Lecture 11. Noether normalisation

Let A be a k-algebra. We say that $a_1, \ldots, a_n \in A$ are **algebraically independent** over k if there is no non-zero polynomial $F \in k[X_1, \ldots, X_n]$ such that $F(a_1, \ldots, a_n) = 0$. This is equivalent to the injectivity of the homomorphism $k[X_1, \ldots, X_n] \to A$, $X_i \mapsto a_i$, that is, to $k[a_1, \ldots, a_n]$ being a polynomial ring in $a_1, \ldots, a_n$.

Theorem 4.25. *(Noether normalisation[6] lemma) Let A be a finitely generated k-algebra. Then there exist $d \geq 0$ and $a_1, \ldots, a_d \in A$ such that*

- *$a_1, \ldots, a_d$ are algebraically independent over k;*
- *A is integral over $k[a_1, \ldots, a_d]$.*

In other words, a finitely generated extension $k \subset A$ can be written as a composition

$$k \subset k[a_1, \ldots, a_d] \subset A$$

where the first extension is "free" (given by a polynomial algebra over k) and the second one is "finite" (finitely generated extension as a module).

$\lhd$ Find a polynomial subalgebra of $A = \mathbb{Q}[X, Y, Z]/(XY - Z^2)$ over which A is integral.

The proof rests on the following change of variables, which makes a given polynomial monic in X_n up to a non-zero constant. The linear change of variables is Noether's original argument and requires k to be infinite; the second is due to Nagata.

Lemma 4.26. *Let $0 \neq f \in k[X_1, \ldots, X_n]$. Then there exist $\phi_1, \ldots, \phi_{n-1} \in k[X_n]$ such that*

$$f(X_1 + \phi_1, \ldots, X_{n-1} + \phi_{n-1}, X_n) = cX_n^N + g_{N-1}X_n^{N-1} + \ldots + g_1 X_n + g_0$$

for some $N \geq 0$, $c \in k^\times$ and $g_j \in k[X_1, \ldots, X_{n-1}]$. If k is infinite, one can take $\phi_i = c_i X_n$ with $c_i \in k$; in general, one can take $\phi_i = X_n^{r_i}$ with $r_i \in \mathbb{N}$.

Proof. k infinite. Let $m = \deg f$ and let f_m be the homogeneous part of f of degree m. For a monomial X^α of degree j and $c_1, \ldots, c_{n-1} \in k$ we have

$$(X_1 + c_1 X_n)^{\alpha_1} \cdots (X_{n-1} + c_{n-1}X_n)^{\alpha_{n-1}} X_n^{\alpha_n} = c_1^{\alpha_1} \cdots c_{n-1}^{\alpha_{n-1}} X_n^j + (\text{terms of lower degree in } X_n).$$

Summing over the monomials of f, we get

$$f(X_1 + c_1 X_n, \ldots, X_{n-1} + c_{n-1}X_n, X_n) = f_m(c_1, \ldots, c_{n-1}, 1)X_n^m + (\text{terms of lower degree in } X_n),$$

so it suffices to choose the c_i with $f_m(c_1, \ldots, c_{n-1}, 1) \neq 0$. Since $f_m \neq 0$ is homogeneous, $f_m(X_1, \ldots, X_{n-1}, 1)$ is a non-zero polynomial (setting $X_n = 1$ sends distinct monomials of degree

[6] Although closely related, the usage of the word "normalisation" here does not agree with the normalisation defined above as the integral closure of an integral domain in its field of fractions. Both usages are standard.

m to distinct monomials); as k is infinite, it does not vanish at some point $(c_1, \ldots, c_{n-1}) \in k^{n-1}$ (see the exercise in Lecture 4).

General k. Write $f = \sum_\alpha a_\alpha X^\alpha$, choose an integer r larger than every exponent α_i occurring in f, and put $r_i = r^{n-i}$. For a monomial X^α we have

$$(X_1 + X_n^{r_1})^{\alpha_1} \cdots (X_{n-1} + X_n^{r_{n-1}})^{\alpha_{n-1}} X_n^{\alpha_n} = X_n^{N(\alpha)} + (\text{terms of lower degree in } X_n),$$

where $N(\alpha) = \alpha_1 r^{n-1} + \alpha_2 r^{n-2} + \ldots + \alpha_{n-1} r + \alpha_n$. Since $0 \le \alpha_i < r$, the α_i are the base-r digits of $N(\alpha)$, so distinct exponents α occurring in f have distinct $N(\alpha)$. Let β be the exponent occurring in f with $N(\beta)$ largest. Then $f(X_1 + X_n^{r_1}, \ldots, X_{n-1} + X_n^{r_{n-1}}, X_n) = a_\beta X_n^{N(\beta)} +$ (terms of lower degree in X_n), as required. □

Proof of Theorem 4.25. Write $A = k[x_1, \ldots, x_n]$ for some $x_i \in A$, and argue by induction on n. If $x_1, \ldots, x_n$ are algebraically independent over k, we take $d = n$ and $a_i = x_i$. Otherwise there is a non-zero $f \in k[X_1, \ldots, X_n]$ with $f(x_1, \ldots, x_n) = 0$. Take $\phi_1, \ldots, \phi_{n-1}$ as in Lemma 4.26, and put $y_i = x_i - \phi_i(x_n) \in A$ for $i = 1, \ldots, n-1$ and $B = k[y_1, \ldots, y_{n-1}]$. Then $x_i = y_i + \phi_i(x_n)$, so $A = B[x_n]$. Substituting $X_i = y_i$ for $i < n$ and $X_n = x_n$ in the identity of Lemma 4.26 gives

$$0 = f(x_1, \ldots, x_n) = c x_n^N + g_{N-1}(y) x_n^{N-1} + \ldots + g_0(y)$$

with $g_j(y) = g_j(y_1, \ldots, y_{n-1}) \in B$. Dividing by c, we see that x_n is integral over B, so $A = B[x_n]$ is integral over B by Corollary 4.23(a). By induction, B is integral over $k[a_1, \ldots, a_d]$ for some $a_1, \ldots, a_d \in B$ algebraically independent over k, and then so is A by Corollary 4.23(c). □

Although we do not give a proof here, it is helpful for the intuition to remark on the geometric meaning of Noether normalisation. Let $V \subset k^n$ be an affine variety and $A = k[X_1, \ldots, X_n]/\mathcal{I}(V)$ the finitely generated k-algebra of polynomial functions on V. Noether normalisation gives polynomial functions $a_1, \ldots, a_d \in A$ on V such that A is integral over the polynomial ring $k[a_1, \ldots, a_d]$. The corresponding map of varieties is $\pi : V \to k^d$, $p \mapsto (a_1(p), \ldots, a_d(p))$, and for k algebraically closed it is onto with finite fibres, as remarked in Lecture 10 (the proof uses Hilbert's Nullstellensatz as well as the lying-over theorem for integral extensions, which we will establish later in the course).

Here is how you can do Noether normalisation in Macaulay2:

```
loadPackage "NoetherNormalization"
R = ZZ/2[x,y]
I = ideal(x*y)
(f,J,X) = noetherNormalization I
-- The computations performed use a random linear change of coordinates.
-- This returns f an automorphism of R, J the image of I under f, and
-- X a list of variables which are algebraically independent in R/J.
-- In our example, we get f: x -> x+y, y -> x, J = x^2+xy, X = {y}
```

Thus, we see that $k[X,Y]/(XY) \simeq k[X,Y]/(X^2+XY)$ (via f) is an integral extension of $k[Y]$ obtained by adjoining X, which satisfies the monic equation $X^2+YX=0$.

◁ Show that an algebraically closed field k is infinite. (Suppose that k is finite with n elements and consider the polynomial $X^n - X + 1$.)

It can be shown that the number d that appeared in Noether normalisation lemma is equal to the maximal number of elements in A that are algebraically independent over k (see Corollary 4.28 that implies this when A is an integral domain, and the general case follows from this using Corollary 4.37). This is another way to measure the dimension as the following proposition shows.

Proposition 4.27. *Let $V \subset k^n$ be an affine variety, $I = \mathcal{I}(V)$ and $A = k[X_1,\dots,X_n]/I$ the co-ordinate ring of V. Then, the maximal number of algebraically independent elements in A is equal to* $\dim V = \deg HP_I(t)$.

Proof. Let $d = \dim V = \deg HP_I$. By Corollary 4.18, there exist $1 \le i_1 < \ldots < i_d \le n$ such that $I \cap k[X_{i_1},\dots,X_{i_d}] = \{0\}$. Denote by $\overline{\ }: k[X_1,\dots,X_n] \to A$ the canonical projection. Its restriction to $k[X_{i_1},\dots,X_{i_d}]$ is injective, so $\overline{X}_{i_1},\dots,\overline{X}_{i_d}$ are algebraically independent in A.

Conversely, let $\overline{f}_1,\dots,\overline{f}_e$ be algebraically independent elements of A, with $f_j \in k[X_1,\dots,X_n]$; we show that $e \le d$. Let $N \ge 1$ be at least the total degree of each f_j. For every $s \ge 0$ there is a k-linear map

$$k[Y_1,\dots,Y_e]_{\le s} \to k[X_1,\dots,X_n]_{\le Ns}/I_{\le Ns}, \qquad F \mapsto \overline{F(f_1,\dots,f_e)},$$

which is injective: if $F(f_1,\dots,f_e) \in I$, then $F(\overline{f}_1,\dots,\overline{f}_e) = 0$ in A, so $F = 0$ by algebraic independence. Therefore

$$\begin{aligned} HF_I(Ns) &= \dim_k\big(k[X_1,\dots,X_n]_{\le Ns}/I_{\le Ns}\big) \\ &\ge \dim_k k[Y_1,\dots,Y_e]_{\le s} = \binom{s+e}{e} = \frac{1}{e!}s^e + \dots \end{aligned}$$

For $s \ge s_0$ we have $HF_I(Ns) = HP_I(Ns)$ by Theorem 4.16, and this is a polynomial in s of degree d. Comparing with the right-hand side for large s, we get $d \ge e$. □

▶ Consider the k-algebra $A = k[X,Y,Z]/(XY,XZ)$ and let $x,y,z \in A$ be the classes of X,Y,Z. Both $\{x\}$ and $\{y,z\}$ are maximal algebraically independent subsets of A over k, that is, we cannot add elements to them keeping them algebraically independent. So, unlike in the case of field extensions, not all maximal algebraically independent subsets have the same cardinality.

We can remedy this by restricting attention to integral domains $A = k[X_1,\dots,X_n]/\mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal, with field of fractions $K = \mathrm{Frac}(A)$. Let $\{a_1,\dots,a_d\}$ be a maximal algebraically independent subset of A. By maximality, every $b \in A$ satisfies a non-zero relation $F(a_1,\dots,a_d,b) = 0$, and F must involve the last variable, so b is algebraic over $k(a_1,\dots,a_d)$. Hence in

$$k \subset k(a_1,\dots,a_d) \subset K$$

the first extension is purely transcendental and the second one is algebraic, that is, $\{a_1, \ldots, a_d\}$ is a transcendence basis of K over k. Recall that all transcendence bases of a field extension $k \subset K$ have the same cardinality, the transcendence degree $\mathrm{trdeg}_k K$. Therefore the cardinality of a maximal algebraically independent subset of A is well-defined and equal to $\mathrm{trdeg}_k K$. Combining this with Proposition 4.27 gives a field-theoretic characterisation of dimension.

Corollary 4.28. *Let $V \subset k^n$ be an affine variety, and suppose that $\mathfrak{p} = \mathcal{I}(V)$ is a prime ideal. Then* $\dim V$ *is equal to the transcendence degree of the field extension $k \subset \mathrm{Frac}(A)$, where $A = k[X_1, \ldots, X_n]/\mathfrak{p}$.*