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

$$\begin{aligned} &f_1(x_1, x_2, \cdots, x_n) = 0, \qquad f_2(x_1, x_2, \cdots, x_n) = 0, \\ (1) \qquad &\cdots, f_r(x_1, x_2, \cdots, x_n) = 0; \\ &g(x_1, x_2, \cdots, x_n) \neq 0 \end{aligned}$$

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_i be the x_j of this kind with the smallest subscript. Denote by l the number of f_ρ in which x_i actually appears. Let m be the smallest positive value which occurs as degree in x_i of one of the f_ρ.[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_ρ, say

Received by the editors November 1, 1947.

[1] Bull. Amer. Math. Soc. vol. 53 (1947) pp. 362–368.

[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 $P_1f_1 + P_2f_2 + \cdots + P_rf_r$, $P_j \in K[x_1, x_2, \cdots, x_n]$, and facts which are immediate consequences.

[4] The numbers k, l, m do not depend on g.

f_1, has degree m in x_i. Set

$$f_1 = hx_i^m + f_1^* \tag{2}$$

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

Neither of the following systems:

$$f_1 = 0, f_2 = 0, \cdots, f_r = 0, h = 0; g \neq 0; \tag{3}$$

$$f_1 = 0, f_2 = 0, \cdots, f_r = 0; hg \neq 0 \tag{4}$$

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

$$f_1^* = 0, f_2 = 0, \cdots, f_r = 0, h = 0; g \neq 0. \tag{3*}$$

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

$$g^s \in (f_1, f_2, \cdots, f_r, h) \tag{5}$$

for a suitable exponent s.

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

Case A. $l \geqq 2$. Then x_i appears in some f_ρ with $\rho \geqq 2$, 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^q of the highest coefficient h of f_1, we can remove the denominators and set

$$h^q f_2 = Qf_1 + R$$

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.

$$f_1 = 0, R = 0, f_3 = 0, \cdots, f_r = 0; \quad hg \neq 0 \tag{4*}$$

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, $(hg)^t \in (f_1, R, f_3, \cdots, f_r)$.

Replacing R by $h^q f_2 - Qf_1$, we obtain

$$h^t g^t \in (f_1, f_2, \cdots, f_r). \tag{6}$$

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

$$g^t(f_1, f_2, \cdots, f_r, h)^t \subseteq g^t(f_1, f_2, \cdots, f_r, h^t) \subseteq (f_1, f_2, \cdots, f_r, g^t h^t).$$

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

Case B. $l = 1$. 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

$$h^q g^{m+1} = Qf_1 + R \tag{7}$$

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

$$f_2 = 0, f_3 = 0, \cdots, f_r = 0; hR \neq 0.\text{[5]} \tag{4**}$$

We wish to show that (4**) cannot be satisfied by values x_j 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 $x_i^{(\mu)}$ in the algebraically closed field K. If g would not vanish when we set $x_i = x_i^{(\mu)}$, 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 $x_i = x_i^{(\mu)}$ and it follows from (7) that the same holds for R. Moreover, as root of the equation $R = 0$ in x_i, the quantity $x_i^{(\mu)}$ 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 $x_i = x_i^{\mu}$. 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

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

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

UNIVERSITY OF TORONTO

[5] If $r = 1$, the system (4**) is to consist only of the inequality $hR \neq 0$.

[6] 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.