UNIMODULAR GROUP MATRICES WITH RATIONAL INTEGERS AS ELEMENTS

R. C. THOMPSON

1. Introduction. Let G be a finite group of order n with elements $g_1, g_2, \cdots, g_n$. Let

$$x_{g_i}\,, \qquad 1 \leqq i \leqq n \tag{1}$$

be variables in one-to-one correspondence with the elements of G. The $n \times n$ matrix

$$X = (x_{g_i g_j^{-1}})_{1 \leqq i, j \leqq n} \tag{2}$$

is called the group matrix for G. If numerical values are substituted for the variables (1) in X, we say X is a group matrix for G. In this paper we study group matrices which have rational integers as elements. Let A' denote the transpose of the matrix A. A generalized permutation matrix is a square matrix with only 0, 1, -1 as elements and having exactly one nonzero element in each row and in each column. A square matrix A is said to be unimodular if the determinant of A is ± 1. The result obtained in this paper is the following theorem.

THEOREM. *Let G be a finite solvable group. Let A be a unimodular matrix of rational integers such that $B = AA'$ is a group matrix for G. Then $A = A_1T$ where A_1 is a unimodular group matrix of rational integers for G and T is a generalized permutation matrix.*

This theorem has already been proved for cyclic groups in [1] and for abelian groups in [2]. The present proof is a modification of the proof in [2].

2. Proof of the theorem. Let

$$1 = H_0 \subset H_1 \subset H_2 \subset \cdots \subset H_{m-1} \subset H_m = G \tag{3}$$

be an ascending chain of subgroups of G, where each H_{i-1} is normal in H_i with cyclic factor group H_i/H_{i-1} of order n_i, $1 \leqq i \leqq m$. We let $n_0 = 1$, so that H_i has order $n_0 n_1 \cdots n_i$. In order to simplify the proof we take the elements of G in a particular order. This will not affect the theorem as a reordering of the elements of G changes the group matrix X to PXP' for P a permutation matrix. Thus let

Received August 20, 1963.

H_i be generated by the elements of H_{i-1} and an element a_i such that the coset a_iH_{i-1} has order n_i. By induction we define column vectors V_i of the elements of H_i. We let

$$V_0 = (1) \tag{4}$$

be the one row column vector whose only element is the identity of G. Suppose

$$V_{i-1} = (h_1, h_2, \cdots, h_t)' \tag{5}$$

with

$$t = n_0n_1 \cdots n_{i-1}\ , \tag{6}$$

has been defined, where $h_1, h_2, \cdots, h_t$ are the ordered elements of H_{i-1}. For any $g \in G$ let

$$g V_{i-1} = (gh_1, gh_2, \cdots, gh_t)'\ ,$$
$$V_{i-1}g = (h_1g, h_2g, \cdots, h_tg)'\ .$$

Then define V_i to be the column vector

$$V_i = \begin{bmatrix} V_{i-1} \\ a_i V_{i-1} \\ a_i^2 V_{i-1} \\ \cdots \\ a_i^{n_i-1} V_{i-1} \end{bmatrix} . \tag{7}$$

For an arbitrary finite group G with ordered elements $g_1, g_2, \cdots, g_n$ we define the *left regular representation* of G by the matrix equations

$$(gg_1, gg_2, \cdots, gg_n) = (g_1, g_2, \cdots, g_n)P^L(g)\ , \qquad g \in G\ .$$

Here $P^L(g)$ is a permutation matrix depending on the element $g \in G$. It is straightforward to check that the matrix X of (2) is given by

$$X = \sum_{g \in G} x_g P^L(g)\ .$$

The set of all $P^L(g)$ for $g \in G$ is denoted by $L(G)$.

We define the *right regular representation* of G by

$$(g_1g, g_2g, \cdots, g_ng)' = P(g)(g_1, g_2, \cdots, g_n)'\ , \qquad g \in G\ .$$

The set of all permutation matrices $P(g)$ for $g \in G$ is denoted by $R(G)$.

The group ring of the left (right) regular representation is the set of all linear combinations of the $P^L(g)$ $(P(g))$ for $g \in G$, and is denoted by $L^*(G)$ $(R^*(G))$. Thus the matrix (2) is the typical member of $L^*(G)$. The following two known facts are vital for the proof of our theorem:

(i) any matrix in $L^*(G)$ commutes with any matrix in $R^*(G)$;

(ii) any matrix that commutes with all the matrices in $R(G)$ is a member of $L^*(G)$.

NOTATION. We let diag $(X_1, X_2, \cdots, X_k)_k$ denote the direct sum of the square matrices $X_1, X_2, \cdots, X_k$:

$$\operatorname{diag}(X_1, X_2, \cdots, X_k)_k = \begin{bmatrix} X_1 & 0 & 0 & \cdots & 0 \\ 0 & X_2 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdots & 0 \\ 0 & 0 & 0 & \cdots & X_k \end{bmatrix}.$$

We set $[X_1]_1 = X_1$. If $k > 1$ and $X_1, X_2, \cdots, X_k$ are square matrices of the same size, we set

$$[X_1, X_2, \cdots, X_k]_k = \begin{bmatrix} 0 & X_1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & X_2 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & 0 & 0 & \cdots & X_{k-1} \\ X_k & 0 & 0 & 0 & \cdots & 0 \end{bmatrix}.$$

We construct certain of the matrices in $R(G)$, where now the elements of G are ordered according to (4), (5), (6), (7). Let i be fixed, $1 \leqq i \leqq m$. Since H_{i-1} is normal in H_i, $V_{i-1}a_i = a_i P_{i-1}(a_i) V_{i-1}$ where $P_{i-1}(a_i)$ is a $t \times t$ permutation matrix (t as in (6)). Then, since

$$(8) \qquad a_i^{n_i} \in H_{i-1} ,$$

and because of (7), $V_i a_i = P_i(a_i) V_i$, where $P_i(a_i)$ is permutation matrix with the structure

$$(9) \qquad P_i(a_i) = [P_{i-1}(a_i), P_{i-1}(a_i), \cdots, P_{i-1}(a_i), \bar{P}_{i-1}(a_i)]_{n_i} .$$

In (9), $\bar{P}_{i-1}(a_i)$ is another $t \times t$ permutation matrix.

Because of (7), we also have for any $g \in H_{i-1}$, that $V_i g = P_i(g) V_i$, where the permutation matrix $P_i(g)$ has the structure

$$(10) \qquad P_i(g) = \operatorname{diag}(P_{i-1}(g), P_{i-1}(g), \cdots, P_{i-1}(g))_{n_i} , \qquad g \in H_{i-1} .$$

In (10), $P_i(g)$ is a block scalar matrix. The diagonal blocks $P_{i-1}(g)$ have dimensions $t \times t$. Furthermore, as g runs over the elements of H_{i-1}, $P_{i-1}(g)$ runs over all the matrices of $R(H_{i-1})$. Since H_i is generated by H_{i-1} and a_i, the matrices $P_i(g)$ for $g \in H_{i-1}$ and $P_i(a_i)$ generate $R(H_i)$.

Because of the ordering of the elements of G, the following block scalar matrices:

$$Q(g) = \operatorname{diag}(P_i(g), \cdots, P_i(g))_u, \qquad g \in H_{i-1} \text{ or } g = a_i, \tag{11}$$

$$u = n/tn_i, \tag{12}$$

are the matrices in $R(G)$ determined by the $g \in H_{i-1}$ and by $g = a_i$. Here $Q(g)$ is $n \times n$.

We now prove our theorem by the following induction argument. Suppose for a fixed i, $1 \leqq i \leqq m$, that $B = AA'$ and that

$$AQ(g) = Q(g)A, \qquad \text{for any } g \in H_{i-1}. \tag{13}$$

(In particular this is satisfied if $i = 1$ since then the only such $Q(g)$ is I_n, the $n \times n$ identity matrix.) We shall then show that a generalized permutation matrix T exists such that $B = (AT)(AT)'$ and such that $ATQ(g) = Q(g)AT$ for any $g \in H_{i-1}$ and for $g = a_i$, and so, in consequence, for any $g \in H_i$. Thus the induction will eventually yield a generalized permutation matrix T_1 such that $B = (AT_1)(AT_1)'$ and such that $AT_1Q(g) = Q(g)AT_1$ for any $g \in G$. It will now follow from (ii) that $AT_1 \in L^*(G)$, and the proof will be complete.

Hence assume $B = AA'$ where A satisfies (13). Partition

$$A = (A_{\alpha,\beta}), \qquad 1 \leqq \alpha, \beta \leqq v = n_i u, \tag{14}$$

into blocks of dimensions $t \times t$. As $Q(g)$ for $g \in H_{i-1}$ is a block scalar matrix with the blocks $P_{i-1}(g)$ of $R(H_{i-1})$ on the main block diagonal, it follows from (ii) and (13) that each

$$A_{\alpha,\beta} \in L^*(H_{i-1}), \qquad 1 \leqq \alpha, \beta \leqq v. \tag{15}$$

Since $B \in L^*(G)$, $BQ(a_i) = Q(a_i)B$ so that if

$$M = A^{-1}Q(a_i)A, \tag{16}$$

then,

$$MM' = I_n. \tag{17}$$

As A is unimodular the elements of M are integers. Hence (17) implies that M is a generalized permutation matrix. Partition A, A^{-1}, $Q(a_i)$, and M into $t \times t$ blocks. As each block of A lies in $L^*(H_{i-1})$ and as A^{-1} is a polynomial in A, each of the $t \times t$ blocks of A, of A^{-1}, and of $Q(a_i)$ is a linear combination of a finite number of $t \times t$ permutation matrices. Therefore each $t \times t$ block of M is a linear combination of a finite number of $t \times t$ permutation matrices. A permutation matrix is *doubly stochastic* in the sense that the sums across each row and down each column all have a common value.

As linear combinations of matrices doubly stochastic in this sense remain doubly stochastic, each $t \times t$ block of M is doubly stochastic. Let M_1 be a typical $t \times t$ block in M. Since M is a generalized permutation matrix, M_1 contains at most one nonzero element in each of its rows and columns. As M_1 is doubly stochastic, it now follows that M_1, if it is not the zero matrix, is either a permutation matrix or the negative of a permutation matrix. Since M is a generalized permutation matrix, it follows that, after partitioning into $t \times t$ blocks, M is a "generalized permutation matrix" in that it has exactly one nonzero block in each of its block rows and in each of its block columns. Each nonzero block is $\pm$ a permutation matrix.

There exists a permutation matrix R consisting of $t \times t$ blocks which are either the $t \times t$ zero matrix or I_t such that $R'MR$ is a direct sum of cycles. That is, $R'MR = \operatorname{diag}(E_1, E_2, \cdots, E_r)_r$ where

$$E_\delta = [E_{\delta,1}, E_{\delta,2}, \cdots, E_{\delta,e_\delta}]_{e_\delta}\,, \qquad 1 \leqq \delta \leqq r\,. \tag{18}$$

Here each $E_{\delta,\omega}$ is $\pm$ a $t \times t$ permutation matrix.

Note that $RQ(g) = Q(g)R$ for any $g \in H_{i-1}$ since each such $Q(g)$ is block scalar when partitioned into $t \times t$ blocks. Thus

$$ARQ(g) = Q(g)AR\,, \qquad \text{for any } g \in H_{i-1}\,,$$

and

$$(AR)^{-1}Q(a_i)AR = R'MR$$

is a direct sum of $E_1, E_2, \cdots, E_r$. Thus if we change notation and replace AR with A and $R'MR$ with M, we have (13), (14), (15), (16), (18) and

$$M = \operatorname{diag}(E_1, E_2, \cdots, E_r)_r\,.$$

Our immediate goal is to prove that each e_δ is n_i and that $r = u$. Because of (8)

$$\begin{aligned} M^{n_i} &= A^{-1}Q(a_i^{n_i})A \\ &= A^{-1}Q(g)A && \text{for some } g \in H_{i-1}\,, \\ &= Q(g) && \text{by (13)}\,. \end{aligned}$$

Hence each cycle E_δ of M has the property that

$$E_\delta^{n_i}$$

is block scalar. This is not possible if $e_\delta > n_i$. Hence each $e_\delta \leqq n_i$.

Counting rows in M we get $t(e_1 + e_2 + \cdots + e_r) = n$. If any $e_\delta < n_i$ we would have

$$r > u \,. \tag{19}$$

Let $A_\alpha = (A_{\alpha,1}, A_{\alpha,2}, \cdots, A_{\alpha,v})$, $1 \leqq \alpha \leqq v$, be the block rows of A. For each fixed d such that $0 \leqq d < u$ it follows from (9), (11), and $Q(a_i)A = AM$ that

$$P_{i-1}(a_i)A_{dn_i+k} = A_{dn_i+k-1}M\,, \qquad 2 \leqq k \leqq n_i\,. \tag{20}$$

Let $w_0 = 0$ and let $w_\delta = e_1 + e_2 + \cdots + e_\delta$ for $1 \leqq \delta \leqq r$. Then (20) implies than for $2 \leqq \mathrm{k} \leqq n_i$ and $0 \leqq \delta \leqq r - 1$,

$$\begin{aligned}(A_{dn_i+k,w_\delta+1}, \cdots, A_{dn_i+k,w_\delta+1}) \\ = P_{i-1}(a_i)^{1-k}(A_{dn_i+1,w_\delta+1}, \cdots, A_{dn_i+1,w_\delta+1})E_{\delta+1}^{k-1}\,.\end{aligned} \tag{21}$$

For each fixed d, δ such that $0 \leqq d < u$, $0 \leqq \delta < r$, let $F_{d,\delta}$ be the submatrix of A containing the blocks $A_{\alpha,\beta}$ with $dn_i + 1 \leqq \alpha \leqq (d+1)n_i$ and $w_\delta + 1 \leqq \beta \leqq w_{\delta+1}$. Since each $A_{\alpha,\beta} \in L^*(H_{i-1})$, each row of a given $A_{\alpha,\beta}$ is a permutation of the first row of this $A_{\alpha,\beta}$. Since $P_{i-1}(a_i)$ and $E_{\delta+1}$ are generalized permutation matrices, this fact and (21) imply that each row of $F_{d,\delta}$ is a generalized permutation of the first row of $F_{d,\delta}$. Thus if we add all the columns of $F_{d,\delta}$ after the first to the first column of $F_{d,\delta}$ we produce a new matrix $\bar{F}_{d,\delta}$ in which the integers in the first column of $\bar{F}_{d,\delta}$ are all equal, modulo 2. Next add the first row of $\bar{F}_{d,\delta}$ to all the other rows of $\bar{F}_{d,\delta}$ to get a new matrix $\tilde{F}_{d,\delta}$. Then all the integers in the first column of $\tilde{F}_{d,\delta}$ below the top element are zero, modulo 2.

Now partition $A = (F_{d,\delta})$ into its blocks $F_{d,\delta}$. For each fixed δ, $0 \leqq \delta < r$, add to that column of A that intersects $F_{0,\delta}$ at the extreme left of $F_{0,\delta}$, all the other columns of A that intersect $F_{0,\delta}$. This produces a new matrix $\bar{A} = (\bar{F}_{d,\delta})$. For each fixed d, $0 \leqq d < u$, add the topmost row of $\bar{A}$ that intersects $\bar{F}_{d,0}$ to all the other rows of $\bar{A}$ that intersect $\bar{F}_{d,0}$. We get a new matrix $\tilde{A} = (\tilde{F}_{d,\delta})$. The r columns of $\tilde{A}$ that intersect $\tilde{F}_{0,\delta}$ at the extreme left of $\tilde{F}_{0,\delta}$, $0 \leqq \delta < r$, may now be regarded as vectors in a u dimensional vector space over the field of two elements. As $r > u$, these vectors are dependent and so $\tilde{A}$ (and hence A) is singular, modulo 2. This is a contradiction since the determinant of A is ± 1.

Consequently each $e_\delta = n_i$, $1 \leqq \delta \leqq r$, and $r = u$.

Now let $E_{p,q} = \varphi_{p,q}\bar{E}_{p,q}$ where $\varphi_{p,q} = \pm 1$ and $\bar{E}_{p,q}$ is a permutation matrix. Let δ be fixed, $1 \leqq \delta \leqq u$. Suppose that $P_{i-1}(a_i)$ has a one at position $(1, \omega)$ and let $\bar{E}_{\delta,1}$ have a one at position $(1, \mu)$. Let $K_{\delta,1}$ be the permutation matrix in $L(H_{i-1})$ with a one at position (μ, ω). ($K_{\delta,1}$ is the matrix in $L(H_{i-1})$ representing $h_\mu h_\omega^{-1}$; see (2) and (5).) Then $\tilde{E}_{\delta,1} = \bar{E}_{\delta,1}K_{\delta,1}$ has the same first row as $P_{i-1}(a_i)$. Similarly, by induction, we determine $K_{\delta,s}$ in $L(H_{i-1})$, $1 < s < n_i$, such that the permutation matrices

$$\tilde{E}_{\delta,s} = K'_{\delta,s-1}\bar{E}_{\delta,s}K_{\delta,s} , \qquad 1 < s < n_i ,$$

each have the same first row as $P_{i-1}(a_i)$. Then let

$$S_\delta = \operatorname{diag}\left(I_t, \varphi_{\delta,1}K_{\delta,1}, \varphi_{\delta,1}\varphi_{\delta,2}K_{\delta,2}, \cdots, \left(\prod_{j=1}^{n_i-1}\varphi_{\delta,j}\right)K_{\delta,n_i-1}\right)_{n_i} ,$$

and let $S = \operatorname{diag}(S_1, S_2, \cdots, S_u)_u$. Then

$$S'MS = \operatorname{diag}(\tilde{E}_1, \tilde{E}_2, \cdots, \tilde{E}_u)_u$$

where

$$\tilde{E}_\delta = [\tilde{E}_{\delta,1}, \tilde{E}_{\delta,2}, \cdots, \tilde{E}_{\delta,n_i-1}, \pm \tilde{E}_{\delta,n_i}]_{n_i} , \qquad 1 \leqq \delta \leqq u . \tag{22}$$

In (22) each $\tilde{E}_{\delta,j}$, $1 \leqq j < n_i$, $1 \leqq \delta \leqq u$, is a permutation matrix with the same first row as $P_{i-1}(a_i)$ and each

$$\tilde{E}_{\delta,n_i} , \qquad 1 \leqq \delta \leqq u ,$$

is some unknown permutation matrix.

Now $SQ(g) = Q(g)S$ if $g \in H_{i-1}$ since S is block diagonal with its blocks in $L^*(H_{i-1})$ whereas $Q(g)$ for $g \in H_{i-1}$ is block scalar with its blocks in $R(H_{i-1})$. Thus if we change notation again and replace AS with A and $S'MS$ with M we retain the validity of (13) and (16) and now

$$M = \operatorname{diag}(\tilde{E}_1, \tilde{E}_2, \cdots, \tilde{E}_u)_u . \tag{23}$$

Since for any $g \in H_{i-1}$, $a_i^{-1}ga_i = \bar{g} \in H_{i-1}$, it follows that for any $g \in H_{i-1}$ there exists a $\bar{g} \in H_{i-1}$ such that $Q(g)Q(a_i) = Q(a_1)Q(\bar{g})$. Hence, using (9), (10), and (11), we find

$$P_{i-1}(g)P_{i-1}(a_i) = P_{i-1}(a_i)P_{i-1}(\bar{g}) , \qquad g, \bar{g} \in H_{i-1} . \tag{24}$$

If we let $g \in H_{i-1}$ be such that $P_{i-1}(g)$ has a one at position $(1, \omega)$ then (24) says: row ω of $P_{i-1}(a_i)$ is determined in terms of row one of $P_{i-1}(a_i)$.

Now for $g \in H_{i-1}$:

$$\begin{aligned} Q(g)M &= Q(g)A^{-1}Q(a_i)A \\ &= A^{-1}Q(g)Q(a_i)A && \text{by (13)} , \\ &= A^{-1}Q(a_i)Q(\bar{g})A && \text{since } ga_i = a_i\bar{g} , \\ &= A^{-1}Q(a_i)AQ(\bar{g}) && \text{by (13)} , \\ &= MQ(\bar{g}) . \end{aligned}$$

Hence, for fixed δ and j, $1 \leqq \delta \leqq u$, $1 \leqq j < n_i$, it now follows (using (10), (11), (22), and (23)) that

$$P_{i-1}(g)\widetilde{E}_{\delta,j} = \widetilde{E}_{\delta,j}P_{i-1}(\bar{g}) , \qquad g, \bar{g} \in H_{i-1} . \tag{25}$$

As with (24), (25) determines each row of $\widetilde{E}_{\delta,j}$ in terms of the first row of $\widetilde{E}_{\delta,j}$. Consequently

$$\widetilde{E}_{\delta,j} = P_{i-1}(a_i) , \qquad 1 \leqq \delta \leqq u,\ 1 \leqq j < n_i . \tag{26}$$

We also have (8), hence

$$M^{n_i} = A^{-1}Q(a_i^{n_i})A = Q(a_i)^{n_i}$$

by (13). Hence, for each δ, $1 \leqq \delta \leqq u$,

$$\widetilde{E}_{\delta}^{n_i} = P_i(a_i)^{n_i} . \tag{27}$$

Each side of (27) is a block diagonal matrix. Equating the topmost diagonal blocks we get

$$\left[\prod_{j=1}^{n_i-1}\widetilde{E}_{\delta,j}\right][\pm\widetilde{E}_{\delta,n_i}] = P_{i-1}(a_i)^{n_i-1}\bar{P}_{i-1}(a_i) .$$

Hence, by (26),

$$\pm\widetilde{E}_{\delta,n_i} = \bar{P}_{i-1}(a_i) , \qquad 1 \leqq \delta \leqq u .$$

We have now proved that $M = Q(a_i)$. Hence $Q(a_i)A = AQ(a_i)$. As indicated earlier, this is enough to complete the proof.

References

1. M. Newman and Olga Taussky, *On a generalization of the normal basis in abelian algebraic number fields*, Comm. Pure App. Math., **9** (1956), 85-91.
2. R. C. Thompson, *Normal matrices and the normal basis in abelian number fields*, Pacific J. Math., **12** (1962), 1115-1124.

The University of British Columbia,
Vancouver, Canada