NOTHER NORMALIZATION AND HILBERT'S NULLSTELLENSTAZ

ZHAN JIANG

CONTENTS

1. NOETHER NORMALIZATION THEOREM

Lemma 1.1. *Let D be a domain and $f \in D[x_1, ..., x_n]$. Let $N \geq 1$ be an integer that bounds all the exponents of x_i's in f. Let ϕ be the automorphism:*

$$\begin{aligned} D[x_1, ..., x_n] &\to D[x_1, ..., x_n] \\ x_1 &\mapsto x_1 + x_n^N \\ x_2 &\mapsto x_1 + x_n^{N^2} \\ &\cdots\cdots \\ x_{n-1} &\mapsto x_1 + x_n^{N^{n-1}} \\ x_n &\mapsto x_n \end{aligned}$$

Then the image $\phi(f)$ is a polynomial whose highest degree term involving x_n has the form cx_n^m, where c is a nonzero element of D.

Proof. Consider any nonzero term of f, which has the form $c_\alpha x_1^{\alpha_1}, ..., x_n^{\alpha_n}$ where $\alpha = (\alpha_1, ..., \alpha_n)$ and c_α is a nonzero element in D.

The image of this term under ϕ is

$$c_\alpha(x_1 + x_n^N)^{\alpha_1}(x_2 + x_n^{N^2})^{\alpha_2} \cdots (x_{n-1} + x_n^{N^{n-1}})^{\alpha_{n-1}} x_n^{\alpha_n}$$

and this contains a unique highest degree term: it is the product of the highest degree terms coming from all the factors, and it is

$$c_\alpha(x_n^N)^{\alpha_1}(x_n^{N^2})^{\alpha_2} \cdots (x_n^{N^{n-1}})^{\alpha_{n-1}} x_n^{\alpha_n} = c_\alpha x_n^{\alpha_n + \alpha_1 N + \alpha_2 N^2 + \cdots + \alpha_{n-1} N^{n-1}}$$

The exponents that one gets on x_n in these largest degree terms coming from distinct terms of f are all distinct, because of uniqueness of representation of integers in base N. Thus no two exponents are the same and no two of them can cancel. □

Let R be an A-algebra and $z_1, ..., z_d \in R$. We shall say that the elements $z_1, ..., z_d$ are algebraically independent over A if the monomials $z_1^{a_1}, ..., z_d^{a_d}$ as $(a_1, ..., a_d)$ varies in $\mathbb{N}^d$ are all distinct and span a free A-submodule of R.

Theorem 1.2 (Noether normalization theorem)**.** *Let D be an integral domain and let R be any finitely generated D-algebra which is an algebra extension of D. Then there is some element $c \neq 0$ in D and elements $z_1, ..., z_d$ in R_c algebraically independent over D_c such that R_c is module-finite over the subring $D_c[z_1, ..., z_d]$.*

Proof. We use induction on the number n of generators of R over D. If $n = 0$, then $R = D$ and we can choose $d = 0$. Now assume that $R = D[\theta_1, ..., \theta_n]$ has n generators. If all the θ_i are algebraically independent over K then we're done. Therefore we may assume that there is a relation $f(\theta_1, ..., \theta_n) = 0$. Apply the automorphism ϕ from Lemma 1.1 and localize at one element we see that $\phi(f) = g$ is monic in θ_n. So θ_n is algebraic over $R' = D_c[\theta_1, ..., \theta_{n-1}]$. But R' is generated by one fewer elements over D_c so by induction hypothesis we can localize at on more element b making R'_b module-finite over $D_{bc}[x_1, ..., x_z[d]]$ for some d. Hence R_{bc} is module-finite over $D_{bc}[z_1, ..., z_d]$ as well. □

Corollary 1.3 (Zariski's Lemma). *Let R be a finitely generated algebra over a field K and suppose that R is a field. Then R is a finite algebraic extension of K.*

Proof. By the Noetherian normalization theorem, R is module-finite over $K[z_1, ..., z_d]$, which is of Krull dimension d. Since R is a field, $d = 0$ and R is module-finite over K. □

Corollary 1.4. *Let K be algebraically closed field, let R be a finitely generated K-algebra. Let m be a maximal ideal of R. Then the composite map $K \to R \twoheadrightarrow R/m$ is an isomorphism*

2. Hilbert's Nullstellensatz

From now on we always assume that K is algebraically closed, and $R = K[x_1, ..., x_n]$ is the polynomial ring over K.

Corollary 2.1 (1st weak form). *Every maximal ideal m of R is of the form $(x_1 - \lambda_1, ..., x_n - \lambda_n)$.*

Proof. Since $R/m \cong K$ for any maximal ideal m, it must be of the form $(x_1 - \lambda_1, ..., x_n - \lambda_n)$. □

Corollary 2.2 (2nd weak form). *Let $f_1, ..., f_l$ be polynomials in R, then the f_i's generate the unit ideal iff the algebraic set $V(f_1, ..., f_l) = \emptyset$.*

Theorem 2.3 (Hilbert's Nullstellensatz, strong form). *In the polynomial ring R, for any ideal $I \subseteq R$, we have*

$$\sqrt{I} = \bigcap_{I \subseteq m \text{ maximal ideal}} m$$

Proof. The $\subseteq$ is obvious, for the other direction, we use a proof called Rabinowitsch's trick: Let $f_1, ..., f_h$ be a set of generators of I and let g be in the other side. Introduce an extra variable z and consider the polynomials $f_1, ..., f_h, 1 - gz \in K[x_1, ..., x_n, z]$. For any point $(y_1, ..., y_{n+1})$ in K^{n+1}, if all polynomials vanish at that point, then all f_i vanish at $(y_1, ..., y_n)$, which implies that $1 - gz$ is $1 - 0$ at that point in K^{n+1}, contradiction! So they generates a unit ideal in $K[n_1, ..., n_, z]$. So we have

$$1 = H_1(z)f_1 + \cdots + H_n(z)f_n + H(z)(1 - gz)$$

where $H_1(z), ..., H_n(z), H(z)$ are polynomials in $K[n_1, ..., n_, z]$. Now we can assign $\frac{1}{g}$ to z and clear the denominators, we have

$$g^N = G_1 f_1 + \cdots + G_n f_n$$

where G_i's are polynomials in $K[x_1, ..., x_n]$. So $g \in \sqrt{I}$. □

Corollary 2.4. *Let $R \to S$ be a homomorphism of finitely generated K-algebras, then every maximal ideal of S contracts to a maximal ideal of R.*

Proof. Suppose that $m \subseteq S$ contracts to $P \subseteq R$, then we have $K \subseteq R/P \subseteq S/m$ where S/m is a module-finite extension of K. So R/P is also a module-finite extension of K, hence P is an maximal ideal. □