Commutative Algebra à la A. J. de Jong

Notes by Matei Ionita and Nilay Kumar

Fall 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 $A^{\oplus d_1 \cdots d_n} \to B$ 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. $\square$

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 2, we see that this polynomial is monic in x_n and hence, since x_i are integral over A, we conclude (by Lemma 1) 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 3 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 4), 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 $\operatorname{Spec}(\mathbb{C}[x])$. Since $\mathbb{C}[x]$ is a PID (and thus a UFD), the primes are principal ideals generated by irreducibles, i.e. linear terms. Hence $\operatorname{Spec}(\mathbb{C}[x]) = \{(0), (x-\lambda) | \lambda \in C\}$. 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 $\operatorname{Spec}(\phi)(\mathfrak{q}_\lambda) = \mathfrak{p}_{\lambda^2}$. 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 $\operatorname{Spec}(\phi)((0)) = (0)$. Since this is everything in $\operatorname{Spec} \mathbb{C}[y]$, we have equality. Note that the fibres of $\operatorname{Spec}(\phi)$ 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 $\operatorname{Spec}(\phi)$ 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 $\operatorname{Spec}(-)$ a bijection $\operatorname{Spec}(A/I) \leftrightarrow V(I) = \{\mathfrak{p} \in \operatorname{Spec}(A) | I \subset \mathfrak{p}\}$.*

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. $\square$

Remark. Consider next the following two diagrams.

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

Clearly the point $\mathfrak{p} \in \operatorname{Spec} A$ corresponds to $(0) \in \operatorname{Spec}(A/\mathfrak{p})$. Thus, by Lemma 5, points in the fibre of $\operatorname{Spec}(\phi)$ over $\mathfrak{p}$ are in 1-1 correspondence with points in the fibre of $\operatorname{Spec}(\bar{\phi})$ over $(0) \in \operatorname{Spec}(A/\mathfrak{p})$. This fact will be very important for our proofs later on.

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

Proof. The only ideals of a field k are (0) and k itself. The sole prime ideals is thus (0) and hence $\operatorname{Spec}(k)$ 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 $(0) \subset A$. $\square$

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 $\operatorname{Spec}(\bar{\phi})$, 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 3 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* $\operatorname{Spec}(S^{-1}A) \leftrightarrow \{\mathfrak{p} \subset A | S \cap \mathfrak{p} = \varnothing\}$.

Proof. It's easy to show that $\operatorname{Spec}(\phi)(S^{-1}(A)) \subset \{\mathfrak{p} \subset A | S \cap \mathfrak{p} = \varnothing\}$. 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, $\square$

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

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

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. $\square$

Remark. An exact functor is one that preserves quotients. What Lemma 8 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 $S^{-1}B \cong \big(\phi(S)\big)^{-1}B$.

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 7, 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 4 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 3) $A/I \to B/IB$ 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. □

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. □

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, 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 11 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 13 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 10, $\bar{\phi}$ 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 12 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 10, the map $A_p \to B_p$ is finite. By Lemma 8, 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 $B^{\text{ad}} B = \det(B) 1_{r\times r}$. 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 3. p'/p is a prime ideal in A/p, and by Lemma 15 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 19, 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 7:

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

$\square$

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 18, 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.
$$\overline{\{\mathfrak{p}\}} = \bigcap_{I \subset \mathfrak{p}} V(I) = V\Big(\bigcap_{I \subset \mathfrak{p}} I\Big) = V(\mathfrak{p})$$
$\square$

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 7, 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* $T = Im\big(\mathrm{Spec}(B) \to \mathrm{Spec}(A)\big)$. *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 $D(f) \subset \mathrm{Spec}\, A$ is an open neighborhood of $\mathfrak{p}$. Then there exists a $\mathfrak{q} \subset B$ with $\mathrm{Spec}(\phi)(\mathfrak{q}) \in D(f)$, 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 $\mathrm{Spec}(B_{\mathfrak{p}}) \neq \varnothing$. We conclude (Lemma 21) 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* $\mathrm{Spec}(\phi)$ *is closed as a map of topological spaces.*

Proof. Let $Z \subset \mathrm{Spec}(B)$ 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 7 we have $Z = \mathrm{Im}\big(\mathrm{Spec}(B/J) \to \mathrm{Spec}(B)\big)$. Then:

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

Note that $\mathrm{Spec}(\phi)(Z) = \mathrm{Im}\big(\mathrm{Spec}(B/J) \to \mathrm{Spec}(A)\big)$. By Lemma 22 it suffices to show that $\mathrm{Spec}(\phi)(Z)$ 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. $\square$

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 26 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 25. □

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

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

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 12 and 14, 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 29, 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 Spec$(A_{\mathfrak{p}})$ in Lemma 21. The rest follows from Lemma 31, 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 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 $t = \max(m, n)$. $\square$

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

Proof. Using Lemmas 31 and 32 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 33 repeatedly. $\square$

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. $\square$

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 34 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 30 $\dim A_\mathfrak{p} = 0$, 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 31, $\dim A = 0$ 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 $d(A) = \min \{d | \exists x_1, \dots, x_d \in m \text{ such that } m = \sqrt{(x_1, \dots, x_d)}\}$. We've seen already that:

$$\dim A = 0 \Leftrightarrow m \text{ nilpotent} \Leftrightarrow d(A) = 0 \quad \text{(Lemma 31 + Lemma 32)}$$

$$\dim A = 1 \Leftrightarrow d(A) = 1 \quad \text{(Lemma 36 + Lemma 38)}$$

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 $x_1, \dots, x_d \in m$ such that $m = \sqrt{(x_1, \dots, x_d)}$. 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 $\mathrm{ht}(p) \leq d - 1$ 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 26). 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 $A(z_1, \dots, z_{d-1})$. By Theorem 36 $\dim A/(z_1, \dots, z_{d-1}) \leq 1$. Then p is minimal over $(z_1, \dots, z_{d-1})$. By Lemma 42, pA_p is minimal over $(z_1, \dots, z_{d-1})A_p$. Finally, by the induction hypothesis $\dim(A_p) \leq d - 1 \Rightarrow \mathrm{ht}(p) \leq d - 1$.

Now we prove that $d(A) \leq \dim(A)$. We may assume that $\dim(A) \geq 1$. Let $p_1, \dots, p_n$ be the finite number of minimal primes of A. (By Lemma 40) Pick $y \in m, y \notin p_i$ for $i = 1, \dots, n$. (Such a y exists by Lemma 39.) 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 $m = \sqrt{(\bar{x}_1, \ldots, \bar{x}_{\dim(A)-1}, y)}$. $\square$

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 7. $\square$

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.

$\square$

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 $I = (f_1, \ldots, f_c)$ 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 41 and 42. $\square$

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

Proof. By Theorem 41 there exists $x_1, \ldots, x_c \in \mathfrak{p}A_\mathfrak{p}$ such that $\mathfrak{p}A_\mathfrak{p} = \sqrt{(x_1, \ldots, x_c)}$. Write $x_i = f_i/g_i, f_i \in \mathfrak{p}$ and $g_i \in A, g_i \notin \mathfrak{p}$. Then $I = (f_1, \ldots, f_c)$ satisfies $IA_\mathfrak{p} = (x_1, \ldots, x_c)A_\mathfrak{p}$ with Lemma 42. $\square$

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 $x_1, \ldots, x_t$ map to $\bar{x}_1, \ldots, \bar{x}_t$ in A/xA such that $\mathfrak{m}_{A/xA} = \sqrt{(\bar{x}_1, \ldots, \bar{x}_t)}$. Then $\mathfrak{m}_A = \sqrt{(x_1, \ldots, x_t, x)}$. 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 41. $\square$

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 30. $\square$

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 $k[x_1, \ldots, x_n]$ is of the form $(x_1 - \lambda_1, \ldots, x_n - \lambda_n)$ 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 $k[t_1, \ldots, t_r] \subset B$ for some $r \geq 0$. Now, by Lemma 15, the map $\operatorname{Spec} B \to \operatorname{Spec} k[t_1, \ldots, t_r]$ 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. $\square$

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 48. Then $\dim_k A/\phi^{-1}(m) < \infty$. Then by Lemma 11 $A/\phi^{-1}(m)$ is a field. $\square$

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 $k[t_1, \ldots, k_r] \hookrightarrow A$. Then by Lemma 29 $\dim(A) = \dim(k[t_1 \ldots t_r]) \geq r$. Hence $(\Rightarrow)$ follows. For the converse use Lemma 12. $\square$

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. $\square$

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

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

Proof. By Theorem 48, the residue field $\kappa = k[x_1 \ldots x_n]/m$ is finite over k. Let $\alpha_i \in \kappa$ be the image of x_i. We look at the chain:

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

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

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

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 41 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 $\dim A = trdeg_k(f.f.A)$.

Proof.

(a) follows from Lemma 29 and Lemma 53

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

$$k[t_1 \dots t_r] \subset A \text{ finite} \overset{L10}{\Rightarrow} k(t_1 \dots t_r) \subset S^{-1}A \text{ finite} \overset{L11}{\Rightarrow} S^{-1}A \text{ is the f.f. of } A$$

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 $M = (a_{ij}) \in \mathrm{Mat}(n \times n, A)$ 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 1. Then by Lemma 55 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 59. □

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 $\{1, \dots, m\}$. But this means that:

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

By Lemmas 1 and 55, 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 60. 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 61. (See also the argument by Tate in Mumford's red book.) For part (2), let

$$x^d + r_1 x^{d-1} + \dots r_d$$

be the minimal polynomial of f over f.f.(R), with $r_i \in R$. (This is possible by Lemma 61.) Then $f_0 = r_d^e$ for some $e \geq 1$. So:

$$f^d + r_1 f^{d-1} + \cdots + r_d = 0 \Rightarrow r_d \in (f) \Rightarrow f_0 \in (f)$$

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 45, $\mathfrak{p}$ minimal over (f) for some $f \in A$. Say $\mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are all the distinct minimal primes over (f). (Lemma 40 says they are finitely many.) Then $\mathfrak{p}_1 \ldots \mathfrak{p}_n \not\subset \mathfrak{p}$. (Prime avoidance.) Then we can pick $g \in p_1 \ldots p_n$, $g \notin \mathfrak{p}$. 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 $k[t_1, \ldots, t_d] \hookrightarrow A$. Set $f_0 = \mathrm{Nm}(f) \in k[t_1, \ldots, t_d]$, by Lemma 62 and $\mathfrak{p} \subset k[t_1, \ldots, t_d] = \sqrt{(f_0)}$, again by Lemma 62. Since $k[t_1, \ldots, t_d]$ 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 $k[t_1, \ldots, t_d]/(f_0) \hookrightarrow A/\mathfrak{p}$ is a finite injective map. Thus:

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

□

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

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

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

Corollary 64. *Let A be a finite type k-algebra. Then:*

(1) A domain $\Rightarrow$ any maximal chain of primes in A has length $\dim A$;

(2) A domain and $\mathfrak{p} \subset A$ prime $\Rightarrow \dim A = \dim(A/\mathfrak{p}) + ht(\mathfrak{p})$;

(3) A domain and $\mathfrak{m} \subset A$ maximal $\Rightarrow \dim(A_\mathfrak{m}) = \dim A$ and all maximal chains of primes in $A_\mathfrak{m}$ have length $\dim A$;

(4) if $\mathfrak{p} \subset \mathfrak{q} \subset A$ then any maximal chain of primes between $\mathfrak{p}$ and $\mathfrak{q}$ has length $\mathrm{trdeg}_k(f.f.(\mathfrak{p})) - \mathrm{trdeg}_k(f.f.(\mathfrak{q}))$;

(5) if $\mathfrak{m} \subset A$ maximal then $\dim(A_m) = \max_{\mathfrak{p}\ minimal} \dim(A/\mathfrak{p}) = \dim_\mathfrak{m} \mathrm{Spec}(A)$.

Proof. (1) Choose a chain of primes:

$$(0) \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_l \subsetneq A$$

We have $\mathrm{ht}(\mathfrak{p}_1) = 1$. Hence Proposition 63 shows that $\dim(A/\mathfrak{p}_1) = \dim(A) - 1$ and thus we get a chain:

$$(0) = \frac{\mathfrak{p}_1}{\mathfrak{p}_1} \subsetneq \frac{\mathfrak{p}_2}{\mathfrak{p}_1} \subsetneq \cdots \subsetneq \frac{\mathfrak{p}_l}{\mathfrak{p}_1}$$

By induction $l = \dim A$.

(2) Let $h = \mathrm{ht}(\mathfrak{p})$ and $d = \dim(A/\mathfrak{p})$. Then we have chains:

$$(0) = \frac{\mathfrak{p}}{\mathfrak{p}} \subsetneq \frac{\mathfrak{p}_1}{\mathfrak{p}} \subsetneq \cdots \subsetneq \frac{\mathfrak{p}_d}{\mathfrak{p}} \subsetneq \frac{A}{\mathfrak{p}}$$

$$(0) \subsetneq \mathfrak{q}_1 A_\mathfrak{p} \subsetneq \cdots \subsetneq \mathfrak{q}_h A_\mathfrak{p}$$

Then $(0) \subsetneq \cdots \subsetneq \mathfrak{q}_{h-1} \subsetneq \mathfrak{q}_h = \mathfrak{p} \subset \ldots \mathfrak{p}_d$ is a maximal chain of primes in A of length $h + d$. By (1) $\dim A = h + d$.

(3) follows from (1).

(4) follows from (3) by looking at $A/\mathfrak{p}$ and $\mathfrak{q}/\mathfrak{p}$ and using Lemma 54.

(5) follows from (3) and Lemma 51.

□

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 $A = k[x_1, \ldots, x_d]$ 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

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

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 66.

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 $x_n^{e-1}x_nM = 0$. 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. □

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 65. 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. □

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

Class 11

Definition 22. Let A be a ring, $I \subset A$ an ideal, M an A-module. Then we define the **completion of** M to be

$$\hat{M} = \varprojlim M/I^n M = \{(x_1, x_2, \dots) \in \prod M/I^n M | x_{n+1} = x_n \mod I^n M\}.$$

There is a canonical map $M \to \hat{M}$ that takes $x \mapsto (x, x, x, \dots)$.

Definition 23. We say that M is **I-adically complete** if $M \to \hat{M}$ is an isomorphism. Note that included is the condition $\cap_n I^n M = (0)$.

Lemma. *If I is finitely-generated then $\hat{M}$ is I-adically complete and moreover $I^n \hat{M} = \ker(\hat{M} \to M/I^n M)$.*

Lemma. *If A is Noetherian then $\hat{A}$ is Noetherian.*

Proof. Say $I = (f_1, \dots, f_r)$ then the map $A[[x_1, \dots, x_{r-1}]] \to \hat{A}$ that takes $\sum a_I x^I \mapsto \sum A_I f^I$ is surjective. So this lemma follows from the fact that $A[x_1, \dots, x_r]]$ is Noetherian. □

Lemma. *If $(A, \mathfrak{m})$ is local and Noetherian then the completion $\hat{A}$ of A with respect to $\mathfrak{m}$ is a Noetherian local ring with maximal ideal $\hat{m} = m\hat{A}$ such that $gr_{\hat{\mathfrak{m}}} \cong gr_{\mathfrak{m}} A$ and $\dim A = \dim \hat{A}$. This can be used to reduce problems to the complete local case.*

Theorem (Cohen Structure Theorem for characteristic 0)**.** *A complete Noetherian local ring A containing a field of characteristic zero is isomorphic to $k[[x_1, \dots, x_n]]/I$ for some field $k = A/\mathfrak{m}$.*

Lemma 67 (Artin-Rees Lemma)**.** *Let A be a Noetherian ring. Let $I \subset A$ be an ideal. Let $N \subset M$ be A-modules with M finite. Then there exists $c \geq 0$ such that*

$$I^n M \cap N = I^{n-c}(I^c M \cap N)$$

for all $n \geq c$.

Proof. Consider $B = A \oplus I \oplus I^2 \oplus \dots$ (the Rees algebra). This is a finitely-generated A-algebra and hence is Noetherian. Consider $P = M \oplus IM \oplus I^2 M \oplus \dots$ By similar considerations, P is a finite B-module, hence Noetherian (a.c.c. for submodules). Hence the B-submodule $N \oplus IM \cap N \oplus I^2 M \cap N \oplus \dots$ is a finitely-generated submodule. Thus there exist $r \geq 0$, $c_1, \dots, c_r \geq 0$ and $x_i \in I^{c_i} M \cap N$ such that $N \oplus IM \cap N \oplus I^2 M \cap N \oplus \dots = \sum B x_i$. Take $n \geq c = \max(c_i)$. Then

$$I^n M \cap N = \left(\sum B x_i\right)_n = \sum I^{n-c_i} x_i \subseteq \sum I^{n-c_i}(I^{c_i} M \cap N) \subseteq I^{n-c}(I^c M \cap N).$$

Hence we've proved the $\subseteq$ inclusion. The reverse inclusion is trivial. □

Let us investigate some of the consequences of this lemma. First note that in a Noetherian local ring $(A, \mathfrak{m})$ we have $\cap \mathfrak{m}^n = (0)$. We can prove this by setting $M = A$ and $N = \cap \mathfrak{m}^n$ and hence $N = \mathfrak{m}^n \cap N = \mathfrak{m}^{n-c}(\mathfrak{m}^c \cap N) = \mathfrak{m}^{n-c} N$, which by Nakayama's lemma implies that $N = 0$.

Moreover, if A is Noetherian, I an ideal, then the functor $M \to \hat{M}$ is exact on the category of finite modules.

Finally, note that $(A, \mathfrak{m})$ Noetherian local implies that $A \to \hat{A}$ is flat.

Definition 24. Let $k \subset K$ be fields. A **discrete valuation** on K/k is a surjective map $v : K^\times \to \mathbb{Z}$ such that:

(i) $v(c) = 0$ for all $c \in k^\times$;

(ii) $v(xy) = v(x) + v(y)$ for all $x, y \in K^\times$;

(iii) $v(x + y) \geq \min(v(x), v(y))$.

Lemma. *If $v(x) \neq v(y)$ then $v(x + y) = \min(v(x), v(y))$.*

Proof. Assume $v(y) > v(x)$. Then $v(y) = v(-y)$ because $-1 \in k$. Then $v(x) = v(x + y - y) \geq \min(v(x + y), v(y))$. □

Example 10. Let $K = k(t)$. Then let $v(f)$ be the order of vanishing of f at $t = 0$. Then we see that $v(t/(1 + t)) = 1$ and $v((1 + t)/(t^2 + t^3)) = -2$.

Now assume that k is algebraically closed, i.e. $\bar{k} = k$. What are all the discrete valuations on $k(t)/k$? Let us proceed by cases.

In the first case, suppose that $v(f) < 0$ for some $f \in k[t]$. Then it's clear that f is non-constant and that we can add a constant to f without changing $v(f)$ (by the lemma). Hence we may assume that $f = tg$ for some $g \in h[t]$. Then either $v(t) < 0$ or $v(g) < 0$. By induction we find that v of some linear polynomial must be less than 0. Suppose $v(at+b) = -m$. Then $v(t+b/a) = -m$

and $v(t+\lambda) = -m$ for all $\lambda \in k$. This shows that $v(a_n t^n + \ldots + a_0) = -nm$, because $k = \bar{k}$. We conclude that $m = 1$ because v is surjective. So

$$v\left(\frac{at^n + \ldots}{bt^l + \ldots}\right) = l - n,$$

which gives us the order of vanishing at infinity.

For the other case, where $v(f) \geq 0$ for all $f \in k[t]$. In this case $\mathfrak{m} = \{f \in k[t] | v(f) > 0\}$, is an ideal, prime, not the zero ideal, and hence maximal via $k[t]$ a PID. Hence $\mathfrak{m}$ is a maximal ideal, i.e. $(t-\alpha)$ for some α. $v(t-a) = m > 0$. Then $v(f)$ is m times the order of vanishing of f at $t-\alpha$. Because v is surjective, we get $m = 1$ and $v(f)$ is the order of vanishing at $t = \alpha$.

Definition 25. The **projective line** $\mathbb{P}^1_k$ over $k = \bar{k}$ is the set of valuations on $k(t)/k$. We define its topology by closed sets being finite subsets of $\mathbf{P}^1_k$ and $\varnothing$ and $\mathbb{P}^1_k$. The **regular functions** given $U \subset \mathbb{P}^1_k$ open are $\mathcal{O}(U) = \{f \in k(t) | v(f) \geq 0 \forall v \in U\}$.

For example, if $U = \mathbb{P}^1_k \setminus \{\infty\}$ then $\mathcal{O}(U) = k[t]$.

Class 12 - Algebraic Curves

Throughout, let $k = \bar{k}$ be our algebraically closed ground field. Let K be a finitely-generated field extension of k with $\operatorname{trdeg}_k K = 1$. Somehow we want to think of K as a function field of an algebraic curve. We will follow van der Waerden's Algebra Vol. II, chapter 19.

We will denote by C the set of discrete valuations of K/k (and think about it as the set of points of K/k. For $v \in C$ we set

$$\mathcal{O}_v = \{f \in K \mid v(f) \geq 0\}$$
$$\mathfrak{m}_v = \{f \in K \mid v(f) > 0\}.$$

Lemma 68. *For a discrete valuation v on a field K, $\mathcal{O}_v$ is a local domain with a maximal ideal $\mathfrak{m}_v$. If $z \in \mathfrak{m}_v$ has $v(z) = 1$ (such z exist by surjectivity of valuations) then $\mathfrak{m}_v = (z)$ and every ideal in $\mathcal{O}_v$ is of the form $(z^n) = \mathfrak{m}_v^n$ for some $n \geq 0$. Such a ring is called a **discrete valuation ring**.*

Proof. If $f \in \mathfrak{m}_v$ then $v(f) \geq 1$ so $v(f/z) \geq 0$ so $f = (f/z)z$ as $f/z \in \mathcal{O}_v$, which proves the claim. □

Lemma 69. *If K/k is finitely-generated of transcendence degree 1 and $v \in C$ then $\kappa_v = \mathcal{O}_v/\mathfrak{m}_v$ is equal to k.*

Proof. Pick $z \in K$ with $v(z) = 1$. Then $z \notin k$ so z is transcendental over k. Hence $n = [K : k(z)] < \infty$. Say $[\kappa_v : k] > 1 \implies [\kappa_v : k] = \infty$. This implies that there exist $u_1, \ldots, u_n \in \mathcal{O}_v$ such that $\bar{u}_1, \ldots, \bar{u}_{n+1} \in \kappa_v$ are k-linearly independent:

$$\sum_i a_i u_i = 0$$

for some $a_i \in k(z)$ not all zero. Clearing denominators, we may assume that $a_i \in k[t]$ and not all in (z). But then we obtain

$$\sum_i \bar{a}_i \bar{u}_i = 0,$$

which is a non-trivial relation in κ_v, which is a contradiction. $\square$

Remark. Now we know that $\mathcal{O}_v$ contains k, has residue field k, and has a **uniformizer** z i.e. $\mathfrak{m}_v = (z)$. Then it follows that $\hat{\mathcal{O}}_v = \varprojlim \mathcal{O}_v/\mathfrak{m}_v^n \cong k[[z]]$. A special case is where $K = k(z)$, $v = \mathrm{ord}_{z=0}$. Then $\mathcal{O}_v = k[z]_{(z)}$ and $\hat{\mathcal{O}}_v = k[[z]]$ in which we see $1/(1+z) \mapsto 1 - z + z^2 - z^3 + \ldots$.

Lemma 70. *Let $v_1, \ldots, v_n$ be pairwise distinct discrete valuations on a field K. Then there exists an $f \in K$ such that $v_1(f) > 0$ and $v_i(f) < 0$ for $i = 2, \ldots n$.*

Proof. If $n = 1$, this is trivial. Suppose $n = 2$ and the statement does not hold, i.e. $v_1(f) > 0$ and $v_2(f) \geq 0$. Pick $z \in K$ with $v_1(z) > 0$. Then for any $f \in K$ we have $v_1(f^a z^b) = av_1(f) + bv_1(z)$ and $v_2(f^a z^b) = av_2(f) + bv_2(z)$. This implies that $v_1(f) > -bv_1(z)/a$ and $v_2(f) \geq -bv_2(f)/a$. Thinking a little bit, we can conclude that $v_2(f) \geq v_1(f)\frac{v_2(z)}{v_1(z)}$. Similarly for f^{-1},

$$-v_2(f) = v_2(f^{-1}) \geq v_1(f^{-1})\frac{v_2(z)}{v_1(z)} = -v_1(f)\frac{v_2(z)}{v_1(z)}.$$

By surjectivity of v_1, v_2 we find that the fraction above must be 1, and hence $v_1 = v_2$.

Now consider $n > 2$. Pick $f \in K$ such that $v_1(f) > 0$ and $v_i(f) < 0$ for $i = 2, \ldots, n-1$ (by induction). If $v_n(f) < 0$ then we are done. If not, pick $g \in K$ such that $f_1(g) > 0$ and $v_r(g) < 0$. Then $h_r = g(1 + f^r)$, and for $r \gg 0$ we get $v_1(h_r) = v_1(g)$ because $f^r \in \mathfrak{m}_v$ and $1 + f^r$ is thus a unit. Now, for $2 \geq i \leq n-1$, note that $v_i(h_r) = v_i(g) + v_i(1 + f^r) = v_i(g) + rv_i(f)$ which goes to $-\infty$ as $r \to \infty$. Finally, we see that $v_n(h_r) = v)n(g) + v_n(1 + f^r) < 0$. We know that $v_n(f) \geq 0$. If $v_n(f) \geq 0$ then $1 + f^r$ os a unit and $v(1 + f^r) = 0$. If $v_n(f) = 0$ then $v_n(1 + f^r) > 0$ only if f^r maps to -1 in κ_{v_n}. We are done as there is an infinite sequence of r such that $f^r = -1$ (except possibly if the char $k = 2$, which we leave as an exercise). $\square$

Definition 26. Let $v_1, \ldots, v_n$ be pairwise distinct discrete valuations on a field K. Let $f_1, \ldots, f_n \in K$. An **approximation to order** N of $f_1, \ldots, f_n$ at $v_1, \ldots, v_n$ is an $f \in K$ such that $v_i(f - f_i) \geq N$ for $i = 1, \ldots, n$.

Theorem 71. *Approximations exist.*

Proof. Pick $f \in K$ as in Lemma 70. Then

$$h_M = \frac{1}{1 + f^M}$$

for $M \gg 0$. This satisfies $h_M \in \mathcal{O}_v$, $h_M \equiv 1 \mod \mathfrak{m}_{v_1}^M$ and that $h_M \in \mathfrak{m}_{v_i}^M$ for $i = 2, \ldots, n$ (compute $v_i(h_M)$). So we see that $h_M \cdot f_1$ approximates $f_1, 0, \ldots, 0$ up to order N if $M \gg N$. But since we can approximate the sum of vectors as well, we are done. □

Lemma 72. *Let $K \subset L$ be a finite extension of fields. Let $w : L^\times \to \mathbb{Z}$ be a discrete valuation. Then $w|_{K^\times} = ev$ for some discrete valuation v on K and integer $e \geq 1$.*

Proof. It is clear that $w|_{K^\times}$ satisfies the properties of a discrete valuation except for possibly being surjective. So $e = [\mathbb{Z} : w(K^\times)]$ works provided that $w(K^\times) \neq 0$. But if $w(K^\times) = 0$ then $K \subset \mathcal{O}_w \subset L$, which by the previous lemma $\mathcal{O}_w$ is a field, which is a contradiction. □

Definition 27. In the situation of Lemma 72 we say that w **extends** v.

Lemma 73. *If $K \subset L$ is finite and $v : K^\times \to \mathbb{Z}$ given then there are at most a finite number of $w : L^\times \to \mathbb{Z}$ such that $w|_{K^\times} = e_N \cdot v$.*

Proof. Say we have pairwise distinct $w_1, \ldots, w_r$ on L extending v. Pick (by a previous lemma) $f_i \in L$ such that $w_i(f_i) > 0$ and $w_j(f_i) < 0$ for $j \neq i$. We'll show that $f_1^{-1} \cdots f_n^{-1}$ are linearly independent, which suffices. Suppose $\sum_i a_i f_i^{-1} = 0$ for some $a_1, \ldots, a_r \in K$. Clearing denominators, we may assume that $a_i \in \mathcal{O}_v$ and that $a_{i_0} \notin \mathfrak{m}_r$ for some i_0. Then

$$w_{i_0}\left(\sum_i a_i f_i^{-1}\right) \geq \min w_{i_0}(a_i f_i^{-1}) \geq \min e_{i_0} v(a_i) + w_{i_0}(f_i^{-1}).$$

But the first term is greater than or equal to zero (equal if $i = j$) and the second is always greater than equal to zero (equal if $i = i_0$). Hence this could not have been zero. So $\sum_i a_i f_i^{-1} \neq 0$. □

Class 13

Definition 28. $v \in C$ is a **zero** (respectively **pole**) of $f \in K^\times$ if $v(f) > 0$, respectively $v(f) < 0$. (The integers are called the order of the zero, and (-1)·the order of the pole.)

Lemma 74. *Let K be a finitely generated extension of k with transcendence degree 1. If $f \in K^\times$, then f has a finite number of zeros and poles.*

Proof. We look at the map $k(t) \to K$ that takes $t \to f$. Then $n = [K : k(t)] < \infty$. If v is a zero of f then v is an extension to K of the valuation $\mathrm{ord}_{t=0}$ on $k(t)$. By Lemma 73, there exist finitely many of these. □

Lemma 75. *Let $k \subset L$ be a finite extension of (arbitrary) fields. Let $v : K^\times \to \mathbb{Z}$ be a discrete valuation. Then there exists $w : L^\times \to \mathbb{Z}$ extending v.*

Last lecture we proved the finiteness of such extensions and this is the existence statement. We will not prove this fact yet; we will do so later using the technology of divisors. There are two approaches we could use to prove it even now, but it would be quite hard.

1. Look at the completion $\hat{K}$ of K. Then look at $\hat{L} = L \otimes_K \hat{K}$. This is not necessarily a field. Then choose a quotient $\hat{L} \twoheadrightarrow L'$ which is a field. Then we can take $v \circ \mathrm{Nm}_{L'/\hat{K}}$ to be the extension.

2. $\mathcal{O}_v \subset K$ can be extended to a valuation ring $\mathcal{O}_v \subset \mathcal{O}_w \subset L$ with $\mathrm{f.f.}(\mathcal{O}_w) = L$. Then we show that $\mathcal{O}_w$ is a discrete valuation ring.

Lemma 76. *Let K/k be finitely generated with transcendence degree 1, then any $f \in K, f \notin k$ (i.e. nonconstant) has a pole.*

Proof. Look at $k(t) \to K$ that takes $t \to f$, then $v = \mathrm{ord}_\infty \in P^1_k$ has an extension w to K. $w(f) < 0$ because $\mathrm{ord}_\infty(t) < 0$. □

Example 11. The poles of $\frac{t^2}{t+1}$ are $-1, \infty$. Its zeros are 0, counted twice.

Let us now fix $k \subset K$ a function field over a curve $C = \{\text{discrete valuations on } K/k\}$.

Definition 29. A **divisor** is a formal sum $D = \sum_{v \in C} n_v v$ with $n_v \in \mathbb{Z}$ almost all zero. D is said to be **effective** iff $n_v \geq 0$ for all $v \in C$. Moreover, we say that $D_1 \geq D_2$ iff $n_{1v} \geq n_{2v}$ for all $v \in C$, i.e. $D_1 - D_2$ is effective. For $f \in K^\times$, the **principal divisor** associated to f is $(f) = \sum_{v \in C} v(f)v$. This is well-defined by Lemma 74. Observe that $(fg) = (f) + (g)$. Next we define the **zero divisor** of f to be $(f)_0 = \sum_{v(f)>0} v(f)v$ and the **pole divisor** of f to be $(f)_\infty = \sum_{v(f)<0} v(f)v$. Observe that $(f) = (f)_0 + (f)_\infty$. If D is a divisor $D = \sum n_v v$ then its **degree** is $\deg(D) = \sum n_v \in \mathbb{Z}$.

Given a divisor $D = \sum n_v v$ we set

$$L(D) = \{f \in K^\times \mid v(f) \geq -n_v \forall n_v \in C\} \cup \{0\}.$$

This is a k-vector space. Let $\ell(D) = \dim_k L(D)$.

Lemma 77. *If $D_1 \geq D_2$ then $L(D_2) \subset L(D_1)$ has codimension at most* $\deg(D_1) - \deg(D_2)$.

Proof. It suffices to prove this for $D_2 = D_1 - v$ for some $v \in C$, and then the result follows by induction. We have the exact sequence of vector spaces:

$$0 \to L(D_2) \to L(D_1) \to \pi^{-n}\mathcal{O}_v/\pi^{-(n-1)}\mathcal{O}_v$$

where $\pi \in \mathcal{O}_v$ is the uniformizer and n is the coefficient of v in D_1. We are done, because $\pi^{-n}\mathcal{O}_v/\pi^{-(n-1)}\mathcal{O}_v$ is a 1-dimensional k-vector space. □

Lemma 78. *Say $D = D_1 - D_2$ with $D_1, D_2 \geq 0$. Then $l(D) \leq \deg(D_1) + 1$.*

Proof. Observe that $L(D) \subset L(D_1)$. Observe also that $L(0) = k$, because by Lemma 76 any nonconstant function has a pole. So the statement holds for the trivial divisor. Now we can induct: add points and use Lemma 77. For example $L(v) \supset L(0)$ of codimension ≤ 1. So either $l(v) = 0$ or $l(v) = 1$. Then $L(v_1 + v_2) \supset L(v_1)$ has codimension ≤ 1, etc. $\square$

Corollary. $l(D) \leq \infty$.

Definition 30. D_1, D_2 are called **rationally equivalent** (notation $D_1 \sim_{\text{rat}} D_2$) if there exists $f \in K^\times$ such that $D_1 = D_2 + (f)$. This is obviously an equivalence relation.

Lemma 79. *If $D_1 \sim_{rat} D_2$, then $l(D_1) = l(D_2)$.*

Proof. We can pass from $L(D_1)$ to $L(D_2)$ and viceversa by multiplying functions by f^{-1} or f respectively. $\square$

Example 12. If $K = k(t)$, then the degree of a principal divisor is 0. Namely every nonzero rational function looks like:

$$f = c \prod_{\lambda \in k} (t - \lambda)^{n_\lambda}$$

Such that almost all $n_\lambda = 0$, and $c \in k^\times$. Then:

$$(f) = \sum_\lambda n_\lambda \operatorname{ord}_{t=\lambda} - \left(\sum_\lambda n_\lambda \right) \cdot \infty$$

Then $\deg(f) = \sum_\lambda n_\lambda - \sum_\lambda n_\lambda = 0$. Caution: in the equation above, the symbol ∞ represents the valuation which is the point at infinity on P^1_K. Clearly, any divisor D is rationally equivalent to $n \cdot \infty$ for some n. (Substract some appropriately chosen (f) to cancel out the other terms.) Then this n is the degree of D. Then we can compute $l(D)$, since:

$$\begin{aligned} L(n \cdot \infty) &= \{f \in k(t) : \operatorname{ord}_{t=\lambda}(f) \geq 0, \operatorname{ord}_{t=\infty}(f) \geq -n\} \\ &= \{f \in k[t] : \operatorname{ord}_{t=\infty}(f) \geq -n\} \\ &= \{f \in k[t] : \deg(f) \leq n\} \end{aligned}$$

This has dimension $n + 1$. Hence the bound in Lemma 78 is optimal.

Lecture 14

Proposition 80. *Let K/k be a function field and $f \in K$ be nonconstant. Set $n = [K : k(t)]$. Then $n = \deg(f)_0 = \deg(f)_\infty$.*

Proof. **STEP 1**. $n \geq \deg(f)_0$. To show this, say:

$$(f)_0 = n_1 v_1 + \ldots n_r v_r \qquad n_i > 0$$

For $1 \leq i \leq r$ and $1 \leq j \leq n_r$ pick $z_{ij} \in K$ such that z_{ij} has order of vanishing j at v_i and it has order of vanishing $> n_i$ at all other points. This is possible by Thm 71. We claim that z_{ij} are linearly independent over $k(f)$. If $\sum a_{ij} z_{ij} = 0$ we can clear denominators and get $a_{ij} \in k[f]$, with not all a_{ij} zero at $f = 0$. Say $a_{i_0 j_0} \neq 0$, with j_0 minimal. Then we see that $v_{i_0}(\sum a_{ij} z_{ij}) = j_0$. This is because, if $a \in k[f]$ is zero at $f = 0$ then $v_{i_0}(a) \geq n_{i_0}$ because $v_{i_0}(f) = n_{i_0}$. Therefore $\sum a_{ij} z_{ij} \neq 0$.

STEP 2. $n \geq \deg(f)_\infty$. To see this, apply step 1 to f^{-1}.

STEP 3. $n \leq \deg(f)_\infty$. To prove this, write $K = \oplus_{i=1}^n k(t) \cdot u_i$ for some $u_1, \ldots, u_n \in K$. Suppose v is a valuation of K lying over $\mathrm{ord}_{f=\lambda}, \lambda \in k$ such that $v(u_i) < 0$. Then after multiplying u_i by $(f-\lambda)^{n_{u_i}}$ the valuation v is no longer a pole of u_i, and we haven't introduced any new poles for u_i, except perhaps poles of f. After doing this finitely many times, we may assume that poles of $u_i \subset$ poles of f. This implies that $\exists m_i \geq 0$ such that $(u_i)_\infty \leq (m_i+1)(f)_\infty$. Choose $m \geq \max\{m_i\}$. Then $u_i, fu_i, f^2 u_i, \ldots f^{m-m_i-1} u_i \in L\big(m(f)_\infty\big)$. Hence $l\big(m(f)_\infty\big) \geq \sum_{i=1}^n (m - m_i) = nm - \sum_{m_i}$. We are done, because by Lemma 78 $l\big(m(f)_\infty\big) \leq m \deg\big((f)_\infty\big) + 1$. ☐

Corollary 81.

1. *The degree of a principal divisor is 0.*

how do you do formatting here?

2. *If $D \sim_{rat} D'$ then* $\deg(D) = \deg(D')$.

Lemma 82. *Let D be a divisor, TFAE:*

1. *$l(D) > 0$;*
2. *D is rationally equivalent to an effective divisor.*

Proof. For $f \in K^\times$ we have $D + (f) \geq 0 \Leftrightarrow f \in L(D)$. ☐

Proposition 83. *There exists a constant c such that* $\deg(D) - l(D) \leq c$ *for all D.*

Proof. Let $f \in K$ be noncosntant, write $K = \oplus k(f) u_i$ with $(u_i)_\infty \leq (m_i + 1)(f)_\infty$ as in the proof of proposition 80. We saw that:

$$\deg(m(f)_\infty) - l(m(f)_\infty) \leq (\sum m_i) + 100$$

Hence the proposition holds for $D = m(f)_\infty$ with $c = (\sum m_i) + 100$. Now let D be arbitrary. By lemma 77 it suffices to find $D' \geq D$ such that $c \geq \deg(D') - l(D') \geq \deg(D) - l(D)$. We may also replace D by $D + (f)$, as this doesn't change $\deg(D)$ or $l(D)$. By the same argument as in the proof of prop 80, D is rationally equivalent to a divisor D' such that the support of the positive part of D' is included in the poles of f. Then $D' \leq m(f)_\infty$ for some $m >> 0$. $\square$

Definition 31. The **genus** of K/k is the smallest integer g such that $\deg(D) - l(D) \leq g - 1$ for all divisors D.

Remark. $g \geq 0$ because for $D = 0$ we have $l(D) = 1$.

If we define the **speciality index** $h^1(D)$ by the formula:

$$l(D) - h^1(D) = \deg(D) + 1 - g$$

Then the **Riemann-Roch theorem** gives a meaning to $h^1(D)$. We have seen in the proof of proposition 83 that given any nonconstant $f \in K$ then the sequence of integers $\deg(m(f)_\infty) - l(m(f)_\infty)$ is nondecreasing and has an upper bound. This upper bound is $g - 1$.

Remark. In proposition 83 we have proved asymptotic Riemann-Roch.

Example 13. The genus of P^1_k. We know that any divisor D is rationally equivalent to $d\infty$ for some integer $d = \deg(D)$. Also:

$$L(\infty) = \{f \in k[t] : \deg(f) \leq d\}$$

So $l(d\infty) = d + 1$ if $d > 0$, and 0 otherwise. Then:

$$\deg(d\infty) - l(d\infty) = \begin{cases} -1 \text{ if } d \geq 0 \\ d \text{ if } d < 0 \end{cases}$$

Example 14. $K = \text{f.f.}(\mathbb{C}[x, y]/(y^2 - x^3 - x))$. What Riemann would say is that this is the surface corresponding to $\sqrt{x^3 + x}$. We could try to compute $L(m\infty')$, where we have that $2 \cdot \infty' = (x)_\infty$, where x is regarded as an element of $K = \mathbb{C}[x, y]$. Note also that elements of K are of the form $a + by$, with $a, b \in \mathbb{C}(x)$.

Class 15

Let K/k be finitely generated of transcendence degree 1. For $v \in C$ an algebraic curve we define K_v to be the v-adic topology $f.f.(\hat{O}_v)$, i.e. the set of all Cauchy sequences (x_n) where $v(x_n - x_m) \to \infty$ as $n, m \to \infty$ (modulo null sequences).

Lemma 84. *K_v is a field. In fact, if $z \in K$ is a uniformizer at v then $\hat{O}_v = k[[z]]$ and $K_v = k((z))$, the field of Laurent series in z over k.*

Proof. Omitted. The idea is that there is a map $k[z] \to \mathcal{O}_v$ which induces an isomorphism on completions $k[[z]] \to \hat{\mathcal{O}}_v$. $\square$

Remark. In the literature, one often finds written $\mathcal{O}_v$ for $\hat{\mathcal{O}}_v$.

Definition 32. The **ring of adeles** is

$$\mathbb{A}_k = \{(x_v) \in \prod_{v \in C} K_v \mid \text{for almost all } v, x_v \in \hat{\mathcal{O}}_v\}$$

Lemma 85. *Let k be a field. Let $L = k((t))$. Then $\mathrm{Hom}_{cts}(L, k)$, the set of $\lambda : L \to k$ k-linear such that $\lambda|_{t^n k[[t]]} \equiv 0$ for some n, is a one-dimensional vector space over L.*

Proof. Consider the map λ_0 given by $f \to \mathrm{Res}_{t=0} \frac{f\,dt}{t}$ given by $\sum_i a_i t^i \mapsto a_0$. We claim that any λ is a multiple of λ_0. Namely, say $\lambda(t^m) = b_m \in k$ for $m \in \mathbb{Z}$. Then $b_m = 0$ for $m \gg 0$. So we can introduce $g = \sum b_m t^{-m} \in L$. We then claim that $\lambda(f) = \lambda_0(gf)$. It suffices to check this for t^i (due to the basis of $L/t^n k[[t]]$). Then $\lambda(t^i) = b_i$ and $\lambda_0(t^i g) = \mathrm{Res}_{t=0} \left(\sum t^{i-m} b_m \frac{dt}{t}\right) = b_i$. □

Definition 33. The module of **covectors** is the module

$$\mathbb{A}_k^* = \{\lambda = (\lambda_v) \in \prod_v \mathrm{Hom}_{cts}(K_v, k) \mid \text{for almost all } v : \lambda_v|_{\hat{\mathcal{O}}_v} = 0\}.$$

Recall now that we have defined a genus g such that

$$\ell(D) - h^1(D) = \deg(D) + 1 - g$$

for some $h^1(D) \geq 0$.

Lemma 86. *If $D' \geq D$ then $h^1(D') \leq h^1(D)$.*

Proof. This is a reformulation of Lemma 77. □

Lemma 87. *For every D there exists a D' with $D' \geq D$ and $h^1(D') = 0$.*

Proof. By the construction of g, there exists a D_0 with $h^1(D_0) = 0$. Choose $D' \geq D_0$ and $D' \geq D$. Apply Lemma 86. □

Now note that there exists a canonical map $K \to \mathbb{A}_k$ given by $f \mapsto (f, f, f, \ldots)$.

Definition 34. A **Weil differential** is a covector $\lambda \in \mathbb{A}_k^*$ such that $\lambda(f) = 0$ for all $f \in K$.

Definition 35. Given $\lambda = (\lambda_n) \in \mathbb{A}_k^*$ and D a divisor, we say $\lambda \geq D$ if and only if $\lambda_v|_{\pi_v^{-n_v}\mathcal{O}_v} = 0$ for all v.

Theorem 88. *$h^1(D)$ is precisely the dimension of the k-vector space of Weil differentials λ such that $\lambda \geq D$.*

Proof. Pick any $D' = \sum_v n'_v v \geq D = \sum_v n_v v$ with $h^1(D') = 0$ (by Lemma 86). Then we have the short exact sequence

$$0 \longrightarrow \frac{L(D')}{L(D)} \longrightarrow \prod_v \frac{\pi_v^{-n'_v}\mathcal{O}_v}{\pi_v^{-n_v}\mathcal{O}_v} \longrightarrow \text{v.s. of dim } h^1(D) \longrightarrow 0.$$

Note that the dimensions work out by our formula for g and that in fact

$$\frac{\pi_v^{-n'_v}\mathcal{O}_v}{\pi_v^{-n_v}\mathcal{O}_v} = \frac{\pi_v^{-n'_v}\hat{\mathcal{O}}_v}{\pi_v^{-n_v}\hat{\mathcal{O}}_v}.$$

We can put all these sequences together for varying $D' \geq D$ with $h^1(D') = 0$:

$$0 \longrightarrow \frac{K}{L(D)} \longrightarrow \prod_v \frac{K_v}{\pi_v^{-n_v}\mathcal{O}_v} \longrightarrow \text{fixed v.s. of dim } h^1(D) \longrightarrow 0.$$

□

Corollary 89. *The k-vector space of regular Weil differentials, i.e. $\lambda \geq 0$, has dimension g.*

Theorem 90. *The collection of all Weil differentials is a one-dimensional K-vector space.*

Proof. It is already clear that the dimension is nonzero. Suppose now that λ_1, λ_2 are K-linearly independent Weil differentials. Choose D such that $\lambda_i \geq D$. Pick a divisor E with huge degree. For $f_1, f_2 \in L(E)$ we get that $\lambda = f_1\lambda_1 + f_2\lambda_2 \geq D-E$ (this is an easy local computation). Thus, $h^1(D-E) \geq 2\ell(E)$ by Theorem 88, which by the formula for g is greater than or equal to $2(\deg E+1-g)$. On the other hand, $\ell(D-E)-h^1(D-E) = \deg D - \deg E + 1 - g$. Putting these together we find that $\ell(D-E) \geq \deg(E) + \text{const} \cdot (\text{something depending on } D, g)$. This is a contradiction. □

Now pick a (fixed) non-zero differential λ_0. Set K_c to be the largest divisor such that $\lambda_0 \geq K_c$ (we leave it as an exercise to show that such a thing exists). In other words, if $K_c = \sum m_v v$ then $\lambda_{0,v}|_{\pi_v^{-m_v}\hat{\mathcal{O}}_v} = 0$ but $\lambda_{0,v}|_{\pi_v^{-m_v-1}\hat{\mathcal{O}}_v} \neq 0$.

Lemma 91. *The rational equivalence class of K_c is well-defined.*

Proof. Let λ be another non-zero differential. Then by Theorem 90 we see that $\lambda = f \cdot \lambda_0$ and K_c is changed by adding (f). □

Definition 36. The divisor of K_c is called the **canonical divisor of** C.

Theorem 92 (Riemann-Roch)**.** *For a divisor D, $\ell(D) - \ell(K_c - D) = \deg D + 1 - g$.*

Proof. The result follows easily by Theorems 88 and 90:

$$\begin{aligned}
\ell(K_c - D) &= \dim\{f \mid (f) + K_c - D \geq 0\} \\
&= \dim\{f \mid (f) + K_c \geq D\} \\
&= \dim\{f \mid f\lambda_0 \geq D\} \\
&= \dim\{\text{Weil differentials } \lambda \mid \lambda \geq D\} \\
&= h^1(D)
\end{aligned}$$

□

Class 16

Modules of differentials

Let $A \to B$ be a ring map. Let M be a B-module.

Definition 37. An A**-derivation** $D : B \to M$ is an A-linear map satisfying the Leibniz rule:

$$D(b_1 b_2) = b_1 D(b_2) + b_2 D(b_1).$$

It is clear that $D(1) = 0$.

Example 15. Consider $A \to B = A[x_1, \ldots, x_n]$ and $D = (\partial_{x_1}, \ldots, \partial_{x_n}) : B \to \oplus_{i=1}^n B$.

Lemma 93. *There exists a universal A-derivation $d : B \to \Omega_{B/A}$, i.e. for any A-derivation $D : B \to M$ there exists a unique B-linear map $\theta : \Omega_{B/A} \to M$ such that $D = \theta \circ d$.*

Proof. Let $\Omega_{B/A}$ be the free B-module on the symbols $d(b)$ for $b \in B$ and then quotient out by the B-submodule generated by $d(a)$ for $a \in A$, $d(b_1 + b_2) - d(b_1) - d(b_2)$ for $b_1, b_2 \in B$, and by $d(b_1 b_2) - b_1 d(b_2) - b_2 d(b_1)$ for $b_1, b_2 \in B$. Now it's clear that our map θ from $\Omega_{B/A}$ to M should take db to $D(b)$. $\square$

Example 16. If $B = A[x_1, \ldots, x_n]$ then $\Omega_{B/A} = \oplus_{i=1}^n A[x_1, \ldots, x_n] dx_i$. Then $d(f) = \sum_{i=1}^n \left(\frac{\partial f}{\partial x_i}\right) dx_i$.

Example 17. Suppose $P \in A[x, y]$ and $B = A[x, y]/(P)$. Then $\Omega_{B/A} = \operatorname{coker}(B \longrightarrow B dx \oplus B dy)$, where the map takes $1 \mapsto dP = \frac{\partial P}{\partial x} dx + \frac{\partial P}{\partial y} dy$.

Lemma 94. *If $S \subset B$ is a multiplicative subset, then $\Omega_{S^{-1}B/A} = S^{-1}\Omega_{B/A}$ (as $S^{-1}B$ modules).*

Proof. See, in the Stacks Project Tag 00RT. $\square$

Example 18. $\Omega_{k(t)/k} = k(t) dt$ because $\Omega_{k[t]/k} = k[t] dt$.

Lemma 95. *Let K/k be a finitely-generated field extension of transcendence degree 1, with k algebraically closed. Then $\Omega_{K/k}$ is a one-dimensional vector space over K.*

Proof. By field theory there exists

(a) an element $x \in K$ such that $K/k(x)$ is finite and separable;

(b) An element $y \in K$ such that K is generated by x, y over k (theorem of the primitive element).

Denote by B the domain $k[x,y]/(P)$. Let $P(x,y) \in k[x,y]$ be an irreducible polynomial such that $P(x,T)$ is $k(x)^\times$ multiple of the minimial polynomial for y over $k(x)$. Then $K = S^{-1}(k[x,y]/(P))$ whence $\Omega_{K/k} = S^{-1}\Omega_{(k[x,y]/(P))/k} = S^{-1}\left(\text{coker}\left(B \overset{(\frac{\partial P}{\partial x},\frac{\partial P}{\partial y})}{\to} Bdx \oplus Bdy\right)\right) = \text{coker}\left(K \overset{(\frac{\partial P}{\partial x},\frac{\partial P}{\partial y})}{\to} Kdx \oplus Kdy\right)$. By (a) above we see that $\frac{\partial P}{\partial y} \neq 0$ in K. Hence the map is not the zero map and the cokernel has dimension one. $\square$

Lemma 96 (Scholium). *If $x \in K$ and $K/k(x)$ is finite and separable then dx is a basis for $\Omega_{K/k}$.*

Now let us return to Weil differentials and the setup from previous classes. Let $\omega \in \Omega_{K/k}$ be nonzero. Then we will construct a covector $\lambda_\omega \in \mathbb{A}_K^*$ by setting $\lambda_\omega((f_v)) = \sum \text{Res}\,(f_v\omega)$. Let us investigate what this means. "As my five-year old likes to say: what the heck?"

Fix $v \in C$ and pick a uniformizer z_v. Then $K_v = k[[z_v]]$, canonically (by Lemma 84). There are maps

$$\Omega_{K/k} \xrightarrow{\text{functoriality}} \Omega_{k_v/k} \xrightarrow{\text{Taylor expansion}} k((z_v))dz_v \tag{1}$$

where the second map sense $\sum f_i dg_i \mapsto \sum \left(\frac{dg_i}{dz_v}\right) dz_v$. Note carefully that the Taylor expansion is not an isomorphism. This can be fixed by replacing $\Omega_{K_v/k}$ by $\Omega_{K_v/k,\text{cont}}$, i.e. continuous differentials. Then we set $\text{Res}_v(f_v\omega) = \text{Res}_{z_v=0}\left(\text{Taylor}_{z_v}(f_v\omega)\right)$.

Lemma 97. *The RHS is independent of choice of local uniformizer.*

Proof. Suppose $\eta \in \Omega_{K_v/k}$ and $h(z_v)dz_v = \text{Taylor}_{z_v}(\eta)$ and $\tilde{h}(\tilde{z}_v)d\tilde{z}_v = \text{Taylor}_{\tilde{z}_v}(\eta)$. Then $\tilde{z}_v = a_1 z_v + a_2 z_v^2 + \cdots$ with $a_1 \neq 0$. We are given that $h(z_v)dz_v = \tilde{h}(a_1 z_v + a_2 z_v^2 + \cdots)d(a_1 z_v + a_2 z_b^2 + \cdots)$. Then we see that $\tilde{h} = \sum b_j(\tilde{z}_v)^j$ is a Laurent series as it has finitely many negative terms and that $\text{Res}_{\tilde{z}_v=0}\left(\tilde{h}(\tilde{z}_v)d\tilde{z}_v\right) = b_{-1}$. It remains to show that the coefficient of z_v^{-1} in

$$\sum b_j(a_1 z_v + a_2 z_v^2 + \cdots)^j (a_1 + 2a_2 z_v + \cdots)$$

is equal to b_{-1}. Factoring, we find

$$\sum a_1^{j+1} b_j z_v^j \left(1 + \frac{a_2}{a_1} z_v + \cdots\right)^j \left(1 + \frac{2a_2}{a_1} z_v + \cdots\right).$$

We claim that the coefficient of z_v^{-1} is now b_{-1}. $\square$

Lemma 98. *For $\omega \in \Omega_{K/k}$ and $(f_v) \in \mathbb{A}_k$ we have $\text{Res}(f_v\omega) = 0$ for almost all v.*

Proof. Say $K = \text{Frac}k[x,y]/(P)\,()$ with $\frac{\partial P}{\partial y} \neq 0$ in K as before. Then $\omega = f dx$ for some $f \in K$. Let v be a discrete valuation of K/k centered on $k[x,y]/(P)$, i.e. $v(h) \geq 0$ for all $h \in k[x,y]/(P)$ and there are only a finite number of v which are not centered on $k[x,y]/(P)$. If v is not a pole or zero of f and v is also not a zero of $\partial P/\partial y$ then Let $(\alpha, \beta) \in k^2$ be coordinates of the point in $\{P = 0\} \subset k^2$ corresponding to v. Then

(a) $x - a$ is a uniformizer at v;

(b) $\omega = cd(x - \alpha)$ with c a unit in $\mathcal{O}_v^*$.

Hence $\text{Res}(f_v\omega) = 0$ if $f_v \in \hat{\mathcal{O}}_v$. □

How do we prove (a) and (b) above? Since (α, β) is a nonsingular point of $\{P = 0\}$ (as defined in the exercises) we have that

$$R = (k[x,y]/(P))_{(x-\alpha, y-\beta)}$$

is a regular local ring of dimension one and hence a discrete valuation ring. Since $R \subset \mathcal{O}_v$ is an inclusion of discrete valuation rings with same fraction field, we see that $R = \mathcal{O}_v$. So you can read off whether $x - \alpha$ is a uniformizer from the structure of R, i.e. show $x - \alpha \notin \mathfrak{m}_R^2$.

Consequently, we see that $\lambda_\omega : \mathbb{A}_k \to k$ given by $(f_v) \mapsto \sum_v \text{Res}_v(f_v\omega)$ is a covector. If $\omega \neq 0$ then $\lambda_\omega \neq 0$ (easy).

Theorem 99. *The covector λ_ω is a Weil differential and the assignment $\omega \mapsto \lambda_\omega$ is an isomorphism from $\Omega_{K/k}$ to the space of Weil differentials.*

Proof. It now suffices to show that if $f \in K$ then $\sum_{v \in C} \text{Res}_v(f_\omega) = 0$. See below. □

Theorem 100. *The sum of the residues of an element in $\Omega_{K/k}$ is zero.*

Example 19. Take $K = k(t)$ and $\omega = dt$. There is a pole of order 2 at infinity: $d(1/s) = -1/s^2 ds$. It's clear that Res_∞ is zero in this case. Let's instead try $\omega = dt/t$. We see that $d(1/s)/(1/s) = -ds/s$ and hence the residue at infinity is -1 which cancels out the residue of 1 at zero.

Let us now prove this theorem (for characteristic zero).

Proof. Let us split this into two cases. For this first, assume $K = k(t)$. In this case

$$\omega = f(t)dt = \sum$$

□ add here

Class 17

We resume the proof of Thm 100. We first recall the statement. Let K/k be a function field, and let $\omega \in \Omega_{K/k}$. Then $\sum_{v\in C} \operatorname{Res}_v(\omega) = 0$.

Proof. **Case I.** $K = k(t)$. In this case, $\omega = f(t)dt = \sum \frac{c_i dt}{(t-\alpha_i)^{e_i}}$. We actually only need to check when $\omega = \frac{dt}{(t-\alpha_i)^{e_i}}$, and we did this last time.

Case II. $K \supset k(t)$ separable and finite. Let $\omega = dt$. Then we claim that:

$$\sum_{w \text{ valuation of } K/k} \operatorname{Res}_w(f\omega) = \sum_{v \text{ valuation of } k(t)/k} \operatorname{Res}_v(\operatorname{Tr}_{K/k(t)}(f)\cdot\omega)$$

This claim follows from Lemma 101. Then we are done, since the RHS is 0 by Case I. □

Lemma 101. *Let $k((x)) \subset k((y))$ be a finite separable extension. For $f \in k((y))$ we have:*

$$\operatorname{Res}_{y=0}(\mathit{Taylor}_y(f dx)) = \operatorname{Res}_{x=0}(\mathit{Taylor}_x(\operatorname{Tr}_{k((y))/k((x))}(f)dx))$$

Proof. We prove this lemma for character 0. In this case, there exists a uniformizer $y' \in k((y))$ such that $x = (y')^e$ for some e. (Using the fact that $\overline{k((x))} = \cup_e k((x^{y_e}))$ if $k = \bar{k}$ has characteristic 0.) By Lemma 97, the LHS does not depend on the choice of uniformizer. We may replace y by y' and assume $y^e = x$. Then we get:

$$LHS = \operatorname{Res}_{y=0}(ef(y)y^{e-1}dy) = e(\text{coeff. of } y^{-e} \text{ in } f)$$

$$RHS = \operatorname{Res}_{x=0}(\sum_{i=0}^{e-1} f(\xi^i y)dx) = e(\text{coeff. of } y^{-e} \text{ in } f)$$

In the above equation ξ is a primitive e^{th} root of unity of k. The last equality follows since:

$$y^n \to \sum_{i=0}^{e-1} \xi^{in} y^n = \begin{cases} 0 \text{ if } & e \nmid n \\ ey^n \text{ if } e|n \end{cases}$$

□

Let us discuss a few applications. First note that the canonical divisor class equals the divisor class of a nonzero meromorphic differential form, i.e. if $\omega \in \Omega_{K/k}$ nonzero then

$$K_c \sim_{\text{rat}} \sum_{v\in C} (\operatorname{ord}_v \omega) v.$$

Note also that we can use this to show that $\deg K_c = 2g-2$. This is because $\ell(0) - \ell(K_c) = 1-g$ and $\ell(K_c) - \ell(0) = \deg K_c + 1 - g$. Hence $0 = \deg K_c + 2 - 2g$.

Furthermore $\ell(K_c) = g$ (number of regular differential forms on C). Finally, note that if $\deg K_c \geq 2g-1$ then $\ell(D) = \deg D + 1 - g$ simply because $\deg(K_c - D) < 0$ so $\ell(K_c - D) = 0$.

Lemma 102. *Let $S \subset C$ be a finite nonempty subset. Then,*

(i) $A = \cap_{v \in C, v \notin S} \mathcal{O}_v$ *is a normal domain with fraction field K of finite type over k*

(ii) $\dim A = 1$

(iii) Closed points of $\operatorname{Spec} A$ *are in one-to-one correspondence with points $C \setminus S$.*

Proof. A is a normal domain because it is the intersection of the normal domains $\mathcal{O}_v$. Once we show finite-type, A will be Noetherian of dimension one, so all of its local rings will be DVRs, i.e. points of A correspond to v. (Then ε more to finish the proof). Let us prove finite-type. Say $S = \{v_1, \ldots, v_n\}$. For each i we have

$$\ell(ev_i) = e + 1 - g, e \geq 2g - 1.$$

Hence we can pick $f_{i,j} \in L(jv_i) \setminus L((j-1)v_i)$ for $j = 2g, \ldots 4g - 1$. Note that $f_{i,j} \in A$. We claim that A is generated as a k-algebra by $f_{i,j}$ and $L((2g-1)(v_1 + \ldots + v_n))$. Namely, if $f \in A$, then

$$(f)_\infty = \sum_{i=1}^{n} e_i v_i, e_i \geq 0.$$

If $e_i \geq 2g$ for some i. Then expanding in a uniformizer at v_i, we see that $f' = f - c$ (some monomial $f_{i,j}$). Some $c \in k^*$ has a lower value of e_i. So f' has a lower degree of pde divisor. Continue until we reach $f \in L((2g-1)(\sum v_i))$. $\square$

Remark. Take C, K/k as above. Put cofinite topology on C, and for $U \subset C$ open, set $\mathcal{O}_v(U) = \cap_{v \in U} \mathcal{O}_v$ (finite-type normal k-algebra with MaxSpec U). Then $(C, \mathcal{O}_v)$ is a "variety over k."

Let us now discuss maps to projective spaces $\mathbb{P}^r = (k^{\oplus r+1} \setminus \{0\})/k^*$.

Definition 38. Let C/k be a curve. A **linear system** on C is a finite-dimensional k-subvector space $V \subset K$.

Let $f_0, \ldots f_r \in V$ be a basis with $r \geq 1$ (i.e. $\dim V \geq 2$). Then we define $(f_0, \ldots, f_r) : C \to \mathbb{P}^r$ given by $v \mapsto [f_0(v) : \cdots : f_r(v)]$. For almost all v, v is not a pole of $f_0, \ldots, f_r$, and some $f_i(v) \neq 0$. In general, let $i_0 \in \{0, \ldots, r\}$ be the index with $-v(f_i)$ maximal, then $f_0/f_i, \ldots, f_r/f_i \in \mathcal{O}_v$ and $f_i/f_i = 1$. So $((f_0/f_i)(v), \ldots, 1, \ldots, (f_r/f_i)(v)) \in k^{r+1} \setminus \{0\}$ gives a point of $\mathbb{P}^r$.

For example, take $K = \mathbb{C}(t)/\mathbb{C}$ with $f_0 = 1/t(t+1), f_1 = 1/t^2(t+1)^2, f_2 = t^2/(t+1)^{10}$. $\phi = (f_0 : f_1 : f_2) : \mathbb{P}^1 \to \mathbb{P}^2$. If $t \neq 0, -1, \infty$ then just take the value. If $t = 0$, $(f_0/f_1, 1, f_2/f_1) = (t(t+1), 1, t^4/(t+1)^8)|_{t=0} = (0, 1, 0)$. For $t = -1$ we get $(0, 0, 1)$ and for $t = \infty$ we get $(1, 0, 0)$. We see that $\phi^{-1}(\text{first } \mathbb{A}^1) = \mathbb{P}^1 \setminus \{0, -1\} = \text{MSpec } k[1/t, 1/(t+1)]$.

Remark. The map to projective space defined by the linear system is the same up to choice of coordinates as the map defined by $f.V$ for $f \in K^*$.

Class 18

Consider the homogeneous coordinates $x_0, \dots, x_r$ on $\mathbb{P}^r$. These do not give functions on $\mathbb{P}^r$ but they do give functions up to k^*. More precisely, if $F \in k[x_0, \dots, x_r]$ is **homogeneous** then

$$V(F) = \{[x_0 : \dots : x_n] \in \mathbb{P}^r \mid F(x_0, \dots, x_n) = 0\}.$$

is well defined. Moreover,

$$\mathbb{P}^r = (\mathbb{P}^r \setminus V(x_0)) \cup \dots \cup (\mathbb{P}^r \setminus V(x_r))$$

and $\mathbb{P}^r \setminus V(x_i)$ is an affine space with coordinates x_j/x_i for $j = 0, \dots, i-1, i+1, r$.

Take $\mathbb{P}^1$, for example. We get $\mathbb{P}^1 \setminus V(X_0)$ with coordinate x_1/x_0 and $\mathbb{P}^1 \setminus V(X_1)$ with coordinates x_0/x_1.

Proposition 103. *A subset $Z \subset \mathbb{P}^r$ is called **Zariski closed** if the following equivalent conditions are satisfied.*

1. *For each $i = 0, \dots, r$ the intersection $Z \cap (\mathbb{P}^r \setminus V(x_i))$ is the zero set of a collection of polynomials $f_\alpha \in k[x_j/x_i]$;*
2. *There exists a collection of homogeneous polynomials $F_\beta \in k[x_0, \dots, x_r]$ such that $Z = \cap_\beta V(F_\beta)$.*

Proof. De(homogenize). □

Exercise 2. *The Zariski topology on $\mathbb{P}^r$ is Noetherian (d.c.c. for closed subsets) of dimension r.*

Lemma 104. *Let C be a curve with function field K/k and let $V = kf_0 + \dots + kf_r$ be a linear system of dimension $r+1$. Then*

$$Im([f_0 : f_1 : \dots : f_r]) : C \to \mathbb{P}^r$$

is Zariski closed.

Proof. Pick $a \in \{0, \dots, r\}$. Then consider $k[x_0/x_i, \dots, x_r/x_i] \to K$ given by $x_j/x_i \mapsto f_j/f_i$. The image is a finite-type k-algebra $B \subset K$. Let $B \subset A \subset K$ be the integral closure. Then A is of finite-type over k [Ha, 3.9A]. Then A is a normal Noetherian domain of dimension one with fraction field K. Then $\mathfrak{m} \in \operatorname{MaxSpec} A$ yields a DVR $A_\mathfrak{m}$ in C with a valuatoin on K/k. By Lemma 15 we get a surjective map from $\operatorname{MaxSpec} A \twoheadrightarrow \operatorname{MaxSpec} B \subset \operatorname{MaxSpec} k[x_0/x_i, \dots, x_r/x_i] = \mathbb{P}^r - V(x_i) \subset \mathbb{P}^r$ and the diagram commutes (proof omitted). □ add diagram

Remark. Of course, in the situation above, the dimension of the image is 1.

Remark. If $f_0, \dots, f_s \in V$ span but are linearly dependent, then we still get a map $C \to \mathbb{P}^s$ with closed image, but now $\operatorname{Im} \Phi \subset V(\sum a_i x_i)$ for some $a_0, \dots, a_r \in k$ not all zero. We say that the image is **linearly degenerate** in this case.

Lemma 105. *Let $D \subset \mathbb{P}^r$ be an irreducible Zariski closed subset of dimension one. There D is the image of a curve C by a map as above.*

Proof. Pick $i \in \{0, \ldots, r\}$ such that $D(\mathbb{P}^r \setminus V(x_i)) \neq \varnothing$. Then $D_i = D \cap (\mathbb{P}^r \setminus V(x_i)) = \operatorname{MaxSpec} k[x_j/x_i]/J$ where J is the set of all polynomials in x_j/x_i vanishing on D_i. By topology, D irreducible implies that D_i is irreducible, and hence J is prime. This implies that $A = k[x_j/x_i]/J$ is a domain. Then, $\dim D = 1$ implies that $\dim D_i = 1$ and thus $\dim A = 1$. By Lemma 54 we see that $K = \operatorname{Frac} A$ is a finitely-generated field extension of k with $\operatorname{trdeg}_k K = 1$.

Let V be k times the class of x_0/x_1 plus ... plus k times the class of x_r/x_i. Denote x_j/x_i by f_j. Then consider $\Phi = [f_0 : \ldots : f_r] : C \to \mathbb{P}^r$. If $h \in J \subset k[x_0/x_1, \ldots, x_r/x_i]$ then $h(f_0, \ldots, \hat{f}_i, f_r) = 0$ in K. Then, thinking a little bit, we see that $\Phi(C) \cap (\mathbb{P}^r \setminus V(x_i)$, which is contained in D_i. Some topology shows that $\Phi(C) = D$ (both closed irreducible and agree on an open). $\square$

Let $V \subset K$ be a linear system. Let $f_0, \ldots, f_r$ be a basis. Let $D = \max((f_i)_\infty) - \min((f_i)_0)$. Then $V \subset L(D)$ and D is minimal with this property.

Definition 39.

(a) We say that V is a **complete linear system** if $V = L(D)$ with D as above;

(b) The **degree** of a linear system V is $\deg D$;

(c) The r of the linear system V is $\dim V - 1$.

In this situation, we say that V is a g^r_d.

Lemma 106. *If V is a g^r_d then Φ_V^{-1}(hyperplane $H \subset \mathbb{P}^r$) is a* ***divisor*** *consisting of exactly d points.*

Proof. Pick a minimal divisor D such that $V \subset L(D)$ Say

$$H = V(a_0x_0 + \ldots + a_rx_r).$$

Then $\Phi^{-1}(H)$ is the set of $v \in C$ such that $v(\sum a_if_i)$ is greater than minus the coefficient of v in D as a divisor $(\sum a_if_i) + D$. This is an effective divisor, as $\sum a_if_i \in V \subset L(D)$ and the degree is equal to $\deg D = d$ because the degree of a principal divisor is zero. Pick i_0 such that $-v(f_{i_0})$ is maximal. Then $\Phi(v)$ has coordinates of f_i/f_{i_0} evaluated at v. So v maps into H if and only if $\sum a_if_i/f_{i_0} = 0$ if and only if $\sum a_if_i$ has lesser pole order than f_{i_0} at v. $\square$

Class 19

Here's another way to think about Φ_V. First, consider $\mathbb{P}^r$ as being the space of r-dimensional linear subspaces of $(k^{r+1})^*$. Given a vector space V, we will set in Grothendieck notation, $\mathbb{P}(V)$ to be the projective space of codimension one linear subspaces of V. Given a linear system $V \subset K$ choose D a divisor minimal with $V \subset L(D)$. Then

$$\begin{aligned} \Phi_V : & C \longrightarrow \mathbb{P}(V) \\ & p \mapsto V(-P) = L(D-P) \cap V \end{aligned}$$

Corollary 107. *The map associated to V is* ***injective*** *if and only if for all $P \neq Q$ in C we have $\dim V(-P-Q) = \dim V - 2$. We say "V separates points."*

Proof. $\Phi_V(P) \neq \Phi_v(Q) \leftrightarrow V(-P) \neq V(-Q)$ and we have

$$V(-P-Q) = V(-P) \cap V(-Q).$$

□

There's a problem here: Φ_V can be injective without being an "isomorphism" onto its image. An example of this is the cuspidal curve. Take $K = k(t)$ and $V = k + kt^2 + kt^3$. Then $\Phi : C = \mathbb{P}^1 \to \mathbb{P}^2$ maps $\mathbb{P}^1$ to something with a singularity. More precisely, $\mathbb{A}^1 = \mathbb{P}^1 - \infty = \Phi^{-1}\left(\mathbb{P}^2 - V(X_0)\right) \mapsto \mathbb{P}^2 - V(X_0) = \mathbb{A}^2$. The image is the curve in $\mathbb{A}^2$ cut out by $y^2 - x^3 = 0$. In characteristic zero, getting a singularity in the image is the only problem. In characteristic $p > 0$, on the other hand, let $V = k + kt^p$. Then we get a map $\Phi : \mathbb{P}^1 \to \mathbb{P}^1$ given by $t \mapsto t^p$, which is injective and surjective. Namely, if $a, b \in k$ and $a^p = b^p$ then $a = b$. But this map is not an isomorphism, as it has degree $p > 1$. We have $k(t) \supset k(t^p)$.

Proposition 108. *Let V be a linear system. If V separates points and tangent vectors, i.e. for all P, Q in C (with $P = Q$ allowed) $\dim V(-P-Q) = \dim V = -2$. Then $\Phi_V : C \to \mathbb{P}^r$ is an isomorphism onto its image. In fact, Φ_V is a closed immersion, i.e. for every $i = 0, \ldots, r$, the ring map*

$$\mathcal{O}_C(\Phi_V^{-1}(\mathbb{P}^r - V(X_i)) \longleftarrow k[x_0/x_i, \ldots x_r/x_i].$$

Proof. Omitted. Roughly speaking, if we let A be the left-hand side and B be a quotient of the right-hand side, we see that A is the integral closure of B in K, A is finite over B, and finally we use Lemma II 7.4 in Hartshorne (see also 7.3). □

Definition 40. Let D be a divisor. We say that D is **basepoint free** if $L(D-P) \neq L(D)$ for all $P \in C$. This really only makes sense as long as $L(D) \geq 1$.

Remark. This exactly means that $L(D)$ is a g_d^r with $d = \deg D$. Furthermore, this exactly means that $L(D) \subset L(D') \leftrightarrow D' \geq D$.

Lemma 109. *Let C be a curve of genus g and D a divisor of degree d. Then*

1. *if $d > 2g - 1$ then D is bpf;*

2. if $d > 2g$ then $L(D)$ separates points and tangent vectors.

Proof. If E is a divisor with $\deg E > 2g-2$ then $\ell(E) = \deg E + 1 - g$. For (2) we simply see that $L(D-P-Q) = d-2+1-g = (d+1-g)-2 = \ell(D)-2$. $\square$

Example 20. Let $g = 0$. If $d = 1$, we get an isomorphism from $\mathbb{P}^1 \to \mathbb{P}^1$. If $d = 2$ we get an isomorphism from $\mathbb{P}^1$ to some curve in $\mathbb{P}^2$ which meets everywhere line in $\mathbb{P}^2$ at two points (counted with multiplicity). Next, take $d = 3$. We get a map $\mathbb{P}^1 \to \mathbb{P}^3$ given by $[1:t] \mapsto [1:t:t^2:t^3]$ whose image is a curve that meets every plane at 3 points. This is called a rational normal curve of degree 3.

Now let $g = 1$ and $d = 3$. Our image is isomorphic to a curve $D \subset \mathbb{P}^2$ which meets every line in 3 points. We claim that $D = V(F)$ where F is a cubic (homogeneous). To see this note that we know D is irreducible of dimension one. In particular, $D \cap (\mathbb{P}^2 - V(X_0))$ corresponds to a prime ideal in $k[x_1/x_0, x_2/x_0]$ which is not maximal and not (0). But since we have a UFD, $\mathfrak{p} = (f)$, f an irreducible polynomial. Then $D = V(F)$ where F is X_0 to the total degree of (f) times $f(x_1/x_0.x_2/x_0)$. Now why is the degree of F 3? Well given a squarefree homogeneous $F \in k[x_0, x_1, x_2]$ we can find a line $L \subset \mathbb{P}^2$ such that the number of points of $L \cap F$ is the degree of F. The idea for proving this is to dehomogenize. Then let $\Delta(x)$ be the discriminant of the dehomogenized polynomial. Clearly $\Delta(x) \neq 0$ everywhere because F is squarefree. Take $\lambda \in k$ such that $\Delta(\lambda) \neq 0$ and now the line $x = \lambda$ i.e. $x_1/x_0 = \lambda$ i.e. $X_1 - \lambda X_0 = 0$ meets $V(F)$ in exactly $\deg F$ points.

Lecture 20

In the previous lectures we proved the statements:

(1) If C has g_d^2 then we get $\Phi : C \to \mathbb{P}^2$ such that every line meets $\Phi(C)$ in d points (counted with multiplicity).

(2) If F homogenous of degree d and squarefree then a general line meets $D = V(F) \subset \mathbb{P}^2$ in d distinct points.

Lemma 110. *In situation (1) above $\Phi(C) = V(F)$, where F is an irreducible homogenous polynomial of degree e, and $e|d$. In fact, d/e is the degree of the function field of C over the function field of D.*

Proof. Pick any $F \neq 0$ homogenous such that $\Phi(C) \subset V(F)$. This is possible because the image is closed. If we can factor $F = F_1F_2$, then $\Phi(C) \subset V(F_1) \cup V(F_2)$, but $\Phi(C)$ irreducible so we have either $\Phi(C) \subset V(F_1)$ or $\Phi(C) \subset V(F_2)$. Therefore we may assume that F is irreducible. But this implies $\Phi(C) = V(F)$. [There's also an alternative way to think about this. $\Phi : C \to \mathbb{P}^2$ is given by $V = kf_0 + kf_1 + kf_2$. Then $\Phi(C) \subset V(F) \Leftrightarrow F(f_0, f_1, f_2) = 0$ in k.]

By (2) we see that $e = \deg F \leq d$. But, to show that $e|d$, we need to use

Lemma 111 below. This shows us that, for every line H, $\deg \Phi^{-1}(H) = [k(C) : k(D)] \cdot \deg(H \subset V(F))$. In conclusion, if D is a degree 3 divisor on a genus 1 curve C, then its complete linear system $L(D)$ defines a closed embedding (injective immersion such that the domain is birational to the image):

$$C \hookrightarrow \mathbb{P}^2$$

whose image is a degree 3 curve. $\square$

Lemma 111. *Suppose $K_1 \supset K_2$ is a finite extension of an extension of k which is f.g. and has transcendence degree 1. The corresponding map $C_1 \to C_2$ has degree $[K_1 : K_2]$ in the sense that its fibers have exactly that many points if you count with muptiplicity.*

Proof. If v valuation on K_2, then $w_1, \ldots, w_i$ extensions of v to K_1, set $e_i =$ the integer such that $w_i|_{K_2} = e_i v$, then $\sum e_i = [K_1 : K_2]$. $\square$

We also prove here the converse of Lemma 110, namely that any nonsingular degree 3 curve has genus 1.

Proof. Let $F \in k[x_0, x_1, x_2]$ homogenous of degree 3 such that $C = V(F)$ is nonsingular, i.e. on the affine pieces you get a nonsingular curve. This means that $\frac{\partial F}{\partial x_1}, \frac{\partial F}{\partial x_2}, \frac{\partial F}{\partial x_3}, F$ have no common 0 in $\mathbb{P}^2$.

Now we work on the affine piece $C \cap (\mathbb{P}^2\ V(x_0))$. Let $x = \frac{x_1}{x_0}, y = \frac{x_2}{x_0}$ such that we can write $f(x, y) = F(1, x, y)$. We know that f_x, f_y are not simultaneously 0 on $f = 0$. So we can look at:

$$\omega = \frac{dx}{f_y} = -\frac{dy}{f_x} \in \Omega_{k(C)/k}$$

The equality holds because $df = f_x dx + f_y dy = 0$. Thus, for every P on $f = 0$, the module of differentials is generated by dx if $f_y(P) \neq 0$ or by dy if $f_x(P) \neq 0$. We conclude that $\omega \in \Omega_{k(C)/k}$ vanishes nowhere and doesn't have a pole at any of the points of this open.

On the overlap with another affine open, say $k[u, v] = k[x_0/x_1, x_2/x_1]$, we have $u = x^{-1}$, $v = yx^{-1}$. Then write $g(u, v) = F(u, 1, v)$. We have:

$$F(1, x, y) = x^3 F(x^{-1}, 1, yx^{-1}) = x^3 g(x^{-1}, yx^{-1})$$

$$f_y = x^3 x^{-1} g_v = u^{-2} g_v$$

For the purpose of generalizing to arbitrary degree d, which we will do shortly, note that the 2 which appears here is $d - 1$.

$$\omega = \frac{dx}{f_y} = \frac{u^{-2} du}{u^{-2} g_v} = \frac{du}{g_v}$$

By similar reasoning, this has no zeros or poles. In conclusion, our C has a global differential form $\omega \in \Omega_{k(C)/k}$ without poles or zeros. Therefore $\deg(K_C) = 0 = 2g_C - 2$, so $g_C = 1$. $\square$

Remark. If $\deg F = d > 3$, then we get:

$$\omega = \frac{dx}{f_y} = -u^{\deg(F)-3}\frac{du}{g_v}$$

Assume we chose coordinates such that $C \cap V(x_0) \cap V(x_1) = \emptyset$. Then $(u = 0) \cap (C \cap (\mathbb{P}^2 - V(x_1))) = V(x_0) \cap C$. This is a divisor of degree d. In conclusion, if $d > 3$ then there exists a regular differential form whose divisor of zeros is $(d-3)\cdot$ divisor at ∞. This has degree $d(d-3)$. Then:

figure out why

$$2g_C - 2 = d(d-3) \Rightarrow g_C = \frac{(d-1)(d-2)}{2}$$

About other embeddings of genus 1 curves

If D is a divisor of degree ≥ 3 on a genus 1 curve C then the full linear system of D is BPF and embeds C as a degree d curve in $\mathbb{P}^{d-1}$. If $d = \deg D = 4 = 2\cdot 2$, then we guess that we should get an intersection of two quadratics. To prove this, we set $V = L(D) \subset K$. We look at:

$$\mathrm{Sym}^2(V) \to L(2D)$$

By Riemann-Roch, $L(2D)$ has dimension $8 + 1 - g = 8$. The dimension of $\mathrm{Sym}^2(V)$ is $\binom{5}{2}$. Therefore the kernel has dimension 2, so C lies on two quadratics.

Lecture 21

Lemma. *Let $U.V, W$ be finite dimensional vector spaces. Let $\phi : V \otimes W \to U$ be a linear map such that $\phi(v \otimes w) \neq 0$ if $v, w \neq 0$. Then $\dim U \geq \dim V + \dim W - 1$.*

Proof. We look at $X = \{v \otimes w \in V \otimes W\} \hookrightarrow V \otimes W$, which is Zariski closed. We have that $\dim V + \dim W - 1$, where the -1 comes from the invariance to rescaling v and w simultaneously. If $U = k^{\oplus n}$, then $\phi = (\phi_1, \ldots, \phi_n)$. Then:

$$\begin{aligned} 0 = \dim(X \cap \mathrm{Ker}(\phi)) &= \dim(X \cap \mathrm{Ker}\,\phi_1 \cap \cdots \cap \mathrm{Ker}\,\phi_n) \\ &= \dim(X) - 1 - 1 \cdots - 1 \\ &= \dim(X) - n \end{aligned}$$

$\square$

Theorem (Clifford's theorem)**.** *Let D be a divisor with $l(D), l(K_C - D) \geq 1$. Then $l(D) \leq \frac{1}{2}\deg(D) + 1$.*

Proof. Apply the lemma to the multiplication map:

$$L(D) \otimes_k L(K_C - D) \to L(K_C)$$

And get $l(D) + l(K_C - D) \leq g + 1$. On the other hand, by RR, we have $l(D) - l(K_C - D) = \deg D + 1 - g$. Adding these two equations gives the desired result. □

Theorem. *If $g(C) \geq 2$, thn C has at most one g_2^1. (Up to multiplication by an element of $K^\times$.)*

Proof. If V is a g_1^2, then it's a complete linear system (by Clifford's theorem). Say we have two divisors D, D' of degree 2, $l(D) = l(D') = 2$. We may assume D, D' are effective. Then $l(D + D') \leq \frac{1}{2} \cdot 4 + 1 = 3$. (Note: to use Clifford's theorem here, we need to check that $l(K_C - D - D') > 0$, but this is an easy consequence of Riemann-Roch.)

If $L(D)$ has basis f_1, f_2 and $L(D')$ has basis g_1, g_2, then:

$$g_2^1 : C \stackrel{f_1/f_2}{\to} \mathbb{P}^1$$

$$g_2^1 : C \stackrel{g_1/g_2}{\to} \mathbb{P}^1$$

We want to show that these maps are the same. There exist $a_{ij} \in k$ not all zero such that:

$$\sum a_{ij} f_i g_j = 0 \text{ in } K$$

The rank of $A = (a_{ij})$ cannot be 1, because then $L(D) \otimes_k L(D')$ would send a pure tensor to 0. Then we can always change basis f_i, g_i such that:

$$f_1 g_2 - f_2 g_1 = 0 \Leftrightarrow \frac{f_1}{f_2} = \frac{g_1}{g_2}$$

□

Theorem (Clifford, part 2)**.** *If we have equality in Clifford's theorem,and $D \not\sim_{rat} 0, D' \not\sim_{rat} 0$, then C is hyperelliptic and $D = mD'$, with D' the unique g_2^1 on C.*

Proof. See Harthshorne. □

Definition 41. Assume (unnecessarily, but in order to make Prof. de Jong less stressed out) that $k = \mathbb{C}$. The **gonality** of the curve C is any of the following equivalent notions:

(1) The minimal degree of a morphism $C \to \mathbb{P}^1$.

(2) The minimal degree of $[K : \mathbb{C}(f)]$ for any $f \in K - \mathbb{C}$.

(3) The minimal integer k such that C has a g_k^1.

Lemma. *The gonality of C is at least the integer k such that there exist $P_1, \ldots, P_k$ in C which do not impose independent conditions on $L(K_C)$,i.e.:*

$$l(K_c - P_1 - \cdots - P_k) > g - k$$

Proof. Suppose $f : C \to \mathbb{P}^1$ has degree k, let:

$$f^{-1}(\{t\}) = \{P_1, \dots, P_k\}$$

for $t \in \mathbb{P}^1(\mathbb{C})$. Then a few moments of thought give:

$$l(P_1 + \cdots + P_k) \geq 2$$

$$\Rightarrow l(K_C - P_1 - \cdots - P_k) \geq 2 - k - 1 + g = 1 + g - k$$

Conversely, if $l(K_C - P_1 - \cdots - P_k) > g - k$, then $l(P_1 + \cdots + P_k) \geq 2$ and we get a g^1_k. $\square$

Theorem (1979)**.** *A smooth plane curve has gonality $d-1$, where $d \geq 4$ is the degree.*

Proof. By projection from a point of C we see that the gonality is $\leq d - 1$ (because a line intersects C in d points, and one of them is the point we project from). For the converse we use the fact from last time:

$$K_C \sim (d-3)H \cap C$$

$H \cap \mathbb{P}^2$ is the hyperplane at (x), so $H = V(x_0)$ and $g_c = \frac{(d-1)(d-2)}{2}$. Hence for every $h \in \mathbb{C}[x, y]$ of total degree $\leq d - 3$ we obtain an element $L(K_C)$:

$$h \to h\omega = \frac{hdx}{f_y} - \frac{hdy}{f_x}$$

Where $f(x, y) = 0$ defines $C \cap (\mathbb{P}^2 - V(x_0))$. This map is injective because $h \notin (f)$ by degree reasons.

$$\dim\{h\} = 1 + 2 + \cdots + d - 2 = \frac{(d-1)(d-2)}{2}$$

Where, for example, the $d - 2$ is the dimension of $\mathbb{C}x^{d-3} + \cdots + \mathbb{C}y^{d-3}$. Hence $\{h\} \cong L(K_C)$. Now if $C\overset{\phi}{\mathbb{P}^1}$ is a g^1_k then picking $t \in \mathbb{P}^1(\mathbb{C})$ general, we see that $\phi^{-1}(\{t\}) = \{P_1, \dots, P_k\}$ are all going to be in $C - C \cap H \subset \mathbb{C}^2$. But $k \leq d - 2$ points in $\mathbb{C}^2$ pose independent conditions on polynomials of degree $d - 3$. So the gonality of C is $\geq d - 1$. $\square$

Corollary. *A smooth plane curve of degree $d \geq 4$ is not hyperelliptic.*

Class 22

Let's approach schemes backwards - let's define schemes and then work backwards to see what it means. Hence, there will be undefined terms at any given point.

Definition 42.

(i) A **scheme** is a **locally ringed space** such that every point has an open neighborhood isomorphic to an **affine scheme**.

(ii) A **morphism of schemes** is a **morphism of locally ringed spaces**.

(iii) A locally ringed space is a **ringed space** (X, O_X) such that the **stalks** of the **structure sheaf** O_X are local rings for $x \in X$

(iv) A morphism of locally ringed spaces is a **morphism of ringed spaces** $f : (X, O_X) \to (Y, O_Y)$ such that for all $x \in X$ the induced map $f_x^{\#} : O_{Y,f(x)} \to O_{X,x}$ is a local homorphism of local rings: $f_x^{\#}(\mathfrak{m}_{f(x)}) \subset \mathfrak{m}_x$.

(v) A **ringed space** (X, O_X) is a pair consisting of a topological space X and a **sheaf of rings** O_X on X called the **structure sheaf** of X

(vi) A morphism of ringed spaces $f : (X, O_X) \to (Y, O_Y)$ is given by a continuous map $f : X \to Y$ and for all $V \subset Y$ open, a map $O_Y(V) \overset{f^{\#}}{\to} O_x(f^{-1}V)$ of rings compatible with the **restriction mapping** of O_X and O_Y.

(vii) Let X be a topological space. A **presheaf** $\mathcal{F}$ of some target category $\mathcal{C}$ on X is a rule which assigns to every open $U \subset X$ an object of the target category $\mathcal{F}(U)$ and for every $V \subset U$ a restriction morphism $\rho_V^U : \mathcal{F}(U) \to \mathcal{F}(V)$ of the target cateory such that $\rho_U^U = \text{id}$ and $\rho_V^U \circ \rho_U^W = \rho_V^W$ if $V \subset U \subset W$ open in X. Often used is the notation that $s|_V = \rho_V^U(s)$.

(viii) A presheaf $\mathcal{F}$ is called a sheaf if given an open covering U_i of any open $U \subset X$, we have that $\mathcal{F}(U)$ maps bijectively to

$$\{(s_i) \in \prod_{i \in J} \mathcal{F}(U_i) \mid \rho_{U_i \cap U_j}^{U_i}(s_i) = \rho_{U_i \cap U_j}^{U_j}(s_j) \text{ for all } i, j \in I$$

with $s \mapsto \rho_{U_i}^U(s)$. This is called the **sheaf condition**. This is essentially saying that local data plus gluing implies global data.

(ix) Given a presheaf $\mathcal{F}$ of $\mathcal{C}$ and a point $x \in X$, **the stalk of $\mathcal{F}$ at** x is

$$\mathcal{F}_x = \{(U, s)\} / \sim$$

where (U, s) are pairs consisting of an open neighborhood U of x and $s \in \mathcal{F}(U)$ with the equivalence

$$(U, s) \sim (U', s') \Leftrightarrow \exists x \in U'' \subset U \cap U' \text{ open s.t. } \rho_{U''}^U(s) = \rho_{U''}^{U'}(s').$$

Note that $\mathcal{F}_x$ is an object in $\mathcal{C}$.

(x) A **morphism of presheaves** $\mathcal{F} \xrightarrow{\phi} \mathcal{G}$ is given by a collection of maps $\phi(U) : \mathcal{F}(U) \to \mathcal{G}(U)$ for $U \subset X$ open compatible with restriction mappings: whenever $V \subset U$ open, the diagram

$$\begin{tikzcd} \mathcal{F}(U) \arrow[r, "\phi(U)"] \arrow[d, "\rho_V^U"'] & \mathcal{G}(U) \arrow[d, "\rho_V^U"] \\ \mathcal{F}(V) \arrow[r, "\phi(V)"] & \mathcal{G}(V) \end{tikzcd}$$

commutes. A **morphism of sheaves** is simple a morphism of presheaves.

Our next goal is to construct affine schemes from rings. The idea is that $\operatorname{Spec} A$ has as a basis of opens the standard opens

$$D(f) = \{\mathfrak{p} \subset A \mid f \notin \mathfrak{p}\}$$

for $f \in A$. We will want (because it works)

$$O_{\operatorname{Spec} A}(D(f)) = A_f.$$

Let $\mathcal{B}$ be a basis for the topology of a topological space X and assume (for simplicity) that if $U, V \in \mathcal{B}$ then $U \cap V \in \mathcal{B}$. Define **presheaves on** $\mathcal{B}$ exactly as before. Furthermore, define **sheaves on** $\mathcal{B}$ exactly as before, i.e. the sheaf condition for coverings $U = \cup_{i \in I} U_i$ when $U_i \in \mathcal{B}$.

Proposition 112. *Let X and $\mathcal{B}$ as above. Then there is an equivalence of categories $\mathfrak{Sh}(X) \Leftrightarrow \mathfrak{Sh}(b)$ with $\mathcal{F} \mapsto \mathcal{F}|_{\mathcal{B}}$. This is in general not correct for presheaves.*

Read this in the Stacks project or in FOAG (Ravi's notes). "Ravi claims that he covers ALL OF THAT in one year. And that his students do all the exercises. It's not possible. I don't believe it... well maybe it's possible." - de Jong.

Proof. If $\mathcal{G}$ is a sheaf on $\mathcal{B}$ and $U \subset X$ is an arbitrary open then we can choose a covering $U = \cup U_i$ with $U_i \in \mathcal{B}$. Then the sheaf $\mathcal{F}$ on X corresponding to $\mathcal{G}$ should satisfy

$$\mathcal{F}(U) = \{(s_i) \in \prod \mathcal{G}(U_i) \mid \rho^{U_i}_{U_i \cap U_j}(s_i) = \rho^{U_j}_{U_i \cap U_j}(s_j).$$

Then we just define $\mathcal{F}$ by this formula! "...and now you have to write up sort of infinitely long checks." $\square$

Example 21. $X = \operatorname{Spec} A$ with the Zariski topology.

$$\mathcal{B} = \{D(f) \mid f \in A\}.$$

This satisfies our assumption $D(f) \cap D(g) = D(fg)$. We want to consider $\mathcal{B} \ni D(f) \mapsto A_f$. But this is nonsense! It might happen that $D(f) = D(g)$ without $f = g$.

Lemma 113. *If $f, g \in A$ and $D(f) \supset D(G)$ then there is a unique A-algebra map $A_f \to A_g$. If $D(f) = D(g)$ then this map is an isomorphism.*

Proof. Recall that $\operatorname{Spec} A_f \to \operatorname{Spec} A$ induces a homeomorphism onto $D(g)$. Thus the assumption $D(f) \supset D(g)$ implies that f maps to an element of A_g not in any prime ideal. So f is invertible in A_g. Hence we get our unique canonical map by the universal property of localization. $\square$

Class 23

Lemma 114. *Let $\mathcal{B}$ be the standard basis of opens of* $\operatorname{Spec} A$. *Given an A-module M the rule $\mathcal{B} \to A-$modules given by $U = D(f) \mapsto M_f = M \otimes_A A_f$ is a sheaf of A-modules on $\mathcal{B}$.*

Proof. Lemma 113 shows that this is well-defined and gives the restriction mappings. It is left as homework to prove the sheaf condition. $\square$

Definition 43. The **structure sheaf** of $\operatorname{Spec} A$ is the sheaf of rings $O_{\operatorname{Spec} A}$ which corresponds via the proposition to the rule $D(f) \mapsto A_f$ on the basis $\mathcal{B}$ of standard opens.

Remark. Similarly, we have a sheaf $\tilde{M}$ corresponding to $D(f) \mapsto M_f$. Observe that $\tilde{M}$ is a sheaf of $O_{\operatorname{Spec} A}$-modules.

Let us look at the stalk of the structure sheaf at $\mathfrak{p}$. Note that since $\mathcal{B}$ is a basis for the topology, to compute the stalk we need only consider pairs $(D(f), s)$ where $\mathfrak{p} \in D(f)$ and $s \in A_f$, i.e. $f \in A \setminus \mathfrak{p}$ and $s = a/f^n$. Then two such pairs $(D(f), a/f^n)$ and $(D(g), b/g^m)$ give the same element of the stalk if and only if there exists $h \in A \setminus \mathfrak{p}$ such that $D(h) \subset D(f), D(h) \subset D(g)$ and a/f^n and b/g^m map to the same element of A_h. Contemplate the diagram:

$$\begin{tikzcd}
& A \arrow[dl] \arrow[dr] & \\
A_f \arrow[dr] \arrow[ddr] & & A_g \arrow[dl] \arrow[ddl] \\
& A_h \arrow[d] & \\
& A_{\mathfrak{p}} &
\end{tikzcd}$$

and conclude that we get a well-defined map $O_{\operatorname{Spec} A, \mathfrak{p}} \to A_{\mathfrak{p}}$ that is both injective and surjective. In fact, it is an algebraic fact that the colimit

$$\varinjlim_{f \in A \setminus \mathfrak{p}} = A_{\mathfrak{p}}$$

and that

$$O_{\operatorname{Spec} A,\mathfrak{p}} = \varinjlim_{U \ni \mathfrak{p}} O(U) = \varinjlim_{U \in \mathcal{B}, \mathfrak{p} \in U} \mathcal{F}(U).$$

In particular $O_{\operatorname{Spec} A,\mathfrak{p}} = A_{\mathfrak{p}}$ is a local ring

Lemma 115. *The stalk of $O_{\operatorname{Spec} A}$ at $\mathfrak{p}$ is $A_{\mathfrak{p}}$. The stalk of $\tilde{M}$ at $\mathfrak{p}$ is $M_{\mathfrak{p}}$.*

Definition 44. An **affine scheme** is a locally ringed space isomorphic[1] to $(\operatorname{Spec} A, O_{\operatorname{Spec} A})$ for some ring A.

Now recall that a scheme X is a locally ringed space that at every point $x \in X$ has an open neighborhood isomorphic to an affine scheme.

Remark. If (X, O_X) is a (locally) ringed space and $U \subset X$ is open, then $(U, O_X|_U)$ is a (locally) ringed space, let us call it an **open subspace**. Moreover, there is an inclusion morphism $j : (U, O_X|_U) \to (X, O_X)$ of (locally) ringed spaces.

Remark. Open subspaces of schemes are again schemes. To see this, it is enough to show that

$$(D(f), \mathcal{O}_{\operatorname{Spec} A}|_{D(f)}) \cong (\operatorname{Spec} A_f, \mathcal{O}_{\operatorname{Spec} A_f}),$$

which we shall do below.

Ring maps and morphisms

Let $\phi : A \to B$ be a ring map and $\operatorname{Spec} \phi : \operatorname{Spec} B \to \operatorname{Spec} A$ be the associated continuous map of topological spaces. Moreover, if $f \in A$, then

$$\operatorname{Spec} \phi^{-1}(D(f)) = D(\phi(f)).$$

Proposition. *Let $f : X \to Y$ be a continuous map of topological spaces. Let $\mathcal{B}$, resp. $\mathcal{C}$, be a basis for the topology on X, resp. Y, bot closed under intersections. Assume $f^{-1}V \in \mathcal{B}$ for all $V \in \mathcal{C}$. Then, given sheaves $\mathcal{F}$, resp. $\mathcal{G}$, on X, resp. Y, to give a collection of maps $\phi(V) : \mathcal{G}(V) \to \mathcal{F}(f^{-1}V)$ for all V open in Y compatible with restriction mappings is the same thing as giving a collection of maps $\phi(V) : \mathcal{G}(V) \to (F)(f^{-1}V)$ for all $V \in \mathcal{C}$ compatible with restriction maps.*

Remark. Such a collection of maps $\phi = \{\phi(V)\}$ is called an f-map from $\mathcal{G}$ to $\mathcal{F}$.

Proof. Given $\phi(V)$ defined for $V \subset \mathcal{C}$ and $W \subset Y$ open, we choose an open covering $W = \cup V_i$ for $V_i \in \mathcal{C}$ and then define $\phi(W)$ by taking

$$\mathcal{G}(W) = \{(s_i) \in \prod \mathcal{G}(V_i) \mid \rho^{V_i}_{V_i \cap V_j}(s_i) = \rho^{V_j}_{V_i \cap V_j}(s_j)\}$$

to

$$\mathcal{F}(f^{-1}(W)) = \{(t_i) \in \prod \mathcal{F}(f^{-1}V_i) \mid \cdots\}$$

One now has to do an infinite number of things to show that this works, and this concludes the proof. ☐

[1] As a (locally) ringed space. It doesn't matter which, because if $\phi : A \to B$ is an isomorphism of rings, and A and B are local, then ϕ is local.

Going back to our ring map $A \to B$ we let $\operatorname{Spec}\phi : (\operatorname{Spec} B, \mathcal{O}_{\operatorname{Spec} B}) \to (\operatorname{Spec} A, \mathcal{O}_{\operatorname{Spec} A})$ defined by the rules:

1. $(\operatorname{Spec}\phi)(\mathfrak{q}) = \phi^{-1}(\mathfrak{q})$ for $\mathfrak{q} \in \operatorname{Spec} B$.
2. $\mathcal{O}_{\operatorname{Spec} A}(D(f)) = A_f \to \mathcal{O}_{\operatorname{Spec} B}(D(\phi(f))) = B_{\phi(f)}$ defined by $a/f^n \mapsto \phi(a)/\phi(f)^n$.

This gives us a morphism of ringed spaces. To check that it is indeed a morphism of schemes, we must check that the induced maps

$$\mathcal{O}_{\operatorname{Spec} A, \phi^{-1}(\mathfrak{q})} A_{\phi^{-1}(\mathfrak{q})} \to B_{\mathfrak{q}} = \mathcal{O}_{\operatorname{Spec} B, \mathfrak{q}}$$

is a local homorphism of local rings. This does hold, as it is the map induced by ϕ.

Remark. Suppose we have $f : X \to Y$ and $\phi : \mathcal{G} \to \mathcal{F}$ and f-map. We need to get an induced map on the stalks $\phi_x : \mathcal{G}_{f(x)} \to \mathcal{F}_x$ for some $x \in X$. We can do this by sending $(V, t) \mapsto (f^{-1}V, \phi(V)(t))$.

Lemma 116. *Let A be a ring and $f \in A$. The ring map $A \to A_f$ induces an isomorphism*

$$\begin{tikzcd}
(\operatorname{Spec} A_f, \mathcal{O}_{\operatorname{Spec} A_f}) \arrow[rr] \arrow[dr, "A \to A_f"] & & (D(f), \mathcal{O}_{\operatorname{Spec} A_f}|_{D(f)}) \arrow[dl, "j"] \\
& (\operatorname{Spec} A, \mathcal{O}_{\operatorname{Spec} A}) &
\end{tikzcd}$$

Proof. Omitted. □

Lemma 117. *Let $f : (X, O_X) \to (Y, O_Y)$ be a morphism of (locally) ringed spaces. Then f is an isomorphism iff f is a homeomorphism and f induces isomorphisms on stalks: for $x \in X$, $\mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$.*

Proof. Obvious by Lemma 118. □

Lemma 118. *Let $\mathcal{F} \xrightarrow{\alpha} \mathcal{G}$ be a map of sheaves on a topological space X. Then α is an isomorphism if and only if $\alpha_x : \mathcal{F}_x \to \mathcal{G}_x$ is an isomorphism for all $x \in X$.*

Proof. We have to construct a $\beta : \mathcal{G} \to \mathcal{F}$ inverse to α. To do this, it is enough if $\alpha(U) : \mathcal{F}(U) \to \mathcal{G}(U)$ is bijective for all $U \subset X$ open. Let us first show injectivity. Suppose $\alpha(s) = \alpha(s')$ for some $s, s' \in \mathcal{F}(U)$. Then $(U, \alpha(s))$ and $(U, \alpha(s'))$ define the same element of the stalk $\mathcal{G}_x$ for all $x \in U$. By assumption, this shows that (U, s) and (U, s') define the same element of $\mathcal{F}_x$ for all $x \in U$. By by definition, for all $x \in U$, there exists $x \in U_X \subset U$ such that $s|_{U_x} = s'|_{U_x}$. But then $U = \cup_{x \in U} U_x$ is an open covering and the sheaf condition for $\mathcal{F}$ shows that $s = s'$. Surjectivity is similarly shown. □

Class 24

Examples of Schemes

Example 22 (Scheme associated to an abstract curve)**.** Let $k = \bar{k}$ be an algebraically closed field, K/k a finitely generated extension of transcendence degree one. As a set,

$$X = \{\text{discrete valuations on } K/k\} \cup \{\eta\},$$

where η is a generic point. Note that the closed subsets are $\varnothing, X$, and finite collections of discrete valuations of K/k. Additionally, if $U = X \setminus \{v_1, \ldots, v_n\}$ is open then we take

$$O_X(U) = \{f \in K \mid v(f) \geq 0 \forall v \in U\}.$$

This is indeed a scheme, with every open $U \subset X, U \neq X$ affine, the rings $O_X(U)$ always of finite type over k, the local ring of O_X at v is $O_{X,v} = O_v = \{f \in K \mid v(f) \geq 0\}$, and the local ring of O_X at η is K.

Example 23 (Affine scheme over a ring R)**.**

$$\mathbb{A}^n_R = \operatorname{Spec} R[x_1, \ldots, x_n] \longrightarrow \operatorname{Spec} R$$

Example 24 (Spectrum of the integers)**.** Consider $\operatorname{Spec} \mathbb{Z} = \{(0), (2), (3), \ldots\}$. The closed subsets are $\varnothing, \operatorname{Spec} \mathbb{Z}$, and finite subsets of $D(0)$. Any open is of the form $D(f)$ where $f \in \mathbb{Z}$ and $O_{\operatorname{Spec} \mathbb{Z}}(D(f)) = \mathbb{Z}[1/f]$. Note that $\operatorname{Spec} \mathbb{Z}$ is a final object in the category of schemes.

Example 25 (Proj of a graded ring)**.** Let $A = \oplus_{d \geq 0} A_d$ a graded ring and $A_+ = \oplus_{d > 0} A_d \subset A$ be the irrelevant ideal. We define $\mathbb{P}A$ to be the graded prime ideals $\mathfrak{p} \subset A$ such that $\mathfrak{p}$ does not contain A_+. As a topology, for $f \in A_+$, we take a homogeneous set

$$D_+(f) = \{\mathfrak{p} \in \operatorname{Proj} A \mid f \notin \mathfrak{p}\}.$$

These subsets are a basis for a topology on $\operatorname{Proj} A$. We take

$$O_{\operatorname{Proj} A}(D_+(f)) = A_{(f)},$$

which is simply the degree 0 part of A_f (which is indeed a ring). Observe that A_f is a $\mathbb{Z}$-graded ring. This yields a sheaf of rings on this basis and hence a sheaf of rings on $\operatorname{Proj} A$. It turns out that $D_+(f)$ is affine, hence $D_+(f) \cong \operatorname{Spec} A_{(f)}$. Finally, if $\mathfrak{p} \in \operatorname{Proj} A$, then

$$O_{\operatorname{Proj} A, \mathfrak{p}} = A_{(\mathfrak{p})}.$$

Remark. Warning: the Proj construction is not functorial (in the variable A). E.g.

$$A = R[x_0, x_1] \to R[y_0, y_1, y_2] = B$$

given by $x_0 \mapsto y_0, x_1 \mapsto y_1$. Then $\mathfrak{q} = (y_0, y_1) \in \operatorname{Proj} B$ but its image under the map $\operatorname{Spec} B \to \operatorname{Spec} A$ is not in $\operatorname{Proj} A$. Namely, it is $(x_0, x_1) = A_+$, which is disallowed. Geometrically, one can think of trying to map $\mathbb{P}^2 \to \mathbb{P}^1$ but the point $(0:0:1)$ gives us trouble as it is sent to $(0:0)$.

Example 26 (Projective space over a ring R)**.** We define

$$\mathbb{P}^n_R = \operatorname{Proj} R[x_1, \ldots, x_n] \longrightarrow \operatorname{Spec} R$$

where the grading is the usual one. Since $R[x_0, \ldots, x_n]_+ = (x_0, \ldots, x_n)$, by the definition of Proj, we see that

$$\mathbb{P}^n_R = D_+(x_0) \cup \cdots \cup D_+(x_n).$$

and

$$D_+(X_i) = \operatorname{Spec} R[\frac{x_0}{x_1}, \cdots, \frac{x_n}{x_i}].$$

Key facts on affine schemes

Let $(X, O_X) = (\operatorname{Spec} A, O_{\operatorname{Spec} A})$ be an affine scheme.

1. $\Gamma(X, O_X) = O_X(X) = A$;
2. $O_X(D(f)) = A_f$;
3. For any scheme (S, O_S), we have

   $$\mathrm{Mor}_{\mathrm{Schemes}}((S, O_S), (X, O_X)) \Leftrightarrow \mathrm{Hom}_{\mathrm{Rings}}(A, O_S(S))$$

   given by $f \mapsto f^\# : A = O_X(X) \to O_S(S)$
4. In particular, the full subcategory (of schemes) of affine schemes is anti-equivalent to the category of rings. Note that this and the above are incorrect if in the definition of morphisms of schemes one does not require "locally."

From point 3, let us construct the map in the other direction. Suppose we are given a ring map $\phi : A \to O_S(S)$. We want to construct $f : (S, O_S) \to (X, O_X)$. As a map of sets, let $s \in S$ and consider

$$A \xrightarrow{\phi} O_S(S) \to O_{S,s}$$

where we have $\mathfrak{m}_s \subset O_{S,s}$ the unique maximal and a prime $\mathfrak{p} \subset A$. Hence we set $f(s) = \mathfrak{p}$ to be the inverse image of $\mathfrak{m}_s$ under this composition. Now why is f continuous? Say $g \in A$. It suffices to show that the inverse image of a basis element is open, i.e. $f^{-1}(D(g))$ is open in S. But $f^{-1}D(g)$ is the set of all $s \in S$ such that g is not contained in the inverse image of m_s, or equivalently, the global section $\phi(g)$ in $O_S(S)$ does not map into $\mathfrak{m}_s$.

Lemma. *Let (T, O_T) be a locally ringed space. Let $g \in O_T(T)$. Then*

$$T_g = U = \{t \in T \mid g \notin \mathfrak{m}_t\}$$

is open in T and moreover, there exists a unique $h \in O_T(U)$ such that $g|_U \cdot h = 1$.

Proof. Idea: if $t \in U$ then g is invertible in $O_{T,t}$. There exists an $h_t \in O_{T,t}$ such that $gh_t = 1$. Then, by definition of stalks, there exists an open neighborhood U_t of t and $h_t \in O_T(U_t)$ such that $g|_{U_t} h_t = 1$. Then $U = \cup U_t$ is open, where the union is over t such that $g \notin \mathfrak{m}_t$. Moreover, by uniqueness of inverses in Rings, and the sheaf condition, the local h_t's glue to an h. $\square$

Now we define $f^\#$. For $D(g) \subset \operatorname{Spec} A$ open we let

$$f^\# : O_{\operatorname{Spec} A}(D(g)) = A_g \to O_S(f^{-1}D(S))$$

be the unique ring map extending

$$A \xrightarrow{\phi} O_S(S) \to O_S(f^{-1}D(g)).$$

This works because the above lemma tells us that g is mapped to an invertible element.

We have to now check that the above constructions do really give a morphism of locally ringed spaces, and we have to check that we indeed do have a inverse.

Example 27 (Surjective morphism $\mathbb{A}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$)**.** Take $t \mapsto [t : t^2 + 1]$ at the level of points. At the level of primes, we take $(0) \mapsto (0) \subset \mathbb{C}[x_0, x_1]$ and take $(x - t) \mapsto ((t^2 + 1)x_0 - tx_1) \subset \mathbb{C}[x_0, x_1]$. At the level of rings, not that $\mathbb{P}^1_{\mathbb{C}} = D_+(x_0) \cup D_+(x_1)$.

$$f^{-1}(D_+(x_0)) = D(x) = \operatorname{Spec} \mathbb{C}[x, x^{-1}] \to \operatorname{Spec} \mathbb{C}[\frac{x_1}{x_0}]$$

with x_1/x_0 on the right mapped to $(x^2 + 1)/x$ on the left. Similarly,

$$f^{-1}(D_+(x_1)) = D(x^2 + 1) = \operatorname{Spec} \mathbb{C}[x, 1/(x^2 + 1)] \to D_+(x_1) = \operatorname{Spec} \mathbb{C}[x_0/x_1]$$

where x_0/x_1 on the right is mapped to $x/(x^2 + 1)$ on the left. We claim that this is surjective, as $x/(x^2 + 1)$ takes on all values while $(x^2 + 1)/x$ takes on every value but zero.

Class 25

Example 28. Consider $A^1_{\mathbb{Z}} \to \operatorname{Spec} \mathbb{Z}$ where $A^1_{\mathbb{Z}} = \operatorname{Spec} \mathbb{Z}[x]$. Note that

$$\dim A^1_{\mathbb{Z}} = 2.$$

The points of $A^1_{\mathbb{Z}}$ are as follows. There is a generic point corresponding to $(0) \subset \operatorname{Spec} \mathbb{Z}[x]$. There are codimension one points corresponding to irreducibles (f) (i.e. primes or irreducible nonconstant polynomials). The closed points correspond to (p, f) where p is a prime number and f is a polynomial which is irreducible modulo p.

One has a very similar picture for

$$\begin{tikzcd} A^1_{\mathbb{C}[t]} \arrow[r] \arrow[d, "\cong"] & \operatorname{Spec} \mathbb{C}[t] \arrow[d, "\cong"] \\ A^2_{\mathbb{C}} \arrow[r] & A^1_{\mathbb{C}} \end{tikzcd}$$

Observe that if $Z \subset A^1_{\mathbb{Z}}$ is closed, the its image in $\operatorname{Spec} \mathbb{Z}$ is either a finite set of closed points or open in $\operatorname{Spec} \mathbb{Z}$. Similarly for the complex case.

Example 29. Consider $A^2_{\mathbb{C}} \to A^2_{\mathbb{C}}$ with the map $\mathbb{C}[x,y] \leftarrow \mathbb{C}[x,y]$ given by $xy \leftarrow x, y \leftarrow y$. "On points," $(x,y) \mapsto (xy, y)$. In the arithmetic case we take $A^1_{\mathbb{Z}} \xrightarrow{g} A^1_{\mathbb{Z}}$ and $\mathbb{Z}[x] \leftarrow \mathbb{Z}[x]$ given by $13x \leftarrow x$. In the geometric case we have $\operatorname{Im}(g) = D(y) \cup$ closed pt $(0,0)$. In the arithmetic case, $\operatorname{Im}(g) = D(13) \cup \{(13, x)\}$.

Definition 45. Let X be a Noetherian topological space. We say $E \subset X$ is **constructible** if E is a finite union of locally closed subsets (closed of an open).

Theorem 119 (Chevalley)**.** *Let $f : X \to Y$ be a finite-type morphism of Noetherian schemes. Then the image of a constructible set under f is constructible.*

We will not define these terms here, but one may look at Hartshorne or the Stacks project. The translation into algebra is the following: given $R \to S$ a finite-type ring map of Noetherian rings, then $\operatorname{Spec} S \to \operatorname{Spec} R$ sends constructibles to constructibles.

Lemma 120. *Let R be a Noetherian ring. $E \subset \operatorname{Spec} R$ is constructible if and only if E is a finite union of subsets of the form $D(f) \cap V(g_1, \ldots, g_m)$ with $f, g_1, \ldots, g_m \in R$.*

Proof. The right-to-left statement is clear. Hence we assume that E is locally closed, i.e. $E = U \cap V^c$ where $U, V \subset \operatorname{Spec} R$ are open. Then $U = D(f_1) \cup \ldots \cup D(f_n)$ and $V = D(g_1) \cup \ldots \cup D(g_m)$ as $\operatorname{Spec} R$ is Noetherian so every subset is quasicompact. Then

$$U \cap V^c = (D(f_1) \cap V(g_1, \ldots, g_m)) \cup \cdots \cup (D(f_n) \cap V(g_1, \ldots, g_m))$$

(look this up). $\square$

Lemma. *Let R be a Noetherian ring, $f \in R, S = R_f$. The the result holds.*

Proof. In this case $\operatorname{Spec} S \to \operatorname{Spec} R$ is a homeomorphism onto an open, hence locally closed subsets map to locally closed subsets. $\square$

Lemma. *Let R be a Noetherian ring, $I \subset R$ and ideal with $S = R/I$. Then the result holds.*

Proof. In this case $\operatorname{Spec} S \to \operatorname{Spec} R$ is a homeomorphism onto an closed subset, hence locally closed subsets map to locally closed subsets. □

Lemma. *Let R be a Noetherian ring. The map* $\operatorname{Spec} R[x] \to \operatorname{Spec} R$ *is open.*

Proof. It is enough to show that the image of $D(f)$ is open in $\operatorname{Spec} R$ for $f \in R[x]$. Suppose $f = a_d x^d + \cdots + a_0$, for $a_i \in R$. Then we claim that the image of $D(f)$ is $D(a_0) \cup \cdots \cup D(a_d)$ (which is open). Let $\mathfrak{p} \subset R$ be a prime ideal. Let $\bar{f} \in \kappa(\mathfrak{p})[x]$ be the image of f. We claim that

$$(R[x]_f)_{\mathfrak{p}}/\mathfrak{p}(R[x]_f)_{\mathfrak{p}} \cong \kappa(\mathfrak{p})[x]_{\bar{f}}.$$

The claim follows by some work based on the stuff we did with fibers early in the semester. Hence we see that $\mathfrak{p}$ is in the image if and only if the ring is not zero. In other words $\mathfrak{p}$ is in the image if and only if $\bar{f} \neq 0$. □

Lemma. *Let R be a Noetherian ring and $f, g \in R[x]$. Assume the leading coefficient of g is a unit in R. Then the image of $D(f) \cap V(g)$ in* $\operatorname{Spec} R$ *is open.*

Proof. Write $g = ux^d + a_{d-1}x^{d-1} + \ldots + a_0$ with $u \in R^\times$. Set $S = R[s]/(g)$. As an R-module S is free with basis $1, x, \ldots, x^{d-1}$. Consider multiplication by f on S - this is an R-linear map so we get a matrix as well as a characteristic polynomial $P(T) \in R[R]$. We write

$$P(T) = T^d + r_{d-1}T^{d-1} + \cdots + r_0.$$

We claim that the image of $D(f) \cap V(g)$ is $D(r_0) \cup \cdots \cup D(r_{d-1})$. Suppose $\mathfrak{q} \in D(f) \cap V(g)$ and $\mathfrak{p} = R \cap \mathfrak{q}$. Then there is a map $S_{\mathfrak{p}}/\mathfrak{p}S_{\mathfrak{p}} \to \kappa(\mathfrak{q})$ compatible with multiplication by f. Since f acts as a unit on $\kappa(\mathfrak{q})$, we see that f is not nilpotent on $S_{\mathfrak{p}}/\mathfrak{p}S_{\mathfrak{p}}$ so $\mathfrak{p} \in D(r_0) \cup \cdots \cup D(r_{d-1})$ (by the lemma below).

Let us now prove the converse. Suppose $r_i \notin \mathfrak{p}$ for some i. Then multiplication by f is not nilpotent on $S_{\mathfrak{p}}/\mathfrak{p}S_{\mathfrak{p}}$. This implies that there exists a maximal ideal $\bar{\mathfrak{q}} \subset S_{\mathfrak{p}}/\mathfrak{p}S_{\mathfrak{p}}$ not containing the image of f, which in turn implies that the inverse image $\mathfrak{q} \subset R[x]$ of $\bar{\mathfrak{q}}$ is a point of $D(f) \cap V(g)$ mapping to $\mathfrak{p}$. □

Lemma. *We have that $\mathfrak{p} \in V(r_0, \ldots, r_{d-1})$ if and only if multiplication by f on $S_{\mathfrak{p}}/\mathfrak{p}S_{\mathfrak{p}}$ is nilpotent.*

Proof. Omitted. Hint: $S_{\mathfrak{p}}/\mathfrak{p}S_{\mathfrak{p}}$ is free with basis $1, x, \ldots, x^{d-1}$ over $\kappa(\mathfrak{p})$. □

Theorem 121 (Chevalley's theorem)**.** *Let $R \to S$ be a finite-type ring map. Let R be Noetherian. Then if $E \subset$* $\operatorname{Spec} S$ *is constructible then the image of E under the map is constructible.*

Proof. Take $S = R[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$. Can factor

$$R \to R[x_1] \to R[x_1, x_2] \to \ldots \to R[x_1, \ldots, x_n] \twoheadrightarrow S$$

and so may assume $S = R[x]$ (as the statement has been shown for surjective maps in the lemmas above). We know that E is a finite union of sets of the form $D(f) \cap V(g_1, \ldots, g_m)$ and hence reduce to $E = D(f) \cap V(g_1, \ldots, g_m)$. Note that if $c \in R$ then $\operatorname{Spec} R = D(c) \sqcup V(c)$ and it suffices to show our set intersected with either piece is construcible (by previous lemmas). The claim is that the shape of E does not change under this procedure, i.e. that the image of $(D(f) \cap V(g)) \cap D(c)$ is the image of $D(f_c) \cap V(g_c)$ in $\operatorname{Spec} R_c$ where $f_c, g_c \in R_c[x]$ are the images of f and g. Similarly for $V(c)$.

We use induction on m and on the degrees of the g_i. Let d be the degree of g_1 where g_1 has leading coefficient c. Cut up R as above. On the R_c part we get that g_1 has invertible leading coefficient, while on the R/c part, the degree of g_1 drops so we are done by induction. For the localization case, we can lower the degrees of $g_2, \ldots, g_m$ if they are bigger or equal to d $(V(g_1, \ldots, g_m) = V(g_1, g_2 - hg_1, \ldots))$ again we are done if some g_i has degree $\geq d$. If not I swap g_1, g_2 and go back to start. (The two base cases were $D(f) \cap V(g)$ and $D(f)$ and were done in the lemmas) $\square$

Class 26

The homework over winter break is to read Hartshorne Chapter II, Sections 1,2,3,4, and to do some of the contained exercises.

Definition 46. A morphism of schemes $f : X \to Y$ is **proper** if it is of finite-type, separated, and universally closed (i.e. closed after any base change).

Today we will discuss this definition for $\mathbb{P}^n_S \to S$.

Proposition. *For any scheme S the projection morphism $\mathbb{P}^n_S \to S$ is closed.*

Proof. We have immediate reduction to the case $S = \operatorname{Spec} R$. Recall that $\mathbb{P}^n_R = D_+(X_0) \cup \cdots \cup D_+(X_n)$ where $D_+(X_i) = \operatorname{Spec} R_i$ where $R_i = R[x_0/x_i, \ldots, x_n/x_i]$. Set $R_{ij} = (R_i)_{x_j/x_i} = (R_j)_{x_i/x_j} = R[x_0/x_i \ldots, x_n/x_i, x_i/x_j] = R[x_0/x_j, \ldots, x_n/x_j, x_j/x_i]$ where we take the degree zero part. Let $Z \subset \mathbb{P}^n_R$ be a closed subset. Then $Z \cap D_+(X_i) = V(I_i)$ for a unique radical ideal $I_i \subset R_i$. Then $(Z \cap D_+(X_i)) \cap D_+(X_j) = Z \cap D_+(X_i X_j) = (Z \cap D_+(X_j)) \cap D_+(X_i)$. Thus we see by the correspondence between the radicals ideals of R_{ij} and the closed subsets of $\operatorname{Spec} R_{ij}$ that $I_i R_{ij} = I_j R_{ij}$ for all $i \neq j$. Note that closed subschemes of $\mathbb{P}^n_R$ correspond exactly to ideals $I_i \subset R_i$ (not necessarily radical) such that the just-stated correspondence holds.

Now set $I \subset R[x_0, \ldots, x_n]$ to be the graded ideal generated by homogeneous elements F of positive degree such that $F/X_i^{\deg F} \in I_i$ for $i = 0, \ldots, n$. If we denote $V_+(F) = \mathbb{P}^n_R \setminus D_+(F)$, this condition is equivalent to saying that $F \in I \iff Z \subset V_+(F)$.

Let $\mathfrak{p} \in \operatorname{Spec} R$ not in the image of Z under $\mathbb{P}^n_R \to \operatorname{Spec} R$. This implies that for all $i = 0, \ldots, n$, $(R_i/I_i)_\mathfrak{p}/\mathfrak{p}(R_i/I_i)_\mathfrak{p} = 0 = (R_i)_\mathfrak{p}/((I_i)_\mathfrak{p} + \mathfrak{p}(R_i)_\mathfrak{p})$, which in turn implies (by clearing denominators) that for all $i = 0, \ldots, n$, there exist $g_i \in R \setminus \mathfrak{p}$ such that $f_i \in I_i$,

$$g_i = f_i + \sum_i a_{i,t} + f_{i,t}$$

where $a_{i,t} \in \mathfrak{p}, f_{i,t} \in R_i$. By the second lemma below (and homogenizing) we find that

$$g_i x_i^N = F_i + \sum_i a_{i,t} F_{i,t}$$

with $F_i \in I_N$ and $F_{i,t} \in (R[X_0, \dots, X_n])_N$ where this notation denotes the Nth graded part of the objects. Then $X_i^N \in (I_N)_\mathfrak{p} + \mathfrak{p}(R[x_0, \dots, x_n]_N)_\mathfrak{p}$. Then $(R[x_0, \dots, x_n]_{(n+1)N})_\mathfrak{p} = (I_{(n+1)N})_\mathfrak{p} + \mathfrak{p}(R[X_0, \dots, X_n)]_{(n+1)N})_\mathfrak{p}$. The left hand side becomes $(R_\mathfrak{p}[X_0, \dots X_n])_{(n+1)N}$, which is finite and free as $R_\mathfrak{p}$-modules on the basis of the monomials. By Nakayama's lemma, we see that $(R[X_0, \dots, X_n]_{(n+1)N})_\mathfrak{p} = (I_{(n+1)N})_\mathfrak{p}$, which implies that $h_i X_i^{(n+1)N} \in I_{(n+1)N}$ for some $h_i \in R \setminus \mathfrak{p}$. Aside: this means that $Z \subset V_+(h_i X_i^{(n+1)N}) = V(h_i X_i)$ (uniquely). This in turn implies that the image of Z to $\operatorname{Spec} R$ is disjoint from $D(h_0) \cap \dots \cap D(h_n) = D(h_0 \cdots h_n)$ which is an open neighborhood of $\mathfrak{p}$. Hence $V_+(X_0) \cap \dots \cap V_+(X_n) = \varnothing$, and we are done. □

Lemma. *If $f \in R_i$ and the image of f is in $I_i R_{ij}$, then $X_j/X_i \cdot f \in I_i$.*

Proof. $f \in I_i R_{ij}$ means that f vanishes on $Z \cap D_+(X_i X_j)$. Then $X_i/X_j \cdot f$ vanishes on $Z \cap D_+(X_i X_j)$ and $V_+(X_j) \cap D_+(X_i) = V(X_j/X_i) \subset D_+(X_i) = \operatorname{Spec} R_i$. So X_j/X_i vanishes on $Z \cap D_+(X_i)$, so $X_j/X_i \cdot f \in I_i$. □

Lemma. *If F is homogeneous of positive degree, and $F/X_i^{\deg F} \in I_i$ for some i, then $X_i F \in I$.*

Proof. Immediate consequence of the lemma above. □