology** on $\mathbb{A}^n_k$. Any subvariety of $\mathbb{A}^n_k$ obtains a **Zariski topology** as the subspace topology from $\mathbb{A}^n_k$.

This topology is not very similar to the Euclidean topology on a manifold; it is much coarser. In fact, this topology is typically non-Hausdorff.

Example 4.10. Let k be an infinite field. The closed subsets in the Zariski topology on $\mathbb{A}^1_k$ are just the finite subsets, along with the whole space. Note that this topology is not Hausdorff; quite on the contrary, any two nonempty open sets have infinite intersection!

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

Definition 4.11. Given any subset X of $\mathbb{A}^d_k$ for a field k, define

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

Exercise 13. $\mathcal{I}(X)$ is an ideal in $k[x_1, \dots, x_d]$ for any $X \subseteq \mathbb{A}^d_k$.

Example 4.12. For any field k, we have $\mathcal{I}((a_1, \dots, a_d)) = (x_1 - a_1, \dots, x_d - a_d)$.

Remark 4.13. For a subset $X \subseteq \mathbb{A}^n_K$ and a subset $S \subseteq K[x_1, \dots, x_n]$, we have

$$X \subseteq \mathcal{Z}(S) \Longleftrightarrow \text{each } s \in S \text{ vanishes at each } x \in X \Longleftrightarrow S \subseteq \mathcal{I}(X).$$

Theorem 4.14. *Let k be a field, and X, X_λ, Y be subsets of $\mathbb{A}^n_k$.*

(1) $\mathcal{I}(\varnothing) = R$ and, if k is infinite, $\mathcal{I}(\mathbb{A}^n_k) = 0$.

(2) If $X \subseteq Y$, then $\mathcal{I}(X) \supseteq \mathcal{I}(Y)$.

(3) $\mathcal{I}(X)$ is a radical ideal.

Proof. For (1), it is clear that $\mathcal{I}(\varnothing) = R$. Now assume k is infinite. We show by induction on n that any nonzero polynomial in $k[x_1, \dots, x_n]$ is nonzero at some point in $\mathbb{A}^n_k$. The case $n = 1$ is standard: a polynomial in $k[x]$ of degree d can have at most d roots — in particular, it cannot have infinitely many roots. Let $n \geqslant 2$ and let $f(x_1, \dots, x_n) \in k[x_1, \dots, x_n]$ be a nonzero polynomial. If f is a nonzero constant, it is nonzero at any point. Otherwise, we can assume that f nontrivially involves some variable, say x_n. Write

$$f(x_1, \dots, x_n) = f_d(x_1, \dots, x_{n-1}) x_n^d + \cdots + f_0(x_1, \dots, x_{n-1}).$$

If f is identically zero, then for every $(a_1, \dots, a_{n-1}) \in \mathbb{A}^{n-1}_k$,

$$f_d(a_1, \dots, a_{n-1}) x_n^d + \cdots + f_0(a_1, \dots, a_{n-1})$$

is a polynomial in one variable that is identically zero, so it is the zero polynomial. Thus each $f_i(a_1, \dots, a_{n-1})$ is identically zero. Since this holds for all $(a_1, \dots, a_{n-1}) \in \mathbb{A}^{n-1}_k$, by the induction hypothesis we conclude that each f_i is the zero polynomial. Therefore, $f(x_1, \dots, x_n)$ is the zero polynomial, as required.

(2) is clear from the definition of $\mathcal{I}$.

For (3), note that $f, g \in \mathcal{I}(X)$ and $r \in R$ implies $X \subseteq \mathcal{Z}(f, g)$ implies $X \subseteq \mathcal{Z}(rf + g)$ implies $rf + g \in \mathcal{I}(X)$, so $\mathcal{I}(X)$ is an ideal. If $f^t \in \mathcal{I}(X)$, then $f(a_1, \dots, a_n)^t = 0$ for all $(a_1, \dots, a_n) \in X$, so $f(a_1, \dots, a_n) = 0$ for all $(a_1, \dots, a_n) \in X$, and $f \in \mathcal{I}(X)$. □

Determining $\mathcal{I}(X)$ can be very difficult; there was already some work involved in settling $\mathcal{I}(\mathbb{A}^n_K)$! We will explore the relationship between the associations $\mathcal{Z}$ and $\mathcal{I}$ more soon.

4.2 The coordinate ring of a variety

The natural condition for a reasonable map between two varieties is that it should also be made from polynomials.

Definition 4.15. Suppose X is a subvariety of $\mathbb{A}_k^m$ and Y is a subvariety of $\mathbb{A}_l^n$. A **morphism of varieties** or **algebraic map** or **regular map** from X to Y is a function $\phi : X \to Y$ defined coordinatewise by polynomials $g_1, \ldots, g_n \in k[x_1, \ldots, x_m]$, that is

$$\phi(a_1, \ldots, a_m) = (g_1(a_1, \ldots, a_m), \ldots, g_n(a_1, \ldots, a_m)) \text{ for all } \mathbf{a} \in \mathbf{X}.$$

A morphism of varieties $\phi : X \to Y$ is an **isomorphism** if there is some morphism of varieties $\phi : Y \to X$ such that $\phi \circ \psi = \mathrm{id}_Y$ and $\psi \circ \phi = \mathrm{id}_X$.

Not every choice of $g_1, \ldots, g_n$ will give such a morphism, because the tuple $(g_1(\mathbf{a}), \ldots, g_n(\mathbf{a}))$ has to satisfy the equations of Y. Furthermore, different choices of $g_1, \ldots, g_n$ may yield the same morphism.

Example 4.16.

a) Let k be an infinite field. Consider $X = \mathcal{Z}(xy - 1) \subseteq \mathbb{A}_k^2$ (i.e., X is a hyperbola) and define $\phi : X \to \mathbb{A}_k^1$ by $\phi(a, b) = a$. Then ϕ is an algebraic map (indeed, it is given by a linear polynomial) and its image is $\mathbb{A}_k^1 \setminus \{0\}$, which is *not* an algebraic subset of $\mathbb{A}_k^1$. So the set-theoretic image of a morphism of varieties need not be a variety.

b) Take an infinite field, and let Y be the classical cuspidal curve:

$$Y = \mathcal{Z}(y^2 - x^3) \subseteq \mathbb{A}_k^2.$$

Define

$$\phi : \mathbb{A}_K^1 \to Y \quad \phi(t) = (t^2, t^3).$$

This ϕ is an algebraic map from $\mathbb{A}_K^1$ to Y, since the component functions are polynomial functions of t and $(t^3)^2 - (t^2)^3 = 0$ for all t.

Note that this ϕ is a bijection of sets. However, it is not an isomorphism. Indeed, if it were, we would have some map ψ such that $\psi \circ \phi = \mathrm{id}_{\mathbb{A}_K^1}$. This ψ would be given by a polynomial h in two variables such that $h(t^2, t^3) = t$. It is easy to see that no such h exists.

c) Consider $\mathbb{A}_k^6$ as the space of 2×3 matrices over K with coordinates $x_{11}, \ldots, x_{23}$, and consider $\mathbb{A}_K^5$ as the space of pairs of 2×1 and 1×3 matrices over K with coordinates y_1, y_2, z_1, z_2, z_3. The map of matrix multiplication from $\mathbb{A}_k^5$ to $\mathbb{A}_k^6$ is a regular map:

$$(y_1, y_2, z_1, z_2, z_3) \mapsto \begin{bmatrix} y_1 z_1 & y_1 z_2 & y_1 z_3 \\ y_2 z_1 & y_2 z_2 & y_2 z_3 \end{bmatrix}.$$

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

Definition 4.17. Let k be a 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.

Since $\mathcal{I}(X)$ is a radical ideal, the coordinate ring $k[X]$ is necessarily a reduced, finitely generated k-algebra.

Definition 4.18. An **affine k-algebra** is any ring of the form

$$k[x_1, \ldots, x_n]/I \text{ for some ideal } I \subseteq k[x_1, \ldots, x_n].$$

Definition 4.19. Let k be a field. Let $X \subseteq \mathbb{A}^m_k$ and $Y \subseteq \mathbb{A}^n_k$ be affine varieties. Let $\phi : X \to Y$ be a morphism given by $(g_1(x), \ldots, g_n(x))$, with $g_i \in k[x_1, \ldots, x_m]$. We define

$$\begin{aligned} k[Y] &\xrightarrow{\quad\phi^*\quad} k[X] \\ f(y_1, \ldots, y_n) &\longmapsto f(g_1(x), \ldots, g_n(x)) \end{aligned}.$$

Alternatively, thinking of $f \in k[Y]$ as a regular map from $Y \to A^1_k$, we have

$$\begin{aligned} k[Y] &\xrightarrow{\quad\phi^*\quad} k[X] \\ Y \xrightarrow{f} \mathbb{A}^1_k &\leadsto X \xrightarrow{f\phi} \mathbb{A}^1_k \\ &\qquad\quad \| \\ &\quad X \xrightarrow{\phi} Y \xrightarrow{f} \mathbb{A}^1_k \end{aligned}$$

We may call this the **homomorphism induced by** ϕ or the **pullback** of ϕ.

Exercise 14. Show that the rule ϕ^* is a well-defined ring homomorphism, and that the map $\phi \mapsto \phi^*$ is well-defined.

Exercise 15. For any field k, there is a contravariant functor from affine varieties over k to affine k-algebras that

- on objects, maps a variety X to its coordinate ring $k[X]$,
- on morphisms, maps a morphism of varieties $X \xrightarrow{\phi} Y$ to its pullback $k[Y] \xrightarrow{\phi^*} k[X]$.

Example 4.20. We saw before that

$$X = \{(t, t^2, t^3) \mid t \in k\}$$

is a subvariety of $\mathbb{A}^3_k$. Thus its coordinate ring is of the form $k[X] = k[x, y, z]/\mathcal{I}(X)$. To compute $\mathcal{I}(X)$, note that the polynomials $f \in k[x, y, z]$ that vanish at every point of X are precisely the polynomials in the kernel of the map $k[x, y, z] \to k[t]$ given by $x \mapsto t$, $y \mapsto t^2$, and $z \mapsto t^3$. Then one can show that $\mathcal{I}(X) = (x^2 - y, x^3 - z)$. For an explicit field like $\mathbb{R}$ or $\mathbb{C}$, we can also compute this kernel in Macaulay2.

Notice, in fact, that $k[X] \cong k[t, t^2, t^3]$.

Example 4.21. Fix a field k, and let $R = k[x,y,z]$. Consider the ideal P given by

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

We will show that the ring homomorphism

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

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

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

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

This shows that P is the kernel of the map

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

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

We showed in Example 4.5 (11) that $\mathcal{Z}(P)$ is the variety

$$X = \{(t^3,t^4,t^5) \mid t \in k\}.$$

Thus we conclude that

$$\mathcal{I}(X) = P = \left(x^3 - yz, y^2 - xz, z^2 - x^2 y\right),$$

and that $k[t^3,t^4,t^5] \cong k[x,y,z]/P$ is the coordinate ring $k[X]$.

4.3 Nullstellensatz

Lemma 4.22. *Let k be a field, and $R = k[x_1, \ldots, x_d]$ be a polynomial ring. There is a bijection*

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

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 $(x_1 - a_1, \ldots, x_d - a_d) = \mathfrak{m}$. $\square$

Example 4.23. 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. Thanks to Zariski's Lemma, if L is a field and a finitely generated k-algebra, then $L = k$. Therefore, the quotient of $k[x_1, \ldots, x_d]$ by any maximal ideal must be isomorphic to k.

Corollary 4.24 (Nullstellensatz)**.** *Let $S = k[x_1, \ldots, x_d]$ be a polynomial ring over an algebraically closed field k. There is a bijection*

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

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

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

Proof. The first part follows immediately from Lemma 4.22 and Zariski's Lemma. Since we skipped the proof of Zariski's Lemma, we give a proof of the case when k is an uncountable field.

Let k be an uncountable algebraically closed field and $\mathfrak{m}$ be any maximal ideal in R. Suppose that $L := R/\mathfrak{m} \ncong k$. Then there exists some element $\alpha \in L$ that is transcendental over k, since k is algebraically closed and L is an extension of k. Now consider the set

$$S = \left\{ \frac{1}{\alpha - c} \mid c \in k \right\}.$$

If S is a linearly dependent set over k, then we can find finitely many $b_1, \dots, b_n, c_1, \dots, c_n \in k$ such that

$$\frac{b_1}{\alpha - c_1} + \cdots + \frac{b_n}{\alpha - c_n} = 0.$$

Rewriting the left side as one fraction, the numerator is a polynomial in α with coefficients in k. But α is transcendental over k, so S is a linearly independent set. But k is uncountable, so S is uncountable, and that means that $\dim_k(L)$ is uncountable. On the other hand, L is by construction algebra-finite over k. Since k is a field, being algebra-finite and module-finite over k are equivalent conditions, and thus L should be a finite dimensional vector space over k. This is a contradiction, so we cannot have any transcendental element over k in L. Since k is algebraically closed, we conclude that $k = L$.

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 $(x_1 - a_1, \dots, x_d - a_d)$ with $I \subseteq (x_1 - a_1, \dots, x_d - a_d)$. These are in bijection with the points $(a_1, \dots, a_d) \in \mathbb{A}_k^d$ satisfying $(a_1, \dots, a_d) \in \mathcal{Z}_k(I)$. □

Theorem 4.25 (Weak Nullstellensatz)**.** *Let k be an algebraically closed field. If I is a proper ideal in $R = k[x_1, \dots, x_d]$, then $\mathcal{Z}_k(I) \neq \varnothing$.*

Proof. If $I \subseteq R$ is a proper ideal, then by Theorem 3.8 there is a maximal ideal $\mathfrak{m} \supseteq I$, so $\mathcal{Z}(\mathfrak{m}) \subseteq \mathcal{Z}(I)$. Since $\mathfrak{m} = (x_1 - a_1, \dots, x_d - a_d)$ for some $a_i \in k$, $\mathcal{Z}(\mathfrak{m})$ is a point, and thus nonempty. □

Over an algebraically closed field, maximal ideals in $k[x_1, \dots, x_d]$ 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 4.26. 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 4.27 (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

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

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

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

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

$$\begin{cases} f_1(\underline{x}) = 0 \\ \vdots \\ f_m(\underline{x}) = 0 \\ yg_1(\underline{x}) \cdots g_n(\underline{x}) - 1 = 0 \end{cases}$$

Theorem 4.28 (Strong Nullstellensatz)**.** *Let $R = k[x_1, \dots, x_d]$ be a polynomial ring over an algebraically closed field k. 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 $n \geqslant 1$. In particular, $\mathcal{I}(\mathcal{Z}(J)) = \sqrt{J}$.*

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 $I = (g_1(\underline{x}), \dots, g_m(\underline{x}))$, 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. □

Remark 4.29. 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 $\sqrt{IJ} = \sqrt{I \cap J}$.

Corollary 4.30. *Let k be an algebraically closed field. The associations $\mathcal{Z}$ and $\mathcal{I}$ induce order-reversing bijections*

$$\begin{array}{ccc} \underline{\textit{in } k[x_1, \dots, x_n]} & & \underline{\textit{in } \mathbb{A}^n_k} \\ \{\textit{radical ideals}\} & \overset{\mathcal{Z}}{\underset{\mathcal{I}}{\rightleftarrows}} & \{\textit{varieties}\} \\ \{\textit{prime ideals}\} & \overset{\mathcal{Z}}{\underset{\mathcal{I}}{\rightleftarrows}} & \{\textit{irred vars}\} \\ \{\textit{maximal ideals}\} & \overset{\mathcal{Z}}{\underset{\mathcal{I}}{\rightleftarrows}} & \{\textit{points}\}. \end{array}$$

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

Likewise, for any variety X over an algebraically closed field, we have order-reversing bijections

$$\begin{array}{ccc}
\underline{\text{in } k[X]} & & \underline{\text{in } X} \\
\{\textit{radical ideals}\} & \leftrightarrows & \{\textit{subvarieties}\} \\
\{\textit{prime ideals}\} & \leftrightarrows & \{\textit{irred subs}\} \\
\{\textit{maximal ideals}\} & \leftrightarrows & \{\textit{points}\}.
\end{array}$$

Under this bijection, irreducible varieties correspond to prime ideals.

Lemma 4.31. *A variety $X \subseteq \mathbb{A}_k^d$ 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

$$V_f = \mathcal{Z}(f) \cap X = \mathcal{Z}(\mathcal{I}(X) + (f)) \quad \text{and} \quad V_g = \mathcal{Z}(g) \cap X = \mathcal{Z}(\mathcal{I}(X) + (g))$$

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. $\square$

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.

Example 4.32. 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 $R = k[x_1, \dots, x_d]$	$\longleftrightarrow$	geometry of $\mathbb{A}^d$
radical ideals	$\longleftrightarrow$	varieties
prime ideals	$\longleftrightarrow$	irreducible varieties
maximal ideals	$\longleftrightarrow$	points
(0)	$\longleftrightarrow$	variety $\mathbb{A}^d$
$k[x_1, \dots, x_d]$	$\longleftrightarrow$	variety $\varnothing$
$(x_1 - a_1, \dots, x_d - a_d)$	$\longleftrightarrow$	point $\{(a_1, \dots, a_d)\}$
smaller ideals	$\longleftrightarrow$	larger varieties
larger ideals	$\longleftrightarrow$	smaller varieties

Chapter 5

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 have graded analogues: in some ways, $\mathbb{N}$-graded k-algebras and their homogeneous ideals behave like a local ring, where the homogenous maximal ideal plays the role of the maximal ideal.

5.1 Local rings

Definition 5.1. 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 5.2. *A ring R is local if and only if the set of nonunits of R forms an ideal.*

Proof. If R is a local with maximal ideal $\mathfrak{m}$, then every nonunit must be in $\mathfrak{m}$, and $\mathfrak{m}$ contains no nonunits, so $\mathfrak{m}$ must be the set of nonunits. Conversely, if the set of nonunits is an ideal, that must be the only maximal ideal, since any other element in R is a unit. □

Example 5.3.

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

b) The ring of power series $k[\![\underline{x}]\!]$ over a field k is local. Indeed, one can show that a power series has an inverse if and only if its constant term is nonzero; this can be done explicitly, by writing down the conditions for a power series to be the inverse of another. The unique maximal ideal is $(\underline{x})$.

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

d) 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).

e) The ring of complex power series holomorphic at the origin, $\mathbb{C}\{\underline{x}\}$, is local. One can show 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 5.4. 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 5.5. *Let $(R, \mathfrak{m}, k)$ be a local ring. Then one of the following holds:*

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

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

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

4) $\operatorname{char}(R) = p^n$, $\operatorname{char}(k) = p$ *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. $\square$

Remark 5.6. 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.

5.2 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 5.7. Let R be a ring.

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

2) If $P \subseteq R$ is a prime ideal, the set $W = R \setminus P$ is multiplicative: this is an immediate translation of the definition.

3) An element that is not a zerodivisor is called a **nonzerodivisor** or **regular element**. The set of regular elements in R forms a multiplicatively closed subset.

Remark 5.8. 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 5.9 (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 $R \longrightarrow W^{-1}R$. This is the contraction of I into R via the canonical map. Given an ideal I in R, we write

$$W^{-1}I := \left\{ \frac{a}{w} \mid a \in I, w \in W \right\}$$

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 5.10. Note that if R is a domain, the equivalence relation simplifies to $rw' = r'w$, so $R \subseteq W^{-1}R \subseteq \operatorname{Frac}(R)$, and in particular $W^{-1}R$ is a domain too. In particular, $\operatorname{Frac}(R)$ 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 5.11. *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:*

$$\begin{tikzcd} R \arrow[r] \arrow[d] & W^{-1}R \arrow[dl, "\alpha"] \\ S & \end{tikzcd}$$

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

Example 5.12 (Most important localizations)**.** Let R be a ring.

1) For $f \in R$ and $W = \{1, f, f^2, f^3, \dots\} = \{f^n \mid n \geqslant 0\}$, we usually write R_f for $W^{-1}R$.

2) 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).

3) For a prime ideal P in R, we generally write R_P for $(R \setminus P)^{-1}R$, and call it **the localization of** R **at** P. Given an ideal I in R, we sometimes write I_P to refer to IR_P, the image of I via the canonical map $R \to R_P$. Notice that when we localize at a prime P, the resulting ring is a local ring (R_P, P_P). We can think of the process of localization at P as *zooming in* at the prime P. Many properties of an ideal I can be checked *locally*, by checking them for IR_P for each prime $P \in V(I)$.

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

Example 5.13.

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

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

the **local ring of the point** $\underline{0} \in X$; some people write this as $\mathcal{O}_{X,\underline{0}}$. 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 $\underline{a} \in X$.

Lemma 5.14. *Let W be multiplicatively closed in R.*

1) If I is an ideal in R, then $W^{-1}I = IW^{-1}R$.

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

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

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

5) 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. 1) Note that

$$W^{-1}I = \left\{ \frac{a}{w} \mid a \in I, w \in W \right\},$$

while $IW^{-1}R$ is the ideal generated by all the elements of the form

$$a \cdot \frac{s}{w} \qquad \text{where } s \in R, w \in W, a \in I.$$

Since we can rewrite

$$a \cdot \frac{s}{w} = \frac{sa}{w}$$

and $sa \in I$, we conclude that $W^{-1}I = IW^{-1}R$.

2) If $wr \in I$ for some $w \in W$, then

$$\frac{r}{1} = \frac{wr}{w} \in W^{-1}I.$$

Conversely, if $r \in W^{-1}I \cap R$, then that means that

$$\frac{r}{1} = \frac{a}{w} \text{ for some } a \in I, w \in W.$$

By definition of the equivalence relation defining $W^{-1}R$, this means that there exists $u \in W$ such that

$$u(rw - a \cdot 1) = 0 \Leftrightarrow r(uw) = ua \in I.$$

Since W is multiplicatively closed, $uw \in W$, and thus the element $t := uw \in W$ satisfies $tr \in I$.

3) 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 it is a unit multiple of an element of J, and thus $a \in J \cap R$, so $\frac{a}{w} \in W^{-1}(J \cap R)$.

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

5) First, by part 4), the map $P \mapsto W^{-1}P$, for $S = \{P \in \mathrm{Spec}(R) \mid P \cap W = \varnothing\}$ sends primes to primes. We claim that

$$\begin{array}{ccc} \mathrm{Spec}(W^{-1}R) & & S \\ Q & \longmapsto & Q \cap R \\ W^{-1}P & \longleftarrow\!\shortmid & P \end{array}$$

are inverse maps.

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

If $W \cap P = \varnothing$, then using part 2) and the definition of prime, we have that

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

Corollary 5.15. *Let R be a ring and P be a prime ideal in R. The map on Spectra induced by the canonical map $R \to R_P$ corresponds to the inclusion*

$$\{\mathfrak{q} \in \mathrm{Spec}(R) \mid \mathfrak{q} \subseteq P\} \subseteq \mathrm{Spec}(R).$$

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

Definition 5.16. 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

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

We will use the notations M_f and M_P analogously to R_f and R_P.

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

Example 5.17. 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

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

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

Definition 5.18. The **annihilator** of a module M is the ideal

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

Definition 5.19. 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-module A, the colon of N and M is

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

Exercise 16. 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 5.20. If $M = Rm$ is a cyclic 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 5.21. 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 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 5.22. If $N \subseteq M$ are R-modules, then $\operatorname{ann}(M/N) = (N :_R M)$.

Lemma 5.23. *Let M be an R-module, and W a multiplicative set. Then*

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

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 5.24. As a consequence of Lemma 5.23, it follows that if R is a domain, then the canonical map $R \to W^{-1}R$ is always injective for any multiplicatively closed set W, since every nonzero $r \in R$ has $\operatorname{ann}(r) = 0$. Notice, however, that even when R is a domain, the elements in a module M may still have nontrivial annihilators, and thus $M \to W^{-1}M$ may fail to be injective.

Remark 5.25. 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 $W^{-1}\alpha(\frac{m}{w}) = \frac{\alpha(m)}{w}$.

Lemma 5.26 (Hom and localization)**.** *Let R be a noetherian ring, W be a multiplicative set, M be a finitely generated R-module, and N an arbitrary R-module. Then,*

$$\operatorname{Hom}_{W^{-1}R}(W^{-1}M, W^{-1}N) \cong W^{-1}\operatorname{Hom}_R(M, N).$$

In particular, if P is prime,

$$\operatorname{Hom}_{R_P}(M_P, N_P) \cong \operatorname{Hom}_R(M, N)_P.$$

Proving this lemma actually requires some homological algebra that we do not have, so for now we will just believe it. Similarly, we will black box the fact that localization has good homological properties: it's an exact functor.

Theorem 5.27. *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 5.28. It follows from Lemma 5.23 that if $N \xrightarrow{\alpha} M$ is injective, then $W^{-1}\alpha$ is also injective, since

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

So this explains some of Theorem 5.27, since it shows that localization preserves inclusions.

Remark 5.29. Given a submodule N of M, we can apply Theorem 5.27 to the short exact sequence

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

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

We want to collect one more lemma for later.

Lemma 5.30. *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 $W^{-1}(N_1 \cap \cdots \cap N_t)$. $\square$

5.3 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 5.31. *Let R be a ring, I an ideal, and M a finitely generated R-module. If $IM = M$, then:*

1) there is an element $r \in 1 + I$ such that $rM = 0$, and

2) 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 $v = [m_i]$, we have a matrix equation $Av = v$. By the Determinantal trick, the element $\det(I_{s\times s} - A) \in R$ kills each m_i, and hence it kills M. Since $\det(I_{s\times s} - A) \equiv \det(I_{s\times s}) \equiv 1(\pmod I)$, this determinant is the element r we seek for the first statement. For the latter statement, set $a = 1 - r$, which is in I and satisfies $am = m - rm = m$ for all $m \in M$. □

Theorem 5.32 (NAK)**.** *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 Proposition 5.31, 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 $M = 0$. □

Theorem 5.33 (NAK)**.** *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 Theorem 5.32, $M = N$. □

Theorem 5.34 (NAK)**.** *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 ($\implies$) is clear. If $m_1, \ldots, m_s \in M$ are such that $\overline{m_1}, \ldots, \overline{m_s}$ generate $M/\mathfrak{m}M$, consider $N = Rm_1 + \cdots + Rm_s \subseteq M$. Since $M/\mathfrak{m}M$ is generated by the image of N, we have $M = N + \mathfrak{m}M$. By Theorem 5.32, $M = N$. □

Remark 5.35. Since $R/\mathfrak{m}$ is a field, $M/\mathfrak{m}M$ is a vector space over the field $R/\mathfrak{m}$.

Definition 5.36. 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 bases for vector spaces, we conclude the following:

Lemma 5.37. *Let $(R, \mathfrak{m}, k)$ be a local ring and M be a finitely generated module. Any generating set for M contains a minimal generating set, and every minimal generating set has the same cardinality.*

Definition 5.38. 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 5.39. *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. If $M \neq 0$, then M has a nonzero homogeneous element. Suppose $M_a \neq 0$. 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. Thus $(R_+)M \neq M$. □

This condition includes all finitely generated $\mathbb{Z}$-graded R-modules.

Remark 5.40. 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 5.41. *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 $M/(R_+)M$ span $M/(R_+)M$ as a vector space over R_0. 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 5.42. 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

$$\mu(M) := \dim_{R/R_+} (M/R_+M) .$$

Macaulay2. In Macaulay2, the command `mingens` returns the a minimal generating set of the given module (as a list), while `numgens` returns the minimal number of generators. Notice that this computation is only reliable if the ring and module you are considering are defined to be graded.

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 6

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 $V(P_i)$ for prime ideals P_i.

6.1 Minimal primes and support

Recall the definition of minimal primes that we discussed before.

Definition 6.1. Let I be an ideal in a ring R. A **minimal prime** of I is a minimal element (with respect to containment) in $V(I)$. More precisely, P is a minimal prime of I if the following hold:

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

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

The **minimal primes of** R are the primes that are minimal in $\operatorname{Spec}(R)$, and it is denoted $\operatorname{Min}(R)$. Note that these are precisely the minimal primes over the ideal (0). The nilpotent elements of a ring R are exactly the elements in every minimal prime of R. The radical of (0) is often called the **nilradical** of R, denoted $\mathcal{N}(R)$.

Remark 6.2. If P is prime, then $\operatorname{Min}(P) = \{P\}$. Also, since $V(I) = V(\sqrt{I})$, we have $\operatorname{Min}(I) = \operatorname{Min}(\sqrt{I})$.

Example 6.3. Let k be a field and $R = k[x, y]$. Every prime containing $I = (x^2, xy)$ must contain x^2, and thus x. On the other hand, (x) is a prime ideal containing I. Therefore, I has a unique minimal prime, and $\operatorname{Min}(I) = \{(x)\}$.

We showed in Theorem 3.26 that

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

Example 6.4. Let k be a field. The radical of the ideal $I = (x^2, xy)$ in the ring $R = k[x, y]$ from Example 6.3 is $\sqrt{I} = (x)$. We saw before that $\operatorname{Min}(I) = \{(x)\}$.

The nilradical of $R = k[x, y]/(x^2, xy)$ corresponds to the radical of (x^2, xy) in $k[x, y]$, so it is the ideal $(x)/(x^2, xy)$.

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

Theorem 6.5. *Over a noetherian ring R, every ideal I has finitely many minimal primes, and thus $\sqrt{I}$ is a finite intersection of primes.*

Proof. Let $S = \{\text{ideals } I \subseteq R \mid \operatorname{Min}(I) \text{ is infinite}\}$, and suppose, to obtain a contradiction, that $S \neq \varnothing$. Since R is noetherian, S has a maximal element J, by Proposition 1.50. If J was a prime ideal, then $\operatorname{Min}(J) = \{J\}$ would be finite, by Remark 6.2, so J is not prime. However, $\operatorname{Min}(J) = \operatorname{Min}(\sqrt{J})$, 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

$$\sqrt{J + (a)} = P_1 \cap \cdots \cap P_t \text{ and } \sqrt{J + (b)} = P_{t+1} \cap \cdots \cap P_s$$

for some prime ideals 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

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

Thus

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

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

$$J = \sqrt{J + (a)} \cap \sqrt{J + (b)} = P_1 \cap \cdots \cap P_t \cap P_{t+1} \cap \cdots \cap P_s.$$

By Lemma 6.7, we see that $\operatorname{Min}(J)$ must be a subset of $\{P_1, \ldots, P_s\}$, so it is finite. $\square$

Lemma 6.6. *If $\operatorname{Min}(I) = \{P_1, \ldots, P_n\}$, no P_i can be deleted in the intersection $P_1 \cap \cdots \cap P_n$.*

Proof. Suppose that we can delete P_i, meaning that

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

Then

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

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

Lemma 6.7. *Let I be an ideal in R. If $I = P_1 \cap \cdots \cap P_n$ where each P_i is prime and $P_i \not\subseteq P_j$ for each $i \neq j$, then $\operatorname{Min}(I) = \{P_1, \ldots, P_n\}$. Moreover, I must be radical.*

Proof. If Q is a prime containing I, then $Q \supseteq (P_1 \cap \cdots \cap P_n)$. We claim that Q must contain one of the P_i. Indeed, if $Q \not\supseteq P_i$ for all i, then there are elements $f_i \in P_i$ such that $f_i \notin Q$, so their product satisfies $f_1 \cdots f_n \in (P_1 \cap \cdots \cap P_n)$ but $f_1 \cdots f_n \notin Q$. This is a contradiction, so indeed any prime containing I must contain some P_i. Therefore, any minimal prime of I must be one of the P_i. Since we assumed that the P_i are incomparable, these are exactly all the minimal primes of I. By assumption, I coincides with the intersection of its minimal primes, which is $\sqrt{I}$ by Theorem 3.26. Therefore, $I = \sqrt{I}$. □

Remark 6.8. If $I = P_1 \cap \cdots \cap P_n$ for some primes P_i, we can always delete unnecessary components until no component can be deleted. Therefore, $\operatorname{Min}(I) \subseteq \{P_1, \ldots, P_n\}$.

As a consequence of Lemma 6.6 and Lemma 6.7, if I is a radical ideal, there is a unique way to write I as a finite intersection of incomparable prime ideals. Moreover, Lemma 6.7, Theorem 6.5, and Theorem 3.26 also imply that an ideal I is equal to a finite intersection of primes if and only if I is radical.

We now wish to understand modules in a similar way.

Definition 6.9. If M is an R-module, the **support** of M is

$$\operatorname{Supp}(M) := \{P \in \operatorname{Spec}(R) \mid M_P \neq 0\}.$$

Proposition 6.10. *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 $M = Rm_1 + \cdots + Rm_n$. We have

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

so by Proposition 3.12,

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

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 $(Rm_i)_P \subseteq M_P$, so

$$P \in \operatorname{Supp}(Rm_i) \implies 0 \neq (Rm_i)_P \subseteq M_P \implies P \in \operatorname{Supp}(M).$$

On the other hand, the images of $m_1, \ldots, m_n$ in M_P generate M_P for each P, and thus $P \in \operatorname{Supp}(M)$ if and only if $P \in \operatorname{Supp}(Rm_i)$ for some m_i. Thus, we can reduce the equality $\operatorname{Supp}(M) = V(\operatorname{ann}_R(M))$ to the case of a cyclic module Rm. By Lemma 5.23, $\frac{m}{1} = 0$ in M_P if and only if $(R \setminus P) \cap \operatorname{ann}_R(m) \neq \varnothing$, which is equivalent to $\operatorname{ann}_R(m) \not\subseteq P$. □

The finitely generated hypothesis is necessary!

Example 6.11. 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.

Any element of M is killed by a large power of x, so $W^{-1}M = 0$ whenever W is a multiplicatively closed subset of R with $W \ni x$. Therefore, if $P \in \operatorname{Supp}(M)$, then $x \in P$, and thus $\operatorname{Supp}(M) \subseteq \{(x)\}$. We will soon see, in Corollary 6.16, 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, $V(\operatorname{ann}_R(M)) = \operatorname{Spec}(R)$, while $\operatorname{Supp}(M) = \{(x)\} \neq \operatorname{Spec}(R)$.

Example 6.12. 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 6.13. *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 5.27, so for any P,

$$0 \longrightarrow L_P \longrightarrow M_P \longrightarrow N_P \longrightarrow 0$$

is exact. If $P \in \operatorname{Supp}(L) \cup \operatorname{Supp}(N)$, then L_P or N_P is nonzero, so M_P must be nonzero as well. On the other hand, if $P \notin \operatorname{Supp}(L) \cup \operatorname{Supp}(N)$, then $L_P = N_P = 0$, so $M_P = 0$. $\square$

Remark 6.14. As a corollary of Lemma 6.13, given modules $L \subseteq M$, $\operatorname{Supp}(L) \subseteq \operatorname{Supp}(M)$.

Lemma 6.15. *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_P *for all* $P \in \operatorname{Spec}(R)$.

3) $\frac{m}{1} = 0$ *in* M_P *for all* $P \in \operatorname{mSpec}(R)$.

Proof. The implications 1) $\Rightarrow$ 2) $\Rightarrow$ 3) are clear. To show 3) $\Rightarrow$ 1), we prove the contrapositive. Given $m \neq 0$, its annihilator is a proper ideal, which must be contained in a maximal ideal by Theorem 3.8. In particular, $V(\operatorname{ann}_R m) = \operatorname{Supp}(Rm)$ contains a maximal ideal, say P, so $\frac{m}{1} \neq 0$ in M_P. □

Corollary 6.16. *If M is an R-module, the following are equivalent:*

1) $M = 0$.

2) $M_P = 0$ *in* M_P *for all* $P \in \operatorname{Spec}(R)$.

3) $M_P = 0$ *in* M_P *for all* $P \in \operatorname{mSpec}(R)$.

Therefore, $\operatorname{Supp}(M) \neq \varnothing$ *for any R-module* $M \neq 0$.

Proof. The implications $\Rightarrow$ are clear. To show 3) $\Rightarrow$ 1), we show the contrapositive. If $m \neq 0$, consider $Rm \subseteq M$. By Lemma 6.15, there is a maximal ideal in $\operatorname{Supp}(Rm)$, and by Lemma 6.13 applied to the inclusion $Rm \subseteq M$, this maximal ideal is in $\operatorname{Supp}(M)$ as well. □

6.2 Associated primes

Remark 6.17. 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 $I \subseteq \operatorname{ann}(m)$. The kernel of the map $R \to M$ given by $1 \mapsto m$ is precisely $\operatorname{ann}(m)$, so a well-defined map $R/I \to M$ given by $1 \mapsto m$ is injective if and only if $I = \operatorname{ann}(m)$.

Definition 6.18. Let R be a ring and M an R-module. We say that $P \in \operatorname{Spec}(R)$ is an **associated prime** of M if $P = \operatorname{ann}_R(m)$ for some $m \in M$. Equivalently, P is associated to M if there is an injective homomorphism $R/P \longrightarrow M$. We write $\operatorname{Ass}_R(M)$ 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 the R-module R/I.

Example 6.19. Let k be a field and let $R = k[\![x,y]\!]$. Consider ideal $I = (x^2, xy)$ and the R-module $M = R/I$. The element $x + I$ in M is killed by both x and y, and thus $(x,y) \subseteq \operatorname{ann}(x+I)$. On the other hand, $x + I \neq 0$, so $\operatorname{ann}(x+I) \neq R$. Since (x,y) is the unique maximal ideal in R, we conclude that $\operatorname{ann}(x+I) = (x,y)$. In particular, $(x,y) \in \operatorname{Ass}(M)$. Since $M = R/I$, this also says that (x,y) is an associated prime of I.

Lemma 6.20. *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 $P_P \in \operatorname{Ass}(M_P)$.*

Proof. Localization is exact, by Theorem 5.27, so any inclusion $R/P \subseteq M$ localizes to an inclusion $R_P/P_P \subseteq M_P$. Conversely, suppose that $P_P = \operatorname{ann}(\frac{m}{w})$ for some $\frac{m}{w} \in M_P$. Let $P = (f_1, \ldots, f_n)$. For each i, since $\frac{f_i}{1}\frac{m}{w} = \frac{0}{1}$, 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 $r \in \operatorname{ann}(um)$, then $\frac{ru}{1} \in \operatorname{ann}(\frac{m}{w}) = P_P$. We conclude that $ru \in P_P \cap R = P$. Since $u \notin P$ and P is prime, we conclude that $r \in P$. $\square$

Lemma 6.21. *If P is prime,* $\operatorname{Ass}_R(R/P) = \{P\}$.

Proof. For any nonzero $r + P \in R/P$, we have $\operatorname{ann}_R(r+P) = \{s \in R \mid rs \in P\} = P$ by definition of prime ideal. $\square$

However, R/I might have a unique associated prime even if I is not prime.

Example 6.22. Let k be a field and $R = k[\![x]\!]$. Consider the ideal $I = (x^2)$, and the R-module $M = R/I$. If P is a prime ideal in R and P is associated to M, then $P = \operatorname{ann}(r+I)$ for some $r \in R$. Since $I = \operatorname{ann}(M)$, P must contain I; since P is prime and $x^2 \in P$, we conclude that $P \supseteq (x)$. On the other hand, (x) is a maximal ideal, so $P = (x)$. Thus $\operatorname{Ass}(M) \subseteq \{(x)\}$. Moreover, by an argument similar to the one we used in Example 6.19, we can show that $(x) = \operatorname{ann}(x+I)$. Therefore, $\operatorname{Ass}(M) = \{(x)\}$, and (x) is the unique associated prime of (x^2). However, (x^2) is not a prime ideal.

In what follows, we will prove some results about associated primes of graded modules over graded rings, and we will need the following lemma:

Lemma 6.23. *If R is a $\mathbb{Z}$-graded ring, then any ideal I 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 do this by induction on the number of nonzero homogeneous components of a plus the number of nonzero homogeneous components of b. This is not interesting if $a = 0$ or $b = 0$, so the base case is when this is two. In that case, both a and b are homogeneous, so the hypothesis already gives us this case. For the induction step, 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 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 $b \in I$. $\square$

Let's recall the definition of zerodivisors on M.

Definition 6.24. Let M be an R-module. An element $r \in R$ is a **zerodivisor** on M if $rm = 0$ for some nonzero $m \in M$. We denote the set of zerodivisors of M by $\mathcal{Z}(M)$.

Lemma 6.25. *If R is noetherian, and M is an arbitrary R-module, then for any nonzero $m \in M$, $\operatorname{ann}_R(m)$ is contained in an associated prime of M. If R and M are graded and m is a homogeneous element, then $\operatorname{ann}_R(m)$ is contained in a homogeneous prime.*

Proof. The set of ideals $S := \{\operatorname{ann}_R(m) \mid m \in M, m \neq 0\}$ 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 $I = \operatorname{ann}(m)$ be any maximal element, and let $rs \in I$, $s \notin I$. We always have $\operatorname{ann}(sm) \supseteq \operatorname{ann}(m)$, and equality holds by the maximality of $\operatorname{ann}(m)$ in S. Then $r(sm) = (rs)m = 0$, so $r \in \operatorname{ann}(sm) = \operatorname{ann}(m) = I$. We conclude that I is prime, and therefore it is an associated prime of M.

The same argument above works if we take $\{\operatorname{ann}_R(m) \mid m \in M, m \neq 0 \text{ homogeneous}\}$, using Lemma 6.23. $\square$

Theorem 6.26. *If R is noetherian, and M is an arbitrary R-module, then*

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

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

Proof. Even if R is not noetherian, $M = 0$ implies $\operatorname{Ass}(M) = \varnothing$ by definition. So we focus on the case when $M \neq 0$. If $M \neq 0$, then M contains a nonzero element m, and $\operatorname{ann}(m)$ is contained in an associated prime of M, by Lemma 6.25. In particular, $\operatorname{Ass}(M) \neq 0$. In the graded setting, Lemma 6.25 gives us a homogeneous associated prime. $\square$

Theorem 6.27. *If R is noetherian, and M is an arbitrary R-module, then*

$$\bigcup_{P \in \operatorname{Ass}(M)} P = \mathcal{Z}(M).$$

Proof. If $r \in \mathcal{Z}(M)$, then by definition we have $r \in \operatorname{ann}(m)$ for some nonzero $m \in M$. Since $\operatorname{ann}(m)$ is contained in some associated prime of M, by Lemma 6.25, then r is also contained in some associated prime of M. On the other hand, if P is an associated prime of M, then by definition all elements in P are zerodivisors on M.

For the graded case, replace the set of zerodivisors with the annihilator of all homogeneous elements. The annihilator of all homogeneous elements 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. $\square$

Lemma 6.28. *If*

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

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

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

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

Thinking of L as a submodule of M, suppose that there exists $r \notin P$ such that $rm \in L$. Then

$$s(rm) = 0 \iff (sr)m = 0 \implies sr \in P \implies s \in P.$$

So $P = \operatorname{ann}(rm)$, and thus $P \in \operatorname{Ass}(L)$.

If $rm \notin L$ for all $r \notin P$, 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 $r \in P$. Since $P = \operatorname{ann}(m) \subseteq \operatorname{ann}(n)$, we conclude that $P = \operatorname{ann}(n)$. Therefore, $P \in \operatorname{Ass}(N)$. $\square$

Note that the inclusions in Lemma 6.28 are not necessarily equalities.

Example 6.29. If M is a module with at least two associated primes, and P is an associated prime of M, then

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

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

Example 6.30. 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 6.31. *Let A and B be R-modules. Then* $\operatorname{Ass}(A \oplus B) = \operatorname{Ass}(A) \cup \operatorname{Ass}(B)$.

Proof. Apply Lemma 6.28 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

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

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

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 2.14.

Definition 6.32. 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 6.33. *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 $M_i/M_{i-1} \cong R/P_i$ for primes $P_i \in \operatorname{Spec}(R)$. This is a **prime filtration** *of M.*

If R and M are $\mathbb{Z}$-graded, there exists a prime filtration of M where the quotients $M_i/M_{i-1} \cong (R/P_i)(t_i)$ are graded modules, the P_i are homogeneous primes, and $t_i \in \mathbb{Z}$.

Proof. If $M \neq 0$, then M has at least one associated prime, by Theorem 6.27, so there is an inclusion $R/P_1 \subseteq M$. 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 $R/P_2 \cong M_2/M_1 \subseteq M/M_1$. Continuing this process, we get a strictly ascending chain of submodules of M where the successive quotients are of the form R/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 P_i is the annihilator of an element m_i of degree t_i, we have a degree-preserving map $(R/P_i)(t_i) \cong Rm_i$ sending the class of 1 to m_i. $\square$

Example 6.34. Let's build a prime filtration for the module $M = R/I$, where $I = (x^2, yz)$ and $R = \mathbb{Q}[x, y, z]$. With a little help from Macaulay2, we find that

```
i4 : associatedPrimes M

o4 = {ideal (y, x), ideal (z, x)}

o4 : List
```

So our first goal is to find $m \in M$ such that $\operatorname{ann}(m) = (x, z)$ or $\operatorname{ann}(m) = (x, y)$. Let's start from (x, z). To find such an element, we can start by searching for all the elements killed by (x, z):

```
i5 : I : ideal"x,z"
                          2
o5 = ideal (y*z, x*y, x )

o5 : Ideal of R
```

Now yz and x^2 are both 0 in M, so the submodule of M generated by xy is precisely the set of elements killed by (x, z). Is $\operatorname{ann}(R \cdot xy) = (x, z)$?

```
i6 : ann ((I + ideal(x*y))/I)

o6 = ideal (z, x)

o6 : Ideal of R
```

Yes, it is! So our prime filtration starts with

$$M_0 = 0 \subseteq M_1 = \frac{I + (xy)}{I},$$

where our computations so far show that $\operatorname{ann}(M_1) = (x, z)$. For step 2, we start from scratch, and compute the associated primes of $M/M_1 \cong R/(I + (y))$:

```
i7 : associatedPrimes (R^1/(I + ideal"xy"))

o7 = {ideal (y, x), ideal (z, x)}

o7 : List
```

Unfortunately, we will again have to find another element killed by (x, z). So we repeat the process:

```
i8 : (I + ideal"xy") : ideal"x,z"

                   2
o8 = ideal (y, x )

o8 : Ideal of R

i9 : ann((I + ideal"y")/(I + ideal"xy"))

o9 = ideal (z, x)

o9 : Ideal of R
```

So in M_1, $\operatorname{ann}(y) = (x, z)$, so we can take the submodule generated by y for our next step, so our prime filtration for now looks like

$$M_0 = 0 \underset{R/(x,z)}{\subseteq} M_1 = \frac{I + (xy)}{I} \underset{R/(x,z)}{\subseteq} M_2 = \frac{I + (y)}{I}.$$

So now we repeat the process with $M/M_2 \cong R/(I + (y))$:

```
i10 : associatedPrimes (R^1/(I + ideal"y"))

o10 = {ideal (y, x)}

o10 : List

i11 : (I + ideal"y") : ideal"x,y"

o11 = ideal (y, x)

o11 : Ideal of R

i12 : ann((I + ideal"x")/(I + ideal"y"))

o12 = ideal (y, x)

o12 : Ideal of R
```

This gives us

$$M_0 = 0 \underset{R/(x,z)}{\subseteq} M_1 = \frac{I+(xy)}{I} \underset{R/(x,z)}{\subseteq} M_2 = \frac{I+(y)}{I} \underset{R/(x,y)}{\subseteq} M_3 = \frac{I+(x,y)}{I}.$$

Next, we take $M/M_3 \cong R/(I+(x,y))$ and find that

```
i13 : associatedPrimes (R^1/(I + ideal"x,y"))

o13 = {ideal (y, x)}

o13 : List

i14 : (I + ideal"x,y") : ideal"x,y"

o14 = ideal 1

o14 : Ideal of R
```

This last computation actually says we are done: since (x,y) kills everything inside M/M_3, we can now complete our prime filtration with

$$0 \underset{R/(x,z)}{\subseteq} M_1 = \frac{I+(xy)}{I} \underset{R/(x,z)}{\subseteq} M_2 = \frac{I+(y)}{I} \underset{R/(x,y)}{\subseteq} M_3 = \frac{I+(x,y)}{I} \underset{R/(x,y)}{\subseteq} M_4 = R/I.$$

The prime ideals that appear in this filtration are (x,y) and (x,z). From the computation in the beginning, these are precisely the associated primes of M.

Corollary 6.35. *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 $M_i/M_{i-1} \cong R/P_i$, then

$$\operatorname{Ass}_R(M) \subseteq \{P_1, \ldots, P_t\}.$$

Therefore, $\operatorname{Ass}_R(M)$ is finite. Moreover, 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 6.28, $\operatorname{Ass}(M_i) \subseteq \operatorname{Ass}(M_{i-1}) \cup \operatorname{Ass}(M_i/M_{i-1}) = \operatorname{Ass}(M_{i-1}) \cup \{P_i\}$. Inductively, we have $\operatorname{Ass}(M_i) \subseteq \{P_1, \ldots, P_i\}$, and $\operatorname{Ass}_R(M) = \operatorname{Ass}_R(M_t) \subseteq \{P_1, \ldots, P_t\}$. This immediately implies that $\operatorname{Ass}(M)$ is finite. In the graded case, Theorem 6.33 gives us a filtration where all the P_i are homogeneous primes, and those include all the associated primes. $\square$

Example 6.36. Any subset $X \subseteq \operatorname{Spec}(R)$ (for any R) can be realized as $\operatorname{Ass}(M)$ for some module M: take $M = \bigoplus_{P \in X} R/P$. However, M is not finitely generated when X is infinite.

Example 6.37. 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 $m \leqslant n$. However, 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 well.

Theorem 6.38 (Associated primes localize in noetherian rings)**.** *Let R be a noetherian ring, W a multiplicative set, and M a module. Then*

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

Proof. Given $P \in \operatorname{Ass}_R(M)$ such that $P \cap W = \varnothing$, Lemma 5.14 says that $W^{-1}P$ is a prime in $W^{-1}R$. Then $W^{-1}R/W^{-1}P \cong W^{-1}(R/P) \hookrightarrow W^{-1}M$ by exactness (see Theorem 5.27), so $W^{-1}P$ is an associated prime of $W^{-1}M$.

Now suppose that $Q \in \operatorname{Spec}(W^{-1}R)$ is associated to $W^{-1}M$. By Lemma 5.14, we know this is of the form $W^{-1}P$ for some prime P in R such that $P \cap W = \varnothing$. Since R is noetherian, P is finitely generated, say $P = (f_1, \dots, f_n)$ in R, and so $Q = \left(\frac{f_1}{1}, \dots, \frac{f_n}{1}\right)$.

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

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

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

Theorem 6.39. *Let R be noetherian and M be an R-module.*

$$\operatorname{Supp}(M) \;=\; \bigcup_{P \in \operatorname{Ass}(M)} V(P).$$

Proof. Let $P \in \operatorname{Ass}_R(M)$, and fix $m \in M$ such that $P = \operatorname{ann}_R(m)$. Let $Q \in V(P)$. By Proposition 6.10, $Q \in \operatorname{Supp}(R/P)$. Since $0 \to R/P \xrightarrow{m} M$ is exact and localization is exact, by Theorem 5.27, $0 \to (R/P)_Q \to M_Q$ is also exact. Since $(R/P)_Q \neq 0$, we must also have $M_Q \neq 0$, and thus $Q \in \operatorname{Supp}(M)$. This shows $\operatorname{Supp}(M) \supseteq \bigcup_{P \in \operatorname{Ass}(M)} V(P)$.

Now let Q be a prime ideal and suppose that

$$Q \notin \bigcup_{P \in \operatorname{Ass}(M)} V(P).$$

In particular, Q does not contain any associated prime of M. Then there is no associated prime of M that does not intersect $R \setminus Q$, so by Theorem 6.38, $\operatorname{Ass}_{R_Q}(M_Q) = \varnothing$. By Theorem 6.27, $M_Q = 0$. ☐

Theorem 6.40. *Let R be noetherian and M be an R-module. 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. By Theorem 6.39,

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

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. $\square$

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 6.41. 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.

Theorem 6.42. *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

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

By the assumptions, Corollary 6.35 applies, and it guarantees that this is a finite set of primes. By prime avoidance, $I \subseteq P$ for some $P \in \operatorname{Ass}(M)$. Equivalently, $I \subseteq \operatorname{ann}_R(m)$ for some nonzero $m \in M$. $\square$

6.3 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 6.43 (Fundamental Theorem of Arithmetic)**.** *Every nonzero 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 6.44. 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 6.45. 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 P**-primary**, where P is prime, if I is primary and $\sqrt{I} = P$.

Lemma 6.46. *The radical of a primary ideal is prime.*

Proof. Suppose that Q is primary and $xy \in \sqrt{Q}$. Then $x^n y^n \in Q$ for some n. If $y \notin \sqrt{Q}$, then $y^n \notin \sqrt{Q}$. Since Q is primary, we must have $x^n \in Q$, so $x \in \sqrt{Q}$. ☐

Example 6.47.

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 is 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 $\deg(y) = \deg(z) = 1$ and $\deg(x) = 0$. 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 6.48. In $R = k[x, y, z]$, the ideal $Q = (x^2, xy)$ is not primary, even though $\sqrt{Q} = (x)$ is prime. The offending product is xy: we have $x \notin Q$ and $y \notin \sqrt{Q}$.

Remark 6.49. One thing that can be confusing about primary ideals is that the definition is not symmetric. For Q to be a primary ideal, given a product $xy \in Q$, the definition says that if $x \notin Q$, then $y \in \sqrt{Q}$, and it *also* says that if $y \notin Q$, then $x \in \sqrt{Q}$. In Example 6.48, we found that $x \notin Q$ and $y \notin \sqrt{Q}$, so Q is not primary. Notice that if we switch the roles of x and y, we *do* have $x \in \sqrt{Q}$, but that is not sufficient to make Q a primary ideal.

Theorem 6.50. *If R is noetherian, the following are equivalent:*

(1) Q is primary.

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

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

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

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

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

Proof. (1) $\iff$ (2): Saying y is a zerodivisor modulo Q if there is some $x \notin Q$ with $xy \in Q$. So the condition that every zerodivisor on R/Q must be nilpotent is equivalent to

$$\exists x \notin Q : xy \in Q \implies y^n \in Q.$$

This is exactly the condition that Q is a primary ideal.

(2) $\iff$ (3): First, note that the associated primes of R/Q are the associated primes of the ideal Q, while the minimal primes of R/Q are the minimal primes of Q. By Theorem 6.27,

$$\bigcup_{P \in \operatorname{Ass}(Q)} P = \mathcal{Z}(R/Q).$$

By Theorem 6.40, every minimal prime of Q is associated to Q, so

$$\bigcap_{P \in \operatorname{Min}(Q)} P = \bigcap_{P \in \operatorname{Ass}(Q)} P.$$

Finally, every nilpotent element is always a zerodivisor. Putting all these together, we always have the following:

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

On the one hand, (2) says that the set of zerodivisors on R/Q coincides with the elements in the nilradical of R/Q; thus (2) is the statement that we have equality throughout. So (2) holds if and only if

$$\bigcup_{P \in \operatorname{Ass}(Q)} P = \bigcap_{P \in \operatorname{Ass}(Q)} P.$$

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

(3) $\iff$ (4) is clear, given that every ideal has a minimal prime and minimal primes are always associated, so having a single associated prime means having only one minimal prime and no embedded primes.

(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): By Lemma 5.14, we have the following characterization:

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

Thus the second condition in (5) is equivalent to $QR_Q \cap R = Q$. □

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

Lemma 6.51. *Let R be a noetherian ring and I be an ideal. If $\sqrt{I} = \mathfrak{m}$ a maximal ideal, then I is a primary ideal.*

Proof. By Theorem 6.39, $\operatorname{Ass}(R/I)$ is nonempty and contained in $\operatorname{Supp}(R/I) = V(I) = \{\mathfrak{m}\}$, so $\operatorname{Ass}(R/I) = \{\mathfrak{m}\}$, and hence by Theorem 6.50 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 6.48. Moreover, even the powers of a prime ideal may fail to be primary.

Example 6.52. Fix a field k and an integer $n \geqslant 2$, and let $R = k[x,y,z]/(xy - z^n)$. Consider the prime ideal $P = (x,z)$ in R. 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 primary, even though its radical is the prime P.

The contraction of primary ideals is always primary.

Lemma 6.53. *Let $R \xrightarrow{f} S$ be a ring homomorphism. If Q is a primary ideal in S, then $Q \cap R$ is a primary ideal in R.*

Proof. If $xy \in Q \cap R$, and $x \notin Q \cap R$, then $f(x) \notin Q$, 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 6.54. *If $I_1, \ldots, I_t$ are ideals, then*

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

Proof. The canonical map $R \to R/I_1 \oplus R/I_2$ sending $r \mapsto (r+I_1, r+I_2)$ has kernel $I_1 \cap I_2$, so there is an inclusion $R/(I_1 \cap I_2) \subseteq R/I_1 \oplus R/I_2$. Hence, by Lemma 6.28 and Corollary 6.31,

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

The statement for larger t follows by an easy induction. □

Corollary 6.55. *A finite intersection of P-primary ideals is P-primary.*

Proof. Let $I_1, \dots, I_t$ be P-primary ideals. Then by Lemma 6.54,

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

On the other hand,

$$\bigcap_{j=1}^{t} I_j \subseteq I_1 \neq R \quad \text{so} \quad R/(\bigcap_{j=1}^{t} I_j) \neq 0.$$

By Theorem 6.27, $\mathrm{Ass}(I_1 \cap \cdots \cap I_t)$ is nonempty, and thus $\mathrm{Ass}(I_1 \cap \cdots \cap I_t) = \{P\}$. Then $I_1 \cap \cdots \cap I_t$ is P-primary by the characterization of primary in Theorem 6.50 (3) above. □

Definition 6.56 (Primary decomposition)**.** A **primary decomposition** of an ideal I is an expression of the form

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

with each Q_i primary. A primary decomposition is **irredundant** if

$$\sqrt{Q_i} \neq \sqrt{Q_j} \text{ for } i \neq j \qquad \text{and} \qquad Q_i \not\supseteq \bigcap_{j \neq i} Q_j \text{ for all } i.$$

Some authors use the term *minimal* instead of irredundant.

Remark 6.57. By Corollary 6.55, the intersection of P-primary ideals is P-primary. Thus we can turn any primary decomposition into an irredundant one by combining the terms with the same radical, then removing redundant terms.

Example 6.58 (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 6.52, powers of primes may fail to be primary! Moreover, an ideal might be primary but not a power of a prime.

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 any noetherian ring (which were yet called that yet at the time) by Emmy Noether in 1921 [Noe21].

Theorem 6.59 (Lasker, 1905, Noether, 1921)**.** *Every ideal in a noetherian ring 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 nonempty, 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.

We claim that every irreducible ideal is primary. If we show this, any decomposition into an intersection of irreducible ideals will be a primary decomposition. To prove the contrapositive, suppose that Q is not primary, and take $xy \in Q$ with $x \notin Q$, $y \notin \sqrt{Q}$. The ascending chain of ideals

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

stabilizes for some n, since R is noetherian. Note that this means that for any element $f \in R$, we have $y^{n+1} f \in Q \implies y^n f \in Q$. Using this, we will show that

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

proving that Q is not irreducible.

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

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

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

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

So

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

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

Primary decompositions, even irredundant ones, are not unique.

Example 6.60. 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 irredundant 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 Lemma 6.51, 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 an irredundant primary decomposition. One thing all of these have in common is the radicals of the primary components: they are always (x) and (x, y).

In the previous example, the fact that the primes that appeared as radicals of the primary components were always the same was not an accident. Indeed, there are some aspects of primary decompositions that are unique, and this is one of them.

Theorem 6.61 (First uniqueness theorem for primary decompositions)**.** *Suppose I is an ideal in a noetherian ring R. Given any irredundant primary decomposition of I, say*

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

we have

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

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

Proof. For any primary decomposition, irredundant or not, by Corollary 6.55 we have

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

We just need to show that in an irredundant decomposition as above, every $P_j := \sqrt{Q_j}$ is indeed an associated prime of I. So fix j, and let

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

Since the decomposition is irredundant, the module I_j/I is nonzero. By Theorem 6.27, I_j/I has an associated prime, say $\mathfrak{a}$. Fix $x_j \in R$ such that $\mathfrak{a}$ is the annihilator of $x_j + I$ in I_j/I for some $x_j \in I_j$. Since

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

we conclude that $Q_j \subseteq \operatorname{ann}(x_j + I) = \mathfrak{a}$. Since P_j is the unique minimal prime of Q_j and $\mathfrak{a}$ is a prime containing Q_j, we must have $P_j \subseteq \mathfrak{a}$. On the other hand, for any $r \in \mathfrak{a}$, we have $rx_j \in I \subseteq Q_j$, and since $x_j \notin Q_j$, we must have $r \in \sqrt{Q_j} = P_j$ by the definition of primary ideal. Thus $\mathfrak{a} \subseteq P_j$, so we can now conclude that $\mathfrak{a} = P_j$. This shows that P_j is an associated prime of I_j/I for all j. But this is a submodule of R/I, and thus P_j is associated to R/I.

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

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

Theorem 6.62 (Second uniqueness theorem for primary decompositions)**.** *If I is an ideal in a noetherian ring R, then the minimal components in any irredundant primary decomposition of I are unique. More precisely, if*

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

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

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

which does not depend on our choice of irredundant decomposition.

Proof. Let Q be a primary ideal, and let P be any prime. If $Q \subseteq P$, then $\sqrt{Q} \subseteq P$. Since the associated primes of an ideal localize well, by Theorem 6.38, Q_P will still have a unique associated prime. Thus, the localization Q_P is either:

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

Finite intersections commute with localization, by Lemma 5.30, so for any prime P,

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

is a primary decomposition, although not necessarily irredundant. Fix a minimal prime $P = P_i$ of I, and let $Q = Q_i$. When we localize at P, all the other components become the unit ideal, since their radicals are not contained in P, and thus $I_P = Q_P$. We can then contract to R to get $I_P \cap R = (Q_i)_{P_i} \cap R = Q_i$, since Q_i is P_i-primary and we can then apply Theorem 6.50 (6). $\square$

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

Back to noetherian rings, is relatively easy to give a primary decomposition for a radical ideal:

Example 6.63. If R is noetherian, and I is a radical ideal, then we have seen that I coincides with the intersection of its minimal primes P_i, meaning $I = P_1 \cap \cdots \cap P_t$. This is the *only* primary decomposition of a radical ideal.

For a more concrete example, take the ideal $I = (xy, xz, yz)$ in $k[x, y, z]$. This ideal is radical, so we just need to find its minimal primes. And indeed, one can check that $(xy, xz, yz) = (x, y) \cap (x, z) \cap (y, z)$. More generally, the radical monomial ideals are precisely those that are squarefree, and the primary components of a monomial ideal are also monomial.

Example 6.64. 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 6.65 (Symbolic power)**.** If P is a prime ideal in a ring R, the n**th symbolic power** of P is $P^{(n)} := P^n R_P \cap R$.

This admits equivalent characterizations.

Proposition 6.66. *Let R be noetherian, and P a prime ideal of R.*

a) $P^{(n)} = \{r \in R \mid rs \in P^n$ for some $s \notin P\}$.

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

c) $P^{(n)}$ is the P-primary component in any minimal primary decomposition of 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 Lemma 5.14.

We know that $P^{(n)}$ is P-primary from one of the characterizations of primary we gave in Theorem 6.50. Any P-primary ideal satisfies $\mathfrak{q}R_P \cap R = \mathfrak{q}$, and if $\mathfrak{q} \supseteq P^n$, then $P^{(n)} = P^n R_P \cap R \subseteq \mathfrak{q}R_P \cap R = \mathfrak{q}$. Thus, $P^{(n)}$ is the unique smallest P-primary ideal containing P^n.

The last characterization follows from the second uniqueness theorem, Theorem 6.62. ☐

In particular, note that $P^n = P^{(n)}$ if and only if P^n is primary.

Example 6.67.

a) In $R = k[x, y, z]$, the prime $P = (y, z)$ satisfies $P^{(n)} = P^n$ for all n. This follows along the same lines as Example 6.47 d.

b) In $R = k[x, y, z]/(xy - z^n)$, where $n \geqslant 2$, we have seen in Example 6.52 that the square of $P = (y, z)$ is not primary, and therefore $P^{(2)} \neq P^2$. Indeed, $xy = z^n \in P^2$, and $x \notin P$, so $y \in P^{(2)}$ but $y \notin P^2$.

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 $P = I_2(X)$ 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 $P^{(n)}$ are precisely the polynomials that vanish *to order* n on the variety corresponding to 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 $k = \mathbb{Z}$ [DSGJ20].

6.4 The Krull Intersection Theorem

Theorem 6.68 (Krull Intersection Theorem for domains)**.** *If R is a domain or a local ring, then*

$$\bigcap_{n \geqslant 1} I^n = 0.$$

for any proper ideal I in R.

Chapter 7

Dimension theory: a global perspective

7.1 Dimension and height

We will now spend a while discussing the notion of dimension of a ring and dimension of a variety. To motivate the definition, let's first think in terms of varieties.

We take our inspiration from the fundamental setting of dimension theory: vector spaces. The notion of basis doesn't make sense for varieties (What does it mean to span? Where is zero?), but one relevant thing we do have for both vector spaces and for varieties is subobjects.

One way to characterize the dimension of a vector space V is the the largest number d such that there is a proper chain of subspaces

$$\{0\} = V_0 \subsetneq V_1 \subsetneq V_2 \subsetneq \cdots \subsetneq V_d = V.$$

We can try something similar for varieties, but for a reducible variety, this is not a very good notion. For example, for a union of m points, we can cook up a chain of m proper subvarieties by adding one more point each time, but a point should be zero-dimensional by any reasonable measure. So, if we want this approach to work, we should stick to chains of irreducible subvarieties.

Definition 7.1. The **dimension** of an affine variety X is defined as

$$\sup\{d \mid \exists \text{ a strictly decreasing chain of irreducible subvarieties of } X\colon X_d \supsetneq X_{d-1} \supsetneq \cdots \supsetneq X_0\}.$$

Over an algebraically closed field k, this information of chains of subvarieties can be translated into information about primes in the coordinate ring: a strictly increasing chain of irreducible subvarieties

$$X_d \supsetneq X_{d-1} \supsetneq \cdots \supsetneq X_0$$

corresponds to strictly increasing chain of prime ideals

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_d$$

in the coordinate ring $k[X]$.

Definition 7.2. The **Krull dimension** of a ring R is

$$\dim(R) := \sup\{d \mid \exists \text{ a strictly increasing chain of prime ideals } P_0 \subsetneq \cdots \subsetneq P_d\}.$$

We often call it simply the dimension of R. A strict chain of primes

$$P_0 \subsetneq \cdots \subsetneq P_d$$

has **length** d. Such a chain is **saturated** if for each i there is no prime Q with $P_i \subsetneq Q \subsetneq P_{i+1}$. So $\dim(R)$ is the supremum of the lengths of saturated chains of primes of R.

The **height** of a prime ideal P in a ring R is the supremum of the lengths of (saturated) chains of primes in R that end in P:

$$\text{height}(P) := \sup\{h \mid \exists \text{ a strictly increasing chain of prime ideals } Q_0 \subsetneq \cdots \subsetneq Q_h = P\}.$$

The **height** of an ideal I is the infimum of the heights of the primes containing I:

$$\text{height}(I) := \inf\{\text{height}(P) \mid P \in V(I)\} = \inf\{\text{height}(P) \mid P \in \text{Min}(I)\}.$$

Definition 7.3. 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 $\text{Supp}_R(M)$.

Example 7.4. a) The dimension of any field is zero.

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

c) The ring of integers $\mathbb{Z}$ has dimension 1, since there is one minimal prime (0) and every other prime is maximal. Likewise, any PID that is not a field has dimension one.

d) It follows from the definition that if k is a field, then

$$\dim(k[x_1, \ldots, x_d]) \geqslant d,$$

since there is a saturated chain of primes

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

When $d = 1$, the ring $k[x]$ is a PID, and thus it has dimension 1.

We will later show that $\dim(k[x_1, \ldots, x_d]) = d$, which should match our expectation that $\mathbb{A}^d$ has dimension d. However, we are not yet ready to prove this.

Lemma 7.5. *Let R be a ring and I be an ideal in R. If R is a UFD, I is a prime of height one if and only if $I = (f)$ for a prime element f.*

Proof. If $I = (f)$ with f irreducible, and $0 \subsetneq P \subseteq I$, then P contains some nonzero multiple of f, say af^n with a and f coprime. Since $a \notin I$, $a \notin P$, so we must have $f \in P$, so $P = (f)$. 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 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. □

Be warned that there are rings that are not noetherian but have finite Krull dimension, and infinite-dimensional noetherian rings.

Example 7.6. For a field k, the ring $R = k[x_1, x_2, \dots]/(x_1^2, x_2^2, \dots)$ is not noetherian, as

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

is an infinite ascending chain, so R is not noetherian. However, $\sqrt{(0)} = (x_1, x_2, \dots)$ is a maximal ideal, and hence $(x_1, x_2, \dots)$ is the unique minimal prime of R, which is also maximal. Therefore, $\dim(R) = 0$.

It is a lot harder to give examples of noetherian rings of infinite dimension, but they do exist. The famous example below is due to Nagata.

Example 7.7 (Nagata)**.** Let $R = k[x_{11}, x_{21}, x_{22}, x_{31}, x_{32}, x_{33}, \ldots]$ be a polynomial ring in infinitely many variables, which we are thinking of as arranged in an infinite triangle. R is clearly infinite-dimensional and not noetherian. Let

$$W = R \setminus \big((x_{11}) \cup (x_{21}, x_{22}) \cup (x_{31}, x_{32}, x_{33}) \cup \cdots \big) = \bigcap_{n \geqslant 1} \big(R \setminus (x_{n1}, \dots, x_{nn}) \big)$$

and $S = W^{-1}R$. Note that W is an intersection of multiplicatively closed subsets, so this is a valid localization of R. For any n, we have a chain of primes

$$(x_{n1}) \subsetneq (x_{n1}, x_{n2}) \subsetneq \cdots \subsetneq (x_{n1}, \dots, x_{nn})$$

in R. As these primes are all contained in $(x_{n1}, \dots, x_{nn})$, none of these intersects W, so the expansion to S of the chain above yields a proper chain of primes in S. It follows that $\dim(S) \geqslant n$ for all $n \geqslant 1$, so S is infinite-dimensional.

It turns out that S is noetherian, which is not at all obvious and a bit technical, so we will not prove it.

Lemma 7.8 (Properties of dimension and height)**.** *Let R be a ring.*

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

(2) An ideal has height zero if and only if it is contained in a minimal prime of R. In particular, in a domain, every nonzero ideal has positive height.

(3) $\dim(R) = \sup\{\dim(R/P) \mid P \in \operatorname{Spec}(R)\} = \sup\{\dim(R/P) \mid P \in \operatorname{Min}(R)\}$.

(4) $\dim(R) = \sup\{\operatorname{height}(P) \mid P \in \operatorname{Spec}(R)\} = \sup\{\operatorname{height}(Q) \mid Q \in \operatorname{mSpec}(R)\}$.

(5) If I is an ideal, then $\dim(R/I) = \sup\{n \mid \exists P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n, P_i \in V(I)\}$.

(6) If P is prime,

$$\dim(R/P) + \operatorname{height}(P) \leqslant \dim(R).$$

(7) If I is an ideal,

$$\dim(R/I) + \operatorname{height}(I) \leqslant \dim(R).$$

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

(9) If P is prime, then $\operatorname{height}(P) = \dim(R_P)$.

(10) If $P \subseteq Q$ are primes, then $\dim(R_Q/PR_Q)$ *is the supremum of the lengths of (saturated) chains of primes in R of the form $P = P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n = Q$.*

Proof. We will prove some of these and leave the rest as an exercise.

(1) A prime has height 0 if and only if it contains no other prime, which is equivalent being a minimal prime of R.

(2) If I is contained in a minimal prime Q of R, then $\operatorname{height}(Q) = 0$ by (1), so $\operatorname{height}(I) = 0$ by definition. Conversely, if $\operatorname{height}(I) = 0$, by definition, there is a minimal prime of I of height 0, so some minimal prime of I is a minimal prime of R, so I is contained in a minimal prime of R.

(6) It suffices to show that if $\dim(R/P) \geqslant a$ and $\operatorname{height}(P) \geqslant b$ then $\dim(R) \geqslant a + b$. By definition, $\operatorname{height}(P) \geqslant b$ means that there is a chain of primes

$$Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_b = P.$$

By (5), $\dim(R/P) \geqslant a$ means that there is a chain of primes

$$\mathfrak{a}_0 \subsetneq \mathfrak{a}_1 \subsetneq \cdots \subsetneq \mathfrak{a}_a$$

with $\mathfrak{a}_0 \supseteq P$. We can assume without loss of generality that $\mathfrak{a}_0 = P$, since if not, we can add it to the bottom of the chain. Putting these chains together, we get a chain of length $a + b$ in $\operatorname{Spec}(R)$, so $\dim(R) \geqslant a + b$.

(7) Let $\dim(R/I) \geqslant a$ and $\operatorname{height}(I) \geqslant b$. The inequality $\operatorname{height}(I) \geqslant b$ means that for every minimal prime P of I, $\operatorname{height}(P) \geqslant b$. The inequality $\dim(R/I) \geqslant a$ implies that there exists a minimal prime of P of I such that $\dim(R/P) \geqslant a$. For such a minimal prime as in the latter statement, using (5), we get the desired conclusion. □

Exercise 17. Prove (3)–(5) and (8)–(10) in Lemma 7.8.

Remark 7.9. We know that in noetherian rings, there can be arbitrarily long chains of primes, since the dimension can be infinite as in Nagata's Example 7.7. On the other hand, any ascending proper chain of primes is finite, as a consequence of the definition. Does this imply that every prime has finite height? This does not prevent that possibility that there could be an infinite descending chain of primes, which would then give any of the primes in the chain infinite height. (This seems strange in conjunction with the fact that in any ring, any prime contains a minimal prime, but it does not contradict this.) Another possible problem is there being two primes $P \subseteq Q$ such that for all $n \geqslant 1$ there exists a chain of primes of length n from P to Q.

However, we will later show that the height of any ideal in a noetherian ring is finite.

Exercise 18. Let $R \subseteq S$ be an integral extension of domains. Show that every nonzero $s \in S$ has a nonzero multiple in R, meaning that there exists $t \in S$ such that $ts \neq 0$ and $ts \in R$.

Example 7.10. Let k be an infinite field and $R = k[t^3, t^4, t^5]$. We have shown that

$$R \cong \frac{k[x, y, z]}{(x^3 - yz, y^2 - xz, z^2 - x^2 y)},$$

and that R is the coordinate ring of the curve

$$X = \{(t^3, t^4, t^5) \mid t \in k\}.$$

As X is a curve (meaning it is parameterized by a single parameter), we should expect the dimension of the variety X, and equivalently of the ring R, to be 1. Let's prove this.

On the one hand, R is a domain, so (0) is the unique minimal prime. To show that $\dim(R) = 1$, we need to show that any nonzero prime ideal is maximal.

Set $S = k[t^3] \subseteq R$. We note that t^3 does not satisfy any algebraic relation over k, so S is isomorphic to a polynomial ring in one variable, where that one variable corresponds to t^3. Moreover, note that the inclusion $S \subseteq R$ is integral, since t^4 satisfies the monic polynomial $(T^4)^3 - (t^3)^4 = 0$ and t^5 satisfies the monic polynomial $(T^5)^3 - (t^3)^5 = 0$. Polynomial rings in one variable have dimension 1, so $\dim(S) = 1$.

Let $P \in \operatorname{Spec}(R)$ be nonzero. Note first that $P \cap S \neq 0$, since if $f \in P$, then there is some nonzero multiple of f in S by Exercise 18. Since $\dim(S) = 1$, $P \cap S$ is maximal. The inclusion

$$\frac{S}{P \cap S} \hookrightarrow \frac{R}{P}$$

is integral: a dependence relation for any representative yields a dependence relation. Since $\frac{S}{P \cap S}$ is a field, $\frac{R}{P}$ is a domain, and the inclusion is integral, by Theorem 1.41 we can conclude that R/P is a field, so P is a maximal ideal. This shows that every nonzero prime in R is maximal, and thus $\dim(R) = 1$.

Definition 7.11. A ring is **catenary** if for every pair of primes $Q \supseteq P$, every saturated chain of primes has the same length. A ring is **equidimensional** if every maximal ideal has the same finite height, and every minimal prime has the same dimension.

It is difficult to come up with examples of rings that are not catenary, but they do exist. Nagata gave the first example of a noetherian noncatenary ring. Here are some examples of what can go wrong.

Example 7.12. 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 $k[x, y, z]$. The prime ideals (x) and (y, z) are incomparable, and $(x) \cap (y, z) = (xy, xz)$, so $\operatorname{Min}(R) = \{(x), (y, z)\}$. We claim that 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.

Here is an example which shows that the inequality $\dim(R/I) + \operatorname{height}(I) \leqslant \dim(R)$ can fail to be an equality, and that domains may fail to be equidimensional.

Example 7.13. The ring $\mathbb{Z}_{(2)}[x]$ is a domain that is not equidimensional. On the one hand, the maximal ideal $(2, x)$ has height at least two, which we see from the chain

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

Thus $\dim(R) \geqslant 2$. On the other hand, we will show later that the prime ideal $P = (2x - 1)$ has height 1, and it is maximal since $R/P \cong \mathbb{Q}$. Therefore, $\dim(R/P) = 0$, and thus

$$\dim(R/P) + \operatorname{height}(P) = 1$$

whereas $\dim R \geqslant 2$.

The ring R in this example is in fact a catenary domain, which we will not justify. Notice that there are maximal ideals of distinct heights in this ring, for example the ideal P given above is a prime of height 1 whereas and the maximal ideal $\mathfrak{m} = (2, x)$ has height 2. Thus this ring is not equidimensional.

7.2 Over, up, and down

In this section, we will collect theorems about the spectrum of a ring: theorems that assert that the map on Spec is surjective, and theorems about lifting chains of primes. Given a ring homomorphism $R \to S$, we want to study the behavior of chains of primes: how chains in R behave under expansion to S and how chains in S behave under contraction to R.

It will be convenient to think in terms of fibers.

Definition 7.14. For a map of topological spaces $f : X \to Y$ and $y \in Y$, the **fiber** over y is the subspace

$$f^{-1}(y) = \{x \in X \mid f(x) = y\} \subseteq X.$$

Note that if f is continuous and $y \in Y$ is a closed point, then $f^{-1}(y) \subseteq X$ is closed.

Definition 7.15. Let $\psi : R \to S$ be a ring homomorphism and $P \in \operatorname{Spec}(R)$. The **fiber ring** of ψ over P is

$$\kappa_\psi(P) := (R \setminus P)^{-1}(S/PS),$$

where by abuse of notation we write $R \setminus P$ for the image of $R \setminus P$ in S, and PS for $\psi(P)S$.

In the special case when $\mathfrak{m}$ is a maximal ideal in R, $S/\mathfrak{m}S$ is an $R/\mathfrak{m}$-module, meaning a vector space over the field $R/\mathfrak{m}$, so every element of $R \setminus \mathfrak{m}$ acts as a unit on $S/\mathfrak{m}S$. Thus the localization is redundant, and

$$\kappa_\psi(\mathfrak{m}) = S/\mathfrak{m}S.$$

For the identity map, we simply write

$$\kappa(P) := R_P/PR_P.$$

The point of this definition is the following.

Lemma 7.16. *Let $\psi : R \to S$ be a ring homomorphism and $P \in \operatorname{Spec}(R)$ be a prime ideal. The natural map $S \to \kappa_\psi(P)$ induces a homeomorphism (in particular, an order-preserving bijection)*

$$\operatorname{Spec}(\kappa_\psi(P)) \cong \{Q \in \operatorname{Spec}(S) \mid \psi^*(Q) = P\},$$

where the right-hand side has the subspace topology induced by the Zariski topology on $\operatorname{Spec}(S)$.

Proof. Consider the maps $S \xrightarrow{\pi} S/PS \xrightarrow{g} (R \setminus P)^{-1}(S/PS)$. For any localization map or any quotient map, the induced map on Spec is a homeomorphism onto its image. The map on spectra induced by π can be identified with the inclusion of $V(PS)$ into $\operatorname{Spec}(S)$. For the second map, g, we saw in Lemma 5.14 that the map on spectra can be identified with the inclusion of the set of primes that do not intersect $R \setminus P$, i.e., those whose contraction is contained in P. Therefore, $(g \circ \pi)^*$ is injective, since it is the composition of two injective maps.

On the one hand, if a prime Q contains PS, then $Q \cap R \supseteq PS \cap R \supseteq P$. If moreover $Q \cap R \subseteq P$, we must have $Q \cap R = P$. We have thus shown that the image of $(g \circ \pi)^*$ is the set of primes in S that contract to P. $\square$

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 7.17 (Image criterion)**.** *Let $R \xrightarrow{\varphi} S$ be a ring homomorphism. For any $P \in \operatorname{Spec}(R)$, $P \in \operatorname{im}(\varphi^*)$ if and only if*

$$PS \cap R = P.$$

Proof. If $PS \cap R = P$, then

$$\frac{R}{P} = \frac{R}{PS \cap R} \hookrightarrow \frac{S}{PS},$$

so localizing at $(R \setminus P)$, we get an inclusion $\kappa(P) \subseteq \kappa_\varphi(P)$. Since $\kappa(P)$ is nonzero, so is $\kappa_\varphi(P)$, and thus its spectrum is nonempty. By Lemma 7.16, there is a prime mapping to P.

If $PS \cap R \neq P$, then $PS \cap R \supsetneq P$. If $Q \cap R = P$, then $Q \supseteq PS$, so $Q \cap R \supsetneq P$. So no prime contracts to P. $\square$

Note that PS may not be prime, in general.

Example 7.18. Let $R = \mathbb{C}[x^n] \subseteq S = \mathbb{C}[x]$. The ideal $x^n R$ is prime, while $x^n S$ is not even radical. Nevertheless, $x^n S \cap R = (x) \cap R = x^n R$.

Example 7.19. Consider the inclusion $R := k[xy, xz, yz] \xhookrightarrow{\varphi} S := k[x, y, z]$ and the prime $P = (xy)$ in R. Notice that $(xz)(yz) \in PS \cap R$, but *not* in P, so $PS \cap R \supsetneq P$, and thus $P \notin \operatorname{im}(\varphi^*)$. We can check this more directly, by noting that any prime Q in S contracting to P would contain $PS = (x) \cap (y)$, so $Q \supseteq (x)$ or $Q \supseteq (y)$. But $(x) \cap R = (xy, xz) \supsetneq P$ and $(y) \cap R = (xy, yz) \supsetneq P$, so no prime in S contracts to P.

Corollary 7.20. *If $R \subseteq S$ is a direct summand, the map* $\operatorname{Spec}(S) \to \operatorname{Spec}(R)$ *is surjective.*

Proof. By Lemma 2.20, we know $IS \cap R = I$ for all ideals in this case, so Lemma 7.17 says the map on Spec is surjective. $\square$

We want to extend the idea of the last corollary to work for all integral extensions.

Definition 7.21. 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 7.22. Notice that $\overline{I}^S \cap R = \overline{I}$ is immediate from the definition.

Exercise 19. 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 7.23 (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 1.36, 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 $v = (b_1, \dots, b_u)$, and $A = [a_{ij}]$. By the determinantal trick, Lemma 1.34, 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 7.22. □

Theorem 7.24 (Lying over). *If $R \subseteq S$ is an integral extension, then $PS \cap R = P$ for every $P \in \operatorname{Spec}(R)$, and the induced map $\operatorname{Spec}(S) \longrightarrow \operatorname{Spec}(R)$ is surjective.*

Proof. Let I be any ideal in R. Given any $r \in \overline{I}$, we have

$$r^n + a_1 r^{n-1} + \cdots + a_{n-1} r + a_n = 0$$

for some n and some $a_i \in I^i$ for all i, so

$$r^n = -a_1 r^{n-1} - \cdots - a_{n-1} r - a_n \in I.$$

Thus $\overline{I} \subseteq \sqrt{I}$. Therefore, if P is a prime in R, by Lemma 7.23 we have $PS \cap R \subseteq \overline{P}$, and

$$PS \cap R \subseteq \overline{P} \subseteq \sqrt{P} = P.$$

Then $PS \cap R = P$, and by Lemma 7.17 we conclude that P is in the image of the map on Spec. □

Both assumptions that the extension is integral and that it is an inclusion are needed in Theorem 7.24; we cannot reduce to the case of an integral inclusion. The point is that $R \to S$ being an inclusion does not translate into a property of the induced map on Spec.

Example 7.25. We saw in Example 7.19 that the map induced on Spec by the inclusion $k[xy, xz, yz] \subseteq k[x, y, z]$ is not surjective. So Theorem 7.24 does not apply — indeed, this inclusion is not module-finite, and thus by Theorem 1.35 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 $k[xy, xz, yz]$.

Example 7.26. 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 $\frac{1}{f}$ is 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 whenever f is a regular element but not a unit, $R \longrightarrow R_f$ 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.

In contrast, the map $R \longrightarrow R/(f)$ is integral, since it is module-finite, but it is not an inclusion. The map on Spec is again not surjective: its image is $V(f)$.

Remark 7.27. Let I be an ideal in S. Suppose $R \to S$ is an integral extension. There is an induced map $R/(I \cap R) \to S/I$, and that map is integral: an equation of integral dependence for $s \in S$ over R gives an equation for integral dependence of its class in S/I over $R/(I \cap R)$.

Recall that we showed in Theorem 1.41 that if $R \subseteq S$ is an integral extension of domains, R is a field if and only S is a field.

Lemma 7.28. *If* $R \xrightarrow{\varphi} S$ *is integral,* $Q \cap R$ *is maximal if and only if* Q *is maximal in* S*.*

Proof. By Remark 7.27, 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 this follows by Theorem 1.41. □

Lemma 7.29. *Let* $R \to S$ *be integral, and let* W *be a multiplicatively closed subset of* R*. Then* $W^{-1}R \to W^{-1}S$ *is integral.*

Proof. Since W is a multiplicatively closed subset of R, its image in S is also multiplicatively closed. Given $x \in S$ and $w \in W$, then we have equations of the form

$$x^n + r_1 x^{n-1} + \cdots + r_n = 0 \implies \left(\frac{x}{w}\right)^n + \frac{r_1}{w}\left(\frac{x}{w}\right)^{n-1} + \cdots + \frac{r_n}{w^n} = 0.$$

Thus $\frac{x}{w}$ is integral over $W^{-1}S$, and S is integral over R. □

The Incomparability Theorem says if S is integral over R, then any two primes in S contracting to the same prime in R must be incomparable.

Theorem 7.30 (Incomparability)**.** *If* $R \longrightarrow S$ *is integral and* $P \subseteq Q$ *are primes in* S *that satisfy* $P \cap R = Q \cap R$*, then* $P = Q$*.*

Proof. In this case we can reduce to the case of an inclusion: $f : R \to S$ factors through $R/\ker f$, and the map induced on Spec factors as

$$\operatorname{Spec}(S) \longrightarrow \operatorname{Spec}(R) = \operatorname{Spec}(S) \longrightarrow \operatorname{Spec}(R/\ker f) \longrightarrow \operatorname{Spec}(R).$$

Since the map on spectra induced by $R \longrightarrow R/\ker(f)$ 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 $\mathfrak{a} = P \cap R = Q \cap R$. By Lemma 7.29, localizing at $(R \setminus \mathfrak{a})$ preserves integrality. By localizing R at $(R \setminus \mathfrak{a})$, the image of $\mathfrak{a}$ is a maximal ideal. So we can reduce to the situation where $P \cap R = Q \cap R$ is a maximal ideal. By Lemma 7.28, $P \subseteq Q$ are both maximal ideals. Therefore, $P = Q$. □

Corollary 7.31. *Let* S *be an integral* R*-algebra. If* S *is noetherian, then only finitely many primes contract to each* $P \in \operatorname{Spec}(R)$*.*

Proof. If $Q' \in \operatorname{Spec}(S)$ contracts to P, then $Q' \supseteq PS$, so in particular Q' contains some prime Q minimal over PS. Then

$$PS \subseteq Q \subseteq Q' \implies P \subseteq Q \cap R \subseteq Q' \cap R = P,$$

so $Q' \cap R = Q \cap R$. By Incomparability, $Q = Q'$. So all the primes contracting to P are in $\operatorname{Min}(PS)$, which is a finite set since R is noetherian, by Theorem 6.5. □

Corollary 7.32. *If $R \longrightarrow S$ is integral, then for any $Q \in \operatorname{Spec}(S)$ we have*

$$\operatorname{height}(Q) \leqslant \operatorname{height}(Q \cap R)$$

In particular, $\dim(S) \leqslant \dim(R)$.

Proof. Given a chain of primes $P_0 \subsetneq \cdots \subsetneq P_n = Q$ in $\operatorname{Spec}(S)$, we can contract to R, and by Incomparability we get a chain of distinct primes in $\operatorname{Spec}(R)$. $\square$

We will now prove two important theorems known as Going up and Going down, which in pictures say the following:

$$\text{Going up:} \qquad \begin{array}{ll} Q & \\ \rotatebox[origin=c]{90}{$\subseteq$} & \\ P \subseteq & P' \end{array} \quad \overset{\exists Q'}{\rightsquigarrow} \quad \begin{array}{ccc} Q & \subseteq & Q' \\ \rotatebox[origin=c]{90}{$\subseteq$} & & \rotatebox[origin=c]{90}{$\subseteq$} \\ P & \subseteq & P' \end{array}$$

$$\text{Going down:} \qquad \begin{array}{rr} & Q' \\ & \rotatebox[origin=c]{90}{$\subseteq$} \\ P \subseteq & P' \end{array} \quad \overset{\exists P}{\rightsquigarrow} \quad \begin{array}{ccc} Q & \subseteq & Q' \\ \rotatebox[origin=c]{90}{$\subseteq$} & & \rotatebox[origin=c]{90}{$\subseteq$} \\ P & \subseteq & P' \end{array}$$

Theorem 7.33 (Going up). *If $R \longrightarrow S$ is integral, then for every $P \subsetneq P'$ in $\operatorname{Spec}(R)$ and $Q \in \operatorname{Spec}(S)$ with $Q \cap R = P$, there is some $Q' \in \operatorname{Spec}(S)$ with $Q \subsetneq Q'$ and $Q' \cap R = P'$.*

Proof. Consider the map $R/P \to S/Q$. This is integral, as we observed in Remark 7.27. It is also injective, so Lying Over applies. Thus, there is a prime $\mathfrak{a}$ of S/Q that contracts to the prime P'/P in $\operatorname{Spec}(R/P)$. We can write $\mathfrak{a} = Q'/Q$ for some $Q' \in \operatorname{Spec}(S)$, and we must have that Q' contracts to P'. $\square$

Corollary 7.34. *If $R \subseteq S$ is integral, then $\dim(R) = \dim(S)$.*

Proof. We have already shown that $\dim(S) \leqslant \dim(R)$ in Corollary 7.32, so we just need to show that $\dim(R) \leqslant \dim(S)$. Fix a chain of primes $P_0 \subsetneq \cdots \subsetneq P_n$ in $\operatorname{Spec}(R)$. By Lying Over, Theorem 7.24, there is a prime $Q_0 \in \operatorname{Spec}(S)$ contracting to P_0. Then by Going up, Theorem 7.33, we have $Q_0 \subsetneq Q_1$ with $Q_1 \cap R = P_1$. Continuing, we can build a chain of distinct primes in S of length n. So $\dim(R) \leqslant \dim(S)$, and equality follows. $\square$

Lemma 7.35. *Let R be a normal domain and let x be an element in some larger domain that is integral over R. 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 P, then $f(t)$ has all of its nonleading coefficients in 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 dependence 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 P. By the same argument as above, all of the x_i are integral over P. Since each $x_i \in \overline{P}^S$, any polynomial in the x_i lies in $\overline{P}^S$. So the nonleading coefficients of f lie in $\overline{P}^S \cap R = P$, by Theorem 7.24. $\square$

Theorem 7.36 (Going down)**.** *Suppose that R is a normal domain, S is a domain, and $R \subseteq S$ is integral. Then, for every $P \subsetneq P'$ in* $\operatorname{Spec}(R)$ *and Q' in* $\operatorname{Spec}(S)$ *with $Q' \cap R = P'$, there is some $Q \in \operatorname{Spec}(S)$ with $Q \subsetneq Q'$ and $Q \cap R = P$.*

Proof. Let $W = (S \setminus Q')(R \setminus P)$ be the multiplicative set in S consisting of products of elements in $S \setminus Q'$ and $R \setminus P$. Note that each of the sets $S \setminus Q'$ and $R \setminus P$ contains 1, so $S \setminus Q'$ and $R \setminus P$ are both contained in W. We will show that $W \cap PS$ is empty. Once we do that, it will follow from Lemma 3.25 that there is a prime ideal Q in S containing PS such that $W \cap Q$ is empty. Since $S \setminus Q' \subseteq W$, our new prime Q must necessarily be contained in Q'. Moreover, $R \setminus P \subseteq W$, so $(Q \cap R) \cap (R \setminus P)$ is empty, or equivalently, $Q \cap R \subseteq P$. Since $Q \cap R \subseteq P$ and $Q \cap R \supseteq P$, we conclude that $Q \cap R = P$.

So our goal is to show that $W \cap PS$ is empty. We proceed by contradiction, and assume there is some $x \in PS \cap W$. We can write $x = rs$ for some $r \in R \setminus P$ and $s \in S \setminus Q'$. Moreover, since $x \in PS$, x is integral over P, by Lemma 7.23.

Consider the minimal polynomial of x over $\operatorname{frac}(R)$, say

$$h(x) = x^n + a_1 x^{n-1} + \cdots + a_n = 0.$$

By Lemma 7.35, each $a_i \in P' \subseteq R$. 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 7.35 says that each $\frac{a_i}{r^i} =: v_i \in R$. Since $r \notin P$ and $r^i v_i = a_i \in P$, we must have $v_i \in P$. The equation $g(s) = 0$ then shows that $s \in \sqrt{PS}$. Since $Q' \in \operatorname{Spec}(S)$ contains $P'S$ and hence PS, we have $s \in \sqrt{PS} \subseteq Q'$. This is the desired contradiction, since $s \notin Q'$ by construction. $\square$

Corollary 7.37. *If R is a normal domain, S is a domain, and $R \subseteq S$ is integral, then* $\operatorname{height}(Q) = \operatorname{height}(Q \cap R)$ *for any $Q \in$* $\operatorname{Spec}(S)$*.*

Proof. We already know from Corollary 7.32 that $\operatorname{height}(Q) \leqslant \operatorname{height}(Q \cap R)$. To show that $\operatorname{height}(Q) \geqslant \operatorname{height}(Q \cap R)$, given a saturated chain up to $Q \cap R$, we can apply Going Down to get a chain just as long that goes up to Q. $\square$

7.3 Noether normalizations

Lemma 7.38 (Making a pure-power leading term)**.** *Let A be a domain, $R = A[x_1, \ldots, x_n]$, and let $f \in R$ be a polynomial of degree at most N. The A-algebra automorphism of R given by*

$$\phi(x_i) = x_i + x_n^{N^{n-i}} \text{ for } i < n \qquad \text{and} \qquad \phi(x_n) = x_n$$

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 $a \in \mathbb{N}$.

Proof. 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. □

Lemma 7.39 (Making a pure-power leading term: graded version)**.** *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. Given Lemma 7.38, 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 7.40 (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 k is a field and R is a finitely generated k-algebra, then there exist $x_1, \ldots, x_t \in R$ algebraically independent over k such that $k[x_1, \ldots, x_t] \subseteq R$ is module-finite.

Proof. We proceed by induction on the number of algebra 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: R is module-finite over $R = A[r_1, \ldots, r_n]$. If not, there is some algebraic relation among the generators $r_1, \ldots, r_n$, meaning there exists $f(x_1, \ldots, x_n) \in A[x_1, \ldots, x_n]$ such that $f(r_1, \ldots, r_n) = 0$. After possibly applying Lemma 7.38 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_n is integral over $A_a[r_1, \ldots, r_{n-1}]$, and thus R_a is module-finite over $A_a[r_1, \ldots, r_{n-1}]$ by Corollary 1.36. 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 $A_{ab}[r_1, \ldots, r_{n-1}]$, then R_{ab} must also be module-finite over $A_{ab}[x_1, \ldots, x_s]$ by Remark 1.24, and we are done. □

Definition 7.41. Let R be a finitely generated algebra for some field k. Then a **Noether normalization** of R is a polynomial ring $A = k[x_1, \dots, x_t] \subseteq R$ such that $x_1, \dots, x_t$ are algebraically independent over k and R is module-finite over A.

Theorem 7.42 (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 $x_1, \dots, x_t \in R_1$ algebraically independent over k such that R is module-finite over $k[x_1, \dots, x_t]$.*

Proof. We repeat the proof of Theorem 7.40 but use Lemma 7.39 in place of Lemma 7.38. □

Remark 7.43. There also exist Noether normalizations for quotients of power series rings over fields: the key change is that after a change of coordinates, one can rewrite any nonzero power series in $k[\![x_1, \dots, x_n]\!]$ 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 $a_0, \dots, a_{d-1} \in k[\![x_1, \dots, x_{n-1}]\!]$. This is called *Weierstrass preparation*. The rest of the proof of the Noether normalization theorem proceeds in essentially the same way. Thus, given $k[\![x_1, \dots, x_n]\!]/I$, we have some module-finite inclusion of another power series ring $k[\![z_1, \dots, z_d]\!] \subseteq k[\![x_1, \dots, x_n]\!]/I$.

Theorem 7.44. *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 $k[z_1, \dots, z_d]$ 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 will 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 Theorem 1.41. Now suppose the statement holds for $d - 1$, and let R be a finitely generated domain over some field k with Noether normalization $A = k[z_1, \dots, z_d]$. Consider a maximal ideal $\mathfrak{m}$ of R and a saturated chain

$$0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_s = \mathfrak{m}.$$

By Incomparability, its contraction to $A = k[z_1, \dots, z_d]$ is a chain of s distinct primes in R:

$$0 \subsetneq P_1 := Q_1 \cap A \subsetneq \cdots \subsetneq P_s := Q_s \cap A.$$

Our assumption that the original chain is saturated implies that Q_1 has height 1. Suppose that P_1 had height 2 or more. By Going Down, we would be able to construct a chain up to Q_1 of length 2 or more, but Q_1 has height 1. Thus P_1 has height 1. Since $k[z_1, \dots, z_d]$ is a UFD, $P_1 = (f)$ for some prime element f, by Lemma 7.5. After a change of variables, as in Lemma 7.38, we can assume that f is monic in z_d with coefficients in $k[z_1, \dots, z_{d-1}]$. So $k[z_1, \dots, z_{d-1}] \subseteq A/(f) \subseteq R/Q_1$ are module-finite extensions, and the induction hypothesis applies to R/Q_1. Now

$$0 = Q_1/Q_1 \subsetneq Q_2/Q_1 \subsetneq \cdots \subsetneq Q_s/Q_1 = \mathfrak{m}/Q_1$$

is a saturated chain in the domain R/Q_1 going up to the maximal ideal $\mathfrak{m}/Q_1$. The induction hypothesis then says that this chain has length $d - 1$, so $s - 1 = d - 1$, and $s = d$. □

Corollary 7.45. *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, so Theorem 7.44 says that it must have dimension d. □

This matches our geometric intuition: $k[x_1, \ldots, x_d]$ corresponds to $\mathbb{A}_k^d$, and we are used to thinking of $\mathbb{A}_k^d$ 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 7.46. *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 7.47. *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

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

Proof.

1) Let $P \subseteq Q$ be primes in R. After quotient out by P, we can assume that R is a domain and $P = 0$. Fix a saturated chain C from Q to a maximal ideal $\mathfrak{m}$. Given two saturated chains C', C'' from 0 to Q, the concatenations $C'|C$ and $C''|C$ are saturated chains from 0 to $\mathfrak{m}$, so by Theorem 7.44 they must have the same length. It follows that C' and C'' have the same length.

2) Equidimensionality is immediate from Theorem 7.44.

3) We have
$$\operatorname{height}(I) = \min\{\operatorname{height}(P) \mid P \in \operatorname{Min}(I)\}$$
and
$$\dim(R/I) = \max\{\dim(R/P) \mid P \in \operatorname{Min}(I)\}.$$
Therefore, it suffices to show the equality for prime ideals, since if $P \in \operatorname{Min}(I)$ attains $\operatorname{height}(I)$, which is the minimal value of $\operatorname{height}(Q)$ for $Q \in \operatorname{Min}(I)$, then it also attains the maximal value of $\dim(R/Q)$ for $Q \in \operatorname{Min}(I)$. Now, take a saturated chain of primes C from 0 to P, and a saturated chain C' from P to a maximal ideal $\mathfrak{m}$. Since R is catenary, C has length $\operatorname{height}(P)$. Moreover, C' has length $\dim(R/P)$ by Theorem 7.44, and $C|C'$ has length $\dim(R)$ by Theorem 7.44. □

Definition 7.48. Let $K \subseteq L$ be an extension of fields. A **transcendence basis** for L over K is a maximal algebraically independent subset of L over K.

Lemma 7.49. *Let $\{x_1, \ldots, x_m\}$ and $\{y_1, \ldots, y_n\}$ be two transcendence bases for L over K. Then, there is some i such that $\{x_i, y_2, \ldots, y_n\}$ is a transcendence basis.*

Proof. Since L is algebraic over $K(y_1, \ldots, y_n)$, for each i there is some $p_i(t) \in K(y_1, \ldots, y_n)[t]$ such that $p_i(x_i) = 0$. We can clear denominators to assume without loss of generality that $p_i(x_i) \in K[y_1, \ldots, y_n][t]$.

We claim that there is some i such that $p_i(t) \notin K[y_2, \ldots, y_n][t]$. If not, then

$$p_i(t) \in K[y_2, \ldots, y_n][t]$$

for all i, and thus that each x_i is algebraic over $K(y_2, \ldots, y_n)$. Thus, $K(x_1, \ldots, x_m)$ is algebraic over $K(y_2, \ldots, y_n)$, and since L is algebraic over $K(x_1, \ldots, x_m)$, y_1 is algebraic over $K(y_2, \ldots, y_n)$, which contradicts that $\{y_1, \ldots, y_n\}$ is a transcendence basis. This shows the claim.

Now, we claim that for such i, $\{x_i, y_2, \ldots, y_n\}$ is a transcendence basis. Thinking of the equation $p_i(x_i) = 0$ as a polynomial expression in $K[x_i, y_2, \ldots, y_n][y_1]$, y_1 is algebraic over $K(x_i, y_2, \ldots, y_n)$, hence $K(y_1, \ldots, y_n)$ is algebraic over $K(x_i, y_2, \ldots, y_n)$, and L as well.

If $\{x_i, y_2, \ldots, y_n\}$ were algebraically dependent, then there is some polynomial equation $p(x_i, y_2, \ldots, y_n) = 0$. This equation must involve x_i, since $y_2, \ldots, y_n$ are algebraically independent. We would then have $K(x_i, y_2, \ldots, y_n)$ is algebraic over $K(y_2, \ldots, y_n)$. But since y_1 is algebraic over $K(x_i, y_2, \ldots, y_n)$, we would have that $K(y_1, \ldots, y_n)$ is algebraic over $K(y_2, \ldots, y_n)$, which would contradict that $y_1, \ldots, y_n$ is a transcendence basis. □

Lemma 7.50. *If $\{x_1, \ldots, x_m\}$ and $\{y_1, \ldots, y_n\}$ are two transcendence bases for L over K, then $m = n$.*

Proof. Say that $m \leqslant n$. If the intersection has $s < m$ elements, then without loss of generality $y_1 \notin \{x_1, \ldots, x_m\}$. Then, for some i, $\{x_i, y_2 \ldots, y_n\}$ is a transcendence basis, and $\{x_1, \ldots, x_m\} \cap \{x_i, y_2 \ldots, y_n\}$ has $s + 1$ elements. Replacing $\{y_1, \ldots, y_n\}$ with $\{x_i, y_2 \ldots, y_n\}$ and repeating this process, we obtain a transcendence basis with n elements such that $\{x_1, \ldots, x_m\} \subseteq \{y_1, \ldots, y_n\}$. But we must then have that these two transcendence bases are equal, so $m = n$. □

This shows that we have a well-defined **transcendence degree**, which we denote by $\operatorname{trdeg}_K(L)$. In particular, if $x_1, \ldots, x_d$ are indeterminates, then the transcendence degree of $K(x_1, \ldots, x_d)$ over K is d.

Corollary 7.51. *If R is a finitely generated domain over a field k, then*

$$\dim(R) = \operatorname{trdeg}_k(\operatorname{frac}(R)).$$

Proof. If $S \subseteq R$ is module-finite, then by Lemma 7.29 $\operatorname{frac}(S) \subseteq \operatorname{frac}(R)$ is integral, or equivalently algebraic. Hence $\operatorname{frac}(S)$ and $\operatorname{frac}(R)$ have the same transcendence degree over k. In particular, if $A = k[z_1, \ldots, z_d]$ is a Noether normalization for R,

$$\operatorname{trdeg}_k(\operatorname{frac}(R)) = \operatorname{trdeg}_k(\operatorname{frac}(A)) = \operatorname{trdeg}_k(k(z_1, \ldots, z_d)) = d = \dim(A) = \dim(R). \quad \square$$

Example 7.52. Let $R = k[xu, xv, yu, yv] \subseteq k[x, y, u, v]$, where k is an algebraically closed field and x, y, u, v are indeterminates. Then

$$\operatorname{frac}(R) = k(xu, xv, yu, yv) = k\left(xu, \frac{v}{u}, \frac{y}{x}, \frac{yv}{xu}\right) = k\left(xu, \frac{v}{u}, \frac{y}{x}\right),$$

and these last three are algebraically independent over k. Thus, $\dim(R) = 3$.

Example 7.53. Let us use our dimension theorems to give two different proofs that over any field k, $R = k[x, y, z]/(y^2 - xz)$ has dimension 2

First, we claim that $A = k[x, z]$ is a Noether normalization of R. First, note that x and z are algebraically independent over k. Moreover, $R = A[y]$ and y satisfies the monic polynomial $t^2 - xz \in A[t]$, so $A \subseteq R = A[y]$ is integral, and thus module-finite by Corollary 1.36. Therefore, $\dim(R) = 2$.

Alternatively, one can show 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 by Corollary 7.47 the dimension of R is

$$\dim(R) = \dim(k[x, y, z]) - \operatorname{height}((y^2 - xz)) = 3 - 1 = 2.$$

Example 7.54. Let us compute the dimension of the ring $R = k[a, b, c, d]/I$, where

$$I = (b^2 - ac, c^2 - bd, bc - ad).$$

We claim that $A = k[a, d] \subseteq R$ is a Noether normalization. The inclusion is integral, since

$$b^2 = ac \implies b^4 = a^2c^2 = a^2bd,$$

so b satisfies $t^4 - a^2dt = 0$. Similarly, one can show that c satisfies $t^4 - ad^2t$.

We also need to show that a, d are algebraically independent over k, or equivalently that the map from the polynomial ring $\psi\colon k[u, v] \to R$ with $\psi(u) = a$, $\psi(v) = d$ is injective.

Observe that the map

$$\begin{aligned} \mathcal{Z}(I) &\xrightarrow{\ \phi\ } \mathbb{A}^2 \\ (a, b, c, d) &\longmapsto (a, d) \end{aligned}$$

is surjective: given $a, d \in k$, write $a = \alpha^3, d = \delta^3$, and note that $(\alpha^3, \alpha^2\delta, \alpha\delta^2, \delta^3)$ is an element of $X = \mathcal{Z}(I)$ that maps to (a, d). Thus, the kernel of the induced map on coordinate rings $k[\mathbb{A}^2] \to k[X]$ is $\mathcal{I}(\mathbb{A}^2) = 0$; i.e, the map is injective. By the Nullstellensatz, $\mathcal{I}(\mathcal{Z}(I)) = \sqrt{I}$, and our induced map on coordinate rings is the map

$$k[u, v] \longrightarrow k[a, b, c, d]/\sqrt{I} \qquad \phi^*(u) = a,\ \phi^*(v) = d.$$

Since this map is injective, and this factors as

$$k[u, v] \xrightarrow{\ \psi\ } k[a, b, c, d]/I \twoheadrightarrow k[a, b, c, d]/\sqrt{I}$$

the first map is injective.

Chapter 8

Dimension: a local perspective

8.1 Height and number of generators

Theorem 8.1 (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.*

Proof. Suppose the theorem is false, so that there is some ring R, a prime P, and an element f such that P is minimal over (f) and $\operatorname{height}(P) > 1$. If we localize at 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 Q be a prime strictly in between (0) and $\mathfrak{m}$, and notice that we necessarily have $f \notin Q$.

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

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

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

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

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

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

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

On the other hand, $Q^{(m)} = Q^m R_Q \cap R$ for all m, and

$$\bigcap_{m\geqslant 1} Q^{(m)} R_Q \subseteq \bigcap_{m\geqslant 1} Q^m R_Q = \bigcap_{m\geqslant 1} (QR_Q)^m = 0$$

by Krull's Intersection theorem. Since R is a domain, the contraction of (0) in R_Q back in R is (0). This is the contradiction we seek. So no such 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. □

Remark 8.2. 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.

Noetherianity is necessary, as the next example shows.

Example 8.3. Let $R = k[x, xy, xy^2, \ldots] \subseteq k[x, y]$. Note that (x) is not prime: for $a > 0$, $xy^a \notin (x)$, since $y^a \notin R$, but $(xy^a)^2 = x \cdot xy^{2a} \in (x)$. Thus, $\mathfrak{m} = (x, xy, xy^2, \ldots) \subseteq \sqrt{(x)}$, and since $\mathfrak{m}$ is a maximal ideal, we have equality, so $\operatorname{Min}(x) = \{\mathfrak{m}\}$. However, the ideal $P = (xy, xy^2, xy^3, \ldots) = (y)k[x, y] \cap R$ is prime, and the chain $(0) \subsetneq P \subsetneq \mathfrak{m}$ shows that $\operatorname{height}(\mathfrak{m}) > 1$.

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 8.4. *Let R be noetherian, $P \subsetneq Q \subsetneq \mathfrak{a}$ be primes, and $f \in \mathfrak{a}$. Then there is some Q' with $P \subsetneq Q' \subsetneq \mathfrak{a}$ and $f \in Q'$.*

Proof. If $f \in P$, there is nothing to prove, since we can simply take $Q' = Q$. Suppose $f \notin P$. After we quotient out by P and localize at $\mathfrak{a}$, we may assume that $\mathfrak{a}$ is the unique maximal ideal and that our ring is a domain. Thus all we need is to find a nonzero prime Q' which is not maximal. Note that by assumption $\operatorname{height}(\mathfrak{a}) \geqslant 2$. Our assumption implies that $f \neq 0$, and then by the principal ideal theorem Krull's Principal Ideal Theorem, minimal primes of (f) have height one, hence are not maximal nor 0. We can take Q' to be one of the minimal primes of f. □

Theorem 8.5 (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 Krull's Principal Ideal Theorem.

Let $I = (f_1, \ldots, f_n)$ be an ideal, P a minimal prime of I, and $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_h = P$ be a saturated chain of length h ending at P. If $f_1 \in P_1$, then we can apply the induction hypothesis to the ring $\overline{R} = R/((f_1) + P_0)$ and the ideal $(f_2, \ldots, f_n)\overline{R}$. Then by induction hypothesis, the chain $P_1\overline{R} \subsetneq \cdots \subsetneq P_h\overline{R}$ has length at most $n - 1$, so $h - 1 \leqslant n - 1$ and P has height at most n.

If $f_1 \notin P_1$, we use the previous lemma to replace our given chain with a chain of the same length but such that $f_1 \in P_1$. To do this, note that $f_1 \in P_i$ for some i; after all, $f_1 \in I \subseteq P$. So in the given chain, suppose that $f_1 \in P_{i+1}$ but $f_1 \notin P_i$. If $i > 0$, apply the previous lemma with $\mathfrak{a} = P_{i+1}$, $Q = P_i$, and $P = P_{i-1}$ to find Q_i such that $f_1 \in Q_i$. Replace the chain with

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_{i-1} \subsetneq Q_i \subsetneq P_i \subsetneq \cdots \subsetneq P_h = P.$$

Repeat until $f_1 \in P_1$. □

The bound in Krull's height theorem is sharp.

Example 8.6. If k is a field and $R = k[x_1, \dots, x_n]$, the ideal $(x_1, x_2, \dots, x_n)$ generated by n variables has height n. There are many other ideals that attain the bound given by Krull's height theorem. 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**.

If I is generated by n elements, I may have minimal primes of height less than n.

Example 8.7. The ideal (xy, xz) in $k[x, y, z]$ has minimal primes of heights 1 and 2.

It is possible to have associated primes of height greater than the number of generators.

Example 8.8. 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). 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.

Noetherianity is necessary in Krull's height theorem.

Example 8.9. 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 $\operatorname{height}(\mathfrak{m}) > 1$.

Corollary 8.10. *If R is a noetherian ring, then any ideal has finite height. If $(R, \mathfrak{m}, k)$ is also local, then* $\dim(R) \leqslant \dim_k(\mathfrak{m}/\mathfrak{m}^2) < \infty$.

Proof. If R is noetherian, then every ideal is finitely generated, by Proposition 1.61, and thus by Krull's height theorem every ideal has finite height.

Now suppose that $(R, \mathfrak{m}, k)$ is a noetherian local ring. By NAK, $\mathfrak{m}$ is generated by $\dim_k(\mathfrak{m}/\mathfrak{m}^2)$ elements, so

$$\dim(R) = \operatorname{height}(\mathfrak{m}) \leqslant \dim_k(\mathfrak{m}/\mathfrak{m}^2). \qquad \square$$

Definition 8.11. 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 8.14 can be restated as $\dim(R) \leqslant \operatorname{embdim}(R)$. Rings whose dimension and embedding dimension agree are very nicely behaved.

Definition 8.12. A noetherian local ring $(R, \mathfrak{m})$ is **regular** if $\dim(R) = \operatorname{embdim}(R)$.

Power series rings $k[\![x_1, \dots, x_d]\!]$ 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.

8.2 Systems of parameters

Here is a sort of converse to the Krull's height theorem.

Theorem 8.13. *Let $(R, \mathfrak{m})$ be a noetherian local ring of dimension d. There there exist $x_1, \ldots, x_d \in \mathfrak{m}$ such that $\mathfrak{m} = \sqrt{(x_1, \ldots, x_d)}$.*

Proof. Let $d := \dim(R)$. If $d = 0$, then $\mathfrak{m} = \sqrt{(0)}$, so the statement holds.

In general, we will show that we can choose $x_1, \ldots, x_i \in \mathfrak{m}$ inductively such that every minimal prime of $J_i = (x_1, \ldots, x_i)$ has height i. The case $i = 0$ is clear from the comment above. Say that we have chosen the first i elements. If $i < d$, note that $\mathfrak{m}$ is not a minimal prime of J_i, as this would contradict Krull's height theorem. Note that R is noetherian and thus J_i has finitely many minimal primes, by Theorem 6.5. Thus, by Prime Avoidance, we can choose $x_{i+1} \in \mathfrak{m}$ not in any minimal prime of J_i. Then by Krull's height theorem every minimal prime of $J_{i+1} := J_i + (x_{i+1})$ has height at most $i + 1$. On the other hand, every $Q \in \operatorname{Min}(J_{i+1})$ contains some $P \in \operatorname{Min}(J_i)$, and in fact we must have $Q \supsetneq P$, since $x_{i+1} \in Q \smallsetminus P$. Since P has height i and $P \supsetneq Q$, then Q must have height at least $i + 1$. Therefore, Q must have height exactly $i + 1$, completing the induction.

Since every minimal prime of $J_d = (x_1, \ldots, x_d)$ has height d, its unique minimal prime must be $\mathfrak{m}$. It follows that $\sqrt{J_d} = \mathfrak{m}$. □

Corollary 8.14. *Let $(R, \mathfrak{m}, k)$ be a noetherian local ring. Then*

$$\dim(R) = \min\{n \mid \sqrt{(f_1, \ldots, f_n)} = \mathfrak{m} \textit{ for some } f_1, \ldots, f_n\} \leqslant \mu(\mathfrak{m}).$$

Proof. Suppose that $\sqrt{(f_1, \ldots, f_n)} = \mathfrak{m}$. Then $\mathfrak{m}$ is a minimal prime of $(f_1, \ldots, f_n)$, and thus $\mathfrak{m}$ has height at most n by Krull's height theorem. The dimension of a local ring is the height of its maximal ideal, so $\dim(R) \leqslant n$, and thus $\dim(R)$ is bounded above by the minimum in the middle. On the other hand, if $d = \dim(R)$ then by Theorem 8.13 there exist $f_1, \ldots, f_d$ such that $\mathfrak{m} = (f_1, \ldots, f_d)$, which gives the other inequality, showing

$$\dim(R) = \min\{n \mid \sqrt{(f_1, \ldots, f_n)} = \mathfrak{m} \text{ for some } f_1, \ldots, f_n\}.$$

Finally, since $\mathfrak{m}$ is generated by $\mu(\mathfrak{m})$ elements, there are in particular $\mu(\mathfrak{m})$ elements whose radical is $\mathfrak{m}$. □

Definition 8.15. A sequence of d elements $x_1, \ldots, x_d$ in a d-dimensional noetherian local ring $(R, \mathfrak{m})$ is a **system of parameters** or **SOP** if $\sqrt{(x_1, \ldots, x_d)} = \mathfrak{m}$. If k is a field, a sequence of d homogeneous elements $x_1, \ldots, x_d$ in a d-dimensional $\mathbb{N}$-graded finitely generated k-algebra R, with $R_0 = k$, is a *homogeneous system of parameters* if $\sqrt{(x_1, \ldots, x_d)} = R_+$.

We say that elements $x_1, \ldots, x_t$ are **parameters** if they are part of a system of parameters; this is a property of the set, not just the elements.

By Theorem 8.13, every local ring admits a system of parameters, and these can be useful in characterizing the dimension of a local noetherian ring, or the height of a prime in a noetherian ring. Note that there is a graded version of Theorem 8.13 as well, where we can choose a homogeneous sop.

Definition 8.16. Let R be a noetherian ring. A prime P of R is an **absolutely minimal prime of** R if $\dim(R) = \dim(R/P)$.

Absolutely minimal primes are minimal, since $\dim(R) \geqslant \dim(R/P) + \text{height}(P)$.

Theorem 8.17. *Let $(R, \mathfrak{m})$ be a noetherian local ring, and $x_1, \dots, x_t \in \mathfrak{m}$.*

1) $\dim(R/(x_1, \dots, x_t)) \geqslant \dim(R) - t$.

2) $x_1, \dots, x_t$ *are parameters if and only if* $\dim(R/(x_1, \dots, x_t)) = \dim(R) - t$.

3) $x_1, \dots, x_t$ *are parameters if and only if x_1 is not in any absolutely minimal prime of R and x_i is not contained in any absolutely minimal prime of $R/(x_1, \dots, x_{i-1})$ for each $i = 2, \dots, t$.*

Proof.

1) If $\dim(R/(x_1, \dots, x_t)) = s$, then take a system of parameters $y_1, \dots, y_s$ for $R/(x_1, \dots, x_t)$, and pull back to R to get $x_1, \dots, x_t, y_1', \dots, y_s'$ in R such that the quotient of R modulo the ideal generated by these elements has dimension zero. By Krull height, we get that $t + s \geqslant \dim(R)$.

2) Let $d = \dim(R)$. Suppose first that $\dim(R/(x_1, \dots, x_t)) = d - t$. Then, there is a SOP $y_1, \dots, y_{d-t}$ for $R/(x_1, \dots, x_t)$; lift back to R to get a sequence of d elements $x_1, \dots, x_t, y_1, \dots, y_{d-t}$ that generate an $\mathfrak{m}$-primary ideal. This is a SOP, so $x_1, \dots, x_t$ are parameters.

   On the other hand, if $x_1, \dots, x_t$, are parameters, extend to a SOP $x_1, \dots, x_d$. If I is the image of $(x_{t+1}, \dots, x_d)$ in $R' = R/(x_1, \dots, x_t)$, we have R'/I is zero-dimensional, hence has finite length, so $\text{Ass}_{R'}(R'/I) = \{\mathfrak{m}\}$, and I is $\mathfrak{m}$-primary in R'. Thus, $\dim(R')$ is equal to the height of I, which is then $\leqslant d - t$ by Krull height. That is, $\dim(R') \leqslant d - t$, and using the first statement, we have equality.

3) This follows from the previous statement and the observation that $\dim(S/(f)) < \dim(S)$ if and only if f is not in any absolutely minimal prime of S. $\square$

It is worth comparing the characterization in part three with our existence proof: we constructed a system of parameters by inductively avoiding all the minimal primes; in general a system a parameters is a sequence where we inductively avoid all of the absolutely minimal primes.

Note that the first inequality in Theorem 8.17 can fail outside of the local case.

Example 8.18. Let $R = \mathbb{Z}_{(2)}[x]$. This ring has dimension at least two, but $R/(2x - 1) \cong \mathbb{Q}$ has dimension zero.

For an example that is a finitely generated algebra over a field, consider $R = S/I$ with $S = k[x, y, z]$ and $I = (xy, xz, x^2 - x)$. This ring has dimension two: $A = k[y, z]$ is a noether normalization, as $x^2 - x = 0$ makes x integral over A, and no nonzero polynomial in y, z in $k[x, y, z]$ can belong to the ideal $(x) \supseteq (xy, xz, x^2 - x)$. However,

$$R/(x - 1) \cong \frac{k[x, y, z]}{(y, z, x - 1)} \cong k$$

has dimension zero.

Appendix A

Macaulay2

There are several computer algebra systems dedicated to algebraic geometry and commutative algebra computations, such as Singular (more popular among algebraic geometers), CoCoA (which is more popular with european commutative algebraists, having originated in Genova, Italy), and Macaulay2. There are many computations you could run on any of these systems (and others), but we will focus on Macaulay2 since it's the most popular computer algebra system among US based commutative algebraists.

Macaulay2, as the name suggests, is a successor of a previous computer algebra system named Macaulay. Macaulay was first developed in 1983 by Dave Bayer and Mike Stillman, and while some still use it today, the system has not been updated since its final release in 2000. In 1993, Daniel Grayson and Mike Stillman released the first version of Macaulay2, and the current stable version if Macaulay2 1.16.

Macaulay2, or M2 for short, is an open-source project, with many contributors writing packages that are then released with the newest Macaulay2 version. Journals like the *Journal of Software for Algebra and Geometry* publish peer-refereed short articles that describe and explain the functionality of new packages, with the package source code being peer reviewed as well.

The National Science Foundation has funded Macaulay2 since 1992. Besides funding the project through direct grants, the NSF has also funded several Macaulay2 workshops — conferences where Macaulay2 package developers gather to work on new packages, and to share updates to the Macaulay2 core code and recent packages.

A.1 Getting started

A Macaulay2 session often starts with defining some ambient ring we will be doing computations over. Common rings such as the rationals and the integers can be defined using the commands `QQ` and `ZZ`; one can easily take quotients or build polynomial rings (in finitely many variables) over these. For example,

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

o1 = R
```

```
o1 : PolynomialRing
```

and

```
i1 : k = ZZ/101;

i2 : R = k[x,y];
```

both store the ring $\mathbb{Z}/101$ as R, with the small difference that in the second example Macaulay2 has named the coefficient field k. One quirk that might make a difference later is that if we use the first option and later set k to be the field $\mathbb{Z}/101$, our ring R is *not* a polynomial ring over k. Also, in the second example we ended each line with a `;`, which tells Macaulay2 to run the command but not display the result of the computation — which is in this case was simply an assignment, so the result is not relevant.

We can now do all sorts of computations over our ring R. For example, we can define an ideal in R, as follows:

```
i3 : I = ideal(x^2,y^2,x*y)

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

o3 : Ideal of R
```

Above we have set I to be the ideal in R that is generated by x^2, y^2, xy. The notation `ideal( )` requires the usage of ˆ for powers and $*$ for products; alternatively, we can define the exact same ideal with the notation `ideal" "`, as follows:

```
i3 : I = ideal"x2,y2,xy"

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

o3 : Ideal of R
```

Now we can use this ideal I to either define a quotient ring $S = R/I$ or the R-module $M = R/I$, as follows:

```
i4 : M = R^1/I

o4 = cokernel | x2 y2 xy |
                                  1
o4 : R-module, quotient of R

i5 : S = R/I

o5 = S

o5 : QuotientRing
```

It's important to note that while R is a ring, R^1 is the R-module R — this is a very important difference for Macaulay2, since these two objects have different types. So S defined above is a ring, while M is a module. Notice that Macaulay2 stored the module M as the cokernel of the map

$$R^3 \xrightarrow{\begin{bmatrix} x^2 & y^2 & xy \end{bmatrix}} R\,.$$

When you make a new definition in Macaulay2, you might want to pay attention to what ring your new object is defined over. For example, now that we defined this ring S, Macaulay2 has automatically taken S to be our current ambient ring, and any calculation or definition we run next will be considered over S and not R. If you want to return to the original ring R, you must first run the command `use R`.

If you want to work over a finitely generated algebra over one of the basic rings you can define in Macaulay2, and your ring is not a quotient of a polynomial ring, you want to rewrite this algebra as a quotient of a polynomial ring. For example, suppose you want to work over the second Veronese in 2 variables over our field k from before, meaning the algebra $k[x^2, xy, y^2]$. We need 3 algebra generators, which we will call a, b, c, corresponding to x^2, xy, and y^2:

```
i6 : U = k[a,b,c]

o6 = U

o6 : PolynomialRing

i7 : f = map(R,U,{x^2,x*y,y^2})
                    2        2
o7 = map(R,U,{x , x*y, y })

o7 : RingMap R <--- U

i8 : J = ker f
               2
o8 = ideal(b  - a*c)

o8 : Ideal of U

i9 : T = U/J

o9 = T

o9 : QuotientRing
```

Our ring T at the end is isomorphic to the 2nd Veronese of R, which is the ring we wanted. Note the syntax order in `map`: first target, then source, then a list with the images of each algebra generator.

A.2 Asking Macaulay2 for help

As you're learning how to use Macaulay2, you will often find yourself needing some help. Luckily, Macaulay2 can help you directly! For example, suppose you know the name of a command, but do not remember the syntax to use it. You can ask `?command`, and Macaulay2 will show you the different usages of the command you want to know about.

```
i10 : ?primaryDecomposition

primaryDecomposition -- irredundant primary decomposition of an ideal

  * Usage:
        primaryDecomposition I
  * Inputs:
      * I, an ideal, in a (quotient of a) polynomial ring R
  * Optional inputs:
      * MinimalGenerators => a Boolean value, default value true, if false, the
        components will not be minimalized
      * Strategy => ..., default value null,
  * Outputs:
      * a list, containing a minimal list of primary ideals whose intersection
        is I

Ways to use primaryDecomposition :
==================================

  * "primaryDecomposition(Ideal)" -- see "primaryDecomposition" -- irredundant
    primary decomposition of an ideal
  * "primaryDecomposition(Module)" -- irredundant primary decomposition of a
    module
  * "primaryDecomposition(Ring)" -- see "primaryDecomposition(Module)" --
    irredundant primary decomposition of a module

For the programmer
==================

The object "primaryDecomposition" is a method function with options.
```

If instead you'd rather read the complete Macaulay2 documentation on the command you are interested in, you can use the `viewHelp` command, which will open an html page with the documentation you asked for. So running

```
i11 : viewHelp "primaryDecomposition"
```

will open an html page dedicate to the method `primaryDecomposition`, which includes examples and links to related methods.

A.3 Basic commands

Many Macaulay2 commands are easy to guess, and named exactly what you would expect them to be named. Often, googling "Macaulay2" followed by a few descriptive words will easily land you on the documentation for whatever you are trying to do.

Here are some basic commands you will likely use:

- `ideal`$(f_1, \ldots, f_n)$ will return the ideal generated by $f_1, \ldots, f_n$. Here products should be indicated by $*$, and powers with $\hat{}$. If you'd rather not use $\hat{}$ (this might be nice if you have lots of powers), you can write `ideal`$(f_1, \ldots, f_n)$ instead.

- `map`$(S, R, f_1, \ldots, f_n)$ gives a ring map $R \to S$ if R and S are rings, and R is a quotient of $k[x_1, \ldots, x_n]$. The resulting ring map will send $x_i \mapsto f_i$. There are many variations of `map` — for example, you can use it to define R-module homomorphisms — but you should carefully input the information in the required format. Try `viewHelp map` in Macaulay2 for more details

- `ker`(f) returns the kernel of the map f.

- `I + J` and `I*J` return the sum and product of the ideals I and J, respectively.

- `A = matrix`$\{\{a_{1,1}, \ldots, a_{1,n}\}, \ldots, \{a_{m,1}, \ldots, a_{m,n}\}\}$ returns the matrix

$$A = \begin{pmatrix} a_{1,1} & \ldots & a_{1,n} \\ & \ddots & \\ a_{m,1} & \ldots & a_{m,n} \end{pmatrix}$$

If you are familiar with any other programming language, many of the basics are still the same. For example, some of the commands we will use return lists, and we might often need to do operations on lists. As with many other programming languages, a list is indicated by { } with the elements separated by commas.

```
i6 : w = {ZZ, 3, ideal"xy3"}
                           3
o6 = {ZZ, 3, ideal(x*y )}

o6 : List
```

As in most programming languages, Macaulay2 follows the convention that the first position in a list is the 0th position.

The method `primaryDecomposition` returns a list of primary ideals whose intersection is the input ideal, and `associatedPrimes` returns the list of associated primes of the given ideal or module. Operations on lists are often intuitive. For example, let's say we want to find the primary component of an ideal with a particular radical.

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

i2 : I = ideal"x2,xy";

o2 : Ideal of R

i3 : prim = primaryDecomposition I
                              2
o3 = {ideal x, ideal (y, x )}

o3 : List

i4 : L = select(prim, Q -> radical(Q) == ideal"x,y")
                     2
o4 = {ideal (y, x )}

o4 : List
```

The method `select` returns a list of all the elements in our list with the required properties. In this case, if we actually want the primary ideal we just selected, as opposed to a list containing it, we need to extract the first component of our list L.

```
i5 : L_0
                    2
o5 = ideal (y, x )

o5 : Ideal of R
```

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.

[DSGJ20] Alessandro De Stefani, Eloísa Grifo, and Jack Jeffries. A Zariski-Nagata theorem for smooth $\mathbb{Z}$-algebras. *J. Reine Angew. Math.*, 761:123–140, 2020.

[EH79] David Eisenbud and Melvin Hochster. A Nullstellensatz with nilpotents and Zariski's main lemma on holomorphic functions. *J. Algebra*, 58(1):157–161, 1979.

[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.

[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.

[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.