Hilbert's Nullstellensatz over the complex numbers

Klaus Pommerening
Fachbereich Mathematik der Johannes-Gutenberg-Universität
Mainz, Federal Republic of Germany

April 1982

The aim of this note is a very simple proof of Hilbert's Nullstellensatz over the field of complex numbers. In fact we use only that the base field k is algebraically closed and uncountably infinite. This proof is of unknown origin, I learned it from H. J. Fendrich.

We denote by $k[T]$ the polynomial ring in n variables $T = (T_1, \ldots, T_n)$. For a subset $F \subseteq k[T]$ the zero set is

$$V(F) = \{x \in k^n \mid f(x) = 0 \text{ for all } f \in F\},$$

i. e. the set of common zeroes (in German: Nullstellen) of all polynomials in F.

Theorem 1 (Weak Nullstellensatz) *Let $\mathfrak{a} \subset k[T]$ be a proper ideal. Then $V(\mathfrak{a}) \neq \emptyset$.*

For the proof we use the lemma:

Lemma 1 *Let $L \supseteq k$ an extension field that is finitely generated as a k-algebra. Then L is algebraic over k.*

Proof. Let $\{u_1, \ldots, u_n\}$ be a system of generators of the k-algebra L. Then the countably many monomials $u_1^{m_1} \cdots u_n^{m_n}$ span the vector space L over k. Therefore $\dim_k L$ is countable.

Now assume there is a $u \in L$ that is not algebraic over k. Then (*this is where our assumption on k enters the proof*) the uncountably many different elements $\frac{1}{u-c}$ with arbitrary $c \in k$ are linearly independent over k: Take a linear combination $\frac{b_1}{u-c_1} + \cdots + \frac{b_m}{u-c_m} = 0$ with $b_i, c_i \in k$ and clear the denominators. This gives a polynomial equation for u with coefficients in k, contradiction. Therefore $\dim_k L$ is uncountably infinite – contradiction. $\diamond$

For the proof of Theorem 1 we can replace $\mathfrak{a}$ by a larger ideal. Therefore we may assume that $\mathfrak{a} = \mathfrak{m}$ is a maximal ideal. Then we have a natural ring homomorphism φ from the following commutative diagram where ν is the canonical map:

$$\begin{tikzcd} k \arrow[rr, "\varphi"] \arrow[dr, "\subseteq"'] & & k[T]/\mathfrak{m} \\ & k[T] \arrow[ur, "\nu"'] & \end{tikzcd}$$

Because k is a field φ is injective. Lemma 1 yields that $k[T]/\mathfrak{m}$ is algebraic over $\varphi(k)$. Because k, and $\varphi(k)$, is algebraically closed, $\varphi(k) = k[T]/\mathfrak{m}$. Let $x_i = \varphi^{-1}(\nu(T_i))$ for $i = 1, \dots, n$. We claim x is a zero of $\mathfrak{m}$.

Let $f = \sum_{r \in \mathbb{N}^n} a_r T^r \in \mathfrak{m}$. Then

$$f(x_1, \dots, x_n) = \sum_r a_r x_1^{r_1} \cdots x_n^{r_n} = \varphi^{-1}(\sum_r a_r \nu(T)^r) = \varphi^{-1}(\nu(f)) = 0.$$

Theorem 1 is proven.

Corollary 1 *Let $F \subseteq k[T]$ be a set of polynomials without a common zero in k^n. Then there are $f_1, \dots, f_m \in F$ and $g_1, \dots, g_m \in k[T]$ such that $g_1 f_1 + \cdots + g_m f_m = 1$.*

Proof. We have to show that $1 \in (F) = \mathfrak{a}$, the ideal generated by F. But because $V(\mathfrak{a}) = \emptyset$, we have $\mathfrak{a} = k[T] \ni 1$. $\diamond$

Appendix 1: The strong Nullstellensatz

The strong Nullstellensatz follows from the weak one also in a quite simple way by the classic Rabinowitsch trick. Remember that for a subset $M \subseteq k^n$ the vanishing ideal is defined as

$$I(M) = \{f \in k[T] \mid f(x) = 0 \text{ for all } x \in M\}.$$

Note that $I(M)$ is a radical ideal: if f vanishes on M so does every power f^m. In particular for an ideal $\mathfrak{a} \subseteq k[T]$ we have $IV(\mathfrak{a}) \supseteq \operatorname{rad} \mathfrak{a}$.

Theorem 2 (Strong Nullstellensatz) *For every ideal $\mathfrak{a} \subset k[T]$ we have $IV(\mathfrak{a}) = \operatorname{rad} \mathfrak{a}$.*

Proof. Let $f \in IV(\mathfrak{a})$. We may assume $f \neq 0$. Consider the polynomial ring $A = k[T, T_0] = k[T_0, T_1, \dots, T_n]$ in one more variable. Let $g := 1 + T_0 f \in A$, and $\mathfrak{A} \subseteq A$, the ideal $\mathfrak{A} = (g, \mathfrak{a})$ generated by g and $\mathfrak{a}$. In k^{n+1} we have $V(\mathfrak{A}) = \emptyset$; otherwise take a point $(t_0, t) \in V(\mathfrak{A})$, $t = (t_1, \dots, t_n)$, then $h(t_0, t) = h(t) = 0$ for all $h \in \mathfrak{a}$, hence $f(t) = 0$, hence $0 = g(t_0, t) = 1 + t_0 \cdot f(t) = 1$, contradiction. The weak Nullstellensatz gives $\mathfrak{A} = A$. Because $1 \in \mathfrak{A}$ we have $h, h' \in A$ and $f' \in \mathfrak{a}$ such that $1 = hg + h'f'$.

Now substituting $T_0 \mapsto -\frac{1}{f}$ gives a ring homomorphism

$$\varphi \colon A = k[T_0, T] \longrightarrow k(T).$$

We have $\varphi(g) = 0$, $1 = \varphi(1) = \varphi(h') \cdot f'$ and

$$\varphi(h') = h'(-\frac{1}{f}, T_1, \ldots, T_n) = \frac{\tilde{h}}{f^r} \quad \text{with } \tilde{h} \in k[T] \text{ and a suitable } r \geq 1.$$

This gives $f^r = \tilde{h} \cdot f' \in \mathfrak{a}$. $\diamond$

A more elementary wording of the strong Nullstellensatz reads as follows:

Corollary 2 *Let $f, f_1, \ldots f_m \in k[T]$ be polynomials such that f vanishes on each common zero of $f_1, \ldots, f_m$. Then there are $h_1, \ldots h_m \in k[T]$ and an exponent $r \geq 1$ such that $f^r = h_1 f_1 + \cdots + h_m f_m$.*

Proof. Consider the ideal $\mathfrak{a} = (f_1, \ldots, f_m)$ generated by the f_i's. Then $f \in \operatorname{rad} \mathfrak{a}$, whence a power $f^r \in \mathfrak{a}$. $\diamond$

Appendix 2: A general proof

To get a proof of the Nullstellensatz (weak or strong) without the assumption on the cardinality of k we only need a proof of Lemma 1 in the general case. The simplest way is using the theory of integral ring extensions, in particular:

Theorem 3 (Hilbert-Noether normalisation) *Let k be a field and $A = k[f_1, \ldots, f_n]$, a finitely generated k-algebra. Then there are algebraically independent $g_1, \ldots, g_r \in A$ such that A is integral over the polynomial ring $k[g_1, \ldots, g_r]$.*

This dates back also to [1]. For a modern proof take any textbook on algebra, for example [2].

Now for the proof of Lemma 1 we get $r = 0$ in Theorem 3 because there is no room for more algebraically independent elements. This means that L is integral over k, hence algebraic.

Historical note

Hilbert's original proof of the (strong) Nullstellensatz is in his famous paper [1, §3] on invariant theory, it takes about 5 pages. Hilbert implicitly took the complex numbers as base field, so the present short proof is completely adequate. Note however that Hilbert's proof works over any algebraically closed field, and that his statement of the theorem is slightly more general. Rabinowitsch's trick is in the 1 page (à 13 lines) paper [3].

References

[1] D. Hilbert: Über die vollen Invariantensysteme. Math. Ann. 42 (1893), 313–373.

[2] S. Lang: *Algebra*. Addison-Wesley, Reading Mass. 1965.

[3] J. L. Rabinowitsch: Zum Hilbertschen Nullstellensatz. Math. Ann. 102 (1930), 520.