Commutative Algebra *

Zhiyuan Bai

Compiled on June 6, 2023

This document serves as a set of revision materials for the Cambridge Mathematical Tripos Part III course *Commutative Algebra* in Michaelmas 2022. However, despite its primary focus, readers should note that it is NOT a verbatim recall of the lectures, since the author might have made further amendments in the content. Therefore, there should always be provisions for errors and typos while this material is being used.

Contents

0 Introduction **2**

1 Polynomial Algebras **2**
1.1 Hilbert Basis Theorem 2
1.2 Noether Normalisation Theorem 3
1.3 Hilbert's Nullstellensatz 6
1.4 The Zariski Topology 8

2 Localisation **9**
2.1 Definition and Universal Property 9
2.2 Ideals in Life 10
2.3 Lying-Over and Going-Up 11
2.4 Going-Down 12

3 Dimension Theory **14**
3.1 Krull Dimension and Transcendental Dimension 14
3.2 Intermezzo: Nakayama's Lemma 17
3.3 Intermezzzo: Artinian Rings 17
3.4 Intermezzzzo: Graded Rings; Composition Series 19
3.5 Poincaré Series and Hilbert Polynomial 21
3.6 Filtrations 22
3.7 Dimension Theory of Noetherian Local Rings 23

4 Tensor Products **26**
4.1 Tensor Products of Modules and Algebras 26
4.2 Flatness 28
4.3 The Tor Functor 29

5 Discrete Valuation Rings **32**

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

0 Introduction

In this course, a ring will always mean a commutative unital ring.
Let k be a field, a very interesting ring is the polynomial ring $A = k[T_1, \ldots, T_n]$ over k. For a subset $S \subset A$, we can look at its zero locus in k^n, namely $V(S) = \{x \in k^n : \forall f \in S, f(x) = 0\}$. A set $X \subset k^n$ is an algebraic set if $X = V(S)$ for some $S \subset A$. They are of central importance in algebraic geometry.
If $I = (S) = \{r_1 s_1 + \cdots + r_m s_m : r_i \in A, s_i \in S\}$ is the ideal generated by S in A, then $V(S) = V(I)$. So the algebraic properties of ideals could correspond to geometric properties of the corresponding algebraic sets, e.g. dimension, reducibility, local structures.
This course will focus on discussing the algebraic aspects of these objects, in order to give develop the correct tools one would use when dealing with objects in algebraic geometry and algebraic number theory.

1 Polynomial Algebras

1.1 Hilbert Basis Theorem

Let $A = k[T_1, \ldots, T_k]$ and $S \subset A$, possibly infinite. The question is whether we can find some finite $S_0 \subset S$ such that $V(S) = V(S_0)$. The answer is yes. This is a consequence of Hilbert's basis theorem.

Definition 1.1. A ring A is Noetherian if it satisfies one of the following equivalent conditions:
(i) Every ideal of A is finitely generated.
(ii) Every ascending chain of ideals $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$ in A stablises (the "ascending chain condition" (ACC) for ideals). That is, there is some m such that $\mathfrak{a}_m = \mathfrak{a}_{m'}$ for all $m' \geq m$.
(iii) Every nonempty set Σ of ideals of A has a maximal element, i.e. not contained in any other element in Σ.

It's clear that these conditions are indeed equivalent.

Example 1.1. 1. Any field is Noetherian since it only has two ideals $(0), (1)$ anyways. 2. Any PID is Noetherian.
3. (non-example) $k[T_1, T_2, \ldots]$ is not Noetherian, since the chain of ideals $(T_1) \subsetneq (T_1, T_2) \subsetneq (T_1, T_2, T_3) \subsetneq \cdots$ doesn't terminate.

Theorem 1.1 (Hilbert's Basis Theorem)**.** *Let B be a Noetherian ring, then every finitely-generated B-algebra A is Noetherian. In particular, $k[T_1, \ldots, T_n]$ is Noetherian.*

Recall that a B-algebra A is simply a ring A with a homomorphism $\phi : B \to A$ (the "structure homomorphism"). A homomorphism of B-algebras is a ring homomorphism commuting with the respective structure homomorphism. For $b \in B, a \in A$, we often write ba to denote $\phi(b)a$.
We say a B-algebra A finitely generated if there is a surjective homomorphism of B-algebras $B[T_1, \ldots, T_n] \to A$ for some n. In other words, there are some $a_1, \ldots, a_n \in A$ such that $A = \mathrm{Span}_B(\{\text{finite products of } a_i^j : i, j \geq 0\})$.

Proof. Quotients of Noetherian rings are obviously Noetherian. Furthermore, the isomorphism $B[T_1, \ldots, T_n] \cong B[T_1, \ldots, T_{n-1}][T_n]$ of B-algebras shows that it suffices to show that $A = B[T]$ is Noetherian.
Let $\mathfrak{a}$ be an ideal of $A = B[T]$. We shall show that it's finitely generated. For $i \geq 0$, we consider $\mathfrak{a}(i) = \{c_0 \in B : \exists c_1, \ldots, c_i, c_0 T^i + \cdots + c_{i-1} T + c_i \in \mathfrak{a}\}$. We shall construct a finitely generated ideal $\mathfrak{b} \leq \mathfrak{a}$ such that $\mathfrak{b}(i) = \mathfrak{a}(i)$ for all $i \geq 0$. We'll then show that this is enough to imply $\mathfrak{a} = \mathfrak{b}$.
We have the ascending chain of ideals $\mathfrak{a}(0) \subset \mathfrak{a}(1) \subset \cdots$ in B, so it stablises since B is Noetherian. Hence each $\mathfrak{a}(i)$ is finitely generated and we can choose some m such that $\mathfrak{a}(m') = \mathfrak{a}(m)$ for all $m' \geq m$.
For each $0 \leq i \leq m$, we take $b_{i,1}, \ldots, b_{i,n_i} \in B$ that generate $\mathfrak{a}(i)$ and take $f_{i,1}, \ldots, f_{i,n_i} \in \mathfrak{a}$ such that $f_{i,j}$ has leading coefficient $b_{i,j}$. It then makes sense to take $\mathfrak{b}$ to be the ideal generated by the (finitely many!) $f_{i,j}$'s. We readily have $\mathfrak{a}(i) = \mathfrak{b}(i)$ for all i.
If $\mathfrak{b} \neq \mathfrak{a}$, then we can take some $f \in \mathfrak{a} \setminus \mathfrak{b}$ of minimal degree, say i. But since $\mathfrak{a}(i) = \mathfrak{b}(i)$, there must some $f \in \mathfrak{b}$ such that $f - g \neq 0$ has degree smaller than i, a contradiction. □

The generating set given by the proof is pretty horrible. There's a better generating set that works way better, known as a Gröbner basis, which one can compute very easily using the Buchberger algorithm.

Remark. In particular, $A = k[T_1, \ldots, T_n]$ is Noetherian and therefore for any $S \subset A$ there is some finite $S_0 \subset A$ (in fact we can choose $S_0 \subset S$) with $(S) = (S_0)$. In particular $V(S) = V(S_0)$.

1.2 Noether Normalisation Theorem

Recall that a B-module M is an abelian group M equipped with a ring homomorphism $B \to \operatorname{End} M$ ("scalar multiplication"). In particular, a B-algebra A is automatically a B-module: The structure homomorphism $B \to A$ gives the scalar multiplication $ba = \theta(b)a$ (i.e. it defines the ring homomorphism $B \to \operatorname{End}((A, +)), b \mapsto (a \mapsto \theta(b)a)$).

Example 1.2. The k-algebra $k \mapsto k[T_1, \ldots, T_n]$ also gives $k[T_1, \ldots, T_n]$ the structure of a k-vector space.

Definition 1.2. Let A be a B-algebra, then A is finite over B if A is finitely generated as a B-module.

Recall that $S = \{s_1, \ldots, s_m\} \subset A$ generates A as a B-algebra if $A = \operatorname{Span}_B\{\text{finite products of } s_i^j : i, j\}$, whereas S generates A as a B-module if $A = \operatorname{Span}_B\{s_i : i\}$. So $k[T_1, \ldots, T_n]$ is finitely generated but not finite.

Theorem 1.2 (Noether Normalisation Theorem)**.** *For any finitely generated k-algebra A, there is a subalgebra $A' \subset A$ such that $A' \cong k[T_1, \ldots, T_n]$ (as k-algebras) for some n and A is finite over A'.*

The geometrical implication of this is that if $X \subset k^n$ is an algebraic set, then there is some $d \geq 0$ and a map $f : X \to k^d$ given by polynomials such that $0 < f^{-1}(\{y\}) < \infty$ for any $y \in k^d$. This d turns out to be equal to the dimension of X.

Example 1.3. 1. If L/K is a field extension with finite degree, then L is a finite K-algebra.
2. Consider $k[T, T^{-1}]$ which is a finitely generated k, $k[T]$ and $k[T - T^{-1}]$-algebra. It is certainly not finite over k or $k[T]$. But it is finite over $k[T - T^{-1}]$ and is spanned by $1, T$. This follows from the identity $T^2 - (T - T^{-1})T - 1 = 0$.

Definition 1.3. Let A be a B-algebra. Then $x \in A$ is integral over B if there is a monic polynomial $P \in B[T]$ such that $P(x) = 0$.
We say A is integral over B if every $x \in A$ is integral over B.

Note that if B is a field, then $x \in A$ is integral iff it is algebraic (i.e. P is allowed to be not monic).

Lemma 1.3 ("Cramer's rule")**.** *Let C be an $n \times n$ matrix over a ring A. Take a column vector $v \in A^n$ such that $Cv = 0$. Then $(\det C)v = 0$.*

Proof. $(\det C)v = ((\det C)I)v = (\operatorname{adj} C)Cv = (\operatorname{adj} C)0 = 0.$ □

Alternative proof. For a column vector $u \in A^n$, we write $C^{(u)}$ for C with the j^{th} column replaced by u. Then

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

as desired. □

Proposition 1.4. *Let A be a B-algebra, then the followings are equivalent:*
(i) A is a finitely generated integral B-algebra.
(ii) A is generated as a B-algebra by a finite set of integral elements.
(iii) A is finite over B.

Proof. (i) $\implies$ (ii): Clear.
(ii) $\implies$ (iii): Take integral $\alpha_1, \ldots, \alpha_n \in A$ that generates A as a B-alegbra. Then A is spanned by the finite products of $\alpha_i^j, 1 \le i \le n, 0 \le j \le m_i$ where m_i is the degree of a monic polynomial in $B[T]$ that vanishes at α_i.
(iii) $\implies$ (i): To be a finite B-module, A must be finitely generated. It suffices to show that A is integral over B. Take any $\alpha \in A$. Write $\phi : B \to A$ for the structure homomorphism of A as a B-algebra. Consider the subring $\phi(B)[\alpha]$ of A. As a $\phi(B)[\alpha]$-module, A is faithful in the sense that for any $b \in \phi(B)[\alpha]$, $bx = 0$ for all $x \in A$ only when $b = 0$ (indeed, one simply take $x = 1$). A is also finite, so the result follows from the next lemma. □

Lemma 1.5. *For rings $B \subset A$, $x \in A$ is B-integral if and only if there is some $B[x]$-submodule M of A that is faithful as a $B[x]$-module and finite as a B-module.*

Proof. For the "if" part, we know that $M = \mathrm{Span}_B\{e_1, \ldots, e_m\}$ for some $e_i \in A$. Since $xM \subset M$, there is some $m \times m$ matrix C over B such that

$$x \begin{pmatrix} e_1 \\ \vdots \\ e_m \end{pmatrix} = C \begin{pmatrix} e_1 \\ \vdots \\ e_m \end{pmatrix}$$

And therefore Lemma 1.3 shows that $\forall m \in M, \det(xI - C)m = 0$. Faithfulness means $\det(xI - C) = 0$. This is a monic polynomial in x with coefficient in B. As for the "only if" part, suppose x is B-integral, i.e. $x^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0$ for some $b_i \in B$. Then $M = \mathrm{Span}_B\{1, x, \ldots, x^{n-1}\}$ satisfies everything. □

Definition 1.4. Suppose A is an algebra over an infinite field k. We say $x_1, \ldots, x_n \in A$ are algebraically independent if whenever $f \in k[T_1, \ldots, T_n]$ has $f(x_1, \ldots, x_n) = 0$ we have $f = 0$. Equivalently, the k-algebra homomorphism $k[T_1, \ldots, T_n] \to k[x_1, \ldots, x_n], T_i \mapsto x_i$ is an isomorphism.

To demonstrate Theorem 1.2, we'll first give an example of how the proof is supposed to work.

Example 1.4. Take again $A = k[T, T^{-1}]$. We saw that A is finite over $k[T - T^{-1}]$.
To illustrate the proof strategy, note that $\{T, T^{-1}\}$ is not algebraically independent as they solve $TT^{-1} - 1 = 0$. However, if we choose some $c \in k$ and observe the formulation $A = k[T^{-1} - cT, T]$ gives the expression $cT^2 + (T^{-1} - cT)T - 1 = 0$. If $c \neq 0$, we can divide over and find T to be integral over $k[T^{-1} - cT]$, and so we are done by the Proposition 1.4 – A is finite over $k[T^{-1} - cT]$!

Proof of Theorem 1.2. For a finitely generated k-algebra A, we'll need to find algebraically independent $x_1, \ldots, x_n$ such that A is finite over $A' = k[x_1, \ldots, x_n]$. We do this by induction on the minimal number of generators of A as a k-algebra.
The base case is clear. For the induction step, assume that $x_1, \ldots, x_m \in A$ generate A as a k-algebra and m is minimal, and that the theorem is true for less than m generators. If $x_1, \ldots, x_m$ are algebraically independent over k, then we are done. Otherwise, we shall see that there are $c_1, \ldots, c_{m-1}$ in k such that x_n is integral over $k[x_1 - c_1x_m, \ldots, x_{m-1} - c_{m-1}x_m]$. This would imply the theorem by the induction hypothesis and Proposition 1.4.
As $x_1, \ldots, x_m$ are algebraically dependent, there is some nonzero polynomial $p \in k[T_1, \ldots, T_m]$ such that $p(x_1, \ldots, x_m) = 0$. Write p as a sum of its homogenous parts and P the part with highest degree. For scalars $c_1, \ldots, c_{m-1} \in k$ we set $g(T_1, \ldots, T_m) = p(T_1 + c_1T_m, \ldots, T_{m-1} + c_{m-1}T_m, T_m)$ which equals $P(c_1, \ldots, c_{m-1}, 1)T_m^r$ plus terms with lower degrees in T_m. We also have $g(x_1 - c_1x_m, \ldots, x_{m-1} - c_{m-1}x_m, x_m) = p(x_1, \ldots, x_m) = 0$.
If $P(c_1, \ldots, c_{m-1}, 1)$ is nonzero, then we can multiply g with some nonzero elements of k to get a monic polynomial and done with it. Now P is a nonzero homogeneous polynomial, which means that $P(T_1, \ldots, T_{m-1}, 1)$ is a nonzero polynomial. So if k is an infinite field then there must be some $c_1, \ldots, c_{m-1}$ such that $P(c_1, \ldots, c_{m-1}, 1)$ is nonzero. □

Remark. 1. To further interpret the proof, one can replace the change of variable in the proof by one that uses an upper-triangular unipotent matrix Q (so that $x = Qy$), in which case one shows that A is finite over $k[x_1, \ldots, x_m]$ for some $m \leq n$ for almost every Q.
2. The last step doesn't work for finite fields but, guess what, we're not proving that case in this course.

1.3 Hilbert's Nullstellensatz

Let k be a field. For each $x \in k^n$, we can associate with it an element of $\mathrm{Hom}_k(k[T_1, \ldots, T_n], k)$ that is the evaluation homomorphism. Conversely, every element $\phi \in \mathrm{Hom}_k(k[T_1, \ldots, T_n], k)$ gives an element $(\phi(T_1), \ldots, \phi(T_n)) \in k^n$. So k^n can be identified in bijection with $\mathrm{Hom}_k(k[T_1, \ldots, T_n], k)$.
On the other hand, every homomorphism $f \in \mathrm{Hom}_k(k[T_1, \ldots, T_n])$ gives rise to an ideal $\ker f \leq k[T_1, \ldots, T_n]$ which is maximal. For $x \in k^n$, the kernel determined by the homomorphism it associated with would be $(T_1 - x_1, \ldots, T_n - x_n)$. We therefore get a map from k^n to $\mathrm{mSpec}(k[T_1, \ldots, T_n])$, the set of maximal ideals of $k[T_1, \ldots, T_n]$. This map is clearly injective, but is it surjective? Not in general: (T^2+1) is maximal in $\mathbb{R}[T]$ but is not of the said form since $\mathbb{R}[T]/(T^2+1) \cong \mathbb{C}$. But the map is surjective if (and only if) k is algebraically closed.

Theorem 1.6 (Weak Nullstellensatz)**.** *Suppose $k = \bar{k}$, then all maximal ideals of $k[T_1, \ldots, T_n]$ have the form $(T_1 - x_1, \ldots, T_n - x_n)$ for some $x \in k^n$.*

Now fix $k = \bar{k}$ and consider the map $\mathbb{V}$ that takes an ideal I to an algebraic set $\mathbb{V}(I) \subset k^n$, which is surjective (with the codomain being the set of all algebraic subsets), and injective on the set of maximal ideals given the weak nullstellensatz. The map $\mathbb{V}$ is not injective in general, e.g. $\mathbb{V}((T_1)) = \mathbb{V}((T_1^2))$, but we do have a map the other way around, namely $\mathcal{I}$ which sends an algebraic subset V to the ideal $\mathcal{I}(V) = \{f \in k[T_1, \ldots, T_n] : f|_V = 0\}$. We do then have $\mathbb{V}(\mathcal{I}(V)) = V$. This is of course not a two-sided inverse. Indeed, we have $\mathcal{I}(\mathbb{V}((T_1^2))) = (T_1)$, so the operation $\mathcal{I}(\mathbb{V}(-))$ is "like taking roots".

Definition 1.5. $\sqrt{I}$ is called the radical of I. An ideal I is called radical if $I = \sqrt{I}$.

Example 1.5. 1. $\sqrt{\sqrt{I}} = \sqrt{I}$ ("the radical is radical").
2. If I is an ideal of $k[T_1, \ldots, T_n]$, then $\mathbb{V}(\sqrt{I}) = \mathbb{V}(I)$, even when k is not necessarily algebraically closed.

If I is an ideal of $k[T_1, \ldots, T_n]$, then it's clear that we have $\mathcal{I}(\mathbb{V}(I)) \supset \sqrt{I} = \{f \in k[T_1, \ldots, T_n] : \exists N, f^N \in I\}$.

Theorem 1.7 (Strong Nullstellensatz)**.** $\mathcal{I}(\mathbb{V}(I)) = \sqrt{I}$ *provided that* $k = \bar{k}$.

Therefore $\mathbb{V}$ becomes a bijection from the set of radical ideals to the set of algebraic subsets of k^n.
Let's now go back to not assume $k = \bar{k}$. Recall that a zerodivisor in a ring A is an element $a \in A$ such that there is some $b \in R \setminus \{0\}$ such that $ab = 0$, and R is an integral domain if 0 is the only zerodivisor.

Lemma 1.8. *If $A \subset B$ are rings and B is integral over A, then $A \cap B^\times = A^\times$.*

Proof. It's clear that $A^\times \subset A \cap B^\times$.
Conversely, suppose $a \in A$ and $b \in B$ have $ba = 1$. As b is integral over A, we have $b^m + a_1 b^{m-1} + \cdots + a_m = 0$ for some $a_i \in A$. Therefore $1 + a_1 a + a_2 a^2 + \cdots + a_m a^m = 0$, hence $a \in A^\times$. □

Lemma 1.9. *Let $A \subset B$ be integral domains with B integral over A. Then B is a field iff A is.*

Proof. If A is a field, then B certainly is as well. Conversely, suppose B is a field, then $B^\times = B \setminus \{0\}$, which means that $A^\times = A \cap B^\times = A \setminus \{0\}$ by the preceding lemma, i.e. A is a field. □

Proposition 1.10 (Zariski Lemma)**.** *Let $k \subset L$ be fields such that L is a finitely generated k-algebra. Then L/k is finite.*

In other words, the only situation where $k[T_1, \ldots, T_n]/I$ is a field is if it also has finite dimension over k.

Proof. By Theorem 1.2, there is some $y_1, \ldots, y_d \in L$ algebraically independent over k such that L is finite (hence integral) over $k[y_1, \ldots, y_d]$. But this means that $k[y_1, \ldots, y_d]$ is a field by the preceding lemma, which is not the case unless $d = 0$. □

Theorem 1.11 (Weak Nullstellensatz, stronger version than Theorem 1.6)**.** *For a field k and a proper ideal $\mathfrak{a}$ of $A = k[T_1, \ldots, T_n]$, there is a field extension L/k of finite degree and $\bar{x} \in L^n$ such that $f(\bar{x}) = 0$ for any $f \in \mathfrak{a}$.*

Proof. Let $\mathfrak{m}$ be a maximal ideal containing $\mathfrak{a}$ and $L = A/\mathfrak{m}$. Then L is generated as a k-algebra by $T_1 + \mathfrak{m}, \ldots, T_m + \mathfrak{m}$, hence by the preceding proposition we know L/k to be finite. And $\bar{x} = (T_1 + \mathfrak{m}, \ldots, T_m + \mathfrak{m})$ solves all the polynomials in $\mathfrak{m}$, hence all those in $\mathfrak{a}$. □

Remark. Let $p_1, \ldots, p_m \in k[T_1, \ldots, T_n]$. If there are $r_1, \ldots, r_m \in k[T_1, \ldots, T_n]$ such that $\sum_i r_i p_i = 1$, then $p_1, \ldots, p_m$ have no common solution in any field extension of k. The theorem says the converse: The existence of such $r_1, \ldots, r_m$ is the only obstruction to $p_1, \ldots, p_m$ having common solution in a (finite) field extension.
There are many versions of what's called the effective nullstellensatz. One of which says that if there is no $r_1, \ldots, r_m$ with

$$\sum_{i=1}^{m} r_i p_i = 1, \deg r_i \leq (\max\{3, \deg p_1, \ldots, \deg p_m\})^n$$

then there is no such $r_1, \ldots, r_m$ (without degree condition) satisfying the equation at all.
For fixed $p_1, \ldots, p_m$ the coefficients of $\sum_i r_i p_i$ are linear combinations of the coefficients of $r_1, \ldots, r_m$. So the effective nullstellensatz means that we can solve for $r_1, \ldots, r_m$ using linear algebraic methods (e.g. Gaussian elimination).

Corollary 1.12. *Theorem 1.6.*

Proof. The only choice of L is k itself. So any maximal ideal $\mathfrak{m}$ of $A = k[T_1, \ldots, T_n]$ admits some $x \in k^n$ with $\forall f \in \mathfrak{m}, f(x) = 0$. But then $\mathfrak{m} \subset (T_1 - x_1, \ldots, T_n - x_n)$, which means that $\mathfrak{m} = (T_1 - x_1, \ldots, T_n - x_n)$ by maximality. □

For a field k, we write $\mathbb{V}_k \subset k^n$ and $\mathcal{I}_k \leq k[T_1, \ldots, T_n]$ to denote what you think they are.

Theorem 1.13 (Strong Nullstellensatz, stated slightly more generally than Theorem 1.7)**.** *Let k be a field and $\bar{k}$ its algebraic closure. For an ideal $I \subset k[T_1, \ldots, T_n]$, we have $\mathcal{I}_k(\mathbb{V}_{\bar{k}}(\mathfrak{a})) = \sqrt{\mathfrak{a}}$.*

Proof. It's clear that $\mathcal{I}_k(\mathbb{V}_{\bar{k}}(I)) \supset \sqrt{I}$. Take $h \in \mathcal{I}_k(\mathbb{V}_{\bar{k}}(\mathfrak{a})) \setminus \{0\}$. Let's show that some power of h is in $\mathfrak{a}$. Choose a finite generating set $g_1, \ldots, g_m$ of $\mathfrak{a}$ and consider the ideal $\mathfrak{b} = (g_1, \ldots, g_m, 1 - Yh) \leq k[T_1, \ldots, T_n, Y]$. Then $\mathbb{V}_{\bar{k}} = \varnothing$, for if $(x_1, \ldots, x_n, t) \in \mathbb{V}_{\bar{k}}(\mathfrak{b})$, then $h(x_1, \ldots, x_n) = 0$ since $h \in \mathfrak{a} = \langle g_1, \ldots, g_m \rangle$ but $0 = 1 - th(x_1, \ldots, x_m) = 1$, contradiction. Therefore $\mathfrak{b} = k[T_1, \ldots, T_n, Y]$, in particular there is some $r_1, \ldots, r_{m+1} \in k[T_1, \ldots, T_n, Y]$ such that

$$1 = \sum_{i=1}^{m} g_i r_i + (1 - Yh) r_{m+1}$$

Consider the ring homomorphism $k[T_1, \ldots, T_n, Y] \to k(T_1, \ldots, T_m)$ given by $T_i \mapsto T_i, Y \mapsto 1/h$. Applying this to the identity above shows that

$$1 = \sum_{i=1}^{m} g_i(T_1, \ldots, T_m) r_i(T_1, \ldots, T_m, 1/h)$$

Multiplying both sides with a sufficiently large power (indeed, the largest power of Y in the r_i's) of h shows that $h \in \sqrt{\langle g_1, \ldots, g_m \rangle} = \sqrt{\mathfrak{a}}$. □

To summarise, if k is a field, then we always have $\mathbb{V}(\mathcal{I}(X)) = X$ when X is an algebraic subset of k^n. Moreover, if $k = \bar{k}$, then $\mathcal{I}(\mathbb{V}(\mathfrak{a})) = \mathfrak{a}$ for every radical ideal $\mathfrak{a}$. Therefore $\mathbb{V}$ and $\mathcal{I}$ are mutual inverses between algebraic subsets of k^n and radical ideals of $k[T_1, \ldots, T_n]$ when $k = \bar{k}$. For any ideal I, they also give a bijection between radical ideals containing I and algebraic sets containing $\mathbb{V}(C)$.

1.4 The Zariski Topology

For a field k, we can define a topology on k^n by naming all algebraic subsets of k^n as closed. This is a topology since $\varnothing = \mathbb{V}((1)), k^n = \mathbb{V}((0)), \mathbb{V}(IJ) = \mathbb{V}(I \cap J) = \mathbb{V}(I) \cup \mathbb{V}(J), \mathbb{V}(\sum_i I_i) = \bigcap_i \mathbb{V}(I_i)$. Provisionally, we write $\mathbb{A}_k^n$ (the "n-dimensional affine space over k") to denote k^n equipped with the Zariski topology.
For $f \in k[T_1, \ldots, T_n]$ we write $D(f) = \{x \in \mathbb{A}_k^n : f(x) \neq 0\}$. It's clear that $\{D(f) : f \in k[T_1, \ldots, T_n]\}$ is a basis for the Zariski topology on $\mathbb{A}_k^n$.

Remark. $\mathbb{A}_k^n$ is Hausdorff iff k is finite or $n = 0$. Indeed, if U, V are nonempty open subsets of $\mathbb{A}_k^n$, we choose $\varnothing \neq D(f) \subset U, \varnothing \neq D(g) \subset V$. Then $\varnothing \neq D(fg) \subset U \cap V$ if k is infinite, in particular $U \cap V \neq \varnothing$.

From here on out, we only consider nonempty topological spaces.

Definition 1.6. A topological space X is reducible if $X = X_1 \cup X_2$ with X_1, X_2 closed proper subsets of X. We say it's irreducible if it's not reducible. Equivalently, X is irreducible iff every two nonempty open subsets of X intersects.

Example 1.6. 1. $\mathbb{A}_k^n$ is irreducible.
2. Every singleton is irreducible.
3. A Hausdorff space is irreducible iff it's a singleton.
4. Suppose $k = \bar{k}$ and $p, q \in k[T_1, \ldots, T_n]$ are irreducible and $(p) \neq (q)$, then $X = \mathbb{V}((p)(q)) = \mathbb{V}((p)) \cup \mathbb{V}((q))$ and therefore X is reducible.

Let's ask the question we all know the answer to: When is $\mathbb{V}(\mathfrak{a})$ irreducible?

Definition 1.7. An ideal $I \lneq R$ is prime if $\forall a, b \in R, (a \notin I, b \notin I) \implies ab \notin I$.

Equivalently, I is prime iff R/I is nonzero and an integral domain.
Note that every maximal ideal is prime, and every prime ideal is radical.

Lemma 1.14. *If $\mathfrak{p} \leq R$ is prime and $I_1 \cap I_2 \subset \mathfrak{p}$, then either $I_1 \subset \mathfrak{p}$ or $I_2 \subset \mathfrak{p}$.*

Proof. Suppose for the sake of contradiction that $I_1 \notin \mathfrak{p}, I_2 \notin \mathfrak{p}$, then we can find $f \in I_1 \setminus \mathfrak{p}, g \in I_2 \setminus \mathfrak{p}$. But $fg \in I_1 \cap I_2 \in \mathfrak{p}$, contradiction. □

Proposition 1.15. *Suppose k is a field. Then $X \subset \mathbb{A}^n_k$ is an algebraic set, then X is irreducible iff $\mathcal{I}(X)$ is prime.*

Proof. Assume first that X is irreducible. Take $f, g \in k[T_1, \ldots, T_n]$ such that $fg \in \mathcal{I}(X)$. Then $X \subset \mathbb{V}(f) \cup \mathbb{V}(g)$, hence either $X \subset \mathbb{V}(f)$ or $X \subset \mathbb{V}(g)$ by irreducibility of X. WLOG the former happens. Then $(f) \subset \mathcal{I}(X)$, which means that $f \in \mathcal{I}(X)$.
Conversely, suppose $\mathcal{I}(X)$ is prime and $X \subset \mathbb{V}(I) \cup \mathbb{V}(J) = \mathbb{V}(IJ)$, then $IJ \subset \mathcal{I}(X)$, so by the preceding lemma either $I \subset \mathcal{I}(X)$ or $J \subset \mathcal{I}(X)$, i.e. either $X \subset \mathbb{V}(I)$ or $X \subset \mathbb{V}(J)$. □

So $\mathbb{V}(\mathfrak{a})$ is irreducible iff $\mathcal{I}(\mathbb{V}(\mathfrak{a}))$ is prime. When $k = \bar{k}$, this strengthens to the statement that $\mathbb{V}(\mathfrak{a})$ is irreducible iff $\sqrt{\mathfrak{a}}$ is prime.
We can in fact define the Zariski topology on a space associated to a general ring. For every ring R, we consider the set $\mathrm{Spec}(R) = \{\mathfrak{p} \leq R \text{ prime}\}$ equipped with a topology (the Zariski topology) whose closed sets are sets of the form $\mathbb{V}(I) = \{\mathfrak{p} \in \mathrm{Spec}\, R : I \leq \mathfrak{p}\}$ for an ideal I of R.
If $R = k[T_1, \ldots, T_n]$ with $k = \bar{k}$, then $\mathrm{Spec}(R)$ is the space of all irreducible algebraic subsets of $\mathbb{A}^n_k$. Indeed, the identification is a homeomorphism between the subspace of closed points in $\mathrm{Spec}(R)$ and $\mathbb{A}^n_k$.
Guess what, we also have a basis on $\mathrm{Spec}(R)$ conveniently of the form $D(f) = \{\mathfrak{p} \in \mathrm{Spec}(R) : f \notin \mathfrak{p}\}$.

2 Localisation

2.1 Definition and Universal Property

Let's speak about localisation (finally). Let A be a ring and $S \subset A$ be a subset. Somehow we want the elements of S invertible, just for fun. In any ring R, if $a, b \in R$ are invertible, then ab is also a unit, so S should at least be closed under multiplication. Moreover, since 1 is supposed to be invertible, we want also that $1 \in S$.

Definition 2.1. A subset $S \subset A$ is multiplicative if $1 \in S$ and $a, b \in S$ implies $ab \in S$.

Definition 2.2. Suppose A is a ring and $S \subset A$ is multiplicative. The localisation of A at S is the set $\{(a, s) : a \in A, s \in S\}/\sim$ where $(a, s) \sim (a', s')$ iff there is some $r \in S$ such that $r(as' - a's) = 0$.

For we denote by a/s the class of (a, s) in $S^{-1}A$. $S^{-1}A$ is made a ring via $(a/s)(a'/s') = (aa')/(ss')$ and $(a/s) + (a'/s') = (as' + a's)/(ss')$.
It's easy to check that this is well-defined and makes $S^{-1}A$ a ring with zero

$0/1$ and identity $1/1$. Since we're bored, let's verify the well-definedness of addition. Suppose $a/s = b/t, a'/s' = b'/t'$, then there are some $r, r' \in S$ such that $r(at-bs) = r'(a't'-b's') = 0$. Now $rr' \in S$ and $rr'((ss')(bt'+b't) - (as'+a's)(tt')) = -r's't'(r(at-bs)) - rst(r'(a't'-b's')) = 0$.
We have natural ring homomorphism $i_S : A \to S^{-1}A, a \mapsto a/1$. It is not necessarily injective. Indeed, $\ker i_S = \{a \in A : \exists s \in S, sa = 0\}$. So $\ker i_S = 0$ iff S has no zerodivisors. When $0 \in S$, then $S^{-1}A$ would indeed be the zero ring.

Proposition 2.1 (Universal Property of Localisation)**.** *For $s \in S$, $i_S(s)$ is a unit in $S^{-1}A$. For every ring B and every ring homomorphism $\phi : A \to B$ such that $\phi(S) \subset B^\times$, there is a unique ring homomorphism $h : S^{-1}A \to B$ such that $\phi = h \circ i_S$. Indeed, we must have $h(a/s) = \phi(a)\phi(s)^{-1}$*

Proof. Virtually nothing worth proving. □

Example 2.1. Suppose A is a ring and $f \in A$. We define $S_f = \{1, f, f^2, \ldots\}$. We write $A_f = S_f^{-1}A$. If f is nilpotent, then $0 \in S_f$ and therefore $A_f = 0$. When A is an integral domain and $f \neq 0$, then $A \hookrightarrow A_f = \{a/f^n : a \in A, n \in \mathbb{N}\} \subset \mathrm{FF}(A)$.
Say $A = \mathbb{Z}, f = 2$, then A_f consists of rational numbers of the form $a/2^n$ for some $a \in \mathbb{Z}, n \in \mathbb{N}$.

Proposition 2.2. *Suppose A is a ring and $S \subset A$ is a multiplicative subset. Then the map $\phi : A[T]/(Tf-1) \to A_f, T \mapsto 1/f$ is an isomorphism.*

Proof. The map $A[T] \to A_f, T \mapsto 1/f$ contains $Tf-1$ in its kernel, so ϕ is well-defined. On the other hand, $A \to A[T]/(Tf-1), a \mapsto a$ sends everything in S to a unit, therefore factors through $A_f \to A[T]/(Tf-1)$, which gives an inverse to ϕ. □

2.2 Ideals in Life

Let $\phi : A \to B$ be a ring homomorphisms. For any ideal $\mathfrak{b} \leq B$, we obtain an ideal $\mathfrak{b}^{\mathrm{c}} = \phi^{-1}\mathfrak{b} \leq A$ (the "contraction" of $\mathfrak{b}$).

Example 2.2. When $A \subset B$ and ϕ is the inclusion map, then $\mathfrak{b}^{\mathrm{c}} = \mathfrak{b} \cap A$.

On the other hand, for any ideal $\mathfrak{a} \leq A$, we can associate to it an ideal $\mathfrak{a}^{\mathrm{e}} = \phi(\mathfrak{a})B \leq B$ (the "extension" of $\mathfrak{a}$).

Example 2.3. 1. If ϕ is surjective, then $\mathfrak{a}^{\mathrm{e}} = \phi(\mathfrak{a})$. When it is in fact a quotient map $A \to B = A/I$, then $\mathfrak{a}^{\mathrm{e}} = (\mathfrak{a}+I)/I$.
2. Consider the inclusion $\phi : \mathbb{Z} \hookrightarrow \mathbb{Q}$, then $(0)^{\mathrm{e}} = (0)$ and $(a)^{\mathrm{e}} = (1)$ whenever $a \neq 0$. On the other hand, $(0)^{\mathrm{c}} = (0), (1)^{\mathrm{c}} = (1)$. So all ideals of $\mathbb{Q}$ can be obtained as extensions from ϕ, and only $(0), (1) \leq \mathbb{Z}$ can be obtained from contraction from ϕ.

In general, we have a bijection between contracted ideals of A and extended ideals of B. The bijection is simply given by extension (and, to the reverse direction, contraction). Indeed,

Proposition 2.3. *(i)* $\mathfrak{a} \subset \mathfrak{a}^{\mathrm{ec}}, \mathfrak{b}^{\mathrm{ce}} \subset \mathfrak{b}$.
(ii) $\mathfrak{a}^{\mathrm{ece}} = \mathfrak{a}^{\mathrm{e}}, \mathfrak{b}^{\mathrm{cec}} = \mathfrak{b}^{\mathrm{c}}$

Proof. (i) Follows from definition.
(ii) From (i) we have $\mathfrak{a}^{\mathrm{e}} \subset \mathfrak{a}^{\mathrm{ece}}$ by extending both sides of $\mathfrak{a} \subset \mathfrak{a}^{\mathrm{ec}}$, and plugging in $\mathfrak{b} = \mathfrak{a}^{\mathrm{e}}$ in $\mathfrak{b}^{\mathrm{ce}} \subset \mathfrak{b}$ gives $\mathfrak{a}^{\mathrm{e}} \supset \mathfrak{a}^{\mathrm{ece}}$, so $\mathfrak{a}^{\mathrm{e}} = \mathfrak{a}^{\mathrm{ece}}$. Similarly we have the second equality. □

Back to localisations. Let A be a ring and $S \subset A$ a multiplicative subset. As usual we take $i_S : A \to S^{-1}A, a \mapsto a/1$. Let $\mathfrak{a}$ be an ideal of A and $\mathfrak{b}$ an ideal of $B = S^{-1}A$. Then $\mathfrak{a}^{\mathrm{e}} = S^{-1}\mathfrak{a} = \{a/s : a \in \mathfrak{a}, s \in S\}$ and $\mathfrak{b}^{\mathrm{c}} = i_S^{-1}\mathfrak{b} = \{a \in A : a/1 \in \mathfrak{b}\}$.

Proposition 2.4. *Let A, S be as above.*
(i) $\mathfrak{b}^{\mathrm{ce}} = \mathfrak{b}$ for every $\mathfrak{b} \leq S^{-1}A$.
(ii) Extension and contraction gives a bijection from the set of prime ideals of A disjoint from S and the set of prime ideals in $S^{-1}A$.

Proof. Example sheet. □

Example 2.4. Let $\mathfrak{p}$ be a prime of A, then $S_{\mathfrak{p}} = A \setminus \mathfrak{p}$ is a multiplicative set. We write $A_{\mathfrak{p}} = S_{\mathfrak{p}}^{-1}A$ to be the localisation of A at the prime $\mathfrak{p}$.

The last proposition implies that there is a bijection between the set of primes of A contained in $\mathfrak{p}$ and the set of primes of $A_{\mathfrak{p}}$. Consequently, $S_{\mathfrak{p}}^{-1}\mathfrak{p} = \mathfrak{p}A_{\mathfrak{p}}$ must be the unique maximal ideal of $A_{\mathfrak{p}}$, so $A_{\mathfrak{p}}$ is a local ring.
Much information about A can be extracted from studying its localisations at primes, as we will see soon.

Example 2.5. Take $A = \mathbb{Z}$ and $\mathfrak{p} = pZ$, then $A_{\mathfrak{p}} = \{a/b : a, b \in \mathbb{Z}, p \nmid b\} \hookrightarrow \mathbb{Q}$, and the unique maximal ideal of $A_{\mathfrak{p}}$ is then $\{a/b : a, b \in \mathbb{Z}, p \mid a, p \nmid b\}$.

2.3 Lying-Over and Going-Up

Suppose we have an inclusion of rings $i : A \hookrightarrow B$. We have a map $i^* : \operatorname{Spec} B \to \operatorname{Spec} A$ given by contraction, which in this case is given by $\mathfrak{p} \mapsto i^{-1}\mathfrak{p} = \mathfrak{p} \cap A$.

Definition 2.3. Let $\mathfrak{p}$ be an ideal of A. An ideal $\mathfrak{q}$ of B is lying over $\mathfrak{p}$ if $\mathfrak{q} \cap A = \mathfrak{p}$.

Recall that if $i : A \hookrightarrow B$ is an integral extension of integral domains, then A is a field if and only if B is a field. Consequently,

Corollary 2.5. *Let $i : A \hookrightarrow B$ be an integral extension of rings. Let $\mathfrak{q}$ be a prime ideal of B, then $\mathfrak{q}$ is maximal in B iff $\mathfrak{q} \cap A$ is maximal in A.*

Remark. 1. For an extension of rings $i : A \hookrightarrow B$ and a multiplicative set $S \subset A$, then $S^{-1}A$ naturally embeds into $S^{-1}B = i(S)^{-1}B$.
2. If the extension $A \hookrightarrow B$ is integral, then $S^{-1}A \hookrightarrow S^{-1}B$ too is integral. Indeed, for any $b/s \in S^{-1}B$, we take some $f(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0 \in A[T]$ monic such that $f(b) = 0$, then $F(b/s) = 0$ where $F(T) = T^n + (a_{n-1}/s)T^{n-1} + \cdots + a_0/s^n \in (S^{-1}A)[T]$.

Proposition 2.6 (Lying-Over)**.** *Let $i : A \hookrightarrow B$ be an integral extension of rings and let $\mathfrak{p}$ be a prime of A. Then there is a prime $\mathfrak{q}$ of B lying over $\mathfrak{p}$.*

Example 2.6 (Non-example)**.** $\mathbb{Z} \subset \mathbb{Q}$ is not integral and the proposition fails.

Proof. By abuse of notation, for any prime $\mathfrak{p}$ of A, we also write $B_\mathfrak{p} = (A\backslash\mathfrak{p})^{-1}B$. $i_\mathfrak{p} : A_\mathfrak{p} \hookrightarrow B_\mathfrak{p}$ is an integral extension.
First of all, any maximal ideal of $B_\mathfrak{p}$ contracts to $\mathfrak{p}A_\mathfrak{p}$ under $i_\mathfrak{p}$ by Corollary 2.5.
Somehow we decided to draw a diagram

$$\begin{array}{ccc} B & \longrightarrow & B_\mathfrak{p} \\ {\scriptstyle i}\big\downarrow & & \big\downarrow{\scriptstyle i_\mathfrak{p}} \\ A & \longrightarrow & A_\mathfrak{p} \end{array}$$

Now for any prime $\mathfrak{p}$ of A, we choose a maximal ideal $\mathfrak{n} \leq B_\mathfrak{p}$ and set $\mathfrak{q} \leq B$ to be the contraction of $\mathfrak{n}$ along $B \to B_\mathfrak{p}$. Then $\mathfrak{q}$ contracts to $\mathfrak{p}$. □

Theorem 2.7 (Going-Up)**.** *Let $A \hookrightarrow B$ be an integral extension of rings. Suppose we have a chain of prime ideals $\mathfrak{p}_1 \leq \cdots \leq \mathfrak{p}_m \leq \cdots \leq \mathfrak{p}_n$ in A and a chain $\mathfrak{q}_1 \leq \cdots \leq \mathfrak{q}_m$ in B such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for any $i \leq m$. Then there are prime ideals $\mathfrak{q}_{m+1} \leq \cdots \leq \mathfrak{q}_n$ of B such that $\mathfrak{q}_m \leq \mathfrak{q}_{m+1}$ and $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for all $i \leq n$.*

Proof. It suffices to prove the case where $n = 2, m = 1$. Suppose we have $\mathfrak{p}_1 \leq \mathfrak{p}_2$ in A and $\mathfrak{q}_1$ in B lying over $\mathfrak{p}_1$. Consider the integral extension $A/\mathfrak{p}_1 \hookrightarrow B/\mathfrak{q}_1$ which is an embedding since $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$. The preceding proposition yields a prime $\tilde{\mathfrak{q}}_2$ of $B/\mathfrak{q}_1$ lying over $\mathfrak{p}_2/\mathfrak{p}_1$. We know that $\tilde{\mathfrak{q}}_2 = \mathfrak{q}_2/\mathfrak{q}_1$ for some ideal $\mathfrak{q}_2$ of B, necessarily prime, containing $\mathfrak{q}_1$. It's easy to verify that $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$. □

Example 2.7 (Non-example)**.** Let's look at the extension $\mathbb{Z} \hookrightarrow \mathbb{Z}[T]$ which is very not an integral extension. And indeed the preceding theorem fails: The chain $(0) \subset (2)$ with $(1 + 2T)$ lying over (0) cannot be extended with an ideal $\mathfrak{q}_2 \subset \mathbb{Z}[T]$ lying over (2). Indeed, that would mean $\mathfrak{q}_2 \supset (1 + 2T, 2) = \mathbb{Z}[T]$ which cannot happen due to the primality of $\mathfrak{q}_2$.

Proposition 2.8 (Incomparability)**.** *Let $A \hookrightarrow B$ be an integral extension of rings and $\mathfrak{p}$ a prime ideal of A. Let $\mathfrak{q} \subset \mathfrak{q}'$ be prime ideals of B such that $\mathfrak{q} \cap A = \mathfrak{q}' \cap A = \mathfrak{p}$, then $\mathfrak{q} = \mathfrak{q}'$.*

Proof. Write $A_\mathfrak{p}$ and $B_\mathfrak{p} = (B \setminus \mathfrak{p})^{-1}B$ as usual. So $A_\mathfrak{p} \hookrightarrow B_\mathfrak{p}$ is an integral extension. Let $\mathfrak{q}B_\mathfrak{p}$ and $\mathfrak{q}'B_\mathfrak{p}$ denote the extensions of $\mathfrak{q}, \mathfrak{q}'$ along $B \to B_\mathfrak{p}$. Note that $\mathfrak{q} \subset \mathfrak{q}'$ are prime ideals of B disjoint from $A\backslash\mathfrak{p}$, so $\mathfrak{q}B_\mathfrak{p} \subset \mathfrak{q}'B_\mathfrak{p}$ with equality iff $\mathfrak{q} = \mathfrak{q}'$. Clearly $(\mathfrak{q}B_\mathfrak{p}) \cap A_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$, so we are done by Corollary 2.5. □

2.4 Going-Down

Definition 2.4. Let $A \hookrightarrow B$ be an extension of rings. The integral closure of A in B is $\{b \in B : b \text{ integral over } A\}$.
If A is an integral domain, the integral closure of A is its integral closure in its fraction field.

Proposition 2.9. *Let $A \hookrightarrow B$ be an extension of rings. The integral closure of A in B is a subring of B.*

Proof. Example sheet. □

Definition 2.5. An integral domain A is integrally closed if A is equal to its integral closure.

Example 2.8. 1. $\mathbb{Z}$ is integrally closed.
2. $A = \mathbb{Z}[\sqrt{5}]$ is not integrally closed: $(1+\sqrt{5})/2$ is integral over A but is not in A.

Proposition 2.10. *Every UFD is integrally closed.*

Proof. Obvious. □

To better understand the consequence for a domain to be integrally closed, let's look at what happens under an extension of its fraction field.

Proposition 2.11. *Let A be an integrally closed integral domain, and let E/K be a field extension, where $K = \mathrm{FF}(A)$. Then $\alpha \in E$ is integral over A iff its minimal polynomial in K has coefficients in A.*

Proof. The "if" part follows from definition.
Conversely, suppose $\alpha \in E$ is integral over A, then there are some $a_1, \dots, a_n$ such that $\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$. In particular, $\alpha \in E$ is algebraic over K. Suppose $f \in K[T]$ is the minimal polynomial of α over K and let L be a splitting field of f over K. Every Galois conjugate β of α in L/K must then have $\beta^n + a_1\beta^{n-1} + \cdots + a_n$, hence integral. This however means that all roots of f are integral over A, so all coefficients of f must also be integral over A, therefore in A. □

Definition 2.6. Let $A \hookrightarrow B$ be rings and $\mathfrak{a} \leq A$ an ideal. An element $b \in B$ is integral over $\mathfrak{a}$ if $b^n + a_1 b^{n-1} + \cdots + a_0 = 0$ for some $a_i \in \mathfrak{a}$.

Clearly if b^m is integral over $\mathfrak{a}$ for some $m \geq 1$ then b is also integral over $\mathfrak{a}$.

Proposition 2.12. *Let $A \hookrightarrow B$ be rings and $\mathfrak{a} \leq A$ an ideal. Then b is integral over $\mathfrak{a}$ iff there is a faithful finite $A[b]$-submodule M of B such that $bM \subset \mathfrak{a}M$.*

Proof. Example sheet. □

Proposition 2.13. *Let $A \hookrightarrow B$ be rings. Let $\bar{A}$ be the integral closure of A in B. For any ideal $\mathfrak{a} \leq A$, the integral closure of $\mathfrak{a}$ in B is $\sqrt{\mathfrak{a}\bar{A}}$.*

In particular, the integral closure of an ideal $\mathfrak{a} \in A$ is an ideal of $\bar{A}$.

Proof. If b is integral over $\mathfrak{a}$, then there are some $a_i \in \mathfrak{a}$ such that $b^n + a_1 b^{n-1} + \cdots + a_n = 0$ which then means that $b^n \in \mathfrak{a}\bar{A}$, so $b \in \sqrt{\mathfrak{a}\bar{A}}$.
Conversely, if $b \in \sqrt{\mathfrak{a}\bar{A}}$, then there is some n such that $b^n = a_1x_1 + \cdots + a_mx_m, a_i \in \mathfrak{a}, x_i \in \bar{A}$. Take $M = A[x_1, \dots, x_n]$ which is a finite A-algebra since each x_i is integral over A (recall Proposition 1.4). It is clearly a faithful $A[b^n]$-module, and we also have $b^nM = (a_1x_1 + \cdots + a_mx_m)M \subset \mathfrak{a}M$, hence b^n is integral over $\mathfrak{a}$, which means that b is integral over $\mathfrak{a}$. □

A similar line of arguments reveals the following:

Proposition 2.14. *Suppose A is an integrally closed integral domain, K its fraction field and E/K a field extension. If $\alpha \in E$ is integral over an ideal $\mathfrak{a}$ of A, then the minimal polynomial of α over K has coefficients in $\sqrt{\mathfrak{a}}$.*

Ok, now let's get to going-down.

Lemma 2.15. *Let A be a ring, $S \subset A$ a multiplicative subset and $I \leq A$ an ideal disjoint from A, then there is a maximal element among the ideals containing I and disjoint from S, which is necessarily prime.*

Proof. What's yellow and equivalent to the Axiom of Choice? □

Proposition 2.16. *Let $\phi : A \to B$ be a ring homomorphism. A prime ideal $\mathfrak{p}$ of A is a contraction from B iff $\mathfrak{p} = \mathfrak{p}^{ec}$.*

Proof. If $\mathfrak{p} = \mathfrak{q}^c$, then $\mathfrak{p}^{ec} = \mathfrak{q}^{cec} = \mathfrak{q}^c = \mathfrak{p}$.
Conversely, suppose $\mathfrak{p} = \mathfrak{p}^{ec}$. It's very tempting to take $\mathfrak{q} = \mathfrak{p}^e$, except that doesn't guarantee to be prime. Fear not: $\phi(A \setminus \mathfrak{p})$ is a multiplicative subset of B disjoint from $\mathfrak{p}^e$. So we can choose, by the preceding lemma, a maximal element $\mathfrak{q}$ among the ideals containing $\mathfrak{p}^e$ and disjoint from $\phi(A \setminus \mathfrak{p})$. Now $\mathfrak{q}$ is prime and $\mathfrak{q}^c$ is a prime ideal of A containing $\mathfrak{p}$ but disjoint from $A \setminus \mathfrak{p}$, which can only happen when $\mathfrak{q}^c = \mathfrak{p}$. □

Theorem 2.17 (Going-Down)**.** *Suppose $A \hookrightarrow B$ is an integral extension of integral domains with A integrally closed. Let $\mathfrak{p}_1 \geq \cdots \geq \mathfrak{p}_n$ be prime ideals of A and $\mathfrak{q}_1 \geq \cdots \geq \mathfrak{q}_m, m < n$ be prime ideals of B such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for all $i \leq m$. Then there exists $\mathfrak{q}_{m+1} \geq \cdots \geq \mathfrak{q}_n$ with $\mathfrak{q}_m \geq \mathfrak{q}_{m+1}$ and $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for all $i \leq n$.*

Proof. It suffices to prove the case where $n = 2$ and $m = 1$. So the situation is that we have prime ideals $\mathfrak{p}_1 \supset \mathfrak{p}_2$ in A and a prime ideal $\mathfrak{q}_1$ of B lying over $\mathfrak{p}_1$. Consider the inclusions $A \hookrightarrow B \hookrightarrow B_{\mathfrak{q}_1}$. We claim that $\mathfrak{p}_2 = (\mathfrak{p}_2 B_{\mathfrak{q}_1}) \cap A$. This is sufficient for the theorem, since the preceding proposition would then grant us an ideal $\bar{\mathfrak{q}}_2$ of $B_{\mathfrak{q}_1}$ contracting to $\mathfrak{p}_2$. $\mathfrak{q}_2 = \bar{\mathfrak{q}}_2 \cap B$ then does the job.
Take $a \in (\mathfrak{p}_2 B_{\mathfrak{q}_1}) \cap A = ((\mathfrak{p}_2 B) B_{\mathfrak{q}_1}) \cap A$, then $a = y/s$ where $y \in \mathfrak{p}_2 B$ and $s \in B \setminus \mathfrak{q}_1$. The integral closure of $\mathfrak{p}_2$ in B is $\sqrt{\mathfrak{p}_2 \bar{A}} = \sqrt{\mathfrak{p}_2 B}$ by Proposition 2.13, in particular all elements of $\mathfrak{p}_2 B$ are integral over $\mathfrak{p}_2$. So y is integral over $\mathfrak{p}_2$. Therefore $y^m + a_1 y^{m-1} + \cdots + a_m$ for some $a_i \in \mathfrak{p}$.
We have $y = as$ in $\mathrm{FF}(B)$, hence $s^m + (a_1/a)s^{m-1} + \cdots + a_m/a^m = 0$. s is then integral over A. Suppose for the sake of contradiction that $a \notin \mathfrak{p}_2$, then $a^i \notin \mathfrak{p}_2$. But since $(a_i/a^i)a^i = a_i \in \mathfrak{p}_2$, we must have $a_i/a^i \in \mathfrak{p}_2$. Therefore $s^m \in \mathfrak{p}_2 B \subset \mathfrak{p}_1 B = (\mathfrak{q}_1 \cap A)B \subset \mathfrak{q}_1$, so $s \in \mathfrak{q}_1$, but $s \in B \setminus \mathfrak{q}_1$, contradiction.
The reverse inclusion is clear. □

3 Dimension Theory

3.1 Krull Dimension and Transcendental Dimension

Definition 3.1. Let A be a ring. The height $\mathrm{ht}(\mathfrak{p})$ of a prime ideal $\mathfrak{p} \leq A$ is the maximal d such that there is a chain of prime ideals $\mathfrak{p} = \mathfrak{p}_d \gneq \mathfrak{p}_{d-1} \gneq \cdots \gneq \mathfrak{p}_0$ (d is known as the length of such a chain).
The Krull dimension $\dim A$ of A is the supremum over the heights of prime ideals in A.

Example 3.1. 1. The Krull dimension of a field is zero.
2. For a field k, $\dim k[T_1, \ldots, T_n] = n$ is at least n due to the chain $(T_1, \ldots, T_n) \gneq (T_1, \ldots, T_{n-1}) \gneq \cdots \gneq (0)$. But it's somehow not obvious that the dimension

is, in fact, exactly n.
3. If A is an integral domain, then $\dim A = 0$ iff A is a field.
4. The dimension of a PID is either 0 or 1.

The height of a prime ideal needs not be finite, e.g. in $k[T_1, T_2, \ldots]$ we have the chain $(T_1, \ldots) \gneq (T_2, \ldots) \gneq (T_3, \ldots)$. Later, we'll see that the height of each prime ideal is finite in a Noetherian ring, but the Krull dimension could still be infinite.
Let's review something about transcendence degrees. Let L/k be a field extension.

Definition 3.2. A subset $A \subset L$ is a transcendence basis for L over k if A is algebraically independent over k and $L/k(A)$ is algebraic.

Proposition 3.1. *(i) If $A \subset L$ is algebraically independent over k, then there is some $A \subset B \subset L$ such that B is a transcendence basis for L over k.*
(ii) All transcendence basis for L over k have the same cardinality.
(iii) For field $E/L/k$, if B is a transcendence basis for L over k and C a transcendence basis for E/L, then $B \cup C$ is a transcendence basis for E over k.

Definition 3.3. The common cardinality of all transcendence basis of L over k is the transcendence degree $\operatorname{trdeg}_k L$ of L over k.

So if $E/L/k$ are field extensions, then $\operatorname{trdeg}_k L + \operatorname{trdeg}_L E = \operatorname{trdeg}_k E$.

Definition 3.4. For an integral domain A which contains a field k, its transcendence degree over k is $\operatorname{trdeg}_k A = \operatorname{trdeg}_k \operatorname{FF}(A)$.

We'll show that $\operatorname{trdeg}_k A = \dim A$ whenever A is a finitely generated k-algebra.
For a ring R and $x \in R$, we consider the multiplicative set $S_{\{x\}} = \{x^n(1 - rx) : n \geq 0, r \in R\}$ and write $R_{\{x\}} = S_{\{x\}}^{-1} R$.

Proposition 3.2. *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. Note first that for any $x \in R$ and maximal ideal $\mathfrak{m} \leq R$, then $\mathfrak{m} \cap S_{\{x\}} \neq \varnothing$. Indeed, if $x \in \mathfrak{m}$ then $x \in \mathfrak{m} \cap S_{\{x\}}$, and if $x \notin \mathfrak{m}$ then $x + \mathfrak{m} \in R/\mathfrak{m}$ has an inverse $r + \mathfrak{m} \in R/\mathfrak{m}$, so $1 - rx \in \mathfrak{m} \cap S_{\{x\}}$.
In addition, if there is some maximal $\mathfrak{m} \leq R$ properly containing a prime $\mathfrak{p}$, then for any $x \in \mathfrak{m} \setminus \mathfrak{p}$ we have $\mathfrak{p} \cap S_{\{x\}} = \varnothing$. To see this, suppose for the sake of contradiction that $x^n(1 - rx) \in \mathfrak{p}$ for some $n \geq 0, r \in R$, then $1 - rx \in \mathfrak{p} \subset \mathfrak{m}$, but $rx \in \mathfrak{m}$ as well, so $1 \in \mathfrak{m}$, contradiction.
Now we are ready for the proof. For $x \in R$, recall that we have a bijection between primes of R disjoint from $S_{\{x\}}$ and primes of $R_{\{x\}}$ given by extension and contraction. Suppose $\dim R \leq n$. Let $x \in R$. Take a chain of distinct prime ideals of $R_{\{x\}}$ of length l. Contract the chain along $R \to R_{\{x\}}$, then the chain is still strict by the bijection. But the contracted chain cannot contain a maximal ideal by our first remark, so $l \leq n - 1$.
Conversely, suppose $\dim R_{\{x\}} \leq n - 1$ for all $x \in R$. If $\dim R = 0$ then we are done. Assume now that $\dim R \geq 1$. Take a maximal chain of distinct prime ideals in R, say with length l. Then it must start with $\mathfrak{m} \gneq \mathfrak{p}$ for some maximal $\mathfrak{m} \leq R$. Remove $\mathfrak{m}$ from the chain, choose $x \in \mathfrak{m} \setminus \mathfrak{p}$ and then extend the rest

of the chain to $S_{\{x\}}$. By the choice of x, the other prime ideals in the chain are disjoint from $S_{\{x\}}$, so after extension the chain is still strict. We therefore have $l-1 \leq n-1$, so $l \leq n$. □

Proposition 3.3. *Let A be an integral domain and k a subfield of A, then* $\dim A \leq \operatorname{trdeg}_k A$.

Proof. If $\operatorname{trdeg}_k A = \infty$ there is nothing to prove. Suppose now that $\operatorname{trdeg}_k A = n \in \mathbb{Z}_{\geq 0}$. We proceed by induction. For $n = 0$, $\mathrm{FF}(A)$ is an algebraic extension of k, so A must also be algebraic, hence integral, over k. We therefore know that A is a field, consequently $\dim A = 0$.
Let $n \geq 1$. Assume the proposition holds for $0, \ldots, n-1$. The preceding proposition means that it suffices to prove $\dim A_{\{x\}} \leq n-1$ for all $x \in A$. Note that $p(x) \in S_{\{x\}}$ for any polynomial with coefficients in A whose lowest nonzero coefficient is 1.
If x is transcendental over k, then we have $\operatorname{trdeg} k(x) = 1$. But since $k(x) \subset A_{\{x\}}$, we also have $\operatorname{trdeg}_{k(x)} A_{\{x\}} = \operatorname{trdeg}_{k(x)} \mathrm{FF}(A) = \operatorname{trdeg}_{k(x)} A = \operatorname{trdeg}_k A - \operatorname{trdeg}_k k(x) = n-1$. Therefore $\dim A_{\{x\}} \leq n-1$ by induction hypothesis.
Otherwise, x is algebraic over k, which however means that $0 \in S_{\{x\}}$ and therefore $A_{\{x\}} = 0$ so certainly $\dim A_{\{x\}} \leq n-1$. □

Example 3.2. We hence have $\dim k[T_1, \ldots, T_n] = n$.

What about the other way around?

Proposition 3.4. *(i) Let $A \hookrightarrow B$ be an integral extension of rings, then* $\dim A = \dim B$.
(ii) Furthermore, if A, B are integral k-algebras and A is a k-subalgebra of B, then $\operatorname{trdeg}_k A = \operatorname{trdeg}_k B$.

Proof. (i) Let $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ be a chain of prime ideals of A with $n = \dim A$. By Proposition 2.6 and Theorem 2.7, we can lift it to a chain $\mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_n$ in B, so $\dim B \geq \dim A$. Conversely, suppose $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_d$ is a chain of primes of B, with $d = \dim B$. Then $\mathfrak{q}_0 \cap A \leq \mathfrak{q}_1 \cap A \subsetneq \cdots \subsetneq \mathfrak{q}_d \cap A$. This chain is strict by Proposition 2.8, so we are done.
(ii) Exercise. □

Theorem 3.5. *Let A be a finitely generated k-algebra with k a field. Suppose A is also a domain, then* $\dim A = \operatorname{trdeg}_k A$.

Proof. By Theorem 1.2, A is integral over $B = k[t_1, \ldots, t_n]$ for some $t_1, \ldots, t_n \in A$, algebraically independent over k. By the preceding proposition, to prove the theorem it suffices to show that $\dim B = \operatorname{trdeg}_k B$. But we already know this. □

Example 3.3. Let $A = k[T_1, T_2]$ where k is an algebraically closed field. Suppose $\mathfrak{p} \leq A$ is a nonzero prime. If $\mathfrak{p}$ is maximal then we already know that $\mathfrak{p} = (T_1 - t_1, T_2 - t_2)$ for some $t_1, t_2 \in k$. Otherwise, take $f \in \mathfrak{p}$ nonzero, then $\mathfrak{p}$ contains an irreducible factor g of f. Then $(0) \subsetneq (g) \leq \mathfrak{p} \subsetneq \mathfrak{m}$ for some $\mathfrak{m} \supsetneq \mathfrak{p}$ maximal. But since $\dim A = \operatorname{trdeg}_k A = 2$, we must have $\mathfrak{p} = (g)$. In other words, $\operatorname{Spec} k[T_1, T_2] = \{(0)\} \cup \{(g) : g \in k[T_1, T_2] \text{ irreducible}\} \cup \{(T_1 - t_1, T_2 - t_2) : t_1, t_2 \in k\}$.

3.2 Intermezzo: Nakayama's Lemma

Definition 3.5. The Jacobson radical of a ring A is $\mathfrak{J}(A) = \bigcap_{\mathfrak{m} \leq A \text{ maximal}} \mathfrak{m}$.

Theorem 3.6 (Nakayama's Lemma)**.** *Let $\mathfrak{a}$ be an ideal of a ring A such that $\mathfrak{a}$ is contained in the Jacobson radical $\mathfrak{J}(A)$. Suppose M is a finite A-module, then:*
(i) If $\mathfrak{a}M = M$, then $M = 0$.
(ii) If $N \leq M$ is a submodule, such that $M = N + \mathfrak{a}M$, then $M = N$.

Proof. (i) Suppose $M \neq 0$, then let's choose a set of generators $e_1, \ldots, e_n$ of M over A, with n minimal. Then $e_1 = \sum_{i=1}^n a_i e_i$ for some $a_i \in \mathfrak{a}$, so $(1 - a_1)e_1 = \sum_{i=2}^n a_i e_i$. But $1 - a_1$ is invertible since it does not belong to any maximal ideal of A, as $a_1 \in \mathfrak{a}$ is in all of them. So indeed M is spanned by $e_2, \ldots, e_n$, contradicting the minimality of n.
(ii) Apply (i) to M/N. □

Proposition 3.7 (Krull's Intersection Theorem)**.** *Suppose $\mathfrak{a}$ is an ideal of a Noetherian ring A contained in $\mathfrak{J}(A)$. Then $\bigcap_{n \geq 1} \mathfrak{a}^n = \{0\}$.*

Proof. By the preceding theorem, it suffices to show that $\bigcap_{n \geq 1} \mathfrak{a}^n = \mathfrak{a} \bigcap_{n \geq 1} \mathfrak{a}^n$. Suppose $\mathfrak{a} = (a_1, \ldots, a_r)$. For all $m \geq 1$, let H_m be the homogenous polynomials of degree m in $A[T_1, \ldots, T_r]$. Then $\mathfrak{a}^n = \{g(a_1, \ldots, a_r) : g \in H_n\}$. Let

$$S_m = \left\{ f \in H_m : f(a_1, \ldots, a_r) \in \bigcap_{n \geq 1} \mathfrak{a}^n \right\}$$

Suppose $\mathfrak{c}$ is the ideal of $A[T_1, \ldots, T_r]$ generated by $\bigcup_{m \geq 1} S_m$. $\mathfrak{c}$ is finitely generated by Theorem 1.1. Say it's generated by $f_1, \ldots, f_s \in \bigcup_{m \geq 1} S_m$. Write $d_i = \deg f_i$ and $d = \max_i d_i$.
Take $b \in \bigcap_{n \geq 1} \mathfrak{a}^n$, then $b \in \mathfrak{a}^{d+1}$, so $b = f(a_1, \ldots, a_r)$ for some $f \in H_{d+1}$. But then $f \in S_{d+1} \subset \mathfrak{c} = \langle f_1, \ldots, f_s \rangle$. Write $f = g_1 f_1 + \cdots + g_s f_s$ for some $g_i \in A[T_1, \ldots, T_r]$. Replace g_i by its $(d + 1 - d_i)$-homogenous part, we can assume WLOG that each g_i is either 0 or homogeneous of degree $d + 1 - d_i > 0$, so $g_i(a_1, \ldots, a_r) \in \mathfrak{a}$. Therefore

$$b = f(a_1, \ldots, a_r) = \sum_i g(a_1, \ldots, a_r) f_i(a_1, \ldots, a_r) \in \mathfrak{a} \bigcap_{n \geq 1} \mathfrak{a}^n$$

as desired. □

3.3 Intermezzzo: Artinian Rings

Definition 3.6. A ring is Artinian if it satisfies the descending chain condition. That is, any descending chain $\mathfrak{a}_1 \geq \mathfrak{a}_2 \geq \cdots$ stabilises. Equivalently, every nonempty set of ideals of A has a minimal element.

We'll show that a nonzero ring A is Artinian if and only if it is Noetherian and zero-dimensional.

Proposition 3.8. *For a nonzero Artinian ring A, we have* $\dim A = 0$.

Proof. We need to show that every prime ideal of A is maximal. Take a prime ideal $\mathfrak{p} \leq A$. Let $A' = A/\mathfrak{p}$. Then A' is an Artinian integral domain, since it's the quotient of an Artinian ring.
Let's show that A' is a field. For any nonzero $a \in A'$, since $(a) \geq (a^2) \geq \cdots$ stabilises, we must have $a^n = ba^{n+1}$ for some $n \geq 1$ and $b \in A'$. So $ba = 1$ as A' is an integral domain. □

Example 3.4. 1. As in the proof, an integral domain is Artinian if and only if it is a field.
2. Every finite ring is Artinian.
3. For any field k, every finite k-algebra (e.g. $k[T]/(T^{69})$) is Artinian.
4. $\mathbb{Z}, k[T]$ are Noetherian but not Artinian.

Definition 3.7. The nilradical $\mathfrak{N}(A)$ of a ring A is the ideal of all nilponents of A.

It has been shown on example sheet that $\mathfrak{N}(A) = \bigcap_{\mathfrak{p} \leq A \text{ prime}} \mathfrak{p}$.

Corollary 3.9. *If A is Artinian, then $\mathfrak{N}(A) = \mathfrak{J}(A)$.*

Proposition 3.10. *For any Artinian ring A, we have $\#\operatorname{mSpec} A < \infty$.*

Proof. Let Σ be the collection of finite intersections of maximal ideals of A. As A is Artinian, Σ has a minimal element $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$, $\mathfrak{m}_i \in \operatorname{mSpec} A$. If $\mathfrak{m} \in \operatorname{mSpec} A$ but $\mathfrak{m} \neq \mathfrak{m}_i$ for any i, then we can take $a_i \in \mathfrak{m}_i \setminus \mathfrak{m}$ for each i. Then $a_1 \cdots a_n \in (\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n) \setminus \mathfrak{m}$. So $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n \cap \mathfrak{m} \lneq \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$, contradicting minimality. □

Proposition 3.11. *If A is Artinian, then there is some n such that $\mathfrak{N}(A)^n = 0$.*

Proof. Consider the chain of ideals $\mathfrak{N}(A) \geq \mathfrak{N}(A)^2 \geq \cdots$. Since A is Artinian, the chain stabilises at $\mathfrak{N}(A)^n$ for some n. We claim that $\mathfrak{N}(A)^{n+1} = 0$.
Suppose not. Then the set Σ of ideals $\mathfrak{a}$ of A such that $\mathfrak{a}\mathfrak{N}(A)^n \neq 0$ is nonempty since $\mathfrak{N}(A) \in \Sigma$. Let $\mathfrak{a}$ be a minimal element of Σ (exists as Σ is nonempty and A is Artinian). Take $x \in \mathfrak{a}$ such that $x\mathfrak{N}(A)^n \neq 0$. As $(x) \leq \mathfrak{a}$, by minimality we must have $\mathfrak{a} = (x)$.
Now $x\mathfrak{N}(A)^n \leq (x)$ and $(x\mathfrak{N}(A)^n)\mathfrak{N}(A)^n = x\mathfrak{N}(A)^n \neq 0$, so $(x) = x\mathfrak{N}(A)^n$ again by minimality. So $x = xy$ for some $y \in \mathfrak{N}(A)$, consequently $x = xy^l$ for every $l \geq 1$. For large enough l, this shows that $x = 0$, contradiction. □

Definition 3.8. Let M be a module over a ring A. Then M is Noetherian (resp. Artinian) if every ascending (resp. descending) chain of submodules stabilises.

Remark. 1. A ring A is Noetherian (resp. Artinian) if and only if A is Noetherian (resp. Artinian) as an A-module.
2. Suppose $N \leq M$ is a submodule, then M is Noetherian (resp. Artinian) iff both $N, M/N$ are Noetherian (resp. Artinian).

Proposition 3.12. *Let A be a ring such that some finite product of its maximal ideals is zero. Then A is Artinian if and only if A is Noetherian.*

Proof. Take $\mathfrak{m}_1 \cdots \mathfrak{m}_n = 0$ for $\mathfrak{m}_i$ maximal. We have the filtration $A \supset \mathfrak{m}_1 \supset \mathfrak{m}_1\mathfrak{m}_2 \supset \cdots \supset \mathfrak{m}_1 \cdots \mathfrak{m}_n = 0$. Let $M_1 = A/\mathfrak{m}_1$ and $M_r = \mathfrak{m}_1 \cdots \mathfrak{m}_{r-1}/\mathfrak{m}_1 \cdots \mathfrak{m}_r$ for $r > 1$. Then M_r is an $A/\mathfrak{m}_r$-vector space.

We have a bijection between $A/\mathfrak{m}_r$-linear subspaces of M_r and A-submodules between $\mathfrak{m}_1 \cdots \mathfrak{m}_r$ and $\mathfrak{m}_1 \cdots \mathfrak{m}_{r-1}$. These satisfy the ascending (resp. descending) chain condition if A is Noetherian (resp. Artinian). Assume that A is either Noetherian or Artinian, then each M_r is finite-dimensional over $A/\mathfrak{m}_r$, therefore both Noetherian and Artinian. But this just implies that A is both Noetherian and Artinian by the second remark above. □

Lemma 3.13. *Let A be a Noetherian ring, then every radical ideal of A is a finite intersection of prime ideals.*

Proof. Example sheet. □

Theorem 3.14. *Let A be a ring. Then A is Artinian if and only if it is Noetherian and* $\dim A = 0$.

Proof. If A is Artinian, then we already know that $\dim A = 0$. Furthermore, if we take l such that $\mathfrak{N}(A)^l = 0$ and take $\mathfrak{m}_1, \ldots, \mathfrak{m}_n \leq A$ maximal such that $\mathfrak{N}(A) = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$, then $(\mathfrak{m}_1 \ldots \mathfrak{m}_n)^l = 0$ which by the preceding proposition means that A is Noetherian.
The converse is on example sheet. □

3.4 Intermezzzzo: Graded Rings; Composition Series

Definition 3.9. Suppose we have a sequence of A-modules and A-linear maps

$$\cdots \longrightarrow M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} M_{i+2} \longrightarrow \cdots$$

We call this sequence exact if $\operatorname{Im} f_i = \ker f_{i+1}$ for each i.
If a sequence of the form

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

is exact, then we call it a short exact sequence.

So if we have a short exact sequence like above, then $N \to M$ is injective, $M \to L$ is surjective and $M/N \cong L$.

Definition 3.10. A graded ring $(A, (A_n)_{n=0}^{\infty})$ is a ring A together with additive subgroups $A_n \subset A$ such that $A = \bigoplus_{n \geq 0} A_n$ and $A_i A_j \subset A_{i+j}$.

Note that A_0 must be a subring of A. Elements of A_n are called homogeneous elements (of degree n). $A_+ = \bigoplus_{n \geq 1} A_n$ is called the irrelevant ideal for irrelevant reasons.

Example 3.5. A polynomial ring $A = k[T_1, \ldots, T_m]$ can be graded by taking A_n to be the subgroup of degree n homogeneous polynomials.

Definition 3.11. Let A be a graded ring, a graded module $(M, (M_n)_{n=0}^{\infty})$ is an A-module together with additive subgroups $M_n \leq M$ such that $M = \bigoplus_{n \geq 0} M_n$ and $A_m M_n \subset M_{m+n}$.
$f : M \to N$ is a homomorphism of graded A-modules if it is A-linear and $f(M_n) \subset N_n$ for all n.

Proposition 3.15. *Let A be a graded ring, then A is Noetherian if and only if A_0 is Noetherian and A is a finitely-generated A_0-algbera.*

Proof. The "if" part follows from Theorem 1.1.
For the "only if" part, suppose A is Noetherian. Then $A_0 \cong A/A_+$ must also be Noetherian. It remains to show that A is finitely generated over A_0. The ideal A_+ is generated by the set of all homogeneous elements of positive degree. As A is Noetherian, we can find $x_i \in A_{k_i}$ such that $x_1, \dots, x_s$ generate A_+.
Let $A' = A_0[x_1, \dots, x_s]$. We want to show that $A = A'$. It suffices to prove that $A_n \subset A'$ for all $n \geq 0$. This is true for $n = 0$. Assuming $n > 1$ and $A_k \subset A'$ for all $k < n$. For $y \in A_n$, we have $y = \sum_i a_i x_i$ for some $a_i \in A$. WLOG $a_i \in A_{n-k_i}$. As $k_i > 0$, the induction hypothesis means that $a_i \in A'$ for all i, therefore $y \in A'$. □

Remark. The proof shows that we can in fact generate A as an A_0-algebra by homogenous elements of positive degrees.

Let A be a ring, $\mathcal{C}$ a class of A-modules. A $\mathbb{Z}$-valued function λ on $\mathcal{C}$ is additive if $\lambda(0) = 0$ and that whenever there's a short exact sequence

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

of A-modules in $\mathcal{C}$, we have $\lambda(M) = \lambda(N) + \lambda(L)$. In particular, $\lambda(M) = \lambda(N) + \lambda(M/N)$ whenever $N \leq M$ is a submodule.

Example 3.6. Suppose $A = k$ is a field and $\mathcal{C}$ is the class of finite-dimensional k-vector spaces, then $\lambda(V) = \dim_k V$ is such a function.

Proposition 3.16. *For an exact sequence*

$$0 \longrightarrow M_0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow \cdots \longrightarrow M_n \longrightarrow 0$$

we have

$$\sum_{i=0}^{n} (-1)^i \lambda(M_i) = 0$$

Proof. Example sheet. □

Definition 3.12. A composition series of an A-module M is a chain $M = M_n \gneq M_{n-1} \gneq \cdots \gneq M_0 = 0$ of submodules of M which is non-refinable, in the sense that it's impossible to add in new submodules to the chain.

Equivalently, each quotient M_i/M_{i-1} is a simple A-module.

Lemma 3.17. *Suppose M has a composition series of length m. Then all composition series of M has length m, and every chain of distinct submodules of M can be refined (i.e. adding in new terms) into a composition series.*

Proof. Example sheet. □

Definition 3.13. The common length of a composition series for M is the length $\ell(M)$ of M. If M does not have a composition series, we set $\ell(M)$

Proposition 3.18. *M has finite length iff M is Artinian and Noetherian.*

Proof. The "only if" part is clear.
Conversely, suppose M is Artinian and Noetherian. Form a descending chain $M = M^0 \supsetneq M^1 \supsetneq \cdots$ where M^{j+1} is a maximal submodule of M^j, which is possible as M is Noetherian. This stabilises since M is Artinian. □

Proposition 3.19. *ℓ is additive.*

Proof. Lemma 3.17. □

3.5 Poincaré Series and Hilbert Polynomial

Let $A = \bigoplus_{n\geq 0} A_n$ a Noetherian graded ring. We know that A_0 is Noetherian and $A = A_0[x_1, \ldots, x_s]$ for some homogeneous elements $x_i \in A$ with positive degree.
Let $M = \bigoplus_{n\geq 0} M_n$ be a finite graded A-module. Then it is generated by some $m_1, \ldots, m_t$ with $m_i \in M_{r_i}$. Therefore every element at M_n is of the form $\sum_{j=1}^t f_j(x_1, \ldots, x_s)m_j$ for $f_j \in A_0[T_1, \ldots, T_s]$. We can assume WLOG that each $f_j(x_1, \ldots, x_s)$ is in A_{n-r_j}. Then M_n is generated as an A_0-module by elements of the form $g(x_1, \ldots, x_s)m_j$ for a monomial $g(T) = T_1^{e_1} \cdots T_s^{e_s}$ with $\sum_i e_i k_i = n - r_j$. In particular, each M_n is a finite A_0-module.
Let λ be an additive function on the class of finite A_0-modules. If so desired, one can always take $\lambda = \ell$ to be the length function and A_0 Artinian (or even a field a field) for a more intuitive picture.

Definition 3.14. The Poincaré series $P(M, T)$ of M (with respect to λ) is

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

Theorem 3.20 (Hilbert-Serre)**.** *$P(M, T)$ is a rational function of the form $P(M, T) = f(T)/\prod_{i=1}^s (1 - T^{k_i})$.*

Proof. A is generated by $x_1, \ldots, x_s$ as an A_0-algebra with $x_i \in A_{k_i}$. We proceed by induction on s.
If $s = 0$, then $A = A_0$. As M is a finite A_0-module, $M_n = 0$ for large n, so the Poincaré series is a polynomial.
Now suppose $s > 0$ and the theorem holds for $s - 1$. Consider the map $M_n \mapsto M_{n+k_s}, m \mapsto x_s m$, which is a homomorphism of A_0-modules.

$$0 \longrightarrow K_n \longrightarrow M_n \xrightarrow{x_s} M_{n+k_s} \longrightarrow L_{n+k_s} \longrightarrow 0$$

where K_n and L_{n+k_s} are the kernel and cokernel of the multiply-by-x_s map, respectively.
Both $K = \bigoplus_n K_n, L = \bigoplus_n L_{n+k_s}$ are finite graded A-modules. They are also both annihilated by x_s, so they are in fact finite graded $A_0[x_1, \ldots, x_{s-1}]$-modules. By the induction hypothesis, we know that $P(K, T)$ and $P(L, T)$ are both rational functions with denominator $\prod_{i=1}^{s-1}(1 - T^{k_i})$. On the other hand, we have by the additivity of λ that

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

for some polynomial $g(T)$. But this gives what we wanted! □

Write $d(M)$ for the order of the pole of the rational function $P(M,T)$ at $T=1$. You know what I mean.

Proposition 3.21. *If $x \in A_k$ is not a zerodivisor in M (i.e. $xm \neq 0$ unless $m=0$), then $d(M/xM) = d(M)-1$.*

Proof. Do the same thing as in the preceding theorem, except with x in place of x_s. Then $K_n = 0$ as x is not a zerodivisor in M, and $L_{n+k} = M_{n+k}/xM_n$, so $d(L) = d(M)-1$. But $d(L) = d(M/xM)$, since the difference of their Poincaré series is just a polynomial with nonnegative coefficients. □

Proposition 3.22. *If $k_1 = \cdots = k_s = 1$, then there is a (necessarily unique) polynomial $\mathrm{HP}_M(T) \in \mathbb{Q}[T]$ of degree $d(M)-1$ such that $\lambda(M_n) = \mathrm{HP}_m(n)$ for all large enough n.*

Proof. Write $d = d(M)$. Theorem 3.20 gives $f \in \mathbb{Z}[T]$ such that $\lambda(M_n)$ is the coefficient of T^n in $f(T)(1-T)^{-d}$ for some $d \in \mathbb{N}$. WLOG $f(1) \neq 0$, so $d = d(M)$. Write $f(T) = \sum_{k=0}^{N} a_k T^k$. Now,

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

So for large enough n, we must have

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

which is a polynomial in n with rational coefficients, and its degree is d with leading coefficient $f(1)/(d-1)! \neq 0$. □

3.6 Filtrations

Let M be a module over a ring A.

Definition 3.15. A (descending) filtration of M is a descending sequence $M = M_0 \supsetneq M_1 \supsetneq \cdots$ of submodules of M.
If $\mathfrak{a}$ is an ideal of A, then a filtration $(M_n)_n$ of M is an $\mathfrak{a}$-filtration if $\mathfrak{a}M_n \subset M_{n+1}$ for all n. It is stable if $\mathfrak{a}M_n = M_{n+1}$ for all large enough n.

Example 3.7. $(\mathfrak{a}^n M)_n$ is a stable $\mathfrak{a}$-filtration of M.

Lemma 3.23 (Bounded Differences Lemma)**.** *If $(M_n)_n, (M'_n)_n$ are stable $\mathfrak{a}$-filtrations of M, then there exists $n_0 \geq 0$ such that $M_{n+n_0} \subset M'_n, M'_{n+n_0} \subset M_n$ for all n.*

Proof. The relation in the conclusion of the lemma is clearly an equivalence relation, so we can assume WLOG that $M'_n = \mathfrak{a}^n M$.
Note that $\mathfrak{a}^n M \subset M_m$ for all $n \geq m$ since $(M_n)_n$ is an $\mathfrak{a}$-filtration. On the other hand, for some $n_0 \geq 0$ we must have $\mathfrak{a}M_n = M_{n+1}$ all $n \geq n_0$ by stability. So $M_{n+n_0} = \mathfrak{a}^n M_{n_0} \subset \mathfrak{a}^n M$. □

We form a graded ring $A^* = \bigoplus_{n=0}^{\infty} \mathfrak{a}^n$ where $\mathfrak{a}^0 = A$. For an $\mathfrak{a}$-filtration $(M_n)_n$ of M, we similarly have a graded A^*-module $M^* = \bigoplus_{n=0}^{\infty} M_n$. If A is Noetherian, then $\mathfrak{a}$ is generated by a finite set of elements $x_1, \ldots, x_s \in A$. Let $\bar{x}_i$ be the image of x_i in $A^1 = \mathfrak{a}$, then $\bar{x}_1, \ldots, \bar{x}_s$ generate A^* as an $A^0 = A$-algebra. In particular, A^* is Noetherian by Theorem 1.1.

Lemma 3.24. *Let A be a Noetherian ring and M a finite A-module. Let $(M_n)_n$ be an $\mathfrak{a}$-filtration of M, then M^* is a finite A^*-module if and only if the filtration $(M_n)_n$ is stable.*

Proof. M is Noetherian since it is finite over A, therefore each M_n is finite and so is $Q_n = \bigoplus_{r=0}^{n} M_r$ for each n. Each Q_n is an additive subgroup of M^*. Since $(M_n)_n$ is an $\mathfrak{a}$-filtration, the A^*-submodule of M^* generated by Q_n is $M_n^* = M_1 \oplus \cdots \oplus M_n \oplus \mathfrak{a}M_n \oplus \mathfrak{a}^2 M_n \oplus \cdots$ which is a finite A^*-module.
Clearly $(M_n)_n$ is stable if and only if the ascending chain $(M_n^*)_n$ stabilises.
If M^* is finite, then it is Noetherian and therefore $(M_n^*)_n$ must stabilise. Conversely, we have $M^* = \bigcup_n M_n^*$, so if M_n^* stabilises then $M^* = M_{n_0}^*$ for some n_0 which means that M^* is finite. □

Proposition 3.25 (Artin-Rees Lemma)**.** *Let $\mathfrak{a}$ be an ideal of a Noetherian ring A and M a finite A-module with a stable $\mathfrak{a}$-filtration $(M_n)_n$. Suppose we have an A-submodule $M' \leq M$. Then $(M_n \cap M')_n$ is a stable $\mathfrak{a}$-filtration of M'.*

Proof. It certainly is an $\mathfrak{a}$-filtration. Write $K_n = M_n \cap M'$ and $K = \bigoplus_n K_n$ which is a graded A^*-submodule of M^*. Since A is Noetherian, so is A^*. The preceding lemma shows that M^* is finite over A^*, therefore K is finite over A^*. Using the preceding lemma again but on K shows that $(K_n)_n$ is stable. □

Definition 3.16. Let A be a ring and $\mathfrak{a} \leq A$ an ideal. We define their associated graded ring to be $G_{\mathfrak{a}}(A) = \bigoplus_{n=0}^{\infty} \mathfrak{a}^n/\mathfrak{a}^{n+1}$.
For an A-module M with an $\mathfrak{a}$-filtration $(M_n)_n$, its associated graded module is $G(M) = \bigoplus_{n=0}^{\infty} M_n/M_{n+1}$ which is a graded $G_{\mathfrak{a}}(A)$-module.

Remark. $G(M)$ depends on the choice of filtration.

Proposition 3.26. *Suppose A is Noetherian and $\mathfrak{a} \leq A$ an ideal, then:*
(i) $G_{\mathfrak{a}}(A)$ is Noetherian.
(ii) If M is a finite A-module and $(M_n)_n$ is a stable $\mathfrak{a}$-filtration of M, then $G(M)$ is a finite graded $G_{\mathfrak{a}}(A)$-module.

Proof. (i) Since A is Noetherian, $\mathfrak{a} = (x_1, \ldots, x_s)$ for some $x_i \in A$. Let $\bar{x}_i$ be the image of x_i in $G_{\mathfrak{a}}(A)_1 = \mathfrak{a}/\mathfrak{a}^2$, then $G_{\mathfrak{a}}(A)$ is finitely generated by $\bar{x}_1, \ldots, \bar{x}_s$ over $G_{\mathfrak{a}}(A)_0 = A/\mathfrak{a}$, therefore $G_{\mathfrak{a}}(A)$ is Noetherian by Theorem 1.1.
(ii) Take n_0 such that $M_{n_0+r} = \mathfrak{a}^r M_{n_0}$ for all $r \geq 0$. Then $G(M)$ is generated by $\bigoplus_{n \leq n_0} M_n/M_{n+1}$ as an $G_{\mathfrak{a}}(A)$-module. Each M_n/M_{n+1} is a Noetherian A-module and is annihilated by $\mathfrak{a}$, so M_n/M_{n+1} is a finite $A/\mathfrak{a}$-module, so $\bigoplus_{n \leq n_0} M_n/M_{n+1}$ must also be a finite $A/\mathfrak{a}$-module. □

3.7 Dimension Theory of Noetherian Local Rings

Definition 3.17. An ideal I of a ring A is primary if $I \neq A$ and every zero divisor of A/I is nilpotent.

You'll prove a bunch of stuff about primary ideals in the example sheet. We state some of them here.

Proposition 3.27. *(i) If I is primary, then $\sqrt{I}$ is the smallest prime ideal containing I. In particular, $I \mapsto \sqrt{I}$ maps primary ideals to prime ideals. We say I is $\mathfrak{p}$-primary if $\mathfrak{p} = \sqrt{I}$.*
(ii) If $\mathfrak{m} \in \operatorname{mSpec} A$ then $\mathfrak{m}^n$ is always $\mathfrak{m}$-primary. For $\mathfrak{p} \in \operatorname{Spec} A$, $\mathfrak{p}^n$ is not necessarily primary, but if it is then it is $\mathfrak{p}$-primary.

Let A be a Noetherian local ring and $\mathfrak{m}$ its unique maximal ideal. For an $\mathfrak{m}$-primary ideal $\mathfrak{q}$, let $\delta(\mathfrak{q})$ be the (finite) size of a minimal generating set of $\mathfrak{q}$. There are three pieces of data we can extract from A, namely $\dim A$, $\delta(A) = \min\{\delta(\mathfrak{q}) : \mathfrak{q}\ \mathfrak{m}\text{-primary}\}$ and $d(G_{\mathfrak{m}}(A))$, the order of the pole at $T = 1$ of the rational function $\sum_{n=0}^{\infty} \ell(\mathfrak{m}^n/\mathfrak{m}^{n+1})T^n$. We'll show that they are all equal.

Lemma 3.28. *For any $p \in \mathbb{Q}[T]$, there is some $q \in \mathbb{Q}[T]$ such that $\sum_{k=0}^{n-1} p(k) = q(n)$, $\deg q = 1 + \deg p$ (with the convention $\deg 0 = -\infty$) and the leading coefficient of q depends only on the leading coefficient of p.*

Proof. An exercise in scarlet. □

For a function $f : \mathbb{Z} \to \mathbb{Z}$, there is at most one polynomial g such that $f(n) = g(n)$ for large enough n. If g exists, the degree and leading coefficients of f are the degree and leading coefficient of g, respectively.

Proposition 3.29. *Let $(A, \mathfrak{m})$ be a Noetherian local ring and $\mathfrak{q}$ an $\mathfrak{m}$-primary ideal. Suppose M is a finite A-module with a $\mathfrak{q}$-stable filtration $(M_n)_n$. Then:*
(i) $\ell(M_n/M_{n+1}) < \infty$.
(ii) There are some $f, g \in \mathbb{Q}[T]$ such that $\ell(M_n/M_{n+1}) = f(n), \ell(M/M_n) = g(n)$ for all large n. Moreover, $1 + \deg f = \deg g \leq \delta(\mathfrak{q})$.
(iii) The leading terms of f and g depend only on $A, M, \mathfrak{q}$, not on the filtration.

Proof. (i) Each M_n/M_{n+1} is a finite $A/\mathfrak{q}$-module. On the other hand, $A/\mathfrak{q}$ is Artinian since it is Noetherian and zero-dimensional (since it has a unique prime, namely $\mathfrak{m}/\mathfrak{q}$). So $\ell(M_n/M_{n+1}) < \infty$.
(ii) We already know that $G_{\mathfrak{q}}(A)$ is Noetherian and $G(M)$ is a finite $G_{\mathfrak{q}}(A)$-module. If $x_1, \dots, x_s$ generate $\mathfrak{q}$, then their images $\bar{x}_1, \dots, \bar{x}_s \in \mathfrak{q}/\mathfrak{q}^2$ generate $G_{\mathfrak{q}}(A)$ as an $A/\mathfrak{q}$-algebra. On the other hand, $n \mapsto \ell(M_n/M_{n+1})$ is a polynomial of degree at most $s - 1$ for all large n. So we get f. g then pops out from the preceding lemma.
(iii) Let $(M'_n)_n$ be a different $\mathfrak{q}$-filtration, and suppose it gives rise to $f'(n) = \ell(M'_n/M'_{n+1}), g'(n) = \ell(M/M'_n)$. By Lemma 3.23, there is some n_0 such that $M_{n+n_0} \subset M'_n, M'_{n+n_0} \subset M_n$ for all n. Then $g(n - n_0) \leq g'(n) \leq g(n + n_0)$, but g, g' are both (eventual) polynomials, so they must share the same leading term. Applying the preceding lemma shows the result for f. □

Corollary 3.30. *If A is a Noetherian local ring with maximal ideal $\mathfrak{m}$ and $\mathfrak{q}$ is $\mathfrak{m}$-primary, then:*
(i) For all large n, $n \mapsto \ell(\mathfrak{q}^n/\mathfrak{q}^{n+1})$ is a polynomial of degree at most $\delta(\mathfrak{q}) - 1$.
(ii) $\deg(n \mapsto \ell(A/\mathfrak{q}^n)) = \deg(n \mapsto A/\mathfrak{m}^n)$ and $\deg(n \mapsto \ell(\mathfrak{q}^n/\mathfrak{q}^{n+1})) = \deg(n \mapsto \ell(\mathfrak{m}^n/\mathfrak{m}^{n+1}))$.

Proof. (i) Follows from the preceding proposition.
(ii) There is some $r \geq 1$ such that $\mathfrak{m}^r \leq \mathfrak{q} \leq \mathfrak{m}$ since $\mathfrak{m} = \sqrt{\mathfrak{q}}$, so $\ell(A/\mathfrak{m}^n) \leq \ell(A/\mathfrak{q}^n) \leq \ell(A/\mathfrak{m}^{rn})$ which suffices since they are all eventual polynomials. □

Corollary 3.31. *For a Noetherian local ring A with maximal ideal $\mathfrak{m}$, we have $\delta(A) \geq d(G_{\mathfrak{m}}(A))$.*

Proof. Let $\mathfrak{q}$ be $\mathfrak{m}$-primary generated by $\delta(A)$ elements, then $\delta(A) = \delta(\mathfrak{q}) \geq \deg(n \mapsto \ell(\mathfrak{q}^n/\mathfrak{q}^{n+1})) + 1 = \deg(n \mapsto \ell(\mathfrak{m}^n/\mathfrak{m}^{n+1})) + 1 = d(G_{\mathfrak{m}}(A))$. □

Proposition 3.32. *For a Noetherian local ring A with maximal ideal $\mathfrak{m}$ and $x \in \mathfrak{m}$ not a zerodivisor, we have $d(G_{\mathfrak{m}/(x)}A/(x)) \leq d(G_{\mathfrak{m}}(A)) - 1$.*

Proof. The map $A \to xA, a \mapsto xa$ is an isomorphism of A-modules since x is not a zerodivisor. Let $A' = A/(x)$ and $\mathfrak{m}' = \mathfrak{m}/(x)$. We have an exact sequence of A-modules

$$0 \longrightarrow xA/(xA \cap \mathfrak{m}^n) \longrightarrow A/\mathfrak{m}^n \longrightarrow A'/(\mathfrak{m}')^n \longrightarrow 0$$

So $\ell(A'/(\mathfrak{m}')^n) = \ell(A/\mathfrak{m}^n) - \ell(xA/(xA \cap \mathfrak{m}^n))$.
A has a stable $\mathfrak{m}$-filtration given by $(\mathfrak{m}^n)_n$. By Proposition 3.25, $(xA \cap \mathfrak{m}^n)_n$ is a stable $\mathfrak{m}$-filtration of xA. The leading terms of $n \mapsto \ell(A/\mathfrak{m}^n)$ and $n \mapsto \ell(xA/(xA \cap \mathfrak{m}^n))$ then must coincide by Proposition 3.29. Hence

$$\begin{aligned} d(G_{\mathfrak{m}'}(A')) &= \deg(n \mapsto \ell((\mathfrak{m}')^n/(\mathfrak{m}')^{n+1})) + 1 = \deg(n \mapsto \ell(A'/(\mathfrak{m}')^n)) \\ &\leq \deg(n \mapsto \ell(A/\mathfrak{m}^n)) - 1 = \deg(n \mapsto \ell(\mathfrak{m}^n/\mathfrak{m}^{n+1})) \\ &= d(G_{\mathfrak{m}}(A)) - 1 \end{aligned}$$

as desired. □

Proposition 3.33. *For a Noetherian local ring A with maximal ideal $\mathfrak{m}$, we have $d(G_{\mathfrak{m}}(A)) \geq \dim A$.*

Proof. Induction on $d(G_{\mathfrak{m}}(A))$. When $d(G_{\mathfrak{m}}(A)) = 0$, we have $\ell(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = 0$ for all large n, so $\mathfrak{m}^n = \mathfrak{m}^{n+1}$, therefore $\mathfrak{m}^n = 0$ by Theorem 3.6, so A is Artinian and hence $\dim A = 0$.
Suppose $d(G_{\mathfrak{m}}(A)) > 0$. If $\dim A = 0$ then we are done. Otherwise, we take a chain $\mathfrak{p}_r \supsetneq \cdots \supsetneq \mathfrak{p}_0$ of primes for some $r \geq 1$.
Consider $A' = A/\mathfrak{p}_0$, which is a Noetherian local domain. Fix $x \in \mathfrak{p}_1 \setminus \mathfrak{p}_0$ and let $x' = x + \mathfrak{p}_0 \neq 0$. By the preceding proposition, we have $d(G_{\mathfrak{m}'/(x')}(A'/(x'))) \leq d(G_{\mathfrak{m}'}(A')) - 1$ where $\mathfrak{m}' = \mathfrak{m}/\mathfrak{p}$.
The surjective A-linear map $A/\mathfrak{m}^n \to A'/(\mathfrak{m}')^n$ tells us $\ell(A/\mathfrak{m}^n) \geq \ell(A'/(\mathfrak{m}')^n)$, so the $\deg(n \mapsto A/\mathfrak{m}^n) \geq \deg(n \mapsto \ell(A'/(\mathfrak{m}')^n))$. Therefore $d(G_{\mathfrak{m}'}(A')) \leq d(G_{\mathfrak{m}}(A))$, so $d(G_{\mathfrak{m}'/(x')}(A'/(x'))) \leq d(G_{\mathfrak{m}}(A)) - 1$.
By the induction hypothesis, $d(G_{\mathfrak{m}'/(x')}(A'/(x'))) \geq \dim A'/(x')$. Since $x \in \mathfrak{p}_1$, the chain $\mathfrak{p}_r \supsetneq \cdots \supsetneq \mathfrak{p}_1$ remains strict in $A'/(x')$, so $r - 1 \leq \dim A'/(x') \leq d(G_{\mathfrak{m}'/(x')}(A'/(x'))) \leq d(G_{\mathfrak{m}}(A)) - 1$. □

Proposition 3.34. *For a Noetherian local ring A with maximal ideal $\mathfrak{m}$, we have $\dim A \geq \delta(A)$. That is, there is an $\mathfrak{m}$-primary ideal of A generated by $\dim A$ elements.*

Proof. Write $d = \dim A$. Let's construct $x_1, \ldots, x_d \in \mathfrak{m}$ such that every prime ideal containing $x_1, \ldots, x_i$ has height at least i. Suppose $x_1, \ldots, x_{i-1}$ has already been constructed and $i \leq d$. There are only finitely many prime ideals of height $i-1$ containing $(x_1, \ldots, x_{i-1})$, since every such prime ideal is minimal for $(x_1, \ldots, x_{i-1})$ (and every ideal has finitely many minimal primes in a Noetherian ring). Let them be $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$. Since $i - 1 < d = \mathrm{ht}(\mathfrak{m})$, $\mathfrak{m} \neq \mathfrak{p}_j$ for any j. $\mathfrak{m}$ is also not contained in $\bigcup_j \mathfrak{p}_j$ by prime avoidance (example sheet). Take $x_i \in \mathfrak{m} \setminus (\bigcup_j \mathfrak{p}_j)$.
Suppose $\mathfrak{q}$ is a prime containing $x_1, \ldots, x_i$. Let $\mathfrak{p}$ be minimal among prime ideals contained in $\mathfrak{q}$ and containing $x_1, \ldots, x_{i-1}$. If $\mathfrak{p} = \mathfrak{p}_j$ for some j then $x_i \in \mathfrak{q} \setminus \mathfrak{p}$, so $\mathrm{ht}(\mathfrak{q}) \geq \mathrm{ht}(\mathfrak{p}) + 1 = i$. Otherwise, $\mathrm{ht}(\mathfrak{q}) \geq \mathrm{ht}(\mathfrak{p}) \geq i$. So this choice of x_i does work.
Now $\sqrt{(x_1, \ldots, x_d)} = \bigcap_{\mathfrak{n} \in \mathrm{Spec}\, A, (x_1, \ldots, x_d) \subset \mathfrak{n}} \mathfrak{n} = \mathfrak{m}$ since $\dim A = d$. So the ideal $(x_1, \ldots, x_d)$ is $\mathfrak{m}$-primary. □

Consequently, $\dim A = \delta(A) = d(G_{\mathfrak{m}}(A))$.

Corollary 3.35 (Krull's Height Theorem)**.** *If A is a Noetherian ring (not necessarily local) and $x_1, \ldots, x_r \in A$, then every minimal prime $\mathfrak{p}$ for $\mathfrak{a} = (x_1, \ldots, x_r)$ has height at most r.*

Proof. Under localisation map $A \to A_{\mathfrak{p}}$, we can only have $\sqrt{\mathfrak{a}^{\mathrm{e}}} = \mathfrak{p}^{\mathrm{e}}$, which is maximal. So $\mathfrak{a}^{\mathrm{e}}$ is $\mathfrak{p}^{\mathrm{e}}$-primary. But $\mathfrak{a}^{\mathrm{e}}$ is generated by $x_1, \ldots, x_r$ in $A_{\mathfrak{p}}$, so $\mathrm{ht}(\mathfrak{p}) = \dim A_{\mathfrak{p}} = \delta(A_{\mathfrak{p}}) \leq \delta(\mathfrak{p}^{\mathrm{e}}) \leq r$. □

4 Tensor Products

4.1 Tensor Products of Modules and Algebras

Suppose M, N are A-modules. $M \otimes_A N$ consists of finite sums of (formal) symbols of the form $m \otimes n, m \in M, n \in N$ subject to the relations $(rm) \otimes n = m \otimes (rn), (m + m') \otimes n = m \otimes n + m' \otimes n, m \otimes (n + n') = m \otimes n + m \otimes n'$.

Example 4.1. 1. $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} = 0$ since $m \otimes n = (3m) \otimes n = m \otimes (3n) = m \otimes 0 = (0m) \otimes 0 = 0 \otimes 0$.
2. If $A = k$ is a field and M, N are finite dimensional k-vector spaces, then $M \otimes_k N$ is a vector space with dimension $(\dim_k M)(\dim_k N)$. Indeed, if B, C are k-bases for M, N, respectively, then $\{b \otimes c : b \in B, c \in C\}$ is a basis for $M \otimes_k N$.

Let's introduce the definition in a more formal way. Whether it's better is open to interpretation.

Definition 4.1. For A-modules M, N, L, an A-bilinear map $f : M \times N \to L$ is a function such that $f(m_0, -), f(-, n_0)$ are A-linear for all $m_0 \in M, n_0 \in N$.
If A is a ring and S is a set, then we can form the direct sum $A^{\oplus S}$ consisting of formal finite sums of elements in S with coefficients in A.

Definition 4.2. Suppose M, N are A-modules. The tensor product $M \otimes_A N$ is $A^{\oplus(M \times N)}/K$ where K is the A-submodule of $A^{\oplus(M \times N)}$ generated by:
1. $(m, n_1) + (m, n_2) - (m, n_1 + n_2), m \in M, n_1, n_2 \in N$.
2. $(m_1, n) + (m_2, n) - (m_1 + m_2, n), m_1, m_2 \in M, n \in N$.

3. $a(m,n) - (am,n), a \in A, m \in M, n \in N$.
4. $a(m,n) - (m,an), a \in A, m \in M, n \in N$.
The image of $(m,n) \in A^{\oplus(M\times N)}$ in $M \otimes_A N$ is denoted $m \otimes n$ or $m \otimes_A n$.

We naturally have a bilinear map $i_{M\otimes_A N} : M \times N \to M \otimes_A N, (m,n) \mapsto (m \otimes n)$. This map is natural in the following sense:

Proposition 4.1 (Universal Property of Tensor Products)**.** *For A-modules M, N, the pair $(M \otimes_A N, i_{M\otimes_A N})$ is universal in the sense that for any A-module L and an A-bilinear map $f : M \times N \to L$, there is a unique A-linear $\tilde{f} : M \otimes_A N \to L$ such that $f = \tilde{f} \circ i_{M\otimes_A N}$.*

$$\begin{array}{ccc} M \times N & \xrightarrow{i_{M\otimes_A N}} & M \otimes_A N \\ {\scriptstyle f}\downarrow & \swarrow_{\exists!\tilde{f}} & \\ L & & \end{array}$$

Proof. Take such $f : M \times N \to L$. The desired factorisation $f = \tilde{f} \circ i_{M\otimes_A N}$ means that our only possible choice is $\tilde{f}(m \otimes n) = f(m,n)$ (extended by linearity). This $\tilde{f}$ is indeed A-linear since it is induced by the A-linear map $A^{\oplus(M\times N)} \to L, (m,n) \mapsto f(m,n)$, which factors through K since f is A-bilinear. □

As usual, the pair $(M \otimes_A N, i_{M\otimes_A N})$ is uniquely determined by this universal property which, funnily enough, isn't quite the best way to work with them.

Proposition 4.2. *Let A be a ring and M, N be A-modules. $\sum_{i=1}^{l} m_i \otimes n_i \neq 0$ if and only if $\sum_{i=1}^{l} f(m_i, n_i) \neq 0$ for some A-bilinear map $f : M \times N \to L$ for some A-module L.*

Proof. Assume $\sum_{i=1}^{l} m_i \otimes n_i = 0$, then any bilinear $f : M \times N \to L$ would have $\sum_{i=1}^{l} f(m_i, n_i) = \sum_{i=1}^{l} \tilde{f}(m_i \otimes n_i) = \tilde{f}(\sum_{i=1}^{l} m_1 \otimes n_i) = \tilde{f}(0) = 0$ by the universal property.
Conversely, if $\sum_{i=1}^{l} m_i \otimes n_i \neq 0$, then $\sum_{i=1}^{l} i_{M\otimes_A N}(m_i, n_i) \neq 0$. □

When the base ring is clear or when the base ring is $\mathbb{Z}$, we often omit it, e.g. writing $M \otimes N$ in place of $M \otimes_A N$.

Example 4.2. Take $A = \mathbb{Z}$. In $\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}$, we have $2 \otimes (1 + 2\mathbb{Z}) = 1 \otimes (2 + 2\mathbb{Z}) = 1 \otimes 0 = 0$. However, in $2\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}$, $2 \otimes (1 + 2\mathbb{Z}) \neq 0$. Indeed, the bilinear map $b : 2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}, b(2n, x + 2\mathbb{Z}) = nx + 2\mathbb{Z}$ has $b(2, 1 + 2\mathbb{Z}) \neq 0$.

Proposition 4.3. *If $\sum_i m_i \otimes n_i = 0$ in $M \otimes_A N$, then there is a finite A-submodules $M' \leq M, N' \leq N$ such that $\sum_i m_i \otimes n_i = 0$ in $M' \otimes_A N'$.*

The proofs of this and of the next proposition are clear.

Proposition 4.4. *We have the following isomorphisms, given by the natural choice of homomorphism in each case.*
1. $M \otimes_A N \cong N \otimes_A M$.
2. $(M \otimes_A N) \otimes_A P = M \otimes_A (N \otimes_A P)$.
3. $(\bigoplus_\alpha M_\alpha) \otimes_A P \cong \bigoplus_\alpha (M_\alpha \otimes P)$.
4. $A \otimes_A M \cong M$.

5. For submodules $M' \leq M, N' \leq N$, we have $(M/M') \otimes_A (N/N') \cong (M \otimes_A N)/L$ where L is generated by $m' \otimes n$ where $m' \in M', n \in N$ and $m \otimes n'$ where $m \in M, n' \in N'$.

Example 4.3. If V, W are k-vector spaces and B, C are their bases respectively, then $B \otimes C = \{b \otimes c : b \in B, c \in C\}$ is a basis for the k-vector space $V \otimes_k W$.

Suppose $f : A \to B$ is a ring homomorphism. Any B-module M can be made an A-module via $am = f(a)m$. Conversely, any A-module N gives rise to a B-module $N_B = B \otimes_A N$ via $b'(b \otimes m) = (b'b) \otimes m$.

Example 4.4. 1. $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^n \cong \mathbb{C}^n$.
2. Suppose A is a ring, S is a set and $M = A^{\oplus S}/K$ for some A-submodule $K \leq A^{\oplus S}$. Let $f : A \to B$ be a ring homomorphism, we have $(A^{\oplus S})_B = B \otimes_A A^{\oplus S} \cong (B \otimes_A A)^{\oplus S} \cong B^{\oplus S}$. We also have $M_B = B \otimes_A A^{\oplus S}/K \cong (B \otimes_A A^{\oplus S})/L \cong B^{\oplus S}/N$ where $L \leq B \otimes_A A^{\oplus S}$ is generated by $\{b \otimes k : b \in B, k \in K\}$ and N is generated by $f(K)$ (where f is viewed as a map $A^{\oplus S} \to B^{\oplus S}$ by coordinate-wise action).
In particular, if M is finite over A, then M_B is finite over B.

Suppose B, C are A-algebras, we can think of them as A-modules and form their tensor product $B \otimes_A C$ as an A-module. We can make this a ring by extending from $(b_1 \otimes c_1)(b_2 \otimes c_2) = (b_1 b_2) \otimes (c_1 c_2)$. To see this is well-defined, observe that for any fixed $b_1 \in B, c_1 \in C$, we have the bilinear map $B \times C \to B \otimes_A C, (b, c) \mapsto (b_1 b) \otimes (c_1 c)$ which has to factor through $B \otimes_A C \to B \otimes_A C$. This makes $B \otimes_A C$ a ring. It is simultaneously a B-algebra and a C-algebra. To wit, $b \in B$ acts as multiplication by $b \otimes 1$ and $c \in C$ acts as multiplication by $1 \otimes c$. We can then make it an A-algebra via both $A \to B$ and $A \to C$, and they give $B \otimes_A C$ the same A-algebra structure.

Example 4.5 (Base Change)**.** Suppose L/k is a field extension and $A = k[T_1, \ldots, T_n]/I$. Then as one can (maybe not so immediately) verify that

$$A_L = L \otimes_k A = L \otimes_k k[T_1, \ldots, T_n]/I \cong L[T_1, \ldots, T_n]/(IL[T_1, \ldots, T_n])$$

So if $I = (f_1, \ldots, f_r)$, then $IL[T_1, \ldots, T_n] = (f_1, \ldots, f_r)$ except they now generate in $L[T_1, \ldots, T_n]$.

4.2 Flatness

Suppose $f : M \to N, g : P \to Q$ are A-module homomorphisms, then we have a natural map $f \otimes g = f \otimes_A g : M \otimes P \to N \otimes Q$ via $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$.

Proposition 4.5 (Right Exactness of Tensor Products)**.** *For an exact sequence of A-modules*

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

and an A-module N, the sequence

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

Proof. Since g is surjective, $g \otimes \mathrm{id}_N$ is surjective since its image contains all elements of the form $m \otimes n, m \in M'', n \in N$.
To see the exactness at $M \otimes_A N$, observe first that $g \circ f = 0$ implies $(g \otimes \mathrm{id}_N) \circ (f \otimes \mathrm{id}_N) = 0$. So $L = \mathrm{Im}\, f \otimes \mathrm{id}_N$ is contained in $\ker g \otimes \mathrm{id}_N$. Then we get a map $\phi : (M \otimes_A N)/L \to M'' \otimes_A N, \phi(x + L) = (g \otimes \mathrm{id}_N)(x)$.
We also have a bilinear map $M \times N \to M \otimes_A N/L, (m, n) \mapsto m \otimes n + L$ which vanishes on $M' \times N$, so it induces a bilinear map $(M/f(M')) \times N \cong M'' \times N \to (M \otimes_A N)/L$. Tracing back everything reveals that this is given by $(g(m), n) \mapsto m \otimes n + L$. It then factors through a map $\psi : M'' \otimes_A N \to (M \otimes_A N)/L$ which sends $g(m) \otimes n$ to $m \otimes n + L$. ψ, ϕ are clearly mutual inverses.
To finish the proof, just see that any $x \in \ker(g \otimes \mathrm{id}_N)$ would have $x + L = \psi(\phi(x + L)) = \psi((g \otimes \mathrm{id}_N)(x)) = 0 + L$, so $x \in L$. □

Remark. The tensor product functor is however not exact: If we only have the exactness of $M' \to M \to M''$, the induced sequence $M' \otimes_A N \to M \otimes_A N \to M'' \otimes_A N$ may not be exact. An example of this is the exact sequence $0 \to \mathbb{Z} \to \mathbb{Z}$ where the second arrow is multiplication by 2. When tensored with $\mathbb{Z}/2\mathbb{Z}$, this becomes $0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ where the second arrow is now zero, which is not injective. So this new sequence is not exact.

Definition 4.3. An A-module N is flat if $f \otimes \mathrm{id}_N$ is injective whenever f is.

In other words, N is flat if tensoring with N is an exact functor, i.e. brings exact sequences to exact sequences (not just right exact sequences).

Example 4.6. 1. Free modules are flat. Indeed, if $f : M_1 \to M_2$ is injective, then $f \otimes \mathrm{id}_{A^{\oplus S}} : M_1 \otimes A^{\oplus S} \to M_2 \otimes A^{\oplus S}$ is the map $M_1^{\oplus S} \to M_2^{\oplus S}$ by applying f entrywise, which is injective.
2. Direct summands of free modules (i.e. projective modules) are flat. If $N_1 \oplus N_2 = A^{\oplus S}$ and $f : M_1 \to M_2$ is injective, then $f \otimes \mathrm{id}_{A^{\oplus S}} : M_1 \otimes_A (N_1 \oplus N_2) \to M_2 \otimes_A (N_1 \oplus N_2)$ is injective. But $M \otimes_A (N_1 \oplus N_2) = (M \otimes_A N_1) \oplus (M \otimes_A N_2)$, so both $f \otimes \mathrm{id}_{N_1}, f \otimes \mathrm{id}_{N_2}$ are injective.

Suppose $x \in A$ is not a zerodivisor. Then $A \to A, a \mapsto xa$ is injective. If M is a flat A-module, then $M \to M, m \mapsto xm$ is injective via the identification $M \cong M \otimes_A A$. Hence M is torsion-free.

4.3 The Tor Functor

Definition 4.4. Let M, N be A-modules.
A free resolution for N is an exact sequence of the form

$$\cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow N \longrightarrow 0$$

such that each F_i is a free A-module.
We set $\mathrm{Tor}_i(M, N) = \mathrm{Tor}_i^A(M, N)$ to be the i-th homology of the chain complex

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

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

Proposition 4.6. *(i) Free resolutions always exist.*
(ii) $\mathrm{Tor}_i^A(M,N)$ *does not depend on the choice of free resolution for* N*.*
(iii) $\mathrm{Tor}_i^A(M,N) \cong \mathrm{Tor}_i^A(N,M)$*.*
(iv) $\mathrm{Tor}_i^A(M,N)$ *can also be computed by taking a free resolution of* M *and tensor them with* N*.*

Proof. Consult your favourite homological algebra book, which will either tell you to do it yourself or point you towards another source (which will either tell you to do it yourself or ...). □

Example 4.7. 1. $\mathrm{Tor}_0^A(M,N) = M \otimes_A N$.
2. Take an A-module N and suppose $x \in A$ is not a zerodivisor. Then there is a free resolution of $A/(x)$ given by

$$\cdots \longrightarrow 0 \longrightarrow A \xrightarrow{a \mapsto xa} A \longrightarrow A/(x) \longrightarrow 0$$

So

$$\mathrm{Tor}_i^A(A/(x),N) = \begin{cases} N/xN & \text{for } i = 0 \\ (0 :_N x) = \{x \in N : xn = 0\} & \text{for } i = 1 \\ 0 & \text{for } i > 1 \end{cases}$$

Take a short exact sequence

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

Suppose

$$\cdots \longrightarrow F_1' \longrightarrow F_0' \longrightarrow N' \longrightarrow 0$$

$$\cdots \longrightarrow F_1'' \longrightarrow F_0'' \longrightarrow N'' \longrightarrow 0$$

are free resolutions for N', N'' respectively, then there must exists a free resolution

$$\cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow N \longrightarrow 0$$

for N such that there are maps $F_i' \to F_i \to F_i''$ making the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & N' & \xrightarrow{f} & N & \xrightarrow{g} & N'' & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & F_0' & \longrightarrow & F_0 & \longrightarrow & F_0'' & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & F_1' & \longrightarrow & F_1 & \longrightarrow & F_1'' & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

commute with exact rows. Indeed, we can just take $F_i = F_i' \oplus F_i''$.
Now what happens if we tensor them with M? It gives a commutative diagram

$$\begin{array}{ccccccccc}
 & & M \otimes_A N' & \longrightarrow & M \otimes_A N & \longrightarrow & M \otimes_A N'' & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & M \otimes_A F_0' & \longrightarrow & M \otimes_A F_0 & \longrightarrow & M \otimes_A F_0'' & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & M \otimes_A F_1' & \longrightarrow & M \otimes_A F_1 & \longrightarrow & M \otimes_A F_1'' & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

with exact rows. We naturally get maps

$$\mathrm{Tor}_i^A(M, N') \longrightarrow \mathrm{Tor}_i^A(M, N) \longrightarrow \mathrm{Tor}_i^A(M, N'')$$

Surprisingly (well it really isn't at this point), we also get "connecting homomorphisms" $\partial : \mathrm{Tor}_i^A(M, N'') \to \mathrm{Tor}_{i-1}^A(M, N')$ giving a long exact sequence

$$\cdots \xrightarrow{\partial} \mathrm{Tor}_i^A(M, N') \longrightarrow \mathrm{Tor}_i^A(M, N) \longrightarrow \mathrm{Tor}_i^A(M, N'') \xrightarrow{\partial} \mathrm{Tor}_{i-1}^A(M, N') \longrightarrow \mathrm{Tor}_{i-1}^A(M, N) \longrightarrow \mathrm{Tor}_{i-1}^A(M, N'') \xrightarrow{\partial} \cdots$$

ending in $\cdots \to \mathrm{Tor}_0^A(M, N') \to \mathrm{Tor}_0^A(M, N) \to \mathrm{Tor}_0^A(M, N'') \to 0$.

Lemma 4.7. *For an ideal $I \leq A$, $I \otimes_A M \to A \otimes_A M \cong M$ is injective iff $\mathrm{Tor}_1^A(A/I, M) = 0$.*

Proof. Look at the long exact sequence associated to the short exact sequence $0 \to I \to A \to A/I \to 0$ and use the fact that $\mathrm{Tor}_i^A(A, M) = 0$ (since A is a free A-module). □

Proposition 4.8. *An A-module M is flat iff $I \otimes_A M \to M$ is injective for every finitely generated ideal $I \leq A$.*

Proof. The "only if" part comes from the definition of flatness.
For the "if" part, suppose $I \otimes_A M \to M$ is injective for any finitely generated ideal I of A.
Step 1: $J \otimes_A M \to M$ is injective for any ideal J of A.
Take $x \in J \otimes_A M$ and write it as a sum of pure tensors $x = \sum_{i=1}^k j_i \otimes m_i, j_i \in J, m_i \in M$. Suppose x gets mapped to 0 under $J \otimes_A M \to M$, then we must have $\sum_{i=1}^k j_i m_i = 0$ in M, which however means that $\sum_{i=1}^k j_i \otimes m_i$ gets mapped to 0 under $(j_1, \ldots, j_k) \otimes_A M \to M$. So we must have $\sum_{i=1}^k j_i \otimes m_i = 0$ in $(j_1, \ldots, j_k) \otimes_A M \to M$, hence $\sum_{i=1}^k j_i \otimes m_i = 0$ in $J \otimes_A M \to M$. This shows that $J \otimes_A M \to M$ is injective.
Step 2: $N' \otimes_A M \to N \otimes M$ is injective for any A-modules $N' \leq N$.
Suppose first that N/N' is cyclic, i.e. generated by a single element x. Then

$A \to N/N', a \mapsto ax$ is a surjective A-linear map, which means that $N/N' \cong A/J$ for some ideal J of A. We have the exact sequence

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

But $\mathrm{Tor}_1^A(N/N', M) \cong \mathrm{Tor}_1^A(A/J, M) = 0$ by the preceding lemma, so $N' \otimes_A M \to N \otimes_A M$ has to be injective.
Now suppose that N/N' is finite. Then we have a filtration $N' = N_0 \leq N_1 \leq \cdots \leq N_m = N$ with N_i/N_{i-1} cyclic. By what we already have, we have injective maps $N_{i-1} \otimes_A M \to N_i \otimes_A M$ which compose to give an injection $N' \otimes_A M \to N \otimes_A M$.
In general, if $N' \otimes_A M \to N \otimes_A M$ is not injective, then there is some $x = \sum_{i=1}^k n_i' \otimes m_i$ in the kernel. So we reduce to the finite case, which we have already dealt with. □

5 Discrete Valuation Rings

With 10 minutes left in the course, what's better than starting DVRs from scratch!

Definition 5.1. A discrete valuation on a field K is a surjective group homomorphism $v : K^\times \to \mathbb{Z}$ such that $v(x + y) \geq \min(v(x), v(y))$.

We use the convention $v(0) = \infty$.

Definition 5.2. The valuating ring $\mathcal{O}_K$ of a discrete valuation v on K is $\{x \in K : v(x) \geq 0\}$. A ring is called a DVR if it's the valuation ring of some discrete valuation.

Example 5.1. For a prime number p, we have a discrete valuation on $\mathbb{Q}$ via $v(p^n a/b) = n$ for $p \nmid a, p \nmid b$. Then $\mathcal{O}_K = \mathbb{Z}_{(p)}$.

If A is a DVR, then it's clear that $x \in A$ is a unit iff $v(x) = 0$. So for nonzero $x, y \in A$, we have $v(x) = v(y)$ iff $v(xy^{-1}) = 0$ iff $(x) = (y)$.
Since v is surjective, there is some $\pi \in A$ with $v(\pi) = 1$ (the "uniformiser"). The only nonzero ideals $\mathfrak{a}$ of A are those of the form (π^n) for some $n \geq 0$. Indeed it must be generated by y for any y minimising positive valuations of elements in $\mathfrak{a}$, for if $x \in \mathfrak{a}$ has positive valuation then by Euclidean algorithm we must have $v(y) \mid v(x)$ by minimality.
So A is a Noetherian local PID.