

HILBERT'S NULLSTELLENSATZ

DRAGOS OPREA

1. INTRODUCTION

Let k be an algebraically closed field. We will employ the following notation. If $I \subset k[X_1, \dots, X_n]$ is an ideal, we let $\mathcal{Z}(I)$ denote the affine algebraic set in \mathbb{A}^n defined by the vanishing of the polynomials in I . Conversely, if X is an affine algebraic set, $\mathcal{I}(X)$ denotes the ideal of polynomials in $k[X_1, \dots, X_n]$ vanishing on X .

We will give a proof of the following result, called the weak Nullstellensatz:

Theorem 1. *Let I be an ideal in $k[X_1, \dots, X_n]$ such that $1 \notin I$. Then $\mathcal{Z}(I) \neq \emptyset$.*

This will immediately imply the strong version of the Nullstellensatz:

Theorem 2. *Let I be an ideal in $k[X_1, \dots, X_n]$. Then*

$$(1) \quad \mathcal{I}(\mathcal{Z}(I)) = \sqrt{I}.$$

Recall that the radical of an ideal $I \subset k[X_1, \dots, X_n]$ is defined as

$$\sqrt{I} = \{f : f^r \in I \text{ for some } r > 0\} \subset k[X_1, \dots, X_n].$$

An ideal I is called radical if

$$\sqrt{I} = I.$$

Remark 1. Note that if X is an affine algebraic set, then $\mathcal{I}(X)$ is a radical ideal. Indeed, if

$$f^r \in \mathcal{I}(X) \implies f^r = 0 \text{ on } X \implies f = 0 \text{ on } X \implies f \in \mathcal{I}(X).$$

In particular, setting $X = \mathcal{Z}(I)$, we obtain that $\mathcal{I}(\mathcal{Z}(I))$ is a radical ideal (which contains I as you can easily check). This explains why we expect to take radicals in equation (1).

Remark 2. It is clear that the strong Nullstellensatz implies the weak Nullstellensatz. Indeed, if $\mathcal{Z}(I) = \emptyset$, using Theorem 2, we have

$$\sqrt{I} = \mathcal{I}(\mathcal{Z}(I)) = \mathcal{I}(\emptyset) = k[X_1, \dots, X_n].$$

Therefore $1 \in \sqrt{I}$, and hence $1 \in I$. Conversely, we will see that the strong Nullstellensatz can be derived from the weak version.

Remark 3. We have seen in class that

$$\mathcal{Z}(\mathcal{I}(X)) = X.$$

Thus, the strong Nullstellensatz implies that \mathcal{I} and \mathcal{Z} are inverse transformations, at least when restricted to radical ideals I . We established an equivalence:

$$\{\text{affine algebraic sets in } \mathbb{A}^n\} \leftrightarrow \{\text{radical ideals in } k[X_1, \dots, X_n]\}.$$

Example 1. Let $I \subset k[X]$ be an ideal. Since $k[X]$ is a PID, I is generated by one polynomial f e.g.

$$I = \langle f \rangle \subset k[X].$$

We may assume f is monic. Since k is algebraically closed, we can write

$$f(X) = \prod_{i=1}^s (X - a_i)^{n_i},$$

with $a_i \neq a_j$, for $i \neq j$. It is clear that

$$\mathcal{Z}(I) = \{a_1, \dots, a_s\}.$$

Moreover, a polynomial vanishing on $\mathcal{Z}(I)$ must contain the factors $X - a_i$ for all $1 \leq i \leq s$. Therefore,

$$\mathcal{I}(\mathcal{Z}(I)) = \langle (X - a_1) \dots (X - a_s) \rangle.$$

The RHS is the ideal \sqrt{I} . Indeed,

$$g \in \sqrt{I} \text{ iff } g^r \text{ is divisible by } f = \prod_i (X - a_i)^{n_i} \text{ iff } g \text{ is divisible by } \prod_i (X - a_i).$$

Example 2. Let

$$I = \langle X^2Y^3, XY^4 \rangle \subset k[X, Y].$$

It is clear that $X^2Y^3 = XY^4$ implies $X = 0$ or $Y = 0$ so $\mathcal{Z}(I)$ is the union of the two coordinate axes in \mathbb{A}^2 . Thus

$$\mathcal{I}(\mathcal{Z}(I)) = \langle XY \rangle.$$

We claim

$$\sqrt{I} = \langle XY \rangle.$$

Indeed, $XY \in \sqrt{I}$ since $(XY)^3 = X \cdot X^2Y^3 \in I$. Conversely, if

$$f \in \sqrt{I} \implies f^r = X^2Y^3P(X, Y) + XY^4Q(X, Y) = XYR(X, Y) \implies XY | f^r \implies XY | f.$$

2. RESULTANTS

To prove the weak Nullstellensatz, we will have to investigate if the zero locus of the polynomials in an ideal I is non-empty. We will make use of resultants to detect if two polynomials have a common root.

To begin, let A be an integral domain. Recall that this means that A is a commutative ring and that moreover A has no zero-divisors e.g.

$$a, b \in A, ab = 0 \implies a = 0 \text{ or } b = 0.$$

This requirement will be used freely, in particular to conclude that the degree of a product of polynomials is the sum of the degrees:

$$\deg(uv) = \deg u + \deg v.$$

Let $f, g \in A[X]$ be any two non-zero polynomials of degrees n and m :

$$f(X) = a_0 + a_1X + \dots + a_nX^n,$$

$$g(X) = b_0 + b_1X + \dots + b_mX^m.$$

Definition 1. We define the resultant of f and g to be the following (Sylvester) determinant of size $n + m$:

$$(2) \quad R_{f,g} = \begin{vmatrix} a_0 & a_1 & \dots & a_n & 0 & 0 & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_n & 0 & \dots & 0 \\ & & & & \dots & & & \\ 0 & \dots & 0 & 0 & a_0 & a_1 & \dots & a_n \\ b_0 & b_1 & \dots & b_m & 0 & 0 & \dots & 0 \\ & & & & \dots & & & \\ 0 & \dots & 0 & 0 & b_0 & b_1 & \dots & b_m \end{vmatrix}.$$

The resultant is an element of A .

Remark 4. Using row operations, we see that

$$R_{f,g} = (-1)^{\deg f \cdot \deg g} R_{g,f}.$$

Example 3. If $f = b_0 + b_1X + b_2X^2$ and $g(X) = X - a$, then

$$R_{f,g} = \begin{vmatrix} b_0 & b_1 & b_2 \\ -a & 1 & 0 \\ 0 & -a & 1 \end{vmatrix} = b_0 + b_1a + b_2a^2 = f(a).$$

Therefore, f and g have a common root iff $R_{f,g} = 0$.

This turns out to be a general fact:

Theorem 3. If f and g have a common nonconstant factor in $A[X]$ then

$$R_{f,g} = 0.$$

Proof. Let $h(X)$ be the common factor and write

$$f(X) = h(X)P(X), g(X) = h(X)Q(X)$$

for some polynomials $P, Q \in A[X]$. Then,

$$\deg P < \deg f, \deg Q < \deg g$$

and

$$(3) \quad f(X)Q(X) = g(X)P(X).$$

Write

$$\begin{aligned} P(X) &= \alpha_0 + \alpha_1X + \dots + \alpha_{n-1}X^{n-1}, \\ Q(X) &= \beta_0 + \beta_1X + \dots + \beta_{m-1}X^{m-1}, \end{aligned}$$

Then, identifying coefficients in equation (3) we see that

$$\begin{aligned} a_0\beta_0 - b_0\alpha_0 &= 0, \\ a_1\beta_0 + a_0\beta_1 - b_1\alpha_0 - b_0\alpha_1 &= 0, \\ a_2\beta_0 + a_1\beta_1 + a_0\beta_2 - b_2\alpha_0 - b_1\alpha_1 - b_0\alpha_2 &= 0, \\ &\dots \end{aligned}$$

These $n + m$ equations form a linear system in the $n + m$ unknowns

$$(\beta_0, \dots, \beta_{m-1}, -\alpha_0, -\alpha_1, \dots, -\alpha_{n-1}).$$

The above discussion implies that the system must have a nontrivial solution. Therefore, the matrix of coefficients must have zero determinant.

Now it is easy to see that the matrix of coefficients has determinant given by (2). Indeed, the coefficients of β_0 in the equations above are $a_0, a_1, \dots, a_n, 0, \dots, 0$; the coefficients of β_1 in the above equations are $0, a_0, a_1, \dots, a_n, 0, \dots, 0$; the coefficients of β_2 are $0, 0, a_0, \dots, a_n, 0, \dots, 0$, and so on.

Remark 5. The converse of Theorem 3 is also true if A is a unique factorization domain. Indeed, the implications in the above proof can be reversed. Thus, the vanishing of $R_{f,g}$ implies the solvability of the system in the α and β 's. In turn, this guarantees existence of nontrivial polynomials P, Q such that

$$fQ = gP,$$

with

$$\deg Q < \deg g, \quad \deg P < \deg f.$$

Since A is a UFD, $A[X]$ is UFD as well. Then, we can write the polynomials above as products of irreducibles (with multiplicities). If f and g have no common factors, then all factors in f will have to be found in P , possibly with higher multiplicities. But this is impossible since $\deg P < \deg f$. Thus f and g must have a common factor.

The following result makes the statement in Theorem 3 more precise:

Theorem 4. *If*

$$f(X) = \prod_{i=1}^n (X - \lambda_i) \text{ and } g(X) = \prod_{j=1}^m (X - \mu_j)$$

then

$$R_{f,g} = \prod_{i,j} (\mu_j - \lambda_i).$$

Proof. We will regard the λ 's and μ 's as variables of degree 1. Since

$$f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0 = \prod_{i=1}^n (X - \lambda_i),$$

we see that the coefficients of f can be expressed in terms of the roots λ via the symmetric functions

$$\begin{aligned} a_0 &= (-\lambda_1) \dots (-\lambda_n), \\ a_{n-1} &= (-\lambda_1) + \dots + (-\lambda_n). \end{aligned}$$

Therefore a_i is a polynomial in the λ 's of degree $n - i$. Similarly, b_j is a polynomial in the μ 's of degree $m - j$:

$$\deg a_i = n - i, \quad \deg b_j = m - j.$$

Claim. *The resultant $R_{f,g}$ is a polynomial in λ and μ 's of degree nm .*

Assuming the *Claim*, we conclude the proof as follows. First, if $\mu_j = \lambda_i$, then f and g have a common factor and therefore $R_{f,g} = 0$. Thus $R_{f,g}$ is divisible by

$$\prod_{i,j} (\mu_j - \lambda_i).$$

By degree considerations, we see that there exists a constant c such that

$$R_{f,g} = c \prod_{i,j} (\mu_j - \lambda_i).$$

It remains to show that $c = 1$. To this end, it suffices to pick two special polynomials f and g . For instance, let $g(X) = X^m$ so that

$$\mu_1 = \dots = \mu_m = 0.$$

The resultant $R_{f,g}$ given by (2) becomes

$$\begin{vmatrix} a_0 & a_1 & \dots & a_n & 0 & 0 & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_n & 0 & \dots & 0 \\ & & & & \dots & & & \\ 0 & \dots & 0 & a_0 & a_1 & \dots & a_{n-1} & a_n \\ 0 & 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ & & & & \dots & & & \\ 0 & \dots & 0 & 0 & 0 & 0 & \dots & 1 \end{vmatrix}.$$

This is an upper triangular matrix, hence the determinant is computed as product of the terms on the main diagonal

$$R_{f,g} = a_0^m.$$

Note that

$$\prod_{i,j} (\mu_j - \lambda_i) = (-\lambda_1)^m \dots (-\lambda_n)^m = a_0^m.$$

This shows that $c = 1$, completing the proof.

Proof of the Claim. Let r_{ij} be the entries of the matrix (2) giving the determinant $R_{f,g}$. Since a_i has degree $n - i$ and b_j has degree $m - j$ in the λ 's and μ 's, we see that

$$\deg(r_{ij}) = \begin{cases} n + i - j, & \text{if } 1 \leq i \leq m, \\ i - j & \text{if } m + 1 \leq i \leq m + n. \end{cases}$$

Then

$$R_{f,g} = \sum_{\sigma \in S_{m+n}} (-1)^\sigma r_{1,\sigma(1)} \cdots r_{m+n,\sigma(m+n)}$$

has degree

$$\sum_{i=1}^m (n + i - \sigma(i)) + \sum_{i=m+1}^{m+n} (i - \sigma(i)) = mn + \sum_{i=1}^{m+n} (i - \sigma(i)) = mn.$$

□

Remark 6. If f and g are not monic the result of Theorem 4 has to be modified slightly. Let a_n and b_m be the leading terms of f and g such that

$$f(X) = a_n \prod_i (X - \lambda_i), \quad g(X) = b_m \prod_j (X - \mu_j).$$

Then the same argument as before shows

$$(4) \quad R_{f,g} = a_n^m b_m^n \prod_{i,j} (\mu_j - \lambda_i).$$

Remark 7. Equation (4) can be rewritten as

$$(5) \quad R_{f,g} = b_m^n \prod_j f(\mu_j),$$

where the μ 's are the roots of g . In particular,

$$R_{f,X-a} = f(a)$$

as we saw in Example 3.

Remark 8. If f_1, f_2 are any two polynomials which split into products of linear factors, we see from (5) that

$$(6) \quad R_{f_1 f_2, g} = b_m^{\deg f_1 + \deg f_2} \prod_j f_1(\mu_j) f_2(\mu_j) = \left(b_m^{\deg f_1} \prod_j f_1(\mu_j) \right) \left(b_m^{\deg f_2} \prod_j f_2(\mu_j) \right) \\ = R_{f_1, g} R_{f_2, g}.$$

Remark 9. If f_1 and f_2 are two polynomials such that

$$f_1 \equiv f_2 \pmod{g}$$

then we claim

$$(7) \quad R_{f_1, g} = b_m^{\deg f_1 - \deg f_2} R_{f_2, g}.$$

Indeed, first write

$$f_1(X) = f_2(X) + g(X)S(X)$$

for some polynomial $S(X)$. Then

$$f_1(\mu_j) = f_2(\mu_j),$$

since $g(\mu_j) = 0$. Therefore, by (6), we have

$$R_{f_1, g} = b_m^{\deg f_1} \prod_j f_1(\mu_j) = b_m^{\deg f_1} \prod_j f_2(\mu_j) = b_m^{\deg f_1 - \deg f_2} R_{f_2, g}.$$

Equations (6) and (7) hold true even if the polynomials involved are not products of linear factors:

Theorem 5. For any nonzero polynomials $f_1, f_2, g \in A[X]$ such that g has leading coefficient b_m we have

(i)

$$R_{f_1 f_2, g} = R_{f_1, g} R_{f_2, g}$$

(ii) If $f_1 \equiv f_2 \pmod{g}$, then

$$R_{f_1, g} = b_m^{\deg f_1 - \deg f_2} R_{f_2, g}.$$

Proof. The Theorem is proved in case the polynomials above split as products of linear factors. We will reduce to this case by means of the following key observation (which will be proved in a future homework):

Claim. *Any integral domain A is contained in a field K .*

Replacing K by its algebraic closure, we may assume that A is contained in an algebraically closed field. Then, viewed as polynomials in $K[X]$, the above polynomials split (even though they may not split in $A[X]$). Therefore, equations (6), (7) are satisfied in K . But since the resultants are elements of A , equations (6) and (7) are satisfied in A . \square

The following result will be crucial in the proof of the Nullstellensatz:

Lemma 1. *The resultant $R_{f,g}$ is an element of the ideal spanned by f and g in $A[X]$.*

Proof. Look at the matrix defining $R_{f,g}$ in (2). Replace the first column by the following expression:

$$1^{\text{st}} \text{ column} + X \cdot 2^{\text{nd}} \text{ column} + X^2 \cdot 3^{\text{rd}} \text{ column} + \dots + X^{m+n-1} \cdot \text{last column} .$$

This replacement does not change the value of the determinant. Moreover, the first column has as entries

$$f(X), Xf(X), \dots, X^{m-1}f(X), g(X), Xg(X), \dots, X^{n-1}g(X).$$

Expanding the determinant along this new first column we obtain

$$(8) \quad R_{f,g} = f(X)P(X) + g(X)Q(X)$$

for some polynomials P and Q with coefficients in A . This proves our Lemma.

Remark 10. The lemma allows us to reprove Theorem 3 and its converse. Indeed, if $f(X)$ and $g(X)$ have a common factor $h(X)$ then, using (8), we see that

$$h(X) | R_{f,g}.$$

But $R_{f,g}$ is a constant polynomial in $A[X]$. This implies that h must be constant (by looking at degrees for instance).

Conversely, if $R_{f,g} = 0$, we must have

$$f(X)P(X) = -g(X)Q(X).$$

From the explicit description of $P(X)$ and $Q(X)$ obtained by expanding the determinant along the first column, we see that

$$\deg P < m \text{ and } \deg Q < n.$$

This recovers equation (3). Finally, we have already seen in Remark 5 that this equation implies that f and g must have a common factor, at least if A is an UFD.

3. RESULTANTS OF POLYNOMIALS IN SEVERAL VARIABLES

Let us now consider the case when f, g are polynomials in two variables in $k[X, Y] = k[Y][X]$. Then, we can view f and g as polynomials in X with coefficients in the ring $A = k[Y]$:

$$(9) \quad f(X, Y) = a_0(Y) + a_1(Y)X + \dots + a_n(Y)X^n$$

$$(10) \quad g(X, Y) = b_0(Y) + b_1(Y)X + \dots + b_m(Y)X^m.$$

Therefore, we can define the resultant

$$R_{f,g}^{(1)} \in k[Y]$$

by the determinant (2):

$$(11) \quad R_{f,g}^{(1)} = \begin{vmatrix} a_0(Y) & a_1(Y) & \dots & a_n(Y) & 0 & 0 & \dots & 0 \\ 0 & a_0(Y) & a_1(Y) & \dots & a_n(Y) & 0 & \dots & 0 \\ & & & & \dots & & & \\ 0 & \dots & 0 & 0 & a_0(Y) & a_1(Y) & \dots & a_n(Y) \\ b_0(Y) & b_1(Y) & \dots & b_m(Y) & 0 & 0 & \dots & 0 \\ & & & & \dots & & & \\ 0 & \dots & 0 & 0 & b_0(Y) & b_1(Y) & \dots & b_m(Y) \end{vmatrix}.$$

Similarly, we can view f, g as polynomials in Y with coefficients in the ring $k[X]$, and we obtain the resultant

$$R_{f,g}^{(2)} \in k[X].$$

Remark 11. In general $R_{f,g}^{(1)}(Y)$ and $R_{f,g}^{(2)}(X)$ can be different polynomials. For instance, let

$$f(X, Y) = X^2 + Y, \quad g(X, Y) = XY + 1.$$

Then

$$R_{f,g}^{(1)} = \begin{vmatrix} Y & 0 & 1 \\ 1 & Y & 0 \\ 0 & 1 & Y \end{vmatrix} = Y^3 + 1,$$

while

$$R_{f,g}^{(2)} = \begin{vmatrix} X^2 & 1 \\ 1 & X \end{vmatrix} = X^3 - 1.$$

Remark 12. (Warning!) If f and g have a common factor in $k[X, Y]$ it doesn't immediately follow that

$$R_{f,g}^{(1)}(Y) = 0.$$

This may fail if the common factor is a polynomial in $A = k[Y]$. In this case, the common factor, viewed as an element in $A[X]$ will be constant as a polynomial in X . However, this is the only way the resultant may fail to be zero. Now, since A is a UFD, we conclude

$$R_{f,g}^{(1)}(Y) = 0 \text{ iff}$$

f and g have a common factor which is not a polynomial only in the variable Y .

You may check this failure in an example if you wish, for instance taking

$$f(X, Y) = XY + Y^2, g(X, Y) = XY.$$

In this case, f and g have a common factor Y , but

$$R_{f,g}^{(1)}(Y) = Y^3 \neq 0.$$

Remark 13. Assume now that $f(X, Y)$ and $g(X, Y)$ are homogeneous polynomials of degrees n and m respectively. In particular, $f(X, Y)$ is a combination of the monomials

$$X^n, X^{n-1}Y, \dots, XY^{n-1}, Y^n.$$

Considering the expression (9), we see that

$$\deg a_i(Y) = n - i.$$

Similarly, $\deg b_i(Y) = m - i$. Now re-examining the proof of the *Claim* used to show Theorem 4 we see that

$$R_{f,g}^{(1)}(Y)$$

is a homogeneous polynomial of degree nm .

Remark 14. The same discussion applies if f and g are polynomials in n variables with coefficients in a field k . In particular, we obtain n resultants

$$R_{f,g}^{(1)} \in k[X_2, \dots, X_n], \dots, R_{f,g}^{(n)} \in k[X_1, \dots, X_{n-1}].$$

Then

Proposition 1. *If f and g are homogeneous polynomials in $k[X_1, \dots, X_n]$ of degrees d and e , then each resultant $R_{f,g}^{(i)}$ is a homogenous polynomial of degree de in the $n - 1$ variables $X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n$.*

This result will be instrumental later in the proof of Bezout's theorem.

4. THE WEAK NULLSTELLENSATZ

We can now prove Theorem 1. We will use induction on the number n of indeterminates.

When $n = 1$, $I \subset k[X]$ is a principal ideal generated by one polynomial f . Since $1 \notin I$, f must be non-constant. Since k is algebraically closed, f must have a root a . Then $a \in \mathcal{Z}(I) \neq \emptyset$.

We will now show the inductive step, assuming that the statement is already proved for ideals in polynomial rings in $n - 1$ variables. Let $I \subset k[X_1, \dots, X_n]$. Pick $f \in I$, and write d for its degree.

Lemma 2. *There are $\lambda_1, \dots, \lambda_{n-1} \in k$ such that*

$$f(X_1 + \lambda_1 X_n, \dots, X_{n-1} + \lambda_{n-1} X_n, X_n) = a \cdot X_n^d + \text{lower terms in } X_n$$

for some constant $a \neq 0$.

Proof. Let us write f as sum of homogeneous pieces such that the leading piece $f_{(d)}$ has degree d . It is clear that it suffices to consider only

$$f_{(d)}(X_1 + \lambda_1 X_n, \dots, X_{n-1} + \lambda_{n-1} X_n, X_n)$$

since the remaining terms will contribute lower powers of X_n . Now,

$$f_{(d)}(X_1 + \lambda_1 X_n, \dots, X_{n-1} + \lambda_{n-1} X_n, X_n) = X_n^d f(\lambda_1, \dots, \lambda_{n-1}, 1) + \text{lower terms}.$$

It suffices to pick $\lambda_1, \dots, \lambda_{n-1}$ such that

$$f(\lambda_1, \dots, \lambda_{n-1}, 1) \neq 0.$$

This is possible since k is infinite. □

Using the lemma, we see that after changing coordinates

$$X_i^{new} = X_i + \lambda_i X_n, \text{ for } 1 \leq i \leq n-1, \quad X_n^{new} = X_n,$$

we may assume that f has the form

$$f = X_n^d + X_n^{d-1} f_1(X_1, \dots, X_{n-1}) + \dots + f_d(X_1, \dots, X_{n-1}).$$

Let $\mathcal{I} = I \cap k[X_1, \dots, X_{n-1}]$. This is an ideal in $k[X_1, \dots, X_{n-1}]$ which does not contain 1 since $1 \notin I$. By induction, there is $(a_1, \dots, a_{n-1}) \in \mathbb{A}^{n-1}$ such that

$$F(a_1, \dots, a_{n-1}) = 0, \text{ for all } F \in \mathcal{I}.$$

Consider the ideal $J \subset k[X_n]$ defined as

$$J = \{f(a_1, \dots, a_{n-1}, X_n) : f \in I\}.$$

If $1 \notin J$, then by the case $n = 1$, we conclude that there exists $a_n \in k$ such that all polynomials in J vanish at a_n . This implies that

$$f(a_1, \dots, a_n) = 0,$$

for all $f \in I$ completing the proof.

It remains to explain that $1 \notin J$. Assume the contrary. Then, there exists $g \in I$ such that

$$g(a_1, \dots, a_{n-1}, X_n) = 1.$$

Writing

$$g = g_0(X_1, \dots, X_{n-1}) + g_1(X_1, \dots, X_{n-1})X_n + \dots + g_e(X_1, \dots, X_{n-1})X_n^e,$$

we conclude

$$g_0(a_1, \dots, a_{n-1}) = 1, g_i(a_1, \dots, a_{n-1}) = 0, \quad 1 \leq i \leq e.$$

Consider the resultant

$$R_{g,f}^{(n)} \in k[X_1, \dots, X_{n-1}].$$

By Lemma 1, this resultant also lies in I , so it must lie in \mathcal{I} . Therefore,

$$(12) \quad R_{g,f}^{(n)}(a_1, \dots, a_{n-1}) = 0.$$

However, the determinant (2) gives the following lower triangular matrix

$$(13) \quad R_{g,f}^{(n)}(a_0, \dots, a_{n-1}) = \begin{vmatrix} 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & 0 & \dots & 0 \\ & & & \dots & & & \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ f_0 & f_1 & \dots & f_{d-1} & 1 & \dots & 0 \\ & & & \dots & & & \\ 0 & \dots & 0 & f_0 & f_1 & \dots & 1 \end{vmatrix} = 1.$$

This contradicts (12), therefore completing the proof.

5. THE STRONG NULLSTELLENSATZ

The strong form of the Nullstellensatz, i.e. Theorem 2, follows from the weak form using a smart trick.

To begin, let I be any ideal in $k[X_1, \dots, X_n]$. Clearly

$$\sqrt{I} \subset \mathcal{I}(\mathcal{Z}(I)).$$

Indeed, if

$$f \in \sqrt{I} \text{ then } f^r \in I$$

for some $r > 0$. Then, we have

$$f^r(p) = 0, \quad \forall p \in \mathcal{Z}(I) \implies f(p) = 0 \quad \forall p \in \mathcal{Z}(I) \implies f \in \mathcal{I}(\mathcal{Z}(I)).$$

Conversely, let $f \in \mathcal{I}(\mathcal{Z}(I))$. We will show that

$$f \in \sqrt{I}.$$

Pick f_1, \dots, f_m generators for I . We adjoin a new variable T and consider the ideal

$$J = \langle f_1(X_1, \dots, X_n), \dots, f_m(X_1, \dots, X_n), Tf(X_1, \dots, X_n) - 1 \rangle \subset k[X_1, \dots, X_n, T].$$

We claim that

$$\mathcal{Z}(J) = \emptyset.$$

Indeed, suppose that $(x, t) \in \mathcal{Z}(J)$. We must have

$$f_1(x) = \dots = f_m(x) = tf(x) - 1 = 0.$$

The first m equations imply that

$$x \in \mathcal{Z}(I),$$

while the last implies $f(x) \neq 0$. This contradicts the assumption that

$$f \in \mathcal{I}(\mathcal{Z}(I)).$$

Therefore $\mathcal{Z}(J) = \emptyset$. By the weak Nullstellensatz, we must have $1 \in J$. Therefore, we can find polynomials $g_0, g_1, \dots, g_m \in k[X_1, \dots, X_n, T]$ such that

$$1 = \sum_{i=1}^m f_i(X_1, \dots, X_n)g_i(X_1, \dots, X_n, T) + (Tf - 1)g_0(X_1, \dots, X_n, T).$$

Let N be the highest power of T appearing in the polynomials g_i . Multiplying by f^N , we get

$$f^N = \sum_{i=1}^m f_i G_i(X_1, \dots, X_n, fT) + (Tf - 1)G_0(X_1, \dots, X_n, fT)$$

where

$$G_i = f^N g_i$$

is considered to be a polynomial in X_1, \dots, X_n, fT . Now, making

$$t = \frac{1}{f(X_1, \dots, X_n)},$$

we obtain

$$f^N = \sum_{i=1}^m f_i G_i(X_1, \dots, X_n, 1) \in I.$$

This proves that $f \in \sqrt{I}$, as claimed.

E-mail address: doprea@math.ucsd.edu