TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 186, December 1973

SYMMETRIC COMPLETIONS AND PRODUCTS OF SYMMETRIC MATRICES

BY

MORRIS NEWMAN

ABSTRACT. We show that any vector of n relatively prime coordinates from a principal ideal ring R may be completed to a symmetric matrix of $\mathrm{SL}(n, R)$, provided that $n \geq 4$. The result is also true for $n = 3$ if R is the ring of integers Z. This implies for example that if F is a field, any matrix of $\mathrm{SL}(n, F)$ is the product of a fixed number of symmetric matrices of $\mathrm{SL}(n, F)$ except when $n = 2$, $F = \mathrm{GF}(3)$, which is a genuine exception.

Introduction. It is known that any matrix over a field may be expressed as the product of two symmetric matrices over that field (see [1], [3]). This classical result has been taken up again by O. Taussky (see [4], [5]) who considered the problem of factoring an integral matrix into the product of two integral symmetric matrices, and showed among other things that such a factorization is not always possible; for example the matrix $\left[\begin{smallmatrix} -8 & 3 \\ 5 & 8 \end{smallmatrix}\right]$ is not the product of two integral symmetric matrices. An interesting problem is to determine whether some result of this kind remains true when the matrices are restricted to lie in $\mathrm{SL}(n, R)$, where R is a principal ideal ring. We prove for example that if F is a field, then any matrix of $\mathrm{SL}(n, F)$ is the product of a fixed number of symmetric matrices of $\mathrm{SL}(n, F)$, except when $n = 2$, $F = \mathrm{GF}(3)$. This case is a genuine exception: there are matrices of $\mathrm{SL}(2, \mathrm{GF}(3))$ which are *not* expressible as the product of finitely many symmetric matrices of $\mathrm{SL}(2, \mathrm{GF}(3))$.

This paper is in two sections. In the first, we derive a number of results on completing rectangular arrays over R to unimodular symmetric matrices over R. In the second, we use these results to derive theorems of the type quoted above on factorization of matrices into products of symmetric matrices. The results of the first section are analogous to the classical ones on completion of rectangular arrays to unimodular matrices, but are naturally more difficult because of the added requirement of symmetry. These results should be useful in other applications. The results of the second section suggest some interesting open problems, which are discussed at the end of the paper.

Received by the editors March 2, 1973.

AMS (MOS) subject classifications (1970). Primary 15A36, 15A21.

Key words and phrases. Principal ideal rings, fields, symmetric matrices, unimodular matrices, symmetric completion.

For a general reference on matrices over R see [1] or [2].

Symmetric completions. The first (and most important) result of this section is the following:

Theorem 1. *Let R be a principal ideal ring. Let $a_1, a_2, \cdots, a_n$ be elements of R such that $(a_1, a_2, \cdots, a_n) = 1$, and suppose that $n \geq 4$. Then there is a symmetric matrix $A \in \mathrm{SL}(n, R)$ with first row $(a_1, a_2, \cdots, a_n)$.*

Proof. By the theorem of the Smith normal form, a matrix $U \in \mathrm{SL}(n-1, R)$ may be determined such that $(a_2, a_3, \cdots, a_n) = (b, 0, \cdots, 0)U$, where $b \in R$ and $(a_1, b) = 1$. Put $M = (1) \dotplus U \in \mathrm{SL}(n, R)$. Suppose there is a symmetric matrix $B \in \mathrm{SL}(n, R)$ such that the first row of B is $(a_1, b, 0, \cdots, 0)$. Put

$$A = M^T B M.$$

Then A is also symmetric and belongs to $\mathrm{SL}(n, R)$. Furthermore, the first row of A is $(a_1, a_2, \cdots, a_n)$. It is sufficient therefore to take $(a_1, a_2, \cdots, a_n) = (a, b, 0, \cdots, 0)$, where $(a, b) = 1$, and to show that $(a, b, 0, 0)$ may be completed to a symmetric matrix of $\mathrm{SL}(4, R)$.

Determine a', b' so that $aa' + bb' = 1$. Then it is readily verified that the matrix

$$A = \begin{bmatrix} a & b & 0 & 0 \\ b & 0 & 1 & 0 \\ 0 & 1 & 0 & b' \\ 0 & 0 & b' & -a'(bb'+1) \end{bmatrix}$$

is symmetric and belongs to $\mathrm{SL}(4, R)$. This completes the proof.

The case $n = 2$ is a genuine exception, since (a, b) may be completed to a symmetric matrix of $\mathrm{SL}(2, R)$ if and only if $b^2 + 1 \equiv 0 \bmod a$. For $n = 3$, however, the theorem remains true when R is taken to be the ring of integers Z. Whether the theorem still holds in this case for an arbitrary principal ideal ring R is an open question.

We now prove

Theorem 2. *Suppose that a, b are arbitrary relatively prime integers. Then the row $(a, b, 0)$ may always be completed to a symmetric matrix of* $\mathrm{SL}(3, Z)$.

Proof. Suppose first that $a = 0$. Then $b = \pm 1$, and

$$\begin{bmatrix} 0 & b & 0 \\ b & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

is the desired completion.

Now suppose that $a \neq 0$. Put

$$A = \begin{bmatrix} a & b & 0 \\ b & x & y \\ 0 & y & z \end{bmatrix}, \qquad x, y, z \text{ integers.}$$

Then $A \in \mathrm{SL}(3, Z)$ if and only if

$$(ax - b^2)z = ay^2 + 1. \tag{1}$$

The discussion proceeds by cases. Suppose first that $a > 0$.

I. $a \equiv 1 \bmod 4$. Choose $x \equiv b^2 + 1 \bmod 4$, so that $x = 4w + b^2 + 1$: Then

$$ax - b^2 = 4aw + (a-1)b^2 + a.$$

By Dirichlet's theorem, w may be determined so that

$$p = ax - b^2 = 4aw + (a-1)b^2 + a$$

is prime, since $(4a, (a-1)b^2 + a) = 1$. Furthermore, $p \equiv 1 \bmod 4$.

Now

$$(-a/p) = (a/p) = (p/a) = (-1/a) = 1,$$

since $p \equiv a \equiv 1 \bmod 4$, $p \equiv -b^2 \bmod a$. (Here and in what follows (a/p) is the Legendre-Jacobi symbol.) It follows that y may be chosen so that (1) has a solution.

II. $a \equiv 3 \bmod 4$. Put $x = -t$, $z = -w$. Then (1) becomes

$$(at + b^2)w = ay^2 + 1. \tag{2}$$

As in case I, determine t so that $p = at + b^2$ is prime. Then $(-a/p) = (p/a) = 1$, since $a \equiv 3 \bmod 4$, $p \equiv b^2 \bmod a$. It follows that y may be chosen so that (2) has a solution, and hence so that (1) has a solution.

III. a *even*. Then b must be odd. Take $t = 4w$ in (2) and choose w so that $p = at + b^2 = 4aw + b^2$ is prime. Then $p \equiv 1 \bmod 8$. Put $a = 2^e n$, n odd. Then

$$(-a/p) = (a/p) = (2^e n/p) = (n/p) = (p/n) = 1,$$

since $p \equiv 1 \bmod 8$, $p \equiv b^2 \bmod n$. It follows as before that (1) has a solution here also.

Now suppose that $a < 0$. Put $a = -c$, $c > 0$. Then (1) becomes

$$(cx + b^2)z = cy^2 - 1. \tag{3}$$

IV. c *odd*. Choose $x \equiv c(1 - b^2) \bmod 4$, $x = 4w + c(1 - b^2)$. Then

$$cx + b^2 = 4cw + c^2(1 - b^2) + b^2.$$

Choose w so that $p = cx + b^2 = 4cw + c^2(1-b^2) + b^2$ is prime. Furthermore, $p \equiv 1 \bmod 4$. Then

$$(c/p) = (p/c) = 1,$$

since $p \equiv 1 \bmod 4$, $p \equiv b^2 \bmod c$. It follows that (3), and hence (1), has a solution.

V. *c even.* Then b is odd. Take $x = 4w$, and determine w so that $p = cx + b^2 = 4cw + b^2$ is prime. Then $p \equiv 1 \bmod 8$. Put $c = 2^e n$, n odd. Then

$$(c/p) = (2^e n/p) = (n/p) = (p/n) = 1,$$

since $p \equiv 1 \bmod 8$, $p \equiv b^2 \bmod n$. Thus (3), and hence (1), has a solution.

This completes the proof.

When $R = F$, a field, the situation is naturally simpler. In fact it is easy to prove

Theorem 3. *Let A be a symmetric $p \times p$ matrix over F, B a $p \times q$ matrix over F. Suppose that the rank of B is p, and that $p < q$. Then a symmetric $q \times q$ matrix C over F may be determined so that*

$$M = \begin{bmatrix} A & B \\ B^T & C \end{bmatrix} \in \mathrm{SL}(n, F), \qquad n = p + q.$$

Proof. Let $U \in \mathrm{SL}(p, F)$, $V \in \mathrm{SL}(q, F)$ be such that $UBV = (D\ \ 0)$, where D is a $p \times p$ matrix. Since B is of rank p, D is nonsingular. Put

$$N = \begin{bmatrix} U & 0 \\ 0 & V^T \end{bmatrix} M \begin{bmatrix} U^T & 0 \\ 0 & V \end{bmatrix} = \begin{bmatrix} UAU^T & UBV \\ V^TB^TU^T & V^TCV \end{bmatrix}.$$

Then $M \in \mathrm{SL}(n, F)$ if and only if $N \in \mathrm{SL}(n, F)$, and so it suffices to choose B in the normal form given above; namely, $B = (D\ \ 0)$. Now put $C = \left[\begin{smallmatrix} 0 & 0 \\ 0 & W \end{smallmatrix}\right]$, where W is $(q-p) \times (q-p)$ and so is nonvacuous since $q > p$. Then

$$M = \begin{bmatrix} A & D & 0 \\ D^T & 0 & 0 \\ 0 & 0 & W \end{bmatrix},$$

$$\det M = \det \begin{bmatrix} A & D \\ D^T & 0 \end{bmatrix} \det W = \pm \det W (\det D)^2.$$

Thus to make $\det M = 1$, it suffices to choose

$$W = (\pm (\det D)^{-2}) \dotplus I_{q-p-1}.$$

This completes the proof.

Products of symmetric matrices. We now consider the problem of expressing a matrix as the product of symmetric matrices. We first prove

Theorem 4. *Let R be a euclidean ring, and suppose that $n > 2$. Then* SL(n, R) *may be generated by symmetric matrices. Thus every matrix of* SL(n, R) *is the product of finitely many symmetric matrices belonging to* SL(n, R).

Proof. It is known (see [2]) that SL(n, R) may be generated by the matrices

$$S(\mu) = \begin{bmatrix} 1 & \mu \\ 0 & 1 \end{bmatrix} \dotplus I_{n-2}, \qquad \mu \in R,$$

and

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

We note first that

$$\begin{bmatrix} 1 & \mu & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 1 & \mu-1 & 0 \\ 0 & 0 & -1 \end{bmatrix},$$

which implies that $S(\mu)$ is the product of 2 symmetric matrices of SL(n, R), provided that $n \geq 3$.

Next, we show by induction that, for $n \geq 3$, P_n is the product of $2n - 4$ symmetric matrices of SL(n, R). For $n = 3$, we have

$$P_3 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix},$$

so that P_3 is indeed the product of $2 \cdot 3 - 4 = 2$ symmetric matrices of SL$(3, R)$. Now suppose that for $n - 1 \geq 3$ we have shown that P_{n-1} is the product of $2(n-1) - 4 = 2n - 6$ symmetric matrices of SL$(n-1, R)$. Then certainly $(1) \dotplus P_{n-1}$ is the product of $2n - 6$ symmetric matrices of SL(n, R).

Furthermore, $P_n = \{(1) \dotplus P_{n-1}\}T$, where $T = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] + I_{n-2}$; and

$$T = \left\{\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix} \dotplus I_{n-3}\right\} \left\{\begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix} \dotplus I_{n-3}\right\}$$

is the product of 2 symmetric matrices of $\mathrm{SL}(n, R)$. We conclude by the induction hypothesis that P_n is the product of $2n - 6 + 2 = 2n - 4$ symmetric matrices of $\mathrm{SL}(n, R)$. The induction is thus complete, and we have shown that we may select a symmetric set of generators of $\mathrm{SL}(n, R)$. This completes the proof.

An appropriate remark at this point is the following: Let G be any matrix group which is closed under transposition, G^* the subgroup of G generated by the symmetric matrices of G. Then G^* is a normal subgroup of G. For if A is any element of G, then G^* is generated by the symmetric matrices S of G, and $A^{-1}G^*A$ is generated by the matrices $A^{-1}SA$, S symmetric. We have

$$A^{-1}SA = (A^TA)^{-1}(A^TSA) \in G^*,$$

$$S = A^{-1}\{(ASA^T)(AA^T)^{-1}\}A \in A^{-1}G^*A,$$

which implies that $A^{-1}G^*A = G^*$.

We now show

Theorem 5. *Let R be a principal ideal ring and suppose that $n > 3$. If every element of* $\mathrm{SL}(n-1, R)$ *is the product of at most k symmetric matrices of* $\mathrm{SL}(n-1, R)$, *then every element of* $\mathrm{SL}(n, R)$ *is the product of at most $k + 3$ symmetric matrices of* $\mathrm{SL}(n, R)$.

Proof. Let A be any element of $\mathrm{SL}(n, R)$ and put $A^{-1} = B = (b_{ij}) \in \mathrm{SL}(n, R)$. By Theorem 1, there is a symmetric matrix $S \in \mathrm{SL}(n, R)$ whose first row is $(b_{11}, b_{12}, \cdots, b_{1n})$. Then

$$SA = \begin{bmatrix} 1 & 0 \\ \beta & A_1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ \beta & I \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & A_1 \end{bmatrix},$$

where $A_1 \in \mathrm{SL}(n-1, R)$.

Suppose now that $\beta \neq 0$. Then we may write $\beta = b\gamma$, where γ has relatively prime entries. By Theorem 1 there is a symmetric matrix

$$M = \begin{bmatrix} 0 & \gamma^T \\ \gamma & N \end{bmatrix}$$

such that $M \in \mathrm{SL}(n, R)$. Furthermore,

$$\begin{bmatrix} 1 & 0 \\ \beta & I \end{bmatrix} M = \begin{bmatrix} 1 & 0 \\ b\gamma & I \end{bmatrix} \begin{bmatrix} 0 & \gamma^T \\ \gamma & N \end{bmatrix} = \begin{bmatrix} 0 & \gamma^T \\ \gamma & b\gamma\gamma^T + N \end{bmatrix}$$

which is symmetric. It follows that $\left[\begin{smallmatrix} 1 & 0 \\ \beta & I \end{smallmatrix}\right]$ is the product of at most 3 symmetric matrices of $\mathrm{SL}(n, R)$. Thus if $A_1 \in \mathrm{SL}(n-1, R)$ is the product of at most k

symmetric matrices of SL$(n-1, R)$, then $\left[\begin{smallmatrix}1 & 0\\ 0 & A_1\end{smallmatrix}\right]$ is the product of at most k symmetric matrices of SL(n, R), and A is the product of at most $k+3$ symmetric matrices of SL(n, R). This completes the proof.

When $R = Z$, the restriction that $n > 3$ may be replaced by $n > 2$, by virtue of Theorem 2.

As a corollary, we have

Corollary 1. *Suppose that every matrix of* SL$(3, R)$ *is the product of at most* k *symmetric matrices of* SL$(3, R)$*. Then every matrix of* SL(n, R) *is the product of at most* $3n + k - 9$ *symmetric matrices of* SL(n, R)*, where* $n \geq 3$.

Let $A \in$ SL$(3, F)$, where F is any field. Put $A^{-1} = B = (b_{ij}) \in$ SL$(3, F)$. By Theorem 3, there is a symmetric matrix $S \in$ SL$(3, F)$ whose first row is (b_{11}, b_{12}, b_{13}). Then as in the proof of Theorem 5 we have that

$$SA = \begin{bmatrix}1 & 0\\ \beta & I\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & C\end{bmatrix},$$

where $C \in$ SL$(2, F)$. Again as in the proof of Theorem 5, but using Theorem 3 instead of Theorem 1, we may conclude that $\left[\begin{smallmatrix}1 & 0\\ \beta & I\end{smallmatrix}\right]$ is the product of at most 2 symmetric matrices of SL$(3, F)$. Thus we need only consider $\left[\begin{smallmatrix}1 & 0\\ 0 & C\end{smallmatrix}\right]$.

Put

$$C = \begin{bmatrix}a & b\\ c & d\end{bmatrix} \in \mathrm{SL}\,(2, F).$$

If $c = 0$,

$$C = \begin{bmatrix}a & b\\ 0 & 1/a\end{bmatrix} = \begin{bmatrix}a & 0\\ 0 & 1/a\end{bmatrix}\begin{bmatrix}1 & b_1\\ 0 & 1\end{bmatrix}, \qquad b_1 \in F.$$

If $c \neq 0$,

$$C = \begin{bmatrix}\alpha & 1\\ 1 & 2/\alpha\end{bmatrix}\begin{bmatrix}a_1 & 0\\ 0 & 1/a_1\end{bmatrix}\begin{bmatrix}1 & b_1\\ 0 & 1\end{bmatrix}, \qquad \alpha = a/c,\ a_1,\ b_1 \in F.$$

Hence we may confine our attention to $\left[\begin{smallmatrix}1 & b\\ 0 & 1\end{smallmatrix}\right]$, $b \in F$.

We have the identity

$$\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & b\\ 0 & 0 & 1\end{bmatrix} = \begin{bmatrix}-1 & 0 & 0\\ 0 & 1 & 1\\ 0 & 1 & 0\end{bmatrix}\begin{bmatrix}-1 & 0 & 0\\ 0 & 0 & 1\\ 0 & 1 & b-1\end{bmatrix},$$

so that

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix}$$

is the product of 2 symmetric matrices of SL(3, F). It follows that $\left[\begin{smallmatrix}1 & 0\\ 0 & C\end{smallmatrix}\right]$ is the product of at most 4 symmetric matrices of SL(3, F), and hence that A is the product of at most 7 symmetric matrices of SL(3, F). Together with the preceding corollary this implies

Theorem 6. *Let F be a field, and suppose that $n \geq 3$. Then every matrix of* SL(n, F) *is the product of at most $3n - 2$ symmetric matrices of* SL(n, F).

The case $n = 2$ is exceptional. We first prove

Theorem 7. *Let F be any field except* GF(3). *Then every element of* SL(2, F) *is the product of at most 5 symmetric elements of* SL(2, F).

Proof. Let $A = \left[\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right]$ be any matrix of SL(2, F). As in the proof of Theorem 6, A is the product of at most 2 symmetric matrices of SL(2, F) and a matrix of of the form $\left[\begin{smallmatrix}1 & b\\ 0 & 1\end{smallmatrix}\right]$, $b \in F$. We may therefore confine our attention to this matrix.

Since $F \neq \mathrm{GF}(3)$, there is a nonzero element β of F such that $\beta^2 \neq 1$. Then

$$\begin{bmatrix} \beta & 0 \\ 0 & 1/\beta \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \beta & \beta b \\ 0 & 1/\beta \end{bmatrix},$$

and

$$\begin{bmatrix} 1 & y \\ y & 1+y^2 \end{bmatrix} \begin{bmatrix} \beta & \beta b \\ 0 & 1/\beta \end{bmatrix} = \begin{bmatrix} * & \beta b + y/\beta \\ \beta y & * \end{bmatrix}.$$

We now choose $y \in F$ so that $\beta b + y/\beta = \beta y$, $y = \beta^2 b/(\beta^2 - 1)$. The choice is possible since $\beta^2 \neq 1$. Thus $\left[\begin{smallmatrix}1 & b\\ 0 & 1\end{smallmatrix}\right]$ has been expressed as the product of 3 symmetric elements of SL(2, F), and it follows that A is the product of at most 5 symmetric elements of SL(2, F). This completes the proof.

The case $F = \mathrm{GF}(3)$ is a genuine exception. If

$$A = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & -1 \\ -1 & -1 \end{bmatrix},$$

then the symmetric elements of SL(2, F) are given by $\pm I$, $\pm A$, $\pm B$. Furthermore, since $A^2 = B^2 = -I$, $AB = -AB$, the subgroup of SL(2, F) generated by its symmetric elements is of order 8 and consists of $\pm I$, $\pm A$, $\pm B$, $\pm AB$. Since $AB = \left[\begin{smallmatrix}0 & 1\\ -1 & 0\end{smallmatrix}\right]$, we may conclude for example that the following is valid:

Theorem 8. *Let $F = \mathrm{GF}(3)$. Then $\left[\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right]$ is never the product of symmetric matrices of* SL(2, *F*).

The group $\Gamma = \mathrm{SL}(2, Z)$ leads to some interesting considerations. As is evident from Theorem 8, it will not be possible to express every element of Γ as the product of symmetric elements of Γ, and it is of interest to determine just when this can be done. For this purpose, we collect some information about Γ and its commutator subgroup Γ'. Γ is generated by the elements $T = \left[\begin{smallmatrix}0 & 1\\ -1 & 0\end{smallmatrix}\right]$, $S = \left[\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right]$ with defining relations $T^2 = (ST)^3 = -I$. Every element A of Γ satisfies

$$ATA^T = A^TTA = T. \tag{4}$$

Γ' is generated by the elements

$$M = \begin{bmatrix}2 & 1\\ 1 & 1\end{bmatrix}, \quad N = \begin{bmatrix}1 & 1\\ 1 & 2\end{bmatrix} \tag{5}$$

and is a free group.

Γ/Γ' is cyclic of order 12, and a complete set of coset representatives for Γ modulo Γ' is given by $(-S)^k$, $0 \le k \le 11$. (See [2] for these and other facts about Γ.)

We first prove

Lemma 1. *Suppose that A is symmetric, $A \in \Gamma$. Then either A or $-A$ (but not both) belongs to Γ'.*

Proof. Certainly not both A and $-A$ can belong to Γ', since $-I$ does not belong to Γ' (Γ' is free and $-I$ is of period 2).

We have $A = \left[\begin{smallmatrix}a & b\\ b & c\end{smallmatrix}\right]$, say, where $ac - b^2 = 1$. Let $\epsilon = \operatorname{sgn} a$ (a cannot be 0). Then the matrix ϵA is a 2×2 integral symmetric positive definite matrix of determinant 1. Since the class number of matrices of this type with respect to congruence transformations by elements of Γ is 1, we must have $\epsilon A = BB^T$, $B \in \Gamma$. Now $B^T = TB^{-1}T^{-1}$, by (4). Hence $\epsilon A = BTB^{-1}T^{-1}$, which is a commutator, and so belongs to Γ'. This completes the proof.

On the basis of this lemma, we now prove

Theorem 9. *Let Γ^* be the subgroup of Γ generated by all symmetric matrices of Γ. Then $\Gamma^* = \{-I, \Gamma'\}$, the subgroup of Γ generated by $-I$ and the elements of Γ'. Γ^* is a normal subgroup of Γ, and Γ/Γ^* is cyclic of order 6. A complete set of coset representatives for Γ modulo Γ^* is given by S^k, $0 \le k \le 5$.*

Proof. Suppose that $A \in \Gamma^*$. Then A is the product of finitely many symmetric elements of Γ, and the previous lemma implies that either A or $-A$ belongs to Γ'. Hence $A \in \{-I, \Gamma'\}$ and so $\Gamma^* \subset \{-I, \Gamma'\}$. Now suppose that $A \in \{-I, \Gamma'\}$. Because of (5) and the fact that $-I$ is symmetric, $\{-I, \Gamma'\}$ is generated by symmetric matrices of Γ. Hence A must be the product of finitely many symmetric matrices of Γ, and so must belong to Γ^*. Thus $\{-I, \Gamma'\} \subset \Gamma^*$, and it follows that $\Gamma^* = \{-I, \Gamma'\}$.

Since Γ^*/Γ' is a subgroup of index 2 of Γ/Γ', and Γ/Γ' is cyclic of order 12, Γ^*/Γ' is cyclic of order 6. The fact about the coset representatives follows from the fact that $(-S)^k$, $0 \le k \le 11$, forms a complete set of coset representatives for Γ modulo Γ'. This completes the proof.

From this theorem we can conclude for example that

Theorem 10. *None of the matrices*

$$T = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad S = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad ST = \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}$$

is the product of finitely many symmetric matrices of Γ.

Proof. None of the matrices $\pm T$, $\pm S$, $\pm ST$ belongs to Γ'.

Some open questions. An interesting open problem is whether or not any element of $\mathrm{SL}(n, R)$ is the product of a *fixed* number of symmetric elements of $\mathrm{SL}(n, R)$, where R is any principal ideal ring. By Theorem 5 it is sufficient to consider $n = 4$ for arbitrary R and $n = 3$ for $R = Z$. Another interesting open problem is whether Theorem 1 remains true for $n = 3$ and any principal ideal ring R, since the proof of Theorem 2 makes use of Dirichlet's theorem on primes in arithmetic progressions and the quadratic reciprocity law, neither of which is available in the general case.

Addendum. Richard T. Bumby has settled the second of the open questions mentioned above: that is, he has proved that Theorem 1 remains true for $n = 3$ and R any principal ideal ring. His proof consists of the observation that if a, b are any relatively prime elements of R, and a', b' are elements of R such that

$$aa' + bb' = 1,$$

then the row $(a, b, 0)$ has the completion

$$\begin{bmatrix} a & b & 0 \\ b & -1 & a'b - b' \\ 0 & a'b - b' & -aa'^2 - b'^2 \end{bmatrix}.$$

REFERENCES

1. C. C. MacDuffee, *The theory of matrices*, Chelsea, New York, 1946.
2. M. Newman, *Integral matrices*, Academic Press, New York, 1972.

3. O. Taussky, *The role of symmetric matrices in the study of general matrices*, Linear Algebra and Appl. 5 (1972), 147–154.

4. ———, *The factorization of an integral matrix into a product of two integral symmetric matrices*. I, Acta Arith. (to appear).

5. ———, *The factorization of an integral matrix into a product of two integral symmetric matrices*. II, Comm. Pure Appl. Math. (to appear).

MATHEMATICS DIVISION, NATIONAL BUREAU OF STANDARDS, WASHINGTON, D. C. 20234