NOTES FOR MATH 200C

STEVEN V SAM

These are notes for a quarter-long introduction to commutative algebra. The original skeleton for these notes are largely based on Atiyah–Macdonald, starting at Chapter 3 (mostly ignoring Chapter 4 on primary decomposition) with some additions and modifications. Notably I have tried to use notation and terminology which is consistent with modern usage (Atiyah–Macdonald was written over 50 years ago). I've also redone some proofs and ordering of results when I thought it might make the dependency trail a bit easier to manage. I will assume that you are familiar with Chapters 1 and 2 but will highlight some results and definitions in §1 that we'll use. I also incorporated some material from Eisenbud's Commutative Algebra book.

All rings in this course are by default commutative with a multiplicative unit 1.

Here is the correspondence (my notes on the left and the corresponding sections of Atiyah–Macdonald on the right):

These notes	Atiyah–Macdonald
§1	Chapters 1, 2
§2	Chapter 3
§3	Chapter 5
§4	Chapters 6, 7, 8
§5	Chapter 10 (ignoring first part), Chapter 11 (first part)
§6	Chapter 11
§7	Chapter 10 (first part)
§8	Chapter 9

Contents

1. Review 2
1.1. Ring theory 2
1.2. Functoriality 3
1.3. Exact sequences 4
1.4. Prime spectrum 4
1.5. Cayley–Hamilton theorem and Nakayama's lemma 5
2. Localization 5
2.1. Definition 5
2.2. Modules 7
2.3. Local properties 9
2.4. Extended and contracted ideals 10
3. Integral dependence 10
3.1. Integral elements 10
3.2. Integral extensions 11

Date: April 28, 2022.

3.3. Going up and down 13
4. Chain conditions 15
4.1. Noetherian modules 15
4.2. Noetherian rings 16
4.3. Hilbert basis theorem 17
4.4. Hilbert nullstellensatz 18
4.5. Artinian modules 18
4.6. Artinian rings 20
5. Gradings and filtrations 22
5.1. Graded rings and Hilbert series 22
5.2. Filtrations 26
5.3. The Hilbert–Samuel polynomial 28
6. Dimension theory 30
6.1. Definition of dimension 30
6.2. Noether normalization 32
6.3. Transcendental dimension 34
6.4. Regular local rings 35
7. Completions 37
7.1. Inverse limits 37
7.2. Krull topology 40
7.3. Completion of modules 41
7.4. Completion and the associated graded ring 43
7.5. Further results for complete rings 45
8. Behavior in low (co)dimension 48
8.1. Associated primes 48
8.2. Reduced rings 49
8.3. Discrete valuation rings 50
8.4. Serre's criterion for normality 52
8.5. Jacobian criterion 53
8.6. Cohen–Macaulay rings 55
8.7. Fractional ideals 56
References 56

1. Review

This section is a brief overview without proofs of some results that may have been encountered in earlier courses. In any case, I will either use these results for proofs or examples, so it may be worthwhile to look up anything that is not familiar.

1.1. Ring theory.

Here are some facts we'll take for granted:

- An ideal I is **prime** if $xy \in I$ implies that either $x \in I$ or $y \in I$. This is equivalent to saying that A/I is an integral domain.
- The **radical** of an ideal $I \subset A$ is defined to be
$$\sqrt{I} = \{x \in A \mid x^k \in I \text{ for some } k \geq 1\}.$$
It is equal to the intersection of all prime ideals containing I and hence is an ideal.

- An ideal I is **maximal** if it is not the unit ideal and is not contained in any other ideals except itself and the unit ideal. These always exist if we assume that the axiom of choice is valid (we will) and all maximal ideals are prime.

A few facts about prime ideals:

- If $\mathfrak{p}$ is a prime ideal and $I_1, \dots, I_k$ are any ideals such that their product belongs to $\mathfrak{p}$, i.e., $I_1 I_2 \cdots I_k \subseteq \mathfrak{p}$, then there is some j such that $I_j \subseteq \mathfrak{p}$. In particular, if $I_1 \cap \cdots \cap I_k \subseteq \mathfrak{p}$, then there is some j such that $I_j \subseteq \mathfrak{p}$.
- (Prime avoidance) If $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ are primes and I is any ideal such that $I \not\subseteq \mathfrak{p}_j$ for all j, then $I \not\subseteq \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n$. More general statements hold, but this is enough for us.

If A is a ring, the polynomial ring $A[t]$ is the ring of polynomials in t with coefficients in A. Also, we use the same notation $A[t_1, t_2, \dots]$ adjoining any number (finite or not) of variables, and $A[\![t]\!]$ is the ring of formal power series in t with coefficients in A. These are represented by series of the form

$$\sum_{n \geq 0} a_n t^n = a_0 + a_1 t + a_2 t^2 + \cdots$$

with $a_i \in A$ and with addition and multiplication defined by

$$\sum_{n\geq 0} a_n t^n + \sum_{n \geq 0} b_n t^n = \sum_{n \geq 0} (a_n + b_n) t^n, \qquad (\sum_{n \geq 0} a_n t^n)(\sum_{n \geq 0} b_n t^n) = \sum_{n \geq 0} \sum_{i+j=n} (a_i b_j) t^n.$$

1.2. **Functoriality.** While we won't do anything specific with category theory, it is extremely useful to use the language to encapsulate recurring properties that we come across, so we give some definitions and important examples now.

A **category** $\mathcal{C}$ consists of a collection of objects and, for any two objects X and Y, a set of morphisms, denoted $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ (for f a morphism from X to Y, we use the notation $f \colon X \to Y$ and think of it as a function though it need not be in any traditional sense) with some additional structure:

- Morphisms can be composed when it makes sense: if $f \colon X \to Y$ and $g \colon Y \to Z$, there is a composition $gf \colon X \to Z$, and this is associative in the obvious sense: $h(gf) = (hg)f$.
- For every object X, there is an identity morphism $1_X \colon X \to X$ such that $1_X f = f$ and $g 1_X = g$ for all $f \colon Y \to X$ and $g \colon X \to Y$.

Typical examples for us:

- The category of rings (objects are commutative rings, morphisms are ring homomorphisms).
- If A is a ring, then the category of A-modules (objects are A-modules, morphisms are A-linear homomorphisms).
- If A is a ring, then the category of A-algebras (objects are A-algebras, morphisms are A-linear ring homomorphisms).
- We could add adjectives to the examples, such as the category of finitely generated modules, or finitely generated A-algebras, etc.

A **functor** is the notion of a homomorphism between categories. Given categories $\mathcal{C}$ and $\mathcal{D}$, a functor $F \colon \mathcal{C} \to \mathcal{D}$ does two things: for each object X of $\mathcal{C}$, we get an object $F(X)$ of $\mathcal{D}$, and for every morphism $f \colon X \to Y$, we get a morphism $F(f) \colon F(X) \to F(Y)$. Most importantly, F respects composition and identity morphisms: $F(gf) = F(g)F(f)$ and $F(1_X) = 1_{F(X)}$.

Many operations that we discuss are going to be functors (typically from modules over one ring to modules over another ring). The verification generally isn't hard, but it's convenient to say that an operation is "functorial" as shorthand to mean that it respects composition of homomorphisms.

A **contravariant functor** $F\colon \mathcal{C} \to \mathcal{D}$ is like a functor except one difference: given a morphism $f\colon X \to Y$ in $\mathcal{C}$, we get a morphism $F(f)\colon F(Y) \to F(X)$ and it respects composition in the sense that $F(gf) = F(f)F(g)$ (i.e., it reverses the direction of morphisms).

1.3. **Exact sequences.** Let A be a ring. Suppose we have A-modules M_1, M_2, M_3 and homomorphisms $f\colon M_1 \to M_2$ and $g\colon M_2 \to M_3$. We draw this as a diagram

$$M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3.$$

This is a **(chain) complex** if $gf = 0$. This implies that $f(M_1) \subseteq \ker g$. We say that it is **exact** (at M_2) if we have equality: $f(M_1) = \ker g$. Given a longer sequence of homomorphisms

$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \to \cdots$$

we make the same definitions if each consecutive 3 terms has the corresponding property. An important special case is the 5-term sequence

$$0 \to M_1 \to M_2 \to M_3 \to 0.$$

In that case, exactness means that $M_1 \to M_2$ is injective (so we can identify M_1 with a submodule of M_2) and $M_2 \to M_3$ is surjective, and that the natural map $M_2/M_1 \to M_3$ is an isomorphism. These are called **short exact sequences**.

A functor F (from A-modules to B-modules) is **exact** if it preserves short exact sequences, i.e., applying F to any short exact sequence results in a short exact sequence (this implies it preserves arbitrary exact sequences). If it only preserves exact sequences of the form $0 \to M_1 \to M_2 \to M_3$, then it is **left exact**, and if it only preserves exact sequences of the form $M_1 \to M_2 \to M_3 \to 0$, then it is **right exact**.

If N is an A-module, then the operation of tensoring with N is a right exact functor.

Finally, we'll make use of the snake lemma:

Lemma 1.3.1 (Snake lemma). *Suppose we have a commutative diagram of A-modules*

$$\begin{tikzcd}
 & X \arrow[r, "f"] \arrow[d, "\alpha"] & Y \arrow[r, "g"] \arrow[d, "\beta"] & Z \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & X' \arrow[r, "f'"] & Y' \arrow[r, "g'"] & Z' &
\end{tikzcd}$$

such that the top and bottom rows are exact. Then there is an exact sequence

$$\ker\alpha \to \ker\beta \to \ker\gamma \to \operatorname{coker}\alpha \to \operatorname{coker}\beta \to \operatorname{coker}\gamma.$$

If f is injective, then so is $\ker\alpha \to \ker\beta$; if g' is surjective, then so $\operatorname{coker}\beta \to \operatorname{coker}\gamma$.

1.4. **Prime spectrum.** Given a ring A, its **prime spectrum** is the set of prime ideals of A, and is denoted $\operatorname{Spec}(A)$. Given an ideal $I \subset A$, we define the subset

$$V(I) = \{\mathfrak{p} \in \operatorname{Spec}(A) \mid I \subseteq \mathfrak{p}\}.$$

The **Zariski topology** on $\operatorname{Spec}(A)$ is defined by declaring the $V(I)$ to be the closed subsets. This is valid since

- $V(1) = \varnothing$,

- $V(0) = \mathrm{Spec}(A)$,
- $V(I) \cup V(J) = V(I \cap J)$,
- $\bigcap_n V(I_n) = V(\sum_n I_n)$.

Given a ring homomorphism $f\colon A \to B$, and a prime ideal $\mathfrak{p} \subset B$, the preimage $f^{-1}(\mathfrak{p})$ is a prime ideal in A, and this defines a continuous function that we denote by $f^*\colon \mathrm{Spec}(B) \to \mathrm{Spec}(A)$. So Spec is a (contravariant) functor from commutative rings to topological spaces (the morphisms for the latter being continuous functions).

A topological space X is **irreducible** if it is not possible to write it as a union of two closed proper subsets, i.e., if $X = X_1 \cup X_2$ with X_1, X_2 closed, then it must be that either $X = X_1$ or $X = X_2$.

1.5. Cayley–Hamilton theorem and Nakayama's lemma.

Theorem 1.5.1 (Cayley–Hamilton theorem). *Let A be a ring, M a finitely generated A-module, and $I \subset A$ an ideal. Let $\varphi\colon M \to M$ be an A-linear map such that $\varphi(M) \subseteq IM$. Then there exist $a_1, \dots, a_n \in I$ such that*

$$(\varphi^n + a_1\varphi^{n-1} + \cdots + a_n)(x) = 0$$

for all $x \in M$.

Proof. We can actually reduce this to the more familiar case when A is a field as follows (let me just give an outline of the steps without the details):

(1) Pick generators $m_1, \dots, m_n$ for M; there exist $\varphi_{ij} \in I$ such that $\varphi(m_i) = \sum_j \varphi_{ji} m_j$. Let $\widetilde{\varphi} = (\varphi_{ij})$ be the corresponding $n \times n$ matrix which is an A-linear map $\widetilde{\varphi}\colon A^n \to A^n$ such that $\widetilde{\varphi}(A^n) \subseteq IA^n$. Then the result is true for φ if it holds for $\widetilde{\varphi}$.

(2) Next, consider the "universal" case where the ring is $\mathbf{Z}[x_{ij} \mid i, j = 1, \dots, n]$ and $\Phi = (x_{ij})$ is the matrix where the entries are independent variables (and the ideal I is the ideal generated by the x_{ij}). There is a ring homomorphism $\mathbf{Z}[x_{ij}] \to A$ such that $x_{ij} \mapsto \varphi_{ij}$ and so if the result holds for the universal case then it holds for $\widetilde{\varphi}$.

(3) Finally, we define $a_k \in \mathbf{Z}[x_{ij}]$ to be the coefficients of the characteristic polynomial $t^n + a_1 t^{n-1} + \cdots + a_n$ of Φ. We have to check that $\Phi^n + a_1\Phi^{n-1} + \cdots + a_n \mathrm{id}$ is the 0 matrix. But to do this, it doesn't matter if we're using $\mathbf{Z}[x_{ij}]$ or its field of fractions, and so we're down to the case of a field. □

An important corollary is Nakayama's lemma:

Theorem 1.5.2 (Nakayama's lemma). *If M is a finitely generated A-module and I is an ideal in the Jacobson radical of A (the intersection of all maximal ideals), then $IM = M$ implies that $M = 0$.*

Proof. If φ is the identity function, then Cayley–Hamilton implies that there exists $a \in I$ (take the sum of $a_1, \dots, a_n$ there) such that $(1 + a)x = 0$ for all $x \in M$. But $1 + a$ is a unit and hence $M = 0$: if not, then there exists a maximal ideal containing it. Since a belongs to all maximal ideals, 1 would also belong to that maximal ideal, which is a problem. □

2. Localization

2.1. Definition.

Let A be a ring. A subset $S \subset A$ is a **multiplicative subset** if $1 \in S$ and S is closed under multiplication. We'd like to build a new ring where elements of S become invertible in as efficient of a way as possible. This goes as follows. Define a relation on $A \times S$ by

$$(a,s) \sim (b,t) \text{ if there exists } x \in S \text{ such that } (at - bs)x = 0.$$

This is clearly symmetric and reflexive, so we verify that it is transitive. Suppose that $(b,t) \sim (c,u)$, i.e., there exists $y \in S$ such that $(bu - ct)y = 0$. Then

$$0 = (at - bs)xuy + (bu - ct)ysx = (au - cs)txy$$

and $txy \in S$, so $(a,s) \sim (c,u)$. Set

$$S^{-1}A = (A \times S)/\sim .$$

Intuitively, we think of (a,s) as a fraction a/s (and we'll usually write a/s instead), which is where the equivalence relation comes from (clearing denominators). We have to allow for the additional flexibility of multiplying by x because S may have zerodivisors (if we don't, $\sim$ won't be transitive in general).

With that intuition, we can define a ring structure on $S^{-1}A$ (the **ring of fractions of A with respect to S**) via

- $(a,s) + (b,t) = (at + bs, st)$.
- $(a,s)(b,t) = (ab, st)$.

We omit the verification this is well-defined on equivalence classes. The additive unit is $(0,1)$ and the multiplicative unit is $(1,1)$.

Example 2.1.1. If $\mathfrak{p} \subset A$ is any prime ideal, then $S = A \setminus \mathfrak{p}$ is multiplicative. In that case, we write $A_{\mathfrak{p}}$ for $S^{-1}A$ and call it the **localization of A at $\mathfrak{p}$**.

A particular special case is when A is a domain and $\mathfrak{p} = (0)$. Then $A_{(0)}$ is the **field of fractions of A**. For example, if $A = \mathbf{Z}$, then $A_{(0)} = \mathbf{Q}$. □

Example 2.1.2. For any $f \in A$, $S = \{1, f, f^2, \dots\}$ is multiplicative. In that case we write either A_f or $A[1/f]$ for $S^{-1}A$. □

There is a canonical homomorphism

$$f \colon A \to S^{-1}A, \qquad f(a) = (a,1).$$

Via this canonical map, we can view $S^{-1}A$ as an A-module. In general, this is not injective. As an extreme example, if $0 \in S$, then $S^{-1}A = 0$ is the zero ring. Now we address the efficiency of this construction.

Proposition 2.1.3. *If $g \colon A \to B$ is any homomorphism such that $g(s)$ is invertible for all $s \in S$, then there exists a unique homomorphism $h \colon S^{-1}A \to B$ such that $g = h \circ f$.*

Proof. Define $h(a,s) = g(a)g(s)^{-1}$. This is well-defined: if $(a,s) \sim (b,t)$, then there exists $x \in S$ such that $(at - bs)x = 0$, so $(g(a)g(t) - g(b)g(s))g(x) = 0$. Multiplying by $(g(t)g(s)g(x))^{-1}$ gives $g(a)g(s)^{-1} = g(b)g(t)^{-1}$.

As for uniqueness, for any homomorphism h' such that $g = h' \circ f$, we have

$$h'(a,s) = h'(a,1)h'(1,s) = h'(a,1)h'(s,1)^{-1} = g(a)g(s)^{-1}. \qquad \square$$

In this sense, $S^{-1}A$ is the "smallest" ring in which the elements of S become invertible.

2.2. **Modules.** Now let M be an A-module. We define $S^{-1}M$ to be $(M \times S)/\sim$ where

$$(m,s) \sim (n,t) \text{ if there exists } x \in S \text{ such that } x(tm - sn) = 0.$$

We omit the (similar) check that $\sim$ is an equivalence relation. Again, we think of (m,s) as a fraction m/s; we define addition as usual:

$$(m,s) + (m',s') = (s'm + sm, ss').$$

Also $S^{-1}M$ is a module over $S^{-1}A$ via the product (with $(a,t) \in S^{-1}A$) defined by

$$(a,t)(m,s) = (am, ts).$$

If $f\colon M \to N$ is a homomorphism of A-modules, then we define

$$S^{-1}(f)\colon S^{-1}M \to S^{-1}N, \qquad (m,s) \mapsto (f(m), s).$$

This is *functorial* in the sense that given another homomorphism $g\colon N \to P$, we have

$$S^{-1}(g \circ f) = S^{-1}(g) \circ S^{-1}(f)$$

and S^{-1} applied to the identity map is again the identity. Hence we think of S^{-1} as an operation that takes A-modules to $S^{-1}A$-modules, and homomorphisms to homomorphisms.

We will generally use the more intuitive shorthand m/s or $\frac{m}{s}$ in place of (m,s).

When $S = A \setminus \mathfrak{p}$ for a prime $\mathfrak{p}$, then $M_\mathfrak{p} = S^{-1}M$ is the **localization of M at $\mathfrak{p}$**.

Proposition 2.2.1. *S^{-1} is exact, i.e., if*

$$M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$$

is exact, then so is

$$S^{-1}M_1 \xrightarrow{S^{-1}(f)} S^{-1}M_2 \xrightarrow{S^{-1}(g)} S^{-1}M_3.$$

Proof. First we have $S^{-1}(g) \circ S^{-1}(f) = S^{-1}(g \circ f) = S^{-1}(0) = 0$, where the last equality is by definition.

Now suppose that $(m,s) \in \ker S^{-1}(g)$. We need to show that it is in the image of $S^{-1}(f)$. By definition, we have $S^{-1}(g)(m,s) = (g(m),s) = 0$, i.e., there exists $x \in S$ such that $xg(m) = 0$. But then $g(xm) = 0$, so that $xm \in \ker g$. By exactness, $xm = f(m')$ for some $m' \in M$. So then

$$S^{-1}(f)(m', xs) = (xm, xs) = (m,s). \qquad \square$$

Of course, this tells us that S^{-1} preserves exactness for longer sequences (just apply it to each consecutive 3 terms).

This also tells us, for example, that if $N \to M$ is injective, then so is $S^{-1}N \to S^{-1}M$, so that we can identify the localizations of submodules of M with submodules of the localization $S^{-1}M$. This operation behaves well:

Corollary 2.2.2. *Let M be an A-module with submodules N, P.*

(1) $S^{-1}(N + P) = S^{-1}N + S^{-1}P$.
(2) $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$.
(3) We have an isomorphism of $S^{-1}A$-modules $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$.

Proof. (1) Given $x \in N$ and $y \in P$ and $s \in S$, we have $(x + y)/s = x/s + y/s$, so the image of $S^{-1}(N + P)$ in $S^{-1}M$ is contained in $S^{-1}N + S^{-1}P$. Conversely, given $x/s \in S^{-1}N$ and $y/t \in S^{-1}P$, we have $x/s + y/t = (xt + ys)/st$, so it comes from an element of $S^{-1}(N + P)$.

(2) If $x \in N \cap P$ and $s \in S$, then $x/s \in S^{-1}N \cap S^{-1}P$ so the image of $S^{-1}(N \cap P)$ in $S^{-1}M$ is contained in $S^{-1}N \cap S^{-1}P$. On the other hand, suppose we have an element in the intersection, so we can write it as either x/s or y/t, where $x \in N$, $y \in P$ and $s, t \in S$. Then there exists $u \in S$ such that $u(tx - sy) = 0$, i.e., if we set $z = utx$, then $z \in N$, but also $z = usy$ so that $z \in P$. Finally, z/uts maps to x/s, so every element of $S^{-1}N \cap S^{-1}P$ comes from an element of $S^{-1}(N \cap P)$.

(3) This follows from the previous result using the short exact sequence $0 \to N \to M \to M/N \to 0$. □

There's another way to get $S^{-1}A$-modules from A-modules: base change along the canonical map. Actually, this is the same as S^{-1}:

Proposition 2.2.3. *The map*

$$S^{-1}A \otimes_A M \to S^{-1}M$$
$$\sum_i (a_i, s_i) \otimes m_i \mapsto \sum_i (a_i m_i, s_i)$$

is an isomorphism of $S^{-1}A$-modules.

Proof. Quick check this is well-defined: it comes from the bilinear function $S^{-1}A \times M \to S^{-1}M$ by $((a, s), m) \mapsto (am, s)$.

It is clear from the definition that this function is surjective, so we just need to show that it is injective. So suppose that $\sum_{i=1}^n (a_i m_i, s_i) = 0$. Let $s = s_1 \cdots s_n$ and $s'_j = s_1 \cdots \hat{s_j} \cdots s_n$. Then we can simplify this sum as

$$\sum_{i=1}^n (a_i m_i, s_i) = (\sum_{i=1}^n a_i m_i s'_i, s),$$

which means that there exists $x \in S$ so that $x \sum_i a_i m_i s'_i = 0$.

On the other hand, we have

$$\sum_i (a_i, s_i) \otimes m_i = \sum_i (a_i s'_i x, sx) \otimes m_i = \sum_i (1, sx) \otimes x a_i s'_i m_i = (1, sx) \cdot 0 = 0. \qquad \square$$

Corollary 2.2.4. *$S^{-1}A$ is a flat A-module.*

Proposition 2.2.5. *Given A-modules M and N, the map*

$$S^{-1}M \otimes_{S^{-1}A} S^{-1}N \to S^{-1}(M \otimes_A N)$$
$$\sum_i (m_i, s_i) \otimes (n_i, t_i) \mapsto \sum_i (m_i \otimes n_i, s_i t_i)$$

is an isomorphism.

Proof. First, this is well-defined since it comes from the bilinear map $S^{-1}M \times S^{-1}N \to S^{-1}(M \otimes_A N)$ given by $((m, s), (n, t)) \mapsto (m \otimes n, st)$. The inverse to this map is given by

$$(\sum_i m_i \otimes n_i, s) \mapsto \sum_i (m_i, 1) \otimes (n_i, s). \qquad \square$$

2.3. **Local properties.** Localization is useful because a lot of properties of A-modules can be checked "locally", i.e., by checking after localizing at prime ideals (or just maximal ideals in some cases). Here's an important example:

Proposition 2.3.1. *The following are equivalent:*

(1) $M = 0$.
(2) $M_{\mathfrak{p}} = 0$ *for all primes* $\mathfrak{p}$.
(3) $M_{\mathfrak{m}} = 0$ *for all maximal ideals* $\mathfrak{m}$.

Proof. Clearly (1) implies (2) which in turn implies (3).

So it suffices to show that if $M \neq 0$, then there exists a maximal ideal $\mathfrak{m}$ so that $M_{\mathfrak{m}} \neq 0$. Pick $m \in M$ nonzero; the annihilator of m is a proper ideal and hence is contained in some maximal ideal $\mathfrak{m}$. Then $(m, 1) \in M_{\mathfrak{m}}$ is nonzero: for any $x \notin \mathfrak{m}$, x does not annihilate m and hence $xm \neq 0$. □

One reason this is useful is because $A_{\mathfrak{p}}$ is always a local ring with maximal ideal given by the extension of $\mathfrak{p}$ along the canonical homomorphism $A \to A_{\mathfrak{p}}$: any element outside of $\mathfrak{p}A_{\mathfrak{p}}$ can be represented as (a, s) with $a \notin \mathfrak{p}$ and hence has inverse (s, a). More results are available for local rings, as we will see throughout the course.

Here are some more fundamental local properties.

Corollary 2.3.2. *Given a homomorphism* $f\colon M \to N$ *of* A*-modules, the following are equivalent:*

(1) f *is an injection.*
(2) $f_{\mathfrak{p}}$ *is an injection for all primes* $\mathfrak{p}$.
(3) $f_{\mathfrak{m}}$ *is an injection for all maximal ideals* $\mathfrak{m}$.

The same statement holds if "injection" is replaced with "surjection" or "isomorphism".

Proof. Consider the exact sequence $0 \to \ker f \to M \to N$. Since f is injective if and only if $\ker f = 0$, and localization is exact (Proposition 2.2.1), the result follows from Proposition 2.3.1 applied to $\ker f$.

For "surjection", we use $\operatorname{coker} f$ instead, and "isomorphism" follows by combining both parts. □

Proposition 2.3.3. *The following are equivalent:*

(1) M *is a flat* A*-module.*
(2) $M_{\mathfrak{p}}$ *is a flat* $A_{\mathfrak{p}}$*-module for all primes* $\mathfrak{p}$.
(3) $M_{\mathfrak{m}}$ *is a flat* $A_{\mathfrak{m}}$*-module for all maximal ideals* $\mathfrak{m}$.

Proof. We first prove (1) implies (2). Suppose that M is flat. Let $N_1 \to N_2$ be an injection of $A_{\mathfrak{p}}$-modules. Then this is also an injection of A-modules via pullback along the canonical map $A \to A_{\mathfrak{p}}$ and so $M \otimes_A N_1 \to M \otimes_A N_2$ is also injective. But we can also localize at $\mathfrak{p}$ to get another injection, and this is the same as first localizing at $\mathfrak{p}$ and then tensoring with $M_{\mathfrak{p}}$ by Proposition 2.2.5, and hence $M_{\mathfrak{p}}$ is a flat $A_{\mathfrak{p}}$-module.

As usual, (2) clearly implies (3).

Finally, we prove that (3) implies (1). Suppose that M is not flat. Then there is an injection $N \to N'$ of A-modules such that $M \otimes_A N \to M \otimes_A N'$ has a non-zero kernel K. But then there exists a maximal ideal $\mathfrak{m}$ so that the $K_{\mathfrak{m}} \neq 0$ (Proposition 2.3.1), but this is also the kernel of $M_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} N_{\mathfrak{m}} \to M_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} N'_{\mathfrak{m}}$, so $M_{\mathfrak{m}}$ is not flat. □

2.4. **Extended and contracted ideals.** Given an ideal $I \subset A$, write $S^{-1}I$ for the extended ideal $(S^{-1}A)I$.

Proposition 2.4.1. *Every ideal $J \subset S^{-1}A$ is of the form $S^{-1}I$ for some ideal $I \subset A$; in particular, we can take I to be the preimage of J along the canonical map $A \to S^{-1}A$.*

Proof. $S^{-1}I \subseteq J$ by general properties of contracted ideals; and we claim that $J = S^{-1}I$: if $(a, s) \in J$, then $(a, 1) \in J$ and hence $a \in I$, and so $(a, s) \in S^{-1}I$. □

Proposition 2.4.2. *The function $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ gives a bijection*

$$\{\mathfrak{p} \in \operatorname{Spec}(A) \mid \mathfrak{p} \cap S = \varnothing\} \to \operatorname{Spec}(S^{-1}A).$$

In particular, for any $f \in A$, $\operatorname{Spec}(A_f)$ is identified with the open subset $\operatorname{Spec}(A) \setminus V(f)$, and for any prime $\mathfrak{p}$, $\operatorname{Spec}(A_\mathfrak{p})$ is in bijection with the prime ideals of A that are contained in $\mathfrak{p}$.

Proof. Suppose $\mathfrak{p} \in \operatorname{Spec}(A)$ and $\mathfrak{p} \cap S = \varnothing$. Let $\overline{S}$ be the image of S under $A \to A/\mathfrak{p}$; this does not contain 0. Since $A/\mathfrak{p}$ is a domain, $\overline{S}^{-1}(A/\mathfrak{p})$ is contained in the field of fractions of $A/\mathfrak{p}$ and hence is a domain, but it is also isomorphic to $S^{-1}(A)/S^{-1}(\mathfrak{p})$, which means that $S^{-1}(\mathfrak{p})$ is prime. Since the canonical map $A/\mathfrak{p} \to \overline{S}^{-1}(A/\mathfrak{p})$ is injective, this also means that the preimage of $S^{-1}(\mathfrak{p})$ along $A \to S^{-1}A$ is $\mathfrak{p}$. On the other hand, given a prime $\mathfrak{q}$ of $S^{-1}A$, its pullback along the canonical map $A \to S^{-1}A$ is a prime $\mathfrak{p}$ such that $\mathfrak{p} \cap S = \varnothing$ and $S^{-1}\mathfrak{p} = \mathfrak{q}$ by Proposition 2.4.1. □

Proposition 2.4.3. *As an operation on ideals, S^{-1} commutes with finite sums, products, and intersections.*

Proof. We've already seen that S^{-1} commutes with finite sums and intersections in Corollary 2.2.2. For products, let I and J be two ideals. Then clearly the image of $S^{-1}(IJ)$ in $S^{-1}A$ is contained in $(S^{-1}I)(S^{-1}J)$, so we just have to show equality. Since the image is closed under addition, we just need to check elements of the form $(x/s)(y/t)$ for $x \in I$, $y \in J$ and $s, t \in S$. But then this comes from $(xy)/(st)$. □

Proposition 2.4.4. *S^{-1} commutes with taking radicals. In particular, if A is reduced, then so is $S^{-1}A$.*

Proof. If $x^n \in I$ for some $n > 0$ and $s \in S$, then $(x/s)^n \in S^{-1}I$, and so $x/s \in \sqrt{S^{-1}I}$. Conversely, suppose that $x/s \in \sqrt{S^{-1}I}$, so that there exists $n > 0$ such that $(x/s)^n \in S^{-1}I$. Then we can write $x^n/s^n = y/t$ where $y \in I$ and $t \in S$, so there exists $u \in S$ such that $ux^nt = us^ny \in I$. But then $(uxt)^n \in I$ so $uxt \in \sqrt{I}$, and $x/s = (uxt)/(ust)$. □

3. Integral dependence

3.1. **Integral elements.** Let A be a subring of B. An element $x \in B$ is **integral** over A if there exists a monic polynomial with coefficients in A for which x is a solution. In other words, there exists a positive integer n and $a_1, \dots, a_n \in A$ such that

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

We'll call such an expression an integrality equation for x. This definition, while simple to state, is quite difficult to work with (for example, as we will see soon, the sum of two integral elements is again integral, but this seems to be very hard to prove using only this definition).

Here are some equivalent formulations. We let $A[x]$ denote the subring of B generated by A and x (not to be confused with the polynomial ring).

Proposition 3.1.1. *The following are equivalent:*

1. *x is integral over A.*
2. *$A[x]$ is a finitely generated A-module.*
3. *There exists a subring C of B that contains $A[x]$ such that C is a finitely generated A-module.*
4. *There exists a faithful (i.e., trivial annihilator) $A[x]$-module M which is finitely generated as an A-module.*

Proof. As an A-module, $A[x]$ is generated by $1, x, x^2, \dots$. If x is integral over A, then there exists n such that $1, x, x^2, \dots, x^{n-1}$ suffice (since x^N for $N \geq n$ is a linear combination of smaller powers), and hence (1) implies (2).

(2) trivially implies (3) by taking $C = A[x]$.

(3) implies (4) by taking $M = C$.

Finally, suppose that (4) holds. We have an A-linear map $\varphi\colon M \to M$ given by $\varphi(m) = xm$. By the Cayley–Hamilton theorem (Theorem 1.5.1), there exist $a_1, \dots, a_n \in A$ such that

$$(\varphi^n + a_1\varphi^{n-1} + \cdots + a_n)(m) = 0$$

for all $m \in M$. In particular, $x^n + \cdots + a_0$ annihilates M. By the assumption M is faithful, we see that $x^n + \cdots + a_0 = 0$, so that x is integral over A. □

Corollary 3.1.2. *The set of elements of B that are integral over A is a subring, i.e., if $x, y \in B$ are integral, then so is $x \pm y$ and xy.*

Proof. Let $x, y \in B$ be integral over A. Then y is also integral over $A[x]$ so that $A[x, y]$ is a finitely generated $A[x]$-module. In turn, $A[x]$ is a finitely generated A-module, so $A[x, y]$ is a finitely generated A-module. Since $A[x + y] \subset A[x, y]$, we see from above that $x + y$ is integral over A. Similarly, $x - y$ and xy are integral over A. □

3.2. **Integral extensions.** Given $A \subset B$, the set of integral elements is denoted $\overline{A}$ and is called the **integral closure of** A **in** B. If $\overline{A} = A$, then A is **integrally closed in** B and if $\overline{A} = B$, then B is **integral over** A. We also say that $A \subseteq B$ is an **integral extension**. We can extend the setup to include arbitrary homomorphisms $f\colon A \to B$, in which case, we consider the inclusion $f(A) \subset B$, and say that B is integral over A, or f is an integral homomorphism, if B is integral over $f(A)$.

Integrality is transitive:

Corollary 3.2.1. *Suppose $A \subseteq B \subseteq C$. If C is integral over B and B is integral over A, then C is integral over A.*

In particular, $\overline{\overline{A}} = \overline{A}$.

Proof. Pick $x \in C$. Since x is integral over B, there exist $b_1, \dots, b_n \in B$ such that

$$x^n + b_1x^{n-1} + \cdots + b_n = 0.$$

Let $B' = A[b_1, \dots, b_n]$. Then x is integral over B', and hence $B'[x]$ is a finitely generated B'-module. Next, each of $b_1, \dots, b_n$ is integral over A, and so B' is a finitely generated A-module. This implies that $B'[x]$ is a finitely generated A-module. Finally, $A[x] \subset B[x]$, so by the equivalence of (1) and (3) in Proposition 3.1.1, x is integral over A.

For the last statement, take $B = \overline{A}$ and $C = \overline{\overline{A}}$, which shows that $\overline{\overline{A}} \subseteq \overline{A}$. □

Proposition 3.2.2. *Let $A \subseteq B$ be an integral extension. If $I \subseteq B$ is an ideal, then $A/(A \cap I) \subseteq B/I$ is integral.*

Proof. Given $x \in B/I$, lift it to an element y in B. Take a monic expression for y with coefficients in A which is 0 and reduce it modulo I to see that x is integral over the image of A in B/I, i.e., $A/(A \cap I)$. □

Proposition 3.2.3. *Let $S \subseteq A$ be a multiplicative subset. If $A \subseteq B$ is integral, then so is $S^{-1}A \subseteq S^{-1}B$.*

Proof. Pick $x/s \in S^{-1}B$, where $x \in B$ and $s \in S$. Then x is integral over A, so we have an equation

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

where $a_i \in A$. Then we have

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

which shows that x/s is integral over $S^{-1}A$. □

An important case is when A is a domain and B is its field of fractions. In that case, $\overline{A}$ is called the **normalization** of A, and we'll denote it by $\widetilde{A}$. A domain A is called **normal** if $A = \widetilde{A}$, i.e., is integrally closed in its field of fractions. This turns out to be a very important property in commutative algebra and algebraic geometry (see §8 for some examples), though we're limited here in what we can explain.

Proposition 3.2.4. *Any unique factorization domain is normal.*

Proof. Let A be a UFD and let B be its field of fractions. Pick $x/y \in B$ with $x, y \in A$. Since A is a UFD, we may assume that x, y have no factors in common in their prime factorizations. Now suppose that x/y is integral, so that we have an equation of the form

$$(x/y)^n + a_1(x/y)^{n-1} + \cdots + a_n = 0$$

for some $a_1, \dots, a_n \in A$. Multiply by y^n and rearrange to get

$$x^n = -(a_1x^{n-1}y + \cdots + a_ny^n)$$

The right hand side is divisible by y and hence so is x^n; by our original assumptions, y must then be a unit in A, so $x/y \in A$. □

Normality is a local property:

Proposition 3.2.5. *Let A be a domain. The following are equivalent:*

(1) A is normal.
(2) $A_{\mathfrak{p}}$ is normal for all primes $\mathfrak{p}$.
(3) $A_{\mathfrak{m}}$ is normal for all maximal ideals $\mathfrak{m}$.

Proof. Let B be the field of fractions of A. Then $B_{\mathfrak{p}} = B$ is the field of fractions of $A_{\mathfrak{p}}$ for any prime $\mathfrak{p}$. In particular, A is normal if and only if the inclusion map $A \to \widetilde{A}$ is surjective. But this can be checked locally by Corollary 2.3.2. □

3.3. **Going up and down.**

Proposition 3.3.1. *Let $A \subseteq B$ be an integral extension of domains. Then A is a field if and only if B is a field.*

Proof. First suppose that A is a field and pick $x \in B$. Then we have an equation of the form

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

for $a_1, \ldots, a_n$. Pick n the smallest degree of such an equation. Then $a_n \neq 0$; if not, then $x^{n-1} + a_1 x^{n-2} + \cdots + a_{n-1} = 0$ since x is a nonzerodivisor contradicting minimality of n. But this tells us that $x^{-1} = -a_n^{-1}(x^{n-1} + a_1 x^{n-2} + \cdots + a_{n-1}) \in B$, so that B is a field.

Conversely, suppose that B is a field. Pick $x \in A$. Then $1/x$ is integral over A, so we have an equation of the form

$$(1/x)^n + a_1(1/x)^{n-1} + \cdots + a_n = 0$$

for $a_1, \ldots, a_n \in A$. Multiplying by x^{n-1} and rearranging shows that

$$1/x = -(a_1 + \cdots + a_n x^{n-1}).$$

so that $1/x \in A$ and hence A is a field. □

Corollary 3.3.2. *Let $A \subseteq B$ be an integral extension and let $\mathfrak{q} \subset B$ be a prime. Then $\mathfrak{q}$ is maximal if and only if $\mathfrak{p} = A \cap \mathfrak{q}$ is maximal.*

Proof. By Proposition 3.2.2, $A/(A \cap \mathfrak{q}) \to B/\mathfrak{q}$ is integral, so we can apply the previous result. □

Theorem 3.3.3 (Incomparability)**.** *Let $A \subset B$ be an integral extension and suppose that $\mathfrak{p} \subseteq \mathfrak{q}$ are prime ideals in B. If $\mathfrak{p} \cap A = \mathfrak{q} \cap A$, then $\mathfrak{p} = \mathfrak{q}$.*

Proof. Let $S = A \setminus (\mathfrak{q} \cap A)$. This is a multiplicative set and so $S^{-1}A \subseteq S^{-1}B$ is integral by Proposition 3.2.3. Then $S^{-1}\mathfrak{p} \cap S^{-1}A = S^{-1}\mathfrak{q} \cap S^{-1}A$, and this is the maximal ideal $S^{-1}(\mathfrak{q} \cap A)$. But then $S^{-1}\mathfrak{p} = S^{-1}\mathfrak{q}$ since they are maximal ideals (one contained in the other) by Corollary 3.3.2. Finally, by the correspondence (Proposition 2.4.2) for prime ideals in the localization (both $\mathfrak{p}$ and $\mathfrak{q}$ do not intersect S), we have $\mathfrak{p} = \mathfrak{q}$. □

Theorem 3.3.4 (Lying over theorem)**.** *Let $A \subset B$ be an integral extension. For every prime ideal $\mathfrak{p} \subset A$, there exists a prime $\mathfrak{q} \subset B$ such that $\mathfrak{q} \cap A = \mathfrak{p}$. In other words, the map* $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ *is surjective.*

Proof. Consider the localized map $f\colon A_\mathfrak{p} \to B_\mathfrak{p} = B \otimes_A A_\mathfrak{p}$ which is integral by Proposition 3.2.3. Pick a maximal ideal $\mathfrak{m}$ of $B_\mathfrak{p}$. By Corollary 3.3.2, $f^{-1}(\mathfrak{m})$ is a maximal ideal and hence equal to $\mathfrak{p}A_\mathfrak{p}$ so that its pullback to A is just $\mathfrak{p}$. In particular, we can take $\mathfrak{q}$ to be the pullback of $\mathfrak{m}$ to B. □

Theorem 3.3.5 (Going-up theorem)**.** *Let $A \subset B$ be an integral extension. Let $\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$ be prime ideals of A and let $\mathfrak{q}_1$ be a prime ideal of B such that $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$. Then there is a chain of prime ideals $\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \cdots \subseteq \mathfrak{q}_n$ so that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for all $i = 1, \ldots, n$.*

Proof. It's enough to consider the case $n = 2$. Furthermore, the extension $A/\mathfrak{p}_1 \subseteq B/\mathfrak{q}_1$ is integral by Proposition 3.2.2, so we may replace A and B by $A/\mathfrak{p}_1$ and $B/\mathfrak{q}_1$, and assume that $\mathfrak{p}_1 = 0$ and $\mathfrak{q}_1 = 0$, and we just need to find a prime in B whose intersection with A is $\mathfrak{q}_2$. But now the result follows from the lying over theorem. □

Lemma 3.3.6. *Let $f\colon A \to B$ be a ring homomorphism and let $\mathfrak{p} \subset A$ be a prime such that $f^{-1}(\mathfrak{p}B) = \mathfrak{p}$. Then there exists a prime $\mathfrak{q} \subset B$ such that $f^{-1}(\mathfrak{q}) = \mathfrak{p}$.*

Proof. Let $S = f(A \setminus \mathfrak{p})$, which is a multiplicative subset of B. The assumption that $f^{-1}(\mathfrak{p}B) = \mathfrak{p}$ implies that $\mathfrak{p}B \cap S = \varnothing$, and so $\mathfrak{p}S^{-1}B$ is a proper ideal in $S^{-1}B$; pick some maximal ideal $\mathfrak{m}$ of $S^{-1}B$ that contains $\mathfrak{p}S^{-1}B$ and let $\mathfrak{q}$ be the pullback of $\mathfrak{m}$ to B. Then $\mathfrak{p} \subseteq f^{-1}(\mathfrak{q})$. If $x \notin \mathfrak{p}$, then $f(x)$ is a unit in $S^{-1}B$, and so $f(x) \notin \mathfrak{q}$, so we see that $f^{-1}(\mathfrak{q}) = \mathfrak{p}$. □

Lemma 3.3.7. *Let A be a domain with field of fractions K and algebraic closure $\overline{K}$.*

(1) Pick monic polynomials $F \in A[t]$ and $G, H \in K[t]$. If $F = GH$, then $G, H \in \widetilde{A}[t]$.

(2) Now assume that A is normal and $x \in \overline{K}$ is integral over A. Then the monic minimal polynomial of x has coefficients in A.

Furthermore, if $\mathfrak{p} \subset A$ is a prime and there is some monic polynomial in A with non-leading coefficients in $\mathfrak{p}$ for which $x \in \overline{K}$ is a root, then its monic minimal polynomial also has non-leading coefficients in $\mathfrak{p}$.

Proof. (1) Let α be a root of either G or H in the algebraic closure of K. Since both are monic, α is integral over A. In particular, the coefficients of G and H are integral over A since they are in the subring generated by the roots.

(2) The first part follows by taking F in (1) to be any integrality equation for x and taking G to be its monic minimal polynomial over K. For the second part, since $A[t]/\mathfrak{p}A[t]$ is a domain and F modulo $\mathfrak{p}$ is a power of t, it follows that both G, H modulo $\mathfrak{p}$ are also powers of t, and hence their non-leading coefficients also belong to $\mathfrak{p}$. □

Theorem 3.3.8 (Going-down theorem)**.** *Let $A \subseteq B$ be an integral extension of domains such that A is normal. Let $\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$ be prime ideals of A and let $\mathfrak{q}_n$ be a prime ideal of B such that $\mathfrak{q}_n \cap A = \mathfrak{p}_n$. Then there is a chain of prime ideals $\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \cdots \subseteq \mathfrak{q}_n$ so that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for all $i = 1, \dots, n$.*

Proof. It suffices to handle the case when $n = 2$.

Let $S = B \setminus \mathfrak{q}_2$ and consider the ring homomorphism $A \to S^{-1}B$. We are done if we can show that $\mathfrak{p}_1 S^{-1}B \cap A = \mathfrak{p}_1$: Lemma 3.3.6 gives a prime $\mathfrak{q}'$ of $S^{-1}B$ whose pullback to A is $\mathfrak{p}_1$, and we can then take $\mathfrak{q}_1$ to be pullback of $\mathfrak{q}'$ to B.

So pick $x \in \mathfrak{p}_1 S^{-1}B \cap A$ and write $x = y/s$ with $y \in \mathfrak{p}_1 B$ and $s \in B \setminus \mathfrak{q}_2$. We need to show that $x \in \mathfrak{p}_1$. First, since $y \in \mathfrak{p}_1 B$, multiplication by y on $A[y]$ takes values in $\mathfrak{p}_1 A[y]$. Hence by the Cayley–Hamilton theorem (Theorem 1.5.1), y satisfies a monic polynomial $F(t)$ whose non-leading coefficients belong to $\mathfrak{p}_1$. By Lemma 3.3.7, we may assume that F is the monic minimal polynomial of y over K. Write out $F(y) = 0$:

$$y^n + a_1 y^{n-1} + \cdots + a_n = 0.$$

Divide by x^n to get

$$s^n + \frac{a_1}{x} s^{n-1} + \cdots + \frac{a_n}{x^n} = 0.$$

Since $x \in A$, the coefficients a_i/x^i belong to K. This is a minimal polynomial for s over K (if not, we can multiply by x^n to get a smaller degree polynomial for y). By Lemma 3.3.7, the coefficients belong to $\widetilde{A} = A$. Since $(a_i/x^i)x^i = a_i \in \mathfrak{p}_1$, we see that either $x \in \mathfrak{p}_1$ (in which case we're done) or $a_i/x^i \in \mathfrak{p}_1$ for all i. In the latter case, the integral equation above shows that $s^n \in \mathfrak{p}_1 B \subseteq \mathfrak{q}_2$, and hence $s \in \mathfrak{q}_2$, which is a contradiction. □

4. Chain conditions

4.1. **Noetherian modules.** Let A be a ring. An A-module M is **noetherian** if every submodule of M is finitely generated (including itself). The ring A is **noetherian** if it is noetherian as a module over itself, i.e., every ideal is finitely generated.

We say that M satisfies the **ascending chain condition (ACC)** if, given any increasing sequence of submodules $M_1 \subseteq M_2 \subseteq \cdots$, we must have $M_i = M_{i+1}$ for $i \gg 0$. For short, we say that the chain **stabilizes**.

Proposition 4.1.1. *The following are equivalent:*

(1) M is noetherian.
(2) M satisfies ACC.
(3) Every nonempty subset of submodules of M has a maximal element.

Proof. Suppose M is noetherian and let $M_1 \subseteq M_2 \subseteq \cdots$ be an increasing sequence of submodules. Let $M' = \bigcup_i M_i$ be the union of these submodules. Then M' is a submodule of M and hence is finitely generated, say by $m_1, \dots, m_n$. Each generator m_i belongs to some $M_{p(i)}$ and in particular they all belong to a particular M_p where $p = \max(p(1), \dots, p(n))$. But then $M_i = M_{i+1}$ if $i \geq p$, so M satisfies ACC.

Now let S be a nonempty subset of submodules. If S does not have a maximal element, then by induction on n we can construct a strictly increasing chain of submodules $M_1 \subsetneqq M_2 \subsetneqq \cdots \subsetneqq M_n$ contained in S. Namely, given such a chain, since M_n isn't maximal, there is some submodule in S that strictly contains it, so we can increase the length by 1 more. Hence (2) implies (3).

Now suppose that M is not noetherian, so that it has a non finitely generated submodule, i.e., there is a sequence of elements $x_1, x_2, \dots \in M$ such that x_i is not in the submodule generated by $x_1, \dots, x_{i-1}$ for all i. Let M_i be the submodule generated by $x_1, \dots, x_i$. Then $\{M_i\}$ is a nonempty subset of submodules that has no maximal element and so (3) implies (1). □

Proposition 4.1.2. *If $0 \to M_1 \to M_2 \xrightarrow{f} M_3 \to 0$ is a short exact sequence, then M_2 is noetherian if and only if M_1 and M_3 are noetherian.*

Proof. Suppose that M_2 is noetherian. Every ascending chain in M_1 is also an ascending chain in M_2 and hence stabilizes. Given an ascending chain in M_3, its preimage under f is an ascending chain which must stabilize, and applying f again gives the original chain, so it also stabilizes.

Now suppose that both M_1 and M_3 are noetherian. Given an inclusion of submodules $N \subseteq N'$ of M_2, we note that they are equal if and only if $N \cap M_1 = N' \cap M_1$ and $f(N) = f(N')$ (if $x \in N' \setminus N$ exists, then either $x \in M_1$ or x represents a nontrivial coset of M_1 that belongs to $f(N') \setminus f(N)$). Hence given any increasing chain of M_2, it stabilizes because its intersection with M_1 stabilizes and its image under f also stabilizes. □

Corollary 4.1.3. *Any finite direct sum of noetherian modules is noetherian.*

Proof. By induction, it suffices to consider the direct sum of 2 noetherian modules M, N. But then the result follows by considering the previous result with the short exact sequence $0 \to M \to M \oplus N \to N \to 0$. □

Corollary 4.1.4. *If A is a noetherian ring, then every finitely generated A-module is noetherian.*

Proof. Let M be a finitely generated module, say generated by $x_1, \dots, x_n$. Then we have a surjective map $f\colon A^n \to M$ given by $f(a_1, \dots, a_n) = a_1x_1 + \cdots + a_nx_n$. By Corollary 4.1.3, A^n is a noetherian module, and hence the same holds for M by Proposition 4.1.2 applied to $0 \to \ker f \to A^n \to M \to 0$. □

4.2. Noetherian rings.

Proposition 4.2.1. *If A is a noetherian ring, then so is A/I for any ideal $I \subset A$. In particular, if $f\colon A \to B$ is a surjective ring homomorphism, then B is noetherian.*

Proof. Every ideal of A/I is the homomorphic image of an ideal in A. For the second statement, $B \cong A/\ker f$. □

Proposition 4.2.2. *If A is a noetherian ring and $S \subseteq A$ is a multiplicative subset, then $S^{-1}A$ is a noetherian ring.*

Proof. By Proposition 2.4.1, every ideal of $S^{-1}A$ is of the form $S^{-1}I$ for some ideal $I \subset A$. We know that I is finitely generated, and the image of this generating set also generates $S^{-1}I$. □

Given an ideal I in A, a **minimal prime** of I is a prime ideal $\mathfrak{p}$ which contains I and is minimal with respect to inclusion amongst all of the prime ideals that contain I, i.e., if $\mathfrak{p} \supset \mathfrak{q} \supset I$ and $\mathfrak{q}$ is prime, then $\mathfrak{p} = \mathfrak{q}$.

Proposition 4.2.3. *If A is a noetherian ring, then every ideal has finitely many minimal primes.*

Proof. Suppose not. Then the set of ideals which do not have finitely minimal primes is nonempty. Since A is noetherian, this set has a maximal element, call it J. Then J is not prime (otherwise it only has one minimal prime, namely itself) and so there exist $x, y \in A$ such that $x, y \notin J$ but $xy \in J$. Let $\mathfrak{p}$ be any minimal prime of J. Then $xy \in \mathfrak{p}$ and hence either $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. In particular, we see that $\mathfrak{p}$ either contains (J, x) or (J, y). Furthermore, $\mathfrak{p}$ is a minimal prime of whichever it contains (since $\mathfrak{p}$ is minimal over J). But both (J, x) and (J, y) strictly contain J, so by definition, each one has finitely many minimal primes, which contradicts that J does not have finitely many minimal primes. □

An ideal I is **irreducible** if it is not the proper intersection of two other ideals, i.e., if $I = J_1 \cap J_2$, then either $J_1 = I$ or $J_2 = I$.

Proposition 4.2.4. *Every ideal in a noetherian ring A is a finite intersection of irreducible ideals.*

Proof. Suppose this is false and consider the subset of ideals which are not the finite intersection of irreducible ideals. Since A is noetherian, this has a maximal element I, which is not irreducible. Hence we can write $I = J_1 \cap J_2$ where both J_1 and J_2 strictly contain I. So J_1 and J_2 are finite intersections of irreducible ideals, but then the same is true for I, which is a contradiction. □

Remark 4.2.5. If I is irreducible, then $V(I) \subset \operatorname{Spec} A$ is an irreducible topological space. Hence the result says that if A is noetherian, then every closed subset of $\operatorname{Spec} A$ can be written as a finite union of irreducible closed subsets. □

This can lead to the notion of primary decomposition, but we're going to skip that topic. But here are some things we'll use.

Let $\mathfrak{q} \subset A$ be a proper ideal. Then $\mathfrak{q}$ is **primary** if, for all $x, y \in A$, $xy \in \mathfrak{q}$ implies that $x \in \mathfrak{q}$ or $y^n \in \mathfrak{q}$ for some $n > 0$. In terms of quotient rings, it means that every zerodivisor of $A/\mathfrak{q}$ is nilpotent.

Proposition 4.2.6. *If $\mathfrak{q}$ is primary, then $\mathfrak{p} = \sqrt{\mathfrak{q}}$ is prime.*

Proof. Suppose that $xy \in \mathfrak{p}$. Then $x^n y^n \in \mathfrak{q}$ for some $n > 0$, so either $x^n \in \mathfrak{q}$ (and hence $x \in \mathfrak{p}$) or $(y^n)^m \in \mathfrak{q}$ for some $m > 0$ (and hence $y \in \mathfrak{p}$). □

Proposition 4.2.7. *If A is noetherian, then an irreducible ideal I is primary. In particular, $\sqrt{I}$ is prime.*

Proof. Pick $x, y \in A/I$ such that $xy = 0$. Consider the chain of ideals

$$\mathrm{Ann}(y) \subseteq \mathrm{Ann}(y^2) \subseteq \cdots .$$

Since A/I is noetherian, this chain stabilizes, so there exists n such that $\mathrm{Ann}(y^n) = \mathrm{Ann}(y^{n+1})$. We claim that $(y^n) \cap (x) = 0$. To see this, pick $z \in (y^n) \cap (x)$, so that there exists $a, b \in A/I$ such that $z = ay^n = bx$. But then $yz = bxy = 0$ and so $ay^{n+1} = 0$ which means that $a \in \mathrm{Ann}(y^{n+1}) = \mathrm{Ann}(y^n)$, and hence $ay^n = z = 0$. In particular, let $\widetilde{x}, \widetilde{y} \in A$ be preimages of x, y; we see that $((\widetilde{y}^n) + I) \cap ((\widetilde{x}) + I) = I$. Since I is irreducible, we have either $\widetilde{x} \in I$ or $\widetilde{y}^n \in I$, i.e., every zerodivisor of A/I is nilpotent. □

Example 4.2.8. The converse can fail: let $A = \mathbf{Q}[x, y]$ and $\mathfrak{m} = (x, y)$. Then $\mathfrak{m}^2 = (x^2, xy, y^2)$ is a primary ideal, but we can write $(x^2, xy, y^2) = (x, y^2) \cap (x^2, y)$ so it is not irreducible. □

4.3. Hilbert basis theorem.

Theorem 4.3.1 (Hilbert basis theorem)**.** *If A is a noetherian ring, then the polynomial ring $A[x]$ is a noetherian ring. In particular, so is $A[x_1, \dots, x_n]$.*

Proof. Given a nonzero polynomial $F(x) = a_n x^n + \cdots + a_0$ with $a_i \in A$, let $\mathrm{init}(F) = a_n x^n$ denote its leading (initial) term, and define $\mathrm{init}(0) = 0$. Next, given an ideal $I \subset A[x]$, define $\mathrm{init}(I)$ to be the additive subgroup generated by $\{\mathrm{init}(F) \mid F \in I\}$. This is again an ideal of $A[x]$ since $\mathrm{init}(x^n F) = x^n \mathrm{init}(F)$, and for $a \in A$, if $a\mathrm{init}(F) \neq 0$, then $a\mathrm{init}(F) = \mathrm{init}(aF)$.

We claim that if $I \subseteq J$ are ideals in $A[x]$ and $\mathrm{init}(I) = \mathrm{init}(J)$, then $I = J$. If not, then pick $F \in J \setminus I$ of lowest possible degree. Then $\mathrm{init}(F) \in \mathrm{init}(I)$, so there exists $G \in I$ such that $\mathrm{init}(F) = \mathrm{init}(G)$, and so $G - F \in J \setminus I$ has lower degree.

Finally, suppose that $A[x]$ is not noetherian, so there exists a strictly increasing chain of ideals $0 = I_0 \subsetneqq I_1 \subsetneqq I_2 \subsetneqq \cdots$. By the claim, we get another strictly increasing chain of ideals $\mathrm{init}(I_1) \subsetneqq \mathrm{init}(I_2) \subsetneqq \cdots$ in $A[x]$. For each i, pick $a_i x^{d_i} \in \mathrm{init}(I_i) \setminus \mathrm{init}(I_{i-1})$. We can pass to a subsequence $i_1 \leq i_2 \leq$ such that $d_{i_1} \leq d_{i_2} \leq \cdots$. The chain of ideals $(a_{i_1}) \subseteq (a_{i_1}, a_{i_2}) \subseteq \cdots$ in A stabilizes, so there is some r such that a_{i_n} is generated by $a_{i_1}, \dots, a_{i_r}$ if $n > r$. But then $a_{i_n} x^{d_{i_n}}$ is generated by $a_{i_1} x^{d_{i_1}}, \dots, a_{i_r} x^{d_{i_r}}$ whenever $n > r$, which is a contradiction. Hence $A[x]$ is noetherian.

For the last statement, use induction on n noting that $A[x_1, \dots, x_n] \cong A[x_1, \dots, x_{n-1}][x]$. □

Corollary 4.3.2. *If A is a noetherian ring and B is a finitely generated A-algebra, then B is noetherian.*

Proof. If B has n generators as an A-algebra, then B is a quotient of $A[x_1, \dots, x_n]$. □

4.4. **Hilbert nullstellensatz.**

Lemma 4.4.1. *Let $A \subseteq B \subseteq C$ be rings. Assume that A is noetherian, that C is finitely generated as an A-algebra and finitely generated as a B-module. Then B is finitely generated as an A-algebra.*

Proof. The idea is to find a ring B' in between A and B which is a finitely generated A-algebra and so that C is a finitely generated B'-module. Once we do that, we know that B' is noetherian and then B is a finitely generated B'-module, and hence a finitely generated A-algebra.

Let $x_1, \dots, x_r \in C$ be A-algebra generators and let $y_1, \dots, y_s \in C$ be B-module generators. Hence every element $x \in C$ can be written as a polynomial in $x_1, \dots, x_r$ with coefficients in A. Furthermore, each x_i is a B-linear combination of the y_j, say $x_i = \sum_j b_{ij} y_j$. Substituting this in shows that x is a polynomial in the y_i with coefficients in the subring generated by A and the b_{ij}. Next, we can rewrite every product $y_i y_j$ in terms of the y_k, say $y_i y_j = \sum_k c_{ijk} y_k$ with $c_{ijk} \in B$. Now arbitrarily substitute products $y_i y_j$ for these linear combinations to see that x can be written as a linear combination of the y_i where the coefficients belong to the subring generated by A, the b_{ij}, and the c_{ijk}. We take B' to be this subring. □

Theorem 4.4.2 (Hilbert nullstellensatz)**.** *Let $\mathbf{k} \subset E$ be a field extension such that E is a finitely generated $\mathbf{k}$-algebra. Then E is finite-dimensional over $\mathbf{k}$.*

Proof. Let $x_1, \dots, x_n \in E$ be $\mathbf{k}$-algebra generators. There is a maximal transcendental subset, so we can reindex so that $x_1, \dots, x_r$ is a transcendental subset and E is a finite extension of $E' = \mathbf{k}(x_1, \dots, x_r)$. Then using the previous setup, we see that E' is a finitely generated $\mathbf{k}$-algebra. If $r = 0$ we are done, so suppose that $r > 0$ and that $f_1/g_1, \dots, f_m/g_m$ are a generating set for E' over $\mathbf{k}$, where the f_i and g_i are polynomials in the x_i with coefficients in $\mathbf{k}$. Then $g_1 g_2 \cdots g_m \neq -1$ (if so, then each $f_i/g_i = -f_i g_1 \cdots \hat{g}_i \cdots g_m$ is a polynomial and they can't generate all rational functions as a $\mathbf{k}$-algebra). Hence $h := g_1 g_2 \cdots g_m + 1$ is nonzero. Then $1/h$ cannot be a polynomial in $f_1/g_1, \dots, f_m/g_m$: if it were then we could clear denominators in such an expression to conclude that $g_1^{p_1} \cdots g_m^{p_m}/h$ is a polynomial in the x_i for some $p_i \geq 0$. But any irreducible polynomial that divides the numerator cannot divide the denominator, so this is a contradiction. □

Corollary 4.4.3. *If $\mathbf{k}$ is a field, and $\mathfrak{m}$ is a maximal ideal of $\mathbf{k}[x_1, \dots, x_n]$, then $\mathbf{k}[x_1, \dots, x_n]/\mathfrak{m}$ is a finite field extension of $\mathbf{k}$. In particular, if $\mathbf{k}$ is algebraically closed, then there exist $\alpha_1, \dots, \alpha_n \in \mathbf{k}$ such that $\mathfrak{m} = (x_1 - \alpha_1, \dots, x_n - \alpha_n)$.*

Proof. Let $E = \mathbf{k}[x_1, \dots, x_n]/\mathfrak{m}$. Then E is a field that is finitely generated over $\mathbf{k}$ and hence must be a finite extension.

If $\mathbf{k}$ is algebraically closed, then by definition the inclusion $\mathbf{k} \to E$ must be an isomorphism. In particular, let α_i be the image of x_i under the quotient map $\mathbf{k}[x_1, \dots, x_n] \to \mathbf{k}$ given by modding out by $\mathfrak{m}$. Then $x_i - \alpha_i \in \mathfrak{m}$, and so $(x_1 - \alpha_1, \dots, x_n - \alpha_n)$ is a maximal ideal contained in $\mathfrak{m}$. Hence they are equal. □

4.5. **Artinian modules.** Let A be a ring and M an A-module. Then M is **artinian** if its submodules satisfy the *descending chain condition* (DCC): for every sequence of submodules $M_1 \supseteq M_2 \supseteq \cdots$, we have $M_n = M_{n+1}$ for $n \gg 0$. We will also say that the chain **stabilizes**.

This is equivalent to the condition that every set of submodules has a minimal element. A ring is artinian if it is artinian as a module over itself, i.e., if its ideals satisfy DCC.

Proposition 4.5.1. *If $0 \to M_1 \to M_2 \to M_3 \to 0$ is a short exact sequence of A-modules, then M_2 is artinian if and only if M_1 and M_3 are artinian.*

Proof. The proof is exactly the same as the proof for Proposition 4.1.2. □

Corollary 4.5.2. *Finite direct sums of artinian modules are artinian. If A is an artinian ring, then every finitely generated A-module is artinian.*

An A-module M is **simple** if every A-submodule is either $\{0\}$ or M. A nonzero module M has a **composition series** if there exist a chain of submodules

$$M = M_0 \supsetneqq M_1 \supsetneqq \cdots \supsetneqq M_n = 0$$

such that M_i/M_{i+1} is a (nonzero) simple A-module for $i = 0, \dots, n-1$. The length of this chain is n (the number of strict inclusions). Define $\ell(M)$ to be the minimum length of a composition series, if it exists, and define $\ell(M) = \infty$ if no composition series exists. This is the **length** of M. In the first case, we say that M is a **finite length module**. We define $\ell(0) = -1$ and say that the zero module is also a finite length module.

Example 4.5.3. If A is a field, then a vector space is simple if and only if it is 0 or 1-dimensional. Furthermore, it has a composition series if and only if it is finite-dimensional and length coincides with dimension. We see here that the length of a composition series is always the same (we'll see that more generally next) but in general it is far from unique. □

Proposition 4.5.4. *Let M be a nonzero finite length module.*

(1) If N is a proper submodule, then $\ell(N) < \ell(M)$ and $\ell(M/N) < \ell(M)$.
(2) Every strict chain has length $\leq \ell(M)$ and every composition series of M has length $\ell(M)$.
(3) Every strictly decreasing chain of submodules of M can be completed to a composition series by inserting extra submodules. In particular, every strict chain of length $\ell(M)$ is a composition series.

Proof. (1) Choose a minimal length composition series for $0 = M_n \subsetneqq M_{n-1} \subsetneqq \cdots \subsetneqq M_0 = M$ for M and set $N_i = M_i \cap N$. Then we have injective maps $N_i/N_{i+1} \to M_i/M_{i+1}$ for all i; since M_i/M_{i+1} is simple, either $N_i/N_{i+1} = 0$, i.e., $N_i = N_{i+1}$, or the map is an isomorphism, so N_i/N_{i+1} is a nonzero simple module. Hence removing the equalities amongst the N_i gives a strict chain of length $\leq n$, and so $\ell(M) = n \geq \ell(N)$. If we have equality, this means that $N_i/N_{i+1} \to M_i/M_{i+1}$ is an isomorphism for all i; reverse induction on i we see that this implies that $N_i = M_i$ for all i (the base case uses that $M_n = N_n = 0$) and hence $N = M$.

Similarly, we can show that $\ell(M/N) < \ell(M)$ by instead considering the image of a composition series for M in M/N, we won't repeat the details.

(2) Now let $0 = M_k \subsetneqq \cdots \subsetneqq M_0 = M$ be any strict chain of submodules. By (1), we have $n = \ell(M) > \ell(M_1) > \cdots > \ell(M_{k-1}) \geq 0$, so that $k \leq n$. In particular, every composition series has length at most $\ell(M)$, but by definition they must all have this particular length.

(3) If $N \subsetneqq N'$ and N'/N is not simple, pick a proper nonzero submodule $P \subset N'/N$. Then the preimage P' of P in N' gives a larger strict chain $N \subsetneqq P' \subsetneqq N'$. Hence, any chain which is not a composition series can be made longer by inserting an extra submodule wherever the corresponding quotient module is not simple. This process must terminate: the original

chain has length at most $\ell(M)$ by (2), each insertion increases the length by 1, and finally, any chain of length $\ell(M)$ must be a composition series since otherwise we would be able to produce a strict chain of length $\ell(M)+1$, contradicting (2). □

Remark 4.5.5. Even more is true: if M has a composition series of length n, then the multiset of isomorphism classes $\{M_i/M_{i+1}\}$ depends only on M and not the choice of composition series. □

Corollary 4.5.6. *M is a finite length module if and only if it is both noetherian and artinian.*

Proof. If M has finite length, then every strict chain has length $\le \ell(M)$ and hence every ascending or descending chain stabilizes.

Conversely, suppose that M is noetherian and artinian and nonzero. The set of proper submodules is nonempty and hence has a maximal element M_1 by Proposition 4.1.1, and so M/M_1 is simple. If $M_1 \ne 0$, then again the set of proper submodules of M_1 is nonempty and has a maximal element M_2 and so M_1/M_2 is simple. Hence we can produce a sequence $M_1 \supsetneqq M_2 \supsetneqq \cdots$. Since M is artinian, this must stabilize (necessarily to 0 by our construction) and so we have produced a composition series. □

Noetherian modules must be finitely generated (because every submodule is finitely generated) but this need not be true for artinian modules.

Example 4.5.7. Consider $A = \mathbf{Q}[x]$ the polynomial ring in 1 variable and consider the Laurent polynomial ring $\mathbf{Q}[x, x^{-1}]$ as an A-module. Let M be the quotient of $\mathbf{Q}[x, x^{-1}]$ by the A-submodule generated by (x), so that M has a $\mathbf{Q}$-basis $\{1, x^{-1}, x^{-2}, \dots\}$ with the rule $x \cdot x^{-i} = x^{-i+1}$ if $i > 0$ and $x \cdot 1 = 0$. Then M is artinian and not finitely generated (left as exercise). □

Proposition 4.5.8. *If $0 \to M_1 \to M_2 \to M_3 \to 0$ is a short exact sequence of A-modules, then $\ell(M_2) = \ell(M_1) + \ell(M_3)$.*

Proof. First suppose that M_1 and M_3 both have composition series, call the first $0 = N_r \subsetneqq \cdots \subsetneqq N_0 = M_1$ and the second $0 = P_s \subsetneqq \cdots \subsetneqq P_0 = M_3$ and let P'_i be the preimage of P_i in M_2. Then

$$0 = N_r \subsetneqq \cdots \subsetneqq N_0 \subsetneqq P'_{s-1} \subsetneqq \cdots \subsetneqq P'_0 = M_2$$

is a composition series for M_2 which shows that $\ell(M_2) = \ell(M_1) + \ell(M_3)$.

On the other hand, if $\ell(M_1) = \infty$ or $\ell(M_3) = \infty$, then we have $\ell(M_2) = \infty$ (otherwise this violates (1) of Proposition 4.5.4). □

4.6. Artinian rings.

Proposition 4.6.1. *If A is artinian, then every prime ideal is maximal.*

Proof. Let $\mathfrak{p} \subset A$ be a prime ideal. Then $A/\mathfrak{p}$ is also artinian and an integral domain. Pick $x \in A/\mathfrak{p}$ nonzero. We have a descending chain of ideals $(x) \supseteq (x^2) \supseteq (x^3) \supseteq \cdots$, which stabilizes, so there exists n such that $(x^n) = (x^{n+1})$. In particular, there exists y such that $x^n = x^{n+1}y$. Since $A/\mathfrak{p}$ is a domain and $x \ne 0$, this implies that $xy = 1$, i.e., that x is a unit. So every nonzero element of $A/\mathfrak{p}$ is a unit, i.e., $A/\mathfrak{p}$ is a field so $\mathfrak{p}$ is a maximal ideal of A. □

Proposition 4.6.2. *An artinian ring has only finitely many maximal ideals.*

Proof. If not, suppose that A is an artinian ring with an infinite list of distinct maximal ideals $\mathfrak{m}_1, \mathfrak{m}_2, \dots$. Consider the descending 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 there exists n such that

$$\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n \cap \mathfrak{m}_{n+1},$$

so $\mathfrak{m}_{n+1} \supseteq \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$. But then there exists i such that $\mathfrak{m}_{n+1} \supseteq \mathfrak{m}_i$ which contradicts that these are all distinct maximal ideals. □

Proposition 4.6.3. *If A is an artinian ring, then A is noetherian.*

Proof. If not, then the set of ideals of A which are not finitely generated is nonempty, and since A is artinian, this set contains a minimal element, call it I. First, we claim that for all $x \in A$, either $xI = I$ or $xI = 0$. If $xI \neq I$, then xI is properly contained in I and hence is finitely generated. Furthermore, xI is a quotient of I via the multiplication by x map $I \to xI$. The kernel K of this map cannot be finitely generated by Proposition 4.1.2, and hence we have $K = I$ by minimality, so $xI = 0$. This proves the claim.

Now let $J = \mathrm{Ann}_A(I) = \{x \in A \mid xI = 0\}$. If $xy \in J$ and $y \notin J$, then by the claim we have $0 = xyI = x(yI) = xI$ and hence $x \in J$. This tells us that J is a prime ideal and so A/J is an artinian domain and I is naturally an A/J-module. By Proposition 4.6.1, A/J is a field, and so I is a vector space (necessarily infinite-dimensional) over this field. However, ideals contained in I correspond to subspaces as an A/J-vector space, so by construction, I is an infinite-dimensional vector space such that every proper subspace is finite-dimensional. But such an example does not exist (take any basis for I and take the span of all but one of the basis vectors), so we have reached a contradiction. □

Corollary 4.6.4. *If A is an artinian ring, then every finitely generated A-module is finite length.*

Proof. From the previous result, A is also noetherian, so every finitely generated A-module is both artinian and noetherian. Now use Corollary 4.5.6. □

Theorem 4.6.5. *A ring is artinian if and only if it is noetherian and every prime ideal is maximal.*

Proof. We've already seen that artinian rings are noetherian and that every prime ideal is maximal.

Now let A be a noetherian ring for which every prime ideal is maximal. By Proposition 4.2.4 we can write the 0 ideal as a finite intersection of irreducible ideals

$$(0) = I_1 \cap \cdots \cap I_r$$

and by Proposition 4.2.7, the radical $\mathfrak{p}_i = \sqrt{I_i}$ is prime for each i. Since radicals commute with finite intersections, the nilradical $\mathfrak{N}$ of A is a finite intersection of primes

$$\mathfrak{N} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r.$$

Since $\mathfrak{N}$ is also the intersection of all prime ideals, for any other prime $\mathfrak{p}$, we have $\mathfrak{p} \supseteq \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$ which means $\mathfrak{p} \in \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ since they are all maximal. Hence there are only finitely many prime ideals. Next, since each $\mathfrak{p}_i$ is maximal, they are coprime to one another, and so

$$A/\mathfrak{N} \cong A/\mathfrak{p}_1 \times \cdots \times A/\mathfrak{p}_r,$$

and the right side is a product of fields, so $A/\mathfrak{N}$ is artinian. Finally, since A is noetherian, $\mathfrak{N}$ is finitely generated and hence $\mathfrak{N}^n = 0$ for some $n > 0$. Each quotient $\mathfrak{N}^i/\mathfrak{N}^{i+1}$ is a finitely generated $A/\mathfrak{N}$-module, and hence has finite length. So

$$\ell(A) = \sum_{i=0}^{n-1} \ell(\mathfrak{N}^i/\mathfrak{N}^{i+1}) < \infty,$$

and so A is artinian (Corollary 4.5.6). □

Theorem 4.6.6. *Every artinian ring A is isomorphic to a finite direct product of local artinian rings, namely the localizations at its maximal ideals. Furthermore, any other such direct product decomposition must be this one (up to permutation and isomorphism).*

Proof. By Proposition 4.6.2, A has only finitely many maximal ideals, call them $\mathfrak{m}_1, \dots, \mathfrak{m}_n$. By Proposition 4.6.1, these are also all of the prime ideals, so using coprimeness of distinct maximal ideals, we have

$$\mathfrak{m}_1 \cdots \mathfrak{m}_n = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n = \mathfrak{N}$$

is the nilradical. Since A is noetherian, $\mathfrak{N}^k = 0$ for some $k > 0$. In particular, using again coprimeness, we get $\mathfrak{m}_1^k \cap \cdots \cap \mathfrak{m}_n^k = \mathfrak{m}_1^k \cdots \mathfrak{m}_n^k = 0$, and so we have an isomorphism

$$A \cong A/\mathfrak{m}_1^k \times \cdots \times A/\mathfrak{m}_n^k.$$

Each of $A/\mathfrak{m}_i^k$ is an artinian local ring. Now localize this decomposition at $\mathfrak{m}_i$. If $j \neq i$, then $(A/\mathfrak{m}_j^k)_{\mathfrak{m}_i} = 0$ since there exists $y \in \mathfrak{m}_j \setminus \mathfrak{m}_i$ which is both nilpotent and invertible in this localization (which forces it to be 0). On the other hand, the image of $\mathfrak{m}_i$ in $A/\mathfrak{m}_i^k$ is its unique maximal ideal, so $(A/\mathfrak{m}_i^k)_{\mathfrak{m}_i}$ is the same as $A/\mathfrak{m}_i^k$. We conclude that

$$A \cong A_{\mathfrak{m}_1} \times \cdots \times A_{\mathfrak{m}_n}.$$

On the other hand, suppose have a direct product decomposition

$$A \cong A_1 \times \cdots \times A_r$$

where the A_i are local artinian rings. Since this is a finite product, every prime ideal is of the form $I_1 \times \cdots \times I_r$ where I_i is a prime ideal for some i and $I_j = A_j$ for $j \neq i$. In particular, since every prime of A and each A_i is maximal, we see that A has r maximal ideals, so $r = n$. Furthermore, if we localize at the ith maximal ideal, call it $\mathfrak{p}_i$, then we get $(A_j)_{\mathfrak{p}_i} = 0$ for $j \neq i$ and $(A_i)_{\mathfrak{p}_i} \cong A_i$, so that $A_{\mathfrak{p}_i} \cong A_i$. This proves the claimed uniqueness statement. □

Let's summarize the above discussion:

Theorem 4.6.7. *The following class of rings are the same:*

1. *Artinian rings.*
2. *Noetherian rings such that every prime ideal is maximal.*
3. *Rings which are finite length as modules over themselves.*
4. *Finite direct products of artinian local rings.*

5. Gradings and filtrations

5.1. **Graded rings and Hilbert series.**

Definition 5.1.1. Let $(\Gamma, +)$ be an abelian semigroup (i.e., $+$ is associative, commutative, and has a unit) and let A be a ring. A Γ-**grading** on A is a direct sum decomposition (of A as an abelian group under addition)

$$A = \bigoplus_{\gamma \in \Gamma} A_\gamma$$

such that if $f \in A_\gamma$ and $f' \in A_{\gamma'}$, then $ff' \in A_{\gamma+\gamma'}$.

Given such a grading on A, a Γ-**grading** on an A-module M is a direct sum decomposition

$$M = \bigoplus_{\gamma \in \Gamma} M_\gamma$$

such that if $f \in A_\gamma$ and $m \in M_{\gamma'}$, then $fm \in M_{\gamma+\gamma'}$. □

Typically, we deal with the case that $\Gamma = \mathbf{Z}$ or $\mathbf{Z}_{\geq 0}$. In that case, we will write $M_{\geq d}$ for the direct sum $\bigoplus_{n \geq d} M_n$. For any integer d, we let $M(d)$ denote M with the adjusted grading $M(d)_n = M_{d+n}$. If $d \leq 0$ and M is $\mathbf{Z}_{\geq 0}$-graded, then $M(d)$ is also $\mathbf{Z}_{\geq 0}$-graded.

A homomorphism between graded modules $f \colon M \to N$ is **homogeneous of degree** d if $f(M_i) \subseteq N_{i+d}$ for all i. We can always interpret it as a degree 0 map by shifting the domain $f \colon M(-d) \to N$ (this is very useful notation).

Finally, if M and N are graded, then their direct sum and tensor product are defined by

$$(M \oplus N)_n = M_n \oplus N_n, \qquad (M \otimes N)_n = \bigoplus_{i=0}^{n} M_i \otimes N_{n-i}.$$

Example 5.1.2. For any ring A, the polynomial ring $A[x_1, \dots, x_n]$ is $\mathbf{Z}_{\geq 0}$-graded by setting $A[x_1, \dots, x_n]_d$ to be the subspace of homogeneous polynomials of degree d, i.e., A-linear combinations of $x_1^{d_1} \cdots x_n^{d_n}$ such that $d_1 + \cdots + d_n = d$. □

For this rest of this section, we fix a noetherian ring A with a $\mathbf{Z}_{\geq 0}$-grading $A = \bigoplus_{d \geq 0} A_d$. Then A_0 is a quotient ring of A (by the ideal $A_+ := \bigoplus_{d>0} A_d$), and so is also noetherian.

We will also fix an **additive function** λ on the class of finitely generated A_0-modules. Precisely, this means that given a finitely generated A_0-module M, $\lambda(M)$ is an integer, and for every short exact sequence

$$0 \to M_1 \to M_2 \to M_3 \to 0,$$

we have $\lambda(M_2) = \lambda(M_1) + \lambda(M_3)$.

Example 5.1.3. If A_0 is a field, then $\lambda = \dim$ is an additive function. In this case, λ is also multiplicative in the sense that $\lambda(V \otimes W) = \lambda(V)\lambda(W)$.

More generally, if A_0 is artinian, then the length function is additive. □

Now let M be a $\mathbf{Z}_{\geq 0}$-graded and finitely generated A-module. Then each M_n is a finitely generated A_0-module: any finite list of homogeneous generators of $M_{\geq n}$ as an A-module gives a finite list of generators for M_n as an A_0-module by only taking those of degree n. In particular, $\lambda(M_n)$ is defined.

The **Hilbert series of M (with respect to λ)**[1] is the formal power series (we'll use the variable t)

$$\mathrm{H}_M(\lambda, t) = \sum_{n \geq 0} \lambda(M_n) t^n \in \mathbf{Z}[\![t]\!].$$

[1] Atiyah–Macdonald call this a Poincaré series, but this is now usually used in a different context.

In the special case that A_0 is a field and $\lambda = \dim$, we will just write $\mathrm{H}_M(t)$. If $d \geq 0$, then

$$\mathrm{H}_{M(-d)}(\lambda, t) = t^d \mathrm{H}_M(\lambda, t).$$

Remark 5.1.4. We could also allow general $\mathbf{Z}$-graded finitely generated modules M. In that case, $M_n = 0$ for n sufficiently negative: A is in non-negative degrees and so the degrees of a finite list of generators gives a lower bound for n such that $M_n \neq 0$. In that case, its Hilbert series is a Laurent series in general. This allows some more flexibility, but also creates additional cumbersome notation, so we try to avoid it. □

For the next result, we recall that a formal power series is a multiplicative unit if and only if its constant term is invertible (in this case, meaning it is ± 1). Hence an expression like $1/(1-t^d)$ means the multiplicative inverse of $1-t^d$ thought of as a formal power series.

Theorem 5.1.5. *Suppose that A is generated as an A_0-algebra by homogeneous elements of positive degrees $d_1, \dots, d_r$. Then for every $\mathbf{Z}_{\geq 0}$-graded finitely generated A-module M, there exists $h_M(t) \in \mathbf{Z}[t]$ such that*

$$\mathrm{H}_M(\lambda, t) = \frac{h_M(t)}{(1-t^{d_1}) \cdots (1-t^{d_r})}.$$

Proof. We do induction on the number of generators r of A. If $r = 0$, then $A = A_0$ and $M_n = 0$ for $n \gg 0$. In particular, $\mathrm{H}_M(\lambda, t)$ is just a polynomial in t, so there is nothing to show.

Otherwise, suppose the result is known for any finitely generated module over a finitely generated A_0-algebra with $r-1$ generators. Let $x_1, \dots, x_r$ be homogeneous generators of degrees $d_1, \dots, d_r$, respectively. Multiplication by x_r gives a degree d_r map from M to itself; let

$$K = \{m \mid x_r m = 0\}$$

be its kernel. Then we have an exact sequence

$$0 \to K(-d_r) \to M(-d_r) \xrightarrow{\cdot x_r} M \to M/x_r M \to 0.$$

Since A is noetherian, K is also finitely generated, and since λ is additive, we have a relation

$$t^{d_r} \mathrm{H}_K(\lambda, t) - t^{d_r} \mathrm{H}_M(\lambda, t) + \mathrm{H}_M(\lambda, t) - \mathrm{H}_{M/x_r M}(\lambda, t) = 0,$$

which can be rewritten as

$$\mathrm{H}_M(\lambda, t) = (1-t^{d_r})^{-1} (\mathrm{H}_{M/x_r M}(\lambda, t) - t^{d_r} \mathrm{H}_K(\lambda, t)).$$

Finally, x_r is in the annihilator of both $M/x_r M$ and K, so that are finitely generated modules over A/x_r, which is inherits a grading from A and is generated by the cosets of $x_1, \dots, x_{r-1}$. Hence, by induction, there exist integer-coefficient polynomials $h_{M/x_r M}(t)$ and $h_K(t)$ such that

$$\mathrm{H}_{M/x_r M}(\lambda, t) = \frac{h_{M/x_r M}(t)}{(1-t^{d_1}) \cdots (1-t^{d_{r-1}})}, \qquad \mathrm{H}_K(\lambda, t) = \frac{h_K(t)}{(1-t^{d_1}) \cdots (1-t^{d_{r-1}})},$$

and hence we can take

$$h_M(t) = h_{M/x_r M}(t) - t^{d_r} h_K(t)$$

to fulfill the statement of the theorem. □

Example 5.1.6. Suppose A_0 is a field and $\lambda = \dim$ and that $A = A_0[x_1, \dots, x_r]$ is a polynomial ring. Then $A \cong A_0[x_1] \otimes \cdots \otimes A_0[x_r]$ and since λ is multiplicative, we have

$$\mathrm{H}_A(t) = \mathrm{H}_{A_0[x_1]}(t) \cdots \mathrm{H}_{A_0[x_r]}(t).$$

But $\mathrm{H}_{A_0[x_i]}(t) = \sum_{n \geq 0} t^{nd_i} = (1 - t^{d_i})^{-1}$, and so

$$\mathrm{H}_A(t) = \frac{1}{(1 - t^{d_1}) \cdots (1 - t^{d_r})}.$$

More generally, if A_0 is an artinian ring and $\lambda = \ell$ is the length function, then

$$\mathrm{H}_A(t) = \frac{\ell(A_0)}{(1 - t^{d_1}) \cdots (1 - t^{d_r})}$$

since each monomial of degree d contributes length $\ell(A_0)$ rather than just 1 dimension. □

Having a Hilbert series in this particular form imposes strong restrictions on the **Hilbert function** $n \mapsto \lambda(M_n)$. First, consider the case when all d_i are 1. We have the following general and elementary statement that is relevant here.

Proposition 5.1.7. *Let a_n be a sequence. Then there exists a polynomial $f(t)$ such that*

$$\sum_{n \geq 0} a_n t^n = \frac{f(t)}{(1-t)^r}$$

if and only if there exists a polynomial $\alpha(x)$ of degree $\leq r - 1$ such that $\alpha(n) = a_n$ for $n \gg 0$.

In particular, if this holds, then $1 + \deg \alpha(x)$ is the order of the pole at $t = 1$ of $\frac{f(t)}{(1-t)^r}$, i.e., r minus the multiplicity of 1 as a root of $f(t)$.

Proof. First suppose that $\sum_{n \geq 0} a_n t^n$ has the above form. We note that $(1 - t)^{-1} = \sum_{n \geq 0} t^n$ and we claim that

$$(1 - t)^{-r} = \sum_{n \geq 0} \binom{r + n - 1}{r - 1} t^n.$$

The coefficient of t^n in $(\sum_{a \geq 0} t^a)^r$ is the number of r-tuples $(a_1, \dots, a_r)$ of non-negative integers such that $a_1 + \cdots + a_r = n$. We can encode each solution with a sequence of n symbols a and $r - 1$ symbols + by placing a + after the first a_1 copies of a, after the next a_2 copies of a, etc. Every such sequence appears exactly once, so we see that the number of solutions is just $\binom{r-1+n}{r-1}$.

Finally, suppose that $N = \deg f$ and write $f(t) = \sum_i f_i t^i$. Then for all $n \geq N$, we have

$$a_n = \sum_{i=0}^{N} f_i \binom{r + n - i - 1}{r - 1}.$$

If we define $g(x) = \frac{1}{(r-1)!}(r + x - 1)(r + x - 2) \cdots (x + 1)$, then

$$g(n) = \binom{r + n - 1}{r - 1}$$

for all $n \geq 0$ (technically all $n \geq -r + 1$, but this is sufficient) and $g(x)$ is a degree $r - 1$ polynomial, and so we take $\alpha(x) = \sum f_i g(x - i)$.

Now we prove the converse, so we assume that there is a polynomial $\alpha(x)$ of degree $\leq r - 1$ such that $\alpha(n) = a_n$ for $n \gg 0$. We prove the result by induction on r; if $r = 1$, then a_n

is eventually constant and hence $\sum_{n\geq 0} a_n t^n$ can be written as a polynomial in t plus this constant times the geometric series $\sum_{n\geq 0} t^n = (1-t)^{-1}$, so the result holds. Otherwise, define $b_n = a_n - a_{n-1}$ (with the convention $a_{-1} = 0$). We note that $\alpha(x) - \alpha(x-1)$ is a polynomial of degree $\leq r-2$ and so by induction, there exists a polynomial $f(t)$ such that

$$(1-t)\sum_{n\geq 0} a_n t^n = \sum_{n\geq 0} b_n t^n = \frac{f(t)}{(1-x)^{r-1}}.$$

Now divide by $1-t$.

For the last statement, let d be the order of the pole of $\sum_{n\geq 0} a_n t^n$ at $t=1$. This means we can write it in the form $\frac{f(t)}{(1-t)^d}$ where $f(1) \neq 0$ and so by the above discussion there is a polynomial $\alpha(x)$ of degree $\leq d-1$ such that $\alpha(n) = a_n$ for $n \gg 0$. Suppose that the degree is $\leq d-2$. Then we have an equality of the form

$$\frac{f(t)}{(1-t)^d} = \frac{g(t)}{(1-t)^{d-1}}.$$

Clearing denominators shows that $f(1) = 0$, which is a contradiction. Hence $\deg \alpha = d-1$. □

Corollary 5.1.8. *If A is generated by r degree 1 elements, then for every finitely generated $\mathbf{Z}_{\geq 0}$-graded A-module M, there exists a polynomial $p_M(t)$ of degree $\leq r-1$ such that $\lambda(M_n) = p_M(n)$ for $n \gg 0$.*

The polynomial $p_M(n)$ is called the **Hilbert polynomial** of M.

The general case can also be described by polynomials, though there is some periodicity involved. A function $g(x)$ defined on the non-negative integers is a **quasi-polynomial function of period** m if there exist polynomials $p_0, \dots, p_{m-1}$ such that $g(n) = p_i(n)$ whenever $n \equiv i \pmod{m}$. We define the degree of g to be the maximum of the degrees of the p_i.

Corollary 5.1.9. *If A is generated by elements $x_1, \dots, x_r$ of positive degrees $d_1, \dots, d_r$, then for every finitely generated $\mathbf{Z}_{\geq 0}$-graded A-module M, there exists a quasi-polynomial $p_M(x)$ of period $\operatorname{lcm}(d_1, \dots, d_r)$ and degree $\leq r-1$ such that $\lambda(M_n) = p_M(n)$ for $n \gg 0$.*

5.2. Filtrations.

Let M be an A-module and let $I \subset A$ be an ideal. A decreasing chain $\mathcal{F}$ of submodules (finite or not) $M = M_0 \supseteq M_1 \supseteq \cdots$ is called a **filtration** of M. It is an I-**filtration** if $IM_n \subseteq M_{n+1}$ for all n and it is a **stable** I-**filtration** if, in addition, $IM_n = M_{n+1}$ for $n \gg 0$. This is equivalent to saying that there exists n such that $I^i M_n = M_{n+i}$ for all $i \geq 0$.

Example 5.2.1. If we set $M_n = I^n M$, then this is a stable I-filtration. □

Lemma 5.2.2. *Let $M = M_0 \supset M_1 \supset \cdots$ and $M = M'_0 \supset M'_1 \supset \cdots$ be I-stable filtrations of a module M. Then there exists n_0 such that $M_{n+n_0} \subseteq M'_n$ and $M'_{n+n_0} \subseteq M_n$ for all $n \geq 0$.*

Proof. Since both filtrations are I-stable, there exists n_0 such that $I^i M_{n_0} = M_{n_0+i}$ and $I^i M'_{n_0} = M'_{n_0+i}$ for all $i \geq 0$. Then, for all $i \geq 0$, we have

$$M_{n_0+i} = I^i M_{n_0} \subseteq I^i M \subseteq M'_i$$

and similarly,

$$M'_{n_0+i} = I^i M'_{n_0} \subseteq I^i M \subseteq M_i.$$

□

The **Rees algebra** of I is the direct sum[2]

$$\mathrm{B}_I A = \bigoplus_{n \geq 0} I^n.$$

As usual, $I^0 = A$. This has a natural ring structure, which we can make clearer by introducing a new variable t. Then we embed $\mathrm{B}_I A$ into the polynomial ring $A[t]$ by identifying I^n with $I^n t^n = \{ft^n \mid f \in I^n\}$. In this case, $\mathrm{B}_I A$ is a subring of $A[t]$. This naturally has the structure of a $\mathbf{Z}_{\geq 0}$-graded A-algebra if we set $(\mathrm{B}_I A)_d = I^d t^d$.

Given an I-filtration $\mathcal{F}$ on M, we define

$$\mathrm{B}_{\mathcal{F}} M = \bigoplus_{n \geq 0} M_n,$$

which is naturally $\mathbf{Z}_{\geq 0}$-graded over the ring $\mathrm{B}_I R$ by setting $(\mathrm{B}_{\mathcal{F}} M)_d = M_d$. For clarity, we will sometimes write $M_n t^n$ when discussing this as a summand of $\mathrm{B}_{\mathcal{F}} M$ to distinguish it from M_n as a submodule of M.

We also define the **associated graded ring** by

$$\mathrm{gr}_I\, A = \bigoplus_{n \geq 0} I^n / I^{n+1} \cong \mathrm{B}_I A / It\mathrm{B}_I A$$

and, if $\mathcal{F}$ is an I-filtration on M, we also define the **associated graded module**

$$\mathrm{gr}_{\mathcal{F}}\, M = \bigoplus_{n \geq 0} M_n / M_{n+1}$$

which is a module over $\mathrm{gr}_I\, A$ in the natural way.

Lemma 5.2.3. *If A is a noetherian ring, then $\mathrm{B}_I A$ and $\mathrm{gr}_I\, A$ are noetherian.*

Proof. Since A is noetherian, I is finitely generated, say by $f_1, \dots, f_r \in I$. Then the elements $f_1 t, \dots, f_r t$ in $\mathrm{B}_I A$ generate it as a ring, and so $\mathrm{B}_I A$ is noetherian by the Hilbert basis theorem. This also implies that $\mathrm{gr}_I\, A$ is noetherian since it is a quotient of $\mathrm{B}_I A$. □

Proposition 5.2.4. *Suppose that A is a noetherian ring and that M is a finitely generated A-module. Given an ideal $I \subset A$, let $\mathcal{F}$ be an I-filtration of M. Then $\mathcal{F}$ is an I-stable filtration if and only if $\mathrm{B}_{\mathcal{F}} M$ is a finitely generated $\mathrm{B}_I A$-module.*

Proof. Suppose that $\mathcal{F}$ is I-stable, so that there exists n such that $M_{n+i} = I^i M_n$ for all $i \geq 0$. In that case, $\mathrm{B}_{\mathcal{F}} M$ is generated as a $\mathrm{B}_I A$-module by the elements of $M_0 t^0, \dots, M_n t^n$. Each of $M_0, \dots, M_n$ is a finitely generated A-module since M is a noetherian module. If we pick a finite list of generators for each, then we get a finite list of generators for $\mathrm{B}_{\mathcal{F}} M$.

Conversely, suppose that $\mathrm{B}_{\mathcal{F}} M$ is a finitely generated $\mathrm{B}_I A$-module. Given a finite list of generators, each one is a finite sum of its homogeneous components, so we can always replace each by its homogeneous components to get a finite list of homogeneous generators. Suppose the maximum degree of one of these generators is n. Then every element in $M_{n+i} t^{n+i}$ is a linear combination of these generators of the form $\sum_j f_j m_j$ where $m_j \in M_{d(j)}$ and $f_j \in I^{n+i-d(j)}$. Note that if $d(j) < n$, then we can always rewrite $f_j m_j$ as a sum of products of elements in I^i and M_n, so that we see that $I^i M_n = M_{n+i}$ and hence $\mathcal{F}$ is I-stable. □

Corollary 5.2.5. *If $\mathcal{F}$ is I-stable, then $\mathrm{gr}_{\mathcal{F}}(M)$ is a finitely generated $\mathrm{gr}_I(A)$-module.*

[2] Sometimes called the **blowup algebra** because of its relation to the blowup procedure in algebraic geometry, and hence the notation B.

Corollary 5.2.6 (Artin–Rees lemma)**.** *Suppose that A is a noetherian ring and that M is a finitely generated A-module. Given an ideal $I \subset A$, let $\mathcal{F}$ be an I-stable filtration of M. For any submodule $M' \subset M$, the filtration $\mathcal{F}'$ given by $M'_n = M' \cap M_n$ is also I-stable.*

Proof. By Proposition 5.2.4, $\mathrm{B}_{\mathcal{F}} M$ is a finitely generated $\mathrm{B}_I A$-module, and hence is noetherian by Lemma 5.2.3. Furthermore, $\mathrm{B}_{\mathcal{F}'} M'$ is naturally a $\mathrm{B}_I A$-submodule of $\mathrm{B}_{\mathcal{F}} M$, and hence is finitely generated. Again by Proposition 5.2.4, $\mathcal{F}'$ is I-stable. □

Corollary 5.2.7. *Let A be a noetherian ring, M a finitely generated A-module, $M' \subseteq M$ a submodule, and let $I \subset A$ be an ideal. There exists an integer k such that if $n \ge k$, then*

$$(I^n M) \cap M' = I^{n-k}((I^k M) \cap M').$$

Proof. Consider the I-stable filtration $M_n = I^n M$ of M. By the Artin–Rees lemma, $M'_n = (I^n M) \cap M'$ is also I-stable. □

5.3. **The Hilbert–Samuel polynomial.** For this section, A is a noetherian local ring with maximal ideal $\mathfrak{m}$, and $\mathfrak{q}$ is an ideal such that $\sqrt{\mathfrak{q}} = \mathfrak{m}$ which can be generated by s elements $x_1, \dots, x_s$. Note that this in fact implies that $\mathfrak{q}$ is a primary ideal, and hence it is called $\mathfrak{m}$-primary. We won't actually need to use this, though we will use the terminology.

Proposition 5.3.1. *Let M be a finitely generated A-module and let $\mathcal{F}$ be a stable $\mathfrak{q}$-filtration of M. The following properties hold.*

1. *M/M_n is finite length for all $n \ge 0$.*
2. *There exists a polynomial $g(x)$ of degree $\le s$ such that $g(n) = \ell(M/M_n)$ for $n \gg 0$. Furthermore, the degree of $g(x)$ is the order of the pole at $t = 1$ of $\mathrm{H}_{\mathrm{gr}_{\mathcal{F}}(M)}(t)$ when written as a rational function.*
3. *The degree and leading coefficient of $g(x)$ do not depend on the choice of $\mathcal{F}$, only on M and $\mathfrak{q}$.*

Proof. Define

$$B = \mathrm{gr}_{\mathfrak{q}}(A) = \bigoplus_{n \ge 0} \mathfrak{q}^n/\mathfrak{q}^{n+1}, \qquad N = \mathrm{gr}_{\mathcal{F}}(M) = \bigoplus_{n \ge 0} M_n/M_{n+1}.$$

By Lemma 5.2.3, B is a noetherian ring and by Corollary 5.2.5, N is a finitely generated B-module. In particular, $N_n = M_n/M_{n+1}$ is a finitely generated B_0-module for all n. Since $\mathfrak{q}$ is $\mathfrak{m}$-primary, $B_0 = A/\mathfrak{q}$ is artinian (the only prime ideal is the image of $\mathfrak{m}$, now use Theorem 4.6.5), and hence M_n/M_{n+1} has finite length (Corollary 4.6.4). Using the short exact sequence

$$0 \to M_{n-1}/M_n \to M/M_n \to M/M_{n-1} \to 0,$$

we see that

$$\ell(M/M_n) = \sum_{i=0}^{n-1} \ell(M_i/M_{i+1})$$

which proves (1). This implies that

$$(1-t) \sum_{n \ge 0} \ell(M/M_n) t^n = t \sum_{n \ge 0} \ell(M_n/M_{n+1}) t^n.$$

Next, B is generated by the degree 1 elements, namely the images of $x_1, \dots, x_s$ under the map $\mathfrak{q} \to \mathfrak{q}/\mathfrak{q}^2$. Hence, by Theorem 5.1.5, $\sum_{n \ge 0} \ell(M_n/M_{n+1}) t^n$ is a rational function with denominator $(1-t)^s$. Now divide the above expression by $1-t$ and use Proposition 5.1.7 to see that there exists a polynomial $g(x)$ of degree $\le s$ such that $g(n) = \ell(M/M_n)$ for $n \gg 0$, which proves (2).

Finally, to prove (3), let $M = M'_0 \supseteq M'_1 \supseteq \cdots$ be another $\mathfrak{q}$-stable filtration of M. Then there exists a polynomial $g'(x)$ of degree $\le s$ such that $g'(n) = \ell(M/M'_n)$ for $n \gg 0$. By Lemma 5.2.2, there exists n_0 such that $M_{n+n_0} \subseteq M'_n$ and $M'_{n+n_0} \subseteq M_n$ for all $n \ge 0$. In particular, for all $n \ge 0$, we have

$$\ell(M/M_{n+n_0}) \ge \ell(M/M'_n), \qquad \ell(M/M'_{n+n_0}) \ge \ell(M/M_n).$$

This implies that for all $n \gg 0$, we have $g(n+n_0) \ge g'(n) \ge g(n-n_0)$. Assuming that g is not identically 0 for large n (in which case g' would also be), divide both sides by $g(n+n_0)$ to get

$$1 \ge \frac{g'(n)}{g(n+n_0)} \ge \frac{g(n-n_0)}{g(n+n_0)}.$$

Since g is a polynomial, the limit of the last term for $n \to \infty$ is 1. This implies that

$$\lim_{n\to\infty} \frac{g'(n)}{g(n+n_0)} = 1$$

and hence that $g'(x)$ and $g(x+n_0)$ have the same leading coefficient and degree. Finally, $g(x+n_0)$ and $g(x)$ also have the same leading coefficient and degree. □

Using the previous result, the **Hilbert–Samuel polynomial** (of M with respect to $\mathfrak{q}$) is denoted $\chi^M_{\mathfrak{q}}(x)$, and defined to be the (unique) polynomial such that

$$\chi^M_{\mathfrak{q}}(n) = \ell(M/\mathfrak{q}^n M) \qquad \text{for } n \gg 0.$$

Importantly, its degree and leading coefficient can be computed using any $\mathfrak{q}$-stable filtration (and this data will be the most important for us later, rather than the actual polynomial). If $M = A$, then we just write $\chi_{\mathfrak{q}}$ in place of $\chi^A_{\mathfrak{q}}$.

Proposition 5.3.2. *Notation as above, we have* $\deg \chi_{\mathfrak{q}}(x) = \deg \chi_{\mathfrak{m}}(x)$.

Proof. Since $\sqrt{\mathfrak{q}} = \mathfrak{m}$ and $\mathfrak{m}$ is finitely generated, there exists d such that $\mathfrak{m}^d \subseteq \mathfrak{q}$. In particular, for all $n \ge 0$, we have $\mathfrak{m}^{dn} \subseteq \mathfrak{q}^n \subseteq \mathfrak{m}^n$. This implies that for all $n \ge 0$, we have

$$\ell(A/\mathfrak{m}^{dn}) \ge \ell(A/\mathfrak{q}^n) \ge \ell(A/\mathfrak{m}^n),$$

and, in particular, for $n \gg 0$, we have $\chi_{\mathfrak{m}}(dn) \ge \chi_{\mathfrak{q}}(n) \ge \chi_{\mathfrak{m}}(n)$. This is only possible if $\deg \chi_{\mathfrak{m}}(x) = \deg \chi_{\mathfrak{q}}(x)$. □

Summarizing the points in the proofs above, we have (with $\mathbf{k} = A/\mathfrak{m}$)

$$(1-t)\sum_{n\ge 0} \dim_{\mathbf{k}}(A/\mathfrak{m}^n)t^n = t\sum_{n\ge 0} \dim_{\mathbf{k}}(\mathfrak{m}/\mathfrak{m}^n)t^n = t \cdot \mathrm{H}_{\mathrm{gr}_{\mathfrak{m}}(A)}(t).$$

In particular, $\deg \chi_{\mathfrak{m}}(x)$ is the order of the pole at $t = 1$ of $\mathrm{H}_{\mathrm{gr}_{\mathfrak{m}}(A)}(t)$ when written as a rational function.

Proposition 5.3.3. *Let $x \in A$ be a nonzerodivisor on M and set $M' = M/xM$. Then*

$$\deg \chi^{M'}_{\mathfrak{q}} \le \deg \chi^M_{\mathfrak{q}} - 1.$$

Proof. Set $N = xM$ and $N_n = N \cap \mathfrak{q}^n M$. By Artin–Rees, this is a stable $\mathfrak{q}$-filtration on N. For each $n \geq 0$, we have a short exact sequence

$$0 \to N/N_n \to M/\mathfrak{q}^n M \to M'/\mathfrak{q}^n M' \to 0.$$

In particular, for all n, we have

$$\chi_{\mathfrak{q}}^{M'}(n) = \chi_{\mathfrak{q}}^{M}(n) - \ell(N/N_n).$$

The map $M \to N$ given by $m \mapsto xm$ is an isomorphism since x is a nonzerodivisor, and so for large n, $\chi_{\mathfrak{q}}^{N}(n)$ agrees with a polynomial that has the same leading coefficient and degree as $\chi_{\mathfrak{q}}^{M}(n)$ by Proposition 5.3.1, and hence the result holds. □

6. Dimension theory

6.1. **Definition of dimension.** Let A be a noetherian local ring with maximal ideal $\mathfrak{m}$. We consider the following 3 quantities.

(1) Let $\delta(A)$ be the least number of generators amongst any $\mathfrak{m}$-primary ideal of A.

(2) Recall that $\mathrm{gr}_{\mathfrak{m}}(A)$ is a noetherian $\mathbf{Z}_{\geq 0}$-graded ring with $(\mathrm{gr}_{\mathfrak{m}} A)_0 = A/\mathfrak{m}$ a field (denote it $\mathbf{k}$) and that it is generated as a $\mathbf{k}$-algebra by degree 1 elements. Letting $\lambda = \dim$, its Hilbert series is a rational function of the form

$$\mathrm{H}_{\mathrm{gr}_{\mathfrak{m}}(A)}(t) = \frac{h(t)}{(1-t)^r}$$

if $\mathfrak{m}$ can be generated by r elements. We let $d(A)$ be the order of the pole at $t = 1$ of this rational function; concretely, this is just r minus the multiplicity of 1 as a root of $h(t)$. Equivalently,

$$d(A) = \deg \chi_{\mathfrak{m}}(x).$$

(3) Let $\dim A$ be the supremum of the length of any strictly increasing chain of prime ideals in A:

$$\dim A = \sup\{d \mid \mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_d \subset A\}$$

Our main goal is to show that all 3 quantities coincide. They will simply be called the **(Krull) dimension** of A.

Proposition 6.1.1. *$\delta(A) \geq d(A)$.*

Proof. Let $s = \delta(A)$. Then there exists an $\mathfrak{m}$-primary ideal $\mathfrak{q}$ which can be generated by s elements. By Proposition 5.3.1, $\deg \chi_{\mathfrak{q}}(x) \leq s$ and by Proposition 5.3.2, we also know that $\deg \chi_{\mathfrak{m}}(x) \leq s$. Finally, $d(A) = \deg \chi_{\mathfrak{m}}(x)$. □

Proposition 6.1.2. *$d(A) \geq \dim A$.*

Proof. We prove this by induction on $d(A)$. If $d(A) = 0$, then $\chi_{\mathfrak{m}}(x)$ is a constant and hence $\ell(A/\mathfrak{m}^n)$ is constant for $n \gg 0$. Choosing n large enough to hit this constant value, this implies that $\mathfrak{m}^n = \mathfrak{m}^{n+1}$, and hence that $\mathfrak{m}^n = 0$ by Nakayama's lemma. If $\mathfrak{p}$ is any prime ideal of A, then $\mathfrak{m}^n \subseteq \mathfrak{p}$ implies that $\mathfrak{m} \subseteq \mathfrak{p}$ by taking radicals, and hence $\mathfrak{m} = \mathfrak{p}$. In particular, there are no nontrivial inclusions of prime ideals so $\dim A = 0$.

Now suppose that $d(A) > 0$. Let $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ be any strictly increasing chain of prime ideals in A. We need to show that $d(A) \geq r$. Set $A' = A/\mathfrak{p}_0$, which is a local domain, and let $\mathfrak{m}'$ be its maximal ideal. Let $\mathfrak{p}_i'$ be the image of $\mathfrak{p}_i$ in A'. Pick any nonzero element x of $\mathfrak{p}_1'$. In particular, x is a nonzerodivisor, so by Proposition 5.3.3 with $M = A'$, we have

$$d(A'/x) \leq d(A') - 1.$$

Furthermore, for all n, we have a surjection $A/\mathfrak{m}^n \to A'/(\mathfrak{m}')^n$, so $\ell(A/\mathfrak{m}^n) \geq \ell(A'/(\mathfrak{m}')^n)$, which implies that $d(A) \geq d(A')$. So by induction, any strictly increasing chain of prime ideals in A'/x has length at most $d(A'/x)$, and in particular, has length at most $d(A) - 1$.

Next, we claim that $\mathfrak{p}_i'/x$ is a proper subset of $\mathfrak{p}_{i+1}'/x$. If not, then any element of $\mathfrak{p}_{i+1}'$ is a linear combination of x and an element of $\mathfrak{p}_i'$, and hence $\mathfrak{p}_{i+1}' = \mathfrak{p}_i'$, which is false. Finally, this means we have a strictly increasing chain of prime ideals of length $r-1$

$$\mathfrak{p}_1'/x \subsetneqq \cdots \subsetneqq \mathfrak{p}_{r-1}'/x$$

in A'/x, and so $r - 1 \leq d(A) - 1$, so we are done. □

Since $d(A)$ is by definition a finite quantity, the last result tells us that in any noetherian local ring, there is an upper bound on the length of any strictly increasing chain of prime ideals. Given a prime ideal $\mathfrak{p}$ in any ring A, define its **height**, denote $\operatorname{height}(\mathfrak{p})$, to be the maximum length of a strictly increasing chain of prime ideals contained in $\mathfrak{p}$ ($\mathfrak{p}$ is allowed to be in the chain). By Proposition 2.4.2, we have

$$\operatorname{height}(\mathfrak{p}) = \dim A_{\mathfrak{p}},$$

so if A is noetherian, then this quantity is always finite.

Proposition 6.1.3. $\dim A \geq \delta(A)$.

Proof. Let $d = \dim A$. It suffices to construct an ideal of the form $(x_1, \dots, x_d)$ in A which is $\mathfrak{m}$-primary.

We will prove the following statement by induction on i: if $i \leq d$, then there exists a sequence $x_1, \dots, x_i$ of elements of A such that every prime ideal containing $(x_1, \dots, x_i)$ has height $\geq i$. The base case is $i = 0$ which is vacuous: we are just saying that every prime ideal has non-negative height.

Otherwise, suppose that $0 < i \leq d$ and that $x_1, \dots, x_{i-1}$ has already been constructed so that every prime ideal containing $(x_1, \dots, x_{i-1})$ has height $\geq i - 1$. Since A is noetherian, $(x_1, \dots, x_{i-1})$ has finitely many minimal primes (Proposition 4.2.3), let $\{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}$ be the set of those minimal primes that have height exactly $i - 1$ (we are not saying that s is positive, though we will see later this is the case). Since $i - 1 < d$ and $\operatorname{height}(\mathfrak{m}) = d$, we see that $\mathfrak{m} \neq \mathfrak{p}_j$ for all j. By prime avoidance, we know that $\mathfrak{m} \setminus (\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_s)$ is non-empty, so let x_i be an element in this set.

Let $\mathfrak{q}$ be a prime containing $(x_1, \dots, x_i)$. We need to show that $\operatorname{height}(\mathfrak{q}) \geq i$. In particular, $\mathfrak{q}$ contains $(x_1, \dots, x_{i-1})$ and hence contains some prime $\mathfrak{p}$ which is a minimal prime containing $(x_1, \dots, x_{i-1})$. If $\mathfrak{p} \in \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}$, then $\operatorname{height}(\mathfrak{p}) = i - 1$ and $\mathfrak{q} \neq \mathfrak{p}$ since $x_i \notin \mathfrak{p}$, and so $\operatorname{height}(\mathfrak{q}) \geq i$. Otherwise, $\operatorname{height}(\mathfrak{p}) \geq i$ by definition of the $\mathfrak{p}_j$, so we have $\operatorname{height}(\mathfrak{q}) \geq \operatorname{height}(\mathfrak{p}) \geq i$. This finishes the proof of our induction.

Finally, we need to show that $(x_1, \dots, x_d)$, as just constructed, is $\mathfrak{m}$-primary. Let $\mathfrak{p}$ be a prime ideal containing $(x_1, \dots, x_d)$. Then $\operatorname{height}(\mathfrak{p}) \geq d$, and hence $\mathfrak{p} = \mathfrak{m}$ since this is the only ideal of A of height d (being the unique maximal ideal). Finally, the radical of $(x_1, \dots, x_d)$ is the intersection of the prime ideals containing it, and hence it must be $\mathfrak{m}$, so $(x_1, \dots, x_d)$ is $\mathfrak{m}$-primary. □

Theorem 6.1.4. *For any noetherian local ring A, we have*

$$d(A) = \delta(A) = \dim(A).$$

If $d = \dim A$, then any set of elements $x_1, \dots, x_d \in A$ that generates an $\mathfrak{m}$-primary ideal is called a **system of parameters**.

Theorem 6.1.5 (Krull principal ideal theorem)**.** *Let A be a noetherian ring and $x_1, \dots, x_r \in A$. If $\mathfrak{p}$ a prime ideal which is minimal amongst those containing $(x_1, \dots, x_r)$, then* $\mathrm{height}(\mathfrak{p}) \le r$.

Proof. Consider the local ring $A_\mathfrak{p}$ and the ideal generated by the images of $x_1, \dots, x_r$ there. Since the image of $\mathfrak{p}$ is a minimal prime over $(x_1, \dots, x_r)$ and also the maximal ideal of $A_\mathfrak{p}$, the radical of $(x_1, \dots, x_r)$ is $\mathfrak{p}A_\mathfrak{p}$ and hence it is a $\mathfrak{p}A_\mathfrak{p}$-primary ideal. In particular, $r \ge \dim A_\mathfrak{p} = \mathrm{height}(\mathfrak{p})$. □

Remark 6.1.6. Here is a geometric intuition (we won't make this precise but it might help to keep this in mind): $\dim(A)$ is to be thought of as the dimension of the space $\operatorname{Spec} A$. We can think of $x_1, \dots, x_r$ as functions on this space and minimal primes $\mathfrak{p}$ correspond to irreducible components of the solution set of where these functions all take value 0. In that case, $\mathrm{height}(\mathfrak{p})$ can be thought of as the codimension of this component, so Krull's result tells us that the dimension of a solution set cannot drop more than the number of equations used to define it. While this may seem like something that should be true, we have to remember that our definition of dimension is quite abstract and this holds in a high level of generality. This is easiest to make sense of when A is the coordinate ring of an algebraic variety over an algebraically closed field. □

Corollary 6.1.7. *If A is a noetherian local ring and $x \in \mathfrak{m}$ is a nonzerodivisor, then* $\dim(A/x) = \dim A - 1$.

Proof. Let $d = \dim(A/x)$. It follows from Proposition 5.3.3 with $M = A$ that $d \le \dim A - 1$. Next, pick $x_1, \dots, x_d \in A$ so that their images in A/x are a system of parameters. If $\mathfrak{p}$ is any prime of A containing $(x, x_1, \dots, x_d)$, then $\mathfrak{p}/x = \mathfrak{m}/x$ and hence $\mathfrak{p} = \mathfrak{m}$ since $\mathfrak{p}$ is the inverse image of $\mathfrak{p}/x$. This shows that $(x, x_1, \dots, x_d)$ is $\mathfrak{m}$-primary and so $d + 1 \ge \dim A$, which shows that $\dim A = d + 1$. □

Finally, we can give a general definition of (Krull) dimension using the third definition above. Let A be any ring. Then its **dimension** is the length of the longest strictly increasing chain of prime ideals in A:

$$\dim A = \sup\{d \mid \text{there exists } \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_d\}.$$

It follows that

$$\dim A = \sup\{\dim A_\mathfrak{p} \mid \mathfrak{p} \in \operatorname{Spec} A\},$$

and in fact we only need to check localizations at maximal ideals. In full generality, dimension can behave in strange ways. Even if A is noetherian, it need not be finite (see exercises).

6.2. **Noether normalization.**

Lemma 6.2.1. *If $F(x_1, \dots, x_n)$ is a nonzero homogeneous polynomial over an infinite field $\mathbf{k}$, then there exists nonzero $\lambda_1, \dots, \lambda_n \in \mathbf{k}$ such that $F(\lambda_1, \dots, \lambda_n) \neq 0$.*

Proof. We prove this by induction on n. If $n = 1$, then $F(x_1) = x_1^d$ for some d and any nonzero λ_1 works. Otherwise, we think of F as a polynomial in x_n whose coefficients are homogeneous polynomials in $x_1, \dots, x_{n-1}$:

$$F(x_1, \dots, x_n) = \sum_{i=0}^{d} F_i(x_1, \dots, x_{n-1}) x_n^i.$$

At least one of the F_i is nonzero; pick one and use induction to find nonzero $\lambda_1, \dots, \lambda_{n-1} \in \mathbf{k}$ such that the substitution into that F_i is nonzero. Then $F(\lambda_1, \dots, \lambda_{n-1}, x_n)$ is a polynomial in x_n which is not identically 0. A polynomial in 1 variable only has finitely many roots, so since $\mathbf{k}$ is infinite, we can pick λ_n to be any nonzero element of $\mathbf{k}$ which is not a root of the resulting polynomial. □

Theorem 6.2.2 (Noether normalization)**.** *Let* $\mathbf{k}$ *be an infinite field and* A *a finitely generated* $\mathbf{k}$*-algebra. There exists a subring* $B \subset A$ *such that* A *is integral over* B *and* B *is isomorphic to a polynomial ring over* $\mathbf{k}$*.*

Proof. We prove this by induction on the number of generators of A. The base case is when A is generated by 0 elements, i.e., $A = \mathbf{k}$, but then there is nothing to prove.

So suppose that A is generated by n elements $x_1, \dots, x_n$ and suppose the result holds for all $\mathbf{k}$-algebras which can be generated by $n-1$ elements. If $x_1, \dots, x_n$ are algebraically independent over $\mathbf{k}$, we can take $B = A$. Otherwise, we may reorder the generators so that $x_1, \dots, x_i$ are algebraically independent over $\mathbf{k}$ and $x_{i+1}, \dots, x_n$ are algebraic over $\mathrm{Frac}(\mathbf{k}[x_1, \dots, x_i])$. In particular, since we are assuming $i < n$, x_n is algebraic over $\mathrm{Frac}(\mathbf{k}[x_1, \dots, x_i])$, so there is a polynomial f in n variables with coefficients in $\mathbf{k}$ so that $f(x_1, \dots, x_n) = 0$. Let F be the sum of the highest degree terms in f, so that F is homogeneous, say of degree d. Since $\mathbf{k}$ is infinite, there exist $\lambda_1, \dots, \lambda_{n-1} \in \mathbf{k}$ so that $F(\lambda_1, \dots, \lambda_{n-1}, 1) \neq 0$ (use Lemma 6.2.1; since F is homogeneous we can scale all of the λ_i by the same amount to assume that the last one is 1). Set $x_i' = x_i - \lambda_i x_n$ for $i = 1, \dots, n-1$ and $A' = \mathbf{k}[x_1', \dots, x_{n-1}']$.

If we do the substitution $x_i \mapsto x_i' + \lambda_i x_n$ for $i = 1, \dots, n-1$ into $f(x_1, \dots, x_n)$, and think of this as a polynomial in x_n, the coefficient of x_n^d (the highest degree possible) is $F(\lambda_1, \dots, \lambda_{n-1}, 1)$, an element of $\mathbf{k}$, which is nonzero by construction. Hence the monic polynomial (in the variable t)

$$\frac{1}{F(\lambda_1, \dots, \lambda_{n-1}, 1)} f(x_1' + \lambda_1 t, \dots, x_{n-1}' + \lambda_{n-1} t, t)$$

has coefficients in A' and x_n is a solution to it, so x_n is integral over A'.

By induction, there is a subring B of A' such that A' is integral over B and B is isomorphic to a polynomial ring over $\mathbf{k}$. By transitivity of integrality (Corollary 3.2.1), A is also integral over B. □

Remark 6.2.3. A consequence of the proof is that if $x_1, \dots, x_n$ are $\mathbf{k}$-algebra generators for A, then we can always take B to be generated by some $\mathbf{k}$-linear combinations of the x_i. In fact, any “generic” choice of linear combinations will work since we really only need that some finite set of polynomial expressions (by invoking Lemma 6.2.1) are nonzero. The only question is how many generators B has, and we will see in the next section that it is $\dim A$. □

For a stronger version, see [Ei, Theorem 13.3].

6.3. **Transcendental dimension.** In classical algebraic geometry, we have a correspondence between (irreducible) algebraic varieties over an algebraically closed field $\mathbf{k}$ and finitely generated $\mathbf{k}$-algebras which are integral domains. In this case, there is yet another way to compute the dimension of this algebra which is more closely connected with the geometry of the variety.

First, we prove a result to motivate the relationship between dimension and algebraic independence.

Proposition 6.3.1. *Let $(A, \mathfrak{m})$ be a d-dimensional noetherian local ring and let $\mathfrak{q} = (x_1, \dots, x_d)$ be an $\mathfrak{m}$-primary ideal which is generated by a system of parameters. Let $f \in A[t_1, \dots, t_d]$ be a homogeneous degree s polynomial such that*

$$f(x_1, \dots, x_d) \in \mathfrak{q}^{s+1}.$$

Let $\overline{f}$ be the reduction of f modulo $\mathfrak{q}$. Then $\overline{f}$ is a zerodivisor in $(A/\mathfrak{q})[t_1, \dots, t_d]$.[3]

Proof. Define a homomorphism of $A/\mathfrak{q}$-algebras

$$\alpha \colon (A/\mathfrak{q})[t_1, \dots, t_d] \to \mathrm{gr}_{\mathfrak{q}}(A)$$

by letting $\alpha(t_i)$ be the image of x_i in $\mathfrak{q}/\mathfrak{q}^2$. Since f is homogeneous of degree s, we see that $\alpha(\overline{f})$ maps to $\mathfrak{q}^s/\mathfrak{q}^{s+1}$ and hence is 0 by our assumption. Since $\mathfrak{q}$ is generated by $x_1, \dots, x_d$, α is surjective, and so for all n, we have

$$\ell(\mathrm{gr}_{\mathfrak{q}}(A)_n) \le \ell(((A/\mathfrak{q})[t_1, \dots, t_d]/(\overline{f}))_n).$$

As functions of n (and considering $n \gg 0$), both sides are given by polynomial functions in n, and the degree of the polynomial for the left expression is $d-1$ (by definition). If $\overline{f}$ is a nonzerodivisor, then the degree of the right expression would be $d-2$ since we would have a short exact sequence (and $n \mapsto \ell(((A/\mathfrak{q})[t_1, \dots, t_d])_n)$ has degree $d-1$ by Example 5.1.6)

$$0 \to (A/\mathfrak{q})[t_1, \dots, t_d]_{n-s} \xrightarrow{\cdot \overline{f}} (A/\mathfrak{q})[t_1, \dots, t_d]_n \to ((A/\mathfrak{q})[t_1, \dots, t_n]/(f'))_n \to 0$$

with the first map being multiplication by $\overline{f}$. This would be a contradiction, and hence $\overline{f}$ is a zerodivisor. □

Corollary 6.3.2. *Let $(A, \mathfrak{m})$ be a d-dimensional noetherian local ring which contains a field $\mathbf{k}$. Then any system of parameters $x_1, \dots, x_d$ is algebraically independent over $\mathbf{k}$.*

Proof. Suppose $x_1, \dots, x_d$ is algebraically dependent. Then there exists a nonzero polynomial $f(t_1, \dots, t_d)$ with coefficients in $\mathbf{k}$ such that $f(x_1, \dots, x_d) = 0$. In particular, let s be the smallest degree of a monomial appearing in f with nonzero coefficient and let f_s be the sum of all such monomials together with their coefficients. Then $f = f_s + g$ where g has all monomials of degree $\ge s+1$, and so $g(x_1, \dots, x_d) \in (x_1, \dots, x_d)^{s+1}$, which means that $f_s(x_1, \dots, x_d) \in (x_1, \dots, x_d)^{s+1}$. Now by Proposition 6.3.1, the reduction of f_s modulo $(x_1, \dots, x_d)$ is a zerodivisor. However, the composition $\mathbf{k} \to A \to A/(x_1, \dots, x_d)$ is injective (since $\mathbf{k}$ is a field), and any polynomial whose nonzero coefficients are units cannot be a zerodivisor. □

[3] Atiyah–Macdonald instead conclude that the coefficients of f belong to $\mathfrak{m}$, though this relies on an exercise which does not seem to have a short proof. This formulation suffices for what we want to do and skips the need for this exercise.

Now suppose that A is a finitely generated $\mathbf{k}$-algebra which is an integral domain. The result above shows that for any maximal ideal $\mathfrak{m}$ of A, if $d = \dim A_{\mathfrak{m}}$, then we can find $f_1, \dots, f_d \in A_m$ which are algebraically independent over $\mathbf{k}$. We may think of $f_1, \dots, f_d$ as elements in $\operatorname{Frac}(A)$, and since $\dim A = \sup\{\dim A_{\mathfrak{m}}\}$, we see that $\dim A$ is a lower bound for the size of the largest set of algebraically independent elements of $\operatorname{Frac}(A)$ over $\mathbf{k}$.

The fraction field $\operatorname{Frac}(A)$ of A is finitely generated over $\mathbf{k}$ and hence has finite transcendence degree, which is the size of any maximal set of algebraically independent elements (implicit in this definition is the fact, which we don't prove here, that all such sets have the same size much like all bases of a vector space have the same size).

Theorem 6.3.3. *Let $\mathbf{k}$ be an algebraically closed field and let A be a finitely generated $\mathbf{k}$-algebra which is an integral domain. Then $\dim A$ agrees with the transcendence degree of $\operatorname{Frac}(A)$ over $\mathbf{k}$. Furthermore, $\dim A = \dim A_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$ of A.*

Proof. First we handle the case when $A \cong \mathbf{k}[x_1, \dots, x_d]$ is a polynomial ring in d variables. Then $\operatorname{Frac}(A)$ is the function field in d variables and hence has transcendence degree d (the set $x_1, \dots, x_d$ is maximal with respect to being algebraically independent). Next, $\dim A = \sup_{\mathfrak{m}} \dim A_{\mathfrak{m}}$ over all maximal ideals $\mathfrak{m}$. We know from the Hilbert nullstellensatz (Theorem 4.4.2) that there exist $\alpha_1, \dots, \alpha_d \in \mathbf{k}$ such that $\mathfrak{m} = (x_1 - \alpha_1, \dots, x_d - \alpha_d)$, and hence we can apply the $\mathbf{k}$-algebra automorphism $x_i \mapsto x_i + \alpha_i$ to see that $\dim A_{\mathfrak{m}} = \dim A_{(x_1,\dots,x_d)}$ for all $\mathfrak{m}$. In that case, $\operatorname{gr}_{(x_1,\dots,x_d)} A_{(x_1,\dots,x_d)} \cong A$ and from Example 5.1.6, $\dim A_{(x_1,\dots,x_d)} = d$, so the result holds in this case.

Now we consider the general case. By Noether normalization (Theorem 6.2.2), there exists a subring $B \subset A$ such that $B \cong \mathbf{k}[x_1, \dots, x_d]$ is isomorphic to a polynomial ring in d variables and $B \subset A$ is an integral extension. In particular, $\dim B = d$. In addition, $\operatorname{Frac}(A)$ is algebraic over $\operatorname{Frac}(B)$, so they have the same transcendence degree over $\mathbf{k}$.

Let $\mathfrak{m}$ be a maximal ideal of A. Then $\mathfrak{n} = B \cap \mathfrak{m}$ is a maximal ideal in B by Corollary 3.3.2. If $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ is any strictly increasing chain of prime ideals in $A_{\mathfrak{m}}$, then $\mathfrak{p}_0 \cap B_{\mathfrak{n}} \subsetneqq \cdots \subsetneqq \mathfrak{p}_r \cap B_{\mathfrak{n}}$ is also strictly increasing by "incomparability" (Theorem 3.3.3). So $\dim A_{\mathfrak{m}} \le \dim B_{\mathfrak{n}} = d$. On the other hand, any strictly increasing chain of primes in $B_{\mathfrak{n}}$ is obtained by intersecting a strictly increasing chain of primes in $A_{\mathfrak{m}}$ by the going-down theorem (Theorem 3.3.8), which applies since B (and hence $B_{\mathfrak{n}}$) is normal (since B is a UFD, see Proposition 3.2.4). In particular, $\dim B_{\mathfrak{n}} \le \dim A_{\mathfrak{m}}$, so we have equality. □

6.4. Regular local rings.

If A is the ring of regular functions on a variety over an algebraically closed field $\mathbf{k}$, then by the Hilbert nullstellensatz, the maximal ideals correspond to the points of the variety and the localization $A_{\mathfrak{m}}$ with respect to a maximal ideal captures some of the local geometry of the variety at this point. We'll give some basic terminology which is more general and especially useful in this context and leave the dictionary to later courses.

So let A be a noetherian local ring with maximal ideal $\mathfrak{m}$. Let $\mathbf{k} = A/\mathfrak{m}$ be its residue field. The **(Zariski) cotangent space** is the $\mathbf{k}$-vector space $\mathfrak{m}/\mathfrak{m}^2$. As we have seen,

$$\dim_{\mathbf{k}}(\mathfrak{m}/\mathfrak{m}^2) \ge \dim A$$

(for example, use that $\dim A$ is the minimal number of generators of any $\mathfrak{m}$-primary ideal and $\dim_{\mathbf{k}}(\mathfrak{m}/\mathfrak{m}^2)$ is the minimal number of generators of $\mathfrak{m}$). When the two quantities are equal, we say that A is a **regular local ring**. A general noetherian ring is **regular** if $A_{\mathfrak{p}}$ is a regular local ring for all prime ideals $\mathfrak{p} \in \operatorname{Spec}(A)$.

Remark 6.4.1. There is a potential mismatch in the definitions: is a regular local ring considered regular by the second definition? i.e., if A is a regular local ring, then is $A_{\mathfrak{p}}$ also a regular local ring for any $\mathfrak{p} \in \operatorname{Spec}(A)$? This turns out to be true but we will not discuss its proof. In complete generality, this is best approached using homological algebra (see [Ei, Corollary 19.14]). □

Intuitively, the dual space of $\mathfrak{m}/\mathfrak{m}^2$ should be thought of as the space of tangent vectors at the point corresponding to $\mathfrak{m}$. Here's a rough sketch of this intuition. In calculus, a tangent vector to a smooth manifold X at a point $x \in X$ is obtained by taking the derivative of a smooth function $\gamma\colon [0,1] \to X$ such that $\gamma(0) = x$, where $[0,1]$ is the unit interval. While we don't have a unit interval in our language, we can instead think of this as the linear part of the Taylor series expansion of γ (second-order and higher pieces don't matter for the first derivative and the constant term is determined by $\gamma(0) = x$). This linear part is the role played by the (dual of) $\mathfrak{m}/\mathfrak{m}^2$ if $\mathfrak{m}$ corresponds to the point of $\operatorname{Spec}(A)$ that we're interested in.

Having "too many" tangent directions is related to the idea of a space being singular at that point.

Example 6.4.2. We'll consider the case of a complex plane curve, i.e., a ring of the form $\mathbf{C}[x,y]/(f)$ where $f \neq 0$ and $\mathbf{C}$ is the field of complex numbers (the curve is the solution set to $f(x,y) = 0$). Since f is a nonzerodivisor, we will have $\dim \mathbf{C}[x,y]/(f) = 1$.

(1) First consider the case of a parabola $f = x^2 - y$ and let $\mathfrak{m} = (x,y)$ be the maximal ideal corresponding to the point $x = 0, y = 0$. Working in $(\mathbf{C}[x,y]/(f))_{\mathfrak{m}}$, we have $\mathfrak{m}^2 = (x^2, xy, y^2)$ which contains the ideal (y) since $x^2 = y$. Hence $\mathfrak{m}/\mathfrak{m}^2$ is spanned by x, and we already know $\dim_{\mathbf{k}} \mathfrak{m}/\mathfrak{m}^2 \geq 1$, so $\{x\}$ is actually a basis, i.e., $x \notin \mathfrak{m}^2$. This matches with the geometric intuition that the parabola is smooth at the point $(0,0)$.

(2) Now consider a cuspidal curve $f = x^3 - y^2$ and again take $\mathfrak{m} = (x,y)$ corresponding to the point $(0,0)$). In this case, no linear combination of x, y belongs to $\mathfrak{m}^2 = (x^2, xy, y^2)$ since no multiple of f contains linear terms (and hence there are no nontrivial ways to rewrite them). Hence $\dim_{\mathbf{k}} \mathfrak{m}/\mathfrak{m}^2 = 2$ in this case which matches the idea that a cusp is not smooth. □

Proposition 6.4.3. *Let A be a d-dimensional noetherian local ring with maximal ideal $\mathfrak{m}$ and residue field $\mathbf{k} = A/\mathfrak{m}$. The following are equivalent:*

(1) A is a regular local ring, i.e., $\dim_{\mathbf{k}}(\mathfrak{m}/\mathfrak{m}^2) = d$.

(2) $\mathfrak{m}$ can be generated by d elements, i.e., a system of parameters.

(3) We have an isomorphism of graded rings $\operatorname{gr}_{\mathfrak{m}}(A) \cong \mathbf{k}[x_1, \dots, x_d]$, where the right side is a polynomial ring in d variables.

Proof. Any lift of a basis for $\mathfrak{m}/\mathfrak{m}^2$ to elements of $\mathfrak{m}$ give generators for $\mathfrak{m}$, so (1) implies (2).

Now assume (2) holds and let $a_1, \dots, a_d \in \mathfrak{m}$ be generators. Define a surjective ring homomorphism

$$\alpha\colon \mathbf{k}[x_1, \dots, x_d] \to \operatorname{gr}_{\mathfrak{m}}(A), \qquad \alpha(f(x_1, \dots, x_d)) = f(a_1, \dots, a_d).$$

This is a map of graded rings in fact, so if $f \in \ker \alpha$, then each homogeneous component of f is also in $\ker \alpha$. By Proposition 6.3.1, given a homogeneous polynomial in $\ker \alpha$, it must be a zerodivisor, but $\mathbf{k}[x_1, \dots, x_d]$ is a domain, and so $\ker \alpha = 0$ and (3) holds.

Finally, (3) implies (1) since $\mathfrak{m}/\mathfrak{m}^2$ corresponds to the vector space spanned by $x_1, \dots, x_d$ under any isomorphism of graded rings between $\mathrm{gr}_{\mathfrak{m}}(A)$ and $\mathbf{k}[x_1, \dots, x_d]$ by considering the degree 1 components. □

Corollary 6.4.4. *A regular local ring is an integral domain.*

Proof. Let A be a regular local ring with maximal ideal $\mathfrak{m}$. Pick nonzero $x, y \in A$. There exist integers r, s such that $x \in \mathfrak{m}^r \setminus \mathfrak{m}^{r+1}$ and $y \in \mathfrak{m}^s \setminus \mathfrak{m}^{s+1}$ since $\bigcap_n \mathfrak{m}^n = 0$ by Nakayama's lemma (because $\mathfrak{m} \bigcap_n \mathfrak{m}^n = \bigcap_n \mathfrak{m}^n$). Then the images of x and y in $\mathrm{gr}_{\mathfrak{m}}(A)_r$ and $\mathrm{gr}_{\mathfrak{m}}(A)_s$ are nonzero. Since $\mathrm{gr}_{\mathfrak{m}}(A) \cong \mathbf{k}[x_1, \dots, x_d]$, the product of their images is nonzero, and hence $xy \neq 0$. □

Remark 6.4.5. More can be shown, for example, every regular local ring is a unique factorization domain (see [Ei, Theorem 19.19]). □

By definition, an artinian local ring (i.e., a local ring of dimension 0) is regular if and only if $\mathfrak{m} = \mathfrak{m}^2$, which means that $\mathfrak{m} = 0$ by Nakayama's lemma. So regular local rings of dimension 0 are the same thing as fields. By Theorem 4.6.6, a general dimension 0 ring is regular if and only if it is isomorphic to a product of fields. We will discuss the dimension 1 case in §8.3.

7. Completions

7.1. **Inverse limits.**

Let $G_0, G_1, \dots$ be a sequence of abelian groups together with group homomorphisms $\theta_n \colon G_n \to G_{n-1}$ for $n \geq 1$. We call this data an **inverse system** and denote it (G_i, θ_i) or just $\{G_i\}$. The **inverse limit** of an inverse system is defined by

$$\varprojlim_i G_i = \{(g_0, g_1, \dots) \in \prod_i G_i \mid \theta_i(g_i) = g_{i-1} \text{ for all } i \geq 1\}.$$

This is a subgroup of $\prod_i G_i$. When the G_i are rings and the θ_i are ring homomorphisms, then $\varprojlim_i G_i$ is a subring.

Given two inverse systems (A_i, θ_i) and (A'_i, θ'_i) of the same kind of object (groups, rings, etc.), a **morphism** $f \colon A \to A'$ between them is a sequence of homomorphisms $f_i \colon A_i \to A'_i$ (depending on what kind of objects the A_i are) such that the following square commutes for all i:

$$\begin{tikzcd} A_i \arrow[r, "f_i"] \arrow[d, "\theta_i"'] & A'_i \arrow[d, "\theta'_i"] \\ A_{i-1} \arrow[r, "f_{i-1}"] & A'_{i-1} \end{tikzcd}$$

(Hence inverse systems form a category.) The morphism is injective or surjective if all of the f_i are injective, or surjective, respectively, and a sequence of morphisms $\{A_i\} \to \{B_i\} \to \{C_i\}$ is exact if this is true for $A_i \to B_i \to C_i$ for all i. Finally, an inverse system (A_i, θ_i) is **surjective** if θ_i is surjective for all i (this is used for the next result and can be relaxed quite a bit, see exercises).

Proposition 7.1.1. *Let*

$$0 \to \{A_i\} \to \{B_i\} \to \{C_i\} \to 0$$

be a short exact sequence of inverse systems of abelian groups. Then the corresponding sequence

$$0 \to \varprojlim A_i \to \varprojlim B_i \to \varprojlim C_i$$

is exact. Furthermore, if $\{A_i\}$ is a surjective system, then we have a short exact sequence

$$0 \to \varprojlim A_i \to \varprojlim B_i \to \varprojlim C_i \to 0.$$

Proof. On the direct product $A = \prod_i A_i$, define $d^A \colon A \to A$ by

$$d^A((a_i)_i) = (a_i - \theta_{i+1}(a_{i+1}))_i.$$

By definition, $\varprojlim A_i = \ker d^A$. Similarly, define B and C and d^B and d^C. The short exact sequence of inverse systems gives a short exact sequence on direct products $0 \to A \to B \to C \to 0$, and in particular, we have a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, "d^A"] & B \arrow[r] \arrow[d, "d^B"] & C \arrow[r] \arrow[d, "d^C"] & 0 . \\
0 \arrow[r] & A \arrow[r] & B \arrow[r] & C \arrow[r] & 0
\end{tikzcd}$$

By the snake lemma (Lemma 1.3.1) we get an exact sequence

$$0 \to \varprojlim A_i \to \varprojlim B_i \to \varprojlim C_i \to \operatorname{coker} d^A \to \operatorname{coker} d^B \to \operatorname{coker} d^C \to 0$$

which proves the first point. We claim that if $\{A_i\}$ is a surjective system, then d^A is surjective: given $(a_i)_i \in A$, we need to find $\alpha_i \in A_i$ so that $\alpha_i - \theta_{i+1}(\alpha_{i+1}) = a_i$ for all i. We do this by induction on i: first set $\alpha_0 = 0$. Next, assuming we have chosen $\alpha_0, \dots, \alpha_n$ so that $\alpha_i - \theta_{i+1}(\alpha_{i+1}) = a_i$ for $i = 1, \dots, n-1$, we let $\alpha_{n+1} \in A_{n+1}$ be any element that maps to $\alpha_n - a_n$ under θ_{n+1}, which is possible since θ_{n+1} is surjective. This proves the claim and hence $\operatorname{coker} d^A = 0$ in this case and we have proven the second point. □

Here is an important example of a surjective inverse system. Let Γ be an abelian group with a decreasing sequence of subgroups

$$\Gamma = \Gamma_0 \supseteq \Gamma_1 \supseteq \cdots .$$

Then we set $G_i = \Gamma/\Gamma_i$ and let $\theta_{i+1} \colon \Gamma/\Gamma_{i+1} \to \Gamma/\Gamma_i$ be the natural quotient map. We will usually denote $\varprojlim_i \Gamma/\Gamma_i$ by $\hat{\Gamma}$ if the choice of the subgroups is understood from context (different choices can give different inverse limits of course). Note that there is a natural homomorphism

$$\Gamma \to \hat{\Gamma}, \qquad g \mapsto (g + \Gamma_i)_i$$

which sends g to the sequence represented by the cosets of g modulo the subgroups Γ_i.

Similarly, if Γ is a ring with a decreasing sequence of ideals, we can define the inverse limit ring with $G_i = \Gamma/\Gamma_i$ and the result is a ring.

Example 7.1.2. Let $\mathbf{k}$ be any ring, and let $\Gamma = \mathbf{k}[x]$ be the polynomial ring in 1 variable. Set $\Gamma_i = (x^i)$. Then the inverse limit of Γ/Γ_i is isomorphic to the power series ring $\mathbf{k}[\![x]\!]$: a power series $f(x) = \sum_{i \geq 0} a_i x^i$ corresponds to the sequence of coset representatives

$$(a_0 + a_1 x + \cdots + a_{i-1}x^{i-1} \pmod{x^i}). \qquad \square$$

The image of Γ is the set of formal power series with $a_i = 0$ for $i \gg 0$, which is the usual way of identifying polynomials as formal power series.

Example 7.1.3. Let $\Gamma = \mathbf{Z}$ and pick a prime p. If we let $\Gamma_i = (p^i)$, then the inverse limit is the ring of p-adic integers, denoted $\mathbf{Z}_p$. By definition, we can represent elements of $\mathbf{Z}_p$ by sequences $(a_0, a_1, a_2, \dots)$ where $a_i \in \mathbf{Z}/p^i$ and $a_i \equiv a_{i+1} \pmod{p^i}$. Using the standard convention that representatives of cosets of $\mathbf{Z}/n$ are chosen from $\{0, 1, \dots, n-1\}$, we see that there exist integers $b_0, b_1, \dots$ with $0 \le b_i \le p-1$ such that the representative for a_i is $b_0 + pb_1 + \cdots + p^{i-1}b_{i-1}$. In this way, we can think of p-adic integers as infinite sums

$$\sum_{i \ge 0} b_i p^i$$

where $0 \le b_i \le p-1$, similar to formal power series. However, addition is not the same as for formal power series, rather we have to perform "carrying". In other words, given another p-adic integer $\sum_{i \ge 0} b'_i p^i$, if $b_0 + b'_0 \le p-1$, then we add those components as usual and move on, otherwise the 0th term of the sum is $b_0 + b'_0 - p$ and we have to consider whether the next term $b_1 + b'_1 + 1$ is $\le p-1$ or not, etc. This leads to some strange expressions. For example, -1 is represented by the infinite series

$$\sum_{i \ge 0} (p-1)p^i$$

since when adding this to 1, we carry the 1 infinitely many times and it never shows up.

Similar considerations apply to multiplying p-adic integers.

$\mathbf{Z}_p$ is a local ring with maximal ideal generated by p. If we invert p, we get the field of p-adic numbers $\mathbf{Q}_p$. We can represent p-adic numbers as infinite sums

$$\sum_{i \ge N} b_i p^i$$

where N is some integer. In particular, there are only finitely many negative powers of p. This is analogous to Laurent series. □

Corollary 7.1.4. *Let $0 \to \Gamma' \to \Gamma \xrightarrow{f} \Gamma'' \to 0$ be a short exact sequence of abelian groups. Suppose we have a descending chain of subgroups of Γ:*

$$\Gamma \supseteq \Gamma_1 \supseteq \Gamma_2 \supseteq \cdots .$$

Define descending chains on Γ' by taking the intersections $\Gamma' \cap \Gamma_i$ and define a descending chain on Γ'' by taking the images under f. Then we have a short exact sequence

$$0 \to \hat{\Gamma}' \to \hat{\Gamma} \to \hat{\Gamma}'' \to 0.$$

In particular, for each n, we can identify $\hat{\Gamma}_n$ with a subgroup of $\hat{\Gamma}$, so we get a decreasing chain of subgroups

$$\hat{\Gamma} \supseteq \hat{\Gamma}_1 \supseteq \hat{\Gamma}_2 \supseteq \cdots$$

and can take the inverse limit once again

$$\hat{\hat{\Gamma}} = \varprojlim \hat{\Gamma}/\hat{\Gamma}_i.$$

Proposition 7.1.5. *The natural map $\hat{\Gamma} \to \hat{\hat{\Gamma}}$ is an isomorphism.*

Proof. First, for each n, the chain of subgroups for Γ/Γ_n is

$$\Gamma/\Gamma_n \supseteq \Gamma_1/\Gamma_n \supseteq \cdots \supseteq \Gamma_{n+1}/\Gamma_n \supseteq 0 \cdots ,$$

i.e., it eventually stabilizes to 0. Since ignoring a finite initial set of groups does not change the inverse limit, we see that $\widehat{\Gamma/\Gamma_n}$ is naturally isomorphic to Γ/Γ_n. By the previous result this is also the quotient $\hat{\Gamma}/\hat{\Gamma}_n$. In particular, using these identifications, the map $\hat{\Gamma} \to \hat{\hat{\Gamma}}$ becomes the identity. □

7.2. **Krull topology.** Different choices of decreasing sequences of subgroups can result in isomorphic inverse limits. For example, omitting any finite number of terms does not change the result. Since we will need to compare different sequences in a few places, it will convenient to understand this more generally.

First, let Γ be an abelian group with a decreasing chain of subgroups Γ_i as before. The **Krull topology** on Γ is the coarsest topology on Γ such that the cosets $g + \Gamma_i$ are open for all $g \in \Gamma$ and all i. Note that this implies that each coset $g + \Gamma_i$ is also closed because its complement is a union of cosets.

Proposition 7.2.1. *Every open set is a union of cosets $g + \Gamma_i$.*

Proof. By definition, all unions of cosets are open, so we just need to show that taking the intersection of any two unions is again a union of cosets. Using the general identity $(\bigcup_i S_i) \cap (\bigcup_j T_j) = \bigcup_{i,j} S_i \cap T_j$, it suffices to consider the case of intersecting two cosets. So pick $g + \Gamma_i$ and $h + \Gamma_j$, and suppose that $i \geq j$ without loss of generality. We claim that either $(g + \Gamma_i) \cap (h + \Gamma_j)$ is empty, or $(g + \Gamma_i) \cap (h + \Gamma_j) = g + \Gamma_i$.

To see this, suppose the intersection is nonempty and pick $x \in (g + \Gamma_i) \cap (h + \Gamma_j)$, so that we can write $x = g + g' = h + h'$ with $g' \in \Gamma_i \subseteq \Gamma_j$ and $h' \in \Gamma_j$. Then $g - h \in \Gamma_j$, i.e., $g \in h + \Gamma_j$. Since $\Gamma_i \subseteq \Gamma_j$, we thus have $g + \Gamma_i \subseteq g + \Gamma_j = h + \Gamma_j$. □

A **Cauchy sequence** is a sequence $g_1, g_2, \ldots \in \Gamma$ such that for each open neighborhood U of 0, there exists n such that $i, j > n$ implies that $g_i - g_j \in U$. We define an equivalence relation on Cauchy sequences by $(g_i) \sim (g'_i)$ if, for each open neighborhood U of 0, there exists n such that $i > n$ implies that $g_i - g'_i \in U$. From the above result, we actually only need to check these conditions when $U = \Gamma_i$ for some i: every open neighborhood is a union of cosets, the only cosets that contain 0 are the trivial ones, and they are all nested; hence if the condition holds whenever $U = \Gamma_i$, it holds for arbitrary open neighborhoods.

Proposition 7.2.2. *The set of Cauchy sequences is a group under pointwise addition, and the subset of Cauchy sequences equivalent to the 0 sequence is a subgroup.*

Proof. Let (g_i) and (h_i) be Cauchy sequences and pick a subgroup Γ_k. Then there exists n such that if $i, j > n$, then $g_i - g_j \in \Gamma_k$ and $h_i - h_j \in \Gamma_k$. But then $(g_i + h_i) - (g_j + h_j) \in \Gamma_k$, so $(g_i + h_i)$ is also a Cauchy sequence. Similarly, we see that $(-g_i)$ is also a Cauchy sequence, so the set of Cauchy sequences is a group under addition.

The proof for the second part is similar, but also is implied by the next result. □

We will temporarily denote the group of Cauchy sequences by $\mathcal{C}(\Gamma)$ and the subgroup of sequences equivalent to 0 by $\mathcal{C}_0(\Gamma)$. Define a homomorphism $\Phi \colon \mathcal{C}(\Gamma) \to \hat{\Gamma}$ as follows. Pick a Cauchy sequence (g_i). By definition, for each Γ_k, there exists n such that if $i, j > n$, then $g_i - g_j \in \Gamma_k$, i.e., the coset $g_i + \Gamma_k$ is independent of i (as long as $i > n$); let c_k denote this coset. Then define $\Phi((g_i))$ to be the sequence of cosets (c_i). This belongs to the inverse limit $\hat{\Gamma}$: for each k, c_k and c_{k+1} are represented by the same element (some g_i for $i \gg 0$) and Φ is a group homomorphism.

Proposition 7.2.3. *$\Phi\colon \mathcal{C}(\Gamma) \to \hat{\Gamma}$ is surjective with kernel $\mathcal{C}_0(\Gamma)$ and hence we have an isomorphism*

$$\mathcal{C}(\Gamma)/\mathcal{C}_0(\Gamma) \cong \hat{\Gamma}.$$

Proof. If $\Phi((g_i)) = 0$, then the cosets c_i are all trivial. This means that for each Γ_k, we have $g_i \in \Gamma_k$ for $i \gg 0$, and hence $(g_i) \sim 0$. Conversely this shows that any Cauchy sequence equivalent to 0 is in the kernel of Φ. To see that Φ is surjective, pick any sequence $(g_i+\Gamma_i) \in \hat{\Gamma}$. Pick a subgroup Γ_k. If $i, j \geq k$, then $g_i \equiv g_k \pmod{\Gamma_k}$ and $g_j \equiv g_k \pmod{\Gamma_k}$ by definition of the inverse limit. In particular, (g_i) is a Cauchy sequence. Since $\Phi((g_i)) = (g_i + \Gamma_i)$, we see that Φ is surjective. □

The important upshot of the previous discussion is that if two decreasing chains of subgroups define identical Krull topologies on Γ, then their inverse limits are isomorphic. Now suppose we have two groups Γ and Γ' equipped with decreasing filtrations of subgroups and a group homomorphism $f\colon \Gamma \to \Gamma'$ which is continuous for the corresponding Krull topologies. Then we get a homomorphism $\hat{f}\colon \hat{\Gamma} \to \hat{\Gamma}'$ which we can define by applying f pointwise to a Cauchy sequence. This is functorial in the sense that $\hat{g}\hat{f} = \widehat{gf}$ for any other continuous homomorphism $g\colon \Gamma' \to \Gamma''$. The advantage is that it does not rely on understanding how the filtrations might interact with f, though when they are compatible in the sense that $f(\Gamma_i) \subseteq \Gamma'_i$ as in the results the previous section, we can naturally identify the resulting maps. We will take advantage of this fact in the next section.

7.3. **Completion of modules.** Let A be a ring, I an ideal, and M an A-module. The **I-adic filtration** of M is the decreasing chain with $M_i = I^i M$. The resulting Krull topology on M will be called the **I-adic topology**. We have obtained some results on this in §5.2. The **I-adic completion** of M is defined by

$$\hat{M} = \varprojlim M/I^i M.$$

While the notation does not take into account I, we will generally only be dealing with one ideal at a time. We have a natural map $M \to \hat{M}$ given by taking m to the sequence of cosets $m + I^i M$ and we say that M is **complete** with respect to I if this map is an isomorphism.

We can give $\hat{M}$ the structure of a module over $\hat{A}$: for $(a_i) \in \hat{A}$ and $(m_i) \in \hat{M}$, the product is simply $(a_i m_i)$. If $f\colon M \to N$ is A-linear, then $\hat{f}\colon \hat{M} \to \hat{N}$ is $\hat{A}$-linear. In particular, completion is a functor from the category of A-modules to the category of $\hat{A}$-modules.

Remark 7.3.1. Suppose that A is complete with respect to an ideal I. Let $a_0, a_1, \dots \in A$ be a sequence of nonzero elements. Then for each i, there is a largest integer $n(i)$ such that $a_i \in I^{n(i)}$ (if not, then a_i maps to 0 under $A \to \hat{A}$). If we assume that for each n, the set $\{i \mid n(i) \leq n\}$ is finite, then we can make sense of the infinite sum $\sum_{i \geq 0} a_i$: as a sequence, the nth component is the sum of the nonzero cosets of the a_i modulo I^n; this is always a finite sum by our assumption. In this sense, we can think of this condition as saying that the series "converges". One easy way this condition arises is when the $n(i)$ are strictly increasing. □

We can rephrase Lemma 5.2.2 as follows (recall that a filtration (M_i) is I-stable if $IM_i = M_{i+1}$ for $i \gg 0$):

Proposition 7.3.2. *The Krull topology of any I-stable filtration of M agrees with the I-adic topology. In particular, if $\mathcal{F} = (M_i)$ is any I-stable filtration of M, then $\varprojlim M/M_i$ is isomorphic to the I-adic completion $\hat{M}$.*

Proof. By Lemma 5.2.2, there exists n_0 such that $M_{i+n_0} \subseteq I^i M$ and $I^{i+n_0} M \subseteq M_i$ for all $i \geq 0$. In particular, for all i, $I^i M$ is a union of cosets of M_{i+n_0} and vice versa, which implies that the Krull topology defined by both filtrations are the same. □

In particular, the Artin–Rees lemma (Corollary 5.2.6) now gives us the following:

Proposition 7.3.3. *Suppose that A is noetherian, and let*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

be a short exact sequence of finitely generated A-modules. Then for any ideal I,

$$0 \to \hat{M}' \xrightarrow{\hat{f}} \hat{M} \xrightarrow{\hat{g}} \hat{M}'' \to 0.$$

is also a short exact sequence of $\hat{A}$-modules.

Proof. By Artin–Rees and Proposition 7.3.2, if we identify M' with a submodule of M via f, then the I-adic topology on M' is the same as the subspace topology inherited from the I-adic topology on M. Furthermore, the I-adic filtration on M'' is simply the image under g of the I-adic filtration on M, and so we can apply Corollary 7.1.4 to get the desired short exact sequence as abelian groups. However, the $\hat{A}$-module structure is irrelevant for exactness, so we don't need to check anything else. □

Recall that we have a canonical homomorphism of abelian groups

$$M \to \hat{M}, \qquad m \mapsto (m + I^i M)_i$$

which we temporarily denote by φ. The map $A \to \hat{A}$ gives $\hat{A}$ the structure of an A-algebra, and we use this to define a $\hat{A}$-module homomorphism for all M

$$\Phi_M \colon \hat{A} \otimes_A M \to \hat{M}, \qquad \sum_i \alpha_i \otimes m_i \mapsto \sum_i \alpha_i \varphi(m_i)$$

where $\alpha_i \in \hat{A}$ and $m_i \in M$. We note that Φ is natural in the sense that if $f \colon M \to N$ is any A-linear map, we have a commutative square

$$\begin{tikzcd}
\hat{A} \otimes_A M \arrow[r, "\Phi_M"] \arrow[d, "1\otimes f"'] & \hat{M} \arrow[d, "\hat{f}"] \\
\hat{A} \otimes_A N \arrow[r, "\Phi_N"] & \hat{N}
\end{tikzcd}.$$

Remark 7.3.4. More formally, we have discussed two functors from the category of A-modules to the category of $\hat{A}$-modules, the first one is completion and the second one is tensoring with $\hat{A}$. The map Φ is a **natural transformation** between these two functors, i.e., can be thought of as a morphism between these two functors. □

Theorem 7.3.5. *If M is finitely generated then Φ_M is surjective. If, in addition, A is noetherian, then Φ_M is an isomorphism. In particular, $\hat{A}$ is a flat A-module when A is noetherian.*

Proof. Since M is finitely generated, we can find a short exact sequence

$$0 \to K \to A^n \to M \to 0$$

for some n. This gives a commutative diagram

$$\begin{tikzcd}
\hat{A} \otimes_A A^n \arrow[r] \arrow[d, "\Phi_{A^n}"'] & \hat{A} \otimes_A M \arrow[d, "\Phi_M"] \\
\widehat{A^n} \arrow[r] & \hat{M}
\end{tikzcd} .$$

The top map is surjective by right-exactness of tensor products and the bottom map is surjective by Corollary 7.1.4. A direct calculation (omitted) shows that Φ_{A^n} is an isomorphism; these facts imply that Φ_M is surjective, which proves the first part.

Now suppose that A is noetherian. Then K is also finitely generated. Consider the diagram

$$\begin{tikzcd}
 & \hat{A} \otimes_A K \arrow[r] \arrow[d, "\Phi_K"] & \hat{A} \otimes_A A^n \arrow[r] \arrow[d, "\Phi_{A^n}"] & \hat{A} \otimes_A M \arrow[r] \arrow[d, "\Phi_M"] & 0 \\
0 \arrow[r] & \hat{K} \arrow[r] & \hat{A}^n \arrow[r] & \hat{M} \arrow[r] & 0
\end{tikzcd} .$$

The top row is exact by right-exactness of tensor products, and the bottom row is exact by Proposition 7.3.3. Hence the snake lemma (Lemma 1.3.1) gives an exact sequence

$$\ker \Phi_{A^n} \to \ker \Phi_M \to \operatorname{coker} \Phi_K.$$

But the first term is 0 since Φ_{A^n} is an isomorphism and the last term is 0 by the first part since K is finitely generated. Hence Φ_M is an isomorphism.

Finally, for $\hat{A}$ to be flat, it suffices to check that $\hat{A} \otimes_A -$ preserves short exact sequences of finitely generated A-modules, so we're done. □

Remark 7.3.6. Let A be noetherian. The previous result implies that the two functors "completion" and "tensor with $\hat{A}$" are isomorphic if we restrict the domain to be the category of finitely generated A-modules. In general, if M is not finitely generated Φ_M might not be an isomorphism, and in fact, completion need not be exact when considering general modules. However, tensoring with $\hat{A}$ is exact when considering general modules since $\hat{A}$ is flat. □

7.4. **Completion and the associated graded ring.**

Theorem 7.4.1 (Krull intersection theorem)**.** *Let A be a noetherian ring, I an ideal, and M a finitely generated A-module. Let $\hat{M}$ be the I-adic completion of M. The kernel of the completion map $M \to \hat{M}$ is*

$$\bigcap_{i=1}^{\infty} I^i M = \{x \in M \mid ax = 0 \textit{ for some } a \textit{ such that } a - 1 \in I\}.$$

Proof. Let $E = \bigcap_{i=1}^{\infty} I^i M$. From the definition of the I-adic completion, we see that the kernel of $M \to \hat{M}$ is E, so we just need to explain the equality above. Using a corollary of the Artin–Rees lemma (Corollary 5.2.7), there is an integer k such that

$$E \cap I^{k+1} M = I(E \cap I^k M)$$

(we take $n = k + 1$ in the notation of Corollary 5.2.7). The left side is just E and the right side is IE. Hence by Cayley–Hamilton (Theorem 1.5.1) applied to the identity map, there exists $a \in A$ such that $a - 1 \in I$ and $ax = 0$ for all $x \in E$. Conversely, pick $x \in M$ such that $ax = 0$ for some a such that $a - 1 \in I$. Then for any $i \geq 1$, we have $(a-1)^i x \in I^i M$ but also $(a-1)^i x = (a-1)^{i-1}(-x)$. By induction on i, we see that $x \in I^i M$ for all i, so $x \in E$. □

If the kernel of $M \to \hat{M}$ is 0, we say that M is **separated with respect to** I.

Corollary 7.4.2. *If A is a noetherian local ring with maximal ideal $\mathfrak{m}$, then any finitely generated A-module is separated with respect to $\mathfrak{m}$.*

Proof. If $a - 1 \in \mathfrak{m}$, then $a \notin \mathfrak{m}$ and hence is a unit. □

Corollary 7.4.3. *If A is a noetherian domain, then A is separated with respect to any proper ideal I.*

Proposition 7.4.4. *Let A be a ring, I an ideal, M an A-module, and $\mathcal{F} = (M_n)$ an I-filtration of M. Suppose that:*

(1) A is I-adically complete,
(2) $\bigcap_n M_n = 0$, and
(3) $\mathrm{gr}_{\mathcal{F}}(M)$ is a finitely generated $\mathrm{gr}_I(A)$-module.

Then M is a finitely generated A-module.

Proof. Since A is I-adically complete, the canonical map $A \to \hat{A}$ is an isomorphism and hence $\bigcap_n I^n = 0$. So given a nonzero element $a \in I$, there exists a largest n such that $a \in I^n$, and we define its initial term $\mathrm{init}(a)$ to be the image of a in $I^n/I^{n+1} = \mathrm{gr}_I(A)_n$. Similarly, for a nonzero $m \in M$, there is a largest n such that $m \in M_n$ and so we define its initial term $\mathrm{init}(m)$ to be its image in $M_n/M_{n+1} = \mathrm{gr}_{\mathcal{F}}(M)_n$. In both cases, we set $\mathrm{init}(0) = 0$.

We claim the following: if $m_1, \dots, m_r \in M$ are elements such that $\mathrm{init}(m_1), \dots, \mathrm{init}(m_r)$ generate $\mathrm{gr}_{\mathcal{F}}(M)$ as a $\mathrm{gr}_I(A)$-module, then $m_1, \dots, m_r$ generate M as an A-module. This claim proves the result since $\mathrm{gr}_{\mathcal{F}}(M)$ has a finite set of generators (which may be assumed homogeneous by replacing each generator by its homogeneous components), and every homogeneous element of $\mathrm{gr}_{\mathcal{F}}(M)$ is the initial term of an element in M.

Now we prove the claim. Pick nonzero $x_0 \in M$. Then we have an expression in $\mathrm{gr}_{\mathcal{F}}(M)$

$$\mathrm{init}(x_0) = c_{0,1}\mathrm{init}(m_1) + \cdots + c_{0,r}\mathrm{init}(m_r)$$

where $c_{0,i}$ is either 0 or homogeneous of degree $\deg(\mathrm{init}(x_0)) - \deg(\mathrm{init}(m_i))$. We can write $c_{0,i} = \mathrm{init}(C_{0,i})$ for some $C_{0,i} \in A$. We define

$$x_1 = x_0 - (C_{0,1}m_1 + \cdots + C_{0,r}m_r).$$

If $x_1 = 0$, then x_0 is generated by $m_1, \dots, m_r$ and we are done. Otherwise, $\deg \mathrm{init}(x_1) > \deg \mathrm{init}(x_0)$. Now we can repeat this procedure. Either it terminates with $x_i = 0$ for some i, in which case we realize x_0 as a linear combination of $m_1, \dots, m_r$, or we have an infinite sequence $x_0, x_1, \dots$ where $\deg \mathrm{init}(x_{i+1}) > \deg \mathrm{init}(x_i)$ for all i, and

$$x_{i+1} = x_i - (C_{i,1}m_1 + \cdots + C_{i,r}m_r)$$

for some $C_{i,j} \in A$ such that $C_{i,j} = 0$ or

$$\deg(\mathrm{init}(C_{i,j})) = \deg(\mathrm{init}(x_i)) - \deg(\mathrm{init}(m_j)).$$

In particular, for fixed j, $\deg(\mathrm{init}(C_{i,j}))$ is increasing with i, and so the sum $C_j := \sum_i C_{i,j}$ is well-defined since A is complete (Remark 7.3.1). Finally, $x_0 - (C_1 m_1 + \cdots + C_r m_r)$ is 0 modulo M_n for all $n \gg 0$, and hence it is identically 0 since $\bigcap_n M_n = 0$, which proves the claim. □

Theorem 7.4.5. *If A is a noetherian ring and I is an ideal, then the I-adic completion $\hat{A}$ is noetherian.*

Proof. Let $J \subset \hat{A}$ be an ideal. Then $\mathrm{gr}_{\hat{I}}(J)$ is an ideal in $\mathrm{gr}_{\hat{I}}(\hat{A}) \cong \mathrm{gr}_I(A)$ which is a noetherian ring (Lemma 5.2.3). Hence $\mathrm{gr}_{\hat{I}}(J)$ is finitely generated. Next, $\bigcap_n \hat{I}^n J \subset \bigcap_n \hat{I}^n = 0$ by Proposition 7.1.5, so by Proposition 7.4.4, we see that J is finitely generated. □

Corollary 7.4.6. *For any noetherian ring A, the power series ring in n variables $A[\![x_1, \dots, x_n]\!]$ is noetherian.*

Proposition 7.4.7. *If A is a noetherian local ring with maximal ideal $\mathfrak{m}$, and $\hat{A}$ is its $\mathfrak{m}$-adic completion, then $\dim A = \dim \hat{A}$. Furthermore, A is a regular local ring if and only if $\hat{A}$ is a regular local ring.*

Proof. The first statement follows from the fact that $\mathrm{gr}_{\hat{\mathfrak{m}}}(\hat{A}) \cong \mathrm{gr}_{\mathfrak{m}}(A)$, and the dimension of either A or $\hat{A}$ is determined by this graded ring. For the second statement, we use that $A/\mathfrak{m} \cong \hat{A}/\hat{\mathfrak{m}}$ and $\mathfrak{m}/\mathfrak{m}^2 \cong \hat{\mathfrak{m}}/\hat{\mathfrak{m}}^2$. □

7.5. **Further results for complete rings.** Our first goal is give a general form of Hensel's lemma (there are many variations which don't seem to imply one another, but we're just doing one version of it) and then specialize to some of its more common applications. Before that, we state some general results about power series with coefficients in a complete ring. For a more general result, see the exercises.

Proposition 7.5.1. *Let A be a complete ring with respect to an ideal I and let $A[\![x]\!]$ be the formal power series ring over A in one variable. Let $F(x) = \sum_{n \ge 0} f_n x^n$ be a formal power series such that $f_0 \in I$. Then there is a unique A-algebra homomorphism $\varphi\colon A[\![x]\!] \to A[\![x]\!]$ such that $\varphi(x) = F(x)$.*

If $f_0 = 0$ and f_1 is a unit in A, then φ is an isomorphism and $\varphi^{-1}(x)$ has no constant term.

We remark that every ring is complete with respect to the 0 ideal, so this is actually more general than it initially appears.

Proof. Let $\alpha = \sum_{n \ge 0} a_i x^i$ be a formal power series with coefficients in A. Since $f_0 \in I$, the coefficient of x^n in $F(x)^{n+i}$ for $i \ge 0$ is an element of I^n. Hence, the coefficient of x^n in the expression

$$\sum_{n \ge 0} a_i F(x)^i$$

is a well-defined element of A by Remark 7.3.1, and hence this infinite sum is well-defined as an element in $A[\![x]\!]$. If we define $\varphi(\alpha)$ to be this sum, then φ is a homomorphism with the desired property. For uniqueness, any ring homomorphism has to agree with φ whenever α is a polynomial, and this determines everything since every power series can be represented as a sequence of polynomials by definition of the inverse limit.

Next, suppose that $f_0 = 0$ and that f_1 is a unit in A. We will define the coefficients g_n for a formal power series $G(x)$ by induction on n as follows. First set $g_1 = 1/f_1$. Assuming $g_1, \dots, g_{n-1}$ have been defined, set

$$g_n = -\frac{1}{f_1} \sum_{i=2}^{n} f_i [x^n](g_1 x + g_2 x^2 + \cdots + g_{n-1} x^{n-1})^i$$

where $[x^n]h(x)$ means the coefficient of x^n in $h(x)$. Now we define $G(x) = \sum_{n \geq 1} g_n x^n$. Then the coefficient of x^n in $F(G(x))$ is

$$f_1 g_n + \sum_{i=2}^{n} f_i [x^n] G(x)^i.$$

If $n = 1$, the sum is empty and we get $f_1 g_1 = 1$. Otherwise, $[x^n]G(x)^i = [x^n](g_1 x + \cdots + g_{n-1}x^{n-1})^i$ since $i \geq 2$ and so the expression above is 0 by definition, and hence $F(G(x)) = x$. Finally, since $g_0 = 0$ and g_1 is invertible, the same argument shows that there exists a formal power series $H(x)$ such that $G(H(x)) = x$. By associativity of composition of formal power series, we conclude that $H(x) = F(x)$, so that the unique homomorphism determined by $x \mapsto G(x)$ is an inverse to φ. □

Theorem 7.5.2 (Hensel's lemma)**.** *Let A be a complete ring with respect to an ideal I. Let $f(x) \in A[x]$ be a polynomial, let $f'(x)$ be its derivative. Pick $a \in A$, set $e = f'(a)$, and suppose that*

$$f(a) \in e^2 I.$$

Then there exists $b \in A$ such that $f(b) = 0$ and $b \equiv a \pmod{eI}$.

If A is complete with respect to I, then A is also complete with respect to I^k for any positive integer k, so that we can use I^k in place of I in Hensel's lemma to get a more refined statement in some cases.

Furthermore, if e is a nonzerodivisor, it can be shown that there is a unique b that satisfies the two properties above, but we omit the calculation.

Proof. There exists a polynomial $h(x)$ so that

$$f(a + x) = f(a) + ex + h(x)x^2.$$

By Proposition 7.5.1, there is an A-algebra homomorphism $\varphi \colon A[\![x]\!] \to A[\![x]\!]$ determined by $\varphi(x) = x + x^2 h(ex)$, and φ is invertible. By hypothesis, we can write $f(a) = e^2 c$ for some $c \in I$, and again by Proposition 7.5.1, we have an A-algebra homomorphism $\psi \colon A[\![x]\!] \to A[\![x]\!]$ given by $\psi(x) = -c$. We define

$$b = a + e\psi(\varphi^{-1}(x)).$$

Then $b \equiv a \pmod{eI}$ and we have

$$\begin{aligned} f(b) &= f(a + e\psi(\varphi^{-1}(x))) \\ &= \psi(f(a + e\varphi^{-1}(x))) \\ &= \psi(f(a) + e^2\varphi^{-1}(x) + h(e\varphi^{-1}x)(e\varphi^{-1}(x))^2) \\ &= f(a) + e^2\psi(\varphi^{-1}(x + h(ex)x^2)) \\ &= f(a) + e^2\psi(x) \\ &= f(a) - e^2 c = 0. \end{aligned}$$

□

Example 7.5.3. We'll use this to show that if p is an odd prime, then every square in $\mathbf{Z}_p$ is of the form $p^{2n}c$ where n is a non-negative integer and c is an element not divisible by p such that its reduction $\overline{c}$ modulo p is a square.

First, since $\mathbf{Z}_p$ is local with maximal ideal generated by p, we see that every element can be written as $p^m c$ for some non-negative integer m and where c is not divisible by p. If $p^m c = (p^n c')^2$, then $m = 2n$ and $\overline{c} = \overline{c'}^2$ in $\mathbf{Z}/p$, so the condition is necessary.

On the other hand, suppose that $c \in \mathbf{Z}_p$ is not divisible by p and that there exists $\overline{a} \in \mathbf{Z}/p$ such that $\overline{c} = \overline{a}^2$. We use Hensel's lemma with $I = (p)$ in $A = \mathbf{Z}_p$. Let $f(x) = x^2 - c \in \mathbf{Z}_p[x]$ and let $a \in \mathbf{Z}_p$ be any preimage of $\overline{a}$. Since $\overline{c} \neq 0$, we conclude that $a \notin (p)$, and so $f'(a) = 2a$ is a unit in $\mathbf{Z}_p$. Hence $f'(a)^2 I = I$ and $f(a) \in I$. Hensel's lemma then tells us that there exists $b \in \mathbf{Z}_p$ such that $f(b) = 0$, i.e., $b^2 = c$. Hence every element of the form $p^{2n}c$ with $\overline{c} \in \mathbf{Z}/p$ a square is in fact a p-adic square. □

Example 7.5.4. We now determine which 2-adic numbers are squares. Namely, they are the elements of the form $4^n c$ where $c \equiv 1 \pmod 8$.

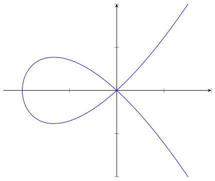
Again, every element is of the form $2^n c$ where c is not divisible by 2, and if $2^n c = (2^m c')^2$, then $n = 2m$ and working modulo 8, we have $\overline{c} = \overline{c'}^2$. But we can write $\overline{c'} = 2d + 1$ for some $d \in \mathbf{Z}/8$ and so $\overline{c} = (2d+1)^2 = 4d(d+1) + 1$, and $4d(d+1) \equiv 0 \pmod 8$ for any d.

On the other hand, suppose we're given $c \in \mathbf{Z}_2$ such that $c \equiv 1 \pmod 8$. We use Hensel's lemma with $A = \mathbf{Z}_2$, $I = (2)$, $f(x) = x^2 - c$, and $a = 1$. Then $f'(1) = 2$ and so $f'(a)^2 I = (8)$. We have $f(1) \in (8)$ by assumption, and so there exists $b \in \mathbf{Z}_2$ such that $f(b) = 0$, i.e., $b^2 = c$. □

Example 7.5.5. Let $\mathbf{k}$ be a field of characteristic different from 2 and consider the ring $A = \mathbf{k}[\![x]\!]$ with $I = (x)$. Then a power series $\alpha = \sum_{n \geq 0} a_n x^n$ is a square if and only if we can write $\alpha = x^{2k}\beta$ for some integer k and power series β such that its constant term is nonzero and a square in $\mathbf{k}$. This is similar to Example 7.5.3, so we omit the details.

If $\mathbf{k}$ has characteristic 2, the answer is very different: from the calculation $(\sum_{n \geq 0} c_n x^n)^2 = \sum_{n \geq 0} c_n^2 x^{2n}$, we see that a power series is a square if and only if the coefficient of x^n is 0 when n is odd and is a square in $\mathbf{k}$ when n is even. □

Example 7.5.6. Consider the ring $A = \mathbf{C}[x,y]/(y^2 - x^2(x+1))$. Since $y^2 - x^2(x+1)$ is an irreducible polynomial, A is a domain, which implies that $\operatorname{Spec} A$ is an irreducible space (i.e., not a union of two closed proper subsets). By the nullstellensatz, it is appropriate to identify this with the subspace $\{(a,b) \in \mathbf{C}^2 \mid b^2 = a(a+1)\}$. Here we draw the real points of that set:



If we zoom in on the origin, the plot looks like the union of two lines, i.e., the solution set of $xy = 0$, which is reducible. Localization does not detect this behavior (localization of a domain is still a domain), but completion does: by Example 7.5.5, $x^2(x+1)$ is a square in $\mathbf{C}[\![x]\!]$, and hence $y^2 - x^2(x+1)$ factors. So completion allows us to "zoom in further" than localization does.

This implies that the completion of a domain need not be a domain. □

We end this section by stating a special case of the Cohen structure theorem for complete noetherian local rings.

Theorem 7.5.7 (Cohen structure theorem)**.** *Let A be a noetherian local ring which is complete with respect to its maximal ideal $\mathfrak{m}$ and let $\mathbf{k} = A/\mathfrak{m}$.*

(1) A is isomorphic to a quotient of a regular local ring.

(2) *If A contains a subring which is a field, then there exists an integer n such that A is isomorphic to a quotient ring of $\mathbf{k}[\![x_1, \dots, x_n]\!]$.*
(3) *Furthermore, if A is a regular local ring and contains a subring which is a field, then there exists an integer n such that $A \cong \mathbf{k}[\![x_1, \dots, x_n]\!]$.*

If A is a quotient of B, then we can identify Spec(B) with a closed subset of Spec(A): namely, if I is the kernel of $B \to A$, then Spec$(A) = V(I)$. Hence the first result tells us that we can always embed Spec(A) into the spectrum of a regular local ring when A is complete. This is analogous to the Whitney embedding theorem which tells us that differentiable manifolds can be embedded into Euclidean space.

If we remove the complete hypothesis, then we can't say that noetherian local rings are quotients of a special kind of ring like the localization of a polynomial ring over a field, and in general their structure can be difficult to control. This is one reason why working with complete local rings can be simpler.

If A contains a field, it is said to be **equicharacteristic** (because the characteristic of this field must match the characteristic of its residue field). Otherwise, it is said to have **mixed characteristic** since this implies that A has characteristic 0, but its residue field has positive characteristic. For an example, take $\mathbf{Z}_p$.

In the mixed characteristic case, there is still something analogous to (2) that can be said, though the statement is more involved and we won't discuss it. See https://stacks.math.columbia.edu/tag/0323 for more details.

Part (3) of the theorem tells us that complete regular local rings are all power series rings (when they contain a field). In contrast, non-complete regular local rings have much more complicated behavior and cannot be classified so easily. This shows that completion does simplify some things, but can simplify other things *too much*.

8. Behavior in low (co)dimension

8.1. Associated primes.

Let $I \subset A$ be an ideal. A prime $\mathfrak{p} \subset A$ is **associated to** I if there exists $x \in A$ such that $\mathfrak{p} = (I : x)$, i.e., $\mathfrak{p}$ is the annihilator of the image of x in A/I. In other words, the A-linear map $A/\mathfrak{p} \to A/I$ given by $a + \mathfrak{p} \mapsto ax + I$ is injective (and well-defined). We write $\mathrm{AP}_A(I)$ to denote the set of associated primes of I (we'll drop the subscript if it's clear from context). If I is generated by a single element which is a nonzerodivisor, then any associated prime of I is said to be **associated to a nonzerodivisor**. Finally, for $I = 0$, a prime associated to 0 is said to be an **associated prime of** A.

Proposition 8.1.1. *Consider the poset of ideals of the form $\{\mathrm{Ann}(x) \mid x \in A,\ x \neq 0\}$. Any maximal element in this set is prime, and in particular is an associated prime of A.*

Proof. Let $I = \mathrm{Ann}(x)$ be a maximal element in this poset. Since $x \neq 0$, we have $1 \notin I$, and so I is a proper ideal. Suppose that $ab \in I$ but $a \notin I$. Then $ax \neq 0$ and $I \subseteq \mathrm{Ann}(ax)$. Since I is maximal, we have equality. Also, $abx = 0$, so $b \in \mathrm{Ann}(ax)$, which means that $b \in \mathrm{Ann}(x)$. Thus I is prime. □

For a general ring, the set of annihilators of nonzero elements may not have any maximal elements. Hence the notion is better behaved if we assume that the ring is noetherian, in which case they are guaranteed to exist.

Corollary 8.1.2. *Let A be a noetherian ring. If $x \in A$ is nonzero, then there exists an associated prime $\mathfrak{p}$ such that the image of x under $A \to A_{\mathfrak{p}}$ is nonzero.*

Proof. The set $\{\mathrm{Ann}(y) \mid y \in A,\ y \neq 0,\ \mathrm{Ann}(x) \subseteq \mathrm{Ann}(y)\}$ is nonempty since it contains $\mathrm{Ann}(x)$. Since A is noetherian, it has a maximal element $\mathfrak{p}$. Then the image of x in $A_\mathfrak{p}$ is nonzero. By Proposition 8.1.1, $\mathfrak{p}$ is an associated prime. □

We're going to be interested in characterizing normal rings in terms of properties of associated primes, so we prove a few preparatory results.

For any ring A, its **total fraction ring** is the localization $A[S^{-1}]$ where S is the set of nonzerodivisors. This is just the field of fractions if A is a domain.

Proposition 8.1.3. *Let A be a noetherian ring with total fraction ring B and pick $x \in B$. Then $x \in A$ if and only if the image of x in $B_\mathfrak{p}$ belongs to $A_\mathfrak{p}$ for all primes $\mathfrak{p}$ associated to a nonzerodivisor in A.*

Proof. Write $x = a/u$ where $a, u \in A$ and u is a nonzerodivisor. If $x \notin A$, then $a \notin (u)$, i.e., a is nonzero in A/u. In particular, by Corollary 8.1.2, there exists $\mathfrak{p}' \in \mathrm{AP}_{A/u}(0)$ such that the image of a is nonzero in $(A/u)_{\mathfrak{p}'}$. Let $\mathfrak{p}$ be the inverse image of $\mathfrak{p}$ in A. Then $(A/u)_{\mathfrak{p}'} = A_\mathfrak{p}/(u)_\mathfrak{p}$, and so $a \notin (u)_\mathfrak{p}$, so that $a/u \notin A_\mathfrak{p}$. □

Let d be a nonnegative integer. We define some properties for a ring A:

- A satisfies (R_d) if for every prime ideal $\mathfrak{p} \subset A$ of height $\leq d$ (recall that the height of $\mathfrak{p}$ agrees with $\dim(A_\mathfrak{p})$), $A_\mathfrak{p}$ is a regular local ring.
- A satisfies (S_1) if every prime associated to 0 has height 0.
- A satisfies (S_2) if A satisfies (S_1) and every prime associated to a nonzerodivisor has height 1.

There is a more general condition (S_d) which is beyond the scope of this course, see Remark [⋆ Steven: ref ⋆].

8.2. Reduced rings.

In §6.4, we explained that a regular local ring of dimension 0 is the same thing as a field. Here is a slightly upgraded statement. Recall that a ring is reduced if it has no nonzero nilpotent elements.

Proposition 8.2.1. *Let A be a 0-dimensional noetherian local ring with maximal ideal $\mathfrak{m}$. The following are equivalent:*

(1) A is a regular local ring, i.e., $\mathfrak{m} = 0$.
(2) A is a field.
(3) A is reduced.

Proof. We've already seen that (1) and (2) are equivalent, and (2) clearly implies (3). Since the nilradical is $\mathfrak{m}$, every element of $\mathfrak{m}$ is nilpotent. So if A is reduced, then $\mathfrak{m} = 0$. □

Theorem 8.2.2. *Let A be a noetherian ring. Then A is reduced if and only if A satisfies (R_0) and (S_1).*

Proof. First suppose that A is reduced. Let $\mathfrak{p}$ be a prime of height 0, so that $A_\mathfrak{p}$ is a reduced 0-dimensional local ring. By the previous result, $A_\mathfrak{p}$ is a regular local ring, and so A satisfies (R_0). Next, suppose that $\mathfrak{p}$ is a prime associated to 0, so that we have $\mathfrak{p} = \mathrm{Ann}(x)$ for some nonzero $x \in A$. If $\mathfrak{p}$ has positive height, then $\mathfrak{p}$ properly contains another prime $\mathfrak{q}$. But then $x\mathfrak{p} = 0 \subseteq \mathfrak{q}$, and since there is some element in $\mathfrak{p}$ not in $\mathfrak{q}$, we conclude that $x \in \mathfrak{q}$. But then $x \in \mathfrak{p} = \mathrm{Ann}(x)$, i.e., $x^2 = 0$, which contradicts that A is reduced. Hence A satisfies (S_1).

Conversely, suppose that A satisfies (R_0) and (S_1). Suppose that $x \in A$ is nilpotent and $x \neq 0$. By Corollary 8.1.2, there is an associated prime $\mathfrak{p}$ of A such that the image of x

under $A \to A_{\mathfrak{p}}$ is nonzero. By (S_1), we have height$(\mathfrak{p}) = 0$, and so by (R_0), $A_{\mathfrak{p}}$ is a reduced ring, i.e., has no nonzero nilpotent elements. But the image of x is nilpotent, so we have a contradiction. Hence A is reduced. □

Recall that a topological space is irreducible if it cannot be written as a union of two closed proper subsets. We'll omit the proof of the next result since it doesn't use any of the new concepts we just introduced and could have been stated at the very beginning.

Proposition 8.2.3. *Let A be a ring. Then A is a domain if and only if A is reduced and* $\mathrm{Spec}(A)$ *is an irreducible topological space.*

Now suppose A is a noetherian ring and we want to know if it is a domain (equivalently, suppose that $A = B/I$ and we want to know if I is prime). The above discussion says we can separate this check into two tasks: that A is reduced, which we can separate further using Theorem 8.2.2 (this can be thought of as an "algebraic" condition) and that $\mathrm{Spec}(A)$ is irreducible (this can be thought of as a "topological" condition). In some important cases, like when B is a polynomial ring over a field, this can be handled with some concrete calculations. We'll discuss some nontrivial examples where this applies in [$\star$ Steven: ref $\star$].

8.3. **Discrete valuation rings.** We wish to discuss regular domains of dimension 1. We start with a discussion of the local situation.

Let K be a field. A **discrete valuation** of K is a surjective function $v \colon K \setminus 0 \to \mathbf{Z}$ such that for all $x, y \in K \setminus 0$, we have

(1) $v(xy) = v(x) + v(y)$, and
(2) $v(x + y) \geq \min(v(x), v(y))$ whenever $x \neq -y$.

Statements can be sometimes simplified by adopting the convention that $v(0) = \infty$.

By (1), we must have $v(1) = 0$. The subset

$$A = \{0\} \cup \{x \in K \mid v(x) \geq 0\}$$

is a subring of K called the **valuation ring** of v; it is a local ring with maximal ideal

$$\mathfrak{m} = \{0\} \cup \{x \in K \mid v(x) > 0\}.$$

To see this, pick $x \in A \setminus \mathfrak{m}$. Then $v(x) = 0$, and so $v(x^{-1}) = 0$ by (1) since $0 = v(1) = v(x) + v(x^{-1})$. Hence $x^{-1} \in A$, which shows that every element of $A \setminus \mathfrak{m}$ is invertible.

Example 8.3.1. (1) Let $K = \mathbf{Q}$ and let p be a prime. Every rational number can be written in the form $p^a x$ where a is an integer and the numerator and denominator of x are prime to p. The p-adic valuation is defined by $v_p(p^a x) = a$. Its valuation ring is $\mathbf{Z}_{(p)}$, the integers localized at the prime p.

(2) Again let p be a prime and let $K = \mathbf{Q}_p$ be the field of p-adic numbers. Using the notation from Example 7.1.3, every p-adic number can be written as an infinite sum $\sum_{n \geq N} a_n p^n$ where $0 \leq a_i \leq p - 1$. If $a_N \neq 0$, we define its valuation to be N. The valuation ring is the ring of p-adic integers $\mathbf{Z}_p$.

(3) Similar to (1), let $\mathbf{k}$ be any field and let $K = \mathbf{k}(x)$ be the field of rational functions. Let $f \in \mathbf{k}[x]$ be an irreducible polynomial. Then every rational function can be written as $f^a g$ where a is an integer and both the numerator and denominator of g are prime to f. We define a valuation by $v_f(f^a g) = a$. Its valuation ring is $\mathbf{k}[x]_{(f)}$, the polynomial ring localized at the prime ideal generated by f.

(4) As a variation of (2) above, let $K = \mathbf{k}(\!(x)\!)$ be the field of Laurent series in 1 variable. Given a Laurent series $\sum_{n \ge N} a_n x^n$ with $a_N \neq 0$, its valuation is defined to be N. The valuation ring is the ring of formal power series. □

A local domain is a **discrete valuation ring** (DVR, for short) if there exists a discrete valuation on its field of fractions so that A is the corresponding valuation ring.

Proposition 8.3.2. *Every discrete valuation ring is noetherian and has Krull dimension* 1.

Proof. Let A be a DVR and let v be a valuation on its field of fractions K. First, note that if $v(x) = v(y)$, then $v(xy^{-1}) = v(x) - v(y) = 0$, and so $xy^{-1} \in A$ and the ideals generated by x and y are the same. Let I be a nonzero ideal of A and let $k = \min\{v(x) \mid x \in I \setminus 0\}$. Then I contains every element x such that $v(x) = k$ by the previous comment, which means that $I = \mathfrak{m}^k$. This means that A satisfies ACC for ideals since we know what all of the ideals are and there are no infinite strictly increasing chains.

Furthermore, the only prime ideals are 0 and $\mathfrak{m}$. Since v is surjective onto $\mathbf{Z}$, we have $\mathfrak{m} \neq 0$, and so $\dim A = 1$ by the definition of dimension using chains of prime ideals. □

Proposition 8.3.3. *Let A be a noetherian local domain of dimension* 1 *with maximal ideal $\mathfrak{m}$ and residue field $\mathbf{k} = A/\mathfrak{m}$. The following are equivalent:*

(1) A is a DVR.
(2) A is normal.
(3) $\mathfrak{m}$ is a principal ideal.
(4) A is a regular local ring, i.e., $\dim_{\mathbf{k}}(\mathfrak{m}/\mathfrak{m}^2) = 1$.
(5) Every nonzero ideal is a power of $\mathfrak{m}$.
(6) There exists $x \in A$ such that every nonzero ideal is of the form (x^k) for some $k \ge 0$.

Proof. Since $\dim A = 1$, we have $\sqrt{I} = \mathfrak{m}$ for any nonzero proper ideal: $\sqrt{I}$ is an intersection of prime ideals, and the only nonzero prime is $\mathfrak{m}$.

(1) implies (2): Assume that A is a DVR and let $v \colon K \to \mathbf{Z}$ be a valuation such that A is its valuation ring. If $x \in K$ is integrally closed over A, then we have an equation

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

with $a_i \in A$. If $v(x) \ge 0$, there is nothing to show. Otherwise, $v(x) < 0$ and so $v(x^{-1}) > 0$ and hence $x^{-1} \in A$. Multiply the above equation by x^{-n+1} and rearrange to get

$$x = -(a_{n-1} + a_{n-2}x^{-1} + \cdots + a_0(x^{-1})^{n-1}),$$

which shows that $x \in A$, a contradiction. Hence $x \in A$, and so A is normal.

(2) implies (3): Assume that A is normal and pick nonzero $a \in \mathfrak{m}$; then $\sqrt{(a)} = \mathfrak{m}$ as noted above. In particular, there exists a minimal positive n such that $\mathfrak{m}^n \subseteq (a)$. Pick $b \in \mathfrak{m}^{n-1}$ such that $b \notin (a)$ and set $x = a/b$ in the field of fractions of A. Then for any $y \in \mathfrak{m}$, we have $by \in \mathfrak{m}^n \subseteq (a)$, and hence $x^{-1}y = by/a \in A$. In particular, $x^{-1}\mathfrak{m}$ is an ideal in A. We claim that $x^{-1}\mathfrak{m}$ is not a proper ideal; if so, then $x^{-1}\mathfrak{m} \subseteq \mathfrak{m}$ and hence $\mathfrak{m}$ is a faithful (since A is a domain) $A[x]$-module which is finitely generated as an A-module. By Proposition 3.1.1, this implies that x^{-1} is integral over A, which means $x^{-1} \in A$, which contradicts that $b \notin (a)$, and our claim is proven. This means that $x^{-1}\mathfrak{m} = A$, and so every element of $\mathfrak{m}$ is a multiple of x, i.e., $\mathfrak{m} = (x)$.

(3) implies (4): if $(x) = \mathfrak{m}$, then the image of x generates $\mathfrak{m}/\mathfrak{m}^2$; if $x \notin \mathfrak{m}^2$ then $\mathfrak{m} = 0$ by Nakayama's lemma, which contradicts that $\dim A = 1$.

(4) implies (5): Let I be a nonzero proper ideal. Then $\sqrt{I} = \mathfrak{m}$ as we have noted above, so there is a positive integer n such that $\mathfrak{m}^n \subseteq I$. If $\mathfrak{m}^n = I$ we are done, otherwise there exists a maximal r such that $I \subseteq \mathfrak{m}^r$. Then $I \not\subseteq \mathfrak{m}^{r+1}$ and we can $y \in I \setminus \mathfrak{m}^{r+1}$. By (4), there exists $x \in A$ such that $(x) = \mathfrak{m}$. Since $I \subseteq \mathfrak{m}^r$, we can write $y = ax^r$ where $a \notin \mathfrak{m}$, i.e., a is a unit. But then $x^r \in I$, i.e., $I = \mathfrak{m}^r$.

(5) implies (6): Since $\mathfrak{m} \neq 0$, we have $\mathfrak{m} \neq \mathfrak{m}^2$ by Nakayama's lemma. Pick $x \in \mathfrak{m} \setminus \mathfrak{m}^2$. Then by (5), there exists k such that $(x) = \mathfrak{m}^k$. But then $k = 1$ by our choice of x, so $\mathfrak{m} = (x)$ and hence every ideal is generated by x^k for some k by (5).

(6) implies (1): We have $(x) = \mathfrak{m}$, and so $(x^k) \neq (x^{k+1})$ for all k by Nakayama's lemma. So given nonzero $a \in A$, there is a unique k such that $(a) = (x^k)$ and we define $v(a) = k$. For $a, a' \in A$, we have $v(aa') = v(a) + v(a')$ by construction. Furthermore,

$$(a + a') \subseteq (a, a') = (x^{v(a)}, x^{v(a')}) \subseteq (x^{\min(v(a),v(a'))}),$$

and so $v(a + a') \geq \min(v(a), v(a'))$.

For any nonzero $a, b \in A$, we set $v(a/b) = v(a) - v(b)$. For any $c \in A$, we have $v(ac/bc) = v(a) - v(b)$ so that this is well-defined. Then

$$v(aa'/bb') = v(a/b) + v(a'/b')$$

by what we have shown, and

$$\begin{aligned} v(\frac{a}{b} + \frac{a'}{b'}) &= v(\frac{ab' + a'b}{bb'}) \\ &= v(ab' + a'b) - v(bb') \\ &\geq \min(v(a) + v(b'), v(a') + v(b)) - v(b) - v(b') \\ &= \min(v(a) - v(b), v(a') - v(b')) \\ &= \min(v(a/b), v(a'/b')). \end{aligned}$$

Furthermore, $v(x) = 1$, and so v is surjective onto $\mathbf{Z}$, and we have verified that v is a valuation. Finally, suppose that $v(a/b) \geq 0$, i.e., that $v(a) \geq v(b)$. Then $(a) \subseteq (b)$, so that there exists $c \in A$ such that $a = bc$. But then $c = a/b$ and so $a/b \in A$. In particular, A is the valuation ring of v and hence is a DVR. □

Corollary 8.3.4. *Let A be a DVR with maximal ideal $\mathfrak{m}$. Then the $\mathfrak{m}$-adic completion of A is a DVR.*

Proof. This follows from Proposition 7.4.7. □

8.4. **Serre's criterion for normality.**

Theorem 8.4.1. *Let A be a noetherian domain. Then A is normal if and only if, for every prime $\mathfrak{p}$ associated to a principal ideal, $\mathfrak{p}A_\mathfrak{p}$ is a principal ideal, i.e., $A_\mathfrak{p}$ is a DVR.*

Proof. Let K be a field of fractions of A.

First suppose that A is normal. Let $\mathfrak{p} = ((a) : b)$ be a prime associated to a principal ideal (a). Define

$$\mathfrak{p}^{-1} = \{x \in K \mid x\mathfrak{p}A_\mathfrak{p} \subseteq A_\mathfrak{p}\},$$

which is an $A_\mathfrak{p}$-submodule of K. We define $\mathfrak{p}^{-1}\mathfrak{p}A_\mathfrak{p}$ to be the set of linear combinations of elements xa where $x \in \mathfrak{p}^{-1}$ and $a \in \mathfrak{p}A_\mathfrak{p}$; this is an ideal of $A_\mathfrak{p}$ and we claim that $\mathfrak{p}^{-1}\mathfrak{p}A_\mathfrak{p} = A_\mathfrak{p}$. If not, then since $\mathfrak{p}A_\mathfrak{p} \subseteq \mathfrak{p}^{-1}\mathfrak{p}A_\mathfrak{p}$, and $\mathfrak{p}A_\mathfrak{p}$ is a maximal ideal of $A_\mathfrak{p}$, we must have $\mathfrak{p}A_\mathfrak{p} = \mathfrak{p}^{-1}\mathfrak{p}A_\mathfrak{p}$. Then by Proposition 3.1.1, each element of $\mathfrak{p}^{-1}$ is integral over $A_\mathfrak{p}$, which implies that $\mathfrak{p}^{-1} \subseteq A_\mathfrak{p}$ since we have assumed that A is normal. By definition, $b\mathfrak{p} \subseteq (a)$, so $b/a \in \mathfrak{p}^{-1} \subseteq A_\mathfrak{p}$, but that contradicts our assumption that b is nonzero modulo a, and our claim is proven.

Finally, for each $x \in \mathfrak{p}^{-1}$, $x\mathfrak{p}A_\mathfrak{p}$ is an ideal of $A_\mathfrak{p}$. Since $\mathfrak{p}^{-1}\mathfrak{p}A_\mathfrak{p} = A_\mathfrak{p}$, and $\mathfrak{p}A_\mathfrak{p}$ is the unique maximal ideal, there must exist $x \in \mathfrak{p}^{-1}$ such that $x\mathfrak{p}A_\mathfrak{p} = A_\mathfrak{p}$. But then $1/x \in \mathfrak{p}A_\mathfrak{p}$ is a generator.

Conversely, suppose that, for every prime $\mathfrak{p}$ associated to a principal ideal, $A_\mathfrak{p}$ is a DVR. If $x \in K$ is integral over A, then it is also integral over each $A_\mathfrak{p}$, which is a normal domain, and hence $x \in \bigcap_\mathfrak{p} A_\mathfrak{p}$. By Proposition 8.1.3, we have $A = \bigcap_\mathfrak{p} A_\mathfrak{p}$ where the intersection is over all primes associated to a principal ideal generated by a nonzerodivisor, which implies that $x \in A$, so that A is normal. □

We now give a more general characterization.

Theorem 8.4.2 (Serre)**.** *Let A be a noetherian ring. Then A is isomorphic to a (finite) direct product of normal domains if and only if A satisfies* (R$_1$) *and* (S$_2$)*.*

Proof. First suppose that $A \cong A_1 \times \cdots \times A_r$ where each A_i is a normal domain. Every prime ideal of A is then of the form $A_1 \times \cdots \times \mathfrak{p}_i \times \cdots \times A_r$ where $\mathfrak{p}_i$ is a prime ideal of A_i (and all of the other factors are the unit ideal) and its height is just the height of $\mathfrak{p}_i$. The localization is $(A_i)_{\mathfrak{p}_i}$, which is a normal domain, and so if $\operatorname{height}(\mathfrak{p}_i) \le 1$, then this is a regular local ring by Propositions 8.2.1 and 8.3.3. Hence A satisfies (R$_1$).

Next, using Theorem 8.2.2, A satisfies (S$_1$) since a product of domains is reduced. Next, every nonzerodivisor of A is of the form $a = (a_1, \dots, a_r)$ where $a_i \in A_i$ is a nonzerodivisor. Then $\mathfrak{p}_i$ is an associated prime of (a_i) if and only if $A_1 \times \cdots \mathfrak{p}_i \cdots \times A_r$ is an associated prime of a. By Theorem 8.4.1, $\mathfrak{p}_i A_{\mathfrak{p}_i} \cong \mathfrak{p}_i (A_i)_{\mathfrak{p}_i}$ is the maximal ideal of a DVR, and hence has height 1.

Conversely, suppose that A satisfies (R$_1$) and (S$_2$). Let $\mathfrak{p}$ be a prime associated to a nonzerodivisor. By (S$_2$), $\mathfrak{p}$ has height 1, so by (R$_1$), $A_\mathfrak{p}$ is a regular local ring, so is a normal domain by Proposition 8.3.3. Let B be the total fraction ring of A. Then $A \to B$ is integral: if $x \in B$ is integral over A, then in particular, the image of x in $B_\mathfrak{p}$ is integral over $A_\mathfrak{p}$ for $\mathfrak{p}$ as above, and hence belongs to $A_\mathfrak{p}$ by normality. Since A is the intersection of the $A_\mathfrak{p}$ by Proposition 8.1.3, we see that $x \in A$.

Next, B is 0-dimensional: any prime ideal consists of zerodivisors, so if there is a strict containment, quotienting by the smaller one would give a non-domain. By Theorem 4.6.6, B is isomorphic to a product of local artinian rings. By Theorem 8.2.2, A is reduced, which implies that B is reduced as well (Proposition 2.4.4), and so in fact B is isomorphic to a product of fields $\mathbf{k}_1 \times \cdots \times \mathbf{k}_r$. Let e_i be the vector which is 1 in $\mathbf{k}_i$ and 0 elsewhere. Then the e_i are orthogonal idempotents, i.e., $e_i e_j = 0$ for $i \ne j$ and $e_i^2 = e_i$. This can be rewritten as $e_i^2 - e_i = 0$, so e_i is integral over A, and hence $e_i \in A$. In particular, if we define $A_i = e_i A$, then $A \cong A_1 \times \cdots \times A_r$ and $\mathbf{k}_i$ is the total fraction ring of A_i, i.e., A_i is a domain. Finally, since A is integral in B, we conclude that A_i is integral in $\mathbf{k}_i$, so that it is a normal domain. □

8.5. **Jacobian criterion.** See [Ei, §16.6] for the material in this section.

How do we actually check the conditions (R$_d$)? For quotients of polynomial rings over a field there is an explicit computation. For simplicity, let $\mathbf{k}$ be an algebraically closed field and consider the polynomial ring $A = \mathbf{k}[x_1, \dots, x_n]$. Let $I = (f_1, \dots, f_r)$ be an ideal of

A. We will explain how to check the (R_d) condition for A/I. Recall that this means that $(A/I)_{\mathfrak{p}}$ is a regular local ring for all primes $\mathfrak{p}$ of A/I whenever $\dim(A/I)_{\mathfrak{p}} \le d$. We define the **singular locus** of A/I to be the set of primes $\mathfrak{p}$ such that $(A/I)_{\mathfrak{p}}$ is not a regular local ring.

The **Jacobian matrix** of I is the $r \times n$ matrix of partial derivatives

$$\mathfrak{J} = \left(\frac{\partial f_i}{\partial x_j}\right)_{i=1,\dots,r,\ j=1,\dots,n}.$$

Let $\mathfrak{p}$ be a prime ideal of A that contains I (which we think of as being naturally in bijection with the primes just mentioned) and let $c = \dim A_{\mathfrak{p}} - \dim(A_{\mathfrak{p}}/I_{\mathfrak{p}})$.

Below, for a matrix with entries in a domain, we can think of it as a matrix over the field of fractions, so that its rank has the usual meaning.

Theorem 8.5.1 (Jacobian criterion)**.** *Keep the notation above.*

(1) The rank of $\mathfrak{J}$ modulo $\mathfrak{p}$ is $\le c$.
(2) $A_{\mathfrak{p}}/I_{\mathfrak{p}}$ is a regular local ring if and only if the rank of $\mathfrak{J}$ modulo $\mathfrak{p}$ is c.

Now suppose that all of the minimal primes $\mathfrak{p}$ containing I have the same codimension $c = n - \dim A_{\mathfrak{p}}$. We say that c has **pure codimension** c in that case.

Corollary 8.5.2. *If I has pure codimension c, let J be the ideal of A/I generated by the determinants of the $c \times c$ submatrices of $\mathfrak{J}$ modulo I. The singular locus of A/I is $V(J)$, i.e., $(A/I)_{\mathfrak{p}}$ is a regular local ring if and only if $\mathfrak{p}$ does not contain J.*

If I has pure codimension c, then $\dim(A/I) = n-c$, and then this result tells us that A/I satisfies property (R_d) if and only if $\dim(A/I)/J < n - c - d$.

This takes on a simple meaning for $d = 0$ (relevant for checking if A/I is reduced). Explicitly, one can show that this means that for every irreducible component of $V(I)$ (which corresponds to a minimal prime $\mathfrak{p}$ of A/I), we have a point $(\alpha_1, \dots, \alpha_n) \in \mathbf{k}^n$ in $V(I)$ (i.e., the maximal ideal $(x_1 - \alpha_1, \dots, x_n - \alpha_n)$ contains $\mathfrak{p}$) such that doing the substitution $x_i \mapsto \alpha_i$ in $\mathfrak{J}$ results in a rank c matrix.

We'll omit the details for why this translation works, and end with an example.

Example 8.5.3. Let $f \in \mathbf{k}[x_1, \dots, x_n]$ be any nonzero polynomial over an algebraically closed field (not necessary, but so we can invoke nullstellensatz). The Jacobian matrix of (f) is

$$\left(\frac{\partial f}{\partial x_1} \cdots \frac{\partial f}{\partial x_n}\right),$$

Hence $\mathbf{k}[x_1, \dots, x_n]/(f)$ satisfies (R_d) if the solution set to $(f, \frac{\partial f}{\partial x_1}, \dots, \frac{\partial f}{\partial x_n})$ has dimension $< n - 1 - d$. Note that if f is homogeneous of degree d and $d \neq 0$ in $\mathbf{k}$, then f is redundant by Euler's formula

$$(\deg f) \cdot f = \sum_{i=1}^n x_i \frac{\partial f}{\partial x_i}.$$

For example, if f is a quadric and $\mathbf{k}$ does not have characteristic 2, then since $\mathbf{k}$ is algebraically closed, f can be diagonalized, i.e., is a sum of squares $x_1^2 + \cdots + x_r^2$ (where r is the rank of f) after some linear change of coordinates. In that case, the solution set of $x_1 = \cdots = x_r$ has dimension $n - r$, so $\mathbf{k}[x_1, \dots, x_n]/(f)$ satisfies (R_r). □

Unfortunately, while explicit, these computations can still be a lot of work, so we won't do anything more complicated in the interest of time.

8.6. Cohen–Macaulay rings.

Finally, we discuss the conditions (S$_1$) and (S$_2$) (and (S$_d$) in general). See [Ei, §18] for more details. We need some definitions first.

Let M be an A-module. A sequence $x_1, \dots, x_r \in A$ is a **regular sequence on** M if $(x_1, \dots, x_r)M \neq M$ and for all $i = 1, \dots, r$, x_i is a nonzerodivisor on $M/(x_1, \dots, x_{i-1})M$ (when $i = 1$, this quotient is M).

Now let A be a noetherian local ring with maximal ideal $\mathfrak{m}$. The **depth** of A, denoted $\mathrm{depth}(A)$, is defined to be the maximum length of a regular sequence on A. It is a fact that

$$\mathrm{depth}(A) \leq \dim(A),$$

and A is defined to be **Cohen–Macaulay** if they are equal. This property is preserved by localization, and we define a general noetherian ring A to be Cohen–Macaulay if $A_{\mathfrak{p}}$ is Cohen–Macaulay for all primes $\mathfrak{p}$.

Next, A satisfies **Serre's condition** (S$_d$) if $\mathrm{depth}(A_{\mathfrak{p}}) \geq \min(d, \dim(A_{\mathfrak{p}}))$ for all primes $\mathfrak{p}$. For $d = 1, 2$ this coincides with our previous definitions (we omit the details). If A is Cohen–Macaulay, then it satisfies (S$_d$) for all d.

Hence an easy way to verify these conditions is to know that A is Cohen–Macaulay. However, while the definition does not seem to be easy to check, there are stronger conditions that are sometimes easy to check, so we just list some of the relevant facts and end with some examples.

Theorem 8.6.1. *Let A be a Cohen–Macaulay ring. The following are true:*

1. *The polynomial ring $A[x]$ is Cohen–Macaulay.*
2. *If $x \in A$ is a nonzerodivisor, then $A/(x)$ is Cohen–Macaulay. In particular, if $x_1, \dots, x_r$ is a regular sequence, then $A/(x_1, \dots, x_r)$ is Cohen–Macaulay.*
3. *If A is local, its $\mathfrak{m}$-adic completion is Cohen–Macaulay.*
4. *Regular local rings are Cohen–Macaulay.*
5. *If $I \subset A$ is an ideal generated by c elements $x_1, \dots, x_c$ and $c = \dim A - \dim(A/I)$, then $x_1, \dots, x_c$ is a regular sequence.*

In particular, since a field $\mathbf{k}$ is automatically Cohen–Macaulay from the definition, so is the polynomial ring $\mathbf{k}[x_1, \dots, x_n]$. In this case, (5) has a nice implication (suppose $\mathbf{k}$ is algebraically closed): if $f_1, \dots, f_c$ are polynomials, then their common solution set has dimension $\geq n - c$ by the Krull principal ideal theorem, and in case of equality, these polynomials are automatically a regular sequence and $\mathbf{k}[x_1, \dots, x_n]/(f_1, \dots, f_c)$ is thus Cohen–Macaulay (and hence automatically satisfies all of Serre's conditions). This is an example of a **complete intersection**.

Example 8.6.2. If $f \in \mathbf{k}[x_1, \dots, x_n]$ is any nonzero polynomial, then it is a nonzerodivisor and hence $\mathbf{k}[x_1, \dots, x_n]/(f)$ is a Cohen–Macaulay ring. Hence we can use the discussion from Example 8.5.3 to determine if this ring is reduced or normal since Serre's conditions are automatically satisfied. □

Example 8.6.3. Let $\mathbf{k}$ be an algebraically closed field, n be a positive integer and consider the polynomial ring in n^2 variables $\mathbf{k}[x_{i,j} \mid 1 \leq i, j \leq n]$. Let φ be the $n \times n$ matrix whose (i, j) entry is $x_{i,j}$ and let I be the ideal generated by the coefficients of the characteristic polynomial of φ (with respect to some new variable t). An $n \times n$ matrix is nilpotent if and only if its characteristic polynomial is t^n. Hence each solution to the polynomials generating I corresponds to a nilpotent matrix with entries in $\mathbf{k}$. Is I a prime ideal?

There are various geometric arguments for why $V(I)$ is irreducible, we will omit this discussion since it is a bit beyond the scope of this course. We claim that I is generated by a regular sequence. First, it is generated by n polynomials. If we work modulo the ideal generated by $x_{i,j}$ for $i \neq j$, then they become elementary symmetric polynomials in the variables $x_{1,1}, \dots, x_{n,n}$ which we have seen in homework form a regular sequence. This implies the claim [why?] and so A/I is Cohen–Macaulay and satisfies all of Serre's conditions.

So then it suffices to show that there is a nilpotent matrix N such that the evaluation of the Jacobian matrix $\mathfrak{J}$ of I at N has rank n. We can take N to be a $n \times n$ Jordan block, i.e., $x_{i,j} = 0$ if $i \neq j - 1$ and $x_{i,i+1} = 1$ for $i = 1, \dots, n-1$. I'll leave that computation as an exercise, but once we have that we see that I is prime (although we didn't explain why $V(I)$ is irreducible).

Actually one can do better and show that A/I is also normal. To do that, we need to show that the solution set of the determinants of the $n \times n$ submatrices of $\mathfrak{J}$ inside $V(I)$ has dimension $\leq n^2 - n - 2$ (we actually get equality) which can also be done with some geometric arguments that we omit. □

There are many other general constructions which result in Cohen–Macaulay rings, but hopefully this gives a small flavor of the kinds of computations that are involved in using the theorems of this section.

8.7. **Fractional ideals.**

References

[Ei] David Eisenbud, *Commutative Algebra with a view toward algbraic geometry*