Lecture 21. Proof of the height theorem; dimension of polynomial rings

Let us now turn to the proof of Krull's height theorem in general.

Proof. (of Theorem 6.18) We argue by induction on r. The case $r = 1$ is Theorem 6.21, so let $r \geq 2$ and assume the theorem for ideals generated by $r-1$ elements. Exactly as in the proof of Theorem 6.21, we may replace A by $A_{\mathfrak{p}}$ and I by $IA_{\mathfrak{p}} = (\frac{a_1}{1}, \ldots, \frac{a_r}{1})$, and assume that A is local with maximal ideal $\mathfrak{p}$. Then $\mathfrak{p}$ is the only prime ideal containing I.

Let $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_h = \mathfrak{p}$ be a chain of prime ideals with $h \geq 1$. We have to show that $h \leq r$. Since A is Noetherian, there is a prime ideal $\mathfrak{q}$ with $\mathfrak{p}_{h-1} \subset \mathfrak{q} \subsetneq \mathfrak{p}$ which is maximal among the prime ideals strictly contained in $\mathfrak{p}$, and $h(\mathfrak{q}) \geq h-1$. We shall find an ideal $I_1 \subset \mathfrak{q}$ generated by $r-1$ elements such that $\mathfrak{q}$ is minimal among the prime ideals containing I_1. The induction hypothesis then gives $h - 1 \leq h(\mathfrak{q}) \leq r-1$, as required.

Step 1: $\mathfrak{q}$ does not contain all of $a_1, \ldots, a_r$. Otherwise $I \subset \mathfrak{q} \subsetneq \mathfrak{p}$, contradicting the minimality of $\mathfrak{p}$. Renumbering, we may assume that $a_1 \notin \mathfrak{q}$.

Step 2: $\sqrt{(a_1) + \mathfrak{q}} = \mathfrak{p}$. A prime ideal containing $(a_1) + \mathfrak{q}$ contains $\mathfrak{q}$, is different from $\mathfrak{q}$ since $a_1 \notin \mathfrak{q}$, and is contained in the unique maximal ideal $\mathfrak{p}$; by the maximality of $\mathfrak{q}$ it is equal to $\mathfrak{p}$. So $\mathfrak{p}$ is the only prime ideal containing $(a_1) + \mathfrak{q}$, and the claim follows from Proposition 2.7. In particular, there is $N \geq 1$ such that $a_i^N \in (a_1) + \mathfrak{q}$ for all i, so that

$$a_i^N = a_1 x_i + y_i \text{ with } x_i \in A \text{ and } y_i \in \mathfrak{q}, \qquad i = 2, \ldots, r.$$

Let $I_1 \coloneqq (y_2, \ldots, y_r) \subset \mathfrak{q}$. The ideals introduced so far are shown in Figure 17.

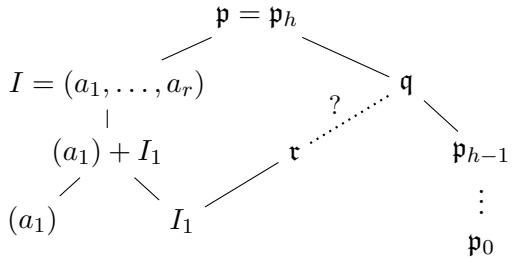

Figure 17: The ideals in the proof of Theorem 6.18, with inclusions going upwards. The prime ideal $\mathfrak{q}$ contains $\mathfrak{p}_{h-1}$, possibly with equality, and I_1, but not a_1. Step 3 shows that no prime ideal $\mathfrak{r}$ with $I_1 \subset \mathfrak{r} \subsetneq \mathfrak{q}$ exists.

Step 3: $\mathfrak{q}$ is minimal among the prime ideals containing I_1. Since $y_i = a_i^N - a_1 x_i$, we have $(a_1) + I_1 = (a_1, a_2^N, \ldots, a_r^N)$. A prime ideal containing this ideal contains $a_1, \ldots, a_r$, hence I, and is therefore equal to $\mathfrak{p}$. Now pass to the Noetherian ring $\overline{A} = A/I_1$, writing $\overline{x}$ and $\overline{\mathfrak{r}}$ for the

images of $x \in A$ and of an ideal $\mathfrak{r} \supset I_1$. The prime ideals of $\overline{A}$ are the $\overline{\mathfrak{r}}$ with $\mathfrak{r} \supset I_1$ prime, with inclusions preserved, and those containing $\overline{a}_1$ correspond to the prime ideals of A containing $(a_1) + I_1$. So $\overline{\mathfrak{p}}$ is the only prime ideal of $\overline{A}$ containing $\overline{a}_1$; in particular, $\overline{a}_1$ is a non-unit and $\overline{\mathfrak{p}}$ is minimal among the prime ideals containing it. By Theorem 6.21, $h(\overline{\mathfrak{p}}) \leq 1$. Since $\overline{\mathfrak{q}} \subsetneq \overline{\mathfrak{p}}$, this forces $h(\overline{\mathfrak{q}}) = 0$: there is no prime ideal $\mathfrak{r}$ with $I_1 \subset \mathfrak{r} \subsetneq \mathfrak{q}$, which is the claim. □

Theorem 6.18 has the following converse.

Theorem 6.23. *Let A be a Noetherian ring, and let $\mathfrak{p} \subset A$ be a prime ideal of height n. Then there exist $a_1, \ldots, a_n \in \mathfrak{p}$ such that $\mathfrak{p}$ is minimal among the prime ideals containing $(a_1, \ldots, a_n)$.*

Proof. We show by induction on i that, for $0 \leq i \leq n$, we can find $a_1, \ldots, a_i \in \mathfrak{p}$ such that every prime ideal containing $I_i \coloneqq (a_1, \ldots, a_i)$ has height at least i. For $i = 0$ we have $I_0 = (0)$, and there is nothing to show.

Let $1 \leq i \leq n$, and suppose that $a_1, \ldots, a_{i-1}$ have been found. We choose $a_i \in \mathfrak{p}$ outside all the prime ideals which are minimal among those containing I_{i-1}. To see that this is possible, note that by Proposition 6.4 there are only finitely many such prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$, and every prime ideal containing I_{i-1} contains one of them. Each $\mathfrak{q}_j$ has height at least $i - 1$ by the induction hypothesis, and at most $i - 1$ by Theorem 6.18. Thus $h(\mathfrak{q}_j) = i - 1 < n = h(\mathfrak{p})$, so that $\mathfrak{p} \not\subset \mathfrak{q}_j$ for every j, and prime avoidance (Proposition 2.9) gives an element $a_i \in \mathfrak{p}$ which lies in none of the $\mathfrak{q}_j$. Now let $\mathfrak{q}$ be a prime ideal containing $I_i = I_{i-1} + (a_i)$. Then $\mathfrak{q}$ contains some $\mathfrak{q}_j$, and $\mathfrak{q} \neq \mathfrak{q}_j$ because $a_i \in \mathfrak{q}$. Hence $h(\mathfrak{q}) \geq h(\mathfrak{q}_j) + 1 = i$.

Finally, let $\mathfrak{q}$ be a prime ideal with $(a_1, \ldots, a_n) \subset \mathfrak{q} \subset \mathfrak{p}$. By the case $i = n$, we have $h(\mathfrak{q}) \geq n = h(\mathfrak{p})$, which is impossible if $\mathfrak{q} \subsetneq \mathfrak{p}$. So $\mathfrak{q} = \mathfrak{p}$, as required. □

Since Theorem 6.18 is now proved, so is Corollary 6.19: a Noetherian local ring has finite dimension. Somewhat disturbingly, a Noetherian ring need not have finite dimension.

◁ (Nagata's example) Let $A = k[X_1, X_2, X_3, \ldots]$ be the polynomial ring in infinitely many variables, and let $m_1 < m_2 < \ldots$ be positive integers with $\lim_{i\to\infty}(m_{i+1} - m_i) = \infty$, for example $m_i = 2^i$. Let $\mathfrak{p}_i = (X_{m_i+1}, X_{m_i+2}, \ldots, X_{m_{i+1}})$, let $S = A \setminus \bigcup_i \mathfrak{p}_i$, and let $R = S^{-1}A$. Show that R is Noetherian, that its maximal ideals are the ideals $\mathfrak{m}_i = S^{-1}\mathfrak{p}_i$, and that $h(\mathfrak{m}_i) = m_{i+1} - m_i$. Thus $\dim R = \infty$. (See [3], Exercise 11.4.)

We can now compute the dimension of a polynomial ring, as promised in Lecture 17. When k is algebraically closed, the maximal ideals of $k[X_1, \ldots, X_n]$ are the ideals $(X_1 - a_1, \ldots, X_n - a_n)$ by the weak Nullstellensatz (Theorem 4.29); for an arbitrary field we need the following version of it.

Theorem 6.24. *(weak Nullstellensatz for an arbitrary field) Let k be an arbitrary field. Every maximal ideal $\mathfrak{m} \subset k[X_1, \ldots, X_n]$ is of the form*

$$\mathfrak{m} = (f_1, f_2, \ldots, f_n) \text{ with } f_i \in k[X_1, \ldots, X_i] = k[X_1, \ldots, X_{i-1}][X_i] \text{ monic in } X_i.$$

Proof. By Zariski's lemma (Lemma 4.30), the field $K = k[X_1, \ldots, X_n]/\mathfrak{m}$ is a finite extension of k. Let $\alpha_i = X_i + \mathfrak{m} \in K$, so that $K = k[\alpha_1, \ldots, \alpha_n]$, and for $0 \le i \le n$ let $K_i = k[\alpha_1, \ldots, \alpha_i] \subset K$. Each K_i is a field: it is a subring of the field K and a finite-dimensional k-vector space, so multiplication by a nonzero element of K_i is an injective, hence surjective, k-linear map $K_i \to K_i$. Let $g_i \in K_{i-1}[X_i]$ be the minimal polynomial of α_i over K_{i-1}. Its coefficients lie in $K_{i-1} = k[\alpha_1, \ldots, \alpha_{i-1}]$, so they are the values at $(\alpha_1, \ldots, \alpha_{i-1})$ of polynomials in $k[X_1, \ldots, X_{i-1}]$. Replacing each coefficient by such a polynomial, we obtain $f_i \in k[X_1, \ldots, X_i]$, monic in X_i, with $f_i(\alpha_1, \ldots, \alpha_{i-1}, X_i) = g_i$. Then $f_i(\alpha_1, \ldots, \alpha_i) = g_i(\alpha_i) = 0$, that is, $f_i \in \mathfrak{m}$.

It remains to show that $(f_1, \ldots, f_n) = \mathfrak{m}$. Since $(f_1, \ldots, f_n) \subset \mathfrak{m}$, it suffices to show that $(f_1, \ldots, f_n)$ is a maximal ideal, that is, that $k[X_1, \ldots, X_n]/(f_1, \ldots, f_n)$ is a field. We show by induction on i that $X_j \mapsto \alpha_j$ induces an isomorphism $k[X_1, \ldots, X_i]/(f_1, \ldots, f_i) \simeq K_i$. For $i = 0$ there is nothing to prove. For $i \ge 1$, the induction hypothesis gives

$$k[X_1, \ldots, X_i]/(f_1, \ldots, f_{i-1}) \simeq K_{i-1}[X_i],$$

under which f_i corresponds to $f_i(\alpha_1, \ldots, \alpha_{i-1}, X_i) = g_i$. Hence

$$k[X_1, \ldots, X_i]/(f_1, \ldots, f_i) \simeq K_{i-1}[X_i]/(g_i) \simeq K_{i-1}[\alpha_i] = K_i,$$

where the second isomorphism is evaluation at α_i, whose kernel is (g_i) because g_i is the minimal polynomial of α_i over K_{i-1}. □

Corollary 6.25. *For any field k,* $\dim k[X_1, \ldots, X_n] = n$.

Proof. Let $A = k[X_1, \ldots, X_n]$. The chain of prime ideals $(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq \ldots \subsetneq (X_1, \ldots, X_n)$ shows that $\dim A \ge n$, as we saw in Lecture 17. Conversely, every chain of prime ideals in A can be extended so that it ends at a maximal ideal, so $\dim A$ is the supremum of $h(\mathfrak{m})$ over the maximal ideals $\mathfrak{m}$ of A. By Theorem 6.24, or by Theorem 4.29 if k is algebraically closed, $\mathfrak{m}$ is generated by n elements, and it is trivially minimal among the prime ideals containing $\mathfrak{m}$. Hence $h(\mathfrak{m}) \le n$ by Theorem 6.18. □