Nullstellensatz for everybody

Marco Manetti*

March 2, 2006

Dedicato alla memoria di Franco Conti

Abstract

The Nullstellensatz, also known as Hilbert's theorem of the zeroes, is a fundamental result in algebraic geometry. This paper proves the theorem using elementary tools from algebra.

1 Introduction

The Nullstellensatz is the generalization of the fundamental theorem of algebra to several dimensions. It is one of the most important results in the field known as algebraic geometry.

In spite of the somewhat esoteric name of the theorem and the fact that in the textbooks of geometry and algebra in current circulation the theorem is proven using techniques that are not understandable by the non-specialist, Hilbert's theorem of zeroes was and remains essentially a result of basic algebra and linear algebra. The theorem may therefore be proven using some relatively well known results of elementary algebra and linear algebra.

The aim of this paper is to present Hilbert's theorem of zeros within this simpler framework. It is only necessary to know a few results of elementary algebra (principle of induction, polynomials in one and more variables and the Euclidean division algorithm) and to possess some knowledge of determinants from linear algebra in order to understand and follow the arguments on the following pages.

*English translation from [6] by Jon Rokne

The title of the paper is a bit of propaganda, rather than a mathematical statement. In any case, it is my hope that that the following pages will be accessible to all students that have completed a first year in a faculty of science.

2 So, what are we talking about?

By a polynomial $p(z)$ of degree d in the variable z is meant

$$p(z) = a_0 z^d + a_1 z^{d-1} + \cdots + a_d,$$

where $a_0, \ldots, a_d$ are complex coefficients and $a_0 \neq 0$. By a root (synonym zero) of the polynomial is meant a complex number u such that the polynomial evaluated at u has the value zero, i.e. $p(u) = 0$. The following result, given without proof, is of fundamental importance for what follows.

THEOREM 1 *(Fundamental theorem of algebra). A polynomial of degree $d > 0$ with complex coefficients has a root.*

If a polynomial $p(z)$ has degree $d < 1$ then it must be a constant, say $p(z) = c$. In this case it can have a root (if $c = 0$) or not have a root (if $c \neq 0$). A result, equivalent to the fundamental theorem of algebra for $d > 0$, which includes the case $d = 0$, is the following:

THEOREM 2 *A polynomial $p(z)$ with complex coefficients does not have roots if and only if there exist a polynomial $q(z)$ such that $p(z)q(z) = 1$.*

In fact, if there exists an polynomial $q(z)$ such that $p(z)q(z) = 1$ then $p(u)q(u) = 1$ for every complex number u and hence $p(u)$ cannot be equal to zero. Conversely, if $p(z)$ does not have roots then $p(z)$ must be a constant c not equal to zero. Setting $q(z) = c^{-1}$ it follows that $p(z)q(z) = 1$.

The next step is to consider a finite set of polynomials $p_1(z), \ldots, p_m(z)$ with complex coefficients. A common zero of these polynomials is a complex number u such that $p_1(u) = \cdots = p_m(u) = 0$.

A first step on the way to the Nullstellensatz is the following generalization of Theorem 2:

THEOREM 3 *A finite set of polynomials $p_1(z), \ldots, p_m(z)$ with complex coefficients does not have common roots if and only if there exists polynomials $q_1(z), \ldots, q_m(z)$ with complex coefficients such that*

$$p_1(z)q_1(z) + \cdots + p_m(z)q_m(z) = 1.$$

This theorem is proven in the next section. The Nullstellensatz is now the further generalization of the above theorem to polynomials in an arbitrary number of variables. Let us see what this means.

Let $\mathbb{C}$ be the field of complex numbers and consider an integer $n > 0$. For every n-tuple $i_1, \ldots, i_n$ where $i_j \geq 0, j = 1, \ldots n$ the function

$$t(z_1, \ldots, z_n) = z_1^{i_1} \cdots z_n^{i_n} : \mathbb{C}^n \to \mathbb{C}, \text{ s.t. } t(a_1, \ldots, a_n) = a_1^{i_1} \cdots a_n^{i_n}$$

is called a monomial of degree $d = i_1 + \cdots + i_n$ in the variables $z_1, \ldots, z_n$ where, with a small abuse of notation, it is intended that $a^0 = 1$ for all complex numbers a. Let us observe that the function whose value is the constant 1 is the unique monomial of degree 0 and that the n monomials $z_1, \ldots, z_n$ are nothing but the canonical system of coordinates in the vector space $\mathbb{C}^n$.

A polynomial $p(z_1, \ldots, z_n)$ in the variables $z_1, \ldots, z_n$ is a function $p : \mathbb{C}^n \to \mathbb{C}$ obtained from linear combinations of a finite number of monomials with complex coefficients. The functions $z_1 z_2 - 2$ and z_1^3 are examples of polynomials in the variables z_1, z_2. Note that polynomials can be added and multipled and that the sums and products of polynomials are also polynomials.

The main theorem of the paper due to Hilbert can now be stated.

THEOREM 4 *(Nullstellensatz). Let $p_1(z_1, \ldots, z_n), \ldots, p_m(z_1, \ldots, z_n)$ be polynomials with complex coefficients. The set of vectors $(a_1, \ldots, a_n) \in \mathbb{C}^n$ for which*

$$p_1(a_1, \ldots, a_n) = \cdots = p_m(a_1, \ldots, a_n) = 0$$

is empty if and only if there exist polynomials $q_1(z_1, \ldots, z_n), \ldots, q_m(z_1, \ldots, z_n)$ such that

$$p_1(z_1, \ldots, z_n)q_1(z_1, \ldots, z_n) + \cdots + p_m(z_1, \ldots, z_n)q_m(z_1, \ldots, z_n) = 1.$$

Clearly, if $n = m = 1$ the theorem reduces to the fundamental theorem of algebra.

The remainder of the paper is mainly concerned with proving Theorem 4.

3 A first generalization

Theorem 3 is a simple consequence of the Euclidean division algorithm for polynomials. Let us therefore recall this algorithm.

Let $p(z)$ be a monic polynomial of degree $d \geq 0$, that is to say, a polynomial of the form

$$p(z) = z^d + a_1 z^{d-1} + \cdots + a_d$$

(by monic is meant that the coefficient of the highest power of z in $p(z)$ is 1).

Let $q(z) = b_0 z^s + b_1 z^{s-1} + \cdots + b_s$, $b_0 \neq 0$ be any polynomial of degree s. Then there exists two polynomials $h(z)$ and $r(z)$ such that:

1. $q(z) - h(z)p(z) = r(z)$,
2. if $s \geq d$ then $h(z)$ has degree $s - d$,
3. either $r(z) = 0$ or $r(z)$ has degree $< d$.

Let us prove the existence and uniqueness of h and r:

EXISTENCE: By induction on the degree s of $q(z)$. If $s < d$ we only need to set $h(z) = 0$ and $r(z) = q(z)$ and the existence is verified. If $s \geq d$ observe that the polynomial $q'(z) = q(z) - b_0 z^{s-d} p(z)$ has degree $< s$. From the induction hypothesis there exist $h'(z)$ and $r(z)$ such that $q'(z) = q(z) - h'(z)p(z) = r(z)$ and hence $q(z) - (b_0 z^{s-d} + h'(z))p(z) = r(z)$.

As a consequence of this we have the following lemma:

LEMMA 1 *Let*

$$p(z) = a_0 z^d + a_1 z^{d-1} + \cdots + a_d, \quad \textit{with } a_0 \neq 0,$$

be a non-zero polynomial of degree d. Then there exist at most d complex numbers $u_1, \ldots, u_d$ such that $p(u_i) = 0, i = 1, \ldots, d$.

Proof. The proof is by induction on d. When $d = 0$, $p(z) = a_0$ which by hypothesis is non-zero. Hence there are no roots. If $d > 0$ then we assume there are $d+1$ distinct roots $u_1, \ldots, u_{d+1}$ of $p(z)$ and show that this leads to a contradiction.

From the Euclidean division algorithm we can write $p(z) = (z-u_{d+1})h(z)+r(z)$ with $r(z)$ having degree < 1, i.e. $r(z)$ is a constant, say $r(z) = c$. From $c = p(u_{d+1}) = 0$ it follows that $u_2, \ldots, u_d$ are roots of $h(z)$. Since $h(z)$ has degree $< d$ we have the required contradiction.

UNIQUENESS OF THE EUCLIDEAN DIVISION.

Suppose that we have $q(z) = h_1(z)p(z) + r_1(z)$, $q(z) = h_2(z)p(z) + r_2(z)$. Subtracting these polynomials we get $(h_1(z)-h_2(z))p(z)+(r_1(z)-r_2(z)) = 0$. The left side of the equality is a polynomial that zeroes out all complex numbers and by the previous lemma it must be the zero polynomial. In particular $h_1 = h_2$ (otherwise the polynomial would have degree $\geq d$) and $r_1 = r_2$.

We now prove Theorem 3 (repeated below for clarity).

THEOREM 5 *A finite set of polynomials $p_1(z), \ldots, p_m(z)$ with complex coefficients does not have common roots if and only if there exist polynomials $q_1(z), \ldots, q_m(z)$ with complex coefficients such that*

$$p_1(z)q_1(z) + \cdots + p_m(z)q_m(z) = 1.$$

Proof. Let J be the set of polynomials of the form $p_1(z)q_1(z) + \cdots + p_m(z)q_m(z)$ with $q_1(z), \ldots, q_m(z)$ being polynomials with complex coefficients.

Clearly, if u is a common root of the polynomials $p_1(z), \ldots, p_m(z)$ then u is a root of every polynomial in J. Moreover, the sum and dif and only iference of polynomials in J is in J and if $p(z) \in J$ then $h(z)p(z) \in J$ for every polynomial $h(z)$.

Let us choose a non-zero polynomial $p(z) \in J \setminus \{0\}$ of minimal degree amongst the polynomials in J. Since $p(z)$ can be multiplied by a non-zero number we can assume $p(z)$ is monic. Let d be the degree of this polynomial. If $d = 0$ then $p(z) = 1$ and $p_1(z), \ldots, p_m(z)$ have no roots in common. If $d > 1$ then we prove that $p(z)$ divides each polynomial $p_1(z), \ldots, p_m(z)$, hence it follows that each root of $p(z)$ is a common root of $p_1(z), \ldots, p_m(z)$.

Let $i = 1, \ldots, m$ be a fixed index, then from the Euclidean division algorithm there exist a polynomial $h(z)$ such that $r(z) = p_i(z) - h(z)p(z)$ of

degree is $< d$. Since $r(z)$ is a element of J it must follow that $r = 0$ and hence $p(z)$ divides $p_i(z)$.

4 How to eliminate a variable

Let $\mathbb{C}[z_1, \ldots, z_n]$ denote the set of polynomials in the variables $z_1, \ldots, z_n$ and let the null polynomial correspond to the null linear combination of monomials.

LEMMA 2 *A polynomial $p : \mathbb{C}^n \to \mathbb{C}$ is the null polynomial if and only if $p(a_1, \ldots, a_n) = 0$ for every $a_1, \ldots, a_n$.*

Proof. The forwards implication is clear (null polynomial evaluates to zero). For the reverse implication let p be a non-null linear combination written as

$$p(z_1, \ldots, z_n) = p_0(z_1, \ldots, z_{n-1}) z_n^d + p_1(z_1, \ldots, z_{n-1}) z_n^{d-1} + \cdots + p_d(z_1, \ldots, z_{n-1})$$

for some polynomials $p_0, \ldots, p_d$ in $z_1, \ldots, z_{n-1}$ not all zero. By induction on n there exists $a_1, \ldots, a_{n-1} \in \mathbb{C}$ such that the numbers $p_0(a_1, \ldots, a_{n-1}), \ldots, p_d(a_1, \ldots, a_{n-1})$ are not all zero and hence the polynomial

$$q(z_n) = p_0(a_1, \ldots, a_{n-1}) z_n^d + p_1(a_1, \ldots, a_{n-1}) z_n^{d-1} + \cdots + p_d(a_1, \ldots, a_{n-1})$$

is non-zero. Therefore we have an $a_n \in \mathbb{C}$ such that $p_1(a_1, \ldots, a_n) = q(a_n) \neq 0$.

A polynomial p is said to be a monic polynomial of of degree d in z_n if it can be written as

$$p(z_1, \ldots, z_n) = z_n^d + p_1(z_1, \ldots, z_{n-1}) z_n^{d-1} + \cdots + p_d(z_1, \ldots, z_{n-1})$$

for some polynomials $p_1, \ldots, p_d$ in the variables $z_1, \ldots, z_{n-1}$.

With the monic polynomials in z_n as divisors, the Euclidean division algorithm can still be applied.. Specifically, if $p(z_1, \ldots, z_n)$ is a monic polynomial of degree d in z_n, then there exists polynomials $h(z_1, \ldots, z_n)$, $r_0(z_1, \ldots, z_{n-1}), \ldots, r_{d-1}(z_1, \ldots, z_{n-1})$ for every $q(z_1, \ldots, z_n)$ such that

$$q(z_1, \ldots, z_n) - h(z_1, \ldots, z_n) p(z_1, \ldots, z_n) = \sum_{i=0}^{d-1} r_i(z_1, \ldots, z_{n-1}) z_n^i.$$

As in the case of polynomials in one variable the division is proven by writing

$$q(z_1, \ldots, z_n) = \sum_{i=0}^{s} q_i(z_1, \ldots, z_{n-1}) z_n^i$$

and then applying induction on s. If $s < d$ then it follows that $r_i = q_i$. Otherwise consider $q' = q - z_n^{s-d} q_s p$ which has degree $< s$ in the variable z_n.

Let us now consider two polynomials $p(z_1, \ldots, z_n)$ and $q(z_1, \ldots, z_n)$ that are monic of degree d with respect to z_n. From the Euclidean division algorithm there exist unique polynomials $h_i(z_1, \ldots, z_n)$ and $r_{ij}(z_1, \ldots, z_{n-1})$ with $i, j = 0, \ldots, d-1$ such that for each $i = 0, \ldots, d-1$ we have

$$z_n^i q(z_1, \ldots, z_n) - h_i(z_1, \ldots, z_n) p(z_1, \ldots, z_n) = \sum_{j=0}^{d-1} r_{ij}(z_1, \ldots, z_{n-1}) z_n^j.$$

The determinant $R(p, q)$ of the quadratic matrix (r_{ij}) is called the resultant of p and q.

In other words, $R(p, q) : \mathbb{C}^{n-1} \to \mathbb{C}$ is the function which at the point $(a_1, \ldots, a_{n-1}) \in \mathbb{C}^{n-1}$ has as value the determinant of the matrix of coefficients $r_{ij}(a_1, \ldots, a_{n-1})$. Denote the determinant of the quadratic matrix $r_{ab}, a \neq i, b \neq j$ of order $d-1$, multiplied by $(-1)^{i+j}$ by R^{ji}. Laplace's rule for evaluating determinants implies that

$$\sum_{i-1}^{d-1} R^{hi} r_{ij} = \begin{cases} R(p, q) & \text{if } h = j, \\ 0 & \text{if } h \neq j. \end{cases}$$

From the formula it follows easily that $R(p, q)$ is a polynomial in the variables $z_1, \ldots, z_{n-1}$. In fact, by induction on d we may assume that R^{0i} is a polynomial for each $i = 0, \ldots, d-1$. In what follows $R(p, q) = \sum_{i=0}^{d} R^{0i} r_{i0}$ is a polynomial.

LEMMA 3 *With the preceding notation there exists two polynomials $f, g \in \mathbb{C}[z_1, \ldots, z_n]$ such that*

$$R(p, q) = fq - gp.$$

Proof. We have seen that $\sum_{i=0}^{d-1} R^{0i} r_{i0} = R(p,q)$ and $\sum_{i=0}^{d-1} R^{0i} r_{ij} = 0$ if $j > 0$. Hence

$$\begin{aligned} R(p,q) &= \sum_{j=1}^{d-1} \left(\sum_{i=0}^{d-1} R^{0i} r_{ij} \right) z_n^j = \sum_{i=0}^{d-1} R^{0i} \left(\sum_{j=1}^{d-1} r_{ij} z_n^j \right) \\ &= \sum_{i=0}^{d-1} R^{0i} (z_n^i q - h_i p) = \left(\sum_{i=0}^{d-1} R^{0i} z_n^i \right) q - \left(\sum_{i=0}^{d-1} R^{0i} h_i \right) p = fq - gp. \end{aligned}$$

LEMMA 4 *With the preceeding notation if there exists a vector* $(a_1, \ldots, a_{n-1}) \in \mathbb{C}^{n-1}$ *such that* $q(a_1, \ldots, a_{n-1}, z_n)$ *is identically equal to 1 then* $R(p,q)(a_1, \ldots, a_{n-1}) = 1$.

Proof. The proof is purely conceptual and does not require any computation.

The uniqueness of the Euclidean division implies that for a fixed $i < d$ the polynomial

$$\sum_{j=0}^{d-1} r_{ij}(a_1, \ldots, a_{n-1}) z_n^j$$

coincides with the remainder of the division of $z_n^i q(a_1, \ldots, a_{n-1}, z_n)$ by $p(a_1, \ldots, a_{n-1}, z_n)$ and hence by hypothesis $z_n^i q(a_1, \ldots, a_{n-1}, z_n) = z_n^i$ from which

$$\sum_{j=0}^{d-1} r_{ij}(a_1, \ldots, a_{n-1}) z_n^j = z_n^i$$

and the matrix $(r_{ij}(a_1, \ldots, a_{n-1}))$ is the identity matrix.

5 Ideals

At this point the idea of using the resultant to provide a proof of Theorem 4 by induction on n seems obvious. The case $n = 1$ is exactly covered by Theorem 3. The approach works well if it is combined with the notion of ideals in $\mathbb{C}[z_1, \ldots, z_n]$ rather than with m-tuples of polynomials.

A subset $I \subset \mathbb{C}[z_1, \ldots, z_n]$ satisfying the conditions:

1. if $f, g \in I$ then $f + g \in I$,
2. if $f \in I$ and $h \in \mathbb{C}[z_1, \ldots, z_n]$ then $fh \in I$

is called an ideal. For example, 0 and $\mathbb{C}[z_1, \ldots, z_n]$ are ideals. More generally, if $p_1, \ldots, p_m]$ are polynomials in $\mathbb{C}[z_1, \ldots, z_n]$ then the set J of all expressions of the form $p_1 q_1 + \ldots, + p_m q_m$ with $q_1, \ldots, q_m \in \mathbb{C}[z_1, \ldots, z_n]$ is an ideal.

It follows that Theorem 4 is an immediate consequence of the following Theorem 6.

THEOREM 6 *Let $J \in \mathbb{C}[z_1, \ldots, z_n]$ be an ideal. Then there exists a vector $(a_1, \ldots, a_n) \in \mathbb{C}^n$ so that $p(a_1, \ldots, a_n) = 0$ for every $p \in J$ if and only if $1 \notin J$.*

Proof. We prove the theorem by using induction on n. For $n = 0$ the theorem is trivially true. Assume therefore that the theorem is true for polynomials in $n - 1$ variables.

The statement is obvious if $1 \in J$, or if $J = 0$. We assume therefore that $J \neq 0$, $1 \notin J$ and we prove that there exist a vector $(a_1, \ldots, a_n)$ that zeroes out all elements of J.

We first show this fact under the assumption that J contains a polynomial p_0 that is monic of degree $d > 0$ in z_n. Then we show how this additional assumption can be removed.

Let us consider the intersection $I = J \cap \mathbb{C}[z, \ldots, z_{n-1}]$. It is an ideal of $\mathbb{C}[z_1, \ldots, z_{n-1}]$ where $1 \notin I$. By Lemma 3, I contains all the resultants $R(p_0, q)$ as q varies in J.

By the inductive hypothesis there exists a vector $(a_1, \ldots, a_{n-1})$ that annihilates all the elements of J. If this were not the case the there would exist $p_1, \ldots, p_s \in J$ such that $p_j(a_1, \ldots, a_{n-1}, u_j) \neq 0$ for all j. The $s + 1$ polynomials $p_j(a_1, \ldots, a_{n-1}, z_n), j = 0, \ldots, s$ do not have common roots and hence by Theorem 3, there exists $h_0, \ldots, h_s \in \mathbb{C}[z_n]$ such that

$$\sum_{j=0}^{s} h_j(z_n) p_j(a_1, \ldots, a_{n-1}, z_n) = 1.$$

Let the h_j be interpreted as polynominals in $z_1, \ldots, z_n$. Then $q = \sum h_i p_i \in J$. By Lemma 4 $q(a_1, \ldots, a_{n-1}, z_n) = 1$ and hence $R(p_0, q)(a_1, \ldots, a_{n-1}) = 1$ contradicting the fact that $R(p_0, q) \in I$.

Now we want to see how we can remove the condition that J contains a polynomial monic in z_n. We note that the condition is not satisfied for the ideal of all polynomials in $\mathbb{C}[z_1, z_2]$ divisible by z_1.

If J contains a polynomial monic in any variable $z_i, i = 1, \ldots, n$ then the problem is solved simply by permuting the indices. This might still not enough.

Let us consider for example the ideal $J \in \mathbb{C}[z_1, z_2]$ of all polynomials that are divisible by $g = z_1 z_2 - 1$. None of the polynomials in J are monic with respect to one variable. We may avoid the problem in this case by a change of coordinates $z_1 = x + y$, $z_2 = x - y$ and the polynomial becomes $x^2 - y^2 - 1$ which is monic of degree 2 in x.

This trick might be generalized and one might be able to prove that "up to a linear coordinate transformation, every non-empty ideal contains a polynomial monic in the variable z_n" by using the following argument.

Let $f : \mathbb{C}^n \to \mathbb{C}^n$ be an invertible linear transformation, if $p : \mathbb{C}^n \to \mathbb{C}$ is a polynomial then the function

$$f^*p : \mathbb{C}^n \to \mathbb{C}, \quad f^*p(a_1, \ldots, a_n) = p(f(a_1, \ldots, a_n))$$

is also a polynomial.

In fact, if f is represented by the matrix (f_{ij}) we have $f^* z_i = \sum_j f_{ij} z_j$ and hence

$$f^*p(a_1, \ldots, a_n) = p\left(\sum_j f_{1j} z_j \ldots, \sum_j f_{nj} z_j\right).$$

Note that f^* commutes with the operations of sum and product:

$$f^*(p + q) = f^*p + f^*q, \quad f^*(pq) = (f^*p)(f^*q)$$

and hence if $J \in \mathbb{C}[z_1, \ldots, z_n]$ is an ideal then so is $f^*(J)$. The map $f^* : \mathbb{C}[z_1, \ldots, z_n] \to \mathbb{C}[z_1, \ldots, z_n]$ is invertible with inverse $(f^{-1})^*$. In other words a vector u zeroes out all elements of $f^*(J)$ if and only if $f(u)$ zeroes out all elements of J. In conclusion we can state that if the theorem of zeroes is valid for an ideal J then it is also valid for all ideals $f^*(J)$ that results from J after applying a linear invertible transformation.

It is enough to can prove that for every ideal $J \neq 0$ there exist an f as shown above such that the ideal $f^*(J)$ contains a polynomial which is monic of positive degree in z_n. Let us take an arbitrary non-zero polynomial $q \in J$ and write $q = q_0 + q_1 + \cdots + q_d$ where q_i is a linear combination of monomials of degree i and $q_d \neq 0$.

By Lemma 2 there exist a vector $u \in \mathbb{C}^n$ such that $q_d(u) \neq 0$. By multiplying q_d by a non-zero constant we may assume that $q_d(u) = 1$. If $d = 0$ then $1 \in J$ and there is nothing to prove. If $d > 0$ then clearly $u \neq 0$ and there exist a linear invertible map $f : \mathbb{C}^n \to \mathbb{C}^n$ such that $f(0, \ldots, 0, 1) = u$ where u coincides with the righthand column of the matrix that represents

f. Let us prove that f^*q is a polynomial that is monic of degree d in z_n. In fact every f^*q_i is a linear combination of monomials of degree i and we may write

$$f^*q_d(z_1,\ldots,z_n) = a_0(z_1,\ldots,z_{n-1})z_n^d + a_1(z_1,\ldots,z_{n-1})z_n^{d-1} + \cdots + a_d(z_1,\ldots,z_{n-1})$$

where each a_i is a linear combination of monomials of degree d. This finally proves that the constant a_0 is equal to 1 by evaluating f^*q_d at the point $(0,\ldots,0,1)$ and obtaining

$$a_0 = f^*q_d(0,\ldots 0,1) = q_d(f(0,\ldots,0,1)) = q_d(u) = 1.$$

This concludes the proof.

6 Das is nicht Mathematik - das ist Theologie!

This famous comment was made by Paul Gordan, a well-known algebraist in Germany of the nineteenth century, when he saw the work of the young Hilbert where two of the most important theorems of algebra were stated and proven. These theorems were the basis theorem and the theorem of zeroes.

In the monograph of Hilbert these two results are preparatory to the proof of the theorem of the finiteness of the invariants, a theorem that generalizes and greatly simplifies a theorem which Gordon proved twenty years earlier.

The, somewhat peevish, comment of Gordan arose from the fact that the proof of Hilbert's theorem is non-constructive and the theorem is limited to proving the existence of certain objects without giving an explicit algorithm for their description. There is probably an element of professional envy in the statement as well.

The basis theorem of Hilbert states that, for every ideal J in $\mathbb{C}[z_1,\ldots,z_n]$ there exists a finite set of polynomials $p_1,\ldots,p_m \in J$ such that J coincide with all expressions $p_1q_1 + \cdots + p_mq_m$ as $q_1,\ldots,q_m$ range over $\mathbb{C}[z_1,\ldots,z_n]$. Therefore, by virtue of the basis theorem, Theorems 4 and 6 are equivalent.

The statement of Hilbert on the theorem of the zeroes includes both Hilbert's basis theorem and what is known today as the strong form of the theorem of zeroes, a further generalization of Theorem 4, which can be stated as follows:

THEOREM 7 *(Hilbert; see [4]). Let J be an ideal in $\mathbb{C}[z_1, \ldots, z_n]$ and let $V(J) \subset \mathbb{C}^n$ denote the set of vectors that annihilates all elements of J. Then there exists an integer $d > 0$, depending on J, such that if $f \in \mathbb{C}[z_1, \ldots, z_n]$ is annihilated by $V(J)$ then $f^d \in J$.*

Even though the proof of this theorem is a simple consequence of Theorem 6 we omit it here since it can be found in almost every algebraic geometry text (see, for example, [2, 5, 8, 9]).

The attentive reader might have noticed that in the proof of these theorems no properties of the complex numbers have been used except that they form a closed algebraic field. Hence, if $\mathbb{C}$ is replaced by any other algebraically closed field in Theorems 6 and 7 then these theorems are still valid.

As a conclusion we want to make some comments on the bibliography. To list all the books that contain proofs of the Nullstellensatz would be an enormous task, and hence we have limited the selection to a short but significant list. The texts [1, 2, 5, 8, 9] are introductory texts in algebraic geometry where one might find the most varied applications of Hilbert's theorems. It is also clear that [4] is not written by Hilbert who in 1993 is not longer in a position to dedicate himself to earthly mathematics. It is a revision of notes taken by a student in a lecture series that Hilbert held at the University of Göttingen in the decennium 1890-1900. The book of Herstein [3] contains all that is needed for understanding this paper (and much more).

References

[1] Cox, D. A., Little, J. and O'Shea D.: *Using Algebraic Geometry.* Second Ed., Springer-Verlag (2004).

[2] Fulton, W.: *Algebraic Curves: An Introduction to Algebraic Geometry.* Benjamin (1969).

[3] Herstein, I. N.: *Abstract Algebra.* 3rd. ed. John Wiley (1996).

[4] Hilbert, D.: *Theory of Algebraic Invariants.* Cambridge University Press (1993).

[5] Manetti, M.: *Corso Introduttivo alla Geometria Algebraica.* Notes for students attending courses in the Scuola Normal Superiore (248 pages) (1998).

[6] Manetti, M.: *Nullstellensatz per tutti.* paper in *miscellanea Franco Conti*, Centro di Ricerca Matematica Ennio De Giorgi, online at http://www.crm.sns.it/publications/articoli.html (March 2, 2006).

[7] Noether, M.: *Paul Gordan.* Mathematische Annalen **75** pp. 1-41 (1914)

[8] Reid, M.: *Undergraduate Algebraic Geometry.* Cambridge University Press (1988).

[9] Shafarevich, I. R.: *Basic Algebraic Geometry.* Springer-Verlag (1972).