AUTOMORPHISMS OF THE PROJECTIVE UNIMODULAR GROUP

BY

L. K. HUA AND I. REINER

Notation. Let \( M_n \) denote the group of \( n \times n \) integral matrices of determinant \( \pm 1 \) (the unimodular group). By \( M_n^+ \) we denote that subset of \( M_n \) where the determinant is +1; \( M_n^- \) is correspondingly defined. Let \( \mathfrak{U}_n \) be obtained from \( M_n \) by identifying +\( X \) and -\( X \), \( X \in M_n \). (This is the same as considering the factor group of \( M_n \) by its centrum.) We correspondingly obtain \( \mathfrak{U}_n^+ \) and \( \mathfrak{U}_n^- \) from \( M_n^+ \) and \( M_n^- \). Let \( I_n \) (or briefly \( I \)) be the identity matrix in \( M_n \), and let \( X' \) denote the transpose of \( X \). The direct sum of \( A \) and \( B \) is represented by \( A + B \), while

\[
A = B
\]

means that \( A \) is similar to \( B \).

In this paper we shall find explicitly the generators of the group \( \mathfrak{U}_n \) of all automorphisms of \( \mathfrak{U}_n \), thereby obtaining a complete description of these automorphisms. This generalizes the result due to Schreier\(^{1}\) for the case \( n = 1 \).

We shall frequently refer to results of an earlier paper: Automorphisms of the unimodular group, L. K. Hua and I. Reiner, Trans. Amer. Math. Soc. vol. 71 (1951) pp. 331-348. We designate this paper by AUT.

1. The commutator subgroup of \( \mathfrak{U}_n \). The following useful result is an immediate consequence of the corresponding theorem for \( M_2 \) (AUT, Theorem 1).

Theorem 1. Let \( \mathfrak{C}_n \) be the commutator subgroup of \( \mathfrak{U}_n \). Then clearly \( \mathfrak{C}_n \subseteq \mathfrak{U}_n \). For \( n = 1 \), \( \mathfrak{C}_2 \) is of index 2 in \( \mathfrak{U}_2^+ \), while for \( n > 1 \), \( \mathfrak{C}_n = \mathfrak{U}_n^\pm \).

Theorem 2. In any automorphism of \( \mathfrak{U}_n \), always \( \mathfrak{U}_n^\pm \) goes into itself.

Proof. This is a corollary to Theorem 1 when \( n > 1 \), since the commutator subgroup goes into itself under any automorphism. For \( n = 1 \), suppose that \( \pm S \rightarrow \pm S_1 \) and \( \pm T \rightarrow \pm T_1 \), where

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

Since \( S \) and \( T \) generate \( M_2^\pm \), it follows that \( \pm S \) and \( \pm T \) generate \( \mathfrak{U}_2^\pm \).

Received by the editors May 18, 1951.

and hence so must $\pm S_1$ and $\pm T_1$. It is therefore sufficient to prove that
$\det S_1=\det T_1=+1$. From $(ST)^3=I$ we deduce $S_1T_1=\pm T_1^{-1}S_1^{-1}T_1^{-1}S_1^{-1}$, so
that $\det S_1T_1=1$. Hence either $S_1$ and $T_1$ are both in $\mathfrak{B}_2^+$ or both in $\mathfrak{B}_2^-$; we
shall show that the latter alternative is impossible.

Suppose that $\det S_1=\det T_1=-1$. From $S_1^2=I$ we deduce $S_1^2 = \pm I$; if
$S_1^2 = -I$, then $S_1^2 + I = 0$ and the characteristic equation of $S_1$ is $x^2 + 1 = 0$, from
which it follows that $\det S_1 = 1$; this contradicts our assumption that
$\det S_1 = -1$, so of necessity $S_1^2 = I$. But if this is the case, then it is easy to show that there exists a matrix $A \in \mathfrak{B}_2$ such that $AS_1A^{-1}$ takes one of the
two canonical forms

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

By considering instead of the original automorphism $\tau$, a new automorphism
$\tau'$ defined by: $X' = AXA^{-1}$, we may hereafter assume that

$$
S_1 = \pm \begin{pmatrix}
1 & 0 \\
0 & -1
\end{pmatrix}
\quad \text{or} \quad
\pm \begin{pmatrix}
1 & 0 \\
1 & -1
\end{pmatrix}.
$$

Let

$$
T_1 = \pm \begin{pmatrix}
a & b \\
c & d
\end{pmatrix};
$$

then $ad-bc = -1$.

Now we observe that $J = (1) \pm (1)$ is distinct from $\pm I$ and $\pm S_1$, that
it commutes with $S_1$, and that $JT$ is an involution. Hence there exists a matrix
$M \in \mathfrak{B}_2$ distinct from $\pm I$ and $\pm S_1$, such that $M$ commutes with $S_1$, and $MT_1$
is an involution.

Case 1.

$$
S_1 = \pm \begin{pmatrix}
1 & 0 \\
0 & -1
\end{pmatrix}.
$$

Since $(S_1T_1)^3 = I$, we find that $a-d = \pm 1$. The only matrices commuting
with $S_1$ which are distinct from $\pm I$ and $\pm S_1$ are

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

If $M$ is either of the first two matrices, then the condition that $MT_1$ be an
involution yields $b+c = 0$. Thus $a=d \pm 1$, $b=-c$, and $ad-bc = -1$. Combin-
ing these, we obtain $d(d \pm 1) + c^2 = -1$, which is impossible. The other two
choices for $M$ imply $b = c$, and therefore $d(d \pm 1) - c^2 = -1$. Hence $1 - 4(1-c^2)$
is a perfect square; but $4c^2 - 3 = f^2$ implies $(2c+f)(2c-f) = 1$, whence $c = \pm 1$.  

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
But then \( ad = 0 \); from \( a - d = \pm 1 \) we deduce that \( a^2 - d^2 = \pm 1 \), whence \((ST)^3 = \pm I\), which is impossible.

**Case 2.**

\[
S_1 = \pm \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}.
\]

From \((ST_1)^3 = \pm I\) we obtain \( a - d + b = \pm 1 \). For \( M \) there are the four possibilities

\[
\pm \begin{pmatrix} 1 & -2 \\ 0 & -1 \end{pmatrix} \quad \text{and} \quad \pm \begin{pmatrix} 1 & -2 \\ 1 & -1 \end{pmatrix}.
\]

Since \( MT_1 \) is an involution, in the first two cases we have \( a - 2c - d = 0 \), whence

\[
ad - bc = \left\{ (a + d)^2 + (a - d + 1)^2 - 1 \right\}/4 \neq -1.
\]

In the second two cases we find that \( a - 2c + b - d = 0 \), so that \( 2c = a + b - d = \pm 1 \), which is again a contradiction. This completes the proof of Theorem 2.

2. **Automorphisms of \( \mathbb{P}_2^+ \).** Let us now determine all automorphisms of \( \mathbb{P}_2^+ \). Since every such automorphism takes \( \mathbb{P}_2^+ \) into itself, we begin by considering all automorphisms of \( \mathbb{P}_2^- \).

**Theorem 3.** Every automorphism of \( \mathbb{P}_2^+ \) is of the form \( X \in \mathbb{P}_2^+ \rightarrow AXA^{-1} \) for some \( A \in \mathbb{M}_2 \); that is, all automorphisms of \( \mathbb{P}_2^+ \) are “inner” (with \( A \in \mathbb{M}_2 \) rather than \( A \in \mathbb{P}_2^- \)).

**Proof.** Let \( \tau \) be any automorphism of \( \mathbb{P}_2^+ \), and define \( S \) and \( T \) as before; let \( S_0 \in \mathbb{M}_2 \) be a fixed representative of \( \pm S^t \). By Theorem 2, \( S_0 \in \mathbb{M}_2^+ \), and therefore \( S_0^3 = -I \). Let \( T_0 \) be that representative of \( \pm T^t \) for which \((S_0T_0)^3 = I\) is valid. Then \( S \rightarrow S_0, T \rightarrow T_0 \) induces a mapping from \( \mathbb{M}_2^+ \) onto itself. The mapping is one-to-one, for although an element of \( \mathbb{M}_2^+ \) can be expressed in many different ways as a product of powers of \( S \) and \( T \), these expressions can be gotten from one another by use of \( S^2 = -I, (ST)^3 = I \); since \( S_0 \) and \( T_0 \) satisfy these same relations, the mapping is one-to-one. It is an automorphism because \( \tau \) is one. Therefore (AUT, Theorem 2) there exists an \( A \in \mathbb{M}_2 \) such that \( S_0 = \pm ASA^{-1}, T_0 = \pm ATA^{-1} \). This proves the result.

**Corollary.** Every automorphism of \( \mathbb{P}_2 \) is of the form \( X \in \mathbb{P}_2 \rightarrow AXA^{-1} \) for some \( A \in \mathbb{M}_2 \).

(This corollary is a simple consequence of Theorem 3, as is shown in AUT by the remarks following the statement of Theorem 4.)

3. **The generators of \( \mathbb{P}_{2n} \).** Our main result may be stated as follows:

**Theorem 4.** The generators of \( \mathbb{P}_{2n} \) are

(i) The set of all inner automorphisms:
\[ \pm X \in \mathfrak{P}_{2n} \rightarrow \pm AXA^{-1} \quad (A \in \mathfrak{M}_{2n}), \]

and

(ii) The automorphism \[ \pm X \in \mathfrak{P}_{2n} \rightarrow \pm X^{-1}. \]

Remark. For \( n=1 \), the automorphism (ii) is a special case of (i).

In the proof of Theorem 4 by induction on \( n \), the following lemma (which has already been established for \( n=1 \)) will be basic:

**Lemma 1.** Let \( J_1 = (-1) + I^{(2n-1)} \). In any automorphism \( \tau \) of \( \mathfrak{P}_{2n} \), \( J_1^\tau = \pm AJ_1A^{-1} \) for some \( A \in \mathfrak{M}_{2n} \).

**Proof.** The result is already known for \( n=1 \). Hereafter let \( n \geq 2 \). Certainly \( (J_1)^2 = \pm I \) and \( \det J_1 = -1 \). If \( (J_1)^2 = -I \), then the minimum function of \( J_1 \) is \( \lambda^2 + 1 \), and its characteristic function must be some power of \( \lambda^2 + 1 \), whence \( \det J_1 = 1 \). Therefore \( (J_1)^2 = I \) is valid in \( \mathfrak{P}_{2n} \). After a suitable inner automorphism, we may assume that

\[ J_1 = W(x, y, z) = L + \cdots + L + (-I)^{(x)} + I^{(z)}, \]

where

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

occurs \( x \) times, \( 2x+y+z=2n \), and \( x+y \) is odd. (This follows from AUT, Lemma 1.)

Let \( \mathfrak{G}_1 \) be the group consisting of all elements of \( \mathfrak{P}_{2n} \) which commute with \( J_1 \), and \( \mathfrak{G}_2 \) the corresponding group for \( J_1^\tau \). The lemma will be proved if we can show that \( \mathfrak{G}_1 \) is not isomorphic to \( \mathfrak{G}_2 \) unless \( J_1^\tau = \pm J_1 \). The group \( \mathfrak{G}_1 \) consists of the matrices \( \pm (1 + X_1) \in \mathfrak{P}_{2n} \), so that \( \mathfrak{G}_1 \cong \mathfrak{M}_{2n-1} \). The number of nonsimilar involutions in \( \mathfrak{G}_1 \) is therefore \( n(n+1) \) (see AUT, §4). We shall prove that \( \mathfrak{G}_2 \) contains more than \( n(n+1) \) involutions which are nonsimilar in \( \mathfrak{G}_2 \), except when \( x = 0, y = 1, z = 2n-1 \) or \( x = 0, y = 2n-1, z = 1 \).

Those elements \( \pm C \in \mathfrak{P}_{2n} \) which commute with \( W \) must satisfy one of the two equations: \( CW = WC \) or \( CW = -WC \). The solutions of the first of these equations form a subgroup of \( \mathfrak{G}_2 \), and this subgroup is known (see AUT, proof of Lemma 2) to be isomorphic to \( \mathfrak{G}_0 = \mathfrak{G}_0(x, y, z) \) consisting of all matrices in \( \mathfrak{P}_{2n} \) of the form

\[
\begin{pmatrix} S_1 & 2R_1 \\ Q_1 & T_1 \end{pmatrix} + \begin{pmatrix} S_2 & Q_2 \\ 2R_2 & T_2 \end{pmatrix},
\]

where \( S_1, S_2, T_1, \) and \( T_2 \) are square matrices of dimensions \( x, x, z, \) and \( y \) respectively, and where \( S_1 \equiv S_2 \pmod{2} \), \( 2x+y+z=2n \), and \( x+y \) and \( x+z \) are both odd.

Next we prove that \( CW = -WC \) is solvable only when \( y = z \). The space
of vectors $u$ such that $Wu = u$ is of dimension $x+z$, while the space $B$ of vectors $v$ for which $Wv = -v$ has dimension $x+y$. But if $CW = -WC$, then $W^2u = -Cu$ and $W^2v = -Cv$, so the dimensions of $u$ and $B$ must be the same, whence $y = z$. Hence if $y \neq z$, there are no solutions of $CW = -WC$, $C \in \mathfrak{M}_{2n}$.

We may now proceed to find a lower bound for the number of nonsimilar matrices in $\mathfrak{S}_0(x, y, z)$. We briefly denote the elements of $\mathfrak{S}_0$ 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 distinct involutions in $\mathfrak{S}_0$, where either

$$A_1 \neq A_2 \quad \text{in} \quad M_{x+z} \quad \text{or} \quad B_1 \neq B_2 \quad \text{in} \quad M_{x+y},$$

then certainly

$$A_1 + B_1 \neq A_2 + B_2 \quad \text{in} \quad \mathfrak{S}_0.$$

Now let

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

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

where $L$ occurs $c_1$ times in $A$ and $c_2$ times in $B$; the various elements $A + B$ gotten by taking different sets of values of $(a_1, b_1, c_1, a_2, b_2, c_2)$, if they lie in $\mathfrak{S}_0$, are certainly nonsimilar in $\mathfrak{S}_0$, except that $A + B$ and $(-A) + (-B)$ are the same element of $\mathfrak{S}_0$. Hence the number $N$ of nonsimilar involutions of $\mathfrak{S}_0$ is at least half of the number $N_1$ of solutions of

$$a_1 + b_1 + 2c_1 = x + z,$$

$$a_2 + b_2 + 2c_2 = x + y,$$

where if $x \neq 0$ we impose the restrictions 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 insure that $A + B \in \mathfrak{S}_0$.) As in the previous paper, one readily shows that $N > n(n+1)$ unless $J_1 = \pm J_1$. We omit the details.

This leaves only the case where $y = z$. If $CW = -WC$, then $C^kW = (-1)^kWC^k$; therefore no odd power of $C$ can be $\pm I$. Let $p$ be a prime such that $n < p < 2n$. Since $x+y = n$, certainly $n$ is odd, and $p \geq n+2$. Now $\mathfrak{S}_1$ (being isomorphic to $\mathfrak{M}_{2n-1}$) contains infinitely many elements of order $p$. However, $\mathfrak{S}_2$ contains only two such elements, since $C^p \neq \pm I$ by the above argument, while if $C \in \mathfrak{S}_0$ and $C^p = \pm I$, then setting $C = A^{(p)} + B^{(p)}$ shows that $A^p = \pm I$ and $B^p = \pm I$. However, $A \in \mathfrak{M}_n$, and if $A^p = \pm I$, then the minimum function of $A$ must divide $\lambda^p + 1$. But the degree of the minimum function is at most $n$, and therefore is less than $p-1$, whereas $\lambda^p + 1$ is the
product of a linear factor $\lambda \mp 1$ and an irreducible factor of degree $p - 1$; thence the minimum function of $A$ is $\lambda \mp 1$, so $A = \pm I$. In the same way $B = \pm I$. Hence the only solutions are $C = I^{(n)} \mp I^{(n)}$ and $C = -I^{(n)} \mp I^{(n)}$. This completes the proof of the lemma. We remark that the use of the existence of the prime $p$ could have been avoided, but the proof is much quicker this way.

4. Proof of the main theorem. We are now ready to prove Theorem 4 by induction on $n$. Hereafter, let $n \geq 2$ and assume that Theorem 4 holds for $n - 1$. Let $\tau$ be any automorphism of $\mathfrak{P}_2n$; then by Lemma 1, $J_1^\tau = \pm AJ_1A^{-1}$ for some $A \in \mathfrak{M}_{2n}$. If we change $\tau$ by a suitable inner automorphism, we may assume that $J_1^\tau = \pm J_1$.

Therefore, every $M \in \mathfrak{P}_2n$ which commutes with $J_1$ goes into another such element, that is,

$$
\pm \begin{bmatrix} 1 & n'' \\ n & X \end{bmatrix}^\tau = \pm \begin{bmatrix} 1 & n'' \\ n & Y \end{bmatrix},
$$

where $n$ denotes a column vector all of whose components are zero, and $X \in \mathfrak{M}_{2n-1}$. Thus, $\tau$ induces an automorphism on $\mathfrak{M}_{2n-1}$. Consequently (AUT, Theorem 4) there exists a matrix $A \in \mathfrak{M}_{2n-1}$ such that $Y = AX^*A^{-1}$ for all $X \in \mathfrak{M}_{2n-1}$, where either $X^* = X$ for all $X \in \mathfrak{M}_{2n-1}$ or $X^* = X'^{-1}$ for all $X \in \mathfrak{M}_{2n-1}$. After a further inner automorphism by a factor of $(1)^{\pm A^{-1}}$, we may assume that $J_1^\tau = \pm J_1$ and also that $X^* = Y = X^*$ for all $X \in \mathfrak{M}_{2n-1}$.

Let $J_\nu$ be obtained from $I^{(2n)}$ by replacing the $\nu$th diagonal element by $-1$. Then

$$(J_1J_{2n})^\tau = \pm \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix}^\tau = \pm \begin{bmatrix} 1 & n' \\ \vrule & \vrule \end{bmatrix},$$

so that $\pm J_{2n}$ is invariant. Similarly, all of the matrices $\pm J_\nu (\nu = 1, \ldots, 2n)$ are invariant. Therefore for any $X \in \mathfrak{M}_{2n-1}$ we have

$$
\pm \begin{bmatrix} 1 & n'' \\ n & X \end{bmatrix} = \pm \begin{bmatrix} 1 & n' \\ n & A_1X^*A_1^{-1} \end{bmatrix}, \cdots, \pm \begin{bmatrix} X & n'' \\ n' & 1 \end{bmatrix} = \pm \begin{bmatrix} A_{2n}X^*A_{2n}^{-1} & n \\ n' & 1 \end{bmatrix},
$$

with $A_\nu \in \mathfrak{M}_{2n-1}$, and in fact $A_1 = I$.

Now suppose that $Z \in \mathfrak{M}_{2n-2}$, and consider $\pm (Z + I^{(2)})$; since it commutes with $J_{2n-1}$ and $J_{2n}$, so does its image. But therefore
\[
A_{2n} \begin{pmatrix} Z & n' \\ n' & 1 \end{pmatrix} A_{2n}^{-1} = \begin{pmatrix} \bar{Z} & n' \\ n' & 1 \end{pmatrix},
\]

where \(Z\) denotes some matrix in \(M_{2n-2}\). From this one easily deduces that \(A_{2n}\) must be of the form \(B \pm (1)\), with \(B \in M_{2n-2}\). By considering the matrices commuting with \(J_v\) and \(J_{2n}\) for \(v = 1, \ldots, 2n-2\) we see that \(A_{2n}\) must be diagonal. Furthermore, it is clear that all of the \(A_v\) (\(v = 1, \ldots, 2n\)) must be diagonal, and all are sections of one diagonal matrix \(D^{(2n)}\). Using the further inner automorphism factor \(D^{-1}\), we find that \(\pm X^\tau = \pm X^*\) for every decomposable matrix \(\pm X \in \mathfrak{P}_{2n}\). Since \(\mathfrak{P}_{2n}\) is generated by the set of its decomposable matrices, the theorem is proved.

Tsing Hua University,
Peking, China.

University of Illinois,
Urbana, Ill.