Can. J. Math., Vol. XXVIII, No. 3, 1976, pp. 455–472

LINEAR TRANSFORMATIONS ON MATRICES: THE INVARIANCE OF GENERALIZED PERMUTATION MATRICES, I

HOCK ONG AND E. P. BOTTA

1. Introduction. Let F be a field, $M_n(F)$ be the vector space of all n-square matrices with entries in F and $\mathscr{U}$ a subset of $M_n(F)$. It is of interest to determine the structure of linear maps $T : M_n(F) \to M_n(F)$ such that $T(\mathscr{U}) \subseteq \mathscr{U}$. For example: Let $\mathscr{U}$ be $GL(n, \mathbf{C})$, the group of all nonsingular $n \times n$ matrices over $\mathbf{C}$ [**5**]; the subset of all rank 1 matrices in $M_{m\times n}(F)$ [**4**] ($M_{m\times n}(F)$ is the vector space of all $m \times n$ matrices over F); the unitary group [**2**]; or the set of all matrices X in $M_n(F)$ such that $\det(X) = 0$ [**1**]. Other results in this direction can be found in [**3**]. In this paper we consider $\mathscr{U}$ to be a set of generalized permutation matrices relative to some permutation group(set) and with entries in some nontrivial subgroup of F^* where F^* is the multiplicative group of F. We classify those $T : M_n(F) \to M_n(F)$ such that $T(\mathscr{U}) = \mathscr{U}$. Furthermore we also determine the structure of the set of all such T. The main results will be stated in Section 4.

2. Definitions and notation. We denote by S_n the symmetric group of degree n acting on the set $\{1, 2, \ldots, n\}$. If S is a subset of F we define

$$\Gamma_n(S) = \{\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) : \alpha_i \in S\}.$$

The identity element of S_n, the additive identity and the multiplicative identity of F will be denoted by e, 0, 1 respectively. The matrix with 1 in the (i, j) position and 0 elsewhere will be denoted by E_{ij}. If $\alpha \in \Gamma_n(F^*)$ and $\sigma \in S_n$ then $P(\alpha, \sigma)$ will be the matrix whose (i, j) entry is $\alpha_i\delta_{i\sigma(j)}$ (where $\delta_{i,j} = 1$ if $i = j$ and 0 elsewhere) and we call $P(\alpha, \sigma)$ a *generalized permutation matrix*. If $\epsilon \in \Gamma_n(F)$ is the sequence all of whose entries are equal to 1 we write $P(\sigma)$ for $P(\epsilon, \sigma)$ and call $P(\sigma)$ a permutation matrix *corresponding to* σ. If G is a nonempty subset of S_n and H a subgroup of F^* we define

$$P(G, H) = \{P(\alpha, \sigma) : \alpha \in \Gamma_n(H) \text{ and } \sigma \in G\},$$

$$\mathscr{T}P(G, H) = \{T : T \text{ is a linear transformation on } M_n(F) \text{ to itself and } T(P(G, H)) = P(G, H)\}.$$

If $\epsilon = \{E_i : i = 1, 2, \ldots, n\} \subset M_n(F)$ is a set of n matrices we say ϵ is a

Received November 14, 1973 and in revised form, February 13, 1976.

https://doi.org/10.4153/CJM-1976-047-9 Published online by Cambridge University Press

$G - H$ unitary set if ϵ is a linearly independent set and for all $\alpha \in \Gamma_n(H)$,

$$E(\alpha) = \sum_{i=1}^{n} \alpha_i E_i$$

belongs to $P(G, H)$.

Let

$$\mathscr{H} = \{H : H \text{ is a subgroup of } F^* \text{ and there do not exist } a, b \in F^* \text{ such that } Ha + b \subseteq H\}.$$

The set $\mathscr{H}$ is nonempty. For example:

(a) It is trivial that F^* is in $\mathscr{H}$ for every field F.

(b) If H is a subgroup of the unit circle $C = \{z : |z| = 1\}$ of the complex plane and $|H| > 2$ where $|H|$ denotes the order of H then H is in $\mathscr{H}$.

Proof. If a, b are in F^* then the circle $|za + b| = 1$ intersects the unit circle at most two points.

(c) Every nontrivial finite subgroup H of F^* is in $\mathscr{H}$.

Proof. If there exist $a, b \in F^*$ such that $Ha + b \subseteq H$ then since H is finite, $Ha + b = H$. It is easily seen that when h runs over H, $ha + b$ also runs over H. Hence

$$\left(\sum_{h \in H} h\right) a + |H| b = \sum_{h \in H} h.$$

It is well known that H is cyclic and elements in H are exactly the roots of $x^{|H|} = 1$. Hence $\sum_{h \in H} h = 0$ and so $|H|b = 0$. Clearly this is impossible if char $F = 0$. If $p = \text{char } F \neq 0$ then $p \| H \| p^r - 1$ for some positive integer r which is again impossible.

The n-square matrices all of whose entries are 0, all of whose entries are 1 and the identity matrix will be denoted by 0_n, J_n, I_n respectively or 0, J, I if no ambiguity arises. If $A = (a_{ij})$ and $B = (b_{ij})$ are in $M_n(F)$ then their Hadamard product $A * B = C = (c_{ij})$ is the n-square matrix defined by $c_{ij} = a_{ij} b_{ij}$. If A is n-square matrix and B is an m-square matrix then $A \oplus B$ will denote their direct sum. If $X = (x_{ij}) \in M_n(F)$ and $\sigma \in S_n$, X_σ will be the matrix whose (i, j) entry is x_{ij} if $\sigma(i) = j$ and 0 elsewhere.

If H is a subgroup of F^* let $M_n(H)$ be the set of all n-square matrices with entries in H. Since H is a group, it is easy to see that the set $M_n(H)$ with the operation Hadamard product is a group and will be denoted by $M_n(H)$. Under the correspondence

$$A \rightarrow (a_{11}, \ldots, a_{1n}, \ldots, a_{n1}, \ldots, a_{nn})$$

where $A = (a_{ij}) \in M_n(H)$, it is obvious that $M_n(H)$ is isomorphic to the direct product $H \times \ldots \times H$ (n^2 times).

We recall that a nonempty subset G of S_n is *transitive* if given $1 \leqq i, j \leqq n$ there exists $\sigma \in G$ such that $\sigma(i) = j$. A transitive subset G of S_n is *regular* if given such a pair i and j there exists exactly one σ with $\sigma(i) = j$. A subset G of S_n is *doubly transitive* if given $1 \leqq i, j, p, q \leqq n$ with $i \neq p, j \neq q$ there exists $\sigma \in G$ with $\sigma(i) = j$, $\sigma(p) = q$. If G is a subgroup of S_n we denote by $N(G)$ the normalizer of G in S_n. If G is a regular subset of S_n we shall write $G = \{g_1, \ldots, g_n\}$ and for simplicity we shall write $g_i^{-1} = h_i$, $i = 1, 2, \ldots, n$.

If S is a set and η a mapping of S into S then s^η will be the image of $s \in S$ under η. If G, K are two groups, $\xi : G \rightarrow \mathrm{Aut}(K)$ a homomorphism (respectively, anti-homomorphism) and for $k \in K$, $g_1, g_2 \in G$,

$$(k^{\xi(g_1)})^{\xi(g_2)} = k^{\xi(g_2)\xi(g_1)}, \quad \text{(respectively, } k^{\xi(g_1)\xi(g_2)}\text{)},$$

then the symbols $\langle g, k\rangle$, $g \in G$, $k \in K$ form a group under the rule

$$\langle g_1, k_1\rangle \cdot \langle g_2, k_2\rangle = \langle g_1g_2, k_1k_2^{\xi(g_1)}\rangle$$
$$(\langle g_1, k_1\rangle \cdot \langle g_2, k_2\rangle = \langle g_1g_2, k_1^{\xi(g_2)}k_2\rangle),$$

i.e. the semi-direct product of K by G with respect to ξ and will be denoted by $\langle G, K\rangle_\xi$ or $\langle G, K\rangle$.

For $T \in \mathscr{T}P(G, H)$ and $\sigma \in G$ we define

$$T(\sigma) = \{T(E_{i\sigma(i)} : i = 1, 2, \ldots, n\},$$
$$P(G) = \{P(\sigma) : \sigma \in G\}.$$

The linear transformations $P(\sigma)$, $\sigma \in G$ and R on $M_n(F)$ to itself are defined as follows: For $X \in M_n(F)$,

$$P(\sigma)(X) = P(\sigma)X,$$
$$R(X) = {}^tX$$

where ${}^tX$ is the transpose of X.

3. The groups $\langle\langle S_n, S_n \times \ldots \times S_n\rangle, M_n(H)\rangle$ and $\langle N(G), M_n(H)\rangle$. Let H be a subgroup of F^* and $S_n \times \ldots \times S_n$ denote the direct product of S_n by n times. For $\nu, \sigma \in S_n$, $(\omega_{\nu(1)}, \ldots, \omega_{\nu(n)})$ in $S_n \times \ldots \times S_n$ define $\varphi_\sigma : S_n \times \ldots \times S_n \rightarrow S_n \times \ldots \times S_n$ by

$$\varphi_\sigma(\omega_{\nu(1)}, \ldots, \omega_{\nu(n)}) = (\omega_{\nu\sigma(1)}, \ldots, \omega_{\nu\sigma(n)}).$$

Then it is easy to see that φ_σ is an automorphism of $S_n \times \ldots \times S_n$, and defines φ, an anti-isomorphism of S_n into the group of all automorphisms of $S_n \times \ldots \times S_n$. We denote by $\langle S_n, S_n \times \ldots \times S_n\rangle$ the semi-direct product of $S_n \times \ldots \times S_n$ by S_n with respect to the anti-isomorphism φ.

Let $G = \{g_1, \ldots, g_n\}$ be a regular subset of S_n. For $A \in M_n(H)$ and $\langle\sigma, (\mu_1, \ldots, \mu_n)\rangle \in \langle S_n, S_n \times \ldots \times S_n\rangle$ we define

$$(3.1) \quad A^{\langle\sigma, (\mu_1, \ldots, \mu_n)\rangle} = \sum_{i=1}^{n} P(\mu_i)A_{h_i}P(h_i\mu_i^{-1}g_{\sigma(i)}).$$

Then for $A, B \in M_n(H)$, since A_{h_i} and B_{h_i} are h_i-diagonal matrices,

$$\begin{aligned}(A * B)^{\langle\sigma,(\mu_1,\ldots,\mu_n)\rangle} &= \sum_{i=1}^{n} P(\mu_i)(A_{h_i} * B_{h_i})P(h_i\mu_i^{-1}g_{\sigma(i)}) \\ &= \sum_{i=1}^{n} P(\mu_i)A_{h_i}P(h_i\mu_i^{-1}g_{\sigma(i)}) * \sum_{j=1}^{n} P(\mu_j)B_{h_j}P(h_j\mu_j^{-1}g_{\sigma(j)}) \\ &= A^{\langle\sigma,(\mu_1,\ldots,\mu_n)\rangle} * B^{\langle\sigma,(\mu_1,\ldots,\mu_n)\rangle}\end{aligned}$$

and $A^{\langle\sigma,(\mu_1,\ldots,\mu_n)\rangle} = J$ if and only if $A = J$. Therefore $\langle\sigma, (\mu_1, \ldots, \mu_n)\rangle$ is an automorphism of $M_n(H)$. For $\langle\sigma, (\mu_1, \ldots, \mu_n)\rangle$ and $\langle\tau, (\nu_1, \ldots, \nu_n)\rangle$ in $\langle S_n, S_n \times \ldots \times S_n\rangle$, a computation shows that

$$(A^{\langle\sigma,(\mu_1,\ldots,\mu_n)\rangle})^{\langle\tau,(\nu_1,\ldots,\nu_n)\rangle} = A^{\langle\tau,(\nu_1,\ldots,\nu_n)\rangle\cdot\langle\sigma,(\mu_1,\ldots,\mu_n)\rangle}.$$

Hence we may define $\langle\langle S_n, S_n \times \ldots \times S_n\rangle, M_n(H)\rangle$, the corresponding semi-direct product of $M_n(H)$ by $\langle S_n, S_n \times \ldots \times S_n\rangle$.

Suppose now that G is a doubly transitive subgroup of S_n and for $\tau \in N(G)$, $A \in M_n(H)$ we define

$$A^\tau = P(\tau)AP(\tau^{-1}).$$

Then it is easy to see that τ is an automorphism of $M_n(H)$ and we denote the corresponding semi-direct product of $M_n(H)$ by $N(G)$ by $\langle N(G), M_n(H)\rangle$.

4. Main results. First we characterize all $G - H$ unitary sets for G a non-empty subset of S_n and H a nontrivial group in $\mathscr{H}$ (Propositions 1 and 2). If G is a transitive subset of S_n and H is a nontrivial subgroup of F^* we show that $\mathscr{T}P(G, H)$ is a subgroup of $GL(n^2, F)$ (Proposition 3). If G is a regular subset or a doubly transitive subset of $S_n (n > 2)$, H a nontrivial group in $\mathscr{H}$ and $T \in \mathscr{T}P(G, H)$ then for $1 \leqq i, j \leqq n$ there exist $1 \leqq p, q \leqq n$ and $\alpha_{ij} \in H$ such that

$$T(E_{ij}) = \alpha_{ij}E_{pq}$$

and for distinct (i, j) we have distinct (p, q), i.e. the matrix representation of T with respect to the usual basis $\{E_{ij} : i, j = 1, 2, \ldots, n\}$ is a generalized permutation matrix (Lemmas 5 and 6). Furthermore we have the following results:

THEOREM 1. *Let $G = \{g_1, \ldots, g_n\}$ be a regular subset of S_n $(n > 2)$ and H a nontrivial group in $\mathscr{H}$. Then $T \in \mathscr{T}P(G, H)$ if and only if there exist $\alpha_i = (\alpha_{i1}, \ldots, \alpha_{in}) \in \Gamma_n(H)$, $i = 1, 2, \ldots, n$ and $\mu_1, \ldots, \mu_n, \sigma \in S_n$ such that*

$$T(E_{ih_k(i)}) = \alpha_{ih_k(i)}E_{\mu_k(i)h_{\sigma(k)}\mu_k(i)}, \quad i, k = 1, \ldots, n$$

https://doi.org/10.4153/CJM-1976-047-9 Published online by Cambridge University Press

or in another form

$$T(X) = A * \sum_{i=1}^{n} P(\mu_i)X_{h_i}P(h_i\mu_i^{-1}g_{\sigma(i)}), \quad X \in M_n(F)$$

where $A = [\alpha_{ij}]^{\langle\sigma,(\mu_1,\ldots,\mu_n)\rangle} \in M_n(H)$ *and* $h_i = g_i^{-1}$.

THEOREM 2. *Let* $G = \{g_1, \ldots, g_n\}$ *be a regular subset of* S_n $(n > 2)$ *and* H *a nontrivial group in* $\mathscr{H}$. *If for*

$$\langle\langle \epsilon, (\mu_1, \ldots, \mu_n)\rangle, A\rangle \in \langle\langle S_n, S_n \times \ldots \times S_n\rangle, M_n(H)\rangle$$

and $X \in M_n(F)$ *we define*

$$X^{\langle\langle\sigma,(\mu_1,\ldots,\mu_n)\rangle,A\rangle} = A * X^{\langle\sigma,(\mu_1,\ldots,\mu_n)\rangle},$$

then $\mathscr{T}P(G, H)$ *is equal to the group* $\langle\langle S_n, S_n \times \ldots \times S_n\rangle, M_n(H)\rangle$.

THEOREM 3. *Let* G *be a doubly transitive subgroup of* S_n $(n > 2)$ *and* H *a nontrivial group in* $\mathscr{H}$. *Then* $T \in \mathscr{T}P(G, H)$ *if and only if there exist* $A \in M_n(H)$, $\mu \in N(G)$ *and* $\sigma \in G$ *such that*

$$T(X) = A * P(\sigma\mu)XP(\mu^{-1}), \quad X \in M_n(F) \quad or$$
$$T(X) = A * P(\sigma\mu)^tXP(\mu^{-1}), \quad X \in M_n(F).$$

THEOREM 4. *Let* G *be a doubly transitive subgroup of* S_n $(n > 2)$ *and* H *a nontrivial group in* $\mathscr{H}$. *If for* $\langle\mu, A\rangle \in \langle N(G), M_n(H)\rangle$ *we define*

$$X^{\langle\sigma,A\rangle} = A * P(\sigma)XP(\sigma^{-1}), \quad X \in M_n(F)$$

then $\mathscr{T}P(G, H)$ *is equal to the group*

$$P(G) \circ \langle N(G), M_n(H)\rangle \circ \{I, R\}$$

where $\circ$ *is the usual composition of linear transformations. As an abstract group, there exists a subgroup* $\mathscr{T}_1P(G, H)$ *of index* $2|G|$ *in* $\mathscr{T}P(G, H)$ *and* $\mathscr{T}_1P(G, H)$ *is isomorphic to the group*

$$\langle N(G), \underbrace{H \times \ldots \times H}_{n^2 \text{ times}}\rangle.$$

To complete our list we have the following

THEOREM 5. *If* $|H| > 2$ *and* $H \in \mathscr{H}$ *then Theorems* 1 *and* 2 *are true when* $n = 2$. *If* $H = \{1, -1\}$ *then* $\mathscr{T}P(S_2, H)$ *consists of the group of linear transformations generated by the set*

$$\left\{T : T(X) = A * \sum_{i=1}^{2} P(\mu_i)X_{g_i}P(g_i\mu_ig_{\sigma(i)}), \quad \sigma, \mu_1, \mu_2 \in S_2, A \in M_2(H)\right\}$$

together with the linear transformation S *defined as follows:*

$$S(E_{11}) = \tfrac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \quad S(E_{12}) = \tfrac{1}{2}\begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix},$$
$$S(E_{21}) = \tfrac{1}{2}\begin{bmatrix} 1 & -1 \\ 1 & -1 \end{bmatrix}, \quad S(E_{22}) = \tfrac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}.$$

5. Structure of $G - H$ unitary sets. Let G be a nonempty subset of S_n and H a group in $\mathscr{H}$.

PROPOSITION 1. *Suppose $|H| > 2$ and $\{A_1, \ldots, A_n\} \subseteq M_n(F)$ is a $G - H$ unitary set. Then there exist $a_1, \ldots, a_n \in H$, $\tau \in S_n$, $\sigma \in G$ such that*

$$A_i = a_i E_{\tau(i)\sigma^{-1}\tau(i)}, \quad i = 1, 2, \ldots, n.$$

Proof. It is obvious for $n = 1$, hence assume $n > 1$. Since $(1, \ldots, 1) \in \Gamma_n(H)$, $\sum_{i-1}^n A_i$ is in $P(G, H)$ hence there exist a $\sigma \in G$ and $\beta = (\beta_1, \ldots, \beta_n) \in \Gamma_n(H)$ such that

$$\sum_{i=1}^n A_i = P(\beta, \sigma).$$

Since $|H| > 2$ there exist distinct $\xi, \eta \in H$ and both are distinct from 1. Then there exist $\tau, \nu \in G$ and $\gamma = (\gamma_1, \ldots, \gamma_n)$, $\delta = (\delta_1, \ldots, \delta_n) \in \Gamma_n(H)$ such that

$$\xi A_1 + \sum_{i=2}^n A_i = P(\gamma, \tau),$$

$$\eta A_1 + \sum_{i=2}^n A_i = P(\delta, \nu).$$

Hence

$$A_1 = (1 - \xi)^{-1}(P(\beta, \sigma) - P(\gamma, \tau)).$$

Assume $\sigma \neq \tau$. Then there exists $1 \leqq i \leqq n$ such that $\sigma^{-1}(i) \neq \tau^{-1}(i)$. But

$$A_1 = (1 - \eta)^{-1}(P(\beta, \sigma) - P(\delta, \nu)) = (\xi - \eta)^{-1}(P(\gamma, \tau) - P(\delta, \nu)),$$

or

$$(1 - \eta)^{-1}P(\beta, \sigma) - (\xi - \eta)^{-1}P(\gamma, \tau) = ((1 - \eta)^{-1} - (\xi - \eta)^{-1})P(\delta, \nu)$$

i.e. the matrix on the left hand side has two nonzero entries in the ith row and the right has at most one, a contradiction. Hence $\sigma = \tau$ and

$$A_1 = P((1 - \xi)^{-1}(\beta - \gamma), \sigma) = P(\theta_1, \sigma)$$

say. Similarly we have $A_i = P(\theta_i, \sigma)$ where $\theta_i \in \Gamma_n(F)$, $i = 1, 2, \ldots, n$.

Now if we write $A_k = (a_{ij}^k)$, $k = 1, 2, \ldots, n$ then $a_{ij}^k = 0$ if $j \neq \sigma^{-1}(i)$ and $\sum_{k-1}^n \alpha_k a^k{}_{i\sigma^{-1}(i)} \in H$ for all $(\alpha_1, \ldots, \alpha_n) \in \Gamma_n(H)$, $i = 1, 2, \ldots, n$. Suppose the number of nonzero terms in $\{a^k{}_{i\sigma^{-1}(i)} : k = 1, 2, \ldots, n\}$ is not less than two, say $a^1{}_{i\sigma^{-1}(i)} \neq 0$ and $a^2{}_{i\sigma^{-1}(i)} \neq 0$. Then we may choose $\alpha_2, \ldots, \alpha_n \in H$ so that $\sum_{k-2}^n \alpha_k a^k{}_{i\sigma^{-1}(i)} \neq 0$. Let

$$a = a^1{}_{i\sigma^{-1}(i)}, \quad b = \textstyle\sum_{k-2}^n \alpha_k a^k{}_{i\sigma^{-1}(i)}.$$

Then $\alpha_1 a + b \in H$ for all $\alpha_1 \in H$, i.e. $Ha + b \subseteq H$ which is a contradiction.

Hence for each $i = 1, 2, \ldots, n$ there exists exactly one k such that $a^k{}_{i\sigma^{-1}(i)} \neq 0$ and $a^l{}_{i\sigma^{-1}(i)} = 0$ for all $l \neq k$. If for some k, $a^k{}_{i\sigma^{-1}(i)} \neq 0$ and $a^k{}_{j\sigma^{-1}(j)} \neq 0$, $i \neq j$ then there exists l such that $A_l = 0$ which is impossible since $A_1, \ldots, A_n$ are linearly independent. Hence there exist $\tau \in S_n$ and $a_1, \ldots, a_n \in H$ such that

$$A_{\tau^{-1}(i)} = a_{\tau^{-1}(i)} E_{i\sigma^{-1}(i)}, \quad i = 1, 2, \ldots, n \quad \text{or}$$
$$A_i = a_i E_{\tau(i)\sigma^{-1}\tau(i)}, \quad i = 1, 2, \ldots, n.$$

PROPOSITION 2. *If $|H| = 2$ and $\{A_1, \ldots, A_n\} \subseteq M_n(F)$ is a $G - H$ unitary set then there exist permutation matrices P and Q, an integer r $(0 \leqq r \leqq n)$ and $\epsilon_i, \zeta_{jk} \in H$ such that $n - r$ is even and if $P\{A_1, \ldots, A_n\}Q = \{E_1, \ldots, E_n\}$ then*

$$E_1 = [\epsilon_1] \oplus O_{n-1},$$
$$E_2 = O_1 \oplus [\epsilon_2] \oplus O_{n-2},$$
$$\vdots$$
$$E_r = O_{r-1} \oplus [\epsilon_r] \oplus O_{n-r},$$
$$E_{r+1} = O_r \oplus \tfrac{1}{2}\begin{bmatrix} \zeta_{11} & \zeta_{12} \\ \zeta_{13} & \zeta_{14} \end{bmatrix} \oplus O_{n-r-2},$$
$$E_{r+2} = O_r \oplus \tfrac{1}{2}\begin{bmatrix} \pm\zeta_{11} & \mp\zeta_{12} \\ \mp\zeta_{13} & \pm\zeta_{14} \end{bmatrix} \oplus O_{n-r-2},$$
$$\vdots$$
$$E_{n-1} = O_{n-2} \oplus \tfrac{1}{2}\begin{bmatrix} \zeta_{t1} & \zeta_{t2} \\ \zeta_{t3} & \zeta_{t4} \end{bmatrix}, t = \tfrac{1}{2}(n - r),$$
$$E_n = O_{n-2} \oplus \tfrac{1}{2}\begin{bmatrix} \pm\zeta_{t1} & \mp\zeta_{t2} \\ \mp\zeta_{t3} & \pm\zeta_{t4} \end{bmatrix}.$$

Proof. It is obvious for $n = 1$ hence assume $n > 1$.

Since $(1, \ldots, 1) \in \Gamma_n(H)$ there exist $\sigma \in G$ and $\alpha = (\alpha_1, \ldots, \alpha_n) \in \Gamma_n(H)$ such that

$$\sum_{i=1}^{n} A_i = P(\alpha, \delta).$$

For $k = 1, 2, \ldots, n$, let $\theta_{ki} = 1$ if $i = k$ and $\theta_{ki} = -1$ if $i \neq k$. Then $\theta_k = (\theta_{k1}, \ldots, \theta_{kn}) \in \Gamma_n(H)$ and hence there exist $\beta_k = (\beta_{k1}, \ldots, \beta_{kn})$ in $\Gamma_n(H)$, τ_i in G, $i = 1, 2, \ldots, n$ such that

$$A_k - \sum_{i \neq k} A_i = P(\beta_k, \tau_k), \quad k = 1, 2, \ldots, n.$$

Hence

$$2A_k = P(\alpha, \sigma) + P(\beta_k, \tau_k), \quad k = 1, 2, \ldots, n.$$

Since $|H| = 2$ we must have $1 \neq -1$. Hence char $\neq 2$ and

$$A_k = 2^{-1}P(\alpha, \sigma) + 2^{-1}P(\beta_k, \tau_k), \quad k = 1, 2, \ldots, n.$$

To complete the proof we need the following lemmas, using the above notations.

LEMMA 1. *If $\sigma^{-1}(q) \neq \tau_s^{-1}(q)$ for some $1 \leqq s, q \leqq n$ then there exists a $t \neq s$ such that $\tau_t^{-1}(q) = \tau_s^{-1}(q)$ and $\tau_i^{-1}(q) \neq \tau_s^{-1}(q)$ for all $i \neq s, t$.*

Proof. We may assume $s = q = 1$.

If $\tau_i^{-1}(1) \neq \tau_1^{-1}(1)$ for all $i \neq 1$ then clearly it is impossible. If $n = 2$ the statement is then clear. Hence assume $n > 2$ and there are r integers, say $1, 2, \ldots, r$, such that $r > 2$, $\tau_1^{-1}(1) = \ldots = \tau_r^{-1}(1)$ and $\tau_i^{-1}(1) \neq \tau_1^{-1}(1)$ for $i = r + 1, \ldots, n$. Now since $A_j - \sum_{i\neq j} A_i = P(\beta_j, \tau_j), j = 1, 2, \ldots, r$ we have

$$\left(A_j - \sum_{i\neq j} A_i\right)_{1\sigma^{-1}(1)} = 0, \quad j = 1, 2, \ldots, r.$$

Since for $k = 1, 2, \ldots, r$, $(A_k)_{1\sigma^{-1}(1)} = 2^{-1}\alpha_1 \neq 0$; hence for $j \neq k$, $1 \leqq j$, $k \leqq r$

$$\left(A_j - A_k - \sum_{i\neq j,k} A_i\right)_{1\sigma^{-1}(1)} \neq 0.$$

Since $A_j + A_k - \sum_{i\neq j,k} A_i$ is a generalized permutation matrix and $\sigma^{-1}(1) \neq \tau_1^{-1}(1)$,

$$\left(A_j + A_k - \sum_{i\neq j,k} A_i\right)_{1\tau_1^{-1}(1)} = 0.$$

Comparing this with $\sum_{i-1}^{n} A_i = P(\alpha, \sigma)$ we conclude that

$$2(A_j + \mathrm{A}_k)_{1\tau_1^{-1}(1)} = 0.$$

Since char $F \neq 2$,

$$(A_j + A_k)_{1\tau_1^{-1}(1)} = 0.$$

But this is true for all $k \neq j$, $1 \leqq j, k \leqq r$ and $r > 2$; hence

$$(A_i)_{1\tau_1^{-1}(1)} = 0, \quad i = 1, 2, \ldots, r$$

a contradiction.

LEMMA 2. *If $\tau_r^{-1}(t) = \tau_s^{-1}(t) \neq \sigma^{-1}(t)$ for some $1 \leqq r, s, t \leqq n$ then for $i \neq r, s$, $(A_i)_{tj} = 0$ for each $j = 1, 2, \ldots, n$.*

Proof. We may assume $r = 1$, $s = 2$ and $t = 1$.

https://doi.org/10.4153/CJM-1976-047-9 Published online by Cambridge University Press

If $n = 2$, the statement is clear. Hence assume $n > 2$. We have seen that $\tau_i^{-1}(1) \neq \tau_1^{-1}(1)$ for $i \neq 1, 2$ in Lemma 1 hence $(A_i)_{1\tau_1^{-1}(1)} = 0$ for all $i \neq 1, 2$.

Suppose there are some $i \neq 1, 2$ such that $(A_i)_{1k} \neq 0$, $k \neq \tau_1^{-1}(1)$. We may assume $(A_i)_{1k} \neq 0$ for $i = 3, 4, \ldots, r$, $3 \leqq r \leqq n$ and $(A_i)_{1k} = 0$ for $i = r + 1, r + 2, \ldots, n$. We choose $\theta_i \in H$, $i = 3, 4, \ldots, n$, according to r is even or r is odd and $k \neq \sigma^{-1}(1)$, $k = \sigma^{-1}(1) \neq \tau_i^{-1}(1)$ or $k = \sigma^{-1}(1) = \tau_i^{-1}(1)$ as follows:

	r even		r odd	
	$k \neq \sigma^{-1}(1)$ or $k = \sigma^{-1}(1) \neq \tau_i^{-1}(1)$	$k = \sigma^{-1}(1) = \tau_i^{-1}(1)$	$k \neq \sigma^{-1}(1)$ or $k = \sigma^{-1}(1) \neq \tau_i^{-1}(1)$	$k = \sigma^{-1}(1) = \tau_i^{-1}(1)$
i even and $3 \leqq i \leqq r - 2$	$\theta_i = -2(A_i)_{1k}$	$\theta_i = -(A_i)_{1k}$	$\theta_i = -2(A_i)_{1k}$	$\theta_i = -(A_i)_{1k}$
i even and $r - 1 \leqq i \leqq r$	$\theta_i = 2(A_i)_{1k}$	$\theta_i = (A_i)_{1k}$		
i odd and $3 \leqq i \leqq r$	$\theta_i = 2(A_i)_{1k}$	$\theta_i = (A_i)_{1k}$	$\theta_i = 2(A_i)_{1k}$	$\theta_i = (A_i)_{1k}$
$r < i \leqq n$	1	1	1	1

Since if $j \neq \sigma^{-1}(1), \tau_1^{-1}(1)$, $(A_i)_{1j} = 0$ for each $i = 1, 2$ and $(A_1)_{1\sigma^{-1}(1)} = (A_2)_{1\sigma^{-1}(1)} = 2^{-1}\alpha_1$ we have

$$(A_1 - A_2)_{1j} = 0 \quad \text{for} \quad j \neq \tau_1^{-1}(1).$$

Hence whether r is even or odd,

$$\left(A_1 - A_2 - \sum_{i=3}^{n} \theta_i A_i\right)_{1k} \neq 0.$$

Since $A_1 - \sum_{1=2}^{n} A_i = P(\beta_1, \tau_1)$ and $(A_i)_{1\tau_1^{-1}(1)} = 0$ for $i \neq 1, 2$ it follows that

$$\left(A_1 - A_2 - \sum_{i=3}^{n} \theta_i A_i\right)_{1\tau_1^{-1}(1)} \neq 0$$

Since $k \neq \tau_1^{-1}(1)$ the matrix $A_1 - A_2 - \sum_{i-3}^{n} \theta_i A_i$ has two nonzero entries in the first row, a contradiction.

This proves $(A_i)_{1j} = 0$ for $i \neq 1, 2$ and $j = 1, 2, \ldots, n$.

LEMMA 3. *If $(A_s)_{t\sigma^{-1}(t)} \neq 0$, $(A_s)_{tj} = 0$ for all $j \neq \sigma^{-1}(t)$, then $(A_i)_{tj} = 0$ for all $i \neq s$, $j = 1, 2, \ldots, n$.*

https://doi.org/10.4153/CJM-1976-047-9 Published online by Cambridge University Press

Proof. We may assume that $s = 1$ and $t = 1$.

Suppose there exist some $i \neq 1$ and $j \neq \sigma^{-1}(1)$ such that $(A_i)_{1j} \neq 0$. Then $A_i = 2^{-1}P(\alpha, \sigma) + 2^{-1}P(\beta, \tau_i)$ and $\tau_i^{-1}(1) = j \neq \sigma^{-1}(1)$ hence $\tau_i \neq \sigma$. By Lemma 2 this is impossible. Hence $(A_i)_{1j} = 0$ for all $i \neq 1$ and $j \neq \sigma^{-1}(1)$.

Now suppose $(A_i)_{1\sigma^{-1}(1)} \neq 0$ for some $i \neq 1$, say $i = 2, 3, \ldots, r$, $2 \leqq r \leqq n$ and $(A_i)_{1\sigma^{-1}(1)} = 0$ for $r + 1 \leqq i \leqq n$. If r is even, choose $\theta_i = (A_i)_{1\sigma^{-1}(1)}$ if i is odd, $1 \leqq i \leqq r$; $\theta_i = -(A_i)_{1\sigma^{-1}(1)}$ if i is even, $1 \leqq i \leqq r$ and $\theta_i = 1$ if $r < i \leqq n$. Then $\theta_i \in H$ for $i = 1, 2, \ldots, n$ and $(\sum_{i-1}^n \theta_i A_i)_{1\sigma^{-1}(1)} = 0$. If r is odd, choose θ_i as in the case r is even for $i = 1, 2, \ldots, r - 2$ and $\theta_i = (A_i)_{1\sigma^{-1}(1)}$ for $i = r - 1, r$; $\theta_i = 1$ for $i = r + 1, r + 2, \ldots, n$. Then $(\sum_{i=1}^n \theta_i A_i)_{1\sigma^{-1}(1)} = 3$. Since we have shown that $(A_i)_{1j} = 0$ for $2 \leqq i \leqq n$, $j \neq \tau^{-1}(1)$ we conclude that $\sum_{i=1}^n \theta_i A_i \notin P(G, H)$ which is a contradiction. This proves Lemma 3.

Now for $A \in M_n(F)$ let $N(A)$ be the number of nonzero entries in A. Recall that

$$A_i = 2^{-1}P(\alpha, \sigma) + 2^{-1}P(\beta_i, \tau_i), \quad i = 1, 2, \ldots, n.$$

If $\tau_i = \sigma$ then $N(A_i) \geqq 1$ since $A_i \neq 0$. If $\tau_i \neq \sigma$ then there exist $j \neq k$ such that $\tau_i^{-1}(j) \neq \sigma^{-1}(j)$, $\tau_i^{-1}(k) \neq \sigma^{-1}(k)$ hence $N(A_i) \geqq 4$. Now with a rearrangement of the subscripts of $A_1, \ldots, A_n$ there exists an integer r, $0 \leqq r \leqq n$ such that $\tau_1 = \tau_2 = \ldots = \tau_r = \sigma$ and for $r < i \leqq n$, $\tau_i \neq \sigma$, i.e. for $1 \leqq i \leqq r$, $N(A_i) \geqq 1$ and $N(A_i) \geqq 4$ for $i = r + 1, r + 2, \ldots, n$. Then the number of nonzero entries in $A_1, \ldots, A_n$ is

$$\sum_{i=1}^{r} N(A_i) + \sum_{i=r+1}^{n} N(A_i) \geqslant r + 4(n - r).$$

On the other hand, by Lemmas 2 and 3, for each t, $1 \leqq t \leqq n$, if $\tau_i^{-1}(t) = \sigma^{-1}(t)$ for all $i = 1, 2, \ldots, n$, there is at most one k such that $(A_k)_{t\sigma^{-1}(t)} \neq 0$ and there is at least one such k for otherwise $\sum_{i=1}^n A_i$ has a zero tth row, a contradiction. If $\tau_j^{-1}(t) \neq \sigma^{-1}(t)$ for some j then there exist exactly one $l \neq j$ such that $\tau_l^{-1}(t) \neq \sigma^{-1}(t)$, $(A_i)_{t\sigma^{-1}(t)} \neq 0$, $(A_i)_{t\tau_i^{-1}(t)} \neq 0$, $i = j, l$ and $(A_i)_{ts} = 0$ for $i \neq j, l$, $s = 1, 2, \ldots, n$. Hence in all $A_1, A_2, \ldots, A_n$ each row either has one nonzero entry or four nonzero entries. Hence there exists an integer s, $0 \leqq s \leqq n$ such that there are s rows with one nonzero entry and $n - s$ rows with four nonzero entries and the number of nonzero entries in $A_1, A_2, \ldots, A_n$ is $s + 4(n - s)$. Hence

$$s + 4(n - s) \geqq r + 4(n - r) \quad \text{or} \quad s - r \geqq 4(s - r)$$

which is possible if and only if $r \geqq s$. But r is the number of matrices among $A_1, A_2, \ldots, A_n$ in which there is at least one row with exactly one nonzero entry. Hence $r > s$ is impossible and $r = s$ or

$$\sum_{i=1}^{r} N(A_i) + \sum_{i=r+1}^{n} N(A_i) = r + 4(n - r).$$

This forces $N(A_i) = 1$ for $i = 1, 2, \ldots, r$ and $N(A_i) = 4$ for $i = r + 1, r + 2, \ldots, n$. Now by multiplying the set $\{A_1, \ldots, A_n\}$ by suitable permutation matrices allows us to assume that for $i = 1, 2, \ldots, r$, $(A_i)_{ii} \neq 0$ and $(A_i)_{jk} = 0$ for either $j \neq i$ or $k \neq i$.

Now if $r = n$ the result is established. If $r < n$ let $r < i \leqq n$. Since $\tau_i \neq \sigma$ there exist distinct $k, l, r < k, l \leqq n$ such that $\sigma^{-1}(k) \neq \tau_i^{-1}(k)$, $\sigma^{-1}(l) \neq \tau_i^{-1}(l)$. Since $N(A_i) = 4$ we have $\sigma^{-1}(q) = \tau_{r+1}^{-1}(q)$ for all $q \neq k, l$. Hence $\tau_i\sigma^{-1} = (kl)$. By Lemma 1 there exists a $j, r < j \leqq n$ and $j \neq i$ such that $\tau_j^{-1}(k) = \tau_i^{-1}(k) \neq \sigma^{-1}(k)$. Also $\tau_j\sigma^{-1} = (kl')$ for some $l' \neq k$. But $\sigma^{-1}(l') = \tau_j^{-1}(k) = \tau_i^{-1}(k) = \sigma^{-1}(l)$. Hence $l = l'$ and $\tau_i = \tau_j$. Since $\sum_{i=1}^{n} A_i = P(\alpha, \sigma)$ it follows that $\beta_{jk} = -\beta_{ik}, \beta_{jl} = -\beta_{il}$ and the matrices have the following form (if $k < l$ and $\sigma^{-1}(k) < \sigma^{-1}(l)$).

$$A_i = \frac{1}{2}\begin{array}{c} \begin{array}{ccccccc} & & \sigma^{-1}(k) & & \sigma^{-1}(l) & & \end{array} \\ \left[\begin{array}{ccccccc} 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & & \vdots \\ & & 0 & & 0 & & \\ 0 & \cdots & 0\ \alpha_k\ 0 & \cdots & 0\ \beta_{ik}\ 0 & \cdots & 0 \\ \vdots & & 0 & & 0 & & \vdots \\ \vdots & & \vdots & & \vdots & & \vdots \\ & & 0 & & 0 & & \\ 0 & \cdots & 0\ \beta_{il}\ 0 & \cdots & 0\ \alpha_l\ 0 & \cdots & \cdot \\ \vdots & & 0 & & 0 & & \vdots \\ \vdots & & \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \end{array}\right] \end{array} \begin{array}{c} \\ \\ \\ \\ k \\ \\ \\ \\ l \\ \\ \\ \\ \end{array}$$

$$A_j = \frac{1}{2}\begin{array}{c} \begin{array}{ccccccc} & & \sigma^{-1}(k) & & \sigma^{-1}(l) & & \end{array} \\ \left[\begin{array}{ccccccc} 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & & \vdots \\ & & 0 & & 0 & & \\ 0 & \cdots & 0\ \alpha_k\ 0 & \cdots & 0\ -\beta_{ik}\ 0 & \cdots & 0 \\ \vdots & & 0 & & 0 & & \vdots \\ \vdots & & \vdots & & \vdots & & \vdots \\ & & 0 & & 0 & & \\ 0 & \cdots & 0\ -\beta_{il}\ 0 & \cdots & 0\ \alpha_l\ 0 & \cdots & 0 \\ \vdots & & 0 & & 0 & & \vdots \\ \vdots & & \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \end{array}\right] \end{array} \begin{array}{c} \\ \\ \\ \\ k \\ \\ \\ \\ l \\ \\ \\ \\ \end{array}.$$

https://doi.org/10.4153/CJM-1976-047-9 Published online by Cambridge University Press

In this way we can pair off the matrices $A_{r+1}, \ldots, A_n$ and multiplying the set $\{A_1, A_2, \ldots, A_n\}$ by suitable permutation matrices we can bring it to the required form. This proves Proposition 2.

6. The group $\mathscr{T}P(G, H)$.

PROPOSITION 3. *If G is a transitive subset of S_n and H a nontrivial subgroup of F^* then $\mathscr{T}P(G, H)$ is a subgroup of the group of all nonsingular $n^2 \times n^2$ matrices over F.*

Proof. We show that span $P(G, H)$ contains a basis for $M_n(F)$. Since G is transitive, given $1 \leqq i, j \leqq n$ we can find $\sigma \in G$ such that $\sigma(j) = i$. Define $\alpha, \beta \in \Gamma_n(H)$ via $\alpha_k = 1$ for all k, $\beta_k = 1$ if $k \neq i$ and $\beta_i = \xi \in H$. Then a simple computation shows that

$$P(\alpha, \sigma) - P(\beta, \sigma) = (1 - \xi)E_{ij}.$$

If $|H| = 2$ then char $F \neq 2$ and choose $\xi = -1$. If $|H| > 2$ choose ξ so that $1 - \xi \neq 0$. Then the set $\{(1 - \xi)E_{ij} : i, j = 1, 2, \ldots, n\}$ is clearly a basis for $M_n(F)$. Hence if $T \in \mathscr{T}P(G, H)$, image $T \supseteq$ span $(P(G, H)) = M_n(F)$ so T is nonsingular.

LEMMA 4. *Let G be a transitive subset of S_n and H a nontrivial subgroup of F^*. If $T \in \mathscr{T}P(G, H)$ and $\sigma \in G$ then $T(\sigma^{-1})$ is a $G - H$ unitary set.*

Proof. Clearly for all $\alpha \in \Gamma_n(H)$ we have

$$\sum_{i=1}^{n} \alpha_i E_{i\sigma^{-1}(i)} = P(\alpha, \sigma) \in P(G, H).$$

Since T preserves $P(G, H)$ we have

$$\sum_{i=1}^{n} \alpha_i T(E_{i\sigma^{-1}(i)}) = T\left(\sum_{i=1}^{n} \alpha_i E_{i\sigma^{-1}(i)}\right) \in P(G, H).$$

Also T is nonsingular hence $T(\sigma^{-1})$ is a linearly independent set and the result follows.

7. Structure of the group $\mathscr{T}P(G, H)$: G regular.

In this section we assume G be a regular subset of S_n ($n > 2$) and H a nontrivial group in $\mathscr{H}$.

LEMMA 5. *If $T \in \mathscr{T}P(G, H)$ and $1 \leqq i, j \leqq n$ then there exist integers $1 \leqq p, q \leqq n$ and $\alpha_{ij} \in H$ such that $T(E_{ij}) = \alpha_{ij}E_{pq}$.*

Proof. If $|H| > 2$ this follows immediately from Proposition 1 and Lemma 4 if we choose $\sigma \in G$ with $\sigma(j) = i$ and consider the $G - H$ unitary set $T(\sigma^{-1})$.

We suppose that $|H| = 2$ then Proposition 2 and Lemma 4 apply. If $r = n$ (i.e. no matrices of the second type appear in $T(\sigma^{-1})$) the result follows. Hence we assume that for some $i \neq l$ we have

https://doi.org/10.4153/CJM-1976-047-9 Published online by Cambridge University Press

$$T(E_{i\sigma^{-1}(i)}) = \begin{array}{c} \begin{array}{ccccccc} & & p & & q & & \end{array} \\ \left[\begin{array}{ccccccc}
0 & \cdots & 0 & \cdots & 0 & \cdots & 0\\
\vdots & & \vdots & & \vdots & & \vdots\\
 & & 0 & & 0 & & \\
0 & \cdots & 0\ \epsilon_1\ 0 & \cdots & 0\ \epsilon_2\ 0 & \cdots & 0\\
\vdots & & 0 & & 0 & & \vdots\\
\vdots & & \vdots & & \vdots & & \vdots\\
 & & 0 & & 0 & & \\
0 & \cdots & 0\ \epsilon_3\ 0 & \cdots & 0\ \epsilon_4\ 0 & \cdots & 0\\
\vdots & & 0, & & 0 & & \vdots\\
\vdots & & \vdots & & \vdots & & \vdots\\
0 & \cdots & 0 & \cdots & 0 & \cdots & 0
\end{array}\right] \end{array} \begin{array}{c} \\ \\ \\ \\ r \\ \\ \\ \\ \\ s \\ \\ \\ \\ \end{array},$$

$$T(E_{l\sigma^{-1}(l)}) = \left[\begin{array}{ccccccc}
0 & \cdots & 0 & \cdots & 0 & \cdots & 0\\
\vdots & & \vdots & & \vdots & & \vdots\\
 & & 0 & & 0 & & \\
0 & \cdots & 0 \pm \epsilon_1\ 0 & \cdots & 0 \mp \epsilon_2\ 0 & \cdots & 0\\
\vdots & & 0 & & 0 & & \vdots\\
\vdots & & \vdots & & \vdots & & \vdots\\
 & & 0 & & 0 & & \\
0 & \cdots & 0 \mp \epsilon_3\ 0 & \cdots & 0 \pm \epsilon_4\ 0 & \cdots & 0\\
\vdots & & 0 & & 0 & & \vdots\\
\vdots & & \vdots & & \vdots & & \vdots\\
0 & \cdots & 0 & \cdots & 0 & \cdots & 0
\end{array}\right] \begin{array}{c} \\ \\ \\ r \\ \\ \\ \\ s \\ \\ \\ \\ \end{array}.$$

We now note that (just writing the appropriate 2-square submatrices and choosing signs properly)

$$X = T(E_{i\sigma^{-1}(i)}) + T(E_{l\sigma^{-1}(l)}) = \begin{array}{c} \begin{array}{cc} p & q \end{array} \\ \begin{bmatrix} \eta_1 & 0 \\ 0 & \eta_2 \end{bmatrix} \end{array} \begin{array}{c} r \\ s \end{array},$$

$$Y = T(E_{i\sigma^{-1}(i)}) - T(E_{l\sigma^{-1}(l)}) = \begin{bmatrix} 0 & \eta_3 \\ \eta_4 & 0 \end{bmatrix} \begin{array}{c} r \\ s \end{array}, \quad \eta_i \in H.$$

Since $n > 2$ there exists an integer k $(1 \leqq k \leqq n)$ such that $k \neq i, l$. The set G is regular so that the knowledge of one nonzero position in a matrix $P(\alpha, \tau)$ determines the permutation τ uniquely. We now note that the two

https://doi.org/10.4153/CJM-1976-047-9 Published online by Cambridge University Press

matrices

$$\sum_{k\neq i,l} T(E_{k\sigma^{-1}(k)}) + X \quad \text{and} \quad \sum_{k\neq i,l} T(E_{k\sigma^{-1}(k)}) + Y$$

belong to $P(G, H)$ and have at least one nonzero entry in common, a contradiction. Therefore the case in question cannot occur and the result follows.

Recall that we write $G = \{g_1, \ldots, g_n\}$ and $h_i = g_i^{-1}$. For $k = 1, 2, \ldots, n$ the set $T(h_k)$ is a $G - H$ unitary set of matrices so it follows that

$$T(h_k) = \{\beta_i E_{ip_k^{-1}(i)} : i = 1, 2, \ldots, n\}$$

for some $p_k \in G$ hence there exists $\mu_k \in S_n$ such that

$$T(E_{ih_k(i)}) = \alpha_{ih_k(i)} E_{\mu_k(i)p_k^{-1}\mu_k(i)}, \quad i = 1, 2, \ldots, n.$$

Since T is nonsingular, there exists $\sigma \in S_n$ such that $p_k = g_{\sigma(k)}$, $k = 1, 2, \ldots, n$. Hence

$$T(E_{ih_k(i)}) = \alpha_{ih_k(i)} E_{\mu_k(i)h_{\sigma(k)}\mu_k(i)}, \quad i, k = 1, 2, \ldots, n.$$

On the other hand, a simple computation verifies that such T is in $\mathscr{T}P(G, H)$ for any choices $\alpha_1, \alpha_2, \ldots, \alpha_n \in \Gamma_n(H)$ and $\mu_1, \mu_2, \ldots, \mu_n, \sigma \in S_n$. This proves Theorem 1.

Now for an n-square matrix $X = (x_{ij})$ and $g_k \in G$ we write

$$X_{h_k} = \sum_{i=1}^{n} x_{ih_k(i)} E_{ih_k(i)}.$$

Then for $T \in \mathscr{T}P(G, H)$,

$$T(X_{h_k}) = \sum_{i=1}^{n} x_{ih_k(i)} \alpha_{ih_k(i)} E_{\mu_k(i)h_{\sigma(k)}\mu_k(i)}$$

for some $\alpha_1, \ldots, \alpha_n \in \Gamma_n(H)$, $\mu_1, \mu_2, \ldots, \mu_n$, $\sigma \in S_n$. By setting $j = \mu_k(i)$ we have

$$T(X_{h_k}) = \sum_{j=1}^{n} x_{\mu_k^{-1}(j)h_k\mu_k^{-1}(j)} \alpha_{\mu_k^{-1}(j)h_k\mu_k^{-1}(j)} E_{jh_{\sigma(k)}(j)}.$$

Since $X_{h_k} = \operatorname{diag}(x_{1h_k(1)}, \ldots, x_{nh_k(n)}) P(g_k)$ we have

$$\begin{aligned} T(X_{h_k}) &= \operatorname{diag}(x_{\mu_k^{-1}(1)h_k\mu_k^{-1}(1)} \alpha_{\mu_k^{-1}(1)h_k\mu_k^{-1}(1)}, \ldots, \\ &\qquad x_{\mu_k^{-1}(n)h_k\mu_k^{-1}(n)} \alpha_{\mu_k^{-1}(n)h_k\mu_k^{-1}(n)}) P(g_{\sigma(k)}) \\ &= P(\mu_k) \operatorname{diag}(x_{1h_k(1)}\alpha_{1h_k(1)}, \ldots, x_{nh_k(n)}\alpha_{nh_k(n)}) P(\mu_k^{-1} g_{\sigma(k)}) \\ &= P(\mu_k)(X_{h_k} * A_{h_k}') P(h_k \mu_k^{-1} g_{\sigma(k)}) \quad \text{where } A' = (\alpha_{ij}) \in M_n(H) \\ &= P(\mu_k) A_{h_k}' P(h_k \mu_k^{-1} g_{\sigma(k)}) * P(\mu_k) X_{h_k} P(h_k \mu_k^{-1} g_{\sigma(k)}). \end{aligned}$$

Since $X = \sum_{k-1}^{n} X_{h_k}$,

$$T(X) = A * \sum_{i=1}^{n} P(\mu_i) X_{h_i} P(h_i \mu_i^{-1} g_{\sigma(i)})$$

https://doi.org/10.4153/CJM-1976-047-9 Published online by Cambridge University Press

where $A = \sum_{j=1}^{n} P(\mu_j)A_{h_j}'P(h_j\mu_j^{-1}g_{\sigma(j)})$. Hence T associates with a matrix A in $M_n(H)$ and $\mu_1, \mu_2, \ldots, \mu_n, \sigma \in S_n$. Let S be another element in $\mathscr{T}P(G, H)$ which associates with B in $M_n(H)$ and $\nu_1, \nu_2, \ldots, \nu_n, \tau \in S_n$, i.e.

$$S(X) = B * \sum_{i=1}^{n} P(\nu_i)X_{h_i}P(h_i\nu_i^{-1}g_{\sigma(i)}).$$

Then

$$\begin{aligned} ST(X) &= B * \sum_{i=1}^{n} P(\nu_{\sigma(i)})(A_{h_{\sigma(i)}} * P(\mu_i)X_{h_i}P(h_i\mu_i^{-1}g_{\sigma(i)})) \\ &\qquad\qquad \times P(h_{\sigma(i)}\nu_{\sigma(i)}^{-1}g_{\tau\sigma(i)}) \\ &= B * \sum_{i=1}^{n} P(\nu_i)A_{h_i}P(h_i\nu_i^{-1}g_{\tau(i)}) * \\ &\qquad\qquad \sum_{j=1}^{n} P(\nu_{\sigma(j)}\mu_j)X_{h_j}P(h_j\mu_j^{-1}\nu_{\sigma(j)}^{-1}g_{\tau\sigma(j)}), \end{aligned}$$

i.e. ST associates with a matrix $B*A^{\langle\tau,(\nu_1,\ldots,\nu_n)\rangle}$ and $\nu_{\sigma(1)}\mu_1, \ldots, \nu_{\sigma(n)}\mu_n, \tau\sigma \in S_n$ if we define $A^{\langle\tau,(\nu_1,\ldots,\nu_n)\rangle}$ as in (3.1). Also it is easy to see that if T associates with $A = J$, $\mu_1 = \ldots = \mu_n = e$ then $T(X) = X$ for all $X \in M_n(F)$. This proves Theorem 2.

8. Structure of the group $\mathscr{T}P(G, H)$: G doubly transitive.

In this section let H be a nontrivial group in $\mathscr{H}$ and $n > 2$.

LEMMA 6. *Suppose G is a doubly transitive subset of S_n. If $T \in \mathscr{T}P(G, H)$ and $1 \leqq i, j \leqq n$ then there exist integers $1 \leqq p, q \leqq n$ and $\alpha_{ij} \in H$ such that $T(E_{ij}) = \alpha_{ij}E_{pq}$.*

Proof. If $|H| > 2$ then the result follows from Proposition 1 and Lemma 4. We suppose that $|H| = 2$ and proceed as in Lemma 5 to obtain (only writing the appropriate 2-square submatrices)

$$T(E_{i\sigma^{-1}(i)}) = \overset{\quad p \qquad q}{\begin{bmatrix} \epsilon_1 & \epsilon_2 \\ \epsilon_3 & \epsilon_4 \end{bmatrix}}\begin{matrix} r \\ s \end{matrix}, \quad T(E_{l\sigma^{-1}(l)}) = \overset{\quad p \qquad q}{\begin{bmatrix} \pm\epsilon_1 & \mp\epsilon_2 \\ \mp\epsilon_3 & \pm\epsilon_4 \end{bmatrix}}\begin{matrix} r \\ s \end{matrix}.$$

Now $n > 2$ so there exists $k \neq i, l$. Since G is doubly transitive, choose $\tau \in G$ such that $\tau^{-1}(l) \neq \sigma^{-1}(l)$ and $\tau^{-1}(i) = \sigma^{-1}(i)$. Repeating the argument for $T(_\tau{}^{-1})$ we find

$$T(E_{i\tau^{-1}(i)}) = \begin{bmatrix} \epsilon_1 & \epsilon_2 \\ \epsilon_3 & \epsilon_4 \end{bmatrix}$$

so by Proposition 2 we find there must exist k such that

$$T(E_{k\tau^{-1}(k)}) = \begin{bmatrix} \pm\epsilon_1 & \mp\epsilon_2 \\ \mp\epsilon_3 & \pm\epsilon_4 \end{bmatrix} = \pm T(E_{l\tau^{-1}(l)}).$$

Now if $l \neq k$ this implies T is singular, and if $l \neq k$, $\tau^{-1}(l) \neq \sigma^{-1}(l)$ so again T is singular, a contradiction.

In the following we assume that G is a doubly transitive subgroup of S_n. Now we have

$$T(E_{ij}) = \alpha_{ij}E_{pq} \quad \text{for some } \alpha_{ij} \in H \text{ and } 1 \leqq p, q \leqq n.$$

If there exist $1 \leqq k \leqq n$ and $\alpha_{ik} \in H$ such that $k \neq j$ and

$$T(E_{ik}) = \alpha_{ik}E_{rs} \quad \text{with } p \neq r \text{ and } q \neq s$$

then choose $\sigma \in G$ such that $\sigma^{-1}(r) = s$ and $\sigma^{-1}(p) = q$. Let $P(\sigma) = \sum_{i=1}^{n} E_{i\sigma^{-1}(i)} \in P(G, H)$. Now $T^{-1} \in \mathscr{T}P(G, H)$ by Proposition 3, however since $T^{-1}(E_{rs}) = \alpha_{ik}{}^{-1}E_{ik}$ and $T^{-1}(E_{pq}) = \alpha_{ij}{}^{-1}E_{ij}$ the matrix $T^{-1}(P(\sigma))$ must have two nonzero entries in row i and since it has n nonzero entries it must have a row equal to zero and is singular, a contradiction. Hence we may conclude that either

$$T(E_{ij}) = \alpha_{ij}E_{p\mu(j)}, \quad j = 1, 2, \ldots, n \quad \text{or}$$
$$T(E_{ij}) = \alpha_{ij}E_{\mu(j)q}, \quad j = 1, 2, \ldots, n$$

for some $\mu \in S_n$. Suppose that for some $1 \leqq i, k \leqq n$ $(i \neq k)$ and $\sigma, \mu \in S_n$ that

$$T(E_{ij}) = \alpha_{ij}E_{p\sigma(j)}, \quad j = 1, 2, \ldots, n,$$
$$T(E_{kr}) = \alpha_{kr}E_{\mu(r)q}, \quad r = 1, 2, \ldots, n.$$

Now $\sigma(j) = q$ for some j, and $\mu(r) = p$ for some r, hence

$$\alpha_{ij}{}^{-1}T(E_{ij}) = E_{p\sigma(j)} = E_{\mu(r)q} = \alpha_{kr}{}^{-1}T(E_{kr})$$

so the matrices $T(E_{ij})$ and $T(E_{kr})$ are linearly dependent and T is singular; a contradiction. Hence either

$$T(E_{ij}) = \alpha_{ij}E_{\sigma(i)\mu(j)}, \quad i, j = 1, 2, \ldots, n \quad \text{or}$$
$$T(E_{ij}) = \alpha_{ij}E_{\mu(j)\sigma(i)}, \quad i, j = 1, 2, \ldots, n$$

for some $\sigma, \mu \in S_n$, or with a short computation either

$$T(X) = A*P(\sigma)XP(\mu^{-1}), \quad X \in M_n(F) \quad \text{or}$$
$$T(X) = A*P(\mu){}^tXP(\sigma^{-1}), \quad X \in M_n(F).$$

Now if the first form occurs let $\tau \in G$. Since $T(P(\tau)) \in P(G, H)$ we have $\sigma\tau\mu^{-1} \in G$. Hence $\sigma G\mu^{-1} \subseteq G$ and it follows that $\sigma G \mu^{-1} = G$. Let

$$L = \{(\sigma, \mu) \in S_nXS_n : \sigma G\mu^{-1} = G\}.$$

Clearly L is a subgroup of $S_n \times S_n$. If $\sigma \notin N(G)$ then since S_n is a group, there exists $\nu \in S_n$ such that $\mu^{-1} = \sigma^{-1}\nu$ and we have $G = \sigma G\mu^{-1} = \sigma G\sigma^{-1}\nu = G'\nu$ where $G' = \sigma G \sigma^{-1}$ is a subgroup of S_n. Hence $\nu \in G'$ and $G = G'$ a contradiction. Similarly $\mu \in N(G)$ hence L is a subgroup of $N(G)XN(G)$. Now clearly if $(\sigma, \mu) \in L$ and one of σ, μ is in G then the other element must be in G. If $\mu \in N(G) - G$ then again we write $\sigma = \nu\mu$ for some $\nu \in S_n$ and $G = \nu\mu G \mu^{-1} = \nu G$ implies $\nu \in G$, i.e. $\sigma \in G\mu$. Consequently if we let $N'(G) = \{(\sigma, \sigma) : \sigma \in N(G)\}$ then $L = (GX\{e\}) \,.\, N'(G)$. If the second form occurs let $\tau \in G$ then again $\mu\tau^{-1}\sigma^{-1} \in G$, i.e. $\mu G^{-1}\sigma^{-1} \subseteq G$. Since G is a group we have $\mu G \sigma^{-1} \subseteq G$ or $\mu G \sigma^{-1} = G$ i.e. $(\mu, \sigma) \in L$. Therefore we have either

(8.1) $\quad T(X) = A * P(\sigma\mu) X P(\mu^{-1}), \quad X \in M_n(F) \quad$ or

(8.2) $\quad T(X) = A * P(\sigma\mu)\, {}^t X P(\mu^{-1}), \quad X \in M_n(F)$

where $\sigma \in G$ and $\mu \in N(G)$. On the other hand it is easily seen that for any $\mu \in N(G)$ and $\sigma \in G$, the T defined by (8.1) and (8.2) are in $\mathscr{T}P(G, H)$. This proves Theorem 3.

Now let $\mathscr{T}_1 P(G, H)$ be the set of all elements in $\mathscr{T}P(G, H)$ of the form (8.1) with $\sigma = e$. If T, S are in $\mathscr{T}_1 P(G, H)$ and associate with $\mu \in N(G)$, $A \in M_n(H)$ and $\tau \in N(G)$, $B \in M_n(H)$ respectively, i.e.

$$T(X) = A * P(\mu) X P(\mu^{-1}), \quad X \in M_n(F),$$
$$S(X) = B * P(\tau) X P(\tau^{-1}), \quad X \in M_n(F)$$

then

$$ST(X) = B * A^{\tau} * P(\tau\mu) X P((\tau\mu)^{-1}), \quad X \in M_n(F)$$

where $A^{\tau} = P(\tau) A P(\tau^{-1})$, i.e. ST associates with the element $\tau\mu \in N(G)$ and $B * A^{\tau}$ in $M_n(H)$. Also if T associate with $e \in N(G)$, $A = J$ then clearly T is the identity linear transformation on $M_n(F)$. Hence $\mathscr{T}_1 P(G, H)$ is isomorphic to the group $\langle N(G), M_n(H) \rangle$.

Recall that $P(G) = \{P(\sigma) : \sigma \in G\}$ and for $\sigma \in G$ we define $P(\sigma)(X) = P(\sigma) X$, $X \in M_n(F)$. Clearly S of the form (8.1) associates with $\sigma \in G$, $\mu \in N(G)$, $A \in M_n(H)$ if and only if $S = P(\sigma) \circ T$ where T in $\mathscr{T}_1 P(G, H)$ associates with $\mu \in N(G)$ and $P(\sigma^{-1}) A \in M_n(H)$. Hence if we denote by $\mathscr{T}_2 P(G, H)$ the set of all elements in $\mathscr{T}P(G, H)$ of the form (8.1) then

$$\mathscr{T}_2 P(G, H) = P(G) \circ \mathscr{T}_1 P(G, H).$$

By a simple computation we see that $\mathscr{T}_2 P(G, H)$ is a group hence $\mathscr{T}_1 P(G, H)$ is of index $|G|$ in $\mathscr{T}_2 P(G, H)$.

Finally if $R(X) = {}^t X$, $X \in M_n(F)$ then clearly S is in $\mathscr{T}P(G, H)$ of the form (8.2) if and only if $S = TR$ where T is in $\mathscr{T}_2 P(G, H)$. This completes the proof of Theorem 4.

References

1. J. Dieudonné, *Sur une généralisation du groupe orthogonal a quatre variables*, Arch. Math. *1* (1949), 282–287.

2. M. Marcus, *All linear operators leaving the unitary group invariant*, Duke Math. J. *26* (1959), 155–163.

https://doi.org/10.4153/CJM-1976-047-9 Published online by Cambridge University Press

3. ——— *Linear transformations on matrices*, J. Res. NBS *75B* (Math. Sci.) No. 3 and 4 (1971), 107–113.

4. M. Marcus and B. Moyls, *Transformations on tensor product spaces*, Pacific J. Math. *9* (1959), 1215–1221.

5. M. Marcus and R. Purves, *Linear transformations on algebras of matrices II: The invariance of the elementary symmetric functions*, Can. J. Math. *11* (1959), 383–396.

University of Toronto,
Toronto, Ontario