TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 157, June 1971

A CORRELATION BETWEEN $PSU_4(3)$, THE SUZUKI GROUP, AND THE CONWAY GROUP

BY
J. H. LINDSEY II

Abstract. We shall use a six dimensional projective representation of $PSU_4(3)$ of order $2^7 3^6 5 \cdot 7$ to construct 12 and 24-dimensional complex projective representations of the Suzuki and Conway groups, respectively, acting on the Leech lattice. The construction makes it easy to show that the Suzuki and Conway simple groups have outer automorphism groups of order two and one, respectively. Also, the simple Suzuki group contains $3 \cdot PSU_4(3) \cdot 2$, $3^5 \cdot M_{11}$, and a group which is probably $PSU_5(2)$, where $A \cdot B$ denotes an extension of the group A by the group B.

1. **The construction.** The motivation for the construction was to find a 12-dimensional linear group where an element $M_2 = \omega I_6 \oplus \bar{\omega} I_6 = \text{diag}(\omega, \omega, \ldots, \bar{\omega}, \bar{\omega})$ is centralized by a central extension by $PSU_4(3)$, where $\omega = (-1 + (-3)^{1/2})/2$. Let

$$U = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \bar{\omega} \\ 1 & \bar{\omega} & \omega \end{pmatrix} \Big/ (-3)^{1/2}.$$

Then our 12-dimensional group S is generated by

$$M_1 = U \oplus \bar{U} \oplus \bar{U} \oplus U, \qquad M_2 = \omega I_6 \oplus \bar{\omega} I_6,$$
$$M_3 = (1, 2, 3)(1', 2', 3')(4', 5', 6'), \qquad M_4 = (4, 5, 6)(1', 2', 3')(4', 6', 5'),$$
$$M_5 = (1, 2, 6)(1', 3', 4')(2', 6', 5'), \qquad M_6 = (1, 2, 2')(5, 4', 4)(6, 5', 6'),$$

where the last four matrices are permutation matrices acting on the 12 variables $x_1, \ldots, x_6, x_{1'}, \ldots, x_{6'}$ corresponding to the given permutations. We later show that $M_0 = \omega I_3 \oplus \bar{\omega} I_3 \oplus \omega I_3 \oplus \bar{\omega} I_3 \in S$. Then M_2 is centralized by $M_i = m_i \oplus \sigma(m_i)$, $i = 0, \ldots, 5$, where m_i are six-dimensional matrices generating a central extension U of Z_6 by $PSU_4(3)$ as in [5]. We show later that σ well defines an automorphism of $U/Z(U) \simeq PSU_4(3)$. By [4], the only finite projective six-dimensional linear group properly containing U comes from adding an odd permutation matrix, and $U/Z(U)$ has index two in the projective group. An ascending chain of subgroups of the automorphism group of $U/Z(U)$ is gotten by successively throwing in α

Presented to the Society on April 14, 1970, at the Symposium on Representation Theory of Finite Groups and Related Topics, held in Madison, Wisconsin; received by the editors May 18, 1970.

AMS 1969 *subject classifications.* Primary 2075.

Key words and phrases. $PSU_4(3)$, Suzuki group, Conway group, Leech lattice, orbit, automorphism group, centralizer of a central involution.

conjugation by an odd six-dimensional permutation matrix, β complex conjugation of elements of U, and σ. As a permutation matrix is real, α and β commute. Since σ fixes m_0 and $\langle m_1\rangle$, and β fixes m_3, m_4, and m_5, σ and β commute. Then β corresponds to the center of the dihedral group of order eight which is the outer automorphism group of $PSU_4(3)$. Only elements of $\langle\alpha, \beta\rangle$ lift to automorphisms of U.

The last generator M_6 was obtained by letting M_6 play the same role in $C_S(M_0)$ as M_5 played in $C_S(M_2)$.

2. **The monomial group PD.** The matrices M_i, $i=3, \ldots, 6$, generate a group P, and ωI_{12}, M_i, $i=2, \ldots, 6$, generate a monomial group $M=PD$ where D is the subgroup of diagonal matrices of M. (Actually, ωI_{12} was not needed as a generator.) The permutation group P permutes the 11 partitions $\{1, \ldots, 6, 1', \ldots, 6'\}=S_i \cup S_i'$, $i=1, \ldots, 11$, where S_i' is the complement of S_i and

$$S_1 = \{1, 2, 3, 4, 5, 6\}, \qquad S_2 = \{1, 2, 3, 1', 2', 3'\},$$
$$S_3 = \{1, 2, 4, 3', 4', 5'\}, \qquad S_4 = \{1, 2, 5, 1', 4', 6'\},$$
$$S_5 = \{1, 3, 4, 2', 4', 6'\}, \qquad S_6 = \{1, 3, 5, 3', 5', 6'\},$$
$$S_7 = \{1, 4, 5, 1', 2', 5'\}, \qquad S_8 = \{2, 3, 4, 1', 5', 6'\},$$
$$S_9 = \{2, 3, 5, 2', 4', 5'\}, \qquad S_{10} = \{2, 4, 5, 2', 3', 6'\},$$
$$S_{11} = \{3, 4, 5, 1', 3', 4'\}.$$

The group $\langle M_3, M_4, M_5\rangle$ restricted to $\{1, \ldots, 6\}$ is doubly transitive because of $\langle M_4, M_5\rangle$, triply transitive because of $\langle M_3, M_5\rangle$, 4-ply transitive because of $\langle M_3\rangle$, and acts as A_6 on the first six letters. As the restriction of the partition corresponding to S_i, $i=2, \ldots, 11$, to the first six letters runs once over all ten partitions of the six letters into two sets of three, P is transitive on S_i, $i=2, \ldots, 11$. Some element in $\langle M_3, M_4, M_5\rangle$ interchanges $\{1, 2, 3\}$ and $\{4, 5, 6\}$ and interchanges S_2 and S_2'. As M_6 does not fix S_1, P is doubly transitive on the partitions. Then P has a cycle of order eleven and is doubly transitive. Because of M_3 and $M_5M_4=(4, 5, 1, 2, 6)\cdot(1', 6', 2', 4', 5')$, $12=1+1+1+3+3+3$ and $12=1+1+5+5$ are refinements for the orbits of the subgroup of P fixing two letters, so P is triply transitive. The only S_i, S_i' containing $\{4, 5, 6\}$ are S_1 and S_2'. Intersecting the complements of these two sets gives $\{1', 2', 3'\}$. As P is triply transitive, this procedure pairs off triples with an antipodal triple in a way preserved by P. As $\langle M_3, M_4\rangle$ fixes S_1 and S_2, and acts transitively on the remaining partitions, P is triply transitive on partitions.

For elements in S of the form $A \oplus B$ with A and B six by six matrices, we have a well-defined automorphism $B=\sigma(A)$ of $U/Z(U)$. Otherwise, by the subdirect product theorem, S has a section $PSU_4(3)\times PSU_4(3)$ and $(3^6)^2 \mid |S|$. This is impossible as we show later that S acts on the Leech lattice and is contained in a central extension of Z_2 by the Conway group. Then $C_P(M_2)$ is isomorphic to A_6 or S_6. In the latter case let t be an odd six by six permutation matrix. Then for $u \in U/Z(U)$, $t(\sigma(t^{-1}ut))t^{-1}=t\sigma(t^{-1})\sigma(u)(t(\sigma(t^{-1})))^{-1}$ where, by maximality of $\langle t, U\rangle$, as a finite

6-dimensional projective group, $t\sigma(t^{-1})$ lies in U. Then the images of α and σ in the outer automorphism group of $U/Z(U)$ commute, a contradiction, since along with the center of the dihedral group, they generate the dihedral group. Since $C_P(M_2)$ is the subset of P fixing S_1 and P acts transitively on $S_1, \ldots, S_{11}$, $|P| = |A_6|(22)$. Let θ be a homomorphism of P with kernel K. If $C_P(M_2) \subseteq K$, then K contains a 3-Sylow subgroup and P, since P is generated by 3-elements. Otherwise, $K \cap C_P(M_2) = \langle 1 \rangle$ and $|K| \mid 22$. If $11 \mid |K|$, then P has a normal 11-subgroup, contrary to $|K| \nmid (11)(10)$. If $|K| = 2$, P has a central involution and is imprimitive, contrary to double transitivity. Then P is simple of order 7920 and is isomorphic to M_{11}.

As P transitively permutes the eleven partitions, $D = \langle \phi I_{12}, d_i, i = 1, \ldots, 11 \rangle$ where $d_i = (a_{hk})$, $a_{hk} = \omega$ for $h = k \in S_i$, $\bar{\omega}$ for $h = k \in S_i'$, and 0 elsewhere. Let ϕ be the homomorphism from D to $V_{12}(GF(3))$ where

$$\phi(\text{diag}\,(\omega^{a_1}, \ldots, \omega^{a_{6'}})) = (a_1, \ldots, a_{6'}).$$

Let $e_i = \phi(d_i)$. The inner product

$$((a_1, \ldots, a_{6'})(b_1, \ldots, b_{6'})) = \sum_{j=1}^{6'} a_j b_j$$

is preserved by P. Since $0 = (e_1, e_1) = (e_1, e_2)$ and P acts doubly transitively on the partitions, $(\phi(D), \phi(D)) = 0$. Then $|D| \leqq 3^6$. As M_0 is a conjugate of M_2 by an element of P, taking S_2 to S_1, we have $M_0 \in D$. Then $\phi(M_0) - \phi(M_2)$ has all entries 1 at components in $\{4, 5, 6\}$, all entries -1 at $\{1', 2', 3'\}$, the antipodal of the first triple, and all entries 0 elsewhere. Since P is triply transitive, for any triple t, $\phi(D)$ has one element which has entries 1 on t, -1 on the antipodal of t, and 0 elsewhere. Adding multiples of $\phi(\omega I_{12})$ to these elements, we get $3\binom{12}{3} = 660$ elements of $\phi(D)$. As $-\phi(M_2) - \phi(\omega I_{12})$ has entries 1 on S_1 and 0 elsewhere, for $i = 1, \ldots, 11$, $\phi(D)$ contains elements which are constant on S_i and a different constant on S_i'. There are $11(9-3) = 66$ such elements. There are 3 elements in $\phi(\langle \omega I_{12} \rangle)$. This gives $660 + 66 + 3 = 729 = 3^6$ elements, so $|D| = 3^6$ and we have classified the elements of D. Note that all elements of $\phi(D)$ have exactly 0, 6, 9, or 12 nonzero components. Also, $\phi(D) = \phi(D)^{\perp}$ and, as $D = \langle \omega I_{12}, d_i, i = 1, \ldots, 11 \rangle$,

$$\phi(D) = \left\{ (a_1, \ldots, a_{6'}) \mid \sum_{j \in S_i} a_j = \sum_{j \in S_i'} a_j = 0, i = 1, \ldots, 11 \right\}. \tag{2.1}$$

For $k \in Z$,

$$\omega^k \equiv 1 - k(-3)^{1/2} \pmod{3Z[\omega]}. \tag{2.2}$$

Let $d = \text{diag}\,(\omega^{a_1}, \ldots, \omega^{a_{6'}})$. Let $S = S_i$ or S_i' for some $i = 1, \ldots, 11$. Then,

$$\sum_{j \in S} \omega^{a_j} \equiv \sum_{j \in S} (1 - a_j(-3)^{1/2}) \equiv -(-3)^{1/2} \sum_{j \in S} a_j \pmod{3Z[\omega]}$$

and by (2.1),

$$(2.3)\qquad d \in D \Leftrightarrow \sum_{j\in S_i} \omega^{a_j} \equiv \sum_{j\in S_i'} \omega^{a_j} \equiv 0 \pmod{3Z[\omega]}, \quad i = 1, \cdots, 11.$$

3. **The Leech lattice $\mathscr{L}$.** I wish to thank Marvin Wunderlich of the Northern Illinois University Mathematics Department who wrote a Fortran program which made it possible to apply the matrices M_i, $i=1, \ldots, 6$, in random succession to images of the column vector with all its entries one. This gave the first indication that the M_i generated a finite group when none of the images had denominator as large as 3. Examination of the output also led to construction of the following lattice. Let $\mathscr{L}$ be the set of $(a_1, \ldots, a_6, a_{1'}, \ldots, a_{6'})$ such that all of the following are satisfied:

$$(3.1)\qquad a_i \in Z[\omega], \quad \text{all } i = 1, \ldots, 6',$$

$$(3.2)\qquad a_i - a_j \in (-3)^{1/2}(Z[\omega]) \quad \text{all } i, j,$$

$$(3.3)\qquad \sum_{j\in S} a_j \in 3(Z[\omega]) \quad \text{for } S = S_i \text{ and } S_i' \text{ all } i,$$

$$(3.4)\qquad 3a_1 + \sum_{j=1}^{6'} a_j \in 3(-3)^{1/2}(Z[\omega]).$$

We now show that $\mathscr{L}$ is preserved by S.

A. By (3.2), $3a_1 - 3a_i \in 3(-3)^{1/2}(Z[\omega])$, so $\mathscr{L}$ is preserved by P.

B. We now show that $\mathscr{L}$ is preserved by D. Let $u=(a_1, \ldots, a_6, a_{1'}, \ldots, a_{6'}) \in \mathscr{L}$. Let $d=\operatorname{diag}(d_1, \ldots, d_{6'}) \in D$. Then $d(u)$ satisfies (3.2) since $d_p a_p - d_q a_q \equiv a_p - a_q \pmod{(-3)^{1/2}(Z[\omega])}$ by (2.2). Now let $S=S_i$ or S_i'. Then by (2.3), (3.2), and (2.2),

$$\sum_{k\in S} d_k a_k \equiv \sum_{k\in S} d_k(a_k - a_1) \equiv \sum_{k\in S} (a_k - a_1) \equiv \sum_{k\in S} a_k \equiv 0 \pmod{3(Z[\omega])}$$

and $d(u)$ satisfies (3.3). By A we may assume that $d = I_6 \oplus \omega I_6$ since $PD = \langle P, I_6 \oplus \omega I_6 \rangle$. By (2.2), (3.3), and (3.4),

$$\begin{aligned} 3d_1 a_1 + \sum_{k=1}^{6'} d_k a_k &\equiv 3a_1 + \sum_{k\in S_1} a_k + \sum_{k\in S_1'} \omega a_k \\ &\equiv 3a_1 + \sum_{k\in S_1} a_k + \sum_{k\in S_1'} a_k \equiv 0 \pmod{3(-3)^{1/2}(Z[\omega])} \end{aligned}$$

and $d(u)$ satisfies (3.4).

C. We are left with showing that $\mathscr{L}$ is preserved by M_1. Let $u=(a_1, \ldots, a_{6'}) \in \mathscr{L}$ and $M_1(u)=(b_1, \ldots, b_{6'})$. For $i=0, 1, 2$,

$$\begin{aligned} (-3)^{1/2} b_{i+1} &= \sum_{k=0}^{2} \omega^{ik} a_{k+1} \equiv \sum_{k=0}^{2} a_{k+1} \\ &\equiv \sum_{k=0}^{2} (a_{k+1} - a_1) \equiv 0 \pmod{(-3)^{1/2}(Z[\omega])}, \end{aligned}$$

so in this fashion $M_1(u)$ satisfies (3.1). For $i, j=0, 1, 2$, by (2.2) and (3.2),

$$(-3)^{1/2}(b_i-b_j) \equiv \sum_{k=0}^{2}(\omega^{ik}-\omega^{jk})a_{k+1} \equiv \sum_{k=0}^{2}(\omega^{ik}-\omega^{jk})a_1 \equiv 0 \pmod{3Z[\omega]}$$

since $\sum_{k=0}^{2}\omega^{ik}$ equals 3 or 0. Similar arguments verify (3.2) if i and j lie in the same partition given by the common refinement of S_1 and S_2. As $b_1=(a_1+a_2+a_3)/(-3)^{1/2}$, $b_4=-(a_4+a_5+a_6)/(-3)^{1/2}$, $b_{1'}=-(a_{1'}+a_{2'}+a_{3'})/(-3)^{1/2}$, and $b_{4'}=(a_{4'}+a_{5'}+a_{6'})/(-3)^{1/2}$, by (3.3) for $j=1, 2$, these components are congruent (mod $(-3)^{1/2}Z[\omega]$) (i.e. $b_1\equiv b_4, b_{1'}$; $b_{4'}\equiv b_4, b_{1'}$) and $M_1(u)$ satisfies (3.2). We now show that M_1u satisfies (3.4). By (3.3) with $S=S_9$ and S_7,

$$\begin{aligned} 3b_1+\sum_{i=1}^{6'} b_i &= (3(a_1+a_2+a_3)+3a_1-3a_4-3a_{1'}+3a_{4'})/(-3)^{1/2} \\ &\equiv (-3)^{1/2}(a_4+a_{1'}-a_{4'}-a_2-a_3+a_1) \\ &\equiv -3(a_4+a_{1'}+(a_5+a_{2'}+a_{5'})+a_1) \\ &\equiv 0 \pmod{3(-3)^{1/2}(Z[\omega])}. \end{aligned}$$

In showing that M_1u satisfies (3.3), we shall often use the fact that $\mathscr{L}$ is preserved by D and, for $d\in D$, $d(a_1, \ldots, a_{6'})=(c_1, \ldots, c_{6'})\in\mathscr{L}$. In our first application of this, diag $(1, \bar\omega, \omega, 1, 1, 1, 1, \omega, \bar\omega, 1, \bar\omega, \omega)\in D$ by the classification of elements in §2, since $\{3, 2', 6'\}$ and $\{2, 3', 5'\}$ are antipodals by S_3 and S_5. As we have checked (3.4), for each $i=1, \ldots, 11$, we need check (3.3) for only one of S_i, S_i'.

$$\sum_{i\in S_1} b_i = (3a_1-3a_4)/(-3)^{1/2} = (-3)^{1/2}(a_4-a_1)\in 3(Z[\omega]).$$

$$\sum_{i\in S_2} b_i = (3a_1-3a_{1'})/(-3)^{1/2}\in 3Z[\omega].$$

$$\begin{aligned} \sum_{i\in S_3} b_i &= (a_1+a_2+a_3+a_1+\omega a_2+\bar\omega a_3-a_4-a_5-a_6 \\ &\qquad -a_{1'}-\omega a_{2'}-\bar\omega a_{3'}+a_{4'}+a_{5'}+a_{6'}+a_{4'}+\omega a_{5'}+\bar\omega a_{6'})/(-3)^{1/2} \\ &= (2a_1-\bar\omega a_2-\omega a_3-a_4-a_5-a_6-a_{1'}-\omega a_{2'}-\bar\omega a_{3'} \\ &\qquad +2a_{4'}-\bar\omega a_{5'}-\omega a_{6'})/(-3)^{1/2} \\ &= -(-3)^{1/2}a_1-(-3)^{1/2}a_4-(a_1+\bar\omega a_2+\omega a_3+a_4+a_5+a_6+a_{1'} \\ &\qquad +\omega a_{2'}+\bar\omega a_{3'}+a_{4'}+\bar\omega a_{5'}+\omega a_{6'})/(-3)^{1/2} \\ &\equiv -2(-3)^{1/2}a_1-\sum_{i=1}^{6'} c_i/(-3)^{1/2} \\ &\equiv (-3)^{1/2}a_1-(-3c_1)/(-3)^{1/2} \\ &= (-3)^{1/2}a_1-(-3a_1)/(-3)^{1/2} \\ &\equiv 0 \pmod{3Z[\omega]}. \end{aligned}$$

Now, $M_3M_1=M_1$ diag $(1, \bar\omega, \omega, 1, 1, 1, 1, \omega, \bar\omega, 1, \bar\omega, \omega)$ and $M_4M_1=M_1$ diag $(1, 1, 1, 1, \omega, \bar\omega, 1, \omega, \bar\omega, 1, \omega, \bar\omega)$ where both diagonal matrices are in

D, since $\{3, 2', 6'\}$ and $\{2, 3', 5'\}$ are antipodal by S_3 and S_5, and $\{5, 2', 5'\}$ and $\{6, 3', 6'\}$ are antipodal by S_7 and S_9. As no nonidentity element in $\langle M_3, M_4\rangle$ fixes the partition S_3, $\langle M_3, M_4\rangle$ acts transitively on $S_3, \ldots, S_{11}$ and, for any $i=3, \ldots, 11$, $T=S_i$ or S_i' is the inverse image of S_3 under some element $R \in \langle M_3, M_4\rangle$. Furthermore, $RM_1=M_1d$ for some $d \in D$. Let $RM_1u=(e_1, \ldots, e_{6'})=M_1(du)$. Then $\sum_{i\in T} b_i=\sum_{i\in S_3} e_i \in 3Z[\omega]$ since $du \in \mathscr{L}$.

We now show that

$$\mathscr{L}' = \{(a_1, \ldots, a_{24}) \mid 3(a_1+ia_2, a_3+ia_4, \ldots, a_{23}+ia_{24})'/2^{1/2} \in \mathscr{L}\}$$

is the Leech lattice. We do this by using the characterization in [1] of the Leech lattice as a unimodular lattice in which every squared length is an even integer greater than two. We examine approximately how many $(a_1, b_1, \ldots, a_{6'}, b_{6'})$ in W, a large rectangular parallelopiped of volume c in Z^{24}, satisfy

$$v = (a_1+b_1(-3)^{1/2}, \ldots, a_{6'}+b_6(-3)^{1/2})/2 \in \mathscr{L}.$$

W corresponds to W^*, a set of volume $c(1/2)^{12}(3^{1/2}/2)^{12}$ in $\mathscr{L}$. By the Chinese remainder theorem, congruences modulo 2 are statistically independent from congruences modulo 3. Now, v has components in $Z[\omega]$ if and only if

$$a_i \equiv b_i \pmod 2, \qquad i = 1, \ldots, 6', \tag{3.5}$$

and (3.5) is satisfied by $c/2^{12}$ points. Also, (3.2) is equivalent to

$$a_i \equiv a_j \pmod 3, \qquad i, j = 1, \ldots, 6', \tag{3.6}$$

and (3.6) is satisfied by $c/3^{11}$ points of W. Finally, by (2.1), (3.3) is equivalent to

$$(\bar{b}_1, \ldots, \bar{b}_{6'}) \in \phi(D) \quad \text{where } \bar{b}_i \text{ is the image of } b_i \text{ in } GF(3). \tag{3.7}$$

As $\phi(D)$ has dimension 6, (3.7) is satisfied by $c/3^6$ points. As (3.5), (3.6), and (3.7) are independent, $c/(2^{12}3^{11}3^6)$ points of W satisfy (3.5), (3.6), and (3.7). For any one of these points, if a_1 is replaced by a_1-6, a_1, or a_1+6, exactly one of these replacements satisfies (3.4). Since

$$(c/(2^{12}3^{11}3^6))/3 = c(1/2)^{12}(3^{1/2}/2)^{12}/(3/2^{1/2})^{24} = (\text{vol } W^*)/(3/2^{1/2})^{24},$$

$\mathscr{L}'$, with its scale reduced by a factor of $2^{1/2}/3$ from that of $\mathscr{L}$, has one point per unit volume and is unimodular.

Let $\|v\|^2=\sum_{k=1}^{6'}(a_k^2+3b_k^2)/4$. As the M_i are unitary, S preserves $\|v\|$ and acts orthogonally on $\mathscr{L}'$. Suppose that $v \in \mathscr{L}$. As $\phi(D)=\phi(D)^\perp$, by (3.7), $\sum_{k=1}^{6'} b_k^2 \equiv 0 \pmod 3$. Then if $3 \mid a_1$, by (3.6), $9 \mid \|v\|^2$. Suppose $3 \nmid a_1$. Then by (3.6),

$$\sum_{k=1}^{6'} a_k^2 \equiv \sum_{k=1}^{6'} (a_k^2-(a_k-a_1)^2) \equiv 2a_1\left(-6a_1+\sum_{k=1}^{6'} a_k\right) \equiv 2a_1\left(3a_1+\sum_{k=1}^{6'} a_k\right) \pmod 9.$$

We have proved

(3.8) $3\nmid a_1$ and v satisfies (3.1), (3.2), (3.3) $\Rightarrow$ (v satisfies (3.4) $\Leftrightarrow 9 \mid \|v\|^2$).
In particular, $v \in \mathscr{L}$ implies $9 \mid \|v\|^2$. Suppose $v \in \mathscr{L}$ and $\|v\|^2 = 9$. Then $3 \mid a_k$, $k = 1, \ldots, 6'$, otherwise, by (3.6), all $a_k \neq 0$ and $\|v\|^2 \geqq 12$. By (3.7) and the classification of elements of $\phi(D)$ in §2, exactly 0, 6, 9, or 12 of the b_i are not divisible by 3. Then all b_i are divisible by 3, otherwise, since $3 \mid a_i$, $\|v\|^2 \geqq 3(6)$. Then exactly one $(a_k + b_k(-3)^{1/2})/2$ is nonzero, and it is divisible exactly by 3. This contradicts (3.4). Going to $\mathscr{L}'$ changes square lengths by a factor 2/9 so all square lengths are even integers greater than two.

4. **Orbits of $\mathscr{L}$.** Here we show that the points of $\mathscr{L}$ of squared length 18, the points closest to the origin, form an orbit for S. We also show the same for points of squared length 27, the second closest points. For v as in §3, we define $\{(a_k^2 + 3b_k^2)/4\}$ counting multiplicities to be the shape of v. For any

$$x = (a + b(-3)^{1/2})/2 \in Z[\omega],$$

we can uniquely write $x = ((-3)^{1/2})^n y$ with $y = (c + d(-3)^{1/2})/2 \in Z[\omega]$ and $3 \nmid c$. Let m be the multiplicative group $\langle -\omega \rangle$. Then modulo $3Z[\omega]$, elements in m run over all elements in $Z[\omega]$ but not in $(-3)^{1/2}Z[\omega]$ exactly once. There is a unique $t \in \langle -\omega \rangle = m$ with $y - t \in 3Z[\omega]$. Let $\alpha(x) = ((-3)^{1/2})^n t$. If the components $c_k = (a_k + b_k(-3)^{1/2})/2$ of v all lie in $(-3)^{1/2}Z[\omega]$, replacing c_k by $\alpha(c_k)$ does not affect whether v lies in $\mathscr{L}$. Suppose that the components do not lie in $(-3)^{1/2}Z[\omega]$, and $9 \mid \|v\|^2$. Then by (3.8), we need check only (3.5), (3.6), and (3.7) to see if $v \in \mathscr{L}$, and these properties are left invariant under replacing c_k by $\alpha(c_k)$. As we are only interested in $\|v\|^2 \leqq 27$, we examine the possible $e = (c^2 + 3d^2)/4$ less than 28 as c runs over integers not divisible by 3 and with the same parity as d: $d = 0$: $e = 1$, 4, 16, 25; $d = 1$: $e = 1$, 7, 13; $d = 2$: $e = 4$, 7, 19; $d = 3$: $e = 7$, 13, 19; $d = 4$: $e = 13$, 16; $d = 5$: $e = 19$, 25. Since the signs of c and d (unless $d = 0$) may be changed, we get 1, 4, 16, and 25 six times and 7, 13, and 19 twelve times. As the set R of elements of $Z[\omega]$ of a fixed squared length $s = 3^n s_0$ with $3 \nmid s_0$ is closed under multiplication by elements of m, all elements in m have the same number of preimages in R. Then α restricted to R is 1 to 1 for $s_0 = 1$, 4, 16, or 25, is 2 to 1 for $s_0 = 7$, 13, or 19, and is q to 1 for s if it is q to 1 for s_0.

By (3.2), for $v \in \mathscr{L}$, the elements of the shape of v are all divisible by 3, or none divisible by 3. By the above, in the former case the elements of the shape are 3, 12, 21, 9, or 27. In the case of 3, 12, or 21 some $\bar{b}_k$ is nonzero and by (3.7) and the classification of elements of $\phi(D)$, exactly six, nine or twelve $\bar{b}_k$ are nonzero. Suppose $\|v\|^2 = 18$ or 27. As $12 + 5(3) = 27$, in the case of 12 or 21, the shape must be

(4.1) 12, 3, 3, 3, 3, 3, 0, 0, . . ., 0.

Otherwise, neither 12 nor 21 occurs, and if 3 occurs, exactly six, nine or twelve 3's occur so we have

(4.2) 3, 3, 3, 3, 3, 3, 0, . . .,

(4.3) 3, 3, 3, 3, 3, 3, 9, 0, . . ., or

(4.4) 3, 3, 3, 3, 3, 3, 3, 3, 3, 0, ...

When only 9 or 27 occur we have

(4.5) $27, 0, \ldots,$

(4.6) $9, 9, 9, 0, \ldots,$ or

(4.7) $9, 9, 0, \ldots.$

Now, we may assume that elements of the shape are only 1, 4, 16, 25, 7, 13, or 19. When more than one 7 occurs in a shape we distinguish between the cosets of $\langle -\omega \rangle$ in R for $s=7$ and denote them by 7 and 7′. The possibilities for the shape are:

(4.8) $16, 1, 1, \ldots, 1,$

(4.9) $13, 4, 1, \ldots,$

(4.10) $7, 7, 4, 1, \ldots,$

(4.11) $7, 7', 4, 1, \ldots,$

(4.12) $7, 4, 4, 4, 1, \ldots,$

(4.13) $7, 1, \ldots,$

(4.14) $4, 4, 4, 4, 4, 1, \ldots,$

(4.15) $4, 4, 1, \ldots.$

Suppose that we have case (4.1), (4.2), (4.3), or (4.4). By (3.7),

$$(\bar{b}_{1'}, \ldots, \bar{b}_{6'}) \in \phi(D).$$

In (4.1), (4.2), and (4.3) exactly six $\bar{b}_i$ are nonzero and by the classification of $\phi(D)$, there are $\binom{12}{3}+44=264$ possibilities for $(\bar{b}_1, \ldots, \bar{b}_{6'})$. In (4.4) exactly nine $\bar{b}_i$ are nonzero and there are 440 possibilities. Suppose $(\bar{b}_1, \ldots, \bar{b}_{6'})$ is fixed. Then the only freedom lies in which nonzero $\bar{b}_i$ corresponds to 12 (6 possibilities for (4.1)), which zero $\bar{b}_i$ corresponds to 9 (6 possibilities for (4.3)), what the complex number of squared length nine is (by α, 6 possibilities for (4.3)), and the possibilities for the complex numbers of squared length 12 or 3. As α is 1 to 1 on R for $s=12$ or 3, for a complex number of squared length 12 or 3, b_k may equal $\pm 1 \pmod 3$, a_k may equal $0, \pm 3 \pmod 9$ independent of $b_k \pmod 3$, and the congruence classes determine the complex number uniquely. Now, $b_k \pmod 3$ has already been fixed by $\bar{b}_k$. The above values of $a_k \pmod 9$ may be chosen arbitrarily except that the last one is determined by (3.4). This gives 3^5 possibilities for the complex number of squared absolute value 12 or 3 in (4.1), (4.2), and (4.3), and 3^8 possibilities in (4.4). Then (4.1) has $(264)(6)(3^5)=384{,}912$ possibilities, (4.2) has $(264)(3^5)=64{,}152$ possibilities, (4.3) has $(264)(6)(6)(3^5)=2{,}309{,}472$ possibilities, and (4.4) has $(440)(3^8)=2{,}886{,}840$ possibilities. By α, complex numbers of absolute value 3 have $a_k \equiv \pm 3 \pmod 9$. For (3.4) there are two ways in (4.7), $3-3$ and $-3+3$, that the a_k can add to 0 (mod 9), and in (4.6) there are two ways, $3+3+3$, and $-3-3-3$. As the class of $b_i \pmod 9$ can be $0, \pm 3$, for (4.6) there are $\binom{12}{3}(3^3)(2)=11{,}880$ possibilities, for (4.7) there are $\binom{12}{2}(3^2)(2)=1188$ possibilities, and for (4.5) there are $(12)(6)=72$ possibilities.

For $v=((a_1+b_1(-3)^{1/2})/2, \ldots, (a_{6'}+b_{6'}(-3)^{1/2})/2) \in \mathscr{L}$ with $3 \nmid a_1$, we consider the possibilities for

$$\begin{aligned} v^* &= (\alpha((a_1+b_1(-3)^{1/2})/2), \ldots, \alpha((a_{6'}+b_{6'}(-3)^{1/2})/2)) \\ &= ((c_1+d_1(-3)^{1/2})/2, \ldots, (c_{6'}+d_{6'}(-3)^{1/2})/2) \end{aligned}$$

with all components in $\langle -\omega \rangle$. Now, $c_1 \equiv \pm 1 \pmod 3$ and this value determines all $c_k \pmod 3$ by (3.2). By (3.7), $(\bar{d}_1, \ldots, \bar{d}_{6'}) \in \phi(D)$ and there are 3^6 possibilities. By (3.8), (3.4) will then be satisfied by v. There are $(2)(3^6) = 1458$ possibilities for v^* and they are permuted transitively by $\langle -I_{12}, D \rangle$. Also, v^* determines v except for the positions of the elements of the shape, and, in the case of $s = 7$, 13, and 19, which of the two cosets of m in R is taken. Then (4.8) has $(12)(1458) = 17{,}496$ possibilities, (4.9) has $(2)(12)(11)(1458) = 384{,}912$ possibilities, (4.10) and (4.11) together have $(2)(2)\binom{12}{2}(10)(1458) = 3{,}849{,}120$ possibilities, (4.12) has $(2)(12)\binom{11}{3}(1458) = 5{,}773{,}680$ possibilities, (4.13) has $(2)(12)(1458) = 34{,}992$ possibilities, (4.14) has $\binom{12}{5}(1458) = 1{,}154{,}736$ possibilities, and (4.15) has $\binom{12}{2}(1458) = 96{,}228$ possibilities. The total for $\|v\|^2 = 18$ comes from (4.2), (4.7), (4.13), and (4.15), and is $196{,}560 = 2^4 3^3 5 \cdot 7 \cdot 13$. The total from $\|v\|^2 = 27$ comes from the rest of (4.1), ..., (4.15) and is $16{,}773{,}120 = 2^{12} 3^2 5 \cdot 7 \cdot 13$. As expected, these are the same figures as in [1].

In the cases of (4.1) through (4.7), since P is triply transitive, by applying some element in P we may put f, the component of v least divisible by $(-3)^{1/2}$, in the first spot and zeros in the next two spots. After applying M_1 to this, we get an element of $\mathscr{L}$ with some component not divisible by $(-3)^{1/2}$ to as large a power as f is. We repeat this process till we reach a case in (4.8) through (4.15). In this way we see that we may omit (4.1) through (4.7) and still have all orbits with $\|v\|^2 = 18$ or 27 represented.

Suppose that $v \in \mathscr{L}$ with v in one of cases (4.8) through (4.15). Let x, y, and z be any three elements of the shape of v. Let $(c_1 + d_1(-3)^{1/2})/2, \ldots, (c_3 + d_3(-3)^{1/2})/2$ be in the same coset of m as the component of v corresponding to x, y, or z, respectively with $0 \not\equiv c_1 \equiv c_2 \equiv c_3 \pmod 3$. By triple transitivity of P we may apply some elements in P to v to make $(a_i + b_i(-3)^{1/2})/2$ lie in the same coset of m as $(c_i + d_i(-3)^{1/2})/2$, for $i = 1, 2, 3$. By (3.2), $a_1 \equiv a_2 \equiv a_3 \pmod 3$ and by applying some element in $\langle -I_{13} \rangle$, we can make $a_i \equiv c_i$, $i = 1, 2, 3$. By the classification of $\phi(D)$, D has some element with three eigenvalues 1, three eigenvalues $\bar{\omega}$, and six eigenvalues ω. By applying some element in P, which is triply transitive, to d, we see that the first three diagonal entries of d can be chosen as arbitrary elements in $\langle \omega \rangle$. Choosing d correctly and applying d to v, we can make $b_i \equiv d_i \pmod 3$, $i = 1, 2, 3$, without losing $a_i \equiv c_i \pmod 3$. As the map α is 1 to 1 when restricted to a coset of m, $(a_i + b_i(-3)^{1/2})/2 = (c_i + d_i(-3)^{1/2})/2$, for $i = 1, 2, 3$. We now can use the following equalities with U as in the definition of M_1 to change the shape of elements of $\mathscr{L}$:

$$U\begin{pmatrix} (1+(-3)^{1/2})/2 \\ 2 \\ 2 \end{pmatrix} = \frac{1}{(-3)^{1/2}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \bar{\omega} \\ 1 & \bar{\omega} & \omega \end{pmatrix} \begin{pmatrix} (1+(-3)^{1/2})/2 \\ 2 \\ 2 \end{pmatrix} \tag{4.16}$$

$$= \begin{pmatrix} (1-3(-3)^{1/2})/2 \\ (1+(-3)^{1/2})/2 \\ (1+(-3)^{1/2})/2 \end{pmatrix} \qquad \begin{pmatrix} 1 \\ 4 \\ 4 \end{pmatrix} \sim \begin{pmatrix} 7 \\ 1 \\ 1 \end{pmatrix}$$

$$(4.17)\qquad U\begin{pmatrix}1+2(-3)^{1/2}\\1\\1\end{pmatrix}=\begin{pmatrix}2-(-3)^{1/2}\\2\\2\end{pmatrix}\qquad\begin{pmatrix}13\\1\\1\end{pmatrix}\sim\begin{pmatrix}7\\4\\4\end{pmatrix};$$

$$(4.18)\qquad U\begin{pmatrix}-2+2(-3)^{1/2}\\1\\1\end{pmatrix}=\begin{pmatrix}2\\2+(-3)^{1/2}\\2+(-3)^{1/2}\end{pmatrix}\qquad\begin{pmatrix}16\\1\\1\end{pmatrix}\sim\begin{pmatrix}4\\7\\7\end{pmatrix}$$

$$(4.19)\qquad U\begin{pmatrix}(7+(-3)^{1/2})/2\\-1\\-1\end{pmatrix}=\begin{pmatrix}(1-(-3)^{1/2})/2\\(1-3(-3)^{1/2})/2\\(1-3(-3)^{1/2})/2\end{pmatrix}\qquad\begin{pmatrix}13\\1\\1\end{pmatrix}\sim\begin{pmatrix}1\\7\\7\end{pmatrix}$$

$$(4.20)\qquad U\begin{pmatrix}1+(-3)^{1/2}\\(5+(-3)^{1/2})/2\\(5-(-3)^{1/2})/2\end{pmatrix}=\begin{pmatrix}1-2(-3)^{1/2}\\1+(-3)^{1/2}\\1\end{pmatrix}\qquad\begin{pmatrix}4\\7\\7'\end{pmatrix}\sim\begin{pmatrix}13\\4\\1\end{pmatrix}$$

For any $v\in\mathscr{L}$ in case (4.14), (since R, for $s=4$ or 1, contains only one coset of m) we may apply (4.16) (actually, apply M_1, which applies U to the first three components) to the right vector obtained from following the procedure above (4.16), and obtain some vector in (4.10), (4.11), or (4.12). Then we may omit (4.14) and still have all orbits represented. We apply (4.16) or its conjugate to any element in (4.13) and obtain some vector in (4.15). Then we may omit (4.13). We may apply (4.17) or its complex conjugate to any element in (4.12) to conclude that all orbits of (4.12) are represented by (4.9) and omit (4.12). We may apply (4.20) or its complex conjugate to any element in (4.11) to get into (4.9) and omit (4.11). We may apply (4.19) or its complex conjugate to any element in (4.9) to get into (4.10) and omit (4.9). We may apply (4.18) or its complex conjugate to any element in (4.10) to get into (4.8) and omit (4.10). We are left with only (4.8) and (4.15). By applying elements of P in these cases, we may put the 16 in any arbitrary component and the 4, 4 in any arbitrary pair of components. Then applying elements of $\langle -I_{12}, D\rangle$ to any such v, we get $(2)(3^6)$ distinct elements of $\mathscr{L}$ with the 16 and 4's in the same places. For (4.8), we get $(12)(2)(3^6)$ distinct vectors in the same orbit for S and in (4.8). For (4.15) we get $\binom{12}{2}(2)(3^6)$ vectors. As these are the total numbers of vectors of $\mathscr{L}$ calculated earlier in cases (4.8) and (4.15), respectively, we see that there is just one orbit of $\mathscr{L}$ with $\|v\|^2=18$ and just one orbit O_2 with $\|v\|^2=27$ for S acting on $\mathscr{L}$. As the subgroup of PD fixing $(3(-3)^{1/2}, 0, 0, \ldots, 0)$ has order $|PD|/(12)(3)$, we see that $2^{14}3^85^27\cdot 11\cdot 13=|O_2|(660)(3^5)|\,|S|$. The subgroup of S fixing $(-3)^{1/2}(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$ has the same order $2^{10}3^55\cdot 11$ as $PSU_5(2)$ and intersects $C_S(I_6\oplus\omega I_6)$ in $Z_3\times PSU_4(2)$, also a subgroup of $PSU_5(2)$.

5. **The Conway group.** We are now able to generate a finite complex linear group on the twenty-four coordinates: $x_1, \ldots, x_6, x_{1'}, \ldots, x_{6'}, x_{\bar{1}}\ldots, x_{\bar{6}}, x_{\bar{1}'}, \ldots, x_{\bar{6}'}$. For T a set of matrices or vectors, define $T\oplus\overline{T}$ to be $\{\left(\begin{smallmatrix}s&0\\0&\bar{s}\end{smallmatrix}\right)\mid s\in T\}$ or

$\{(v_1, \ldots, v_{6'}, \bar{v}_1, \ldots, \bar{v}_{6'}) \mid (v_1, \ldots, v_{6'})\} \in T$. Let $C = \langle N_i \rangle$ where, for $i = 1, \ldots, 6$, $N_i = M_i \oplus \overline{M}_i$ with the M_i defined in §1, and the permutation matrix N_7 is given by

$$(1, 2, \bar{6}')(\bar{3}', 6, 5)(\bar{1}', \bar{2}', 4)(\bar{1}, \bar{2}, 6')(3', \bar{6}, \bar{5})(1', 2', \bar{4}).$$

Then $Q = \langle N_7, P \oplus P \rangle$ is imprimitive on the pairs $\{i, \bar{i}\}$, $i = 1, \ldots, 6'$.

We shall show that this twenty-four dimensional group preserves the lattice $\mathscr{L} \oplus \overline{\mathscr{L}}$ which is isomorphic to $\mathscr{L}$ and contains a basis for our 24-dimensional complex space in the variables $x_1, \ldots, x_{\bar{6}'}$. Then C acts faithfully, orthogonally, and Z-linearly on $\mathscr{L} \oplus \overline{\mathscr{L}}$ and this representation tensored with the complex numbers over Z gives the complex linear representation on the variables $x_1, \ldots, x_{\bar{6}'}$. Then C is a subgroup of the Conway linear group. As S preserves $\mathscr{L}$, this lattice is preserved by the N_i, $i = 1, \ldots, 6$. By its imprimitivity on the pairs $\{i, \bar{i}\}$, N_7 preserves the property that the ith and $\bar{i}$th coordinates are complex conjugates, $i = 1, \ldots, 6'$. The first twelve coordinates of $N_7(a_1, \ldots, a_{6'}, \bar{a}_1, \ldots, \bar{a}_{6'})'$ are given by

$$(b_1, \cdots, b_{6'}) = (\bar{a}_{6'}, a_1, a_3, \bar{a}_{2'}, a_6, \bar{a}_{3'}, \bar{a}_4, a_{1'}, \bar{a}_5, a_{4'}, a_{5'}, \bar{a}_2).$$

We must check that this vector lies in $\mathscr{L}$. Writing $x \in Z[\omega]$ as $(a + b(-3)^{1/2})/2$, $a, b \in Z$, we see

(5.1) $x \equiv \bar{x} \pmod{(-3)^{1/2} Z[\omega]}$,

(5.2) if $x \in (-3)^{1/2} Z[\omega]$, then $x \equiv -\bar{x} \pmod{3Z[\omega]}$,

(5.3) if $x \in 3Z[\omega]$, then $x \equiv \bar{x} \pmod{3(-3)^{1/2} Z[\omega]}$.

By (5.1), (3.2) is satisfied. Also, by (5.3),

$$\begin{aligned} 3b_1 + \sum_{i=1}^{6'} b_i &= 3\bar{a}_{6'} + \sum_{i \in S_{10}} a_i + \overline{\sum_{i \in S_{10}} a_i} \equiv 3a_6 + \sum_{i \in S_{10}} a_i + \sum_{i \in S_{10}} a_i \\ &\equiv 3a_1 + \sum a_i \equiv 0 \pmod{3(-3)^{1/2} Z[\omega]}. \end{aligned}$$

We need only check (3.3) for $S = S_1, \ldots, S_{11}$.

$$\sum_{i \in S_1} b_i = \bar{a}_{6'} + a_1 + a_3 + \bar{a}_{2'} + a_6 + \bar{a}_{3'}.$$

By (3.2), $\bar{a}_{6'} + \bar{a}_{2'} + \bar{a}_{3'} \equiv 3\bar{a}_{6'} \equiv 0 \pmod{(-3)^{1/2} Z[\omega]}$, so by (5.2) and (3.3) for S_{10} and S_1

$$\bar{a}_{6'} + \bar{a}_{2'} + \bar{a}_{3'} \equiv -a_{6'} - a_{2'} - a_{3'} \equiv a_2 + a_4 + a_5 \equiv -a_1 - a_3 - a_6 \pmod{3Z[\omega]}.$$

By S_2 and S_{10}

$$\begin{aligned} \sum_{i \in S_2} b_i &= a_1 + a_3 + a_{1'} + \bar{a}_4 + \bar{a}_5 + \bar{a}_{6'} \equiv -a_2 - a_{2'} - a_{3'} - a_4 - a_5 - a_{6'} \\ &\equiv 0 \pmod{3Z[\omega]}. \end{aligned}$$

By S_3 and S_{10}

$$\begin{aligned} \sum_{i \in S_3} b_i &= a_1 + a_{4'} + a_{5'} + \bar{a}_{6'} + \bar{a}_{2'} + \bar{a}_5 \equiv -a_2 - a_4 - a_{3'} - a_{6'} - a_{2'} - a_5 \\ &\equiv 0 \pmod{3Z[\omega]}. \end{aligned}$$

By S'_{10} and S_8

$$\sum_{i\in S_4} b_i = a_1+a_6+a_{4'}+\bar{a}_{6'}+\bar{a}_4+\bar{a}_2 \equiv -a_3-a_{1'}-a_{5'}-a_{6'}-a_4-a_2$$
$$\equiv 0 \pmod{3Z[\omega]}.$$

By S_{11} and S_{10}

$$\sum_{i\in S_5} b_i = a_3+a_{1'}+a_{4'}+\bar{a}_{6'}+\bar{a}_{2'}+\bar{a}_2 \equiv -a_4+a_5-a_{3'}-a_{6'}-a_{2'}-a_2$$
$$\equiv 0 \pmod{3Z[\omega]}.$$

By S'_{10} and S_4

$$\sum_{i\in S_6} b_i = a_3+a_6+a_{5'}+\bar{a}_{6'}+\bar{a}_5+\bar{a}_2 \equiv -a_1-a_{1'}-a_{4'}-a_{6'}-a_5-a_2$$
$$\equiv 0 \pmod{3Z[\omega]}.$$

By S'_{10} and S_5

$$\sum_{i\in S_7} b_i = a_6+a_{1'}+a_{5'}+\bar{a}_{6'}+\bar{a}_{2'}+\bar{a}_4 \equiv -a_1-a_3-a_{4'}-a_{6'}-a_{2'}-a_4$$
$$\equiv 0 \pmod{3Z[\omega]}.$$

By S_6 and S_{10}

$$\sum_{i\in S_8} b_i = a_1+a_3+a_{5'}+\bar{a}_{2'}+\bar{a}_4+\bar{a}_2 \equiv -a_5-a_{3'}-a_{6'}-a_{2'}-a_4-a_2$$
$$\equiv 0 \pmod{3Z[\omega]}.$$

By S'_{10}

$$\sum_{i\in S_9} b_i = a_1+a_3+a_6+a_{1'}+a_{4'}+a_{5'} \equiv 0 \pmod{3Z[\omega]}.$$

By S'_{10} and S_9

$$\sum_{i\in S_{10}} b_i = a_1+a_6+a_{1'}+\bar{a}_{2'}+\bar{a}_5+\bar{a}_2 \equiv -a_3-a_{4'}-a_{5'}-a_{2'}-a_5-a_2$$
$$\equiv 0 \pmod{3Z[\omega]}.$$

By S'_{10} and S_7

$$\sum_{i\in S_{11}} b_i = a_3+a_6+a_{4'}+\bar{a}_{2'}+\bar{a}_5+\bar{a}_4 \equiv -a_1-a_{1'}-a_{5'}-a_{2'}-a_5-a_4$$
$$\equiv 0 \pmod{3Z[\omega]}.$$

By imprimitivity of Q, $d\in(D\oplus\bar{D})^{(D\oplus\bar{D})Q}$ implies $d=(d_1,\ldots,d_{6'},\ldots,d_{\bar{1}'},\ldots,d_{\bar{6}'})$ with $d_{\bar{k}}=\bar{d}_k\in\langle\omega\rangle$, $k=1,\ldots,6'$. Let $\gamma(d)=\operatorname{diag}(d_1,\ldots,d_{6'})$. As $\gamma(d)$ preserves $\mathscr{L}$, $\gamma(d)(4,1,1,\ldots,1)=(4d_1,\ldots,d_{6'})$ satisfies (3.3), so by (2.3), $\gamma(d)\in D$. Then Q normalizes $D\oplus\bar{D}$. Then Q permutes the subset Y of D of elements with no eigenvalue 1. If $d\in Y$ then $\gamma(d)$ has no eigenvalue 1, and by classification of elements of $\phi(D)$ in §2, for some $S=S_i$ or S'_i, $i=1,\ldots,11$, $\phi(d)$ has components all 1 on S

and -1 on S', or $\phi(d)$ has components all equal. Then Q acts on the twelve partitions of $\{1, \ldots, \bar{6}'\}$ into T_i and its complement where

$$T_0 = \{1, \ldots, 6'\}, \qquad T_i = S_i \cup \overline{(\{1, \ldots, 6'\} - S_i)}, \quad \text{for } i = 1, \ldots, 11.$$

As N_7 does not fix the 0th partition, by §2, Q is quadruply transitive on the partitions. Let j be the permutation matrix corresponding to $(1, \bar{1}) \cdots (6', \bar{6}')$. We replace Q by $\langle Q, j \rangle$. (It probably already contained j anyway.) Then $j \in Z(Q)$. Then Q permutes the 12 T_i and their complements transitively. By §2, the subgroup of Q fixing T_0 permutes the 11 sets T_i and their complements transitively. Since C preserves the Leech lattice $\mathscr{L}$, C is a subgroup of the Conway group and $3^{10} \nmid |C|$. Let $W = \{x \mid x \in C$ and x is 6 by 6 block diagonal$\} = C_C(\langle d_1, d_2 \rangle)$ where $d_1 = \omega I_{12} \oplus \bar{\omega} I_{12}$ and $d_2 = \omega I_6 \oplus \bar{\omega} I_6 \oplus \bar{\omega} I_6 \oplus \omega I_6$. (In fact, N_7 was constructed by letting d_2 play the same role as d_1). Then as in §2, W is a central extension of some abelian group A by $PSU_4(3)$. The subgroup of Q, fixing T_0 and T_1, is A_6, so $|Q| = (24)(22)(360) = 2|M_{12}|$. Then $Q/\langle j \rangle \simeq M_{12}$. This also shows that M_{11} is contained in $M_{12} \simeq Q/\langle j \rangle$ in two nonconjugate ways, first, as the subgroup fixing a partition, and, second, as the subgroup fixing a pair $\{i, \bar{i}\}$. As C is written in $Q(\omega)$, all elements of A have the form $a_1 I_6 \oplus \cdots \oplus a_4 I_6$, $a_i \in \langle -\omega \rangle$ and $A = A_2 \times A_3$, the 2 and 3 parts of A. Now, $A_3 \subseteq D \oplus \bar{D}$, otherwise, $3^{10} \mid |A_3(D + \bar{D})Q| \mid |C|$, a contradiction. By the classification of $\phi(D)$, $A_3 = \langle d_1, d_2 \rangle$. Let

$$a = a_1 I_6 \oplus \cdots \oplus a_4 I_6 \in A_2.$$

As a takes $(4, 1, \ldots, 1, 4, 1, \ldots, 1) \in \mathscr{L} + \bar{\mathscr{L}}$ into $\mathscr{L} + \bar{\mathscr{L}}$, $a_1 = a_3$, $a_2 = a_4$, and by (3.2), $a_1 = a_2$. Then $|A| = 18$. The subgroup of Q fixing the partitions corresponding to T_0 and T_1 extends W by the outer automorphism group $\langle \beta, \sigma \rangle$ of order 4. The centralizer in the 24-dimensional Conway group of some element y, with eigenvalues 12 ω's and 12 $\bar{\omega}$'s, is known to be a central extension of Z_6 by the Suzuki group. Now, $(D \oplus \bar{D})Q$ contains a 3-Sylow subgroup of the Conway group. (Later we show that DP contains a 3-Sylow subgroup of S and a similar argument will apply to S.) Three-elements in $(D \oplus \bar{D})Q$ not in $D \oplus \bar{D}$ give monomial matrices with cycles of length 3 and at least three distinct eigenvalues. Therefore, $D \oplus \bar{D}$ contains within conjugacy all elements whose eigenvalues are all ω's and $\bar{\omega}$'s. We showed earlier in this section that $D \oplus \bar{D}$ contains 24 such elements and they are conjugate under Q. Then we may take $y = \omega I_{12} \oplus \bar{\omega} I_{12}$. Then $S \oplus \bar{S} \subseteq C_C(y) \subseteq$(a central extension of Z_6 by the Suzuki group). By §4, the order of the last term divides the order of the first term and we have equality. Now,

$$\begin{aligned} |C| &\geqq |C_C(d_1)| \; |C_C(d_2)| / |C_C(\langle d_1, d_2 \rangle)| \\ &= 2^{28} 3^{16} 5^4 7^2 11^2 13^2 / (18) 2^7 3^6 5 \cdot 7 \\ &= 2^{20} 3^8 5^3 7 \cdot 11^2 13^2 = |\text{24-dimensional Conway group}| / q \end{aligned}$$

where $q = 2^2 3 \cdot 5 \cdot 7 \cdot 11^{-1} 13^{-1} 23 < 68$. As the only proper normal subgroup of the Conway group has order two, and $PSU_4(3)$ contains no subgroup of index

less than 68 by the character table in [5], C is the entire Conway group. By transitivity of S on the closest and second closest points of $\mathscr{L}$ to the origin, $C=SF_1=SF_2$ where F_i is the subgroup of C fixing a fixed ith closest point to the origin, $i=1, 2$.

6. **The automorphism groups of $S/Z(S)$ and $C/Z(C)$.** For $F\subseteq S$, let $\bar{F}$ be the image of F in $S/Z(S)$. Then the following theorem gives the automorphism group of the new simple Suzuki group.

THEOREM 1. *There is only one conjugacy class of subgroups isomorphic to H, a proper central extension of Z_3 by $PSU_4(3)$ in $\bar{S}$. The only automorphisms of $\bar{S}$ fixing H pointwise are inner automorphisms by elements in $Z(H)$. The outer automorphism group of $\bar{S}$ is Z_2 coming from complex conjugation of elements in S.*

Proof. For $d_1=\omega I_6\oplus\bar{\omega}I_6$ let $H=[C_S(d_1)]^-=\langle D, M_0, \ldots, M_5\rangle^-$ by §5. Let $Z(S)\subseteq K\subseteq S$ with $\bar{K}$ another proper central extension of Z_3 by $PSU_4(3)$. Then $|Z(K)|=(3)|Z(S)|$ and K is a reducible linear group. From H we see that non-identity elements in a 7-Sylow subgroup of S have all primitive seventh roots of unity occurring twice as eigenvalues. Therefore, all irreducible constituents of the linear group K have kernels lying in $Z(K)$. By a classification of groups of degree less than six, constituents of K have degree 6. An element of order 9 in $Z(K)$ would have a 9th root of unity as an eigenvalue with multiplicity 6. As the character for S lies in $Z(\omega)$, it would have at least 18 eigenvalues, a contradiction. As $9\mid|Z(K)|$, $Z(K)$ has an element T with six eigenvalues ω, and six eigenvalues $\bar{\omega}$. As in §5, this element is conjugate to d_1, and $C_S(d_1)$ is a central extension of $\langle d_1\rangle Z(S)$ by $PSU_4(3)$. This proves the first statement of the theorem.

Suppose that the automorphism θ of $\bar{S}$ fixes H pointwise. Then θ fixes $\bar{D}$ and $N_{\bar{S}}(\bar{D})$. Now, $N_S(D)=PD$ since $|N_S(D)|=(22)|C_S(d_1)\cap N_S(D)|$ and by [5, Character Table], $[DC_P(d_1)Z(S)]^-$, having index 112 in $\bar{H}$, is maximal in $\bar{H}$ and equals $N_{\bar{H}}(\bar{D})$. Then $C_S(D)=DZ(S)$. Any element in S centralizing $DZ(S)/Z(S)$ centralizes $\langle d_i\mid i=1, \ldots, 11\rangle$ (with d_i as in §2) and centralizes D. Then $C_{\bar{S}}(\bar{D})=\bar{D}$. As θ fixes $\bar{D}$ pointwise, for all $x\in N_{\bar{S}}(\bar{D})$, $x^{-1}\theta(x)$ fixes $\bar{D}$ pointwise and $x^{-1}\theta(x)\in\bar{D}$. Take u to have order 5 in $\bar{P}\cap H$ and normalize $\langle v\rangle$ of order 11 in $\bar{P}$. Then $v^{-1}\theta(v)\in\bar{D}$. Since v has order 11, $|C_{\bar{D}}(v)|=1$ and we may find $d\in\bar{D}$ with $\theta(v)=d^{-1}vd=v^d$. Then $u=\theta(u)$ normalizes $\langle\theta(v)\rangle$ and u^d normalizes $\langle v^d\rangle=\langle\theta(v)\rangle$ so $u^{-1}u^d\in\bar{D}$ normalizes $\langle\theta(v)\rangle$. Therefore, $u^{-1}u^d\in C_{\bar{D}}(\theta(v))=\langle 1\rangle$ and $d\in C(u)$. Then by (2.3) for S_1 and S_1', $d\in\langle d_1\rangle^-$. As I_d, conjugation by d, has the same effect as θ on v, H, which generate $\bar{S}$, we have proved the second statement of the theorem.

Finally, let ρ be any automorphism of $\bar{S}$. By the first statement, without changing the outer automorphism represented by ρ, we may assume that ρ fixes H. As some element of P transposes S_1 and S_1', $[N_S(\langle d_1\rangle Z(S)):C_S(d_1)]=2$. By §5, $C_S(d_1)$ is a central extension of $\langle d_1\rangle Z(S)$ by $PSU_4(3)$. Then $N_S(C_S(d_1))=N_S(\langle d_1\rangle Z(S))$ extends $C_S(d_1)/\langle d_1\rangle Z(S)\simeq PSU_4(3)$ by the automorphism σ from §1, and σ gives an

outer automorphism of $PSU_4(3)$ of order 2. Let $x \in N_S(H) - H$. As $[N_S(H):H] = [N_S(\langle d_1 \rangle Z(S)):[C_S(d_1)]^-] = 2$ and σ normalizes $N_S(H)$, we may let $w = \rho(x)x^{-1} \in H$. Also, I_x, conjugation by x, corresponds to σ of §1. Then, for $y \in H$, $I_x^{-1}\rho I_x y = x\rho(x^{-1}yx)x^{-1} = x\rho(x)^{-1}\rho(y)\rho(x)x^{-1} = w^{-1}\rho(y)w$ and the outer automorphism ρ induces on $H/Z(H) \simeq PSU_4(3)$ commutes with the outer automorphism given by σ and, by §1, lies in $\langle \beta, \sigma \rangle$. Possibly replacing ρ by a product with I_x and/or complex conjugation of S, we may assume that ρ acts as an inner automorphism on $H/Z(H)$. Replacing ρ by a product with I_h for some h in H we may assume that ρ acts trivially on $H/Z(H)$ and H. This finishes the proof by the second statement of the theorem.

THEOREM 2. *There is only one conjugacy class of subgroups isomorphic to L^*, a central extension of Z_3 by $\bar{S}$ in C^*, the simple Conway group where, for $E \subseteq C$, we let E^* be the image of E in $C^* = C/Z(C)$. Furthermore, C^* is complete.*

Proof. Let $Z(C) \subseteq L \subseteq C$ with $L/Z(C)$ a central extension of Z_3 by $\bar{S}$. From $S \oplus \bar{S} \subseteq C$, we see that nonidentity elements in a 13-Sylow subgroup S_{13} of C have all primitive 13th roots of unity occurring twice as eigenvalues. Therefore, all irreducible constituents of the linear group L have kernels lying in $Z(L)$. Since $|Z(L)| = (3)|Z(C)|$, L is a reducible linear group. As $N_S(S_{13})/C(S_{13})$ has order 6 (this can be calculated from $|S|$ since, as in [2, (3F)] $C_S(S_{13}) = S_{13}Z(S)$), all constituents of L have degree divisible by 6. By a classification of complex linear groups of degree 6, and rationality of the character for C, $Z(L)$ has an element T with 12 eigenvalues ω, and 12 eigenvalues $\bar{\omega}$. By §5, this element is conjugate to $d_0 = \omega I_{12} + \bar{\omega} I_{12}$, where $C_C(d_0) = S \oplus \bar{S} \simeq S$. This proves the first statement of Theorem 2.

Therefore, if ψ is any automorphism of C^*, we may assume that ψ fixes $(S \oplus \bar{S})^*$. Let $F = d_0^* = (\omega I_{12} + \bar{\omega} I_{12})^*$. As the permutation matrix $(1, \bar{1}) \cdots (6', \bar{6}')$ acts as complex conjugation on S, by Theorem 1, we may assume that ψ fixes $C_{C^*}(F)$ pointwise. Then ψ fixes $E = (\omega I_6 + \bar{\omega} I_6 + \bar{\omega} I_6 + \omega I_6)^*$, a conjugate of F, and ψ fixes $C_{C^*}(E) \simeq C_{C^*}(F)$. Also, ψ fixes $C_{C^*}(\langle F, E \rangle)$, a central extension by $PSU_4(3)$, pointwise. Applying Theorem 1 to $C_{C^*}(\langle F, E \rangle)/\langle E \rangle \subseteq C_{C^*}(E)/\langle E \rangle \simeq \bar{S}$, we conclude that ψ acts on $C_{C^*}(E)/\langle E \rangle$ as conjugation by some element in $\langle F \rangle$. Replacing ψ by its product with the inner automorphism by some element in $\langle F \rangle$, we may assume also that ψ fixes $C_{C^*}(E)$ pointwise. Since, by §5, $C_{C^*}(F)$ and $C_{C^*}(E)$ generate C^*, this concludes the proof.

7. **The central involutions of $PSU_4(3)$, the Suzuki group, and the Conway group.** Our linear groups U, S, and C have the relationship that the centralizer of some element of order 3 comes from the matrix sum of two twisted copies of the immediately previous group. They also have similar centralizers H_i, $i = 1, 2, 3$, for $G_i = U$, S, and C, respectively, of a central involution. Let K_i be a complement in H_i for the three part of $Z(G_i)$ in H_i. For $i = 1, 3$, and probably for $i = 2$ also, K_i is a central extension of Z_2 by a subgroup $L_i \cdot J_i$ of index two in the automorphism

group of L_i, the central product of the quaternions with themselves $i+1$ times, where J_i is of index 2 in $O_{2i+2}^{(-)^{i+1}}(2)$. One irreducible constituent X_i of the linear group has dimension 2^{i+1}, and the other has dimension 2^i and has L_i in the kernel. For $i=1$ or 3 and probably for $i=2$ also, $X_i(L_i \cdot J_i)$ contains a subgroup of index two in the tensor product of the unimodular 2-dimensional linear group M, isomorphic to $GL(2, 3)$, with itself $i+1$ times. Then, if T is of order 3 in M, $T \otimes I_2 \otimes I_2 \otimes \cdots \otimes I_2$ (i I_2's) corresponds to $\omega I_{3\cdot 2^i-1} \oplus \bar{\omega} I_{3\cdot 2^i-1}$ in U, S, and C, respectively, $i=1, 2, 3$.

References

1. J. H. Conway, *A group of order* 8,315,553,613,086,720,000, Bull. London Math. Soc. **1** (1969), 79–88. MR **40** #1470.

2. R. Brauer, *Über endliche lineare Gruppen von Primzahlgrad*, Math. Ann. **169** (1967), 73–96. MR **34** #5913.

3. J. H. Lindsey II, *Linear groups with an irreducible, normal, rank two p-subgroup* (to appear).

4. ———, *Finite linear groups of degree six* (to appear).

5. ———, *On a six-dimensional projective representation of* $PSU_4(3)$, Pacific J. Math. **36** (1971).

Northern Illinois University,
De Kalb, Illinois 60115