# Contents

# Chapter 0

# Introduction

All rings, unless specified otherwise, are commutative with $0 \neq 1$.

All ideals $I$ are assumed to be strict subsets $I \neq R$. We will call the unit “ideal” an improper ideal.

# Chapter 1

# Finiteness conditions

**Question 1.1.** Given a (finite) set of symmetries, one can consider the collection of polynomial functions that are fixed by all of them. Is there a finite set of fixed polynomials such that any fixed polynomial can be expressed in terms of them?

## 1.1 Invariant rings

Let $G$ be a group acting on a ring $R$, or just as well, a group of automorphisms of $R$. The main case we have in mind is when $R = K[x_1, \dots, x_d]$ is a polynomial ring over a field. We are interested in the set of elements that are *invariant* under the action

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

If $r, s \in R^G$, then

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

since each $g$ is a homomorphism. Thus, $R^G$ is a subring of $R$.

We note that if $G = \langle g_1, \dots, g_t \rangle$, then $r \in R^G$ if and only if $g_i(r) = r$ for $i = 1, \dots, t$.

**Example 1.2** (Standard representation of the symmetric group)**.** Let $\mathcal{S}_d$ be the symmetric group on $d$ letters acting on $R = K[x_1, \dots, x_d]$ via $\sigma(x_i) = x_{\sigma_i}$.

For example, if $d = 3$, 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.

It is a theorem that you may have seen this in an earlier algebra class that every element of $R^G$ can be written as polynomial expression in the elementary symmetric polynomials $e_i = \sum\limits_{I \subseteq [d],\, |I| = i} (\prod_{j \in I} x_j)$. E.g, $f$ above is $e_1^2 - 2e_2$.

**Example 1.3** (Roots of unity)**.** Let $G = \{e, g\}$ act on $R = K[x_1, \dots, x_d]$ by negating the variables: $g \cdot x_i = -x_i$ for all $i$, so $g \cdot f(\underline{x}) = f(-\underline{x})$. Suppose that the characteristic of $K$ is not 2, so $-1 \neq 1$. Given a general $f$, we can write it as a sum of its *homogeneous* pieces: that is,

$$f = f_r + f_{r-1} + \cdots + f_1 + f_0,$$

where each $f_i$ is a sum of monomials of degree $i$. We have $g(f_i) = (-1)^i f_i$, so

$$g(f) = (-1)^r f_r + (-1)^{r-1} f_{r-1} + \cdots - f_1 + f_0,$$

which differs from $f$ unless every homogeneous piece of $f$ has even degree. That is,

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

This computation readily generalizes to the case of a field $K$ that contains $t$-th roots of unity, and a cyclic group $G = \langle g \rangle$ of order $t$ acting on $R$ by the rule $g(x_i) = \zeta_t \cdot x_i$ for all $i$. In this case, we have

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

This ring is called the *$t$-th Veronese ring*.

**Example 1.4** (A an action of the dihedral group of order 8)**.** Let $R = \mathbb{C}[x, y]$, and $G$ be the subgroup of $\mathrm{GL}_2(\mathbb{C})$ generated by

$$A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

acting on $(x, y)$ as on the vector $\begin{bmatrix} x \\ y \end{bmatrix}$. This subgroup isomorphic to the dihedral group of order 8. One can find some invariants

$$1, x^2y^2, x^4 + y^4, xy(x^4 - y^4), x^4y^4, x^2y^2(x^4 + y^4), x^8 + 2x^4y^4 + y^8, \ldots$$

and easily check that they all are invariant. Let's also check that I didn't miss any invariants of degree at most two. The elements $A$ and $B$ induce maps on $\mathbb{C}[x, y]_{\leq 2}$:

$$\widetilde{A} = \begin{array}{c|cccccc} & 1 & x & y & x^2 & xy & y^2 \\ \hline 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ x & 0 & i & 0 & 0 & 0 & 0 \\ y & 0 & 0 & -i & 0 & 0 & 0 \\ x^2 & 0 & 0 & 0 & -1 & 0 & 0 \\ xy & 0 & 0 & 0 & 0 & 1 & 0 \\ y^2 & 0 & 0 & 0 & 0 & 0 & -1 \end{array} \qquad \widetilde{B} = \begin{array}{c|cccccc} & 1 & x & y & x^2 & xy & y^2 \\ \hline 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ x & 0 & 0 & -1 & 0 & 0 & 0 \\ y & 0 & 1 & 0 & 0 & 0 & 0 \\ x^2 & 0 & 0 & 0 & 0 & 0 & 1 \\ xy & 0 & 0 & 0 & 0 & -1 & 0 \\ y^2 & 0 & 0 & 0 & 1 & 0 & 0 \end{array},$$

and to find invariants of degree at most two, we get a linear algebra problem: find the intersection of the kernels of $I - \widetilde{A}$ and $I - \widetilde{B}$, or equivalently, the kernel of $\begin{bmatrix} I - \widetilde{A} \\ I - \widetilde{B} \end{bmatrix}$; it's relatively easy to see here that we get just the span of 1. Of course, when we fix a degree cutoff, we can turn the problem of finding invariants into this linear algebra problem, but it's a problem that gets larger and larger.

**Example 1.5.** Some of the most interesting examples come from infinite groups $G$. Let $X = X_{2\times 3}$, be a matrix of indeterminates, and $\mathbb{C}[X]$ be the polynomial ring on those indeterminates. The group $\mathrm{SL}_2(\mathbb{C})$ acts on the matrix $X$ by left multiplication. Write $X_{\hat{i}}$ for the matrix $X$ with column $i$ removed. If $g \in \mathrm{SL}_2(\mathbb{C})$, then $gX_{\hat{i}} = (gX)_{\hat{i}}$, since left multiplication by $g$ can be computed column-by-column. Thus,

$$\det((gX)_{\hat{i}}) = \det(gX_{\hat{i}}) = \det(g)\det(X_{\hat{i}}) = \det(X_{\hat{i}}).$$

We find that the $2 \times 2$ minors of $X$ $(x_{11}x_{22} - x_{12}x_{21}, x_{11}x_{23} - x_{13}x_{21}, x_{12}x_{23} - x_{13}x_{22})$ must be invariant functions. This readily generalizes to $m \times n$ matrices with $m \leq n$ and maximal minors. It is harder to show that these maximal minors "account for" all of the invariants.

**Remark 1.6** (Invariants of actions on vectors spaces)**.** It's worth mentioning another important point of view. Given a finite dimensional vector space $V = K^d$, if we let $\{e_1, \dots, e_d\}$ be a basis of $V$ and $\{x_1, \dots, x_d\}$ be its dual basis in $V^*$, then we may think of $K[x_1, \dots, x_d]$ as the ring of polynomial functions on $V$. Given an action of $G$ on $V$, we obtain an action of $G$ on $V^*$ by $g \cdot \ell(v) = \ell(g^{-1} \cdot v)$, and then a degree-preserving $K$-linear action of $G$ on $K[x_1, \dots, x_d]$. (The $g^{-1}$ is to keep the action on the left.) Conversely, given a degree-preserving $K$-linear action of $G$ on $K[x_1, \dots, x_d]$, by restricting to the linear forms we get an action of $G$ on $V^*$, and then an action of $G$ on $V$. To translate between these points-of-view, if an element $g$ acts on $V$ by the matrix $A$, then $g$ acts on $V^*$ by $(A^T)^{-1}$.

## 1.2 Finitely generated algebras

Let $\varphi : A \to R$ be a ring homomorphism. Another piece of terminology for this situation is to say that $R$ is an *$A$-algebra.* An $A$-algebra is a ring $R$ and a homomorphism $\varphi : A \to R$; the same ring $R$ with two different maps $\varphi, \varphi' : A \to R$ yields two different $A$-algebras.

A set of elements $\Lambda \subseteq R$ *generates* $R$ as an $A$-algebra if the only subring of $R$ containing $\varphi(A)$ and $\Lambda$ is $R$ itself. This can be unpackaged more concretely in a number of equivalent ways:

1. $\Lambda$ generates $R$ as an $A$-algebra.

2. Every element of $R$ can be expressed in terms of $A$ and $\Lambda$ using the ring operations: for any $r$, there exist $b_1, \dots, b_t \in \varphi(A) \cup \Lambda$ such that $r = b_1 \Box b_2 \Box \cdots \Box b_t$ where each $\Box$ is a $+$ or $\cdot$.

3. Every element of $R$ admits a polynomial expression in $\Lambda$ with coefficients in $\varphi(A)$.

4. The homomorphism $\psi : A[X] \to R$, where $A[X]$ is a polynomial ring on $|\Lambda|$ indeterminates, and $\psi(x_i) = \lambda_i$, is surjective.

To see (1)⇔(2), note that the collection of elements of $r$ of the form $b_1 +/\times\, b_2 +/\times \cdots +/\times\, b_t$ with $b_i \in \varphi(A) \cup \Lambda$ is a subring of $R$ containing $\varphi(A) \cup \Lambda$. The assumption (1) says this subring is all of $R$ so (2) holds. On the other hand, any subring containing $\varphi(A) \cup \Lambda$ must contain all of these elements, giving the converse.

(2)⇔(3): We didn't give a proper definition for "polynomial expression," but any expression as in (2) simplifies to a polynomial expression by collecting like terms, and any polynomial expression expands as in (2). (3)⇔(4) is clear.

We say that $\varphi : A \to R$ is *algebra-finite*, or $R$ is a *finitely generated $A$-algebra*, if there exists a *finite* set of elements $f_1, \dots, f_t \in R$ that generates $R$ as an $A$-algebra. The term *finite-type* is also used to mean this. A better name might be *finitely generatable*, since to say that an algebra is finitely generated does not require knowing any actual finite set of generators.

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

A quick observation: any surjective $\varphi$ is algebra-finite: the target is generated by 1. Since any homomorphism $\varphi : A \to R$ can be factored as the surjection $A \to A/\ker(\varphi)$ followed by the inclusion $A/\ker(\varphi) \hookrightarrow R$, to understand algebra-finiteness, it suffices to restrict our attention to injective homomorphisms.

Evidently, our motivating question asks whether invariant rings of finite groups acting on $K[x_1, \dots, x_d]$ are finitely generated $K$-algebras.

**Example 1.7.** The Fundamental Theorem of Symmetric Functions says that if $\mathcal{S}_d$ is the symmetric group on $d$ letters acting on $R = K[x_1, \dots, x_d]$ via $\sigma(x_i) = x_{\sigma_i}$, then the invariant ring is $R^{\mathcal{S}_d} = K[e_1, \dots, e_d] \subseteq R$, where the $e_i$'s are those elementary symmetric functions mentioned above.

**Example 1.8** (Return to roots of unity)**.** We return to Example 1.3: if $R = K[x_1, \dots, x_d]$, $\zeta_t$ is a primitive $t$-th root of unity in $K$, and $G = \langle g \rangle$ of order $t$ acts on $R$ by the rule $g(x_i) = \zeta_t \cdot x_i$ for all $i$, we have

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

This ring of invariants is generated over $K$ by the finite set of monomials $\{x_1^{a_1} \cdots x_d^{a_d} \mid \sum_i a_i = t\}$. To see that these generate $R^G$, it suffices to show that we can use these elements to generate any monomial with degree $kt$ for some $k \in \mathbb{N}$, since any element of $R^G$ is a sum of such monomials. This translates to the fact that for any $\underline{b} = (b_1, \dots, b_d) \in \mathbb{N}^d$ with $\sum_i b_i = kt$ we can write $\underline{b} = \underline{b}^{(1)} + \cdots + \underline{b}^{(k)}$ with $\underline{b}^{(j)} \in \mathbb{N}^d$ and $\sum_i \underline{b}_i^{(j)} = t$ for each $j$. (Check this if you don't see how!)

**Remark 1.9.** 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, and
- $A \subseteq C$ algebra-finite $\Longrightarrow$ $B \subseteq C$ algebra-finite.

However, $A \subseteq C$ algebra-finite $\not\Longrightarrow$ $A \subseteq B$ algebra-finite. For example, let $A = K$ be a field, and $B = K[x, xy, xy^2, xy^3, \cdots] \subseteq C = K[x, y]$, where $x$ and $y$ are indeterminates. Any finitely generated subalgebra of $B$ is contained in $K[x, xy, \dots, xy^m]$ for some $m$, since we can write the elements in any finite generating set as polynomial expressions in the finitely many specified generators of $B$. But, every element of $K[x, xy, \dots, xy^m]$ is a $K$-linear combination of monomials with the property that the $y$ exponent is no more than $m$ times the $x$ exponent, so this ring does not contain $xy^{m+1}$. Thus, $B$ is not a finitely generated $A$-algebra.

## 1.3 Integral extensions

We will also find it quite useful to consider a stronger finiteness property for maps. Recall that if $\varphi : A \to R$ is a ring homomorphism, then $R$ acquires an $A$-module structure via $\varphi$ by $a \cdot r = \varphi(a)r$; this is a particular case of *restriction of scalars*. We may write ${}_\varphi R$ for this $A$-module if we think we will have trouble remembering the map. Of course, if $\varphi$ is injective and we identify it with the inclusion $A \subseteq R$, then this $A$-action is just $a \cdot r = ar$.

Recall that an $A$-module $M$ is generated by a set of elements $\Gamma \subseteq M$ if the only submodule of $M$ that contains $\Gamma$ is $M$ itself. This also has some equivalent realizations:

1. $\Gamma$ generates $M$ as an $A$-module.
2. Every element of $M$ can be expressed in terms of $\Gamma$ using the module operations: for any $m$, there exist $\gamma_1, \dots, \gamma_t \in \Gamma$ and $a_1, \dots, a_t \in R$ such that $m = \sum a_i \gamma_i$.
3. Every element of $M$ admits a linear combination expression in $\Gamma$ with coefficients in $A$.
4. The homomorphism $\theta : A^{\oplus Y} \to M$, where $A^{\oplus Y}$ is a free $A$-module on $|\Gamma|$ basis elements, and $\theta(y_i) = \gamma_i$, is surjective.

We recall that a *basis* for an $R$-module is a generating set $\Gamma$ such that $\sum_i a_i\gamma_i = 0$ implies all $a_i = 0$, for $a_i \in R$, $\gamma_i \in \Gamma$; a *free module* is a module that admits a basis. Every ring that is not a field admits a non-free module, namely the cyclic module $R/I$ for an ideal $I \subseteq R$.

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

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

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

**Example 1.10.**
1. If $K \subseteq L$ are fields, $L$ is module-finite over $K$ just means that $L$ is a finite field extension of $K$.

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

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

4. Another map that is *not* module-finite is the inclusion of $K[x] \subseteq K[x, 1/x]$. Note that any element of $K[x, 1/x]$ can be written in the form $f(x)/x^n$ for some $f$ and $n$. Then, any finitely generated $K[x]$-submodule $M$ of $K[x, 1/x]$ is of the form $M = \sum_i \frac{f_i(x)}{x^{n_i}} \cdot K[x]$; taking $N = \max\{n_i \mid i\}$, we find that $M \subseteq 1/x^N \cdot K[x] \neq K[x, 1/x]$.

**Lemma 1.11.** *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 $S = \sum_{i=1}^r Ra_i$ and $N = \sum_{j=1}^s Sb_j$. Then, $N = \sum_{i=1}^r \sum_{j=1}^s Ra_ib_j$: given $n = \sum_{j=1}^s s_jb_j$, rewrite each $s_j = \sum_{i=1}^r r_{ij}a_i$ and substitute to get $t = \sum_{i=1}^r \sum_{j=1}^s r_{ij}a_ib_j$ as an $R$-linear combination of the $a_ib_j$. □

In field theory, there is a close relationship between (vector space-)finite field extensions and algebraic equations. The situation for rings is similar.

**Definition 1.12** (Integral element/extension)**.** *Let $\varphi : A \to R$ be a ring homomorphism, and $r \in R$. The element $r$ is* integral *if there are elements $a_0, \dots, a_{n-1} \in A$ such that*

$$r^n + \varphi(a_{n-1})r^{n-1} + \cdots + \varphi(a_1)r + \varphi(a_0) = 0;$$

*i.e., $r$ satisfies a* equation of integral dependence *over $A$.*

*We say that $R$ is an* integral over $A$ *of $A$ if every $r \in R$ is integral over $A$.*

Like our other smallness hypotheses for maps, we see that $r \in R$ is integral over $A$ if an only if $r$ is integral over the subring $\varphi(A) \subseteq R$. Again, we can restrict our focus to inclusion maps $\varphi(A) \subseteq R$.

Evidently, integral implies algebraically dependent, and the condition that there exists an equation of algebraic dependence that is *monic* is stronger in the setting of rings.

**Proposition 1.13.** *Let $A \subseteq R$ be rings.*

1. *If $r \in R$ is integral over $A$ then $A[r]$ is module-finite over $A$.*
2. *If $r_1, \dots, r_t \in R$ are integral over $A$ then $A[r_1, \dots, r_t]$ is module-finite over $A$.*

*Proof.*

1. Suppose $r$ is integral over $A$, satisfying the equation $r^n + a_{n-1}r^{n-1} + \cdots + a_1 r + a_0 = 0$. Then $A[r] = \sum_{i=0}^{n-1} Ar^i$. Indeed, given a polynomial in $p(r)$ of degree $\geq n$, we can use the equation above to rewrite the leading term $a^m r^m$ as $-a_m r^{m-n}(a_{n-1}r^{n-1} + \cdots + a_1 r + a_0)$, and decrease the degree in $r$.
2. Write $A_0 := A \subseteq A_1 := A[r_1] \subseteq A_2 := A[r_1, r_2] \subseteq \cdots \subseteq A_t := A[r_1, \dots, r_t]$. Note that $r_i$ is integral over $A_{i-1}$: use the same monic equation of $r_i$ over $A$. Then, the inclusion $A \subseteq A[r_1, \dots, r_t]$ is a composition of module-finite maps, hence is module-finite. □

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

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

**Lemma 1.14** (Determinant trick)**.** *Let $R$ be a ring, and $B \in M_{n\times n}(R)$. Then* $\mathrm{adj}(B)B = \det(B)I_{n\times n}$.

*Proof.* When $R$ is a field, this is a basic fact. We deduce the case of a general commutative ring from the field case.

The ring $R$ is a $\mathbb{Z}$-algebra (every ring is a $\mathbb{Z}$-algebra, but generally not finitely generated as such), so we can write $R$ as a quotient of some polynomial ring $\mathbb{Z}[X]$. Let $\psi : \mathbb{Z}[X] \to R$ be a surjection, let $a_{ij} \in \mathbb{Z}[X]$ be such that $\psi(a_{ij}) = b_{ij}$, and let $A = [a_{ij}]$. Note that $\psi(\mathrm{adj}(A)_{ij}) = \mathrm{adj}(B)_{ij}$ and $\psi((\mathrm{adj}(A)A)_{ij}) = (\mathrm{adj}(B)B)_{ij}$, since $\psi$ 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 the lemma in the case $R = \mathbb{Z}[X]$. Now, $R = \mathbb{Z}[X]$ is an integral domain, hence a subring of its fraction field. Since both sides of the equation live in $R$ and are equal in the fraction field (by linear algebra) they are equal in $R$. □

**Theorem 1.15** (Module finite implies integral)**.** *Let $A \subseteq R$ be module-finite. Then $R$ is integral over $A$.*

*Proof.* Let $r \in R$. The idea is to show that multiplication by $r$, realized as a linear transformation over $A$, satisfies the characteristic polynomial of that linear transformation.

Write $R = \sum_{i=1}^{t} Ar_i$. We may assume that $r_1 = 1$, since we can add module generators. By assumption, we can find $a_{ij} \in A$ such that

$$rr_i = \sum_{j=1}^{t} a_{ij} r_j$$

for each $i$. Let $C = [a_{ij}]$, and $v$ be the column vector $(r_1, \dots, r_t)$. We then have $rI_{n\times n}v = Cv$, so $(rI_{n\times n} - C)v = 0$. Set $B = rI_{n\times n} - C$. By the lemma, $0 = \mathrm{adj}(B)0 = \mathrm{adj}(B)Bv = \det(B)v$, and in particular, considering the first entry, we get $\det(B) = 0$. That is, $r$ satisfies the characterstic polynomial $\det(rI_{n\times n} - C)$, which is a monic equation with coefficients in $A$. □

**Corollary 1.16** (Characterization of module-finite extensions)**.** *Let $A \subseteq R$ be rings. $R$ is module-finite over $A$ if and only if $R$ is integral and algebra-finite over $A$.*

*Proof.* ($\Rightarrow$): A generating set for $R$ as an $A$-module serves as a generating set as an $A$-algebra. The rest of this direction comes from the previous theorem. ($\Leftarrow$): If $R = A[r_1, \dots, r_t]$ is integral over $A$, so that each $r_i$ is integral over $A$, then $R$ is module-finite over $A$ by Proposition 1.13. □

**Corollary 1.17.** *If $R$ is generated over $A$ by integral elements, then $R$ is integral. Thus, if $A \subseteq S$, the set of elements of $S$ that are integral over $A$ form a subring of $S$.*

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

For the latter statement,

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

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

**Definition 1.18.** *If $A \subseteq R$, the* integral closure of $A$ in $R$ *is the set of elements of $R$ that are integral over $A$.*

**Example 1.19.**

1. Let $R = \mathbb{C}[x, y] \subseteq S = \mathbb{C}[x, y, z]/(x^2 + y^2 + z^2)$. The ring $S$ is module-finite over $R$: indeed, $S$ is generated over $R$ as an algebra by one element $z$ that is integral over $R$.

2. Let $R = \mathbb{C}[u, v] \subseteq S = \mathbb{C}[u, v, w]/(u^2 + vw)$. (Note that this $S$ is isomorphic to the previous $S$ by the map $u \mapsto x, v \mapsto y + iz, w \mapsto y - iz$, and this $R$ corresponds to the polynomial subring $\mathbb{C}[x, y + iz]$.) We claim that $S$ is *not* integral and hence *not* module-finite over $R$. Indeed, the minimal polynomial of $w$ over the fraction field of $R$ is $f(t) = vt + u^2$. Any equation that $w$ satisfies is a $\mathbb{C}(u, v)[t]$-multiple of this: write $g(t) = f(t)h(t)$ with $g(t) \in \mathbb{C}(u, v)[t]$ monic. By Gauss' lemma, there is some $a \in \mathbb{C}(u, v)$ such that $a^{-1}f(t), ah(t) \in \mathbb{C}[u, v][t]$. Since the leading coefficient of $h$ is $v^-1$, the numerator of $a$ must be a multiple of $v$ when written in lowest terms. But this contradicts that $a^{-1}f(t) \in \mathbb{C}[u, v][t]$.

3. Not all integral extensions are module-finite. Let $K = \overline{K}$, and consider the ring $R = K[x, x^{1/2}, x^{1/3}, x^{1/4}, x^{1/5}, \dots] \subseteq \overline{K(x)}$. Clearly $R$ is generated by integral elements over $K[x]$, but is not algebra-finite over $K[x]$. (Prove it!)

**Remark 1.20.** Let $A \subseteq B \subseteq C$ be rings. As with algebra-finiteness, it follows from the definitions that

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

but again, $A \subseteq C$ module-finite $\not\Longrightarrow A \subseteq B$ module-finite. Here is a general construction that we can put to use for this purpose. If $R$ is a ring and $M$ a module, the *idealization* of $M$ is the ring $R \rtimes M$ with additive/set-theoretic structure $R \oplus M$ and multiplication $(r, m)(s, n) = (rs, rn + sm)$. Let $R$ be a ring, and $M = I$ be an ideal that is not finitely generated (see the next section for many examples of this). Then $R \subseteq R \rtimes I \subseteq R \rtimes R$ serves as a counterexample.

Returning to our motivating question, we note that module-finite maps show up in the context of invariant rings.

**Proposition 1.21.** *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.* We will show that $R$ is algebra-finite and integral over $R^G$.

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

Now, for $r \in R$, consider the polynomial $F_r(t) = \prod_{g \in G}(t - g(r)) \in R[t]$. Clearly $g(F_r(t)) = F_r(t)$, where $G$ fixes $t$. Thus, $F_r(t) \in R^G[t]$. The leading term (with respect to $t$) is $t^{|G|}$, so $F_r(t)$ is monic. Thus, $r$ is integral over $R^G$. Therefore, $R$ is integral over $R^G$. □

## 1.4 Noetherian rings and modules

The last ingredient we need is a finiteness condition for a ring $R$.

**Definition 1.22** (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 $n > N$.*

This condition also admits some equivalences.

**Proposition 1.23** (Equivalences for Noetherian ring)**.** *The following are equivalent for a ring $R$.*

1. *$R$ is a Noetherian ring.*

2. *Every nonempty family of ideals has a maximal element (under containment).*

3. *Every ascending chain of finitely generated ideals of $R$ eventually stabilizes.*

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

5. *Every ideal of $R$ is finitely generated.*

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

(2)⇒(1): Clear.

(1)⇒(3): Clear.

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

(4)⇒(5): Clear.

(5)⇒(1): Given an ascending chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ let $I = \bigcup_{n \in \mathbb{N}} I_n$. The ideal $I$ is finitely generated, say $I = (a_1, \dots, a_t)$, and since each $a_i$ is in some $I_{n_i}$, there is an $N$ such that each $a_i$ is in $I_N$. But then $I_n = I = I_N$ for all $n > N$. □

**Example 1.24.**

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

2. If $R$ is a PID, then $R$ is Noetherian. Every ideal is finitely generated!

3. As a special case of the previous, 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 $z^n g(z)$ with $g(z) \neq 0$, 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 $K$: 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. Another ring that is *not* Noetherian is the ring $R = K[x, x^{1/2}, x^{1/3}, x^{1/4}, x^{1/5}, \dots] \subseteq \overline{K(x)}$ from earlier. A nice ascending chain of ideals is
$$(x) \subseteq (x^{1/2}) \subseteq (x^{1/3}) \subseteq (x^{1/4}) \subseteq \cdots .$$

6. A variation on the last example: the ring of *nonnegatively valued Puiseux series*: $R = \bigcup_{n\in\mathbb{N}} \mathbb{C}[\![z^{1/n}]\!] \subseteq \overline{\mathbb{C}((z))}$.[1]

7. The ring of continuous real-valued functions $\mathcal{C}(\mathbb{R}, \mathbb{R})$ is not Noetherian: the chain of ideals $I_n = \{f(x) \mid f|_{[-1/n,1/n]} \equiv 0\}$ is increasing and proper. The same construction shows that the ring of infinitely differentiable real functions $\mathcal{C}^\infty(\mathbb{R}, \mathbb{R})$ is not Noetherian: properness of the chain follows from, e.g., Urysohn's lemma (though it's not too hard to find functions distinguishing the ideals in the chain). Note that if we asked for analytic functions instead of infinitely-differentiable functions, every element of the chain would be the zero ideal!

**Definition 1.25** (Noetherian module)**.** *An $R$-module $M$ is* Noetherian *if every ascending chain of submodules of $M$ eventually stabilizes.*

There are analogous criteria for modules to (1)–(5) above namely:

**Proposition 1.26** (Equivalences for Noetherian module)**.** *The following are equivalent for a module $M$:*

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.*

We observe that if $R$ is Noetherian, and $I$ is an ideal of $R$, then $R/I$ is Noetherian as well, since there is an order-preserving bijection
$$\{\text{ideals of } R \text{ that contain } I\} \leftrightarrow \{\text{ideals of } R/I\}.$$

**Lemma 1.27.** *Let $M$ be a module, and $M', M'', N$ be submodules of $M$.*

[1] In fact, the algebraic closure of the field of Laurent series $\mathbb{C}((z))$ is $\bigcup_{n\in\mathbb{N}} \mathbb{C}((z^{1/n})) = R[1/t]$.

1. *Then $M' = M''$ if and only if $M' \cap N = M'' \cap N$ and $M'/(M' \cap N) = M''/(M'' \cap N)$.*

2. *$M$ is Noetherian if and only if $N$ and $M/N$ Noetherian.*

*Proof.* 1. ($\Rightarrow$) is clear. Suppose that $M' \subsetneq M''$ and $M' \cap N = M'' \cap N$. Then, there is some $m \in M'' \smallsetminus M'$. We claim that the class of $m$ in $M''/(M'' \cap N)$ is not equal to the class of $m'$ in $M''/(M'' \cap N)$ for any $m' \in M'$. Indeed, if it were, then $m - m' \in M'' \cap N = M' \cap N$, so that $m \in M' + M' \cap N = M'$, a contradiction.

2. A chain of submodules of $N$ is a chain of submodules of $M$, and a (proper) chain of submodules of $M/N$ lifts to a (proper) chain of submodules of $M$, so $M$ Noetherian implies $N$ and $M/N$ are. Conversely, if $N$ and $M/N$ are Noetherian, then for any chain

$$M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots$$

of submodules of $M$, the chains

$$(M_0 \cap N) \subseteq (M_1 \cap N) \subseteq (M_2 \cap N) \subseteq \cdots$$

in $N$ and

$$\frac{M_0}{M_0 \cap N} \subseteq \frac{M_1}{M_1 \cap N} \subseteq \frac{M_2}{M_2 \cap N} \subseteq \cdots$$

in $M/N$ stabilize eventually. If both chains are stable past index $n$, then the chain in $M$ is stable past index $n$ by part 1. □

**Proposition 1.28.** *Let $R$ be a Noetherian ring. Then $M$ is a Noetherian module if and only if $M$ is finitely generated.*

*Consequently, if $R$ is Noetherian, then any submodule of a finitely generated $R$-module is also finitely generated.*

*Proof.* If $M$ is Noetherian, it (and all of its submodules) is finitely generated by the equivalences above.

Now let $R$ be Noetherian and $M$ be f.g.. First, we show that the free module $R^{\oplus n} = \bigoplus_{i=1}^n Re_i$ is Noetherian for all $n \in \mathbb{N}$ by induction on $n$. For the base case, we note that $R$ is a Noetherian ring iff the free cyclic module $R^{\oplus 1}$ is a Noetherian module, since ideals of $R$ correspond to submodules of $R^{\oplus 1}$. The inductive step follows since we have an isomorphism $(\bigoplus_{i=1}^n Re_i)/Re_n \cong \bigoplus_{i=1}^{n-1} Re_i$. Now, a finitely generated module $M$ is quotient of a finitely generated free module, so is Noetherian by the previous lemma. □

It is now clear that a module-finite extension $R$ of a Noetherian ring $A$ is Noetherian: $R$ is a Noetherian $A$-module, and any ideal of $R$ is an $A$-submodule of $R$, so an ascending chain necessarily stabilizes.

You likely already are familiar with the stronger statement:

**Theorem 1.29** (Hilbert Basis Theorem)**.** *Let $A$ be a Noetherian ring. Then $A[x_1, \dots, x_d]$ and $A[\![x_1, \dots, x_d]\!]$ are Noetherian.*

*Proof.* We give the proof for polynomial rings, and indicate the difference in the power series argument.

By induction on $d$, we reduce to the case $d = 1$. Let $I \subseteq A[x]$, and let

$$J = \{a \in A \mid \exists\, ax^n + \text{lower order terms (wrt } x) \in I\}.$$

This is easily seen to be an ideal of $A$, which is finitely generated by hypothesis; let $J = (a_1, \dots, a_t)$. Pick $f_1, \dots, f_t \in A[x]$ such that the leading coefficient of $f_i$ is $a_i$, and set $i' = (f_1, \dots, f_t)$. Let $N = \max_i \deg f_i$.

Given $f \in I$ of degree greater than $N$, we can cancel off the leading term of $f$ by subtracting a suitable multiple of some $f_i$, so any $f \in I$ can be written as $g + h$ with $g \in I \cap \sum_{i=0}^{N} Ax^i$ and $h \in I'$. Since $I \cap \sum_{i=0}^{N} Ax^i$ is a submodule of a finitely generated free $A$-module, it is also finitely generated as an $A$-module. Given such a generating set, we can clearly write any such $f$ as an $A[x]$-linear combination of these generators and the $f_i$'s.

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

**Corollary 1.30.** *If $A$ is a Noetherian ring, then any finitely generated $A$-algebra is Noetherian. In particular, any finitely generated algebra over a field is Noetherian.*

The converse to this statement is false: there are lots of Noetherian rings that are not f.g. algebras over a field. For example, $\mathbb{C}\{z\}$ is not algebra-finite over $\mathbb{C}$. You will show (modulo some steps) that rings of power series and rings of complex functions analytic near a point are both Noetherian. We will also see huge classes of easy examples once we switch to localization. However, we'll see a converse in a very special case soon.

Now, we prove a technical theorem that relates all of our finiteness notions. The statement is a bit complicated, but the result will be pretty useful.

**Theorem 1.31** (Artin-Tate Lemma)**.** *Let $A \subseteq B \subseteq C$ be rings. Assume that*

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

*Then, $B$ is algebra-finite over $A$.*

*Proof.* Let $C = A[f_1, \dots, f_r]$ and $C = \sum_{i=1}^{s} Bg_i$. Then,

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

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

We claim that $C = \sum_{i=1}^{s} B_0 \, g_i$. Given an element $c \in C$, write $c$ as a polynomial expression in $\underline{f}$. We have that $c \in A[\{b_{ij}\}][g_1, \dots, g_s]$. Then, using the equations for $g_i g_j$, we can write $c$ in the form required.

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

Now we can give an answer to our motivating question.

**Theorem 1.32.** *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 $R^G$ is a finitely-generated $K$-algebra.*

*Proof.* We have $K \subseteq R^G \subseteq R$. To apply the Artin-Tate Lemma, we observe that $K$ is Noetherian, $R$ is module-finite over $R^G$ by an earlier Proposition, and $R$ is algebra-finite over $K$. We conclude that $R^G$ is algebra-finite over $K$. □

## 1.5 Graded rings

A useful bit of extra structure that one commonly encounters, and that we have already used, even, is that of a grading on a ring.

**Definition 1.33.** *Let $R$ be a ring, and $A$ be a monoid. The ring $R$ is $A$-*graded *if there exists a direct sum decomposition of $R$ as an abelian group indexed by $A$: $R = \bigoplus_{a \in A} R_a$ such that, for any $a, b \in A$, and any $r \in R_a, s \in R_b$, one has $rs \in R_{a+b}$.*

*An element that lies in one of the summands $R_a$ is said to be* homogeneous *of* degree *$a$; we often use $|r|$ to denote the degree of a homogeneous element $r$.*

**Definition 1.34.** *Let $R$ and $S$ be $A$-graded rings (same grading monoid). A ring homomorphism $\varphi : R \to S$ is* degree-preserving *if $\varphi(R_a) \subseteq S_a$ for all $a \in A$.*

By definition, an element in a graded ring is, in a unique way, a sum of homogeneous elements, which we call its homogeneous components or graded components.

**Example 1.35.**

1. If $K$ is a field, and $R = K[x_1, \dots, x_n]$ is a polynomial ring, then there is an $\mathbb{N}$-grading on $R$ where $R_d$ is the $K$-vector space with basis given by monomials $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ with $\sum_i \alpha_i = d$. Of course, this is the notion of degree familiar from grade school. This is called the *standard grading*.

2. With $K$ and $R$ as above, for any $(\beta_1, \dots, \beta_n) \in \mathbb{N}^n$, one can give a different $\mathbb{N}$-grading on $R$ by letting $x_i$ have degree $\beta_i$ for some integers $\beta_i$; 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 is homogeneous of degree 6 under the $\mathbb{N}$-grading with weights $(3, 2)$.

3. Again with $K$ and $R$ as above, $R$ admits an $\mathbb{N}^n$-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*.

4. Let $\Gamma \subseteq \mathbb{N}^n$ be a subsemigroup. Then $\bigoplus_{\gamma \in \Gamma} K\underline{x}^{\gamma} \subseteq K[\underline{x}]$ is an $\mathbb{N}^n$-graded subring. Conversely, every $\mathbb{N}^n$-graded subring of $K[x_1, \dots, x_n]$ is of this form. (Check it!)

5. 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 $R$. (I.e., $R^G$ is graded with respect to the same grading monoid.)

**Definition 1.36.** *An ideal $I$ in a graded ring $R$ is called* homogeneous *if it is generated by homogeneous elements.*

We observe that an ideal is homogeneous if and only if, for any $f \in R$, one has $f \in I$ if and only if every homogeneous component of $f$ lies in $I$. To see "if," take a generating set $\{f_\lambda\}_\Lambda$ for $I$; all of its homogeneous components of each $f_\lambda$ lie in $I$, and each $f_\lambda$ lies in the ideal generated by these components. Thus the set of components generates $I$. The other direction is also easy.

We now observe the following:

**Lemma 1.37.** *Let $R$ be an $A$-graded ring, and $I$ be a homogeneous ideal. Then $R/I$ is also $A$-graded.*

**Example 1.38.**

1. The ring $R = K[w, x, y, z]/(w^2x + wyz + z^3, x^2 + 3xy + 5xz + 7yz + 11z^2)$ admits an $\mathbb{N}$-grading with $|w| = |x| = |y| = |z| = 1$.

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

**Definition 1.39.** *Let $R$ be an $A$-graded ring, and $M$ a module. The module $R$ is $A$-*graded *if there exists a direct sum decomposition of $M$ as an abelian group indexed by $A$: $M = \bigoplus_{a \in A} M_a$ such that, for any $a, b \in M$, and any $r \in R_a, m \in R_b$, one has $rm \in M_{a+b}$.*

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 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 1.40.** *Let $R$ be an $\mathbb{N}$-graded ring, and $f_1, \dots, f_n$ 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.*

*Consequently, $R$ is Noetherian if and only if $R_0$ is Noetherian and $R$ is algebra-finite over $R_0$.*

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

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

We leave the "consequently" part to you as an exercise. □

At this point, we have earned the right to moralize a little.

**Moral 1.41.** *The Noetherian property is a natural and useful finiteness property for rings.*

**Moral 1.42.** *For a ring homomorphism $\varphi : R \to S$, it is useful and meaningful to examine the $R$-module structure of $S$.*

# Chapter 2

# The Nullstellensatz

**Question 2.1.** To what extent is a system of polynomial equations determined by its solution set?

At first glance, things look pretty bad. For example, the systems of equations

$$\begin{cases} x = 0 \\ y = 0 \end{cases}, \qquad \begin{cases} x^2 = -y^2 \end{cases}, \qquad \text{and} \begin{cases} xy^2 + x = -x^3 \\ yx^2 + y = -y^3 \end{cases}$$

all have the same solution set in $\mathbb{R}^2$. For that matter, the systems of equations

$$\begin{cases} 2x + 3y + 4z + 5w = 1 \\ 4x + 6y + 8z + 10w = 3 \end{cases}, \qquad \begin{cases} x^2 + y^2 + z^2 + w^2 - 7 = 0 \\ xyzw = 4 \end{cases}, \qquad \text{and} \begin{cases} 1 = 0 \end{cases}$$

all have the solution set in $\mathbb{Q}^4$.

Let's consider one polynomial equation in one variable. Over $\mathbb{R}, \mathbb{Q}$, or other fields that aren't algebraically closed, there are many polynomials with an empty solution set. On the other hand, over $\mathbb{C}$, or any algebraically closed field, if $f(z) = 0$ has solutions $z_1, \dots, z_d$, we know that $f(z) = \alpha(z - z_1)^{a_1} \cdots (z - z_d)^{a_d}$, so that $f$ is determined up to scalar multiple and repeated factors. This suggests that in general, we may want to restrict to algebraically closed fields $K$, so we'll do that soon. We will be rewarded by an a posteriori justification for this myopia, but we don't assume it yet.

Now, given a system of polynomial equations in $d$ variables, we can always subtract over to rewrite it in the form $f_\lambda(\underline{x}) = 0, \lambda \in \Lambda$. We will write

$$Z_K(\{f_\lambda \mid \lambda \in \Lambda\}) := \{\underline{a} \in K^d \mid f_\lambda(\underline{a}) = 0 \text{ for all } \lambda \in \Lambda\}$$

to denote the solution set. Note that adding in more equations gives us a smaller solution set, but not necessarily strictly. In fact, given a set of equations, many other equations follow for free as consequences; namely, if $r_1, \dots, r_t \in K[x_1, \dots, x_d]$, then any solution $\underline{a}$ to the system $f_\lambda(\underline{x}) = 0, \lambda \in \Lambda$ is also a solution to

$$r_1(\underline{x}) f_{\lambda_1}(\underline{x}) + \cdots + r_t(\underline{x}) f_{\lambda_t}(\underline{x}) = 0.$$

That is, every equation in the ideal generated by a set of equations is an automatic consequence. Thus, the set of solutions to $(\star)$ is the same as the set of solutions to $Z_K(I)$, where $I$ is the ideal $(\{f_\lambda(\underline{x}) = 0 \mid \lambda \in \Lambda\})$. In particular, by the Hilbert basis theorem, any system of polynomial equations is equivalent to a system of finitely many polynomial equations!

We have associations

$$\begin{array}{lclcr} \text{system of equations} & \rightsquigarrow & \text{ideal} & \rightsquigarrow & \text{solution set} \\ f_1, \dots, f_t & \mapsto & I = (f_1, \dots, f_t) & \mapsto & Z(I) \end{array}$$

We will deal with second part in this chapter: to what extent is the association $I \mapsto Z(I)$ reversible?

By way of terminology, if $K$ is a field, and $X \subseteq K^n$ is a subset of the form $Z_K(\{f_\lambda\})$ for some polynomials $f_\lambda$, or equivalently, $X = Z_K(I)$ for some ideal $I \subseteq K[x_1, \dots, x_n]$, then we call $X$ an *affine variety*, or a *subvariety of $K^n$*.

**Example 2.2.** Clearly, linear subspaces of $K^n$ are subvarieties of $K^n$, since linear equations are polynomial equations. Thus, the geometry of linear algebra is under the purview of the geometry of affine varieties. A next class of geometric objects is unions of linear spaces. For example, the union of the $x$-axis and $y$-axis in $K^2$ is $Z_K(xy)$: $xy = 0$ if and only if $x = 0$ or $y = 0$. We could also take the union $X$ of two planes in $K^4$ that meet at a point: we claim this is the same as $Y = Z_K(xu, xv, yu, yv)$. Indeed, $Y$ is the set of points such that

$$(x = 0 \text{ or } u = 0) \text{ and } (x = 0 \text{ or } v = 0) \text{ and } (y = 0 \text{ or } u = 0) \text{ and } (y = 0 \text{ or } v = 0).$$

If $x$ and $y$ are zero, or $u$ and $v$ are zero, then we can see that all of the equations above hold. Conversely, if one of each of $u, v$ and $x, y$ is nonzero, then one of the products above is nonzero. Thus, $Y$ is the union of two coordinate planes ($X = Y$). We claim that $X = Z_K(xu, xv + yu, yv)$ as well. Indeed, $X \subseteq Z_K(xu, xv + yu, yv)$ is clear, and any point in the difference would have $xv$ or $yu$ nonzero and $xv = -yu$, so both nonzero, hence $xu$ nonzero as well, a contradiction. The ideals $(xu, xv + yu, yv)$ and $(xu, xv, yu, yv)$ are different, since $xv$ is not in the first; we can see this by using the graded structure.

**Remark 2.3.** More generally, the union of two subvarieties of $K^n$ is a subvariety of $K^n$: $Z_K(I) \cup Z_K(J) = Z_K(IJ)$. (Exercise!)

**Example 2.4.** Let $R = K\begin{bmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{bmatrix}$, and $I = (\Delta_1, \Delta_2, \Delta_3)$, the $2 \times 2$-minors of the matrix. Thinking of these generators as equations, a solution is just a matrix of rank at most one, so $Z_K(I)$ is the set of rank at most one matrices. Let $J = (x_1, x_2, x_3)$, and observe that $I \subseteq J$. We then have that $Z_K(J) \subseteq Z_K(I)$: this just translates to the fact that a $2 \times 3$ matrix with a zero row has rank at most 1.

## 2.1 Solutions, algebra homomorphisms, and maximal ideals

We now wish to consider solutions of polynomial equations in great generality. A *homomorphism of $R$-algebras* from $S$ to $T$ is a ring homomorphism such that

$$\begin{tikzcd} S \arrow[rr] & & T \\ & R \arrow[ul] \arrow[ur] & \end{tikzcd}$$

commutes.

Let $R$ be a ring, and $S$ an $R$-algebra. Given a system of polynomial equations

$$(\star) : \{f(\underline{x}) = 0, f \in \Lambda\}, \quad f \in R[x_1, \dots, x_d],$$

consider the $R$-algebra $R[\underline{x}]/I$, where $I = (\Lambda)$. If $\underline{a} \in S^d$ is a solution to $(\star)$ so that all $f(\underline{a}) = 0$ as polynomial expressions in $S$, then the $R$-algebra homomorphism from $R[\underline{x}] \to S$ given by $x_i \mapsto a_i$ descends to an $R$-algebra map $R[\underline{x}]/I \to S$. Conversely, any $R$-algebra map from $R[\underline{x}]/I$ to $S$ is determined by the images of $\underline{a}$, which must satisfy all of the equations $f_\lambda(\underline{x}) = 0$. We summarize:

**Proposition 2.5.** *Let $R$ be a ring, and $S$ an $R$-algebra. Let $(\star)$ and $I$ be as above. There is a bijection*

$$\begin{array}{ccc} Z_S(I) & \leftrightarrow & \mathrm{Hom}_{R-\mathrm{alg}}\left(R[\underline{x}]/I, S\right) \\ (a_1, \dots, a_d) & \mapsto & \varphi|_R = \mathrm{id}, \varphi(x_i) = a_i. \end{array}$$

Now, we focus on polynomial equations over fields.

**Proposition 2.6.** *Let $K$ be a field, and $R = K[x_1, \dots, x_d]$ be a polynomial ring. There is a bijection*

$$\begin{array}{ccc} K^d & \leftrightarrow & \{\textit{maximal ideals } \mathfrak{m} \textit{ of } R \textit{ such that } R/\mathfrak{m} \cong K\} \\ (a_1, \dots, a_d) & \mapsto & (x_1 - a_1, \dots, x_d - a_d). \end{array}$$

*Proof.* We observe first that each ideal $(x_1 - a_1, \dots, x_d - a_d)$ is a maximal ideal with residue field $K$, and that 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. To see that the map is surjective, let $\pi : R \twoheadrightarrow K$ be a surjective map. We have $\pi(x_i) \in K$ so $(x_1 - \pi(x_1), \dots, x_d - \pi(x_d)) \subseteq \mathfrak{m}$. The quotient by this ideal is already $K$, so $(x_1 - \pi(x_1), \dots, x_d - \pi(x_d)) = \mathfrak{m}$. □

**Theorem 2.7.** *Let $K$ be a field, and $R = K[x_1, \dots, x_d]/I$ be a finitely generated $K$-algebra. There are bijections*

$$\begin{array}{ccccc} Z_K(I) & \leftrightarrow & \{\textit{maximal ideals } \mathfrak{m} \textit{ of } R \textit{ s.t. } R/\mathfrak{m} \cong K\} & \leftrightarrow & \mathrm{Hom}_{K-\mathrm{alg}}(R, K) \\ (a_1, \dots, a_d) \in Z(I) \subseteq K^d & \mapsto & (x_1 - a_1, \dots, x_d - a_d) & & \\ & & \mathfrak{m} & \mapsto & R \twoheadrightarrow R/\mathfrak{m} \cong K \end{array}$$

*Proof.* We note first that the maximal ideals of $R$ are in bijection with the maximal ideals of $K[\underline{x}]$ that contain $I$. The first bijection is then induced from the previous proposition. The second map is clearly bijective. □

## 2.2 Maximal ideals of polynomial rings

**Lemma 2.8** (Zariski's Lemma). *Let $K \subseteq L$ be fields. If $L$ is a finitely generated $K$-algebra, then $L$ is a finite dimensional $K$-vector space.*

*Proof.* Let $L = K[x_1, \dots, x_d]$, and suppose that $L$ is not a finite dimensional $K$-vector space. Since $L = K(x_1, \dots, x_d)$, we can choose a transcendence basis for $L/K$ from among the $x$'s, and after reordering, we may assume that $x_1, \dots, x_c$ form a transcendence basis, and $x_{c+1}, \dots, x_d$ are algebraic over $K' = K(x_1, \dots, x_c)$. Then $L$ is integral and algebra-finite over $K'$, hence module-finite. We can apply the Artin-Tate Lemma to $K \subseteq K' \subseteq L$ to see that $K'$ is algebra-finite over $K$. In particular, there are $f_i, g_i$ in the polynomial ring $K[x_1, \dots, x_c]$ such that $K' = K[\frac{f_1}{g_1}, \dots, \frac{f_c}{g_c}]$.

This implies that any element of $K'$ can be written as a fraction with denominator $(g_1 \cdots g_c)^n$ for some $n$. But, the element $\frac{1}{g_1 \cdots g_c + 1} \in K'$ cannot be written this way; if so, we would have

$$\frac{v}{(g_1 \cdots g_c)^n} = \frac{1}{g_1 \cdots g_c + 1},$$

for some $v$ with $g_1 \cdots g_c \nmid v$ (since the polynomial ring is a UFD). But, the equation $g_1 \cdots g_c v + v = (g_1 \cdots g_c)^n$ contradicts this. □

**Corollary 2.9.** *Let $K$ be a field, and $R$ be a finitely generated $K$-algebra. For any maximal ideal $\mathfrak{m}$ of $R$, $R/\mathfrak{m}$ is a finite extension of $K$.*

*In particular, if $K$ is algebraically closed, $R/\mathfrak{m} \cong K$.*

Along similar lines, we have the following:

**Exercise 2.10.** If $R$ is a finitely generated $\mathbb{Z}$-algebra, and $K = R/\mathfrak{m}$ is a residue field of $R$, then $K$ is finite.

**Corollary 2.11** (Maximal ideals of f.g. $K = \overline{K}$-algebras)**.** *Let $K$ be an algebraically closed field, and $S = K[x_1, \ldots, x_d]$ be a polynomial ring. There is a bijection*

$$K^d \leftrightarrow \{\textit{maximal ideals } \mathfrak{m} \textit{ of } S\}$$

*given by $(a_1, \ldots, a_d) \mapsto (x_1 - a_1, \ldots, x_d - a_d)$. 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*

$$Z_K(I) \subseteq K^d \leftrightarrow \{\textit{maximal ideals } \mathfrak{m} \textit{ of } R\}.$$

**Theorem 2.12** (Medium Nullstellensatz)**.** *Let $K$ be an algebraically closed field, and $R = K[x_1, \ldots, x_d]$ be a polynomial ring. Let $I \subseteq R$ be a (possibly improper) ideal. Then $Z_K(I) = \varnothing$ if and only if $I = (1)$.*

*Proof.* If $I = (1)$, clearly $Z(I) = \varnothing$.

Let $I \subsetneq R$ be a proper ideal. Then, there is some maximal ideal $I \subseteq \mathfrak{m}$, and $Z(\mathfrak{m}) \subseteq Z(I)$. We can write $\mathfrak{m} = (x_1 - a_1, \ldots, x_d - a_d)$, so $Z(\mathfrak{m}) = \{(a_1, \ldots, a_d)\}$; in particular, it is nonempty. □

We can now give a good justification for restricting to algebraically closed fields.

**Corollary 2.13.** *Let $K$ be an arbitrary field, and $\{f_\lambda\}$ a set of polynomial equations in $d$ variables with coefficients in $\lambda$. If $\{f_\lambda\}$ has a solution over any $K$-algebra $R$, then there is a solution over $\overline{K}$.*

*Proof.* First, we observe that if there is a solution in some ring $R$, there is a solution in an algebraically closed field containing $K$. Indeed, given a $R$ in which there is a solution, we can quotient out by a maximal ideal to get a solution in a field, and include into the algebraic closure to get a solution in an algebraically closed field.

Now, if there is no solution over $\overline{K}$, then $1 \in (\{f_\lambda\})$, considered as an (improper) ideal in $\overline{K}[\underline{x}]$. Any other algebraically closed field $L$ containing $K$ contains (a $K$-algebra isomorphic copy of) $\overline{K}$, so we can express 1 as a $L[\underline{x}]$-linear combination of the $f$'s (by the same polynomials). Thus, there is no solution over $L$ either. By contraposition, a solution over some algebraically closed field implies a solution over $\overline{K}$. □

To attack the main question, we will need an observation on inequations. Observe that, if $f(\underline{x})$ is a polynomial, $f(\underline{a}) \neq 0$ if and only if there is a solution $y = b \in K$ to $yf(\underline{a}) - 1 = 0$. In particular, a system of polynomial equations and inequations

$$f_1(\underline{x}) = 0, \ldots, f_m(\underline{x}) = 0, g_1(\underline{x}) \neq 0, \ldots, g_n(\underline{x}) \neq 0$$

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

$$f_1(\underline{x}) = 0, \ldots, f_m(\underline{x}) = 0, y_1 g_1(\underline{x}) - 1 = 0, \ldots, y_n g_n(\underline{x}) - 1 = 0$$

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

$$f_1(\underline{x}) = 0, \dots, f_m(\underline{x}) = 0, yg_1(\underline{x}) \cdots g_n(\underline{x}) - 1 = 0.$$

**Theorem 2.14** (Strong Nullstellensatz)**.** *Let $K$ be an algebraically closed field, and $R = K[x_1, \dots, x_d]$ be a polynomial ring. Let $I \subseteq R$ be an ideal. The polynomial $f$ vanishes on $Z_K(I)$ if and only if $f^n \in I$ for some $n \in \mathbb{N}$.*

*Proof.* If $f^n \in I$, and $\underline{a} \in Z_K(I)$, then $f(\underline{a}) \in K$ satisfies $f(\underline{a})^n = 0 \in K$. Since $K$ is a field, $f(\underline{a}) = 0$. Thus, $f \in Z_K(I)$ as well.

Suppose that $f(\underline{x})$ vanishes along $Z_K(I)$. By the discussion above, this implies that $Z_K(I + (yf - 1)) = \varnothing$, in a polynomial ring in one more variable. By the Medium Nullstellensatz, we see that $1 \in IR[y] + (yf - 1)$. 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 (on the LHS) $f^n$ as a polynomial combination of the $g$'s (on the RHS). □

**Definition 2.15.** *The* radical *of an ideal $I$ is the ideal $\sqrt{I} := \{f \in R \mid \exists n : f^n \in I\}$. An ideal is a* radical ideal *if $I = \sqrt{I}$.*

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

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

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

In this terminology, the Strong Nullstellensatz asserts that, if $K = \overline{K}$, $f$ vanishes along $Z_K(I)$ if and only if $f \in \sqrt{I}$.

**Lemma 2.16.** *Let $R$ be a ring, and $I$ be an ideal. The quotient $R/I$ is reduced (i.e., has no nonzero nilpotent elements) if and only if $I$ is radical.*

*Proof.* The class of $f$ mod $I$ is a nonzero nilpotent if and only if $f \notin I$ but $f^n \in I$ for some $n$. Thus, the existence of nonzero nilpotents if equivalent to nonreducedness of $I$. □

**Corollary 2.17.** *Let $K$ be an algebraically closed field, and $R = K[x_1, \dots, x_d]$ a polynomial ring. There is an order-reversing bijection between the collection of subvarieties of $K^d$ and the collection of radical ideals of $R$:*

$$\{\textit{subvarieties of } K^d\} \qquad \leftrightarrow \qquad \{\textit{radical ideals } I \subseteq R\}.$$

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

*Proof.* The map ← is given by $Z_K(I) \overset{\mathcal{Z}}{\longleftarrow} I$, and the map → is given by $X \xrightarrow{\mathcal{I}} \{f \in R \mid f|_X \equiv 0\}$. We check that $\mathcal{I}$ and $\mathcal{Z}$ are inverse operations on the specified sets; namely that $\mathcal{Z}(\mathcal{I}(X)) = X$ for any subvariety $X$, and $\mathcal{I}(\mathcal{Z}(J)) = J$ for any radical ideal $J$.

Given a set $X = Z_K(\{f_\lambda\})$, we can write $X = Z_K(J)$, where $J = (\{f_\lambda\})$. By the Strong Nullstellensatz, $\mathcal{I}(X) = \sqrt{J}$. We claim that $Z_K(\sqrt{J}) = Z_K(J)$. The containment $\subseteq$ is clear. For the other, if $\underline{a} \notin Z_K(\sqrt{J})$, then there is some $f$ such that $f^n \in J$, and $f(\underline{a}) \neq 0$ in $K$; we then have $f^n(\underline{a}) \neq 0$ in $K$ as well, so that $\underline{a} \notin Z_K(J)$. This shows the claim. Now, $\mathcal{Z}(\mathcal{I}(X)) = \mathcal{Z}(\sqrt{J}) = Z_K(\sqrt{J}) = Z_K(J) = X$.

On the other hand, the Strong Nullstellensatz says that $\mathcal{I}(\mathcal{Z}(J)) = \sqrt{J}$ for any ideal $J$, hence $\mathcal{I}(\mathcal{Z}(J)) = J$ for a radical ideal $J$. □

**Definition 2.18.** *Let $K$ be an algebraically closed field, and $X = Z_K(I) \subseteq K^d$ be a subvariety of $K^d$. The* coordinate ring *of $X$ is the ring $K[X] := K[x_1, \dots, x_d]/\sqrt{I}$.*

Since $K[X]$ is obtained from the polynomial ring on the ambient $K^d$ 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 zeroset $X$, and conversely.

Rings of invariants of finite groups acting on polynomial rings (in finitely many variables) by $K$-algebra automorphisms are domains (since they are subrings of polynomial rings) that are finitely generated $K$-algebras. Hence, if $K = \overline{K}$, they are coordinate rings of affine varieties. We can use the Nullstellensatz to try to find expressions as quotients of polynomial rings, and as coordinate rings.

**Example 2.19.** Let $K$ be an algebraically closed field, and $R = K[x^2, xy, y^2] \subseteq K[x, y]$.

We claim that $R \cong \frac{K[u,v,w]}{(v^2-uw)}$, via $u \mapsto x^2, \mapsto yx, w \mapsto y^2$. Let $I$ denote the kernel of the map from $K[u, v, w] \to K[x^2, xy, y^2]$ given as such: $I = \{g(u, v, w) \mid g(x^2, xy, y^2) = 0\}$. We claim that $Z_K(I) = Z_K(v^2 - uw)$. Since $v^2 - uw \in I$, we get $Z_K(I) \subseteq Z_K(v^2 - uw)$. For the other containment, let $(a, b, c) \in Z_K(v^2 - uw)$; i.e., elements of $K$ with $b^2 = ac$. We can write $a = \alpha^2, c = \gamma^2$, and $b = \alpha\gamma$ in $K$ for some choice of square roots of $a$ and $c$. Then, if $f \in I$, $f(x^2, xy, y^2)$ is the zero function, so $f(a, b, c) = f(\alpha^2, \alpha\gamma, \gamma^2)$ is an evaluation of the polynomial $f(x^2, xy, y^2)$, hence is zero. This shows that $Z_K(v^2 - uw) \subseteq Z_K(I)$ and the sets are equal.

By the Strong Nullstellensatz, $I$ which must be radical since the quotient ring is reduced, must be $\sqrt{(v^2 - uw)}$. You can check that this polynomial is irreducible in $K[u, v, w]$, hence generates a prime ideal, which is thus a radical ideal. The claim is shown.

**Example 2.20.** Let $K$ be an algebraically closed field, and $R = K[x^3, x^2y, xy^2, y^3]$. This is the third Veronese subring of $K[x, y]$.

We can play roughly the same game as above to conclude that the kernel of the map $\varphi : K[t, u, v, w] \to R$ given by $t \mapsto x^3, u \mapsto x^2y, v \mapsto xy^2, w \mapsto y^3$ is *the radical of* $(u^2 - tv, v^2 - uw, tw - uv)$. Namely, these are all in the kernel, and we can show that if any point $(a, b, c, d)$ that satisfies these three equations can be written in the form $(\alpha^3, \alpha^2\beta, \alpha\beta^2, \beta^3)$ for some $\alpha, \beta \in K$; check this! It follows that

$$\begin{aligned} Z_K(u^2 - tv, v^2 - uw, tw - uv) &\subseteq \{(\alpha^3, \alpha^2\beta, \alpha\beta^2, \beta^3) \mid (\alpha, \beta) \in K^2\} \\ &\subseteq Z_K(\ker(\varphi)) \subseteq Z_K(u^2 - tv, v^2 - uw, tw - uv), \end{aligned}$$

and the claim follows by the Nullstellensatz. Now it is a bit trickier to check that this ideal is radical; i.e., that we have found all of the equations. We should have two or three good tools for this by the end of the course.

We have seen that the set of maximal ideals in a finitely generated algebra over an algebraically closed field has a natural geometric interpretation. We can extend this to arbitrary fields.

**Proposition 2.21.** *Let $K$ be an arbitrary field, and $S = K[x_1, \dots, x_n]$.*

1. *Every maximal ideal of $S$ can be realized as $\mathfrak{m}_{\underline{a}} := \{f \in S \mid f(\underline{a}) = 0\}$ for some $\underline{a} \in \overline{K}^n$.*
2. *The map $\underline{a} \mapsto \mathfrak{m}_{\underline{a}}$ descends to a bijection $\overline{K}^n / \operatorname{Aut}(\overline{K}/K) \leftrightarrow \{$maximal ideals of $S\}$.*

*Proof.* If $\mathfrak{m}$ is a maximal ideal of $S$, then $S/\mathfrak{m}$ is a finite extension of $K$ by the Weak Nullstellensatz. Thus, $S/\mathfrak{m}$ embeds into $\overline{K}$, so $\mathfrak{m}$ is the kernel of a $K$-algebra map $\varphi$ from $S$ to $\overline{K}$. Thus, any such $\mathfrak{m}$ is given as $\mathfrak{m}_{\underline{a}}$, where $\varphi(x_i) = a_i$ for all $i$.

To see this map is well-defined, suppose that $g \cdot \underline{a} = \underline{b}$; i.e., $g(a_i) = b_i$ for all $i$. The group $\operatorname{Aut}(\overline{K}/K)$ acts trivially on $K$, so $0 = g(0) = g \cdot f(\underline{a}) = f(g \cdot \underline{a}) = f(\underline{b})$.

To see it is injective, suppose that $\mathfrak{m}_{\underline{a}} = \mathfrak{m}_{\underline{b}}$. Then, the map $\varphi : S \to S/\mathfrak{m}_{\underline{b}}$ given by $\varphi(x_i) = b_i$ descends to a $K$-algebra isomorphism $K(a_1, \dots, a_n) \cong K(b_1, \dots, b_n)$ sending $a_i \mapsto b_i$. This extends to a an automorphism of $\overline{K}$ over $K$ that sends $a_i \mapsto b_i$, as required. □

## 2.3 The prime spectrum of a ring

We have seen that the set of maximal ideals in a (reduced) finitely generated algebra over an algebraically closed field is bijective to a subset of $K^n$ for some $n$.

We can carry more of the geometric information on this set of maximal ideals by giving it a topology. The *Zariski topology* on $K^n$ is the topology whose closed sets are zero sets of polynomial equations, equivalently, $Z_K(I)$ for the ideals $I \subseteq K[x_1, \dots, x_n]$. In light of the Nullstellensatz, we can generalize this construction to all rings.

The *maximal spectrum* of a ring $R$, denoted $\operatorname{Max}(R)$, is the set of maximal ideals of $R$ endowed with the topology with closed sets given by $V_{\operatorname{Max}}(I) := \{\mathfrak{m} \in \operatorname{Max}(R) \mid \mathfrak{m} \supseteq I\}$ as $I$ varies. By the Nullstellensatz, for polynomial rings $S$ over an algebraically closed field $K$, this space $\operatorname{Max}(S)$ has a natural homeomorphism to $K^n$ with its Zariski topology, and for an ideal $I$ and $S$ as above, $\operatorname{Max}(S/I)$ has a natural homeomorphism to $Z_K(I) \subseteq K^n$ with the subspace topology coming from the Zariski topology.

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

**Definition 2.22.** *Let $R$ be a ring. The* prime spectrum, *or* spectrum *of $R$ is the set of prime ideals of $R$, denoted* $\operatorname{Spec}(R)$. *It is naturally a poset, partially ordered by inclusion. We also endow it with the topology with closed sets $V(I) := \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \supseteq I\}$ for ideals $I \subseteq R$.*

Note that $\operatorname{Max}(R)$ is a subspace of $\operatorname{Spec}(R)$.

**Proposition 2.23.** *Let $R$ be a ring, and $I_\lambda, J$ be ideals.*

1. *If $I \subseteq J$, then $V(J) \subseteq V(I)$.*
2. *$V(I) \cup V(J) = V(I \cap J) = V(IJ)$*

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

4. Spec$(R)$ *has a basis given by open sets of the form* $D(f) := \operatorname{Spec}(R) \smallsetminus V(f)$.

5. *If $R$ is Noetherian,* Spec$(R)$ *is quasicompact.*

*Proof.* 1. Clear.

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

3. Clear.

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

5. Given a sequence of ideals $I_\lambda$, by the ascending chain condition, their sum $\sum_\lambda I_\lambda$ can be realized as a sum over finitely many indices: $\sum_\lambda I_\lambda = I_{\lambda_1} + \cdots + I_{\lambda_t}$. Thus, if we have a family of closed sets with empty intersection,

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

so some finite subintersection is empty. □

We will see soon that an analogue to the Corollary 2.17 holds for all rings with Spec and $V$: there is an order reversing bijection between closed subsets of $V$ and radical ideals in $R$.

**Definition 2.24** (Induced map on Spec)**.** *Given a homomorphism of rings $\varphi : R \to S$, we obtain a map on spectra $\varphi^* : \operatorname{Spec}(S) \to \operatorname{Spec}(R)$ given by $\varphi^*(\mathfrak{p}) = \varphi^{-1}(\mathfrak{p})$.*

The key point is that the preimage of a prime ideal is also prime. If $\varphi$ is injective, we often write $\varphi^*(p)$ as $\mathfrak{p} \cap R$.

We now want to understand what the induced map on Spec is for algebras that are finitely generated over fields.

We prepare with some lemmas that we will use later.

**Lemma 2.25.** *Let $R \subseteq S$ be an integral extension. Then every nonzero element of $S$ has a nonzero $S$-multiple in $R$.*

*Proof.* Let $s \in S$. Take an integral equation of dependence for $s$ over $R$:

$$s^n + r_1 s^{n-1} + \cdots + r_n = 0.$$

WLOG, $r_n \neq 0$, otherwise we could take an integral equation of lower degree. Rewriting, we have $r_n = s(-s^{n-1} - r_1 s^{n-1} - \cdots - r_{n-1}) \in R$, as required. □

**Proposition 2.26.** *Let $K \subseteq R$ be an integral extension, with $K$ a field, and $R$ a domain. Then, $R$ is a field.*

*Proof.* Given $r \in R \smallsetminus 0$, there is some $s \in R$ such that $k = rs \in K \smallsetminus 0$. Then $sk^{-1}$ is an inverse for $r$. □

**Proposition 2.27.** *Let $K$ be a field, and $\varphi : R \to S$ be a map of finitely generated $K$-algebras. Then, for any maximal ideal $\mathfrak{n}$ of $S$, $\mathfrak{m} = \mathfrak{n} \cap R$ is a maximal ideal of $R$.*

*Proof.* The map $K \subseteq S/\mathfrak{n}$ is module-finite, hence the intermediate extension $K \subseteq R/(\mathfrak{n} \cap R)$ is module-finite as well. Since $R/(\mathfrak{n} \cap R) \subseteq S/\mathfrak{n}$, it is a domain. By the previous lemma, $R/(\mathfrak{n} \cap R)$ is a field. □

**Proposition 2.28.** *Let $K$ be an algebraically closed field. Let $R = K[x_1, \dots, x_c]/I$ and $S = [y_1, \dots, y_d]/J$. Let $\varphi : R \to S$ be a $K$-algebra homomorphism, which is necessarily of the form $\varphi(x_i) = f_i(\underline{y})$ for some polynomials $f_i$. For $\underline{a} = (a_1, \dots, a_d) \in Z_K(J) \subseteq K^d$, set $\phi^*(\underline{a}) = (f_1(\underline{a}), \dots, f_c(\underline{a})) \in Z_K(I)$. The map $\varphi^*$ sends $\mathfrak{m}_{\underline{a}}$ to $\mathfrak{m}_{\phi^*(\underline{a})}$.*

## 2.4 Projective varieties and Proj

For graded rings and homogeneous ideals, there are closely related geometric objects to the ones we have just discussed that are much better to deal with in many geometric situations.

Recall, for a field $K$, $n$-dimensional *projective space* over $K$ is the set

$$\mathbb{P}^n_K = (\{(x_0, \dots, x_n) \in K^{n+1}\} \smallsetminus \{(0, \dots, 0)\}) / \sim$$

where $\sim$ is the equivalence relation $(x_0, \dots, x_n) \sim (\lambda x_0, \dots, \lambda x_n)$ for all $\lambda \in K \smallsetminus 0$.

**Lemma 2.29.** *Let $K$ be an algebraically closed field, and $R = K[x_0, \dots, x_n]$ be a polynomial ring with the standard grading. Let $I \subseteq R$ be a homogeneous ideal. If $\underline{a} \in Z_K(I)$, then $\lambda\underline{a} \in Z_K(I)$ for all $\lambda \in K$. Thus, $Z_K(I)$ determines a well-defined subset of $\mathbb{P}^n_K$.*

*Proof.* Let $\underline{a} \in Z_K(I)$, $\lambda \in K$, and $f \in I$. Since $I$ is homogeneous, we know that the homogeneous components of $f$ lie in $I$. Write $f = f_{d_1} + \cdots + f_{d_t}$ as a sum of homogeneous forms of degrees $d_1, \dots, d_t$, respectively. By homogeneity, $f_{d_i}(\lambda\underline{a}) = \lambda^{d_i} f_{d_i}(\underline{a}) = 0$ for all $i$. Thus, $f(\lambda\underline{a}) = 0$.

Since any representative for the same point in $\mathbb{P}^n_K$ simultaneously passes or fails the membership test for $Z_K(I)$, this determines a well-defined subset. □

In the context of the previous lemma, we write $\overline{Z}_K(I) \subseteq \mathbb{P}^n_K$ for the subset we obtained. We call a subset of the form $\overline{Z}_K(I)$ a *subvariety* of $\mathbb{P}^n_K$.

Along the same lines as Corollary 2.17, we obtain:

**Theorem 2.30.** *Let $K$ be an algebraically closed field, and $R = K[x_0, \dots, x_n]$ be a polynomial ring with the standard grading. There is an order-reversing bijection between the collection of subvarieties of $\mathbb{P}^n$ and the collection of homogeneous radical ideals of $R$, other than the homogeneous maximal ideal:*

$$\{\textit{subvarieties of } \mathbb{P}^n_K\} \quad \leftrightarrow \quad \{\textit{homogeneous radical ideals } I \subseteq R \mid I \subsetneq (x_0, \dots, x_n)\}.$$

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

As with $Z$ and Spec, it is quite useful to extend the notion $\overline{Z}$ to greater generality.

**Definition 2.31** (Proj). *Let $R$ be an $\mathbb{N}$-graded ring. The* projective spectrum *or simply* "Proj" *of $R$ is the set of homogeneous prime ideals of $R$ that do not contain $R_+ = \bigoplus_{n>0} R_n$. The set* Proj$(R)$ *is naturally a poset partially ordered by inclusion. We endow* Proj$(R)$ *with a topology in which the closed sets are $V(I) := \{\mathfrak{p} \in \mathrm{Proj}(R) \mid \mathfrak{p} \supseteq I\}$ for $I$ homogeneous.*

Given a degree-preserving homomorphism of $\mathbb{N}$-graded rings $\varphi : R \to S$, we do not always obtain a map on projective spectra $\varphi^* : \operatorname{Proj}(S) \to \operatorname{Proj}(R)$ given by the rule analogous to that for maps of Spec: $\varphi^*(\mathfrak{p}) := \varphi^{-1}(\mathfrak{p})$. The problem is that one might have $R_+ \subseteq \varphi^{-1}(\mathfrak{p})$ but $S_+ \not\subseteq \mathfrak{p}$. However, this map makes sense sometimes; we leave further discussion of maps of projective varieties to 631.

# Chapter 3

# Localization

We made some progress on the question:

**Question 3.1.** To what extent is a system of polynomial equations determined by its solution set?

From last time, we broke this into two pieces: for $f_1, \dots, f_t \in K[\underline{x}]$, with $K = \overline{K}$

$$\begin{array}{ccccc} \text{system of equations} & \rightsquigarrow & \text{ideal} & \rightsquigarrow & \text{solution set} \\ f_1(\underline{x}) = 0, \dots, f_t(\underline{x}) = 0 & \mapsto & I = (f_1, \dots, f_t) & \mapsto & Z(I), \end{array}$$

and showed that $Z(I) = Z(J)$ if and only if $\sqrt{I} = \sqrt{J}$. Now, we wish to address the relationship between an ideal and a generating set. We can always do stupid things like repeat generators, or throw in $R$-linear combinations of our generators to the generating set. We can ask though: when does an ideal have a minimal generating set, and to what extent is such a generating set unique? We will find two positive answers: there are essentially unique generating sets for homogeneous ideals in graded rings, and there is some uniqueness for generating sets for ideals *locally*.

## 3.1 Localization of rings and modules

**Definition 3.2** (Multiplicative set)**.** *A* multiplicative set *in a ring $R$ is a subset $W \subseteq R$ such that $1 \in W$ and $v, w \in W \Rightarrow vw \in W$.*

Our three most important classes of examples are the first three below.

**Example 3.3.** 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 $\mathfrak{p} \subseteq R$ is a prime ideal, the set $W = R \smallsetminus \mathfrak{p}$ is multiplicative: this is an immediate translation of the definition.

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

4. An arbitrary intersection of multiplicatively closed subsets is multiplicatively closed. In particular, for any family of primes $\{\mathfrak{p}_\lambda\}$, the set $R \smallsetminus \bigcup_\lambda \mathfrak{p}_\lambda$ is multiplicatively closed.

**Definition 3.4** (Localization of a ring)**.** *Let $R$ be a ring, and $W$ be a multiplicative set. The* localization *of $R$ at $W$ is the ring*

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

*where $\sim$ is the equivalence relation $\dfrac{r}{w} \sim \dfrac{r'}{w'}$ if $\exists u \in W : u(rw' - r'w) = 0$. The operations are given by $\frac{r}{v} + \frac{s}{w} = \frac{rw+sv}{vw}$ and $\frac{r}{v}\frac{s}{w} = \frac{rs}{vw}$.*

The condition $rw' - r'w = 0$ (with no $u$) corresponds to the obvious $\frac{r}{w} - \frac{r'}{w'} = \frac{0}{ww'}$. The business about the $u$ arises from the fact that if $ur = 0$ for some $u \in W$, then one must have $\frac{r}{1} = \frac{ur}{u} = \frac{0}{u} = 0$ as well. The single statement for the equivalence relation above is just the consequence of these two rules. We will return to this idea shortly.

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

**Definition 3.5.** *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*

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

*where $\sim$ is the equivalence relation $\dfrac{m}{w} \sim \dfrac{m'}{w'}$ if $\exists u \in W : u(mw' - m'w) = 0$. The operations are given by $\frac{m}{v} + \frac{n}{w} = \frac{mw+nv}{vw}$ and $\frac{r}{v}\frac{m}{w} = \frac{rm}{vw}$.*

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

To understand localizations of rings and modules, we will want to understand better how they are built from $R$. The following definition will be useful.

**Definition 3.6.** *Let $M$ be an $R$-module, and $W$ a multiplicative set. The $W$-*torsion *submodule of $M$ is*

$$M^{W-\text{tors}} := \{m \in M \mid \exists w \in W : wm = 0\}.$$

*It is a submodule of $M$. As a special case, we can take $M = R$, and then the $R^{W-\text{tors}}$ is an ideal.*

**Lemma 3.7.** *Let $M$ be an $R$-module, and $W$ a multiplicative set. The class*

$$\frac{m}{w} \in W^{-1}M \text{ is zero} \iff m \in M^{W-\text{tors}} \iff \operatorname{ann}_R(m) \cap W \neq \varnothing.$$

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

*Proof.* For the first equivalence, we compute: $\frac{m}{w} = \frac{0}{1}$ in $W^{-1}M$ if and only if $v \in W$ such that $0 = v(1m - 0w) = vm$. The second equivalence just comes from the definition of the annihilator. □

We need one more technical lemma.

**Lemma 3.8.** *Let $N \subseteq M$ be $R$-modules, and $W$ a multiplicative set. Then $W^{-1}N \subseteq W^{-1}M$, and $W^{-1}(M/N) \cong \frac{W^{-1}M}{W^{-1}N}$.*

*Proof.* The condition for $\frac{n}{w} \in W^{-1}N$ to be zero in $W^{-1}M$ is the same as the condition to be zero in $W^{-1}N$, so $W^{-1}N \subseteq W^{-1}M$ is an inclusion. Now, the map $W^{-1}M \to W^{-1}(M/N)$ sending $\frac{m}{w} \mapsto \frac{\bar{m}}{w}$ is certainly surjective, and its kernel consists of elements $\frac{m}{w}$ such that $\bar{m}$ is $W$-torsion: $vm \in N$ for some $v$. Such an element is of the form $\frac{1}{v}\frac{mv}{w}$, and hence lies in $W^{-1}N$. □

**Proposition 3.9.** *Let $M$ be an $R$-module, and $W$ a multiplicative set. Set $\overline{M} = M/M^{W-\text{tors}}$. Then,*

$$W^{-1}M = \bigcup_{w\in W} \frac{1}{w}\overline{M},$$

*where each $\frac{1}{w}\overline{M}$ is an isomorphic copy of $\overline{M}$ as an $R$-module.*

*Proof.* First, we have $W^{-1}\overline{M} \cong W^{-1}(M/M^{W-\text{tors}}) \cong \frac{W^{-1}M}{W^{-1}(M^{W-\text{tors}})} \cong W^{-1}M$, so we can replace $M$ by the $W$-torsion free module $\overline{M}$. It is clear that every element of $W^{-1}M$ has the form on the RHS. The map $\overline{M} \to \frac{1}{w}\overline{M}$ sending $m \mapsto \frac{m}{w}$ is clearly $R$-linear, and is injective by the $W$-torsion free assumption. □

**Example 3.10** (Most important localizations)**.** Let $R$ be a ring.

1. For $f \in R$ and $W = \{1, f, f^2, f^3, \dots\}$, we usually write $R_f$ for $W^{-1}R$. If $f$ is a nonzerodivisor, so are all of its powers, and the condition on $u \in W$ above is vacuous other than $rw' - r'w = 0$. That is, if $R$ is a nonzerodivisor, $R_f \cong R[x]/(fx-1)$. Otherwise, write $\overline{R} = R/\operatorname{ann}_R(f)$. In general, $R_f \cong \overline{R}[x]/(fx-1)$.

2. For $\mathfrak{p} \subset R$ prime, we generally write $R_\mathfrak{p}$ for $(R \smallsetminus \mathfrak{p})^{-1}R$.

3. 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 $R$.

In $W^{-1}R$, the elements of $W$ become units (the inverses are the $\frac{1}{w}$'s, of course). The localization in universal with respect to this property: if $S$ is a ring and $\alpha : R \to S$ is such that $\alpha(w)$ is a unit in $S$ for each $w \in W$, then there is a factorization of $\alpha$:

$$\begin{tikzcd} & W^{-1}R \arrow[dr, "\beta"] & \\ R \arrow[ur, "\varphi"] \arrow[rr, "\alpha"] & & S. \end{tikzcd}$$

We want to collect one more lemma for later.

**Lemma 3.11.** *Let $M$ be a module, and $N_1, \dots, N_t$ be a finite collection of submodules. Let $W$ be a multiplcative 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 "$\subseteq$" is clear. An element of the RHS is of the form $\frac{n_1}{w_1} = \cdots = \frac{n_t}{w_t}$; we can find a common denominator to realize this in the LHS. □

## 3.2 Primes in localizations

We now wish to relate the ideals and prime ideals in localizations to those in the original ring. We need a definition:

**Definition 3.12.** *Let $R$ be a ring, $W$ be a multiplicative set, and $I$ be an ideal. The* saturation *of $I$ with respect to $W$ is*

$$I^{W-\text{sat}} := \{r \in R \mid \exists w \in W : wr \in I\}.$$

*Observe that $r \in I^{W-\text{sat}}$ if and only if $\bar{r} \in (R/I)^{W-\text{tors}}$.*

**Lemma 3.13** (Expansion and contraction to localizations). *Let $R$ be a ring and $W$ be a multiplicative set.*

1. *If $I \subset R$ is an ideal, $IW^{-1}R \cap R = I^{W-\text{sat}}$.*
2. *If $J \subseteq W^{-1}R$ is a (possibly improper) ideal, $(J \cap R)W^{-1}R = J$.*

*Proof.*

1. Given an element in the LHS, we can write it as $\frac{a}{w} = \frac{r}{1}$ with $a \in I$, $w \in W$, $r \in R$. Then, there is some $v \in W$ with $0 = v(a - wr) = va - vwr$ in $R$. Since $va \in I$, some $u = vw \in W$ multiplies $r$ into $I$, so $r \in I^{W-\text{sat}}$. Conversely, if $r \in I^{W-\text{sat}} \subseteq R$, take $wr = a$ with $a \in I$, $w \in W$. We then have $\frac{r}{1} = \frac{a}{w} = a\frac{1}{w} \in IW^{-1}R$, as required.
2. The containment "$\subseteq$" is clear. For the other, take $\frac{b}{w} \in J$; we also have its multiple $\frac{b}{1} \in J \cap R$. Then, $\frac{b}{w} = \frac{1}{w}\frac{b}{1} \in (J \cap R)W^{-1}R$, as required. □

**Remark 3.14.** $IW^{-1}R$ is a proper ideal if and only if $I \cap W = \varnothing$. Indeed, if $\frac{1}{1} = \frac{a}{w}$ with $a \in I, w \in W$, then there is some $v$ with $v(w - a) = 0$, so $va = vw \in W \cap I$. The converse is equally easy.

**Proposition 3.15.** *Let $R$ be a ring, and $W$ be a multiplicatively closed subset. The maps*

$$\begin{array}{lcl} \{\textit{(possibly improper) ideals of } R\} & & \{\textit{(possibly improper) ideals of } W^{-1}R\} \\ I & \mapsto & I(W^{-1}R) \\ J \cap R & \leftarrow\!\shortmid & J \end{array}$$

*induce order-preserving bijections*

$$\begin{array}{lcl} \{\textit{ideals of } R \textit{ saturated with respect to } W\} & \leftrightarrow & \{\textit{ideals of } W^{-1}R\} \\ \{\textit{prime ideals of } R \textit{ such that } W \cap R = \varnothing\} & \leftrightarrow & \{\textit{prime ideals of } W^{-1}R\} \end{array}$$

*Thus, the map $\varphi^* : \operatorname{Spec}(W^{-1}R) \to \operatorname{Spec}(R)$ is the inclusion map of the subspace consisting of primes disjoint from $W$.*

*Proof.* The expansion map sends ideals of $R$ saturated with respect to $W$ to ideals of $W^{-1}R$, since a saturated ideal of $R$ must not intersect $W$. The reverse map always sends ideals to ideals. Then, the fact these maps are mutually inverse in these sets follows from the last lemma.

If $\mathfrak{p} \subset R$ is prime, we want to show that $\mathfrak{p}(W^{-1}R)$ is prime. Suppose that $(a/w')(b/w'') = (p/w)$ for $p \in \mathfrak{p}$, $a, b \in R$, $w', w'' \in W$. Then, $vwab = vw'w''p \in \mathfrak{p}$ for some $v \in W$. Since $v, w \notin \mathfrak{p}$, $ab \in \mathfrak{p}$, so $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. But this implies that $a/w'$ or $b/w'' \in \mathfrak{p}(W^{-1}R)$. The reverse map always sends primes to primes, and since the ideal is saturated and proper, must not intersect $W$. Thus, the bijection sends primes to primes. □

**Example 3.16.**

1. $\operatorname{Spec}(R_f)$ is bijective to the set of primes that do not contain $f$.
2. $\operatorname{Spec}(R_\mathfrak{p})$ is bijective to the set of primes that do not intersect $R \smallsetminus \mathfrak{p}$; i.e., the primes that are *contained in* $\mathfrak{p}$. This corresponds to a *downward interval* in the poset $\operatorname{Spec}(R)$; this is an upside-down analogue of $V(\mathfrak{p})$.

Suppose that $R$ is the coordinate ring of a variety over an algebraically closed field $K$. Given $f \in R$, the complement of the set of primes that contain $f$ is an open set $D(f)$, and these open sets form a basis. We interpret $R_f$ as the coordinate ring of $D(f)$.

Now, let $\mathfrak{m} = \mathfrak{m}_{\underline{a}}$ be a maximal ideal in $R$. The set of primes that contain corresponds to those subvarieties $Z_K$ that contain $\underline{a}$. Thus, $\operatorname{Spec}(R_\mathfrak{m})$ detects the geometric behavior near $\underline{a}$.

**Example 3.17.** Let $R = \dfrac{\mathbb{C}[x,y]}{(xy)}$.

In the ring $R_{(x,y)}$, everything that is not in the ideal $(x,y)$ becomes a unit, in particular, the elements $x-\alpha$ and $y-\alpha$ for $\alpha \neq 0$. Thus, the only maximal ideal of $R$ not containing a unit in the localization is $(x,y)$. The spectrum of this local ring is $\{(x),(y),(x,y)\}$, which are the primes of $R$ contained in $(x,y)$.

In the ring $R_{(x,y-1)}$, everything that is not in the ideal $(x,y-1)$ becomes a unit. Since $y \in R \smallsetminus (x,y-1)$, and $y$ kills $x$, $x$ goes to zero in the localization. We then have $R_{(x,y-1)} \cong \mathbb{C}[x,y]_{(x,y-1)}/(xy,x) \cong \mathbb{C}[y]_{(y-1)}$. This is the subring of $\mathbb{C}(y)$ consisting of polynomials whose denominators are *not* divisible by $y-1$. Since everything not divisible by $y-1$ is a unit here, this ring has a unique maximal ideal $(y-1)$; the spectrum of this is $\{(0),(y-1)\}$, which are the images of $\{(x),(x,y-1)\}$.

**Definition 3.18** (Fiber of a map over a point)**.** *Let $\phi : R \to S$ be a ring homomorphism, and $\mathfrak{p} \in \operatorname{Spec}(R)$. We define the* fiber *of $\phi$ over $\mathfrak{p}$ to the the ring $\kappa_\phi(\mathfrak{p}) := (\phi(R \smallsetminus \mathfrak{p}))^{-1}(S/\phi(\mathfrak{p})S)$.*

**Proposition 3.19.** *The map $S \to \kappa_\phi(\mathfrak{p})$ induces a homeomorphism between $\operatorname{Spec}(\kappa_\phi(\mathfrak{p}))$ and the subspace $(\phi^*)^{-1}(\mathfrak{p}) = \{\mathfrak{q} \in \operatorname{Spec}(S) \mid \phi^*(\mathfrak{q}) = \mathfrak{p}\}$.*

*Proof.* We factor the map as $S \to S/\phi(\mathfrak{p})S \to (\phi(R \smallsetminus \mathfrak{p}))^{-1}(S/\phi(\mathfrak{p})S)$. We have that

$$\operatorname{Spec}(S/\phi(\mathfrak{p})) = \{\bar{\mathfrak{q}} \mid \mathfrak{q} \in \operatorname{Spec}(S), \mathfrak{q} \supseteq \phi(\mathfrak{p})\} = \{\bar{\mathfrak{q}} \mid \mathfrak{q} \in \operatorname{Spec}(S), \phi^{-1}(\mathfrak{q}) \supseteq \mathfrak{p}\},$$

and the induced map on spec to $\operatorname{Spec}(S)$ is the inclusion map. We also have

$$\begin{aligned}\operatorname{Spec}((\phi(R \smallsetminus \mathfrak{p}))^{-1}(S/\phi(\mathfrak{p})S)) &= \{(\phi(R \smallsetminus \mathfrak{p}))^{-1}\mathfrak{a} \mid \mathfrak{a} \in \operatorname{Spec}(S/\phi(\mathfrak{p})S), \mathfrak{a} \cap \phi(R \smallsetminus \mathfrak{p}) = \varnothing\} \\ &= \{(\phi(R \smallsetminus \mathfrak{p}))^{-1}\mathfrak{a} \mid \mathfrak{a} \in \operatorname{Spec}(S/\phi(\mathfrak{p})S), \phi^{-1}(\mathfrak{a}) \subseteq \mathfrak{p}\},\end{aligned}$$

and the induced map on Spec it the inclusion map again. Put together, we obtain the statement. □

**Example 3.20.** Let $R = K[x,y] \to S = \frac{K[x,y,u,v]}{(xu-yv)}$. We want to understand which primes in $S$ map to $(x) \in \operatorname{Spec}(R)$. We can do this directly by considering the primes in $S$ that contain $x$, and determining which of those intersect to $(x)$. Primes in $S$ containing $(x)$ correspond to primes in $S/(x) \cong K[y,u,v]/(yv)$. Any prime in this ring contains $y$ or $v$, so the primes in $S$ we want contain $(x,y)$ or $(x,v)$. If a prime contains $y$, it contracts to something larger, so we must discard the primes containing $(x,y)$. Now, we want to determine which primes containing $(x,v)$ contract to $(x)$. This consists of the primes containing $(x,v)$ that do not any irreducible polynomial involving only $y$. We can identify this with the set of primes in localization of the ring $S/(x,v) \cong K[y,u]$ at the multiplicative set containing all nonzero polynomials involving just $y$, which is $K(y)[u]$.

Let's compute the fiber ring for comparison. We have

$$(K[x,y] \smallsetminus (x))^{-1}(S/(x)S) \cong (\overline{K[x,y] \smallsetminus (x)})^{-1}\frac{K[y,u,v]}{(yv)} \cong (K[y] \smallsetminus (0))^{-1}\frac{K[y,u,v]}{(yv)}.$$

Now, $v$ is a torsion with respect to this multiplicative set, so we quotient out by $v$, and then adjoin inverses of every nonzero polynomial in $y$:

$$\kappa_\phi((x)) \cong K(y)[u].$$

We now return to give a general analogue to the Strong Nullstellensatz. It is worthwhile to compare the statement and the proof to that of the original Strong Nullstellensatz.

**Proposition 3.21** ("$V$satz"). *Let $R$ be a ring, and $I$ be an ideal. For $f \in R$,*

$$f \in \mathfrak{p} \text{ for all } \mathfrak{p} \in V(I) \Longleftrightarrow f \in \sqrt{I}.$$

*That is, $\bigcap_{\mathfrak{p} \in V(I)} \mathfrak{p} = \sqrt{I}$.*

*Proof.* $f \notin \sqrt{I} \Longleftrightarrow f^n \notin I$ for all $n \Longleftrightarrow 1 \notin IR_f \Longleftrightarrow IR_f \subseteq \mathfrak{p}$ for some prime in $R_f \Longleftrightarrow I \subseteq \mathfrak{p}'$ for some prime in $R$ (that does not contain $f$). □

The following corollary follows in exactly the same way as the analogous statement for subvarieties of $K^n$, Corollary 2.17.

**Corollary 3.22.** *Let $R$ a ring. There is an order-reversing bijection*

$$\{\textit{closed subsets of } \operatorname{Spec}(R)\} \qquad \leftrightarrow \qquad \{\textit{radical ideals } I \subseteq R\}.$$

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

## 3.3 Local rings

**Definition 3.23.** *A ring $R$ is called 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.*

An easy equivalent characterization is that $R$ is local if and only if the set of nonunits of $R$ forms an ideal: this must then be the unique maximal ideal.

The following lemma is an easy source of local rings.

**Lemma 3.24.** *Let $R$ be a ring, and $\mathfrak{p}$ be a prime ideal. Then $(R_\mathfrak{p}, \mathfrak{p}R_\mathfrak{p})$ is a local ring.*

*Proof.* The primes of $R_\mathfrak{p}$ are just the expansions of primes of $R$ that are contained in $\mathfrak{p}$. In $R$, $\mathfrak{p}$ is uniquely maximal among primes contained in $\mathfrak{p}$. □

**Example 3.25.**

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

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

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

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

5. A polynomial ring over a field is certainly not local; you know so many maximal ideals! A local ring we will often encounter 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. (We can talk about lowest terms since the polynomial ring is a UFD.)

6. Extending the following example, we have local rings like $(K[x_1,\dots,x_d]/I)_{(x_1,\dots,x_d)}$. 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 $X \subseteq K^d$). Then we call $(K[x_1,\dots,x_d]/I)_{(x_1,\dots,x_d)} = K[X]_{\mathfrak{m}_{\underline{0}}}$ the *local ring of the point* $\underline{0} \in X$; some people write $\mathcal{O}_{X,\underline{0}}$. The radical ideals of this ring consist of radical ideals of $K[X]$ that are contained in $\mathfrak{m}_{\underline{0}}$, which by the Nullstellensatz correspond to subvarieties of $X$ that contain $\underline{0}$.

We want to make a quick observation about local rings: let $(R,\mathfrak{m},k)$ be local. Since $k$ is a quotient of $R$, the characteristic of $R$ must be a multiple of the characteristic of $k$; the kernel of the map from $\mathbb{Z}$ can only get bigger in the composition. Of course, with example 2 in mind, 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 $\operatorname{char}(R) = p^n \cdot m$ with $m$ coprime to $p$, then $m \notin \mathfrak{m}$, since this would imply that $1 \in \mathfrak{m}$. This means that $m$ is a unit. But then, $p^n m = 0$ implies $p^n = 0$, so the characteristic must be $p^n$. We summarize and add one more observation.

**Proposition 3.26.** *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 $p$. We say that $R$ has* mixed characteristic $(0,p)$.

3. $\operatorname{char}(R) = \operatorname{char}(k) = p$ *for a prime $p$. We say that $R$ 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.*

We will grow to like local rings. It's worth noting that $\operatorname{Max}(R)$ for a local ring is quite a useless object, but that $\operatorname{Spec}(R)$ can still be quite interesting.

## 3.4 NAK, a.k.a., Nakayama's Lemma

There are a range of statements the go under the banner of Nakayama's Lemma a.k.a. NAK.

**Proposition 3.27.** *Let $R$ be a ring, $I$ an ideal, and $M$ a finitely generated $R$-module. If $IM = M$, then*

- *there is an element $r \in 1 + I$ such that $rM = 0$, and*
- *there is an element $a \in I$ such that $am = m$ for all $m \in M$.*

*Proof.* Let $m_1,\dots,m_s$ be a generating set for $M$. By assumption, we have equations

$$m_1 = a_{11}m_1 + \cdots + a_{1s}m_s \ , \ \dots \ , \ m_s = a_{s1}m_1 + \cdots + a_{ss}m_s,$$

with $a_{ij} \in I$. Setting $A = [a_{ij}]$ and $X = [x_i]$ we have a matrix equations $AX = X$, and hence $(I_s - A)X = 0$. By the adjoint trick, we have $\operatorname{adj}(I_s - A)(I_s - A)X = \det(I_s - A)I_sX = 0$, so $\det(I_s - A)$ kills each $m_i$, and hence $M$. Since $\det(I_s - A) \equiv \det(I_s) \equiv 1 \bmod I$, this determinant is the element $r$ we seek for the first statement.

For the latter statement, set $a = 1 - r$; this is in $I$ and satisfies $am = m - rm = m$ for all $m \in M$. □

**Example 3.28.** We will use this to give a quick proof of the fact that, if $M$ is a finitely generated $R$-module, and $\varphi : M \to M$ is a surjective $R$-linear endomorphism, then $\varphi$ is an isomorphism. In this setting, $M$ is an $R[x]$-module by the rule $xm = \varphi(m)$, $x^2m = \varphi^2(m)$, etc. The hypothesis that $\varphi$ is surjective says that $xM = M$. Then, some element of $(x)$ acts as the identity on $M$: $f(x)x$ is the identity, so $f(\varphi) \circ \varphi$ is the identity. Thus, $\varphi$ is an isomorphism.

**Proposition 3.29.** *Let $(R, \mathfrak{m}, k)$ be a local ring, and $M$ be a finitely generated module. If $M = \mathfrak{m}M$, then $M = 0$.*

*Proof.* By the previous lemma, there exists an element $r \in 1 + \mathfrak{m}$ that annihilates $M$. Such an $r$ must be a unit, so 1 annihilates $M$; i.e., $M = 0$. □

**Proposition 3.30.** *Let $(R, \mathfrak{m}, k)$ be a local ring, and $M$ be a finitely generated module. For $m_1, \dots, m_s \in M$,*

$$m_1, \dots, m_s \text{ generate } M \iff \overline{m_1}, \dots, \overline{m_s} \text{ generate } M/\mathfrak{m}M.$$

*Thus, any generating set for $M$ consists of at least $\dim_k(M/\mathfrak{m}M)$ elements.*

*Proof.* The implication $\Rightarrow$ is clear. Let $N = \langle m_1, \dots, m_s \rangle \subseteq M$. We have that $M/N = 0$ iff $M/N = \mathfrak{m}(M/N)$ iff $M = \mathfrak{m}M + N$ iff $M/\mathfrak{m}M$ is generated by the image of $N$. □

**Definition 3.31.** *Let $(R, \mathfrak{m})$ be a local ring, and $M$ a finitely generated module. A set of elements $\{m_1, \dots, m_t\}$ is a* minimal generating set *of $M$ if the images of $m_1, \dots, m_t$ form a basis for the $R/\mathfrak{m}$ vector space $M/\mathfrak{m}M$.*

**Example 3.32.** Let $R = K\begin{bmatrix} u & v & w \\ x & y & z \end{bmatrix}$, and $I = I_2\left(\begin{bmatrix} u & v & w \\ x & y & z \end{bmatrix}\right) = (uy - vx, uz - wx, vz - wy)$.

We claim that (the expansion of) $I$ is minimally generated by 3 elements in $R_{(u,v,w,x,y,z)}$. Indeed, any nonzero element of $(u, v, w, x, y, z)I$ has all of its terms with degree at least 3, so $a(uy - vx) + b(uz - wx) + c(vz - wy) \in (u, v, w, x, y, z)I$ implies the sum is zero or else we can assume $a, b, c \in (u, v, w, x, y, z)$, so this is the trivial dependence relation over the residue field. But if the sum is zero in $R$, we must have $a, b, c = 0$, since these are linearly independent elements of the polynomial ring.

We claim that $I$ is minimally generated by 2 elements in $R_{(u-1,v,w,x,y,z)}$. In this ring, we can write $uy - vx = u(y - vx/u)$, $uz - wx = u(z - wx/u)$, and $vz - wy = v(z - wx/u) + w(y - vx/u)$; since $u$ is a unit, we have that (the expansion of) $I$ is $(y - vx/u, z - wx/u)$. You can check that these are linearly independent mod $(u - 1, v, w, x, y, z)I$.

The same argument will show that $I$ is minimally generated by 2 elements in $R_{(x,y,z)}$.

Observe that any generating set for $M$ contains a minimal generating set, and that every minimal generating set has the same cardinality.

We now want to give graded analogues for the results above.

**Proposition 3.33.** *Let $R$ be an $\mathbb{N}$-graded ring, and $M$ a finitely-generated $\mathbb{Z}$-graded module. If $M = (R_+)M$, then $M = 0$.*

*Proof.* If $M$ is finitely-generated, then it can be generated by finitely generated homogeneous elements (the homogeneous pieces of some finite generating set); let $a$ be the lowest degree of a generator in this set. Then, $M$ lives in degrees at least $a$, but $(R_+)M$ lives in degrees strictly bigger than $a$. This implies that $M = 0$. □

Just as above, we obtain the following:

**Proposition 3.34.** *Let $R$ be an $\mathbb{N}$-graded ring, with $R_0$ a field, and $M$ a finitely-generated $\mathbb{Z}$-graded module. A set of elements of $M$ generates $M$ if and only if their images in $M/(R_+)M$ spans as a vector space. Since $M$ and $(R_+)M$ are graded, $M/(R_+)M$ admits a basis of homogeneous elements.*

In particular, if $K$ is a field, $R$ is a positively graded $K$-algebra, and $I$ is a homogeneous ideal, then $I$ has a minimal generating set by homogeneous elements, and this set is unique up to $K$-linear combinations.

## 3.5 Normal rings

We pause to define an important class of rings.

**Definition 3.35.** *An integral domain is* normal *if it is equal to its integral closure in its fraction field. More generally, a ring is* normal *if it is integrally closed in its total quotient ring.*

Here is a good source of normal domains.

**Lemma 3.36.** *UFDs are normal.*

*Proof.* Let $R$ be a UFD, and $a/b \in \operatorname{frac}(R)$, with $a, b$ coprime, be integral over $R$: there is an integral equation

$$(\frac{a}{b})^n + r_1(\frac{a}{b})^{n-1} + \cdots + r_n = 0$$

with $r_i \in R$. Clearing the denominator, we get

$$a^n + r_1 a^{n-1} b + \cdots + r_n b^n = 0.$$

This shows that $b|a^n$. If $b$ is not a unit, it has an irreducible factor, which must then be an irreducible factor of $a$, which contradicts that these are coprime. Thus, $b$ is a unit, so $a/b \in R$. □

**Lemma 3.37.** *Let $R$ be a domain, $K = \operatorname{frac}(R)$, and $K \subseteq L$ an extension field. Then the integral closure of $R$ in $L$ is normal.*

*Proof.* Let $S$ be the integral closure of $R$ in $L$. Let $x \in L$ be integral over $S$. Take a dependence relation

$$x^n + s_1 x^{n-1} + \cdots + s_n = 0$$

over $S$; we have that $x$ is integral over $R' = R[s_1, \dots, s_n]$ as well, so $R'[x]$ is module-finite over $R'$. Since $S$ is integral over $R$, $R'$ is module-finite over $R$. Then $R'[x]$ is module-finite over $R$, so $x$ is integral over $R$. This means that $x \in S$, as required. □

**Definition 3.38.** *If $K$ is a vector space-finite extension of $\mathbb{Q}$, then the* ring of integers *in $K$, denoted $\mathcal{O}_K$, is the integral closure of $\mathbb{Z}$ in $K$.*

**Lemma 3.39.** *If $R \subseteq S$ are domains, with $S$ normal, and $R$ a direct summand of $S$ as an $R$-module, then $R$ is also normal.*

*Proof.* Let $a/b$ be integral over $R$, with $a, b \in R$. This fraction is necessarily integral over $S$, hence in $S$, so $a = bs$ for some $s \in S$. Let $\pi : S \to R$ be an $R$-linear splitting of the inclusion map. We have $a = \pi(a) = \pi(bs) = b\pi(s)$, so that $a/b = \pi(s) \in R$. □

**Example 3.40.** 1. If $K$ is a field, then $K[\underline{x}]$ is normal, since it is a UFD.

2. The rings of integers $\mathbb{Z}[i], \mathbb{Z}[\sqrt{2}], \mathbb{Z}[\sqrt{-5}], \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ are all normal.

3. The ring $K[x^2, x^3] \subseteq K[x]$ is not normal. Its fraction field is $K(x)$, but $x$ is an integral element over this ring (a root of $T^2 - x^2$ or $T^3 - x^3$) that is not in it.

4. The domain $K[x, y, z]/(x^2 y - z^2)$ is not normal either. Notice that $y = (z/x)^2$, so $z/x$ is an element of the fraction field that is integral over $R$, but not in it.

5. The ring $K[x^2, xy, y^2] \subseteq K[x, y]$ is normal, but not a UFD. It is a direct summand of the bigger polynomial ring (if the characterstic of $K$ is not two, we saw that it was the invariant ring of an finite group action or order 2, and is thus a direct summand by an exercise; you are encouraged to find a characteristic free argument), hence it is normal. It is not a UFD, since $x^2$, $y^2$, and $xy$ are all irreducibles (for degree reasons) but $(x^2)(y^2) = (xy)^2$ is a nonunique factorization.

We now want to give a finiteness statement for integral closures of normal domains in larger fields.

If $K \subseteq L$ is a vector-space finite inclusion of fields, the *trace map* from $L$ to $K$ is defined as $\mathrm{Tr}_{L/K}(x)$ is the trace, as a $K$-linear transformation, of the map "multiplication by $x$." Recall that the trace of a linear map can be computed as the sum of the diagonal entries in the matrix of the transformation for any choice of basis, or as the (negative of the) second coefficient of the characteristic polynomial of the transformation.

**Proposition 3.41.** *Let $K \subseteq L \subseteq M$ be finite algebraic extensions of fields.*

1. $\mathrm{Tr}_{L/K}$ *is $K$-linear.*

2. $\mathrm{Tr}_{L/K}(x) = [L : K]x$ *for $x \in K$.*

3. $-\mathrm{Tr}_{K(x)/K}(x)$ *is the second coefficient of the minimal polynomial of $x$ over $K$.*

4. *If $K \subseteq L \subseteq M$ are fields, then* $\mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}$.

5. *If $L/K$ is separable then the bilinear pairing $(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$ is* nondegenerate*: for any $x \in L$, there is some $y \in L$ such that* $\mathrm{Tr}_{L/K}(xy) \neq 0$.

*Proof.* We leave these as exercises. □

**Lemma 3.42.** *Let $R$ be a normal domain, $K = \mathrm{frac}(R)$, and $a$ an element that is integral over $R$ in some larger domain $S \supseteq R$. Then the minimal monic polynomial of $a$ over $K$ has all of its coefficients in $R$.*

*Proof.* Let $f(x) \in K[x]$ be the minimal (monic) polynomial of $x$, and $g(x) \in R[x]$ be some integral equation for $a$. By definition of $f$, we have $f(x)|g(x)$ in $K[x]$. Over some extension field of $K(x)$, the minimal polynomial of $x$ splits into linear factors $\prod_i (x - r_i)$. Each root $r_i$ of $f$ is a root of $g$, and hence integral over $R$. The coefficients of $f(x)$ can be determined as polynomial expressions in terms of the roots (namely, the elementary symmetric polynomial expressions). Thus, $f(x) \in R[r_1, \ldots, r_t][x] \bigcap K[x]$. Since $R[r_1, \ldots, r_t]$ is integral over $R$ and $R$ is normal, we find that $f(x) \in R[x]$. □

**Lemma 3.43.** *If $K \subseteq L$ is a finite extension field and $x \in L$ is integral over $R$, then* $\mathrm{Tr}_{L/K}(x) \in R$.

*Proof.* We have

$$\operatorname{Tr}_{L/K}(x) = \operatorname{Tr}_{K(x)/K}(\operatorname{Tr}_{L/K(x)}(x)) = -[L : K(x)] \cdot \text{“second coefficient of minimal poly of } x\text{”} \in R.$$

□

**Theorem 3.44.** *Let $R$ be a Noetherian normal domain, $K$ its fraction field, and $L$ a finite separable extension field of $K$. The integral closure of $R$ in $L$ is module-finite over $R$, and hence Noetherian.*

*Proof.* Write $S$ for the integral closure of $R$ in $L$. First, we claim that there is a $K$-vector space basis for $L$ over $K$ consisting of elements of elements of $S$. Since $L$ is algebraic over $K$, any element $x \in L$ satisfies an algebraic relation with coefficients in $K$. We can multiply by the finitely man denominators in such a relation to get a (no longer monic) dependence relation for $x$ with coefficients in $R$:

$$a_0x^n + a_1x^{n-1} + \cdots + a_n = 0.$$

Multiply by $a_0^{n-1}$ and regroup

$$(a_0x)^n + a_1(a_0x)^{n-1} + a_2a_0(a_0x)^{n-2} + \cdots + a_0^{n-1}a_n = 0.$$

This equation shows that $a_0x$ is integral over $R$, and thus lies in $S$. Thus, given a basis for $L$ over $K$, we can rescale the new elements by nonzero elements in $K$ to get a basis for $L$ over $K$ consisting of elements of elements of $S$; call it $\{s_1, \dots, s_d\}$.

Since the trace form is nondegenerate, we can use Gram-Schmidt to find a dual basis for our given basis: $\{t_1, \dots, t_d\} \subseteq L$. We will show that $S \subseteq \sum Rt_i$. Let $s \in S$, and write $s = \sum_i k_it_i$, with $k_i \in K$. For each $i$, $ss_i \in S$, so $\operatorname{Tr}_{L/K}(ss_i) \in R$ by the previous lemma. On the other hand,

$$\operatorname{Tr}_{L/K}(ss_i) = \operatorname{Tr}_{L/K}((\sum_j k_jt_j)s_i) = \sum_j k_j \operatorname{Tr}_{L/K}(s_it_j) = k_i.$$

This shows that the expression we had for $s$ before realizes $s$ in $\sum Rt_i$. Since $R$ is Noetherian, $S$ is module-finite over $R$. □

# Chapter 4

# Exact functors, localization, flatness

## 4.1 Exact, left-exact, right-exact functors

**Definition 4.1.** *A sequence of maps of $R$-modules*

$$\cdots \to M_1 \xrightarrow{\alpha_1} M_2 \xrightarrow{\alpha_2} \cdots \xrightarrow{\alpha_{t-1}} M_t \to \cdots$$

*is said to be* exact *if for all $1 < i < t$, one has $\ker(\alpha_i) = \operatorname{im}(\alpha_{i-1})$ as submodules of $M_i$. We allow sequences that may or may not continue indefinitely in either direction.*

For a while, we will be happy to focus on a few special cases.

**Definition 4.2.** *A* short exact sequence *of $R$-modules is an exact sequence of the form*

$$0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0;$$

*that is:*

- $\ker(\alpha) = 0$*; i.e., $\alpha$ is injective,*
- $\operatorname{coker}(\beta) = 0$*; i.e., $\beta$ is surjective, and*
- $\ker(\beta) = \operatorname{im}(\alpha)$*.*

Since $\alpha$ is injective, $L \cong \alpha(L)$. If we identify $L$ with $\alpha(L)$, then the data of the short exact sequence above translates to $N \cong M/L$, with $\alpha : L \to M$ the inclusion map, and $\beta : M \to N$ to quotient map.

**Definition 4.3.** *A* right exact sequence *of $R$-modules is an exact sequence of the form*

$$L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0;$$

*that is:*

- $\operatorname{coker}(\beta) = 0$*; i.e., $\beta$ is surjective, and*
- $\ker(\beta) = \operatorname{im}(\alpha)$*.*

The data of a right exact sequence translates to $N \cong \operatorname{coker}(\alpha) = M/\operatorname{im}(\alpha)$, with $\beta : M \to N$ the quotient map from the target onto the cokernel.

A special case of this is when $M$ and $N$ are free.

**Definition 4.4.** *A* presentation *of a module $N$ is a right-exact sequence of the form*

$$F_1 \xrightarrow{\alpha} F_0 \to N \to 0$$

*with $F_1$ and $F_0$ free.*

The image of the free basis of $F_0$ in $N$ is a generating set for $N$; this is equivalent to surjectivity. The image of $F_1$ in $F_0$ gives the *relations* on those generators.

**Remark 4.5.** We say that a module is *finitely presented* or *finitely presentable* if it admits a presentation by finitely generated free modules. If $R$ is Noetherian, then finitely generated and finitely presented are equivalent.

**Definition 4.6.** *A* left exact sequence *of $R$-modules is an exact sequence of the form*

$$0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N;$$

*that is:*

- $\ker(\alpha) = 0$*; i.e., $\alpha$ is injective, and*
- $\ker(\beta) = \operatorname{im}(\alpha)$.

The data of a left exact sequence translates to $L \cong \ker(\beta)$, and $\alpha : L \to M$ is the inclusion of the kernel into the source.

Observe that a sequence of maps $0 \to L \to M \to N \to 0$ is short exact if and only if it is left and right exact.

**Remark 4.7.** A sequence of $R$-modules is exact if and only if when we view it as a sequence of abelian groups by forgetting the module structure, it is exact. In particular, If our sequence of $R$-modules is also a sequence of $S$-modules with the same additive structure, exactness can be judged equivalently by either structure.

## 4.2 Exactnesses of Hom and Tensor

**Definition 4.8.** *Let $L, M, N$ be $R$-modules.*

- *The* module of homomorphisms *from $M$ to $N$ is*

  $$\operatorname{Hom}_R(M, N) := \{\phi : M \to N \mid \phi \text{ is } R\text{-linear}\}.$$

  *The $R$-module structure is given by the rule $r \cdot \phi$ is the homomorphism $m \mapsto r\phi(m) = \phi(rm)$.*

- *If $\alpha : M \to N$ is a module homomorphism, we define a map* $\operatorname{Hom}_R(L, \alpha)$ *or $\alpha_*$ from* $\operatorname{Hom}_R(L, M) \to \operatorname{Hom}_R(L, N)$ *by the rule*

  $$\alpha_*(\phi) = \alpha \circ \phi;$$

  *i.e.,*

  $$\alpha_* : \qquad (\ L \xrightarrow{\phi} M\ ) \ \mapsto \ (\ L \xrightarrow{\alpha} M \xrightarrow{\phi} N\ ).$$

- *If $\alpha : M \to N$ is a module homomorphism, we define a map* $\operatorname{Hom}_R(\alpha, L)$ *or* $\alpha^*$ *from* $\operatorname{Hom}_R(N, L) \to \operatorname{Hom}_R(M, L)$ *by the rule*

$$\alpha^*(\phi) = \phi \circ \alpha;$$

*i.e.,*

$$\alpha^* : \qquad ( N \xrightarrow{\phi} L ) \;\; \mapsto \;\; ( M \xrightarrow{\alpha} N \xrightarrow{\phi} L ).$$

Thus, given a fixed $R$-module $L$, $F(-) := \operatorname{Hom}_R(L, -)$ is rule that assigns to any $R$-module $M$ another $R$-module $F(M)$, and to any homomorphism $M \xrightarrow{\phi} N$ a homomorphism $F(M) \xrightarrow{F(\phi)} F(N)$. This (plus the fact that $F$ takes the identity map to the identity map and compositions to compositions) makes $F$ a *covariant functor* from $R$-modules to $R$-modules.

Similarly, given a fixed $R$-module $L$, $G(-) := \operatorname{Hom}_R(-, L)$ is rule that assigns to any $R$-module $M$ another $R$-module $G(M)$, and to any homomorphism $G(M) \xrightarrow{\phi} G(N)$ a homomorphism $G(N) \xrightarrow{G(\phi)} G(M)$. This (with the same caveats as above) makes $G$ a *contravariant functor* from $R$-modules to $R$-modules. The covariant vs. contravariant bit refers to whether the directions of maps have changed.

**Example 4.9.** $\operatorname{Hom}_R(R, M) \cong M$ by $\phi \mapsto \phi(1)$, and under this isomorphism, $M \xrightarrow{\alpha} N$ corresponds to $1 \mapsto m \rightsquigarrow 1 \mapsto \alpha(m)$ under this isomorphism.

If $I$ is an ideal, $\operatorname{Hom}_R(R/I, M) \cong \operatorname{ann}_M(I)$ by the same map: the image of 1 in $R/I$ must map to something killed by $I$, and there is a unique $R$-linear map that does this. The same recipe for maps as above holds. Thus, we can identify $\operatorname{Hom}_R(R/I, -)$ with the functor that sends modules $M$ to $\operatorname{ann}_M(I)$, and sends maps to their restrictions to these submodules.

**Theorem 4.10.** 1. *A sequence of maps*

$$0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N$$

*is left-exact if and only if, for all $R$-modules $X$, the sequence*

$$0 \to \operatorname{Hom}_R(X, L) \xrightarrow{\alpha_*} \operatorname{Hom}_R(X, M) \xrightarrow{\beta_*} \operatorname{Hom}_R(X, N)$$

*is left-exact.*

2. *A sequence of maps*

$$L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$$

*is right-exact if and only if, for all $R$-modules $X$, the sequence*

$$0 \to \operatorname{Hom}_R(N, X) \xrightarrow{\beta^*} \operatorname{Hom}_R(M, X) \xrightarrow{\alpha^*} \operatorname{Hom}_R(L, X)$$

*is left-exact.*

*Proof.* Let $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N$ be left-exact, and $X$ be an $R$-module.

- $\alpha_*$ is injective: if $X \xrightarrow{\phi} L$ is nonzero, $X \xrightarrow{\phi} L \xrightarrow{\alpha} M$ is as well, since a nonzero element in the image of $\phi$ goes to something nonzero in the composition.

- $\ker(\beta_*) = \operatorname{im}(\alpha_*)$: $X \xrightarrow{\phi} M \xrightarrow{\beta} N$ is zero if and only if $\operatorname{im}(\phi) \subseteq \ker(\beta) = \operatorname{im}(\alpha)$, which happens if and only if $\phi$ factors through $L$; i.e., $\phi \in \operatorname{im}(\alpha_*)$.

The other direction of the first part follows from the example above; we can use $X = R$.

Let $L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ be a right-exact sequence, and $X$ be an $R$-module.

- $\beta^*$ is injective: if $N \xrightarrow{\phi} X$ is nonzero, pick $n \in N$ not in the kernel, and $m \in M$ that maps to $n$. Then, the image of $m$ under $M \xrightarrow{\beta} N \xrightarrow{\phi} X$ is nonzero.

- $\ker(\alpha^*) = \operatorname{im}(\beta_*)$: $L \xrightarrow{\alpha} M \xrightarrow{\phi} X$ is zero if and only if $\operatorname{im}(\alpha) \subseteq \ker(\phi)$, which happens if and only if $\phi$ descends to a map of the form $N \cong M/\operatorname{im}(\alpha) \to X$; i.e., $\phi \in \operatorname{im}(\alpha^*)$.

Let $L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ be a sequence of maps, and suppose that it is exact after applying $\operatorname{Hom}_R(-, X)$ for all $X$.

- $\beta$ is surjective: if not, let $X = N/\operatorname{im}(\beta)$. There is a nonzero projection map $N \xrightarrow{\phi} X$, but $M \xrightarrow{\beta} N \xrightarrow{\phi} X$, contradicting injectivity of $\beta^*$.

- $\ker(\beta) \supseteq \operatorname{im}(\alpha)$: Take $X = N$, and $N \xrightarrow{\mathrm{id}} X$. Since $\ker(\alpha^*) \supseteq \operatorname{im}(\beta^*)$, $L \xrightarrow{\alpha} M \xrightarrow{\beta} N \xrightarrow{\mathrm{id}} X = L \xrightarrow{\alpha} M \xrightarrow{\beta} N$ is zero.

- $\ker(\beta) \subseteq \operatorname{im}(\alpha)$: Take $X = M/\operatorname{im}(\alpha)$, and $M \xrightarrow{\phi} X$ the projection map. Since $L \xrightarrow{\alpha} M \xrightarrow{\phi} X$ is zero, $\phi$ is in the image of $\beta^*$, so it factors through $\beta$. This is equivalent to the stated containment. □

In short, $\operatorname{Hom}_R(X, -)$ is kernel-preserving, and $\operatorname{Hom}_R(-, X)$ turns cokernels into kernels.

**Definition 4.11.** *If $L \xrightarrow{\alpha} L'$ is a map of $R$-modules, and $M$ is another $R$-module, there is an $R$-module homomorphism $L \otimes_R M \xrightarrow{\alpha \otimes M} L' \otimes_R M$ given by given by $\alpha \otimes M(l \otimes m) = \alpha(l) \otimes m$ on simple tensors. This is the map coming from the universal property applied to $L \times M \xrightarrow{\alpha \times \mathrm{id_M}} L' \times M \to L' \otimes_R M$.*

Thus, if $N$ is an $R$-module, $- \otimes_R N$ is a covariant functor.

**Theorem 4.12** (Hom-tensor adjointness). *Let $L, M, N$ be $R$-modules. There is an isomorphism $\operatorname{Hom}_R(L \otimes_R M, N) \cong \operatorname{Hom}_R(L, \operatorname{Hom}_R(M, N))$. Moreover, given $L \xrightarrow{\alpha} L', M \xrightarrow{\alpha} M'$, and $N \xrightarrow{\alpha} N'$ the diagram*

$$\begin{tikzcd}
\operatorname{Hom}_R(L' \otimes_R M', N) \arrow[r, "\operatorname{Hom}(\alpha\otimes\beta,\gamma)"] \arrow[d, "\cong"] & \operatorname{Hom}_R(L' \otimes_R M', N) \arrow[d, "\cong"] \\
\operatorname{Hom}_R(L', \operatorname{Hom}_R(M', N)) \arrow[r, "\operatorname{Hom}(\alpha,\operatorname{Hom}(\beta,\gamma))"] & \operatorname{Hom}_R(L, \operatorname{Hom}_R(M, N'))
\end{tikzcd}$$

*commutes.*

*Proof.* We will relate both sides to something else. Let $\operatorname{Lin}_R(X, Y; Z)$ be the set of maps $X \times Y \to R$ that are linear on each argument $X, Y$: $\phi(rx, y) = \phi(x, ry) = r\phi(x, y)$. This is an $R$-module, where the action is given by the action on any factor. The universal property of the tensor product translates to the fact that $\operatorname{Hom}_R(X \otimes_R Y, Z) \cong \operatorname{Lin}_R(X, Y; Z)$ for all $Z$ by the map sending

$$X \otimes_R Y \to Z \quad \rightsquigarrow \quad X \times Y \to X \otimes_R Y \to Z.$$

We claim that $\operatorname{Lin}_R(X, Y; Z) \cong \operatorname{Hom}_R(X, \operatorname{Hom}_R(Y, Z))$ by the map sending $\phi \mapsto (x \mapsto \phi(x, -))$; the inverse is $\psi \mapsto ((x, y) \mapsto \psi(x)(y))$.

Finally, under the stated isomorphisms, one checks easily that $\operatorname{Hom}(\alpha\otimes\beta,\gamma)$ and $\operatorname{Hom}(\alpha,\operatorname{Hom}(\beta,\gamma))$ both correspond to the obvious map $\operatorname{Lin}(\alpha,\beta;\gamma)$ given by precomposition on the inputs and postcomposition on the target. □

**Theorem 4.13.** *If a sequence of maps*

$$L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$$

*is right-exact, then*

$$L \otimes_R X \xrightarrow{\alpha\otimes X} M \otimes_R X \xrightarrow{\beta\otimes X} N \otimes_R X \to 0$$

*is right-exact.*

*Proof.* To see that the latter sequence is right-exact, we show that if we apply $\operatorname{Hom}_R(-,Y)$ to it, it is exact, for all $R$-modules $Y$. The sequence becomes

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Hom}_R(N\otimes X,Y) \arrow[r, "\operatorname{Hom}(\beta\otimes X,Y)"] \arrow[d, "\cong"] & \operatorname{Hom}_R(M\otimes X,Y) \arrow[r, "\operatorname{Hom}(\alpha\otimes X,Y)"] \arrow[d, "\cong"] & \operatorname{Hom}_R(L\otimes X,Y) \arrow[d, "\cong"] \\
0 \arrow[r] & \operatorname{Hom}_R(N,\operatorname{Hom}_R(X,Y)) \arrow[r, "\operatorname{Hom}(\beta,\operatorname{Hom}(X,Y))"] & \operatorname{Hom}_R(M,\operatorname{Hom}_R(X,Y)) \arrow[r, "\operatorname{Hom}(\alpha,\operatorname{Hom}(X,Y))"] & \operatorname{Hom}_R(L,\operatorname{Hom}_R(X,Y)).
\end{tikzcd}$$

It follows from left-exactness of Hom that the latter is left-exact. □

**Remark 4.14.** Let $S$ be an $R$-algebra. If $M$ is an $R$-module, then $S\otimes_R M$ is an $S$-module, where $S$ acts on the $S$-factor. If $M \xrightarrow{\alpha} N$ is a map of $R$-modules, then $S\otimes_R M \xrightarrow{S\otimes\alpha} S\otimes_R N$ is a map of $S$-modules. The functor $S\otimes_R -$ is called *extension of scalars* from $R$ to $S$.

Observe that $S\otimes R^{\oplus\Lambda} \cong S^{\oplus\Lambda}$ as $S$-modules. By right-exactness, it follows that extension of scalars preserves presentations. That is, if

$$R^m \xrightarrow{A} R^n \to M \to 0$$

is a presentation, then

$$S^m \xrightarrow{A} S^n \to S\otimes_R M \to 0$$

is a presentation.

**Remark 4.15.** Let $S$ be an $R$-algebra, and $M$ and $N$ be $R$-modules.

If $M$ is also an $S$-module, then $\operatorname{Hom}_R(M,N)$ is an $S$-module by the precomposition $s\cdot\phi = \phi\circ(\times s)$. It is clear that this rule is $S$-linear: $ss'\cdot\phi = \phi\circ(\times ss') = (\phi\circ(\times s'))\circ(\times s) = s\cdot(s'\cdot\phi)$. It is equally straightforward to check that is $N \xrightarrow{\alpha} N'$ is $R$-linear, then $\operatorname{Hom}_R(M,\alpha)$ is $S$-linear. Thus, $\operatorname{Hom}_R(M,-)$ is a functor from $R$-modules to $S$-modules.

Similarly, if $N$ is an $S$-module, then $\operatorname{Hom}_R(M,N)$ is an $S$-module by postcomposition $s\cdot\phi = (\times s)\circ\phi$. Like above, $\operatorname{Hom}_R(-,N)$ is a functor from $R$-modules to $S$-modules.

The important warning is that if $M$ and $N$ are $S$-modules, then the two different recipes for $S$-module structures on $\operatorname{Hom}_R(M,N)$ may disagree (though they restrict to the same $R$-module action). For example, let $R = K$ be a field, $S = K[x]$, and consider $\operatorname{Hom}_R(K[x], K[x]/(x))$. In the postcomposition action, every map is killed by $x$. On the other hand, there is an $R$-linear projection of a polynomial onto its $x$-coefficient. The precomposition of this map by $x$ is the map that sends a polynomial to its constant term.

**Definition 4.16.** *An $R$-module is projective $P$ if the functor* $\mathrm{Hom}_R(P, -)$ *sends short exact sequences to short exact sequences. Equivalently, $P$ is projective if $M \xrightarrow{\alpha} N$ surjective implies* $\mathrm{Hom}_R(P, M) \xrightarrow{\mathrm{Hom}(P,\alpha)} \mathrm{Hom}_R(P, N)$ *is surjective.*

Free modules are always projective: $\mathrm{Hom}_R(R^{\oplus\Gamma}, M) \cong M^{\oplus\Gamma}$, and a map $\alpha$ gets sent to $\Gamma$ copies of itself. Every projective module is a direct summand of a free module: we can map a free module $F$ onto $P$, and since $\mathrm{Hom}_R(P, F) \twoheadrightarrow \mathrm{Hom}_R(P, P)$, the identity map of $P$ is in the image: the identity factors through $F$. Every direct summand of a free module is projective as well (exercise!).

For now, the only other thing we care to note about projectives is that they are not always free. Let $R = \mathbb{R}[x, y, z]/(x^2 + y^2 + z^2 - 1)$. Elements of this ring can be interpreted as functions from the real sphere $\mathbb{S}^2$ to $\mathbb{R}$; different polynomial functions representing the same class give the same function, since their difference is zero on the sphere. Elements of the free module $R^3$ can be thought of as functions from the real sphere $\mathbb{S}^2$ to $\mathbb{R}^3$, or vector fields along the sphere. Consider the map $v : R^3 \xrightarrow{[x\ y\ z]} R^1$. This takes the vector field $p \mapsto f(p) = (f_x(p), f_y(p), f_z(p))$ to the function $p \mapsto xf_x(p) + yf_y(p) + zf_z(p) = p \cdot f(p)$. This map $v$ is surjective: the identity vector field $i$ returns the constant function one. (Alternatively, look at the equation of the sphere!) Then, since $R^1$ is free, we can find an $R$-module splitting of the map $v$: send $1 \in R$ to the identity vector field. So, $R^3 = R \cdot i \oplus P$, where $P$ is the kernel of the map $v$. Thinking of $P \subseteq R^3$, the elements of $P$ are exactly the vector fields that satisfy $f(p) \cdot p = 0$: the vector fields that are orthogonal to the sphere. By topology, every such vector field vanishes at a point $q$. But then, any $R$-linear map $P \to R^1$ is *not* surjective, since every element of $P$ vanishes at a point, it must map to something that vanishes at a point, hence cannot map to a generator of the module $R^1$. We conclude that $P$ is projective, since it is a direct summand of a free module, but is not itself free.

## 4.3 Flatness

One of the many desirable properties that free modules have is that any relation between elements is a consequence of a relation in the ring. Namely, let $F = R^{\oplus\Gamma}$, and suppose that $r_1 f_1 + \cdots + r_t f_t = 0$ for some $r$'s in $R$ and $f$'s in $F$. Then, taking $\gamma$-coefficients for $\gamma \in \Gamma$, we get $r_1(f_1)_\gamma + \cdots + r_t(f_t)_\gamma = 0$ for each $\gamma$, with $(f_i)_\gamma \in R$. That is, every element $[\underline{f}]^T$ of $\ker([\underline{r}])$ in $F^t$ can be written as a combination $\sum [\underline{f_\gamma}]^T e_\gamma$, with $[\underline{f_\gamma}]^T$ in $\ker([\underline{r}])$ in $R^t$.

This desideratum is captured in generality by flat modules. We will see also that this more general notion of flatness is closely related to freeness.

**Definition 4.17** (Flat module)**.** *An $R$-module $N$ is* flat *if, for any inclusion of modules $M' \hookrightarrow M$, the map $M' \otimes_R N \to M \otimes_R N$ is injective.*

*If $\phi : R \to S$ is a map of rings, we say that $S$ is a* flat $R$-algebra *or $\phi$ is a* flat homomorphism *if ${}_\phi S$ is a flat $R$-module.*

**Lemma 4.18.** *Projective modules, and in particular, free modules, are flat.*

*Proof.* Exercise! □

**Lemma 4.19.** *If $\phi : R \to S$ is a ring homomorphism, and $M$ is a flat $R$-module, then $S \otimes_R M$ is a flat $S$-module.*

*Proof.* $(S \otimes_R M) \otimes_S N \cong M \otimes_R (S \otimes_S N) \cong M \otimes_R N$, and under this identification, $(S \otimes_R M) \otimes_S \alpha$ agrees with $M \otimes_R \alpha$. □

**Example 4.20.** If $K$ is a field, $L \supseteq K$ a larger field, and $R$ a $K$-algebra, then $R \otimes_K L$ is a flat $R$-algebra. (Take $R = K$ above, $S = R$ above, and $M = L$.) I.e., $K[\underline{x}]/I \to L[\underline{x}]/IL[\underline{x}]$ is flat.

**Proposition 4.21** (Flatness of localization)**.** *Let $R$ be a ring, and $W$ a multiplicative system. Then*

1. *$W^{-1}R \otimes_R M \cong W^{-1}M$ as $W^{-1}R$-modules,*

2. *With the isomorphisms as above, the following diagram commutes for all module homomorphisms $\alpha$:*

$$\begin{tikzcd}
W^{-1}R \otimes_R M \arrow[r, "W^{-1}R \otimes \alpha"] \arrow[d, "\cong"] & W^{-1}R \otimes_R N \arrow[d, "\cong"] \\
W^{-1}M \arrow[r, "\frac{m}{w} \mapsto \frac{\alpha(m)}{w}"] & W^{-1}N,
\end{tikzcd}$$

3. *$W^{-1}R$ is flat over $R$.*

*Proof.* 1. The bilinear map $(r/w, m) \mapsto rw/m$ induces a map from the tensor product that is clearly surjective. For an inverse map, send $m/w$ to the simple tensor $1/w \otimes m$. To see this is well-defined, suppose $m/w = m'/w'$, so $\exists v \in W$ such that $v(mw' - m'w) = 0$. The difference of the images of $m/w$ and $m'/w'$ is $1/w \otimes m - 1/w' \otimes m'$. We can multiply through by $vww'/vww'$ to get $\frac{vw'}{vww'} \otimes m - \frac{vw}{vww'} \otimes m' = \frac{1}{vww'} \otimes v(mw' - m'w) = 0$. It is equally easy to verify that this is a homomorphism. The composition sends $r/w \otimes m \mapsto rm/w \mapsto 1/w \otimes rm = r/w \otimes m$; since it is the identity on simple tensors and additive, it is the identity.

2. Straightforward computation using above.

3. Let $M \xrightarrow{\alpha} N$ be injective, and consider $W^{-1}R \otimes_R M \xrightarrow{W^{-1}R \otimes \alpha} W^{-1}R \otimes_R N$. By the previous part, it suffices to check that the bottom row of the diagram above is injective. If $\alpha(m)/w = 0$ in $W^{-1}N$, then there is some $v \in W$ such that $0 = v\alpha(m) = \alpha(vm)$, so $vm = 0$ by hypothesis, and $m/w = 0$ in $W^{-1}M$. □

**Definition 4.22.** *The* localization *of a map $M \xrightarrow{\alpha} N$ at the multiplicative set $W$ is the map $W^{-1}\alpha : W^{-1}M \to W^{-1}N$ given by $\alpha(m/w) = \alpha(m)/w$.*

*The rule $M \rightsquigarrow W^{-1}M$, $\alpha \rightsquigarrow W^{-1}\alpha$ defines a covariant functor from $R$-modules to $W^{-1}R$-modules; the* localization functor*. This functor is* exact*: it turns exact sequences into exact sequences.*

**Proposition 4.23** (Equational criterion)**.** *If $M$ is flat, the following condition holds:*

*For any $\underline{r} = (r_1, \ldots, r_t) \in R^t$ and $\underline{m} = (m_1, \ldots, m_t) \in M^t$ with $\underline{r} \cdot \underline{m} = 0$, there exist $\underline{s}_j = (s_{1j}, \ldots, s_{tj}) \in R^t$ for $j = 1, \ldots, a$ such that $\underline{r} \cdot \underline{s}_j = 0$ and $n_1, \ldots, n_a \in M$ such that $\underline{m} = \sum_{j=1}^{a} \underline{s}_j n_j$.*

*Proof.* Let $M$ be flat, and $\underline{r}$ and $\underline{m}$ as above. Consider the exact sequence $K \to R^t \xrightarrow{[\underline{r}]} R$, where $K$ is the kernel. By assumption, $K \otimes_R M \to M^t \xrightarrow{[\underline{r}]} M$ is exact. This means that the kernel of $M^t \xrightarrow{[\underline{r}]} M$, the $\underline{m}$'s in $M^t$ with $\underline{r} \cdot \underline{m} = 0$, all lie in $K \otimes_R M$. Thus, such an $\underline{m}$ can be written as $\sum_j k_j \otimes n_j$ for some $k_j \in K$ and $n_j \in M$. Unpackaging the definitions gives the elements we want. □

**Proposition 4.24** (F.g. flat modules are locally free)**.** *Let $(R, \mathfrak{m}, k)$ be a local ring, and $M$ be a finitely generated module. Then $M$ is flat if and only if $M$ is free.*

*Proof.* Free modules are always flat, so we show the other direction.

We will show that a minimal generating set for $M$ is a free basis. To see this, it suffices to show that if $x_1, \dots, x_t \in M$ are such that $\overline{x_1}, \dots, \overline{x_t} \in M/\mathfrak{m}M$ are linearly independent over $k$, then $x_1, \dots, x_t$ are linearly independent over $R$. (We are using NAK in a crucial way to say that such a set for some $t$ actually generates M.) We show this statement by induction on $t$, using the equational criterion.

For the base case, suppose that $rx_1 = 0$ for some $r \in R$, and $x_1$ as above. By the equational criterion, we can write $x_1 = \sum s_j n_j$, with $n_j \in M, s_j \in R$, and $rs_j = 0$. Since $\overline{x_1} = \overline{\sum s_j n_j} \neq 0$ in $M/\mathfrak{m}M$, some $s_j$ is not in $\mathfrak{m}$, and hence is a unit. But then $rs_j = 0$ implies $r = 0$, as required.

For the inductive step, suppose $\sum_{i=1}^t r_i x_i = 0$, with $x_1, \dots, x_t$ as above. Write $x_i = \sum s_{ij} n_j$ and $\sum r_i s_{ij} = 0$ for some $s_{ij}$'s in $R$ and $n_j$'s in $M$ by the equational criterion. Since $\overline{x_t} \neq 0$, $x_t \notin \mathfrak{m}M$, so $s_{tj} \notin \mathfrak{m}$ for some $j$, hence is a unit. We can then solve to write $r_t = \sum_{i=1}^{t-1} \frac{-s_{ij}}{s_{tj}} r_i$. Substitute to get a relation

$$0 = \sum_{i=1}^{t} r_i x_i = r_1 \left( x_1 - \frac{s_{1j}}{s_{tj}} x_t \right) + \cdots + r_{t-1} \left( x_{t-1} - \frac{s_{t-1,j}}{s_{tj}} x_t \right).$$

The images of the elements $\{x_1 - \frac{s_{1j}}{s_{tj}} x_t, \dots, x_{t-1} - \frac{s_{t-1,j}}{s_{tj}} x_t\}$ are linearly independent in $M/\mathfrak{m}M$; a nonzero relation on these yields a nonzero relation on the $\overline{x_1}, \dots, \overline{x_t}$ if we distribute. We can then apply the induction hypothesis to get that $r_1 = \cdots = r_{t-1} = 0$. By our expression for $r_t$, that is zero as well. □

**Remark 4.25.** The same proof shows that if $R$ is $\mathbb{N}$-graded, and $M$ is a finitely generated $\mathbb{Z}$-graded module, then $M$ is flat if and only if it is free.

**Example 4.26.** Let $R = K[x,y]_{(x,y)}$, and $S = K[x^2, xy, y^2]_{(x^2,xy,y^2)}$. We claim that $R$ is not a flat $S$-algebra. If it were, $R$ would be free of rank 2, since $R \otimes_S \operatorname{frac}(S) \cong (S \smallsetminus 0)^{-1} R \cong \operatorname{frac}(R) \cong \operatorname{frac}(S)^2$. However, the minimal number of generators of $R$ as an $S$-module is $\dim_K(R/(x^2, xy, y^2)R) = 3$. Note that $S$ is a direct summand of $R$ though.

Now, let $T = K[x^2, y^2]_{(x^2,y^2)} \subseteq S$. We claim that $S$ is a flat $T$-algebra. First, note that $K[x^2, xy, y^2] = K[x^2, y^2] \oplus xy \cdot K[x^2, y^2]$ is a free module. Then, $(K[x^2, y^2] \smallsetminus (x^2, y^2))^{-1} K[x^2, xy, y^2]$ is a free $K[x^2, y^2]_{(x^2,y^2)}$ module (since we obtain it by extension of scalars of a free module), and $S$ is a localization of $(K[x^2, y^2] \smallsetminus (x^2, y^2))^{-1} K[x^2, xy, y^2]$, so $S$ is flat over $T$.

We now want to observe that intersections of ideals behaves well in flat extensions.

**Lemma 4.27.** *Let $I, J \subseteq R$ be ideals. Then, there is a short exact sequence*

$$0 \to \frac{R}{I \cap J} \xrightarrow{\bar r \to (\bar r, \bar r)} \frac{R}{I} \oplus \frac{R}{J} \xrightarrow{(\bar r, \bar s) \mapsto \overline{r-s}} \frac{R}{I+J} \to 0.$$

*Proof.* The latter map is well-defined, since if $i \in I, j \in J$, we have $(r+i, s+j) \mapsto (r-s)+(i-j) \equiv r-s$ (modulo $I+J$). It is also surjective: the class of $(r, 0)$ maps to the class of $r$. The map $R \to R/I \oplus R/J$ given by $r \to (\bar r, \bar r)$ has kernel $I \cap J$, so the first map above is indeed injective. For the exactness in the middle, clearly the image of the first map is contained in the kernel of the second. It is also easy to see that an element in the kernel can be rewritten as a class of the form $(\bar r, \bar r)$, as required. □

**Proposition 4.28.** *Let $I_1, \dots, I_t \subseteq R$ be ideals, and $R \to S$ be flat. Then $I_1 S \cap \cdots \cap I_t S = (I_1 \cap \cdots \cap I_t)S$.*

*Proof.* It suffices to deal with the case $t = 2$. We have a short exact sequence

$$0 \to \frac{R}{I_1 \cap I_2} \to \frac{R}{I_1} \oplus \frac{R}{I_2} \to \frac{R}{I_1 + I_2} \to 0,$$

and applying $\otimes_R S$ we get an exact sequence

$$0 \to \frac{S}{(I_1 \cap I_2)S} \to \frac{S}{I_1 S} \oplus \frac{S}{I_2 S} \to \frac{S}{(I_1 + I_2)S} \to 0,$$

from which the claim follows. □

**Definition 4.29.** *If $I, J \subseteq R$ are ideals, the* colon ideal *is*

$$I : J := \{r \in R \mid rJ \subseteq I\}.$$

Note that $J \subseteq I$ if and only if $I : J = R$.

**Proposition 4.30.** *Let $I, J$ be ideals in $R$, with $J$ finitely generated, and $S$ be a flat $R$-algebra. Then $(IS : JS) = (I : J)S$.*

*Proof.* We start with the case $J = jR$ is principal. There is a left exact sequence of the form

$$0 \to I : jR \to R \xrightarrow{\times j} \frac{R}{I};$$

this is clear from the definition. Then, by flatness,

$$0 \to (I : jR) \otimes_R S \to S \xrightarrow{\times j} \frac{S}{IS}$$

is exact, so $(I : jR) \otimes_R S = IS : jS$, in light of the first left exact sequence. But, again by flatness, $(I : jR) \otimes_R S \cong (I : jR)S$.

Now, in general, $I : (j_1, \dots, j_t) = \bigcap_{i=1}^{t} I : j_i R$, so the claim follows for the statement for intersections. □

Another useful fact:

**Proposition 4.31** (Hom and flat base change)**.** *Let $S$ be a flat $R$ algebra, and $M, N$ be two $R$-modules. Suppose that $M$ is finitely presented. Then*

$$\begin{array}{ccc} S \otimes_R \operatorname{Hom}_R(M, N) & \cong & \operatorname{Hom}_S(S \otimes_R M, S \otimes_R N) \\ s \otimes \varphi & \mapsto & s(S \otimes \varphi) \end{array}$$

*is an isomorphism.*

*Proof.* When $M$ is $R$ or a finitely generated free module $R^{\oplus a}$, this is clear: both sides are isomorphic to $(S \otimes_R N)^{\oplus a}$, and it is easy to see that the map above realizes this.

Now, take a presentation

$$R^{\oplus b} \to R^{\oplus a} \to M \to 0.$$

If we apply $S \otimes_R -$, we obtain another right exact sequence; if we then apply $\operatorname{Hom}_S(-, S \otimes_R N)$ to this presentation, we obtain a left-exact sequence

$$0 \to \operatorname{Hom}_S(S \otimes_R M, S \otimes_R N) \to \operatorname{Hom}_S(S \otimes_R R^{\oplus a}, S \otimes_R N) \to \operatorname{Hom}_S(S \otimes_R R^{\oplus b}, S \otimes_R N).$$

Likewise, if we apply $\operatorname{Hom}_R(-,N)$, we obtain a left exact sequence; if we then apply $S \otimes_R -$, we obtain by flatness another left exact sequence

$$0 \to S \otimes_R \operatorname{Hom}_R(M,N) \to S \otimes_R \operatorname{Hom}_R(R^{\oplus a},N) \to \operatorname{Hom}_R(R^{\oplus b},N).$$

We then have a diagram

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Hom}_S(S \otimes_R M, S \otimes_R N) \arrow[r] & \operatorname{Hom}_S(S \otimes_R R^{\oplus a}, S \otimes_R N) \arrow[r] & \operatorname{Hom}_S(S \otimes_R R^{\oplus b}, S \otimes_R N) \\
0 \arrow[r] & S \otimes_R \operatorname{Hom}_R(M,N) \arrow[r] \arrow[u] & S \otimes_R \operatorname{Hom}_R(R^{\oplus a},N) \arrow[r] \arrow[u, "\cong"] & \operatorname{Hom}_R(R^{\oplus b},N), \arrow[u, "\cong"]
\end{tikzcd}$$

where the vertical maps are given by the formula of the statement. We claim that the squares commute. Indeed, given $X \xrightarrow{\alpha} Y$,

$$\begin{tikzcd}
\operatorname{Hom}_S(S \otimes_R Y, S \otimes_R N) \arrow[r, "\operatorname{Hom}(S\otimes\alpha, S\otimes N)"] & \operatorname{Hom}_S(S \otimes_R X, S \otimes_R N)\ , \\
S \otimes_R \operatorname{Hom}_R(Y,N) \arrow[r, "S\otimes\operatorname{Hom}(\alpha,N)"] \arrow[u] & S \otimes_R \operatorname{Hom}_R(X,N) \arrow[u]
\end{tikzcd}$$

an element $s \otimes \varphi$ in the bottom left goes $\uparrow$ to $s \cdot (S \otimes \varphi)$ and then $\to$ to $s \cdot (S \otimes (\varphi \circ \alpha))$, whereas $s \otimes \varphi$ goes $\to$ to $s \otimes (\varphi \circ \alpha)$ and then $\uparrow$ to $s \cdot (S \otimes (\varphi \circ \alpha))$. It then follows that there is an isomorphism in the first vertical map in the previous diagram. □

**Corollary 4.32** (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 $\mathfrak{p}$ is prime,*

$$\operatorname{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p}) \cong \operatorname{Hom}_R(M,N)_\mathfrak{p}.$$

We want to briefly note a definition related to flatness.

**Definition 4.33** (Faithfully flat module)**.** *A module $N$ over a ring $R$ is* faithfully flat *if $L \xrightarrow{\alpha} M$ is injective if and only if $L \otimes_R N \xrightarrow{\alpha\otimes N} M \otimes_R N$ is injective.*

*We can talk of faithfully flat algebras / morphisms as with flat algebras / morphisms.*

## 4.4 Local properties

To deal with many questions in commutative algebra, we can often reduce to the case of a local ring, where NAK applies.

**Definition 4.34.** *We say that a property $\mathcal{P}$ of a ring is a* local property *if*

$$\mathcal{P} \text{ holds for } R \iff \mathcal{P} \text{ holds for } R_\mathfrak{p} \text{ for all } \mathfrak{p} \in \operatorname{Spec}(R) \iff \mathcal{P} \text{ holds for } R_\mathfrak{m} \text{ for all } \operatorname{Max}(R).$$

*Similarly, we can talk about local properties of a module (looking at $M_\mathfrak{p}$ all $\mathfrak{p} \in \operatorname{Spec}(R)$) or of an element (looking at $m/1$ in $M_\mathfrak{p}$), or a homomorphism (considering $\alpha_\mathfrak{p}$), etc.*

**Proposition 4.35.** *1. Let $M$ be a module. For an element $x \in M$, the property $x = 0$ is local.*

2. *Let $M$ be a module. The property $M = 0$ is local.*

3. *Let $R$ be a domain. For an element $\alpha = r/s \in \operatorname{Frac}(R)$, the property $\alpha \in R$ is local.*

4. *Let $N \subseteq M$ be modules. The property $N = M$ is local.*

5. *Let $M \xrightarrow{\alpha} N$ be a module homomorphism. The property $\alpha$ is injective is local.*

6. *Let $M \xrightarrow{\alpha} N$ be a module homomorphism. The property $\alpha$ is surjective is local.*

7. *The property that a ring $R$ is reduced is local.*

8. *If $R$ is a domain, normality is a local property.*

*Proof.* 1. If $x = 0$, then clearly $x/1 = 0$ in any localization. We just need to show that if $x \neq 0$, then $x/1 \neq 0$ in $M_\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. By assumption, $\operatorname{ann}_R(x) \subsetneq R$, so it is contained in a maximal ideal $\mathfrak{m}$. Then, no element of $(R \smallsetminus \mathfrak{m})$ annihilates $x$ in $M$, so $x/1 \neq 0$ in $M_\mathfrak{m}$.

2. It is clear that $M = 0 \Longrightarrow M_\mathfrak{p} = 0$ for any localization. It then suffices to show that if $M \neq 0$, then $M_\mathfrak{m} \neq 0$ for some $\mathfrak{m} \in \operatorname{Max}(R)$. But this follows from the previous part, since if $M \neq 0$, it has a nonzero element, which is then nonzero in some localization.

3. Again, it is clear that $r/s \in R$ implies $r/s$ is in any localization of $R$, since $R$ injects into its localizations. For the other direction, note that we have $r/s \in R_\mathfrak{p}$ if and only if $r \in sR_\mathfrak{p}$, which happens if and only if $(sR_\mathfrak{p} : rR_\mathfrak{p}) = R_\mathfrak{p}$. If $(s : r) \subsetneq R$, then it is contained in a maximal ideal $\mathfrak{m}$, and then $(sR_\mathfrak{m} : rR_\mathfrak{m}) = (s : r)R_\mathfrak{m} \subsetneq R_\mathfrak{m}$, where the first equality is from colons and flat maps, and the second is from the behavior of expansions of ideals under localization.

4. Once again, we just need to check that if $N \subsetneq M$, then $N_\mathfrak{m} \subsetneq M_\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. Since localization is exact, we have

$$0 \to N \to M \to M/N \to 0 \text{ exact} \Longrightarrow 0 \to N_\mathfrak{m} \to M_\mathfrak{m} \to (M/N)_\mathfrak{m} \to 0 \text{ exact},$$

so $(M/N)_\mathfrak{m} = M_\mathfrak{m}/N_\mathfrak{m}$. Thus, this reduces to the claim that $M/N \neq 0 \Longrightarrow (M/N)_\mathfrak{m} \neq 0$ for some $\mathfrak{m}$, which is part (2).

5. Consider the left exact sequence $0 \to \ker(\alpha) \to M \xrightarrow{\alpha} N$. The sequence $0 \to \ker(\alpha)_\mathfrak{p} \to M_\mathfrak{p} \xrightarrow{\alpha_\mathfrak{p}} N_\mathfrak{p}$ is left exact for all $\mathfrak{p}$, so $\ker(\alpha_\mathfrak{p}) = \ker(\alpha)_\mathfrak{p}$. Since $\alpha_\mathfrak{p}$ is injective if and only if $\ker(\alpha)_\mathfrak{p} = 0$, this follows from part (2).

6. So similar to the past one...

7. Let $R$ be reduced, and $\mathfrak{p} \in \operatorname{Spec}(R)$. Suppose that $r/w \in R_\mathfrak{p}$ is such that $(r/w)^n = 0$. Then there is some $v \notin \mathfrak{p}$ such that $vr^n = 0$ in $R$. We then have $(vr)^n = 0$, so $r = 0$ by assumption, and hence $r/w = 0$.

   Now, suppose that $R$ is not reduced: take $r^n = 0$ with $r \neq 0$. Take a maximal ideal $\mathfrak{m} \supseteq \operatorname{ann}_R(r)$. Then, $r/1 \neq 0 \in R_\mathfrak{m}$, since $R \smallsetminus \mathfrak{m}$ contains no elements that kill $r$, but $(r/1)^n = r^n/1 = 0$ in $R_\mathfrak{m}$, so $R_\mathfrak{m}$ is not reduced.

8. Let $R$ be a domain; any localization $W^{-1}R$ of $R$ is a domain as well since $(r/v)(s/w) = 0$ implies some element of $W$ kills $rs$, so $rs = 0$ and $r/v$ or $s/w$ is zero. Note that any localization of $R$ has the same fraction field as $R$ itself.

   Assume $R$ is normal, $\mathfrak{p} \in \operatorname{Spec}(R)$, and let $r/s$ be integral over $R_{\mathfrak{p}}$:

   $$(r/s)^n + (a_1/w_1)(r/s)^{n-1} + \cdots + (a_n/w_n) = 0,$$

   with $r, s, a_1, \ldots, a_n \in R$, and all $w_i \notin \mathfrak{p}$. Wlog, we can assume $w_1 = \cdots = w_n =: w$, and multiply through by $w^n$ to get

   $$(rw/s)^n + (a_1 w)(rw/s)^{n-1} + \cdots + a_n w^n = 0.$$

   We then have $rw/s$ is integral over $R$, hence is in $R$, and since $w \notin \mathfrak{p}$, $r/s = (1/w)(rw/s) \in R_{\mathfrak{p}}$, as required.

   Now, suppose that $R$ is not normal. Then there is some $r/s \in \operatorname{Frac}(R) \setminus R$ that is integral over $R$. Passing to any localization gives an integral dependence relation over that localization. By a previous part, $r/s \notin R_{\mathfrak{m}}$ for some $\mathfrak{m} \in \operatorname{Max}(R)$. □

A weaker condition that is also useful is for a property to be preserved by localization: $\mathcal{P}$ holds for $R$ implies that $\mathcal{P}$ holds for $R_{\mathfrak{p}}$ for all $\mathfrak{p} \in \operatorname{Spec}(R)$. Be vigilant for this motif!

**Example 4.36.** The properties "$R$ is a domain" or "$R$ is Noetherian" are preserved by localization, but neither is a local property! (Find counterexamples!)

# Chapter 5

# Decomposition of ideals

## 5.1 Minimal primes and support

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

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

**Lemma 5.2.** *Let $R$ be a ring, and $I$ an ideal. Every prime $\mathfrak{p}$ that contains $I$ contains a minimal prime of $I$. Consequently, $\sqrt{I} = \bigcap_{\mathfrak{p}\in V(I)} \mathfrak{p} = \bigcap_{\mathfrak{p}\in \operatorname{Min}(I)} \mathfrak{p}$.*

*Proof.* This follows from Zorn's lemma. We just need to check that the intersection of a descending chain of prime ideals that contain $I$ is prime and contains $I$. These are both trivial. The first equality in the "consequently" we already know; the second is basic set theory. □

As a special case, the nilpotent elements of a ring $R$ are exactly the elements in every minimal prime of $R$ (equivalently, every minimal prime of the zero ideal).

**Proposition 5.3.** *Let $R$ be a Noetherian ring.*

1. *For any radical ideal $I$, there is a finite set of primes $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ such that $I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_t$.*
2. *For any closed subset $X = V(I) \subseteq \operatorname{Spec}(R)$, there is a finite set of primes $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ such that $X = V(\mathfrak{p}_1) \cup \cdots \cup V(\mathfrak{p}_t)$.*
3. *For any affine variety $Y = Z_K(I) \subseteq K^n$, there is a finite set of primes $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ such that $Y = Z_K(\mathfrak{p}_1) \cup \cdots \cup Z_K(\mathfrak{p}_t)$.*

*Proof.* For part (1), let $R$ be Noetherian, and consider the set of radical ideals $I$ that are *not* intersections of finitely many primes. If this set is nonempty, by Noetherianity, it has a maximal element $J$. Such a $J$ is definitely not prime, so pick $a, b \in R \smallsetminus J$ such that $ab \in J$. Since $a \in \sqrt{J+(a)} \smallsetminus \sqrt{J} = J$ and $b \in \sqrt{J+(b)} \smallsetminus \sqrt{J} = J$, these radical ideals are intersections of finitely many prime ideals, or one is improper. We claim that $\sqrt{J+(a)} \cap \sqrt{J+(b)} = J$, in which case we are done. This, we leave to you!

For part (2), there is a finite set of primes such that $\sqrt{I} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_t$. Then, $V(I) = V(\sqrt{I}) = V(\mathfrak{p}_1) \cup \cdots \cup V(\mathfrak{p}_t)$.

(3) is the same. □

Note that part (2) says that the closed subsets of $\operatorname{Spec}(R)$ for a Noetherian ring $R$ are just the specialization-closed subsets with finitely many minimal elements.

There is a uniqueness result for decompositions as above.

**Proposition 5.4.** *Let $R$ be a ring, $I$ be an ideal, and suppose that $\sqrt{I} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_t$, with $\mathfrak{p}_i \not\supseteq \mathfrak{p}_j$ for all $i \neq j$; if $R$ is Noetherian, we can always find such an expression for $\sqrt{I}$. Then, the primes $\{\mathfrak{p}_i\}$ are uniquely determined (up to reordering) as $\operatorname{Min}(I)$.*

*Proof.* It suffices to show that if

$$V(I) = V(\mathfrak{p}_1) \cup \cdots \cup V(\mathfrak{p}_t)$$

for primes with $\mathfrak{p}_i \not\supseteq \mathfrak{p}_j$ for all $i \neq j$, that then the set of $\mathfrak{p}_i$'s is exactly the set of minimal elements in $V(I)$. Suppose that $\mathfrak{q}$ is minimal in $V(I)$. Then $\mathfrak{q} \notin V(\mathfrak{p}_i)$ for any $\mathfrak{p}_i \neq \mathfrak{q}$ such that $\mathfrak{p}_i \supseteq I$. Thus, $\mathfrak{q}$ must appear as some $\mathfrak{p}_i$. Conversely, any of the primes $\mathfrak{p}_i$ must be minimal, since it does not contain any prime in $V(\mathfrak{p}_i)$ (properly) or in any other $V(\mathfrak{p}_j)$. □

We now wish to give a similar geometric decomposition for modules.

**Definition 5.5.** *If $M$ is an $R$-module, the* support *of $M$ is* $\operatorname{Supp}(M) := \{\mathfrak{p} \in \operatorname{Spec}(R) \mid M_\mathfrak{p} \neq 0\}$.

**Example 5.6.** If $M = R/I$, then $\operatorname{Supp}(M) = V(I)$. Indeed, $M_\mathfrak{p}$ is generated by the image of 1, so $M_\mathfrak{p} = 0$ iff the image of 1 is zero in the localization. But this happens if and only if $\exists w \notin \mathfrak{p} : w \cdot 1 = 0$ in $R/I \Leftrightarrow \exists w \notin \mathfrak{p}, w \in I \Leftrightarrow \mathfrak{p} \not\supseteq I$.

We observe that if $M$ is any module, then $\operatorname{Supp}(M)$ is *specialization-closed*: if $\mathfrak{p} \subset \mathfrak{q}$ and $\mathfrak{p} \in \operatorname{Supp}(M)$, then $\mathfrak{q} \in \operatorname{Supp}(M)$. Indeed, if $\mathfrak{q} \notin \operatorname{Supp}(M)$, so that $M_\mathfrak{q} = 0$, then we can obtain $M_\mathfrak{p}$ from $M_\mathfrak{q}$ by inverting more elements: $M_\mathfrak{p} = (M_\mathfrak{q})_\mathfrak{p} = 0_\mathfrak{p} = 0$. Any closed subset of $\operatorname{Spec}(R)$ is specialization-closed, so we might hope to realize supports as closed subsets. This holds for finitely generated modules.

**Proposition 5.7.** *If $R$ is a ring, and $M$ a finitely generated module, then* $\operatorname{Supp}(M) = V(\operatorname{ann}_R(M))$.

*Proof.* Let $M = \sum_i Rm_i$, so $\operatorname{ann}_R(M) = \bigcap_i \operatorname{ann}_R(m_i)$. We have that $M_\mathfrak{p} = 0 \Leftrightarrow \frac{m_i}{1} = 0$ in $M_\mathfrak{p}$ for all $i \Leftrightarrow \operatorname{ann}_R(m_i) \not\subseteq \mathfrak{p}$ for all $i \Leftrightarrow \operatorname{ann}_R(M) = \bigcap_i \operatorname{ann}_R(m_i) \not\subseteq \mathfrak{p}$. □

The finite generating hypothesis is necessary!

**Example 5.8.** Let $K$ be a field, and $R = K[x]$. Take $M = R_x/R = \bigoplus_{i>0} Kx^{-i}$. With this $K$-vector space structure, the action is given by multiplication in the obvious way, then killing any nonnegative degree terms.

On one hand, $\operatorname{Supp}(M) = \{(x)\}$. Indeed, any element of $M$ is killed by a large power of $x$, so $W^{-1}M = 0$ if $x \in W$.

On the other hand, the annihilator of the class of $x^{-n}$ is $x^n$, so $\operatorname{ann}_R(M) \subseteq \bigcap_{n \in \mathbb{N}} (x^n) = 0$.

**Example 5.9.** Let $R = \mathbb{C}[x]$, and $M = \bigoplus_{n \in \mathbb{Z}} R/(x-n)$.

On the one hand, $\operatorname{Supp}(M) = \{(x-n) \mid n \in \mathbb{Z}\}$. Indeed, $M_\mathfrak{p} = \bigoplus_{n \in \mathbb{Z}} (R/(x-n))_\mathfrak{p}$, and $\operatorname{Supp}(R/(x-n)) = \{(x-n)\}$.

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 the support is not even closed.

**Definition 5.10.** *If $M$ is an $R$-module, the* minimal primes *of $M$ are the minimal elements of* $\operatorname{Supp}(M)$. *If $M$ is finitely generated, then these are the minimal primes of the ideal* $\operatorname{ann}_R(M)$.

It is worth a stern warning now that this is not a priori a good definition if $M$ is not finitely generated: we don't know if specialization-closed subsets of Spec have minimal elements.

## 5.2 Associated primes and prime filtrations

We now refine our decomposition of ideals/modules.

**Definition 5.11.** *Let $R$ be a ring, and $M$ a module. We say that $\mathfrak{p} \in \operatorname{Spec}(R)$ is an* associated prime *of $M$ if $\mathfrak{p} = \operatorname{ann}_R(m)$ for some $m \in M$. Equivalently, $\mathfrak{p}$ is associated to $M$ if there is an injective homomorphism $R/\mathfrak{p} \hookrightarrow M$. 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 $R/I$; but we'll try to write $\operatorname{Ass}_R(R/I)$.*

**Lemma 5.12.** *If $\mathfrak{p}$ is prime, $\operatorname{Ass}_R(R/\mathfrak{p}) = \{\mathfrak{p}\}$.*

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

**Lemma 5.13.** *If $R$ is Noetherian, and $M$ an arbitrary $R$-module, then*

1. $\operatorname{Ass}(M) \neq \varnothing \Leftrightarrow M = 0$, *and*

2. $\displaystyle\bigcup_{\mathfrak{p} \in \operatorname{Ass}(M)} \mathfrak{p} = \{\textit{zerodivisors on } M\} := \{r \in R \mid rm = 0 \textit{ for some } m \in M \smallsetminus \{0\}\}$.

*Proof.* ($\Leftarrow$) is clear in part 1 (and certainly doesn't require Noetherian).

The interesting direction of 1 and part 2 will both follow from the fact that any ideal of the form $\operatorname{ann}_R(m)$ is contained in an associated prime; such a prime will certainly exist, and if something is a zerodivisor, it must belong to an associated prime.

The set $\{\operatorname{ann}_R(m) \mid m \in M\}$ has a maximal element, by Noetherianity. Let $I = \operatorname{ann}(m)$ be such an element, and let $rs \in I$, $s \notin I$. Clearly $\operatorname{ann}(sm) \supseteq \operatorname{ann}(m)$, and equality holds by maximality. Then, $(rs)m = r(sm) = 0$, so $r \in \operatorname{ann}(sm) = \operatorname{ann}(m) = I$. Thus, $I$ is prime. □

**Lemma 5.14.** *If $0 \to L \to M \to N \to 0$ is exact, then $\operatorname{Ass}(L) \subseteq \operatorname{Ass}(M) \subseteq \operatorname{Ass}(L) \cup \operatorname{Ass}(N)$.*

*Proof.* If $R/\mathfrak{p} \hookrightarrow L$, then composition with the inclusion $L \hookrightarrow M$ gives $R/\mathfrak{p} \hookrightarrow M$. Let $\mathfrak{p} \in \operatorname{Ass}(M) \smallsetminus \operatorname{Ass}(L)$, and let $\mathfrak{p} = \operatorname{ann}(m)$. Now, every submodule of $Rm$ consists of 0 and elements with annihilator $\mathfrak{p}$, so $Rm \cap L = 0$. Thus, $Rm \subseteq M$ bijects onto its image in $N$ in the map $M \to N$, so $R/\mathfrak{p} \hookrightarrow N$. □

**Theorem 5.15.** *If $R$ is a Noetherian ring, and $M$ is a finitely generated module, then there exists a* filtration *of $M$*

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

*such that $M_i/M_{i+1} \cong R/\mathfrak{p}_i$ for primes $\mathfrak{p}_i \in \operatorname{Spec}(R)$.*

*Proof.* If $M \neq 0$, then $M$ has an associated prime, so that $M_1 = R/\mathfrak{p}_1 \hookrightarrow M$. If $M/M_1 \neq 0$, it has an associated prime, so that $M_2/M_1 = R/\mathfrak{p}_2 \hookrightarrow R/M_1$. Pulling back to $M$, this process yields an ascending chain, so it must stop by hypothesis. □

Prime filtrations often allow us to reduce statements about finitely generated modules to statements about quotient domains of $R$: modules of the form $R/\mathfrak{p}$ for primes $\mathfrak{p}$. Here is a nice consequence of prime filtrations that we will generalize later.

**Corollary 5.16** (Generic freeness "junior")**.** *Let $R$ be a domain, and $M$ a finitely generated module. There exists some nonzero $f \in R$ such that $M_f$ is a free $R_f$ module.*

*Proof.* Take a prime filtration for $M$, and let $\mathfrak{p}_i$ be the nonzero primes that occur. Note that if $f \in \prod_i \mathfrak{p}_i$ (which contains a nonzero element since $R$ is a domain), then $(R/\mathfrak{p}_i)_f = 0$ for all $i$. Thus, in the filtration $(M_j)_f = (M_{j-1})_f$ for all $j$ except when $M_j/M_{j-1} \cong R$. We must have $(M_j)_f \cong (M_{j-1})_f \oplus R_f$ in this case, since $R_f$ is a projective $R_f$-module. We conclude that $M_f$ is free. □

**Corollary 5.17.** *If $R$ is a Noetherian ring, and $M$ is a finitely generated module, then* $|\operatorname{Ass}(R)| < \infty$.

*Proof.* We have $\operatorname{Ass}(M_i) \subseteq \operatorname{Ass}(M_{i-1}) \cup \operatorname{Ass}(R/\mathfrak{p}_i) = \operatorname{Ass}(M_{i-1}) \cup \{\mathfrak{p}_i\}$, so that, inductively, $\operatorname{Ass}(M_i) \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_i\}$. □

We will need that associated primes localize.

**Lemma 5.18.** *Let $R$ be a Noetherian ring, $W$ a multiplicative set, and $M$ a module. Then* $\operatorname{Ass}_{W^{-1}R}(W^{-1}M) = \{W^{-1}\mathfrak{p} \mid \mathfrak{p} \in \operatorname{Ass}_R(M), \mathfrak{p} \cap W = \varnothing\}$.

*Proof.* Given $\mathfrak{p} \in \operatorname{Ass}_R(M), \mathfrak{p} \cap W = \varnothing$, we have that $W^{-1}\mathfrak{p}$ is a prime (proper ideal) in $W^{-1}R$. Then $W^{-1}R/W^{-1}\mathfrak{p} \cong W^{-1}(R/\mathfrak{p}) \hookrightarrow W^{-1}M$ by exactness, so it is associated. Conversely, if $W^{-1}\mathfrak{p}$ is associated to $W^{-1}M$, there is an embedding $i : W^{-1}(R/\mathfrak{p}) \cong W^{-1}R/W^{-1}\mathfrak{p} \hookrightarrow W^{-1}M$. By the Noetherian hypothesis, since $R/\mathfrak{p}$ is finitely generated, Hom localizes: $W^{-1}\operatorname{Hom}_R(R/\mathfrak{p}, M) \cong \operatorname{Hom}_{W^{-1}R}(W^{-1}R/W^{-1}\mathfrak{p}, W^{-1}M)$, so the embedding we just found occurs as the localization of a map from $i' : R/\mathfrak{p} \to M$. Let $K = \ker(i')$. Since $W^{-1}K = 0$, every element of $K$ is killed by something in $W$. But, $K \subseteq R/\mathfrak{p}$, so elements of $W$ act as nonzerodivisors on $K$, hence, $K = 0$. Thus, $R/\mathfrak{p}$ injects into $M$, so $\mathfrak{p} \in \operatorname{Ass}_R(M)$. □

**Corollary 5.19.** *If $R$ is Noetherian and $M$ is an $R$-module, then* $\operatorname{Min}_R(M) \subseteq \operatorname{Ass}_R(M)$.

**Example 5.20.** Any subset $X \subseteq \operatorname{Spec}(R)$ (for any $R$) can be realized as $\operatorname{Ass}(M)$ for some $M$: take $M = \bigoplus_{\mathfrak{p} \in X} R/\mathfrak{p}$. Of course, if $X$ is infinite, $M$ is not finitely generated.

**Example 5.21.** If $R$ is not Noetherian, then there may be modules 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. 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 must be an annihilator of $x^{m/n} + (x)$ for some $m \leq n$. 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 $x^{1/2-m/2n}$.

**Remark 5.22.** We have that $\bigcap_{\mathfrak{p} \in \operatorname{Min}(R)} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \operatorname{Ass}(R)} \mathfrak{p} = \{\text{nilpotent elements}\}$ and $\bigcup_{\mathfrak{p} \in \operatorname{Ass}(R)} \mathfrak{p} = \{\text{zerodivisors}\}$. It's natural to ask what $\bigcup_{\mathfrak{p} \in \operatorname{Min}(R)} \mathfrak{p}$ is. We will have an interpretation before too long.

We take a quick detour to introduce an important lemma.

**Lemma 5.23** (Prime avoidance)**.** *Let $R$ be a ring, $I_1, \ldots, I_n, J$ be ideals, and suppose that $I_i$ is prime for $i > 2$ (at most two are not prime).*

*If $J \not\subseteq I_i$ for all $i$, then $J \not\subseteq \bigcup_i I_i$; equivalently, if $J \subseteq \bigcup_i I_i$, then $J \subseteq I_i$ for some $i$.*

*Moreover, if $R$ is $\mathbb{N}$-graded, and all of the ideals are homogeneous, all $I_i$ are prime, and $J \not\subseteq I_i$ for all $i$, then there is a homogeneous element in $J \smallsetminus \bigcup_i I_i$.*

*Proof.* We proceed by induction on $n$. If $n = 1$, there is nothing to show.

By induction hypothesis, we can find elements $a_i \in J \smallsetminus \bigcup_{j \neq i} I_j$ for each $i$. If some $a_i \notin I_i$, we are done, so suppose that $a_i \in I_i$ for each $i$. Consider $a = a_n + a_1 \cdots a_{n-1}$. This belongs to $J$. If $a \in I_i$ for $i < n$, then, since $a_1 \cdots a_{n-1} = a_i(a_1 \cdots \widehat{a_i} \cdots a_{n-1}) \in I_i$, we also have $a_n \in I_i$, a contradiction. If $a \in I_n$, then, since $a_n \in I_n$, we also have $a_1 \cdots a_{n-1} \in I_n$. If $n = 2$, this says $a_1 \in I_2$, a contradiction. If $n > 2$, then $I_n$ is prime, so one of $a_1, \dots, a_{n-1} \in I_n$, a contradiction.

If all $I_i$ are homogeneous and prime, we proceed as above, replacing $a_n$ and $a_1, \dots, a_{n-1}$ with suitable powers (e.g., $|a_1| + \cdots + |a_{n-1}|$ and $|a_n|$ each, respectively) so that $a_n + a_1 \cdots a_{n-1}$ is homogeneous. The primeness assumption guarantees that noncontainments in ideals is preserved. □

**Corollary 5.24.** *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 $m \in M$.*

*Proof.* We have that $I \subseteq \bigcup_{\mathfrak{p} \in \mathrm{Ass}(M)}(\mathfrak{p})$. By the assumptions, this is a finite set of primes. By prime avoidance, $I \subseteq \mathfrak{p}$ for some $\mathfrak{p} \in \mathrm{Ass}(M)$. That is $I \subseteq \mathrm{ann}_R(m)$ for some $m \in M$. □

## 5.3 Primary decomposition

We refine our decomposition theory once again.

**Definition 5.25.** *We say that an ideal is* primary *if $xy \in I \Rightarrow x \in I$ or $y \in \sqrt{I}$. We say that an ideal is* $\mathfrak{p}$-primary *if $I$ is primary and $\sqrt{I} = \mathfrak{p}$.*

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

**Example 5.26.**

1. If $R$ is a UFD, 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 $xy \in (f^n) \Leftrightarrow f^n | xy \Leftrightarrow f^n | x$ or $f | y \Leftrightarrow x \in (f^n)$ or $y \in \sqrt{(f^n)} = (f)$. Conversely, if $a = gh$, for some $g$, $h$ with no common factor, then take $gh \in (a)$ but $g \notin a$ and $h \notin \sqrt{(a)}$.

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

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

The definition of primary can be reinterpreted in many forms.

**Proposition 5.27.** *The following are equivalent:*

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

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

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

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

5. *$\sqrt{\mathfrak{q}} = \mathfrak{p}$ is prime and $\mathfrak{q}$ is saturated with respect to the multiplicative set $(R \setminus \mathfrak{p})$.*

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

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

(2) $\iff$ (3): (2) translates to $\bigcup_{\mathfrak{p}\in \operatorname{Ass}(R/\mathfrak{q})} \mathfrak{p} = \bigcap_{\mathfrak{p}\in \operatorname{Ass}(R/\mathfrak{q})} \mathfrak{p}$. This holds is and only if there is one associated prime.

(3) $\iff$ (4): is clear.

(1) $\iff$ (5): The saturation condition just means $xy \in \mathfrak{q}$, $y \notin \mathfrak{p}$ implies $x \in \mathfrak{p}$, which is the definition.

(5) $\iff$ (6): We already know this. □

Next, we observe:

**Lemma 5.28.** *If $I_1, \ldots, I_t$ are ideals, then $\operatorname{Ass}(R/(\bigcap_{j=1}^t I_j)) \subseteq \bigcup_{j=i}^t \operatorname{Ass}(R/I_j)$. In particular, a finite intersection of $\mathfrak{p}$-primary ideals is $\mathfrak{p}$-primary.*

*Proof.* Recall that there is an injection $R/(I_1 \cap I_2) \hookrightarrow R/I_1 \oplus R/I_2$. Hence, $\operatorname{Ass}(R/(I_1 \cap I_2)) \subseteq \operatorname{Ass}(R/I_1) \cup \operatorname{Ass}(R/I_2)$; the statement for larger $t$ is an obvious induction.

The latter statement follows from characterization #3 above. □

**Definition 5.29** (Primary decomposition)**.** *A* primary decomposition *of an ideal $I$ is an expression of the form*

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t,$$

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

By the previous lemma, we can turn a primary decomposition into a minimal one by combining the terms with the same radical, then removing redundant terms.

**Theorem 5.30** (Existence of primary decompositions)**.** *If $R$ is Noetherian, then every ideal of $R$ admits a primary decomposition.*

*Proof.* We will say that an ideal is irreducible if it cannot be written as a proper intersection of larger ideals. If $R$ is Noetherian, any ideal of $R$ can be expressed as a finite intersection of irreducible ideals: if not, there would be an ideal maximal with the property of not being an intersection of irreducible ideals, which must be an intersection of two larger ideals, each of with are finite intersections of irreducibles, giving a contradiction.

Now, we claim that every irreducible ideal is primary. To establish the contrapositive, take $xy \in \mathfrak{q}$ with $x \notin \mathfrak{q}$, $y \notin \sqrt{\mathfrak{q}}$. The ascending chain of ideals $J_n = (\mathfrak{q} : y^n)$ stabilizes for some $n$. We will show that $(\mathfrak{q} + (y^n)) \cap (\mathfrak{q} + (x)) = \mathfrak{q}$.

The containment $\mathfrak{q} \subseteq (\mathfrak{q} + (y^n)) \cap (\mathfrak{q} + (x))$ is clear. If $a$ is in the RHS, we have $a = q + by^n$ for some $q \in \mathfrak{q}$, and $ya \in \mathfrak{q}$, so $by^{n+1} \in \mathfrak{q}$. Then, $b \in (\mathfrak{q} : y^{n+1}) = (\mathfrak{q} : y^n)$, so $by^n \in \mathfrak{q}$, and hence $a \in \mathfrak{q}$, as required. This shows that $\mathfrak{q}$ is decomposable, concluding the proof. □

There are also some uniqueness theorems for primary decomposition.

**Theorem 5.31** (First uniqueness theorem for primary decompositions)**.** *If $I$ is an ideal in a Noetherian ring $R$, then for any minimal primary decomposition of $I$, $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$, we have $\{\sqrt{\mathfrak{q}_1}, \ldots, \sqrt{\mathfrak{q}_t}\} = \operatorname{Ass}(R/I)$. In particular, this set is the same for all minimal primary decompositions of $I$.*

*Proof.* For any primary decomposition (minimal or not), we have $\operatorname{Ass}(R/I) \subseteq \bigcup_i \operatorname{Ass}(R/\mathfrak{q}_i) = \{\sqrt{\mathfrak{q}_1}, \dots, \sqrt{\mathfrak{q}_t}\}$ from the lemma on intersections above. We just need to show that in a minimal decomposition, every associated prime occurs are the radical of some component.

Let $I_j = \bigcap_{i \neq j} \mathfrak{q}_i \supseteq I$. Since the decomposition is minimal, the module $I_j/I$ is nonzero, hence has an associated prime $\mathfrak{p}$. Let $\mathfrak{p}$ be the annihilator of $\overline{x_j}$ in $I_j/I$, with $x_j \in R$. Since $\mathfrak{q}_j x_j \subseteq I$, we have that $\mathfrak{q}_j$ is contained in the annihilator of $\overline{x_j}$, and since $\mathfrak{p}_j$ is the unique minimal prime of $\mathfrak{q}_j$, $\mathfrak{p}_j \subseteq \operatorname{ann}_R(\overline{x_j})$. On the other hand, if $r \in \operatorname{ann}_R(\overline{x_j})$, we have $rx_j \in \mathfrak{q}_j$, and since $x_j \notin \mathfrak{q}_j$, we must have $r \in \mathfrak{p}_j$ by the definition of primary. □

We note that if we don't assume that $R$ is Noetherian, we may or may not have a primary decomposition for a given ideal. It is true that if an ideal $I$ in a general ring has a primary decomposition, then the primes occurring are the same in any minimal decomposition. However, they are not the associated primes in general; rather, they are the primes that occur as radicals of annihilators of elements.

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

**Theorem 5.32** (Second uniqueness theorem for primary decompositions). *If $I$ is an ideal in a Noetherian ring $R$, then for any minimal primary decomposition of $I$, $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$, the set of* minimal components $\{\mathfrak{q}_i \mid \sqrt{\mathfrak{q}_i} \in \operatorname{Min}(R/I)\}$ *is the same. Namely, $\mathfrak{q}_i = IR_{\sqrt{\mathfrak{q}_i}} \cap R$.*

*Proof.* We observe that a localization $\mathfrak{q}_\mathfrak{a}$ of a $\mathfrak{p}$-primary ideal $\mathfrak{q}$ is either the unit ideal (if $\mathfrak{a} \not\supseteq \mathfrak{p}$), or is a $\mathfrak{p}_\mathfrak{a}$-primary ideal: this follows from the fact that the associated primes of $R/\mathfrak{q}$ localize.

Now, since finite intersections commute with localization, for any prime $\mathfrak{a}$, we have

$$I_\mathfrak{a} = (\mathfrak{q}_1)_\mathfrak{a} \cap \cdots \cap (\mathfrak{q}_t)_\mathfrak{a}$$

is a (not necessarily minimal) primary decomposition. In a minimal decomposition, choose a minimal prime $\mathfrak{a} = \mathfrak{p}_i$ to get $I_{\mathfrak{p}_i} = (\mathfrak{q}_i)_{\mathfrak{p}_i}$; the other components in the intersection become the unit ideal since their radicals are not contained in $\mathfrak{p}_i$. We can then contract to $R$ to get $I_{\mathfrak{p}_i} \cap R = (\mathfrak{q}_i)_{\mathfrak{p}_i} \cap R = \mathfrak{q}_i$, since $\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary. □

We record the following corollary of the primary decomposition theorem.

**Theorem 5.33** (Krull intersection theorem). *Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring. Then $\bigcap_{n \in \mathbb{N}} \mathfrak{m}^n = 0$.*

*Proof.* Let $J = \bigcap_{n \in \mathbb{N}} \mathfrak{m}^n$. We will show that $J \subseteq \mathfrak{m}J$, hence $J = \mathfrak{m}J$, and thus $J = 0$ by NAK.

Let $\mathfrak{m}J = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$ be a primary decomposition. We claim that $J \subseteq \mathfrak{q}_i$ for each $i$. If $\sqrt{\mathfrak{q}_i} \neq \mathfrak{m}$, pick $x \in \mathfrak{m} \smallsetminus \sqrt{\mathfrak{q}_i}$. We have $xJ \subseteq \mathfrak{m}J \subseteq \mathfrak{q}_i$, with $x \notin \sqrt{\mathfrak{q}_i}$, so $J \subseteq \mathfrak{q}_i$ by definition of primary. If instead $\sqrt{\mathfrak{q}_i} = \mathfrak{m}$, each generator of $\mathfrak{m}$ has a power in $\mathfrak{q}_i$, and $\mathfrak{m}$ is finitely generated, so there is some $N$ with $\mathfrak{m}^N \subseteq \mathfrak{q}_i$. We then have $J \subseteq \mathfrak{m}^N \subseteq \mathfrak{q}_i$, and we are done. □

**Definition 5.34** (Symbolic power). *If $\mathfrak{p}$ is a prime ideal in a ring $R$, the $n$th* symbolic power *of $\mathfrak{p}$ is $\mathfrak{p}^{(n)} := \mathfrak{p}^n R_\mathfrak{p} \cap R$.*

This admits equivalent characterizations.

**Proposition 5.35.** *Let $R$ be Noetherian, and $\mathfrak{p}$ a prime ideal of $R$.*

1. $\mathfrak{p}^{(n)} = \{r \in R \mid \exists s \notin \mathfrak{p} : rs \in \mathfrak{p}^n\}$.

2. $\mathfrak{p}^{(n)}$ *is the unique smallest* $\mathfrak{p}$*-primary ideal containing* $\mathfrak{p}^n$*.*

3. $\mathfrak{p}^{(n)}$ *is the* $\mathfrak{p}$*-primary component in any minimal primary decomposition of* $\mathfrak{p}^n$*.*

*Proof.* The first characterization follows from the definition, and the fact that expanding and contraction to/from a localization is equivalent to saturating with respect to the multiplicative set.

We know that $\mathfrak{p}^{(n)}$ is $\mathfrak{p}$-primary from a characterization of primary above. Any $\mathfrak{p}$-primary ideal satisfies $\mathfrak{q}R_\mathfrak{p} \cap R = \mathfrak{q}$, and if $\mathfrak{q} \supseteq \mathfrak{p}^n$, then $\mathfrak{p}^{(n)} = \mathfrak{p}^n R^\mathfrak{p} \cap R \subseteq \mathfrak{q}R_\mathfrak{p} \cap R = \mathfrak{q}$. Thus, $\mathfrak{p}^{(n)}$ is the unique smallest $\mathfrak{p}$-primary ideal containing $\mathfrak{p}^n$.

The last characterization follows from the second uniqueness theorem above. □

**Example 5.36.** 1. In $R = K[x, y, z]$, $\mathfrak{p} = (y, z)$, we have $\mathfrak{p}^{(n)} = \mathfrak{p}^n$ for all $n$. This follows along the same lines as an example above.

2. In $R = K[x, y, z] = (xy - z^2)$, $\mathfrak{p} = (y, z)$, we have $\mathfrak{p}^(2) \neq \mathfrak{p}^2$. Indeed, $xy = z^2 \in \mathfrak{p}^2$, and $x \notin \mathfrak{p}$, so $y \in \mathfrak{p}^{(2)} \setminus \mathfrak{p}^2$.

3. Let $X = X_{3\times 3}$ be a $3 \times 3$ matrix of indeterminates, and $K[X]$ be a polynomial ring over a field $K$. Let $\mathfrak{p} = I_2(X)$ be the ideal generated by $2 \times 2$ minors of $X$. We will write $\Delta_{\substack{i|k\\j|l}}$ for the determinant of the submatrix with rows $i, j$ and columns $k, l$. We find

$$\begin{aligned} x_{11}\det(X) &= x_{11}x_{31}\Delta_{\substack{1|2\\2|3}} - x_{11}x_{32}\Delta_{\substack{1|1\\2|3}} + x_{11}x_{33}\Delta_{\substack{1|1\\2|2}} \\ &= (x_{11}x_{31}\Delta_{\substack{1|2\\2|3}} - x_{11}x_{32}\Delta_{\substack{1|1\\2|3}} + x_{11}x_{33}\Delta_{\substack{1|1\\2|2}}) - (x_{11}x_{31}\Delta_{\substack{1|2\\2|3}} - x_{12}x_{31}\Delta_{\substack{1|1\\2|3}} + x_{13}x_{31}\Delta_{\substack{1|1\\2|2}}) \\ &= -\Delta_{\substack{1|1\\3|2}}\Delta_{\substack{1|1\\2|3}} + \Delta_{\substack{1|1\\3|3}}\Delta_{\substack{1|1\\2|2}} \in I_2(X)^2. \end{aligned}$$

Note that in the second row, we subtracted the Laplace expansion of determinant of the matrix with row 3 replaced by another copy of row 1. That is, we subtracted zero.

# Chapter 6

# Spec and dimension

## 6.1 Dimension and height

**Definition 6.1.**

- *A* chain of primes *of* length $n$ *in a ring* $R$ *is*

$$\mathfrak{a}_0 \subsetneq \mathfrak{a}_1 \subsetneq \cdots \subsetneq \mathfrak{a}_n \quad \textit{with } \mathfrak{a}_i \in \operatorname{Spec}(R).$$

- *A chain of primes as above is* saturated *if for each* $i$*, there is no* $\mathfrak{q} \in \operatorname{Spec}(R)$ *with* $\mathfrak{a}_i \subsetneq \mathfrak{q} \subsetneq \mathfrak{a}_{i+1}$.

- *The* dimension *or* Krull dimension *of a ring* $R$ *is the supremum of the lengths of chains of primes in* $R$*. Equivalently, it is the supremum of the lengths of saturated chains of primes in* $R$*.*

- *The* height *of a prime* $\mathfrak{p}$ *is the supremum of the lengths of chains of primes in* $R$ *that end in* $\mathfrak{p}$ *(i.e.,* $\mathfrak{p} = \mathfrak{a}_n$ *above). Equivalently, it is the supremum of the lengths of saturated chains of primes in* $R$ *that end in* $\mathfrak{p}$*.*

- *The* height *of an ideal* $I$ *is the infimum of the heights of the minimal primes of* $I$*.*

To get a feel for these definitions, we make a sequence of easy observations.

1. If $\mathfrak{p}$ is prime, then $\dim(R/\mathfrak{p})$ is the supremum of the lengths of (saturated) chains of primes in $R$
$$\mathfrak{a}_0 \subsetneq \mathfrak{a}_1 \subsetneq \cdots \subsetneq \mathfrak{a}_n$$
with each $\mathfrak{a}_i \in V(\mathfrak{p})$.

2. If $I$ is an ideal, then $\dim(R/I)$ is the supremum of the lengths of (saturated) chains of primes in $R$
$$\mathfrak{a}_0 \subsetneq \mathfrak{a}_1 \subsetneq \cdots \subsetneq \mathfrak{a}_n$$
with each $\mathfrak{a}_i \in V(I)$.

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

4. If $\mathfrak{p}$ is prime, then $\operatorname{height}(\mathfrak{p}) = \dim(R_{\mathfrak{p}})$.

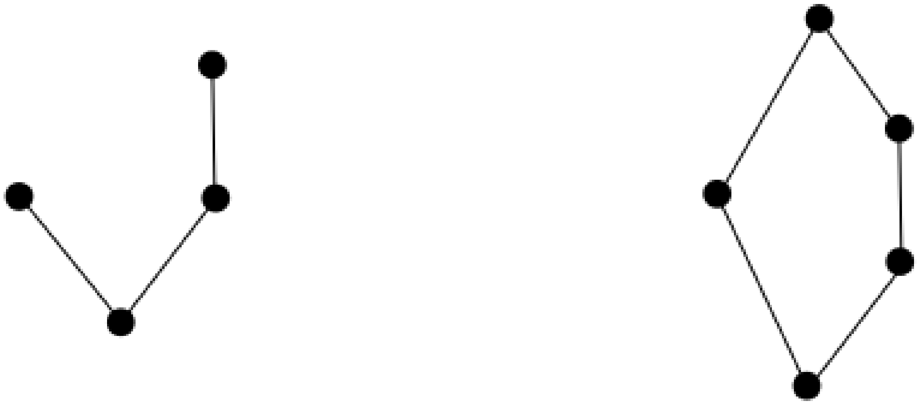

Figure 6.1: Some failures of equality in 8

5. If $\mathfrak{q} \supseteq \mathfrak{p}$ are primes, then $\dim(R_{\mathfrak{q}}/\mathfrak{p}R_{\mathfrak{q}})$ is the supremum of the lengths of (saturated) chains of primes in $R$
$$\mathfrak{a}_0 \subsetneq \mathfrak{a}_1 \subsetneq \cdots \subsetneq \mathfrak{a}_n$$
with $\mathfrak{a}_0 = \mathfrak{p}$ and $\mathfrak{a}_n = \mathfrak{q}$.

6. $\dim(R) = \sup\{\mathrm{height}(\mathfrak{m}) \mid \mathfrak{m} \in \mathrm{Max}(R)\}$.

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

8. If $\mathfrak{p}$ is prime, $\dim(R/\mathfrak{p}) + \mathrm{height}(\mathfrak{p}) \leq \dim(R)$.

9. If $I$ is an ideal, $\dim(R/I) + \mathrm{height}(I) \leq \dim(R)$.

10. A prime has height zero if and only if it is a minimal prime.

11. The dimension of a field is zero.

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

13. The ring of integers $\mathbb{Z}$ has dimension one.

14. It follows from the definition that $\dim(K[x_1, \ldots, x_d]) \geq d$, since there is a saturated chain of primes $(0) \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \cdots \subsetneq (x_1, \ldots, x_d)$.

We observe that the inequalities we gave in 8 and 9 above are not obviously equalities. Figure 6.1 gives two posets where the dot on the left would yield a strict inequality on 8.

**Definition 6.2.**

- *A ring is* ***catenary*** *if for every pair of primes $\mathfrak{q} \supseteq \mathfrak{p}$ in $R$, every saturated chain of primes*
$$\mathfrak{a}_0 \subsetneq \mathfrak{a}_1 \subsetneq \cdots \subsetneq \mathfrak{a}_n$$
*with $\mathfrak{a}_0 = \mathfrak{p}$ and $\mathfrak{a}_n = \mathfrak{q}$ 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.*

The left diagram corresponds to something that is not equidimensional. The right diagram corresponds to something that is not catenary.

We collect some more basics.

1. $\dfrac{K[x,y,z]}{(xy,xz)}$ is not equidimensional: 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 just one element since this is a PID. The height of $(x,y-1,z)$ is at least two, as witnessed by the chain $(x) \subsetneq (x,y-1) \subsetneq (x,y-1,z)$.

2. If $(R,\mathfrak{m})$ is a catenary local domain, then for any $\mathfrak{p} \in \operatorname{Spec}(R)$, $\dim(R/\mathfrak{p}) + \operatorname{height}(\mathfrak{p}) = \dim(R)$.

3. $\mathbb{Z}_{(2)}[x]$ is a domain that is not equidimensional: consider the maximal ideal $(2,x)$ that has height at least two, and the maximal ideal $(2x-1)$; this is maximal since the quotient is $\mathbb{Q}$!

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

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

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

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

8. If $R$ is a UFD, $I$ is a prime of height one if and only if $I=(f)$ for a prime element $f$.

The one warning to make about dimension before we get too optimistic is that there are Noetherian rings of infinite dimension.

**Example 6.3.** Let $R = K[x_1,x_2,\dots]$. $R$ is clearly infinite-dimensional, but is not Noetherian. Let

$$W = R \smallsetminus ((x_1) \cup (x_2,x_3) \cup (x_4,x_5,x_6) \cdots)$$

and $S = W^{-1}R$. This ring has primes of arbitrarily large height, given by the images of those primes we cut out from $W$. Thus, it has infinite dimension. The work is to show that this ring is Noetherian. Do it!

## 6.2 Over, up, down theorems

In this section, we will collect theorems of three forms about the spectrum of a ring: theorems that assert that the map on Spec is surjective, and theorems about lifting chains of primes.

Recall that the fiber ring over $\mathfrak{p}$ of a homomorphism $\varphi : R \to S$ is given by

$$\kappa_\varphi(\mathfrak{p}) = (R \smallsetminus \mathfrak{p})^{-1}(S/\mathfrak{p}S),$$

and that

$$\operatorname{Spec}(\kappa_\varphi(\mathfrak{p})) \cong (\varphi^*)^{-1}(\mathfrak{p}),$$

the subspace of $\operatorname{Spec}(S)$ consisting of primes that contract to $\mathfrak{p}$. As a special case, we write $\kappa(\mathfrak{p})$ for the fiber of the identity map; this is $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$, the residue field of the local ring $R_\mathfrak{p}$.

**Lemma 6.4** (Image criterion)**.** *Let $\varphi : R \to S$ be a ring homomorphism, and $\mathfrak{p} \in \operatorname{Spec}(R)$. Then $\mathfrak{p} \in \operatorname{im}(\varphi^*)$ if and only if $\mathfrak{p}S \cap R = \mathfrak{p}$.*

*Proof.* If $\mathfrak{p}S \cap R = \mathfrak{p}$, then

$$\frac{R}{\mathfrak{p}} = \frac{R}{\mathfrak{p}S \cap R} \hookrightarrow \frac{S}{\mathfrak{p}S},$$

so, localizing at $(R \smallsetminus \mathfrak{p})$, we get an injection $\kappa(\mathfrak{p}) \hookrightarrow \kappa_\varphi(\mathfrak{p})$. The latter ring is nonzero, so its spectrum is nonempty. Thus, there is a prime mapping to $\mathfrak{p}$.

If $\mathfrak{p}S \cap R \neq \mathfrak{p}$, then $\mathfrak{p}S \cap R \supsetneq \mathfrak{p}$ (the other containment always holds). Then, is $\mathfrak{q} \cap R = \mathfrak{p}$, we have $\mathfrak{q} \supseteq \mathfrak{p}S$, so $\mathfrak{q} \cap R \supsetneq \mathfrak{p}$. □

Note that $\mathfrak{p}S$ may not be prime, in general.

**Example 6.5.** Let $R = \mathbb{C}[x^n] \subseteq S = \mathbb{C}[x]$. The ideal $(x^n - 1)R$ is prime, while $(x^n-1)S = (\prod_{i=0}^{n-1} x - \zeta^i)S$ is not. However, each of its minimal primes $(x - \zeta^i)S$ contracts to $(x^n - 1)R$.

**Corollary 6.6.** *If $R \subseteq S$ is a direct summand, then $\operatorname{Spec}(S) \to \operatorname{Spec}(R)$ is surjective.*

*Proof.* From the homework, we know that $IS \cap R = I$ for all ideals in this case. □

We want to extend the idea of the last corollary to work for all integral extensions. The key idea is encapsulated in a definition.

**Definition 6.7.** *Let $R$ be a ring, $S$ an $R$-algebra, and $I$ an ideal.*

- *An element $r$ of $R$ is* integral *over $I$ if it satisfies an equation of the form*

$$r^n + a_1 r^{n-1} + \cdots + a_{n-1} r + a_n = 0 \qquad \text{with } a_i \in I^i \text{ for all } i.$$

- *An element of $S$ is integral over $I$ if the same condition holds (with $a_i$ replaced by their images in $S$).*
- *The* integral closure *of $I$ in $R$ is $\overline{I}$, the set of elements of $R$ that are integral over $I$.*
- *Similarly, we write $\overline{I}^S$ for the integral closure of $I$ in $S$.*

We leave a little exercise for you.

**Exercise 6.8.** Let $R \subseteq S$, $I$ be an ideal of $S$, and $t$ be an indeterminate. Consider the rings $R[It] \subseteq R[t] \subseteq S[t]$.

1. $\overline{I}^S = \{s \in S \mid st \in S[t] \text{ is integral over the ring } R[It]\}$.
2. $\overline{I}^S$ is an ideal.

We note that in older texts and papers (e.g., Atiyah-Macdonald and Kunz) a different definition is given for integral closure of an ideal. The one we use here is more-or-less universally accepted as the correct notion.

**Lemma 6.9** (Extension-contraction lemma for integral extensions)**.** *Let $R \subseteq S$ be integral, and $I$ be an ideal of $R$. Then, $IS \subseteq \overline{I}^S$. Hence, $IS \cap R \subseteq \overline{I}$.*

*Proof.* Let $x \in IS$. We can write $x = \sum_{i=1}^{t} a_i s_i$ with $a_i \in I$. Taking $S' = R[s_1, \dots, s_t]$, we also have $x \in IS'$. Thus, it suffices to show the statements in the case $S$ is module-finite over $R$.

Let $S = \sum Rb_i$. We have $xb_i = (\sum_k a_k s_k)b_i = \sum_j a_{ij} b_j$ with $a_{ij} \in I$. We can write this as a matrix equation $xIv = Av$, where $v = (b_1, \dots, b_u)$, and $A = [a_{ij}]$. By the adjoint trick, 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.

The last statement follows from the fact that $\overline{I}^S \cap R = \overline{I}$, which is immediate from the definition. □

**Theorem 6.10** (Lying over). *If $R \subseteq S$ is an integral inclusion, then* $\operatorname{Spec}(S) \to \operatorname{Spec}(R)$ *is surjective.*

*Proof.* We observe that $\overline{I} \subseteq \sqrt{I}$. Thus, for $\mathfrak{p}$ prime, by the previous lemma, $\mathfrak{p}S \cap R = \mathfrak{p}$, and the result follows from the image criterion. □

**Remark 6.11.** Both "integral" and "inclusion" are important: the map $R \to R_f$ is a nonintegral inclusion if $f$ is a nonzerodivisor, and the image is the complement of $V(f)$; the map $R \to R/(f)$ is an integral noninclusion, and the the image is $V(f)$.

**Theorem 6.12** (Incomparability). *If $\varphi : R \to S$ is integral, and $\mathfrak{q} \subseteq \mathfrak{q}'$ are such that $\varphi^*(\mathfrak{q}) = \varphi^*(\mathfrak{q}')$, then $\mathfrak{q} = \mathfrak{q}'$.*

*Proof.* Since the map $R \to R/\ker(R)$ is injective on spectra, we can replace $R$ by the quotient and assume $\varphi$ is an integral inclusion.

Now, if $R \hookrightarrow S$ is integral, then $R/\mathfrak{p} \hookrightarrow S/\mathfrak{p}S$ (injective by the lemma above) is integral; take an integral equation for a representative. Furthermore, localizing at $(R \smallsetminus \mathfrak{p})$ preserves integrality. We then have that $\kappa(\mathfrak{p}) \hookrightarrow \kappa_\varphi(\mathfrak{p})$ is integral. If $\mathfrak{q}$ is a prime of $\kappa_\varphi(\mathfrak{p})$, then $\kappa(\mathfrak{p}) \subseteq \kappa_\varphi(\mathfrak{p})/\mathfrak{q}$ is integral, and by a lemma from a while ago, we must have that $\kappa_\varphi(\mathfrak{p})/\mathfrak{q}$ is a field. Therefore, every ideal of $\mathfrak{q}$ is maximal (and hence every ideal is minimal). Since there are no inclusions between primes in $\kappa_\varphi(\mathfrak{p})$, there are no inclusions between primes that contract to $\mathfrak{p}$. □

**Corollary 6.13.** *If $R \to S$ is integral, and $S$ is Noetherian, then for any $\mathfrak{p} \in \operatorname{Spec}(R)$, only finitely many primes contract to $\mathfrak{p}$.*

*Proof.* This is more a corollary of the proof: in this case the ring $\kappa_\varphi(\mathfrak{p})$ of any prime is also Noetherian, hence has finitely many minimal primes. Every prime of the fiber is minimal, though. □

**Remark 6.14.** Again, hypotheses matter! The fiber over $\mathfrak{p}$ for the inclusion $R \to R[x]$ contains the incomparable $\mathfrak{p}[x]$ and $\mathfrak{p}[x] + (x)$.

**Remark 6.15.** If $\phi : R \to S$ is module-finite, and $S$ is generated by $t$ elements as an $R$-module, write $S = \sum_{i=1}^{t} Rf_i$. Then, we also have $\kappa_\phi = \sum_{i=1}^{t} \kappa(\mathfrak{p})\bar{f}_i/1$, and hence $\kappa_\phi$ is a $\kappa(\mathfrak{p})$ vector space of dimension at most $t$. We will see soon that such a ring can have at most $t$ maximal ideals (or you can prove it now!), and thus every fiber of the map contains at most $t$ primes!

**Corollary 6.16.** *If $R \to S$ is integral, then* $\operatorname{height}(\mathfrak{q}) \leq \operatorname{height}(\mathfrak{q} \cap R)$ *for any* $\mathfrak{q} \in \operatorname{Spec}(S)$. *In particular,* $\dim(S) \leq \dim(R)$.

**Theorem 6.17** (Going up). *If $R \to S$ is integral, then for every $\mathfrak{p} \subsetneq \mathfrak{p}'$ in* $\operatorname{Spec}(R)$ *and $\mathfrak{q}$ in* $\operatorname{Spec}(S)$ *with $\mathfrak{q} \cap R = \mathfrak{p}$, there is some $\mathfrak{q}' \in \operatorname{Spec}(S)$ with $\mathfrak{q} \subsetneq \mathfrak{q}'$ and $\mathfrak{q}' \cap R = \mathfrak{p}'$.*

*Proof.* Exercise. (This is easy.) □

**Corollary 6.18.** *If $R \subseteq S$ is integral, then* $\dim(R) = \dim(S)$.

**Lemma 6.19.** *Let $R$ be a normal domain, $x$ be an element integral over $R$ in some larger domain. Let $K$ be the fraction field of $R$, and $f(t) \in K[t]$ be the minimal polynomial of $x$ over $K$.*

1. *If $x$ is integral over $R$, then $f(t) \in R[t] \subseteq K[t]$.*

2. *If $x$ is integral over a prime $\mathfrak{p}$, then $f(t)$ has all of its nonleading coefficients in $\mathfrak{p}$.*

*Proof.* Let $x$ be integral over $R$. Fix an algebraic closure of $K$ containing $x$, and let $x_1 = x, x_2, \ldots, x_u$ be the roots of $f$. Since $f(t)$ divides a monic equation for $x$, each $x_i$ is 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 coefficients of $f(t)$ are elementary symmetric polynomials in the $x$'s, hence they lie in $S$. But, $S \cap K = R$ since $R$ is normal. Thus, the first statement holds.

Now, let $x$ be integral over $\mathfrak{p}$. All of the $x$'s are integral over $\mathfrak{p}$ by the same argument as above. Since each $x_j \in \overline{\mathfrak{p}}^S$, any elementary symmetric polynomial in the $x$'s lies in $\overline{\mathfrak{p}}^S$. Thus, the nonleading coefficients lie in $\overline{\mathfrak{p}}^S \cap R = \mathfrak{p}$. □

**Theorem 6.20** (Going down)**.** *If $R$ is a normal domain, $S$ is a domain, and $R \subseteq S$ is integral, then for every $\mathfrak{p}' \subsetneq \mathfrak{p}$ in* $\operatorname{Spec}(R)$ *and $\mathfrak{q}$ in* $\operatorname{Spec}(S)$ *with $\mathfrak{q} \cap R = \mathfrak{p}$, there is some $\mathfrak{q}' \in \operatorname{Spec}(S)$ with $\mathfrak{q}' \subsetneq \mathfrak{q}$ and $\mathfrak{q}' \cap R = \mathfrak{p}'$.*

*Proof.* Let $W = (S \smallsetminus \mathfrak{q})(R \smallsetminus \mathfrak{p}')$ be the multiplicative set consisting of products of elements in $S \smallsetminus \mathfrak{q}$ and $R \smallsetminus \mathfrak{p}'$. Note that each of these sets contains 1, so each set is in the product. We want to show that $W \cap \mathfrak{p}'S$ is empty. It will follow that $W^{-1}(S/\mathfrak{p}'S) = (S \smallsetminus \mathfrak{q})^{-1}\kappa_S(\mathfrak{p}')$ has a prime ideal, and hence there is a prime of $S$ contained in $\mathfrak{q}$ contracting to $\mathfrak{p}'$.

To that end, suppose $x \in \mathfrak{p}'S \cap W$. Since $x \in \mathfrak{p}'S$, it is integral over $\mathfrak{p}'$, so write $x = rs$ with $r \in R \smallsetminus \mathfrak{p}', s \in S \smallsetminus \mathfrak{q}$, and consider the minimal polynomial of $x$ over $\operatorname{frac}(R)$:

$$h(x) = x^n + a_1 x^{n-1} + \cdots + a_n = 0.$$

By the lemma above, each $a_i \in \mathfrak{p}' \subseteq R$. Then, since $r \in K$, substituting $x = rs$ yields and dividing by $r^n$ yields a polynomial that, viewed as a polynomial in $s$, is irreducible. That is, the minimal polynomial of $s$ is

$$g(s) = s^n + \frac{a_1}{r}s^{n-1} + \cdots + \frac{a_n}{r^n} = 0.$$

Since $s \in S$, hence is integral over $R$, the lemma above says that each $\frac{a_i}{r^i} =: v_i \in R$. Since $r \notin \mathfrak{p}'$, and $r^i v_i = a_i \in \mathfrak{p}'$, we have $v_i \in \mathfrak{p}'$, and the equation $g(s) = 0$ then shows that $s \in \sqrt{\mathfrak{p}'S}$. Since $\mathfrak{q} \in \operatorname{Spec}(S)$ contains $\mathfrak{p}S$ and hence $\mathfrak{p}'S$, we have $s \in \sqrt{\mathfrak{p}'S} \subseteq \mathfrak{q}$. This is the desired contradiction. □

**Remark 6.21.** We have used the fact that our rings are domains to put the theory of minimal polynomials to use. The one hypothesis we can weaken is that the target is a domain: it suffices to assume that it is torisonfree as a module over the source. Here's why we can't get rind of more hypotheses.

Let $R = K[x] \subseteq S = K[x,y]/(xy, y^2 - y)$. $R$ is a normal domain, and the inclusion is integral: $y^2 - y = 0$ is an integral dependence relation for $y$ over $R$, so $S$ is generated by one integral element. Now, $(1 - y)$ is a minimal prime of $S$: $y \in S \smallsetminus (1 - y)$, so $x$ goes to zero in the localization (since $xy = 0$) and $1 - y$ goes to zero in the localization (since $y(1 - y) = 0$), so the localization is a copy of $K$, which has only one prime, $(0)$. We have $x = x - xy = x(1-y) \in (1-y)$, so the contraction contains $(x)$, so must be $(x)$. But, by minimality, we can't "go down" from $(1-y)$ to a prime lying over $(0)$.

The normality hypothesis is important too. Take $R = K[x(1-x), x^2(1-x), y, xy] \subseteq S = K[x,y]$. The element $x$ is integral over $R$: $x(1-x) \in R$ is a recipe: $x$ is a root of $z^2 - z - x(1-x)$. Note that $x$ is in the fraction field of $R$, so this element shows both that $S$ is integral over $R$, and that $R$ is not normal. Now, $\mathfrak{q} = (1-x, y) \subseteq S$ is a maximal ideal lying over the maximal ideal $\mathfrak{p}$ generated by the specified generating set in $R$. We have $xS \cap R = (x(1-x), x^2(1-x), xy)R = \mathfrak{p}'$, but we claim that no prime contained in $\mathfrak{q}$ lies over $\mathfrak{p}'$. Such a prime must contain $x(1-x)$ and $xy$, but not $x$ (this would make it the unit ideal), so must contain $y$ and $1-x$, and the contraction is then $\mathfrak{p}$, which is too big!

**Corollary 6.22.** *If $R$ is a normal domain, $S$ is a domain, and $R \subseteq S$ is integral, then* $\operatorname{height}(\mathfrak{q}) = \operatorname{height}(\mathfrak{q} \cap R)$ *for any* $\mathfrak{q} \in \operatorname{Spec}(S)$.

*Proof.* We already know that $\operatorname{ht}(\mathfrak{q}) \leq \operatorname{ht}(\mathfrak{q} \cap R)$ (by taking a maximal chain up to $\mathfrak{q}$ and applying incomparability to the contractions). Now, take a maximal chain up to $\mathfrak{q} \cap R$, and apply going down to get a chain just as long that goes up to $\mathfrak{q}$. □

## 6.3 Noether normalization and dimension of affine rings

**Lemma 6.23** (Making a pure-power leading term). *1. Let $A$ be a domain, and $f \in R = A[x_1, \ldots, x_n]$ be a (not necessarily homogeneous) polynomial of degree at most $N$. The $A$-algebra automorphism of $R$ given by $\phi(x_i) = x_i + x_n^{N^{n-i}}$ for $i < n$ and $\phi(x_n) = x_n$ maps $f$ to a polynomial that, viewed as a polynomial in $x_n$ with coefficients in $A[x_1, \ldots, x_{n-1}]$, has leading term $dx_n^a$ for some $d \in A$, $a \in \mathbb{N}$.*

*2. Let $K$ be an infinite field, and $f \in R = K[x_1, \ldots, x_n]$ 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 $kx_n^N$ for some $k \in K$.*

*Proof.* 1. The map $\phi$ sends a monomial term $dx_1^{a_1} \cdots x_n^{a_n}$ to a polynomial with unique highest degree term $dx_n^{a_1 N^{n-1} + a_2 N^{n-2} + \cdots + a_{n-1}N + a_n}$. Since each $a_i$ is less than $N$ in each monomial, 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; thus, none of the terms can cancel. We find that the leading term is of the promised form.

2. We just need to show that the $x^N$ coefficient is nonzero for some choice of $a$'s. You can check that the coefficient of the $x^N$ term is $f(-a_1, \ldots, -a_{n-1}, 1)$. But if this, thought of as a polynomial in the $a$'s, is identically zero, then $f$ must be the zero polynomial. □

**Theorem 6.24** (Noether Normalization). *1. Let $A$ be a domain, and $R$ be a finitely generated $A$-algebra. Then, there is some nonzero $a \in A$ and $x_1, \ldots, x_t \in R$ algebraically independent over $A$ such that $R_a$ is module-finite over $A_a[x_1, \ldots, x_t]$. In particular, if $A = K$ is a field, then $R$ is module-finite over $K[x_1, \ldots, x_t]$.*

*2. Let $K$ be an infinite field, and $R$ be a finitely generated $\mathbb{N}$-graded $K$-algebra (with $R_0 = K$). Then there are homogeneous elements $x_1, \ldots, x_t \in R$ algebraically independent over $K$ such that $R$ is module-finite over $K[x_1, \ldots, x_t]$.*

*Proof.* We proceed by induction on the number of generators $n$ of $R$ over $A$, with the case $n = 0$ trivial.

Now, suppose that we know the result for $A$-algebras generated by at most $n-1$ elements. If $R = A[r_1, \dots, r_n]$, with $r_1, \dots, r_n$ algebraically independent over $A$, we are done. Assume that there is some relation on the $r$'s: there is some $f(x_1, \dots, x_n) \in A[x_1, \dots, x_n]$ such that $f(r_1, \dots, r_n) = 0$. By taking an $A$-algebra automorphism (changing our generators), we can assume that $f$ has leading term $ax_n^N$ (in terms of $x_n$) for some $a$. Then, $f$ is monic in $x_n$ after inverting $a$, so $R_a$ is module-finite over $A_a[r_1', \dots, r_{n-1}']$. By hypothesis, $A_{ab}[r_1', \dots, r_{n-1}']$ is module-finite over $A_{ab}[r_1'', \dots, r_s'']$ for some $b \in A$ and $r_1'', \dots, r_s''$ that are algebraically independent over $A$. Since $R_{ab}$ is module-finite over $A_{ab}[r_1', \dots, r_{n-1}']$, we are done.

In the graded case, using the graded part of the previous lemma, we can find a homogeneous Noether normalization when $R$ is generated in a single degree. If $R$ is not generated in a single degree, by the homework, $R$ does have a subring $R^{(d)} = \bigoplus_{n \in \mathbb{N}} R_{nd} \subseteq R$ that is generated in a single degree. $R$ is integral over $R^{(d)}$ (any homogeneous element satisfies a relation of the form $t^d - x^d = 0$) and algebra-finite over $K$, hence over $R^{(d)}$, so $R^{(d)} \subseteq R$ is module-finite. Then, we can find $A \subseteq R^{(d)} \subseteq R$ module-finite, as required. □

**Theorem 6.25.** *Let $R$ be a finitely generated domain over a field $K$. Let $K[z_1, \dots, z_d]$ be any Noether normalization for $R$. Then, 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, the dimension of $R$ is $d$.*

*Proof.* We 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 is a field, so the statement follows trivially.

Pick a saturated chain

$$0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_k = \mathfrak{m}$$

and consider the contractions to $A = K[z_1, \dots, z_d]$:

$$0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_k.$$

By the saturated condition, $\mathfrak{q}_1$ has height 1, and so does $\mathfrak{p}_1$, by going down. Since $A$ is a UFD, $\mathfrak{p}_1 = (f)$ for some prime element $f$. After a change of variables, we can assume that $f$ is monic in $z_d$ over $K[z_1, \dots, z_{d-1}]$. Then,

$$0 = \mathfrak{q}_1/\mathfrak{q}_1 \subsetneq \mathfrak{q}_2/\mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_k/\mathfrak{q}_1 = \mathfrak{m}/\mathfrak{q}_1$$

is a saturated chain in the affine domain $R/\mathfrak{q}_1$ to the maximal ideal $\mathfrak{m}/\mathfrak{q}_1$. Now, $K[z_1, \dots, z_{d_1}] \subseteq A/(f) \subseteq R/\mathfrak{q}_1$ are module-finite, and we can apply the induction hypothesis to say that the chain we found in $R/\mathfrak{q}_1$ has length $d-1$, so $k-1 = d-1$, and $k = d$. □

**Corollary 6.26.** *The dimension of the polynomial ring $K[x_1, \dots, x_d]$ is $d$.*

**Corollary 6.27.** *If $R$ is a $K$-algebra, the dimension of $R$ is less than or equal to the minimal size of a generating set for $R$. If equality holds for some finite generating set, then $R$ is isomorphic to a polynomial ring over $K$, and the generators are algebraically independent.*

*Proof.* The first statement is trivial unless $R$ is finitely generated, in which case we can write $R = K[f_1, \dots, f_s] \cong K[x_1, \dots, x_s]/I$ for some ideal $I$. $\dim(R) \leq s$, for certain. If $I \neq 0$, then $\dim(R) < s$, since the zero ideal is not contained in $I$. □

**Corollary 6.28.** *Let $R$ be a finitely generated domain over a field.*

- *$R$ is catenary (this does not need domain);*
- *$R$ is equidimensional;*
- $\mathrm{ht}(I) = \dim(R) - \dim(R/I)$ *for all ideals $I$.*

*Proof.* Let $\mathfrak{p} \subseteq \mathfrak{q}$ be primes in $R$. We can quotient out by $\mathfrak{p}$, and assume that $R$ is a domain and $\mathfrak{p} = 0$. Fix a saturated chain $C$ from $\mathfrak{q}$ to a maximal ideal $\mathfrak{m}$. Given two saturated chains $C'$, $C''$ from 0 to $\mathfrak{q}$, the concatenations $C'|C$ and $C''|C$ are saturated chains from 0 to $\mathfrak{m}$, and hence must have the same length. It follows that $C'$ and $C''$ have the same length.

Equidimensionality is clear from the theorem.

We have $\mathrm{ht}(I) = \min\{\mathrm{ht}(\mathfrak{p}) \mid \mathfrak{p} \in \mathrm{Min}(I)\}$ and $\dim(R/I) = \max\{\dim(R/\mathfrak{p}) \mid \mathfrak{p} \in \mathrm{Min}(I)\}$. Thus, it suffices to show the equality for prime ideals. Now, take a saturated chain of primes $C$ from 0 to $\mathfrak{p}$, and a saturated chain $C'$ from $\mathfrak{p}$ to a maximal ideal $\mathfrak{m}$. $C$ has length $\mathrm{ht}(\mathfrak{p})$ by catenarity and definition of height, $C'$ has length $\dim(R/\mathfrak{p})$ by the theorem, and $C|C'$ has length $\dim(R)$ by the theorem. □

**Corollary 6.29.** *If $R$ is a finitely generated domain over a field $K$, then* $\dim(R) = \mathrm{trdeg}_K(\mathrm{frac}(R))$.

*Proof.* If $R \subseteq S$ is module-finite, then $\mathrm{frac}(R) \subseteq \mathrm{frac}(S)$ is algebraic, and hence they have the same transcendence degree over $K$. In particular, if $A = K[z_1, \dots, z_d]$ is a Noether normalization for $R$,

$$\mathrm{trdeg}_K(\mathrm{frac}(R)) = \mathrm{trdeg}_K(\mathrm{frac}(A)) = \mathrm{trdeg}_K(K(z_1, \dots, z_d)) = d = \dim(A) = \dim(R).$$

□

**Example 6.30.** Let $R = \mathbb{C}[X_{2\times 3}]$, $I = I_2(X)$. It follows from the Nullstellensatz that $\sqrt{I}$ is the kernel of the obvious map from $R$ to $\mathbb{C}[ar, as, at, br, bs, bt] \subseteq \mathbb{C}[a, b, r, s, t]$, since the minors cut out the set of rank one matrices. We saw in a worksheet that $I$ is prime. We can compute the dimension of $R/I$ by taking the transcendence degree of the fraction field over $K$. We have $\mathbb{C}(ar, as, at, br, bs, bt) = \mathbb{C}(a/b, br, bs, bt)$ and these are algebraically independent, so $\dim(R/I) = 4$. Thus, $I$ is a prime of height two. Recall also that $I$ cannot be generated by fewer than three elements. You'll have no trouble generalizing this to see that $I_2(X_{2\times n}) \subseteq K[X_{2\times n}]$ is an $\binom{n}{2}$-generated prime of height $n-1$.

**Example 6.31.** We are guaranteed Noether normalizations, even when the target is not a domain. For example, let $R = \dfrac{K[x, y, z]}{(xz, yz)}$. A Noether normalization for $R$ is $A = K[x - z, y - z] \subseteq R$: $x - z$ and $y - z$ are algebraically independent, no polynomial expression of $x - z, y - z$ lies in $(z^2 + z(x - z), z^2 + z(y - z))$, and $z$, then $x$ and $y$, are definitely integral over it. Note that $x - y = (x + z) - (y + z) \in A \cap (x, y)R$, so $R/\mathfrak{p}$ is no longer a Noether normalization for $R/\mathfrak{p}$ for a minimal prime of $R$. Thankfully, existence of Noether normalizations does not contradict the fact that some rings aren't equidimensional.

Note that having a minimal prime of $R$ that contracts to a nonminimal prime of $A$ is a failure of the conclusion of going down. This is because the hypothesis that $R$ was torsionfree over $A$ failed: equivalently, one of its associated primes had a nonzero intersection with $A$!

Here is an extremely handy corollary of Noether normalization and basic dimension theory.

**Theorem 6.32** (Generic freeness)**.** *Let $A \to R$ be a map of rings, with $R$ finitely generated as an $A$-algebra, and $A$ a Noetherian domain. Then, there exists a nonzero $a \in A$ such that $R_a$ is free over $A_a$.*

*Proof.* Let $K = \operatorname{frac}(A)$. We induce on the dimension $t$ of $K \otimes_A R = (A \smallsetminus 0)^{-1}R$.

First, we observe that $(A \smallsetminus 0)^{-1}R \neq 0$ if and only if the map above is injective. If it is not injective, then there is some nonzero $a$ in the kernel, and $R_a = 0$ is free over $A_a$.

Now, if $(A\smallsetminus 0)^{-1}R \neq 0$, by Noether normalization, we have $R_a$ is module-finite over $A_a[z_1, \dots, z_s]$ for some $a \in A$, and hence $(A\smallsetminus 0)^{-1}R_a = (A\smallsetminus 0)^{-1}R$ is module-finite over $(A\smallsetminus 0)^{-1}A_a[z_1, \dots, z_s] = K[z_1, \dots, z_s]$. Thus, $t$ is finite, and is equal to the number of indeterminates in a Noether normalization for $R_a$ over $A_a$.

If $t = 0$, then $A_a \subseteq R_a$ is module-finite for some $a$, by Noether normalization. Take a prime filtration of $R_a$ as an $A_a$-module:

$$R_a = M_n \supseteq M_{n-1} \supseteq \cdots \supseteq M_0 = 0, \qquad \text{with } M_{i+1}/M_i \cong R/\mathfrak{p}_i,\ \mathfrak{p}_i \text{ prime.}$$

We can pick an element $b$ that is in the product of the nonzero $\mathfrak{p}_i$'s, so that $(M_{i+1})_b/(M_i)_b \cong (A/\mathfrak{p}_i)_b$ is either $A_b$ or 0 depending on whether $\mathfrak{p}_i$ is zero or not. In the nonzero case, we have $0 \to (M_i)_b \to (M_{i+1})_b \to A_b \to 0$, which splits, so $(M_{i+1})_b \cong A_b \oplus M_i$, and inductively we find that $(R_a)_b = R_{ab}$ is free over $A_b$.

In general, apply Noether normalization to write $A_a \subseteq A_a[z_1, \dots, z_t] \subseteq R_a$ with the latter map module-finite. Take a prime filtration of $R_a$ as a $A_a[z_1, \dots, z_t]$-module. All of the factors are either free, or are proper quotients of the domain $A_a[z_1, \dots, z_t]$: $M_{i+1}/M_i \cong A_a[z_1, \dots, z_t]/\mathfrak{p}$ for some nonzero prime $\mathfrak{p}$ of $A_a[z_1, \dots, z_t]$. Localizing at $(A \smallsetminus 0)$, this quotient ring is of the form $K[z_1, \dots, z_t]/\mathfrak{p}'$ for some $\mathfrak{p}'$ (the expansion of $\mathfrak{p}$ to this larger localized domain) that is nonzero, so either $\mathfrak{p} \cap A_a$ is nonzero, or else $\dim(K \otimes (A_a[z_1, \dots, z_t]/\mathfrak{p})) < t$.

If $\mathfrak{p} \cap A_a \neq 0$, then let $b_i$ be in the intersection; the localization $(M_{i+1}/M_i)_{b_i} \cong (A_a[z_1, \dots, z_t]/\mathfrak{p})_{b_i}$ is then zero, which is free! If $\dim(K \otimes (A_a[z_1, \dots, z_t]/\mathfrak{p})) < t$, the induction hypothesis applies. Thus, for each $i$, there is some $b_i$ such that $(M_{i+1}/M_i)_{b_i}$ is free over $(A_a)_{b_i}$. Replacing $a$ with $ab_1 \cdots b_n$, we obtain the desired conclusion. □

**Corollary 6.33.** *Let $\phi : R \to S$ be an algebra-finite ring map, with $R$ Noetherian. Then the image of $\phi^*$ contains a nonempty open subset of $V(\ker(\phi))$.*

*Proof.* Let $\operatorname{Min}(\ker(\phi)) = \{\mathfrak{p}_i\}$. We will show the stronger statement that the image of $\phi^*$ contains a nonempty open subset of $V(\mathfrak{p}_i)$ for each $i$. First, we claim that each $\mathfrak{p}_i$ is in the image: this follows from the fact that $R/\ker(\phi) \hookrightarrow S$ implies $(R/\ker(\phi))_{\mathfrak{p}_i} \hookrightarrow (R \smallsetminus \mathfrak{p})^{-1}S$, and hence the latter ring is nonzero, so some prime contracts to something contained in $\mathfrak{p}_i$ containing the kernel, which must be $\mathfrak{p}_i$ by minimality. Now, if $\mathfrak{q}_i \cap R = \mathfrak{p}_i$, we have an algebra-finite inclusion of domains $A/\mathfrak{p}_i \hookrightarrow B/\mathfrak{q}_i$. By generic freeness, we can invert an element of the base to make the target a free module. In particular, there is a module surjection of the target onto the source, so it is a direct summand, and hence surjective on spectra. Thus, every prime of $(A/\mathfrak{p}_i)_{f_i}$ is in the image of the induced map on spectra. Equivalently, every prime of $A$ in $V(\mathfrak{p}_i) \smallsetminus V(f_i)$ is in the image. □

## 6.4 Artinian rings

To prepare for our next big theorems in dimension theory, we need to understand the structure of zero-dimensional Noetherian rings. To get started on that, we will take a theorem on primary decomposition for certain ideals in not necessarily Noetherian rings.

**Theorem 6.34.** *Let $R$ be a ring, not necessarily Noetherian. Let $I$ be an ideal such that $V(I)$ is a finite set of maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_t$. Then, there is a primary decomposition $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$ and we also have $I = \mathfrak{q}_1 \cdots \mathfrak{q}_t$, and $R/I \cong R/\mathfrak{q}_1 \times \cdots \times R/\mathfrak{q}_t$.*

*Proof.* First, we claim that $IR_{\mathfrak{m}_i}$ is $\mathfrak{m}_i R_{\mathfrak{m}_i}$-primary. Indeed, note that $(R/I)_{\mathfrak{m}_i} = R_{\mathfrak{m}_i}/IR_{\mathfrak{m}_i}$ has a unique maximal ideal $\mathfrak{m}_i R_{\mathfrak{m}_i}$. Thus, if $x, y \in R_{\mathfrak{m}_i}$ are such that $xy \in IR_{\mathfrak{m}_i}$, and $x \notin \mathfrak{m}_i R_{\mathfrak{m}_i}$, then $x$ is a unit modulo $I_{\mathfrak{m}_i}$, so $y \in IR_{\mathfrak{m}_i}$. Then, the contraction of a primary ideal is primary (prove it!) so $\mathfrak{q}_i = IR_{\mathfrak{m}_i} \cap R$ is $\mathfrak{m}_i$-primary, and $I \subseteq \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$. On the other hand, equality of these modules is a local property; if $\mathfrak{p} \notin V(I)$, then both sides are the unit ideal in $R_{\mathfrak{p}}$, otherwise, in $R_{\mathfrak{m}_i}$ they are proper but equal. Thus, the primary decomposition.

The fact that this intersection is a product and the quotient ring is a direct product follows from the Chinese remainder theorem: $V(\mathfrak{q}_i + \mathfrak{q}_j) = V(\mathfrak{q}_i) \cap V(\mathfrak{q}_j) = \varnothing$, so each pair of ideals is comaximal. □

**Definition 6.35.** *A nonzero module is* simple *if it has no proper submodules. Equivalently, $M$ is simple if it isomorphic to $R/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$.*

The nontrivial implication comes from the fact that any nonzero module contains a cyclic module, and if $M \cong R/I$ with $I$ not maximal, we can surject to $R/\mathfrak{m}$ for a maximal ideal containing $I$, which has a proper kernel. Note already that if $R$ is local, any simple module is isomorphic to the residue field.

**Definition 6.36.** *A module $M$ has* finite length *if it has a filtration of the form*

$$0 = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n = M$$

*with $M_{i+1}/M_i$ simple for each $i$; such a filtration is called a* composition series *of* length *$n$. The* length *of a finite length module $M$, denoted $\ell(M)$, is the minimum of the lengths of a composition series of $M$.*

We recall the Jordan-Holder theorem and some of its consequences:

- For a module of finite length, any filtration can be refined to a composition series.
- Every composition series for a fixed module of finite length has the same length.
- If $M \subseteq N$, then $\ell(N) = \ell(M) + \ell(N/M)$. (Extend a composition series for $M$ to one for $N$.)
- If $M \subseteq N$, then $\ell(M) \leq \ell(N)$, with equality only if $M = N$.
- If $M$ has finite length, then any *descending* chain of submodules of $M$ stabilizes. Likewise, any *ascending* chain of submodule stabilizes.

We also note that if $M$ is annihilated by a maximal ideal $\mathfrak{m}$, so that $M$ is an $R/\mathfrak{m}$-module, the length of $M$ is equal to its dimension as an $R/\mathfrak{m}$-vector space. In particular, $\ell(M/\mathfrak{m}M) = \dim_{R/\mathfrak{m}}(M/\mathfrak{m}M)$.

**Definition 6.37.** *A ring is* Artinian *if every descending chain of ideals eventually stabilizes. A module is* Artinian *if every descending chain of submodules eventually stabilizes.*

**Theorem 6.38.** *The following are equivalent:*

1. *$R$ is Noetherian of dimension zero.*

2. *$R$ is a finite product of local Noetherian rings of dimension zero.*

3. *$R$ has finite length as an $R$-module.*

4. *$R$ is Artinian.*

*Proof.* (1)⇒(2): Since $R$ is Noetherian of dimension zero, every prime is maximal and minimal, and there are thus finitely many. By the theorem from above, decomposes as a direct product of Noetherian local rings, which all must have dimension zero.

(2)⇒(3): It suffices to deal with the case $(R, \mathfrak{m})$ is local. In this case, the maximal ideal is the unique minimal prime, so it consists of the nilpotents in $R$. Since $R$ is Noetherian, $\mathfrak{m}$ is finitely generated, and thus $\mathfrak{m}^N = 0$ for some $N$. Each $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ has finite length (finite dimension over $R/\mathfrak{m}$), so the total length of $R$ is finite.

(3)⇒(4): Since proper submodules of a finite length module have strictly smaller length, any finite length module has DCC. In particular, $R$ has DCC.

(4)⇒(1): First we show that $R$ has dimension zero. If $\mathfrak{p}$ is any prime, then $A = R/\mathfrak{p}$ is Artinian; pick $a \in A$ some nonzero element. The ideals

$$(a) \supseteq (a^2) \supseteq (a^3) \supseteq \cdots$$

stabilize, so $a^n = a^{n+1}b$ for some $b$. Since $A$ is a domain, $ab = 1$ in $A$, so $a$ is a unit. Thus, $R/\mathfrak{p}$ is a field, so every prime is maximal.

Second, note that there are only finitely many maximal ideals. Otherwise, consider the chain

$$\mathfrak{m}_1 \supseteq \mathfrak{m}_1 \cap \mathfrak{m}_2 \supseteq \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \mathfrak{m}_3 \supseteq \cdots .$$

This stabilizes, so $\mathfrak{m}_{n+1} \supseteq \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n \supseteq \mathfrak{m}_1 \cdots \mathfrak{m}_n$. By distinctness, we can pick $f_i \in \mathfrak{m}_i \smallsetminus \mathfrak{m}_{n+1}$, but then $f_1 \cdots f_n \in \mathfrak{m}_1 \cdots \mathfrak{m}_n \smallsetminus \mathfrak{m}_{n+1}$, which is a contradiction. Now, we apply the decomposition theorem from earlier to conclude that $R = (R, \mathfrak{m})$ is a finite direct product of local rings of dimension zero. Since each of the factors is a quotient ring, each is Artinian. It suffices to show that each factor is Noetherian.

Now, to see $R$ is Noetherian, $\mathfrak{m} \supseteq \mathfrak{m}^2 \supseteq \mathfrak{m}^3 \supseteq \cdots$ stabilizes again, so that $\mathfrak{m}^n = \mathfrak{m}^{n+1}$; we can't apply NAK yet since we don't know $\mathfrak{m}^n$ is finitely generated. If $\mathfrak{m}^n \neq 0$, consider the family $S$ of ideals $I \subseteq \mathfrak{m}$ such that $I\mathfrak{m}^n \neq 0$; this contains $\mathfrak{m}$. Just as the Noetherian property guarantees maximal elements of nonempty families, the Artinian property guarantees minimal elements; take $J$ minimal in $S$. For some $x \in J$, $x\mathfrak{m}^n \neq 0$, and $(x) \subseteq J \subseteq \mathfrak{m}$, so $J = (x)$ is principal by minimality. Now, $x\mathfrak{m}(\mathfrak{m}^n) = x\mathfrak{m}^{n+1} = x\mathfrak{m}^n \neq 0$, so $x\mathfrak{m} \subseteq (x)$ is in the family $S$ of ideals, and by minimality, $(x) = \mathfrak{m}(x)$. NAK applies to this, so $(x) = (0)$, contradicting that $\mathfrak{m}^n \neq 0$. Then, we have

$$0 = \mathfrak{m}^n \subseteq \mathfrak{m}^{n-1} \subseteq \cdots \subseteq \mathfrak{m} \subseteq R,$$

and since the Artinian property descends to submodules and quotients, each factor has finite length. Thus, $R$ has finite length, so ideals in $R$ satisfy ACC, as required. □

**Example 6.39.** Some Artinian local rings include $K[x,y]/(x^2,y^2)$, $K[x,y]/(x^2,xy,y^2)$, and $\mathbb{Z}/(p^n)$.

**Example 6.40.** Even though every Artinian ring is Noetherian and finite length, it is not true that Artinian modules are always Noetherian or finite length. Let $R = \mathbb{C}[\![x]\!]$, and $M = R[1/x]/R$. Note that $R[1/x]$ is the ring of Laurent series, so $M$ is the module of "tails" of these functions. It does not have finite length; it is not even finitely generated! Observe that any submodule $N$ of $M$ either contains $1/x^n$ for all $n$, or else there is a largest $n$ for which $1/x^n \in N$, and $N = R \cdot 1/x^n$ for this $n$. The module $R \cdot 1/x^n \subseteq M$ has length $n$, so is Artinian, thus $M$ is Artinian.

**Lemma 6.41.** *Let $R$ be a Noetherian ring, and $M$ be an $R$-module. $M$ has finite length if and only if it is finitely generated and all of its associated primes are maximal ideals of $R$.*

*Proof.* If $M$ has finite length, then it is Noetherian, hence finitely generated, and a composition series is a prime filtration, so all the associated primes must occur as factors.

Conversely, if $M$ is finitely generated, and every associated prime is maximal, then take a prime filtration of $M$. Every factor in the prime filtration must contain an associated prime of $M$, hence must be maximal, so this is a composition series. □

**Definition 6.42.** *If $(R, \mathfrak{m}, k)$ is local, a* coefficient field *for $R$ is a subfield $K \subseteq R$ such that the map $K \to R \to R/\mathfrak{m} \cong k$ is an isomorphism.*

Rings like $K[\underline{x}]_{(\underline{x})}/I$ have coefficient fields: the copy of $K$. Some rings without coefficient fields are $\mathbb{Z}_{(p)}$, $\mathbb{R}[x]_{(x^2+1)}$. Some rings have lots of them: $\mathbb{C}[x, y]_{(x)}$ contains $\mathbb{C}(y)$ and $\mathbb{C}(x + y)$, which both are coefficient fields!

**Remark 6.43.** If $(R, \mathfrak{m}, k)$ is local with coefficient field $K$, then a finite length $R$-module $M$ may not be a $k$-module (it may not be killed by $\mathfrak{m}$), but it is a $K$-vector space by restriction of scalars, and $\ell(M) = \dim_K(M)$.

# Chapter 7

# Dimension, locally

**Question 7.1.** Given a polynomial ring in $n$ variables over a field, we know that every system of polynomial equations has the same solution set as a finite system of polynomial equations. Is there some $N$ such that every system of equations is equivalent to a system of at most $N$ equations?

First, let's suppose our field is $\mathbb{R}$. Then, the answer is yes, and $N = 1$! Given a system of equations, which might as well be finite by Hilbert Basis, write it as $f_1(\underline{x}) = f_2(\underline{x}) = \cdots = f_t(\underline{x}) = 0$. Then, the system $f_1(\underline{x})^2 + f_2(\underline{x})^2 + \cdots + f_t(\underline{x})^2 = 0$ has the same solution set. This trick generalizes easily to any field that is not algebraically closed.

If we have an algebraically closed field, nothing this silly can work. By the Nullstellensatz, our question translates to: is there an $N$ such that every ideal is the radical of an $N$-generated ideal? This latter statement makes sense not only for polynomial rings over any field, but over any ring.

## 7.1 Height and number of generators

**Theorem 7.2** (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.*

We note that this is stronger than the statement that the height of $(f)$ is at most one: we recall that that means that some minimal prime of $(f)$ has height at most one.

*Proof.* If the theorem is false, so that there is some $R$, $\mathfrak{p}$, $f$ with $\mathfrak{p}$ minimal over $(f)$ and $\mathrm{ht}(\mathfrak{p}) > 1$, localize at $\mathfrak{p}$ and mod out by a minimal prime to obtain a Noetherian local domain $(R, \mathfrak{m})$ of dimension at least two in which $\mathfrak{m}$ is the unique minimal prime of $(f)$. In particular, $\overline{R} = R/(f)$ is zero-dimensional. Let $\mathfrak{q}$ be a prime in between $(0)$ and $\mathfrak{m}$.

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

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

stabilizes. We then have, for some $n$ and all $m > n$, that $\mathfrak{q}^{(n)}\overline{R} \subseteq \mathfrak{q}^{(m)}\overline{R}$ for all . Pulling back to $R$, $\mathfrak{q}^{(n)} \subseteq \mathfrak{q}^{(m)} + (f)$. For $q \in \mathfrak{q}^{(n)}$, write $q = q' + fr$, with $q' \in \mathfrak{q}^{(m)} \subseteq \mathfrak{q}^{(n)}$, so that $fr \in \mathfrak{q}^{(n)}$. Since $f \notin \mathfrak{q}$, $r \in \mathfrak{q}^{(n)}$. This yields $\mathfrak{q}^{(n)} = \mathfrak{q}^{(m)} + f\mathfrak{q}^{(n)}$. Thus, $\mathfrak{q}^{(n)}/\mathfrak{q}^{(m)} = f(\mathfrak{q}^{(n)}/\mathfrak{q}^{(m)})$, so $\mathfrak{q}^{(n)}/\mathfrak{q}^{(m)} = \mathfrak{m}(\mathfrak{q}^{(n)}/\mathfrak{q}^{(m)})$, and by NAK, $\mathfrak{q}^{(n)} = \mathfrak{q}^{(m)}$ in $R$.

Now, if $a \in \mathfrak{q}$ is nonzero, we have $a^n \in \mathfrak{q}^n \subseteq \mathfrak{q}^{(n)} = \mathfrak{q}^{(m)}$ for all $m$, so $\bigcap_{m\in\mathbb{N}} \mathfrak{q}^{(m)} \neq 0$. On the other hand, $\mathfrak{q}^{(m)} \subseteq \mathfrak{q}^m R_{\mathfrak{q}}$, and $\bigcap_{m\in\mathbb{N}} \mathfrak{q}^{(m)} \subseteq \bigcap_{m\in\mathbb{N}} \mathfrak{q}^m R_{\mathfrak{q}} = 0$ by Krull intersection. This is the contradiction we seek. □

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

*Proof.* We can quotient out by $\mathfrak{p}$ and localize at $\mathfrak{r}$, and assume that $\mathfrak{r}$ is the maximal ideal, and that $f$ is nonzero (for otherwise we are done); once we have succeeded in this case, we can pull back our prime to $R$. Then, by the principal ideal theorem, minimal primes of $(f)$ have height one, hence are not $\mathfrak{r}$; we can take $\mathfrak{q}'$ to be one of those. □

**Theorem 7.4** (Krull height theorem)**.** *Let $R$ be a Noetherian ring, and $I = (f_1, \dots, f_n)$ be an ideal generated by $n$ elements. Then every minimal prime of $I$ has height at most $n$.*

*Proof.* We proceed by induction on $n$. The case $n = 1$ is the principal ideal theorem.

Let $I = (f_1, \dots, f_n)$ be an ideal, $\mathfrak{p}$ be a minimal prime of $I$, and $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_h = \mathfrak{p}$ be a saturated chain of length $h$ ending at $\mathfrak{p}$. If $f_1 \in \mathfrak{p}_1$, then we can apply the induction hypothesis to the ring $\overline{R} = R/(f_1)$ and the ideal $(f_2, \dots, f_n)\overline{R}$: the chain $\mathfrak{p}_1\overline{R} \subsetneq \cdots \subsetneq \mathfrak{p}_h\overline{R}$ has length at most $h - 1 = n - 1$, and we will be done. We use the previous lemma to replace our given chain with a chain of the same length that satisfies this hypothesis.

In the given chain, let $f_1 \in \mathfrak{p}_{i+1} \smallsetminus \mathfrak{p}_i$. If whenever $i > 0$ we can decrease $i$, we can eventually get to the chain we want. To do this, we just need to apply the previous lemma with $\mathfrak{r} = \mathfrak{p}_{i+1}$, $\mathfrak{q} = \mathfrak{p}_i$, and $\mathfrak{p} = \mathfrak{p}_{i-1}$. □

**Example 7.5.**

1. The bound is certainly sharp: an ideal generated by $n$ variables $(x_1, x_2, \dots, x_n)$ in a polynomial ring has height $n$. There are many other such ideals, like $(u^3 - xyz, x^2 + 2xz - 6y^5, vx + 7vy) \in K[u, v, w, x, y, z]$. An ideal of height $n$ generated by $n$ elements is called a *complete intersection*.

2. The ideal $(xy, xz)$ in $K[x, y, z]$ has minimal primes of heights 1 and 2.

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

4. For the same phenomenon, but in a nice polynomial ring, $I = (x^3, y^3, x^2u + xyv + y^2w) \subset R = K[u, v, w, x, y]$. Note that $(u, v, w, x, y) = (I : x^2y^2)$, so $I$ has an associated prime of height 5.

5. Noetherian is necessary. Let $R = K[x, xy, xy^2, \dots] \subseteq K[x, y]$. 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, $\mathfrak{m} = (x, xy, xy^2, \dots) \subseteq \sqrt{(x)}$, and since $\mathfrak{m}$ is a maximal ideal, we have equality, so $\operatorname{Min}(x) = \{\mathfrak{m}\}$. However, the ideal $\mathfrak{p} = (xy, xy^2, xy^3, \dots) = (y)K[x, y] \cap R$ is prime, and the chain $(0) \subsetneq \mathfrak{p} \subsetneq \mathfrak{m}$ shows that $\operatorname{ht}(\mathfrak{m}) > 1$.

**Lemma 7.6.** *Let $R$ be a Noetherian ring, and $I$ be an ideals. Let $f_1, \dots, f_t \in I$, and $J_i = (f_1, \dots, f_i)$ for each $i$. If $f_i \notin \bigcup_{\mathfrak{a} \in \operatorname{Min}(J_{i-1}) \smallsetminus V(I)} \mathfrak{a}$ for each $i$, then any minimal prime of $J_i$ either contains $I$, or else has height $i$.*

*Proof.* By induction on $i$. For $i = 0$, $J_0 = (0)$, and every minimal prime has height zero.

If we know the statement for $i = m$, consider a minimal prime $\mathfrak{q}$ of $J_{m+1}$. Since $J_m \subseteq J_{m+1}$, $\mathfrak{q}$ must contain a minimal prime of $J_m$, say $\mathfrak{p}$. If $\mathfrak{p} \supseteq I$, then $\mathfrak{q} \supseteq I$. If $\mathfrak{p}$ does not contain $I$, it has height $m$, then $f_{m+1} \in \mathfrak{q} \smallsetminus \mathfrak{p}$, so $\mathfrak{q} \supsetneq \mathfrak{p}$, and the height of $\mathfrak{q}$ is strictly greater than $m$. By Krull height, it is then exactly $m + 1$. □

**Theorem 7.7.** *Let $R$ be a Noetherian ring of dimension $d$.*

1. *If $\mathfrak{p}$ is a prime of height $h$, then there are $h$ elements $f_1, \ldots, f_h \in \mathfrak{p}$ such that $\mathfrak{p}$ is a minimal prime of $(f_1, \ldots, f_h)$.*

2. *If $I$ is any ideal in $R$, then there are $d + 1$ elements $f_1, \ldots, f_{d+1} \in I$ such that $I = \sqrt{(f_1, \ldots, f_{d+1})}$.*

3. *If $R$ is local or graded ($\mathbb{N}$-graded, with $R_0$ a field), and $I$ is an ideal (homogeneous in the graded case), then there are $d$ elements (homogeneous) $f_1, \ldots, f_d \in I$ such that $I = \sqrt{(f_1, \ldots, f_d)}$.*

*Proof.* We will use the notation from the previous lemma.

1. If $\mathfrak{p}$ is a minimal prime, then we take the “empty sequence:” $\mathfrak{p}$ is minimal over $(0)$. Otherwise, we will use the recipe from the lemma above, with $I = \mathfrak{p}$. We need to show that we can choose $h$ elements satisfying the hypotheses. Note first that unless $i \geq h$, $\operatorname{Min}(J_i)$ cannot meet $V(\mathfrak{p})$, by Krull height. If $\mathfrak{p} \subseteq \bigcup_{\operatorname{Min}(J_i)} \mathfrak{q}$, then by prime avoidance, $\mathfrak{p}$ is contained in a minimal prime of $J_i$, which cannot happen for $i < h$. Thus, we can choose $(f_1, \ldots, f_h)$ as in the lemma, and its minimal primes have height $h$, or else contain $\mathfrak{p}$. Since $J_h = (f_1, \ldots, f_h) \subseteq \mathfrak{p}$, some minimal prime $\mathfrak{q}$ of $J_h$ is contained in $\mathfrak{p}$. We know that this $\mathfrak{q}$ either contains $\mathfrak{p}$, and hence is $\mathfrak{p}$, or else is contained in and has the same height as $\mathfrak{p}$, so again must be equal to $\mathfrak{p}$.

2. Again, we use the recipe from above. We again need to see that we can do this. Inductively, we are choosing elements inside of $I$, so each $J_i$ is contained in $I$, and $V(I) \subseteq V(J_i)$. If for some $i$ we have $\operatorname{Min}(J_{i-1}) \smallsetminus V(I) = \varnothing$, then each minimal prime of $J_i$ will lie in $V(I)$, so $V(J_i) \subseteq V(I)$, and equality holds. If $\operatorname{Min}(J_{i-1}) \smallsetminus V(I) \neq \varnothing$, then $I \nsubseteq \mathfrak{q}$ for any $\mathfrak{q} \in \operatorname{Min}(J_{i-1}) \smallsetminus V(I)$, and $I \nsubseteq \bigcup_{\operatorname{Min}(J_{i-1}) \smallsetminus V(I)} \mathfrak{p}$ by prime avoidance, so we can choose elements as in the lemma.

   Thus, by the lemma, we get elements $(f_1, \ldots, f_{d+1}) = J_{d+1} \subseteq I$ such that the minimal primes contain $I$ or have height at least $d + 1$. By the assumption on the dimension, no prime has height $d + 1$, so all the minimal primes of $J_{d+1}$ contain $I$. But, if they are minimal over the smaller ideal, and contain the larger one, they are minimal over the larger one too.

3. We run the same argument as in the last part (using homogeneous prime avoidance in the graded case). The point is that the only (homogeneous, in the graded case) ideal of height $d$ already contains $I$. □

**Corollary 7.8.** *Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring. Then,*

$$\dim(R) = \min\{n \mid \exists f_1, \ldots, f_n : \sqrt{(f_1, \ldots, f_n)} = \mathfrak{m}\} \leq \dim_k(\mathfrak{m}/\mathfrak{m}^2).$$

*That is, the dimension of a Noetherian local ring is bounded by minimal the number of generators of its maximal ideal.*

*In particular, a Noetherian local ring has finite dimension.*

*Proof.* The dimension of a local ring is the height of its maximal ideal. Thus, by Krull height, the minimum $n$ in the middle is at least $\dim(R)$, and the previous theorem gives the other direction. The second inequality just follows from the fact that the right-hand quantity is the minimal number of generators of the ideal $\mathfrak{m}$. □

Compare the last inequality to the fact that, for an algebra over a field, the dimension is bounded by the number of generators as a $K$-algebra. We also want to compare this with the characterization of the dimension of a vector space as the least number of linear equations needed to cut out the origin.

**Definition 7.9.** *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 $\sqrt{(x_1, \ldots, x_d)} = \mathfrak{m}$.*

*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.*

**Lemma 7.10.** *Let $(R, \mathfrak{m})$ be a Noetherian local ring, and $x_1, \ldots, x_t \in R$. Then, $\dim(R/(x_1, \ldots, x_t)) \geq \dim(R) - t$, and $x_1, \ldots, x_t$ are parameters if and only if $\dim(R/(x_1, \ldots, x_t)) = \dim(R) - t$.*

*Proof.* First, we deal with the inequality. If $\dim(R/(x_1, \ldots, x_t)) = s$, then take a system of parameters $y_1, \ldots, y_s$ for $R/(x_1, \ldots, x_t)$, and pull back to $R$ to get $x_1, \ldots, x_t, y_1', \ldots, y_s'$ in $R$ such that the quotient of $R$ modulo the ideal generated by these elements has dimension zero. By Krull height, we get that $t + s \geq \dim(R)$.

For the second statement, the condition is sufficient, since one can lift a SOP $y_1, \ldots, y_{d-t}$ for $R/(x_1, \ldots, x_t)$ back to $R$ to get an SOP $x_1, \ldots, x_t, y_1, \ldots, y_{d-t}$. On the other hand, if $x_1, \ldots, x_d$ is a system of parameters, then if $I$ is the image of $(x_{t+1}, \ldots, x_d)$ in $R' = R/(x_1, \ldots, x_t)$, we have $R'/I$ is zero-dimensional, so $I$ is primary to $\mathfrak{m}$ in $R'$. Thus, the height of $I$ is equal to $\dim(R')$, which is then $\leq d - t$ by Krull height, and equality holds. □

## 7.2 Regular rings

We saw that for finitely generated algebras, the dimension was bounded above by the number of generators, and equality forced our ring to be a polynomial ring. The Krull height theorem provided us a local analogue to this bound on dimension: the number of generators of the maximal ideal. One might expect that the rings for which equality holds might be good like polynomial rings.

**Definition 7.11** (Regular ring)**.** *A Noetherian local ring $(R, \mathfrak{m}, k)$ is* regular *if $\dim(R) = \dim_k(\mathfrak{m}/\mathfrak{m}^2)$.*

**Example 7.12.**

1. If $(R, \mathfrak{m})$ is zero-dimensional, then $\mathfrak{m}$ must be zero: a zero-dimensional regular ring is a field.

2. $\mathbb{C}[\![x]\!]$ is one-dimensional (PID) and the maximal ideal is principal, so it is regular.

3. $\mathbb{C}[\![x^2, x^3]\!] \subseteq \mathbb{C}[\![x]\!]$ is one-dimensional (since it is integral in the larger ring), but has a 2-generated maximal ideal, so is not regular.

4. Let $K = \overline{K}$. Then, for any maximal ideal $\mathfrak{m}$ of $K[\underline{x}]$, $K[\underline{x}]_{\mathfrak{m}}$ is regular.

**Example 7.13.** Let

$$R = \frac{k\begin{bmatrix} u & v & w \\ x & y & z \end{bmatrix}}{(uy - vx, uz - wx, vz - wy)} \qquad \mathfrak{m} = \frac{(u, v, w, x, y, z)}{(uy - vx, uz - wx, vz - wy)}$$

The local ring $R_{\mathfrak{m}}$ is not a regular ring, since $u, v, w, x, y, z$ are linearly independent in $\mathfrak{m}/\mathfrak{m}^2$.

However, $R_{\mathfrak{n}}$ is regular for

$$\mathfrak{n} = \frac{(u-1, v, w, x, y, z)}{(uy - vx, uz - wx, vz - wy)}.$$

In fact, $y \in (vx)$, $z \in (wx)$, so $\mathfrak{n}R_{\mathfrak{n}} = (u-1, v, w, x)$.

Finally, for the prime ideal $\mathfrak{p} = (v, w, x, y, z)$, $R_{\mathfrak{p}}$ is regular with $\mathfrak{p}R_{\mathfrak{p}} = (v, w, x)$.

**Lemma 7.14.** *A regular local ring is a domain.*

*Proof.* By induction on $d = \dim R$, where $R$ is a regular local ring. If $d = 0$, then $R$ must be a field, and thus a domain.

If $d > 0$, consider $x \in \mathfrak{m} \smallsetminus \left(\mathfrak{m}^2 \cup \bigcup_{\mathfrak{p} \in \operatorname{Min} R} \mathfrak{p}\right)$; such $x$ exists by prime avoidance. By NAK, $\mathfrak{m}/xR$ is generated by $d-1$ elements, so that $\dim R/xR \leqslant d-1$ by Krull's height theorem. Then $\dim R/xR = d-1$, and $R/xR$ is regular. We want to show that 0 is prime. By the induction hypothesis, $R/xR$ is a domain, and thus $xR$ is a prime ideal in $R$ that is not minimal. Take a prime ideal $0 \subseteq \mathfrak{p} \subseteq xR$. If $y \in \mathfrak{p}$, we can write $y = ax$ for some $a \in R$, and if $x \notin \mathfrak{p}$, then $a \in \mathfrak{p}$. Thus $x\mathfrak{p} = \mathfrak{p}$, which by NAK implies that $\mathfrak{p} = 0$. Thus $R$ is a domain. □

**Definition 7.15.** *A sequence of elements $x_1, \dots, x_t$ in a regular local ring $(R, \mathfrak{m}, k)$ are* regular parameters *if each $x_i \in \mathfrak{m}$, and the images of the $x$'s in $\mathfrak{m}/\mathfrak{m}^2$ are $k$-linearly independent.*

We observe that regular parameters are parameters, since quotienting out by each decreases the dimension by one and produces another regular ring. By the previous lemma, they generate a prime ideal, too.

We want to determine now when the local ring of a point of some affine variety over the complex numbers is regular, and to get some geometric idea behind this notion. We are looking at a local ring of the form $R = \mathbb{C}[x_1, \dots, x_d]_{\mathfrak{n}}/I$, where $I = (f_1, \dots, f_t)$ is prime and $\mathfrak{n} = (x_1 - a_1, \dots, x_d - a_d)$. This corresponds to looking at the point $\underline{a} \in Z_{\mathbb{C}}(I) \subseteq \mathbb{C}^d$. In $\mathbb{C}^d$, there is a vector subspace $T_{Z_{\mathbb{C}}(f_i), \underline{a}}$ of tangent vectors to $Z_{\mathbb{C}}(f_i)$ at $\underline{a}$: this is computed by the gradient form $\nabla_{\underline{a}}(f_i) = \sum_j \frac{\partial f_i}{\partial x_j}(\underline{a})(x_j - a_j) = 0$ (where we think of the tangent space as centered at $\underline{a}$ with coordinates $x_j - a_j$). We know that $f_i \in \mathfrak{n}$ by assumption that $\underline{a} \in Z_{\mathbb{C}}(f_i)$. We can use Taylor's formula to write $f_i = 0 + \sum_j \frac{\partial f_i}{\partial x_j}(\underline{a})(x_j - a_j) + \cdots$, with $\cdots \in (\{x_j - a_j\})^2$, so that the image of $f_i$ in $\mathfrak{n}/\mathfrak{n}^2$ is exactly the class of $\nabla_{\underline{a}}(f_i)$. Now, the tangent space to $Z_{\mathbb{C}}(f_1, \dots, f_t)$ consists of vectors tangent to each, so it is the subspace of $\mathbb{C}^d$ given by the linear equations $\nabla_{\underline{a}}(f_1), \dots, \nabla_{\underline{a}}(f_t)$, which is in turn isomorphic to the subspace of $\mathfrak{n}/\mathfrak{n}^2$ given by the images of the $f$'s.

Now, let $\mathfrak{m}$ be the maximal ideal of $R$, which is the image of $\mathfrak{n}$ modulo $I$. We have that $\mathfrak{m}/\mathfrak{m}^2$ is the quotient of $\mathfrak{n}/\mathfrak{n}^2$ by the subspace generated by the image of $I$ modulo $\mathfrak{n}^2$, and hence

$$\begin{aligned} \dim_{\mathbb{C}}(\mathfrak{m}/\mathfrak{m}^2) &= \dim_{\mathbb{C}}(\mathfrak{n}/\mathfrak{n}^2) - \dim_{\mathbb{C}}\langle\{f_i \bmod \mathfrak{n}^2\}\rangle = d - \dim_{\mathbb{C}}\langle\{\nabla_{\underline{a}}(f_i)\}\rangle \\ &= \text{dimension of tangent space to } Z_{\mathbb{C}}(I) \text{ at } \underline{a}. \end{aligned}$$

We find that $\dim(R) = \dim_{\mathbb{C}}(\mathfrak{m}/\mathfrak{m}^2)$ if and only if the tangent space to the variety at that point has the same dimension as the variety, which holds if and only if these gradient vectors generate a space of rank equal to the height of $I$ modulo $\mathfrak{n}$.

We summarize:

**Proposition 7.16.** *Let $R = \mathbb{C}[x_1, \dots, x_d]_{\mathfrak{n}}/I$, where $I = (f_1, \dots, f_t)$ is a prime of height $h$, and $\mathfrak{n}$ is a maximal ideal. The following are equivalent:*

- *$R$ is regular;*

- *The tangent space to $Z_{\mathbb{C}}(I)$ has dimension equal to* $\dim(R) = d$*;*

- $\mathfrak{n}$ *does not contain the ideal of $h \times h$ minors of the matrix*

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

The point of the third bullet is that when we go modulo $\mathfrak{n}$, the rows are the coordinates of $\nabla_{\underline{a}}(f_i)$ with respect to the basis $\{x_j - a_j\}$ in $\mathfrak{n}/\mathfrak{n}^2$, so we can use the rank of matrix to compute the dimension.

Note that this last condition matches the hypotheses of the implicit function theorem of calc 3 / differential geometry: the regular hypothesis for a complex variety at a point basically means locally diffeomorphic to $\mathbb{C}^{\dim(R)}$.

**Theorem 7.17** (Jacobian criterion (sufficiency))**.** *Let $K$ be an arbitrary field. Let $S = K[x_1, \dots, x_d]$, $\mathfrak{p} = (f_1, \dots, f_t)$ be a prime ideal of height $h$, $\mathfrak{q} \supseteq \mathfrak{p}$ be prime, and $R = (S/\mathfrak{p})_{\mathfrak{q}}$. Then $R$ is regular if $\mathfrak{q} \not\supseteq I_h(J)(S/\mathfrak{p})$, where*

$$J = \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_t}{\partial x_1} & \cdots & \frac{\partial f_t}{\partial x_n} \end{bmatrix}.$$

*Proof.* Wlog, the minor coming from $f_1, \dots, f_h$ and $x_1, \dots, x_h$ is nonzero modulo $\mathfrak{q}$. We claim that $f_1, \dots, f_h$ are regular parameters in $S_{\mathfrak{q}}$. Indeed, if $\sum s_i f_i \in \mathfrak{q}^2 S_{\mathfrak{q}}$, then clearing denominators, we get some $s \in S \smallsetminus \mathfrak{q}$ with $s(\sum s_i f_i) = \sum (ss_i) f_i = \sum q_k q'_k \in \mathfrak{q}^2$. Then, by the product rule, we get $\sum_i \frac{\partial(ss_i)}{\partial x_j} f_i + \sum_i ss_i \frac{\partial f_i}{\partial x_j} = \sum_k q'_k \frac{\partial q_k}{\partial x_j} + \sum_k q_k \frac{\partial q'_k}{\partial x_j} \in \mathfrak{q}$ for each $j$.

In $R$, this gives the relation $\sum \overline{ss_i} \frac{\partial f_i}{\partial x_j} \in \mathfrak{q}R$ for each $j$. Thus, in the residue field $R/\mathfrak{q}R$, this is a dependence relation on the vectors $v_j = (\frac{\partial f_1}{\partial x_j}, \dots, \frac{\partial f_h}{\partial x_j})$ for $j = 1, \dots, h$, which must be trivial by the hypothesis of the nonvanishing of the determinant. Thus, since $s \notin \mathfrak{q}$, we must have each $s_i \in \mathfrak{q}$, so the dependence relation is trivial, showing the claim.

Now, the regular parameters $f_1, \dots, f_h$ in $S_{\mathfrak{q}}$ generate a prime of height $h$ that is contained in $\mathfrak{p}S_{\mathfrak{q}}$, so equality must hold. Then, $R \cong S_{\mathfrak{q}}/(f_1, \dots, f_h)S_{\mathfrak{q}}$ is regular. □

**Example 7.18.**

1. Let $R = K[x, y, z]/(x^2 + y^2 + z^2 - 1)$ for $K$ a field of characteristic not two; if $K = \mathbb{R}$, this the the equation for the unit sphere. The matrix $J$ is $[2x, 2y, 2z]$. No prime of $R$ contains $(x, y, z)$, since it must also contain 1 in this case. We conclude that $R_{\mathfrak{p}}$ is regular for all $\mathfrak{p} \in \operatorname{Spec}(R)$.

2. Let $R = K[x, y, z]/(x^2 + y^2 + z^2)$ for $K$ a field of characteristic not two. The matrix $J$ is $[2x, 2y, 2z]$. We find that $R_{\mathfrak{p}}$ is regular possibly unless $\mathfrak{p} = (x, y, z)$. We see directly here that this ideal of height two is 3-generated, so $R_{(x,y,z)}$ is not regular.

3. Let $R = K[X_{2\times 3}]/I_2(X)$. We find that this is regular except possibly at $(X)$.

4. Let $R = K[X_{3\times 3}]/(\det(X))$. We find that this is regular except possibly for primes containing $I_2(X)$.

5. Let $R = K[x, y, z]/(x^2 - y^2 z)$. The matrix $J$ is $[2x, 2yz, y^2]$, and $\sqrt{I_1(J)} = (x, y)$, which has height one. $R_{(x,y)}$ is not regular, since it has dimension one, and $(x, y)/(x, y)^2$ is a two-dimensional $R_{(x,y)}/(x, y)R_{(x,y)} \cong K(z)$ vector space.

6. Without the Jacobian criterion, we can check that $\mathbb{Z}[x, y]_{(2,x,y)}/(2 - x^2 + y^2)$ is regular. First, $\mathbb{Z}[x, y]_{(2,x,y)}$ is a three-dimensional regular domain: a domain since it's a localization of a domain, and three-dimensional regular since killing 2 returns the 2-dim local domain $\mathbb{F}_2[x, y]_{(x,y)}$. Then, killing the nonzero element $(2 - x^2 + y^2)$ returns a 2 dimensional local ring. Now, $2 \in (x, y)$ in $R$, so the maximal ideal is generated by two things, and $R$ is regular.

7. However, $\mathbb{Z}[x, y]_{(2,x,y)}/(4-x^2+y^2)$ is not regular. It has dimension two by the same argument, but $(4, x, y)$ are linearly independent modulo $(2, x, y)^2$.

**Definition 7.19.** *A regular local ring of dimension one is called a* discrete valuation ring *or* DVR.

The point of the name is as follows: Let $(V, \mathfrak{m})$ be a DVR. We have $\mathfrak{m} = (\pi)$ for some $\pi \in V$. By Krull intersection, for any element of $R$, there is some $n$ such that $f \in \mathfrak{m}^n \smallsetminus \mathfrak{m}^{n+1}$. We can write $f = \pi^n v$, and $v \notin \mathfrak{m}$ must be a unit. Thus, there is a map ord from $R \smallsetminus 0$ to $\mathbb{N}$ given by $f \mapsto n$ as above. This map satisfies the rules $\operatorname{ord}(fg) = \operatorname{ord}(f)+\operatorname{ord}(g)$ and $\operatorname{ord}(f+g) \geq \min\{\operatorname{ord}(f), \operatorname{ord}(g)\}$. Such a map to an ordered group is called a *valuation*; the fact that the target group is $\mathbb{Z}$ makes it discrete.

Note that such a map extends to the fraction field of $V$ by the rule $\operatorname{ord}(f/g) = \operatorname{ord}(f) - \operatorname{ord}(g)$, and that, given the fraction field and this map, we can recover $V$ as the elements with nonnegative order.

**Example 7.20.** Some DVRs are $K[x]_{(x)}$, $K[x, y]_{(y-x^2)}$, $\mathbb{Z}_{(p)}$, and $\frac{K[x,y,u,v]_{(x,y)}}{(xu-yv)}$. For the last, note that $y = x(u/v)$.

**Exercise 7.21.** A DVR is normal.

**Surprisingly difficult theorem:** If $(R, \mathfrak{m})$ is regular, and $\mathfrak{p} \in \operatorname{Spec}(R)$, then $R_\mathfrak{p}$ is regular.

The key idea is the following:

**Theorem 7.22** (Auslander-Buchsbaum-Serre)**.** *Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring. The following are equivalent:*

- *$R$ is regular.*
- *For every finitely generated module $M$, there are finitely generated free modules $F_0, \ldots, F_t$ and maps*

$$0 \to F_t \xrightarrow{d_{t-1}} F_{t-1} \xrightarrow{d_{t-2}} \cdots \xrightarrow{d_1} F_1 \xrightarrow{d_0} F_0 \xrightarrow{d_{-1}} M \to 0$$

  *such that* $\ker(d_{i-1}) = \operatorname{im}(d_i)$ *for all $i$. This is called a* finite free resolution *of $M$.*
- *The residue field $k$ has a finite free resolution.*

*Proof of Surprisingly difficult theorem from Auslander-Buchsbaum-Serre:* Take a finite free resolution of $M = R/\mathfrak{p}$, and localize at $\mathfrak{p}$: this yields a finite free resolution of $\kappa(\mathfrak{p})$ as an $R_\mathfrak{p}$-module.

**Definition 7.23.** *A Noetherian ring is* regular *if $R_\mathfrak{m}$ is regular for all $\mathfrak{m} \in \operatorname{Max}(R)$, which, by the Theorem, is equivalent to $R_\mathfrak{p}$ is regular for all $\mathfrak{p} \in \operatorname{Spec}(R)$.*

Evidently, being regular is a local property.

## 7.3 Normal rings

So far, in discussing normal rings, we have focused on domains. While this is the main case of interest, there are some important reasons to generalize a bit.

We recall that for a ring $R$, its *total ring of fractions* is the localization of $R$ at the multiplicative set consisting of nonzerodivisors on $R$. This is the largest possible multiplicative set such that the ring embeds into the localization. We will write $K(R)$ for this.

Suppose that $R$ is reduced and Noetherian. Then the set of nonzerodivisors is the complement of the minimal primes of $R$. It follows that $K(R)$ is Noetherian and reduced (since these properties are preserved under localization) and zero dimensional (since all its primes are minimal). By the structure theory of Artinian rings we conclude that $R$ is a direct product of fields that are each of the form $K(R)/\mathfrak{a}'$ with $\mathfrak{a}' \in \operatorname{Min}(K(R))$. These correspond bijectively to $\mathfrak{a} \in \operatorname{Min}(R)$ (as the localizations), and the image in $R/\mathfrak{a}$ of the set of nonzerodivisors in $R$ is the set of nonzerodivisors of $R/\mathfrak{a}$. Thus, $K(R) \cong \prod_{\mathfrak{a} \in \operatorname{Min}(R)} K(R/\mathfrak{a})$, the product of fractions fields modulo minimal primes.

Note also that, for $\mathfrak{p} \in \operatorname{Spec}(R)$, the minimal primes of $R_{\mathfrak{p}}$ correspond to the minimal primes of $R$ that are contained in $\mathfrak{p}$, so there is a natural isomorphism $K(R_{\mathfrak{p}}) \cong \prod_{\mathfrak{a} \in \operatorname{Min}(R), \mathfrak{p} \supseteq \mathfrak{a}} K(R/\mathfrak{a}) \cong K(R)_{\mathfrak{p}}$.

Observe the corollary: any reduced Noetherian ring embeds as a subring into a finite product of fields.

**Definition 7.24.** *A ring that may or may not be a domain is* normal *if it is reduced and integrally closed in its total rings of fractions.*

**Lemma 7.25.** *If $R$ is reduced and Noetherian, and $x \in K(R)$, then $x \in R$ if and only $x \in R_{\mathfrak{p}}$ for all $\mathfrak{p}$ such that $\mathfrak{p} \in \operatorname{Ass}(R/(f))$ for some nonzerodivisor $f$.*

*Proof.* Write $x = r/u \in K(R)$ with $u$ a nonzerodivisor. If $x \notin R$, then $r \notin uR$, so $r(R/uR) \neq 0$. Thus, there is some $\mathfrak{p} \in \operatorname{Ass}(r(R/uR)) \subseteq \operatorname{Ass}(R/uR)$, and $(r(R/uR))_{\mathfrak{p}} \neq 0$ implies $r \notin uR_{\mathfrak{p}}$. □

**Lemma 7.26.** *If $R$ is Noetherian, and $f$ is a nonzerodivisor. If $\mathfrak{p} \in \operatorname{Ass}(R/fR)$, and $g$ is a nonzerodivisor in $\mathfrak{p}$, then $\mathfrak{p} \in \operatorname{Ass}(R/gR)$.*

*Proof.* Exercise now, or look for this to show up again in different words soon! □

**Theorem 7.27.** *Let $R$ be reduced and Noetherian. The following are equivalent:*

*(i) $R$ is integrally closed in its total ring of fractions;*

*(ii) $R$ is a direct product of normal domains;*

*(iii) For every nonzerodivisor $f \in R$ and every $\mathfrak{p} \in \operatorname{Ass}(R/(f))$, $R_{\mathfrak{p}}$ is a DVR;*

*(iv) The two conditions:*

*(a) The localization of $R$ at any height one prime is a DVR, and*

*(b) Every associated prime of a nonzerodivisor has height one.*

*Proof.* **(iii)⇔(iv):** This is all obvious once we see that any height one prime is associated to a nonzerdivisor. A height one prime is not contained in any minimal prime, hence not contained in the union of the minimal primes by prime avoidance. Since the associated primes are minimal by reducedness, such a prime must then contain a nonzerodivisor, and must be a minimal prime of this nonzerodivisor by the principal ideal theorem.

**(i)⇒(ii):** The ring $K(R)$ is a direct product of fields: $K(R) \cong \prod_{\mathfrak{p}_i \in \mathrm{Min}(R)} K(R/\mathfrak{p}_i)$. The elements $e_i \in K(R)$ consisting of 1 in just the $K(R/\mathfrak{p}_i)$ coordinate satisfy $e_i^2 - e_i = 0$, so are integral over $R$. These must live in $R$, so $R$ decomposes as a direct product $R \cong \prod_{\mathfrak{p}_i \in \mathrm{Min}(R)} R/\mathfrak{p}_i$. It is then easy to see that each $R/\mathfrak{p}_i$ must be integrally closed in $K(R/\mathfrak{p}_i)$.

**(ii)⇒(iii):** If $R$ is a direct product of rings $R = R_1 \times \cdots \times R_i \times \cdots \times R_n$, then the primes of $R$ are of the form $R_1 \times \cdots \times \mathfrak{q} \times \cdots \times R_n$, with $\mathfrak{q} \in \mathrm{Spec}(R_i)$. Moreover, the primes associated to a nonzerodivisor $(a_1, \dots, a_i, \dots, a_n)$ are of the form above, with $\mathfrak{q}$ associated to $a_i$. Thus, we can assume that $R$ is a normal domain.

Let $x$ be nonzero in $R$, and $\mathfrak{p}$ be associated to $(x)$. Let $S = R_\mathfrak{p}$, $\mathfrak{m} = \mathfrak{p}S$. We need to show that $\mathfrak{m}$ is principal. By NAK, $\mathfrak{m} \neq \mathfrak{m}^2$, so pick $y \in \mathfrak{m} \smallsetminus \mathfrak{m}^2$. We will see that $\mathfrak{m} = yS$. By the lemma above, $\mathfrak{m} \in \mathrm{Ass}(S/yS)$. Thus, there is $a \in S$ with $a \notin yS$, but $\mathfrak{m}a \subseteq yS$. If $a$ is a unit, $\mathfrak{m} = yS$, in which case we are done. So, suppose $a \in \mathfrak{m}$; we will obtain a contradiction. In this case, $a\mathfrak{m} \subseteq y\mathfrak{m}$; otherwise, $a\mathfrak{m} \subseteq yS$ but $a\mathfrak{m} \not\subseteq y\mathfrak{m}$, so there is some $m \in \mathfrak{m}$ and $u$ a unit with $am = yu$, then $yu \in \mathfrak{m}^2$ implies $y \in \mathfrak{m}^2$, a contradiction.

Let $\mathfrak{m} = (f_1, \dots, f_n)$. We can now write $af_i = y \sum_j r_{ij} f_j$. In the fraction field of $S$, we have $\frac{a}{y} f_i = \sum_j s_{ij} f_j$. By the usual determinant trick, $\det(\frac{a}{y} I - [s_{ij}]) = 0$. That is, $\frac{a}{y}$ satisfies a monic polynomial with coefficients in $S$, which is normal, so $a/y \in S$, so $a \in yS$, the desired contradiction.

**(iii)⇒(i):** Let $x \in K(R)$ be integral over $R$. By using the same dependence relation, we find that the image of $x$ in $K(R)_\mathfrak{p} \cong K(R_\mathfrak{p})$ is integral over $R_\mathfrak{p}$ for all $\mathfrak{p} \in \mathrm{Spec}(R)$. In particular, this is true for every prime $\mathfrak{p}$ associated to a nonzerodivisor. Each such $R_\mathfrak{p}$ is a DVR, hence normal, so $x \in R_\mathfrak{p}$ for each such $\mathfrak{p}$, and by the lemma above, $x \in R$. □

**Corollary 7.28.** *In a Noetherian normal domain, the stronger version of the principal ideal theorem holds: every associated prime of principal ideal has height one.*

**Corollary 7.29.** *If $R$ is a Noetherian normal domain, every nonzero nonunit element $f \in R$ has a primary decomposition of the form $(f) = \mathfrak{p}_1^{(e_1)} \cap \cdots \cap \mathfrak{p}_t^{(e_t)}$, with $\mathfrak{p}_i$ of height one, and $e_i = \mathrm{ord}_i(f)$, where* $\mathrm{ord}_i$ *is the discrete valuation associated to the DVR $R_{\mathfrak{p}_i}$.*

*In particular, in a Noetherian normal domain, any element is determined up to unit by its vanishing set (minimal primes $\{\mathfrak{p}_i\}$) and order of vanishing on each $\mathfrak{p}_i$.*

*Proof.* We have $(f) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$, with $\mathfrak{q}_i$ primary to $\mathfrak{p}_i$ of height one. We compute $\mathfrak{q}_i$ by expanding and contracting to the localization: $\mathfrak{q}_i = fR_{\mathfrak{p}_i} \cap R$. By definition of order, $fR_{\mathfrak{p}_i} = (\mathfrak{p}_i)^{e_i} R_{\mathfrak{p}_i}$. By definition of symbolic power, $(\mathfrak{p}_i)^{e_i} R_{\mathfrak{p}_i} \cap R = \mathfrak{p}_i^{(e_i)}$. □

**Example 7.30.**

1. If $R$ is a UFD, then every height one prime is principal, and the minimal primary decomposition above corresponds to the unique factorization into prime powers.

2. Let $R = \mathbb{C}[x, y, u, v]/(xy - uv)$. The ideal generated by $x$ is not prime, but factors as $(x) = (x, u) \cap (x, v)$.

# Chapter 8

# Filtrations and completions

We often want to study the powers of an ideal. The basic piece of terminology to get started is the following.

**Definition 8.1.** *Let $I$ be an ideal in a ring $R$. The* standard $I$-adic filtration *on $R$ is*

$$\cdots \subseteq I^n \subseteq I^{n-1} \subseteq \cdots \subseteq I \subseteq R.$$

*Likewise, if $M$ is an $R$ module, the* standard $I$-adic filtration *on $M$ is*

$$\cdots \subseteq I^n M \subseteq I^{n-1} M \subseteq \cdots \subseteq IM \subseteq M.$$

The standard $I$-adic filtration tells us which power of $I$ an element lives in. We might think of elements in large powers of $I$ as vanishing to a high order along $V(I)$ (as an intuitive definition), so elements that are deep in the filtration are “close to zero” $I$-adically. This motivates the following definition.

**Definition 8.2.** *The* $I$-adic topology *on $R$ is the topology with open basis $\{r + I^n \mid r \in R, n \in \mathbb{N}\}$. The* $I$-adic topology *on a module $M$ is the topology with open basis $\{m + I^n M \mid m \in R, n \in \mathbb{N}\}$.*

We leave it to you to verify that these sets satisfy the necessary condition for an open basis. Even better, note that this topology corresponds to a pseudometric space given by the pseudometric $|x - y| = e^{-\max\{n \ \mid \ x-y \in I^n\}}$, which satisfies a stronger (nonarchimedean) version of the triangle inequality: $|x - y| \leq \max\{|x - z|, |y - z|\}$. We recall that a pseudometric is a metric that might have distinct points of distance zero apart.

Here are three important constructions coming from the $I$-adic filtration.

1. **The Rees ring:** We can package all of the filtered pieces into one ring. Let $t$ be an indeterminate. The *Rees ring* of $I$ is the ring

$$R[It] = R \oplus It \oplus I^2 t^2 \oplus I^3 t^3 \oplus \cdots \subseteq R[t].$$

The *Rees module* of $I$ on $M$ is

$$M[It] = M \oplus IMt \oplus I^2 M t^2 \oplus I^3 M t^3 \oplus \cdots \subseteq M[t].$$

Observe that $M[It]$ is a module over $R[It]$ that is generated by $M$. We generally consider Rees rings and modules as $\mathbb{N}$-graded by given $t$ degree 1, and everything in $R$ degree zero.

2. **The associated graded ring:** We can also make a graded ring out of $R$. The associated graded ring of $R$ with respect to $I$ is

$$\mathrm{gr}_I(R) := R/I \oplus I/I^2 \oplus I^2/I^3 \oplus \cdots ,$$

where we give the elements of $I^i/I^{i+1}$ degree $i$. Check that the multiplication is well-defined! We end up with an $\mathbb{N}$-graded ring that has many uses. There is also the module version:

$$\mathrm{gr}_I(M) := M/IM \oplus IM/I^2M \oplus I^2M/I^3M \oplus \cdots ,$$

which is a $\mathrm{gr}_I(R)$-module.

3. **The completion:** The completion as a topological space of $R$ is another ring that is closely related to $R$ but has better "compactness" type properties. We will discuss this in more detail.

We want to note now before we do anything else that all three of these constructions can be done for wider classes of filtrations.

The following definition is a generalization of the $I$-adic filtration.

**Definition 8.3.** *1. A filtration on a module $M$ by submodules,*

$$\cdots \subseteq M_n \subseteq M_{n-1} \subseteq \cdots \subseteq M_1 \subseteq M_0 = M,$$

*is $I$-*consistent *if $IM_i \subseteq M_{i+1}$ for all $i$.*

*2. The filtration is $I$-*stable *if it is $I$-consistent and, for some $c \in \mathbb{N}$, $IM_j = M_{j+1}$ for all $j > c$.*

**Remark 8.4.** An $I$-consistent filtration as above is $I$-stable if and only if there is some $c$ such that $I^nM_c = M_{n+c}$ for all $n$.

**Lemma 8.5.** *1. A filtration on $M$ as above is $I$-consistent if and only if the subset*

$$\widetilde{M} = M \oplus M_1t \oplus M_2t^2 \oplus M_3t^3 \oplus \cdots \subseteq M[t]$$

*is an $R[It]$-submodule of $M[t]$.*

*2. The filtration is $I$-stable if and only if $\widetilde{M}$ is generated by elements of degree $\leq n$ for some $n$.*

*In particular, if $M$ is finitely generated, the filtration is $I$-stable if and only if $\widetilde{M}$ is a finitely generated $R[It]$-module.*

*Proof.* The condition that $IM_i \subseteq M_{i+1}$ for all $i$ translates into $\widetilde{M}$ being an $R[It]$-submodule: $\widetilde{M}$ is always closed under addition, and $R[It]$ is generated by $R$ and $It$; $\widetilde{M}$ is always closed under multiplication by $R$, and closure under multiplication by $It$ is the same as the stated condition.

Now, $\widetilde{M}$ is generated in degree $\leq n$ if and only if its homogeneous elements of degree at least $n$ are generated by things of lower degree, i.e., $[\widetilde{M}]_j = \sum_{i\leq n}[R[It]]_{j-i}[\widetilde{M}]_i$ for all $j > n$, which is equivalent to $M_j = \sum_{i\leq n} I^{j-i}M_i$ for all $j > n$. By the condition, $IM_i \subseteq M_{i+1}$, we have $\sum_{i\leq n} I^{j-i}M_i = I^{j-n}M_n$. The equivalence is now clear. □

**Theorem 8.6** (Artin-Rees Lemma). *Let $R$ be a Noetherian ring, $N \subseteq M$ finitely generated modules, and $I$ an ideal. If $\{M_i\}$ is an $I$-stable filtration of $M$, then $\{M_i \cap N\}$ is an $I$-stable filtration of $N$.*

*Proof.* Since $R$ is Noetherian, $I$ is a finitely generated ideal, and the Rees ring $R[It]$ is Noetherian since it is a finitely generated $R$-algebra. Now, $\widetilde{M} = \bigoplus M_i t^i \subseteq M[t]$ is a finitely generated $R[It]$-module by the Lemma. Now, $I(N \cap M_i) \subseteq IN \cap IM_i \subseteq N \cap IM_{i+1}$, so $\widetilde{N} = \bigoplus (N \cap M_i)t^i \subseteq N[t]$ is an $R[It]$-module by the Lemma. But, $\widetilde{N}$ is a submodule of $\widetilde{M}$. By Noetherianity, it is finitely generated, so we are done. □

**Corollary 8.7.** *Let $R$ be a Noetherian ring, and $N \subseteq M$ finitely generated modules. Then there is some $c$ such that $I^{n+c}M \cap N \subseteq I^n N$ for all $n$.*

*Proof.* We have some $c$ such that $I^n(I^c M \cap N) = I^{n+c}M \cap N$, so that $I^n N \supseteq I^n(I^c M \cap N) = I^{n+c}M \cap N$ for all $n$. □

**Corollary 8.8** (Krull intersection theorem)**.** *Let $R$ be a Noetherian ring, $I$ an ideal, and $M$ a finitely generated $R$-module. Then there is some $a \in I$ such that $a$ acts as the identity map on $\bigcap_{n\in\mathbb{N}} I^n M$. In particular,*

- *If $R$ is a domain, then $\bigcap_{n\in\mathbb{N}} I^n = 0$, (so $R$ is Hausdorff in the $I$-adic topology) and*
- *If $(R, \mathfrak{m})$ is local, and $M$ is finitely generated, then $\bigcap_{n\in\mathbb{N}} I^n M = 0$ (so $M$ is Hausdorff in the $I$-adic topology).*

*Proof.* Set $N \subseteq M$ to be $\bigcap_{n\in\mathbb{N}} I^n M$. By the definition and Artin-Rees, for some $c$, we have $N \subseteq I^{c+1}M \cap N \subseteq IN$, so $N = IN$. The first statement follows from NAK, and the others follows directly. □

We now discuss completions.

A *Cauchy sequence* in a module $M$ in the $I$-adic topology is simply a Cauchy sequence in the $I$-adic topology metric space. Namely, it is a sequence of elements $\{m_i\}$ such that for each $n \in \mathbb{N}$, there is some $N$ such that $m_i - m_j \in I^n$ for all $i, j < N$. Two Cauchy sequences $\{m_i\}, \{m_i'\}$ are equivalent if for each $n \in \mathbb{N}$, there is some $N$ such that $m_i - m_i' \in I^n M$ for all $i > N$. It is easy to see that

- the (termwise) sum, difference, or product of two Cauchy sequences in $R$ is Cauchy, so the set of Cauchy sequences in $R$ forms a ring,
- the set of Cauchy sequences that are equivalent to the constant zero sequence is an ideal,
- the set of equivalence classes of Cauchy sequences forms a ring.

The ring we have specified is the *$I$-adic completion* of $R$, denoted $\widehat{R}^I$.

Similarly,

- termwise addition, subtraction, and scalar multiplication of a Cauchy sequences in $R$ and Cauchy sequences in $M$ return Cauchy sequences in $M$,
- this descends to a well-defined $\widehat{R}^I$-module structure on the set of equivalence classes of Cauchy sequences on $M$.

The module we have specified is the *$I$-adic completion* of $M$, denoted $\widehat{M}^I$. Evidently, these objects are topological/metric space completions of $R$ and $M$ in the $I$-adic topology.

If $(R, \mathfrak{m})$ is a local ring, we just write $\widehat{R}$ for $\widehat{R}^{\mathfrak{m}}$, and call this simply *the completion of* $R$. We say that a local ring is *complete* if it is isomorphic to its completion.

**Proposition 8.9.** *There are ring maps $R \to \widehat{R}^I$ and $R$-module maps $M \to \widehat{M}^I$ for each $I$ given by sending an element to the constant sequence. The kernel of these maps is $\bigcap_{n\in\mathbb{N}} I^n M$.*

**Proposition 8.10.** *Let $R$ be Noetherian, and $N \subseteq M$ be finitely generated $R$-modules, and $I$ an ideal.*

1. *If $\{n_i\} \subseteq N$ is a Cauchy sequence in the $I$-adic topology on $M$, then $\{n_i\}$ is a Cauchy sequence in the $I$-adic topology on $N$.*
2. *If $\{n_i\} \subseteq N$ converges to $0$ in the $I$-adic topology on $M$, then $\{n_i\}$ converges to $0$ in the $I$-adic topology on $N$.*
3. *The sequence of $\widehat{R}$-modules $0 \to \widehat{N}^I \to \widehat{M}^I \to \widehat{(M/N)}^I \to 0$ is exact.*

*Proof.*

1. This is a direct consequence of the corollary of Artin-Rees: $n_i - n_j \in I^{a+c}M \cap N \subseteq I^a N$; for any large $a$, this happens for sufficiently large $i, j$ ...
2. Again by Artin Rees: $n_i \in I^{a+c}M \cap N \subseteq I^a N$.
3. The map $\widehat{N}^I \to \widehat{M}^I$ is well-defined and injective by the previous parts. We can prove the other conditions for exactness directly here, or observe them as a consequence of another theorem soon. □

To understand these objects, we want a better way of expressing elements. For an element $f = [\{r_i\}] \in \widehat{R}^I$, for any $n$, there is a unique $f_n \in R/I^n$ such that for any representative, there is some $N$ such that $r_i \bmod I^n = f_n$ for all $i > N$. Thus, we get a well-defined notion of $f$ modulo $I^n$, and we obtain a standard form for $f$ as the sequence $(f_1, f_2, f_3, \dots)$ with $f_i \in R/I^i$, and $f_i \equiv f_{i-1} \bmod I^{i-1}$ (consistent sequence).

Another more intuitive form for writing elements starts with the form as above. By the conditions $f_i \equiv f_{i-1} \bmod I^{n-1}$, we can take $g_0 \in R$ with $g \equiv f_1 \bmod I$, $g_i \in R$ with $g_i = f_i - f_{i-1} \in I^{i-1} \bmod I^{i-1}$, and write $f = g_0 + g_1 + g_2 + \cdots$. The partial sums represent the elements $f_i$ modulo $I^i$, and hence form a Cauchy sequence.

**Example 8.11.** Let's compute the completion of $R = K[x_1, \dots, x_n]$ with respect to the ideal $I = (x_1, \dots, x_n)$. Any element of $R/I^n$ is represented by a polynomial $f_n$ of degree at most $n-1$, and these for a consistent sequence if $f_{n+1} - f_n$ is homogeneous of degree $n$. Thus, a consistent sequence corresponds to a unique power series, and $\widehat{R}^I = K[\![x_1, \dots, x_n]\!]$.

The same computation shows that $\widehat{K[\underline{x}]_{(\underline{x})}} = K[\![\underline{x}]\!]$.

**Proposition 8.12.** *If $R$ is a Noetherian ring, $I$ an ideal, and $M$ finitely generated, then $\widehat{M}^I \cong \widehat{R} \otimes_R M$.*

*Proof.* Consider the maps $\theta_M : \widehat{R} \otimes_R M \to \widehat{M}$ given on simple tensors by the rule $\{r_i\} \otimes m \mapsto \{r_i m\}$. Clearly, $\theta_R$ is an isomorphism, and $\theta_{R^{\oplus n}}$ is an isomorphism (an $n$-tuple of consistent sequences is a consistent sequence of $n$-tuples...). Now, take a presentation for $M$: $R^m \to R^n \to M \to 0$, and consider the commutative diagram

$$\begin{tikzcd}
R^m \otimes_R \widehat{R} \arrow[r] \arrow[d, "\theta_{R^m}"] & R^n \otimes_R \widehat{R} \arrow[r] \arrow[d, "\theta_{R^n}"] & M \otimes_R \widehat{R} \arrow[r] \arrow[d, "\theta_M"] & 0 \\
\widehat{R^m} \arrow[r] & \widehat{R^n} \arrow[r] & \widehat{M} \arrow[r] & 0.
\end{tikzcd}$$

The first two vertical maps are isomorphisms, so the last is as well. □

**Corollary 8.13.** *If $R$ is a local ring, and $I$ an ideal, then $\widehat{R/I} \cong \widehat{R}/I\widehat{R}$. In particular, $\widehat{\frac{K[\underline{x}]_{(\underline{x})}}{I}} \cong \frac{K[\![\underline{x}]\!]}{IK[\![\underline{x}]\!]}$.*

*Proof.* We have $\widehat{R/I} \cong \widehat{R} \otimes_R R/I \cong \widehat{R}/I\widehat{R}$. □

**Exercise 8.14.** Let $R$ be a ring, and $F$ be an $R$-module. If, for every injective map of finitely generated modules $N \xrightarrow{\alpha} M$, the map $F \otimes \alpha$ is injective, then $F$ is flat.

**Theorem 8.15.** *$\widehat{R}^I$ is a flat $R$-algebra.*

*Proof.* This follows from the last few results. □

**Proposition 8.16.** *If $R$ is Noetherian, and $I$ an ideal, then $\widehat{R}^I$ is Noetherian.*

**Theorem 8.17** (Cohen structure theorem)**.** *Let $(R, \mathfrak{m}, k)$ be a complete Noetherian local ring.*

1. *One can write $R \cong A[\![\underline{x}]\!]/I$, where*

   - *$A \cong K$, a field, if $R$ has equal characteristic, or*
   - *$A \cong V$, a complete DVR with uniformizer $p$ if $R$ has mixed characteristic.*

   *That is, every complete local ring is a quotient of a power series ring.*

2. *$R$ is regular if and only if*

   - *$R \cong K[\![\underline{x}]\!]$ in equal characteristic, or*
   - *either $R \cong V[\![\underline{x}]\!]$ or $R \cong V[\![\underline{x}]\!]/(p - f)$ with $f \in \mathfrak{m}^2$ in mixed characteristic.*

3. *There exists a power series ring $S = K[\![\underline{y}]\!]$ or $S = V[\![\underline{y}]\!]$ such that $S \subseteq R$ is module-finite.*

4. *If $R$ has equal characteristic, there exists a subfield $K \subseteq R$ such that the composition $K \subseteq R \to k$ is an isomorphism. Such a $K$ is called a* coefficient field *for $R$. In (1)–(3), one can choose a coefficient field for the stated $K$.*

The proof of this theorem is beyond the scope of these notes. Everyone who uses commutative algebra should know it though! This special classification serves as a good proxy for a classification theorem for all local rings. In fact, for many problems, one can reduce to the local case, and then reduce to the complete local case (using flatness), and pretend we are dealing with a quotient of a power series ring!

# Chapter 9

# Depth

## 9.1 Regular sequences and depth

**Definition 9.1.** *A sequence of elements $x_1, \dots, x_t$ in a ring $R$ is a* regular sequence *on a module $M$ if*

- *$x_1$ is a nonzerodivisor on $M$,*
- *$x_2$ is a nonzerodivisor on $M/x_1M$,*

  ⋮ ⋮ ⋮
- *$x_t$ is a nonzerodivisor on $M/(x_1, \dots, x_{t-1})M$, and*
- *$M \neq (x_1, \dots, x_t)M$.*

*A regular sequence $x_1, \dots, x_t$ is maximal if there is no regular sequence of the form $x_1, \dots, x_t, x_{t+1}$. When we don't specify a module $M$, we mean a regular sequence on $R$.*

**Remark 9.2.** We say that a sequence $x_1, \dots, x_t$ in a ring $R$ is a *prime sequence* if each of the ideals $(x_1)$, $(x_1, x_2)$, …, $(x_1, \dots, x_t)$ is prime and distinct. A prime sequence is a regular sequence, since the image of each $x_i$ is a nonzero modulo $(x_1, \dots, x_{i-1})$ by distinctness, and a nonzerodivisor in the quotient, since the quotient is a domain. The final condition is because a prime ideal is proper.

**Example 9.3.**

1. The sequence of variables in a polynomial ring over a field is a prime sequence, hence a regular sequence.
2. More generally, a sequence of monomials in a polynomial ring over a field is a regular sequence if and only if no pair has a common variable factor (check it!).
3. In $K[x, y, z]$, the sequence $x, y(x-1), z(x-1)$ is a regular sequence: $x$ is a nonzerodivisor, and modulo $x$, the next two elements are equivalent to $y, z$. However, if we permute to $y(x-1), z(x-1), x$, we have $y \notin (y(x-1))$, but $yz(x-1) \in (y(x-1))$, so this is not a regular sequence.

**Lemma 9.4.** *If $(R, \mathfrak{m})$ is a local ring, and $(f_1, \dots, f_t)$ is a regular sequence, then $(f_{\sigma(1)}, \dots, f_{\sigma(t)})$ is a regular sequence for any $\sigma \in \Sigma_t$.*

*If $R$ is graded, and the $f$'s are homogeneous, the same holds.*

*Proof.* In either case, it suffices to show the statement for two elements $f, g$, since any permutation is a product of transpositions of adjacent elements.

If $f, g$ is a regular sequence, we need to show that $g, f$ is; i.e., that $g$ is a nonzerodivisor on $R$, and $f$ is a nonzerodivisor on $R/gR$.

Suppose $gr = 0$ in $R$. We know $g$ is a nonzerodivisor in $R/fR$, so $g\overline{r} = 0$ in $R/fR$ implies $\overline{r} = 0$ in $R/fR$, so $r = fr'$ for some $r' \in R$. Now, $gfr' = 0$ in $R$ implies $gr' = 0$, since $f$ is a nonzerodivisor in $R$. Thus, if $I = \operatorname{ann}_R(g)$, then $I = fI$, so $I = \mathfrak{m}I$, and hence $I = 0$ by NAK. That is, $g$ is a nonzerodivisor in $R$.

Now, suppose $fr \in (g)$. We can write $fr = gr'$, so $gr' \in (f)$, and then $r' \in (f)$, by hypothesis. We can write $r' = fr''$, so $fr = fgr''$. Now, $f$ is a nonzerodivisor, so $r = gr''$, so that $r \in (g)$, as required. □

**Remark 9.5.** If $R$ is Noetherian, then every regular sequence extends to a *maximal* one: one that does not extend to a longer one. This is just because a counterexample would lead to an infinite ascending chain of ideals.

Likewise, if $M$ is finitely generated, every regular sequence on $M$ extends to a maximal one.

Also, if $(R, \mathfrak{m})$ is local, a regular sequence on $R$ must consist of parameters, since a nonzerodivisor is not in any minimal prime, and thus quotienting out by one decreases dimension by one.

**Theorem 9.6.** *If $(R, \mathfrak{m})$ is a Noetherian local ring, and $M$ a finitely generated module, then every maximal regular sequence on $M$ has the same length.*

*Proof.* Let $a_1, \dots, a_n$ be a maximal regular sequence on $M$ with $n$ minimal. It suffices to show that for any other regular sequence $b_1, \dots, b_n$, then every element of $\mathfrak{m}$ is a zerodivisor on $M/(b_1, \dots, b_n)$. We show the statement for all modules $M$ by induction on $n$.

If $n = 0$, $\mathfrak{m}$ consists only of zerodivisors on $M$, so there is nothing to do.

If $a_1$ is a maximal regular sequence on $M$, every element of $\mathfrak{m}$ must be a zerodivisor on $M/a_1M$, so $\mathfrak{m} = \bigcup_{\operatorname{Ass}(M/a_1M)} \mathfrak{p}$, and hence $\mathfrak{m} \in \operatorname{Ass}(M/a_1M)$ by prime avoidance. Thus, there is some $m \in M$ with $\mathfrak{m}m \subseteq a_1M$. In particular, we have $b_1m = a_1m'$ for some $m' \in M$. Note that $m' \notin b_1M$, since this would give $m \in a_1M$. We claim $\mathfrak{m}m' \subseteq b_1M$. Indeed, $a_1\mathfrak{m}m' = b_1\mathfrak{m}m \subseteq a_1b_1M$, and the claim follows from the fact $a_1$ is a nonzerodivisor.

Now suppose the claim is true for all modules in which there is a maximal regular sequence of length $< n$. Take an element $c \in \mathfrak{m}$ that is a nonzerodivisor on $M/(a_1, \dots, a_i)M$ and $M/(b_1, \dots, b_i)M$ for all $i < n$: we can do this by prime avoidance, since we are looking for elements in $\mathfrak{m}$ that avoid the finitely many associated primes of these finitely many ideals. In particular, $a_1, \dots, a_{n-1}, c$ and $b_1, \dots, b_{n-1}, c$ are regular sequences. We know that $a_1, \dots, a_{n-1}, c$ is a maximal regular sequence by the case $n = 1$ applied to $M/(a_1, \dots, a_{n-1})M$. By the lemma above, $c, a_1, \dots, a_{n-1}$ and $c, b_1, \dots, b_{n-1}$ are regular sequences. We have that $a_1, \dots, a_{n-1}$ is a maximal regular sequence on $M/cM$, and by the IH, $b_1, \dots, b_{n-1}$ is a maximal regular sequence on $M/cM$, so $b_1, \dots, b_{n-1}, c$ is a maximal regular sequence on $M$. By the $n = 1$ case again, we find that $b_1, \dots, b_n$ a maximal regular sequence on $M$. □

**Definition 9.7.** *Let $(R, \mathfrak{m})$ be a local ring. The* depth *of a module $M$ is the maximal length of a regular sequence on $M$, denoted* $\operatorname{depth}(M)$. *The* depth *of $R$ is* $\operatorname{depth}(R)$.

**Remark 9.8.** The depth of a local ring is bounded above by its dimension.

**Proposition 9.9.** *Let $R$ be Noetherian local.*

1. *For $\mathfrak{p} \in \operatorname{Spec}(R)$, $\operatorname{depth}(R_\mathfrak{p}) = 0$ if and only if $\mathfrak{p}R_\mathfrak{p} \in \operatorname{Ass}(R_\mathfrak{p})$ if and only if $\mathfrak{p} \in \operatorname{Ass}(R)$.*

2. *If* $\mathfrak{p} \in \operatorname{Spec}(R)$*,* $\operatorname{depth}(R_{\mathfrak{p}}) = 1$ *if and only if* $\mathfrak{p} \notin \operatorname{Ass}(R)$*, but* $\mathfrak{p} \in \operatorname{Ass}(R/(f))$ *for all* $f \notin \operatorname{Ass}(R)$*.*

**Remark 9.10.** For $\mathfrak{p} \in \operatorname{Spec}(R)$, $\dim(R_{\mathfrak{p}}) = 0$ if and only if $\mathfrak{p}R_{\mathfrak{p}} \in \operatorname{Min}(R_{\mathfrak{p}})$ if and only if $\mathfrak{p} \in \operatorname{Min}(R)$. If $\mathfrak{p} \in \operatorname{Spec}(R)$, $\dim(R_{\mathfrak{p}}) = 1$ if and only if $\mathfrak{p} \notin \operatorname{Min}(R)$, but $\mathfrak{p} \in \operatorname{Min}(R/(f))$ for all $f \notin \operatorname{Min}(R)$. In this way, depth can be thought of as an analogue of dimension where minimal primes are replaced by the more sophisticated notion of associated primes.

**Example 9.11.**

1. The depth of $K[x,y]_{(x,y)}/(x^2,xy)$ is zero, since every nonunit kills $x$, so there are no nonzerodivisors.

2. The depth of the two dimensional ring $K[x,y,z]_{(x,y,z)}/(xy,xz)$ is one. Indeed, there is a nonzerodivisor $x-z$. We can see that this is a nonzerodivisor by noting that $(xy,xz) = (x) \cap (y,z)$, so the associated primes of $(xy,xz)$ in $K[x,y,z]_{(x,y,z)}$ are $(x)$ and $(y,z)$. Thus, the associated primes of the ring are $(x)$ and $(y,z)$, and the element we found is not in the union of these, hence is a nonzerodivisor. Now, we want to see that $x-z$ is a maximal regular sequence. The quotient is isomorphic to $K[x,y]_{(x,y)}/(x^2,xy)$!

3. The depth of $K[x,y,z]_{(x,y,z)}/(x^2-yz)$ is two. $y,z$ is a regular sequence, and there can be no longer, for dimension reasons.

**Theorem 9.12.** *Let* $(R,\mathfrak{m})$ *be local, and* $M$ *be finitely generated. Then* $\operatorname{depth}(M) \leq \operatorname{Min}_{\mathfrak{p}\in\operatorname{Ass}(M)} \dim(R/\mathfrak{p})$*.*

*Proof.* We proceed by induction of the depth of $M$. The base case of depth zero is trivial.

For the inductive step, we have some nonzerodivisor $x \in \mathfrak{m}$ on $M$. Fix $\mathfrak{p} \in \operatorname{Ass}(M)$.

Take $z$ such that $Rz \subseteq M$ is a maximal element in the set $\{Ra \subseteq M \mid \mathfrak{p}(Ra) = 0\}$. We claim that $\overline{z} \in M/(x)M$ is nonzero. If not, $z = xz'$ for some $z' \in M$. Note that, for $p \in \mathfrak{p}$, $pz = pxz' = 0$, and $x$ a nonzerodivisor implies $pz' = 0$, so $\mathfrak{p}z' = 0$, and $Rz \subsetneq Rz'$, a contradiction. We note also that $\mathfrak{p} + (x) \subseteq \operatorname{ann}(\overline{z})$.

Since $\mathfrak{p} + (x)$ annihilates a nonzero element of $M/xM$, there is an associated prime $\mathfrak{q}$ of $M/xM$ containing this ideal. In particular $\mathfrak{q} \supsetneq \mathfrak{p}$. Now, using the inductive hypothesis, $\operatorname{depth}(M) - 1 = \operatorname{depth}(M/xM) =\leq \dim(R/\mathfrak{q}) \leq \dim(R/\mathfrak{p}) - 1$, and the theorem follows. □

**Example 9.13.** The inequality can be sharp. The ring $\dfrac{K[u,v,x,y]_{(u,v,x,y)}}{(xu,xv,yu,yv)}$ has two associated primes $(u,v)$ and $(x,y)$, each of dimension two. However, if we quotient out by the nonzerodivisor $u-x$, we get the ring $\dfrac{K[u,v,y]_{(u,v,y)}}{(u^2,uv,yu,yv)}$, in which $u$ is annihilated by the maximal ideal, so the depth is only one.

## 9.2 Cohen-Macaulay rings

**Definition 9.14.** *A Noetherian local ring is* Cohen-Macaulay *if* $\operatorname{depth}(R) = \dim(R)$*. A finitely generated module over a Noetherian local ring is a* Cohen-Macaulay module *if* $\operatorname{depth}(M) = \dim(M)$*. It is a* maximal Cohen-Macaulay module *if* $\operatorname{depth}(M) = \dim(M) = \dim(R)$*.*

One nice consequence of the Cohen-Macaulay property is unmixedness.

**Proposition 9.15.** *If* $M$ *is a Cohen-Macaulay* $R$*-module, then* $\operatorname{depth}(M) = \dim(R/\mathfrak{p})$ *for every* $\mathfrak{p} \in \operatorname{Ass}(M)$*. In particular, if* $R$ *is a Cohen-Macaulay ring, then* $R$ *has no embedded primes, and* $\dim(R/\mathfrak{p}) = \dim(R)$ *for each* $\mathfrak{p} \in \operatorname{Min}(R)$*.*

*Proof.* This follows from the inequality on depth and dimension of associated primes: $\dim(M) = \max\{\dim(R/\mathfrak{p}) \mid \mathfrak{p} \in \mathrm{Ass}(M)\} \geq \min\{\dim(R/\mathfrak{p}) \mid \mathfrak{p} \in \mathrm{Ass}(M)\} \geq \mathrm{depth}(M)$, so equality holds throughout, and for each $\dim(R/\mathfrak{p})$ with $\mathfrak{p} \in \mathrm{Ass}(M)$. □

**Remark 9.16.** If $(R, \mathfrak{m})$ is Cohen-Macaulay, and $x_1, \dots, x_a$ is a regular sequence in $R$, then $R/(x_1, \dots, x_a)$ is Cohen-Macaulay. Indeed, each $x_i$ is nonzerodivisor modulo the previous $x$'s, so $\dim(R/(x_1, \dots, x_a)) = \dim(R) - a$, and each $x_i$ decreases the depth by 1.

**Proposition 9.17** (Regular sequences and systems of parameters)**.** *Let $f_1, \dots, f_t$ be a sequence of elements in a Noetherian local ring $(R, \mathfrak{m})$. For the conditions*

*(i)* $f_1, \dots, f_t$ *is a regular sequence;*

*(ii)* $\mathrm{ht}((f_1, \dots, f_i)) = i$ *for all* $i$*;*

*(iii)* $\mathrm{ht}((f_1, \dots, f_t)) = t$*;*

*(iv)* $f_1, \dots, f_t$ *is part of a system of parameters for* $R$*,*

*we have (1)⇒(2)⇒(3)⇒(4) in general, and if $R$ is Cohen-Macaulay, (4)⇒(1), so all of the above are equivalent.*

*Proof.* **(1)⇒(2):** By Krull height, $\mathrm{ht}((f_1, \dots, f_i)) \leq i$ for all $i$ always. The condition that $f_i$ is a nonzerodivisor in $R/(f_1, \dots, f_{i-1})$ implies that $f_i$ is not in any associated prime, hence any minimal prime, of $(f_1, \dots, f_{i-1})$ so its height is larger. Inductively, we get the equality.

**(2)⇒(3):** Trivial.

**(3)⇒(4):** $\mathrm{ht}((f_1, \dots, f_t)) + \dim(R/(f_1, \dots, f_t)) \leq \dim(R)$, so $\dim(R) - \dim(R/(f_1, \dots, f_t)) \geq t$, which makes these elements parameters.

**(4)⇒(1) if $R$ is CM:** It suffices to show the statement when $t = \dim(R)$, so that $f_1, \dots, f_d$ is a system of parameters. Since $f_1$ is a parameter, it is not in any minimal prime, hence not in any associated prime by unmixedness. Thus $f_1$ is a nonzerodivisor. Now, $R/(f_1)$ is Cohen-Macaulay, so by induction on dimension, we are done. □

**Corollary 9.18.** *Let $(R, \mathfrak{m})$ be a Noetherian local ring. The following are equivalent:*

- *$R$ is Cohen-Macaulay;*
- *Some system of parameters of $R$ is a regular sequence;*
- *Every system of parameters of $R$ is a regular sequence.*

*Proof.* The equivalence of the first two is basically the definition. The equivalence of the second two comes from the last theorem. □

**Example 9.19.**

1. Every regular local ring is Cohen-Macaulay, since a regular system of parameters is a prime sequence. In particular, $K[\underline{x}]_{\underline{x}}$ is Cohen-Macaulay.

2. The ring $R = \dfrac{K[x, y, z]_{(x,y,z)}}{(x^2 + y^3 + z^7)}$ is Cohen-Macaulay by the last example and the remark above. For the same reason, if $R$ is a regular local ring, then $R/(f)$ is Cohen-Macaulay.

3. Every zero-dimensional local ring is Cohen-Macaulay: depth zero and dimension zero.

4. Every one-dimensional local domain is Cohen-Macaulay: the depth is one since a domain has a nonzerodivisor.

5. The ring $\dfrac{K[x,y]_{(x,y)}}{(x^2,xy)}$ is *not* Cohen-Macaulay, since it has an associated prime of dimension zero, although the ring is dimension one.

6. The ring $\dfrac{K[x,y]_{(x,y,z)}}{(xy,xz)}$ is *not* Cohen-Macaulay since it has minimal (a fortiori, associated) primes of different dimensions.

7. $\dfrac{K[x,y]_{(x,y)}}{(xy)}$ is Cohen-Macaulay by example #2 above. We can check by showing an SOP is a regular sequence. The element $x-y$ is a SOP, since the quotient is $K[x]/(x^2)$, which is zero-dimensional. This element is also a nonzerodivisor on the ring: any element in the ring can be represented by $f(x,y) = a + xb(x) + yc(y)$. $(x-y)f(x,y) = ax - ay + x^2b(x) - y^2c(y) = 0$ in $R$ implies $f(x,y) = 0$. Thus, $R$ is CM.

8. $K[x^4,x^3y,xy^3,y^4]_{(x^4,x^3y,xy^3,y^4)}$ is not CM. An SOP is $x^4, y^4$, but $y^4$ is a zerodivisor mod $(x^4)$, since $y^4 \cdot (x^3y)^2 = x^4 \cdot (xy^3)^2 \in (x^4)$, but $(x^3y)^2 \notin (x^4)$, since $x^2y^2 \notin R$.

9. $\dfrac{K[X_{2\times 3}]_X}{I_2(X)}$ is Cohen-Macaulay. A SOP is $x_{11}, x_{21}-x_{12}, x_{31}-x_{22}, x_{23}$; check that it is a regular sequence!

**Proposition 9.20.** *Let $R$ be a Cohen-Macaulay local ring, and $\mathfrak{p}$ be prime. Then $R_\mathfrak{p}$ is Cohen-Macaulay.*

*Proof.* We claim that there is a regular sequence contained in $R$ of length equal to the height of $\mathfrak{p}$. If $\mathfrak{p}$ is not minimal, it is not contained in the union of the minimal primes, hence not in the union of the associated primes by unmixedness. Thus, there is a nonzerodivisor in $\mathfrak{p}$. We can mod out by this to get a CM ring of lower dimension, and inductively, the claim follows.

Now, localizing at $\mathfrak{p}$, this stays a regular sequence that is a SOP for $R_\mathfrak{p}$. □

**Definition 9.21.** *A Noetherian local ring that may or may not be local is* Cohen-Macaulay *if $R_\mathfrak{m}$ is Cohen-Macaulay for all $\mathfrak{m} \in \operatorname{Max}(R)$. Equivalently, $R$ is Cohen-Macaulay if $R_\mathfrak{p}$ is Cohen-Macaulay for all $\mathfrak{p} \in \operatorname{Spec}(R)$.*

**Remark 9.22.** Any regular ring is Cohen-Macaulay. In particular, $\mathbb{Z}$, $K[\underline{x}]$, $\mathbb{Z}[\underline{x}]$ are Cohen-Macaulay.

**Theorem 9.23** (Macaulay's unmixedness theorem)**.** *Let $R$ be Cohen-Macaulay. If $I = (f_1, \dots, f_r)$ has height $r$, then every associated prime of $I$ has height $r$. In particular, this holds true in a polynomial ring.*

*Proof.* By Krull height, every minimal prime of $I$ has height exactly $r$. We just need to show that $I$ has no embedded primes. To obtain a contradiction, suppose that $\mathfrak{p}$ is an embedded prime of $I$. The prime $\mathfrak{p}$ is not minimal over $I$, so $\dim((R/I)_\mathfrak{p}) > 0$. In the CM local ring $R_\mathfrak{p}$, the $f$'s form a regular sequence (by the height hypothesis), so $R_\mathfrak{p}/I \cong (R/I)_\mathfrak{p}$ is Cohen-Macaulay. However, its maximal ideal is associated, so the depth of this ring is zero, which is a contradiction. □

**Theorem 9.24** (Dimension formula)**.** *Let $R$ be a Cohen-Macaulay ring, and $\mathfrak{p} \subseteq \mathfrak{q}$ be primes. Then,* $\operatorname{height}(\mathfrak{q}) - \operatorname{height}(\mathfrak{p}) = \dim(R_\mathfrak{q}/\mathfrak{p}R_\mathfrak{q})$*. In particular, if $(R, \mathfrak{m})$ is Cohen-Macaulay and local, then* $\dim(R) - \operatorname{height}(\mathfrak{p}) = \dim(R/\mathfrak{p})$*.*

*Proof.* $R_\mathfrak{q}$ is CM local of dimension $\operatorname{height}(\mathfrak{q})$. Pick $h = \operatorname{ht}(\mathfrak{p})$ elements $r_1, \dots, r_h$ in $\mathfrak{p}$. These form a regular sequence, so $R_\mathfrak{q}/(r_1, \dots, r_h)R_\mathfrak{q}$ is CM, and $\dim(R_\mathfrak{q}/(r_1, \dots, r_h)R_\mathfrak{q}) = \dim(R_\mathfrak{q}/\mathfrak{p}R_\mathfrak{q})$, since $\mathfrak{p}R_\mathfrak{q} \in \operatorname{Ass}(R_\mathfrak{q}/(r_1, \dots, r_h)R_\mathfrak{q})$. On the other hand, $\dim(R_\mathfrak{q}/(r_1, \dots, r_h)R_\mathfrak{q}) = \dim(R_\mathfrak{q}) - h$. The equality follows. □

**Theorem 9.25.** *Let $(R, \mathfrak{m}) \subseteq (S, \mathfrak{n})$ be a module-finite local inclusion of Noetherian local rings, with $R$ regular. Then $S$ is Cohen-Macaulay if and only if $S$ is a free $R$-module.*

*Proof.* Let $x_1, \dots, x_d$ be a regular system of parameters for $R$. We have that $S$ is Cohen-Macaulay if and only if $x_1, \dots, x_d$ is a regular sequence on $S$.

One implication is clear: if $S$ is free over $R$, then $x_1, \dots, x_d$ is a regular sequence on $S$.

We show the other direction by induction on the dimension of $R$ (= dimension of $S$). If $R$ has dimension zero, all its modules are free, and any module-finite $S$ has dimension zero and is Cohen-Macaulay. For the general case, assume that $x_1, \dots, x_d$ form a regular sequence on $S$, and fix a minimal generating set for $S$ as an $R$-module, $s_1, \dots, s_t$; we want to show that any $R$-linear relation on these is trivial.

If we have a nontrivial relation $r_1 s_1 + \cdots + r_t s_t = 0$, then there is a nontrivial relation where not all of the $r_i$'s lie in $(x_d)$. Indeed, given such a relation, we could cancel off $x_d$ from each $r_i$ and get another relation, since $x_d$ is a nonzerodivisor. By the Krull Intersection Theorem, if $r_i \neq 0$, there is some $N$ such that $r_i \notin \mathfrak{m}^N$, so $r_i \notin (x_d)^N$, so we can cancel off $x_d$ finitely many times to get the relation we seek.

On the other hand, the images of $s_1, \dots, s_t$ in $S/x_d S$ form a minimal generating set for $S/x_d S$ as a $R/x_d R$-module. Since $R/x_d R$ is regular, and the images of $x_1, \dots, x_{d-1}$ form a regular sequence on $S/x_d S$, the induction hypothesis yields that our relation is trivial in $R/x_d R$. That is, all of the $r_i$'s must lie in $(x_d)$. Thus, any such relation must be trivial. We conclude that $S$ is free over $R$. □

**Remark 9.26.** By the Cohen structure theorem, every complete local ring $S$ is module-finite over a regular local ring.

# Index