AUTOMORPHISMS OF THE UNIMODULAR GROUP

BY

L. K. HUA AND I. REINER

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

\[
A = B
\]

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

1. The commutator subgroup of \( \mathcal{M}_n \). The following result is useful, and is of independent interest.

Theorem 1. Let \( \mathcal{R}_n \) be the commutator subgroup of \( \mathcal{M}_n \). Then trivially \( \mathcal{R}_n \subset \mathcal{M}_n^+ \). For \( n = 2 \), \( \mathcal{R}_n \) is of index 2 in \( \mathcal{M}_2^+ \), while for \( n > 2 \), \( \mathcal{R}_n = \mathcal{M}_n^+ \).

Proof. Consider first the case where \( n = 2 \). Define

\[
S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.
\]

It is well known that \( S \) and \( T \) generate \( \mathcal{M}_2^+ \). An element \( X \) of \( \mathcal{M}_2^+ \) 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

\[
S^2 = -I, \quad (ST)^3 = I,
\]

it follows that the parity of \( X \in \mathcal{M}_2^+ \) depends only on \( X \), and not on the manner in which \( X \) is expressed as a product of powers of \( S \) and \( T \), the sum of the exponents is even; otherwise, \( X \) is called odd. Since all relations satisfied by \( S \) and \( T \) are consequences of

\[
S^2 = -I, \quad (ST)^3 = I,
\]

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

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

\[
J = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},
\]

Presented to the Society, December 29, 1950; received by the editors January 8, 1951.
and $X$ and $Y \in \mathbb{M}_n^+$. Then $A^2 = XY = XJ^{-1}XJ$. Hence we need only prove that if $X \in \mathbb{M}_n^+$, $X$ and $J^{-1}XJ$ are of the same parity. This is easily verified for $X = S$ or $T$; since $S$ and $T$ generate $\mathbb{M}_n^+$, 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 $\mathbb{E} \subset \mathbb{R}_2$. For, $\mathbb{E}$ is generated by $T^2$ and $ST$, since $TS = (ST \cdot T^{-2})^2$. However, $T^2 = TJT^{-1}J^{-1} \in \mathbb{R}_2$, and therefore also $(T')^{-2} \in \mathbb{R}_2$. Furthermore, $ST = TST^{-1}(T')^{-2}T^2 \in \mathbb{R}_2$. This completes the proof for $n = 2$.

Suppose now that $n > 2$, and define

$$R = \begin{pmatrix} 0 & \cdots & 0 & (-1)^{n-1} \\ 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots \\ 0 & \cdots & 1 & 0 \end{pmatrix} \in \mathbb{M}_n^+, \quad S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + I^{(n-2)}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} + I^{(n-2)}.$$  

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

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

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

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

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

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

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

**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

Then \( ST \in \mathbb{R}_n \) implies \( S_1T_1 \in \mathbb{R}_n \), so \( \det (S_1T_1) = 1 \). Further, \( S^2 = -I \) implies \( S^2 = -I \), 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 \( \mathbb{M}_2^+ \). We wish to determine the automorphisms of \( \mathbb{M}_2 \). Since every automorphism of \( \mathbb{M}_2 \) takes \( \mathbb{M}_2^+ \) into itself, we shall first determine all automorphisms of \( \mathbb{M}_2^+ \). For \( X \in \mathbb{M}_2^+ \), define \( \epsilon(X) = +1 \) or \(-1\), according as \( X \) is even or odd.

**Theorem 2.** Every automorphism of \( \mathbb{M}_2^+ \) is of one of the forms

(I) \[ X \in \mathbb{M}_2^+ \rightarrow AXA^{-1}, \quad A \in \mathbb{M}_2 \]

or

(II) \[ X \in \mathbb{M}_2^+ \rightarrow \epsilon(X) \cdot AXA^{-1}, \quad A \in \mathbb{M}_2. \]

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

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

\[ T' = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \]

From \((ST)^3 = I\) we obtain \((ST')^3 = I\), whence \( b - c = 1 \). Since \( \det T' = 1 \), we get

\[ ad = 1 + bc = c^2 + c + 1 > 0. \]

Set \( N = |a + d| \). If \( N \geq 3 \), consider the elements generated by \( S \) and \( T' \) \((\mod N)\). Since \( a + d \equiv 0 \) \((\mod N)\), we find that \((T')^2 \equiv I \) \((\mod N)\). Furthermore \((ST')^3 \equiv I \) \((\mod N)\); therefore \( S \) and \( T' \) generate \((\mod N)\) at most the 12 elements

\[ \pm I, \pm S, \pm T', \pm ST', \pm T'S, \pm ST'S. \]

But if \( \tau \) is an automorphism, \( S \) and \( T' \) generate \( \mathbb{M}_2^+ \), which has more than 12 elements \((\mod N)\) for \( N \geq 3 \).

Therefore \( N \leq 2 \). 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 \( T' \):
Since \( S \) and \( T \) generate \( \mathbb{M}_n^+ \), to determine \( \tau \) it is sufficient to specify \( S^\tau \) and \( T^\tau \). Thus every automorphism of \( \mathbb{M}_n^+ \) is of the form \( S \to BSB^{-1}, T \to BTB^{-1} \) (for some \( i, i = 0, 1, 2, 3 \)), where \( B \in \mathbb{M}_n \). 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:

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

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

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

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

These automorphisms are of two types: for \( i = 0 \) and \( 1 \), \( S \to \alpha S \alpha^{-1}, T \to \alpha T \alpha^{-1} \), which imply that \( X \in \mathbb{M}_n^+ \to AXA^{-1} \); for \( i = 2 \) and \( 3 \), \( S \to -AS \alpha^{-1}, T \to -AT \alpha^{-1} \), which imply that \( X \in \mathbb{M}_n^+ \to e(X) \cdot AXA^{-1} \). This completes the proof.

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

**Theorem 3.** For \( n > 2 \), the group of those automorphisms of \( \mathbb{M}_n^+ \) which are induced by automorphisms of \( \mathbb{M}_n \) is generated by

(i) the set of all "inner" automorphisms

\[
X \in \mathbb{M}_n^+ \to AXA^{-1} \quad (A \in \mathbb{M}_n),
\]

and

(ii) the automorphism

\[
X \in \mathbb{M}_n^+ \to X'^{-1}.
\]

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

**Theorem 4.** The generators of \( \mathfrak{A}_n \) are

(i) the set of all inner automorphisms

\[
X \in \mathfrak{A}_n \to AXA^{-1} \quad (A \in \mathfrak{M}_n),
\]
(ii) the automorphism $X \in \mathbb{M}_n \to X^t$.
(iii) for even $n$ only, the automorphism

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

and

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

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

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 $\tau$ be any automorphism of $\mathbb{M}_n$. By Corollary 1, $\tau$ induces an automorphism on $\mathbb{M}_n^+$ which, by Theorems 2 and 3, can be written as:

$$X \in \mathbb{M}_n^+ \to \alpha(X) \cdot AXA^{-1},$$

where $A \in \mathbb{M}_n$, $\alpha(X) = 1$ 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 $Z \in \mathbb{M}_n$; then

$$YZ^r = (YZ)^r = \alpha(YZ) \cdot A(YZ)A^{-1},$$

whence

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

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

$$Y^r = \alpha(YZ) \cdot AY^*B$$

for all $Y \in \mathbb{M}_n^-$,

where $A$ and $B$ are independent of $Y$. But then

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

so that

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

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

\[
W(x, y, z) = L + \cdots + L + (-1)^{(y)} + I^{(z)},
\]

where \( 2x + y + z = n \) and

\[
L = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.
\]

**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

\[
\begin{pmatrix} I^{(1)} & \ast \\ M & -I^{(n-1)} \end{pmatrix}.
\]

For \( n = 1 \) and 2, this is trivial. Let the theorem be proved for \( n \), and assume that \( X^2 = I^{(n+1)} \), where \( n \geq 2 \). 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 \( t = (t_1, \ldots, t_{n+1})' \) with integral elements such that \( t'X = t' \). Choose \( P \in \mathfrak{M}_{n+1} \) with first row \( t' \). Then

\[
PXP^{-1} = \begin{pmatrix} 1 & n' \\ \xi & X_1 \end{pmatrix},
\]

where \( n \) denotes a vector whose components are 0; thus

\[
X = \begin{pmatrix} 1 & n' \\ \xi & X_1 \end{pmatrix}.
\]

But

\[
I^{(n+1)} = X^2 = \begin{pmatrix} 1 & n' \\ (I + X_1\xi) & X_1^2 \end{pmatrix}
\]

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

\[
X_1 = \begin{pmatrix} I^{(m)} & 0 \\ M & -I^{(n-m)} \end{pmatrix},
\]

and, after making the similarity transformation, we have (as a consequence of \((I + X_1)\xi = n\))

\[
\begin{pmatrix} 2I^{(m)} & 0 \\ \gamma M & 0 \end{pmatrix}\xi = n.
\]

Therefore
\[ x = (0, \cdots, 0, *, \cdots, *)', \]

where * denotes an arbitrary element. Thus

\[
X = \begin{pmatrix}
1 & n' \\
0 & I^{(m)} \\
\vdots & 0 \\
* & \vdots \\
* & M \\
* & -I^{(n-m)}
\end{pmatrix}
= \begin{pmatrix}
I^{(m+1)} & 0 \\
\overline{M} & -I^{(n-m)}
\end{pmatrix}.
\]

This completes the first part of the proof.

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

\[
\begin{pmatrix}
A^{(i)} \\
C \\
D^{(n-i)}
\end{pmatrix} \in \mathcal{M}_n.
\]

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

\[
W(x, y, z) = W(\bar{x}, \bar{y}, \bar{z})
\]

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 \( \mathcal{M}_n \) is therefore equal to the number of solutions of \( 2x + y + z = n \), \( x \geq 0 \), \( y \geq 0 \), \( z \geq 0 \). This gives

\[
A_n = \begin{cases} 
\frac{(n + 2)^2}{2}, & n \text{ even}, \\
\frac{(n + 1)(n + 3)}{4}, & n \text{ odd}.
\end{cases}
\]

(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

\[
B_n = \begin{cases} 
\frac{(A_n - 1)}{2}, & \text{if } n \equiv 0 \, (\text{mod } 4), \\
A_n/2, & \text{otherwise.}
\end{cases}
\]

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

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

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

\[X = I_1 \text{ or } I_2.\]

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 $\mathfrak{M}_3$. 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

\[
\begin{pmatrix} e & f \\ h & i \end{pmatrix} \in \mathfrak{M}_2, \quad \begin{cases} e \equiv 1 \\ h \equiv 0 \text{ (mod 2)} \end{cases}
\]

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
\[
\begin{pmatrix} X & \eta' \\ n & \pm 1 \end{pmatrix} \in \mathfrak{M}_3^+ \rightarrow \begin{pmatrix} X^r & \eta' \\ n & \pm 1 \end{pmatrix}.
\]

Since this induces an automorphism \( X \rightarrow X^r \) on \( \mathfrak{M}_2 \), we see that \( \det X^r = \det X \), 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 \( X^r = \pm AXA^{-1} \); 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 \( A^{-1} + I^{(1)} \), we may assume that

\[
\begin{pmatrix} X & \eta' \\ n & \pm 1 \end{pmatrix} \in \mathfrak{M}_3^+ \rightarrow \begin{pmatrix} \pm X & \eta' \\ n & \pm 1 \end{pmatrix},
\]

so that

\[
M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \rightarrow M \quad \text{or} \quad M \rightarrow N = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.
\]

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

\[
\begin{pmatrix} X & \eta \\ n' & \pm 1 \end{pmatrix} \in \mathfrak{M}_3^+ \rightarrow \begin{pmatrix} \pm AXA^{-1} & \eta \\ n' & \pm 1 \end{pmatrix},
\]

\[
\begin{pmatrix} \pm 1 & \eta' \\ n & X \end{pmatrix} \in \mathfrak{M}_3^+ \rightarrow \begin{pmatrix} \pm 1 & \eta' \\ n & \pm BXB^{-1} \end{pmatrix},
\]

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

where

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

and \( \eta = (0, 0)' \). 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 $\text{det} A$ and $\text{det} B$. Suppose hereafter, without loss of generality, that $\text{det} A = \text{det} B = 1$.

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

$$\left( \begin{array}{c} \pm A \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} A^{-1} \\ n \\ -1 \end{array} \right),$$

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 $\text{det} C = \pm 1$).

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

$$T = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \rightarrow \left( \begin{array}{c} \pm \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array} \end{array} \right).$$

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

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \rightarrow \left( \begin{array}{c} -1 & 0 & 0 \\ 0 & \pm \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{array} \right).$$
Therefore

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

is mapped into

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

where \( V = I_1 U_1 I_1^{-1} \). Thus, in this case, \( T \to T = I_1 T I_1^{-1} \), and either \( U \to U \) or \( U \to I_1 U I_1^{-1} \). Since \( T \) and \( U \) generate \((9) \mathfrak{M}^+_a\), 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

\[
U \to \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{pmatrix} \text{ or } \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.
\]

If we set \( Z = T U^2 \), then

\[
(10) \quad \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (UZ^{-1})^2 UZ^2.
\]

Now certainly the left side of (10) maps into

\[
\begin{pmatrix} -1 & 0 & 0 \\ -1 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix},
\]

\((9) \text{ L. K. Hua and I. Reiner, loc. cit.}\)
whereas, knowing $T^r$ and $U^r$, we can compute $Z^r$ and hence can find the image of the right side of (10). We readily find (for either value of $U^r$) that the right side of (10) maps into

$$\begin{pmatrix} 1 & \ldots \\ 3 & \ldots \\ \vdots & \ddots \end{pmatrix},$$

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

$$T \rightarrow \left( \pm \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \right).$$

**Case 1**.

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 $U^r = U$ or $V$. After a further inner automorphism by a factor of $I_1$ (in the latter case) we also have $U \rightarrow U$. But then

$$T \rightarrow T'^{-1}, \quad U \rightarrow U'^{-1}.$$ 

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

**Case 2**.

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

Then
and again we find that there are two possibilities for $U^r$, 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 $n \geq 4$, and define $J_1 = (-1)^n I^{(n-1)}$. In any automorphism $\tau$ of $\mathcal{M}_n$, $J_1^\tau = \pm AJ_1A^{-1}$ for some $A \in \mathcal{M}_n$.

**Proof.** By Corollary 1, $J_1^\tau \in \mathcal{M}_n^+$, and $J_1^\tau$ 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 $\mathcal{M}_n$ which commutes with $J_1$ maps into an element of $\mathcal{M}_n$ which commutes with $W$. Every matrix in $\mathcal{M}_n^+$ maps into a matrix in $\mathcal{M}_n^+$. Combining these facts, we see that the group $G_1$ consisting of those elements of $\mathcal{M}_n^+$ which commute with $J_1$ is isomorphic to $G_2$, 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 $G_1$ consists of the matrices in $\mathcal{M}_n^+$ of the form $(\pm 1)^x X_1$, $X_1 \in \mathcal{M}_{n-1}$, and so clearly $G_1 \cong \mathcal{M}_{n-1}$.

The group $G_2$ is easily found to consist of all matrices $C \in \mathcal{M}_1^+$ of the form (we illustrate the case where $x = 2$):

$$
\begin{bmatrix}
\alpha_1 & 0 & 0 & \cdots & 0 & 2\alpha_1 & \cdots & 2\alpha_x \\
\alpha_2 & 0 & 0 & \cdots & 0 & 2\beta_1 & \cdots & 2\beta_z \\
\alpha_3 & 0 & 0 & \cdots & 0 & 2\delta_1 & \cdots & 2\delta_z \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \cdots & \vdots \\
\alpha_y & 0 & 0 & \cdots & 0 & 2\gamma_1 & \cdots & 2\gamma_z \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \cdots & \vdots \\
\alpha_z & 0 & 0 & \cdots & 0 & 2\delta_1 & \cdots & 2\delta_z \\
\end{bmatrix}
$$

with $2x$ rows, $y$ columns, and $z$ columns.
For the moment put

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

Then a simple calculation gives:

$$KCK^{-1} = \begin{bmatrix} a_1 & 0 & a_2 & 0 & 0 & \cdots & 0 & 2\beta_1 & \cdots & 2\beta_z \\ 0 & d_1 & 0 & d_2 & \alpha_1 & \cdots & \alpha_y & 0 & \cdots & 0 \\ a_3 & 0 & a_4 & 0 & 0 & \cdots & 0 & 2\delta_1 & \cdots & 2\delta_z \\ 0 & d_3 & 0 & d_4 & \gamma_1 & \cdots & \gamma_y & 0 & \cdots & 0 \\ 0 & -2\epsilon_1 & 0 & -2\xi_1 & & & & U & 0 \\ \vdots & \vdots & \vdots & \vdots & & & & \vdots & \vdots \\ 0 & -2\epsilon_y & 0 & -2\xi_y & & & & U & 0 \\ \eta_1 & 0 & \theta_1 & 0 & & & & 0 & V \\ \vdots & \vdots & \vdots & \vdots & & & & \vdots & \vdots \\ \eta_z & 0 & \theta_z & 0 & & & & \vdots & \vdots \end{bmatrix}$$

and so $C$ is similar to

$$\begin{bmatrix} a_1 & a_2 & 2\beta_1 & \cdots & 2\beta_z \\ a_3 & a_4 & 2\delta_1 & \cdots & 2\delta_z \\ \eta_1 & \theta_1 & & & \\ \vdots & \vdots & & & V \\ \eta_z & \theta_z & & & \end{bmatrix} + \begin{bmatrix} d_1 & d_2 & \alpha_1 & \cdots & \alpha_y \\ d_3 & d_4 & \gamma_1 & \cdots & \gamma_y \\ -2\epsilon_1 & -2\xi_1 & & & \\ \vdots & \vdots & & & U \\ -2\epsilon_y & -2\xi_y & & & \end{bmatrix}$$

$$= \begin{bmatrix} S_1 & 2R_1 \\ Q_1 & T_1 \end{bmatrix}^x + \begin{bmatrix} S_2 & Q_2 \\ 2R_2 & T_2 \end{bmatrix}^y,$$

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

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

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 $A + B$, 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 $A_1 + B_1$ and $A_2 + B_2$ are two involutions in $\mathfrak{G}$, where either $A_1 \leq A_2$ in $\mathfrak{M}_{x+z}$ or $B_1 \leq B_2$ in $\mathfrak{M}_{x+y}$, then certainly $A_1 + B_1 \neq A_2 + B_2$ in $\mathfrak{G}$ (these may be similar in $\mathfrak{M}_n$, however). Therefore, the matrices $A + B$, where

$$A = I^{(a_1)} + (-1)^{(b_1)} + L + \cdots + L,$$

$$B = I^{(a_2)} + (-1)^{(b_2)} + L + \cdots + L,$$

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 $c_1 \leq (z+1)/2$, $c_2 \leq (y+1)/2$, and that in $B$ instead of $L$ we use $L'$. These conditions will insure that $A + B \subseteq \mathfrak{G}$. 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 $N = B_1 B_2 + (A_1 - B_1)(A_2 - B_2)$. Since $y$ is odd, $A_y = 2B_y$, and therefore

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

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

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

so that

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

For $n = 4$, $x = 0$, either $y = 1$ or $z = 1$. For $n \geq 6$, we have $N > A_{n-1}$. Hence in
this case \( \mathfrak{S} \) 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 \( n \geq 5 \).

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

\[
\begin{align*}
    a_1 + b_1 + 2c_1 &= x + z, \\
    a_2 + b_2 + 2c_2 &= x + y, \\
    b_1 + b_2 + c_1 + c_2 &= \text{even},
\end{align*}
\]

\[0 \leq c_1 \leq \frac{z+1}{2}, \quad 0 \leq c_2 \leq \frac{y+1}{2} \cdot\]

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

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

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 \( N \geq A_{n-1} \) in all cases except when both \( y \) and \( z \) are zero. Leaving aside this case for the moment, consider the matrix \( A_0 + I(x+y) \in \mathfrak{S} \), where \( A_0 \in \mathfrak{M}_{x+z} \) is given by

\[
A_0 = \begin{bmatrix}
1 & 2 & 2 & \cdots & 2 \\
0 & -1 & 0 & \cdots & 0 \\
0 & 0 & -1 & \cdots & 0 \\
\vdots & \vdots & \ddots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & -1
\end{bmatrix}.
\]

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

\[
A_0 = \begin{bmatrix}
1 & 0 & \cdots & 0 \\
0 & -1 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & -1
\end{bmatrix} = A_1,
\]

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

\[
A_1 \cdot \begin{bmatrix}
a_1 & a_2 & \cdots & a_x & 2b_1 & \cdots & 2b_z \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
\end{bmatrix} = \begin{bmatrix}
a_1 & a_2 & \cdots & a_x & 2b_1 & \cdots & 2b_z \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
\end{bmatrix} \cdot A_0
\]

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 \( A = W(c_1, b_1, a_1), B = W(c_2, b_2, a_2) \), where

\[ a_1 + b_1 + 2c_1 = x, \quad a_2 + b_2 + 2c_1 = x, \quad b_1 + b_2 \text{ even.} \]

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 \( n \geq 14 \). 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 \( n \geq 4 \) and suppose that Theorem 3 holds for \( n - 1 \). If \( \tau \) is any automorphism of \( \mathfrak{M}_n \), by Corollary 1 and Lemma 2 we know that \( \tau \) takes \( \mathfrak{M}_n^+ \) into itself, and \( J_1^* = \pm A J_1 A^{-1} \). If we change \( \tau \) 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 \( \tau \) 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,

\[
\begin{pmatrix}
\pm 1 & n' \\
n & X
\end{pmatrix}^r = \begin{pmatrix}
\pm 1 & n' \\
n & X^r
\end{pmatrix}.
\]

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

\[
X^r = \pm AX^*A^{-1},
\]

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 \( I^{(n)} A^{-1} \), we may assume that \( X^r = \pm X^* \).

Let \( J_n \) be obtained from \( I^{(n)} \) by replacing the \( n \)th diagonal element by \( -1 \). Then

\[
J_n = \begin{pmatrix}
-1 & 0 & \cdots & 0 & 0 \\
0 & 1 & \cdots & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & 1 & 0 \\
0 & 0 & \cdots & 0 & -1
\end{pmatrix}
\]


\[
J_n J_n = \begin{pmatrix}
-1 & n' \\
n & X
\end{pmatrix} = \begin{pmatrix}
1 & \cdots & 0 & 0 \\
\cdots & \cdots & \cdots & \cdots \\
0 & \cdots & 1 & 0 \\
0 & \cdots & 0 & -1
\end{pmatrix}^*.
\]
The minus sign here is impossible by Lemma 2, since \( n \geq 4 \). Hence \( J_1J_n \) is invariant, and therefore so is \( J_n \). By the same reasoning all of the \( J_v \) \((v = 1, \ldots, n)\) are invariant.

From the above remarks we see that for \( X \in \mathcal{M}^+_n \),

\[
\begin{pmatrix} 1 & n' \\ n & X \end{pmatrix}^r = \begin{pmatrix} 1 & n' \\ n & A_1X^*A_1^{-1} \end{pmatrix}, \ldots, \begin{pmatrix} X & n' \\ n' & 1 \end{pmatrix}^r = \begin{pmatrix} A_nX^*A_n^{-1} & n' \\ n' & 1 \end{pmatrix},
\]

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

\[
A_1\begin{pmatrix} 1 & n' \\ n & Z \end{pmatrix}A_1^{-1} = \begin{pmatrix} 1 & n' \\ n & Z \end{pmatrix}
\]

for every \( Z \in \mathcal{M}^+_{n-2} \). Setting

\[
A_1 = \begin{pmatrix} a & \xi' \\ \psi & A \end{pmatrix}
\]

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

Tsing Hua University,
Peking, China.
University of Illinois,
Urbana, Ill.