A NOTE ON HILBERT'S NULLSTELLENSATZ

RICHARD BRAUER

In a recent paper, O. Zariski\(^1\) has given a very simple proof of Hilbert's "Nullstellensatz." We give here another proof which while slightly longer is still more elementary.

Let \(K\) be an algebraically closed field. We consider a system of conditions

\[
\begin{align*}
f_1(x_1, x_2, \cdots, x_n) &= 0, \\
& \quad \cdots, \\
f_r(x_1, x_2, \cdots, x_n) &= 0; \\
g(x_1, x_2, \cdots, x_n) &\neq 0
\end{align*}
\]

where \(f_1, f_2, \cdots, f_r\), and \(g\) are polynomials in \(n\) indeterminates \(x_1, x_2, \cdots, x_n\) with coefficients in \(K\). The theorem states that if the conditions (1) cannot be satisfied by any values \(x_i\) of \(K\),\(^2\) a suitable power of \(g\) belongs to the ideal \((f_1, f_2, \cdots, f_r)\).\(^3\)

PROOF. Let \(k\) be the number of \(x_j\) which actually appear in \(f_1, f_2, \cdots, f_r\) and let \(x_1\) be the \(x_j\) of this kind with the smallest subscript. Denote by \(l\) the number of \(f_p\) in which \(x_1\) actually appears. Let \(m\) be the smallest positive value which occurs as degree in \(x_1\) of one of the \(f_p\).\(^4\) Now define a partial order for the different systems (1) using a lexicographical arrangement. If (1*) is a second system of the same type as (1) and if \(k^*, l^*,\) and \(m^*\) have the corresponding significance, we shall say that (1*) is lower than (1) if either \(k^*<k\), or \(k^*=k\) and \(l^*<l\), or \(k^*=k\), \(l^*=l\), and \(m^*<m\).

Suppose now that Hilbert's theorem is false. Then there exist systems (1) which are not satisfied by any values \(x_j\) in \(K\), and for which no power of \(g\) lies in \((f_1, f_2, \cdots, f_r)\). Choose such a system (1) taking it as low as possible. Then for all systems (1*) lower than (1) the theorem will hold.

If \(k, l, m\) have the same significance as above, one of the \(f_p\), say

\(f_1\), is a system (1) which is not satisfied by any values \(x_j\) in \(K\), and for which no power of \(g\) lies in \((f_1, f_2, \cdots, f_r)\). Choose such a system (1) taking it as low as possible. Then for all systems (1*) lower than (1) the theorem will hold.

Received by the editors November 1, 1947.


\(^2\) If we wish to formulate the theorem for arbitrary fields \(K\) as it is done in Zariski's paper, we have to consider a system of values \(x_1, x_2, \cdots, x_n\) belonging to extension fields of finite degree over \(K\). If no such system satisfies the conditions (1), the same conclusion can be drawn. The same proof can be used.

\(^3\) We do not use anything from the theory of ideals except the notation \((f_1, f_2, \cdots, f_r)\) for the set of all polynomials of the form \(P_1 f_1 + P_2 f_2 + \cdots + P_r f_r \subseteq K[x_1, x_2, \cdots, x_n]\), and facts which are immediate consequences.

\(^4\) The numbers \(k, l, m\) do not depend on \(g\).
HILBERT’S NULLSTELLENSATZ 895

$f_1$, has degree $m$ in $x_i$. Set

\[(2) \quad f_1 = hx_i^m + f_1^*\]

where $h$ is the highest coefficient of $f_1$ as polynomial in $x_i$.

Neither of the following systems:

\[(3) \quad f_1 = 0, f_2 = 0, \ldots, f_r = 0, h = 0; g \neq 0;\]
\[(4) \quad f_1 = 0, f_2 = 0, \ldots, f_r = 0; hg \neq 0\]

can be satisfied by values $x_j$ of $K$, since otherwise (1) would be satisfied by the same values. Replace (3) by

\[(3^*) \quad f_1^* = 0, f_2 = 0, \ldots, f_r = 0, h = 0; g \neq 0.\]

Then (3*) too cannot be satisfied by values $x_j$ in $K$. Clearly, (3*) is lower than (1). Since Hilbert’s theorem then holds for (3*), we have

\[(5) \quad g^* \subseteq (f_1, f_2, \ldots, f_r, h)\]

for a suitable exponent $s$.

In the discussion of (4), we distinguish two cases.

Case A. $\ell \geq 2$. Then $x_i$ appears in some $f_\rho$ with $\rho \geq 2$, say in $f_2$. Divide $f_2$ by $f_1$ considering both as polynomials in $x_i$ alone. If we multiply by a suitable power $h^s$ of the highest coefficient $h$ of $f_1$, we can remove the denominators and set

\[h^s f_2 = Q f_1 + R\]

where $Q$ and $R$ are polynomials in all the $x_j$ and where $R$ is of degree smaller than $m$ in $x_i$. The system.

\[(4^*) \quad f_1 = 0, R = 0, f_3 = 0, \ldots, f_r = 0; hg \neq 0\]

cannot be satisfied by any values $x_j$ in $K$, since (4*) would imply (4). But (4*) is lower than (1) and hence Hilbert’s theorem holds for (4*). Then, for a suitable exponent $t$, $(hg)^t \subseteq (f_1, R, f_3, \ldots, f_r)$.

Replacing $R$ by $h^g f_2 - Q f_1$, we obtain

\[(6) \quad h^t g^t \subseteq (f_1, f_2, \ldots, f_t).\]

It follows from (5) that $g^{t+t^t}$ belongs to

\[g^t(f_1, f_2, \ldots, f_r, h^t) \subseteq g^t(f_1, f_2, \ldots, f_r, h^t) \subseteq (f_1, f_2, \ldots, f_r, h^t).\]

Then (6) shows that $g^{t+t^t} \subseteq (f_1, f_2, \ldots, f_r)$, in contradiction to the assumption that no power of $g$ belongs to $(f_1, f_2, \ldots, f_r)$.

Case B. $\ell = 1$. If we succeed again in establishing (6), we have the same contradiction as in the Case A, and Hilbert’s theorem will be proved.
In this case divide \( g^{m+1} \) by \( f_1 \), considering both as polynomials in \( x_i \) alone. We may then set

\[
h^q g^{m+1} = Qf_1 + R
\]

where \( q \) is again a positive integer, where \( Q \) and \( R \) are polynomials in all the \( x_i \), and where the degree of \( R \) in \( x_i \) is smaller than \( m \). Consider here the system

\[
(f_2 = 0, f_3 = 0, \cdots, f_r = 0; hR \neq 0)\tag{4**}
\]

We wish to show that \((4**)\) cannot be satisfied by values \( x_i \) in \( K \).

If this were not so, choose a system of values \( x_1^*, x_2^*, \cdots, x_n^* \) of \( K \) which satisfy the conditions \((4**)\). Replace here \( x_i^* \) by an indeterminate \( x_i \), leaving all the other \( x_j^* \) fixed. The conditions \( f_2 = 0, f_3 = 0, \cdots, f_r = 0, \) and \( h \neq 0 \) are not affected, since \( x_i \) does not appear in them. As shown by \((2)\), the equation \( f_1 = 0 \) is of degree \( m \) in \( x_i \) and has therefore \( m \) roots \( x_i^{(0)} \) in the algebraically closed field \( K \). If \( g \) would not vanish when we set \( x_i = x_i^{(0)} \), we would thus find a system of values of \( K \) which satisfies all the conditions \((4)\) and this is impossible. Hence \( g \) must vanish when we set \( x_i = x_i^{(0)} \) and it follows from \((7)\) that the same holds for \( R \). Moreover, as root of the equation \( R = 0 \) in \( x_i \), the quantity \( x_i^{(0)} \) has the same multiplicity as for \( f_1 = 0 \). Thus the equation \( R = 0 \) of degree less than \( m \) in \( x_i \) has \( m \) roots \( x_i = x_i^{(0)} \). Consequently, \( R \) must vanish identically in \( x_i \). However, for \( x_i = x_i^{*} \), we had \( R \neq 0 \), as shown by \((4**)\). Thus the assumption that \((4**)\) can be satisfied by values of \( K \) leads to a contradiction.

If \( r > 1 \), the system \((4**)\) is lower than \((1)\) and we may again apply Hilbert's theorem. This shows that a suitable power \((hR)^v\) belongs to \((f_2, f_3, \cdots, f_r)\). This still holds for \( r = 1 \), when we interpret \((f_2, f_3, \cdots, f_r)\) as the zero ideal. Indeed, since \((4**)\) cannot be satisfied, \( hR \) must vanish for all systems of values \( x_i \) of \( K \), and hence identically.\(^6\) Now \((7)\) yields

\[
(h^{q+1}g^{m+1})^v = (hQf_1 + hR)^v \subseteq (f_1, f_2, \cdots, f_r).
\]

If the integer \( t \) satisfies the inequalities \( t \geq (q+1)v, t \geq (m+1)v \), then \((6)\) will hold again. But this is all we had to show and the proof of Hilbert's theorem is complete.

\[\text{University of Toronto}\]

---

\(^6\) If \( r = 1 \), the system \((4**)\) is to consist only of the inequality \( hR \neq 0 \).

\(^5\) We assume the elementary theorem that if a polynomial in several variables vanishes for all systems of values of the underlying field \( K \) and if \( K \) is either infinite or contains at least sufficiently many elements, the polynomial vanishes identically.