Commutative Algebra *

Artie Khovanov

Compiled on May 26, 2023

These are some notes for the Cambridge Mathematical Tripos Part III course *Commutative Algebra* in Michaelmas 2022. This is NOT a verbatim copy of the lectured material: I've edited the content to help me understand it. As a result, any errors are mine alone.

I'm actively maintaining these notes. If you want to report typos or mistakes, please email aik31@cam.ac.uk or message me on Discord at `FM22#2007`.

Contents

*Based on the lectures under the same name taught by Dr O. Becker in Michaelmas 2022.

1 Introduction

In this course, a **ring** R is commutative and unital (unless otherwise stated).

Commutative algebra is the basis for algebraic geometry and algebraic number theory. The course will focus on motivation from algebraic geometry.

Let k be a field, and consider the ring $A = k[T_1, \ldots, T_n]$ of polynomials in n variables over k. By convention, uppercase letters will represent indeterminates, and lowercase letters will represent specific values.

Consider $S \subseteq A$. Its **zero locus** in k^n is

$$\mathbb{V}(S) = \{(x_1, \ldots, x_n) \in k^n \mid f(x_1, \ldots, x_n) = 0; \forall f \in S\}.$$

We say $X \subseteq k^n$ is **algebraic** if $X = \mathbb{V}(S)$ for some $S \subseteq A$.

Let $I = (S)$ be the **ideal generated by** S. This is the intersection of all ideals of A containing S, or equivalently the set of linear combinations of elements of S with coefficients in A. Note that $\mathbb{V}(I) = \mathbb{V}(S)$.

We wish to study how the algebraic properties of ideals correspond to geometric properties of algebraic sets, such as dimension, reducibility and local structure. We focus on the geometry itself in III Algebraic Geometry, but here we use it as motivation for studying the algebra.

2 Finitely-generated algebras

Consider, as usual, $A = k[T_1 \ldots, T_n]$, $S \subseteq A$ and $X = \mathbb{V}(S)$; let $\mathcal{I}(X)$ be the ideal of functions vanishing on X. We want to understand $\mathcal{I}(X)$ in terms of S, and study the *coordinate ring* $k[X] = k[T_1, \ldots, T_n]/\mathcal{I}(X)$. Such rings are (nilpotent-free) examples of *finitely-generated k-algebras*, objects which generalise polynomial rings by allowing relations between the generators.

2.1 Noetherian rings and Hilbert's basis theorem

Is there a *finite* set $S_0 \subseteq A$ with $\mathbb{V}(S_0) = \mathbb{V}(S)$? The answer is in fact yes! This is a consequence of Hilbert's basis theorem, which we will meet in a moment.

Definition 2.1. A ring A is **Noetherian** if it satisfies the following equivalent conditions:

1. Every ideal of A is finitely generated.
2. Every ascending chain $A_1 \subseteq A_2 \subseteq \ldots$ of ideals of A stabilises; that is, the chain is eventually constant. This is known as the **ascending chain condition** (ACC).
3. Every nonempty set Σ of ideals of A has a maximal element (with respect to inclusion).

Examples 2.2.

1. All fields are Noetherian since their only ideals are (0) and (1).
2. All PIDs are Noetherian by definition.
3. $k[T_1, T_2, \dots]$ is *not* Noetherian as $(T_1) \subsetneq (T_1, T_2) \subsetneq \dots$ is a nonterminating ascending chain.

Recall that we can view a B-module M as an abelian group along with a ring homomorphism $\varphi : B \to \operatorname{End} M$, where $\operatorname{End} M$ is the ring of group homomorphisms (with multiplication being composition). Scalar multiplication is then given by $bm \coloneqq \varphi(b)(m)$. We define algebras in a similar way.

Definition 2.3. Given a ring B, a (unital associative commutative) **B-algebra** is a ring A along with a ring homomorphism $\theta : B \to A$ called the **structure homomorphism**; scalar multiplication is given by $ba = \theta(b)a$.

A is then also a B-module, with $\varphi(b)(a) = \theta(b)a$.

For example, $k[T_1, \dots, T_n]$ is a k-algebra via the inclusion $\theta(x) = x = xT_1^0 \dots T_n^0$. This is then also a k-vector space.

Definition 2.4. A is **finitely generated** (as an algebra) over B if A is the set of polynomials over B in some finite generating set $\{a_1 \dots, a_n\} \subseteq A$, that is, if

$$A = \operatorname{span}_B\{a_1^{e_1}, \dots a_n^{e_n} \mid e_i \geq 0\}.$$

Equivalently, A is finitely generated over B if it is isomorphic to a quotient of some polynomial ring $B[T_1, \dots, T_n]$.

Theorem 2.5 (Hilbert's Basis Theorem)**.** *Let B be a Noetherian ring. Then every finitely generated B-algebra is Noetherian.*

Proof. Since a quotient of a Noetherian ring is itself Noetherian, it suffices to show that $B[T_1, \dots, T_n]$ is Noetherian. Since $B[T_1, \dots, T_n] \cong B[T_1, \dots, T_{n-1}][T_n]$ are isomorphic as B-algebras, it suffices (by induction) to show that $B[T]$ is Noetherian.

Indeed, let $\mathfrak{a} \trianglelefteq B[T]$. For $i \in \mathbb{N}$, define

$$\mathfrak{a}_i = \{c_0 \in B \mid \exists c_1, \dots, c_i \in B \text{ where } c_0T^i + \dots + c_iT^0 \in \mathfrak{a}\}.$$

This is the ideal of leading coefficients of degree-i polynomials in $\mathfrak{a}$ (along with 0). We will construct a finitely generated ideal $\mathfrak{b}$ with $\mathfrak{b}_i = \mathfrak{a}_i$ for all i.

Since B is Noetherian, the chain $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \dots$ stabilises at $m \in \mathbb{N}$, and each term is finitely generated; write $\mathfrak{a}_i = (a_{i,1}, \dots, a_{i,n_i})$. For $0 \leq i \leq m$, find $f_{i,j} \in \mathfrak{a}$ such that $f_{i,j} = a_{i,j}T^i + \dots$, and take $\mathfrak{b}$ to be the ideal generated by the (finitely many) $f_{i,j}$. By construction, $\mathfrak{b} \subseteq \mathfrak{a}$ is a finitely generated ideal with $\mathfrak{b}_i = \mathfrak{a}_i$ for all i.

If $\mathfrak{b} \subsetneq \mathfrak{a}$, take a minimal-degree polynomial f in the complement. By construction, there exists some $g \in \mathfrak{b}$ with the same degree and leading coefficient as f; then $f - g \in \mathfrak{a}$ has strictly smaller degree than f, so $f - g \in \mathfrak{b}$. But then $f = (f - g) + g \in \mathfrak{b}$.$_\#$ □

2.2 Integral algebras and Noether's normalisation theorem

Noether's normalisation theorem classifies finitely-generated algebras. Geometrically, it says the following. Let $X \subseteq k^n$ be an algebraic set. Then $\exists d \geq 0$ and a surjective polynomial map $f : X \to k^d$ which has all fibres finite, that is,

$$0 < |f^{-1}(y)| < \infty \text{ for every } y \in k^d.$$

The value d will turn out to be the *dimension* of X.

Definition 2.6. Let A be a B-algebra. Then A is **finite** over B if A is finitely generated as a B-module, that is, if $A = \mathrm{span}_B\{a_1, \ldots, a_m\}$.

Examples 2.7.

1. Let L/K be a finite field extension. Then L is a finite K-algebra.
2. Consider $A = k[T, T^{-1}] = \{\sum_{i=-a}^{b} c_i T^i \mid a, b \geq 0;\ c_i \in k\}$. This is (in particular) a k-algebra, a $k[T]$-algebra, and a $k[T - T^{-1}]$-algebra.

   Now, A is not finite as a k-algebra, or even as a $k[T]$-algebra, since any finite subset S has a lower bound on the powers of T that appear in it, but scalar multiplication by $k[T]$ can only increase the power of T.

   However, A *is* finite over $k[T-T^{-1}]$. This is because $T^2 = (T-T^{-1})T+1$ and $T^{-1} = T + (T - T^{-1})$, so in fact A is generated by $\{1, T\}$ over this ring.

Theorem 2.8 (Noether's normalisation theorem)**.** *Let A be a finitely generated algebra over a field k. Then there is a subalgebra $A' \subseteq A$ such that $A' \cong k[T_1, \ldots, T_d]$ for some $d \geq 0$ and A is finite over A'.*

In order to prove this theorem, we need to develop the theory of *integral* algebras.

Definition 2.9. Let A be a B-algebra. An element $x \in A$ is **integral over** B if x is the root of a monic polynomial over B. Then A itself is an **integral** B-algebra if all its elements are integral over B.

Lemma 2.10. *Let C be an $n \times n$ matrix over a ring A. Suppose $v \in A^n$ has $Cv = 0$. Then $(detC)v = 0$.*

Note that rings can have zero divisors, so this lemma is nontrivial.

For $u \in A^n$ and $C \in \mathcal{M}_n(A)$, write $C_j^{(u)}$ for C with the jth column replaced by u.

Proof of Lemma 2.10. Have $\det C_j^{(Cv)} = C_j^{(0)} = 0$. Then $Cv = \sum_{l=1}^{n} \mathrm{col}_l(C) \cdot v_l$, so

$$0 = \det C_j^{(Cv)} = \sum_{l=1}^{n} \det C_j^{(\mathrm{col}_l(c))} \cdot v_l = \det C_j^{(\mathrm{col}_j(c))} \cdot v_j = \det C \cdot v_j,$$

where the other terms vanish as they have two identical columns. □

For the next proposition, we need the following notion:

Definition 2.11. A B-module A is **faithful** if the only element $b \in B$ satisfying $ba = 0$ for all $a \in A$ is 0.

Proposition 2.12. *Let A be a B-algebra. TFAE:*

1. *A is a finitely generated integral B-algebra.*
2. *A is generated (as a B-algebra) by a finite set of integral elements.*
3. *A is finite over B*

Proof.
1 $\implies$ 2: Clear

2 $\implies$ 3: Let $\alpha_1, \ldots, \alpha_n \in A$ be integral generators over B. Then there are some $n_i \geq 0$ and $b_i, j \in B$ such that

$$\alpha_i^{n_i} + b_{i,1}\alpha_i^{n_i-1} + \cdots + b_{i,n_i}\alpha_i^0 = 0,$$

so, moving the lower-order terms to the other side, have

$$\alpha_i^{n_i} \in \operatorname{span}_B\{\alpha_i^0, \ldots, \alpha_i^{n_i-1}\}.$$

Done by induction.

3 $\implies$ 1: A is finitely generated as a B-module, so it is finitely generated as a B-algebra by the same generators. Fix $\alpha \in A$; it remains to show α is integral over B.

Indeed, let $\varphi : B \to A$ be the structure homomorphism, and consider the subring $\varphi(B)[\alpha] \leq A$. Now, A is a finitely-generated B-module, and it is faithful (over $\varphi(B)[\alpha]$) since $1 \in A$. This immediately implies α is integral over B by the following lemma. □

Lemma 2.13. *Let $B \leq A$ be rings. Then $x \in A$ is integral over B iff there is a $B[x]$-submodule M of A such that*

(i) M is faithful over $B[x]$.

(ii) M is finitely generated over B

Proof. Suppose (i) and (ii) hold. By (ii), $M = \operatorname{span}_B\{e_1, \ldots, e_n\}$ for $n \geq 0$ and some $e_i \in A$. Write $\mathbf{e} = (e_1, \ldots, e_n)^\top$.

Since $xe_i \in \operatorname{span}_B\{e_1, \ldots, e_n\}$, have $x\mathbf{e} = C\mathbf{e}$ for some matrix $C \in \mathcal{M}_n(B)$. Then $(xI - C)\mathbf{e} = 0$, so, by the previous lemma, $\det(xI - C)e_i = 0$ for each i. Since the e_i generate M, $\det(xI - C) \in B[x]$ annihilates all of M; since M is faithful, in fact $\det(xI - C) = 0$. But this determinant is a monic polynomial in x with coefficients in B, so in fact x is integral over B.

Conversely, suppose $x \in A$ is integral over B. If x satisfies a monic degree-n polynomial, then $M = B[x] = \operatorname{span}_B\{1, x, \ldots, x^{n-1}\}$ easily satisfies (i) and (ii), since $1 \in M$. □

Definition 2.14. Let A be an algebra over a field k. The elements $x_1, \ldots, x_n \in A$ are **algebraically independent** if the only polynomial $p \in k[T_1, \ldots, T_n]$ with $p(x_1, \ldots, x_n) = 0$ is the zero polynomial.

Equivalently, the x_i are independent if the k-algebra homomorphism $k[T_1, \ldots, T_n] \to A$ given by evaluation at the x_i is injective.

This definition allows us to restate Noether's normalisation theorem:

Theorem 2.15 (Noether's Normalisation Theorem, second version)**.**
Let A be a finitely generated algebra over a field k. Then there exist elements $x_1, \ldots, x_n \in A$ ($n \geq 0$), algebraically independent over k, such that A is finite over $A' = k[x_1, \ldots, x_n]$.

We will first demonstrate the proof method with an example.

Example 2.16. Let $A = k[T, T^{-1}]$. We want to prove the theorem in this case.

$\{T, T^{-1}\}$ are not algebraically independent: have the relation $T \cdot T^{-1} - 1 = 0$. Write $A = k[T^{-1} - cT, T]$; then, using the previous relation, get

$$0 = ((T^{-1} - cT) + cT) \cdot T - 1 = cT^2 + (T^{-1} - cT) \cdot T - 1.$$

Dividing out by c, have that T is integral over $k[T - cT^{-1}]$ for $c \neq 0$. Thus, by the previous proposition, $A = k[T^{-1} - cT][T]$ is finite over $k[T^{-1} - cT]$.

We prove the theorem only in the case where k is infinite.

Proof of Noether's Normalisation Theorem. Proceed by induction on the (minimal) size m of a generating set for A as a k-algebra.

If $m = 0$, then $A = k$, so take $A' = A = k$.

Now suppose that $\{x_1, \ldots, x_m\}$ generate A as a k-algebra. If the x_i are algebraically independent over k, then we are done: again set $A' = A$. Otherwise:

Claim: There exist $c_1, \ldots c_{m-1} \in k$ such that x_m is integral over

$$B = k[x_1 - c_1 x_m, \ldots, x_{m-1} - c_{m-1} x_m],$$

which is generated by $m - 1$ elements.

By the previous proposition, A is finite over B. By induction, take algebraically independent elements $z_1, \ldots, z_d \in B$ such that B is finite over $A' = k[z_1, \ldots, z_d]$. By transitivity of finiteness, A is then finite over A', proving the theorem.

It remains to prove the claim. In fact, almost every choice of constants c_i works!

Indeed, let $p \in k[T_1, \ldots, T_m]$ be a nontrivial relation between the x_i. Let P be the highest-degree homogeneous component of p; for scalars $\mathbf{c} = (c_1, \ldots, c_{m-1})$ with $c_i \in k$, have

$$\begin{aligned} g(T_1, \ldots, T_m) &\coloneqq p(T_1 + x_1 T_m, \ldots, T_{m-1} + x_{m-1} T_{m-1}, T_m) \\ &= P(\mathbf{c}, 1) T_m^r + \ldots \\ &\coloneqq Q(\mathbf{c}) T_m^r + \ldots, \end{aligned}$$

expanding in powers of T_m. Then

$$g(x_1 - c_1 x_m, \ldots, x_{m-1} - c_{m-1} x_m, x_m) = p(x_1, \ldots, x_m) = 0.$$

If the leading coefficient $Q(\mathbf{c})$ is nonzero, then we can divide out by it to get a monic polynomial over B vanishing at x_m, proving the claim. Explicitly, the polynomial is

$$\frac{1}{Q(\mathbf{c})} \cdot g(x_1 - c_1 x_m, \ldots, x_{m-1} - c_{m-1} x_m, T_m) = T_m^r + \cdots \in B[T_m]$$

It remains to find c_i such that $Q(\mathbf{c}) \neq 0$. Now, $Q \in k[T_1, \ldots, T_{m-1}]$ is nonzero: expanding P in powers of T_m, every coefficient must have a different degree as P is homogeneous. Since k is infinite, and a nonzero univariate polynomial has only finitely many roots, there are in fact infinitely many non-roots of Q (by induction on m). □

In fact, we can show that there is a matrix

$$Q = \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in \mathcal{M}_n(k)$$

satisfying $\mathbf{y} = Q\mathbf{x}$, such that, for some $r \leq m$, the entries $y_1, \ldots, y_r$ are algebraically independent and A is finite over $k[y_1, \ldots, y_r]$. Indeed, almost all matrices work – the condition is that the entries fail to solve a certain polynomial. This approach works in the case where k is finite, too, but the proof is omitted here.

2.3 Hilbert's Nullstellensatz

Let k be a field. We have a bijection

$$\begin{aligned} k^n &\xleftrightarrow{\simeq} \mathrm{Hom}_{k\text{-alg}}(k[T_1, \ldots, T_n], k) \\ \mathbf{x} = (x_1, \ldots, x_n) &\longrightarrow \mathrm{ev}_{\mathbf{x}} \\ \mathbf{x}_f(f(T_1), \ldots, f(T_n)) &\longleftarrow f \end{aligned}$$

taking the kernel, we get

$$\begin{aligned} \mathrm{Hom}_{k\text{-alg}}(k[T_1, \ldots, T_n], k) &\xrightarrow{\ker} \mathrm{Id}(k[T_1, \ldots, T_n]) \\ \mathrm{ev}_{\mathbf{x}} &\xrightarrow{\ker} (T_1 - x_1, \ldots, T_n - x_n) \end{aligned}$$

where Id is the set of ideals. Indeed, given $f \in k[T_1, \ldots, T_n]$, linearly change variables to $(T_1 - x_1, \ldots, T_n - x_n)$, and observe that the constant term vanishes exactly when $f(\mathbf{x})$ does.

Taking mSpec to be the set of maximal ideals, the composition of the two maps above gives a map

$$\begin{aligned} k^n &\xrightarrow{\ker \mathrm{ev}_{\mathbf{x}}} \mathrm{mSpec}\, k[T_1, \ldots, T_n] \\ \mathbf{x} &\longrightarrow (T_1 - x_1, \ldots, T_n - x_n). \end{aligned}$$

Since these maximal ideals are determined by the single point at which they vanish, this map is injective. This map is not in general surjective: over $\mathbb{R}$,

(T^2+1) is a maximal ideal (adjoining a root gives the field $\mathbb{C}$) that does not have the form $(T-x)$. When k is algebraically closed, however, this map *is* surjective, giving a bijection

$$k^n \xleftrightarrow[\ker \mathrm{ev}_{\mathbf{x}}]{\simeq} \mathrm{mSpec}\, k[T_1, \ldots, T_n].$$

This is the content of the (weak) Nullstellensatz.

Consider the vanishing set map $\mathbb{V} : \mathcal{P}(k[T_1, \ldots, T_n]) \to \{\text{algebraic subsets of } k^n\}$. On mSpec, $\mathbb{V}$ is injective, and its image is the set of singletons. On Id, $\mathbb{V}$ is surjective, but fails to be injective: for example, $\mathbb{V}(T) = \mathbb{V}(T^2) = \{0\}$. However, we do have a right inverse to $\mathbb{V}$, given by

$$\begin{aligned} \{\text{algebraic subsets of } k^n\} &\xrightarrow{\mathcal{I}} \mathrm{Id}\, k[T_1, \ldots, T_n] \\ X &\longrightarrow \{f \in k[T_1, \ldots, T_n] \mid f(x) = 0\ \forall x \in X\} \end{aligned}$$

Clearly, $\mathbb{V} \circ \mathcal{I} = \mathrm{Id}$. We also have $\mathcal{I}(\mathbb{V}(\mathfrak{a})) \supseteq \mathfrak{a}$, but we do not have the reverse inclusion as $\mathbb{V}$ is not injective.

Indeed, let's consider our earlier example of non-injectivity. We have $\mathcal{I}(\mathbb{V}(T)) = T$, but also $\mathcal{I}(\mathbb{V}(T^2)) = T$. It looks like $I \circ \mathbb{V}$ is "taking the root".

Definition 2.17. Let $I \trianglelefteq R$ be an ideal. Define its **radical** by $\sqrt{I} = \{x \in R \mid x^k \in I \text{ for some } k \in \mathbb{N}\}$. If $I = \sqrt{I}$, I is called a **radical ideal**.

Lemma 2.18.

(i) $\sqrt{\sqrt{I}} = \sqrt{I}$

(ii) Let k be a field, and let $\mathfrak{a} \trianglelefteq k[T_1, \ldots, T_n]$. Then $\mathbb{V}(\sqrt{\mathfrak{a}}) = \mathbb{V}(\mathfrak{a})$.

Proof.

(i) If $x \in \sqrt{\sqrt{I}}$, then $x^k \in \sqrt{I}$ for some $k \in \mathbb{N}$, so $x^{kl} \in I$ for some $l \in \mathbb{N}$. Hence $x \in \sqrt{I}$. The other inclusion is trivial.

(ii) Suppose $x \in \mathbb{V}(\mathfrak{a})$, and fix $h \in \sqrt{\mathfrak{a}}$. Then $h^k(x) = 0$ for some $k \in \mathbb{N}$; since $k[T_1, \ldots, T_n]$ is an integral domain, $h(x) = 0$. Hence $x \in \mathbb{V}(\sqrt{\mathfrak{a}})$. Again, the other inclusion is trivial.

□

The strong Nullstellensatz then says that, when k is algebraically closed, we really do have $\mathcal{I}(\mathbb{V}(\mathfrak{a})) = \sqrt{\mathfrak{a}}$. This yields a bijection

$$\{\text{algebraic subsets of } k^n\} \xleftrightarrow[\mathbb{V};\mathcal{I}]{\simeq} \{\text{radical ideals of } k[T_1, \ldots, T_n]\}.$$

We now turn to proving the weak and strong NSS.

Lemma 2.19. *Let $A \leq B$ be rings, and suppose B is integral over A.*

(i) $A \cap B^\times = A^\times$.

(ii) Suppose B is an integral domain. Then A is a field iff B is a field.

Note that, if B is a field, then it is in particular an integral domain.

Proof.

(i) Clearly, $A^\times \subseteq A \cap B^\times$. Conversely, suppose $a \in A \cap B^\times$ has inverse $b \in B$. Then there are constants $c_1, \ldots, c_n \in A$ such that

$$b^n + c_1 b^{n-1} + \cdots + c_n b^0 = 0.$$

Multiplying by a^{n-1}, get

$$b + \underbrace{c_1 + c_2 a + \cdots + c_n a^{n-1}}_{\in A} = 0,$$

so in fact $b \in A$.

(ii) $\Leftarrow$: Have $B^\times = B \setminus \{0\}$. By (i), $A^\times = A \cap B^\times = A \cap B \setminus \{0\} = A \setminus \{0\}$.

$\Rightarrow$: Suppose A is a field, and take $b \in B \setminus \{0\}$. Again find $a_1, \ldots, c_n \in A$ (with n minimal) such that

$$b^n + c_1 b^{n-1} + \cdots + c_n b^0 = 0;$$

then

$$b \underbrace{(b^{n-1} + c_1 b^{n-2} + \cdots + c_{n-1})}_{\Delta} = -c_n.$$

By minimality of n, $\Delta \neq 0$; since B is an integral domain, $-c_n \neq 0$. Dividing through by $-c_n$, then, we find an inverse for b.

□

Proposition 2.20 (Zariski's Lemma)**.** *Let $k \subseteq L$ be fields, and suppose L is finitely generated as a k-algebra. Then L is finite over k.*

A more useful restatement is that, if a finitely generated algebra L over a field k happens to itself be a field, then L is finite over k.

Proof. By Noether's normalisation theorem, find algebraically independent variables $y_1, \ldots, y_d \in L$ ($d \geq 0$) such that L is integral, and therefore finite, over $B = k[y_1, \ldots, y_d]$.

Since L is a field, by (ii) of the previous lemma B must also be a field. Since polynomial rings in $d \geq 1$ variables are not fields (T_1 has no inverse), in fact $d = 0$, that is, $B = k$. □

Let $p \in k[T]$. If we want a finite field extension L/k containing a root of p, we set $L = k[X]/(g)$, where g is an irreducible factor of p. More abstractly, all we need is that (g) is a maximal ideal containing (p); then the image of the indeterminate X still solves p over L.

Now let $\mathfrak{a} \trianglelefteq k[T_1, \ldots, T_n]$. We want a finite extension L of k containing a simultaneous solution of all polynomials in $\mathfrak{a}$. Analogously, we can take a maximal ideal $\mathfrak{m} \supseteq \mathfrak{a}$, and set $L = k[T_1, \ldots, T_n]/\mathfrak{m}$. By Zariski's lemma, this turns out to work!

Theorem 2.21 (Weak Nullstellensatz)**.** *Let k be a field, and $\mathfrak{a}$ a proper ideal of $k[T_1, \dots, T_n]$. Then there is a finite extension L/k and a point $\mathbf{x} \in L$ such that $f(\mathbf{x}) = 0$ for all $f \in \mathfrak{a}$.*

In particular, if k is algebraically closed, then the only ideal with empty vanishing set is $k[T_1, \dots, T_n]$.

Proof. Since $k[T_1, \dots, T_n]$ is Noetherian, take a maximal ideal $\mathfrak{m} \supseteq \mathfrak{a}$, and set

$$L = \frac{k[T_1, \dots, T_n]}{\mathfrak{m}}.$$

Then L is finitely generated as a k-algebra by the $T_i + \mathfrak{m}$, so, by Zariski's lemma, L/k is finite. Then set $\bar{\mathbf{x}} = (T_1 + \mathfrak{m}, \dots, T_n + \mathfrak{m})$; for $f \in \mathfrak{m}$, have

$$f(\overline{\mathfrak{m}}) = \underbrace{f(T_1, \dots, T_m)}_{\in \mathfrak{a} \subseteq \mathfrak{m}} + \mathfrak{m} = 0 + \mathfrak{m}.$$

□

Here is another way to view the weak NSS. Let $p_1, \dots, p_m \in k[T_1, \dots, T_m]$. If there are $r_1, \dots, r_m \in k[T_1, \dots, T_m]$ such that

$$\sum_i r_i p_i = 1, \tag{$\star$}$$

then the p_i clearly have no common solution in any extension of k. The weak NSS shows the converse for finitely generated extensions: condition ($\star$) is the only obstruction to the existence of such a solution. Indeed, if ($\star$) is not satisfied, then (p_i) is a proper ideal.

We can, in fact, compute the r_i (if they exist) for fixed p_i. Indeed, we have the following result.

Theorem 2.22 (Effective Nullstellensatz)**.** *If there are no r_i with*

$$\deg(r_i) \leq (\max\{3, \deg p_1, \dots, \deg p_m\})^n$$

satisfying ($\star$), then there are no r_i satisfying ($\star$) at all.

Proof. Omitted. □

Now, the coefficients of $\sum_i r_i p_i$ are linear combinations of the coefficients of the r_i. By the degree bound, we can check if ($\star$) has a solution, and find one if it exists, using Gaussian elimination.

Corollary 2.23 (Corollary of weak NSS)**.** *Suppose further that k is algebraically closed. Then the map*

$$\begin{aligned} k^n &\xrightarrow{\ker \mathrm{ev}_{\mathbf{x}}} \mathrm{mSpec}\, k[T_1, \dots, T_n] \\ \mathbf{x} &\longrightarrow (T_1 - x_1, \dots, T_n - x_n). \end{aligned}$$

is a bijection.

Proof. We remarked earlier that this map is injective. To show surjectivity, fix a maximal ideal $\mathfrak{m}$. By the weak NSS, find $\mathbf{x} \in k^n$ with $f(\mathbf{x}) = 0$ for all $f \in \mathfrak{m}$. Then

$$\mathfrak{m} \subseteq \ker \mathrm{ev}_{\mathbf{x}} = (T_1 - x_1, \ldots, T_n - x_n);$$

by maximality, $\mathfrak{m} = \ker \mathrm{ev}_{\mathbf{x}}$. □

Theorem 2.24 (Strong Nullstellensatz)**.** *Let k be a field, k^{al} its algebraic closure, and $\mathfrak{a} \trianglelefteq k[T_1, \ldots, T_n]$. Define*

$$\mathbb{V}_{al}(\mathfrak{a}) = \{\mathbf{x} \in (k^{al})^n \mid f(\mathbf{x}) = 0 \; \forall x \in \mathfrak{a}\}.$$

Then $\mathcal{I}(\mathbb{V}_{al}(\mathfrak{a})) = \sqrt{\mathfrak{a}}$.

Proof. For any $X \subseteq k^n$, we have that $\mathcal{I}(X)$ is radical: if $h^n(x) = 0$, then $h(x) = 0$. Now, we have $\mathcal{I}(\mathbb{V}_{\mathrm{al}}(\mathfrak{a})) \supseteq \mathfrak{a}$, and the LHS is radical, so in fact $\mathcal{I}(\mathbb{V}_{\mathrm{al}}(\mathfrak{a})) \supseteq \sqrt{\mathfrak{a}}$.

For the reverse inclusion, fix $h \in \mathcal{I}(\mathbb{V}_{\mathrm{al}}(\mathfrak{a}))$. If $h = 0$, then certainly $h \in \sqrt{\mathfrak{a}}$. Suppose $h \neq 0$; we want to show that $h^l \in \mathfrak{a}$ for some $l \in \mathbb{N}$. By Hilbert's basis theorem, we have $\mathfrak{a} = (g_1, \ldots, g_m)$. Consider the ideal

$$\mathfrak{b} = (g_1, \ldots, g_m, 1 - Y \cdot h) \trianglelefteq k[T_1, \ldots, T_n, Y].$$

Claim: $\mathbb{V}_{\mathrm{al}}(\mathfrak{b}) = \emptyset$.

Indeed, suppose $(x_1, \ldots, x_n, t)$ solves the g_i and $1 - Y \cdot h$. Then $\mathbf{x} \in \mathbb{V}_{\mathrm{al}}(\mathfrak{a})$, and, $h \in \mathfrak{a}$, so $h(\mathbf{x}) = 0$. But then $1 - t \cdot h(\mathbf{x}) = 1 \neq 0$.#

By the weak NSS, $\mathfrak{b} = k[T_1, \ldots, T_n, Y] \ni 1$. Find $r_i \in k[T_1, \ldots, T_n, Y]$ such that

$$(\star) \quad \sum_i r_i g_i + r_{m+1}(1 - Yh) = 1,$$

and consider the map

$$\begin{aligned} k[T_1, \ldots, T_n] &\to k(T_1, \ldots, T_n) \\ T_i &\to T_i \\ Y &\to h^{-1} \text{ (as } h \neq 0) \end{aligned}$$

Applying this map to $(\star)$, we get

$$1 = \sum_i r_i(T_1, \ldots, T_n, h^{-1}) \cdot g_i.$$

For large enough l, we have that each $h^l \cdot r_i(T_1, \ldots, T_n, h^{-1})$ is, in fact, a polynomial. Thus

$$h^l = \sum_i \underbrace{h^l r_i(T_1, \ldots, T_n, h^{-1})}_{\in k[T_1, \ldots, T_n]} \cdot \underbrace{g_i}_{\mathfrak{a}} \in \mathfrak{a}.$$

Hence $h \in \sqrt{\mathfrak{a}}$. □

This proof is known as the *Rabinowitsch trick*; it is an example of *localisation*, which we will meet later.

By the correspondence theorem, the bijection descends to coordinate rings:

$$\{\text{algebraic subsets of } \mathbb{V}(\mathfrak{c})\} \underset{\mathbb{V};\mathcal{I}}{\overset{\simeq}{\longleftrightarrow}} \{\text{radical ideals of } k[T_1,\dots,T_n]/\mathfrak{c}\}.$$

This is because radicality is preserved by correspondence.

2.4 The Zariski topology

Definition 2.25. Let k be a field. The **Zariski topology** on k^n is the topology whose closed sets are the algebraic subsets $\mathbb{V}(\mathfrak{a})$ of k^n. Call k^n equipped with this topology **n-dimensional affine space** $\mathbb{A}^n_k$ (or just $\mathbb{A}^n$).

The Zariski topology is indeed a topology:

- $k^n = \mathbb{V}((0))$ and $\emptyset = \mathbb{V}((1))$.
- $\mathbb{V}(\mathfrak{a}) \cup \mathbb{V}(\mathfrak{b}) = \mathbb{V}(\mathfrak{a} \cap \mathfrak{b}) = \mathbb{V}(\mathfrak{a}\mathfrak{b})$.

  Indeed, if $\mathbf{x} \notin \mathbb{V}(\mathfrak{a}) \cup \mathbb{V}(\mathfrak{b})$, then there are $f \in \mathfrak{a}$ and $g \in \mathfrak{b}$ with $f(\mathbf{x}), g(\mathbf{x}) \neq 0$. Then $fg \in \mathfrak{a}\mathfrak{b}$, but $fg(\mathbf{x}) \neq 0$, so $\mathbf{x} \notin \mathbb{V}(\mathfrak{a}\mathfrak{b})$. The reverse inclusions are trivial.
- $\bigcap_{i\in I} \mathbb{V}(\mathfrak{a}_i) = \mathbb{V}(\sum_{i\in I} \mathfrak{a}_i)$ essentially by definition.

For $f \in k[T_1,\dots,T_n]$, write $D(f) = \{\mathbf{x} \in \mathbb{A}^n_k \mid f(\mathbf{x}) \neq 0\}$. The sets $D(f)$ form a basis for the Zariski topology.

Note that $\mathbb{A}^n_k$ is only Hausdorff if $n = 0$ or k is finite. Indeed, let U and V be nonempty open sets in $\mathbb{A}^n_k$; find $f \in U$ and $g \in V$. If k is infinite and $n > 0$, then $D(fg)$ is nonempty. Since $D(fg) \subseteq U \cap V$, U meets V.

Definition 2.26. A (nonempty) topological space X is **irreducible** if it cannot be written $X = X_1 \cup X_2$, where the X_i are closed proper subsets.

Equivalently, X is irreducible iff every pair of nonempty open subsets of X intersects.

Examples 2.27.

1. A Hausdorff space is irreducible only if it is a singleton.
2. $\mathbb{A}^n_k$ is irreducible for infinite k and $n > 0$.
3. Suppose k is algebraically closed, and take irreducible polynomials $p, q \in k[T_1,\dots,T_n]$ with $(p) \neq (q)$ (in particular, $(p) \not\subseteq (q)$). Since (p) and (q) are prime and therefore radical, $\mathbb{V}((q)) \not\subseteq \mathbb{V}((p))$ by the strong NSS. By the same reasoning, $\mathbb{V}((p)) \not\subseteq \mathbb{V}((q))$. Then $\mathbb{V}((pq)) = \mathbb{V}((p)) \cup \mathbb{V}((q))$ is not irreducible.

We can in fact check whether $\mathbb{V}(\mathfrak{a})$ is irreducible algebraically.

Indeed, recall that an ideal $I \trianglelefteq R$ is prime iff R/I is an integral domain, and that, for ideals, maximal implies prime. We also have that I is radical iff R/I is **reduced** (that is, its only nilpotent is 0), and that prime implies radical.

Lemma 2.28. *Let $\mathfrak{p} \trianglelefteq R$ be prime. If $I \cap J \subseteq \mathfrak{p}$ for some $I, J \trianglelefteq R$, then either $I \subseteq \mathfrak{p}$ or $J \subseteq \mathfrak{p}$.*

Proof. Assume not; take $f \in I \setminus \mathfrak{p}$ and $g \in J \setminus \mathfrak{p}$. Then $fg \in I \cap J \subseteq \mathfrak{p}$, so either $f \in \mathfrak{p}$ or $g \in \mathfrak{p}$ by primality.$_{\#}$ □

Proposition 2.29. *An algebraic set $X \subset \mathbb{A}^n_k$ is irreducible iff $\mathcal{I}(X) \trianglelefteq k[T_1, \ldots, T_n]$ is prime.*

Proof. Suppose X is irreducible, and take polynomials $f, g \in k[T_1, \ldots, T_n]$ with $fg \in \mathcal{I}(X)$. Then $X \subseteq \mathbb{V}(fg) = \mathbb{V}(f) \cup \mathbb{V}(g)$. By irreducibility, suppose (wlog) that $X \subseteq \mathbb{V}(f)$; then $f \in \mathcal{I}(X)$. Hence $\mathcal{I}(X)$ is prime.

Conversely, suppose that $\mathcal{I}(X)$ is prime and that $X = \mathbb{V}(I) \cup \mathbb{V}(J) = \mathbb{V}(IJ)$. Then $IJ \subseteq \mathcal{I}(X)$, so, by the previous lemma, suppose wlog that $I \subseteq \mathcal{I}(X)$. Then $X \subseteq \mathbb{V}(I)$, so $X = \mathbb{V}(I)$. □

When k is algebraically closed, we have by the strong NSS that $\mathbb{V}(\mathfrak{a})$ is irreducible iff $\sqrt{\mathfrak{a}}$ is prime. This can fail if k is not algebraically closed.

Example 2.30. Consider the real polynomial $p(T_1, T_2) = T_1^2 + T_2(T_2 - 1) \in \mathbb{R}[T_1, T_2]$. Then p is irreducible (in fact, it is irreducible over $\mathbb{C}$) by Gauss' lemma, so we certainly have that $\sqrt{(p)} = (p)$ is prime. However, $\mathbb{V}((p))$ consists of the two points $(0, 0)$ and $(0, 1)$, and is therefore irreducible.

We want to view the Zariski topology algebraically. First, assume k is algebraically closed, and recall that the weak NSS gives a bijection

$$\begin{aligned} k^n &\xleftrightarrow{\simeq} \operatorname{mSpec} k[T_1, \ldots, T_n] \\ \mathbf{x} &\longrightarrow (T_1 - x_1, \ldots, T_n - x_n). \end{aligned}$$

Pulling the Zariski topology through this bijection, the closed subsets of $\operatorname{mSpec} k[T_1, \ldots, T_n]$ are (exactly) those of the form $\{\mathfrak{m} \mid \mathfrak{a} \subseteq \mathfrak{m}\}$ for some $\mathfrak{a} \trianglelefteq k[T_1, \ldots, T_n]$.

We can generalise this to define a topology on $\operatorname{Spec} k[T_1, \ldots, T_n]$, making the closed sets those of form $\{\mathfrak{p} \mid \mathfrak{a} \subseteq \mathfrak{p}\}$. Translating via the bijection

$$\{\text{irreducible algebraic subsets of } k^n\} \xleftrightarrow[\mathbb{V};\mathcal{I}]{\simeq} \operatorname{Spec} k[T_1, \ldots, T_n]$$

induced by the strong NSS and the last proposition, this is a topology on the space of irreducible closed subsets of $\mathbb{A}^n_k$ extending the Zariski topology in a natural way.

But we don't need a geometric space to translate to. We can define this topology on *any* ring:

Definition 2.31. Let A be a ring. Its **spectrum** $\operatorname{Spec} A$ is the set of prime ideals of A, equipped with the topology whose closed sets are (exactly) those of form

$$\mathbb{V}(\mathfrak{a}) \coloneqq \{\mathfrak{p} \mid \mathfrak{a} \subseteq \mathfrak{p}\} \text{ for } \mathfrak{a} \trianglelefteq A.$$

This is indeed a topology: as in the geometric case, we have

- $\mathrm{Spec}(A) = \mathbb{V}((0))$ and $\emptyset = \mathbb{V}((1))$.
- $\mathbb{V}(\mathfrak{a}) \cup \mathbb{V}(\mathfrak{b}) = \mathbb{V}(\mathfrak{a} \cap \mathfrak{b}) = \mathbb{V}(\mathfrak{ab})$ (essentially the same proof as in the geometric case).
- $\bigcap_{i \in I} \mathbb{V}(\mathfrak{a}_i) = \mathbb{V}(\sum_{i \in I} \mathfrak{a}_i)$.

As before, the open sets $D(f) = \{\mathfrak{p} \mid f \notin \mathfrak{p}\}$ form a basis for the topology on Spec.

3 Ideals in ring extensions

Let A be a ring. We want to study $\operatorname{Spec} A$, so we need to understand the structure of its ideals. We will do this by studying what happens to ideals of A under ring homomorphisms.

3.1 Localisation

Let A be a ring, and suppose $S \subseteq A$. We want to construct from A a new ring $S^{-1}A$ in which the elements of S are invertible.

Observe that if $a, b \in A^\times$ then $ab \in A^\times$.

Definition 3.1. $S \subseteq A$ is **multiplicative** if $1 \in S$ and $ab \in S$ for $a, b \in S$.

We can now define the *localisation* $S^{-1}A$.

Definition 3.2. Define an relation $\sim$ on $A \times S$ by setting $(a_1, s_1) \sim (a_2, s_2)$ iff $u(a_1 s_2 - a_2 s_1) = 0$ for some $u \in S$. This is an equivalence relation; set $\frac{a}{s} \coloneqq [(a, s)]_\sim$. Define algebraic operations on $S^{-1}A \coloneqq (A \times S)/\sim$ by

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1 s_2 + a_2 s_1}{s_1 s_2}; \quad \frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2}.$$

These are indeed well defined; then $S^{-1}A$ equipped with these operations forms a ring called the **localisation of A by S**.

Proof that addition is well defined.
Let $\frac{a_1}{s_1} = \frac{b_1}{t_1}$ and $\frac{a_2}{s_2} = \frac{b_2}{t_2}$; we want $\frac{a_1 s_2 + a_2 s_1}{s_1 s_2} = \frac{b_1 t_2 + b_2 t_1}{t_1 t_2}$.
Find $u, v \in S$ such that

$$u(a_1 t_1 - b_1 s_1) = v(a_2 t_2 - b_2 s_2) = 0;$$

then the difference in the sums is

$$(a_1 s_2 + a_2 s_1) t_1 t_2 - (b_1 t_2 + b_2 t_1) s_1 s_2 = (a_1 t_1 - b_1 s_1) s_2 t_2 + (a_2 t_2 - b_2 s_2) s_1 t_1.$$

The product of the last expression and $uv \in S$ is 0. □

We also get a ring homomorphism $i_S : A \to S^{-1}A$ mapping $a \to \frac{a}{1}$. Its kernel is

$$\ker i_S = \left\{ a \in A \;\middle|\; \frac{a}{1} = \frac{0}{1} \right\} = \{a \in A \mid \exists u \in S : ua = 0\}.$$

Hence i_S is injective iff S has no zero divisors. In particular, if A is an integral domain and $0 \notin S$, then i_S is always injective.

Proposition 3.3 (Universal Property of $S^{-1}A$)**.**

1. *$i_S(s)$ is a unit for all $s \in S$.*
2. *For any ring B and map $f : A \to B$ such that $f(S) \subseteq B^\times$, there is a unique ring homomorphism $h : S^{-1}A \to B$ such that $f = h \circ i_S$.*

$$\begin{array}{ccc} A & \xrightarrow{i_S} & S^{-1}A \\ & \searrow^{f} & \downarrow{\scriptstyle \exists! h} \\ & & B \end{array}$$

Proof.

1. We have $\frac{1}{s} i_S(s) = \frac{1}{s}\frac{s}{1} = 1_{S^{-1}A}$.
2. If h exists, we must have

$$f(a) = h\left(\frac{a}{1}\right) = h\left(\frac{a}{s}\right) h\left(\frac{s}{1}\right) = h\left(\frac{a}{s}\right) f(s),$$

so $h(\frac{a}{s}) = f(a)f(s)^{-1}$. Therefore h is unique if it exists; it remains to show that this h is indeed well-defined (then it is clearly a homomorphism).

Indeed, let $\frac{a}{s} = \frac{b}{t}$, and find $u \in S$ such that $u(at - bs) = 0$. We have

$$f(u)(f(a)f(t) - f(b)f(s)) = 0 \text{ so } f(a)f(t) = f(b)f(s)$$

(since $f(u)$ is a unit), so $h(\frac{a}{s}) = f(a)f(s)^{-1} = f(b)f(t)^{-1} = h(\frac{b}{t})$.

□

Example 3.4. Let $h \in A$, and set $S_h = \{1, h, h^2, \dots\}$ and $A_h = S_h^{-1}A$. If h is nilpotent, then $A_h = 0$; if A is an integral domain and $h \neq 0$, then

$$A_h = \left\{ \frac{a}{h^m} \;\middle|\; a \in A, m \geq 0 \right\} \leq \operatorname{Frac} A.$$

For example, if $A = \mathbb{Z}$ and $h = 2$, then $S_2^{-1}\mathbb{Z}$ is the set of dyadic fractions.

Proposition 3.5. *Let A be a ring and $h \in A$. Then*

$$\frac{A[T]}{(1 - hT)} \cong A_h \text{ via } \sum_i a_i T^i \xrightarrow{\varphi} \sum_i \frac{a_i}{h^i}.$$

Proof. Viewing φ as a map from $A[T]$, have

$$\varphi(1 - hT) = 1 = h \cdot h^{-1} = 0,$$

so φ descends to the quotient. It remains to show it is an isomorphism.

Indeed, let $\psi' : A \to A[T]/(1 - hT)$ be the natural map. Then

$$\psi'(h^n)T^n = h^n T^n = (hT)^n = 1,$$

so $\psi'(S_h) \subseteq (A[T]/(1-hT))^\times$. By the universal property, we get a map

$$\begin{aligned} \psi : A_h &\to A[T]/(1-hT) \\ \frac{a}{h^n} &\to aT^n. \end{aligned}$$

This is clearly an inverse to φ. □

What do the ideals of a localisation $S^{-1}A$ look like? We first consider a more general definition.

Definition 3.6. Let $\varphi : A \to B$ be a ring homomorphism. If $\mathfrak{b} \trianglelefteq B$, then $\mathfrak{b}^c \coloneqq \varphi^{-1}(\mathfrak{b}) \trianglelefteq A$ is called the **contraction** of $\mathfrak{b}$ (wrt φ).

On the other hand, for $\mathfrak{a} \trianglelefteq A$ the set $\varphi(\mathfrak{a})$ is not necessarily an ideal; define instead $\mathfrak{a}^e \coloneqq (\varphi(\mathfrak{a}))$ the **extension** of $\mathfrak{a}$.

If φ is an inclusion map, then $\mathfrak{b}^c = \mathfrak{b} \cap A$; if φ is a quotient by I, then in fact $\mathfrak{b}^e = \varphi(\mathfrak{b}) = \mathfrak{b} + I$.

Example 3.7. Let $\varphi : \mathbb{Z} \hookrightarrow \mathbb{Q}$ be the natural inclusion. The nonzero ideals of $\mathbb{Z}$ extend to $\mathbb{Q}$ (since prime integers have inverses), and $\mathbb{Q}$ itself contracts to $\mathbb{Z}$. Note the ideals $(n) \trianglelefteq \mathbb{Z}$ for $n \neq 0$ do not occur as contractions.

Proposition 3.8. *$(-)^e$ and $(-)^c$ give a bijection*

$$\mathrm{im}(-)^c = \{\textit{contracted ideals of } A\} \longleftrightarrow \{\textit{extended ideals of } B\} = \mathrm{im}(-)^e.$$

Proof. Clearly, $\mathfrak{a} \subseteq \mathfrak{a}^{ec}$ and $\mathfrak{b}^{ce} \subseteq \mathfrak{b}$. Setting $\mathfrak{b} = \mathfrak{a}^e$, we get $\mathfrak{a}^{ece} \subseteq \mathfrak{a}^e$, so in fact $\mathfrak{a}^e = \mathfrak{a}^{ece}$. Since extended ideals of B have form $\mathfrak{a}^e$, the map $(-)^{ce}$ is the identity on $\mathrm{im}(-)^e$. Dually, setting $\mathfrak{a} = \mathfrak{b}^c$, we get $\mathfrak{b}^c = \mathfrak{b}^{ece}$, so $(-)^{ec}$ is also the identity. Hence extension and contraction are inverse on these domains. □

We now consider the case of a localisation. Indeed, let A be a ring, $S \subseteq A$ a multiplicative subset, and $i_S : A \to S^{-1}A$ the natural map. If $\mathfrak{a} \trianglelefteq A$ and $\mathfrak{b} \trianglelefteq S^{-1}A$, then

$$\mathfrak{a}^e = S^{-1}\mathfrak{a} = \left\{ \frac{a}{s} \;\middle|\; a \in \mathfrak{a}, s \in S \right\} \text{ and } \mathfrak{b}^c = \left\{ a \in A \;\middle|\; \frac{a}{1} \in \mathfrak{b} \right\}.$$

Proposition 3.9. *Take A, S, $\mathfrak{a}$ and $\mathfrak{b}$ as above. Then*

(i) $\mathfrak{b}^{ce} = \mathfrak{b}$

(ii) *$(-)^e$ and $(-)^c$ give a bijection*

$$\begin{aligned} \{\textit{ideals of } A \textit{ disjoint from } S\} &\longleftrightarrow \{\textit{ideals of } S^{-1}A\} \\ \mathfrak{p} &\longrightarrow \mathfrak{p}^e = S^{-1}\mathfrak{p} \\ \mathfrak{q}^c &\longleftarrow \mathfrak{q}. \end{aligned}$$

Further, this bijection preserves prime ideals.

Proof. Exercise, or see notes. □

Example 3.10. Let $\mathfrak{p}$ be a prime ideal of A. Let $S_\mathfrak{p} := A \setminus \mathfrak{p}$; then $S_\mathfrak{p}$ is multiplicative. Write $A_\mathfrak{p} = S_\mathfrak{p}^{-1}A$. The proposition gives a bijection

$$\begin{aligned}\{\text{prime ideals of } A \text{ contained in } \mathfrak{p}\} &\longleftrightarrow \{\text{prime ideals of } A_\mathfrak{p}\}\\ \mathfrak{p}' &\longrightarrow \mathfrak{p}'^e = S_\mathfrak{p}^{-1}\mathfrak{p}'\\ \mathfrak{q}^c &\longleftarrow \mathfrak{q}.\end{aligned}$$

Then $S_\mathfrak{p}^{-1}\mathfrak{p}$ contains all prime ideals of A_p, so $S_\mathfrak{p}^{-1}\mathfrak{p}$ is the unique maximal ideal of $A_\mathfrak{p}$. Hence $A_\mathfrak{p}$ is a local ring.

We can study A by studying localisations of the form $A_\mathfrak{p}$.

Example 3.11. Let $A = \mathbb{Z}$ and $\mathfrak{p} = (p)$. Then the ring

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{s} \;\middle|\; a, s \in \mathbb{Z}, p \nmid s \right\}$$

has unique maximal ideal

$$(p)^e = \left\{ \frac{a}{s} \;\middle|\; a, s \in \mathbb{Z}, p \nmid s, p \mid a \right\}.$$

3.2 Lying over problem

Let $f : A \hookrightarrow B$ be an inclusion of rings, and consider the map

$$\begin{aligned}f^* : \operatorname{Spec} B &\longrightarrow \operatorname{Spec} A\\ \mathfrak{p} &\longrightarrow \mathfrak{p} \cap A.\end{aligned}$$

The *lying over* and *going up* theorems deal with finding an ideal $\mathfrak{q} \trianglelefteq B$ such that $\mathfrak{q} \cap A = \mathfrak{p}$. In this case, we say $\mathfrak{q}$ **lies over** $\mathfrak{p}$. To do this in general, we will need the extension $A \leq B$ to be integral.

Lemma 3.12. *Let $A \leq B$ be an integral extension of rings, and suppose $\mathfrak{q} \trianglelefteq B$ is prime. Then $\mathfrak{q}$ is maximal (in B) iff $\mathfrak{q} \cap A$ is maximal in A.*

Proof. $B/\mathfrak{q}$ is an integral domain; since $A/(\mathfrak{q} \cap A) \hookrightarrow B/\mathfrak{q}$ by the second isomorphism theorem, $A/(\mathfrak{q} \cap A)$ is also an integral domain, and the inclusion gives an integral extension. We showed earlier that one quotient is a field iff the other is, so $\mathfrak{q}$ is maximal iff $\mathfrak{q} \cap A$ is. □

Take rings $A \leq B$ and a multiplicative set $S \subseteq A$. Then we can view $S^{-1}A$ as a subset of $S^{-1}B$ in a natural way. Indeed, consider the composition $A \hookrightarrow B \to S^{-1}B$. This sends elements of S to units in $S^{-1}B$, so, by the universal property, it extends to a map $\varphi : S^{-1}A \to S^{-1}B$ with $\varphi(a/s) = (1/s) \cdot (a/1) = a/s$. By definition, φ is injective, so it is the desired inclusion.

Lemma 3.13. *Let A, B and S be as above, and suppose further that $A \leq B$ is an integral extension. Then the extension is $S^{-1}A \leq S^{-1}B$ is integral.*

Proof. Fix $\frac{b}{s} \in S^{-1}B$, and let

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

for some $n \geq 1$ and $a_1, \dots a_n \in A$. Dividing by s^n, get

$$\left(\frac{b}{s}\right)^n + \left(\frac{a_1}{s}\right)\left(\frac{b}{s}\right)^{n-1} + \cdots + \left(\frac{a_n}{s^n}\right)\left(\frac{b}{s}\right)^0 = 0.$$

□

Proposition 3.14 (Lying over)**.** *Let $A \leq B$ be an integral extension of rings, and let $\mathfrak{p} \trianglelefteq A$ be prime. Then there is a prime $\mathfrak{q} \trianglelefteq B$ lying over $\mathfrak{p}$.*

Example 3.15. The extension $\mathbb{Z} \leq \mathbb{Q}$ is not integral, and no ideal of $\mathbb{Q}$ lies over $(2) \trianglelefteq \mathbb{Z}$.

Proof. Let $B_\mathfrak{p} \coloneqq (A \setminus \mathfrak{p})^{-1}B$; then $A_\mathfrak{p} \leq B_\mathfrak{p}$ is an integral extension.

We first solve the lying over problem for $\mathfrak{p}A_\mathfrak{p} = \mathfrak{p}^e$ in $A_\mathfrak{p} \leq B_\mathfrak{p}$.

Let $\mathfrak{n}$ be a maximal ideal of $B_\mathfrak{p}$. By the previous lemma, $\mathfrak{n} \cap A_\mathfrak{p}$ is maximal in $A_\mathfrak{p}$, so $\mathfrak{n} \cap A = \mathfrak{p}A_\mathfrak{p}$ by uniqueness. Hence $\mathfrak{n}$ lies over $\mathfrak{p}A_\mathfrak{p}$. We therefore have the diagram

$$\begin{array}{ccccccc} \mathfrak{q} \coloneqq \mathfrak{n} \cap B & \subseteq & B & \hookrightarrow & B_\mathfrak{p} & \supseteq & \mathfrak{n} \\ & & \uparrow & & \uparrow & & \\ \mathfrak{p} & \subseteq & A & \hookrightarrow & A_\mathfrak{p} & \supseteq & \mathfrak{p}A_\mathfrak{p} \end{array}$$

Claim: $\mathfrak{q}$ lies over $\mathfrak{p}$ (i.e., the square commutes on the ideals).

Indeed, $\mathfrak{p}$ is a prime ideal of A contained in $\mathfrak{p}$, so the solid arrows of the diagram induce bijections under contraction and expansion. Then

$$\mathfrak{q}^c = \mathfrak{n}^{cc} = (\mathfrak{p}A_\mathfrak{p})^c = \mathfrak{p}.$$

□

Theorem 3.16 (Going up)**.** *Let $A \leq B$ be an integral extension of rings, and suppose there are ascending chains of primes*

$$\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \cdots \subseteq \mathfrak{p}_n \trianglelefteq A \text{ and } \mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \cdots \subseteq \mathfrak{q}_m \trianglelefteq B$$

with $\mathfrak{q}_i$ lying over $\mathfrak{p}_i$ for $1 \leq i \leq m \leq n$.

Then we can extend the second chain by primes

$$\mathfrak{q}_m \subseteq \cdots \subseteq \mathfrak{q}_n \trianglelefteq B$$

with $\mathfrak{q}_i$ lying over $\mathfrak{p}_i$ for $m < i \leq n$.

Proof. By induction, it suffices to show the case $n = 2$ and $m = 1$.

That is, we have an inclusion $\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \trianglelefteq A$ and $\mathfrak{q}_1 \trianglelefteq B$ lying over $\mathfrak{p}_1$; we want a prime $\mathfrak{q}_2 \trianglelefteq A$ containing $\mathfrak{q}_1$ and lying over $\mathfrak{p}$. We enforce this by taking a quotient.

Indeed, consider the inclusion $A/\mathfrak{p}_1 \hookrightarrow B/\mathfrak{q}_1$, and let the prime $\tilde{\mathfrak{q}}_2 \trianglelefteq B/\mathfrak{q}_1$ lie over $\mathfrak{p}_2/\mathfrak{p}_1 \trianglelefteq A/\mathfrak{p}_1$. Then $\tilde{\mathfrak{q}}_2 = \mathfrak{q}_2/\mathfrak{q}_1$ for some prime $\mathfrak{q}_2 \trianglelefteq B$; this is the ideal we want.

Indeed, $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$, and, identifying the quotients via the inclusion,

$$\frac{\mathfrak{q}_2}{\mathfrak{q}_1} \cap \frac{A}{\mathfrak{p}_1} = \frac{\mathfrak{p}_2}{\mathfrak{p}_1}.$$

For $a \in \mathfrak{p}_2 \subseteq A$, we have $a + \mathfrak{q}_1 \in \mathfrak{q}_2/\mathfrak{q}_1$, so $a \in \mathfrak{q}_2$.

Conversely, take $a \in A \cap \mathfrak{q}_2$; then $a + \mathfrak{q}_1 \in \mathfrak{p}_2/\mathfrak{p}_1$. Write $a = a' + b$ for $a' \in \mathfrak{p}_2$ and $b \in \mathfrak{q}_1$; then $b = a - a' \in A$, so $b \in A \cap \mathfrak{q}_1 = \mathfrak{p}_1$. Hence $a \in \mathfrak{p}_2 + \mathfrak{p}_1 = \mathfrak{p}_2$. □

Example 3.17. Let $\mathbb{Z} \leq \mathbb{Z}[T]$; this is not an integral extension. Then going up fails: consider $(0) \subseteq (2)$, and consider the ideal $(1+2T)$ lying over (0). Then, if $\mathfrak{q} \trianglelefteq \mathbb{Z}[T]$ lies over (2) and contains $(1+2T)$, then $2 \in \mathfrak{q}$ so $1 = (2T+1) - T(2) \in \mathfrak{q}$, so $\mathfrak{q} = \mathbb{Z}[T]$ cannot be prime.

Proposition 3.18 (Incomparability)**.** *Let $A \leq B$ be an integral extension of rings, and let $\mathfrak{p} \trianglelefteq A$ be prime. Let $\mathfrak{q} \subseteq \mathfrak{q}' \trianglelefteq B$ be nested primes both lying over $\mathfrak{p}$. Then in fact $\mathfrak{q} = \mathfrak{q}'$.*

Proof. Recall that $A_{\mathfrak{p}} \leq B_{\mathfrak{p}}$ is an integral extension. Since $\mathfrak{q}$ and $\mathfrak{q}'$ are contained in $\mathfrak{p}^e$ (that is, disjoint from $B \setminus \mathfrak{p}^e$), their extensions $\mathfrak{q}B_{\mathfrak{p}} \subseteq \mathfrak{q}'B_{\mathfrak{p}}$ to $B_{\mathfrak{p}}$ are prime.

Claim: $\mathfrak{q}B_{\mathfrak{p}}$ contracts to $\mathfrak{p}A_{\mathfrak{p}}$ in $A_{\mathfrak{p}}$.

Indeed, we have the diagram

$$\begin{array}{ccccccc} \mathfrak{q}, \mathfrak{q}' & \subseteq & B & \hookrightarrow & B_{\mathfrak{p}} & \supseteq & \mathfrak{q}B_{\mathfrak{p}}, \mathfrak{q}'B_{\mathfrak{p}} \\ & & \hat{\vdots} & & \hat{\vdots} & & \\ \mathfrak{p} & \subseteq & A & \hookrightarrow & A_{\mathfrak{p}} & \supseteq & \mathfrak{p}A_{\mathfrak{p}} \end{array}$$

The solid arrows induce bijections by contraction and expansion. Let $\mathfrak{q}B_{\mathfrak{p}}$ contract to some prime $\mathfrak{p}'A_{\mathfrak{p}}$; this contracts to $\mathfrak{p}$, as

$$(\mathfrak{p}'A_{\mathfrak{p}})^c = (\mathfrak{q}B_{\mathfrak{p}})^{cc} = \mathfrak{q}^c = \mathfrak{p},$$

so in fact $\mathfrak{p}' = \mathfrak{p}$.

Then $\mathfrak{q}B_{\mathfrak{p}}$ and $\mathfrak{q}'B_{\mathfrak{p}}$ both lie over the maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$, so they are both maximal, and therefore equal as they are nested. □

3.3 Integrally closed domains

The dual theorem to going up, called *going down*, requires stronger conditions on A and B.

Definition 3.19. Let A and B be rings. The **integral closure** of A in B is the set $\{b \in B \mid b \text{ integral over } A\}$.

If A is an integral domain, its **integral closure** is its integral closure in $\operatorname{Frac} A$.

Proposition 3.20. *Let $A \leq B$ be rings. The integral closure of A in B is a subring of B.*

Proof. Example sheet. □

Definition 3.21. An integral domain A is **integrally closed** if it is equal to its own integral closure.

Example 3.22. $\mathbb{Z}$ is integrally closed, but $\mathbb{Z}[\sqrt{5}]$ is not: $\frac{1+\sqrt{5}}{2}$ satisfies the monic polynomial $X^2 - X - 1 \in \mathbb{Z}[X]$

Proposition 3.23. *Every UFD is integrally closed.*

Proof. Let A be a UFD, and let $x \in \operatorname{Frac} A$. Then we can write $x = \frac{a}{b}$ for some $a \in A$ and $0 \neq b \in B$. Suppose that x is integral over A; then

$$\left(\frac{a}{b}\right)^n + a_1 \left(\frac{a}{b}\right)^{n-1} + \cdots + a_n \left(\frac{a}{b}\right)^0 = 0$$

for some $a_i \in A$. Multiplying by b^n and rearranging, we get

$$a^n = -b(a_1 a^{n-1} + \cdots + a_n b^{n-1}),$$

so $b \mid a$ and so $x \in A$. □

Proposition 3.24. *Let A be an integrally closed integral domain, and let $E/\operatorname{Frac} A$ be a finite field extension. Then $\alpha \in E$ is integral over A iff its minimal polynomial over* $\operatorname{Frac} A$ *is in $A[T]$.*

Proof. Let f be the minimal polynomial of α over $\operatorname{Frac} A$. If $f \in A[T]$, then α is integral over A.

Conversely, suppose α is integral over A; let L be a splitting field for f over $\operatorname{Frac} A$. The roots of f have form $\sigma\alpha$ for $\sigma \in \operatorname{Aut}(L/\operatorname{Frac} A)$, so they are integral over A. By the Vieta formulae, the coefficients of f are sums of products of its roots, and therefore integral over A. Since $f \in (\operatorname{Frac} A)[T]$ and A is integrally closed, in fact $f \in A[T]$. □

Definition 3.25. Let $A \leq B$ be rings, and let $\mathfrak{a} \trianglelefteq A$. Then $b \in B$ is **integral over** I if it is the root of a monic polynomial in the A-module $\mathfrak{a}[X]$.

Note that, if b^m is integral over $\mathfrak{a}$, then so is b.

Proposition 3.26. *Let $A \leq B$ be rings, let $\mathfrak{a} \trianglelefteq A$, and fix $b \in B$. Then b is integral over $\mathfrak{a}$ if there is an $A[b]$-submodule $M \leq B$ such that*

(i) M is faithful over $A[b]$.

(ii) M is a finitely generated A-module.

(iii) $bM \subseteq \mathfrak{a}M$.

Proof. Exercise; analogous to the proof in the case of integrality over a ring. □

Proposition 3.27. *Let $A \leq B$ be rings, and let $\overline{A}$ be the integral closure of A in B. Let $\mathfrak{a} \trianglelefteq A$. Then the integral closure of $\mathfrak{a}$ in B is $\sqrt{\mathfrak{a}\overline{A}}$.*

Proof. Suppose $b \in B$ is integral over $\mathfrak{a}$; then in particular $b \in \overline{A}$, and

$$b^n + \underbrace{\in a_1}_{\mathfrak{a}} \underbrace{b^{n-1}}_{\in \overline{A}} + \cdots + a_n b^0 = 0 \text{ for some } a_i \in \mathfrak{a},$$

so $b^n \in \mathfrak{a}\overline{A}$. Hence $b \in \sqrt{\mathfrak{a}\overline{A}}$.

Conversely, suppose $b \in \sqrt{\mathfrak{a}\overline{A}}$. Then

$$b^n = a_1 x_1 + \cdots + a_m x_m \text{ for some } a_i \in \mathfrak{a},\ x_i \in \overline{A},\ n \in \mathbb{N}.$$

Since each x_i is integral over A, the ring $M \coloneqq A[x_1, \ldots, x_n]$ is a finite A-algebra. Then M is also faithful over $A[b]$ as $1 \in M$. Finally, $b^n M \subseteq \mathfrak{a}M$ by the relation. By the last proposition, b^n is integral over $\mathfrak{a}$, and so b is integral over $\mathfrak{a}$. □

Proposition 3.28. *Let A be an integrally closed integral domain, and let $E/\operatorname{Frac} A$ be an extension. If $x \in E$ is integral over $\mathfrak{a} \trianglelefteq A$, then the minimal polynomial of x over $\operatorname{Frac} A$ has coefficients in $\sqrt{\mathfrak{a}}$.*

Proof. Example sheet; analogous to the proof in the case of integrality over a ring. □

We now prove a sharp condition for solving the lying over problem.

Lemma 3.29. *Let A be a ring, and $I \trianglelefteq A$. Let S be a multiplicative set disjoint from I. Then there is an ideal $J \supseteq I$ of A which is maximal wrt being disjoint from S, and further J is prime.*

Proof. Apply Zorn's lemma to the poset of ideals containing I and disjoint from S. A maximal element of this poset is prime (see example sheet 1). □

Proposition 3.30. *Let $\varphi : A \to B$ be a ring homomorphism, and let $\mathfrak{p} \trianglelefteq A$ be prime. Then $\mathfrak{p}$ is a contraction under φ of some prime ideal in B iff $\mathfrak{p}^{ec} = \mathfrak{p}$.*

Proof. We already showed that, if $\mathfrak{p} \in \operatorname{im}(-)^c$, then $\mathfrak{p} = \mathfrak{p}^{ec}$.

Conversely, suppose $\mathfrak{p} = \mathfrak{p}^{ec}$, and let $S = A \setminus \mathfrak{p}$. Then $\varphi(S)$ is a multiplicative set disjoint from $\mathfrak{p}^e$: indeed, $\varphi(a) \in \mathfrak{p}^e \implies a \in \mathfrak{p}^{ec} = \mathfrak{p} \implies a \notin S$. By the last lemma, there is a prime $\mathfrak{q} \supseteq \mathfrak{p}^e$ in B disjoint from $\varphi(S)$. Then $\mathfrak{q}^c \supseteq \mathfrak{p}$, but $\mathfrak{q}^c$ is disjoint from $S = A \setminus \mathfrak{p}$, so in fact $\mathfrak{q}^c = \mathfrak{p}$. □

Theorem 3.31 (Going down)**.** *Let $A \leq B$ be an integral extension of integral domains, and suppose A is integrally closed. Take descending chains of primes*

$$A \trianglerighteq \mathfrak{p}_1 \supseteq \mathfrak{p}_2 \supseteq \cdots \supseteq \mathfrak{p}_n \text{ and } B \trianglerighteq \mathfrak{q}_1 \supseteq \mathfrak{q}_2 \supseteq \cdots \supseteq \mathfrak{q}_m$$

with $\mathfrak{q}_i$ lying over $\mathfrak{p}_i$ for $1 \leq i \leq m \leq n$.

Then we can extend the second chain by primes

$$B \trianglerighteq \mathfrak{q}_m \supseteq \cdots \supseteq \mathfrak{q}_n$$

with $\mathfrak{q}_i$ *lying over* $\mathfrak{p}_i$ *for* $m < i \leq n$.

Proof. By induction, it suffices to prove the case where $m = 1$ and $n = 2$.

We have $\mathfrak{p}_1 \supseteq \mathfrak{p}_2$, and $\mathfrak{q}_1$ lying above $\mathfrak{p}_1$.

Consider the inclusions $A \subseteq B \subseteq B_{\mathfrak{q}_1}$.

Claim: $\mathfrak{p}_2 = \mathfrak{p}^{ec} = (\mathfrak{p}_2 B_{\mathfrak{q}_1}) \cap A$.

Assuming the claim, we are done. Indeed, by the last proposition, we have a prime $\overline{\mathfrak{q}_2} \trianglelefteq B_{\mathfrak{q}_1}$ lying over $\mathfrak{p}_2$. Let $\mathfrak{q}_2 = \overline{\mathfrak{q}_2} \cap B$ be the contraction of $\overline{\mathfrak{q}_2}$ in B. Then $\mathfrak{q}_2$ is the contraction of a prime ideal in $B_{\mathfrak{q}_1}$, so, by the bijection, it is a prime containing $\mathfrak{q}_1$. But $\mathfrak{q}_2$ lies over $\mathfrak{p}_2$ by construction.

Proof of claim: We have $\mathfrak{p}_2 \subseteq \mathfrak{p}_2^{ec} = (\mathfrak{p}_2 B_{\mathfrak{q}_1}) \cap A$. Conversely, fix $a \in (\mathfrak{p}_2 B_{\mathfrak{q}_1}) \cap A$; write $a = \frac{y}{s}$ for some $y \in \mathfrak{p}_2 B$ and $s \in B \setminus \mathfrak{q}_1$. The integral closure of $\mathfrak{p}_2$ in B is $\sqrt{\mathfrak{p}_2 B}$, so y is integral over $\mathfrak{p}_2$. The minimal polynomial of y over $\operatorname{Frac} A$ therefore has coefficients in $\mathfrak{p}_2$; concretely, write

$$y^m + c_1 y^{m-1} + \cdots + c_m y^0 = 0 \text{ for some } c_i \in \mathfrak{p}_2.$$

Substituting $y = as$ and dividing out the leading coefficient, we get that s has minimal polynomial

$$X^m + \frac{c_1}{a} X^{m-1} + \cdots + \frac{c_m}{a^m} X^0 = 0$$

over $\operatorname{Frac} A$. Since $s \in B$ is also integral over A, each coefficient $\frac{c_i}{a^i}$ lies in A.

Suppose (for a contradiction) that $a \notin \mathfrak{p}_2$; since $\frac{c_i}{a^i} \cdot a^i = c_i \in \mathfrak{p}_2$, the coefficients $\frac{c_i}{a^i}$ all lie in $\mathfrak{p}_2$, and so $s^m \in \mathfrak{p}_2 B$. But

$$s^m \in \mathfrak{p}_2 B \subseteq \mathfrak{p}_1 B \subseteq \mathfrak{q}_1,$$

so in fact $s \in \mathfrak{q}_{1.\#}$ Therefore $a \in \mathfrak{p}_2$. □

4 Dimension theory

4.1 Krull dimension

Definition 4.1. Let A be a ring. The **height** of a prime ideal $\mathfrak{p} \neq A$ is the maximal length d of a descending chain of prime ideals

$$A \trianglerighteq \mathfrak{p} = \mathfrak{p}_d \supsetneq \mathfrak{p}_{d-1} \supsetneq \cdots \supsetneq \mathfrak{p}_0.$$

The **Krull dimension** $\dim A$ of A is the supremum over all heights of prime ideals.

By convention, we set $\dim 0 = -1$.

Examples 4.2.

1. A field has dimension 0.
2. Let k be a field. Clearly, $\dim k[T_1, \dots, T_n] \geq n$ due to the chain
$$(T_1, \dots, T_n) \supsetneq \cdots \supsetneq (T_1) \supsetneq 0.$$
Showing the dimension is *exactly* n (that is, there are no longer chains) is much harder.
3. If A is an integral domain, then $\dim A = 0$ iff A is a field. Indeed, $(0) \trianglelefteq A$ is prime.
4. The dimension of a PID which is not a field is 1.

Note that the height of a prime ideal need not be finite: for example, $k[T_1, T_2, \dots]$ contains the infinite descending chain
$$(T_1, T_2, T_3, \dots) \supseteq (T_2, T_3, \dots) \supseteq (T_3, \dots) \supseteq \dots$$
If A is Noetherian, we will show that heights remain finite. However, they are not necessarily bounded, so the Krull dimension of a Noetherian ring can still be infinite.

We now state some equivalent definitions of, and facts about, the *transcendence degree* of a field extension L/k. The proofs are not hard, and can be found in any book on field theory.

Definition 4.3. A subset $A \subseteq L$ is a **transcendence basis** over k if A is algebraically independent over k and $L/k(A)$ is algebraic.

Proposition 4.4.

(i) Let $A \subseteq L$ be algebraically independent over k. Then there is an extension $A \subseteq B \subseteq L$ such that B is a transcendence basis for L over k. In particular, taking $A = \emptyset$, transcendence bases exist.

(ii) All transcendence bases for L/k have the same cardinality.

(iii) Take another extension $E/L/k$. If B is a transcendence basis for E/L and C is a transcendence basis for L/k, then $B \cup C$ is a transcendence basis for E/k.

Definition 4.5. The cardinality of a (any) transcendence basis of L/k is the **transcendence degree** $\operatorname{trdeg}_k L$ for L/k.

In this language, (iii) of the proposition says that $\operatorname{trdeg}_k E = \operatorname{trdeg}_k L + \operatorname{trdeg}_L E$.

Definition 4.6. Let A be an integral domain containing a field k. The **transcendence degree** of A over k is $\operatorname{trdeg}_k A \coloneqq \operatorname{trdeg}_k \operatorname{Frac} A$.

We will show that, when A is a finitely generated k-algebra,
$$\operatorname{trdeg}_k A = \dim A.$$

Let R be a ring, and let $x \in R$. Consider the multiplicative set
$$S_{\{x\}} \coloneqq \{x^n(1 - rx) \mid n \geq 0, r \in R\},$$
and write $R_{\{x\}} = S_{\{x\}}^{-1} R$. Note that $x \in S_{\{x\}}$.

Proposition 4.7. *Let R be a ring and $n \geq 0$. Then $\dim R \leq n$ iff $\dim R_{\{x\}} \leq n-1$ for all $x \in R$.*

Proof. We begin by observing some facts.

Fact 1: If $\mathfrak{m} \trianglelefteq R$ is maximal and $x \in R$, then $\mathfrak{m} \cap S_{\{x\}} \neq \emptyset$.

Indeed, if $x \notin \mathfrak{m}$, then x has an inverse y modulo $\mathfrak{m}$ (since the quotient is a field), so $1 - yx \in \mathfrak{m}$.

Fact 2: If $\mathfrak{p} \subsetneq \mathfrak{m} \trianglelefteq R$, with $\mathfrak{p}$ prime and $\mathfrak{m}$ maximal, then, for $x \in \mathfrak{m} \setminus \mathfrak{p}$, we have $\mathfrak{p} \cap S_{\{x\}} = \emptyset$.

Indeed, suppose $y = x^n(1 - rx) \in \mathfrak{p} \cap S_{\{x\}}$. Then $1 - rx \in \mathfrak{p} \subseteq \mathfrak{m}$, so, since $x \in \mathfrak{m}$, also $1 \in \mathfrak{m}$.$_\#$

Now, suppose $\dim R \leq n$ and fix $x \in R$. Expansion and contraction along the inclusion $R \hookrightarrow R_{\{x\}}$ induce a bijection between prime ideals of $R_{\{x\}}$ and prime ideals of R disjoint from $S_{\{x\}}$. In particular, this bijection preserves strict inclusion. Take a descending chain of primes in $R_{\{x\}}$ of length l. Contracting this chain along the inclusion gives a chain of primes of length l in R; by fact 1, the contracted chain cannot contain a maximal ideal, so we can add on a maximal ideal to obtain a chain of length $l+1$ in R. Then $l + 1 \leq n$, so $\dim R_{\{x\}} \leq n - 1$.

Conversely, suppose $\dim R_{\{x\}} \leq n - 1$ for $x \in R$. If $\dim R = 0$ then we are done, so suppose $\dim R > 0$. Take a maximal descending chain of primes in R; it must start $\mathfrak{m} \supsetneq \mathfrak{p} \supsetneq \dots$ for some maximal $\mathfrak{m}$. Say this chain has length l. Fix $x \in \mathfrak{m} \setminus \mathfrak{p}$; by fact 2, the prime ideals in the chain from $\mathfrak{p}$ onwards are disjoint from $S_{\{x\}}$, so the chain $\mathfrak{p} \supsetneq \dots$ (which has length $l - 1$) extends along the inclusion to a descending chain of primes in $R_{\{x\}}$ of length $l - 1$. By assumption, $l - 1 \leq n - 1$, so $l \leq n$. □

Proposition 4.8. *Let A be an integral domain, and let $k \leq A$ be a subfield. Then $\dim A \leq \operatorname{trdeg}_k A$.*

Proof. If $\operatorname{trdeg}_k A = \infty$, we are done, so suppose $\operatorname{trdeg}_k A = n \in \mathbb{N}$, and proceed by induction.

For $n = 0$, $\operatorname{Frac} A/k$ is algebraic, so A is also algebraic, and therefore integral, over k. But this means A is a field, and so $\dim A = 0$.

Let $n > 0$. Fix $x \in A$; by the last proposition, it suffices to show $\dim A_{\{x\}} \leq n - 1$.

We have $k(x) \subseteq A_{\{x\}}$. Indeed, every element of $k(x)$ can be written as a ratio $f(x)/g(x)$, where $f, g \in k[X]$ and the lowest nonzero coefficient of g is 1. Then we can write

$$g(x) = x^k + \sum_{j=k+1}^{n} a_j x^j = x^k \left(1 - \sum_{j=k+1}^{n} (-a_j x^{j-k})\right) \in S_{\{x\}}.$$

If x is transcendental over k, then $\operatorname{trdeg}_k k(x) = 1$. Then

$$\operatorname{trdeg}_{k(x)} \underbrace{\operatorname{Frac} A_{\{x\}}}_{=\operatorname{Frac} A} = \underbrace{\operatorname{trdeg}_{k(x)} \operatorname{Frac} A}_{=\operatorname{trdeg}_{k(x)} A} - \operatorname{trdeg}_k k(x) = n - 1,$$

so, by induction, $\dim A_{\{x\}} \leq n - 1$, as required.

If x is algebraic over k, then $0 \in S_{\{x\}}$, and so $A_{\{x\}} = 0$, so $\dim A_{\{}x\} = 0 \leq n - 1$. □

In particular, we have shown that

$$\dim k[T_1, \ldots, T_n] = n.$$

We now want a converse to this result.

Proposition 4.9. *Let $A \leq B$ be an integral extension of rings. Then*

(i) $\dim A = \dim B$.

(ii) If, further, A and B are integral domains, and k is a field such that A is a k-subalgebra of B, then $\operatorname{trdeg}_k A = \operatorname{trdeg}_k B$.

Proof.

(i) Let $\mathfrak{p}_n \supsetneq \cdots \supsetneq \mathfrak{p}_0$ be a chain of primes in A. By the lying over and going up theorems, we can lift this to a chain of primes in B, so $\dim A \leq \dim B$.

Conversely, let $\mathfrak{q}_n \supsetneq \cdots \supsetneq \mathfrak{q}_0$ be a chain of primes in B. Let $\mathfrak{p}_i = \mathfrak{q}_i \cap A$; then the $\mathfrak{p}_i$ form a descending chain in A of length n. It remains to show the chain is strict; then $\dim B \leq \dim A$. Indeed, if $\mathfrak{p}_i = \mathfrak{p}_{i+1}$, then, by incomparability, $\mathfrak{q}_i = \mathfrak{q}_{i+1}$.#

(ii) Example sheet.

□

This justifies the notion of dimension from Noether normalisation described earlier: if a k-algebra A is finite (and hence integral) over a subring $A' \cong k[T_1, \ldots, T_d]$, then $\dim A = d$.

Theorem 4.10. *Let k be a field, and let A be a finitely generated k-algebra and an integral domain. Then*

$$\dim A = \operatorname{trdeg}_k A.$$

Proof. By Noether normalisation, A is integral over some $B = k[t_1, \ldots, t_n]$, with the t_i algebraically independent over k. By the last proposition, $\dim A = \dim B$, so it suffices to show that $\dim B = \operatorname{trdeg}_k B$. We already showed that $\dim B \leq \operatorname{trdeg}_k B$; conversely, the chain

$$(t_1, \ldots, t_n) \supsetneq (t_1, \ldots, t_{n-1}) \supsetneq \cdots \supsetneq (t_1) \supsetneq 0$$

of primes of B has length $n = \operatorname{trdeg}_k B$. □

Example 4.11. Let $A = k[T_1, T_2]$, with k an algebraically closed field. Let $\mathfrak{p} \in \operatorname{Spec} A$ be a nonzero non-maximal prime, and take $0 \neq f \in \mathfrak{p}$. Then $\mathfrak{p}$ contains some irreducible factor $g \mid f$; taking a maximal ideal $\mathfrak{m}$ containing $\mathfrak{p}$, we have a chain

$$0 \subsetneq (g) \subseteq \mathfrak{p} \subsetneq \mathfrak{m}$$

of primes in A. Since $\dim A = 2$, we have that, in fact, $\mathfrak{p} = (g)$.

By the weak NSS, we can already classify the maximal ideals. Hence

$$\operatorname{Spec} A = \{0\} \cup \{(g) \mid g \in k[T_1, T_2] \text{ irreducible}\} \cup \{(T - t_1, T - t_2) \mid t_1, t_2 \in k\}.$$

4.2 Nakayama's Lemma

Definition 4.12. Let A be a ring. Write $\operatorname{nil}(A) = \sqrt{0} = \bigcap \operatorname{Spec} A$ for the **nilradical**, and $J(A) = \bigcap \operatorname{mSpec} A$ for the **Jacobson radical**.

Theorem 4.13 (Nakayama's Lemma)**.** *Let $\mathfrak{a} \trianglelefteq A$ such that $\mathfrak{a} \subseteq J(A)$, and let M be a finitely generated A-module. Then*

(i) If $\mathfrak{a}M = M$, then $M = 0$.

(ii) If $N \leq M$ is such that $M = N + \mathfrak{a}M$, then $M = N$.

Proof.

(i) Suppose $\mathfrak{a}M = M$, but $M \neq 0$. Take a minimal generating set $\{e_1, \ldots, e_n\}$ of M; by assumption, $n \geq 1$.

Since $e_1 \in M = \mathfrak{a}M$, write $e_1 = \sum_{i=1}^{n} a_i e_i$ for some $a_i \in \mathfrak{a}$; rearranging, we have

$$(1 - a_1)e_1 = \sum_{i=2}^{n} a_i e_i.$$

Now, $(1 - a_1) \notin \mathfrak{m}$ for any $\mathfrak{m} \in \operatorname{mSpec} A$, since otherwise $1 \in \mathfrak{m}$ as $a_1 \in \mathfrak{a} \subseteq \mathfrak{m}$. Hence $(1 - a_1)$ is a unit, and so $e_1 \in \langle e_2, \ldots, e_n \rangle_A$, contradicting minimality.

(ii) Apply (i) to the finitely generated A-module M/N. Indeed, $\mathfrak{a}M/N = M/N$, so $M/N = 0$, and so $M = N$.

□

Proposition 4.14 (Krull's intersection theorem)**.** *Let A be Noetherian, and take $\mathfrak{a} \trianglelefteq A$ with $\mathfrak{a} \subseteq J(A)$. Then*

$$\bigcap_{n \geq 1} \mathfrak{a}^n = 0.$$

Proof. Write $M = \bigcap_{n \geq 1} \mathfrak{a}^n$.

Claim: $M = \mathfrak{a}M$.

Since $M \trianglelefteq A$, it is an A-module; since A is Noetherian, M is finitely generated, and also $M \subseteq J(A)$ by assumption. Therefore, assuming the claim, we are done by Nakayama's lemma.

Proof of claim: We clearly have the $\supseteq$ inclusion. For the converse, observe that, since A is Noetherian, $\mathfrak{a}$ is finitely generated; write $\mathfrak{a} = (a_1, \ldots, a_r)$ for some $a_i \in A$.

Let H_n be the set of homogeneous polynomials of degree n in r variables; then

$$\mathfrak{a}^n = \{g(a_1, \ldots, a_r) \mid g \in H_n\}.$$

Let $S_m = \{f \in H_m \mid f(a_1, \ldots, a_r) \in M\}$, and let $\mathfrak{c}$ be the ideal of $A[T_1, \ldots, T_r]$ generated by $\bigcup_{m \geq 1} S_m$.

By (corollaries of) Hilbert's basis theorem, $\mathfrak{c}$ is generated by some finite set $\{f_1, \ldots, f_s\} \subseteq \bigcup_{m \geq 1} S_m$ of homogeneous polynomials (of degree at most m). Let $d_i = \deg f_i$ and $d = \max_i d_i$.

Now, fix $b \in M$. In particular, $b \in \mathfrak{a}^{d+1}$, so $b = f(a_1, \ldots, a_r)$ for some $f \in H_{d+1}$. Thus $f \in S_{d+1} \subseteq \mathfrak{c}$, and so $f = \sum_i g_i f_i$ for some $g_i \in A[T_1, \ldots, T_r]$.

Taking the degree-$(d+1)$ homogeneous part of both sides of the summation, we get

$$f = (g_1)_{[d-d_1]} f_1 + \cdots + (g_s)_{[d-d_s]} f_s,$$

where $h_{[j]}$ is the degree-j homogeneous part of h. Since none of the $(g_i)_{[d-d_i]}$ have a constant term, we get

$$b = f(a_1, \ldots, a_r) = \sum_{i=1}^{s} \underbrace{(g_i)_{[d-d_i]}(a_1, \ldots, a_r)}_{\in \mathfrak{a}} \cdot \underbrace{f_i(a_1, \ldots, a_r)}_{\in M} \in \mathfrak{a}M.$$

□

4.3 Artinian rings

Definition 4.15. A ring A is **Artinian** if every descending chain of ideals stabilises. Equivalently, every nonempty set of ideals of A has a minimal element.

Observe that quotients of an Artinian ring are Artinian, by correspondence.

Let $A \neq 0$. We want to show that A is Artinian iff it is Noetherian of dimension 0.

Proposition 4.16. *A nonzero Artinian ring has dimension zero.*

Proof. Let $\mathfrak{p} \in \operatorname{Spec} A$, and let $A' = A/\mathfrak{p}$. Then A' is an Artinian integral domain. If we can show A' is a field, we are done since then $\mathfrak{p}$ is maximal.

Let $0 \neq a \in A'$; let the descending chain $(a) \supseteq (a^2) \supseteq (a^3) \ldots$ stabilise at (a^n). Then $(a^n) = (a^{n+1})$, so $a^n = ba^{n+1}$ for some $b \in A'$. Since A' is an integral domain, $1 = ab$. Hence A' is indeed a field. □

Examples 4.17.

1. An integral domain is Artinian iff it is a field: indeed, fields are Artinian and Artinian integral domains have dimension 0.
2. Every finite ring is Artinian.

3. Let k be a field. Then $k \times k$ is Artinian, and so is $k[T]/(T^n)$.

4. $\mathbb{Z}$ and $k[T]$ are Noetherian, but not Artinian.

Corollary 4.18. *If a ring A is Artinian, then* $\operatorname{nil}(A) = J(A)$.

Proposition 4.19. *Let A be an Artinian ring. Then A has finitely many maximal ideals.*

Proof. Let Σ be the collection of finite intersections of maximal ideals of A. Since A is Artinian, let $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{m}_n$ be a minimal element of Σ.

Claim: $\operatorname{mSpec} A = \{\mathfrak{m}_1, \dots, \mathfrak{m}_n\}$.

Indeed, suppose there is some other maximal ideal $\mathfrak{m}$. Find elements $a_i \in \mathfrak{m}_i \setminus \mathfrak{m}$; then $a_1 \dots a_n \in \bigcap_{i=1}^{m} \mathfrak{m}_i \setminus \mathfrak{m}$ (since $\mathfrak{m}$ is in particular prime), so

$$\bigcap_{i=1}^{m} \mathfrak{m}_i \cap \mathfrak{m} \subsetneq \bigcap_{i=1}^{n} \mathfrak{m}_i = \mathfrak{a}.\#$$

□

Proposition 4.20. *Let A be an Artinian ring. Then* $\operatorname{nil}(A)^n = 0$ *for some n.*

Proof. Consider the chain $\operatorname{nil}(A) \supseteq \operatorname{nil}(A)^2 \supseteq \dots$; this stabilises, so $\operatorname{nil}(A)^{n+1} = \operatorname{nil}(A)^n$ for some $n \in \mathbb{N}$.

Claim: $\operatorname{nil}(A)^n = 0$.

Suppose not; then

$$\operatorname{nil}(A) \in \Sigma \coloneqq \{\mathfrak{a} \trianglelefteq A \mid \mathfrak{a} \operatorname{nil}(A)^n \neq 0\}$$

so $\Sigma \neq \emptyset$. Let $\mathfrak{a}$ be a minimal element of Σ, and take $x \in \mathfrak{a}$ such that $x \operatorname{nil}(A)^n \neq 0$. Then $(x) \operatorname{nil}(A)^n \neq 0$, so, by minimality, $\mathfrak{a} = (x)$. Since $\operatorname{nil}(A)^{n+1} = \operatorname{nil}(A)^n$, we have

$$(x \operatorname{nil}(A)^n)(\operatorname{nil}(A)^n) = x \operatorname{nil}(A)^{2n} = x \operatorname{nil}(A)^n \neq 0,$$

so $x \operatorname{nil}(A)^n \in \Sigma$. But $x \operatorname{nil}(A)^n \subseteq (x)$, so, again by minimality, $(x) = x \operatorname{nil}(A)^n$. There is therefore some $y \in \operatorname{nil}(A)^n$ such that $x = xy$; since y is nilpotent, write $y^k = 0$. But then $x^k = x^k y^k = 0.\#$ □

Definition 4.21. Let M be a module over a ring A. Then M is **Noetherian/Artinian** if every ascending/descending chain of submodules of M stabilises.

Note that A is Noetherian/Artinian as a ring iff it is Noetherian/Artinian as an A-module (by definition). Note also that, for a submodule $N \leq M$, M is Noetherian/Artinian iff both M/N and N are.

Proposition 4.22. *Let A be a ring, and suppose there are $\mathfrak{m}_1, \dots, \mathfrak{m}_n \in \operatorname{mSpec} A$ such that $\mathfrak{m}_1 \dots \mathfrak{m}_n = 0$. Then A is Noetherian iff it is Artinian.*

Proof. Consider the (finite) descending chain

$$A \supseteq \mathfrak{m}_1 \supseteq \mathfrak{m}_1\mathfrak{m}_2 \supseteq \cdots \supseteq \mathfrak{m}_1 \dots \mathfrak{m}_n = 0.$$

Let $M_r = \mathfrak{m}_1 \dots \mathfrak{m}_{r-1}/\mathfrak{m}_1 \dots \mathfrak{m}_r$ (so that $M_1 = A/\mathfrak{m}_1$). The M_r are naturally A-modules; since $\mathfrak{m}_r$ acts trivially on M_r, the M_r are in fact $A/\mathfrak{m}_r$-vector spaces. By correspondence, we have a bijection

$$\{A/\mathfrak{m}_r\text{-linear subspaces of } M_r\} \longleftrightarrow \left\{ \begin{smallmatrix} A\text{-submodules of } \mathfrak{m}_1 \dots \mathfrak{m}_{r-1} \\ \text{containing } \mathfrak{m}_1 \dots \mathfrak{m}_r \end{smallmatrix} \right\}.$$

Note that the set on the LHS satisfies the ACC/DCC iff the set on the RHS does. The sets on the RHS all satisfy the ACC (as r varies) iff A is Noetherian, and all satisfy the DCC iff A is Artinian. The sets on the LHS satisfy the ACC and the DCC iff each M_r is finite-dimensional. Therefore A satisfies the ACC iff it satisfies the DCC. □

Lemma 4.23. *Let A be a Noetherian ring. Then every radical ideal of A is an intersection of finitely many primes.*

Proof. Exercise. □

Theorem 4.24. *A ring A is Artinian iff it is Noetherian of dimension 0.*

Proof. Suppose A is Artinian. Then $\dim A = 0$, and we have $\operatorname{mSpec} A = \{\mathfrak{m}_1, \dots, \mathfrak{m}_n\}$, and some $l \in \mathbb{N}$ such that

$$0 = \operatorname{nil} A^l = (\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n)^l \supseteq (\mathfrak{m}_1 \dots \mathfrak{m}_n)^l.$$

By the last proposition, A is Noetherian.

The converse is on the example sheet. □

4.4 Exact sequences

Definition 4.25. Let A be a ring. A sequence

$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} \dots \xrightarrow{f_{n-1}} M_n$$

of A-modules is an **exact sequence** if, for all i,

$$\operatorname{im} f_i = \ker f_{i+1}.$$

A **short exact sequence** is an exact sequence of the form

$$0 \longrightarrow N \hookrightarrow M \twoheadrightarrow L \longrightarrow 0$$

Note that, in the short exact sequence above, we have $M/N \cong L$.

Definition 4.26. A **graded ring** $(A, (A_n))$ is a ring A along with a sequence $(A_n)_{n=0}^{\infty}$ of additive subgroups of A such that

- $A = \bigoplus_j A_j$.

- $A_i A_j \subseteq A_{i+j}$ for all i, j.

Write $A_+ = \bigoplus_{i \geq 1} A_i \trianglelefteq A$, and let $x \in A$ be **homogeneous** if $x \in A_n$ for some n.

Example 4.27.

$$k[T_1, \ldots, T_n] = \sum_{n=0}^{\infty} H_n,$$

where H_n is the additive group of homogeneous polynomials of degree n.

Lemma 4.28. *A_0 is a ring.*

Proof. A_0 is a multiplicatively closed abelian subgroup of A; it remains to show $1_A \in A_0$.

Indeed, write $1_A = \sum_{i=0}^{m} a_i$ for some $a_i \in A_i$ and $m \in \mathbb{N}$. For $b \in A_n$, we have

$$b = \sum_{i=0}^{m} \underbrace{ba_i}_{\in A_{n+i}}$$

so, since $A = \oplus_m A_m$, in fact $b = ba_0$. Then $x = xa_0$ for all $x \in A$, so $1_A = a_0 \in A_0$. □ □

Each A_m is then an A_0-module.

Definition 4.29. Let A be a graded ring. A **graded A-module** $(M, (M_n))$ is an A-module, along with a sequence $(M_n)_{n=0}^{\infty}$ of A-submodules of M such that

- $M = \bigoplus_j M_j$.
- $A_i M_j \subseteq M_{i+j}$ for all i, j.

For example, a graded ring is a graded module over itself.

A homomorphism $f : M \to N$ of graded A-modules is then an A-module homomorphism with $f(M_i) \subseteq N_i$ for all i.

Proposition 4.30. *Let A be a graded ring. Then A is Noetherian iff A_0 is Noetherian and A is finitely generated as an A_0-algebra.*

Proof.
$\Leftarrow$: Hilbert's basis theorem.

$\Rightarrow$: Suppose A is Noetherian; then $A_0 \cong A/A_+$ is Noetherian. Now, $A_+ \trianglelefteq A$ is generated by the set of all homogeneous elements of positive degree; let $A_+ = (x_1 \ldots, x_s)$, with $x_i \in A_{k_i}$ $(k_i > 0)$. Let $A' = A_0[x_1, \ldots, x_s]$.

Claim: $A' = A$.

It suffices to show $A_n \subseteq A'$ for all $n \in \mathbb{N}$. For $n = 0$, we have $A_0 \subseteq A'$; for $n > 0$, take $y \in A_n$, and write

$$y = \sum_{i=1}^{s} a_i x_i.$$

Taking the n^{th} homogeneous component (formally, projecting onto A_n), we can assume wlog that $a_i \in A_{n-k_i}$. But $n - k_i < n$, so, by induction, $a_i \in A'$. Hence $y \in A'$. □

Definition 4.31. Let A be a ring, and let $\mathcal{C}$ be a class of A-modules. Then a mapping $\lambda : \mathcal{C} \to \mathbb{Z}$ is an **additive function** on $\mathcal{C}$ if for all short exact sequences

$$0 \longrightarrow N \hookrightarrow M \twoheadrightarrow L \longrightarrow 0$$

we have $\lambda(M) = \lambda(N) + \lambda(L)$; that is,

$$\lambda(M) = \lambda(N) + \lambda(M/N)$$

for all submodules $N \leq M$.

Example 4.32. Let $A = k$ be a field, and $\mathcal{C}$ the class of finite-dimensional k-vector spaces. Then $\lambda(V) = \dim_k V$ is an additive function.

Proposition 4.33. *For an exact sequence*

$$0 \longrightarrow M_1 \longrightarrow \ldots \longrightarrow M_n \longrightarrow 0$$

we have

$$\sum_{k=0}^{n} (-1)^k \lambda(M_k) = 0.$$

Proof. Example sheet. □

Definition 4.34. Let M be an A-module. A **composition series** for M is a maximal descending chain of submodules

$$M = M_n \gneq M_{n-1} \gneq \cdots \gneq M_0 = 0$$

Maximality here is with respect to chain refinement.

Lemma 4.35. *If a module M has a composition series of length M, then all composition series of M have length n. Further, every chain of submodules of M can be refined to a composition series.*

Proof. Exercise. □

Definition 4.36. The length of a (any) composition series for M is called its **length** $l(M)$. If no composition series exists, say the length is ∞.

Proposition 4.37. *An A-module M has finite length iff M is Noetherian and Artinian.*

Proof.
$\Rightarrow$: All chains of submodules have finite length.

$\Leftarrow$: Since M is Noetherian, we have a chain of submodules

$$M = M_0 \gneq M_1 \gneq M_2 \gneq \ldots$$

where M_i is maximal in M_{i-1}. Indeed, given M_{i-1}, take an ascending chain of submodules of it, and let M_i be the submodule at which this chain terminates. Since M is Artinian, this chain (M_i) itself terminates. By construction, it must terminate at 0, so this chain is a composition series for M. □

Proposition 4.38. *The mapping $M \to l(M)$ is additive.*

Proof. Exercise. □

4.5 Hilbert polynomials

Let $A = \bigoplus_n A_n$ be a Noetherian graded ring. As we have seen, A_0 is Noetherian and $A = A_0[x_1, \ldots, x_s]$ for some homogeneous $x_i \in A_{k_i}$ with $k_i > 0$. Now, let $M = \bigoplus_n M_n$ be a finitely-generated graded A-module; let M be generated over A by $m_1, \ldots, m_b$ for some $m_i \in M_{r_i}$.

Every element of M_n is of form

$$\sum_{j=1}^{b} f_j(x_1, \ldots, x_s) \cdot m_j,$$

for some $f_j \in A_0[T_1, \ldots, T_s]$ such that $f_j(x_1, \ldots, x_s) \in A_{n-r_j}$. Therefore M_n is generated as an A_0-module by elements of the form $x_1^{e_1} \ldots x_s^{e_s} \cdot m_j$, where $1 \leq j \leq n$ and $\sum_i e_i k_i = n - r_j$. There are finitely many such elements, so M_n is a finitely generated A_0-module.

Let λ be an additive function on the class of finitely-generated A_0-modules. A good example for intuition is $\lambda = l$ and A_0 Artinian.

Definition 4.39. The **Poincaré Series** of M wrt λ is

$$P(M, T) \coloneqq \sum_{n=0}^{\infty} \lambda(M_n) T^n \in \mathbb{Z}[\![T]\!].$$

Theorem 4.40 (Hilbert-Serre)**.** *$P(M, T)$ is a rational function in T of form*

$$P(M, T) = \frac{f(T)}{\prod_{i=1}^{s}(1 - T^{k_i})} \text{ with } f(T) \in \mathbb{Z}[T].$$

Proof. Proceed by induction on s.

If $s = 0$, then $A = A_0$. Since M is a finite A_0-module, for sufficiently large n we have $M_n = 0$, and so $\lambda(M_n) = 0$. Hence $P(M, T) \in \mathbb{Z}[T]$.

For $s > 0$, consider the A_0-module homomorphism $\cdot x_s : M_n \to M_{n+k_s}$ given by multiplication by x_s. This yields the exact sequence of A_0-modules below.

$$K_n = \ker(\cdot x_s) \hookrightarrow M_n \xrightarrow{\cdot x_s} M_{n+k_s} \twoheadrightarrow \frac{M_{n+k_s}}{\operatorname{im}(\cdot x_s)} = L_{n+k_s}$$

Let $K \coloneqq \bigoplus_n K_n$ and $L \coloneqq \bigoplus_n L_{n+k_s}$; these are both finitely-generated graded A-modules since they are, respectively, an A-submodule and a quotient of M in

a way that respects the grading. But, by construction ,both are annihilated by x_s, so they are in fact finitely-generated graded $A_0[x_1, \ldots, x_{s-1}]$-modules.

By induction, $P(K,T)$ and $P(L,T)$ are rational functions with denominator $\prod_{i=1}^{s-1}(1-T^{k_i})$. But additivity of λ gives

$$\lambda(K_n) - \lambda(M_n) + \lambda(M_{n+k_s}) - \lambda(L_{n+k_s}) = 0;$$

multiplying by T^{n+k_s} and rearranging, we have

$$\lambda(M_{n+k_s}) \cdot T^{n+k_s} - T^{k_s}\lambda(M_n) \cdot T^n = \lambda(L_{n+k_s}) \cdot T^{n+k_s} - T^{k_s}\lambda(K_n) \cdot T^n.$$

Summing over all $n \geq 0$, we therefore have

$$(1-T^{k_s})P(M,T) = P(L,T) - T^{k_s}P(K,T) + g(T)$$

for some correction term $g(T) \in \mathbb{Z}[T]$ of degree at most k_s. This gives the result. □

From now on, assume λ takes values on $\mathbb{Z}_{\geq 0}$ and $\lambda(N) = 0$ only for $N = 0$ (we have in any case $\lambda(0) = 0$, by additivity).

Write $d(M)$ for the order of the pole of $P(M,T)$ at $T = 1$. We have $d(M) \geq 0$ for $M \neq 0$. Indeed, if $d(M) \leq 0$, then in particular

$$\lim_{T \to 1^-} \frac{f(T)}{\prod_{i=1}^{s}(1-T^{k_i})} = 0;$$

since the r.o.c. of the rational function is 1, we also have $\lim_{T\to 1^-} P(M,T) = 0$. But then $\lambda(M_n) = 0$ for all $n \in \mathbb{N}$, and so $M = 0$.

Proposition 4.41. *Suppose $x \in A_k$ is not a zero divisor in M. Then $d(M/xM) = d(M) - 1$.*

Proof. Construct the exact sequence as in the previous theorem, but with x in place of x_s. Then $K_n = 0$ since x annihilates only 0, and $L_{n+k} = M_{n+k}/xM_n$. Then we get

$$(1-T^k)P(M,T) = P(L,T) + g(T);$$

since $(1-T^k)$ has a simple zero at 1, $d(M) = d(L) + 1$. But we can write $L = (\oplus_{n \geq k} M_n)/xM$, so $P(L,T)$ and $P(M/xM,T)$ differ by a polynomial in $\mathbb{Z}[T]$, and so $d(M/xM) = d(L) = d(M) - 1$. □

Example 4.42. Let $A = k[T_1, \ldots, T_s] = \bigoplus_n H_n$. Now, $H_0 = k$, so A is generated as an H_0-algebra by $T_1, \ldots, T_s \in A_1$. Therefore $k_i = 1$ for $1 \leq i \leq s$.

Proposition 4.43. *Suppose $k_i = 1$ for $1 \leq i \leq s$. Then there is a polynomial $HP_M \in \mathbb{Q}[T]$ of degree $d(M) - 1$ (where $\deg 0 = -1$) such that $\lambda(M_n) = HP_M(n)$ for large enough n.*

Note that such a polynomial is necessarily unique, since it is determined at infinitely many points.

Proof. Write $d = d(M)$. Applying Hilbert-Serre and cancelling any factors of $T-1$ in the numerator of $P(M,T)$, there is some $f \in \mathbb{Z}[T]$ such that $f(1) \neq 0$ and

$$\sum_{k=0}^{\infty} \lambda(M_k)T^k = P(M,T) = (1-T)^{1-s} f(T) \coloneqq (1-T)^{-d} \sum_{i=0}^{N} a_k T^k,$$

for some $d \leq k-1$ and $a_k \in \mathbb{Z}$. Then

$$(1-T)^{-d} = \sum_{k=0}^{\infty} \binom{d+k-1}{d-1} T^k.$$

Therefore, comparing coefficients, for large enough n we must have

$$\lambda(M_n) = \sum_{k=0}^{N} a_k \binom{d+n-k-1}{d-1} \coloneqq HP_M(n).$$

This is a polynomial over $\mathbb{Q}$ in n. The leading coefficient is

$$\frac{\sum_{k=0}^{N} a_k}{(d-1)!} = \frac{f(1)}{(d-1)!} \neq 0,$$

so the polynomial has degree $d-1$. □

The polynomial HP_M is called the **Hilbert polynomial** of M (wrt λ). Note that HP_M maps $\mathbb{Z} \to \mathbb{Z}$, yet it lies in $\mathbb{Q}[T]$ in general.

Example 4.44. Let k be a field and $A = k[T_1, \ldots, T_s]$. Then A_n is a k-vector space with basis $\{T_1^{e_1} \ldots T_s^{e_s} \mid \sum_i e_i = n\}$, so $\dim A_n = \binom{s+n-1}{s-1}$. Set $\lambda(V) = \dim_k(V)$; then $P(A,T) = (1-T)^{-s}$, $f = 1$ and $HP_A(n) = \binom{s+n-1}{s-1}$.

4.6 Filtrations

Definition 4.45. Let M be a module over a ring A. A **filtration** of M is a descending chain $M = M_0 \geq M_1 \geq \ldots$ of submodules. If $\mathfrak{a} \trianglelefteq A$, then the chain $(M_n)_{n=0}^{\infty}$ is an **$\mathfrak{a}$-filtration** if $\mathfrak{a}M_n \leq M_{n+1}$ for all $n \in \mathbb{N}$. An $\mathfrak{a}$-filtration is **stable** if $\mathfrak{a}M_n = M_{n+1}$ for sufficiently large n.

Example 4.46. $(\mathfrak{a}_n M)$ is a stable $\mathfrak{a}$-filtration of M.

Stable $\mathfrak{a}$-filtrations of M are all in a sense equivalent.

Lemma 4.47 (Bounded Differences)**.** *Let (M_n) and (M'_n) be stable $\mathfrak{a}$-filtrations of M. Then there is some $n_0 \in \mathbb{N}$ such that $M_{n+n_0} \leq M'_n$ and $M'_{n+n_0} \leq M_n$ for all $n \in \mathbb{N}$.*

Proof. The conclusion is an equivalence relation, so it suffices so prove the case $M'_n = \mathfrak{a}^n M$.

On the one hand, $\mathfrak{a}^n M \leq M_n$ by definition. On the other, there is some $n_0 \in \mathbb{N}$ such that $M_{n+1} = \mathfrak{a}M_n$ for all $n \geq n_0$; then, for any $n \in \mathbb{N}$, we have

$$M_{n+n_0} = \mathfrak{a}^n M_{n_0} \leq \mathfrak{a}^n M.$$

□

Let A be a ring and $\mathfrak{a} \trianglelefteq A$. Set $\mathfrak{a}^0 = A$; then $A^* = \bigoplus_{n=0}^{\infty} \mathfrak{a}^n$ is a graded ring. If M is an A-module with an $\mathfrak{a}$-filtration (M_n), then $M^* = \bigoplus_n M_n$ is a graded A^*-module.

Suppose A is Noetherian; let $\mathfrak{a} = (x_1, \dots, x_s)$. Then A^* is generated as an A-algebra by $\bar{x}_1, \dots, \bar{x}_s$, where $\bar{x}_i$ is the image of x_i in the $\mathfrak{a}$-entry of A^*:

$$\bar{x}_i = (0, x_i, 0, 0, \dots) \in A \oplus \mathfrak{a} \oplus \mathfrak{a}^2 \oplus \mathfrak{a}^3 \cdots = A^*.$$

By HBT, A^* is Noetherian.

Lemma 4.48. *Let A be a Noetherian ring, M a finitely generated A-module, and M_n an $\mathfrak{a}$-filtration of M. Then TFAE:*

(i) M^* is a finitely generated A^*-module.

(ii) (M_n) is $\mathfrak{a}$-stable.

Proof. M is Noetherian (since it is finitely generated over a Noetherian ring), so each M_n is finitely generated. Therefore each $Q_n \coloneqq \bigoplus_{i=1}^{n} M_n$ is finitely generated as an A-module; Q_n is also a subgroup of M^*. The A^*-submodule of M^* generated by Q_n is

$$M_n^* \coloneqq A^* Q_n = M_0 \oplus \cdots \oplus M_n \oplus \mathfrak{a}M_n \oplus \mathfrak{a}^2 M_n \oplus \dots$$

Then M_n^* is finitely generated over the Noetherian ring A^*, and so itself Noetherian.

Now, the filtration (M_n) is $\mathfrak{a}$-stable iff the ascending chain (M_n^*) stabilises. Indeed, by definition, this chain stabilises at $n = k$ iff $M_{k+m} = \mathfrak{a}^m M_k$ for all $m \in \mathbb{N}$.

Suppose M^* is finitely generated over A^*. Then M^* is Noetherian, and so (M_n^*) stabilises. Conversely, suppose (M_n^*) stabilises; since $M^* = \bigcup_n M_n^*$, we have $M^* = M_{n_0}^*$ for some $n_0 \in \mathbb{N}$. Then M^* is finitely generated over A^*. □

Proposition 4.49 (Artin-Rees theorem)**.** *Suppose A is Noetherian, $\mathfrak{a} \trianglelefteq A$ and M is a finitely generated module over A with an stable $\mathfrak{a}$-filtration (M_n). Let $M' \leq M$ be an A-submodule. Then $(M_n \cap M')$ is a stable $\mathfrak{a}$-filtration of M'.*

Proof. Write $K_n \coloneqq M_n \cap M'$. We want to show K_n is a stable $\mathfrak{a}$-filtration.

Since $\mathfrak{a}M' \subseteq M'$ and $\mathfrak{a}M_n \subseteq M_{n+1}$, (K_n) is an $\mathfrak{a}$-filtration. It remains to show it is stable.

Now, $K = \bigoplus_n K_n$ is a graded M^*-submodule of A^*. By the previous lemma, M^* is finitely generated over A^* since (M_n) is $\mathfrak{a}$-stable. Since A^* is Noetherian (as A is), $K \leq M^*$ is finitely generated over A^*; applying the lemma again, (K_n) is $\mathfrak{a}$-stable. □

Definition 4.50. Let A be a ring, and let $\mathfrak{a} \trianglelefteq A$. The **associated graded ring** is

$$G_{\mathfrak{a}}(A) = \bigoplus_{n=0}^{\infty} \frac{\mathfrak{a}^n}{\mathfrak{a}^{n+1}},$$

where we again take $\mathfrak{a}^0 = A$.

If M is an A-module and (M_n) an $\mathfrak{a}$-filtration,

$$G(M) = \bigoplus_{n=0}^{\infty} \frac{M_n}{M_{n+1}}$$

is the **associated graded module**; it is a graded $G_{\mathfrak{a}}(A)$-module.

Proposition 4.51. *Let A be a Noetherian ring with $\mathfrak{a} \trianglelefteq A$. Then*

(1) $G_{\mathfrak{a}}(A)$ is a Noetherian ring.

(2) If M is a finitely generated A-module and (M_n) is a stable $\mathfrak{a}$-filtration, then $G(M)$ is a finitely generated graded $G_{\mathfrak{a}}(A)$ module.

Proof.

(1) Since A is Noetherian, $\mathfrak{a} = (x_1, \ldots, x_s)$. As before, let $\bar{x}_i$ be the image of x_i in the second entry of $G_{\mathfrak{a}}A$. Then $G_{\mathfrak{a}}A$ is generated by the $\bar{x}_i$ as an A-algebra; by HBT, $G_{\mathfrak{a}}(A)$ is Noetherian.

(2) There is some $n_0 \in \mathbb{N}$ such that $M_{n_0+r} = \mathfrak{a}^r M_{n_0}$ for all $r \in \mathbb{N}$. Then $G(M)$ is generated as a $G_{\mathfrak{a}}(A)$-module by $\bigoplus_{n=0}^{n_0} M_n$.

Now, each quotient M_n/M_{n+1} is a Noetherian A-module (since M_n is) which is annihilated by $\mathfrak{a}$. Hence M_n/M_{n+1} is finitely generated over $A/\mathfrak{a}$, and so $\bigoplus_{n=0}^{n_0} M_n$ is finitely generated over $A/\mathfrak{a}$. Hence $G(M)$ is finitely generated over $G_{\mathfrak{a}}(A)$.

□

4.7 Dimension theory of local rings

Definition 4.52. Let R be a ring. An ideal $I \trianglelefteq R$ is **primary** if $I \neq R$ and every zero divisor of R/I is nilpotent.

Let $I \trianglelefteq R$ be primary. Then $\sqrt{I} \coloneqq \mathfrak{p}$ is the smallest prime containing I; say that I is **$\mathfrak{p}$-primary**. In particular, $\sqrt{\cdot}$ maps primary ideals to prime ones.

Let $\mathfrak{p} \trianglelefteq R$ be prime. Now, $\mathfrak{p}^k$ is not necessarily primary; if it is primary, then it must be $\mathfrak{p}$-primary. Note that, for $\mathfrak{m} \trianglelefteq R$ maximal, $\mathfrak{m}^n$ is always $\mathfrak{m}$-primary. Not every primary ideal arises as a prime power, however: the ring $k[X, Y]$ (k a field) is a counterexample.

Let $(A, \mathfrak{m})$ be a Noetherian local ring. For a $\mathfrak{m}$-primary ideal $\mathfrak{q}$, let $\delta(\mathfrak{q})$ be the minimal cardinality of a generating set of $\mathfrak{q}$. We get three numbers from A:

(1) $\dim A$

(2) $\delta(A) = \min\{\delta(\mathfrak{q}) \mid \mathfrak{q} \trianglelefteq A \text{ } \mathfrak{m}\text{-primary}\}$.

(3) $d(G_{\mathfrak{m}}(A))$; that is, the order of the pole of $P(G_{\mathfrak{m}}(A), T)$ at $T = 1$.

We will show that, in fact, these three values are all equal.

Lemma 4.53. *Let $p \in \mathbb{Q}[T]$. Then, for $n \geq 0$, there is some $q \in \mathbb{Q}[T]$ such that*

$$\sum_{k=0}^{n-1} p(k) = q(n),$$

where the leading coefficient of q depends only on the leading coefficient of p, and $\deg q = \deg p + 1$ (where we take $\deg 0 = -\infty$).

Proof. Omitted. □

Suppose $f : \mathbb{Z} \to \mathbb{Z}$ is equal to a polynomial $g \in \mathbb{Q}[T]$ at sufficiently large values. Since g is uniquely determined, we will talk about $\deg f$, the leading term/coefficient of f, and so on, without explicitly referring to g.

Proposition 4.54. *Let $(A, \mathfrak{m})$ be a Noetherian local ring, and let $\mathfrak{q} \trianglelefteq A$ be $\mathfrak{m}$-primary. Let M be a finitely generated A-module, and (M_n) a $\mathfrak{q}$-stable filtration. Then*

(1) $l(M_n/M_{n+1}) < \infty$.

(2) For n sufficiently large, there are $f, g \in \mathbb{Q}[T]$ such that $l(M_n/M_{n+1}) = f(n)$ and $l(M/M_n) = g(n)$, and $1 + \deg l(M_n/M_{n+1}) - \deg l(M/M_n) \leq \delta(\mathfrak{q})$.

(3) The leading terms of $l(M_n/M_{n+1})$ and $l(M/M_n)$ depend only on A, $\mathfrak{m}$ and $\mathfrak{q}$; that is, they are independent of the choice of filtration.

Proof.

(1) M_n/M_{n+1} is a finitely generated $A/\mathfrak{q}$-module. Now, $A/\mathfrak{q}$ is Noetherian, and has dimension 0: there are no prime ideals between $\mathfrak{q}$ and $\mathfrak{m}$, and $\mathfrak{m}$ is maximal. Therefore $A/\mathfrak{q}$ is Artinian. Hence M_n/M_{n+1} is both Noetherian and Artinian, and so it has finite length.

(2) By the proposition, $G_{\mathfrak{q}}(M)$ is Noetherian. Then $G(M) = \bigoplus_n M_n/M_{n+1}$ is a finitely generated $G_{\mathfrak{q}}(A)$-module. If $x_1, \ldots, x_s$ generate $\mathfrak{q}$, then their (degree-1 homogeneous) images in the second entry of $G_{\mathfrak{q}}(A)$ generate $G_{\mathfrak{q}}(A)$ as a $A/\mathfrak{q}$-algebra. But then $l(M_n/M_{n+1})$ is equal to its Hilbert polynomial, which has degree $s - 1$, for sufficiently large values of n. Since

$$l(M/M_n) = \sum_{k=0}^{n-1} l(M_k/M_{k+1}),$$

this is also eventually polynomial in n by the last lemma.

(3) Let (M'_n) be another stable $\mathfrak{q}$-filtration of M, and let

$$g(n) = l(M/M_n) = \sum_{k=0}^{n-1} l(M_k/M_{k+1})$$

and

$$f(n) = l(M/M'_n) = \sum_{k=0}^{n-1} l(M'_k/M'_{k+1}).$$

Then f and g are polynomials for sufficiently large values of n; by the last lemma, their leading coefficients depend only on the leading coefficients of $l(M_k/M_{k+1})$ and $l(M'_k/M'_{k+1})$, respectively.

But (M_n) and (M'_n) have bounded differences; that is, there is some $n_0 \in \mathbb{N}$ such that, for all n, $M_{n+n_0} \leq M'_n$ and $M'_{n+n_0} \leq M_n$. Therefore f and g have the same growth rate: precisely,

$$g(n - n_0) \leq f(n) \leq g(n + n_0) \text{ for } n \in \mathbb{N}.$$

Hence g and f must have the same degree and leading coefficient.

□

Corollary 4.55. *Let $(A, \mathfrak{m})$ be a Noetherian local ring and $\mathfrak{q}$ a $\mathfrak{m}$-primary ideal. Then*

(i) For sufficiently large n, $l(\mathfrak{q}^n/\mathfrak{q}^{n+1})$ is a polynomial of degree at most $\delta(\mathfrak{q}) - 1$.

(ii) $\deg l(A/\mathfrak{q}^n) = \deg l(A/\mathfrak{m}^n)$ and $\deg l(\mathfrak{q}^n/\mathfrak{q}^{n+1}) = \deg l(\mathfrak{m}^n/\mathfrak{m}^{n+1})$.

Proof.

(i) Apply the last proposition to $M = A$, with $M_n = \mathfrak{q}^n$.

(ii) Since A is Noetherian and $\mathfrak{m} = \sqrt{\mathfrak{q}}$, we showed on the example sheet that there is some $r \in \mathbb{N}$ such that $\mathfrak{m}^r \subseteq \mathfrak{q} \subseteq \mathfrak{m}$. Therefore

$$l(\mathfrak{m}/\mathfrak{m}^n) \leq l(\mathfrak{m}/\mathfrak{q}^n) \leq l(\mathfrak{m}/\mathfrak{m}^{rn}),$$

so

$$g'(n) \leq g(n) \leq g'(rn),$$

and hence $\deg l(\mathfrak{m}/\mathfrak{q}^n) = \deg l(\mathfrak{m}/\mathfrak{m}^n)$.

□

Proposition 4.56. *Let $(A, \mathfrak{m})$ be a Noetherian local ring. Then $\delta(A) \geq d(G_{\mathfrak{m}}(A))$.*

Proof. Let $\mathfrak{q}$ be an $\mathfrak{m}$-primary ideal of A generated by $\delta(A)$ elements. By the corollary,

$$\delta(A) = \delta(\mathfrak{q}) \geq l(\mathfrak{q}^n/\mathfrak{q}^{n+1}) + 1 = \deg l(\mathfrak{m}^n/\mathfrak{m}^{n+1}) + 1 = d(G_{\mathfrak{m}}(A)).$$

□

Proposition 4.57. *Let $(A, \mathfrak{m})$ be a Noetherian local ring. If $x \in \mathfrak{m}$ is not a zero divisor, then*

$$d(G_{\mathfrak{m}/x}(A/(x))) < d(G_{\mathfrak{m}}(A)).$$

Proof. Since x is not a zero divisor, the map $a \to xa$ is an A-module isomorphism $A \to xA$. Let $A' = A/(x)$ and $\mathfrak{m}' = \mathfrak{m}/(x)$. We get an exact sequence of A-modules

$$\frac{xA}{xA \cap \mathfrak{m}^n} \hookrightarrow \frac{A}{\mathfrak{m}^n} \twoheadrightarrow \frac{A'}{\mathfrak{m}'^n}$$

By additivity of l, we have

$$l\left(\frac{A'}{\mathfrak{m}'^n}\right) = l\left(\frac{A}{\mathfrak{m}^n}\right) - l\left(\frac{xA}{xA \cap \mathfrak{m}^n}\right).$$

Now, $(\mathfrak{m}^n)$ is a stable $\mathfrak{m}$-filtration of A, so $(xA \cap \mathfrak{m})$ is a stable $\mathfrak{m}$-filtration of $xA \cong A$. Therefore the degrees and leading terms of $l(A/\mathfrak{m}^n)$ and $l(xA/(xA \cap \mathfrak{m}^n))$ are equal, so their difference has strictly lower degree. Then

$$\underbrace{\deg l\left(\frac{\mathfrak{m}'^n}{\mathfrak{m}'^{n-1}}\right) + 1}_{d(G_{\mathfrak{m}/x}(A/(x)))} = \deg l\left(\frac{A'}{\mathfrak{m}'^n}\right) < \deg l\left(\frac{A}{\mathfrak{m}^n}\right) = \underbrace{\deg l\left(\frac{\mathfrak{m}^n}{\mathfrak{m}^{n+1}}\right) + 1}_{d(G_{\mathfrak{m}/x}(A/(x)))}.$$

□

Proposition 4.58. *Let $(A, \mathfrak{m})$ be a Noetherian local ring. Then*

$$d(G_{\mathfrak{m}}(A)) \geq \dim A.$$

Proof. Proceed by induction on $d(G_{\mathfrak{m}}(A))$. If $d(G_{\mathfrak{m}}(A)) = 0$, then, for n sufficiently large, $l(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = 0$, so $\mathfrak{m}^n = \mathfrak{m}^{n+1}$. By Nakayama's lemma, $\mathfrak{m}^n = 0$. Sice A is Noetherian, it is Artinian. Therefore $\dim A = 0$.

Now suppose $d(G_{\mathfrak{m}}(A)) > 0$. If $\dim A = 0$, we are done; otherwise, take a nontrivial strictly descending chain of primes $\mathfrak{p}_r \supsetneq \cdots \supsetneq \mathfrak{p}_0$ $(r \geq 1)$. Now, $A' = A/\mathfrak{p}_0$ is a Noetherian local integral domain with maximal ideal $\mathfrak{m}' = \mathfrak{m}/\mathfrak{p}_0$. Let $x \in \mathfrak{p}_1 \setminus \mathfrak{p}_0$; then $x' = x + \mathfrak{p} \neq 0$. By the last proposition, $d(G_{\mathfrak{m}'/(x)}(A'/(x))) < d_{\mathfrak{m}'}(A')$.

We also have a surjective A-module homomorphism $A/\mathfrak{m}^n \twoheadrightarrow A'/\mathfrak{m}'^n$, so $l(A/\mathfrak{m}^n) \geq l(A'/\mathfrak{m}'^n)$; then $\deg(A/\mathfrak{m}^n) \geq \deg(A'/\mathfrak{m}'^n)$ and so $d(G_{\mathfrak{m}}(A) \geq G_{\mathfrak{m}'}(A'))$. By the proposition defining Hilbert polynomials, we get

$$d(G_{\mathfrak{m}'/(x)})\left(\frac{A'}{(x)}\right) < d(G_{\mathfrak{m}}(A)).$$

By induction, $\dim A'/(x) < d(G_{\mathfrak{m}}(A))$. Since the images of the $\mathfrak{p}_i$ in $A'/(x)$ remain distinct, $r - 1 \leq d(G_{\mathfrak{m}}(A)) - 1$. Hence $\dim A \leq d(G_{\mathfrak{m}}(A))$. □

Corollary 4.59. *The dimension of a Noetherian local ring is finite.*

Proposition 4.60. *Let $(A, \mathfrak{m})$ be a Noetherian local ring. Then*

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

Proof. Let $d = \dim A$. We want to show A contains an $\mathfrak{m}$-primary ideal generated by (at least) d elements.

We construct $x_1, \ldots, x_i \in \mathfrak{m}$ such that every prime ideal containing all of the x_i has height at least i. The $i = 0$ case is trivial; suppose $i \leq d$, and $x_1, \ldots, x_{i-1}$ have been constructed.

Claim: Let $I \trianglelefteq B$, where B is Noetherian. Then there are finitely many prime ideals of B minimal over I.

Indeed, consider $\operatorname{nil} B/I$. This is a finite intersection $\bigcap_i \mathfrak{p}_i$ of primes (exercise); by correspondence, every prime in R that is minimal over I descends to one of the $\mathfrak{p}_i$.

There are therefore only finitely many prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ of height $i-1$ containing $\{x_1, \dots, x_{i-1}\}$. Indeed, every such prime ideal is minimal among those containing $(x_1, \dots, x_{i-1})$. Now, by maximality, $\mathfrak{m}$ has height d; since $i-1 < d$, we must have $\mathfrak{m} \neq \mathfrak{p}_i$ for all i. By prime avoidance, $\mathfrak{m} \not\subseteq \bigcup_{j=1}^{s} \mathfrak{p}_j$, so find $x_i \in \mathfrak{m} \setminus \bigcup_j \mathfrak{p}_j$.

Let $\mathfrak{q}$ be a prime ideal containing $(x_1, \dots, x_i)$, and let $\mathfrak{p}$ be minimal among prime ideals between $(x_1, \dots, x_i)$ and $\mathfrak{q}$. If $\mathfrak{p} = \mathfrak{p}_j$ for some $1 \leq j \leq s$, we have $x_i \in \mathfrak{q} \setminus \mathfrak{p}$, so $\mathfrak{q} \supsetneq \mathfrak{p}$; then

$$\operatorname{ht} \mathfrak{q} > \operatorname{ht} \mathfrak{p} = i - 1.$$

Otherwise, by induction we have

$$\operatorname{ht} \mathfrak{q} \geq \operatorname{ht} \mathfrak{p} \geq i.$$

In any case, $\operatorname{ht} \mathfrak{q} \geq i$.

Then consider

$$\sqrt{(x_1, \dots, x_d)} = \bigcap_{\substack{\mathfrak{p} \in \operatorname{Spec} A \\ (x_1, \dots, x_d) \in \mathfrak{p}}} \mathfrak{p} = \mathfrak{m},$$

since the only prime of height at least d is $\mathfrak{m}$. □

Proposition 4.61 (Krull's height theorem)**.** *Let A be a Noetherian ring, and let $x_1, \dots, x_r \in A$. Then every minimal prime $\mathfrak{p}$ containing $\mathfrak{a} = (x_1, \dots, x_r)$ has height at most r.*

Proof. We localise at $\mathfrak{p}$. Now, $\mathfrak{p}^e$ is the unique prime ideal containing $\mathfrak{a}^e$, so $\sqrt{\mathfrak{a}^e} = \mathfrak{p}^e$ (since $A_\mathfrak{p}$ is Noetherian). Therefore $\mathfrak{a}^e$ is $\mathfrak{p}^e$-primary. Then

$$\mathfrak{a}^e = \left(\frac{x_1}{1}, \dots, \frac{x_r}{1} \right),$$

so $\operatorname{ht} \mathfrak{p} = \dim A_\mathfrak{p} = \delta(A_\mathfrak{p}) \leq \delta(\mathfrak{p}^e) \leq r$. □

5 Tensor products and flatness

5.1 Tensor products

Let A be a ring, and suppose M and N are A-modules. Their *tensor product* $M \otimes N$ is the A-module of finite sums of formal products $m \otimes n$, constrained by A-linearity. We will make this precise soon, but first we will look at an example.

Example 5.1. Let $A = \mathbb{Z}$. Then $\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/3\mathbb{Z} = 0$. Indeed,

$$a \otimes b = (3a) \otimes b = a \otimes (3b) = a \otimes 0 = 0$$

Example 5.2. Let $A = k$ be a field. If V and W are k-vector spaces, then $V \otimes W$ is a vector space of dimension $\dim V \cdot \dim W$.

Definition 5.3. For A-modules M,N and L, an A-bilinear map $f : M \times N \to L$ is a map such that $f(m, -) : N \to L$ and $f(-, n) : M \to L$ are A-linear for all $m \in M$ and $n \in N$.

Let A be a ring, and let S be a set. Write

$$A^{\oplus S} = \bigoplus_{s \in S} A \cdot s = \left\{ \sum_{i=1}^{l} a_s \cdot s \mid l \geq 0, a_s \in A \right\}.$$

Definition 5.4. Let M and N be A-modules. Their **tensor product** is

$$M \otimes N = \frac{A^{\otimes M \times N}}{K},$$

where K is the A-submodule generated by

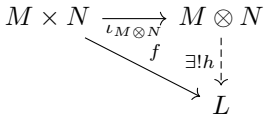
- $(m_1, n) + (m_2, n) - (m_1 + m_2, n)$ for each $m_1, m_2 \in M$ and $n \in N$.
- $(m, n_1) + (m, n_2) - (m, n_1 + n_2)$ for each $m \in M$ and $n_1, n_2 \in N$.
- $a(m, n) - (am, n)$ and $a(m, n) - (m, an)$ for each $m \in M$, $n \in N$ and $a \in A$.

The image of $1(m, n)$ in $M \otimes N$ is written $m \otimes n$.

We have a natural A-bilinear map

$$\begin{aligned} \iota_{M \otimes N} : M \times N &\to M \otimes N \\ (m, n) &\to m \otimes n. \end{aligned}$$

Proposition 5.5 (Universal property of the tensor product)**.** *For every A-module L and A-bilinear map $f : M \times N \to L$, there is a unique A-module homomorphism $h : M \otimes N \to L$ such that $f = h \circ i_{M \otimes N}$.*



Proof. Suppose such a map h exists. Then $f(m, n) = h(m \otimes n)$, so h is determined by $\operatorname{im} \iota_{M \otimes N}$, which generates $M \otimes N$. Thus we have uniqueness.

For existence, consider the A-linear map $\tilde{h} : A^{\oplus M \times N} \to L$ given on a basis by $\tilde{h}(1 \cdot (m, n)) = f(m, n)$. Since f is bilinear, it maps $K \to 0$, so $\tilde{h}$ descends to a linear map $h : M \otimes N \to L$. By construction,

$$h(m \otimes n) = \tilde{h}(1(m, n)) = f(m, n).$$

□

As with localisation, the tensor product – precisely, the pair $(M \otimes N, \iota_{M \otimes N})$ – is determined up to unique isomorphism by this universal property.

Showing that an element in a particular tensor product doesn't vanish might seem difficult. The next proposition provides a way of doing this.

Proposition 5.6. *Consider $x = \sum_{i=1}^{l} m_i \otimes n_i \in M \otimes N$. Then $x \neq 0$ iff there is some A-module L and A-bilinear map $f : M \times N \to L$ such that $\sum_{i=1}^{l} f(m_i, n_i) \neq 0$.*

Proof. Suppose $x = 0$, and let $f : M \times N \to L$ be an A-bilinear map. By the universal property, $f = h \circ \iota_{M \otimes N}$ for some A-linear map $h : M \otimes N \to L$. Then

$$\sum_{i=1}^{l} f(m, n) = \sum_{i=1}^{l} h(m_i \otimes n_i) = h(0) = 0.$$

Conversely, suppose $x \neq 0$. Let $L = M \otimes N$ and $f = \iota_{M \otimes N}$; then

$$0 \neq x = \sum_{i=1}^{l} \iota_{M \otimes N}(m_i, n_i).$$

□

Example 5.7. Let $A = \mathbb{Z}$, and consider $2 \otimes 1 \in \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}$. Then

$$2 \otimes 1 = 1 \otimes 2 = 1 \otimes 0 = 0.$$

However, consider $2 \otimes 1 \in 2\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}$. Then in fact $2 \otimes 1 \neq 0$. Indeed, let $L = \mathbb{Z}/2\mathbb{Z}$, and map

$$\begin{aligned} b : 2\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} &\to \mathbb{Z}/2\mathbb{Z} \\ (2n, x + 2\mathbb{Z}) &\to nx + 2\mathbb{Z}. \end{aligned}$$

Then $b(2 \otimes 1) = 1 \neq 0$.

This example shows that tensor products of submodules do not embed.

Proposition 5.8. *If $\sum_i m_i \otimes n_i = 0$ in $M \otimes N$, then there are finitely-generated submodules $M' \leq M$, $N' \leq N$ such that $\sum_i m_i \otimes n_i = 0$ in $M' \otimes N'$.*

Proof. Exercise. Intuitively, the relation making the sum vanish only uses finitely many element of M and N. □

Proposition 5.9. *There are natural isomorphisms*

(i)

$$\begin{aligned} M \otimes N &\xrightarrow{\simeq} N \otimes M \\ m \otimes n &\longrightarrow n \otimes m. \end{aligned}$$

(ii)

$$\begin{aligned} (M \otimes N) \otimes P &\xrightarrow{\simeq} M \otimes (N \otimes P) \coloneqq M \otimes N \otimes P \\ (m \otimes n) \otimes p &\longrightarrow m \otimes (n \otimes p) \end{aligned}$$

(iii)

$$\left(\bigoplus_{i\in I} M_i\right) \otimes P \xrightarrow{\simeq} \bigoplus_{i\in I}(M_i \otimes P)$$
$$(m_i \otimes p) \longrightarrow (m_i \otimes p)$$

(iv)

$$A \otimes M \xrightarrow{\simeq} M$$
$$(a, m) \longrightarrow am.$$

(v) Let $M' \leq M$ and $N' \leq N$ be submodules. Then

$$\frac{M}{M'} \otimes \frac{N}{N'} \xrightarrow{\simeq} \frac{M \otimes N}{L}$$
$$m \otimes n \longrightarrow m \otimes n,$$

where

$$L = \operatorname{span}_A \left(\{m' \otimes n \mid (m', n) \in M' \times N\} \cup \{m \otimes n' \mid (m, n') \in M \times N'\}\right).$$

Proof. Omitted: easy but tedious check. □

Example 5.10. Let V, W be vector spaces over k, with bases $\mathcal{B}$ and $\mathcal{C}$ respectively. Then $V \otimes W$ is a k-vector space with basis

$$\{b \otimes c \mid b \in \mathcal{B}, c \in \mathcal{C}\}.$$

In particular, $\dim(V \otimes W) = \dim V \cdot \dim W$.

5.2 Extension of scalars

Let $f : A \to B$ be a ring homomorphism.

Definition 5.11. Let M be a B-module. Then M is an A-module via

$$a \cdot m \coloneqq f(a) \cdot m.$$

This is called *restriction of scalars* from B to A. We have a dual notion, called *extension of scalars* from A to B.

Definition 5.12. Let N be an A-module. View B as an A-module; then the tensor product $N_B \coloneqq B \otimes_A N$ is a B-module via

$$b_0(b \otimes n) = (b_0 b) \otimes n.$$

Indeed, this multiplication arises from descending the A-bilinear maps

$$B \times N \to B \otimes_A N$$
$$(b, n) \to (b_0 b, n)$$

to maps $h_{b_0} : B \otimes_A N \to B \otimes_A N$. The map

$$\begin{aligned} B &\to \mathrm{End}_{\mathbb{Z}}(B \otimes_A N) \\ b_0 &\to h_{b_0} \end{aligned}$$

is then a ring homomorphism.

Example 5.13. Consider the inclusion $\mathbb{R} \hookrightarrow \mathbb{C}$. We have

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^n \cong \mathbb{C}^n.$$

Example 5.14. Let A be a ring, S a set, and $M = A^{\oplus S}/K$ for some submodule K. Let $f : A \to B$ be a ring homomorphism. We have

$$(A^{\oplus S})_B = B \otimes_A A^{\oplus S} \cong (B \otimes_A A)^{\oplus S} \cong B^{\oplus S};$$

this maps $b \otimes v \to bf(v)$, where f acts coordinate-wise.

Then

$$M_B = \left(\frac{A^{\oplus S}}{K}\right)_B = \frac{B}{0} \otimes_A \frac{A^{\oplus S}}{K} \cong \frac{B \otimes_A A^{\oplus S}}{\{b \otimes k \mid b \in B, k \in K\}} \cong \frac{B^{\oplus S}}{\mathrm{span}_B f(K)},$$

where f acts coordinate-wise on K.

In particular, if M is finitely generated (as an A-module), then so is M_B (as a B-module).

Now suppose B and C be A-algebras. Then $B \otimes_A C$ is in fact a ring via the multiplication

$$(b_1 \otimes c_1)(b_2 \otimes c_2) = (b_1 b_2) \otimes (c_1 c_2).$$

This is well defined. Indeed, fix $b_1 \in B$ and $c_1 \in C$; then the map

$$\begin{aligned} B \times C &\to B \otimes C \\ (b, c) &\to (b_1 b) \otimes (c_1 c) \end{aligned}$$

is bilinear, and gives rise to the multiplication above, so multiplication is linear; it is then easy to check it is a ring multiplication.

Now, $B \otimes C$ is a B- and a C- algebra via $b \to b \otimes 1$ and $c \to 1 \otimes c$. Then $B \otimes C$ is an A-algebra in two ways: $A \to B \to B \otimes C$ and $A \to C \to B \otimes C$. By construction, these ways coincide.

Example 5.15. We can change the base ring of an algebra. Let $k \subseteq L$ be an extension of fields, and let $A = k[T_1, \ldots, T_n]/I$. Then $A_L = L \otimes_k A = L[T_1, \ldots, T_n]/I^e$. Note that, if $I = (f_1, \ldots, f_s)$, then also $I^e = (f_1, \ldots, f_s)$, so the tensor product has the same relations.

Tensor products are functorial: given maps $f : M \to N$ and $g : P \to Q$ of modules over a ring A, define

$$\begin{aligned} f \otimes g : M \otimes P &\to N \otimes Q \\ m \otimes p &\to f(m) \otimes g(p). \end{aligned}$$

This is an A-module homomorphism.

5.3 Flat modules

Proposition 5.16. *For an exact sequence*

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

of A-modules, and an A-module N, the sequence

$$M' \otimes N \xrightarrow{f\otimes \mathrm{Id}_N} M \otimes N \xrightarrow{g\otimes \mathrm{Id}_N} M'' \otimes N \longrightarrow 0$$

is exact.

Proof. Since g is surjective, so is $g \otimes \mathrm{Id}_N$: indeed, its image contains all pure tensors.

Now, $g \circ f = 0$, so

$$(g \otimes \mathrm{Id}_N) \circ (f \otimes \mathrm{Id}_N) = (g \circ f) \otimes \mathrm{Id}_N = 0 \otimes \mathrm{Id}_N = 0.$$

Hence $L \coloneqq \mathrm{im}(f \otimes \mathrm{Id}_N) \subseteq \ker(g \otimes \mathrm{Id}_N)$. Now consider

$$\begin{aligned} \varphi : \frac{M \otimes N}{L} &\to M'' \otimes N \\ x + L &\to (g \otimes \mathrm{Id}_N)(x). \end{aligned}$$

Further, the bilinear map

$$\begin{aligned} M \times N &\to \frac{M \otimes N}{L} \\ m \otimes n + L \end{aligned}$$

vanishes on $f(M') \times N$, so it descends to a bilinear map $M/f(M') \times N \to (M \otimes N)/L$. But $M/f(M') \cong M''$, so we get a bilinear map

$$\begin{aligned} M'' \times N &\to \frac{M \otimes N}{L} \\ (g(m), n) &\to m \otimes n + L. \end{aligned}$$

By the universal property, we get a map

$$\begin{aligned} \psi : M'' \otimes N \&to \frac{M \otimes N}{L} \\ g(m) \otimes n &\to m \otimes n + L. \end{aligned}$$

Evaluating on pure tensors, we see φ and ψ are inverses. Fix $x \in \ker(g \otimes \mathrm{Id}_N)$; then

$$x + L = \psi(\varphi(x + L)) = \psi(\underbrace{(g \otimes \mathrm{Id}_N)x}_{=0}) = 0 + L.$$

Hence $x \in L = \mathrm{im}(f \otimes \mathrm{Id}_N)$. □

Note that, if $M' \to M \to M''$ is exact, then $M' \otimes N \to M \otimes N \to M'' \otimes N$ might *not* be. For example, consider

$$0 \longrightarrow \mathbb{Z} \xhookrightarrow{\cdot 2} \mathbb{Z}$$

and tensor with $\mathbb{Z}/2\mathbb{Z}$. We get

$$0 \longrightarrow \mathbb{Z} \otimes \tfrac{\mathbb{Z}}{2\mathbb{Z}} \xrightarrow{\cdot 2} \mathbb{Z} \otimes \tfrac{\mathbb{Z}}{2\mathbb{Z}}$$

Since the map is not injective, the sequence is not exact.

Definition 5.17. An A-module N is **flat** if, for all injections $f : M_1 \hookrightarrow M_2$ of A-modules, the map $f \otimes \mathrm{Id}_N : M_1 \otimes N \to M_2 \otimes N$ is also injective.

Examples 5.18.

1. Free A-modules are flat: under the isomorphisms $M_i \otimes A^{\bigoplus S} \cong M_i^{\bigoplus S}$, $f \otimes \mathrm{Id}_{A^{\bigoplus S}}$ just becomes f applied component-wise.
2. Projective A-modules are flat. These are A-modules N_1 such that the sum $N_1 \oplus N_2 \cong A^{\bigoplus S}$ is free for some A-module N_2.

   Indeed,
   $$M_1 \otimes (N_1 \oplus N_2) \xrightarrow{f \otimes \mathrm{Id}} M_2 \otimes (N_1 \oplus N_2)$$
   is injective, so
   $$(M_1 \otimes N_1) \oplus (M_1 \otimes N_2) \xrightarrow{(f \otimes \mathrm{Id}) \oplus (f \otimes \mathrm{Id})} (M_2 \otimes N_1) \oplus (M_2 \otimes N_2)$$
   is injective. Thus N_1 is flat.

Suppose $x \in A$ is not a zero divisor; then the map $A \xrightarrow{\cdot x} A$ is injective. Let M be a flat A-module; applying the isomorphism $M \cong A \oplus_A M$, we see $M \xrightarrow{\cdot x} M$ is injective. Hence M is torsion-free.

5.4 The Tor functor

We will now meet some homological algebra.

Definition 5.19. Let M and N be modules over a ring A. A **free resolution** for N is an exact sequence

$$\ldots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow\!\!\!\!\rightarrow N$$

where each F_i is a free A-module. Then let $\mathrm{Tor}_i^A(M, N)$ be the i^{th} homology group of the chain complex below (a chain complex is a sequence of A-modules such that the composition of each pair of adjacent transition maps is 0).

$$\ldots \longrightarrow M \otimes_A F_1 \longrightarrow M \otimes_A F_0 \longrightarrow 0$$

Explicitly,

$$\mathrm{Tor}_i^A(M, N) = \frac{\ker(M \otimes_A F_i \to M \otimes_A F_{i-1})}{\mathrm{im}(M \otimes_A F_{i+1} \to M \otimes_A F_i)}.$$

We can omit A from the notation, writing $\mathrm{Tor}_i(M,N)$. Free resolutions always exist, and the groups $\mathrm{Tor}_i^A(M,N)$ are independent of the choice of resolution. We also have $\mathrm{Tor}_i(M,N) \cong \mathrm{Tor}_i(N,M)$. We will not prove any of these facts, but they are in any book on homological algebra.

Examples 5.20.

(i) By right exactness, $\mathrm{Tor}_0^A(M,N) = M \otimes_A N$.

(ii) Suppose $x \in A$ is not a zero divisor. Then $A/(x)$ has a free resolution

$$\ldots \longrightarrow 0 \longrightarrow A \xrightarrow{\cdot x} A \longrightarrow\!\!\!\!\!\rightarrow A/(x)$$

Let M be an A-module; we can then compute

$$\mathrm{Tor}_i\left(\frac{A}{x}, N\right) = \begin{cases} \frac{N}{xN} & i = 0 \\ (0 :_N x) & i = 1 \\ 0 & i > 1 \end{cases}.$$

Here, $(0 :_N x) = \{x \in N \mid xn = 0\}$.

Take a SES of A-modules

$$N' \hookrightarrow N \longrightarrow\!\!\!\!\!\rightarrow N''$$

and free resolutions

$$F_1' \longrightarrow F_0' \longrightarrow\!\!\!\!\!\rightarrow N'$$

$$F_1'' \longrightarrow F_0'' \longrightarrow\!\!\!\!\!\rightarrow N''$$

Then $F_i = F_i' \oplus F_i''$ yields a free resolution for N. The diagram below then commutes, with exact rows and columns.

$$\begin{array}{ccccc}
N' & \hookrightarrow & N & \longrightarrow\!\!\!\!\!\rightarrow & N'' \\
\uparrow\!\!\uparrow & & \uparrow\!\!\uparrow & & \uparrow\!\!\uparrow \\
F_0' & \hookrightarrow & F_0 & \longrightarrow\!\!\!\!\!\rightarrow & F_0'' \\
\uparrow & & \uparrow & & \uparrow \\
F_1' & \hookrightarrow & F_1 & \longrightarrow\!\!\!\!\!\rightarrow & F_1'' \\
\uparrow & & \uparrow & & \uparrow \\
\vdots & & \vdots & & \vdots
\end{array}$$

Tensoring with M, we get a commutative diagram with exact rows (by right

exactness); each column remains a chain complex.

$$\begin{array}{ccccc}
N' \otimes M & \hookrightarrow & N \otimes M & \twoheadrightarrow & N'' \otimes M \\
\uparrow\uparrow & & \uparrow\uparrow & & \uparrow\uparrow \\
F_0' \otimes M & \hookrightarrow & F_0 \otimes M & \twoheadrightarrow & F_0'' \otimes M \\
\uparrow & & \uparrow & & \uparrow \\
F_1' \otimes M & \hookrightarrow & F_1 \otimes M & \twoheadrightarrow & F_1'' \otimes M \\
\uparrow & & \uparrow & & \uparrow \\
\vdots & & \vdots & & \vdots
\end{array}$$

This naturally induces an exact sequence

$$\mathrm{Tor}_i(M, N') \to \mathrm{Tor}_i(M, N) \to \mathrm{Tor}_i(M, N'');$$

we also get a *connecting homomorphism* $\partial_i : \mathrm{Tor}_i(M, N'') \to \mathrm{Tor}_{i-1}(M, N')$ which gives a LES

$$\begin{array}{ccccccc}
\ldots & \xrightarrow{\partial_{i+1}} & \mathrm{Tor}_i(M, N') & \longrightarrow & \mathrm{Tor}_i(M, N) & \longrightarrow & \mathrm{Tor}_i(M, N'') \\
& & & \searrow^{\partial_i} & & & \\
& & \mathrm{Tor}_{i-1}(M, N') & \longrightarrow & \mathrm{Tor}_{i-1}(M, N) & \longrightarrow & \mathrm{Tor}_{i-1}(M, N'') \xrightarrow{\partial_{i-1}} \ldots
\end{array}$$

We construct the connecting maps by doing the only sensible thing possible at each step to traverse the previous diagram.

This sequence ends

$$\cdots \to N' \otimes M \to N \otimes M \twoheadrightarrow N'' \otimes M.$$

Recall that, since $- \otimes M$ is not left exact, the map $N' \otimes M \to N \otimes M$ need not be injective. The connecting maps ∂_i allow us to instead continue the exact sequence to the left indefinitely.

Lemma 5.21. *Let $I \trianglelefteq A$. The natural map $I \otimes_A M \to A \otimes_A M \cong M$ is injective iff $\mathrm{Tor}_1(A/I, M) = 0$.*

Proof. We have a SES $I \hookrightarrow A \twoheadrightarrow A/I$; the induced LES on Tor is

$$\cdots \to \mathrm{Tor}_1(A, M) \to \mathrm{Tor}_1(A/I, M) \to I \otimes M \to A \otimes M \twoheadrightarrow A/I \otimes M.$$

Using the free resolution $0 \to A \twoheadrightarrow A$, we can compute that $\mathrm{Tor}_1(A, M) = 0$. Therefore $I \otimes M \to A \otimes M$ is injective iff the injection $\mathrm{Tor}_1(A/I, M) \hookrightarrow I \otimes M$ is zero. □

We now apply these ideas to flatness.

Proposition 5.22. *An A-module M is flat iff, for every finitely generated ideal $I \trianglelefteq A$, the natural map $\iota_I : I \otimes_A M \to M$ is injective.*

Proof.
$\Rightarrow$: Apply flatness to $I \hookrightarrow A$.

$\Leftarrow$: Suppose ι_I is injective for any finitely generated I.

Claim 1: The natural map $\iota_J : J \otimes_A M \to M$ is injective for *any* ideal $J \trianglelefteq A$.

Indeed, take $x = \sum_{i=1}^{k} j_i \otimes m_i \in \ker \iota_J$, so that $\sum_i j_i m_i = 0 \in M$. Let $I = (j_1, \ldots, j_k)$; then $x \in \ker \iota_I$. Since I is finitely generated, by assumption $x = 0$. Hence ι_J is injective.

Now let $N' \hookrightarrow N$ be an inclusion of A-modules. Identifying N' with its image in N, we can assume that $N' \leq N$. Let $\iota : N' \otimes_A M \to N \otimes_A M$ be the natural map.

Claim 2: If N'/N is cyclic, then ι is injective.

Let $N/N' = xA$. Since the map $A \xrightarrow{\cdot x} N/N'$ is surjective, we have $N/N' \cong A/J$ for some $J \trianglelefteq A$. Now, consider the exact sequence

$$\mathrm{Tor}_1(N/N', M) \longrightarrow N' \otimes_A M \xrightarrow{\iota} N \otimes_A M$$

Then $\mathrm{Tor}_1(N/N', M) \cong \mathrm{Tor}_1(A/J, M)$; by the last lemma and claim 1, $\mathrm{Tor}_1(A/J, M) = 0$, and so ι is injective by exactness.

Claim 3: If N'/N is finitely generated, then ι is injective.

We have a filtration

$$N' = N_0 \leq N_1 \leq \cdots \leq N_m = N$$

with each successive quotient N_{i+1}/N_i cyclic. By claim 2, the natural maps $N_i \otimes_A M \to N_{i+1} \otimes_A M$ are all injective. Therefore their composition ι is injective.

We have now done enough prove the result in general. Indeed, suppose

$$x \in \sum_{i=1}^{k} n_i' \otimes m_i \in \ker \iota.$$

As in claim 1, we restrict ι to the finitely generated module $n_1'A + \cdots + n_k'A$; by claim 3, $x = 0$. Hence ι is injective. □

6 Discrete Valuation Rings

Definition 6.1. Let K be a field. A (normalised) **discrete valuation** on K is a surjective group homomorphism $v : K^\times \to \mathbb{Z}$ such that $v(x + y) \geq \min\{v(x), v(y)\}$.

By convention, write $v(0) = \infty$.

Definition 6.2. Let v be a discrete valuation on a field K. Its **valuation ring** is

$$\mathcal{O}_K = \{x \in K \mid v(x) \geq 0\}.$$

Such a ring is called a **discrete valuation ring** (DVR).

Note that $\operatorname{Frac} \mathcal{O}_K = K$.

Example 6.3. Let $p \in \mathbb{Z}$ be prime. Write $x \in \mathbb{Q}$ as $x = p^k \frac{a}{b}$ for $a, b \nmid p$; then $v(x) = k$ is a discrete valuation on $\mathbb{Q}$ with valuation ring $\mathcal{O}_K = \mathbb{Z}_{(p)}$.

Proposition 6.4. *Every DVR A is a local PID.*

Proof. Let the associated field and valuation be K and v.

Take nonzero elements $x, y \in A$. Since $v(x^{-1}) = -v(x)$, we have that $x \in A^\times$ iff $v(x) = 0$. Therefore, $v(x) = v(y)$ iff $v(xy^{-1}) = 0$, iff x, y are associate.

Since $v : K \to \mathbb{Z}$ is surjective, there is some $\pi \in A$ with $v(\pi) = 1$. This is called a *uniformiser* of A. Observe that $x \sim \pi^{v(x)}$ (they are associate).

Claim: The nonzero ideals of A are exactly (π^k) $(k \in \mathbb{N})$.

Indeed, let $\mathfrak{a} \trianglelefteq A$ be nonzero. Let $l = \min v(\mathfrak{a})$, and find $y \in \mathfrak{a}$ such that $v(y) = l$; then $y \sim \pi^l$, so $\pi^l \in \mathfrak{a}$. If $x \in \mathfrak{a}$, then $v(x) \geq l$, so

$$x \sim \pi^{v(x)} = \pi^{v(x)-l}\pi^l,$$

and so $x \in (\pi^l)$. Hence $\mathfrak{a} = (\pi^l)$.

Therefore A is a PID with unique maximal ideal (π). □

The converse is also true: let $K = \operatorname{Frac} A$, and let $v(u\pi^k) = k$, where $u \in A^\times$. It is easy to check that all elements of $K^\times$ are of this form, and that v is indeed a valuation on K.