AUTOMORPHISMS OF THE UNIMODULAR GROUP

BY

L. K. HUA AND I. REINER

Notation. Let $\mathfrak{M}_n$ denote the group of $n \times n$ integral matrices of determinant ± 1 (the unimodular group). By $\mathfrak{M}_n^+$ we denote that subset of $\mathfrak{M}_n$ where the determinant is $+1$; $\mathfrak{M}_n^-$ is correspondingly defined. Let $I^{(n)}$ (or briefly I) be the identity matrix in $\mathfrak{M}_n$, and let X' represent the transpose of X. The direct sum of the matrices A and B will be represented by $A \dotplus B$;

$$A \overset{s}{=} B$$

will mean that A is similar to B. In this paper, we shall find explicitly the generators of the group $\mathfrak{A}_n$ of all automorphisms of $\mathfrak{M}_n$.

1. **The commutator subgroup of $\mathfrak{M}_n$.** The following result is useful, and is of independent interest.

THEOREM 1. *Let $\mathfrak{R}_n$ be the commutator subgroup of $\mathfrak{M}_n$. Then trivially $\mathfrak{R}_n \subset \mathfrak{M}_n^+$. For $n=2$, $\mathfrak{R}_n$ is of index 2 in $\mathfrak{M}_n^+$, while for $n>2$, $\mathfrak{R}_n = \mathfrak{M}_n^+$.*

Proof. Consider first the case where $n=2$. Define

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}. \tag{1}$$

It is well known that S and T generate $\mathfrak{M}_2^+$. An element X of $\mathfrak{M}_2^+$ is called *even* if, when X is expressed as a product of powers of S and T, the sum of the exponents is even; otherwise, X is called *odd*. Since all relations satisfied by S and T are consequences of

$$S^2 = -I, \qquad (ST)^3 = I,$$

it follows that the parity of $X \in \mathfrak{M}_2^+$ depends only on X, and not on the manner in which X is expressed as a product of powers of S and T. Let $\mathfrak{E}$ be the subgroup of $\mathfrak{M}_2^+$ consisting of all even elements; then clearly $\mathfrak{E}$ is of index 2 in $\mathfrak{M}_2^+$. It suffices to prove that $\mathfrak{E} = \mathfrak{R}_2$.

We prove first that $\mathfrak{R}_2 \subset \mathfrak{E}$. Since the commutator subgroup of a group is always generated by squares, it suffices to show that $A \in \mathfrak{M}_2$ implies $A^2 \in \mathfrak{E}$. For $A \in \mathfrak{M}_2^+$, this is clear. If $A \in \mathfrak{M}_2^-$, set $A = XJ = JY$, where

$$J = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{2}$$

Presented to the Society, December 29, 1950; received by the editors January 8, 1951.

and X and $Y \in \mathfrak{M}_2^+$. Then $A^2 = XY = XJ^{-1}XJ$. Hence we need only prove that if $X \in \mathfrak{M}_2^+$, X and $J^{-1}XJ$ are of the same parity. This is easily verified for $X = S$ or T; since S and T generate $\mathfrak{M}_2^+$, and $J^{-1}X_1X_2J = J^{-1}X_1J \cdot J^{-1}X_2J$, the result follows.

On the other hand we can show that $\mathfrak{E} \subset \mathfrak{R}_2$. For, $\mathfrak{E}$ is generated by T^2 and ST, since $TS = (ST \cdot T^{-2})^2$. However, $T^2 = TJT^{-1}J^{-1} \in \mathfrak{R}_2$, and therefore also $(T')^{-2} \in \mathfrak{R}_2$. Furthermore, $ST = TST^{-1}S^{-1}(T')^{-2}T^2 \in \mathfrak{R}_2$. This completes the proof for $n = 2$.

Suppose now that $n > 2$, and define

$$(3) \qquad R = \begin{pmatrix} 0 \cdots 0 & (-1)^{n-1} \\ 1 \cdots 0 & 0 \\ \cdot \quad \cdots \quad \cdot & \cdot \\ 0 \cdots 1 & 0 \end{pmatrix} \in \mathfrak{M}_n^+, \qquad S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + I^{(n-2)},$$

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} + I^{(n-2)}.$$

(The symbols S and T defined here are the analogues in $\mathfrak{M}_n^+$ of those defined by (1). It will be clear from the context which are meant.) For $n > 2$ we have[1]

$$T' = [R^{-1}(TR)^{-(n-2)}R(TR)^{n-2}](TR)^{-1}[R(TR)^{-(n-2)}R^{-1}(TR)^{n-2}](TR) \in \mathfrak{R}_n.$$

Further $S = TST^{-1}S^{-1}(T')^{-2}T \in \mathfrak{R}_n$. Finally, for odd n there exists a permutation matrix P such that $R^2 = P^{-1}RP$, whence $R = R^{-1}P^{-1}RP \in \mathfrak{R}_n$. For even n, R represents the monomial transformation

$$\begin{pmatrix} x_1 & x_2 \cdots x_{n-1} & x_n \\ x_2 & x_3 \cdots x_n & -x_1 \end{pmatrix},$$

which is a product of

$$\begin{pmatrix} x_1 & x_2 & x_3 \cdots x_{n-1} & x_n \\ x_2 & -x_1 & x_3 \cdots x_{n-1} & x_n \end{pmatrix}, \quad \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \cdots x_n \\ -x_3 & x_2 & x_1 & x_4 \cdots x_n \end{pmatrix},$$

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \cdots x_n \\ x_4 & x_2 & x_3 & -x_1 \cdots x_n \end{pmatrix}, \cdots, \begin{pmatrix} x_1 & x_2 \cdots x_{n-1} & x_n \\ x_n & x_2 \cdots x_{n-1} & -x_1 \end{pmatrix},$$

each factor of which is similar to S (and hence is in $\mathfrak{R}_n$). Since T and R generate $\mathfrak{M}_n^+$, the theorem is proved.

COROLLARY 1. *In any automorphism of $\mathfrak{M}_n$, always $\mathfrak{M}_n^+ \to \mathfrak{M}_n^+$.*

Proof. For $n > 2$ this is an immediate corollary, since the commutator subgroup goes into itself in any automorphism. For $n = 2$, let $S \to S_1$ and

[1] L. K. Hua and I. Reiner, Trans. Amer. Math. Soc. vol. 65 (1949) p. 423.

$T \to T_1$. Then $ST \in \mathfrak{N}_2$ implies $S_1T_1 \in \mathfrak{N}_2$, so $\det(S_1T_1) = 1$. Further, $S^2 = -I$ implies $S_1^2 = -I$, so $\det S_1 = 1$, since the minimum function of S_1 is x^2+1, and the characteristic function must therefore be a power of x^2+1. This completes the proof when $n = 2$.

2. **Automorphisms of $\mathfrak{M}_2^+$.** We wish to determine the automorphisms of $\mathfrak{M}_2$. Since every automorphism of $\mathfrak{M}_2$ takes $\mathfrak{M}_2^+$ into itself, we shall first determine all automorphisms of $\mathfrak{M}_2^+$. For $X \in \mathfrak{M}_2^+$, define $\epsilon(X) = +1$ or -1, according as X is even or odd.

THEOREM 2. *Every automorphism of $\mathfrak{M}_2^+$ is of one of the forms*

$$X \in \mathfrak{M}_2^+ \to AXA^{-1} \qquad A \in \mathfrak{M}_2 \tag{I}$$

or

$$X \in \mathfrak{M}_2^+ \to \epsilon(X) \cdot AXA^{-1}, \qquad A \in \mathfrak{M}_2. \tag{II}$$

That is, the automorphism group of $\mathfrak{M}_2^+$ is generated by the set of "inner" automorphisms $X \to AXA^{-1}$ $(A \in \mathfrak{M}_2)$ and the automorphism $X \to \epsilon(X) \cdot X$.

Proof. Let τ be an automorphism of $\mathfrak{M}_2^+$; it certainly leaves $I^{(2)}$ and $-I^{(2)}$ individually unaltered. Let S and T (as given by (1)) be mapped into S^τ and T^τ. Then $(S^\tau)^2 = -I$. Since all second order fixed points are equivalent, there exists a matrix $B \in \mathfrak{M}_2$ such that $BS^\tau B^{-1} = S$. Instead of τ, consider the automorphism τ': $X \to BX^\tau B^{-1}$, which leaves S unaltered. Assume hereafter that τ leaves S invariant. (It is this sort of replacement of τ by τ' which we shall mean when we refer to some property holding "after a suitable inner automorphism.") Set

$$T^\tau = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

From $(ST)^3 = I$ we obtain $(ST^\tau)^3 = I$, whence $b - c = 1$. Since $\det T^\tau = 1$, we get

$$ad = 1 + bc = c^2 + c + 1 > 0.$$

Set $N = |a+d|$. If $N \geqq 3$, consider the elements generated by S and T^τ (mod N). Since $a+d \equiv 0 \pmod N$, we find that $(T^\tau)^2 \equiv I \pmod N$. Furthermore $(ST^\tau)^3 \equiv I \pmod N$; therefore S and T^τ generate (mod N) at most the 12 elements

$$\pm I, \ \pm S, \ \pm T^\tau, \ \pm ST^\tau, \ \pm T^\tau S, \ \pm ST^\tau S.$$

But if τ is an automorphism, S and T^τ generate $\mathfrak{M}_2^+$, which has more than 12 elements (mod N) for $N \geqq 3$.

Therefore $N \leqq 2$. Since $ad > 0$, either $a = d = 1$ or $a = d = -1$, and thence $b = 1$, $c = 0$ or $b = 0$, $c = -1$. There are 4 possibilities for T^τ:

$$T^\tau = \begin{cases} T_0 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, & T_2 = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}, \\ T_1 = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}, & T_3 = \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix}. \end{cases}$$

Since S and T generate $\mathfrak{M}_2^+$, to determine τ it is sufficient to specify S^τ and T^τ. Thus every automorphism of $\mathfrak{M}_2^+$ is of the form $S \to BSB^{-1}$, $T \to BT_iB^{-1}$ (for some i, $i = 0, 1, 2, 3$), where $B \in \mathfrak{M}_2$. If J is given by (2), we have:

$$T_0 = T, \quad T_1 = STS^{-1}, \quad T_2 = -JTJ^{-1}, \quad T_3 = -SJTJ^{-1}S^{-1},$$

and also $S = -JSJ^{-1}$. The possible automorphisms are:

$i = 0$: $S \to BSB^{-1}$, $T \to BTB^{-1}$.

$i = 1$: $S \to BS \cdot S \cdot S^{-1}B^{-1}$, $T \to BS \cdot T \cdot S^{-1}B^{-1}$.

$i = 2$: $S \to -BJ \cdot S \cdot J^{-1}B^{-1}$, $T \to -BJ \cdot T \cdot J^{-1}B^{-1}$.

$i = 3$: $S \to -BSJ \cdot S \cdot J^{-1}S^{-1}B^{-1}$, $T \to -BSJ \cdot T \cdot J^{-1}S^{-1}B^{-1}$.

These automorphisms are of two types: for $i = 0$ and 1, $S \to ASA^{-1}$, $T \to ATA^{-1}$, which imply that $X \in \mathfrak{M}_2^+ \to AXA^{-1}$; for $i = 2$ and 3, $S \to -ASA^{-1}$, $T \to -ATA^{-1}$, which imply that $X \in \mathfrak{M}_2^+ \to \epsilon(X) \cdot AXA^{-1}$. This completes the proof.

3. **Automorphisms of $\mathfrak{M}_n^+$ and $\mathfrak{M}_n$.** We are now faced with the problem of determining the automorphisms of $\mathfrak{M}_2$ from those of $\mathfrak{M}_2^+$. We shall have the same problem for $\mathfrak{M}_n$ and $\mathfrak{M}_n^+$. As we shall see, the passage from $\mathfrak{M}_n^+$ to $\mathfrak{M}_n$ is trivial, and most of the difficulty lies in determining the automorphisms of $\mathfrak{M}_n^+$. In this paper we shall prove the following results:

THEOREM 3. *For $n > 2$, the group of those automorphisms of $\mathfrak{M}_n^+$ which are induced by automorphisms of $\mathfrak{M}_n$ is generated by*

(i) *the set of all "inner" automorphisms*

$$X \in \mathfrak{M}_n^+ \to AXA^{-1} \qquad (A \in \mathfrak{M}_n),$$

and

(ii) *the automorphism*

$$X \in \mathfrak{M}_n^+ \to X'^{-1}.$$

REMARK. When $n = 2$, the automorphism (ii) is the same as $X \to SXS^{-1}$, hence is included in (i). The automorphism $X \to \epsilon(X) \cdot X$ occurs only for $n = 2$. Furthermore, for odd n all automorphisms of $\mathfrak{M}_n^+$ are induced by automorphisms of $\mathfrak{M}_n$.

THEOREM 4. *The generators of $\mathfrak{A}_n$ are*

(i) *the set of all inner automorphisms*

$$X \in \mathfrak{M}_n \to AXA^{-1} \qquad (A \in \mathfrak{M}_n),$$

(ii) *the automorphism* $X \in \mathfrak{M}_n \to X'^{-1}$,

(iii) *for even n only, the automorphism*

$$X \in \mathfrak{M}_n \to (\det X) \cdot X,$$

and

(iv) *for* $n=2$ *only, the automorphism*

$$X \in \mathfrak{M}_2^+ \to \epsilon(X) \cdot X, \qquad X \in \mathfrak{M}_2^- \to \epsilon(JX) \cdot X,$$

where J is given by (2).

Further, when $n=2$, *the automorphism* (ii) *may be omitted from this list.*

Let us show that Theorem 4 is a simple consequence of Theorem 3. Let τ be any automorphism of $\mathfrak{M}_n$. By Corollary 1, τ induces an automorphism on $\mathfrak{M}_n^+$ which, by Theorems 2 and 3, can be written as:

$$X \in \mathfrak{M}_n^+ \to \alpha(X) \cdot AX^*A^{-1},$$

where $A \in \mathfrak{M}_n$, $\alpha(X)=1$ for all X or $\alpha(X)=\epsilon(X)$ for all X (this can occur only when $n=2$), and where either $X^*=X$ for all X or $X^*=X'^{-1}$ for all X.

Let Y and $Z \in \mathfrak{M}_n^-$; then

$$Y^\tau Z^\tau = (YZ)^\tau = \alpha(YZ) \cdot A(YZ)^*A^{-1},$$

whence

$$Y^\tau = \alpha(YZ) \cdot AY^*Z^*A^{-1}(Z^\tau)^{-1}.$$

Let $Z \in \mathfrak{M}_n^-$ be fixed; then

$$Y^\tau = \alpha(YZ) \cdot AY^*B \qquad \text{for all } Y \in \mathfrak{M}_n^-,$$

where A and B are independent of Y. But then

$$AY^*B \cdot AY^*B = (Y^\tau)^2 = (Y^2)^\tau = \alpha(Y^2)A(Y^2)^*A^{-1},$$

so that

$$(BA)Y^*(BA) = \alpha(Y^2)Y^*.$$

Since this is valid for all $Y \in \mathfrak{M}_n^-$, we see that of necessity $\alpha(Y^2)=1$ for all Y, and $BA = \pm I$. This shows that either $Y^\tau = \alpha(YZ) \cdot AY^*A^{-1}$ for all $Y \in \mathfrak{M}_n^-$, or $Y^\tau = -\alpha(YZ) \cdot AY^*A^{-1}$ for all $Y \in \mathfrak{M}_n^-$. If $n=2$ and $\alpha(YZ)=\epsilon(YZ)$, it is trivial to verify that either $\epsilon(YZ)=\epsilon(JY)$ for all $Y \in \mathfrak{M}_2^-$ or $\epsilon(YZ) = -\epsilon(JY)$ for all $Y \in \mathfrak{M}_2^-$.

The remainder of the paper will be concerned with proving Theorem 3.

4. **Canonical forms for involutions.** In the proof of Theorem 3 we shall use certain canonical forms of involutions under similarity transformations.

LEMMA 1. *Under a similarity transformation, every involution* $X \in \mathfrak{M}_n$ *such*

that $X^2=I^{(n)}$ can be brought into the form

$$W(x, y, z) = \underbrace{L \dotplus \cdots \dotplus L}_{(x \text{ terms})} \dotplus (-I)^{(y)} \dotplus I^{(z)}, \tag{4}$$

where $2x+y+z=n$ and

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

Proof. We prove first, by induction on n, that every $X \in \mathfrak{M}_n$ satisfying $X^2=I$ is similar to a matrix of the form

$$\begin{pmatrix} I^{(l)} & 0 \\ M & -I^{(n-l)} \end{pmatrix}. \tag{5}$$

For $n=1$ and 2, this is trivial. Let the theorem be proved for n, and assume that $X^2=I^{(n+1)}$, where $n \geqq 2$. Then $X^2-I=0$, or $(X-I)(X+I)=0$. If $X-I$ is nonsingular, then $X=-I$ and the result is obvious. Hence, supposing that $X-I$ is singular (so that $\lambda=1$ is a characteristic root of X), there exists a primitive column vector $\mathfrak{t}=(t_1, \cdots, t_{n+1})'$ with integral elements such that $\mathfrak{t}'X=\mathfrak{t}'$. Choose $P \in \mathfrak{M}_{n+1}$ with first row $\mathfrak{t}'$. Then

$$PXP^{-1} = \begin{pmatrix} 1 & \mathfrak{n}' \\ \mathfrak{x} & X_1 \end{pmatrix},$$

where $\mathfrak{n}$ denotes a vector whose components are 0; thus

$$X \overset{s}{=} \begin{pmatrix} 1 & \mathfrak{n}' \\ \mathfrak{x} & X_1 \end{pmatrix}.$$

But

$$I^{(n+1)} = X^2 \overset{s}{=} \begin{pmatrix} 1 & \mathfrak{n}' \\ (I + X_1)\mathfrak{x} & X_1^2 \end{pmatrix}$$

shows that $X_1^2=I^{(n)}$ and $(I+X_1)\mathfrak{x}=\mathfrak{n}$. By the induction hypothesis,

$$X_1 \overset{s}{=} \begin{pmatrix} I^{(m)} & 0 \\ M & -I^{(n-m)} \end{pmatrix},$$

and, after making the similarity transformation, we have (as a consequence of $(I+X_1)\mathfrak{x}=\mathfrak{n}$)

$$\begin{pmatrix} 2I^{(m)} & 0 \\ \mathfrak{x}_1 M & 0 \end{pmatrix} \mathfrak{x} = \mathfrak{n}.$$

Therefore

$$\mathfrak{x} = (\underbrace{0, \cdots, 0}_{(m \text{ terms})}, \underbrace{*, \cdots, *}_{(n-m \text{ terms})})',$$

where * denotes an arbitrary element. Thus

$$X \overset{s}{=} \begin{pmatrix} 1 & & \mathfrak{n}' & \\ 0 & & & \\ \cdot & & & \\ \cdot & I^{(m)} & & 0 \\ \cdot & & & \\ 0 & & & \\ * & & & \\ \cdot & & & \\ \cdot & M & & -I^{(n-m)} \\ \cdot & & & \\ * & & & \end{pmatrix} = \begin{pmatrix} I^{(m+1)} & 0 \\ \overline{M} & -I^{(n-m)} \end{pmatrix}.$$

This completes the first part of the proof.

Suppose we now subject (5) to a further similarity transformation by

$$\begin{pmatrix} A^{(l)} & 0 \\ C & D^{(n-l)} \end{pmatrix} \in \mathfrak{M}_n.$$

A simple calculation shows that we obtain a matrix given by (5) with M replaced by $\overline{M}$, where $\overline{M} = 2CA^{-1} + DMA^{-1}$. Choosing firstly $C = 0$, A and D unimodular, we find that $\overline{M} = DMA^{-1}$, and by proper choice of A and D we can make $\overline{M}$ diagonal. Supposing this done, secondly put $A = I$, $D = I$; we find that $\overline{M} = M + 2C$. Since C is arbitrary, we can bring $\overline{M}$ into the form

$$\begin{pmatrix} I^{(k)} & 0 \\ 0 & 0 \end{pmatrix},$$

where k is the rank of M. Since we can interchange two rows and simultaneously interchange the corresponding columns by means of a similarity transformation, the lemma follows.

It is easily seen that

$$W(x, y, z) \overset{s}{=} W(\bar{x}, \bar{y}, \bar{z})$$

only when $x = \bar{x}$, $y = \bar{y}$, and $z = \bar{z}$. Furthermore, changing the order of terms in the direct summation does not alter the similarity class. The number A_n of nonsimilar involutions in $\mathfrak{M}_n$ is therefore equal to the number of solutions of $2x + y + z = n$, $x \geqq 0$, $y \geqq 0$, $z \geqq 0$. This gives

$$A_n = \begin{cases} \left(\dfrac{n+2}{2}\right)^2, & n \text{ even}, \\ \dfrac{(n+1)(n+3)}{4}, & n \text{ odd}. \end{cases} \tag{6}$$

Let B_n be the number of nonsimilar involutions in $\mathfrak{M}_n^+$, where the similarity factors are in $\mathfrak{M}_n$. One easily obtains

$$B_n = \begin{cases} (A_n - 1)/2, & \text{if } n \equiv 0 \pmod 4, \\ A_n/2, & \text{otherwise.} \end{cases} \tag{7}$$

5. **Automorphisms of $\mathfrak{M}_3^+$.** We shall now prove Theorem 3 for $n=3$. Let

$$I_1 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad I_2 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \in \mathfrak{M}_3^+.$$

Then $I_1^2 = I^{(3)}$. Let τ be any automorphism of $\mathfrak{M}_3^+$ and let $X = I_1^\tau$; then $X^2 = I^{(3)}$. By Lemma 1, the matrices I_1, I_2, and $I^{(3)}$ form a complete system of nonsimilar involutions in $\mathfrak{M}_3^+$. Therefore

$$X \overset{S}{=} I_1 \text{ or } I_2.$$

After a suitable inner automorphism, we may assume that either $I_1 \to I_1$ or $I_1 \to I_2$. We shall show that this latter case is impossible by considering the normalizer groups of I_1 and I_2. The normalizer group of I_1, that is, the group of matrices $\in \mathfrak{M}_3^+$ which commute with I_1, consists of all elements of $\mathfrak{M}_3^+$ of the form

$$\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & e \end{pmatrix},$$

and is isomorphic to $\mathfrak{M}_2$. That of I_2 consists of all elements of $\mathfrak{M}_3^+$ of the form

$$\begin{pmatrix} a & 0 & 0 \\ (a-e)/2 & e & f \\ -h/2 & h & i \end{pmatrix},$$

and is isomorphic to that subgroup $\mathfrak{G}$ of $\mathfrak{M}_2$ consisting of the elements

$$\begin{pmatrix} e & f \\ h & i \end{pmatrix} \in \mathfrak{M}_2, \qquad \text{where } \left.\begin{matrix} e \equiv 1 \\ h \equiv 0 \\ i \equiv 1 \end{matrix}\right\} \pmod 2.$$

Since e and i are both odd, $\mathfrak{G}$ contains no element of order 3, and hence is not isomorphic to $\mathfrak{M}_2$. But then $I_1 \to I_2$ is impossible.

We may assume thus that after a suitable inner automorphism, I_1 is invariant. Thence elements of $\mathfrak{M}_3^+$ which commute with I_1 map into elements of the same kind, so that

$$\begin{pmatrix} X & \mathfrak{n}' \\ \mathfrak{n} & \pm 1 \end{pmatrix} \in \mathfrak{M}_3^+ \to \begin{pmatrix} X^\tau & \mathfrak{n}' \\ \mathfrak{n} & \pm 1 \end{pmatrix}.$$

Since this induces an automorphism $X \to X^\tau$ on $\mathfrak{M}_2$, we see that $\det X^\tau = \det X$, and hence the plus signs go together, and so do the minus signs. By Theorem 2 and that part of Theorem 4 which follows from Theorem 2, there exists a matrix $A \in \mathfrak{M}_2$ such that $X^\tau = \pm AXA^{-1}$; here, the plus sign certainly occurs when X is an even element of $\mathfrak{M}_2^+$, and if the minus sign occurs for one odd element of $\mathfrak{M}_2^+$, then it occurs for *every* odd element of $\mathfrak{M}_2^+$. By use of a further inner automorphism using the factor $A^{-1} \dot{+} I^{(1)}$, we may assume that

$$\begin{pmatrix} X & \mathfrak{n}' \\ \mathfrak{n} & \pm 1 \end{pmatrix} \in \mathfrak{M}_3^+ \to \begin{pmatrix} \pm X & \mathfrak{n}' \\ \mathfrak{n} & \pm 1 \end{pmatrix}, \tag{8}$$

so that

$$M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \to M \quad \text{or} \quad M \to N = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Since

$$N = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot M \cdot \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

we may assume (after a further inner automorphism, if necessary) that I_1, M, and N are all invariant under the automorphism (but (8) need not hold).

Thus, after a suitably chosen inner automorphism, we have I_1, M, and N invariant. Therefore there exist A, B, and $C \in \mathfrak{M}_2$ such that

$$\begin{pmatrix} X & \mathfrak{n} \\ \mathfrak{n}' & \pm 1 \end{pmatrix} \in \mathfrak{M}_3^+ \to \begin{pmatrix} \pm AXA^{-1} & \mathfrak{n} \\ \mathfrak{n}' & \pm 1 \end{pmatrix},$$

$$\begin{pmatrix} \pm 1 & \mathfrak{n}' \\ \mathfrak{n} & X \end{pmatrix} \in \mathfrak{M}_3^+ \to \begin{pmatrix} \pm 1 & \mathfrak{n}' \\ \mathfrak{n} & \pm BXB^{-1} \end{pmatrix}, \tag{9}$$

$$\begin{pmatrix} a & 0 & b \\ 0 & \pm 1 & 0 \\ c & 0 & d \end{pmatrix} \in \mathfrak{M}_3^+ \to \begin{pmatrix} \alpha & 0 & \beta \\ 0 & \pm 1 & 0 \\ \gamma & 0 & \delta \end{pmatrix},$$

where

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \pm C \begin{pmatrix} a & b \\ c & d \end{pmatrix} C^{-1},$$

and $\mathfrak{n} = (0, 0)'$. Here, the $+1$ on the left goes with the $+1$ on the right al-

ways (and the -1's go together); further, when X is an even element of $\mathfrak{M}_2^+$, the plus sign occurs before AXA^{-1}, BXB^{-1}, and CXC^{-1}, while if the minus sign occurs before one of these for any odd $X\in\mathfrak{M}_2^+$, it occurs there for every odd $X\in\mathfrak{M}_2^+$.

Now we may assume that at most one of A, B, and C has determinant -1; for if both A and B (say) have determinant -1, apply a further inner automorphism (with factor N) which leaves I_1, M, and N invariant and changes the signs of det A and det B. Suppose hereafter, without loss of generality, that det $A=$det $B=1$.

Next, N is invariant, but by (9) goes into

$$\begin{pmatrix} \pm A\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}A^{-1} & \mathfrak{n}' \\ \mathfrak{n} & -1 \end{pmatrix},$$

so that

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

This gives two possibilities:

$$A = I^{(2)} \quad \text{or} \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

The same holds true for B (but not necessarily for C, since det $C=\pm 1$).

Suppose firstly that either A or B is $I^{(2)}$, say $A=I^{(2)}$. Then

$$T = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} \pm\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} & 0 \\ 0 \quad 0 & 1 \end{pmatrix}.$$

Case 1. T invariant. Then

$$\begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

are both invariant. (The first matrix is invariant in virtue of the remarks after (9); the second is invariant because it is M times the first.) For either possible choice of B we find that

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

Therefore

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

is mapped into

$$\begin{pmatrix}-1&0&0\\0&-1&0\\0&0&1\end{pmatrix}\begin{pmatrix}-1&0&0\\0&\pm\begin{pmatrix}0&1\\1&0\end{pmatrix}\end{pmatrix}\begin{pmatrix}0&1&0\\1&0&0\\0&0&-1\end{pmatrix}=\begin{cases}U, & \text{if } + \text{ is used,}\\ V, & \text{if } - \text{ is used,}\end{cases}$$

where $V=I_1UI_1^{-1}$. Thus, in this case, $T\to T=I_1TI_1^{-1}$, and either $U\to U$ or $U\to I_1UI_1^{-1}$. Since T and U generate(2) $\mathfrak{M}_3^+$, the automorphism is inner.

Case 2.

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

Then

$$\begin{pmatrix}0&1&0\\1&0&0\\0&0&-1\end{pmatrix}\to\begin{pmatrix}0&-1&0\\-1&0&0\\0&0&-1\end{pmatrix},$$

and one finds in this case that

$$U\to\begin{pmatrix}0&-1&0\\0&0&1\\-1&0&0\end{pmatrix}\quad\text{or}\quad\begin{pmatrix}0&-1&0\\0&0&-1\\1&0&0\end{pmatrix}.$$

If we set $Z=TU^2$, then

$$\begin{pmatrix}1&0&0\\1&1&0\\0&0&1\end{pmatrix}=(UZ^{-1})^2UZ^2. \tag{10}$$

Now certainly the left side of (10) maps into

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

(2) L. K. Hua and I. Reiner, loc. cit.

whereas, knowing T^τ and U^τ, we can compute Z^τ and thence can find the image of the right side of (10). We readily find (for either value of U^τ) that the right side of (10) maps into

$$\begin{pmatrix} 1 & \cdot & \cdot \\ 3 & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{pmatrix},$$

and hence we have a contradiction.

Therefore case 2 cannot occur, and so if either A or B equals $I^{(2)}$, the automorphism is inner. Suppose hereafter that

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

In this case we have

$$T \to \begin{pmatrix} \pm \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} & \begin{matrix} 0 \\ 0 \end{matrix} \\ \begin{matrix} 0 & 0 \end{matrix} & 1 \end{pmatrix}.$$

Case 1*.

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

Then as before

$$\begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

are invariant, and again $U^\tau = U$ or V. After a further inner automorphism by a factor of I_1 (in the latter case) we also have $U \to U$. But then

$$T \to T'^{-1}, \qquad U \to U'^{-1}.$$

(This automorphism is easily shown to be a non-inner automorphism.)

Case 2*.

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

Then

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} \to \begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

and again we find that there are two possibilities for U^τ, each of which leads to a contradiction, just as in case 2. Therefore Theorem 3 holds when $n=3$.

6. **A fundamental lemma.** Theorem 3 will be proved by induction on n; the result has already been established for $n=2$ and 3. In going from $n-1$ to n, the following lemma is basic:

LEMMA 2. *Let $n \geqq 4$, and define $J_1 = (-1) \dotplus I^{(n-1)}$. In any automorphism τ of $\mathfrak{M}_n$, $J_1^\tau = \pm A J_1 A^{-1}$ for some $A \in \mathfrak{M}_n$.*

Proof. By Corollary 1, $J_1^\tau \in \mathfrak{M}_n^-$, and J_1^τ is an involution. After a suitable inner automorphism, we may assume that $J_1^\tau = W(x, y, z)$ (as defined by (4)), where $2x+y+z=n$ and $x+y$ is odd. Every element of $\mathfrak{M}_n$ which commutes with J_1 maps into an element of $\mathfrak{M}_n$ which commutes with W. Every matrix in $\mathfrak{M}_n^+$ maps into a matrix in $\mathfrak{M}_n^+$. Combining these facts, we see that the group $\mathfrak{G}_1$ consisting of those elements of $\mathfrak{M}_n^+$ which commute with J_1 is isomorphic to $\mathfrak{G}_2$, the corresponding group for W. If we prove that this can happen only for $x=0$, $y=1$, $z=n-1$ or $x=0$, $y=n-1$, $z=1$, the result will follow.

The group $\mathfrak{G}_1$ consists of the matrices in $\mathfrak{M}_n^+$ of the form $(\pm 1) \dotplus X_1$, $X_1 \in \mathfrak{M}_{n-1}$, and so clearly $\mathfrak{G}_1 \cong \mathfrak{M}_{n-1}$.

The group $\mathfrak{G}_2$ is easily found to consist of all matrices $C \in \mathfrak{M}_1^+$ of the form (we illustrate the case where $x=2$):

$$C = \begin{bmatrix} a_1 & 0 & a_2 & 0 & 0 \cdots 0 & 2\beta_1 \cdots 2\beta_z \\ \frac{a_1 - d_1}{2} & d_1 & \frac{a_2 - d_2}{2} & d_2 & \alpha_1 \cdots \alpha_y & \beta_1 \cdots \beta_z \\ a_3 & 0 & a_4 & 0 & 0 \cdots 0 & 2\delta_1 \cdots 2\delta_z \\ \frac{a_3 - d_3}{2} & d_3 & \frac{a_4 - d_4}{2} & d_4 & \gamma_1 \cdots \gamma_y & \delta_1 \cdots \delta_z \\ \epsilon_1 & -2\epsilon_1 & \zeta_1 & -2\zeta_1 & & \\ \vdots & \vdots & \vdots & \vdots & U & 0 \\ \epsilon_y & -2\epsilon_y & \zeta_y & -2\zeta_y & & \\ \eta_1 & 0 & \theta_1 & 0 & & \\ \vdots & \vdots & \vdots & \vdots & 0 & V \\ \eta_z & 0 & \theta_z & 0 & & \end{bmatrix} \begin{matrix} \\ \\ 2x \text{ rows} \\ \\ \\ y \text{ rows} \\ \\ z \text{ rows} \end{matrix}$$

$$\begin{matrix} & 2x \text{ columns} & & & y \text{ columns} & z \text{ columns} \end{matrix}$$

For the moment put

$$K = \begin{pmatrix} 1 & 0 \\ -1/2 & 1 \end{pmatrix} \dotplus \cdots \dotplus \underset{(x \text{ terms})}{\begin{pmatrix} 1 & 0 \\ -1/2 & 1 \end{pmatrix}} \dotplus I^{(n-2x)}.$$

Then a simple calculation gives:

$$KCK^{-1} = \begin{bmatrix} a_1 & 0 & a_2 & 0 & 0 \cdots 0 & 2\beta_1 \cdots 2\beta_z \\ 0 & d_1 & 0 & d_2 & \alpha_1 \cdots \alpha_y & 0 \cdots 0 \\ a_3 & 0 & a_4 & 0 & 0 \cdots 0 & 2\delta_1 \cdots 2\delta_z \\ 0 & d_3 & 0 & d_4 & \gamma_1 \cdots \gamma_y & 0 \cdots 0 \\ 0 & -2\epsilon_1 & 0 & -2\zeta_1 & & \\ \vdots & \vdots & \vdots & \vdots & U & 0 \\ 0 & -2\epsilon_y & 0 & -2\zeta_y & & \\ \eta_1 & 0 & \theta_1 & 0 & & \\ \vdots & \vdots & \vdots & \vdots & 0 & V \\ \eta_z & 0 & \theta_z & 0 & & \end{bmatrix}$$

and so C is similar to

$$\begin{bmatrix} a_1 & a_2 & 2\beta_1 \cdots 2\beta_z \\ a_3 & a_4 & 2\delta_1 \cdots 2\delta_z \\ \eta_1 & \theta_1 & \\ \vdots & \vdots & V \\ \eta_z & \theta_z & \end{bmatrix} \dotplus \begin{bmatrix} d_1 & d_2 & \alpha_1 \cdots \alpha_y \\ d_3 & d_4 & \gamma_1 \cdots \gamma_y \\ -2\epsilon_1 & -2\zeta_1 & \\ \vdots & \vdots & U \\ -2\epsilon_y & -2\zeta_y & \end{bmatrix}$$

$$= \underset{x \quad z}{\begin{bmatrix} S_1 & 2R_1 \\ Q_1 & T_1 \end{bmatrix}}\begin{matrix} x \\ z \end{matrix} \dotplus \underset{x \quad y}{\begin{bmatrix} S_2 & Q_2 \\ 2R_2 & T_2 \end{bmatrix}}\begin{matrix} x \\ y \end{matrix},$$

with a fixed similarity factor depending only on W. Therefore $\mathfrak{G}_2 \cong \mathfrak{G}$, where $\mathfrak{G} = \mathfrak{G}(x, y, z)$ is the group of matrices in $\mathfrak{M}_n^+$ of the form

$$\underset{x \quad z}{\begin{bmatrix} S_1 & 2R_1 \\ Q_1 & T_1 \end{bmatrix}}\begin{matrix} x \\ z \end{matrix} + \underset{x \quad y}{\begin{bmatrix} S_2 & Q_2 \\ 2R_2 & T_2 \end{bmatrix}}\begin{matrix} x \\ y \end{matrix},$$

where $S_1 \equiv S_2 \pmod 2$. Here $2x+y+z=n$ and $x+y$ is odd.

We wish to prove that $\mathfrak{M}_{n-1} \cong \mathfrak{G}(x, y, z)$ only when $x=0$, $y=1$, $z=n-1$ or $x=0$, $y=n-1$, $z=1$. In order to establish this, we shall prove that in all other cases the number of involutions in $\mathfrak{G}$ which are nonsimilar in $\mathfrak{G}$ is greater than the number of involutions in $\mathfrak{M}_{n-1}$ which are nonsimilar in $\mathfrak{M}_{n-1}$;

this latter number is, of course, A_{n-1} (given by (6)).

We shall briefly denote the elements of $\mathfrak{G}$ by $A \dotplus B$, where

$$A = \begin{pmatrix} S_1 & 2R_1 \\ Q_1 & T_1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} S_2 & Q_2 \\ 2R_2 & T_2 \end{pmatrix}.$$

If $A_1 \dotplus B_1$ and $A_2 \dotplus B_2$ are two involutions in $\mathfrak{G}$, where either

$$A_1 \overset{s}{\neq} A_2$$

in $\mathfrak{M}_{x+z}$ or

$$B_1 \overset{s}{\neq} B_2$$

in $\mathfrak{M}_{x+y}$, then certainly

$$A_1 \dotplus B_1 \overset{s}{\neq} A_2 \dotplus B_2$$

in $\mathfrak{G}$ (these may be similar in $\mathfrak{M}_n$, however). Therefore, the matrices $A \dotplus B$, where

$$A = I^{(a_1)} \dotplus (-I)^{(b_1)} \dotplus L \dotplus \cdots \dotplus L \quad (c_1 \text{ terms}),$$

$$B = I^{(a_2)} \dotplus (-I)^{(b_2)} \dotplus L \dotplus \cdots \dotplus L \quad (c_2 \text{ terms}),$$

obtained by taking different sets of values of $(a_1, b_1, c_1, a_2, b_2, c_2)$, if they lie in $\mathfrak{G}$, are certainly nonsimilar in $\mathfrak{G}$. Here we have

$$a_1 + b_1 + 2c_1 = x + z, \quad a_2 + b_2 + 2c_2 = x + y, \quad b_1 + b_2 + c_1 + c_2 \text{ even}.$$

If $x \neq 0$, we impose the further restriction that $c_1 \leqq (z+1)/2$, $c_2 \leqq (y+1)/2$, and that in B instead of L we use L'. These conditions will insure that $A \dotplus B \in \mathfrak{G}$. We certainly do not (in general) get all of the nonsimilar involutions of $\mathfrak{G}$ in this way, but instead we obtain only a subset thereof. Call the number of such matrices N.

For $x=0$, we have $N = B_y B_z + (A_y - B_y)(A_z - B_z)$. Since y is odd, $A_y = 2B_y$, and therefore

$$N = B_y A_z = B_y A_{n-y}.$$

Case 1. n even. Then $N=(y+1)(y+3)(n-y+1)(n-y+3)/32$. If neither y nor $n-y$ is 1 (certainly neither can be zero), then

$$(y + 1)(n - y + 1) \geqq 4(n - 2) \quad \text{and} \quad (y + 3)(n - y + 3) \geqq 6n,$$

so that

$$N \geqq (24/32)\, n(n - 2).$$

For $n=4$, $x=0$, either $y=1$ or $z=1$. For $n \geqq 6$, we have $N > A_{n-1}$. Hence in

this case $\mathfrak{G}$ is not isomorphic to $\mathfrak{M}_{n-1}$. (If either y or $n-y=1$, then $W(x, y, z) = \pm J_1$.)

Case 2. n odd. Then $N=(y+1)(y+3)(n-y+2)^2/32$. We find again that $N>A_{n-1}$ for $n\geqq 5$.

This settles the cases where $x=0$. Suppose that $x\neq 0$ hereafter. Then N is the number of solutions of

$$a_1 + b_1 + 2c_1 = x + z, \quad a_2 + b_2 + 2c_2 = x + y, \quad b_1 + b_2 + c_1 + c_2 \text{ even},$$

$$0 \leqq c_1 \leqq \frac{z+1}{2}, \qquad 0 \leqq c_2 \leqq \frac{y+1}{2}.$$

Using $[r]$ to denote the greatest integer less than or equal to r, we readily find that N is given by

$$\frac{1}{2}\left[\frac{z+3}{2}\right]\left[\frac{y+3}{2}\right]\left(x+z+1-\left[\frac{z+1}{2}\right]\right)\left(x+y+1-\left[\frac{y+1}{2}\right]\right).$$

By considering separately the cases where y and z are both even, one even and one odd, and so on, it is easy to prove that $N\geqq A_{n-1}$ in all cases except when both y and z are zero. Leaving aside this case for the moment, consider the matrix $A_0+I^{(x+y)}\in\mathfrak{G}$, where $A_0\in\mathfrak{M}_{x+z}$ is given by

$$A_0 = \begin{pmatrix} 1 & 2 & 2\cdots & 2 \\ 0 & -1 & 0\cdots & 0 \\ 0 & 0 & -1\cdots & 0 \\ \cdot & \cdot & \cdots\cdot & \cdot \\ 0 & 0 & 0\cdots & -1 \end{pmatrix}.$$

The matrix $A_0+I^{(x+y)}$ is certainly an involution in $\mathfrak{G}$. Since, in $\mathfrak{M}_{x+z}$,

$$A_0 \overset{s}{=} \begin{pmatrix} 1 & 0\cdots & 0 \\ 0 & -1\cdots & 0 \\ \cdot & \cdots\cdot & \cdot \\ 0 & 0\cdots & -1 \end{pmatrix} = A_1,$$

$A_0+I^{(x+y)}$ can be similar (in $\mathfrak{G}$) only to that matrix (counted in the N matrices) of the form $A_1+I^{(x+y)}$. But from

$$A_1\cdot\begin{pmatrix} a_1 & a_2\cdots a_x & 2b_1\cdots 2b_z \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot \end{pmatrix} = \begin{pmatrix} a_1 & a_2\cdots a_x & 2b_1\cdots 2b_z \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot \end{pmatrix}\cdot A_0$$

we obtain

$$a_1 = a_2 = \cdots = a_x = 2b_1,$$

which is impossible. Hence $\mathfrak{G}$ contains at least $N+1$ nonsimilar involutions, and therefore $\mathfrak{G}$ is not isomorphic to $\mathfrak{M}_{n-1}$ in these cases.

We have left only the case $y=z=0$, $x=n/2$; then n is singly even. Here we may choose $A=W(c_1, b_1, a_1)$, $B=W(c_1, b_2, a_2)$, where

$$a_1 + b_1 + 2c_1 = x, \qquad a_2 + b_2 + 2c_1 = x, \qquad b_1 + b_2 \text{ even}.$$

Then $A+B\in\mathfrak{G}$, and the various matrices are nonsimilar. The number of such matrices is $(x+1)(x+2)(x+3)/12$, which is greater than A_{n-1} for $n\geqq 14$. For $n=6$, $\mathfrak{M}_{n-1}$ contains an element of order 5, while $\mathfrak{G}$ does not. For $n=10$, $\mathfrak{M}_{n-1}$ contains an element of order 7, while $\mathfrak{G}$ does not. This completes the proof of the lemma.

7. **Proof of Theorem 3.** We are now ready to give a proof of Theorem 3 by induction on n. Hereafter, let $n\geqq 4$ and suppose that Theorem 3 holds for $n-1$. If τ is any automorphism of $\mathfrak{M}_n$, by Corollary 1 and Lemma 2 we know that τ takes $\mathfrak{M}_n^+$ into itself, and $J_1^\tau = \pm A J_1 A^{-1}$. If we change τ by a suitable inner automorphism, then we may assume that $J_1\to\pm J_1$. When n is odd, certainly $J_1\to J_1$; when n is even, by multiplying τ by the automorphism $X\in\mathfrak{M}_n\to(\det X)\cdot X$ if necessary, we may again assume $J_1\to J_1$.

Therefore, every $M\in\mathfrak{M}_n^+$ which commutes with J_1 goes into another such element, that is,

$$\begin{pmatrix} \pm 1 & \mathfrak{n}' \\ \mathfrak{n} & X \end{pmatrix}^\tau = \begin{pmatrix} \pm 1 & \mathfrak{n}' \\ \mathfrak{n} & X^\tau \end{pmatrix}.$$

Since this induces an automorphism on $\mathfrak{M}_{n-1}$, we have $\det X^\tau = \det X$, so that the plus signs go together, as do the minus signs. Furthermore, by our induction hypothesis,

$$X^\tau = \pm AX^*A^{-1},$$

where $A\in\mathfrak{M}_{n-1}$ and either $X^*=X$ for all $X\in\mathfrak{M}_{n-1}$ or $X^*=X'^{-1}$ for all $X\in\mathfrak{M}_{n-1}$; here the minus sign can occur only for $X\in\mathfrak{M}_{n-1}^-$, and if it occurs for one such X, it occurs for all $X\in\mathfrak{M}_{n-1}^-$. After changing our original automorphism by a factor of $I^{(1)}+A^{-1}$, we may assume that $X^\tau = \pm X^*$.

Let J_ν be obtained from $I^{(n)}$ by replacing the νth diagonal element by -1. Then

$$J_1 J_n = \begin{pmatrix} -1 & 0\cdots 0 & 0 \\ 0 & 1\cdots 0 & 0 \\ \cdot & \cdots\cdots & \cdot \\ 0 & 0\cdots 1 & 0 \\ 0 & 0\cdots 0 & -1 \end{pmatrix} \to \begin{pmatrix} -1 & & \mathfrak{n}' & \\ & \mathfrak{n} \pm & \begin{pmatrix} 1\cdots 0 & 0 \\ \cdots 0 & 0 \\ 0\cdots 1 & 0 \\ 0\cdots 0 & -1 \end{pmatrix} & * \end{pmatrix}.$$

The minus sign here is impossible by Lemma 2, since $n \geqq 4$. Hence $J_1 J_n$ is invariant, and therefore so is J_n. By the same reasoning all of the J_ν $(\nu = 1, \cdots, n)$ are invariant.

From the above remarks we see that for $X \in \mathfrak{M}_{n-1}^+$,

$$\begin{pmatrix} 1 & \mathfrak{n}' \\ \mathfrak{n} & X \end{pmatrix}^\tau = \begin{pmatrix} 1 & \mathfrak{n}' \\ \mathfrak{n} & A_1 X^* A_1^{-1} \end{pmatrix}, \cdots, \begin{pmatrix} X & \mathfrak{n} \\ \mathfrak{n}' & 1 \end{pmatrix}^\tau = \begin{pmatrix} A_n X^* A_n^{-1} & \mathfrak{n} \\ \mathfrak{n}' & 1 \end{pmatrix},$$

where $A_\nu \in \mathfrak{M}_{n-1}$, and in fact $A_1 = I$. Now suppose that $Z \in \mathfrak{M}_{n-2}^+$, and form $I^{(2)} \dotplus Z$. Since it commutes with both J_1 and J_2, its image must do likewise. But then

$$A_1 \begin{pmatrix} 1 & \mathfrak{n}' \\ \mathfrak{n} & Z \end{pmatrix} A_1^{-1} = \begin{pmatrix} 1 & \mathfrak{n}' \\ \mathfrak{n} & \overline{Z} \end{pmatrix}$$

for every $Z \in \mathfrak{M}_{n-2}^+$. Setting

$$A_1 = \begin{pmatrix} a & \mathfrak{x}' \\ \mathfrak{y} & A \end{pmatrix}$$

we obtain $\mathfrak{x}' Z = \mathfrak{x}'$, $\mathfrak{y} = \overline{Z}\mathfrak{y}$. Since this holds for all $Z \in \mathfrak{M}_{n-2}^+$, we must have $\mathfrak{x} = \mathfrak{y} = \mathfrak{n}$, so that A_1 is itself decomposable. A similar argument (considering the matrices commuting with both J_1 and J_ν, for $\nu = 3, \cdots, n$) shows that A_1 is diagonal. Correspondingly, all of the A_ν are diagonal. It is further clear that all of the A_ν $(\nu = 1, \cdots, n)$ are sections of a single diagonal matrix $D^{(n)}$. Using the further inner automorphism factor D^{-1}, we may henceforth assume that $X^\tau = X^*$ for every decomposable $X \in \mathfrak{M}_n^+$, where either $X^* = X$ always or $X^* = X'^{-1}$ always. Since $\mathfrak{M}_n^+$ is generated by the set of decomposable elements of $\mathfrak{M}_n^+$, the theorem is proved.

TSING HUA UNIVERSITY,
PEKING, CHINA.
UNIVERSITY OF ILLINOIS,
URBANA, ILL.