Lecture 20. Krull's height theorem and the principal ideal theorem

In the last lecture we defined, for a Noetherian local ring A with maximal ideal $\mathfrak{m}$ and residue field k, the minimal number of generators $\mu(A) = \dim_k \mathfrak{m}/\mathfrak{m}^2$ of $\mathfrak{m}$, and we saw that for the local ring of an affine variety V at a point $\mathbf{v}$ this is the dimension of the tangent space $T_{\mathbf{v}}V$.

Question: What is the relation between $\mu(A)$ and $\dim A$?

The answer will be given by the following important theorem of Krull, which we prove in this lecture and the next. It provides a lower estimate for the number of generators of an ideal in a Noetherian ring (and for the number of equations needed to describe an affine variety).

Theorem 6.18. *(Krull's height theorem) Let A be a Noetherian ring, and let $I = (a_1, \dots, a_r)$ be an ideal generated by r elements. Let $\mathfrak{p} \subset A$ be a prime ideal which is minimal (with respect to inclusion) among the prime ideals containing I. Then*

$$h(\mathfrak{p}) \leq r.$$

Corollary 6.19. *Let A be a Noetherian local ring with maximal ideal $\mathfrak{m}$. Then $\dim A \leq \mu(A)$. In particular, $\dim A$ is finite.*

Proof. Every chain of prime ideals of A can be extended to end at $\mathfrak{m}$, so $\dim A = h(\mathfrak{m})$, and $\mathfrak{m}$ is the only prime ideal containing $\mathfrak{m}$. So Theorem 6.18 applied to $I = \mathfrak{m} = (a_1, \dots, a_r)$ with $r = \mu(A)$ gives $\dim A = h(\mathfrak{m}) \leq \mu(A)$. □

Theorem 6.18 makes precise the intuition that each additional equation can decrease the dimension of the space of solutions by at most one. Note that one can give a lower bound for $\dim A$ by exhibiting a chain of prime ideals in A, but an upper bound is not straightforward to obtain from the definition. This is another reason why Theorem 6.18 is important.

Definition 6.20. *A Noetherian local ring A is said to be* **regular** *if $\dim A = \mu(A)$.*

▶ For a point $\mathbf{v} \in k^n$, the local ring $A = k[X_1, \dots, X_n]_{\mathfrak{m}_\mathbf{v}}$ is regular of dimension n. Indeed, $\mu(A) = n$, since $\mathfrak{m}_\mathbf{v}/\mathfrak{m}_\mathbf{v}^2$ has basis $X_1 - v_1, \dots, X_n - v_n$, and the chain of prime ideals $(0) \subsetneq (X_1 - v_1) \subsetneq (X_1 - v_1, X_2 - v_2) \subsetneq \dots \subsetneq \mathfrak{m}_\mathbf{v}$, whose quotients are polynomial rings, gives $h(\mathfrak{m}_\mathbf{v}) \geq n$, so $\dim A = n$ by Corollary 6.19. More generally, a point $\mathbf{v}$ of an affine variety V is called a **smooth point** if $\dim_k T_\mathbf{v}V = \dim k[V]_{\mathfrak{m}_\mathbf{v}}$, that is, if the local ring of V at $\mathbf{v}$ is regular. By Corollary 6.19, $\dim_k T_\mathbf{v}V \geq \dim k[V]_{\mathfrak{m}_\mathbf{v}}$ always, and the origin of the cusp in Figure 14 is not a smooth point.

An important theorem due to Auslander and Buchsbaum states that regular local rings are UFDs. Unfortunately, we do not have time to prove this result in this course; see [4], where you can also find a proof that the localisation $k[X_1, \dots, X_n]_\mathfrak{p}$ at any prime ideal $\mathfrak{p}$ is regular.

(These are applications of the homological methods in algebra, which we do not get into in this course.)

We now begin the proof of Theorem 6.18. The general case is obtained by induction on the number r of generators. The case $r = 1$ is the hardest part of the proof, and we state it separately.

Theorem 6.21. *(Krull's principal ideal theorem / Hauptidealsatz) Let A be a Noetherian ring, let $a \in A$ be a non-unit, and let $\mathfrak{p}$ be a prime ideal which is minimal among the prime ideals containing a. Then $h(\mathfrak{p}) \leq 1$.*

Proof. We may suppose that A is a local ring with maximal ideal $\mathfrak{p}$. Indeed, by Corollary 6.15(ii), the prime ideals of $A_\mathfrak{p}$ containing $\frac{a}{1}$ correspond to the prime ideals of A contained in $\mathfrak{p}$ and containing a, so $\mathfrak{p}A_\mathfrak{p}$ is minimal among the prime ideals of $A_\mathfrak{p}$ containing $\frac{a}{1}$, and $h(\mathfrak{p}) = \dim A_\mathfrak{p} = h(\mathfrak{p}A_\mathfrak{p})$.

So let A be local with maximal ideal $\mathfrak{p}$, and let $\mathfrak{q} \subsetneq \mathfrak{p}$ be a prime ideal. We want to show that $h(\mathfrak{q}) = 0$, that is, that there is no prime ideal $\mathfrak{r} \subsetneq \mathfrak{q}$, see Figure 15. Equivalently, $\mathfrak{q}A_\mathfrak{q}$ is the only prime ideal of the local ring $A_\mathfrak{q}$. Since $\sqrt{(0)}$ is the intersection of all prime ideals, it suffices to show that the maximal ideal $\mathfrak{q}A_\mathfrak{q}$ is nilpotent. Note that $a \notin \mathfrak{q}$, as $\mathfrak{p}$ is minimal among the prime ideals containing a, so $\frac{a}{1}$ is a unit in $A_\mathfrak{q}$.

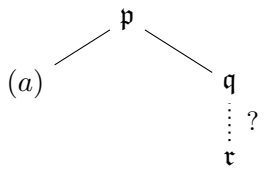

Figure 15: The ideals in the proof of Theorem 6.21: $\mathfrak{p}$ is minimal among the prime ideals containing (a), and $\mathfrak{q} \subsetneq \mathfrak{p}$ is a prime ideal. We have to show that no prime ideal $\mathfrak{r} \subsetneq \mathfrak{q}$ exists.

Let $\iota : A \to A_\mathfrak{q}$ be the localisation map, and let

$$\mathfrak{q}^{(n)} := \iota^{-1}(\mathfrak{q}^n A_\mathfrak{q}) = \{x \in A : xs \in \mathfrak{q}^n \text{ for some } s \in A \setminus \mathfrak{q}\}$$

be the n-th **symbolic power** of $\mathfrak{q}$; the second equality is Lemma 6.14(i). These form a chain of ideals $\mathfrak{q} = \mathfrak{q}^{(1)} \supset \mathfrak{q}^{(2)} \supset \dots$ in A, and by Lemma 6.14(i) we have $\mathfrak{q}^{(n)}A_\mathfrak{q} = \mathfrak{q}^n A_\mathfrak{q}$.

Step 1: $(a) + \mathfrak{q}^{(n)} = (a) + \mathfrak{q}^{(n+1)}$ for some n. The prime ideals of $A/(a)$ correspond to the prime ideals of A containing a, and $\mathfrak{p}$ is the only one of these, as A is local and $\mathfrak{p}$ is minimal over a. So $\dim A/(a) = 0$, and $A/(a)$ is Artinian by Theorem 6.8. Hence the chain of images of $(a) + \mathfrak{q}^{(1)} \supset (a) + \mathfrak{q}^{(2)} \supset \dots$ in $A/(a)$ becomes stationary, which gives the claim.

Step 2: $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)}$. Let $x \in \mathfrak{q}^{(n)}$. By Step 1, $x = ra + y$ with $r \in A$ and $y \in \mathfrak{q}^{(n+1)}$. Then $ra = x - y \in \mathfrak{q}^{(n)}$, so $\frac{r}{1}\frac{a}{1} \in \mathfrak{q}^n A_\mathfrak{q}$, and since $\frac{a}{1}$ is a unit, $\frac{r}{1} \in \mathfrak{q}^n A_\mathfrak{q}$, that is, $r \in \mathfrak{q}^{(n)}$. As $a \in \mathfrak{p}$, we get $x = ra + y \in \mathfrak{p}\mathfrak{q}^{(n)} + \mathfrak{q}^{(n+1)}$. This shows that

$$\mathfrak{q}^{(n)} = \mathfrak{p}\mathfrak{q}^{(n)} + \mathfrak{q}^{(n+1)}.$$

As A is Noetherian, $\mathfrak{q}^{(n)}$ is a finitely generated A-module, and Nakayama's lemma for the submodule $\mathfrak{q}^{(n+1)} \subset \mathfrak{q}^{(n)}$ gives $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)}$.

Step 3: $\mathfrak{q}A_\mathfrak{q}$ is nilpotent. By Step 2, $\mathfrak{q}^n A_\mathfrak{q} = \mathfrak{q}^{(n)} A_\mathfrak{q} = \mathfrak{q}^{(n+1)} A_\mathfrak{q} = \mathfrak{q}^{n+1} A_\mathfrak{q} = (\mathfrak{q}A_\mathfrak{q})(\mathfrak{q}^n A_\mathfrak{q})$. The ring $A_\mathfrak{q}$ is Noetherian by Lemma 6.14(i), so Nakayama's lemma for the $A_\mathfrak{q}$-module $\mathfrak{q}^n A_\mathfrak{q}$ gives $\mathfrak{q}^n A_\mathfrak{q} = \{0\}$. □

▶ Geometrically, let $f \in k[X_1, \ldots, X_n]$ be non-constant, with k algebraically closed. By the dictionary of Lecture 14, the irreducible components of the hypersurface $\mathcal{V}(f)$ are the sets $\mathcal{V}(\mathfrak{p})$, where $\mathfrak{p}$ runs over the minimal prime ideals containing f. The theorem says that each of these has $h(\mathfrak{p}) \leq 1$, and since $(0) \subsetneq \mathfrak{p}$, in fact $h(\mathfrak{p}) = 1$. Thus every irreducible component of a hypersurface has codimension one.

▶ If (a) is itself a prime ideal, so that $\mathfrak{p} = (a)$, the theorem has an elementary proof which avoids symbolic powers; see Problem 36 in the collection of problems. This special case suffices when A is a UFD, as in the previous remark: the prime ideals minimal over (a) are then generated by the irreducible factors of a. In general, however, $\mathfrak{p}$ need not be principal: on the cone with coordinate ring $k[X, Y, Z]/(XY - Z^2)$, the ideal (X, Z) of the line $X = Z = 0$ is minimal among the prime ideals containing X, but no single element generates it. We shall also need the theorem for a principal ideal which is not prime in the proof of Theorem 6.18.

▶ The symbolic powers also have a geometric meaning. Let k be algebraically closed, let $\mathfrak{q} \subset k[X_1, \ldots, X_n]$ be a prime ideal and $W = \mathcal{V}(\mathfrak{q})$. A polynomial g **vanishes to order at least** d at a point $\mathbf{v}$ if $g \in \mathfrak{m}_\mathbf{v}^d$, that is, if its Taylor expansion at $\mathbf{v}$ has no terms of degree less than d. A theorem of Zariski and Nagata[12] states that

$$\mathfrak{q}^{(d)} = \bigcap_{\mathbf{v} \in W} \mathfrak{m}_\mathbf{v}^d,$$

so $\mathfrak{q}^{(d)}$ consists of the polynomials which vanish to order at least d at every point of W. It contains $\mathfrak{q}^d$, the ideal generated by the products of d polynomials vanishing on W, but it can be larger, as the exercise on the curve (T^3, T^5, T^7) below shows. By definition, $g \in \mathfrak{q}^{(d)}$ means that $sg \in \mathfrak{q}^d$ for some polynomial s which does not vanish identically on W: thus g is a combination of such products near a general point of W, where we may divide by s, but possibly not near every point.

▶ Here is the picture behind the proof. After localising, we think of A as the ring of germs of functions at the point $P = \mathfrak{p}$, and the assumption on a says that the hypersurface $a = 0$ consists of the point P alone. The prime ideal $\mathfrak{q}$ corresponds to an irreducible closed set $W = \mathcal{V}(\mathfrak{q})$ through P, and we have to show that W is not contained in a larger irreducible closed set. To do so, we measure the room around W by the ideals $\mathfrak{q}^{(n)}$, which we think of as the functions vanishing to order at least n along W. If W were a line in a plane, say $\mathfrak{q} = (Y) \subset k[X, Y]$, then Y^n would vanish to order exactly n along W, and the chain $\mathfrak{q}^{(1)} \supset \mathfrak{q}^{(2)} \supset \ldots$ would never become stationary. The proof shows that in our situation it does.

[12] See D. Eisenbud, Commutative Algebra with a View Toward Algebraic Geometry, Springer, 1995, Theorem 3.14.

In Step 1, since the hypersurface $a = 0$ is a single point, the ring $A/(a)$ of functions on it is Artinian, so every descending chain of ideals in it becomes stationary: for large n, modulo a, vanishing to order n along W is the same as vanishing to order $n+1$. Step 2 extends this from the hypersurface to the whole space. If x vanishes to order n along W, then $x = ra + y$ with y vanishing to order $n+1$, and since a does not vanish identically on W, the factor r again vanishes to order n. Repeating the argument with r in place of x, we see that modulo $\mathfrak{q}^{(n+1)}$ the element x is divisible by every power of a. As a vanishes at P, Nakayama's lemma says that this is only possible if $x \in \mathfrak{q}^{(n+1)}$. In Step 3 we read the result at the generic point of W: there $\mathfrak{q}^n A_\mathfrak{q} = \mathfrak{q}^{n+1} A_\mathfrak{q}$, and this forces $\mathfrak{q}^n A_\mathfrak{q} = \{0\}$. So there is no room around W.

◁ Let $A = k[X,Y]/(XY)$ be the coordinate ring of two lines crossing at the origin, and let $\mathfrak{p} = (X,Y)$, $a = X + Y$ and $\mathfrak{q} = (X)$. Show that $\mathfrak{p}$ is the only prime ideal of A containing a, that $\mathfrak{q}^{(n)} = \mathfrak{q}$ for all $n \geq 1$, and that $\mathfrak{q}^n \neq \mathfrak{q}^{n+1}$ for all $n \geq 1$. Which step of the proof breaks down for the ordinary powers?

◁ Let $\mathfrak{p} = (X^4 - YZ, Y^2 - XZ, X^3Y - Z^2) \subset k[X,Y,Z]$. This is the kernel of the homomorphism $k[X,Y,Z] \to k[T]$ sending X, Y, Z to T^3, T^5, T^7, hence a prime ideal. Show that $\mathfrak{p}^{(2)} \neq \mathfrak{p}^2$.

Before we go on to the proof of Krull's height theorem, let us see an application of the principal ideal theorem.

Theorem 6.22. *Let $\mathfrak{p} \subset \mathfrak{q}$ be prime ideals in a Noetherian ring A. If there exists a prime ideal strictly between them, then there are infinitely many.*

Proof. The prime ideals between $\mathfrak{p}$ and $\mathfrak{q}$ correspond to the prime ideals between (0) and $\mathfrak{q}/\mathfrak{p}$ in the integral domain $A/\mathfrak{p}$, so we may suppose that A is an integral domain and $\mathfrak{p} = (0)$. Suppose for a contradiction that $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$, with $n \geq 1$, are the only prime ideals strictly between (0) and $\mathfrak{q}$. By prime avoidance (Proposition 2.9), $\mathfrak{q} \not\subset \mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_n$, so we can pick $a \in \mathfrak{q}$ with $a \notin \mathfrak{p}_i$ for all i. Then $\mathfrak{q}$ is minimal among the prime ideals containing a: such a prime ideal contained in $\mathfrak{q}$ is (0), one of the $\mathfrak{p}_i$, or $\mathfrak{q}$, and the first two do not contain a. By Theorem 6.21, $h(\mathfrak{q}) \leq 1$, contradicting the chain $(0) \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{q}$. □

▶ In $k[X,Y]$, the prime ideals strictly between (0) and (X,Y) are the ideals (f) with f irreducible and $f(0,0) = 0$, that is, the irreducible curves through the origin, see Figure 16.

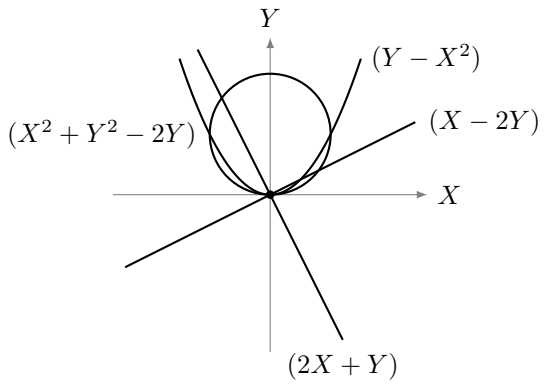

Figure 16: Some of the infinitely many prime ideals strictly between (0) and (X, Y) in $k[X, Y]$: the irreducible curves through the origin.

$\lhd$ Let A be a Noetherian ring with minimal prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$, so that $\sqrt{(0)} = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_s$ by Proposition 6.4. Show that every element of $\bigcup_{i=1}^{s} \mathfrak{p}_i$ is a zero-divisor. Deduce that, with the assumptions of Theorem 6.21, $h(\mathfrak{p}) = 1$ if a is not a zero-divisor.