TWO PROOFS OF A THEOREM ON ALGEBRAIC GROUPS

C. CHEVALLEY AND E. KOLCHIN

1. **Introduction.** We shall be considering $(n\times n)$-matrices with coefficients in some field K, which will be assumed to contain infinitely many elements. Such matrices may also be considered to represent endomorphisms of a vector space V over K, in which a base has been selected once and for all. We shall also be considering functions $F(x_1, \cdots, x_m)$ of m arguments in V, with values in K; such a function is called a *polynomial function* if its value may be expressed as a polynomial (with coefficients in K) in the mn coordinates of its arguments with respect to our base in V. The polynomial functions of m arguments form a ring, which will be denoted by $\mathfrak{o}_m$; this ring is isomorphic with the ring of polynomials in mn variables with coefficients in K (because K is infinite). The ring $\mathfrak{o}_m$ may therefore be imbedded in its field of quotients, which will be denoted by $\mathfrak{R}_m$; the elements of $\mathfrak{R}_m$ will be called the *rational expressions* in m elements of V.

Let s be any inversible matrix. Then we may associate to s an automorphism $\eta(s)$ of the ring $\mathfrak{o}_m$ which maps any polynomial function F upon the function $\eta(s)F$ defined by

$$(\eta(s)F)(x_1, \cdots, x_m) = F(sx_1, \cdots, sx_m).$$

The automorphism $\eta(s)$ may be extended to an automorphism of the field $\mathfrak{R}_m$ which we shall still denote by $\eta(s)$.

Let G be a group of $(n\times n)$-matrices (it will always be assumed, when we speak of a group of matrices, that the neutral element of the group is the unit matrix, which implies that every element of the group is an inversible matrix). An element R of $\mathfrak{R}_m$ is called an *invariant* of the group G if we have $\eta(s)R=R$ for every $s\in G$. It is clear that, if P and Q are invariants of G in $\mathfrak{o}_m$, and $Q\neq 0$, then PQ^{-1} is an invariant. However, not every invariant in $\mathfrak{R}_m$ may be represented as a quotient of two polynomial invariants. But, let R be any invariant of G in $\mathfrak{R}_m$, and let R be represented in the form PQ^{-1}, where P and Q are relatively prime to each other in the ring $\mathfrak{o}_m$. Then, if $s\in G$, $\eta(s)P=MP$ and $\eta(s)Q=MQ$, where M is an element of $\mathfrak{o}_m$. On the other hand, it is easily seen that $\eta(s)$ cannot raise the degree of a polynomial function; it follows that M is a scalar. This leads to the following definition: an element P of $\mathfrak{o}_m$ is called a *semi-invariant* of G if there exists a function M on G with values in K such that $\eta(s)P$

Received by the editors November 16, 1949.

$=M(s)P$ for all $s\in G$. The function $M(s)$ is uniquely determined if $P\neq 0$, and is called the *weight* of P. Thus we see that a necessary and sufficient condition for an element R of $\mathfrak{R}_m$ to be an invariant of G is that R be representable as the quotient of two semi-invariants belonging to the same weight; and, if this is the case, then any representation of R in the form of an irreducible fraction with terms in $\mathfrak{o}_m$ is a representation of R as a quotient of semi-invariants.

We may identify the set of all $(n\times n)$-matrices with coefficients in K with the set of systems of n elements of V; the elements of $\mathfrak{o}_n$ may therefore be considered as polynomial functions of matrices. A function of matrices is a polynomial function when its value for any matrix s may be expressed as a polynomial in the elements of s. A group G of matrices is called an *algebraic group* when the condition for an inversible matrix s to belong to G may be expressed by a system of equations of the form $F(s)=0$, where each F is a polynomial function. Given any $m>0$ and a set E of elements of $\mathfrak{o}_m$, it is not difficult to see that the group G of all inversible matrices s such that $\eta(s)R=R$ for every $R\in E$ is an algebraic group. Similarly, given any set E' of elements of $\mathfrak{o}_m$, the set of inversible matrices s such that $\eta(s)P$ is a scalar multiple of P whenever $P\in E'$ is an algebraic group. Our purpose is to establish partial converses of these statements, namely, Theorems 1 and 2 below.

THEOREM 1. *Let G be an algebraic group of $(n\times n)$-matrices. Then there exists a finite subset E of $\mathfrak{R}_n$ such that G consists of all inversible matrices s such that $\eta(s)R=R$ for all $R\in E$.*

THEOREM 2. *Let G be an algebraic group of $(n\times n)$-matrices. Then there exists a finite subset E' of $\mathfrak{o}_n$ such that G consists of all inversible matrices s such that $\eta(s)P$ is a scalar multiple of P whenever $P\in E'$.*

We shall give two proofs of these two theorems. The first one (§II) is pretty straightforward, and goes through without any restriction on the characteristic of the basic field. The second proof (§III) applies only to the case where the basic field is of characteristic 0, but it has the interest of connecting our problem with a seemingly altogether different question, namely, the algebraic theory of differential equations. The first proof gives at the same time proofs for both theorems; the second one establishes Theorem 1. We shall see now that Theorem 1 implies trivially Theorem 2. Assume that Theorem 1 is true; let G be an algebraic group, and let E be a set of elements of $\mathfrak{R}_n$ which has the property stated in Theorem 1. We may obviously assume that this set does not contain any element of the basic field K. Let R_i $(1\leqq i\leqq h)$ be the elements of E; write $R_i=P_iQ_i^{-1}$,

where P_i and Q_i are in $\mathfrak{o}_n$ and relatively prime to each other. Then P_i and Q_i are semi-invariants of G of the same weight, which shows that P_i+Q_i is a semi-invariant. Let E' be the set composed of the elements P_i, Q_i, and P_i+Q_i $(1\leqq i\leqq h)$, and let s be an inversible matrix such that $\eta(s)P_i=a_iP_i$, $\eta(s)Q_i=b_iQ_i$, and $\eta(s)(P_i+Q_i)=c_i(P_i+Q_i)$ $(1\leqq i\leqq h)$, where the a_i's ,the b_i's, and the c_i's are scalars. Since R_i is not in K, P_i and Q_i are linearly independent over K, and it follows immediately that $a_i=b_i$, whence $\eta(s)R_i=R_i$ $(1\leqq i\leqq h)$, and therefore $s\in G$. This shows that Theorem 2 is true.

REMARK. In Theorems 1 and 2, we characterized an algebraic group either by its rational invariants or by its polynomial semi-invariants. It is not true that every algebraic group can be characterized by its polynomial invariants, even if we do not place any restriction on the number m of arguments. This is easily seen by taking for G the group of all inversible diagonal matrices, for then the only polynomial invariants of G (in any number m of arguments) are the constant functions. On the other hand, it is not true that every algebraic group can be characterized by its rational invariants in $\mathfrak{R}_{n-1}$, as one can see without difficulty by taking G to consist of all matrices in special triangular form (0's above the main diagonal, 1's along the main diagonal).

In a final section (§IV) we apply Theorem 2 to show that a factor group of two algebraic groups always has a faithful representation. More precisely, we prove the following result.

THEOREM 3. *Let G be an algebraic group of matrices, let H be a distinguished algebraic subgroup of G. Then there exists a representation ρ of G such that the kernel of ρ is H.*

It can be shown, although we do not do so here, that when the coefficient field is algebraically closed, then the group $\rho(G)$ is itself algebraic.

2. **The first proof.** Let G be an algebraic group of $(n\times n)$-matrices. We have said already that the polynomial functions of n arguments in V are the same thing as the polynomial functions of matrices. Let $\mathfrak{a}$ be the ideal of polynomial functions of n arguments which are 0 at every point of G. If s is an inversible matrix, then a necessary and sufficient condition for s to belong to G is that $\eta(s)$ (operating on $\mathfrak{o}_n$) should map $\mathfrak{a}$ into itself. For, if $s\in G$ and $P\in\mathfrak{a}$, then we have, for any matrix t, $(\eta(s)P)(t)=P(st)$; if $t\in G$, then so is st, which proves that $\eta(s)P\in\mathfrak{a}$. Conversely, let s be an inversible matrix such that $\eta(s)$ maps $\mathfrak{a}$ into itself. If $P\in\mathfrak{a}$, then $\eta(s)P$ is 0 at every point of G, and, in particular, at the neutral element I, whence

$P(s)=(\eta(s)P)\ (I)=0$; since G is algebraic, it follows that $s\in G$.

If r is any integer, denote by L_r the set of polynomial functions of matrices which are represented by polynomials of degrees less than or equal to r in the elements of the matrix. Then it is clear that, for any matrix s, $\eta(s)$ maps L_r into itself. Set $A_r=L_r\cap\mathfrak{a}$; then, if $s\in G$, $\eta(s)$ also maps A_r into itself. Now, the ideal $\mathfrak{a}$ has a finite set of generators; we select r in such a way that A_r contains a set of generators of $\mathfrak{a}$. Then, if an inversible matrix s is such that $\eta(s)$ maps A_r into itself, $\eta(s)$ maps $\mathfrak{a}$ into itself, whence $s\in G$.

The space L_r is finite-dimensional, for it has a base composed of the functions which may be expressed as monomials of degrees less than or equal to r in the coefficients of a matrix. Let $\{u_1, \cdots, u_a\}$ be a base of L_r which contains a base $\{u_1, \cdots, u_b\}$ of A_r. We construct the exterior algebra E over L_r and the subspace E_b of E which is spanned by the exterior products of b elements of L_r. This space has a base $\{v_1, \cdots, v_c\}$ which is composed of the exterior products $u_{i_1}\cdots u_{i_b}$, where $i_1<\cdots<i_b$; we assume that $v_1=u_1\cdots u_b$. Let s be any inversible matrix; since $\eta(s^{-1})=(\eta(s))^{-1}$ (as follows immediately from the definition), the restriction $\eta_r(s)$ of $\eta(s)$ to L_r is an automorphism of this vector space. This automorphism may be extended to an automorphism $\zeta(s)$ of the exterior algebra E, whose restriction $\zeta_b(s)$ to E_b is the bth skew-symmetric power of $\eta_r(s)$ (cf. N. Bourbaki, *Éléments de mathématique, Algèbre*, III, §5, no. 7). If $\eta_r(s)$ maps A_r into itself, then it is clear that $\zeta_b(s)$ maps v_1 upon a scalar multiple of itself. Conversely, assume that $\zeta_b(s)v_1=ev_1$, where e is a scalar. Since $\zeta_b(s)$ is an automorphism, we have $e\neq 0$. Now, the elements of A_r are the elements u of L_r such that $uv_1=0$ (cf. N. Bourbaki, loc. cit., Corollary to Proposition 3, §7, no. 3). Thus, if $u\in A_r$, we have $(\zeta(s))(uv_1)=(\eta_r(s)u)ev_1=0$, whence $\eta_r(s)u\in A_r$, which shows that $\eta_r(s)$ maps A_r into itself.

If P is any given polynomial function of matrices, the coefficients of the expression of $\eta(s)P$ as a polynomial in the coefficients of the matrix argument are obviously polynomial functions of s. It follows immediately that the elements of the matrix which represents $\eta_r(s)$ with respect to the base $\{u_1, \cdots, u_a\}$ are polynomial functions of s. The coefficients of the matrix which represents $\zeta_b(s)$ with respect to the base $\{v_1, \cdots, v_c\}$ are certain minors of the preceding matrix, which proves that they are polynomial functions of s. Set $\zeta_b(s)v_i=\sum_{j=1}^{c}P_{ij}(s)v_j$ $(1\leqq i\leqq c)$, and denote by $\mathfrak{P}(s)$ the matrix $(P_{ij}(s))$. It follows immediately from the definition that, for any matrices s and s', we have $\eta(ss')=\eta(s')\eta(s)$, whence $\eta_r(ss')=\eta_r(s')\eta_r(s)$ and $\zeta_b(ss')=\zeta_b(s')\zeta_b(s)$, which proves that the matrix $\mathfrak{P}(ss')$ is $\mathfrak{P}(s)\mathfrak{P}(s')$.

If $s \in G$, then we have $P_{1j}(s) = 0$ $(2 \leqq j \leqq c)$, whence, for any matrix t, $P_{1j}(st) = P_{11}(s)P_{1j}(t)$ for $1 \leqq j \leqq c$. This means that each P_{1j} is a semi-invariant of G. Now, let s be any inversible matrix such that $P_{1j}(st) = a_j P_{1j}(t)$ identically in t, each a_j being a scalar. If I is the unit matrix, we have $P_{1j}(I) = 0$ $(2 \leqq j \leqq c)$; it follows that $P_{1j}(s) = 0$ $(2 \leqq j \leqq c)$, which means that $\zeta_b(s)$ maps v_1 upon a scalar multiple of itself, therefore the $\eta_r(s)$ maps A_r into itself and that $s \in G$. Thus we see that the set E' composed of the elements P_{1j} $(1 \leqq j \leqq c)$ has the property stated in Theorem 2. The function P_{11} is not equal to 0 (for $P_{11}(I) = 1$), and it follows from the formulas $P_{1j}(st) = P_{11}(s)P_{1j}(t)$ $(1 \leqq j \leqq c)$ that the rational expressions $R_j = P_{1j}P_{11}^{-1}$ are invariants of G. Let s be an inversible matrix such that $\eta(s)R_j = R_j$ $(1 \leqq j \leqq c)$; then, since $R_j(I) = 0$ $(2 \leqq j \leqq c)$, we see that $P_{1j}(s) = R_j(I)P_{11}(s) = 0$ for $j > 1$, and we conclude as above that $s \in G$. Thus the set E composed of $R_1, \cdots, R_c$ has the property stated in Theorem 1.

3. **The second proof.** Let G be an algebraic group of $(n \times n)$-matrices with coefficients in a field K of characteristic 0. We first show that in proving Theorem 1 it is permissible to assume that K is algebraically closed. Suppose then that K is not algebraically closed and that Theorem 1 is known to be true for algebraically closed fields. Let $\mathfrak{a}$ be the ideal of all polynomial functions over K which vanish for every $s \in G$, and let $\overline{G}$ be the set of all inversible matrices $\bar{s}$ with coefficients in the algebraic closure $\overline{K}$ of K such that $P(\bar{s}) = 0$ for every $P \in \mathfrak{a}$. The first step is to show that $\overline{G}$ is an algebraic group of matrices with coefficients in $\overline{K}$. Let $\overline{P}$ be a polynomial function over $\overline{K}$ such that $\overline{P}(s) = 0$ for all $s \in G$. If we write $\overline{P} = \sum \omega_i P_i$, where $\omega_1, \omega_2, \cdots$ are elements of $\overline{K}$ linearly independent over K and each P_i is a polynomial function over K, we find that $P_i(s) = 0$ for all $s \in G$, so that each $P_i \in \mathfrak{a}$. It follows that if we let $\overline{\mathfrak{G}}$ denote the smallest algebraic variety over $\overline{K}$ which contains G, then $\overline{G}$ consists of the inversible matrices in $\overline{\mathfrak{G}}$. Therefore[1] $\overline{G}$ is an algebraic group over $\overline{K}$. This being so, there exists a finite set $\overline{E}$ of rational invariants of $\overline{G}$ with the property stated in Theorem 1. For each $\overline{R} \in \overline{E}$ we may write $\overline{R} = \sum \omega_i R_i$ where $\omega_1, \omega_2, \cdots$ are elements of $\overline{K}$ linearly independent over K and each R_i is a rational expression over K; let E be the finite set of all rational expressions R_i obtained as $\overline{R}$ runs over $\overline{E}$. If $s \in G$, then for each $\overline{R} \in \overline{E}$ we have $\eta(s)\overline{R} = \overline{R}$, that is, $\sum \omega_i \eta(s) R_i = \sum \omega_i R_i$. It follows that E is a set of rational invariants of G. Conversely, if s is an inversible matrix with coefficients in K such that $\eta(s)R = R$ for all $R \in E$, then for every $\overline{R} \in \overline{E}$ we have $\eta(s)\overline{R} = \sum \omega_i \eta(s) R_i = \sum \omega_i R_i = \overline{R}$,

[1] E. Kolchin, Ann. of Math. vol. 49 (1948) pp. 1–42; see §3, Lemma 2.

so that $s \in \overline{G}$, whence $s \in G$. Therefore E has the property stated in Theorem 1. This shows that it suffices to prove Theorem 1 when the coefficient field is algebraically closed.

Assume then that K is algebraically closed. By defining a derivation $c \to c'$ in K by the formula $c' = 0$ for all $c \in K$ we make K an ordinary differential field. Let

$$y_1, \cdots, y_n, y_1', \cdots, y_n', \cdots, y_1^{(i)}, \cdots, y_n^{(i)}, \cdots$$

be an infinite sequence of elements of an extension field of K which are algebraically independent over K, and let $\mathcal{G}$ denote the field obtained by adjoining all these elements to K. It is well known that the differential field structure of K can be extended to $\mathcal{G}$ in one and only one way so that the derivative of $y_j^{(i)}$ is $y_j^{(i+1)}$ $(i \geqq 0,\ 1 \leqq j \leqq n)$; in the language of differential field extensions we then have $\mathcal{G} = K\langle y_1, \cdots, y_n \rangle$. It is easy to see that the field of constants of $\mathcal{G}$ (that is, the field of all elements $R \in \mathcal{G}$ such that $R' = 0$) is K.

If $s = (a_{ij})$ is any matrix in the group $GL(n, K)$ of all inversible $(n \times n)$-matrices with coefficients in K, then the substitution $y_j \to \sum_{h=1}^{n} a_{hj} y_h$ $(1 \leqq j \leqq n)$ defines an automorphism over K of the differential field $\mathcal{G}$; under this automorphism $y_j^{(i)} \to \sum_{h=1}^{n} a_{hj} y_h^{(i)}$. The mapping which in this way assigns to each $s \in GL(n, K)$ an automorphism of $\mathcal{G}$ is an isomorphism of the group $GL(n, K)$ into the group of all automorphisms of $\mathcal{G}$ over K; therefore we may and henceforth do identify each matrix with the corresponding automorphism of $\mathcal{G}$.

The set of all elements $R \in \mathcal{G}$ such that $sR = R$ for all $s \in GL(n, K)$ is a differential subfield $\mathcal{E}$ of $\mathcal{G}$. $W(z, y_1, \cdots, y_n)/W(y_1, \cdots, y_n) = L(z)$ (quotient of two Wronskian determinants) is a homogeneous linear differential polynomial in z with coefficients in $\mathcal{G}$; since these coefficients obviously are invariant under every $s \in GL(n, K)$ they must belong to $\mathcal{E}$. It is obvious that $y_1, \cdots, y_n$ are n solutions of the differential equation $L(z) = 0$ and are linearly independent over K; also $\mathcal{E}\langle y_1, \cdots, y_n \rangle = \mathcal{G}$. Therefore $\mathcal{G}$ is a Picard-Vessiot extension of $\mathcal{E}$ and $GL(n, K)$ is the group of all automorphisms of $\mathcal{G}$ over $\mathcal{E}$.[2]

Since G is an algebraic subgroup of $GL(n, K)$ we know by the Picard-Vessiot theory that the set of all elements of $\mathcal{G}$ which are invariant under every $s \in G$ is a differential field $\mathcal{F}$ such that $\mathcal{E} \subseteq \mathcal{F} \subseteq \mathcal{G}$ and such that $s \in GL(n, K)$ belongs to G if $sR = R$ for all $R \in \mathcal{F}$.

[2] The relevant facts concerning the Picard-Vessiot theory can be found in the paper cited in footnote 1.

Now it is easy to see that the differential field $\mathcal{J}$ is finitely generated over $\mathcal{E}$; therefore if m is large and if we let $\mathcal{J}_m$ denote the set of all elements of $\mathcal{J}$ which are of order[3] less than or equal to m, we shall have the following criterion: a matrix $s \in GL(n, K)$ belongs to G if and only if $sR = R$ for all $R \in \mathcal{J}_m$. In the language of §1 this means that G is characterized by its rational invariants in $m+1$ arguments.

To complete the proof of Theorem 1 it remains to show that G is characterized by its rational invariants in n arguments, that is, that in this criterion we may replace $\mathcal{J}_m$ by $\mathcal{J}_{n-1}$; we do this by proving that if the criterion holds for a given $m \geqq n$ then it continues to hold when m is replaced by $m-1$. To this end we observe that each y_j is a zero of the homogeneous linear differential polynomial in z

$$W(y_1, \cdots, y_n)^{-1} \begin{vmatrix} z & y_1 & \cdots & y_n \\ z' & y_1' & \cdots & y_n' \\ \cdot & \cdot & \cdots & \cdot \\ z^{(n-1)} & y_1^{(n-1)} & \cdots & y_n^{(n-1)} \\ z^{(m)} & y_1^{(m)} & \cdots & y_n^{(m)} \end{vmatrix}$$

which we write as $M(z) = z^{(m)} + q_1 z^{(n-1)} + \cdots + q_n z$; the coefficients $q_1, \cdots, q_n$ are clearly invariant under every $s \in GL(n, K)$ and therefore belong to $\mathcal{E}$. We observe further that the elements $y_j^{(i)}$ $(0 \leqq i \leqq m-1,\ 1 \leqq j \leqq n)$ and q_k $(1 \leqq k \leqq n)$ are algebraically independent over K. Now let $R \in \mathcal{J}_m$. By means of the equation $M(y_j) = 0$ $(1 \leqq j \leqq n)$ we write $R = AB^{-1}$, where A and B are polynomials in $q_1, \cdots, q_n$ without common divisor and with coefficients which are rational expressions over K in the elements $y_j^{(i)}$ $(0 \leqq i \leqq m-1,\ 1 \leqq j \leqq n)$; we assume without loss of generality that one of the coefficients in A is 1. Because of this assumption, and the lack of common divisor of A and B, and the algebraic independence mentioned above, every $s \in GL(n, K)$ which leaves R invariant also leaves invariant all the coefficients in A and B; therefore all these coefficients are invariants of G and consequently belong to $\mathcal{J}_{m-1}$. It follows that s leaves every $R \in \mathcal{J}_{m-1}$ invariant if and only if s leaves every $R \in \mathcal{J}_m$ invariant. This establishes the criterion with m replaced by $m-1$ and, as we have seen, completes the proof of Theorem 1.

4. Factor groups. Let G again be an algebraic group of $(n \times n)$-matrices with coefficients in an infinite field K, and let H be a distinguished algebraic subgroup of G. Denoting by E_r' the set of all

[3] An element of $\mathcal{G}$ is of order less than or equal to m if the element belongs to $K(y_1, \cdots, y_n, y_1', \cdots, y_n', \cdots, y_1^{(m)}, \cdots, y_n^{(m)})$.

semi-invariants of H in $\mathfrak{o}_n$ which are of degree less than or equal to r, we see by Theorem 2 applied to H that for large r an inversible matrix s belongs to H if and only if $\eta(s)P$ is a scalar multiple of P for all $P \in E_r'$. It is obvious that the elements of E_r' of a given weight form a vector space. We now show that a sum $\sum_{i=1}^{h} P_i$ of nonzero elements of E_r' of distinct weights $M_1, \cdots, M_h$ is never 0. For $h=1$ this is trivial; let $h>1$ and suppose the statement already verified for sums of fewer than h terms. If $\sum_{i=1}^{h} P_i$ were zero, we would have $\sum_{i=1}^{h} P_i M_i(t) - \eta(t) \sum_{i=1}^{h} P_i = 0$ for every $t \in H$ and therefore $\sum_{i=1}^{h-1} P_i \cdot (M_i(t) - M_h(t)) = 0$, whence by the induction assumption $P_i \cdot (M_i(t) - M_h(t)) = 0$, $1 \leqq i \leqq h-1$. Since M_i and M_h are distinct, there exists a $t_i \in H$ such that $M_i(t_i) \neq M_h(t_i)$, so that we would have $P_i = 0$ for $1 \leqq i \leqq h-1$ and therefore also for $1 \leqq i \leqq h$.

As a consequence we conclude that there exist a finite number of weights $M_1, \cdots, M_h$ such that the vector space W spanned by E_r' can be written as a direct sum $W = W_1 + \cdots + W_h$, where W_i consists of all the elements of E_r' which have weight M_i. Now if P is a semi-invariant of H of some weight M and if $s \in G$, then we have, for all $t \in H$, $\eta(t)(\eta(s)P) = \eta(s)$ $(\eta(sts^{-1})P) = \eta(s)(M(sts^{-1}) \cdot P)$ $= M(sts^{-1}) \cdot (\eta(s)P)$, so that $\eta(s)P$ is a semi-invariant of H of weight N where N is the function on H defined by $N(t) = M(s^{-1}st)$. Moreover, if the degree of P is less than or equal to r, then so is the degree of $\eta(s)P$. It follows that the restriction $\xi(s)$ of $\eta(s)$ to W is a vector space automorphism of W which maps each W_i onto some W_j. Therefore if we introduce a base in each space W_i the restriction of $\xi(s)$ to W_i may be identified with an inversible matrix $\xi_i(s)$, and $\xi(t)$ itself then identified with a matrix which is composed of h^2 blocks, h of these blocks being $\xi_1(s), \cdots, \xi_h(s)$ and the others being 0. The element $s \in G$ belongs to H if and only if all these nonzero blocks $\xi_i(s)$ are on the main diagonal and are scalar matrices.

Let d_i be the dimension of W_i, so that $\xi_i(s)$ is a $(d_i \times d_i)$-matrix. The mapping $\alpha \to \xi_i(s)^{-1} \alpha \xi_i(s)$ is an automorphism of the vector space consisting of all $(d_i \times d_i)$-matrices α with coefficients in K. Choosing a basis for this vector space, we denote the matrix of this automorphism by $\rho_i(s)$; then $\rho_i(s)$ is an inversible $(d_i^2 \times d_i^2)$-matrix. Finally, let $\rho(s)$ be the matrix composed of h^2 blocks, h of these blocks being $\rho_1(s), \cdots, \rho_h(s)$ and the others being 0, the arrangement of these nonzero blocks in $\rho(s)$ being the same as the arrangement of the blocks $\xi_1(s), \cdots, \xi_h(s)$ in $\xi(s)$. Thus $\rho(s)$ is an inversible $(d \times d)$-matrix, where $d = \sum_{i=1}^{h} d_i^2$.

It can be seen without great difficulty that the mapping $\rho: s \to \rho(s)$ is a representation of G. If $s \in G$, then $\rho(s)$ is the unit matrix if and only

if each nonzero block $\rho_i(s)$ is on the main diagonal of $\rho(s)$ and is itself a unit matrix, that is, if and only if each nonzero block $\xi_i(s)$ is on the main diagonal of $\xi(s)$ and is a scalar matrix, that is, if and only if $s \in H$. Thus the kernel of the representation ρ is H. This proves Theorem 3.

COLUMBIA UNIVERSITY