Commutative Algebra

Matei Ionita and Nilay Kumar

September 2013

Class 1

Definition 1. Given a ring R, a **finite-type** R-algebra is any R-algebra A which can be generated *as an R-algebra* by finitely many elements over R. Equivalently, $A \cong R[x_1, \ldots, x_n]/I$.

Definition 2. A ring map $\phi : A \to B$ is **finite** (or B is finite over A) if there exist finitely many elements of B that generate B *as an A-module*. Equivalently, there exists a surjective map $A^{\oplus n} \to B$ as A-modules.

Example 1. Consider $A = k[x_1, x_2]/(x_1x_2 - 1) \cong k[t, t^{-1}] \subset k(t)$. The map $k[x_1, x_2] \twoheadrightarrow A$ is finite but not injective. On the other hand, $k[x_1] \to A$ is injective but not finite. The map $k[y] \xrightarrow{\phi} A$ given by $y \mapsto x_1 + x_2$ works, as one can show.

Theorem (Noether Normalization)**.** *Let k be a field, and A be a finite-type k-algebra. Then there exists an $r \geq 0$ and a finite injective k-algebra map $k[y_1, \ldots, y_r] \to A$.*

Before we prove the theorem let us state some useful lemmas.

Lemma 1. *If $A \to B$ is a ring map such that B is generated as an A-algebra by $x_1, \ldots, x_n \in B$ and each x_i satisfies a monic equation*

$$x_n^{d_n} + \phi(a_{n-1})x_{n-1}^{d_{n-1}} + \ldots + \phi(a_1) = 0$$

over A, then ϕ is finite.

Proof. The map $A^{\oplus d_1 \ldots d_n} \to B$ given by

$$(a_{i_1}, \ldots, a_{i_n}) \mapsto \sum \phi(a_{i_1}, \ldots, a_{i_n}) x_1^{i_1} \cdots x_n^{i_n}$$

is surjective. □

Definition 3. Given a ring map $A \to B$ we say that an element $b \in B$ is **integral** over A if there exists a monic $P(T) \in A[T]$ such that $P(b) = 0$ in B.

Lemma 2 (Horrible lemma)**.** *Suppose $f \in k[x_1, \ldots, x_n]$ is non-zero. Pick natural numbers $e_1 \gg e_2 \gg \ldots \gg e_{n-1}$. Then $f(x_1 + x_n^{e_1}, \ldots, x_{n-1} + x_n^{e_{n-1}}, x_n)$ is of the form ax_n^N + lower order terms, where $a \in k^\times$.*

Proof. Write $f = \sum_{I \in k} a_I x^I$ with $a_I \neq 0$ for all $I \in k$, where k is a finite set of multi-indices. Substituting, we get something of the form

$$(x_1 + x_n^{e_1})^{i_i} \cdots (x_{n-1} + x_n^{e_{n-1}})^{i_{n-1}} x_n^{i_n} = x_n^{i_1 e_1 + \ldots + i_{n-1} e_{n-1} + i_n}.$$

It suffices to show that if $I, I' \in k$, for distinct I, I' we have that

$$i_1 e_1 + \ldots + i_{n-1} e_{n-1} + i_n \neq i'_1 e_1 + \ldots + i'_{n-1} e_{n-1} + i'_n.$$

If I is lexicographically larger than I' then the left hand side is greater than the right hand side. □

Lemma 3. *Suppose we have $A \to B \to C$ ring maps. If $A \to C$ is finite, then $B \to C$ is finite.*

Proof. Trivial. □

Lemma 4. *Suppose we have $A \to B \to C$ ring maps. If $A \to B$ and $B \to C$ are finite, then $A \to C$ is finite as well.*

Proof. Trivial. □

We now have enough machinery to prove Noether normalization.

Proof. Let A be as in the theorem. We write $A = k[x_1, \ldots, x_n]/I$. We proceed by induction on n. For $n = 0$, we simply have $A = k$, and we can take the identity map $k \to A$, which is clearly finite and injective. Now suppose the statement holds for $n - 1$, i.e. for algebras generated by $n - 1$ or fewer elements. If the generators $x_1, \ldots, x_n$ are algebraically independent over k (i.e. $I = 0$), we are done and we may take $r = n$ and $y_i = x_i$. If not, pick a non-zero $f \in I$. For $e_1 \gg e_2 \gg \ldots \gg e_{n-1} \gg 1$, set

$$y_1 = x_1 - x_n^{e_1}, \ldots y_{n-1} = x_{n-1} - x_n^{e_{n-1}}, x_n = x_n,$$

and consider $f(x_1, \ldots, x_n) = f(y_1 + x_n^{e_1}, \ldots, y_{n-1} + x_n^{e_{n-1}}, y_n)$. By Lemma **??**, we see that this polynomial is monic in x_n and hence, since x_i are integral over A, we conclude (by Lemma **??**) that $A = k[x_1, \ldots, x_n]/I$ is finite over $B = k[y_1, \ldots, y_{n-1}]$. To show that $B \to A$ is injective, let $J = \mathrm{Ker}(B \to A)$ and replace B by B/J. Now $B/J \to A$ is injective, and by Lemma **??** it is finite. But since B/J is finite over $k[y_1, \ldots, y_r]$ by the induction hypothesis, A must be as well (see Lemma **??**), and we are done. □

Class 2

Let A be a ring. Then we define the **spectrum of** A, $\operatorname{Spec} A$, to be the set of prime ideals of A. Note that $\operatorname{Spec}(-)$ is a contravariant functor in the sense that if $\phi : A \to B$ is a ring map we get a map $\operatorname{Spec}(\phi) : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ given by $q \mapsto \phi^{-1}(\mathfrak{q})$. In order for this to work we want $\mathfrak{q}$ prime in $B \Leftrightarrow \phi^{-1}(\mathfrak{q})$ prime in A. Notice that $\mathfrak{q}$ prime implies that $B/\mathfrak{q}$ is a domain. But ϕ induces a homomorphism $A/\phi^{-1}(\mathfrak{q}) \to B/\mathfrak{q}$ and this homomorphism must preserve multiplication. In particular, if the product of two elements in $A/\phi^{-1}(\mathfrak{q})$ is 0, then so is the product of their images in $B/\mathfrak{q}$. So $B/\mathfrak{q}$ domain implies that $A/\phi^{-1}(\mathfrak{q})$ is a domain. Then $\phi^{-1}(\mathfrak{q})$ is prime. The converse can be proved in the same way.

Remark. Abuse of notation: often we write $A \cap \mathfrak{q}$ for $\phi^{-1}(\mathfrak{q})$ even if ϕ is not injective. Note also that $\operatorname{Spec}(-)$ is in fact a functor from **Ring** to **Top**, though we will postpone discussion about topology until later.

Example 2. Consider $\mathrm{Spec}(\mathbb{C}[x])$. Since $\mathbb{C}[x]$ is a PID (and thus a UFD), the primes are principal ideals generated by irreducibles, i.e. linear terms. Hence $\mathrm{Spec}(\mathbb{C}[x]) = \{(0), (x-\lambda) | \lambda \in C\}$. Consider $\phi : \mathbb{C}[x] \to \mathbb{C}[y]$, given by $x \mapsto y^2$. Set $\mathfrak{q}_\lambda = (y-\lambda)$ and $\mathfrak{p}_\lambda = (x-\lambda)$. Then $\mathrm{Spec}(\phi)(\mathfrak{q}_\lambda) = \mathfrak{p}_{\lambda^2}$. Why is this? First note that $\phi(\mathfrak{p}_{\lambda^2}) = (x^2 - \lambda^2) = (x-\lambda)(x+\lambda) \subset \mathfrak{p}_\lambda$, which gives us an inclusion. Additionally, we have that $\mathrm{Spec}(\phi)\left((0)\right) = (0)$. Since this is everything in $\mathrm{Spec}\,\mathbb{C}[y]$, we have equality. Note that the fibres of $\mathrm{Spec}(\phi)$ are finite!

Indeed, the goal of the next couple lectures will be to show that the fibres of maps on spectra of a finite ring map are finite.

Let us start by considering the following setup. Let $\phi : A \to B$ be a ring map and $\mathfrak{p} \subset A$ a prime ideal. What is the fibre of $\mathrm{Spec}(\phi)$ over $\mathfrak{p}$? First of all, note that if $\phi^{-1}(\mathfrak{q}) = \mathfrak{q} \cap A = \mathfrak{p}$, then $\mathfrak{p}B = \phi(\phi^{-1}(\mathfrak{q}))B \subset \mathfrak{q}$.

Lemma 5. *If $I \subset A$ is an ideal in a ring A then the ring map $A \to A/I$ induces via* $\mathrm{Spec}(-)$ *a bijection* $\mathrm{Spec}(A/I) \leftrightarrow V(I) = \{\mathfrak{p} \in \mathrm{Spec}(A) | I \subset \mathfrak{p}\}$.

Proof. We use the fact that the ideals of A/I are in 1-to-1 correspondence with ideals of A containing I. We wish to extend this to prime ideals. By the third isomorphism theorem, given $J \subset I \subset A$, we have that $A/I \cong (A/J)/(I/J)$. We see that A/I is a domain iff I/J is prime in A/J iff I is prime in A; this gives us the 1-to-1 correspondence. □

Remark. Consider next the following two diagrams.

$$\begin{tikzcd} B \arrow[r] & B/\mathfrak{p}B & & \mathrm{Spec}\,B \arrow[d, "\mathrm{Spec}(\phi)"'] & \mathrm{Spec}(B/\mathfrak{p}B) \arrow[l] \arrow[d, "\mathrm{Spec}(\bar\phi)"] \\ A \arrow[u, "\phi"] \arrow[r] & A/\mathfrak{p} \arrow[u, "\bar\phi"'] \arrow[r, phantom, "\longleftrightarrow"] & & \mathrm{Spec}\,A & \mathrm{Spec}(A/\mathfrak{p}) \arrow[l] \end{tikzcd}$$

Clearly the point $\mathfrak{p} \in \mathrm{Spec}\ A$ corresponds to $(0) \in \mathrm{Spec}(A/\mathfrak{p})$. Thus, by Lemma **??**, points in the fibre of $\mathrm{Spec}(\phi)$ over $\mathfrak{p}$ are in 1-1 correspondence with points in the fibre of $\mathrm{Spec}(\bar\phi)$ over $(0) \in \mathrm{Spec}(A/\mathfrak{p})$. This fact will be very important for our proofs later on.

Lemma 6. *If k is a field, then* $\mathrm{Spec}(k)$ *has exactly one point. If k is the fraction field of a domain A, then* $\mathrm{Spec}(k) \to \mathrm{Spec}(A)$ *maps the unique point to* $(0) \in \mathrm{Spec}(A)$.

Proof. The only ideals of a field k are (0) and k itself. The sole prime ideals is thus (0) and hence $\mathrm{Spec}(k)$ has only one point. If k is the fraction field of the domain A then we have an injective map $A \to k$ which clearly pulls $(0) \subset k$ back to $(0) \subset A$. □

Next we wish to invert some elements in $B/\mathfrak{p}B$. More specifically, since we are interested in the ideals of $B/\mathfrak{p}B$ that are mapped to (0) by $\mathrm{Spec}(\bar\phi)$, we would like to 'throw out' the other ones. We do this by creating inverses for elements of $A/\mathfrak{p} - \{0\}$, such that none of them will be primes anymore. (See example **??** below for how this works.) This leads to a very general notion of localization, which we discuss in detail for the rest of the lecture.

Definition 4. Let A be a ring. A **multiplicative subset** of A is a subset $S \subset A$ such that $1 \in S$ and if $a, b \in S$, then $ab \in S$.

Definition 5. Given a multiplicative subset S, we can define the **localization of A with respect to** S, $S^{-1}A$, as the set of pairs (a, s) with $a \in A, s \in S$ modulo the equivalence relation $(a, s) \sim (a', s') \iff \exists s'' \in S$ such that $s''(as' - a's) = 0$ in A. Elements of $S^{-1}A$ are denoted $\frac{a}{s}$. Addition proceeds as usual. One checks that this is indeed a ring.

Lemma 7. *The ring map $A \to S^{-1}A$ given by $a \mapsto \frac{a}{1}$ induces a bijection* $\mathrm{Spec}(S^{-1}A) \leftrightarrow \{\mathfrak{p} \subset A | S \cap \mathfrak{p} = \varnothing\}$.

Proof. It's easy to show that $\mathrm{Spec}(\phi)(S^{-1}(A)) \subset \{\mathfrak{p} \subset A | S \cap \mathfrak{p} = \varnothing\}$. Let $\mathfrak{q}$ be a prime in $S^{-1}A$; if ϕ^{-1} contains some $s \in S$, then $\phi(s) \in \mathfrak{q}$. But $\phi(s)$ is a unit, so $\mathfrak{q} = S^{-1}A$. For the converse, □

how did this work again?

Note that any element of S becomes invertible in $S^{-1}A$ so it is not in any prime ideal of $S^{-1}A$.

Example 3. Suppose $A = \mathbb{C}[x] \to B = \mathbb{C}[y]$ with $x \mapsto 5y^2 + 3y + 2$. Then $\mathrm{Spec}(\phi)^{-1}((x)) = \mathrm{Spec}\left((A/\mathfrak{p} - \{0\})^{-1}B/\mathfrak{p}B\right) = \mathrm{Spec}\left((\mathbb{C}^\times)^{-1}\mathbb{C}[y]/(5y^2+3y+2)\right) = \mathrm{Spec}\left(\mathbb{C}[y]/(5y^2+3y+2)\right)$. There are two points in this space, since this quadratic factors into two prime ideals containing the ideal generated by this quadratic (see Lemma **??**). More generally, one may refer to the following diagram, which will be very useful next lecture.

$$\begin{tikzcd}
B \arrow[r] & B/\mathfrak{p}B \arrow[r] & \bar{\phi}\left(A/\mathfrak{p} - \{0\}\right)^{-1} B/\mathfrak{p}B \\
A \arrow[r] \arrow[u] & A/\mathfrak{p} \arrow[r] \arrow[u] & \mathrm{Fr}(A/\mathfrak{p}) = \left(A/\mathfrak{p} - \{0\}\right)^{-1} A/\mathfrak{p} \arrow[u]
\end{tikzcd}$$

Given $S \subset A$ multiplicative, and an A-module M, we can form an $S^{-1}A$-module

$$S^{-1}M = \left\{\frac{m}{s} | m \in M, s \in S\right\} / \sim$$

where the equivalence relation is the same as before. The construction $M \to S^{-1}M$ is a functor $\mathbf{Mod}_A \to \mathbf{Mod}_{S^{-1}A}$.

Lemma 8. *The localization functor $M \to S^{-1}M$ is exact.*

Proof. Suppose the sequence $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$ is exact. We wish to show that the sequence $0 \to S^{-1}M' \xrightarrow{S^{-1}\alpha} S^{-1}M \xrightarrow{S^{-1}\beta} S^{-1}M'' \to 0$ is exact. Let us first show that this sequence is exact at $S^{-1}M$, i.e. that $\mathrm{Im}(S^{-1}\alpha) = \ker(S^{-1}\beta)$. Pick $m'/s \in S^{-1}M'$. We take $S^{-1}\alpha(m'/s) = \alpha(m')/s$ and then compute $S^{-1}\beta(\alpha(m')/s) = \beta(\alpha(m'))/s = 0$ by the given exactness. This shows the inclusion $\mathrm{Im}(S^{-1}\alpha) \subset \ker(S^{-1}\beta)$. Next, choose an element $m/s \in \ker(S^{-1}\beta)$. Then $\beta(m)/s = 0$ in $S^{-1}M''$, i.e. there exists a $t \in S$ such that $t\beta(m) = 0$ in M''. Since β is a A-module homomorphism, $t\beta(m) = \beta(tm)$ and so $tm \in \ker(\beta) = \mathrm{Im}(\alpha)$. Therefore $tm = \alpha(m')$ for some $m' \in M'$. Hence we have $m/s = \alpha(m')/st = (S^{-1}\alpha)(m'/st) \in \mathrm{Im}(S^{-1}\alpha)$, which demonstrates the reverse inclusion.

The rest of the proof is left as a exercise. □

Remark. An exact functor is one that preserves quotients. What Lemma **??** says is that if $N \subset M$ then $S^{-1}M/S^{-1}N \cong S^{-1}(M/N)$. In particular, if $I \subset A$ is an ideal, then $S^{-1}(A/I) = S^{-1}A/S^{-1}I$.

Remark. If $A \xrightarrow{\phi} B$, then $S^{-1}B$ is an $S^{-1}A$-algebra and $S^{-1}B \cong \left(\phi(S)\right)^{-1}B$.

Definition 6. Let A be a ring and $\mathfrak{p} \subset A$ be a prime ideal, then $A_\mathfrak{p} = (A - \mathfrak{p})^{-1}A$ is the **local ring of A at $\mathfrak{p}$** (or the localization of A at $\mathfrak{p}$). If M is an A-module, then we set $M_\mathfrak{p} = (A - \mathfrak{p})^{-1}M$.

Definition 7. A **local ring** is a ring with a unique maximal ideal.

Lemma 9. *$A_\mathfrak{p}$ is a local ring.*

Proof. Consider the quotient $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$. By the remark above, we can factor $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} = (A-\mathfrak{p})^{-1}(A/\mathfrak{p})$. This is justified because $A_{\mathfrak{p}} = (A-\mathfrak{p})^{-1}A$ by definition and because $\mathfrak{p}A_{\mathfrak{p}} = (A-\mathfrak{p})^{-1}\mathfrak{p}$ for some reason. Next, by the remark directly above, if we let $\phi : A \to A/\mathfrak{p}$ be the natural surjection, then $(A-\mathfrak{p})^{-1}(A/\mathfrak{p}) = (\phi(A-\mathfrak{p}))^{-1}(A/\mathfrak{p}) = (A/\mathfrak{p}-\{0\})^{-1}(A/\mathfrak{p})$. But this is just the fraction field of $A/\mathfrak{p}$, i.e. $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ is a field. Hence $\mathfrak{p}A_{\mathfrak{p}}$ is maximal.

This is the unique maximal ideal because by Lemma **??**, the primes of $A_{\mathfrak{p}}$ are the primes $\mathfrak{q} \subset A$ that do not intersect $A-\mathfrak{p}$. This implies that $q \subset p$, and thus $\mathfrak{q}$ cannot be maximal unless $\mathfrak{q} = \mathfrak{p}$. $\square$

Class 3

Lemma 10. *Let $A \xrightarrow{\phi} B$ be a finite ring map. Then*

(a) for $I \subset A$ ideal, the ring map $A/I \to B/IB$ is finite;

(b) for $S \subset A$ multiplicative subset, $S^{-1}A \to S^{-1}B$ is finite;

(c) for $A \to A'$ ring map, $A' \to B \otimes_A A'$ is finite.

Proof. (a) Consider the following diagram:

$$\begin{array}{ccc} B & \longrightarrow & B/IB \\ \uparrow & & \uparrow \\ A & \longrightarrow & A/I \end{array}$$

By Lemma **??** we see that if the map $B \to B/IB$ is finite, then so is $A \to B/IB$, which would imply that (by Lemma **??**) $A/I \to B/IB$ is finite. But $B \to B/IB$ is obviously finite, as it is generated as a B-module by $\{1\}$.

(b) Since $A \to B$ is finite, there exists a surjection $A^{\oplus n} \twoheadrightarrow B$. The statement that $S^{-1}A \to S^{-1}B$ is finite follows immediately from the fact that localization is exact and hence preserves surjectivity of $(S^{-1}A)^{\oplus n} \twoheadrightarrow S^{-1}B$.

(c) We haven't yet discussed tensor products, so we will leave this for now.

$\square$

Lemma 11. *Suppose k is a field, A is a domain and $k \to A$ a finite ring map. Then A is a field.*

Proof. Since A is an algebra, multiplication by an element $a \in A$ defines a k-linear map $A \to A$. The map is also injective: $\mathrm{Ker}(a) = \{a' \in A | aa' = 0\} = \{0\}$, because A has no zero divisors. But, since $\dim_k(A)$ is finite, injectivity implies surjectivity. Then there exists a'' such that $aa'' = 1$, so a is a unit. $\square$

Lemma 12. *Let k be a field and $k \to A$ a finite ring map. Then:*

(a) Spec(A) is finite.

(b) there are no inclusions among prime ideals of A.

In other words, $\mathrm{Spec}(A)$ *is a finite discrete topological space with respect to the Zariski topology.*

Proof. For some $\mathfrak{p}$ prime in A, $A/\mathfrak{p}$ is a domain and the natural map $k \to A/\mathfrak{p}$ is finite since $k \to A$ and $A \to A/\mathfrak{p}$ are both finite. By Lemma **??** we see that $A/\mathfrak{p}$ must be a field, and that $\mathfrak{p}$ must be maximal. Hence all primes of A are maximal. This shows (b), as there can be no inclusions among maximal ideals. Moreover, by the Chinese remainder theorem (see Lemma **??** below) the map $A \to A/\mathfrak{m}_1 \times \ldots \times A/\mathfrak{m}_n$ is surjective. Since A and its quotients are vector spaces, this translates into a statement about their dimension: $\dim_k A \geq \sum_i \dim_k A/\mathfrak{m}_i \geq n$. Thus n is finite, which shows (a). $\square$

Lemma 13 (Chinese remainder theorem)**.** *Let A be a ring, and $I_1, ..., I_n$ ideals of A such that $I_i + I_j = A, \forall i \neq j$. Then there exists a surjective ring map $A \twoheadrightarrow A/I_1 \times ... \times A/I_n$ with kernel $I_1 \cap ... \cap I_n = I_1 ... I_n$.*

Proof. Omitted. $\square$

Lemma 14. *Let $A \xrightarrow{\phi} B$ be a finite ring map. The fibres of Spec(ϕ) are finite.*

Proof. Consider the following diagram:

$$\begin{tikzcd}
B \arrow[r] & B/\mathfrak{p}B \arrow[r] & B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}} = \bar{\phi}\,(A/\mathfrak{p} - \{0\})^{-1}\, B/\mathfrak{p}B \\
A \arrow[u, "\phi"] \arrow[r] & A/\mathfrak{p} \arrow[u, "\bar{\phi}"] \arrow[r] & \mathrm{Fr}(A/\mathfrak{p}) = (A/\mathfrak{p} - \{0\})^{-1}\, A/\mathfrak{p} \arrow[u]
\end{tikzcd}$$

By (a) and (b) of Lemma **??**, $\bar{\phi}$ and $\mathrm{Fr}(A/\mathfrak{p}) \to B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}$ are finite. Now recall that the points in the fibre of $\mathrm{Spec}(\phi)$ over $\mathfrak{p} \in \mathrm{Spec}(A)$ correspond to points in the fibre of $\mathrm{Spec}(\bar{\phi})$ over $(0) \in \mathrm{Spec}(A/\mathfrak{p})$. If we now look at the third column of the diagram, we see that since $\mathrm{Fr}(A/\mathfrak{p})$ is a field, Lemma **??** implies that $\mathrm{Spec}(B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}})$ is finite. Hence there must be a finite number of points in $\mathrm{Spec}(B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}})$ that map to $(0) \in \mathrm{Spec}(\mathrm{Fr}(A/\mathfrak{p}))$, and thus (again arguing via correspondence), the points in the fibre of $\mathrm{Spec}(\phi)$ over $\mathfrak{p} \in \mathrm{Spec}(A)$ must be finite. $\square$

Lemma 15. *Suppose that $A \subset B$ is a finite extension (i.e. there exists a finite injective map $A \to B$). Then Spec$(B) \to$ Spec(A) is surjective.*

Proof. We want to reduce the problem to the case where A is a local ring. For this, let $p \subset A$ be a prime. By part b of Lemma **??**, the map $A_p \to B_p$ is finite. By Lemma **??**, the same map is injective. Then we can replace A and B in the statement of the lemma by A_p and B_p.

Now, assuming that A is local, p is the maximal ideal of A, and we denote it by m in what follows. The following statements are equivalent:

$$\begin{aligned} \exists q \subset B \text{ lying over } m &\Leftrightarrow \exists q \subset B \text{ such that } mB \subset q \\ &\Leftrightarrow B/mB \neq 0 \end{aligned}$$

But the last statement is always true, since Nakayama's lemma (see below) says that $mB = B$ implies $B = 0$. $\square$

Lemma 16 (Nakayama's lemma)**.** *Let A be a local ring with maximal ideal m, and let M be a finite A-module such that $M = mM$. Then $M = 0$.*

Proof. Let $x_1, ..., x_r \in M$ be generators of M. Since $M = mM$ we can write $x_i = \sum_{j=1}^r a_{ij} x_j$, for some $a_{ij} \in m$. Then define the $r \times r$ matrix $B = 1_{r\times r} - (a_{ij})$. The above relation for the generators translates into:

$$B \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = 0$$

Now consider B^{ad}, the matrix such that $B^{\mathrm{ad}} B = \det(B) 1_{r\times r}$. Multiplying the above equation on the left by B^{ad} we obtain:

$$\det(B) \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = 0$$

Thus $\det(B) x_i = 0$ for all i. If we assume that the generators of M are nonzero, the fact that $\det(B)$ annihilates all generators implies that it is equal to 0. But, by expanding out the determinant of $B = 1_{r\times r} - (a_{ij})$, we see that it is of the form $1 + a$ for some $a \in m$. Since (A, m) is a local ring, this implies that $\det(a)$ is a unit. A unit cannot be zero in (A, m), so this is a contradiction. Thus all generators of M are zero, and $M = 0$. $\square$

Lemma 17 (Going up for finite ring maps)**.** *Let $A \to B$ be a finite ring map, p a prime ideal in A and q a prime ideal in B which belongs to the fibre of p. If there exists a prime p' such that $p \subset p' \subset A$, then there exists a prime q' such that $q \subset q' \subset B$ and q' belongs to the fibre of p'.*

$$\begin{tikzcd} B & & q \arrow[r, hook, dashed] \arrow[d] & ? \arrow[d, dashed] \\ A \arrow[u] & & p \arrow[r, hook] & p' \end{tikzcd}$$

Proof. Consider $A/p \to B/q$. This is injective since $p = A \cap q$ and finite by Lemma **??**. p'/p is a prime ideal in A/p, and by Lemma **??** its preimage is nonempty. Thus there exists a prime q'/q in A/p which maps to p'/p, and this corresponds to a prime q' in B that contains q. $\square$

Class 4

Lemma 18. *The following are equivalent for a ring A:*

(1) A is local;

(2) Spec(A) has a unique closed point;

(3) A has a maximal ideal m such that every element of $A - m$ is invertible;

(4) A is not zero and $x \in A \Rightarrow x \in A^*$ or $1 - x \in A^*$.

Proof. (1) $\Leftrightarrow$ (2) In the Zariski topology for Spec(A), a closed set looks like $V(\mathfrak{p})$ for some prime $\mathfrak{p}$. Therefore a closed point is a maximal ideal.

(1) $\Rightarrow$ (3) Let $m \subset A$ be the maximal ideal and take $x \notin m$. Then $V(x) = \emptyset$, and, by Lemma **??**, x is invertible.

(3) $\Rightarrow$ (4) If $x \notin m$ then x is invertible, so assume $x \in m$. But then $1-x \notin m$, since this would imply $1 \in m$. Therefore $1-x$ is invertible.

(4) $\Rightarrow$ (1) Let $m = A - A^*$. It's easy to show that m is an ideal. Moreover, m is maximal: assume $m \subset I$ and $m \neq I$, then I must contain a unit, and so $I = A$. There can be no other maximal ideal, since all elements of $A - m$ are units. $\square$

Lemma 19. *For $x \in A$, A local, $V(x) = \emptyset \Leftrightarrow x \in A^*$.*

Proof. The $\Leftarrow$ direction is trivial. For the converse, note that by Lemma **??**:

$$V(x) = \emptyset \Rightarrow \mathrm{Spec}(A/xA) = \emptyset \Leftrightarrow A/xA = 0 \Leftrightarrow x \text{ unit}$$

$\square$

Example 4. Examples of local rings:

(a) fields, the maximal ideal is (0).

(b) $\mathbb{C}[[z]]$, power series ring, the maximal ideal is (z). Note that something of the form $z - \lambda$ is invertible by some power series, and thus cannot be maximal.

(c) for X topological space and $x \in X$, $O_{X,x}$, the ring of germs of continuous $\mathbb{C}$-valued functions at x. The maximal ideal is $m_x = \{(U, f) \in O_{X,x} | f(x) = 0\}$. Note that, if $g \notin m_x$, then $g \neq 0$ on a neighborhood of x, because of continuity. Therefore g is invertible on this neighborhood. Then, by Lemma **??**, m_x is maximal.

(d) for k a field, $k[x]/(x^n)$, the maximal ideal is $(x)/(x^n)$.

For the rest of the lecture, we examine the closedness of maps on spectra.

Definition 8. Let X be a topological space, $x, y \in X$. We say that x **specializes to** y or y **is a generalization of** x if $y \in \overline{\{x\}}$. We denote this as $x \rightsquigarrow y$.

Example 5. In Spec$\mathbb{Z}$ we have $(0) \rightsquigarrow (p)$ for all primes p, but not $(p) \rightsquigarrow (0)$ or $(p) \rightsquigarrow (q)$, unless $p = q$.

Lemma 20. *The closure of $\mathfrak{p}$ in Spec(A) is $V(\mathfrak{p})$. In particular, $\mathfrak{p} \rightsquigarrow \mathfrak{q}$ iff $\mathfrak{p} \subset \mathfrak{q}$.*

Proof.

$$\overline{\{\mathfrak{p}\}} = \bigcap_{I \subset \mathfrak{p}} V(I) = V(\bigcap_{I \subset \mathfrak{p}} I) = V(\mathfrak{p})$$

$\square$

Lemma 21. *The image of Spec$(A_{\mathfrak{p}}) \to \mathrm{Spec}(A)$ is the set of all generators of $\mathfrak{p}$.*

Proof. By Lemma **??**, there is a bijection between primes of $A_{\mathfrak{p}}$ and primes of A contained in $\mathfrak{p}$. But the latter are all ideals generated by a subset of the generators of $\mathfrak{p}$, and in particular the generators themselves. $\square$

Definition 9. A subset T of a topological space is **closed under specialization** if $x \in T$ and $x \rightsquigarrow y$ imply $y \in T$.

Notation: for $f \in A$, let $D(f) = \mathrm{Spec}(A) - (f) = \{\mathfrak{q} \in A | f \notin \mathfrak{q}\}$. Obviously $D(f)$ is open.

Lemma 22. *Let $A \to B$ be a ring map. Set $T = Im\big(\operatorname{Spec}(B) \to \operatorname{Spec}(A)\big)$. If T is closed under specialization then T is closed.*

Proof. Suppose $\mathfrak{p} \in \bar{T}$. Then every open neighborhood of $\mathfrak{p}$ contains a point of T. Now pick $f \in A \setminus \mathfrak{p}$. Then $D(f) \subset \operatorname{Spec} A$ is an open neighborhood of $\mathfrak{p}$. Then there exists a $\mathfrak{q} \subset B$ with $\operatorname{Spec}(\phi)(\mathfrak{q}) \in D(f)$, which implies that ther exists a $\mathfrak{q} \subset B$ such that $\phi(f) \neq \mathfrak{q}$. Hence $B_f \neq 0$.

Thus we see $\phi(f) \cdot 1 \neq 0$ for all $f \in A \setminus \mathfrak{p}$. Hence $B_{\mathfrak{p}} \neq 0$ ($1 \neq 0$) and thus $\operatorname{Spec}(B_{\mathfrak{p}}) \neq \varnothing$. We conclude (Lemma **??**) that there exists a $\mathfrak{q}' \subset B$ such that $\mathfrak{p}' = \phi^{-1}(\mathfrak{q}') \in T$ is a generalization of $\mathfrak{p}$, i.e. $\mathfrak{p}$ is a specialization of a point of T, and we conclude that $\mathfrak{p} \in T$. $\square$ understand this

Lemma 23. *If going up holds from A to B, then $\operatorname{Spec}(\phi)$ is closed as a map of topological spaces.*

Proof. Let $Z \subset \operatorname{Spec}(B)$ be a closed subset; we want to show that its image is closed. In the Zariski topology closed sets look like $V(J)$ for some prime J, and by Lemma **??** we have $Z = \operatorname{Im}\big(\operatorname{Spec}(B/J) \to \operatorname{Spec}(B)\big)$. Then:

$$\begin{tikzcd}
& \operatorname{Spec}(B/J) \arrow[dl] \arrow[dr, "\cong"] & \\
\operatorname{Spec}(B) \arrow[d, "\operatorname{Spec}(\phi)"'] & & Z \arrow[ll, hook'] \arrow[d, "\operatorname{Spec}(\phi)"] \\
\operatorname{Spec}(A) & & \operatorname{Spec}(\phi)(Z) \arrow[ll, hook']
\end{tikzcd}$$

Note that $\operatorname{Spec}(\phi)(Z) = \operatorname{Im}\big(\operatorname{Spec}(B/J) \to \operatorname{Spec}(A)\big)$. By Lemma **??** it suffices to show that $\operatorname{Spec}(\phi)(Z)$ is closed under specialization. That is, if there exists some prime $\mathfrak{p}' \subset A$ which specializes to another prime $\mathfrak{p}$ and is the image of a prime $\mathfrak{q}' \subset B$, then $\mathfrak{p}$ is also the image of some prime $\mathfrak{q} \subset B$. Suppose we have the solid part of the diagram; by going up we can find $\mathfrak{q}$ fitting into the diagram below, therefore $p \in \operatorname{Spec}(\phi)(Z)$ as long as $p' \in \operatorname{Spec}(\phi)(Z)$.

$$\begin{tikzcd}
B & J \arrow[r, hook] & q' \arrow[r, hook, dashed] \arrow[d] & ? \arrow[d, dashed] \\
A \arrow[u] & & p' \arrow[r, hook] & p
\end{tikzcd}$$

$\square$ understand this

Class 5: Krull dimension

Definition 10.

(a) A topological space X is **reducible** if it can be written as the union $X = Z_1 \cup Z_2$ of two closed, proper subsets Z_i of X. A topological space is **irreducible** if it is not reducible.

(b) A subset $T \subset X$ is called **irreducible** iff T is irreducible as a topological space with the induced topology.

(c) An **irreducible component** of X is a maximal irreducible subset of X.

Example 6.

(a) In $\mathbb{R}^n$ with the usual topology, the only irreducible subsets are the singletons. This is true in general for any Hausdorff topological space.

(b) $\operatorname{Spec} \mathbb{Z}$ is irreducible.

(c) If A is a domain, then $\operatorname{Spec} A$ is irreducible. This is because $(0) \in V(I) \iff I \subset (0) \iff I \subset (0) \iff I = (0) \implies V(I) = \operatorname{Spec} A$.

(d) $\operatorname{Spec}(k[x, y]/(xy))$ is reducible because it is $V(x) \cup V(y)$: geometrically speaking, the coordinate axes

Lemma 24. *Let X be a topological space.*

(a) If $T \subset X$ is irreducible so is $\bar{T} \subset X$;

(b) An irreducible component of X is closed;

(c) X is the union of its irreducible components, i.e. $X = \cup_{i \in I} Z_i$ where $Z_i \subset X$ are closed and irreducible with no inclusions among them.

Proof. Omitted. □

Lemma 25. *Let $X = \operatorname{Spec} A$ where A is a ring. Then,*

(a) $V(I)$ is irreducible if and only if $\sqrt{I}$ is a prime;

(b) Any closed irreducible subset of X is of the form $V(\mathfrak{p})$, $\mathfrak{p}$ a prime;

(c) Irreducible components of X are in one-to-one correspondence with the minimal primes of A

Proof.

(a) $V(I) = \{\mathfrak{p} : I \subset \mathfrak{p}\} = V(\sqrt{I})$ so we may replace I by $\sqrt{I}$. For the backwards direction, let I be a prime. Then A/I is a domain, so $\operatorname{Spec}(A/I) = V(I)$ by a previous lemma (this is true both as sets and topologies), which is irreducible by the example (c) above. Conversely, if $V(I)$ is irreducible and $ab \in I$, then
$$V(I) = V(I, a) \cup V(I, b).$$
By irreduciblity we have that $V(I) = V(I, a)$ or $V(I) = V(I, b)$. This implies that either $a \in I$ or $b \in I$ by Lemma **??** below.

(b) Omitted.

(c) Omitted.

□

Lemma 26. $\sqrt{I} = \cap_{I \subset \mathfrak{p}} \mathfrak{p}$

Proof. That the left-hand side is included in the right-hand side is clear. Conversely, suppose f is contained in the right-hand side. Then $\operatorname{Spec}((A/I)_f) = \varnothing$ and hence $(A/I)_f = 0$ as a ring. This implies that $f^n \cdot 1 = 0$ in A/I, and hence that $f^n \in I$. □

Definition 11. Let X be a topological space. We set

$$\dim X = \sup \{n | \exists Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_n \subset X\}$$

with $Z_i \subset X$ irreducible and closed. We call $\dim X$ the **Krull** or **combinatorial** dimension of X. Furthermore, for $x \in X$ and for $U \ni x$ open subsets of X, we set

$$\dim_x X = \min_U \dim U,$$

which is called the **dimension of** X **at x**.

Lemma 27. *Let A be a ring. The dimension of* $\operatorname{Spec} A$ *is*

$$\dim \operatorname{Spec} A = \sup\{n | \exists \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq p_n \subset A\},$$

(for $\mathfrak{p}_i$ primes) and is called the dimension of A.

Proof. Clear from Lemma **??**. ☐

Lemma 28. *Let A be a ring. Then*

$$\dim A = \sup_{\mathfrak{p} \subset A} \dim A_{\mathfrak{p}} = \sup_{\mathfrak{m} \subset A} \dim A_{\mathfrak{m}}.$$

Definition 12. If $\mathfrak{p} \subset A$ is prime, then the **height** of $\mathfrak{p}$ is

$$\operatorname{ht}(\mathfrak{p}) = \dim A_{\mathfrak{p}}.$$

Informally, one might think of this as the "codimension" of $V(p)$ in $\operatorname{Spec} A$.

Exercise 1. *If $\mathfrak{p} \subset A$ is a prime, then $\mathfrak{p}$ is a minimal prime if and only if $ht(\mathfrak{p}) = 0$.*

Let us now prove the lemma.

Proof. Any chain of primes in A has a last one. If we consider

$$\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n$$

we can localize to get the chain

$$\mathfrak{p}_0 A_{\mathfrak{p}_n} \subsetneq \cdots \subsetneq \mathfrak{p}_n A_{\mathfrak{p}_n}$$

in $A_{\mathfrak{p}_n}$. ☐

Lemma 29. *Let $A \xrightarrow{\phi} B$ be a finite ring map such that* $\operatorname{Spec} \phi$ *is surjective. Then* $\dim A = \dim B$.

Proof. By our description of fibres of $\operatorname{Spec}(\phi)$ in the proofs of Lemma **??** and **??**, there are no strict inclusions among primes in a fibre. If we take the chain

$$\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \mathfrak{q}_n$$

in B then $A \cap \mathfrak{q}_0 \subsetneq \cdots \subsetneq A \cap \mathfrak{q}_n$ is a chain in A. Hence $\dim B \leq \dim A$. On the other hand, let $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ be a chain of primes in A. Pick $\mathfrak{q}_0$ lying over $\mathfrak{p}_0$ in B (since $\operatorname{Spec}(\phi)$ is surjective). We can now use going up to succesively pick $\mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_n$ lying over $\mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ (a previous lemma showed that going up holds for finite ring maps). We conclude that $\dim B \geq \dim A$. ☐

Remark. There are a few remarks to be made here:

(a) The proof shows that if $A \xrightarrow{\phi} B$ has going up and $\operatorname{Spec}(\phi)$ is surjective, then $\dim A = \dim B$. The same statement holds for going down in place of going up.

(b) By Noether normalization together with Lemma **??**, we can conclude that the dimension of a finite-type algebra over a field k is equal to the dimension of $k[t_1, \ldots, t_r]$ for some r.

(c) It will turn out that $\dim k[t_1, \ldots, t_r] = r$. For now all we can say is that it is certainly greater than r because we can construct the chain

$$(0) \subset (t_1) \subset (t_1, t_2) \subset \ldots \subset (t_1, \ldots, t_r).$$

Now we talk for a bit about dimension 0 rings.

Definition 13. An ideal $I \subset A$ is **nilpotent** if there exists $n \geq 1$ such that $I^n = 0$. It is **locally nilpotent** if $\forall x \in I, \exists n \geq 1$ such that $x^n = 0$.

Lemma 30. *For $\mathfrak{p} \subset A$ prime, the following are equivalent:*

(a) $\mathfrak{p}$ *minimal*

(b) $ht(\mathfrak{p}) = 0$

(c) the maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$ *of* $A_{\mathfrak{p}}$ *is locally nilpotent*

Proof. (a)$\Leftrightarrow$(b) follows from the description of $\operatorname{Spec}(A_{\mathfrak{p}})$ in Lemma **??**. The rest follows from Lemma **??**, stated below. ☐

Lemma 31. *If (A, m) is local, the following are equivalent:*

(a) $dim(A) = 0$

(b) $Spec(A) = \{m\}$

(c) m *is locally nilpotent*

Proof. (b) $\Rightarrow$ (c) If $f \in m$ is not nilpotent, then $A_f \neq 0$, so $\operatorname{Spec}(A_f) \neq 0$, so $\exists \mathfrak{p} \subset A, f \notin \mathfrak{p}$, which is a contradiction; hence $\mathfrak{p} = m$. ☐

Definition 14. A ring is **Noetherian** if every ideal is finitely generated.

Lemma 32. *Let $I \subset A$ be an ideal. If I is locally nilpotent and finitely generated, then I is nilpotent. In particular, if A is Noetherian then all locally nilpotent ideals are nilpotent.*

Proof. If $I = (f_1, ..., f_n)$ and $f_i^{e_i} = 0$, then consider:

$$(a_1 f_1 + ... + a_n f_n)^{(e_1 - 1) + ... + (e_n - 1) + 1} = \sum (\text{binomial coefficient}) a_1^{i_1} ... a_n^{i_n} f_1^{i_1} ... f_n^{i_n} = 0$$

Since in each term at least one of the i_j will be $\geq e_j$, which will make $f_j^{i_j} = 0$. ☐

Class 6

Definition 15. Let A be a ring and M be an A-module. We say that M is **Artinian** ring if it satisfies the descending chain condition on ideals. We say that A is Artinian if A is Artinian as an A-module.

Lemma 33. *Let*

$$0 \to M' \to M \to M'' \to 0$$

be a short exact sequence of A-modules. If M' and M'' are Artinian (of length m, n) then M is as well (of length $\max(m, n)$*).*

Proof. Suppose $M \subset M_1 \subset \dots$ are submodules of M. By assumption, there exists an n such that $M_n \cap M' = M_{n+1} \cap M' = \cdots$ and there exists an m such that $\pi(M_m) = \pi(M_{m+1}) = \cdots$. Then $M_t = M_{t+1} = \cdots$ for $t = \max(m, n)$. □

Lemma 34. *A Noetherian local ring of dimension 0 is Artinian.*

Proof. Using Lemmas **??** and **??** we get that $\mathfrak{m}^n = 0$ for some $n \geq 1$. So $0 = \mathfrak{m}^n \subset \mathfrak{m}^{n-1} \subset \cdots \subset \mathfrak{m} \subset A$. Then $\mathfrak{m}^i/\mathfrak{m}^{i+1} = (A/\mathfrak{m})^{\oplus r_i}$ is an $A/\mathfrak{m}$-module generated by finitely many elements (since A is Noetherian). So it is clear that $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ is Artinian as an $A/\mathfrak{m}$-module, hence over A. Apply Lemma **??** repeatedly. □

Lemma 35. *If A is Noetherian then so is*

(a) A/I for $I \subset A$ an ideal;

(b) $S^{-1}A$ with $S \subset A$ multiplicative;

(c) $A[x_1, \dots, x_n]$;

(d) any localization of a finite-type A-algebra.

Proof. Omitted. □

Remark. Any finite-type algebra over a field or over $\mathbb{Z}$ is Noetherian.

Theorem 36 (Hauptidealsatz, v.1)**.** *Let $(A, \mathfrak{m})$ be a Noetherian local ring. If $\mathfrak{m} = \sqrt{(x)}$ for some $x \in \mathfrak{m}$ then* $\dim A \leq 1$.

Proof. Take $\mathfrak{p} \subset A, \mathfrak{p} \neq \mathfrak{m}$. We will show $\mathrm{ht}(p) = 0$ and the theorem will follow. Observe that $x \notin \mathfrak{p}$ because if it were, by primeness of $\mathfrak{p}$, $\sqrt{(x)}$ would be contained in $\mathfrak{p}$, which is a contradiction. Set for $n \geq 1$,

$$\mathfrak{p}^{(n)} = \{a \in A | \frac{a}{1} \in \mathfrak{p}^n A_\mathfrak{p}\}.$$

We will use later that $\mathfrak{p}^{(n)} A_\mathfrak{p} = \mathfrak{p}^n A_\mathfrak{p}$ (proof omitted). The ring $B = A/(x)$ is local and Noetherian with nilpotent maximal ideal (since $\mathfrak{m} = \sqrt{(x)}$). By Lemma **??** B is Artinian. Hence

$$\frac{\mathfrak{p} + (x)}{(x)} \supset \frac{\mathfrak{p}^{(2)} + (x)}{(x)} \supset \frac{\mathfrak{p}^{(3)} + (x)}{(x)} \supset \cdots$$

stabilizes and $\mathfrak{p}^{(n)} + (x) = \mathfrak{p}^{(n+1)} + (x)$ for some n. Then every $f \in \mathfrak{p}^{(n)}$ is of the form $f = ax + b$ where $a \in A, b \in \mathfrak{p}^{(n+1)}$. This implies that $\frac{a}{1} \cdot \frac{x}{1} = \frac{f-b}{1} \in \mathfrak{p}^n A_\mathfrak{p}$ and $\frac{x}{1}$ is a unit in $A_\mathfrak{p}$. Thus $\frac{a}{1} \in \mathfrak{p}^n A_\mathfrak{p}$ and $a \in \mathfrak{p}^{(n)}$. Hence $\mathfrak{p}^{(n)} = x\mathfrak{p}^{(n)} + \mathfrak{p}^{(n+1)}$. Since $x \in \mathfrak{m}$ and $\mathfrak{p}^{(n)}$ and $\mathfrak{p}^{(n+1)}$ are finite A-modules, Nakayama's lemma implies that $\mathfrak{p}^{(n)} = \mathfrak{p}^{(n+1)}$. Going back to $A_\mathfrak{p}$, we get $\mathfrak{p}^{(n)}A_\mathfrak{p} = \mathfrak{p}^{(n+1)}A_\mathfrak{p}$, which implies that $\mathfrak{p}^n A_\mathfrak{p} = \mathfrak{p}^{n+1}A_\mathfrak{p}$. By Nakayama's lemma, $\mathfrak{p}^n A_\mathfrak{p} = 0$. Finally, by Lemma **??** $\dim A_\mathfrak{p} = 0$, i.e. $\mathrm{ht}(\mathfrak{p}) = 0$. □

Lemma 37. *In the situation of the previous theorem,* $\dim A = 0$ *if and only if* x *is nilpotent and* $\dim A = 1$ *if and only if* x *is not nilpotent.*

Proof. By Lemma **??**, $\dim A = 0$ if and only if $\mathfrak{m}$ is locally nilpotent. □

Lemma 38. *If* $(A, \mathfrak{m})$ *is a local Noetherian ring and* $\dim A = 1$ *then there exists an* $x \in M$ *such that* $\mathfrak{m} = \sqrt{(x)}$*.*

Proof. Since the dimension of A is 1 there must exist primes other than $\mathfrak{m}$, $\mathfrak{p}_i$ which are all minimal. To finish the proof, we will use two facts: first, that a Noetherian ring has finitely many minimal ideals and secondly, that one can find $x \in \mathfrak{m}$ with $x \notin \mathfrak{p}_i$ for $i \in I$. We shall prove these lemmas below next. Assuming these facts, $V(x) = \{\mathfrak{m}\}$, which implies that $\sqrt{(x)} = \mathfrak{m}$. □

Lemma 39 (Prime avoidance)**.** *Let* A *be a ring,* $I \subset A$ *an ideal, and* $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \subset A$ *primes. If* $I \not\subset \mathfrak{p}_i$ *for all* i *then* $I \not\subset \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n$ *(i.e. we can find a function vanishing on* I *but not on* $\mathfrak{p}_i$*, Urysohn's lemma).*

Proof. We proceed by induction on n. It's clearly true for $n = 1$. We may assume that there are no inclusions among $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ (drop smaller ones). Pick $x \in I, x \notin \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_{n-1}$ (induction hypothesis). If $x \notin \mathfrak{p}_n$, we are done; if $\mathfrak{p}_1, \ldots, \mathfrak{p}_{n-1} \subset \mathfrak{p}_n$ then $\mathfrak{p}_j \subset \mathfrak{p}_n$ for some j ($\mathfrak{p}_n$ is prime). This contradicts previous mangling of the primes. So $\mathfrak{p}_1, \ldots, \mathfrak{p}_{n-1} \not\subset \mathfrak{p}_n$ and $I \not\subset \mathfrak{p}_n$ which implies (since $\mathfrak{p}_n$ is prime) that $\mathfrak{p}_1 \cdots \mathfrak{p}_{n-1} I \not\subset \mathfrak{p}_n$. Pick $y \in \mathfrak{p}_1 \cdots \mathfrak{p}_{n-1} I$ with $y \notin \mathfrak{p}_n$. Then $x + y$ works. Indeed, $x + y \in I$, $x + y \notin \mathfrak{p}_j$ for $j = 1, \cdots, n-1$, and $x + y \notin \mathfrak{p}_n$ ($x \in \mathfrak{p}_n$ but not y). □

Lemma 40. *Let* A *be a Noetherian ring. Then*

(a) For all ideals $I \subset A$*, there exists a list of primes* $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ *such that* $I \subset \mathfrak{p}_i$ *and* $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subset I$*;*

(b) The set of primes minimal over I *is a subset of this list;*

(c) A *has a finite number of minimal primes (i.e. the spectrum has a finite number of irreducible components)*

Proof.

(a) Look at $\mathcal{I} = \{I \subset A | \text{(a) does not hold}\}$. If $\mathcal{I} \neq \varnothing$ there must exist an $I \in \mathcal{I}$ maximal with respect to inclusion (since A is Noetherian). So if $ab \in I$ and $a \notin I, b \notin I$ then $\mathfrak{p}_i \supset (I, a)$ and $(I, a) \supset \mathfrak{p}_1 \cdots \mathfrak{p}_n$, and $\mathfrak{q}_j \supset (I, b)$ and $(I, b) \supset \mathfrak{q}_1 \cdots \mathfrak{q}_m$. This implies that $I \supset (I, a)(I, b) \supset \mathfrak{p}_1 \cdots \mathfrak{p}_n \mathfrak{q}_1 \cdots \mathfrak{q}_m$ and $I \subset \mathfrak{p}_i, I \subset \mathfrak{q}_j$. This can't happen because $I \in \mathcal{I}$ and hence we conclude that I is a prime which is a contradiction.

(b) If I is minimal in $\mathfrak{p}$ then $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subset \mathfrak{p}$ and $\mathfrak{p}_j \subset \mathfrak{p}$ for some j, i.e. $\mathfrak{p}_j = \mathfrak{p}$ and $\mathfrak{p}_{\min} \supset I$.

(c) Apply (a) and (b) to $I = (0)$.

□

Class 7

For a local Noetherian ring (A, m) set $\dim A =$ the Krull dimension of A, and $d(A) = \min\,\{d | \exists x_1, \ldots, x_d \in m \text{ such that } m = \sqrt{(x_1, \ldots, x_d)}\}$. We've seen already that:

$$\dim A = 0 \Leftrightarrow m \text{ nilpotent} \Leftrightarrow d(A) = 0 \quad (\text{Lemma } \mathbf{??} + \text{Lemma } \mathbf{??})$$

$$\dim A = 1 \Leftrightarrow d(A) = 1 \quad (\text{Lemma } \mathbf{??} + \text{Lemma } \mathbf{??})$$

Theorem 41 (Krull Hauptidealsatz, v. 2)**.** $\dim A = d(A)$.

Proof. We first prove that $\dim(A) \leq d(A)$ by induction on d. Let $x_1, \ldots, x_d \in m$ such that $m = \sqrt{(x_1, \ldots, x_d)}$. Because A is Noetherian, $\forall q \subsetneq m, q \neq m$ there exists a $q \subset p \subset m$ such that there exists no prime strictly between p and m. Hence it suffices to show $\operatorname{ht}(p) \leq d - 1$ for such a p. We may assume $x_d \notin p$ (by reordering). Then $m = \sqrt{(p, x_d)}$ because there exists no prime strictly between p and m (+ Lemma **??**). Hence:

$$x_i^{n_i} = a_i x_d + z_i \quad (*)$$

For some $n_i \geq 1, z_i \in p, a_i \in A$. Then we have:

Hence $\sqrt{(x_d)} =$ maximal ideal of $A(z_1, \ldots, z_{d-1})$. By Theorem **??** $\dim A/(z_1, \ldots, z_{d-1}) \leq 1$. Then p is minimal over $(z_1, \ldots, z_{d-1})$. By Lemma **??**, pA_p is minimal over $(z_1, \ldots, z_{d-1})A_p$. Finally, by the induction hypothesis $\dim(A_p) \leq d - 1 \Rightarrow \operatorname{ht}(p) \leq d - 1$.

Now we prove that $d(A) \leq \dim(A)$. We may assume that $\dim(A) \geq 1$. Let $p_1, \ldots, p_n$ be the finite number of minimal primes of A. (By Lemma **??**) Pick $y \in m, y \notin p_i$ for $i = 1, \ldots, n$. (Such a y exists by Lemma **??**.) Then:

$$\dim\big(A/(y)\big) \leq \dim(A) - 1$$

Because all chains of primes in $A/(y)$ can be seen as a chain of primes in A that can be extended by one of the p_i). Then by the induction hypothesis there exists $\bar{x}_1, \ldots, \bar{x}_{\dim(A)-}$ in $m/(y)$ such that $m/(y) = \sqrt{(\bar{x}_1, \ldots, \bar{x}_{\dim(A)-1})}$. It follows that $m = \sqrt{(\bar{x}_1, \ldots, \bar{x}_{\dim(A)-1}, y)}$. □

Lemma 42. *Let A be a ring, $I \subset A$ an ideal, $I \subset p$ prime, $S \subset A$ a multiplicative subset, $S \cap p = \emptyset$. Then p minimal over $I \Leftrightarrow S^{-1}p$ is minimal over $S^{-1}I$ of $S^{-1}A$.*

Proof. See Lemma **??**. □

Lemma 43. *Let $(A, \mathfrak{m})$ be a Noetherian local ring. Then the dimension of A is less than or equal to the number of generators of $\mathfrak{m} = \dim_{A/\mathfrak{m}}\left(\mathfrak{m}/\mathfrak{m}^2\right)$. In particular, $\dim A < \infty$.*

Proof. The inequality is clear because if $\mathfrak{m} = (x_1, \ldots, x_n)$ then $\mathfrak{m} = \sqrt{(\mathfrak{m}_1, \ldots, \mathfrak{m}_n)}$. Equality follows from one of Nakayama's many lemmas:

- if M is finite and $\mathfrak{m}M = M$, then $M = 0$;
- if $N \subset M$, $M = \mathfrak{m}M + N$, everything finite, then $M = N$;
- if $x_1, \ldots, x_t \in M$ which generate $M/\mathfrak{m}M$, then $x_1, \ldots, x_n$ generate M.

□

Remark. Note that there do indeed exist infinte-dimensional Noetherian rings. Constructing them is not particularly fun.

Lemma 44. *Let A be a Noetherian ring. Let $I = (f_1, \dots, f_c)$ be an ideal generated by c elements (c somehow stands for codimension). If $\mathfrak{p}$ is a minimal prime over I, then $ht(p) \leq c$.*

Proof. Combine Theorem **??** and **??**. ☐

Lemma 45. *Let A be a Noetherian ring, $\mathfrak{p} \subset A$ prime. If $ht(\mathfrak{p}) = c$ then there exist $f_1, \dots, f_c \in A$ such that $\mathfrak{p}$ is minimal over $I = (f_1, \dots, f_c)$.*

Proof. By Theorem **??** there exists $x_1, \dots, x_c \in \mathfrak{p}A_\mathfrak{p}$ such that $\mathfrak{p}A_\mathfrak{p} = \sqrt{(x_1, \dots, x_c)}$. Write $x_i = f_i/g_i, f_i \in \mathfrak{p}$ and $g_i \in A, g_i \notin \mathfrak{p}$. Then $I = (f_1, \dots, f_c)$ satisfies $IA_\mathfrak{p} = (x_1, \dots, x_c)A_\mathfrak{p}$ with Lemma **??**. ☐

Lemma 46. *Let $(A, \mathfrak{m})$ be a Noetherian local ring. Let $x \in \mathfrak{m}$. Then $\dim(A/xA) \in \{\dim A, \dim A - 1\}$. If x is not contained in any minimal prime of A, e.g. if x is a nonzerodivisor, then $\dim(A/xA) = \dim A - 1$.*

Proof. If $x_1, \dots, x_t$ map to $\bar{x}_1, \dots, \bar{x}_t$ in A/xA such that $\mathfrak{m}_{A/xA} = \sqrt{(\bar{x}_1, \dots, \bar{x}_t)}$. Then $\mathfrak{m}_A = \sqrt{(x_1, \dots, x_t, x)}$. Hence $\mathrm{d}(A) \leq \mathrm{d}(A/xA) + 1$. Conversely, $\mathrm{d}(A) \leq \mathrm{d}(A/xA)$ is easy. Thus $\mathrm{d}(A/xA) \in \{\mathrm{d}(A), \mathrm{d}(A) - 1\}$ and hence the same for dimension by Theorem **??**. ☐

Lemma 47. *A nonzerodivisor of any ring is not contained in a minimal prime.*

Proof. Let $x \in A$ be a nonzerodivisor. Then the map $A \xrightarrow{a} A$ is injective. By exactness of localization, $x/1$ is a nonzerodivisor in $A_\mathfrak{p}$ for all minimal $\mathfrak{p}$. Hence x is not nilpotent in $A_\mathfrak{p}$. Note also that $x/1 \notin \mathfrak{p}A_\mathfrak{p}$ because $\mathfrak{p}A_\mathfrak{p}$ is locally nilpotent when $\mathfrak{p}$ is minimal by Lemma **??**. ☐

Example 7.

- Consider $A = (k[x, y]/(xy))_{(x,y)}$. It's clear from a previous homework exercise that $\dim A = 1$ (the primes look like $(x), (y)$, and (x, y)). Note that if we consider $A/(x)$, which is now a domain as (x) is prime in A, (x, y) is now simply (y), and the chain we are left with is $(0) \subset (y)$. Hence $\dim A/(x) = 1$.

- Consider $A = k[x, y, z]_{(x,y,z)}$. By one of the lemmas we have just proved above, since $\mathfrak{m} = (x, y, z)$ has 3 generators, it's clear that $\dim A \leq 3$. However, it must be at least 3 due to the presence of the chain $(0) \subset (x) \subset (x, y) \subset (x, y, z)$. Hence $\dim A = 3$.

- $\dim \left(k[x, y, z]/(x^2 + y^2 + z^2)\right)_{(x,y,z)} = 2 = 3 - 1$, since $(x^2 + y^2 + z^2)$ is not a zerodivisor

- $\dim \left(k[x, y, z]/(x^2 + y^2 + z^2, x^3 + y^3 + z^3)\right)_{(x,y,z)} = 1 = 3 - 2$. It suffices to check that $x^3 + y^3 + z^3$ is not 0 in the domain $k[x, y, z]/(x^2 + y^2 + z^2)$.

- $\dim \left(k[x, y, z]/(xy, yz, xz)\right)_{(x,y,z)} = 1$. This is because $\dim A/(x + y + z) = 0$, and we've seen in the problem sets that $(x + y + z)$ is not a minimal prime.

Class 8

Theorem 48 (Hilbert Nullstellensatz)**.** *Let k be a field. For any finite-type k-algebra A we have:*

(i) If $\mathfrak{m} \subset A$ is a maximal ideal then $A/\mathfrak{m}$ is a finite extension of k;

(ii) If $I \subset A$ is a radical ideal (i.e. $I = \sqrt{I}$) then $I = \cap_{I \subset \mathfrak{m}} \mathfrak{m}$.

Remark. Note that if $k = \bar{k}$ then this says that the residue fields at maximal ideals are equal to k. In particular, every maximal ideal of $k[x_1, \dots, x_n]$ is of the form $(x_1 - \lambda_1, \dots, x_n - \lambda_n)$ for some $\lambda_i \in k$.

In every ring, if I is radical then $I = \cap_{\mathfrak{p} \supset I} \mathfrak{p}$. Hence closed subsets of $\operatorname{Spec} A$ are in one-to-one correspondence with radical ideals. Part (ii) of the theorem says that if A is a finite-type k-algebra then closed points are dense in all closed subsets.

Proof. Let us prove (i) first. Note that $B = A/\mathfrak{m}$ is a finite-type k-algebra which is a field. By Noether normalization there exists some $k[t_1, \dots, t_r] \subset B$ for some $r \geq 0$. Now, by Lemma **??**, the map $\operatorname{Spec} B \to \operatorname{Spec} k[t_1, \dots, t_r]$ is surjective. Since $\operatorname{Spec} B$ is simply a point, we can conclude that $r = 0$. Hence $\dim_k B \leq \infty$.

The proof of (ii) follows from (i). We omit it. □

Lemma 49. *Let k be a field and $A \xrightarrow{\phi} B$ be a homomorphism of finite type k-algebras. Then* $\operatorname{Spec} \phi$ *maps closed points to closed points.*

Proof. We have to show that $m \in B$ maximal implies $\phi^{-1}(m)$ maximal. We look at $k \subset A/\phi^{-1}(m) \subset B/m$. Note that the latter is a finite field extension of k, by Theorem **??**. Then $\dim_k A/\phi^{-1}(m) < \infty$. Then by Lemma **??** $A/\phi^{-1}(m)$ is a field. □

Lemma 50. *For k field and A finite type k-algebra,* $\dim(A) = 0 \Leftrightarrow \dim_k A < \infty$.

Proof. By Noether normalization there exists a finite map $k[t_1, \dots, k_r] \hookrightarrow A$. Then by Lemma **??** $\dim(A) = \dim(k[t_1 \dots t_r]) \geq r$. Hence $(\Rightarrow)$ follows. For the converse use Lemma **??**. □

Our goal is now to construct a "good" dimension theory for finite type algebras over fields.

Lemma 51.

(a) For X a topological space with irreducible components Z_i then $\dim(X) = \sup \dim(Z_i)$;

(b) For a ring A, $\dim(A) = \sup_{p \subset A \text{ minimal}} \dim(A/p)$.

Proof. Omitted. □

Definition 16. Let $k \subset K$ be a field extension. The **transcendence degree** $\operatorname{trdeg}_k K = \sup\{n | \ \exists x_1, \dots, x_n$ algebraically independent over $k\}$. This means that the map $k[t_1 \dots t_n] \to K$ that takes $t_i \to x_i$ is injective.

Lemma 52. *Let k be a field, then every maximal ideal m of the ring $k[x_1 \dots x_n]$ can be generated by n numbers, and* $\dim(k[x_1 \dots x_n])_m = n$.

Proof. By Theorem **??**, the residue field $\kappa = k[x_1 \dots x_n]/m$ is finite over k. Let $\alpha_i \in \kappa$ be the image of x_i. We look at the chain:

$$k = \kappa_0 \subset \kappa_1 = k(\alpha_1) \subset \cdots \subset \kappa = k(\alpha_1, \dots, \alpha_n)$$

We know from field theory that $x_i \in k[\alpha_1, \dots, \alpha_i]$. Choose $f_i \in k[x_1 \dots x_i]$ such that $f(\alpha_1, \dots, \alpha_{i-1}, x_i)$ is the minimal polynomial of α_i over κ_{i-1}. Then $f_i(\alpha_1, \dots, \alpha_i) = 0$, so $f_i \subset m$. Now we claim that $\kappa_i \cong k[x_1, \dots, x_i]/(f_1, \dots, f_i)$. We prove this by induction:

$$k[x_1, \dots, x_i]/(f_1, \dots, f_i) \cong k[x_1, \dots, x_{i-1}]/(f_1, \dots, f_{i-1})[x_i]/(f_i)$$

If we let $i = n$, this proves the first statement of the lemma. Finally, we have a chain of primes:

$$(0) \subset (f_1) \subset \cdots \subset (f_1 \dots f_n) = m$$

because $k[x_1, \dots, x_i]/(f_1, \dots, f_i) \cong \kappa_i[x_{i+1}, \dots, x_n]$. Therefore $\dim(k[x_1, \dots, x_n])_m \geq n$. But by Lemma **??** it is at most n, so this finishes the proof. □

Lemma 53. $\dim(k[x_1, \dots, x_n]) = n$.

Proof. Omitted. □

Remark. For a Noetherian local ring $(A, \mathfrak{m})$ we have:

$$\dim A \leq \text{minimum number of generators of } \mathfrak{m} = \dim_{A/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$$

$(A, \mathfrak{m})$ is called **regular** if we have equality. The above shows that $k[x_1, \dots, x_n]_\mathfrak{m}$ is regular for all maximal ideals $\mathfrak{m}$.

Lemma 54. *Let k be a field and A be a finite type k-algebra. Then:*

(a) the integer r from Noether Normalization is equal to $\dim A$*;*

(b) if A is a domain, then $\dim A = \mathit{trdeg}_k(\mathit{f.f.}A)$.

Proof.

(a) follows from Lemma **??** and Lemma **??**

(b) follows from (a) and the fact:

$$k[t_1 \dots t_r] \subset A \text{ finite} \overset{L??}{\Rightarrow} k(t_1 \dots t_r) \subset S^{-1}A \text{ finite} \overset{L??}{\Rightarrow} S^{-1}A \text{ is the f.f. of } A$$

Then:

$$k(t_1 \dots t_r) \subset \text{f.f.}(A) \Rightarrow \text{trdeg}_k\text{f.f.}(A) = \text{trdeg}_k k(t_1 \dots t_r) = r$$

The last two equalities should be familiar from field theory. □

Remark. If $k \to A$ is a finite type domain then $\dim(A) = \dim(A_f) \forall f \in A, f \neq 0$. We may regard this as a very weak form of "equidimensionality".

Remark. So far we missed proving an important result; we will do so later. We will want to show that for A finite type domain over a field, $p \subset A$ prime, we have $\dim(A) = \dim(A/p) + \text{ht}(p)$. Intuitively it's clear why this should be so: take a chain in A and some p in this chain, then $\dim(A/p)$ counts elements containing p, and $\text{ht}(p)$ counts elements contained in p.

Definition 17. Let $A \to B$ be a ring map. The **integral closure** of A in B is $B' = \{b \in B | \text{b is integral over} A\}$. We say that B **is integral over** A iff $B' = B$.

Lemma 55. *If $A \to B$ finite, then B is integral over A.*

Proof. Pick $b \in B$. Choose $b_1, \ldots b_n, \in B$ such that $B = \sum Ab_i$. Write, for $a_ij \in A$,

$$bb_i = \sum_{a_{ij}} b_j.$$

Let $M = (a_{ij}) \in \text{Mat}(n \times n, A)$ and let $P(T) \in A[T]$ be the characteristic polynomial of M. By Cayley-Hamilton, $P(M) = 0$, which implies that $P(b) = 0$. □

Class 9

Lemma 56. *The integral closure of a ring A is an A-algebra.*

Proof. Suppose $b, b' \in B'$, we want to show that $b + b', bb' \in B'$. Let C be the A-algebra generated by b, b'. Then C is finite over A by Lemma **??**. Then by Lemma **??** C is integral over A, so $C \subset B'$. □

Lemma 57. *If $A \to B \to C$ are ring maps then:*

1. *$A \to B, B \to C$ integral $\Rightarrow A \to C$ integral;*

2. *$A \to C$ integral $\Rightarrow B \to C$ integral.*

Proof. Omitted. □

Definition 18. A **normal domain** is a domain which is integrally closed in its field of fractions. (In other words, it is equal to its integral closure in its field of fractions.)

Lemma 58. *For a field k, $k[x_1, \ldots, x_n]$ is a normal domain.*

Proof. Polynomial rings are UFDs, so this follows from Lemma **??**. □

Lemma 59. *A UFD is a normal domain.*

Proof. Suppose that $a/b \in \text{f.f.}(A)$ is in least terms (we can always reduce a fraction to least terms, due to unique factorization) and is integral over A. Thus there exist some $a_i \in A$ such that:

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

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

Therefore $a^n \in (b)$, which, unless b is a unit, contradicts the fact that a, b are relatively prime. Therefore the only elements of the field of fractions that are integral over A are those of A itself. □

Lemma 60. *Let R be a domain with field of fractions K, and let $a_0, \ldots, a_{n-1}$, $b_0, \ldots, b_{m-1} \in R$. If $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ divides $x^m + b_{m-1}x^{m-1} + \cdots + b_0$, then a_i are integral over the $\mathbb{Z}$ subalgebra of R generated by $\{b_j\}$.*

Proof. Choose some field extension L of K with $\beta_1, \beta_m \in L$ such that:

$$x^m + b_{m-1}x^{m-1} + \cdots + b_0 = \prod_{i=1}^{m}(x - \beta_i)$$

Then by unique factorization in $L[x]$ we get:

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = \prod_{j}(x - \beta_j)$$

Where j runs over a subset of $\{1, \ldots, m\}$. But this means that:

$$a_i \in \mathbb{Z}[b_0, \ldots, b_{m-1}, \beta_1, \ldots, \beta_m] \supset \mathbb{Z}[b_0, \ldots, b_{m-1}]$$

By Lemmas **??** and **??**, the inclusion is integral. □

Lemma 61. *Let $R \subset A$ be a finite extension of domains, R normal. For $a \in A$ we have:*

(1) the coefficients of the minimal polynomial of a over the field of fractions of R are in R;

(2) $\mathrm{Nm}(a) \in R$*, where* Nm *denotes the norm.*

Proof. Apply Lemma **??**. For example, a must satisfy a monic polynomial with coefficients in R, and the minimal polynomial must divide that. □

Lemma 62. *Suppose $R \subset A$ is a finite extension of domains, and R is normal. Suppose also that $f \in A$, $\mathfrak{p} \subset A$ prime with $V(f) \subset V(\mathfrak{p})$. Then setting $f_0 = \mathrm{Nm}_{\mathit{ff}(A)/\mathit{ff}R}(f)$ we have:*

1. *$f_0 \in R$;*
2. *$R \cap \mathfrak{p} = \sqrt{(f_0)}$.*

[(1)]

Proof. (1) follows by Lemma **??**. (See also the argument by Tate in Mumford's red book.) For part (2), let

$$x^d + r_1x^{d-1} + \ldots r_d$$

be the minimal polynomial of f over f.f.(R), with $r_i \in R$. (This is possible by Lemma **??**.) Then $f_0 = r_d^e$ for some $e \geq 1$. So:

$$f^d + r_1f^{d-1} + \cdots + r_d = 0 \Rightarrow r_d \in (f) \Rightarrow f_0 \in (f)$$

We already know that $f \in \mathfrak{p}$ by assumption $V(f) = V(\mathfrak{p})$, so we get $\sqrt{f_0} \subset R \cap \mathfrak{p}$. Conversely, if $r \in R \cap \mathfrak{p}$ we have $r^n \in (f)$ for some n, because $V(f) = V(\mathfrak{p})$. Say $r^n = af$, then:

$$(r^n)^{[\text{f.f.}(A):\text{f.f.}(R)]} = \mathrm{Nm}(r^n) = \mathrm{Nm}(a)\,\mathrm{Nm}(f) = \{\text{sth in } R\}f_0$$

Then $r \in \sqrt{f_0}$. □

Remark. This lemma says that the image (under a finite map) of an irreducible hypersurface is an irreducible hypersurface.

Now we use this lemma to prove the missing link from dimension theory.

Theorem 63. *Given a finite type k-algebra A which is a domain and a height 1 prime $\mathfrak{p}$, then:*

$$\dim A = \dim(A/\mathfrak{p}) + 1$$

Proof. By Lemma **??**, $\mathfrak{p}$ minimal over (f) for some $f \in A$. Say $\mathfrak{p}, \mathfrak{p}_1, \dots, \mathfrak{p}_n$ are all the distinct minimal primes over (f). (Lemma **??** says they are finitely many.) Then $\mathfrak{p}_1 \dots \mathfrak{p}_n \not\subset \mathfrak{p}$. (Prime avoidance.) Then we can pick $g \in p_1 \dots p_n$, $g \notin \mathfrak{p}$. After replacing A by A_g and $\mathfrak{p}$ by $\mathfrak{p}A_g$ and f by $f/1$ we may assume $\mathfrak{p}$ is the only prime minimal over (f), i.e. $V(f) = V(\mathfrak{p})$. By an earlier remark, $\dim A = \dim A_g$, so the statement of the theorem doesn't change if we do the replacement.

Now by Noether Normalization we choose a finite injective map $k[t_1, \dots, t_d] \hookrightarrow A$. Set $f_0 = \mathrm{Nm}(f) \in k[t_1, \dots, t_d]$, by Lemma **??** and $\mathfrak{p} \subset k[t_1, \dots, t_d] = \sqrt{(f_0)}$, again by Lemma **??**. Since $k[t_1, \dots, t_d]$ is a UFD, we can write $f_0 = cf^e$, for some $c \in k^*, e \geq 1$. Then $\sqrt{(f_0)} = (f_0)$ and we see that $k[t_1, \dots, t_d]/(f_0) \hookrightarrow A/\mathfrak{p}$ is a finite injective map. Thus:

$$\mathrm{trdeg}_k(\text{f.f.}(A/\mathfrak{p})) \subset \mathrm{trdeg}_k(\text{f.f.}(k[t_1, \dots, t_d]/(f_0))) = d - 1$$

□

Example 8. We compute the integral closure of $k[x,y]/(y^2 - x^3)$ in its field of fractions. (This is called "normalization".)

$$k[x,y]/(y^2 - x^3) \subset \text{f.f.}(k[x,y]/(y^2 - x^3))$$

To get some element in the integral closure which is not in the ring, we look at the equation:

$$y^2 - x^3 = 0 \Rightarrow \frac{y}{x} = x^{1/2}$$

We see that $t = y/x$ is both in the integral closure and in the field of fractions. We therefore add it to the ring and see what happens. We construct the map:

$$\begin{aligned} k[x,y]/(y^2 - x^3) &\to k[t] \\ x &\to t^2 \\ y &\to t^3 \end{aligned}$$

We need to check that this induces an isomorphism of fraction fields, namely maps y/x to t. We also need to check that the map is integral (it is, because t is integral). We are now done, because $k[t]$ is a UFD and therefore a normal domain.

Class 10

Matei fill in stuff here

Lemma 64.

Definition 19. A **graded ring** is a ring A together with a given direct sum decomposition $A = \oplus_{d \geq 0} A_d$ such that $A_d A_e \subset A_{d+e}$. A **graded module** M over A is an A-module M equipped with a direct sum decomposition $M = \oplus_{d \in \mathbb{Z}} Md$ such that $A_d M_e \subset M_{d+e}$. We say that B is a **graded A-algebra** if there is a direct sum decomposition as R-modules.

Example 9. If we take $A = k[x_1, \dots, x_d]$ and A_d to be the homogeneous polynomials of degree d, we see that A is a graded ring.

Theorem 65. *Let M be a finitely-generated, graded, A-module, where A is a graded k-algebra which is generated (as a k-algebra) by a finite number of elements of degree 1. Then the function $d \mapsto \dim_k(M_d)$ is a numerical polynomial. This function is known as the* ***Hilbert polynomial****.* trdeg?

Definition 20. A function $f : \mathbb{Z} \to \mathbb{Z}$ is a **numerical polynomial** iff there exists an $r \geq 0, a_i \in \mathbb{Z}$ such that

$$f(d) = \sum_{i=0}^{r} a_i \binom{d}{i}$$

for all $d \gg 0$.

Lemma 66. *If $f : \mathbb{Z} \to \mathbb{Z}$ is a function and $d \mapsto f(d) - f(d-1)$ is a numerical polynomial, then so is f.*

Let us now prove the theorem.

Proof. We may assume that $A = k[x_1, \ldots, x_d]$, graded as in the above example. The proof proceeds by induction on n. Let us consider three distinct cases. In the first, we suppose that x_n is a nonzerodivisor on M. Then we have a short exact sequence

$$0 \to M \xrightarrow{x_n} M \to M/x_nM \to 0.$$

Note that the multiplication by x_n shifts the grading by 1 and that

$$-\dim M_{d-1} + \dim M_d - \dim \left(M/x_nM\right)_d = 0.$$

Now M/x_nM is a finitely-generated graded module as $k[x_1, \ldots, x_{d-1}]$ so we are done by induction and Lemma **??**. why? morphism shifts grading

Next consider the case where $x_n^e M = 0$ for some $e \geq 0$. In this case we get a short exact sequence

$$0 \to x_nM \to M \to M/x_nM \to 0.$$

Note that $x_n^{e-1} x_n M = 0$. Hence we are done by induction on e and n.

Finally, consider the general case. Let $N = \{m \in M | x_n^e m = 0 \text{ for some } e\}$. Then we get an exact sequence

$$0 \to N \to M \to M/N \to 0.$$

At N, this follows from the nilpotent cases, as A is Noetherian and M being finitely-generated implies that N is. At M/N this follows from the nonzerodivisor case. $\square$

Definition 21. Let $(A, \mathfrak{m}, k)$ be a Noetherian local ring. Set

$$\mathrm{gr}_{\mathfrak{m}} A = \bigoplus_{n \geq 0} \mathfrak{m}^n / \mathfrak{m}^{n+1}.$$

This is a graded k-algebra generated by $\mathfrak{m}/\mathfrak{m}^2$ over k. Hence $n \mapsto \dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1})$ is a numerical polynomial by Theorem **??**. We denote by $d(A)$ the degree of this polynomial; if $\mathfrak{m}^n = 0$ for some n, we take -1.

Theorem. *For $(A, \mathfrak{m}, k)$ a Noetherian local ring, $d(A) = \dim A - 1$.*

Proof. We will only sketch the proof of this theorem. The result is clear for $\dim A = 0$. Suppose $\dim A > 0$. Suppose you can find an $x \in \mathfrak{m}$ such that x is a nonzerodivisor in A and $\bar{x} \in \mathfrak{m}/\mathfrak{m}^2$ is a nonzerodivisor in $\mathrm{gr}_{\mathfrak{m}} A$. Then $\dim A/xA = \dim A - 1$. The sequences

$$0 \to \mathfrak{m}^{n-1}/\mathfrak{m}^n \xrightarrow{x} \mathfrak{m}^n/\mathfrak{m}^{n+1} \to \bar{\mathfrak{m}}^n/\bar{\mathfrak{m}}^{n+1} \to 0$$

are exact, where $\bar{\mathfrak{m}} \subset A/xA$ is the maximal ideal. Then $d(A/xA) = d(A) - 1$, and we are done by induction on $\dim A$.

This argument will not work if such an x does not exist. Roughly speaking, one finds an x such that $\bar{x}$ is in the none of the minimal primes of $\mathrm{gr}_{\mathfrak{m}} A$ and one shows that $d(A/xA)$ does actually drop by 1. $\square$

Theorem. *If B is a graded k-algebra generated by finitely many elements of degree 1, then* $\dim B - 1$ *is the degree of the numerical polynomial $n \mapsto \dim_k B_n$.*

Corollary. $\dim A = \dim gr_{\mathfrak{m}} A$.