SOME SUBGROUPS OF SL(3, $\mathbb{Z}$) GENERATED BY INVOLUTIONS

by STEPHEN P. HUMPHRIES

(Received 24 October, 1988)

Introduction. For R a commutative ring with identity 1 we let SL(n, R) denote the group of $n \times n$ integral matrices with determinant 1. A *transvection* T is an element of SL(n, R) which we represent (see [1]) as a pair (φ, d) where $\varphi \in (R^n)^*$, the dual space of R^n, $d \in R^n$, $\varphi(d) = 0$, and for all $x \in R^n$ we have

$$T(x) = x + \varphi(x)d.$$

Throughout this paper an *involution* is an element Y of SL(n, R) which has order two. Let $n = 3$ and $R = \mathbb{Z}$ and let $C = \mathrm{diag}(-1, -1, -1)$ be the central element of GL(3, $\mathbb{Z}$). Then any involution Y in SL(3, $\mathbb{Z}$) is conjugate to the matrix

$$\begin{pmatrix} 1 & \alpha & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

where $\alpha = 0$ or 1, there being thus two conjugacy classes which we will call *even* and *odd* respectively. In the even case we see that YC is a reflection and we note that groups generated by reflections are well understood (see [2] for example). It is our goal to study subgroups of SL(3, $\mathbb{Z}$) generated by odd involutions. In either case we note that we can also specify an involution Y as a pair (φ, d) where in this case $\varphi \in (\mathbb{Z}^3)^*$, $d \in \mathbb{Z}^3$, $\varphi(d) = 2$, and for all $x \in \mathbb{Z}^3$ we have

$$Y(x) = -x + \varphi(x)d.$$

This similarity between transvections and involutions in SL(3, $\mathbb{Z}$) enables us to apply techniques which we have used in previous work to the investigation of subgroups of SL(3, $\mathbb{Z}$) generated by involutions. Our results concern a certain matrix associated to a set of involutions, together with its accompanying graph. In order to explain our main result (Theorem 1.1 below) we will need the following definitions.

Let $S = \{Y_1, \ldots, Y_k\}$ be a set of involutions in SL(n, R) where $Y_1 = (\varphi_1, d_1), \ldots, Y_k = (\varphi_k, d_k)$ and let In(S) be the subgroup of SL(n, R) generated by $Y_1, \ldots, Y_k$. Associate to the set S the $k \times k$ matrix $M(S) = (\varphi_i(d_j))$. Now given any $k \times k$ matrix $M = (a_{ij})$ we let $G(M)$ be the directed graph with vertices $v_1, \ldots, v_k$ and a directed edge between v_i and v_j if and only if $a_{ij} \neq 0$. In particular, if $M = M(S)$, then we will also denote $G(M(S))$ by $G(S)$ and we will identify the vertices $v_1, \ldots, v_k$ with the involutions $Y_1, \ldots, Y_k$.

Let S' be another set of involutions in SL(n, R). Then an *elementary t-equivalence* is a surjection $f : S \to S'$ such that there are Y_i, $Y_j \in S$ with

$$f(Y_h) = \begin{cases} Y_h & \text{if} \quad h \neq j \\ Y_i Y_j Y_i^{-1} & \text{if} \quad h = j. \end{cases}$$

We denote such an f by t_{ij}. These generate the equivalence relation of *t-equivalence*. The

matrices $M(S)$ and the graphs $G(S)$ are acted upon by t-equivalences in the following natural way: let f be a t-equivalence and define $f(M(S)) = M(f(S))$, $f(G(S)) = G(f(S))$.

In the case where $n = 3$ and S is a set of three involutions we will show that if the images of $\mathrm{In}(S)$ under all of the projections $\Phi_p : \mathrm{SL}(3, \mathbb{Z}) \to \mathrm{SL}(3, \mathbb{Z}/p\mathbb{Z})$ are transitive subgroups (in particular if $\mathrm{In}(S) = \mathrm{SL}(3, \mathbb{Z})$), then the t-equivalence class of the matrix $M(S)$ contains one of the following matrices

$$A_\beta = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 1 & \beta & 2 \end{pmatrix}; \quad \text{or} \quad B = \begin{pmatrix} 2 & 1 & 1 \\ 5 & 2 & 2 \\ 7 & 3 & 2 \end{pmatrix};$$

where $\beta = 4$ or 5, or their transposes. The above hypotheses on $\mathrm{In}(S)$ will be shown to be equivalent to a simple determinant type condition on the matrix $M(S)$. We will show that if S and Q are sets of involutions with $M(S) = M(Q)$ and $\det(M(S)) \neq 0$, then $\mathrm{In}(S)$ and $\mathrm{In}(Q)$ are isomorphic (in fact conjugate) subgroups of $\mathrm{SL}(3, \mathbb{Z})$. This shows that in all cases of interest the matrix $M(S)$ completely determines the group $\mathrm{In}(S)$, at least up to conjugacy. In each of the above cases we show that $\mathrm{In}(S) = \mathrm{SL}(3, \mathbb{Z})$. Thus this gives a complete classification of such subgroups of $\mathrm{SL}(3, \mathbb{Z})$. Since the methods are constructive, one can easily devise an algorithm to determine which case one has. If M is a matrix, then M^t will denote the transpose of M. Our main result may now be stated as

THEOREM 1.1. *Let S be a set of three involutions in $\mathrm{SL}(3, \mathbb{Z})$ and let $M(S) = (a_{ij})$. Then the following conditions are equivalent*:

(i) *for all primes p the image of $\mathrm{In}(S)$ under the projection*

$$\Phi_p : \mathrm{SL}(3, \mathbb{Z}) \to \mathrm{SL}(3, \mathbb{Z}/p\mathbb{Z})$$

is a transitive subgroup of $\mathrm{SL}(3, \mathbb{Z}/p\mathbb{Z})$ and for $p = 2$ this image does not fix any quadratic form on $(\mathbb{Z}/2\mathbb{Z})^3$;

(ii) $\det(M(S)) = \pm 1$ *and* $a_{12}a_{23}a_{31} - a_{21}a_{13}a_{32} = \pm 1$;

(iii) *$M(S)$ is t-equivalent to one of the matrices A_4, A_4^t, A_5, A_5^t, B or B^t*;

(iv) $\mathrm{In}(S) = \mathrm{SL}(3, \mathbb{Z})$.

This result is in direct contrast to the case of subgroups of $\mathrm{SL}(3, \mathbb{Z})$ generated by transvections where it is possible to find a set of three transvections generating a subgroup H which projects onto all of the $\mathrm{SL}(3, \mathbb{Z}/p\mathbb{Z})$'s (in fact onto all of the $\mathrm{SL}(3, \mathbb{Z}/m\mathbb{Z})$'s for integers $m > 1$) but which is a rank three free group and so is not the whole of $\mathrm{SL}(3, \mathbb{Z})$; see [**4**] for details.

2. Generation of $\mathrm{SL}(n, \mathbb{Z})$ by involutions. Let E_{ij} be the $n \times n$ matrix whose only non-zero entry is a 1 in the (i, j) position. Let $B_{ij} = I + E_{ij}$ be the i, j elementary matrix in $\mathrm{SL}(n, \mathbb{Z})$. Let R_{ij} be the $n \times n$ diagonal matrix differing from the identity only in the ith and jth diagonal positions which are both -1. It is easily seen that $\mathrm{SL}(2, \mathbb{Z})$ is not generated by involutions and that $\mathrm{GL}(2, \mathbb{Z})$ is generated by two involutions. In this section we note the following (well-known) result:

PROPOSITION 2.1. *If $n \geq 3$, then $\mathrm{SL}(n, \mathbb{Z})$ is generated by n involutions.*

Proof. The cases $n = 3$ and $n > 3$ need to be treated differently. Suppose $n = 3$ and let $Y_1 = R_{23}B_{21}$, $Y_2 = R_{12}B_{32}^{-1}$ and $Y_3 = R_{12}B_{13}^{-1}$. Then Y_1, Y_2 and Y_3 are involutions and

https://doi.org/10.1017/S0017089500009150 Published online by Cambridge University Press

one easily checks the following:

$$(Y_1Y_2)^2 = B_{31}, \qquad B_{31}^{-1}(Y_3B_{31})^2 = B_{13}, \qquad B_{13}^{-2}(Y_3Y_1)^2 = B_{23}^{-1},$$
$$B_{23}^{-1}(Y_2B_{23})^2 = B_{32}, \qquad B_{13}^2B_{32}^{-2}(Y_2Y_3)^2 = B_{12}^{-1}.$$

Since B_{12}, B_{23} and B_{31} generate SL(3, $\mathbb{Z}$) the result follows for $n = 3$.

For $n > 3$ and $i = 1, 2, \ldots, n$ we define $Y_i = R_{i+1\,i+2}B_{i+1\,i-1}$ where all indices are to be taken mod n. Then, since $n > 3$ we have $(Y_iY_{i+1})^2 = B_{i+2\,i}^{\pm 1}$ and $(B_{i\,i-2}Y_i)^2 = B_{i+1\,i-2}^{\pm 1}$ where again all indices are to be read mod n. It is left to the reader to check that all the elementary matrices $B_{i\,i-2}$ and $B_{i\,i-3}$ also generate SL(n, Z).

3. Preliminary results. In this section we give some basic properties of involutions, t-equivalences and transitive subgroups of SL(n, R) generated by involutions. These are results which hold for all $n \geqslant 3$. We first prove a statement made in §1.

LEMMA 3.1. *Let S and Q be sets of involutions in* SL(n, R) *with* $M(S) = M(Q)$ *and* $\det(M(S)) \neq 0$. *Then* In(S) *and* In(q) *are conjugate subgroups of* SL(n, R).

Proof. Suppose that $S = \{Y_1, \ldots, Y_n\}$ and $Q = \{U_1, \ldots, U_n\}$, where $Y_i = (\varphi_i, d_i)$, $U_i = (\eta_i, e_i)$. Since $\det(M(S)) \neq 0$ we see that $\{d_1, \ldots, d_n\}$ and $\{e_1, \ldots, e_n\}$ are bases for R^n. Then one easily checks that the matrix of Y_i relative to the basis $\{d_1, \ldots, d_n\}$ is the same as the matrix of U_i relative to the basis $\{e_1, \ldots, e_n\}$. The result follows.

LEMMA 3.2. (i) *Let $T = (\varphi, d)$, $U = (\psi, e)$ be two involutions. Then*

$$UTU^{-1} = (\varphi - \varphi(e)\psi, -U(d)).$$

(ii) *Let $S = \{Y_1, \ldots, Y_k\}$ be a set of involutions as above and let $M(S) = (a_{rs})$. Then $t_{hj}(M(S)) = (b_{ij})$, where*

$$b_{ij} = a_{ij} - a_{hj}a_{ih}, \qquad \text{if } i \neq j;$$
$$b_{ji} = a_{ji} - a_{jh}a_{hi}, \qquad \text{if } i \neq j;$$
$$b_{ki} = a_{ki} \qquad \text{if } k \neq j,\ i \neq j; \text{ and}$$
$$b_{ii} = a_{ii} \qquad \text{for all } i = 1, \ldots, k.$$

Proof. This is an easy calculation.

PROPOSITION 3.3. *Let $f : S \to S'$ be a t-equivalence. Then*

(i) $\mathrm{In}(f(S)) = \mathrm{In}(S)$;
(ii) $\mathrm{rank}(M(f(S))) = \mathrm{rank}(M(S))$;
(iii) $\det(M(f(S))) = \det(M(S))$; *and*
(iv) $G(M(S'))$ *is connected if and only if* $G(M(S))$ *is connected.*

Proof. Clearly we need only prove these results in the case when f is an elementary t-equivalence, say $f = t_{ij}$ for $i \neq j = 1, \ldots, k$. In this case (i) is clear since an elementary t-equivalence is just a Nielsen transformation. Now (ii) and (iii) follow from Lemma 3.2 since $M(f(S))$ is obtained from $M(S)$ by adding multiples of the ith row and column to the jth row and column. For a proof of (iv) see Proposition 3.2 of [**3**, **I**].

REMARK. In the case $n = k = 3$, as above, let $M(S) = (a_{ij})$. It follows easily from Lemma 3.2 that not only is $\det(M(S))$ preserved by t-equivalences but the quantity $|a_{12}a_{23}a_{31} - a_{21}a_{13}a_{32}|$ is also preserved.

LEMMA 3.4. *If $R = \mathbb{Z}/p\mathbb{Z}$ for p a prime and $S = \{Y_1, \ldots, Y_n\}$, $Y_i = (\varphi_i, d_i)$, is a set of involutions in* $\mathrm{SL}(n, R)$ *such that* $\mathrm{In}(S)$ *is transitive, then $d_1, \ldots, d_n$ span R^n and $\varphi_1, \ldots, \varphi_n$ span $(R^n)^*$. In the case $R = \mathbb{Z}$, $d_1, \ldots, d_n$ is a $\mathbb{Z}$-basis for $\mathbb{Z}^n$.*

Proof. The proof is exactly the same as in the transvection case (see Proposition 2.5 of [**3**, I]).

This immediately gives:

COROLLARY 3.5. *The minimal number of involutions needed to generate* $\mathrm{SL}(n, \mathbb{Z})$, $n \geq 3$, *is n.*

We will say that a subgroup H of $\mathrm{SL}(n, \mathbb{Z})$ is *p-transitive* if its images under all of the natural homomorphisms

$$\Phi_q : \mathrm{SL}(n, \mathbb{Z}) \to \mathrm{SL}(n, \mathbb{Z}/q\mathbb{Z}) \text{ are transitive (where } q \text{ is a prime number).}$$

PROPOSITION 3.6. *If $S = \{Y_1, \ldots, Y_n\}$, $Y_i = (\varphi_i, d_i)$, is a set of involutions in* $\mathrm{SL}(n, R)$ *such that* $\mathrm{In}(S)$ *is p-transitive, then* $\det(M(S)) = \pm 1$. *In particular, in the case $n = 3$ all of the involutions are odd.*

Proof. Let $M = M(S)$, and suppose that $\det(M) \equiv 0 \bmod p$ for some prime p. We will now be thinking of M as a matrix with $\mathbb{Z}_p$ coefficients. Let $c_1, \ldots, c_n$ be the columns of M. Then there are $\lambda_1, \ldots, \lambda_n \in \mathbb{Z}_p$ such that

$$\lambda_1 c_1 + \lambda_2 c_2 + \ldots + \lambda_n c_n = 0.$$

Let $d = \lambda_1 d_1 + \ldots + \lambda_n d_n$. Then one easily checks that $Y_i(d) = -d$ for all $i = 1, \ldots, n$. It easily follows that $\mathrm{In}(S)$ is not p-transitive. If $n = 3$ and some Y_i is even, then one easily checks that $\det(M(S))$ is even; this gives the second statement.

As we are only interested in the case where $\mathrm{In}(S)$ is p-transitive, the above result shows that from now on we may assume that $\det(M(S)) = \pm 1$. It turns out that this condition does not guarantee that $\mathrm{In}(S)$ is p-transitive as we will see in the next section. In the case $n = 3$ it follows from the condition $\det(M(S)) = \pm 1$ that the graph $G(M(S))$ is connected. In general we have the following result, a proof of which can be obtained from the corresponding result (Proposition 2.2) of [**3**, **I**].

LEMMA 3.7. If $\mathrm{In}(S)$ is transitive, then $G(M(S))$ is connected.

4. The case $n = 3$. If $k = n = 3$ we can say something more about when $\mathrm{In}(S)$ is p-transitive, however in order to do so we must prove the following result which classifies the involutions in $\mathrm{SL}(3, \mathbb{Z})$. An involution Y in $\mathrm{SL}(n, R)$ is of *rank r* if $\mathrm{rank}(Y + \mathrm{Id}) = r$. Clearly there is at most one conjugacy class of involutions of rank 0. We now prove

PROPOSITION 4.1. *Any involution Y in* $\mathrm{SL}(3, \mathbb{Z})$ *is of rank* 1 *and is conjugate in* $\mathrm{SL}(3, \mathbb{Z})$ *to the matrix*

$$\begin{pmatrix} 1 & w & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

where $w = 0$, 1. Moreover the involution Y can be represented as a pair (φ, d) where

https://doi.org/10.1017/S0017089500009150 Published online by Cambridge University Press

$\varphi \in (\mathbb{Z}^3)^*$, $d \in \mathbb{Z}^3$, $\varphi(d) = 2$ *and for all* $x \in \mathbb{Z}^3$ *we have*

$$Y(x) = -x + \varphi(x)d.$$

Proof. By Exercise 2 on page 54 of [5] we see that any involution in SL(3, $\mathbb{Z}$) is conjugate to a matrix of the above type. It is clear that any such matrix is a rank one involution. The rest follows easily.

REMARK. The above result shows that involutions in SL(3, $\mathbb{Z}$) have a similar form to transvections. It is this result together with the fact that SL(3, $\mathbb{Z}$) is generated by (rank 1) involutions which allows us to make some progress. Note that for a transvection T the rank of $T - \mathrm{Id}$ is equal to one.

THEOREM 4.2. *Let* $R = \mathbb{Z}$ *or* $\mathbb{Z}/p\mathbb{Z}$ *for some prime* p. *If* $S = \{Y_1, Y_2, Y_3\}$, $M(S) = (a_{ij})$, $\mathrm{In}(S)$ *is* p*-transitive and for* $p = 2$ *the group* $\Phi_p(\mathrm{In}(S))$ *does not fix any quadratic form on* $(\mathbb{Z}/2\mathbb{Z})^3$, *then*

$$(a_{12}a_{23}a_{31} - a_{21}a_{13}a_{32})(\det(M(S))$$

is a unit in R. *In particular, if* $R = \mathbb{Z}$ *we have* $\det(M(S)) = \pm 1$ *and* $(a_{12}a_{23}a_{31} - a_{21}a_{13}a_{32}) = \pm 1$.

Proof. We show that if the above expression is not a unit, then $\Phi_p(\mathrm{In}(S))$ fixes a quadratic form. We then show that this contradicts our hypotheses. Let $M(S) = (a_{ij})$ and let $S' = (s_{ij})$ be a symmetric matrix. Then by a suitable choice of basis (i.e. $\{d_1, d_2, d_3\}$-see Lemma 3.1) we may take Y_1, Y_2, Y_3 to be the matrices

$$Y_1 = \begin{pmatrix} 1 & a_{12} & a_{13} \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad Y_2 = \begin{pmatrix} -1 & 0 & 0 \\ a_{21} & 1 & a_{23} \\ 0 & 0 & -1 \end{pmatrix} \quad Y_3 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ a_{31} & a_{32} & 1 \end{pmatrix}.$$

Then the conditions $Y_i S' Y_i^t = S'$, $i = 1, 2, 3$, give the following equations

$$2s_{12} + a_{12}s_{22} + a_{13}s_{23} = 0; \quad 2s_{13} + a_{12}s_{23} + a_{13}s_{33} = 0;$$
$$2s_{12} + a_{21}s_{11} + a_{23}s_{13} = 0; \quad 2s_{23} + a_{21}s_{13} + a_{23}s_{33} = 0;$$
$$2s_{13} + a_{31}s_{11} + a_{32}s_{12} = 0; \quad 2s_{23} + a_{31}s_{12} + a_{32}s_{22} = 0.$$

We write these in the following form:

$$\begin{pmatrix} 0 & a_{12} & 0 & 2 & 0 & a_{13} \\ 0 & 0 & a_{13} & 0 & 2 & a_{12} \\ a_{21} & 0 & 0 & 2 & a_{23} & 0 \\ 0 & 0 & a_{23} & 0 & a_{21} & 2 \\ a_{31} & 0 & 0 & a_{32} & 2 & 0 \\ 0 & a_{32} & 0 & a_{31} & 0 & 2 \end{pmatrix} \begin{pmatrix} s_{11} \\ s_{22} \\ s_{33} \\ s_{12} \\ s_{13} \\ s_{23} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

One calculates that the determinant of the above matrix is the expression in the statement of Theorem 4.2. If $R = \mathbb{Z}$ and this determinant is not a unit let $q > 1$ be a prime dividing it. Otherwise, if $R = \mathbb{Z}/p\mathbb{Z}$ we let $q = p$. Then mod q there is a non-zero solution to these equations and so there is a quadratic form which is fixed by $\mathrm{In}(S)$ as required. This

https://doi.org/10.1017/S0017089500009150 Published online by Cambridge University Press

directly contradicts our hypotheses if $q = 2$. If $q > 2$, then we obtain a contradiction using the following result.

LEMMA 4.3. *If $p > 2$ is a prime and G is a subgroup of $\mathrm{SL}(3, \mathbb{Z}/p\mathbb{Z})$ which fixes a non-trivial quadratic form S on $(\mathbb{Z}/p\mathbb{Z})^3$, then G does not act transitively on the non-trivial elements of $(\mathbb{Z}/p\mathbb{Z})^3$.*

Proof. One easily checks that if S is represented by a symmetric matrix (also called S), then the condition $v^tSv = w^tSw$ for all $v, w \in (\mathbb{Z}/p\mathbb{Z})^3$ implies that S is the zero matrix. Now if G were transitive then this condition would have to be satisfied; this gives the contradiction.

REMARKS 1. By the above results, in the case $R = \mathbb{Z}$ we now need only consider the case where $\det(M(S)) = \pm 1$ and $(a_{12}a_{23}a_{31} - a_{21}a_{13}a_{32}) = \pm 1$. 2. The above result shows that condition (i) of Theorem 1.1 implies condition (ii).

5. t-Equivalence classes of matrices. In this section we show that condition (ii) of Theorem 1.1 implies condition (iii). Let $S = \{Y_1, Y_2, Y_3\}$ be a set of 3 involutions in $\mathrm{SL}(3, \mathbb{Z})$ as in the previous sections. We further assume that $\det(M(S)) = \pm 1$ and $a_{12}a_{23}a_{31} - a_{21}a_{13}a_{32} = \pm 1$. Let $M = M(S) = (a_{ij})$. Define *t-deg(M)*, the *t-degree of M* to be the largest number of zeros occuring in some element of the t-equivalence class of M. Note that if $Y_i = (\varphi_i, d_i)$, then the effect of replacing φ_i and d_i by their negatives has no effect on Y_i, however it has the effect of multiplying the ith row and column of $M(S)$ by -1.

PROPOSITION 5.1. *Let $n = 3$ and assume that $\det(M) = \pm 1$ and $a_{12}a_{23}a_{31} - a_{21}a_{13}a_{32} = \pm 1$. Then (up to some permutation of Y_1, Y_2, Y_3) M is t-equivalent to A_4 or A_4^t (if $\det(M) = 1$); or A_5 or A_5^t (if $\det(M) = -1$) if and only if $t - \deg(M) \neq 0$. Further, A_4 and A_5 are not t-equivalent.*

Proof. Certainly t-deg$(M) \neq 0$ if M is t-equivalent to A_4, A_5 or their transposes. Now suppose that t-deg$(M) \neq 0$. Let us assume first that $a_{13} = 0$. Since $a_{12}a_{23}a_{31} - a_{21}a_{13}a_{32} = \pm 1$ we see that a_{12}, a_{23} and a_{31} all have absolute value 1. By replacing d_1 and φ_1 by their negatives if necessary we see that we can assume that $a_{12} = 1$. Similarly by changing d_3 and φ_3 we can arrange that $a_{23} = 1$. Now Lemma 3.2 shows that doing t_{13} allows us to assume that $a_{31} = 1$ also. In this situation $\det(M) = 9 - 2a_{32} - 2a_{21}$, and so $a_{32} + a_{21} = 4$ or 5. Consider the following t-equivalences:

$$\begin{pmatrix} 2 & 1 & 0 \\ a_{21} & 2 & 1 \\ 1 & a_{32} & 2 \end{pmatrix} \to \begin{pmatrix} 2 & -1 & 0 \\ -a_{21} & 2 & 1 \\ 1 & a_{32}-1 & 2 \end{pmatrix} \to \begin{pmatrix} 2 & -1 & 0 \\ -a_{21}-1 & 2 & -1 \\ 1 & -a_{32}+1 & 2 \end{pmatrix}$$
$$\to \begin{pmatrix} 2 & 1 & 0 \\ a_{21}+1 & 2 & -1 \\ 1 & -a_{32}+2 & 2 \end{pmatrix} \to \begin{pmatrix} 2 & 1 & 0 \\ a_{21}+2 & 2 & 1 \\ 1 & a_{32}-2 & 2 \end{pmatrix}.$$

By these moves (which we will refer to as *basic*) we can reduce to the case where $a_{21} = 0$

https://doi.org/10.1017/S0017089500009150 Published online by Cambridge University Press

or 1. If $a_{21} = 1$, then we do the following:

$$\begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 1 \\ 1 & a_{32} & 2 \end{pmatrix} \to \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & -1 \\ 1 & -a_{32} & 2 \end{pmatrix} \to \begin{pmatrix} 2 & -1 & 0 \\ 0 & 2 & -1 \\ 1 & -a_{32}-1 & 2 \end{pmatrix}.$$

Replacing d_2 and φ_2 by their negatives shows that we can now assume that $a_{21} = 0$ and that $a_{32} = 4$ or 5. Thus we have A_4 or A_5. It is easily seen that these two cases correspond to distinct t-equivalence classes since $\det(M)$ is different in the two cases and $\det(M)$ is fixed by t-equivalences (Proposition 3.3) and by the operation of permuting Y_1, Y_2, Y_3.

The cases where $a_{31} = 0$ are dealt with similarly: here one obtains A_4' or A_5'. Now if $a_{12} = 0$, then an analogous process to the above reduces to the case $a_{12} = a_{23} = a_{31} = 1$, $a_{21} = 0$ and either (i) $a_{13} = 0$ or (ii) $a_{32} = 0$. Note that case (ii) is A_β for some $\beta = 4, 5$ and that case (i) is t-equivalent to some A_β by a process similar to the basic moves above. All remaining cases are treated similarly. This concludes the proof.

We now investigate the case where M is of t-degree zero. We will say that any 3×3 matrix $M = M(S) = (a_{ij})$ is *t-reduced* if $\det(M) = \pm 1$, $a_{12}a_{23}a_{31} - a_{21}a_{13}a_{32} = \pm 1$ and M is of t-degree zero or

$$|a_{ij} - a_{ik}a_{kj}| > |a_{ij}|$$

for all distinct i, j, k. We now prove:

THEOREM 5.2. *Any t-reduced t-degree zero* 3×3 *matrix* $M = M(S)$ *is t-equivalent to the matrix*

$$\begin{pmatrix} 2 & 1 & 1 \\ 5 & 2 & 2 \\ 7 & 3 & 2 \end{pmatrix}$$

or its transpose.

Proof. Assume throughout that $S = \{Y_1, Y_2, Y_3\}$, $Y_i = (\varphi_i, d_i)$, where $M(S)$ is t-reduced and of t-degree zero. We first observe that if $\det(M) = \delta$ and $a_{12}a_{23}a_{31} - a_{21}a_{13}a_{32} = \epsilon$ (where $\delta, \epsilon = \pm 1$), then

$$a_{32} = \frac{(a_{12}^2 a_{23}a_{21} + \epsilon a_{13} - (8 - \delta + \epsilon)a_{12}a_{23}/2)}{(a_{12}a_{13}a_{21}a_{23} - a_{12}a_{23}^2 - a_{21}a_{13}^2)} \tag{1}$$

unless $a_{12}a_{13}a_{21}a_{23} - a_{12}a_{23}^2 - a_{21}a_{13}^2 = 0$. However if this is the case, then we also have

$$a_{12}^2 a_{23}a_{21} + \epsilon a_{13} - (8 - \delta + \epsilon)a_{12}a_{23}/2 = 0.$$

Using the second equation we can express a_{13} as a function of a_{12}, a_{23} and a_{21}. Substituting into the first equation and simplifying gives

$$a_{12}a_{21}[\epsilon(\lambda - a_{12}a_{21}) - (\lambda + a_{12}a_{21})^2] = 1,$$

where $\lambda = (8 - \delta + \epsilon)/2$. Thus $a_{12}a_{21} = \pm 1$ and one now checks that it is not possible to satisfy the above equation with $\epsilon = \pm 1$ and $\lambda = 3, 4, 5$. Thus $a_{12}a_{13}a_{21}a_{23} - a_{12}a_{23}^2 - a_{21}a_{13}^2 \neq 0$ and so we may always use equation (1).

https://doi.org/10.1017/S0017089500009150 Published online by Cambridge University Press

We next show that we may impose certain conditions on the matrix $M(S)$ in order to restrict the set of such matrices which we have to consider, while keeping the group $\mathrm{In}(S)$ fixed. First note that changing the order of the involutions in S will give a permutation of the entries of $M(S)$. This clearly has no effect on the group $\mathrm{In}(S)$. We noted above that $Y_i = (\varphi_i, d_i) = (-\varphi_i, -d_i)$. Using this idea we now prove:

LEMMA 5.3. *Replacing some φ_i and d_i by their negatives if necessary we may assume that all of the entries of $M(S)$ are positive.*

Proof. Let $M(S) = (a_{ij})$. If $a_{12} < 0$, then replace φ_2 and d_2 by their negatives. If now $a_{13} < 0$, then we do the same to φ_3 and d_3. Thus we may now assume that $a_{12} > 0$ and $a_{13} > 0$. Next note that since $a_{12}a_{23}a_{31} - a_{21}a_{13}a_{32} = \pm 1$ and all the a_{ij} are non-zero we must have $\mathrm{sign}(a_{23}a_{31}) = \mathrm{sign}(a_{32}a_{21})$. Now suppose, for example, that $a_{21} > 0$ and $a_{23} < 0$. Then by (1) and the choices made above we see that $a_{32} > 0$ and so we must have $a_{31} < 0$. Now

$$\det(M(S)) = 8 - 2a_{12}a_{21} - 2a_{23}a_{32} - 2a_{13}a_{31} + a_{12}a_{23}a_{31} + a_{21}a_{13}a_{32}$$

and since each of these terms is positive except for $-2a_{12}a_{21}$ we see that $|\det(M(S))| > 1$, a contradiction. All other cases are checked similarly. This proves Lemma 5.3.

From now on we will always invoke the above result and assume that $a_{ij} > 0$ for all i, j. With this assumption and the fact that $M(S)$ is t-reduced we may now assume that $a_{ij}a_{jk} \geq 2a_{ik}$ for all distinct i, j, k. If M is a matrix, then M^t will denote its transpose.

LEMMA 5.4. *If S and S' are two sets of three involutions such that $M(S) = M(S')^t$, then* $\mathrm{In}(S)$ *and* $\mathrm{In}(S')$ *are isomorphic groups.*

Proof. It is easily checked that the action of $\mathrm{In}(S)$ on the dual space $(\mathbb{Z}^3)^*$ is that of a group of involutions having matrix $M(S)^t$. The result now easily follows.

We now proceed more directly with the proof of Theorem 5.2. We consider two cases:

Case 1: Here one of the inequalities $a_{ij}a_{jk} \geq 2a_{ik}$ is actually an equality. Since the a_{ij} are positive integers and $a_{12}a_{23}a_{31} - a_{21}a_{13}a_{32} = \pm 1$ we must have $a_{ij} = a_{ik} = 1$ and $a_{jk} = 2$ or $a_{jk} = a_{ik} = 1$ and $a_{ij} = 2$. By Lemma 5.4 and suitably permuting Y_1, Y_2, Y_3 we may assume that $a_{12} = a_{13} = 1$ and $a_{23} = 2$. Further we see that all of the other inequalities are strict. We then have

$$a_{32} = \frac{(2a_{21} + \epsilon - (8 - \delta + \epsilon))}{(a_{21} - 4)}$$

and so the condition $a_{13}a_{32} > 2a_{12}$ gives $a_{32} > 2$. If $a_{32} > 3$, then

$$(2a_{21} + \epsilon - (8 - \delta + \epsilon)) > 3(a_{21} - 4)$$

and so $a_{21} < 6$. But knowing a_{12}, a_{13}, a_{21} and a_{23} we can calculate a_{31} and a_{32} using the non-degeneracy conditions. Similarly if we have $a_{32} = 3$ together with a_{12}, a_{13}, a_{23}, then we can calculate a_{21} and a_{31}. In each case we obtain $a_{21} = 5$, $a_{31} = 7$ and $a_{32} = 3$. This concludes our considerations of this case.

Case 2: All of the inequalities $a_{ij}a_{jk} \geq 2a_{ik}$ are strict. Since $a_{13}a_{32} > 2a_{12}$ we see that

$$a_{13}[a_{12}^2 a_{23}a_{21} + \epsilon a_{13} - \lambda a_{12}a_{23}] > 2a_{12}[a_{12}a_{13}a_{21}a_{23} - a_{12}a_{23}^2 - a_{21}a_{13}^2]$$

https://doi.org/10.1017/S0017089500009150 Published online by Cambridge University Press

where $\lambda = (8 - \delta + \epsilon)/2$. Thus

$$a_{13}[\epsilon a_{13} - \lambda a_{12}a_{23}] > a_{12}(a_{12}a_{13}a_{23}a_{21} - 2a_{12}a_{23}^2 - 2a_{21}a_{13}^2).$$

Assume that $\epsilon = 1$. The case where $\epsilon = -1$ is dealt with in a similar way by considering the transposed matrix $M(S)^t$ (see Lemma 5.4). Then $\lambda \geq 4$ and so $-\lambda \leq -4$. Thus we have

$$\begin{aligned} a_{21} &< \frac{a_{13}(a_{13} - \lambda a_{12}a_{23}) + 2a_{12}^2a_{23}^2}{a_{12}a_{13}(a_{12}a_{23} - 2a_{13})} \\ &\leq \frac{a_{12}a_{23}(2a_{12}a_{23} - 4a_{13}) + a_{13}^2}{a_{12}a_{13}(a_{12}a_{23} - 2a_{13})} \\ &\leq \frac{2a_{23}}{a_{13}} + \frac{a_{13}}{a_{12}(a_{12}a_{23} - 2a_{13})} \end{aligned} \tag{2}$$

If $a_{23} < a_{21}$, then we now have

$$\begin{aligned} 1 &< \frac{2}{a_{13}} + \frac{a_{13}}{a_{12}a_{23}(a_{12}a_{23} - 2a_{13})} \\ &< \frac{2}{a_{13}} + \frac{1}{2(a_{12}a_{23} - 2a_{13})}. \end{aligned} \tag{3}$$

The above equation shows that $a_{13} \leq 3$ and in fact that if $a_{13} = 3$, then $6 < a_{12}a_{23} < 9$. Thus we have shown

(i) if $a_{23} < a_{21}$, then $a_{13} \leq 3$.

Since permuting the indices of $M(S) = (a_{ij})$ by the permutation (123) does not change the value of ϵ can similarly show that

(ii) if $a_{31} < a_{32}$, then $a_{21} \leq 3$; or

(iii) if $a_{12} < a_{13}$, then $a_{32} \leq 3$.

Note that at least one of the above conditions must be satisfied since $a_{12}a_{23}a_{31} - a_{21}a_{13}a_{32} = \pm 1$. The rest of the proof is just more case checking. Suppose without loss that (i) is satisfied. If $a_{13} = 3$, then by (3) we have $6 < a_{12}a_{23} < 9$. Thus

$$a_{32} = \frac{(a_{12}^2a_{23}a_{21} + 3 - (9 - \delta)a_{12}a_{23}/2)}{(3a_{12}a_{21}a_{23} - a_{12}a_{23}^2 - 9a_{21})}$$

and one checks that a_{32} is not an integer (a contradiction) for all possible cases with $a_{12}a_{23} = 7$, 8 and $\delta = \pm 1$.

If now $a_{13} = 2$, then from (2) we have $a_{12} = 1$, $a_{21} < a_{23} + 2$ and so $a_{21} = a_{23} + 1$. One now similarly checks that a_{32} cannot be an integer.

Lastly, if $a_{13} = 1$, then $a_{21} > 2a_{23}$ and so by (2) we have

$$2a_{23} < a_{21} < 2a_{23} + 1/(a_{12}(a_{12}a_{23} - a_{13})),$$

and so a_{21} is not an integer. This concludes the proof of Theorem 5.2.

REMARK. It is possible to show that A_4, A_5 and B are not t-equivalent. The proof of this fact is accomplished by considering more inequalities of the entries of these matrices.

6. Some sets of three involutions generating SL(3, $\mathbb{Z}$)**.** In this section we show that condition (iii) of Theorem 1.1 implies condition (iv). In the last section we showed that to each set S of three involutions in SL(3, $\mathbb{Z}$) there is a t-equivalence $S \to S'$ such that up to a

https://doi.org/10.1017/S0017089500009150 Published online by Cambridge University Press

permutation of the elements of S, $M(S')$ is one of three matrices. We now show that in each of these cases these involutions generate $\mathrm{SL}(3,\mathbb{Z})$.

Case 1: $M(S)$ is the matrix A_4. Here we note that A_4 is the matrix of the set of three involutions which were shown to generate $\mathrm{SL}(3,\mathbb{Z})$ in Theorem 2.1.

Case 2: $M(S)$ is the matrix A_5. Let Y_1, Y_2 and Y_3 (respectively) be the following matrices having $M(\{Y_1, Y_2, Y_3\}) = A_5$.

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 1 & 5 & 1 \end{pmatrix}.$$

Then $X = (Y_1Y_2)^2 = B_{12}^{-2}B_{13}^{-1}$ and $Z = (Y_1Y_3)^2 = B_{31}^2B_{32}$. Also $Y_3Y_1(XZ)^2 = B_{31}^{-1}B_{32}^{-1}$, which together with Z allows us to generate B_{31} and B_{32}. Now $U = B_{32}Y_3$ is the matrix

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 1 & 4 & 1 \end{pmatrix}$$

But $M(\{Y_1, Y_2, U\}) = A_4$ and so Y_1, Y_2 and U generate $\mathrm{SL}(3,\mathbb{Z})$ by case 1 above.

Case 3: $M(S)$ is the matrix B. In this case we have not been able to directly show that $\mathrm{In}(S) = \mathrm{SL}(3,\mathbb{Z})$, however using the Todd–Coxeter algorithm as implemented in the group theory package 'Cayley' it can be shown that $\mathrm{In}(S)$ has index 1 in $\mathrm{SL}(3,\mathbb{Z})$.

This concludes our proof of all of the claims made in §1 since condition (i) of Theorem 1.1 clearly follows from condition (iv). Thus we have been able to characterise all integral 3×3 matrices $M(S)$ (and the groups $\mathrm{In}(S)$ associated to them) satisfying the two non-degeneracy conditions $\det(M(S)) = \pm 1$ and $a_{12}a_{23}a_{31} - a_{21}a_{13}a_{32} = \pm 1$. If we consider matrices satisfying only the last condition, then it is possible to say something about the groups $\mathrm{In}(S)$ in certain special cases. For example if $a_{12}a_{23}a_{31} - a_{21}a_{13}a_{32} = \pm 1$ and $M(S) = (a_{ij})$ where we have either

(i) $|a_{ij}| > 7$ for all $i \neq j$; or

(ii) $|a_{ij}a_{jk}| \geq 6\,|a_{ik}|$ for all distinct i, j, k;

then $\mathrm{In}(S)$ is isomorphic to the free product $\mathbb{Z}_2^*\mathbb{Z}_2^*\mathbb{Z}_2$. This is proved exactly as in [**4**] for the transvection case.

REFERENCES

1. E. Artin *Geometric algebra*, (Interscience 1957).

2. H. S. M. Coxeter, Discrete groups generated by reflections, *Ann. Math.* **35** (1934) 588–621.

3. R. Brown and S. P. Humphries, Orbits under symplectic transvections I and II, *Proc. London Math. Soc.* (3) **52** (1986), 517–531 *and* 532–556.

4. S. P. Humphries, Free subgroups of $\mathrm{SL}(n,\mathbb{Z})$, $n > 2$, generated by transvections, *J. Algebra* **116** (1988), 155–162.

5. M. Newman, *Integral matrices* (Academic Press 1972).

Department of Mathematics
Brigham Young University
Provo
Utah 84602
U.S.A.