CONCERNING A THEOREM OF L. K. HUA AND I. REINER

PETER STANEK

1. Denote by $\mathrm{Sp}(2n)$ the group of all $2n$ by $2n$ matrices of rational integers which satisfy

$$(1)\quad XHX^T = H, \qquad H = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}, \qquad X^T = X \text{ transpose.}$$

This is the symplectic modular group and in [1] Hua and Reiner show that $\mathrm{Sp}(2n)$ may be generated by two matrices for $n=1$, and by four matrices for $n>1$. In this paper we improve their result and prove

THEOREM. $\mathrm{Sp}(2n)$ *is generated by three matrices for* $n=2$ *and* $n=3$, *and by two matrices for* $n>3$.

2. We define the following types of symplectic matrices:

(i) rotations

$$\begin{pmatrix} A^T & 0 \\ 0 & A^{-1} \end{pmatrix}, \qquad \det A = \pm 1,$$

(ii) translations

$$\begin{pmatrix} I & S \\ 0 & I \end{pmatrix}, \qquad S^T = S,$$

(iii) semi-involutions

$$\begin{pmatrix} Q & I-Q \\ Q-I & Q \end{pmatrix},$$

where Q is a diagonal matrix of zeros and ones. Then [1] $\mathrm{Sp}(2n)$ is generated by the set of rotations, translations, and semi-involutions. Let E_{ij} be the n by n matrix, all zero except for a one in the ijth entry. Let $R_{ij}(x)$ be the rotation, as above, with $A=I+xE_{ji}$, for $i\neq j$; $T_i(x)$ the translation with $S=xE_{ii}$; and $T_{ij}(x)$ the translation with $S=xE_{ij}+xE_{ji}$. Then the T's commute and

$$(2)\quad \begin{aligned} (T_i(x))^{\pm k} &= T_i(\pm kx), \\ (T_{ij}(x))^{\pm k} &= T_{ij}(\pm kx), \qquad k \text{ any integer.} \end{aligned}$$

If we let (U, V) be the commutator, $UVU^{-1}V^{-1}$, then

Received by the editors August 17, 1962.

(3) $$(R_{ij}(x))^{\pm k} = R_{ij}(\pm kx), \qquad k \text{ any integer},$$

(4) $$(R_{ij}(x),\, R_{j\rho}(y)) = R_{i\rho}(xy), \qquad i \neq \rho.$$

Now, for $n>3$, $\mathrm{Sp}(2n)$ is generated by $J=R_{21}(1)T_n(1)$ and D:

$$D = \begin{pmatrix} \sum_{i=1}^{n-1} E_{i,i+1} & -E_{n1} \\ E_{n1} & \sum_{i=1}^{n-1} E_{i,i+1} \end{pmatrix}.$$

We compute

(5) $$(J,\, D^{-1}JD) = R_{31}(-1).$$

For indices i and j, $n \geqq i > j \geqq 1$,

(6) $$D^{-k}R_{ij}(x)D^{k} = R_{i+k,j+k}(x), \qquad 0 \leqq k \leqq n-i;$$

(7) $$D^{-1}R_{n,j+n-i}(x)D = (T_{j+n-i+1,1}(x))^T;$$

(8) $$D^{-k}(T_{j+n-i+1,1}(x))^TD^k = (T_{j+n-i+1+k,1+k}(x))^T, \quad 0 \leqq k \leqq i-1-j;$$

(9) $$D^{-1}(T_{n,i-j}(x))^TD = R_{1,i-j+1}(-x);$$

(10) $$D^{-k}R_{1,i-j+1}(-x)D^k = R_{1+k,i-j+1+k}(-x), \quad 0 \leqq k \leqq n+j-i-1;$$

(11) $$D^{-1}R_{n+j-i,n}(-x)D = T_{n+j-i+1,1}(-x);$$

(12) $$D^{-k}T_{n+j-i+1,1}(-x)D^k = T_{n+j-i+1+k,1+k}(-x), \quad 0 \leqq k \leqq i-j-1;$$

(13) $$D^{-1}T_{n,i-j}(-x)D = R_{i-j+1,1}(x);$$

and

(14) $$D^{1-j}R_{i-j+1,1}(x)D^{j-1} = R_{ij}(x).$$

Hence $R_{13}(1)$ is obtained from D and J.

(15) $$(J,\, R_{13}(1)) = R_{23}(1).$$

Equations (6)–(14) show D and J generate every $R_{i,i+1}(1)$, $R_{i+1,i}(1)$. Repeated use of (3) and (4) will show every $R_{ij}(k)$, $i\neq j$, k any integer is obtained. Hence, the group generated by D and J contains every rotation, as above, with $\det A=1$.

(16) $$JR_{21}(-1) = T_n(1);$$

and

(17) $$D^{n-1}T_n(1)D^{1-n} = T_1(1).$$

(18) $$D^{-1}T_n(1)D = (T_1(-1))^T = P.$$

$$T_1(1)PT_1(1) = \begin{pmatrix} I - E_{11} & E_{11} \\ -E_{11} & I - E_{11} \end{pmatrix} = S_1. \tag{19}$$

But S_1^2 is a rotation with $A = I - 2E_{11}$. Therefore, from D and J any rotation may be had. If we let $S_{i,j,k,\ldots}$ be the semi-involution where Q has zeros in the iith, jjth, kkth, $\cdots$, positions and ones in the other diagonal positions, then

$$(S_{i,j,k,\ldots})(S_{i_1,j_1,k_1,\ldots}) = S_{i,j,k,\ldots,i_1,j_1,k_1,\ldots}. \tag{20}$$

Since

$$D^{-k}S_1D^k = S_{1+k}, \qquad 0 \leqq k \leqq n-1, \tag{21}$$

clearly all semi-involutions are available.

To obtain all translations,

$$D^{-1}R_{1n}(k)D = T_{12}(k). \tag{22}$$

Since

$$\begin{gathered} \begin{pmatrix} I & S \\ 0 & I \end{pmatrix}\begin{pmatrix} I & S^1 \\ 0 & I \end{pmatrix} = \begin{pmatrix} I & S+S^1 \\ 0 & I \end{pmatrix}, \\ \begin{pmatrix} U & 0 \\ 0 & (U^T)^{-1} \end{pmatrix}\begin{pmatrix} I & S \\ 0 & I \end{pmatrix}\begin{pmatrix} U^{-1} & 0 \\ 0 & U^T \end{pmatrix} = \begin{pmatrix} I & USU^T \\ 0 & I \end{pmatrix}, \end{gathered} \tag{23}$$

by simultaneously interchanging rows and corresponding columns of the symmetric matrices kE_{11} and $kE_{12}+kE_{21}$ of $T_1(k)$ and $T_{12}(k)$, respectively, every translation is available. This completes the proof for $n>3$.

3. For $n=2$ or 3, it is now easy to see that the matrices D, $R_{21}(1)$, and $T_1(1)$ will generate $\mathrm{Sp}(2n)$.

Reference

1. L. K. Hua and I. Reiner, *Generation of the symplectic modular group*, Trans. Amer. Math. Soc. **65** (1949), 415–426.

Institute for Defense Analyses