Raising each side of this equation to the power l' where

$$l'\frac{l-1}{2} \equiv 1, \qquad (\text{mod } l),$$

we have Kummer's result for $d=1, 2, \cdots, (l-3)/2$.

I think it highly probable that Kummer encountered this question in connection with a problem involving the second factor of the class number of $k(\zeta)$. I shall prove in another article that if the second factor of the class number is divisible by l, then (1) holds with not all the a's divisible by l. A somewhat similar result is proved by Hilbert.*

THE UNIVERSITY OF TEXAS

ON THE RANK EQUATION OF ANY NORMAL DIVISION ALGEBRA†

BY A. A. ALBERT‡

1. *Introduction.* The different types of normal division algebras which have been discovered up to the present depend upon equations with different groups. It has been thought that, as the rank equation of an algebra is invariant under a change of basal units, the groups of the rank equations of these various types of algebras might serve to show their non-equivalence. This notion is shown to be false here, as the group of the rank equation of any normal division algebra is the symmetric group. In proving this theorem a new theorem in the Hilbert theory of an irreducible polynomial whose coefficients are rational functions, with coefficients in any infinite field K, of several parameters is developed.

2. *General Theory.* We shall first give several presupposed

* Loc. cit., pp. 435–437.

† Presented to the Society, December 27, 1928.

‡ National Research Fellow.

results as lemmas. Lemma 3 is an immediate consequence of Lemmas 1 and 2.

LEMMA 1. *The group of the general equation for the field K determined by its coefficients and any constants finite in number is the symmetric group.*

LEMMA 2. THE HILBERT IRREDUCIBILITY THEOREM. *Let K be any infinite field. Consider the equation*

$$(1)\quad f(x;\lambda_1,\cdots,\lambda_r) \equiv x^n + F_1(\lambda_1,\cdots,\lambda_r)x^{n-1} + \cdots + F_n(\lambda_1,\cdots,\lambda_r) = 0,$$

where $F_i(\lambda_1,\cdots,\lambda_r)$ are rational functions, with coefficients in K, of the independent parameters $\lambda_1,\cdots,\lambda_r$. Let the group of $f(x)$ with respect to $K(\lambda_1,\cdots,\lambda_r)$ be Γ. Then there exist an infinity of rational values of the parameters $\lambda_1,\cdots,\lambda_r$, such that the resulting numerical equation has the group Γ with respect to K.

LEMMA 3. *There exist an infinity of equations with leading coefficients unity and further coefficients in K such that the group of each equation with respect to K is the symmetric group.*

LEMMA 4. *Let A be the algebra of all n-rowed square matrices in K. Let*

$$(2)\qquad \phi(\omega) \equiv \omega^n + \alpha_1\omega^{n-1} + \cdots + \alpha_n = 0$$

be any equation of degree n in K. Then there exists an element of A whose characteristic equation is $\phi(\omega)=0$.

PROOF. The matrix $(\lambda_{ij} \mid i, j=1, 2, \cdots, n)$, where

$$\lambda_{ij} = -\alpha_j, \qquad (j=1, 2, \cdots, n),$$

$$\lambda_{i+1,i} = 1, \qquad (i = 1,2,\cdots, n-1),$$

and all other elements are zero, has for its characteristic equation $\phi(\omega)=0$.

As a consequence of these lemmas we have the following theorems.

THEOREM 1. *There exists an element of A, the algebra of all n-rowed square matrices with coefficients in K, whose mini-*

mum equation has degree n and the symmetric group with respect to K.

THEOREM 2. *Let $f(x; \lambda_1, \cdots, \lambda_r) = 0$ be an equation* (1) *with group Γ. Let $\lambda_1', \cdots, \lambda_r'$ be any set of scalars and let the resulting numerical equation*

$$(3)\quad f(x; \lambda_1', \cdots, \lambda_r') \equiv x^n + a_1x^{n-1} + \cdots + a_n = 0$$

have the group Γ_0 with respect to $K(\lambda_1', \cdots, \lambda_r')$. Then Γ_0 is a sub-group of Γ.

PROOF. Form all permutations $i_1, i_2, \cdots, i_n$ of the numbers $1, 2, \cdots, n$. Consider the product

$$P \equiv \Pi(u + x_{i_1}u_1 + \cdots + x_{i_n}u_n)$$

taken over all such permutations of the roots $x_1, \cdots, x_n$ of (1). This is a polynomial with coefficients in $K(\lambda_1, \cdots, \lambda_r)$ of the indeterminates $u, u_1, \cdots, u_n$. Let $G(u, u_1, \cdots, u_n; \lambda_1, \cdots, \lambda_r)$ be any factor of P with coefficients in $K(\lambda_1, \cdots, \lambda_r)$, irreducible in $K(\lambda_1, \cdots, \lambda_r)$. Then the group Γ of the equation $f(x; \lambda_1, \cdots, \lambda_r)$ is defined as the set of all permutations leaving G unaltered. If we replace the indeterminates $\lambda_1, \cdots, \lambda_r$ by $\lambda_1', \cdots, \lambda_r'$ as in the theorem and consider the equation $f(x; \lambda_1', \cdots, \lambda_r') = 0$, we shall obtain its group by finding all permutations leaving any factor g of $G(u, u_1, \cdots, u_n; \lambda_1', \cdots, \lambda_r')$, having coefficients in $K(\lambda_1', \cdots, \lambda_r')$ and irreducible in $K(\lambda_1', \cdots, \lambda_r')$, unaltered. But the group of $f(x; \lambda_1', \cdots, \lambda_r')$ is unique, and hence any permutation leaving g unaltered leaves any of the other factors of $G(u, u_1, \cdots, u_n; \lambda_1', \cdots, \lambda_r')$ unaltered and hence the product $G(u, u_1, \cdots; u_n, \lambda_1', \cdots, \lambda_r')$. Hence *all* substitutions of Γ_0 leave $G(u, \cdots, u_n; \lambda_1', \cdots, \lambda_r')$ unaltered. The number of permutations that leave $G(u, u_1, \cdots, u_n; \lambda_1', \cdots, \lambda_r')$ unaltered is not greater than the number leaving $G(u, \cdots, u_n; \lambda_1, \cdots, \lambda_r,$ unaltered since the degree of both polynomials in the indeterminates $u_1, \cdots, u_n$ is the same. Hence *the only* substitutions leaving $G(u, \cdots, u_n; \lambda_1', \cdots, \lambda_r')$ unaltered are substitutions of Γ.

Hence the substitutions of Γ_0 are substitutions of Γ and Γ_0 is a subgroup of Γ. This leads to the following conclusion.

THEOREM 3. *Let D be a normal division algebra in n^2 units over a field K. Then the group of the rank equation of D is the symmetric group.*

PROOF. Let $x=\sum_{i=1}^{n^2}\xi_i u_i$ be an element of D whose coordinates $\xi_1, \cdots, \xi_{n^2}$ are independent variables in K and let $R(\omega;\ \xi_1, \cdots, \xi_{n^2})=0$ be the rank equation of D. Then $R=0$ is an equation with leading coefficient unity and further coefficients polynomials in $\xi_1, \cdots, \xi_{n^2}$ with coefficients in K, and the degree of R is n. Let K' be an extension of K such that the algebra D', with the same basal units as D, is equivalent, by a transformation of basal elements, to the algebra of all n-rowed square matrices with coefficients in K'. This can be done by the adjunction of a finite number of constants to K.* It is also easily shown that the rank equation of D' is $R(\omega;\ \xi_1', \cdots, \xi_{n^2}')=0$, where $\xi_1', \cdots, \xi_{n^2}'$ are independent variables in K'.

By Theorem 1, D' contains an element y whose minimum equation is of degree n and has the symmetric group with respect to K'. Let $y=\sum_{i=1}^{n^2}\bar{\xi}_i' u_i$. Then the minimum equation of y is $R(\omega;\bar{\xi}_1', \cdots, \bar{\xi}_{n^2}')=0$. Hence for some values of $\xi_1, \cdots, \xi_{n^2}$ in K' the group of $R(\omega;\ \xi_1, \cdots, \xi_{n^2})$ with respect to K' is the symmetric group. Again, by Theorem 2, the symmetric group is a subgroup of the group Γ of $R(\omega;\ \xi_1, \cdots, \xi_{n^2})$ with respect to $K(\xi_1, \cdots, \xi_{n^2})$. Hence Γ is the symmetric group. This proves the theorem. As a corollary we have the following result.

COROLLARY. *Every normal division algebra in n^2 units over K contains an infinity of elements whose minimum equations each have degree n and the symmetric group with respect to K.*

PRINCETON UNIVERSITY

* L. E. Dickson, *Algebren und ihre Zahlentheorie*, p. 137.