

Lecture IX: Noether Normalization

§ 1. Noether Normalization:

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

Theorem 1 (Noether Normalization): Let K be a field and A a finitely generated K -algebra. Say $A = K[x_1, \dots, x_n] / \mathcal{I} = K[x_1, \dots, x_n]$. Assume A is a domain.

Then $\exists r = 0, \dots, n$ & $u_1, \dots, u_r \in A$ algebraically independent over K such that A is integral over $K[u_1, \dots, u_r]$. Moreover, $r = \text{tr deg}_K(\text{Quot}(A))$
 (Recall: $f \in A$ 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 K , the result is clear since

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

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

• Otherwise, we proceed by induction on n .

• Base case: $n = 0$ The result is clear since $A = K$

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

$$(*) \quad g_{(x_j)} = \sum_{\alpha} a_{\alpha} x_1^{\alpha_1} \dots x_n^{\alpha_n} = 0 \quad \text{with } a_{\alpha} \in K \setminus \{0\}$$

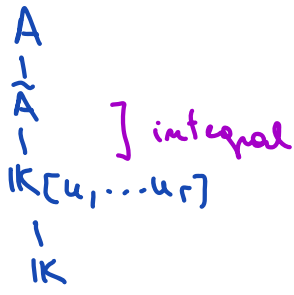
IDEA: If $\exists i = 1, \dots, n$ such that $\text{LT}_{x_i}(g) \in K$ (ie the largest

monomial in x_i -variable in g is a pure power of x_i), then $\frac{1}{\text{LT}_{x_i}(g)} \cdot g \in K[x_1, \dots, x_n]$

is monic in x_i & so x_i is integral over $K[x_1, \dots, \hat{x}_i, \dots, x_n]$

$$\begin{array}{c} A = \tilde{A}[x_i] \\ | \\ \tilde{A} = K[x_1, \dots, \hat{x}_i, \dots, x_n] \\ | \\ K \end{array} \left. \begin{array}{l} \\ \\ \end{array} \right\} \text{integral domain \& f.g. } K\text{-algebra}$$

The inductive step on \tilde{A} will produce $\{u_1, \dots, u_r\} \in \tilde{A}$ algebraically independent with A integral over $K[u_1, \dots, u_r]$. So $A | K[u_1, \dots, u_r]$ 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 $\underline{m} = (m_1, m_2, \dots, m_n)$ & set $y_j = x_j - x_1^{m_j}$ for $j > 1$

Substitute $x_j = y_j + x_1^{m_j}$ in (*) By construction $\underline{x} := x_1^{\underline{\alpha}} \dots x_n^{\underline{\alpha}}$ 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 $K[y_2, \dots, y_n][x_1]$ we get:

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

where no monomial in f is a pure power of x_1 . Furthermore, by construction, we have $\deg_{x_1}(f) < \deg_{x_1}(g)$ 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 $\sum_{\underline{\alpha}} a_{\underline{\alpha}} x_1^{\underline{\alpha} \cdot \underline{m}} \neq 0$ in $K[x_1]$. The degree constraints \square allow us to find $c \in K \setminus \{0\}$ where $c \cdot g(x) \in K[y_2, \dots, y_n][x]$ is monic in x & $c \cdot g(x) = 0$. Thus, x_1 is integral over $K[y_2, \dots, y_n]$.

• Since $A = K[x_2, \dots, x_n][x_1] = K[x_1, y_2, \dots, y_n]$ 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 $\mathbb{K}[y_2, \dots, y_n]$.

$$\begin{array}{c} A = \mathbb{K}[y_2, \dots, y_n][x_1] \\ | \\ \mathbb{K}[y_2, \dots, y_n] \\ | \\ \mathbb{K} \end{array} \left. \begin{array}{l} \text{domain} \\ \text{fg } \mathbb{K}\text{-algebra} \end{array} \right\} \text{integral}$$

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

$$\begin{array}{c} \mathbb{K}[y_2, \dots, y_n] \\ | \\ \mathbb{K}[u_1, \dots, u_r] \\ | \\ \mathbb{K} \end{array} \left. \right\} \text{integral}$$

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

From $\begin{array}{c} \text{Quot}(A) \\ | \\ \mathbb{K}(u_1, \dots, u_r) \\ | \\ \mathbb{K} \end{array} \left. \begin{array}{l} \text{algebraic} \\ \text{tr deg } r \end{array} \right\}$, we conclude that $r = \text{tr deg}_{\mathbb{K}} \text{Quot}(A)$.

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 $d_i > 0$

The d_i 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:

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

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

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

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

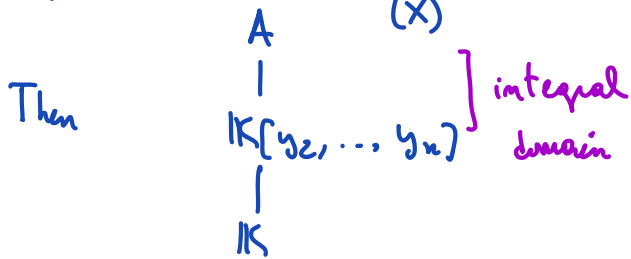
$$g(x_1) = c_d(b_2, \dots, b_n) x_1^d + \sum_{j=0}^{d-1} c_j(b_2, \dots, b_n, y_2, \dots, y_n) x_1^j \in \mathbb{K}[y_2, \dots, y_n][x_1]$$

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

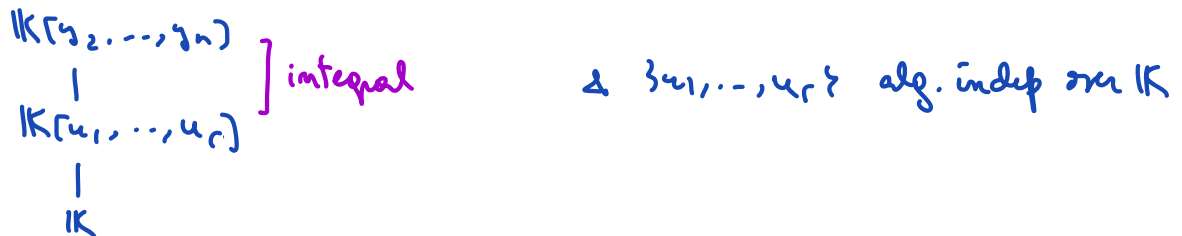
By construction $c_d(b_2, \dots, b_n) = \sum_{\|\alpha\|_1=d} a_{\underline{\alpha}} b_2^{\alpha_2} \dots b_n^{\alpha_n} \neq 0$ in $\mathbb{K}[b_2, \dots, b_n]$

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

It follows that $c^{-1}g \in \mathbb{K}[y_2, \dots, y_n][x]$ is monic in x & vanishes in x_1 .



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



$\Rightarrow \{u_1, \dots, u_r\}$ 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 $\text{char } \mathbb{K} \neq 2, 3$.

Then, A is an integral domain & $\text{Quot}(A)$ is the function field of the elliptic curve

$$V(y^2 - x^3 - ax - b) \subseteq \mathbb{A}_{\mathbb{K}}^2. \quad \text{Tr deg}_{\mathbb{K}} \text{Quot}(A) = 1.$$

For the Noether position, we can take ① $\{x, t\} \rightsquigarrow \{y, t\}$,

$$\text{② } \{y + x^d\} \text{ for } d \gg 1$$

$$\text{③ } \{y + cx\} \text{ for } c \text{ generic}$$

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

• 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, $\text{LT}_x = -1$ is non 0. so any $c \in \mathbb{K}$ works.

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