Lecture IX: Noether Normalization

§1. Noether Normalization:

The statement has many incarnations. We choose the ones that are more interesting for concrete computations (ie, ones where we know how to build $y_1,\dots,y_k$). The Theorem is valid for general fields $\mathbb{K}$.

Theorem 1 (Noether Normalization): Let $\mathbb{K}$ be a field and A a finitely generated $\mathbb{K}$-algebra. Say $A = \mathbb{K}[X_1\dots X_n]/I = \mathbb{K}[x_1,\dots,x_n]$. Assume A is a domain.
Then $\exists\, r = 0,\dots,n$ & $u_1,\dots,u_r \in A$ algebraically independent over $\mathbb{K}$ such that A is integral over $\mathbb{K}[u_1,\dots,u_r]$. Moreover, $r = \operatorname{Trdeg}_{\mathbb{K}}(\operatorname{Quot}(A))$

(Recall: $r \in A$ is integral over S if $\exists\, f \in S[z]$ monic with $f(r) = 0$.)

Proof: • If $\{x_1,\dots,x_n\}$ are alg. indep over $\mathbb{K}$, the result is clear since

$$\operatorname{Quot}(A) = \mathbb{K}(x_1,\dots,x_n)$$

& every element of $\operatorname{Quot}(A)$ is algebraic over $\mathbb{K}$, hence integral over $\mathbb{K}[y_1,\dots,y_n]$.

• Otherwise, we proceed by induction on n.

• Base case: $n = 0$ The result is clear since $A = \mathbb{K}$

• Inductive Step: Pick $n > 0$ & an algebraic dependency relation among $x_1,\dots,x_n$.

$$(*)\quad g(\underline{x}) = \sum_{\underline{\alpha}} a_{\underline{\alpha}}\, x_1^{\alpha_1}\cdots x_n^{\alpha_n} = 0 \qquad \text{with } a_{\underline{\alpha}} \in \mathbb{K}\smallsetminus\{0\}$$

IDEA: If $\exists\, i = 1,\dots,n$ such that $LT_{x_i}(g) \in \mathbb{K}$ (ie the largest monomial in x_i-variable in g is a pure power of x_i), then $\frac{1}{LT_{x_i}(g)}\cdot g \in \mathbb{K}[x_1,\dots x_n]$ is monic in x_i & so x_i is integral over $\mathbb{K}[x_1,\dots,\hat{x}_i\dots x_n]$

$$\begin{array}{ll}
A = \tilde{A}[x_i] & \\
\quad | & \Big\}\ \text{integral} \\
\tilde{A} = \mathbb{K}[x_1,\dots,\hat{x}_i,\dots x_n] & \quad \text{domain \& f.g } \mathbb{K}\text{-algebra} \\
\quad | & \\
\quad \mathbb{K} &
\end{array}$$

The inductive step on $\tilde{A}$ will produce $\{u_1, \dots u_r\} \in \tilde{A}$ algebraically independent with

$$\begin{array}{c} A \\ | \\ \tilde{A} \\ | \\ \mathbb{K}[u_1, \dots u_r] \\ | \\ \mathbb{K} \end{array} \quad \Big] \text{ integral}$$

So $A \mid \mathbb{K}[u_1, \dots u_r]$ becomes integral by the transitivity of integral extensions.

- If no such x_i exists, we'll need to do a change of coordinates to achieve this. (not necessarily linear!)

Consider $\underline{m} = (1, m_2, \dots, m_n)$ & set $y_j = x_j - x_1^{m_j}$ for $j > 1$

Substitute $x_j = y_j + x_1^{m_j}$ in $(*)$ By construction $\underline{x}^{\underline{\alpha}} := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ becomes

$x_1^{\underline{\alpha} \cdot \underline{m}}$ + polynomial with no pure power in x_1. & with all monomials of $\deg_{x_1} < \underline{\alpha} \cdot \underline{m}$.

Expanding the relation in $\mathbb{K}[y_2, \dots y_n][x_1]$ we get:

$$g(x_1) := \sum_{\underline{\alpha}} a_{\underline{\alpha}} \, x_1^{\underline{\alpha} \cdot \underline{m}} + f(x_1, y_2, \dots, y_n) = 0 \in \mathbb{K}[y_2, \dots y_n][x_1]$$

where no monomial in f is a pure power of x_1. Furthermore, by construction, we have $\boxed{\deg_{x_1}(f) < \deg_{x_1}(g)}$ if the expected degree of $g - f$ is attained. We will achieve this if no terms in $g - f$ cancel out. We need to pick suitable $\underline{m}$ for this to happen.

- Next, we pick $d \gg 1$ (for example, $d > \|\underline{\alpha}\|_\infty$ with $a_{\underline{\alpha}} \neq 0$) & set $m_j = d^{j-1}$ for $j > 1$ If so: $\underline{\alpha} \cdot \underline{m} \xleftrightarrow{1\text{-to-}1} \underline{\alpha}$ via writing $\underline{\alpha} \cdot \underline{m}$ in base d.

This choice ensures that $\sum_{\underline{\alpha}} a_{\underline{\alpha}} \, x_1^{\underline{\alpha} \cdot \underline{m}} \not\equiv 0$ in $\mathbb{K}[x_1]$ The degree constraints $\boxed{}$ allow us to find $c \in \mathbb{K} \setminus \{0\}$ where $c \cdot g(x) \in \mathbb{K}[y_2 \dots y_r][x]$ is monic in x & $c\,g(x_1) = 0$. Thus, x_1 is integral over $\mathbb{K}[y_2, \dots y_n]$.

- Since $A = \mathbb{K}[x_2, \dots x_n][x_1] = \mathbb{K}[x_1, y_2, \dots, y_n]$ because $x_j - (y_j + x_1^{m_j}) = 0$ for $j > 1$

we conclude that $A = \mathbb{K}[x_1, \dots, x_n]$ is integral over $\mathbb{K}[y_2, \dots, y_n]$.

$$\begin{array}{ll} A = \mathbb{K}[y_2, \dots, y_n][x_1] & \\ \quad | & \Big] \text{ integral} \\ \mathbb{K}[y_2, \dots, y_n] & \text{domain} \\ & \text{fg } \mathbb{K}\text{-algebra} \\ \quad | & \\ \mathbb{K} & \end{array}$$

By inductive hypothesis, we can find $\{u_1, \dots, u_r\}$ alg indep over $\mathbb{K}$ with

$$\begin{array}{ll} \mathbb{K}[y_2, \dots, y_n] & \\ \quad | & \Big] \text{ integral} \\ \mathbb{K}[u_1, \dots, u_r] & \\ \quad | & \\ \mathbb{K} & \end{array}$$

By transitivity of integral extensions, we conclude A is integral over $\mathbb{K}[u_1, \dots u_r]$.

From
$$\begin{array}{ll} \mathrm{Quot}(A) & \\ \quad | & \Big] \text{ algebraic} \\ \mathbb{K}(u_1, \dots, u_r) & \\ \quad | & \Big] \text{ tr deg } r \\ \mathbb{K} & \end{array}$$
, we conclude that $r = \mathrm{tr\,deg}_{\mathbb{K}} \mathrm{Quot}(A)$.

Remark: The proof gives us an algorithm for computing $\{u_1 \dots u_r\}$ in "Noether position"

- If $\{x_1, \dots, x_n\}$ are algebraically independent over $\mathbb{K}$, we take $u_i = x_i$ for all i.
- Otherwise, up to reordering of the variables $x_1, \dots, x_n$ we can write $y_1 = x_1$ & $y_i = x_i - x_n^{d^i}$ for $i = 2, \dots, r$ for suitable $d \gg 0$
  The d will be determined from the algebraic relation among $x_1, \dots x_n$.
- Recursion will give $u_1, \dots, u_r$.

The following lemma is due to Noether & simplifies the construction of $\{u_1, \dots, u_r\}$ in "Noether position" when $\mathbb{K}$ is infinite.

Lemma 1: If $\mathbb{K}$ is infinite, we can take $u_1, \dots, u_r$ to be $\mathbb{K}$-linear combinations of $x_1, \dots, x_n$. (a generic one will do)

Proof: It's enough to discuss the case where $\{x_1, \dots, x_n\}$ are algebraically dep.

We proceed by induction on $n \geq 1$, starting from the non-trivial relation:

$$(*) \qquad \sum_{\underline{\alpha}} a_{\underline{\alpha}} \, x_1^{\alpha_1} \cdots x_n^{\alpha_n} = 0 \qquad \text{with } a_{\underline{\alpha}} \in \mathbb{K} \setminus \{0\}$$

- **Base case:** $n = 1$ $\quad A = \mathbb{K}[x_1]$ is integral over $\mathbb{K}$ $\quad \{u_1, \dots, u_r\} = \emptyset$.

- **Inductive Step:** Pick $n > 1$ & set $y_i = x_i - \underset{\mathbb{K}^* \text{ (to be determined)}}{b_i} x_1$ for $i = 2, \dots, n$

Substituting $x_i = y_i + b_i x_1$ in $(*)$ we get

$$g(x_1) = c_d(b_2, \dots, b_n)\, x_1^d + \sum_{j=0}^{d-1} c_j(b_2, \dots, b_n, y_2, \dots, y_n)\, x_1^j \in \mathbb{K}[y_1, \dots, y_n][X_1]$$

where $d = \max \|\alpha\|_1$

By construction $c_d(b_2, \dots, b_n) = \sum_{\|\alpha\|_1 = d} a_{\underline{\alpha}} \, b_2^{\alpha_1} \cdots b_n^{\alpha_n} \neq 0$ in $\mathbb{K}[b_2, \dots, b_n]$

Since $\mathbb{K}$ is infinite, we can find $b_2, \dots, b_n \in \mathbb{A}^{n-1}_{\mathbb{K}}$ with $c = c_d(b_2, \dots, b_n) \neq 0$ in $\mathbb{K}$

It follows that $c^{-1} g_{(X)} \in \mathbb{K}[y_2, \dots, y_n][X]$ is monic in X & vanishes on x_1.

Then
$$\begin{tikzcd} A \arrow[d, dash, "\text{integral domain}"] \\ \mathbb{K}[y_2, \dots, y_n] \arrow[d, dash] \\ \mathbb{K} \end{tikzcd}$$

By inductive hypothesis $\exists\, u_1, \dots, u_r$ $\mathbb{K}$-linear combinations of $y_2, \dots, y_n$ with

$$\begin{tikzcd} \mathbb{K}[y_2, \dots, y_n] \arrow[d, dash, "\text{integral}"] \\ \mathbb{K}[u_1, \dots, u_r] \arrow[d, dash] \\ \mathbb{K} \end{tikzcd}$$

& $\{u_1, \dots, u_r\}$ alg. indep over $\mathbb{K}$

$\Rightarrow \{u_1, \dots, u_r\}$ are $\mathbb{K}$-linear combinations of $x_1, \dots, x_n$ & A is integral over $\mathbb{K}[u_1, \dots, u_r]$ as we wanted. $\square$

Remark: A generic $\mathbb{K}$-linear combination will suffice since the coefficients must lie outside a finite set of hypersurfaces (eg $b_2, \dots, b_n$ must lie outside $V(c_d)$).

Example: $A = \mathbb{K}[x,y]/(y^2-x^3-ax-b)$ for $a,b \in \mathbb{K}\setminus\{0\}$. We assume char $\mathbb{K} \neq 2,3$.

Then, A is an integral domain & $\mathrm{Quot}(A)$ is the function field of the elliptic curve $V(y^2-x^3-ax-b) \subseteq \mathbb{A}^2_{\mathbb{K}}$. $\mathrm{Trdeg}_{\mathbb{K}} \mathrm{Quot}(A) = 1$.

For the Noether position, we can take
1. $\{x\}$ or $\{y\}$,
2. $\{y+x^d\}$ for $d \gg 1$
3. $\{y+cx\}$ for c generic

Note: y is integral over $\mathbb{K}[x]$ & $[\mathrm{Quot}(A), \mathbb{K}(x)] = 2$
x ——— $\mathbb{K}[y]$ & $[\mathrm{Quot}(A), \mathbb{K}(y)] = 3$

- For 2: $\{x, \tilde{y} = y + x^d\}$ so $(\tilde{y}-x^d)^2 - x^3 - ax - b = \tilde{y}^2 + x^{2d} - 2x\tilde{y} - x^3 - ax - b$
says $x^{2d} - x^3 - ax - b + (\tilde{y}^2 - 2x\tilde{y}) = 0$ so x is integral over $\mathbb{K}[\tilde{y}]$.
$\Rightarrow u_1 = \tilde{y} = y + x^d$ work for any $d > 3$.

- For 3: $\{x, \tilde{y} = y + cx\}$ so $(\tilde{y}-cx)^2 - x^3 - ax - b = c^2x^2 - x^3 - ax - b + (\tilde{y}^2 - 2cx)$
says $-x^3 + c^2x^2 - ax - b + (\tilde{y}^2 - 2cx) = 0$ so x is integral over $\mathbb{K}[\tilde{y}]$
Here, $LT_x = -1$ is never 0. so any $c \in \mathbb{K}$ works.

$\Rightarrow u_1 = \tilde{y} = y + cx$ works for any $c \in \mathbb{K}$.