A NOTE ON SYSTEMS OF HOMOGENEOUS ALGEBRAIC EQUATIONS

RICHARD BRAUER

1. Introduction. Consider a system of algebraic equations

$$
\begin{aligned}
f_1(x_1, x_2, \cdots, x_n) &= 0, \\
f_2(x_1, x_2, \cdots, x_n) &= 0, \\
\cdots\cdots&\cdots \\
f_h(x_1, x_2, \cdots, x_n) &= 0,
\end{aligned} \tag{1}
$$

where f_i is a homogeneous polynomial of degree r_i with coefficients belonging to a given field K. We interpret $x_1, x_2, \cdots, x_n$ as homogeneous coordinates in an $(n-1)$-dimensional projective space. When $n > h$, the system (1) has non-trivial solutions $(x_1, x_2, \cdots, x_n)$ in an algebraically closed extension field of K, but there may not exist any such solutions in K itself. It is, in general, extremely difficult to decide whether adjunction of irrationalities of a certain type to K is sufficient to guarantee the existence of non-trivial solutions of (1) in the extended field. However, the situation is much simpler, when n is very large, in the sense that n lies above a certain expression depending on the number of equations h and the degrees $r_1, r_2, \cdots, r_h$.

We shall show:

THEOREM A. *For any system of h positive degrees $r_1, r_2, \cdots, r_h$ there exists an integer $\Phi(r_1, r_2, \cdots, r_h)$ such that for $n \geqq \Phi(r_1, r_2, \cdots, r_h)$ the system* (1) *has a non-trivial solution in a soluble extension field K_1 of K. The field K_1 may be chosen such that its degree N_1 over K lies below a value depending on $r_1, r_2, \cdots, r_h$ alone and that any prime factor of N_1 is at most equal to* $\max(r_1, r_2, \cdots, r_h)$.

This Theorem A is evidently contained in the following theorem.

THEOREM B. *For any system of positive integers $r_1, r_2, \cdots, r_h$ and any integer $m \geqq 0$, there exists an integer $\Phi(r_1, r_2, \cdots, r_h; m)$ with the following property: For $n \geqq \Phi(r_1, \cdots, r_h; m)$, there exists a soluble extension field K_2 of K such that all points $(x_1, x_2, \cdots, x_n)$ of an m-dimensional linear manifold L, defined in K_2, satisfy the equations* (1). *Here K_2 may be chosen so that its degree N_2 over K lies below a bound depending on $r_1, r_2, \cdots, r_h$ and m and that no prime factor of N_2 exceeds* $\max(r_1, r_2, \cdots, r_h)$.

Presented to the Society, September 17, 1945; received by the editors July 17, 1945.

At the same time, we shall prove the theorem:

THEOREM C. *Assume that the field K has the following property:*
(*) *For every integer $r>0$, there exists an integer $\Psi(r)$ such that for $n\geqq\Psi(r)$ every equation*

$$a_1x_1^r + a_2x_2^r + \cdots + a_nx_n^r = 0 \tag{2}$$

with coefficients a_i in K has a non-trivial solution in K.

Then, for every system of positive degrees $r_1, r_2, \cdots, r_h$ and every integer $m\geqq 0$, there exists an expression $\Omega(r_1, r_2, \cdots, r_h; m)$ with the following property: For $n\geqq\Omega(r_1, r_2, \cdots, r_h; m)$, there exists an m-dimensional linear manifold M, defined in K, whose points satisfy the equations (1).

We shall prove Theorem C in §2. The changes necessary in order to obtain Theorem B are obvious. In §3, some applications are given. One of them is concerned with Hilbert's resolvent problem. We prove here a recent conjecture of B. Segre.[1]

2. **Proof of Theorem C.** 1. Assume that Theorem C is not true. We choose a system $r_1, r_2, \cdots, r_h; m$ for which no $\Omega(r_1, \cdots, r_h; m)$ exists. We select this system such that max $(r_1, \cdots, r_h)=s$ has the smallest possible value, and that for fixed s the number h has the smallest possible value. If $r_1', r_2', \cdots, r_{h'}'$ is any system of positive integers and m' a non-negative integer, then $\Omega(r_1', r_2', \cdots, r_{h'}'; m')$ exists, if either

$$\max(r_1', r_2', \cdots, r_{h'}') < s \tag{3a}$$

or if

$$\max(r_1', r_2', \cdots, r_{h'}') = s, \qquad h' < h. \tag{3b}$$

Assume first that $h>1$. We may assume that $r_h=s$. It follows that $\Omega(r_1, r_2, \cdots, r_{h-1}; m)$ exists (cf. the conditions (3a) and (3b)) and also that $\Omega(s; m'-1)$ exists for any integer $m'>0$. We set $m'=\Omega(r_1, \cdots, r_{h-1}; m)$. If $n\geqq\Omega(s; m'-1)$, the equation $f_h=0$ is satisfied by all points of an $(m'-1)$-dimensional linear manifold M_1. If we restrict ourselves to points of M_1, we may express $x_1, \cdots, x_n$ linearly and homogeneously by m' parameters $y_1, \cdots, y_{m'}$ with coefficients in K. Then $f_i(x_1, \cdots, x_n)$ becomes a homogeneous polynomial g_i of $y_1, \cdots, y_{m'}$. The degree of g_i is r_i; the coefficients of g_i belong to K. In particular, g_h vanishes identically. In order to solve

[1] B. Segre, Ann. of Math. vol. 46 (1945) p. 287. *Added September* 10: In the meantime, I learned from Mr. Segre that he also found Theorem A from which the proof of the conjecture can be derived.

(1), we have to solve

$$(4) \qquad g_1 = 0,\ g_2 = 0, \cdots, g_{h-1} = 0.$$

Since $m' = \Omega(r_1, \cdots, r_{h-1}; m)$, the equations (4) will be satisfied by all points of an m-dimensional manifold M_2 of the $(y_1, \cdots, y_{m'})$-space. This then gives an m-dimensional linear manifold of the $(x_1, \cdots, x_n)$-space for which the equations (1) hold. But this shows that the expression $\Omega(r_1, \cdots, r_h; m)$ exists; we may take

$$\Omega(r_1, \cdots, r_h; m) = \Omega(\max(r_1, \cdots, r_h); \Omega(r_1, \cdots, r_{h-1}; m) - 1).$$

Hence the case $h > 1$ is impossible.

2. We now consider the case $h = 1$. The system (1) consists of only one equation

$$f(x_1, x_2, \cdots, x_n) = 0$$

of degree $r_1 = s$.

From the way the number s was chosen it follows that $\Omega(s; m)$ does not exist while for every system $r_1', r_2', \cdots, r_{h'}$ with $r_1' < s$, $r_2' < s, \cdots, r_{h'} < s$ and all m' the existence of $\Omega(r_1', r_2', \cdots, r_{h'}; m')$ may be assumed.

We first discuss the case $m = 0$. Denoting the point $(x_1, x_2, \cdots, x_n)$ by $\mathfrak{x}$, we write $f(x_1, x_2, \cdots, x_n) = f(\mathfrak{x})$.

If $\mathfrak{x}_1, \mathfrak{x}_2, \cdots, \mathfrak{x}_n$ are n points whose coordinates are independent indeterminates and if $u_1, u_2, \cdots, u_n$ are n further independent indeterminates, we may set

$$(5)\ f(u_1\mathfrak{x}_1 + u_2\mathfrak{x}_2 + \cdots + u_n\mathfrak{x}_n) = \sum u_1^{\mu} u_2^{\nu} \cdots u_n^{\tau} f_{\mu\nu\cdots\tau}(\mathfrak{x}_1, \mathfrak{x}_2, \cdots, \mathfrak{x}_n),$$

where the sum on the right side extends over all systems of n nonnegative integers $(\mu, \nu, \cdots, \tau)$ with

$$(5a) \qquad \mu + \nu + \cdots + \tau = s.$$

The expressions $f_{\mu,\nu,\cdots,\tau}(\mathfrak{x}_1, \mathfrak{x}_2, \cdots, \mathfrak{x}_n)$ (the polar forms of f) are homogeneous polynomials in the coordinates of each $\mathfrak{x}_i$. As is easily seen, $f_{\mu,\nu,\cdots,\tau}(\mathfrak{x}_1, \mathfrak{x}_2, \cdots, \mathfrak{x}_n)$ is of degree μ in the coordinates of $\mathfrak{x}_1$, of degree ν in the coordinates of $\mathfrak{x}_2, \cdots$, of degree τ in the coordinates of $\mathfrak{x}_n$.

Let $\mathfrak{a}_1 \neq \mathfrak{o}$ be a fixed point.[2] Choose $n-1$ points $\mathfrak{e}_1, \mathfrak{e}_2, \cdots, \mathfrak{e}_{n-1}$ which together with $\mathfrak{a}_1$ form a full linearly independent system, and set $\mathfrak{y} = y_1\mathfrak{e}_1 + y_2\mathfrak{e}_2 + \cdots + y_{n-1}\mathfrak{e}_{n-1}$ where the coefficients $y_1, y_2, \cdots, y_{n-1}$ are indeterminates.

Consider the system of equations

[2] We denote by $\mathfrak{o}$ the row $(0, 0, \cdots, 0)$ consisting of n numbers 0.

$$
(6) \qquad
\begin{aligned}
&f_{s-1,1,0,\cdots,0}(\mathfrak{a}_1, \mathfrak{y}, \mathfrak{o}, \cdots, \mathfrak{o}) = 0,\\
&f_{s-2,2,0,\cdots,0}(\mathfrak{a}_1, \mathfrak{y}, \mathfrak{o}, \cdots, \mathfrak{o}) = 0,\\
&\cdots\cdots\cdots\cdots\cdots\\
&f_{1,s-1,0,\cdots,0}(\mathfrak{a}_1, \mathfrak{y}, \mathfrak{o}, \cdots, \mathfrak{o}) = 0.
\end{aligned}
$$

These equations are homogeneous in $y_1, y_2, \cdots, y_{n-1}$; the degrees are $1, 2, \cdots, s-1$ respectively.

From the remarks above it follows that the expression $\Omega(1, 2, \cdots, s-1; 0)$ exists. Hence for sufficiently large[3] n the equations (6) will have a non-trivial solution. Let $\mathfrak{y}=\mathfrak{a}_2$ be the corresponding point $\mathfrak{y}$. Then $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are linearly independent.

Let $\mathfrak{e}_1', \mathfrak{e}_2', \cdots, \mathfrak{e}_{n-2}'$ be a system of points which together with $\mathfrak{a}_1$ and $\mathfrak{a}_2$ form a full linearly independent system and set

$$\mathfrak{z} = z_1\mathfrak{e}_1' + \cdots + z_{n-2}\mathfrak{e}_{n-2}'$$

with indeterminate coefficients $z_1, z_2, \cdots, z_{n-2}$. Consider next the equations

$$(7) \qquad f_{\mu,\nu,\rho,0,\cdots,0}(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{z}, \mathfrak{o}, \cdots, \mathfrak{o}) = 0,$$

where μ, ν, ρ range over all systems of non-negative integers with

$$\mu + \nu + \rho = s, \qquad 0 < \rho < s.$$

Again, $\Omega(r_1', \cdots, r_{h'}'; 0)$ exists for the degrees $r_1', \cdots, r_{h'}'$ of these equations in $z_1, z_2, \cdots, z_{n-2}$. It follows for sufficiently large n that the system (7) has a non-trivial solution $(z_1, \cdots, z_{n-2})$. Let $\mathfrak{z}=\mathfrak{a}_3$ be the corresponding point. Then $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3$ are linearly independent.

Set $t=\Psi(s)$.[4] Assuming that n is sufficiently large we continue with our procedure until we obtain t linearly independent points $\mathfrak{a}_1, \mathfrak{a}_2, \cdots, \mathfrak{a}_t$ such that[5]

$$f_{\mu,\nu,\cdots,\tau}(\mathfrak{a}_1, \mathfrak{a}_2, \cdots, \mathfrak{a}_t, \mathfrak{o}, \cdots, \mathfrak{o}) = 0$$

for every system of n non-negative indices $(\mu, \nu, \cdots, \tau)$ with $\mu+\nu+\cdots+\tau=s$ in which the first t of our indices are all less than s.

For $\mathfrak{x}_1=\mathfrak{a}_1, \mathfrak{x}_2=\mathfrak{a}_2, \cdots, \mathfrak{x}_t=\mathfrak{a}_t, \mathfrak{x}_{t+1}=\mathfrak{o}, \cdots, \mathfrak{x}_n=\mathfrak{o}$, the identity

[3] In part 2 of the proof we mean by "sufficiently large n" all values of n which lie above a suitable lower bound $\Lambda(s)$ depending only on s.

[4] In the case of Theorem B, we take $t=2$. The equation (8) will have a solution if we extend the field K by the adjunction of an sth root.

[5] If one of the last $n-t$ indices in $(\mu, \nu, \cdots, \tau)$ does not vanish, this equation is trivial, since the left side then contains an $\mathfrak{x}_i=\mathfrak{o}$ to a positive degree.

(5) gives a relation

$$f(u_1\mathfrak{a}_1 + u_2\mathfrak{a}_2 + \cdots + u_t\mathfrak{a}_t) = \sum_{i=1}^{t} a_i u_i^s,$$

where a_i is a certain number of K. Actually, $a_i = f(\mathfrak{a}_i)$.

Since $t = \Psi(s)$, the equation

$$\sum_{i=1}^{t} u_i^s a_i = 0 \tag{8}$$

has a non-trivial solution $(u_1, u_2, \cdots, u_t)$ in K. The corresponding point $\mathfrak{x} = \sum u_i\mathfrak{a}_i$ then yields a non-trivial solution of the equation $(\mathfrak{x}) = 0$ in K.

This argument shows the existence of $\Omega(s; 0)$.

3. We assume that the existence of $m' = \Omega(s; m-1)$ has already been shown. If n is sufficiently large,[6] the result of 2 shows that we may find a point $\mathfrak{a}_1 \neq 0$ such that

$$f(\mathfrak{a}_1) = 0. \tag{9}$$

Consider again the equations (6) where $\mathfrak{y}$ has the old significance. Again, $\Omega(1, 2, \cdots, s-1; m'-1)$ exists. If $n \geqq \Omega(1, 2, \cdots, s-1; m'-1)$, it follows that there exists an $(m'-1)$-dimensional linear space M_0 such that the equations (6) hold for all points $\mathfrak{y}$ of M_0, and that M_0 does not contain $\mathfrak{a}_1$.

The identity (5) for $\mathfrak{x}_1 = \mathfrak{a}_1$, $\mathfrak{x}_2 = \mathfrak{y}$, $\mathfrak{x}_3 = \mathfrak{o}, \cdots, \mathfrak{x}_n = \mathfrak{o}$ yields

$$f(u_1\mathfrak{a}_1 + u_2\mathfrak{y}) = u_2^s f(\mathfrak{y}), \tag{10}$$

on account of (6) and (9). Restricting the point $\mathfrak{y}$ to the linear manifold M_0, we may consider the coordinates of $\mathfrak{y}$ as linear homogeneous functions of m' parameters $z_1, z_2, \cdots, z_{m'}$. Since $m' = \Omega(s; m-1)$, it follows that there exists an $(m-1)$-dimensional linear subspace M_1 of M_0 such that $f(\mathfrak{y}) = 0$ for all points $\mathfrak{y}$ of M_1. But (10) shows that $\mathfrak{a}_1$ and M_1 together span an m-dimensional linear space M which consists entirely of solutions of $f(\mathfrak{x}) = 0$. This proves the existence of $\Omega(s; m)$ which contradicts the assumptions made above.

This finishes the proof of Theorem C. The same method yields the proof of Theorem B, and hence the Theorem A.

3. **Applications.**[7] Consider the general algebraic equation of degree

[6] In part 3 of the proof we shall say that n is sufficiently large if it lies above a suitable lower bound $M(s, m)$, depending on s and m only.

[7] For Hilbert's resolvent problem, see the paper by Segre quoted in footnote 1 and the literature mentioned in this paper, also A. Wiman, Nova Acta Uppsala (1927).

n in one unknown

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_n = 0.$$

If the roots are $\omega_1, \omega_2, \cdots, \omega_n$ and if we set

$$\theta_i = u_0 + u_1\omega_i + \cdots + u_{n-1}\omega_i^{n-1}$$

then the θ_i are the roots of an equation

$$g(x) = x^n + b_1x^{n-1} + \cdots + b_n = 0$$

and it is well known that the coefficient b_i of this Tschirnhaus transformation is a homogeneous polynomial $B_i(u_0, u_1, \cdots, u_{n-1})$ of degree i in the $u_0, u_1, \cdots, u_{n-1}$. For a fixed k, we determine the quantities $u_0, u_1, \cdots, u_{n-1}$ as a non-trivial solution of the equations

$$B_1(u_0, u_1, \cdots, u_{n-1}) = 0,$$
$$B_2(u_0, u_1, \cdots, u_{n-1}) = 0, \cdots, B_k(u_1, u_2, \cdots, u_{n-1}) = 0.$$

It follows from Theorem A that for sufficiently large n it is possible to take $u_0, u_1, \cdots, u_{n-1}$ in a field obtained from the field of the rational functions of $a_1, a_2, \cdots, a_n$ by adjunction of a finite number of radicals. The equation $g(x)$ then has the form

$$x^n + b_{k+1}x^{n-k-1} + \cdots + b_n = 0.$$

Its roots then may be considered as algebraic functions of $n-k$ quantities $b_{k+1}, b_{k+2}, \cdots, b_n$. Since ω_i can be expressed in terms of θ_i, it follows that the solution of the general equation of nth degree can be expressed in terms of the coefficients if we use radicals and one algebraic function of $n-k$ arguments.[8] Here k was a fixed number and n was to be taken sufficiently large.

Hilbert's resolvent problem deals with the question of finding the smallest number l_n for given n such that the roots of the general equation of degree n may be expressed in terms of the coefficients by means of algebraic functions of at most l_n parameters. Our above remark shows that $l_n \leqq n-k$ for fixed k and sufficiently large n. In other words, we have shown that[9]

[8] Since we can make $b_n = 1$ through a simple transformation, we could replace the last function by one depending on $n-k-1$ arguments.

[9] This result shows that in Segre's notation an infinite series of theorems H_i exists. The same is true for the theorems B_i, if in the statement beside the adjunction of square roots and cube roots the adjunction of a finite number of other radicals is admitted. On the other hand, icosahedral irrationalities are superfluous. The existence of these infinite series of theorems H_i and B_i had been stated as a conjecture in Segre's paper.

$$\lim_{n\to\infty} (n - l_n) = \infty.$$

Hilbert's observation that $l_n \leqq n-5$, at least for $n \geqq 9$, and Segre's observation that $l_n \leqq n-6$, at least for $n \geqq 157$,[10] can be supplemented by an infinite number of analogous observations. The method of §2 would allow us to find explicit values n_k such that $l_n \leqq n-k$ for $n \geqq n_k$. However, the values obtained would probably be far too large.

As an example of a field which satisfies the assumption (*) of Theorem C, we may take any field K which is closed with regard to forming radicals $a^{1/m}$, a in K, $m=2, 3, 4, \cdots$. We have here $\Psi(r)=2$ for all r. In particular, any homogeneous equation $f(x_1, x_2, \cdots, x_n)=0$ of degree r has a non-trivial solution, provided that n lies above a certain number depending on r only.

An example of a somewhat less trivial nature is obtained by considering a $\mathfrak{p}$-adic field K. As is well known the multiplicative group of all α^r ($\alpha \neq 0$, α in K) is of finite index in the group of all α ($\alpha \neq 0$, α in K). From this it follows at once that the assumption (*) of Theorem C is satisfied, and the statement of Theorem C holds for K. In particular, *a homogeneous equation* $f(x_1, \cdots, x_n)=0$ *of degree* r *in a* $\mathfrak{p}$*-adic field has a non-trivial solution* $(x_1, x_2, \cdots, x_n)$, *if* n *is sufficiently large, say* $n \geqq N(r)$.[11]

UNIVERSITY OF TORONTO

[10] The somewhat rough method of our proof does not allow us to derive this result. The bound obtained for n would be much larger.

[11] E. Artin has remarked that it follows at once from the existence of normal division algebras of rank r^2 over K that $N(r) > r^2$.