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 \( \mathcal{N}_n \) 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 \( \mathcal{R}_n \subseteq \mathcal{M}_n^+ \). For \( n = 2 \), \( \mathcal{R}_n \) is of index 2 in \( \mathcal{M}_n^+ \), 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 \( T \). 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 \( \mathcal{R}_2 \subseteq \mathcal{C} \). 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

\[ J = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \]
and $X$ and $Y \in \mathfrak{M}_n^+$. Then $A^2 = XY = XJ^{-1}XJ$. Hence we need only prove that if $X \in \mathfrak{M}_n^+$, $X$ and $J^{-1}XJ$ are of the same parity. This is easily verified for $X = S$ or $T$; since $S$ and $T$ generate $\mathfrak{M}_n^+$, 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 $\mathfrak{E} \subseteq \mathfrak{S}_2$. For, $\mathfrak{E}$ is generated by $T^2$ and $ST$, since $TS = (ST \cdot T^{-2})^2$. However, $T^2 = TJT^{-1}J^{-1} \in \mathfrak{S}_2$, and therefore also $(T')^{-2} \in \mathfrak{S}_2$. Furthermore, $ST = TST^{-1}(T')^{-2}T^2 \in \mathfrak{S}_2$. This completes the proof for $n = 2$.

Suppose now that $n > 2$, and define

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

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

(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)

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

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

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

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

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

**Corollary 1.** In any automorphism of $\mathfrak{M}_n$, always $\mathfrak{M}_n^+ \rightarrow \mathfrak{S}_n$.

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

---

Then $ST \in \mathfrak{H}_2$ implies $S_1 T_1 \in \mathfrak{H}_2$, so $\det (S_1 T_1) = 1$. 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 $\mathfrak{M}_n^+$. We wish to determine the automorphisms of $\mathfrak{M}_n$. Since every automorphism of $\mathfrak{M}_n$ takes $W$ 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

(I) $X \in \mathfrak{M}_2^+ \to AXA^{-1}$ \hspace{1cm} $A \in \mathfrak{M}_2$

or

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

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 $\tau$ 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 $S^\tau$ and $T^\tau$. Then $(S^\tau)^2 = -I$. Since all second order fixed points are equivalent, there exists a matrix $B \in \mathfrak{M}_2$ such that $BSB^{-1} = S$. Instead of $\tau$, consider the automorphism $\tau': X \to BX^\tau B^{-1}$, 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 $T^\tau = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

From $(ST)^4 = I$ we obtain $(ST^\tau)^4 = I$, whence $b - c = 1$. Since $\det T^\tau = 1$, we get $ad = 1 + bc = c^2 + c + 1 > 0$.

Set $N = |a + d|$. If $N \geq 3$, consider the elements generated by $S$ and $T^\tau$ (mod $N$). Since $a + d = 0$ (mod $N$), we find that $(T^\tau)^2 \equiv I$ (mod $N$). Furthermore $(ST^\tau)^2 \equiv I$ (mod $N$); therefore $S$ and $T^\tau$ 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 $\tau$ is an automorphism, $S$ and $T^\tau$ generate $\mathfrak{M}_2^+$, 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 $T^\tau$:
Since $S$ and $T$ generate $SD_3^+$, to determine $\tau$ it is sufficient to specify $S^\tau$ and $T^\tau$. Thus every automorphism of $SD_3^+$ is of the form $S \rightarrow BSB^{-1}$, $T \rightarrow BTB^{-1}$ (for some $i$, $i = 0, 1, 2, 3$), where $B \in SD_2$. If $J$ is given by (2), we have:

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

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

- $i = 0$: $S \rightarrow BSB^{-1}$, $T \rightarrow BTB^{-1}$.
- $i = 1$: $S \rightarrow BS \cdot S \cdot S^{-1}B^{-1}$, $T \rightarrow BS \cdot T \cdot S^{-1}B^{-1}$.
- $i = 2$: $S \rightarrow -BJ \cdot S \cdot J^{-1}B^{-1}$, $T \rightarrow -BJ \cdot T \cdot J^{-1}B^{-1}$.
- $i = 3$: $S \rightarrow -BSJ \cdot S \cdot J^{-1}S^{-1}B^{-1}$, $T \rightarrow -BSJ \cdot T \cdot J^{-1}S^{-1}B^{-1}$.

These automorphisms are of two types: for $i = 0$ and 1, $S \rightarrow ASA^{-1}$, $T \rightarrow A^2A^{-1}$, which imply that $X \in SD_3^+ \rightarrow AXA^{-1}$, for $i = 2$ and 3, $S \rightarrow ASA^{-1}$, $T \rightarrow A^2A^{-1}$, which imply that $X \in SD_3^+ \rightarrow e(X) \cdot AXA^{-1}$. This completes the proof.

3. Automorphisms of $SD_3^+$ and $SD_6$. We are now faced with the problem of determining the automorphisms of $SD_6$ from those of $SD_3^+$. We shall have the same problem for $SD_4$ and $SD_6$. As we shall see, the passage from $SD_3^+$ to $SD_6$ is trivial, and most of the difficulty lies in determining the automorphisms of $SD_6$. In this paper we shall prove the following results:

**Theorem 3.** For $n > 2$, the group of those automorphisms of $SD_6$ which are induced by automorphisms of $SD_3^+$ is generated by

(i) the set of all “inner” automorphisms 

$$X \in SD_3^+ \rightarrow AXA^{-1} \quad (A \in SD_3),$$

and

(ii) the automorphism 

$$X \in SD_3^+ \rightarrow X^\tau.$$ 

**Remark.** When $n = 2$, the automorphism (ii) is the same as $X \rightarrow SXS^{-1}$, hence is included in (i). The automorphism $X \rightarrow e(X) \cdot X$ occurs only for $n = 2$. Furthermore, for odd $n$ all automorphisms of $SD_3^+$ are induced by automorphisms of $SD_3$.

**Theorem 4.** The generators of $SD_6$ are

(i) the set of all inner automorphisms 

$$X \in SD_3 \rightarrow AXA^{-1} \quad (A \in SD_3),$$
(ii) the automorphism $X \in M_n \rightarrow X^{t-1},$
(iii) for even $n$ only, the automorphism
$$X \in M_n \rightarrow (\det X) \cdot X,$$
and
(iv) for $n = 2$ only, the automorphism
$$X \in M_2^+ \rightarrow e(X) \cdot X, \quad X \in M_2^- \rightarrow e(JX) \cdot X,$$
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 $M_n$. By Corollary 1, $\tau$ induces an automorphism on $M_n^+$ which, by Theorems 2 and 3, can be written as:
$$X \in M_n^+ \rightarrow \alpha(X) \cdot AXA^{-1},$$
where $A \in M_n, \alpha(X) = 1$ for all $X$ or $\alpha(X) = e(X)$ 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 $Z \in M_n$; then
$$YZ^r = (YZ)^r = \alpha(YZ) \cdot (YZ)^A A^{-1},$$
whence
$$Y^r = \alpha(YZ) \cdot AYZA^{-1}(Z^r)^{-1}.$$ Let $Z \in M_n^-$ be fixed; then
$$Y^r = \alpha(YZ) \cdot AYZB$$
for all $Y \in M_n^-$,
where $A$ and $B$ are independent of $Y$. But then
$$AY^*B \cdot AYZB = (Y^r)^2 = (Y^r)^r = \alpha(Y^2)A(Y^2)A^{-1},$$
so that
$$(BA)Y^*(BA) = \alpha(Y^2)Y^r.$$ Since this is valid for all $Y \in M_n^-$, we see that of necessity $\alpha(Y^2) = 1$ for all $Y$, and $BA = \pm I$. This shows that either $Y^r = \alpha(YZ) \cdot AYZA^{-1}$ for all $Y \in M_n^-$, or $Y^r = -\alpha(YZ) \cdot AYZA^{-1}$ for all $Y \in M_n^-$. If $n = 2$ and $\alpha(YZ) = e(YZ)$, it is trivial to verify that either $e(YZ) = e(JY)$ for all $Y \in M_2^-$ or $e(YZ) = -e(JY)$ for all $Y \in M_2^-.$

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 $X \in M_n$ 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

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

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

\[
\begin{pmatrix} I^{(t)} & 0 \\ M & -I^{(n-t)} \end{pmatrix}.
\]

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 \( P \in \mathbb{M}_{n+1} \) 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 \((I + X_1)\xi = n\))

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

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

where * denotes an arbitrary element. Thus

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

This completes the first part of the proof.

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

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

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

\[ W(x, y, z) = W(x, y, z) \]

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

\[ A_n = \begin{cases}
\binom{n + 2}{2}, & n \text{ even}, \\
\frac{(n + 1)(n + 3)}{4}, & n \text{ odd}.
\end{cases} \]
Let \( B_n \) be the number of nonsimilar involutions in \( \mathbb{M}^+_n \), where the similarity factors are in \( \mathbb{M}_n \). One easily obtains

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

5. Automorphisms of \( \mathbb{M}^+_n \). We shall now prove Theorem 3 for \( n = 3 \). Let

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

Then \( I_2^3 = I^{(3)} \). Let \( \tau \) be any automorphism of \( \mathbb{M}^+_3 \) 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 nonsimilar involutions in \( \mathbb{M}^+_3 \). 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 \( \in \mathbb{M}^+_3 \) which commute with \( I_1 \), consists of all elements of \( \mathbb{M}^+_3 \) of the form

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

and is isomorphic to \( \mathbb{M}_3 \). That of \( I_2 \) consists of all elements of \( \mathbb{M}^+_3 \) 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 \( \mathbb{M}_3 \) consisting of the elements

\[
\begin{pmatrix}
e & f \\
h & i
\end{pmatrix} \in \mathbb{M}_3, \quad \begin{cases} 
e \equiv 1 \\
h \equiv 0 \pmod{2}.
\end{cases}
\]

Since \( e \) and \( i \) are both odd, \( \mathfrak{G} \) contains no element of order 3, and hence is not isomorphic to \( \mathbb{M}_3 \). 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 \( \mathbb{M}^+_3 \) which commute with \( I_1 \) map into elements of the same kind, so that
(X' \ n') \in \mathfrak{M}_3^+ \rightarrow (X' \ n') \in \mathfrak{M}_3^+\rightarrow (X' \ n').

Since this induces an automorphism $X \rightarrow X'$ on $\mathfrak{M}_3$, we see that $\det X' = \det X$, 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 $A \in \mathfrak{M}_3$ such that $X' = \pm AXA^{-1}$; here, the plus sign certainly occurs when $X$ is an even element of $\mathfrak{M}_3^+$, and if the minus sign occurs for one odd element of $\mathfrak{M}_3^+$, then it occurs for every odd element of $\mathfrak{M}_3^+$. By use of a further inner automorphism using the factor $A^{-1} + I^{(1)}$, we may assume that

(8) \[
\begin{pmatrix} X \ n' \\ n \pm 1 \end{pmatrix} \in \mathfrak{M}_3^+ \rightarrow \begin{pmatrix} \pm X \ n' \\ n \pm 1 \end{pmatrix},
\]

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

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

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 $C \in \mathfrak{M}_3$ such that

(9) \[
\begin{pmatrix} X \ n' \\ n \pm 1 \end{pmatrix} \in \mathfrak{M}_3^+ \rightarrow \begin{pmatrix} \pm AXA^{-1} \ n' \\ n \pm 1 \end{pmatrix},
\]

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

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

where

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

and $n = (0, 0)'$. 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 $\mathbb{M}_2^+$, 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 $X \in \mathbb{M}_2^+$, it occurs there for every odd $X \in \mathbb{M}_2^+$.

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

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

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

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

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

$$
\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} -1 & 0 & 0 \\ 0 & \pm 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.
$$
1951] AUTOMORPHISMS OF THE UNIMODULAR GROUP 341

Therefore
\[
U = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}
\]
is mapped into
\[
\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -1 \end{pmatrix} = \begin{cases} U, & \text{if } + \text{ is used,} \\
V, & \text{if } - \text{ is used,} \end{cases}
\]
where \( V = I_3 U T_1^{-1} \). Thus, in this case, \( T \rightarrow T = I_3 T T_1^{-1} \), and either \( U \rightarrow U \) or \( U \rightarrow I_3 U T_1^{-1} \). Since \( T \) and \( U \) generate \((9) \mathbb{M}_3^+\), the automorphism is inner.

Case 2.

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

Then
\[
\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} \rightarrow \begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix},
\]
and one finds in this case that
\[
U \rightarrow \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{pmatrix} \text{ or } \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix}.
\]

If we set \( Z = T U^2 \), then
\[
(10) \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (UZ^{-1})^2 UZ^2.
\]

Now certainly the left side of (10) maps into
\[
\begin{pmatrix} -1 & 0 & 0 \\ -1 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.
\]

(9) L. K. Hua and I. Reiner, loc. cit.
whereas, knowing \( T^r \) and \( U^r \), we can compute \( Z^r \) and thence 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

\[
\begin{pmatrix}
1 \\
3 \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \\
. \
\end{pmatrix},
\]

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

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

**Case 1**.

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

Then as before

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

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 $J_1 = (-1)^{n-1} I$. In any automorphism $\tau$ of $\mathcal{M}_n$, $J_1^r = \pm AJ_1A^{-1}$ for some $A \in \mathcal{M}_n$.

**Proof.** By Corollary 1, $J_1^r \in \mathcal{M}_n^+$, and $J_1^r$ is an involution. After a suitable inner automorphism, we may assume that $J_1^r = W(x, y, z)$ (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 $(\pm 1)^r X_1$, $X_1 \in \mathcal{M}_{n-1}$, 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 $x = 2$):

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

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
For the moment put
\[ K = \left( \begin{array}{cc} 1 & 0 \\ -1/2 & 1 \end{array} \right) + \cdots + \left( \begin{array}{cc} 1 & 0 \\ -1/2 & 1 \end{array} \right) + I^{(n-2z)}. \]

Then a simple calculation gives:

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

and so \( C \) is similar to

\[ \left[ \begin{array}{ccc} a_1 & a_2 & 2\beta_1 \cdots 2\beta_z \\
a_3 & a_4 & 2\delta_1 \cdots 2\delta_z \\
\eta_1 & \theta_1 & \vdots \\
\eta_z & \theta_z & \vdots \\
\end{array} \right] \] + \[ \left[ \begin{array}{ccc} d_1 & d_2 & \alpha_1 \cdots \alpha_y \\
d_3 & d_4 & \gamma_1 \cdots \gamma_y \\
-2\epsilon_1 & -2\xi_1 & \vdots \\
-2\epsilon_y & -2\xi_y & \vdots \\
U & \vdots & \ddots \\
\end{array} \right] \]

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

\[ \left[ \begin{array}{cc} S_1 & 2R_1 \\
Q_1 & T_1 \end{array} \right] z + \left[ \begin{array}{cc} S_2 & Q_2 \\
2R_2 & T_2 \end{array} \right] y, \]

where \( S_1 \equiv S_2 \) (mod 2). Here \( 2x+t+y+z=n \) and \( x+y \) is odd.

We wish to prove that \( \mathcal{M}_{n-1} \cong \mathcal{G}(x, y, z) \) 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 \( \mathcal{G} \) which are nonsimilar in \( \mathcal{G} \) is greater than the number of involutions in \( \mathcal{M}_{n-1} \) which are nonsimilar in \( \mathcal{M}_{n-1} \);
this latter number is, of course, $A_{n-1}$ (given by (6)).

We shall briefly denote the elements of $\mathfrak{O}$ 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 $\mathfrak{O}$, where either

\[ A_1 \neq A_2 \]

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

\[ B_1 \neq B_2 \]

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

\[ A_1 + B_1 \neq A_2 + B_2 \]

in $\mathfrak{O}$ (these may be similar in $\mathcal{M}_{n}$, however). Therefore, the matrices $A + B$, where

\[ A = I^{(a_1)} + (-1)^{(b_1)} + L + \cdots + L, \quad \text{(c_1 terms)} \]
\[ B = I^{(a_2)} + (-1)^{(b_2)} + L + \cdots + L, \quad \text{(c_2 terms)} \]

obtained by taking different sets of values of $(a_1, b_1, c_1, a_2, b_2, c_2)$, if they lie in $\mathfrak{O}$, are certainly nonsimilar in $\mathfrak{O}$. 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 $A + B \subseteq \mathfrak{O}$. We certainly do not (in general) get all of the nonsimilar involutions of $\mathfrak{O}$ 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

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

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 $\mathfrak{G}$ 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 $n \geq 5$.

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

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

$$0 \leq c_1 \leq \frac{z+1}{2}, \quad 0 \leq c_2 \leq \frac{y+1}{2}.$$

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

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

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 $A_0 + I^{(x+y)} \in \mathfrak{G}$, where $A_0 \in \mathfrak{M}_{x+z}$ is given by

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

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

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

$A_0 + I^{(x+y)}$ 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

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

we obtain
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 $A + B \not\in \mathfrak{G}$, 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 $J_1^\tau = \pm AJ_1A^{-1}$. If we change $\tau$ by a suitable inner automorphism, then we may assume that $J_1 \rightarrow \pm J_1$. When $n$ is odd, certainly $J_1 \rightarrow J_1$; when $n$ is even, by multiplying $\tau$ by the automorphism $X \in \mathfrak{M}_n \rightarrow (\operatorname{det} X) \cdot X$ if necessary, we may again assume $J_1 \rightarrow J_1$.

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

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

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 $I^{(1)} \pm A^{-1}$, we may assume that $X^\tau = \pm X^*$. Let $J_n$ be obtained from $I^{(n)}$ by replacing the $n$th diagonal element by $-1$. Then

$$J_nJ = \begin{pmatrix} -1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & -1 \end{pmatrix} \rightarrow \begin{pmatrix} -1 & n' \\ n & \pm \begin{pmatrix} 1 & \cdots & 0 & 0 \\ \cdot & \cdots & 0 & 0 \\ 0 & \cdots & 1 & 0 \\ 0 & \cdots & 0 & -1 \end{pmatrix} \end{pmatrix}.$$
The minus sign here is impossible by Lemma 2, since \( n \geq 4 \). Hence \( J_1J_n \) is invariant, and therefore so is \( J_n \). By the same reasoning all of the \( J_\nu \) (\( \nu = 1, \cdots, n \)) are invariant.

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

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

where \( A_\nu \in \mathcal{M}_{n-1} \), 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

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

we obtain \( \xi'Z = \xi', \ \eta = \bar{Z}\eta \). 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 \( J_\nu \), for \( \nu = 3, \cdots, n \)) shows that \( A_1 \) is diagonal. Correspondingly, all of the \( A_\nu \) are diagonal. It is further clear that all of the \( A_\nu \) (\( \nu = 1, \cdots, n \)) are sections of a single diagonal matrix \( D^{(n)} \).

Using the further inner automorphism factor \( D^{-1} \), we may henceforth assume that \( X^* = X \) 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.