ON THE GENERATORS OF THE SYMPLECTIC MODULAR GROUP

BY
L. K. HUA AND I. REINER

Introduction. Let n be a positive integer. Throughout this paper, unless the contrary is stated, we shall use capital Latin letters to denote n-rowed matrices and capital German letters to denote $2n$-rowed matrices. Furthermore, an r-rowed matrix R will be denoted by $R^{(r)}$. Let

$$\mathfrak{F} = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix},$$

where I and 0 denote the identity and zero matrices respectively. Let Γ be the group of all matrices $\mathfrak{M}$ with rational integral elements which satisfy

$$\mathfrak{M}\mathfrak{F}\mathfrak{M}' = \mathfrak{F}, \tag{1}$$

where $\mathfrak{M}'$ denotes the transpose of $\mathfrak{M}$. Let Γ_0 be the factor group of Γ over its centrum; Γ_0 is called the symplectic modular group. It can be thought of as being obtained from Γ by identifying the elements $\mathfrak{M}$ and $-\mathfrak{M}$. In applications to modular functions of the nth degree[1] and to the projective geometry of matrices[2] it is customary to identify $\mathfrak{M}$ and $-\mathfrak{M}$ as a single transformation. For this reason we have considered Γ_0 rather than Γ; it might be pointed out, however, that the generators of Γ_0 obtained in this paper happen to be a set of generators of Γ.

It is the aim of this paper to find the generators of the symplectic modular group. It will be proved here that this group is generated by two or four independent elements, according as $n=1$ or $n>1$. The method used here can be extended so as to give a set of generators for matrices with elements in any Euclidean ring. In particular, we give the details for the generalized Picard group at the end of this paper.

Problems of this type have been considered previously. Poincaré[3] stated without proof that every matrix $\mathfrak{M}$ with integral elements for which $\mathfrak{M}\mathfrak{S}\mathfrak{M}' = \mathfrak{S}$, where $\mathfrak{S}$ is the direct sum of n two-rowed skew-symmetric matrices, is expressible as a product of elementary matrices of two simple types. Brahana[4] proved this and extended the result to the case where $\mathfrak{S}$ is any skew-symmetric matrix by showing in this case that every such matrix $\mathfrak{M}$ is ex-

Presented to the Society, February 28, 1948; received by the editors March 6, 1948.

[1] C. L. Siegel, Math. Ann. vol. 116 (1939) pp. 617–657.

[2] L. K. Hua, Trans. Amer. Math. Soc. vol. 57 (1945) pp. 441–490.

[3] H. Poincaré, Rend. Circ. Mat. Palermo vol. 18 (1904) pp. 45–110.

[4] H. R. Brahana, Ann. of Math. (2) vol. 24 (1923) pp. 265–270.

pressible as a product of matrices taken from some finite set of matrices. From the results given in the present paper, a much stronger form of Brahana's result can be easily deduced.

1. If we set

$$\mathfrak{M} = \begin{pmatrix} A & B \\ C & D \end{pmatrix}, \tag{2}$$

(1) is equivalent to

$$AB' = BA', \qquad CD' = DC', \qquad AD' - BC' = I. \tag{3}$$

By taking inverses of both sides of (1) and using $\mathfrak{F}^{-1} = -\mathfrak{F}$, we can deduce that $\mathfrak{M}'\mathfrak{F}\mathfrak{M} = \mathfrak{F}$, so that

$$A'C = C'A, \qquad B'D = D'B, \qquad A'D - C'B = I. \tag{4}$$

We shall begin by showing in §3 that Γ_0 is generated by the following types of elements:

(I) *Translations*:

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

where S is symmetric.

(II) *Rotations*:

$$\mathfrak{R} = \begin{pmatrix} U & 0 \\ 0 & U'^{-1} \end{pmatrix},$$

where U is unimodular, that is, abs $U = 1$ (where abs U denotes the absolute value of the determinant of U).

(III) *Semi-involutions*:

$$\mathfrak{S} = \begin{pmatrix} J & I - J \\ J - I & J \end{pmatrix}$$

where J is a diagonal matrix whose diagonal elements are 0's and 1's, so that $J^2 = J$ and $(I - J)^2 = I - J$.

It is easily verified that matrices of types I, II and III satisfy (1).

2. In this section we prove two lemmas on matrices.

LEMMA 1. *Let m be a nonzero integer, and let T be an n-rowed symmetric matrix at least one of whose elements is not divisible by m. There exists a symmetric matrix S with integral elements such that*

$$0 < \text{abs } (T - mS) < |m|^n. \tag{5}$$

Proof. The lemma is evident for $n = 1$. Consider next $n = 2$; let $T = (t_{ij})$, $S = (s_{ij})$. Then

$$\text{(6)} \qquad \operatorname{abs}(T - mS) = |(t_{11} - ms_{11})(t_{22} - ms_{22}) - (t_{12} - ms_{12})^2|.$$

If m divides both t_{11} and t_{22}, it cannot divide t_{12}; we can then choose S so that $t_{11}-ms_{11}=t_{22}-ms_{22}=0$ and $0<|t_{12}-ms_{12}|<|m|$. Suppose on the other hand that m does not divide one of the diagonal elements, say t_{11}. Fix s_{12} arbitrarily, and choose s_{11} so that $0<|t_{11}-ms_{11}|<|m|$. Since (6) can be written as

$$\operatorname{abs}(T - mS) = |-m(t_{11} - ms_{11})s_{22} + \cdots |,$$

where $\cdots$ represents terms not involving s_{22}, we can choose an integer s_{22} by the Euclidean algorithm so that

$$0 < \operatorname{abs}(T - mS) \leqq |m(t_{11} - ms_{11})| < |m|^2.$$

Suppose now that the result has been established for $n=r-1$ with $r\geqq 3$; we shall deduce it for $n=r$. Let $T=T^{(r)}$ and let some element t_{ij} of T be not divisible by m. Since $r\geqq 3$, there exists a diagonal element t_{kk} of T which is not in the same row or column as t_{ij}. Let T_1 be the symmetric $(r-1)$-rowed matrix obtained from T by omitting the kth row and kth column; let S_1 be similarly related to S. By the induction hypothesis, we may choose S_1 symmetric so that

$$\text{(7)} \qquad 0 < \operatorname{abs}(T_1 - mS_1) < |m|^{r-1}.$$

However, we have

$$\text{(8)} \qquad \operatorname{abs}(T - mS) = |(t_{kk} - ms_{kk}) \det(T_1 - mS_1) + \cdots |,$$

where $\cdots$ represents terms not involving s_{kk}. Choose s_{lk} arbitrarily for $l=1, 2, \cdots, k-1, k+1, \cdots, r$. Then by the Euclidean algorithm we can choose s_{kk} so that

$$0 < \operatorname{abs}(T - mS) \leqq |m| \operatorname{abs}(T_1 - mS_1) < |m|^r.$$

This completes the proof of the lemma.

LEMMA 2. *Let A and B satisfy $AB'=BA'$ and let* $\det A\neq 0$. *There exists a symmetric matrix S such that either*

$$\text{(9)} \qquad B - AS = 0$$

or

$$\text{(10)} \qquad 0 < \operatorname{abs}(B - AS) < \operatorname{abs} A.$$

Proof. From $AB'=BA'$ and $\det A\neq 0$, we may deduce that A^*B is symmetric, where A^* denotes the adjoint of A. We apply Lemma 1 with $T=A^*B$ and $m=\det A$. Either every element of A^*B is divisible by m, in which case there exists a symmetric matrix S with $A^*B=mS$, or else there exist symmetric matrices R and S such that $A^*B=mS+R$ with $0<\operatorname{abs} R<|m|^n$. In virtue of the relation $A^*A=mI$, these alternatives become: either $B=AS$ (in which case (9) holds), or $B-AS=AR/m$; however,

$$\text{abs}\,\frac{AR}{m}=\frac{(\text{abs}\,A)(\text{abs}\,R)}{|m|^n}=\frac{\text{abs}\,R}{|m|^{n-1}},$$

so that

$$0<\text{abs}\,(B-AS)<|m|=\text{abs}\,A.$$

3. We are now ready to show that Γ_0 is generated by matrices of types I, II and III. Let $\mathfrak{M}$ given by (2) be an arbitrary element of Γ_0. It suffices to prove that by multiplying $\mathfrak{M}$ by matrices of types I, II and III, one obtains a product of matrices of those types.

(3) implies that not both A and B are 0. Since

$$\begin{pmatrix}A & B\\ C & D\end{pmatrix}\begin{pmatrix}0 & I\\ -I & 0\end{pmatrix}=\begin{pmatrix}-B & A\\ * & *\end{pmatrix},$$

we may assume that A has rank $r>0$. Furthermore,

$$\begin{pmatrix}U & 0\\ 0 & U'^{-1}\end{pmatrix}\begin{pmatrix}A & B\\ C & D\end{pmatrix}\begin{pmatrix}V & 0\\ 0 & V'^{-1}\end{pmatrix}=\begin{pmatrix}UAV & *\\ * & *\end{pmatrix},$$

so that A may be taken to be of the form

$$A=\begin{pmatrix}A_1 & 0\\ A_2 & 0\end{pmatrix}, \tag{11}$$

where A_1 is an r-rowed nonsingular matrix. We similarly decompose B as

$$B=\begin{pmatrix}B_1^{(r)} & *\\ * & *\end{pmatrix}.$$

From (3) it is easily seen that $A_1B_1'=B_1A_1'$. By Lemma 2, there exists a symmetric matrix S_1 with either $A_1S_1+B_1=0$ or $0<\text{abs}\,R_1<\text{abs}\,A_1$, where $R_1=A_1S_1+B_1$. Define

$$S=\begin{pmatrix}S_1^{(r)} & 0\\ 0 & 0\end{pmatrix}.$$

Then

$$\begin{pmatrix}A & B\\ C & D\end{pmatrix}\begin{pmatrix}I & S\\ 0 & I\end{pmatrix}=\begin{pmatrix}A & AS+B\\ * & *\end{pmatrix}, \tag{12}$$

so that A remains unaltered while B_1 of B is replaced by 0 or R_1. If the second alternative occurs, we proceed as follows: let

$$J = \begin{pmatrix} 0 & 0 \\ 0 & I^{(n-r)} \end{pmatrix}. \tag{13}$$

Then

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} J & I-J \\ J-I & J \end{pmatrix} = \begin{pmatrix} \bar{A} & * \\ * & * \end{pmatrix}, \tag{14}$$

where

$$\bar{A} = AJ - B(I-J) = \begin{pmatrix} -R_1 & 0 \\ * & 0 \end{pmatrix}.$$

We now repeat the process as before, and so on. Since there are only finitely many positive integers less than abs A_1, this process eventually terminates. Thus, by multiplying $\mathfrak{M}$ by matrices of types I, II and III one arrives at a matrix

$$\begin{pmatrix} A_0 & B_0 \\ * & * \end{pmatrix}$$

with

$$A_0 = \begin{pmatrix} R & 0 \\ * & 0 \end{pmatrix}, \qquad B_0 = \begin{pmatrix} 0 & * \\ * & * \end{pmatrix}$$

and det $R \neq 0$. One readily deduces from $A_0B_0' = B_0A_0'$ that B_0 must be of the form

$$B_0 = \begin{pmatrix} 0 & * \\ 0 & * \end{pmatrix}.$$

But then

$$\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}\begin{pmatrix} A_0 & B_0 \\ C_0 & D_0 \end{pmatrix}\begin{pmatrix} J & I-J \\ J-I & J \end{pmatrix} = \begin{pmatrix} A^+ & B^+ \\ 0 & D^+ \end{pmatrix}$$

where J is given by (13). Finally we notice that for a matrix

$$\begin{pmatrix} A & B \\ 0 & D \end{pmatrix}$$

of Γ_0, we must have $A = U$ unimodular, $D = U'^{-1}$, and thence from (3), $B = SU'^{-1}$ with symmetric S. Therefore

$$\begin{pmatrix} A & B \\ 0 & D \end{pmatrix} = \begin{pmatrix} I & S \\ 0 & I \end{pmatrix}\begin{pmatrix} U & 0 \\ 0 & U'^{-1} \end{pmatrix}.$$

This completes the proof that Γ_0 is generated by the matrices of types I, II and III.

4. The set of matrices of types I, II and III which generate Γ_0 are certainly not independent generators. Let us reduce the number of generators as much as possible. Since

$$\begin{pmatrix} I & S_1 \\ 0 & I \end{pmatrix}\begin{pmatrix} I & S_2 \\ 0 & I \end{pmatrix} = \begin{pmatrix} I & S_1 + S_2 \\ 0 & I \end{pmatrix},$$

the subgroup formed by matrices of type I is generated by those type I matrices whose S's are given by

$$(15) \qquad S_0 = \begin{bmatrix} 1 & 0 \cdots 0 \\ 0 & 0 \cdots 0 \\ \cdot & \cdot\ \cdot\ \cdot\ \cdot \\ 0 & 0 \cdots 0 \end{bmatrix}, \qquad S_1 = \begin{bmatrix} 0 & 1 & 0 \cdots 0 \\ 1 & 0 & 0 \cdots 0 \\ 0 & 0 & 0 \cdots 0 \\ \cdot & \cdot & \cdot\ \cdot\ \cdot\ \cdot \\ 0 & 0 & 0 \cdots 0 \end{bmatrix}$$

and all matrices obtained from these by interchanging any two rows and the corresponding columns. Next we note that

$$\begin{pmatrix} U & 0 \\ 0 & U'^{-1} \end{pmatrix}\begin{pmatrix} I & S \\ 0 & I \end{pmatrix}\begin{pmatrix} U^{-1} & 0 \\ 0 & U' \end{pmatrix} = \begin{pmatrix} I & USU' \\ 0 & I \end{pmatrix},$$

so that the group generated by matrices of types I and II is the same as that generated by all type II matrices and the two translations whose S's are given by (15). However, we have

$$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Hence the translation with S_1 is obtainable from that with S_0 and the matrices of type II. Therefore Γ_0 is generated by the matrix

$$(16) \qquad \mathfrak{T}_0 = \begin{pmatrix} I & S_0 \\ 0 & I \end{pmatrix}$$

with S_0 given by (15), and all matrices of types II and III.

Since

$$\begin{pmatrix} U & 0 \\ 0 & U'^{-1} \end{pmatrix}\begin{pmatrix} V & 0 \\ 0 & V'^{-1} \end{pmatrix} = \begin{pmatrix} UV & 0 \\ 0 & (UV)'^{-1} \end{pmatrix},$$

in order to find the generators of the subgroup of rotations we have merely to find the generators of the group of unimodular matrices. These are given by the following theorem.

THEOREM 1. *Let $n \geqq 2$. Every unimodular matrix with rational integral elements is a product of the matrices U_1, U_2, U_3 and their inverses, where*

$$(17)\qquad U_1 = \begin{pmatrix} 0 & 0 \cdots 0 & 1 \\ 1 & 0 \cdots 0 & 0 \\ \cdot & \cdot\ \cdot\ \cdot\ \cdot & \cdot \\ 0 & 0 \cdots 0 & 0 \\ 0 & 0 \cdots 1 & 0 \end{pmatrix}, \qquad U_2 = \begin{pmatrix} 1 & 1 \cdots 0 & 0 \\ 0 & 1 \cdots 0 & 0 \\ \cdot & \cdot\ \cdot\ \cdot\ \cdot & \cdot \\ 0 & 0 \cdots 1 & 0 \\ 0 & 0 \cdots 0 & 1 \end{pmatrix},$$

$$U_3 = \begin{pmatrix} -1 & 0 \cdots 0 & 0 \\ 0 & 1 \cdots 0 & 0 \\ \cdot & \cdot\ \cdot\ \cdot\ \cdot & \cdot \\ 0 & 0 \cdots 1 & 0 \\ 0 & 0 \cdots 0 & 1 \end{pmatrix}.$$

Proof. It is known[5] that every unimodular matrix is a product of U_1, U_2, U_3, and

$$U_4 = = \begin{pmatrix} 0 & 1 \cdots 0 & 0 \\ 1 & 0 \cdots 0 & 0 \\ \cdot & \cdot\ \cdot\ \cdot\ \cdot & \cdot \\ 0 & 0 \cdots 1 & 0 \\ 0 & 0 \cdots 0 & 1 \end{pmatrix},$$

and their inverses. It is sufficient to show that U_4 is expressible as a product of U_1, U_2, U_3 and their inverses. We define $T = U_2 U_1$ for the remainder of this proof, and let $\mathfrak{r} = (r_1, \cdots, r_n)'$ be a column vector. Then

$$T\mathfrak{r} = \begin{pmatrix} r_n + r_1 \\ r_1 \\ \cdot \\ \cdot \\ \cdot \\ r_{n-1} \end{pmatrix},$$

$$T^2\mathfrak{r} = \begin{pmatrix} r_{n-1} + r_n + r_1 \\ r_n + r_1 \\ r_1 \\ \cdot \\ \cdot \\ \cdot \\ r_{n-2} \end{pmatrix}, \cdots, T^{n-1}\mathfrak{r} = \begin{pmatrix} r_2 + r_3 + \cdots + r_n + r_1 \\ r_3 + \cdots + r_n + r_1 \\ \cdot \\ \cdot \\ \cdot \\ r_n + r_1 \\ r_1 \end{pmatrix}.$$

[5] See for example, C. C. MacDuffee, *The theory of matrices*, Berlin, 1933, p. 34, Theorem 22.5.

Therefore

$$U_1^{-1}T^{n-1}\mathfrak{r} = \begin{pmatrix} r_3 + \cdots + r_n + r_1 \\ \vdots \\ r_n + r_1 \\ r_1 \\ r_2 + r_3 + \cdots + r_n + r_1 \end{pmatrix},$$

so that

$$(T^{-1})^{n-2}U_1^{-1}T^{n-1}\mathfrak{r} = \begin{pmatrix} r_1 \\ r_2 + \cdots + r_n + r_1 \\ r_3 \\ \vdots \\ r_n \end{pmatrix},$$

$$U_1(T^{-1})^{n-2}U_1^{-1}T^{n-1}\mathfrak{r} = \begin{pmatrix} r_n \\ r_1 \\ r_2 + \cdots + r_n + r_1 \\ r_3 \\ \vdots \\ r_{n-1} \end{pmatrix}.$$

From this we see that

$$T^{n-3}U_1(T^{-1})^{n-2}U_1^{-1}T^{n-1}\mathfrak{r} = \begin{pmatrix} r_3 + r_4 + \cdots + r_n \\ r_4 + \cdots + r_n \\ \vdots \\ r_n \\ r_1 \\ r_2 + \cdots + r_n + r_1 \end{pmatrix}$$

and

$$(T^{-1})^{n-2}U_1T^{n-3}U_1(T^{-1})^{n-2}U_1^{-1}T^{n-1}\mathfrak{r} = \begin{pmatrix} r_n \\ r_1 \\ r_2 + r_1 \\ \vdots \\ r_{n-1} \end{pmatrix}.$$

Define

$$U\dagger = U_1^{-1}(T^{-1})^{n-2}U_1T^{n-3}U_1(T^{-1})^{n-2}U_1^{-1}T^{n-1}.$$

Then

$$U\dagger = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \dotplus I^{(n-2)},$$

where $\dotplus$ denotes the direct sum of matrices. But from

$$U_3 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \dotplus I^{(n-2)} \quad \text{and} \quad U_2^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \dotplus I^{(n-2)}$$

we deduce

$$\begin{aligned} U_3U\dagger U_2^{-1}U\dagger &= \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \dotplus I^{(n-2)} \\ &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \dotplus I^{(n-2)} = U_4. \end{aligned}$$

This completes the proof of the theorem.

COROLLARY. *Let $n \geqq 2$. Every unimodular matrix with rational integral elements of determinant $+1$ is a product of powers of U_2 and*

$$U_5 = \begin{bmatrix} 0 \cdots 0 & (-1)^{n-1} \\ 1 \cdots 0 & 0 \\ \cdots\cdots & \cdots \\ 0 \cdots 0 & 0 \\ 0 \cdots 1 & 0 \end{bmatrix}.$$

By Theorem 1 we see now that Γ_0 is generated by $\mathfrak{T}_0$ and the set of all semi-involutions and the three rotations defined by

$$\mathfrak{R}_i = \begin{pmatrix} U_i & 0 \\ 0 & U_i'^{-1} \end{pmatrix}, \qquad i = 1, 2, 3. \tag{18}$$

We finally consider type III matrices. Let J_r be the diagonal matrix obtained from the identity matrix by replacing the rth 1 by 0. In that case, if $r \neq s$, we have

$$\begin{pmatrix} J_r & I - J_r \\ J_r - I & J_r \end{pmatrix}\begin{pmatrix} J_s & I - J_s \\ J_s - I & J_s \end{pmatrix} = \begin{pmatrix} J_{rs} & I - J_{rs} \\ J_{rs} - I & J_{rs} \end{pmatrix},$$

where J_{rs} is obtained from the identity matrix by replacing the rth and sth ones by 0's. Therefore, in order to obtain all type III matrices, we need only those semi-involutions

$$\begin{pmatrix} J_r & I-J_r \\ J_r-I & J_r \end{pmatrix}, \qquad r=1,2,\cdots,n, \tag{19}$$

with J_r defined above. Now, let U be that unimodular matrix obtained from I by interchanging the 1st and rth rows; then we have

$$\begin{pmatrix} U & 0 \\ 0 & U'^{-1} \end{pmatrix}\begin{pmatrix} J_r & I-J_r \\ J_r-I & J_r \end{pmatrix}\begin{pmatrix} U^{-1} & 0 \\ 0 & U' \end{pmatrix}=\begin{pmatrix} J_1 & I-J_1 \\ J_1-I & J_1 \end{pmatrix}.$$

Therefore Γ_0 is generated by the matrices $\mathfrak{T}_0$, $\mathfrak{R}_i$ $(i=1, 2, 3)$ and the matrix

$$\mathfrak{S}_0=\begin{pmatrix} J_1 & I-J_1 \\ J_1-I & J_1 \end{pmatrix}, \tag{20}$$

with J, previously defined. But

$$\mathfrak{S}_0^2=\mathfrak{R}_3,$$

so that $\mathfrak{R}_3$ may be dropped from the list of generators. Therefore we have the following theorem.

THEOREM 2. *Γ_0 is generated by the four matrices $\mathfrak{T}_0$, $\mathfrak{R}_1$, $\mathfrak{R}_2$ and $\mathfrak{S}_0$ given by* (15), (18) *and* (20), *for $n>1$. For $n=1$, Γ_0 is generated by $\mathfrak{T}_0$ and $\mathfrak{S}_0$.*

5. In this section we shall prove the independence of the generators given in Theorem 2. For $n=1$, this is trivial because $\mathfrak{S}_0$ is of finite order while $\mathfrak{T}_0$ is not. Hereafter we suppose that $n>1$.

(1) *Independence of* $\mathfrak{T}_0$. We consider the transformation

$$(X_1, Y_1)=(X, Y)\mathfrak{M}; \tag{21}$$

if XY' is symmetric, it is easily verified that X_1Y_1' is also symmetric. We shall show that if the diagonal elements of XY' are even, those of X_1Y_1' will also be even if $\mathfrak{M}$ is $\mathfrak{R}_1$, $\mathfrak{R}_2$ or $\mathfrak{S}_0$, while if $\mathfrak{M}=\mathfrak{T}_0$, it is possible to choose X and Y so that some diagonal element of X_1Y_1' is odd. This will show that $\mathfrak{T}_0$ is not expressible as a product of $\mathfrak{R}_1$, $\mathfrak{R}_2$ and $\mathfrak{S}_0$ and their inverses.

Assume now that the diagonal elements of XY' are even. From (21) one readily deduces that if $\mathfrak{M}$ is a rotation, $X_1Y_1'=XY'$, so that the diagonal elements of X_1Y_1' are also even. If secondly $\mathfrak{M}$ is a semi-involution, we have

$$X_1=XJ+Y(I-J), \qquad Y_1=-X(I-J)+YJ,$$

so that

$$X_1Y_1'=XJY'-Y(I-J)X'=XJY'+YJX'-YX'.$$

Since XJY' is the transpose of YJX', it is again clear that the diagonal elements of X_1Y_1' are even. Finally, suppose $\mathfrak{M}=\mathfrak{T}_0$. Then we obtain

$$X_1Y_1' = X(XS_0+Y)' = XY' + XS_0X'$$

and for $X=I$ the first diagonal element of X_1Y_1' is odd. This completes the proof of the independence of $\mathfrak{T}_0$. We may remark in passing, however, that $\mathfrak{T}_0^2$ is expressible as a product of the powers of $\mathfrak{R}_1$, $\mathfrak{R}_2$ and $\mathfrak{S}_0$.

(2) *Independence of* $\mathfrak{R}_1$. Let $\mathfrak{r}=(r_1, \cdots, r_n, s_1, \cdots, s_n)'$ be a column vector with $2n$ components. It is clear that the second component r_2 is unaffected when $\mathfrak{r}$ is multiplied on the left by any of the matrices $\mathfrak{T}_0$, $\mathfrak{R}_2$, and $\mathfrak{S}_0$ and their inverses. Under multiplication on the left by $\mathfrak{R}_1$, however, r_2 is replaced by r_1. Hence $\mathfrak{R}_1$ cannot be expressed as a product of $\mathfrak{T}_0$, $\mathfrak{R}_2$ and $\mathfrak{S}_0$ and their inverses.

(3) *Independence of* $\mathfrak{R}_2$. Multiplying $\mathfrak{r}$ on the left by $\mathfrak{R}_1$ or $\mathfrak{S}_0$ or their inverses permutes components of $\mathfrak{r}$; under any such permutation, however, any r_i and its corresponding s_i remain n components apart. Since the effect of multiplying on the left by $\mathfrak{T}_0$ is to replace r_1 by r_1+s_1, it is clear that by multiplying $\mathfrak{r}$ on the left by a product of $\mathfrak{R}_1$, $\mathfrak{S}_0$ and $\mathfrak{T}_0$ and their inverses, r_1 may be replaced by a linear combination of r_1 and s_1 and its position may be changed. It is however impossible to replace r_1 by r_1+r_2 in this way, and this is exactly the effect of multiplication of $\mathfrak{r}$ on the left by $\mathfrak{R}_2$. This proves the independence of $\mathfrak{R}_2$.

(4) *Independence of* $\mathfrak{S}_0$. We note that

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\begin{pmatrix} * & * \\ 0 & * \end{pmatrix} = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}.$$

Since $\mathfrak{T}_0$, $\mathfrak{R}_1$ and $\mathfrak{R}_2$ and their inverses are all of the form

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$$

and $\mathfrak{S}_0$ is not of this form, it is clear that $\mathfrak{S}_0$ is not expressible as a product of $\mathfrak{T}_0$, $\mathfrak{R}_1$ and $\mathfrak{R}_2$ and their inverses.

6. Our previous method can be extended to any Euclidean ring; in particular, for the ring formed by the Gaussian integers, we have the following result:

THEOREM 3. *Let* Γ' *be the group of matrices* $\mathfrak{M}$ *with Gaussian integers as elements which satisfy* (1). *Let* Γ_0' *be obtained from* Γ' *by identifying the four elements* $\pm\mathfrak{M}$ *and* $\pm i\mathfrak{M}$. *Then for* $n>1$, Γ_0' *is generated by the matrices* $\mathfrak{T}_0$, $\mathfrak{R}_1$, $\mathfrak{R}_2$ *and* $\mathfrak{S}_0$ *defined previously, and the matrix*

$$\mathfrak{T}_1 = \begin{pmatrix} I & S_1 \\ 0 & I \end{pmatrix} \qquad \textit{where } S_1 = iS_0. \tag{22}$$

For $n=1$, Γ_0' *is generated by* $\mathfrak{T}_0$, $\mathfrak{T}_1$ *and* $\mathfrak{S}_0$.

The independence of the generators is shown as follows (with suitable modifications when $n=1$):

(1) *Independence of* $\mathfrak{T}_0$. We use the method of §5, (1). Let XY' be a symmetric matrix with Gaussian integers as elements, such that the real part of each diagonal element is even. This property is preserved when (X, Y) is subjected to the transformations $\mathfrak{T}_1$, $\mathfrak{R}_1$, $\mathfrak{R}_2$ and $\mathfrak{S}_0$ according to (21), but not for the transformation $\mathfrak{T}_0$.

(2) *Independence of* $\mathfrak{T}_1$. This is clear since $\mathfrak{T}_1$ is the only generator which is not real.

(3) The independence of $\mathfrak{R}_1$, $\mathfrak{R}_2$ and $\mathfrak{S}_0$ follow exactly as before.

TSING HUA UNIVERSITY,
PEIPING, CHINA.
INSTITUTE FOR ADVANCED STUDY,
PRINCETON, N. J.