AUTOMORPHISMS OF THE PROJECTIVE UNIMODULAR GROUP

BY

L. K. HUA AND I. REINER

Notation. Let $\mathfrak{M}_n$ denote the group of $n \times n$ integral matrices of determinant ± 1 (the unimodular group). By $\mathfrak{M}_n^+$ we denote that subset of $\mathfrak{M}_n$ where the determinant is $+1$; $\mathfrak{M}_n^-$ is correspondingly defined. Let $\mathfrak{P}_{2n}$ be obtained from $\mathfrak{M}_{2n}$ by identifying $+X$ and $-X$, $X \in \mathfrak{M}_{2n}$. (This is the same as considering the factor group of $\mathfrak{M}_{2n}$ by its centrum.) We correspondingly obtain $\mathfrak{P}_{2n}^+$ and $\mathfrak{P}_{2n}^-$ from $\mathfrak{M}_{2n}^+$ and $\mathfrak{M}_{2n}^-$. Let $I^{(n)}$ (or briefly I) be the identity matrix in $\mathfrak{M}_n$, and let X' denote the transpose of X. The direct sum of A and B is represented by $A \dotplus B$, while

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

means that A is similar to B.

In this paper we shall find explicitly the generators of the group $\mathfrak{B}_{2n}$ of all automorphisms of $\mathfrak{P}_{2n}$, 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 $\mathfrak{P}_{2n}$.** The following useful result is an immediate consequence of the corresponding theorem for $\mathfrak{M}_{2n}$ (AUT, Theorem 1).

THEOREM 1. *Let $\mathfrak{S}_{2n}$ be the commutator subgroup of $\mathfrak{P}_{2n}$. Then clearly $\mathfrak{S}_{2n} \subset \mathfrak{P}_{2n}^+$. For $n=1$, $\mathfrak{S}_{2n}$ is of index 2 in $\mathfrak{P}_{2n}^+$, while for $n>1$, $\mathfrak{S}_{2n} = \mathfrak{P}_{2n}^+$.*

THEOREM 2. *In any automorphism of $\mathfrak{P}_{2n}$, always $\mathfrak{P}_{2n}^+$ 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

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

Since S and T generate $\mathfrak{M}_2^+$, it follows that $\pm S$ and $\pm T$ generate $\mathfrak{P}_2^+$,

Received by the editors May 18, 1951.

(1) Abh. Math. Sem. Hamburgischen Univ. vol. 3 (1924) p. 167.

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 $\mathfrak{P}_2^+$ or both in $\mathfrak{P}_2^-$; we shall show that the latter alternative is impossible.

Suppose that det S_1=det $T_1=-1$. From $S^2=I$ 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 $\lambda^2+1=0$, 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 $A\in\mathfrak{M}_2$ 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 τ, a new automorphism τ' defined by: $X^{\tau'}=AX^{\tau}A^{-1}$, 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 $J=(1)\dotplus(-1)$ is distinct from $\pm I$ and $\pm S$, that it commutes with S, and that JT is an involution. Hence there exists a matrix $M\in\mathfrak{P}_2$ 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 $(S_1T_1)^3=\pm I$, 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 $ad-bc=-1$. Combining 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 $c=\pm 1$.

But then $ad=0$; from $a-d=\pm 1$ we deduce that $a^2-d^2=\pm 1$, whence $(S_1T_1^2)^3=\pm I$, which is impossible.

Case 2.

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

From $(S_1T_1)^3=\pm I$ 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

$$ad - bc = \{(a + d)^2 + (a - d \pm 1)^2 - 1\}/4 \neq -1.$$

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 $\mathfrak{P}_2^+$.** Let us now determine all automorphisms of $\mathfrak{P}_2$. Since every such automorphism takes $\mathfrak{P}_2^+$ into itself, we begin by considering all automorphisms of $\mathfrak{P}_2^+$.

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

Proof. Let τ be any automorphism of $\mathfrak{P}_2^+$, and define S and T as before; let $S_0\in\mathfrak{M}_2$ be a fixed representative of $\pm S^\tau$. By Theorem 2, $S_0\in\mathfrak{M}_2^+$, and therefore $S_0^2=-I$. Let T_0 be that representative of $\pm T^\tau$ for which $(S_0T_0)^3=I$ is valid. Then $S\rightarrow S_0$, $T\rightarrow T_0$ induces a mapping from $\mathfrak{M}_2^+$ onto itself. The mapping is one-to-one, for although an element of $\mathfrak{M}_2^+$ 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 τ is one. Therefore (AUT, Theorem 2) there exists an $A\in\mathfrak{M}_2$ such that $S_0=\pm ASA^{-1}$, $T_0=\pm ATA^{-1}$. This proves the result.

COROLLARY. *Every automorphism of $\mathfrak{P}_2$ is of the form $X\in\mathfrak{P}_2\rightarrow AXA^{-1}$ for some $A\in\mathfrak{M}_2$.*

(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 $\mathfrak{B}_{2n}$.** Our main result may be stated as follows:

THEOREM 4. *The generators of $\mathfrak{B}_{2n}$ are*

(i) *The set of all inner automorphisms*:

$$\pm X \in \mathfrak{P}_{2n} \rightarrow \pm AXA^{-1} \qquad (A \in \mathfrak{M}_{2n}),$$

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* $J_1=(-1)\dotplus I^{(2n-1)}$. *In any automorphism* τ *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 $n \geqq 2$. Certainly $(J_1^\tau)^2 = \pm I$ and $\det J_1^\tau = -1$. If $(J_1^\tau)^2 = -I$, then the minimum function of J_1^τ is λ^2+1, and its characteristic function must be some power of λ^2+1, whence $\det J_1^\tau = 1$. Therefore $(J_1^\tau)^2 = I$ is valid in $\mathfrak{M}_{2n}$. After a suitable inner automorphism, we may assume that

$$J_1^\tau = W(x, y, z) = L \dotplus \cdots \dotplus L \dotplus (-I)^{(y)} \dotplus I^{(z)},$$

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^τ. 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 $\pm(1\dotplus X_1) \in \mathfrak{P}_{2n}$, 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

$$\begin{pmatrix} S_1 & 2R_1 \\ Q_1 & T_1 \end{pmatrix} \dotplus \begin{pmatrix} S_2 & Q_2 \\ 2R_2 & T_2 \end{pmatrix},$$

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 $\overline{C}W = -W\overline{C}$ is solvable only when $y=z$. The space

$\mathfrak{U}$ of vectors $\mathfrak{u}$ such that $W\mathfrak{u}=\mathfrak{u}$ is of dimension $x+z$, while the space $\mathfrak{V}$ of vectors $\mathfrak{v}$ for which $W\mathfrak{v}=-\mathfrak{v}$ has dimension $x+y$. But if $\overline{C}W=-W\overline{C}$, then $W\overline{C}\mathfrak{u}=-\overline{C}\mathfrak{u}$ and $W\overline{C}^{-1}\mathfrak{v}=\overline{C}^{-1}\mathfrak{v}$, so the dimensions of $\mathfrak{U}$ and $\mathfrak{V}$ must be the same, whence $y=z$. Hence if $y\neq z$, there are no solutions of $\overline{C}W=-W\overline{C}$, $\overline{C}\in\mathfrak{M}_{2n}$.

We may now proceed to find a lower bound for the number of nonsimilar matrices in $\mathfrak{G}_0(x, y, z)$. We briefly denote the elements of $\mathfrak{G}_0$ by $A\dot{+}B$, 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 $A_1\dot{+}B_1$ and $A_2\dot{+}B_2$ are two distinct involutions in $\mathfrak{G}_0$, where either

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

then certainly

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

Now let

$$A = I^{(a_1)} \dot{+} (-I)^{(b_1)} \dot{+} L \dot{+} \cdots \dot{+} L,$$
$$B = I^{(a_2)} \dot{+} (-I)^{(b_2)} \dot{+} L \dot{+} \cdots \dot{+} L,$$

where L occurs c_1 times in A and c_2 times in B; the various elements $A\dot{+}B$ gotten by taking different sets of values of $(a_1, b_1, c_1, a_2, b_2, c_2)$, if they lie in $\mathfrak{G}_0$, are certainly nonsimilar in $\mathfrak{G}_0$, except that $A\dot{+}B$ and $(-A)\dot{+}(-B)$ are the same element of $\mathfrak{G}_0$. Hence the number N of nonsimilar involutions of $\mathfrak{G}_0$ 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 $c_1\leqq(z+1)/2$, $c_2\leqq(y+1)/2$, and that in B instead of L we use L'. (These conditions insure that $A\dot{+}B\in\mathfrak{G}_0$.) As in the previous paper, one readily shows that $N>n(n+1)$ unless $J_1^{\tau}=\pm J_1$. We omit the details.

This leaves only the case where $y=z$. If $\overline{C}W=-W\overline{C}$, then $\overline{C}^kW=(-1)^kW\overline{C}^k$; therefore no odd power of $\overline{C}$ can be $\pm I$. Let p be a prime such that $n<p<2n$. Since $x+y=n$, certainly n is odd, and $p\geqq n+2$. Now $\mathfrak{G}_1$ (being isomorphic to $\mathfrak{M}_{2n-1}$) contains infinitely many elements of order p. However, $\mathfrak{G}_2$ contains only two such elements, since $\overline{C}^p\neq\pm I$ by the above argument, while if $C\in\mathfrak{G}_0$ and $C^p=\pm I$, then setting $C=A^{(n)}\dot{+}B^{(n)}$ 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 $\lambda^p\mp 1$. But the degree of the minimum function is at most n, and therefore is less than $p-1$, whereas $\lambda^p\mp 1$ 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 $C=I^{(n)}\dotplus I^{(n)}$ and $C=-I^{(n)}\dotplus I^{(n)}$. 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 $n \geqq 2$ and assume that Theorem 4 holds for $n-1$. Let τ 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 τ 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,

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

where $\mathfrak{n}$ denotes a column vector all of whose components are zero, and $X \in \mathfrak{M}_{2n-1}$. Thus, τ 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 $(1)\dotplus A^{-1}$, we may assume that $J_1^\tau = \pm J_1$ and also that $X^\tau = Y = X^*$ for all $X \in \mathfrak{M}_{2n-1}$.

Let J_ν be obtained from $I^{(2n)}$ by replacing the νth diagonal element by -1. Then

$$(J_1J_{2n})^\tau = \pm \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & -1 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & \cdots & -1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix}^\tau = \pm \begin{bmatrix} 1 & \mathfrak{n}' \\ \mathfrak{n} & \begin{bmatrix} -1 & \cdots & 0 & 0 \\ \cdot & \cdots & \cdot & \cdot \\ 0 & \cdots & -1 & 0 \\ 0 & \cdots & 0 & 1 \end{bmatrix}^* \end{bmatrix}$$

$$= \pm J_1J_{2n},$$

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

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

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 $\pm(Z \dotplus I^{(2)})$; since it commutes with J_{2n-1} and J_{2n}, so does its image. But therefore

$$A_{2n}\begin{pmatrix} Z & \mathfrak{n} \\ \mathfrak{n}' & 1 \end{pmatrix} A_{2n}^{-1} = \begin{pmatrix} \overline{Z} & \mathfrak{n} \\ \mathfrak{n}' & 1 \end{pmatrix},$$

where $\overline{Z}$ denotes some matrix in $\mathfrak{M}_{2n-2}$. From this one easily deduces that A_{2n} must be of the form $B \dot{+} (1)$, with $B \in \mathfrak{M}_{2n-2}$. By considering the matrices commuting with J_ν and J_{2n} for $\nu = 1, \cdots, 2n-2$ we see that A_{2n} must be diagonal. Furthermore, it is clear that all of the A_ν $(\nu = 1, \cdots, 2n)$ 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.