On the Resolvent Problem (*) (**).

RICHARD BRAUER (Cambridge, Mass, U.S.A.)

TO BENIAMINO SEGRE

Summary. — *See the Introduction.*

1. — Introduction.

In the following, F will be a fixed field which will be assumed to be of characteristic 0. If A and $B \subset A$ are two extension fields of F and if t is a positive integer, we shall write $p(B:A) \leq t$, if there exist elements $\lambda \in B$ which satisfy the following conditions:

(i) $B = A(\lambda)$

(ii) λ satisfies an equation

$$a_0 \lambda^r + a_1 \lambda^{r-1} + \dots + a_r = 0, \quad (a_0 \neq 0)$$

in which each a_j has the form

$$a_j = f_j(u_1, u_2, \dots, u_t)$$

where $f_j \in F[U_1, U_2, \dots, U_t]$ is a polynomial of t indeterminates $U_1, U_2, \dots, U_t$ with coefficients in F and where $\{u_1, u_2, \dots, u_t\}$ is a system of t elements of A . In other words, λ is the value of an algebraic function of t variables over F for arguments taken in A . We set $p(B:A) = 0$, if $B = A(\lambda)$ with λ algebraic over F .

Then Hilbert's resolvent problem can be stated as follows. Let k be an extension field of F and let f be a polynomial of positive degree n of an indeterminate X with coefficients in k . Let $t \geq 0$ be an integer. Does there exist a finite tower

(1) $k = k_0 \subseteq k_1 \subseteq \dots \subseteq k_m$

(*) Entrata in Redazione il 7 maggio 1973.

(**) This research has been supported by NSF Grant GP 30809X.

of extension fields such that k_m contains a root of f and that

$$(2) \quad p(k_j:k_{j-1}) \leq t \quad \text{for } j = 1, 2, \dots, m?$$

We shall denote by $p_k(f)$ the smallest non-negative integer t for which the answer to the question is in the affirmative. It is clear that $p_k(f)$ is at most equal to the transcendence degree of k over Γ .

It is well-known and proved easily by the use of Tschirnhausen transformations that $p_k(f) \leq 1$ if the degree n of f is less than or equal to 5. Likewise, $p_k(f) \leq n - 4$ for $n \geq 5$. It came rather as a surprise when HILBERT [2] proved that, in the case of the general polynomial f of degree nine, $p_k(f) \leq 4$. Subsequently, WIMAN [7] showed that $p_k(f) \leq n - 5$ for $n \geq 9$. Later, B. SEGRE [4] obtained the result that $p_k(f) \leq n - 6$ for $n \geq 157$. It was observed independently by him [5] and by the author [1] that, for every positive integer r , there exist bounds n_r depending on r such that

$$(3) \quad p_k(f) \leq n - r$$

for all polynomials f of a degree $n \geq n_r$. In fact, this still remains true, if stronger conditions are imposed on the tower (1). For instance, one may require in the case of the general polynomial f that, for $j = 1, 2, \dots, m - 1$, the field k_j is obtained from k_{j-1} by the adjunction of a radical of an element of k_{j-1} (which of course implies $p(k_j:k_{j-1}) \leq 1$).

We shall obtain here an explicit value of n_r such that (3) holds for $n \geq n_r$. We shall prove:

THEOREM 1. — *Let k be an extension field of the given field Γ of characteristic 0 and let f be a polynomial of degree n of an indeterminate X with coefficients in Γ . Let $r \geq 4$ be an integer. If $n \geq (r - 1)! + 1$, then $p_k(f) \leq n - r$.*

Thus, for $r = 5$, we have to require $n \geq 25$. This shows that our method is not strong enough to yield the Hilbert-Wiman result quoted above. On the other hand, for $r = 6$, we have to require that $n \geq 121$ which improves the previously known results.

The proof of Theorem 1 is given in § 2. It is based on Tschirnhausen transformations, and it is rather obvious. As is discussed in § 3, our proof yields a fairly explicit construction of a suitable tower (1) in the case of a general polynomial f . § 4 contains some supplementary remarks for arbitrary f .

Our discussion will also show that Theorem 1 remains valid, if the definition of $p_k(f)$ is changed by requiring that k_m in (1) includes a splitting field of f .

2. — Proof of Theorem 1.

Let k be an extension field of Γ and let

$$(4) \quad f = X^n + c_1 X^{n-1} + \dots + c_n$$

be a polynomial of degree $n > 0$ of an indeterminate X with coefficients $c_i \in k$.

Let $\{x_1, x_2, \dots, x_n\}$ be a full system of roots of f in an algebraic closure $\bar{k}$ of k . Let $U_0, U_1, \dots, U_{r-1}$ be r indeterminates for the given number r . Set

$$(5) \quad Y_i = U_0 + U_1 x_i + \dots + U_{r-1} x_i^{r-1}$$

for $i = 1, 2, \dots, n$.

We form the power sums of the x_i and the Y_i ,

$$(6) \quad s(\nu) = \sum_{i=1}^n x_i^\nu \quad S_\nu = \sum_{i=1}^n Y_i^\nu$$

$\nu = 0, 1, 2, \dots$ (It is for typographical reasons that we use the notation $s(\nu)$ rather than s_ν). Then

$$(7) \quad S_\nu = \sum_{i_1, i_2, \dots, i_\nu=0} U_{i_1} U_{i_2} \dots U_{i_\nu} s(i_1 + i_2 + \dots + i_\nu).$$

If j_0 of the indices i_λ are 0, if j_1 of the i_λ are 1, ..., if j_{r-1} of the i_λ are $r-1$, the term of the sum in (7) can be written as

$$U_0^{j_0} U_1^{j_1} \dots U_{r-1}^{j_{r-1}} s(j_1 + 2j_2 + \dots + (r-1)j_{r-1})$$

with

$$(8) \quad j_0 + j_1 + \dots + j_{r-1} = \nu.$$

Then (7) takes the form

$$(9) \quad S_\nu = \sum_{[j]} \gamma_{[j]}^{(\nu)} U^{[j]} s(j_1 + 2j_2 + \dots + (r-1)j_{r-1})$$

where $[j]$ ranges over the systems $(j_0, j_1, \dots, j_{r-1})$ of non-negative integers which satisfy the condition (8), where $U^{[j]}$ is the power product

$$(10) \quad U^{[j]} = U_0^{j_0} U_1^{j_1} \dots U_{r-1}^{j_{r-1}}$$

and where $\gamma_{[j]}^{(\nu)}$ is a positive integer. In fact, $\gamma_{[j]}^{(\nu)} = \nu! / (j_0! j_1! \dots j_{r-1}!)$.

The $r-1$ equations

$$(11) \quad S_1 = 0, \quad S_2 = 0, \quad \dots, \quad S_{r-1} = 0$$

define an algebraic set V in an $(r-1)$ -dimensional projective space over k . There exist then points u of V with coordinates in $\bar{k}$. Since the product of the degrees of the equations (11) is $(r-1)!$, it is well known that the point u of V can be chosen such that, for a suitable choice of its coordinates $(u_0, u_1, \dots, u_{r-1})$, we have

$$(12) \quad [k(u_0, u_1, \dots, u_{r-1}); k] \leq (r-1)!.$$

This point will be discussed in detail below in § 3 and § 4.

As remarked in § 1, Theorem 1 holds for $r=4$. (It would even suffice to assume $n \geq 5$ instead of $n \geq 7$ here.) We may then assume that $r \geq 5$ and that Theorem 1 holds when r is replaced by an integer $r' < r$.

Let u^* be a primitive element of $k(u_0, u_1, \dots, u_{r-1})$ over k , let f^* denote the minimal k -polynomial for u^* and let n^* be the degree of f^* . By (12), $n^* \leq (r-1)!$. We claim that

$$(13) \quad p_k(f^*) \leq n - r.$$

Indeed, if $n^* > (r-2)!$, we can apply Theorem 1 with r replaced by $r-1$ and find

$$p_k(f^*) \leq n^* - (r-1) \leq (r-1)! - (r-1).$$

Since by assumption $n > (r-1)!$, then (13) holds. On the other hand, if $n^* \leq (r-2)!$, we have

$$p_k(f^*) \leq (r-2)! < (r-1)! - (r-1) \leq n - r$$

and (13) holds again. It follows that there exists a tower of fields

$$k_0 = k \subseteq k_1 \subseteq \dots \subseteq k_q$$

such that

$$(14) \quad p(k_j : k_{j-1}) \leq n - r \quad \text{for } j = 1, 2, \dots, q$$

and that k_q contains a root of f^* . Since we may replace u^* above by a conjugate over k with a corresponding change of the point u , we may assume that u^* and hence $u_0, u_1, \dots, u_{r-1}$ lie in k_q .

With $u_0, u_1, \dots, u_{r-1}$ now chosen, set

$$(15) \quad y_i = u_0 + u_1 x_i + \dots + u_{r-1} x_i^{r-1}$$

for $i = 1, 2, \dots, n$ and take

$$g(X) = \prod_{i=1}^n (X - y_i) = X^n + b_1 X^{n-1} + \dots + b_n.$$

Then $g \in k_q[X]$. Since the first r power sums of the y_i vanish by (11), Newton's formulas yield

$$b_1 = b_2 = \dots = b_{r-1} = 0.$$

Case I. Not all b_i are 0.

Let b denote the b_j with the smallest subscript j which does not vanish. Then $j \geq r$. Let z denote a value of $\sqrt[j]{b}$ and set $k_{q+1} = k_q(z)$. The coefficients of

$$\prod_{z=1}^n (X - y_i z^{-1}) = X^n + X^{n-j} + b_{j+1} z^{-j-1} X^{n-j-1} + \dots + b_n z^{-n}$$

lie in k_{q+1} . If we now take $k_{q+2} = k_{q+1}(y_1 z^{-1})$, it is clear that

$$(16) \quad p(k_{q+1}:k_q) \leq 1, \quad p(k_{q+2}:k_{q+1}) \leq n - r.$$

Case II. All b_i are 0.

Take here $k_{q+2} = k_{q+1} = k_q$. Of course, (16) holds again.

In either case, $y_1 \in k_{q+2}$. Note that we cannot have $u_1 = u_2 = \dots = u_{r-1} = 0$, since then all y_i were equal to $u_0 \neq 0$ and the coefficient b_1 of $g(X)$ would not vanish. If we now set $k_{q+3} = k_{q+2}(x_1)$, then (15) implies that

$$(17) \quad p(k_{q+3}:k_{q+2}) < r \leq n - r.$$

Since k_{q+3} contains x_1 , it follows from (14), (16), and (17) that $p_k(f) \leq n - r$ as we wished to show.

COROLLARY. — *If $n \geq (r-1)! + (r-1)$, we can choose a tower (1) with $m = 4$ such that (2) holds with $t = n - r$ and that k_4 contains a root of f .*

Indeed, if u^* and n^* have the same significance as above, we have

$$p(k(u^*):k) \leq n^* - 1 \leq (r-1)! - 1 \leq n - r$$

and we may take $q = 1$ in the preceding proof.

No induction is needed in the case of the Corollary and the construction of the tower (1) is fairly explicit.

3. — The case of the general polynomial.

We shall discuss now the construction of the point u of the algebraic set V in the case that f in (4) is the general polynomial of degree n , i.e. that $c_1, c_2, \dots, c_n$ are algebraically independent over Γ and that $k = \Gamma(c_1, c_2, \dots, c_n)$. We shall show that Bezout's Theorem applies. Actually a weaker assumption will suffice.

THEOREM 2. — *Suppose that $s(1), s(2), \dots, s((r-1)^2)$ are algebraically independent over Γ . Let*

$$(18) \quad T_0 = Z_0 U_0 + Z_1 U_1 + \dots + Z_{r-1} U_{r-1}$$

denote a linear form with indeterminate coefficients Z_i . Then the resultant

$$R(S_{r-1}, S_{r-2}, \dots, S_1, T_0)$$

of the forms $S_{r-1}, S_{r-2}, \dots, S_1, T_0$ in $U_0, U_1, \dots, U_{r-1}$ is a form of degree $(r-1)!$ in $Z_0, Z_1, \dots, Z_{r-1}$ in which the coefficient of $Z_0^{(r-1)!}$ is different from 0.

PROOF. — Let T_ν be a form of degree $\nu \geq 1$ in $U_0, U_1, \dots, U_{r-1}$ with indeterminate coefficients $A_{[j]}^{(\nu)}$,

$$(19) \quad T_\nu = \sum_{[j]} A_{[j]}^{(\nu)} U^{[j]},$$

where $U^{[j]}$ has the same significance as in (10) and where $[j]$ again ranges over the systems $(j_0, j_1, \dots, j_{r-1})$ of non-negative integers with the sum ν . We set $A_{[j]}^{(0)} = Z_\mu$ if $j_\mu = 1$ and $j_\rho = 0$ for $\rho \neq \mu$. Then (19) holds for $\nu = 0$ too.

We form the resultant

$$R = R(T_{r-1}, T_{r-2}, \dots, T_1, T_0).$$

Then R is a linear combination with integral coefficients of products of factors $A_{[j]}^{(\nu)}$ with $0 \leq \nu \leq r-1$. Set

$$h = (r-1)!.$$

As is well-known, R has the following properties:

(i) For $\nu = r-1, r-2, \dots, 1$, R is homogeneous of degree h/ν in the coefficients $A_{[j]}^{(\nu)}$ of T_ν . Also, R is homogeneous of degree 1 in the coefficients of T_0 .

(ii) If $A^{(\nu)}$ is the leading coefficient of T_ν with regard to U_ν ,

$$(20) \quad T_\nu = A^{(\nu)} U_\nu^\nu + \dots, \quad (\nu = r-1, r-2, \dots, 1)$$

(i.e. if $A^{(\nu)} = A_{[j]}^{(\nu)}$ where $j_\nu = \nu$ and all $j_\mu = 0$ for $\mu \neq \nu$) and if $A^{(0)} = Z_0$, then R contains the term

$$(21) \quad L = (A^{(r-1)})^{h/(r-1)} (A^{(r-2)})^{h/(r-2)} \dots (A^{(1)})^h Z_0^h$$

with the coefficient 1.

(iii) Define the weight of a coefficient $A_{[j]}^{(\nu)}$ with regard to the index μ as the coefficient j_μ of $[j]$ and define the weight of a product of factors $A_{[j]}^{(\nu)}$ with regard to μ as the sum of the weights of the factors. Then R consists only of terms of weight h with regard to each $\mu = 0, 1, \dots, r-1$.

For the properties (i) and (ii), cf. [6, § 82]. The property (iii) is obtained easily as follows. Let μ be a fixed index, $0 \leq \mu \leq r-1$. Let T_ν^* denote the form obtained from T_ν when U_μ is replaced by tU_ν , t an indeterminate. Let R^* denote the resultant of $T_{r-1}^*, \dots, T_1^*, T_0^*$. It follows from the basic properties of resultants that R^* vanishes for each specialization of the $A_{[j]}^{(\nu)}$ for which R vanishes. Since R is absolutely irreducible, this implies

$$R^* = g(t)R$$

with $g(t) \in \Gamma(t)$. Now, (ii) shows that $g(t) = t^h$ and this yields (iii).

We consider now the specialization θ of the $A_{[j]}^{(\nu)}$ with $\nu > 0$ which maps

$$T_{r-1} \rightarrow S_{r-1}, \quad T_{r-2} \rightarrow S_{r-2}, \quad \dots, \quad T_1 \rightarrow S_1.$$

By (19) and (9), then

$$(22) \quad \theta: A_{[j]}^{(\nu)} \rightarrow \gamma_{[j]}^{(\nu)} s(j_1 + 2j_2 + \dots + (r-1)j_{r-1})$$

for $\nu = r-1, r-2, \dots, 1$. In particular,

$$(23) \quad \theta: A^{(\nu)} \rightarrow s(\nu^2)$$

for $\nu = r-1, r-2, \dots, 1$, cf. (20).

It is clear that

$$R^\theta = R(S_{r-1}, S_{r-2}, \dots, S_1, T_0).$$

We prove a lemma.

LEMMA. — If M is a product of factors $A_{[j]}^{(\nu)}$ which occurs in R with a non-zero numerical coefficient and if $M^\theta = \lambda L^\theta$ with $\lambda \in \Gamma$ then $M = L$.

PROOF OF THE LEMMA. — By (21) and (23) we have

$$(24) \quad M^\theta = \lambda s((r-1)^2)^{h/(r-1)} s((r-2)^2)^{h/(r-2)} \dots s(1)^h Z_0^h.$$

It follows from (22) that $s((r-1)^2)$ occurs in $(A_{[j]}^{(\nu)})^\theta$ only if $\nu = r-1$ and then only in $(A^{(r-1)})^\theta$, in which case $\gamma_{[j]}^{(r-1)} = 1$. Now (24) shows that M has a factor $(A^{(r-1)})^{h/(r-1)}$. If we set

$$M = (A^{(r-1)})^{h/(r-1)} M_1,$$

the properties (i) and (iii) show that M_1 is a product of factors $A_{[j]}^{(\nu)}$ with $\nu < r-1$, of degree h/ν in the factors $A_{[j]}^{(\nu)}$ for each fixed ν , and of weight 0 with regard to the index $r-1$.

Suppose we have already shown for some integer ϱ with $r-1 \geq \varrho > 1$ that

$$(25) \quad M = (A^{(r-1)})^{h/(r-1)} (A^{(r-2)})^{h/(r-2)} \dots (A^{(\varrho)})^{h/\varrho} M_{r-\varrho}$$

where $M_{r-\varrho}$ is a product of factors $A_{[ij]}^{(\nu)}$ with $\nu < \varrho$, of degree h/ν with regard to the $A_{[ij]}^{(\nu)}$ with fixed ν , and of weight 0 with regard to the indices $r-1, r-2, \dots, \varrho$. This is certainly true for $\varrho = r-1$.

On account of (24), (25), and (23), we have

$$(26) \quad M_{r-\varrho}^\theta = \lambda s((\varrho-1)^2)^{h/(\varrho-1)} \dots s(1)^h Z_0^h.$$

If $A_{[ij]}^{(\nu)}$ is a factor of $M_{r-\varrho}$, then by the above, $\nu < \varrho$ and

$$j_\varrho = j_{\varrho+1} = \dots = j_{r-1} = 0.$$

Then (22) shows that $s((\varrho-1)^2)$ can occur in $(A_{[ij]}^{(\nu)})^\theta$ only when $\nu = \varrho-1$ and then only if $A_{[ij-1]}^{(\varrho-1)} = A^{(\varrho-1)}$. In this case, $(A^{(\varrho-1)})^\theta = s((\varrho-1)^2)$ by (23). It is now clear from (26) that $M_{r-\varrho}$ must have a factor $(A^{(\varrho-1)})^{h/(\varrho-1)}$. If we set

$$M_{r-\varrho} = (A^{(\varrho-1)})^{h/(\varrho-1)} M_{r-\varrho+1}$$

and substitute this in (25), we see that (25) holds with ϱ replaced by $\varrho-1$. It follows from (i) and (iii) that $M_{r-\varrho+1}$ is a product of factors $A_{[ij]}^{(\nu)}$ with $\nu < \varrho-1$, that the degree of the factors with a fixed such ν is h/ν , and that the weight of $M_{r-\varrho+1}$ with regard to each of the indices $r-1, r-2, \dots, \varrho-1$ is zero. Thus, $M_{r-\varrho+1}$ satisfy conditions analogous to those stated above for $M_{r-\varrho}$.

Continuing in this manner, we see that (25) holds for $\varrho=1$ and that M_{r-1} is necessarily equal to Z_0^h . Thus, $M=L$ and the Lemma is proved.

It follows from (9) and (18) that

$$R^\theta = R(S_{r-1}, \dots, S_1, T_0) \in \Gamma[s(1), \dots, s((r-1)^2), Z_0, Z_1, \dots, Z_{r-1}].$$

Since $s(1), s(2), \dots, s((r-1)^2)$ were assumed to be algebraically independent over Γ , the Lemma shows that R^θ contains the term

$$s((r-1)^2)^{h/(r-1)} s((r-2)^2)^{h/(r-2)} \dots s(1)^h Z_0^h$$

with the exact coefficient 1. Thus, Theorem 2 holds.

If f is the general polynomial of degree $n > (r-1)!$ and if $r \geq 5$, then $n \geq (r-1)^2$. Since the coefficients c_i of f in (4) are algebraically independent over Γ , Newton's formulas imply that $s(1), s(2), \dots, s(n)$ are algebraically independent over Γ and Theorem 2 applies. Thus, the resultant R^θ of $S_{r-1}, S_{r-2}, \dots, S_1$ and T_0 does not vanish

and Bezout's Theorem holds, cf. [6, § 83]. In particular, we see that the algebraic set V defined by (ii) consists of exactly $h = (r-1)!$ points $u^{(1)}, u^{(2)}, \dots, u^{(h)}$ with coordinates in $\bar{k}$, each point counted with its proper multiplicity. Moreover, if H is the coefficient of Z_0^h in R^θ then as $H \neq 0$, the coordinate vector of $u^{(i)}$ can be taken in the form

$$(u^{(i)}) = (1, u_1^{(i)}, u_2^{(i)}, \dots, u_{r-1}^{(i)})$$

for $i = 1, 2, \dots, h$ and we have

$$R^\theta = H \prod_{i=1}^{(r-1)!} (Z_0 + u_1^{(i)} Z_1 + \dots + u_{r-1}^{(i)} Z_{r-1}).$$

Let Ω denote the normal field over k generated by the $u_j^{(i)}$ and their conjugates over k . Since each element of the Galois group of Ω over k maps $(u^{(1)})$ necessarily on some $(u^{(i)})$ with $1 \leq i \leq (r-1)!$, $(u^{(1)})$ has at most $(r-1)!$ distinct images. This implies

$$[k(u_1^{(1)}, u_2^{(1)}, \dots, u_{r-1}^{(1)} : k) \leq (r-1)!.$$

Thus, the condition (12) is satisfied for

$$u_0 = 1, \quad u_1 = u_1^{(1)}, \quad \dots, \quad u_{r-1} = u_{r-1}^{(1)}.$$

The proof of Theorem 1 in § 2 now gives the construction of a tower (1) with the required properties.

4. – The case of an arbitrary polynomial f .

If f is an arbitrary polynomial of degree n with coefficients in k and if the resultant

$$R^\theta = R(S_{r-1}, S_{r-2}, \dots, S_1, T_0)$$

does not vanish, the construction in § 3 of a point u of V satisfying the condition (12) can still be applied (with a minor modification if the coefficient H of Z_0^h in R^θ vanishes). However, the method breaks down if R^θ vanishes. We then have infinitely many points of V which are rational in $\bar{k}$.

For the sake of completeness, we give a short proof which shows that we always have points u of V which satisfy the condition (12) in § 2.

Let

$$F = X^n + C_1 X^{n-1} + \dots + C_n$$

now denote the general polynomial of degree n ; $C_1, C_2, \dots, C_n$ indeterminates. Set

$$K_0 = \Gamma(C_1, C_2, \dots, C_n), \quad K = k(C_1, C_2, \dots, C_n).$$

Denote by S_v^* the forms of degree v with coefficients in K_0 obtained from S_v in (9) when f is replaced by F . As shown in § 3, there exists a point P in an $(r-1)$ -dimensional space such that the forms $S_{r-1}^*, S_{r-2}^*, \dots, S_1^*$ vanish for P and that adjunction of the coordinates $(P_0, P_1, \dots, P_{r-1})$ of P to K_0 gives a field of degree at most $(r-1)!$ over K_0 . The P_i can be taken in a fixed algebraic closure of K . If $K_1 = K(P_0, P_1, \dots, P_{r-1})$, then

$$[K_1:K] \leq (r-1)! = h.$$

Let f in (4) be an arbitrary polynomial of degree n with coefficients in the field $k \supseteq \Gamma$. The homomorphism

$$\varphi \rightarrow \varphi(c_1, c_2, \dots, c_n)$$

of $k[C_1, \dots, C_n]$ onto k can easily be extended to a homomorphism η of a valuation ring $\mathfrak{D}$ of K onto k . For instance, we can choose $\mathfrak{D}$ as the ring of elements φ of K for which

$$\lim_{c_n \rightarrow c_n} \left(\lim_{c_{n-1} \rightarrow c_{n-1}} \dots \left(\lim_{c_1 \rightarrow c_1} \varphi \right) \dots \right)$$

exists and take $\eta(\varphi)$ as the value of this limit.

Again, we can extend η to a homomorphism ζ of a valuation ring $\mathfrak{D}_1$ of K_1 into $\bar{k}$, cf. [3, Chapter I, 4] or [8, Chapter VI]. After multiplying the coordinates of P with a suitable element of K_1 , we may assume that all P_i lie in $\mathfrak{D}_1$ and that $P_j = 1$ for some index j . Set $P_i^{\zeta} = u_i$. Then $(u_0, u_1, \dots, u_{r-1})$ will represent a point of the algebraic set V defined by means of the polynomial f as in § 2. Let $\lambda_0, \lambda_1, \dots, \lambda_{r-1}$ be r arbitrary integers and set

$$(27) \quad A = \lambda_0 P_0 + \lambda_1 P_1 + \dots + \lambda_{r-1} P_{r-1}.$$

Then $A \in \mathfrak{D}_1 \subseteq K_1$ and hence A is algebraic over K of degree at most equal to $h = (r-1)!$, say

$$\varphi_0 A^h + \varphi_1 A^{h-1} + \dots + \varphi_h = 0$$

with $\varphi_i \in K$, $\varphi_0 \neq 0$. Again, we may choose the $\varphi_i \in \mathfrak{D}$ such that at least one of the φ_i is 1. It follows that

$$\varphi_0^{\zeta}(A^{\zeta}) + \varphi_1^{\zeta}(A^{\zeta})^{h-1} + \dots + \varphi_h^{\zeta} = 0.$$

Since the φ_i^{ζ} belong to k and at least one of them is 1, this shows that A^{ζ} is algebraic of degree at most h over k . In particular, each $u_i = P_i^{\zeta}$ is algebraic over k . Thus, if we set

$$k^* = k(u_0, u_1, \dots, u_{r-1}),$$

the degree $[k^*:k]$ is finite. Then k^* has a primitive element of the form

$$\lambda_0 u_0 + \lambda_1 u_1 + \dots + \lambda_{r-1} u_{r-1}$$

with integral λ_i . If we now choose these λ_i in (27), our argument implies that

$$[k^*:k] \leq h \leq (r-1)!.$$

This proves that the condition (12) is satisfied as we wished to show.

The method used here can be applied when we have an algebraic set V in a projective $(r-1)$ -dimensional space defined by $r-1$ homogeneous equations. We take here the specialization mapping the corresponding forms with indeterminate coefficients on the particular forms defining V . In particular, we can use this method in connection with the specialization θ in (22). We then obtain a proof for the existence of points u of the algebraic set V in § 2 satisfying (12) which does not require Theorem 2.

REFERENCES

- [1] R. BRAUER, *A note on systems of homogeneous algebraic equations*, Bull. Amer. Math. Soc., **51** (1945), pp. 749-755.
- [2] D. HILBERT, *Über die Gleichung neunten Grades*, Math. Ann., **97** (1927), pp. 243-250; Collected Papers, Berlin, 1933, vol. 2, pp. 393-400.
- [3] S. LANG, *Introduction to Algebraic Geometry*, Interscience, New York, 1958.
- [4] B. SEGRE, *The algebraic equations of degrees 5, 9, 157, ... and the arithmetic upon an algebraic variety*, Ann. of Math., **46** (1945), pp. 297-301.
- [5] B. SEGRE, *Sulle irrazionalità da cui può farsi dipendere la determinazione di S_k appartenenti a varietà intersezioni complete di forme*, Rend. Accad. Lincei, **4** (1948), pp. 149-154.
- [6] B. L. VAN DER WAERDEN, *Moderne Algebra*, vol. 2, 2nd edition, Springer, Berlin, 1940.
- [7] A. WIMAN, *Über die Anwendung der Tschirnhausen-Transformation auf die Reduktion algebraischer Gleichungen*, Nova Acta Soc. Sci. Upsaliensis, 1927, pp. 3-6.
- [8] O. ZARISKI - P. SAMUEL, *Commutative Algebra*, vol. 2, Van Nostrand, Princeton, 1960.