AUTOMORPHISMS OF THE GAUSSIAN UNIMODULAR GROUP

BY

JOSEPH LANDIN AND IRVING REINER(1)

1. **Introduction.** Let G be the ring of Gaussian integers, and G_n the group of $n\times n$ unimodular matrices over G. Define $G_n^+ = \{X\in G_n: \det X = +1\}$, and likewise define G_n^-, G_n^i, G_n^{-i}. Let X' = transpose of X, $\overline{X}$ = conjugate of X, $I^{(n)}$ = identity matrix in G_n, 0 = null matrix of appropriate size, and $A \dotplus B$ = direct sum of A and B. For $X, Y\in G_n$, write $X\sim Y$ if X and Y are conjugate in G_n. We assume throughout that $n\geqq 2$. For a = unit in G_n and $A\in G_{n-1}$ define $(a)\dotplus^r A$ to be the matrix B for which $b_{rr}=a$, $b_{rj}=b_{jr}=0$ for $j\neq r$, and such that the submatrix obtained by deleting the rth row and rth column from B coincides with A. Thus $(a)\dotplus^1 A$ coincides with the ordinary direct sum $(a)\dotplus A$. We use $[a_1, \cdots, a_n]$ to denote the diagonal matrix with diagonal elements $a_1, \cdots, a_n$.

The generators of G_n are [1, p. 425]

$$(1.1)\qquad T=\begin{pmatrix}1&1\\0&1\end{pmatrix}\dotplus I^{(n-2)},\quad S=\begin{bmatrix}0&\cdots&0&(-1)^{n-1}\\1&\cdots&0&0\\\cdot&\cdot\cdot\cdot&\cdot&\cdot\\0&\cdots&1&0\end{bmatrix},\quad P=(i)\dotplus I^{(n-1)}.$$

For the case $n=2$ we shall use T_0, S_0, P_0 as symbols for the generators, where S_0 now denotes the matrix

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

In this paper we prove the following

Main Theorem. *Let $\mathfrak{A}_n$ be the automorphism group of G_n. Then $\mathfrak{A}_n$ is generated by*

1. $X\to AXA^{-1}$, $A\in G_n$;
2. $X\to X'^{-1}$ (*may be omitted when* $n=2$);
3. $X\to \overline{X}$;
4. $X\to(\det X)^k X$, *where* $k=1$ *if* n *is even, and* $k=2$ *if* n *is odd*;
5. *For* $n=2$ *only*, $(P_0, S_0, T_0)\to(P_0, -S_0, -T_0)$.

Presented to the Society February 25, 1956; received by the editors March 12, 1956.

(1) The work of the second author was supported in part by a research contract with the National Science Foundation.

We may remark that 1., 2. and 3. are obviously automorphisms. We shall prove later (Lemmas 3.2 and 3.3) that 4. and 5. are also automorphisms. For $n=2$, it is easily verified that 2. is expressible in terms of the other automorphisms in the list, hence may be omitted.

2. **Involutions in G_n.** We begin by giving a canonical form for involutions in G_n under conjugacy. Throughout this paper let ξ denote $1+i$, and set

$$J_\alpha = \begin{pmatrix} -1 & 0 \\ \alpha & 1 \end{pmatrix}, \tag{2.1}$$

$$W(a, b, c, d) = (J_1 \dotplus \cdots \dotplus J_1) \dotplus (J_\xi \dotplus \cdots \dotplus J_\xi) \dotplus (-I)^{(c)} \dotplus I^{(d)}, \tag{2.2}$$

where a J_1's and b J_ξ's occur in (2.2).

Theorem 2.1. *As (a, b, c, d) range over all non-negative integers for which $2a+2b+c+d=n$, the matrices $W(a, b, c, d)$ give a full set of non-conjugate involutions in G_n.*

Proof. The proof given in [2, pp. 336–337] can be used with a few modifications, due to the fact that G is a principal ideal ring. From the reasoning there, it is easily established that for any involution $X \in G_n$, we have

$$X \sim \begin{pmatrix} -I^{(q)} & 0 \\ T & I^{(p)} \end{pmatrix} \tag{2.3}$$

where T is a diagonal matrix with entries 0, 1 or ξ. The right-hand side of (2.3) is conjugate to some $W(a, b, c, d)$, and it is not hard to verify that two distinct $W(a_j, b_j, c_j, d_j)$ $(j=1, 2)$ cannot be conjugate in G_n.

We may remark that p, q in (2.3) are the dimensions of the plus-space X^+, and the minus-space X^-, respectively, of the involution X. Call X a (p, q) involution in such case. We find at once that $W(a, b, c, d)$ is an $(a+b+d, a+b+c)$ involution.

Our next step will be to characterize the $\pm(1, n-1)$ involutions in G_n. Let $\mathfrak{C}(S)$ denote the centralizer in G_n of a set S of elements in G_n.

Lemma 2.1. *Let $X \in G_n$ be an involution and let*

$$\mathfrak{M} = \{M \in \mathfrak{C}(X) : M \equiv X \pmod 2\}.$$

Then the only involutions in $\mathfrak{C}(\mathfrak{M})$ are $\pm I^{(n)}$, $\pm X$.

Proof. For fixed $B \in G_n$ we note that $M \in \mathfrak{M}$ implies $BMB^{-1} \in \mathfrak{C}(BXB^{-1})$ and $BMB^{-1} \equiv BXB^{-1} \pmod 2$, and conversely. Without loss of generality, we may therefore take X in the form of the right-hand side of (2.3). In that case, $\mathfrak{C}(X)$ consists of all elements $K \in G_n$ given by

$$K = \begin{pmatrix} A & 0 \\ C & D \end{pmatrix}, \qquad A \in G_q, \qquad D \in G_p, \qquad C = (DT - TA)/2. \tag{2.4}$$

Since $A \equiv -I \pmod 4$ and $D \equiv I \pmod 4$ imply $C \equiv T \pmod 2$ we see that $\mathfrak{M}$ contains all elements K satisfying

$$A \equiv -I \pmod 4, \qquad D \equiv \mathrm{I} \pmod 4. \tag{2.5}$$

Now if $Y \in \mathfrak{C}(\mathfrak{M})$, then Y commutes with all K satisfying (2.5). Set

$$Y = \begin{pmatrix} Y_1 & 0 \\ Y_2 & Y_3 \end{pmatrix}.$$

In that case, Y_1 commutes with all $A \in G_q$ for which $A \equiv -I \pmod 4$, and Y_3 commutes with all $D \in G_p$ for which $D = I \pmod 4$. This shows at once that $Y_1 = u \cdot I$, $Y_3 = v \cdot I$, u, v units. If, further, Y is to be an involution, it follows that $Y_1 = \pm I$, $Y_3 = \pm I$. Since $Y \in \mathfrak{C}(\mathfrak{M})$ implies $Y \in \mathfrak{C}(X)$, therefore $Y_2 = (Y_3 T - T Y_1)/2$, and Y_2 is uniquely determined by Y_1 and Y_3. Hence $\mathfrak{C}(\mathfrak{M})$ contains at most four involutions.

THEOREM 2.2. *The image of any* $(1, n-1)$ *involution in* G_n *under any* $\tau \in \mathfrak{A}_n$ *must be either a* $(1, n-1)$ *or an* $(n-1, 1)$ *involution.*

Proof. The result is trivial for $n=2$ and $n=3$. Assume hereafter that $n>3$. We shall characterize the $\pm(1, n-1)$ involutions in G_n by intrinsic properties using a method due to Mackey [5]; see also Rickart [7]. Letting $\mathfrak{C}^2(\cdots)$ denote $\mathfrak{C}(\mathfrak{C}(\cdots))$, define for an involution $X \in G_n$

$$\nu(X) = \mathrm{Max}\ (\text{number of involutions in } \mathfrak{C}^2(X, X_1)), \tag{2.6}$$

where X_1 ranges over all involutions in $\mathfrak{C}(X)$. Taking X to be a (p, q) involution we shall show that $\nu(X) \geqq 16$ if $\mathrm{Min}\ (p, q) > 1$, while $\nu(X) = 8$ if $\mathrm{Min}\ (p, q) = 1$; this will imply the theorem.

To begin with, note that $\nu(X)$ depends only upon the conjugate class of the involution X. We may therefore take X as the right-hand side of (2.3), and then $\mathfrak{C}(X)$ is given by all K satisfying (2.4). For $\mathrm{Min}\ (p, q) > 1$ define

$$X_1 = \begin{pmatrix} -1 & & & \\ & I & & \\ & & -1 & \\ & & & I \end{pmatrix}, \qquad W = \begin{pmatrix} 1 & & & \\ & I & & \\ -t & & -1 & \\ & & & I \end{pmatrix} \tag{2.7}$$

where we have set T (occurring in (2.3)) $= (t) \dotplus T_1$. Then both X_1 and W are involutions in $\mathfrak{C}(X)$. Since every $K \in \mathfrak{C}(X_1)$ is of the form

$$K = \begin{pmatrix} a & & b & \\ & A_1 & & B_1 \\ c & & d & \\ & C_1 & & D_1 \end{pmatrix},$$

we see that the general element of $\mathfrak{C}(X, X_1)$ is given by

$$K = \begin{bmatrix} a & 0 & \\ & A_1 & \\ c & d & \\ & C_1 & D_1 \end{bmatrix}, \tag{2.8}$$

where

$$c = (d - a)t/2, \qquad C_1 = (D_1 T_1 - T_1 A_1)/2. \tag{2.9}$$

But then the involution W defined above commutes with all such K, so that $\mathfrak{C}^2(X, X_1)$ contains the 16 distinct involutions $\pm X^a X_1^b W^c$, $(a, b, c = 0, 1)$, and $\nu(X) \geqq 16$ for Min $(p, q) > 1$. (Indeed, $\nu(X) = 16$ for this case although we do not need the stronger result here.)

We now show that $\nu(X) = 8$ for $p = 1$. We may choose

$$X = \begin{pmatrix} -1 & 0 \\ \mathfrak{t} & I^{(n-1)} \end{pmatrix}, \tag{2.10}$$

$\mathfrak{t} = (t, 0, \cdots, 0)'$. Then $\mathfrak{C}(X)$ consists of all elements

$$K = \begin{pmatrix} a & 0 \\ \mathfrak{c} & D \end{pmatrix}, \quad a \in G_1, \quad D \in G_{n-1}, \quad \mathfrak{c} = (D - aI)\mathfrak{t}/2. \tag{2.11}$$

To compute $\nu(X)$ we may assume that $X_1 \in \mathfrak{C}(X)$ is given by

$$X_1 = \begin{pmatrix} 1 & 0 \\ \mathfrak{u} & U \end{pmatrix}, \qquad \mathfrak{u} = (U - I)\mathfrak{t}/2, \tag{2.12}$$

where $U \in G_{n-1}$ is an involution. Then $\mathfrak{C}(X, X_1)$ consists of all K given by (2.11) for which $D \in \mathfrak{C}(U)$. In particular, whenever $D \in \mathfrak{C}(U)$ and $D \equiv U$ (mod 2) then (2.11), with $a = 1$, defines an element of $\mathfrak{C}(X, X_1)$. If now $L \in \mathfrak{C}^2(X, X_1)$ is an involution, then L has the form

$$L = \begin{pmatrix} a^* & 0 \\ \mathfrak{c}^* & D^* \end{pmatrix}, \qquad \mathfrak{c}^* = (D^* - a^* I)\mathfrak{t}^*/2$$

and L commutes with every K for which $a = 1$, $D \in \mathfrak{C}(U)$ and $D \equiv U$ (mod 2). Then D^* commutes with all such D, whence by Lemma 2.1, $D^* = \pm I$ or $\pm U$. Certainly $a^* = \pm 1$. Since a^* and D^* uniquely determine $\mathfrak{c}^*$ it follows that $\mathfrak{C}^2(X, X_1)$ contains at most 8 involutions. Since $\pm I$, $\pm X$, $\pm X_1$, $\pm X X_1$ are all in $\mathfrak{C}^2(X, X_1)$ we have established that $\nu(X) = 8$ if Min $(p, q) = 1$.

Let us now set

$$L_\alpha = J_\alpha \dotplus I^{(n-2)}, \qquad \alpha = 0, 1 \text{ or } \xi.$$

Then every $(1, n-1)$ involution in G_n is conjugate to one of L_0, L_1, L_ξ, and hence any $\tau \in \mathfrak{A}_n$ maps L_0 onto $\pm AL_\alpha A^{-1}$ for some $A \in G_n$, where $\alpha = 0$, 1 or ξ.

THEOREM 2.3. *For $\tau \in \mathfrak{A}_n$ there exists $A \in G_n$ such that $L_0^\tau = \pm AL_0A^{-1}$.*

Proof. For $n \geqq 3$ we shall use the method of maximal sets of involutions (see [6]). By a *maximal set* in G_n we mean an abelian group of 2^n involutions in G_n. As in [6] we may at once establish the following results:

(i) The number of elements in any abelian group of involutions is $\leqq 2^n$.

(ii) A maximal set contains precisely $C_{n,p}$ involutions of type (p, q).

(iii) Any maximal set may be obtained from a *generating matrix* M^n (whose columns are primitive vectors with components in G) by choosing any p columns of M as basis for the plus-space W^+ of an involution, and the remaining q columns as basis for W^-. Each such choice defines a unique involution W, and this process gives rise to $C_{n,p}$ involutions of type (p, q). If this process is carried out for $p = 0, 1, \cdots, n$, an abelian group of 2^n involutions is obtained. Furthermore, if each of the invariant factors of M is either 1, ξ or 2, then each of the 2^n involutions will lie in G_n. In this case we call M a *permissible* generating matrix.

(iv) Two permissible generators M_1, M_2 give rise to conjugate maximal sets if and only if there exist $A, B \in G_n$, where B is obtained from I by permuting columns and multiplying them by units, such that $M_2 = AM_1B$. In such case call M_1, M_2 *equivalent.*

(v) Every permissible generating matrix is equivalent to one of the form

$$M^{(n)} = \begin{pmatrix} I^{(r)} & A & B \\ 0 & \xi I^{(s)} & C \\ 0 & 0 & 2I^{(t)} \end{pmatrix}, \tag{2.13}$$

where the columns of M are primitive, the elements of A are 0's and 1's, those of B are 0, 1 or ξ, and those of C are 0 or ξ.

Now define M_1 by: $s = 1$, $t = 0$, all entries in A are 1's; M_2 by: $r = 1$, $t = 0$, all entries in A are 1's; M_3 by: $s = 0$, $t = 1$, all entries in B are 1's; M_4 by: $r = 1$, $s = 0$, all entries in B are 1's. The maximal sets generated by M_1 and M_2 are nonconjugate (since $n \geqq 3$), and each contains n involutions which are conjugate to L_ξ. The maximal sets generated by M_3 and M_4 are nonconjugate, and each contains n involutions conjugate to L_1.

On the other hand, it is easy to show that any two maximal sets, each of which contains n involutions conjugate to L_0, must be conjugate. Hence for $n \geqq 3$ the class of L_0 is characterized by intrinsic properties, and the theorem holds. We postpone until later the proof for $n = 2$.

3. General remarks.

Before we turn to the question of determining all automorphisms of G_n, it is desirable to state several lemmas.

LEMMA 3.1. *For any automorphism τ of G_n, either* $\det X^\tau = \det X$ *for all $X \in G_n$ or* $\det X^\tau =$ *conjugate of* $\det X$ *for all $X \in G_n$.*

Proof. Let $S^{(k)}=P^{-k}SP^k$, $T^{(k)}=P^{-k}TP^k$. Since every $X\in G_n$ is expressible as a power product of P, S and T we find that every X can be written as

$$X = P^m\Pi(S, T, S^{(k)}, T^{(k)}),$$

and then $\det X=i^m$. Exactly as in [2, Corollary 1 of Theorem 1], we deduce that $\det S^\tau=\det T^\tau=1$, whence also $\det (S^{(k)})^\tau=\det (T^{(k)})^\tau=1$. Hence we have

$$\det X^\tau = (\det\ P^\tau)^m.$$

But $\det P^\tau=\pm i$, since if $\det P^\tau=\pm 1$, then $G_n^\tau\subset(G_n^+\cup G_n^-)$, which is impossible. Hence $\det X^\tau=(\pm i)^m$, where $\det X=i^m$, whence the result follows.

LEMMA 3.2. *For n even the mapping $X\to(\det X)X$ is an automorphism of G_n. For n odd $X\to(\det X)^2X$ is an automorphism of G_n.*

Proof. Consider first the case where n is even. The mapping is clearly an endomorphism of G_n. If $X^\tau=I$, then $(\det X)X=I$ whence $X=u\cdot I$, $u=(\det X)^{-1}$. But then $\det X=u^n$, so $u^n=u^{-1}$, whence $u=1$ (because n is even). Therefore τ is one-to-one.

To show that τ is onto, we observe that $S^\tau=S$, $T^\tau=T$; set $Q=-iP$ for $n\equiv 0 \pmod 4$, and $Q=iP$ for $n\equiv 2 \pmod 4$. In either case $Q^\tau=P$, whence τ is onto.

A similar proof is valid for odd n.

LEMMA 3.3. *For $n=2$, the mapping τ defined by $P_0^\tau=P_0$, $S_0^\tau=-S_0$, $T_0^\tau=-T_0$ is an automorphism of G_2.*

Proof. To begin with, we must show that τ induces a well-defined mapping of G_2 into itself. This will be so if we can show that if a power product $\prod(P_0, S_0, T_0)=I$ in G_2 then the total number of factors of S_0 and T_0 is even.

Letting $\xi=1+i$ as usual, we remark that since

$$P_0 \equiv I \pmod{\xi}, \qquad \prod (P_0, S_0, T_0) = I$$

implies

$$\prod(S_0, T_0) \equiv I \pmod{\xi}. \tag{3.1}$$

However, there are only 6 elements in G_2 mod ξ, represented by I, S_0, T_0, S_0T_0, T_0S_0, $S_0T_0S_0$, since $S_0^2\equiv T_0^2\equiv I \pmod{\xi}$. Any power product $\prod(S_0, T_0)$ can be brought into one of these 6 forms by repeated use of $S_0^2\equiv T_0^2\equiv(S_0T_0)^3\equiv I \pmod{\xi}$. Hence in the left-hand side of (3.1), the total number of S_0's and T_0's must be even.

Now that τ has been shown to be well-defined we see at once that τ is onto. Further $\tau^2=1$ implies τ is one-to-one, whence τ is indeed an automorphism of G_2.

4. **Generators of $\mathfrak{A}_2$.** We shall obtain here the generators of $\mathfrak{A}_2$, the automorphism group of G_2. As before, define

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

Our previous discussion shows that $\pm I$ and J_α, $\alpha = 0, 1, \xi$ constitute a full set of nonconjugate involutions in G_2.

LEMMA 4.1. *For any $\tau \in \mathfrak{A}_2$, there exists an $A \in G_2$ such that $J_1^\tau = AJ_1A^{-1}$.*

Proof. By Theorem 2.2, to within an inner automorphism we have $J_1^\tau = \pm J_\alpha$, $\alpha = 0$, 1 or ξ. However, the centralizer $\mathfrak{C}(J_1)$ contains 8 elements, whereas $\mathfrak{C}(J_\alpha)$ contains 16 elements for $\alpha = 0$ or ξ. This completes the proof since $-J_1$ is conjugate to J_1.

THEOREM 4.1. *$\mathfrak{A}_2$ is generated by the automorphisms*

1. $X \to AXA^{-1}$,
2. $X \to X'^{-1}$,
3. $X \to \overline{X}$,
4. $X \to (\det X)X$,
5. $(P_0, S_0, T_0) \to (P_0, -S_0, -T_0)$.

Proof. Let $\tau \in \mathfrak{A}_2$; changing τ by an inner automorphism if necessary, we may assume hereafter that $J_1^\tau = J_1$. Let $K = S_0 J_0$, then

$$K = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad KJ_1 = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}, \quad (KJ_1)^3 = -I, \quad K^2 = I. \tag{4.1}$$

Let us put

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

Using the fact $J_1^\tau = J_1$, (4.1) implies that

$$-a + b + d = 1, \quad b(a + d) = c(a + d) = 0, \quad a^2 + bc = d^2 + bc = 1.$$

These imply that $d = -a$, $b = 2a + 1$, and

$$a^2 + (2a + 1)c = 1,$$

that is

$$4(a + c)^2 - (2c - 1)^2 = 3.$$

There are only 4 solutions in Gaussian integers of this equation, and therefore K^τ has only 4 possible expressions given by K, K_1, K_2, K_3 where

$$K_1 = \begin{pmatrix} 1 & 3 \\ 0 & -1 \end{pmatrix}, \quad K_2 = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}, \quad K_3 = \begin{pmatrix} -2 & -3 \\ 1 & 2 \end{pmatrix}.$$

A further inner automorphism by a factor of J_1 leaves J_1^τ unaltered, but takes

K_2 into K, and K_3 into K_1. We may therefore assume from now on that $J_1^\tau = J_1$ and either $K^\tau = K$ or $K^\tau = K_1$. In the latter case, replace τ by the automorphism

$$X \to (V^{-1}X^\tau V)'^{-1}, \quad \text{where} \quad V = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}.$$

This new automorphism leaves J_1 and K invariant. Hence in all cases, after changing τ by automorphisms chosen from the list in Theorem 4.1, we may assume that $J_1^\tau = J_1$ and $K^\tau = K$.

LEMMA 4.2. *If $\tau \in \mathfrak{A}_2$ is such that $J_1^\tau = J_1$ and $K^\tau = K$, then $J_0^\tau = \pm J_0$.*

Proof. We have $J_0 K = -KJ_0$, $J_0^2 = I$. Setting

$$J_0^\tau = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

we have $d = -a$, $c = -b$, $a^2 - b^2 = 1$. Solving this last equation in Gaussian integers, we find that there are only 4 possibilities for J_0^τ, namely $\pm J_0$ or $\pm iS_0$.

Suppose now that $J_0 = \pm iS_0$. Since $J_0 = P_0^2$, setting

$$P_0^\tau = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

we obtain

$$\begin{pmatrix} a^2 + bc & b(a + d) \\ c(a + d) & d^2 + bc \end{pmatrix} = \pm \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

Hence $a+d$ is a unit. On the other hand,

$$a^2 + d^2 = -2bc, \qquad (a + d)^2 = 2(ad - bc),$$

so $(a+d)^2$ is a nonunit. This is a contradiction, whence J_0^τ must be $\pm J_0$.

We have now shown that by changing the given τ by automorphisms in the list, we can assume that

$$J_0^\tau = \pm J_0, \qquad J_1^\tau = J_1, \qquad K^\tau = K.$$

CASE I. $J_0^\tau = J_0$. Then $S_0 = KJ_0$ implies $S_0^\tau = S_0$, and $T_0 = KJ_0J_1K$ implies $T_0^\tau = T_0$. From $P_0^2 = J_0$, setting

$$P_0^\tau = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

we have

$$a^2 + bc = -1, \qquad d^2 + bc = 1, \qquad b(a + d) = c(a + d) = 0.$$

These imply that $b=c=0$, and $a=\pm i$, $d=\pm 1$. Hence $P_0^\tau=\pm P_0$ or $\pm\overline{P}_0$. In the latter case, changing τ by $X\rightarrow\overline{X}$, we may assume $P_0^\tau=\pm P_0$. This new τ is the automorphism $X\rightarrow(\det X)^m X$ where $m=4$ or 2, and hence is a product of automorphisms on the list.

CASE II. $J_0^\tau=-J_0$. As above, we find that $S_0^\tau=-S_0$, $T_0^\tau=-T_0$, $P_0^\tau=\pm iP_0$ or $\pm i\overline{P}_0$. In the latter case, change τ by $X\rightarrow\overline{X}$ to obtain

$$S_0^\tau = -S_0, \qquad T_0^\tau = -T_0, \qquad P_0^\tau = \pm iP_0.$$

This automorphism is an obvious product of automorphisms on the list.

This completes the proof of Theorem 4.1. We may remark that $X\rightarrow X'^{-1}$ can be omitted from the list, since it can be expressed as a product of the other automorphisms on the list. Further, Theorem 4.1 implies Theorem 2.3 for the case $n=2$.

5. **Generators of $\mathfrak{A}_3$.** In this section we prove the main theorem for the case $n=3$.

STEP 1. Let D_j be obtained from $I^{(3)}$ by changing the jth diagonal element to -1. Given any automorphism $\tau\in\mathfrak{A}_3$, we may assume by Theorem 2.3 (after changing τ by an inner automorphism) that $D_1^\tau=\pm D_1$. In that case τ maps $\mathfrak{C}(D_1)$ onto itself, that is,

$$\begin{pmatrix} a & 0 \\ 0 & A \end{pmatrix}^\tau = \begin{pmatrix} b & 0 \\ 0 & B \end{pmatrix} \tag{5.1}$$

where a is a unit in G, $A\in G_2$. By Lemma 3.1 τ: $G_3^+\rightarrow G_3^+$ so that τ: $\mathfrak{C}(D_1)\cap G_3^+\rightarrow\mathfrak{C}(D_1)\cap G_3^+$. For each $A\in G_2$ choose a to be a unit for which $a\dotplus A\in G_3^+$. Then b and B in (5.1) are uniquely determined by A. Set

$$\begin{pmatrix} a & 0 \\ 0 & A \end{pmatrix}^\tau = \begin{pmatrix} \lambda(A) & 0 \\ 0 & A^\sigma \end{pmatrix}, \quad \text{where} \quad a\cdot\det A = 1,\ A \in G_2. \tag{5.2}$$

Then λ: $G_2\rightarrow G_1$ is a homomorphism, as is σ: $G_2\rightarrow G_2$. Since $\lambda(A)\cdot\det A^\sigma=1$ we see that if $A^\sigma=I$ then $\lambda(A)=1$, and so $A=I$. Hence σ is one-to-one, and from this we see that σ is an automorphism of G_2. Consequently $\det A^\sigma=\det A$ always or conjugate of $\det A$ always, whence $\lambda(A)=a$ always or $\bar{a}$ always. Therefore $\lambda(A)=1$ for $A\in G_2^+$ and $\lambda(A)=-1$ for $A\in G_2^-$.

Using the results of the preceding section, we deduce that there exists a $Y\in G_2$ such that

$$A^\sigma = (\det A)^m Y A^* Y^{-1}$$

for all $A\in G_2$ where A^* is obtained from A by applying neither, or one, or both of automorphisms 3., 5. (§4). If we change τ by an inner automorphism with a factor of $1\dotplus Y^{-1}$, we may then assume that $A^\sigma=(\det A)^m A^*$, and that $D_1^\tau=\pm D_1$ is still valid.

Let us apply the above results to evaluate D_j^τ, $j=2, 3$. We have

$$(D_1D_2)^\tau = \begin{Bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{Bmatrix}^\tau = \begin{pmatrix} \lambda(A) & 0 \\ 0 & A^\sigma \end{pmatrix},$$

where $A=(-1)\dotplus(1)$. Then $\lambda(A)=-1$ by the above remarks since $A\in G_2^-$. Further, $A=P_0^2$, so $A^*=A$ for any choice of $*$. Therefore $A^\sigma=\pm A$, whence $(D_1D_2)^\tau=D_1D_2$ or D_1D_3. The latter case is reduced to the former by changing τ by an inner automorphism with factor $(1)\dotplus K$ where K is given in (4.1). Therefore we obtain $D_1^\tau=\pm D_1$, $D_2^\tau=\pm D_2$. Since $(-I)^\tau=-I$ we also have $D_3^\tau=\pm D_3$. Thus, starting with any $\tau\in\mathfrak{A}_3$ and changing τ by inner automorphisms, we arrive at a new τ for which $D_j^\tau=\pm D_j$, $j=1, 2, 3$.

STEP 2. Now let $\tau\in\mathfrak{A}_3$ satisfy $D_r^\tau=\pm D_r$, where $r=1, 2, 3$. By the preceding discussion we may set

$$((a) +^r A)^\tau = (\lambda_r(A) +^r A^{\sigma_r}), \tag{5.3}$$

where $A\in G_2$ is arbitrary, a is a unit such that $a\cdot\det A=1$, $\lambda_r\colon G_2\to G_1$ is a homomorphism such that either $\lambda_r(A)=a$ for all $A\in G_2$ or $\lambda_r(A)=\bar{a}$ for all $A\in G_2$, and $\sigma_r\in\mathfrak{A}_2$ is expressible as

$$A^{\sigma_r} = (\det A)^{m_r}Y_rA^{\omega_r}Y_r^{-1}, \qquad \text{for all } A\in G_2, \tag{5.4}$$

where $Y_r\in G_2$, and A^{ω_r} is obtained by applying to A neither, or one, or both of automorphisms 3. and 5. (§4).

Now we evaluate $((-1)\dotplus A)^\tau$ where $A=(-1)\dotplus(1)$. By the above this yields

$$Y_1AY_1^{-1} = \pm A$$

whence Y_1 is either diagonal or anti-diagonal, that is

$$Y_1 = \begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix} \quad \text{or} \quad Y_1 = \begin{pmatrix} 0 & u \\ v & 0 \end{pmatrix},$$

u and v units. A similar argument shows that each Y_r is either diagonal or anti-diagonal.

CASE I. Suppose to begin with that at least one Y_r is diagonal; without loss of generality we may assume that Y_1 is diagonal. After an inner automorphism with factor $(1)\dotplus Y_1^{-1}$ we may assume that $Y_1=I$ in (5.4); Y_2 and Y_3 will now be different, but $D_r^\tau=\pm D_r$ is still valid. We may again deduce that Y_3 is either diagonal or anti-diagonal.

CASE I(a). Suppose Y_3 is diagonal, say $Y_3=[u, v]$. Then changing τ by an inner automorphism with factor $[u^{-1}, v^{-1}, v^{-1}]$ we still have $Y_1=I$, $D_r^\tau=\pm D_r$, and now also $Y_3=I$. Therefore

$$T^{\tau} = (T_0 \dot{+} (1))^{\tau} = T_0^{\omega_3} \dot{+} (1),$$

where now $T_0^{\omega_3} = \pm T_0$; the minus sign occurs if and only if automorphism 5. (§4) is one of the factors of ω_3. We show next that $T_0^{\omega_3} = -T_0$ is impossible.

For, if $T^{\tau} = -T_0 \dot{+} (1)$, then $(S_0 \dot{+} (1))^{\tau} = -S_0 \dot{+} (1)$. Set

$$U = ((1) \dot{+} S_0) \cdot (S_0 \dot{+} (1)) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}. \tag{5.5}$$

Then $U^{\tau} = ((1) \dot{+} (\pm S_0))(-S_0 \dot{+} (1)) = U_1$ or U_2, according to the sign, where

$$U_1 = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix}, \qquad U_2 = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{pmatrix}.$$

Set $Z = TU^2$; then

$$T' = T_0' \dot{+} (1) = (UZ^{-1})^2 UZ^2 \tag{5.6}$$

and $T_0' = S_0^{-1} T_0 S_0$. Therefore $(T_0')^{\omega_3} = -T_0'$. Applying τ to both sides of (5.6), and using $U^{\tau} = U_1$ or U_2 we obtain a contradiction. Hence $T_0^{\omega_3} = -T_0$ cannot occur.

We may now assume that both T and $S_0 \dot{+} (1)$ are invariant under τ. In that case, again defining U by (5.5), U^{τ} has the two possible values U, U_3, where $U_3 = D_3 U D_3$. But $S = U^2$ so that either $S^{\tau} = S$ or $S^{\tau} = D_3 S D_3$.

In order to find P^{τ}, we observe that

$$V = D_1 D_2 \cdot iP = [1, -i, i] = (1) \dot{+} V_1$$

where $V_1 = [-i, i]$; hence $V = (1) \dot{+} V_1^{\sigma_1}$. But $V_1 = P_0^3 S_0^{-1} P_0 S_0$, whence $V_1^{\sigma_1} = V_1$ or $\overline{V}_1$. Using the fact that $(iI)^{\tau} = \pm iI$ we obtain $P^{\tau} = \pm P$ or $\pm \overline{P}$. In the latter case, change τ by the automorphism 3. to get $P^{\tau} = \pm P$. If $P^{\tau} = -P$ change τ by the automorphism 4. to get $P^{\tau} = P$. Hence after changing τ by automorphisms on the list, we may assume $T^{\tau} = T$, $S^{\tau} = D_3 S D_3$, $P^{\tau} = P$. But then τ is just an inner automorphism by a factor of D_3, and therefore is on our list. This completes the proof for the present case.

CASE I(b). Suppose next that Y_3 is anti-diagonal, say

$$Y_3 = \begin{pmatrix} 0 & u \\ v & 0 \end{pmatrix}.$$

After changing τ by an inner automorphism with factor $[u^{-1}, -v^{-1}, -v^{-1}]$, we may assume that $Y_1 = I$, $D_r^{\tau} = \pm D_r$ and $Y_3 = S_0$. Then $T^{\tau} = \pm S_0^{-1} T_0 S_0 \dot{+} (1)$; the same type of argument as above shows that the minus sign is impossible. Hence $T^{\tau} = S_0^{-1} T_0 S_0 \dot{+} (1) = T'^{-1}$, and we find again that either $U^{\tau} = U$ or $U^{\tau} = U_3$, whence $S^{\tau} = S$ or $S^{\tau} = D_3 S D_3^{-1}$. Furthermore, we obtain $P^{\tau} = \pm P$ or

$\pm\overline{P}$ as before, and changing τ by 3. and 4. as needed, we get $P^\tau = P$. Now change τ by 2. Since $S = S'^{-1}$, $\overline{P} = P'^{-1}$ we find that $T^\tau = T$, $S^\tau = S$ or D_3SD_3, $P^\tau = \overline{P}$ which is clearly a product of automorphisms on the list. We have completed the proof for this case.

CASE II. Suppose that in (5.4) each Y_r is anti-diagonal. After an inner automorphism by a suitably chosen diagonal matrix, we may assume that $Y_1 = Y_3 = S_0$. We then find that $T^\tau = (\pm T_0'^{-1}) \dotplus (1)$, and the same reasoning as before shows that the minus sign cannot occur. Thence we obtain $(S_0 \dotplus (1))^\tau = S_0 \dotplus (1)$, and $S^\tau = S$ or D_3SD_3. In the latter case, an inner automorphism by a factor of D_3 gives a new τ with $T^\tau = T'^{-1}$, $S^\tau = S$. Changing this τ by $X \to X'^{-1}$ we arrive at an automorphism τ which leaves U, S and T invariant. The same reasoning as in Case I(a) shows that $P^\tau = \pm P$ or $\pm\overline{P}$, and the remainder of the proof is as before.

6. **Generators of $\mathfrak{A}_n$.** We are now ready to prove the main theorem by induction on n.

We suppose $n \geqq 4$, and that the result holds for $n-1$. Let D_j be the diagonal matrix $[1, \cdots, 1, -1, 1, \cdots, 1]$ with -1 occurring in the jth position. By Theorem 2.3, given any $\tau \in \mathfrak{A}_n$, we may change τ by an inner automorphism so as to achieve $D_1^\tau = \pm D_1$. Therefore τ maps $\mathfrak{C}(D_1) \cap G_n^+$ onto itself. Hence if $A \in G_{n-1}$ and $a \cdot \det A = 1$, we have

$$\begin{pmatrix} a & 0 \\ 0 & A \end{pmatrix}^\tau = \begin{pmatrix} \lambda_1(A) & 0 \\ 0 & A^{\sigma_1} \end{pmatrix}$$

where $\lambda_1 : G_{n-1} \to G_1$ is a homomorphism and σ_1 is an automorphism of G_{n-1}. As before, $\lambda_1(a) = a$ always or $\bar{a}$ always. Using the induction hypothesis, we may write

$$A^{\sigma_1} = (\det A)^{m_1} Y_1 A^{\omega_1} Y_1^{-1}, \qquad Y_1 \in G_{n-1},$$

where ω_1 is a product of automorphisms chosen from 2. or 3. After an inner automorphism with factor $(1) \dotplus Y_1^{-1}$, we may take $Y_1 = I$. Now $D_1D_2 = [-1, -1, 1, \cdots, 1]$; by computing $(D_1D_2)^\tau$ we find that $D_2^\tau = \pm D_2$. Likewise $D_r^\tau = \pm D_r$, $1 \leqq r \leqq n$. We may therefore write

$$((a) \dotplus^r A)^\tau = \lambda_r(A) \dotplus^r (\det A)^{m_r} Y_r A^{\omega_r} Y_r^{-1}, \tag{6.1}$$

where $A \in G_{n-1}$ is arbitrary, $a \cdot \det A = 1$, $\lambda_r : G_{n-1} \to G_1$ is a homomorphism such that either $\lambda_r(A) = a$ always or $\bar{a}$ always, where $Y_r \in G_{n-1}$, and ω_r is a product of some (of none) of the automorphisms 2., 3. (Further, we have already seen that we may choose $Y_1 = I$.)

Now let $Z \in G_{n-2}$; since $(I^{(2)} \dotplus Z) \in \mathfrak{C}(D_1) \cap \mathfrak{C}(D_2)$ we can compute $(I^{(2)} \dotplus Z)^\tau$ in two ways. This gives

$$Y_1 \begin{pmatrix} 1 & 0 \\ 0 & Z \end{pmatrix} Y_1^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & Z_1 \end{pmatrix}$$

for some $Z_1 \in G_{n-2}$. Since such a relation holds for all $Z \in G_{n-2}$, it follows that $Y_1 = (y_1) \dotplus \tilde{Y}$. By a similar argument we see that Y_1, and indeed each Y_r, must be diagonal, and that all Y_r are sections of a single diagonal matrix D. Following τ with an inner automorphism with factor D^{-1}, we see that we may assume each $Y_r = I$. The same type of argument shows that the various m_r are all the same, and that all the ω_r coincide. Hence we have

$$X^\tau = X^\omega$$

for all decomposable $X \in G_n^+$, where ω is the common automorphism $\omega_1 = \omega_2 = \cdots$, i.e., ω is a product of automorphisms chosen from 2. or 3. Changing τ by the automorphisms 2., 3. as needed we may thus assume that $X^\tau = X$ for all decomposable $X \in G_n^+$. For $n \geqq 4$, these decomposable matrices generate G_n^+, and so $X^\tau = X$ for all $X \in G_n^+$.

We now determine the effect of τ on G_n^- and $G_n^{\pm i}$. Let $Y, Z \in G_n^-$ where Z is fixed. Then

$$Y^\tau Z^\tau = (YZ)^\tau$$

implies

$$Y^\tau = YB$$

for all $Y \in G_n^-$, where B is independent of Y. Using $(Y^2)^\tau = (Y^\tau)^2$, we obtain

$$BYB = Y$$

for all $Y \in G_n^-$. This implies that $B = \pm I$ or $\pm iI$. However, $B = \pm iI$ is impossible, and therefore $B = \pm I$, whence

$$Y^\tau = \pm Y$$

for all $Y \in G_n^-$. If n is odd, $\tau: G_n^- \to G_n^-$ shows that only the plus sign can hold. If n is even, then changing τ by the automorphism $X \to (\det X)X$, if necessary, we may assume that $X^\tau = X$ for all $X \in G_n^+ \cup G_n^-$.

The same argument as above shows that $Y^\tau = \pm Y$ for all $Y \in G_n^{\pm i}$. If the plus sign occurs, τ is the identity; if the minus sign occurs, then τ is simply the automorphism $X^\tau = (\det X)^2 X$. This concludes the proof of the Main Theorem.

Another approach to the proof of the Main Theorem, which is less computational than that given here, is contained in references [3] and [4].

References

1. L. K. Hua and I. Reiner, *On the generators of the symplectic modular group*, Trans. Amer. Math. Soc. vol. 65 (1949) pp. 415–426.

2. ———, *Automorphisms of the unimodular group*, Trans. Amer. Math. Soc. vol. 71 (1951) pp. 331–348.

3. J. Landin and I. Reiner, *Automorphisms of the general linear group over a principal ideal domain*, Ann. of Math. vol. 65 (1957) pp. 519–526.

4. ———, *Automorphisms of the two-dimensional general linear group over a euclidean ring*, to appear in Proc. Amer. Math. Soc.

5. G. W. Mackey, *Isomorphisms of normed linear spaces*, Ann. of Math. vol. 43 (1942) pp. 244–260.

6. I. Reiner, *Maximal sets of involutions*, Trans. Amer. Math. Soc. vol. 79 (1955) pp. 459–476.

7. C. E. Rickart, *Isomorphic groups of linear transformations*, Amer. J. Math. vol. 72 (1950) pp. 451–464.

UNIVERSITY OF ILLINOIS
URBANA, ILLINOIS