Course 311: Hilary Term 2006
Part V: Hilbert's Nullstellensatz

D. R. Wilkins

Contents

5 Hilbert's Nullstellensatz

5.1 Commutative Algebras of Finite Type

Definition Let K be a field. A unital ring R is said to be a *K-algebra* if $K \subset R$, the multiplicative identity elements of K and R coincide, and $ab = ba$ for all $a \in K$ and $b \in R$.

It follows from this definition that a unital commutative ring R is a K-algebra if $K \subset R$ and K and R have the same multiplicative identity element. Note that if $L\colon K$ is a field extension, then the field L is a unital K-algebra.

Definition Let K be a field, and let R_1 and R_2 be K-algebras. A ring homomorphism $\varphi\colon R_1 \to R_2$ is said to be a K-homomorphism if $\varphi(k) = k$ for all $k \in K$.

Given any subset A of a unital commutative K-algebra R, we denote by $K[A]$ the subring of R generated by $K \cup A$ (i.e., the smallest subring of R containing $K \cup A$). In particular, if $a_1, a_2, \ldots, a_k$ are elements of R then we denote by $K[a_1, a_2, \ldots, a_k]$ the subring of R generated by $K \cup \{a_1, a_2, \ldots, a_k\}$. If $R = K[A]$ then we say that the set A *generates* the K-algebra R.

Note that any element of $K[a_1, a_2, \ldots, a_k]$ is of the form $f(a_1, a_2, \ldots, a_k)$ for some polynomial f in k independent indeterminates with coefficients in K. Indeed the set of elements of R that are of this form is a subring of R, and is clearly the smallest subring of R containing $K \cup \{a_1, a_2, \ldots, a_k\}$.

Definition Let K be a field. A unital commutative ring R is said to be a *K-algebra of finite type* if $K \subset R$, the identity elements of K and R coincide, and there exists a finite subset $a_1, a_2, \ldots, a_k$ of R such that $R = K[a_1, a_2, \ldots, a_k]$.

Lemma 5.1 *Let K be a field. Then every K-algebra of finite type is a Noetherian ring.*

Proof Let R be a K-algebra of finite type. Then there exist $a_1, a_2, \ldots, a_k \in R$ such that $R = K[a_1, a_2, \ldots, a_k]$. Now it follows from the Hilbert Basis Theorem that the ring $K[x_1, x_2, \ldots, x_k]$ of polynomials in the independent indeterminates $x_1, x_2, \ldots, x_k$ with coefficients in K is a Noetherian ring (see Corollary 3.25). Moreover $R \cong K[x_1, x_2, \ldots, x_k]/\mathfrak{a}$, where $\mathfrak{a}$ is the kernel of the homomorphism

$$\varepsilon\colon K[x_1, x_2, \ldots, x_k] \to R$$

that sends $f \in K[x_1, x_2, \ldots, x_k]$ to $f(a_1, a_2, \ldots, a_k)$. (Note that the homomorphism ε is surjective; indeed the image of this homomorphism is a subring of R containing K and a_i for $i = 1, 2, \ldots, k$, and is therefore the whole of R.) Thus R is isomorphic to the quotient of a Noetherian ring, and is therefore itself Noetherian (see Lemma 3.22). ∎

If $K(\alpha){:}\,K$ is a simple algebraic extension then $K(\alpha)$ is a K-algebra of finite type. Indeed $K(\alpha)$ is a finite-dimensional vector space over K (see Theorem 4.13). If $a_1, a_2, \ldots, a_k$ span $K(\alpha)$ as a vector space over K then clearly $K(\alpha) = K[a_1, a_2, \ldots, a_k]$.

5.2 Zariski's Theorem

Proposition 5.2 *Let K and L be fields, with $K \subset L$. Suppose that $L{:}\,K$ is a simple field extension and that L is a K-algebra of finite type. Then the extension $L{:}\,K$ is finite.*

Proof The field L is a K-algebra of finite type, and therefore there exist elements $\beta_1, \beta_2, \ldots, \beta_m$ of L such that $L = K[\beta_1, \beta_2, \ldots, \beta_m]$. Also the field extension $L{:}\,K$ is simple, and therefore $L = K(\alpha)$ for some element α of K. Now, given any element β of L there exist polynomials f and g in $K(x)$ such that $g(\alpha) \neq 0$ and $\beta = f(\alpha)g(\alpha)^{-1}$. Indeed one may readily verify that the set of elements of L that may be expressed in the form $f(\alpha)g(\alpha)^{-1}$ for some polynomials $f, g \in K[x]$ with $g(\alpha) \neq 0$ is a subfield of L which contains $K \cup \{\alpha\}$. It is therefore the whole of L, since $L = K(\alpha)$. It follows that there exist polynomials f_i and g_i in $K[x]$ such that $g_i(\alpha) \neq 0$ and $\beta_i = f_i(\alpha)g_i(\alpha)^{-1}$ for $i = 1, 2, \ldots, m$. Let $e(x) = g_1(x)g_2(x)\ldots, g_m(x)$. We shall show that if the element α of L were not algebraic over K then every irreducible polynomial with coefficients in K would divide $e(x)$,

Let $p \in K[x]$ be an irreducible polynomial with coefficients in K, where $p(\alpha) \neq 0$. Now $L = K[\beta_1, \beta_2, \ldots, \beta_m]$, and therefore every element of L is expressible as a polynomial in $\beta_1, \beta_2, \ldots, \beta_m$ with coefficients in K. Thus there exists some polynomial H_p in m indeterminates, with coefficents in K, such that

$$p(\alpha)^{-1} = H_p(\beta_1, \beta_2, \ldots, \beta_m).$$

Let d be the total degree of H. One can readily verify that

$$e(\alpha)^d H_p(\beta_1, \beta_2, \ldots, \beta_m) = q(\alpha),$$

for some polynomial $q(x)$ with coefficients in K. But then $p(\alpha)q(\alpha) = e(\alpha)^d$, and therefore α is a zero of the polynomial $pq - e^d$. If it were the case that α were not algebraic over K then this polynomial $pq - e^d$ would be the zero polynomial, and thus $p(x)q(x) = e(x)^d$. But it follows from Proposition 4.5

that an irreducible polynomial divides a product of polynomials if and only if it divides at least one of the factors. Therefore the irreducible polynomial p would be an irreducible factor of the polynomial e, and so would be an irreducible factor of one of the polynomials $g_1, g_2, \ldots, g_m$. We see therefore that if α were not algebraic over K then the polynomial e would be divisible by every irreducible polynomial in $K[x]$. But this is impossible, because a given polynomial in $K[x]$ can have only finitely many irreducible factors, whereas $K[x]$ contains infinitely many irreducible polynomials (Lemma 4.4). We conclude therefore that α must be algebraic over K. But any simple algebraic field extension is finite (Theorem 4.13). Therefore $L: K$ is finite, as required. ∎

Lemma 5.3 *Suppose that $K \subset A \subset B$, where A and B are unital commutative rings, and B is both a K-algebra of finite type and a finitely generated A-module. Then A is also a K-algebra of finite type.*

Proof There exist $\alpha_1, \alpha_2, \ldots, \alpha_m \in B$ such that $B = K[\alpha_1, \alpha_2, \ldots, \alpha_m]$, since B is a K-algebra of finite type. Also there exist $\beta_1, \beta_2, \ldots, \beta_n \in B$ such that

$$B = A\beta_1 + A\beta_2 + \cdots + A\beta_n,$$

since B is a finitely generated A-module. Moreover we can choose $\beta_1 = 1$. But then there exist elements λ_{qi} of A such that $\alpha_q = \sum_{i=1}^n \lambda_{qi}\beta_i$ for $q = 1, 2, \ldots, n$. Also there exist elements μ_{ijk} of A such that $\beta_i\beta_j = \sum_{k=1}^n \mu_{ijk}\beta_k$ for $i, j = 1, 2 \ldots, n$. Let

$$S = \{\lambda_{qi} : 1 \leq q \leq m,\ \ 1 \leq i \leq n\} \cup \{\mu_{ijk} : 1 \leq i, j, k \leq n\},$$

let $A_0 = K[S]$, and let

$$B_0 = A_0\beta_1 + A_0\beta_2 + \cdots + A_0\beta_n.$$

Now each product $\beta_i\beta_j$ is a linear combination of $\beta_1, \beta_2, \ldots, \beta_n$ with coefficients μ_{ijk} in A_0, and therefore $\beta_i\beta_j \in B_0$ for all i and j. It follows from this that the product of any two elements of B_0 must itself belong to B_0. Therefore B_0 is a subring of B. Now $K \subset B_0$, since $K \subset A_0$ and $\beta_1 = 1$. Also $\alpha_q \in B_0$ for $q = 1, 2, \ldots, m$. But $B = K(\alpha_1, \alpha_2, \cdots \alpha_m)$. It follows that $B_0 = B$, and therefore B is a finitely-generated A_0-module.

Now any K-algebra of finite type is a Noetherian ring (Lemma 5.1). It follows that A_0 is a Noetherian ring, and therefore any finitely-generated module over A_0 is Noetherian (see Corollary 3.21). In particular B is a Noetherian A_0-module, and therefore every submodule of B is a finitely-generated A_0-module. In particular, A is a finitely-generated A_0-module.

Let $\gamma_1, \gamma_2, \ldots, \gamma_p$ be a finite collection of elements of A that generate A as an A_0-module. Then any element a of A can be written in the form

$$a = a_1\gamma_1 + a_2\gamma_2 + \cdots + a_p\gamma_p,$$

where $a_l \in A_0$ for $l = 1, 2, \ldots, p$. But each element of A_0 can be expressed as a polynomial in the elements λ_{qi} and μ_{ijk} with coefficients in K. It follows that each element of A can be expressed as a polynomial in the elements λ_{qi}, μ_{ijk} and γ_l (with coefficients in K), and thus $A = K[T]$, where

$$T = S \cup \{\gamma_l : 1 \leq l \leq p\}.$$

Thus A is a K-algebra of finite type, as required. ∎

Theorem 5.4 (Zariski) *Let $L\colon K$ be a field extension. Suppose that the field L is a K-algebra of finite type. Then $L\colon K$ is a finite extension of K.*

Proof We prove the result by induction on the number of elements required to generate L as a K-algebra. Thus suppose that $L = K[\alpha_1, \alpha_2, \ldots, \alpha_n]$, and that the result is true for all field extensions $L_1\colon K_1$ with the property that L_1 is generated as a K_1-algebra by fewer than n elements (i.e., there exist elements $\beta_1, \beta_2, \ldots, \beta_m$ of L_1, where $m < n$, such that $L_1 = K_1[\beta_1, \beta_2, \ldots, \beta_m]$). Let $K_1 = K(\alpha_1)$. Then $L = K_1[\alpha_2, \alpha_3, \cdots, \alpha_n]$. It follows from the induction hypothesis that $L\colon K_1$ is a finite field extension (and thus L is a finitely-generated K_1-module). It then follows from Lemma 5.3 that K_1 is a K-algebra of finite type.

But the extension $K_1\colon K$ is a simple extension. It therefore follows from Proposition 5.2 that the extension $K_1\colon K$ is finite. Thus both $L\colon K_1$ and $K_1\colon K$ are finite extensions. It follows from the Tower Law (Proposition 4.10) that $L\colon K$ is a finite extension, as required. ∎

5.3 Hilbert's Nullstellensatz

Proposition 5.5 *Let K be an algebraically closed field, let R be a commutative K-algebra of finite type, and let $\mathfrak{m}$ be a maximal ideal of R. Then there exists a surjective K-homomorphism $\xi\colon R \to K$ from R to K such that $\mathfrak{m} = \ker \xi$.*

Proof Let $L = R/\mathfrak{m}$, and let $\varphi\colon R \to L$ denote the quotient homomorphism. Then L is a field (Lemma 3.30). Now $\mathfrak{m} = \ker \varphi$ and $1 \notin \mathfrak{m}$, and therefore $\varphi|K \neq 0$. It follows that $\mathfrak{m} \cap K$ is a proper ideal of the field K. But the only proper ideal of a field is the zero ideal (Lemma 3.4). Therefore

$\mathfrak{m} \cap K = \{0\}$. It follows that the restriction of φ to K is injective and maps K isomorphically onto a subfield of L. Let $K_1 = \varphi(K)$, and let $\iota: K \to K_1$ be the isomorphism obtained on restricting $\varphi: R \to L$ to K. Then $L: K_1$ is a field extension, and L is a K_1-algebra of finite type. It follows from Zariski's Theorem (Theorem 5.4) that $L: K_1$ is a finite field extension. But then $L = K_1$, since the field K_1 is algebraically closed (Lemma 4.16). Let $\xi = \iota^{-1} \circ \varphi$. Then $\xi: R \to K$ is the required K-homomorphism from R to K.

Theorem 5.6 *Let K be an algebraically closed field, and let R be a commutative K-algebra of finite type. Let $\mathfrak{a}$ be a proper ideal of R. Then there exists a K-homomorphism $\xi: R \to K$ from R to K such that $\mathfrak{a} \subset \ker \xi$.*

Proof Every proper ideal of R is contained in some maximal ideal (Theorem 3.31). Let $\mathfrak{m}$ be a maximal ideal of R with $\mathfrak{a} \subset \mathfrak{m}$. It follows from Proposition 5.5 that $\mathfrak{m} = \ker \xi$ for some K-homomorphism $\xi: R \to K$. Then $\mathfrak{a} \subset \ker \xi$, as required. ∎

Theorem 5.7 (Weak Nullstellensatz) *Let K be an algebraically closed field, and let $\mathfrak{a}$ be a proper ideal of the polynomial ring $K[X_1, X_2, \ldots, X_n]$, where $X_1, X_2, \ldots, X_n$ are independent indeterminates. Then there exists some point $(a_1, a_2, \ldots, a_n)$ of $\mathbb{A}^n(K)$ such that $f(a_1, a_2, \ldots, a_n) = 0$ for all $f \in \mathfrak{a}$.*

Proof Let $R = K[X_1, X_2, \ldots, X_n]$. Then R is a K-algebra of finite type. It follows from Theorem 5.6 that there exists a K-homomorphism $\xi: R \to K$ such that $\mathfrak{a} \subset \ker \xi$. Let $a_i = \xi(X_i)$ for $i = 1, 2, \ldots, n$. Then $\xi(f) = f(a_1, a_2, \ldots, a_n)$ for all $f \in R$. It follows that $f(a_1, a_2, \ldots, a_n) = 0$ for all $f \in \mathfrak{a}$, as required. ∎

Theorem 5.8 (Strong Nullstellensatz) *Let K be an algebraically closed field, let $\mathfrak{a}$ be an ideal of the polynomial ring $K[X_1, X_2, \ldots, X_n]$, and let $f \in K[X_1, X_2, \ldots, X_n]$ be a polynomial with the property that $f(x_1, x_2, \ldots, x_n) = 0$ for all $(x_1, x_2, \ldots, x_n) \in V(\mathfrak{a})$, where*

$$V(\mathfrak{a}) = \{(x_1, x_2, \ldots, x_n) \in \mathbb{A}^n(K) : g(x_1, x_2, \ldots, x_n) = 0 \textit{ for all } g \in \mathfrak{a}\}.$$

Then $f^r \in \mathfrak{a}$ for some natural number r.

Proof Let $R = K[X_1, X_2, \ldots, X_n]$, and let S denote the ring $R[Y]$ of polynomials in a single indeterminate Y with coefficients in the ring R. Then S can be viewed as the ring $K[X_1, X_2, \ldots, X_n, Y]$ of polynomials in the $n+1$ indeterminate indeterminates $X_1, X_2, \ldots, X_n, Y$ with coefficients in the field K.

The ideal $\mathfrak{a}$ of R determines a corresponding ideal $\mathfrak{b}$ of S consisting of those elements of S that are of the form

$$g_0 + g_1 Y + g_2 Y^2 + \cdots + g_r Y^r$$

with $g_0, g_1, \ldots, g_r \in \mathfrak{a}$. (Thus the ideal $\mathfrak{b}$ consists of those elements of the ring S that can be considered as polynomials in the indeterminate Y with coefficients in the ideal $\mathfrak{a}$ of R.)

Let $f \in R$ be a polynomial in the indeterminates $X_1, X_2, \ldots, X_n$ with the property that $f(x_1, x_2, \ldots, x_n) = 0$ for all $(x_1, x_2, \ldots, x_n) \in V(\mathfrak{a})$, and let $\mathfrak{c}$ be the ideal of S defined by

$$\mathfrak{c} = \mathfrak{b} + (1 - fY).$$

(Here $(1 - fY)$ denotes the ideal of the polynomial ring S generated by the polynomial $1 - f(X_1, X_2, \ldots, X_n)Y$.) Let $V(\mathfrak{c})$ be the subset of $(n+1)$-dimensional affine space $\mathbb{A}^{n+1}(K)$ consisting of all points $(x_1, x_2, \ldots, x_n, y) \in \mathbb{A}^{n+1}(K)$ with the property that $h(x_1, x_2, \ldots, x_n, y) = 0$ for all $h \in \mathfrak{c}$. We claim that $V(\mathfrak{c}) = \emptyset$.

Let $(x_1, x_2, \ldots, x_n, y)$ be a point of $V(\mathfrak{b})$. Then $g(x_1, x_2, \ldots, x_n) = 0$ for all $g \in \mathfrak{a}$, and therefore $(x_1, x_2, \ldots, x_n) \in V(\mathfrak{a})$. But the polynomial f has the value zero at each point of $V(\mathfrak{a})$. It follows that the polynomial $1 - fY$ has the value 1 at each point of $V(\mathfrak{b})$, and therefore

$$V(\mathfrak{c}) = V(\mathfrak{b}) \cap V(1 - fY) = \emptyset.$$

It now follows immediately from the Weak Nullstellensatz (Theorem 5.7) that $\mathfrak{c}$ cannot be a proper ideal of S, and therefore $1 \in \mathfrak{c}$. Thus there exists a polynomial h belonging to the ideal $\mathfrak{b}$ of S such that $h - 1 \in (1 - fY)$. Moreover this polynomial h is of the form

$$h(X_1, X_2, \ldots, X_n, Y) = \sum_{j=0}^{r} g_j(X_1, X_2, \ldots, X_n) Y^j,$$

where $g_1, g_2, \ldots, g_n \in \mathfrak{a}$.

Let $g \in \mathfrak{a}$ be defined by $g = \sum\limits_{j=0}^{r} g_j f^{r-j}$. Now $g - f^r = g - f^r h + f^r(h-1)$. Also

$$g - f^r h = \sum_{j=0}^{r} g_j f^{r-j}(1 - f^j Y^j) \in (1 - fY),$$

since the polynomial $1 - f^j Y^j$ is divisible by the polynomial $1 - fY$ for all positive integers j. It follows that $g - f^r \in (1 - fY)$. But the polynomial $g - f^r$

is a polynomial in the indeterminates $X_1, X_2, \dots, X_n$, and, if non-zero, would be of degree zero when considered as a polynomial in the indeterminate Y with coefficients in the ring R. Also any non-zero element of the ideal $(1 - fY)$ of S is divisible by the polynomial $1 - fY$, and is therefore of strictly positive degree when considered as a polynomial in the indeterminate Y with coefficients in R. We conclude, therefore that $g - f^r = 0$. But $g \in \mathfrak{a}$. Therefore $f^r \in \mathfrak{a}$, as required. ∎