A moonshine path for $5A$ and associated lattices of ranks 8 and 16

Robert L. Griess Jr.
Department of Mathematics
University of Michigan
Ann Arbor, MI 48109 USA
rlg@umich.edu

Ching Hung Lam
Institute of Mathematics
Academia Sinica
Taipei 10617, Taiwan
chlam@math.sinica.edu.tw

Abstract

We continue the program, begun in [20], to make a moonshine path between a node of the extended $E_8$-diagram and the Monster simple group. Our goal is to provide a context for observations of McKay, Glauberman and Norton by realizing their theories in a more concrete form. In this article, we treat the $5A$-node. Most work in this article is a study of certain lattices of ranks 8, 16 and 24 whose determinants are powers of 5.
Contents

1 Introduction 3
  1.1 Acknowledgments 5

2 A preliminary observation 7

3 Uniqueness for $R$ 7

4 Uniqueness of $Q$ 9

5 Embeddings of $Q$ and $R$ in Niemeier lattices 14

6 A suggestion of triality 15

7 Pieces of Eight, à la $DIH_{10}(16)$ 16

A Some general results about lattices 17
  A.1 About the centralizer of an $EE_8$ dihedral group of order 10 in $O(N(A_8^6))$ 23

B The finite orthogonal groups 24

C Finite subgroups of $E_8(\mathbb{C})$ 28

D Finite subgroups of $O(n,\mathbb{F})$ which centralize root groups 30
1 Introduction

In [20], we initiated a program for establishing moonshine paths between the extended $E_8$-diagram and the monster simple group and treated the case of the $3C$-node in detail. The present article treats the case of the $5A$-node, which corresponds to a pair of Monster involutions in class $2A$ which generate a dihedral group of order 10.

Such a group corresponds naturally to a dihedral group of order 10 which acts on the rank 24 Leech lattice and which is generated by pairs of trace 8 involutions. Most work in this article is a study of lattices, in particular certain rootless rank 8 and 16 lattices of determinant $5^4$ and their embeddings in Niemeier lattices and other related embeddings. We give attention to the role of $EE_8$-sublattices because of their occurrence within $Q$ and $\Lambda$ and their role in VOA theory [19].

The introduction of [20] has a detailed discussion of context, which involves lattices, VOAs, Lie theory and finite groups. Our desire is to take mystery out of McKay’s $E_8$-Monster connection. In particular, we note the Glauberman-Norton theory [10] with its interesting observation that particular centralizers in the Monster involve “half” the Weyl group of a node in the extended $E_8$-diagram. In [20], we gave an interpretation within our moonshine path theory for why just half a Weyl group occurs in the $3C$-case. The present article treats the $5A$-case. Work on other nodes is planned.

Theorem 1.1. Suppose that $R$ is a rank 8 rootless even lattice such that $D(R) \cong 5^4$. Then

(i) $R$ is unique up to isometry.

(ii) $O(R) \cong O^+(4,5)$.

(iii) $O(R)$ acts faithfully on $D(R)$ and $O(R)$ contains no SSD involutions.

Theorem 1.2. Suppose that $Q$ is a rank 16 rootless even lattice such that $D(Q) \cong 5^4$. Then

(i) $Q$ is unique up to isometry.

(ii) There exists an embedding $O(Q) \rightarrow \text{Frob}(20) \times O^+(4,5)$ such that the image has index 2 and contains neither direct factor.

(iii) The action of $O(Q)$ on $D(Q)$ induces $O(D(Q)) \cong O^+(4,5)$ and the kernel is isomorphic to $\text{Dih}_{10}$. The set of SSD-involutions in $O(Q)$ generates this kernel.
Theorem 1.3. Let $\Lambda$ be a Leech lattice. Let $R, Q$ be integer lattices of respective ranks 8, 16, such that $D(R) \cong D(Q) \cong 5^4$.

(i) In $\Lambda$, the set of sublattices isometric to $R$ forms an orbit under $O(\Lambda)$.

(ii) In $\Lambda$, the set of sublattices isometric to $Q$ forms an orbit under $O(\Lambda)$.

Corollary 1.4. Let $D$ be the dihedral group generated by a pair of defining $E_{8}$-involutions in $Q \cong \text{DIH}_{10}(16)$. Then $N := N_{O(\Lambda)}(D)$ has shape $N/D \cong O^{+}(4, 5)$ and is isomorphic to the unique subgroup of index 2 in $\text{Frob}(20) \times O^{+}(4, 5)$ which contains the subgroup $\text{Dih}_{10} \times \text{GL}(2, 5)$ and does not contain either direct factor of $\text{Frob}(20) \times O^{+}(4, 5)$. The action of $N$ on $Q$ is faithful and the action of $N$ on $R$ has kernel $D$.

Corollary 1.5. In $O(R)$, the set of SSD involutions is empty. In $O(Q)$, the set of SSD involutions is the set of five $E_{8}-$involutions in the normal dihedral group.

Proof. Use (1.1), (1.2) and (A.9). □

Corollary 1.6. The centralizer in $O(\Lambda)$ of $D$ is isomorphic to

$$(SL(2, 5) \circ SL(2, 5)):2,$$

where the outer elements of order 2 normalize each of the two quasisimple central factors under conjugation and induce noninner automorphisms.

Theorem 1.7. Let $R, Q$ be as in (1.1), (1.2). There are three orbits of $O(Q \perp R)$ on the set of Niemeier overlattices of $Q \perp R$. Let $L$ be such an overlattice and define the integer $e$ by $5^{e} := |Q \otimes R \cap L : R|$. The three orbits are distinguished by the common value of $e \in \{0, 1, 2\}$ for their members. We have $L \cong \Lambda, N(A^3_1), E_8^3$ for $e = 0, 1, 2$, respectively. The stabilizer in $O(Q) \times O(R)$ of a Niemeier overlattice is a subgroup $H$ of the following form (we identify $O(Q) \times O(R)$ with $O(Q \perp R)$ in the obvious way):

- $e = 0$: $H \cap O(R) = 1, H \cap O(Q) \cong \text{Dih}_{10}, H \cong O(Q)$ (so $H/(H \cap O(Q)) \cong O^{+}(4, 5)$);
- $e = 1$: $H \cap O(R) = 5, H \cap O(Q) \cong \text{Dih}_{10} \times 5, H/(H \cap O(Q)) \cong O^{+}(2, 2) \cong 4 \rtimes 2$.
- $e = 2$: $H = (H \cap O(Q)) \times (H \cap O(R)), H \cap Q \cong \text{Dih}_{10,5} \times \text{GL}(2, 5), H \cap O(R) \cong 5 \times \text{GL}(2, 5)$. 
We obtain a structure analysis of $C_{O(\Lambda)}(D)$ and in particular show that $C_{O(\Lambda)}(D)/O_2(C_{O(\Lambda)}(D))$ is isomorphic to “half” of the Weyl group of type $A_2^3$. These results may be lifted to a statements [10] about the Monster as follows. There exist suitable $x, y, z$ in the Monster $(x, y$ in $2A, xy$ in $5A, z \in 2B \cap C_5(x, y))$ so that $C_5(x, y, z)$ has a homomorphism onto $C_{O(\Lambda)}(D)/O_2(C_{O(\Lambda)}(D))$. In analogy with [20], we point out a presence of triality.

As in [20], a study of associated conformal vectors of central charge $\frac{1}{2}$ leads to embedding results for certain VOAs. We shall refer to [20], Section 2 and Appendix B, for details.

1.1 Acknowledgments

The first author thanks the United States National Science Foundation (NSF DMS-0600854) and National Security Agency (NSA H98230-10-1-0201) for financial support and the Academia Sinica for hospitality during a visit, December, 2009.

The second author thanks National Science Council (NSC 97-2115-M-006-015-MY3) and National Center for Theoretical Sciences of Taiwan for financial support and University of Michigan for hospitality during a visit, March, 2010.

We thank Gabriele Nebe, Rudolf Scharlau and Rainer Schulze-Pillot for helpful advice about integer lattices. After we obtained our results, we learned that the characterization of $R$ as in (1.1) had been known [30]. Also, see the earlier articles [5], [26].

Quite recently, a study of the genus of rank 16, discriminant group $5^4$ integral lattices was completed by Scharlau and Hemkemeier, using the software package “tn” [34]. Those authors found that the genus has 848 members, just one of which is rootless. This is in agreement with our (1.2). A reference to this lattice and its isometry group is row 11 in [28], page 86 and [31].
### Notation and Terminology

| Notation | Explanation | Examples in text |
|----------|-------------|------------------|
| $2A, 2B, 3A,\ldots$ | conjugacy classes of the Monster: the first number denotes the order of the elements and the second letter is arranged in descending order of the size of the centralizers | Introduction |
| $A_1,\cdots,E_8$ | root lattice for root system | Sec. 2 |
| $AA_1,\cdots,EE_8$ | lattice isometric to $\sqrt{2}$ times the lattice $A_1,\cdots,E_8$ | Page 2 |
| $A \circ B$ | central product of groups $A$ and $B$ | Coro B.3 |
| $\mathcal{D}(L)$ | discriminant group of integral lattice $L$: $L^*/L$ | Notation 2.1, Lemma 2.2 |
| $EE_8$-involution | SSD involution whose negated space is isometric to $EE_8$ | (4.11) |
| $G', G'',\ldots$ | first, second, … commutator subgroup of the group $G$ | (A.17) |
| $G^{(\infty)}$ | the terminal member of the derived series (commutator series) of the group $G$ | (A.17) |
| $h$ | a fixed point free automorphism of $E_8$ of order 5 | Remark 3.3 |
| $L(a,\cdots)$ | a lattice created by a gluing of 2-spaces from orbit of 2-spaces from orbit of type $O\,\text{orbit}(a,\cdots)$ | (4.6) |
| Niemeier lattice | a rank 24 even unimodular lattice | Lemma 5.2 |
| $\mathcal{N}(X)$ | Niemeier lattice whose root system has type $X$ | Lemma 5.2 |
| $O(X)$ | the isometry group of the quadratic space $X$ | (3.4), (4.7) |
| $O\,\text{orbit}(a,\cdots)$ | orbit of $O^+(4,q)$ on 2-spaces: $a$ denotes the dimension of the radical of the 2-space | (B.6) |
| root group | subgroup of group of Lie type associated to a root (see [2]) | (D.1) |
2 A preliminary observation

Notation 2.1. Let \( L \) be an integral lattice. We shall denote the discriminant group \( L^* / L \) of \( L \) by \( \mathcal{D}(L) \).

Lemma 2.2. Let \( R, Q \) be integer lattices of respective ranks 8, 16, such that \( \mathcal{D}(R) \cong \mathcal{D}(Q) \cong 5^4 \). (i) The quadratic spaces \( \mathcal{D}(R) \) and \( \mathcal{D}(Q) \) have maximal Witt index.

(ii) In each case there exist overlattices of the same rank which are even and unimodular.

Proof. The assumptions in (1.1) imply that the quadratic space \( \mathcal{D}(R) \) has maximal Witt index. The reason is that there exists an \( R \) with all these properties (see (3.2), for example) and all lattices with these properties have the same genus. See [4], p.386, and [30]. A similar discussion applies to the lattices of (1.2); see [19] or (C.5) or just observe that \( Q \) and \( E_8 \perp R \) are in the same genus. \( \square \)

3 Uniqueness for \( R \)

Notation 3.1. We let \( R \) be a rootless rank 8 even integral lattice.

In this section, we shall establish the uniqueness for \( R \) and prove Theorem 1.1.

Lemma 3.2. Let \( R \) be as in (3.1).

(i) Then \( R \) is contained in a copy of the \( E_8 \) lattice in \( \mathbb{Q} \otimes R \).

(ii) The orthogonal group on \( \mathbb{Q} \otimes R \) has one orbit on the set \( \mathcal{A} \) of pairs \( (X,Y) \) where \( X \cong R, Y \cong E_8 \) and \( X \leq Y \). In particular, the conditions of (3.1) characterize \( R \) up to isometry.

(iii) If \( X \cong R \), the number of \( Y \cong E_8 \) so that \( (X,Y) \in \mathcal{A} \) is 12.

(iv) If \( Y \cong E_8 \), the number of \( X \cong R \) so that \( (X,Y) \in \mathcal{A} \) is \( \frac{|\text{Weyl}(E_8)|}{|S \times \text{GL}(2,5)|} = 2^9 3^4 7 \).

Proof. (i) Since \( \mathcal{D}(R) \) has Witt index 2, there exists an integral lattice \( J \) so that \( J \geq R \) and \( |J : R| = 25 \). Since \( R \) is even and its index is odd, \( J \) is even. By the well-known characterization of \( E_8 \), \( J \cong E_8 \). (See [17] for a survey of characterizations of \( E_8 \).)

(ii) The second statement follows from (C.3).
(iii) The number of totally singular subspaces in $D(R)$ is 12. A lattice between $R$ and $R^*$ which is even and unimodular corresponds to such a subspace. The lattice between $R$ and $R^*$ corresponding to such a subspace is even and unimodular, hence isometric to $E_8$.

(iv) This follows from (C.3)(iii). □

**Remark 3.3.** Let $h$ be a fixed point free order 5 element in $O(E_8)$. Then $h$ is unique up to conjugacy in $O(E_8)$ and $(h - 1)E_8$ has the discriminant group $5^4$ and has maximal Witt index. In addition, $(h - 1)E_8$ is rootless (C.2). Thus, $(h - 1)E_8 \cong R$.

**Lemma 3.4.** We use the notation of (C.3)(iii). Let $Y = E_8$ and let $X \leq Y$ be a rootless sublattice so that $Y/X \cong 5^2$.

(i) $O(X) \cap O(Y)$ has order 2400 and is isomorphic to $5:GL(2, 5) \cong (5 \times SL(2, 5)) : 4$, order $2^53^{-5}2$.

(ii) $O(X) \cap O(Y)$ acts faithfully on $D(X)$ and on $D(Y)$ and has index 12 in $O(X)$.

(iii) $O(X)$ acts faithfully on $D(X)$ and induces $O(D(X)) \cong O^+(4, 5) \cong (SL(2, 5) \circ SL(2, 5)) : 2^2$ on it. In particular, $|O(X)| = 2^7325^2$.

**Proof.** (i) This follows from (C.3)(iii). Since $O(X) \cap O(Y)$ induces $GL(2, 5)$ on $Y/X$, the kernel of the action on $D(X)$ is contained in the normal subgroup of order 5. Such an element of order 5 in fact acts on $D(X)$ and on $D(Y)$ with a pair of Jordan blocks of degree 2 (this follows from (C.3)(iv)). Compare with (B.3). Thus, (ii) follows.

(iii): By transitivity in (3.2)(iii), we get $|O(X) : O(X) \cap O(Y)| = 12$, whence $|O(X)| = |O^+(4, 5)|$. By faithful action (i), we get $O(X) \cong O^+(4, 5)$. □

Now Theorem 1.1 follows from Lemma 3.2 (ii) and Lemma 3.4 (iii).

**Lemma 3.5.** (i) There exists a sublattice in $R$ isometric to $A_4(1) \perp A_4(1)$. We obtain an overlattice $R$ from a sublattice of shape $A_4(1) \perp A_4(1)$ in $R$ are obtained by gluing a singular vector in $D(A_4(1))$ to a singular vector in $D(A_4(1))$. Therefore, $R$ is isometric to a sublattice of index 5 in $A_4 \perp A_4$.

(ii) The cosets of $R$ in $R^*$ have the following minimal norms

- zero coset: 0
- singular coset: 2
- nonsingular coset (the numerator is a square mod 5): $\frac{4}{5}, \frac{6}{5}$,
- nonsingular coset (the numerator is a nonsquare mod 5): $\frac{2}{5}, \frac{12}{5}$.
Proof. (i) For the first statement, see (C.3)(iv). A look at minimum norms in duals (3.1) shows that only a gluing of singular cosets allows the overlattice $R$ to be rootless. Now use $O(A_4(1)) \cong 2 \times PGL(2, 5)$ [19].

(ii) By (B.1) and Witt’s theorem applied to the action of $O(R)$ on $D(R)$, the norms in $\mathbb{F}_5$ indicate the orbits. The norms may be read off from (A.5) because of the gluing described in (i). □

4 Uniqueness of $Q$

Notation 4.1. We let $Q$ be a rank 16 rootless integral lattice with $D(Q) \cong 5^4$. By Lemma 2.2, $D(Q)$ is a quadratic space with maximal Witt index. We let $U$ be a unimodular rank 16 even integral lattice which contains $Q$. The Witt classification [36] allows two possibilities, $U \cong HS_{16}$ or $U \cong E_8 \perp E_8$.

Next we shall study the isometry type of $Q$ and establish Main Theorem 1.2.

Lemma 4.2. A lattice $Q$ as in (4.1) does not embed in $HS_{16}$.

Proof. Suppose that there is such an embedding of $Q$ into $S \cong HS_{16}$. Then $S/Q \cong 5^2$. If $T$ is the root sublattice of $S$, then $Q \cap T$ is a rootless sublattice of $T$. This corresponds to an elementary abelian group of order 25 in the Lie group of type $D_{16}$ whose centralizer is just a torus. By (D.3), no such group exists. □

Theorem 4.3. We let $Q$ be as in (4.1). Then $Q$ is unique up to isometry. In particular, $Q \cong DIH_{10}(16)$ [19].

Proof. (4.2), (C.5). □

Lemma 4.4. Let $U_1, U_2$ be the orthogonal direct summands of $U$ which are isometric to $E_8$.

(i) Let $W$ be any sublattice of $U$ which is rootless and has determinant $5^4$. Then $W \cap U_i$ is isometric to $R$, for $i = 1, 2$.

(ii) The natural map of $W$ in $D((W \cap U_i))$ is onto, for $i = 1, 2$.

Proof. (i) Since $W$ is rootless, so are the $W \cap U_i$ and so each $|U_i : U_i \cap W|$ is divisible by $5^2$ (C.1). Since $\text{det}(W) = 5^4$, $5^2 = |U : W| \geq |U_i : U_i \cap W|$, for $i = 1, 2$, whence equality. Now use (3.2).

(ii) This follows from (i) and determinant considerations. □
Remark 4.5. As in Section 2 of [20], we can obtain an explicit embedding of $Q \cong DIH_{10}(16)$ in $E_8 \perp E_8$ as follows. Let $h \in O(E_8)$ be a fixed point free element of order 5. Denote
\[
M := \{(\alpha, \alpha) \in E_8 \perp E_8 \mid \alpha \in E_8\},
\]
\[
N := \{(h\alpha, \alpha) \in E_8 \perp E_8 \mid \alpha \in E_8\}.
\]
By direct calculation, it is easy to show that $t_M t_N = h^{-1} \oplus h$ has order 5. Notice that $t_M(\alpha, \beta) = -\beta, \alpha)$ and $t_N(\alpha, \beta) = -(h\beta, h^{-1}\alpha)$ for any $(\alpha, \beta) \in E_8 \perp E_8$. Moreover, $M + N$ is rootless since $(h^{-1})E_8$ is (C.2). Thus, $M + N \cong DIH_{10}(16) \cong Q$ by the classification of rootless $EE_8$ pairs [19].

Lemma 4.6. (i) Let $J$ be an overlattice of $R_1 \perp R_2$, where $R_1 \cong R_2 \cong R$, such that $J$ is obtained by gluing 2-spaces $W_1$ from $D(R_1)$ and $W_2$ from $D(R_2)$. If $J$ is integral, then $W_1$ and $W_2$ are isometric.

(ii) An integral overlattice $J$ of $R_1 \perp R_2$ corresponding to a gluing of 2-spaces from orbits of type $\text{Orbit}(a, \cdots)$ (see (B.6)) in the respective quadratic spaces $D(R_1)$ and $D(R_2)$ is denoted $L(a, \cdots)$. The minimum norms are given below. The associated discriminant groups have maximal Witt index.

\[
\begin{align*}
L(2) & : 4, \\
L(1, s) & : 2, \\
L(1, n) & : 4, \\
L(0, 1) & : 2, \\
L(0, 0) & : 2.
\end{align*}
\]

Proof. (i) The projections $p_i$ to the spaces $\mathbb{Q} \otimes R_i$ have the property that for all $v \in J$, $p_i(v)$ has norm in $\frac{5}{2}\mathbb{Z}$ for $i = 1, 2$ and that the sum of these two norms is in $2\mathbb{Z}$. This means that the associated linear isomorphism $W_1 \to W_2$ is the negative of an isometry. Since $-1$ is a square modulo 5, the quadratic spaces $W_1, W_2$ are isometric.

(ii) Use (B.6), (3.5) and the fact that $-1$ is a square modulo 5. □

Corollary 4.7. We use the notation of (4.6). Suppose $J$ is isometric to $Q$ and is in $\text{Orbit}(2)$. Let $p_i$ be the orthogonal projection to $\mathbb{Q} \otimes R_i$, $i = 1, 2$. Then

(i) $\text{Stab}_{O(R_i)}(p_i(J))$ has shape $5:GL(2,5) \cong (5 \times SL(2,5)):4$, for $i = 1, 2$.

(ii) The kernel of the action of $\text{Stab}_{O(R_i)}(J)$ on $p_i(J)/R_i$ is the normal subgroup of order 5, for $i = 1, 2$. 

10
Lemma 4.9. Let $D$ be the action on $D$ such that the image has index 2 and contains neither direct factor.

Proof. The order of $D$ is 8, hence $D$ is a subgroup of order 5.

Orbit Corollary 4.10. There exists an embedding $O(Q) \to Frob(20) \times O^+(4,5)$ such that the image has index 2 and contains neither direct factor.

Proof. Use (B.10) and follow the arguments of (4.7).

Lemma 4.9. $|O(Q)| = 10|O^+(4,5)| = 2^83^25^2$ and $O(Q)$ induces $O^+(4,5)$ on $D(Q)$. The kernel of the action is $K$, the dihedral group generated by a pair of $EE_8$-involutions whose negative eigenspaces generate $Q$.

Proof. The order of $O(Q)$ is determined since $O(Q)$ acts transitively on the set of overlattices isometric to $E_8 \perp E_8$ and the stabilizer of one of them has the form given in (4.6)(v).
Proof. A consequence of (A.10) is that $O(Q)$ maps onto $\text{Aut}(\text{Dih}_{10}) \cong \text{Frob}(20)$ by its doubly transitive action on the involutions of $\langle t, u \rangle$. Therefore, the normal subgroup $H$ of $O(Q)$ which centralizes $\langle t, u \rangle$ has index 20. It follows that $H$ acts faithfully on $\mathcal{D}(Q)$ and induces on $\mathcal{D}(Q)$ a subgroup of index 2 in $O^+(4,5)$. We have $H \cap \langle t, u \rangle = 1$. □

Lemma 4.11. Since $Q \cong \text{DIH}_{10}(16)$, $Q$ is spanned by a pair of $EE_8$-lattices. The SSD-involutions corresponding to any $EE_8$-sublattice stabilize any $E_8^2$ overlattice of $Q$ and interchange its two indecomposable summands.

Proof. Use (A.11). □

Lemma 4.12. The cosets of $Q$ in $Q^*$ have the following minimal norms:

- zero coset: 0
- singular coset: 2
- nonsingular coset (the numerator is a square mod 5): $\frac{11}{5}, \frac{16}{5}$
- nonsingular coset (the numerator is a nonsquare mod 5): $\frac{8}{5}, \frac{12}{5}$

Proof. Let $U$ be an overlattice of $Q$, where $U = U_1 \perp U_2$, $U_i \cong E_8$, $i = 1, 2$. Denote $R_i = Q \cap U_i$, $i = 1, 2$. Then $R_1 \cong R_2 \cong R$. We may also assume

$$Q = \text{span}\{\{(\alpha, \alpha) \mid \alpha \in E_8\} \cup R_1 \cup R_2\}.$$ 

Then

$$Q^* = \text{span}\{\{(\gamma, -\gamma) \mid \gamma \in R^*\} \cup U_1 \cup U_2\}.$$ 

The minimum norms of the cosets may be read off from (3.5). □

We summarize our results on rank 16 lattices.

Notation 4.13. We define the following pairs of lattices in Euclidean space $\mathbb{R}^{16}$:

- $A := \{(X, Y) \mid X \leq Y, X \cong R_1 \perp R_2, Y \cong Q\}$,
- $A^+ := \{(X, Y) \in A \mid Y \in \text{Orbit}(2) \text{ with respect to } X; \text{ see } (4.6)\}$ and
- $A^- := \{(X, Y) \in A \mid Y \in \text{Orbit}(1, n) \text{ with respect to } X; \text{ see } (4.6)\}$,
- $B := \{(Y, Z) \mid Y \leq Z, Y \cong Q, Z \cong E_8 \perp E_8\}$.

Theorem 4.14. (i) The group $O(16, \mathbb{R})$ acts transitively on each of the sets $A^+, A^-, B$. 

12
(ii.a+) If \((X,Y) \in \mathcal{A}^+\), we have

\[
\begin{align*}
O(X) &\cong O^+(4,5) \cdot 2, & |O(X)| &= 2^{15}3^45^4, \\
O(Y) &\cong \text{Dih}_{10} \cdot O^+(4,5), & |O(Y)| &= 2^{8}3^25^3, \\
O(X) \cap O(Y) &\cong (\text{Dih}_{10} \times 5):\text{GL}(2,5), & |O(X) \cap O(Y)| &= 2^63^25^2, \\
|O(X) : O(X) \cap O(Y)| &= 2^93^52^5, & |O(Y) : O(X) \cap O(Y)| &= 2^23^55^2.
\end{align*}
\]

(ii.a−) If \((X,Y) \in \mathcal{A}^-\), we have

\[
\begin{align*}
O(X) &\cong O^+(4,5) \cdot 2, & |O(X)| &= 2^{15}3^45^4, \\
O(Y) &\cong \text{Dih}_{10} \cdot O^+(4,5), & |O(Y)| &= 2^{8}3^25^3, \\
O(X) \cap O(Y) &\cong 5^2(4 \times 2 \times 2 \times 2), & |O(X) \cap O(Y)| &= 2^55^2, \\
|O(X) : O(X) \cap O(Y)| &= 2^{10}3^45^2, & |O(Y) : O(X) \cap O(Y)| &= 2^33^25.
\end{align*}
\]

(ii.b) If \((Y,Z) \in \mathcal{B}\), we have

\[
\begin{align*}
O(Y) &\cong \text{Dih}_{10} \cdot O^+(4,5), & |O(Y)| &= 2^{8}3^25^3, \\
O(Z) &\cong O(E_8) \cdot 2, & |O(Z)| &= 2^{20}3^{10}5^47^2, \\
O(Y) \cap O(Z) &\cong \text{Dih}_{10} \cdot (5 \times \text{GL}(2,5)), & |O(Y) \cap O(Z)| &= 2^63^25^3, \\
|O(Y) : O(Y) \cap O(Z)| &= 2^23, & |O(Z) : O(Y) \cap O(Z)| &= 2^{23}3^{9}5^27^2.
\end{align*}
\]

(iii) Given \(Y \cong Q\), there is a bijection between the set of \(X\) such that \((X,Y) \in \mathcal{A}^+\) and the set of \(Z\) such that \((Y,Z) \in \mathcal{B}\). The bijection may be described as follows.

If we write \(X = X_1 \perp X_2 \ (X_1 \cong X_2 \cong R)\), the associated \(Z\) is \(\text{proj}_{X_1}(Y) \perp \text{proj}_{X_2}(Y)\).

If we write \(Z = Z_1 \perp Z_2 \ (Z_1 \cong Z_2 \cong E_8)\), the associated \(X\) is \((Z_1 \cap Y) \perp (Z_2 \cap Y)\).

\textbf{Proof.} For orders of \(O(R), O(Q)\), see (3.4), (4.9). The order of \(O(E_8)\) is \(2^{143527}7\).

For \(\mathcal{A}^+\), see (4.7)(iii).

For \(\mathcal{A}^-\), see (4.8)(iii).

For \(\mathcal{B}\), see (4.9) and note that an even unimodular overlattice of \(Q\) must correspond to a maximal totally singular subspace of \(\mathcal{D}(Q)\). \(\square\)
5 Embeddings of $Q$ and $R$ in Niemeier lattices

Notation 5.1. We suppose that $\Lambda$ is a Leech lattice containing a sublattice $Q'$ isometric to $Q$. We define $R' := \text{ann}_\Lambda(Q')$. Then $R'$ is an even rank 8 lattice and $D(R') \cong D(Q') \cong 5^4$ [21]. By (3.2), $R' \cong R$.

Proposition 5.2. Let $N$ be a Niemeier overlattice of $Q \perp R$. Let $X := N \cap R^*$ and $Y := N \cap Q^*$. Define the integer $e$ by $5e = |X : R| = |Y : Q|$. Then $e \in \{0, 1, 2\}$. There exists a Niemeier overlattice of $Q \perp R$ which realizes each of these values of $e$.

(i) If $e = 0$, then $N \cong \Lambda$. Moreover, $O(Q \perp R)$ acts transitively on the set of Niemeier overlattices which contain each of $Q$ and $R$ as a direct summand. Therefore, the embedding of $Q \perp R$ into $\Lambda$ is essentially unique;

(ii) If $e = 1$, then $N \cong N(A_4^6)$ and $O(Q \perp R)$ acts transitively on the set of Niemeier overlattices such that $X/R \cong Y/Q \cong 5$; these Niemeier lattices are isometric to $N(A_4^6)$.

(iii) If $X/R \cong Y/Q \cong 5^2$, then $N \cong E_8^3$ and $O(Q \perp R)$ acts transitively on the set of Niemeier overlattices such that $X/R \cong Y/Q \cong 5^2$; these Niemeier lattices are isometric to $E_8^3$.

Proof. Since an integral overlattice corresponds to a totally singular subspace of the discriminant group, $e \leq 2$. In all three cases, transitivity follows from (A.12), (A.13) and the fact that the projection of $N$ to $R^*$ lies in $X^*$. Finally, we must settle the isometry types in those respective orbits.

Since the minimal norms for $Q^*$ and $R^*$ are $8/5$ and $4/5$, respectively (see (4.12) and (3.5)) and $8/5 + 4/5 = 12/5 > 2$, the roots of $N$ must be in $Y \perp X$. For case (i), this means $N$ is rootless, so is isometric to the Leech lattice. For (ii), note that since $X$ is a direct summand, the root sublattice of $N$ has an indecomposable orthogonal component isometric to $A_4$. Since the Coxeter number of all components of the root system is the same [35], the root system of $N$ is $A_4^6$ and $N \cong N(A_4^6)$.

(iii) If $X/R \cong Y/Q \cong 5^2$, then $X$ and $Y$ are both even unimodular. Thus, $X \cong E_8$ and $Y \cong E_8^2$ or $HS_{16}$. However, $Q$ cannot be embedded into $HS_{16}$ by (4.2) and hence $N \not\cong N(D_{16}E_8)$. Therefore, $N \cong E_8^3$. □

Main Theorems 1.3 and 1.4 now follow from (4.10) and (5.2).

Finally, we shall prove Corollary 1.6 and Main Theorem 1.7.
Proof of Corollary 1.6. The centralizer in $O(\Lambda)$ of $D$ is isomorphic to a group $H$ of index 2 in $O^+(4,5)$ (4.10), (5.2). Let $Z := Z(O^+(4,5))$. We have that $H/Z$ is isomorphic to one of $Alt_5 \wr 2$ or the even subgroup of $Sym_5 \times Sym_5$ (B.4). Both of these groups contain subgroups isomorphic to upwards extensions of $PSL(2,5)$ by nonidentity cyclic 2-groups but only the latter contains such a subgroup which normalizes a group of order 5. By (4.7), $Alt_5 \wr 2$ can not occur as the central quotient of $O(\Lambda)(D)$. □

Proof of Main Theorem 1.7.

We use (5.2) and (A.16)(iii), applied to $X$ and $Y$ in the notation of (5.2) to obtain a group $S$. The group $H$ is $S \cap O(Q \cap R)$.

For all $e = 0, 1, 2$, $S \cap O(Q \cap R)$ covers $S/(S \cap O(X) \times (S \cap O(Y))$ since $O(Q), O(R)$ induces the full orthogonal group on $D(Q), D(R)$, respectively; see (A.13). Therefore, $H$ is an extension of normal subgroup $\{g \in O(R) \cap O(X) \mid (g - 1)N \leq X\} \times \{g \in O(Q) \cap O(Y) \mid (g - 1)N \leq Y\}$ by quotient isomorphic to $O(D(X)) \cong O(D(Y))$ (we have $D(X) \cong D(Y) \cong \mathbb{F}_2^{3,2e}$, a quadratic space of maximal Witt index). We give descriptions of the normal subgroup $\{g \in O(R) \cap O(X) \mid (g - 1)N \leq X\} \times \{g \in O(Q) \cap O(Y) \mid (g - 1)N \leq Y\}$ in the respective cases below.

For $e = 0$, $\{g \in O(R) \cap O(X) \mid (g - 1)N \leq X\} \cong 1$ and $\{g \in O(Q) \cap O(Y) \mid (g - 1)N \leq Y\} \cong Dih_{10}$.

For $e = 1$, $\{g \in O(R) \cap O(X) \mid (g - 1)N \leq X\} \cong 5$ and $\{g \in O(Q) \cap O(Y) \mid (g - 1)N \leq Y\} \cong Dih_{10} \times 5$.

For $e = 2$, $\{g \in O(R) \cap O(X) \mid (g - 1)N \leq X\} = O(R) \cap O(X) \cong 5:GL(2,5)$ and $\{g \in O(Q) \cap O(Y) \mid (g - 1)N \leq Y\} = O(Q) \cap O(Y) \cong (Dih_{10} \times 5):GL(2,5)$.

6 A suggestion of triality

The moonshine VOA [9] was built from a VOA based on the Leech lattice and some of its modules. A so-called extra automorphism (sometimes called “triality”) was constructed which, with a natural group acting on the VOA, generated a copy of the Monster acting as VOA automorphisms.

For the 3C-case [20], a Weyl group is associated to one type of overlattice and triality is used to create a twist of this Weyl group and a corresponding twist of glue map, which is used to define a different type of overlattice. (The Weyl group of $E_8$ has a unique nonsolvable compostion factor isomorphic to
$D_4(2)$, which has a group of graph automorphisms representing triality.) The “loss” of half the Weyl group was due to passing to a half-spin module which affords a projective representation of the special orthogonal group but not the whole orthogonal group.

Remark 6.1. For our 5A-situation, it is not obvious how to imitate the above program. Nevertheless, one can point to weak analogues of our 3C story. For example, the cases $e = 0$ and $e = 2$ in (1.7) give a central extension of $SL(2,5) \circ SL(2,5)$ to $SL(2,5) \times SL(2,5)$. Such an extension can be created by lifting from the special orthogonal group to the spin group (of type $D_4$, which has triality).

If we consider the isometry groups of the three kinds of Niemeier overlattices, we see a variety of upward and downward extensions of $PSL(2,5) \times PSL(2,5)$ within the centralizer of the dihedral group of order 10.

Let $N$ be a Niemeier overlattice and $D$ a dihedral group of order 10 generated by a pair of $EE_8$-involutions.

If $N \cong E_8^3$, $O_{O(N)}(D) \cong O(E_8) \times Dih_{10} \times 5 \times 2$; this group contains both $Sym_5 \wr 2$ and $O^+(4, 5)$.

If $N \cong \Lambda$, $O_{O(N)}(D) \cong (SL(2,5) \circ SL(2,5)) : 2$; this group does not contain a subgroup isomorphic to $Alt_5 \times Alt_5$.

If $N \cong N(A_4^6)$, $O_{O(N)}(D)$ contains $Alt_5 \times Alt_5$ but not $SL(2,5) \circ SL(2,5)$ (A.17).

7 Pieces of Eight, à la $D IH_{10}(16)$

The basic POE program [13] to study the Leech lattice, Mathieu and Conway groups, was centered on a study of $EE_8^3$-lattices. This program can be carried out using a new viewpoint. We start with a triple of pairwise orthogonal lattices $R_1, R_2, R_3$ which are isometric to $R$, classify overlattices of $R_1 \perp R_2$ which are isometric to $Q$ and correspond to $Orbit(2)$ in the sense of (B.6), then finally glue such a $Q$ with $R_3$ to get a Leech lattice. This program offers new proofs of 5-local information about $O(\Lambda)$. 

16
Appendices

A Some general results about lattices

Lemma A.1. Let $L$ be a lattice of rank $p-1$ and $h$ an isometry of order $p$. Suppose that $M, N$ are $h$-submodules of $QL$ and that $N$ has index a power of $p$ in $M$. Then $M/N$ is a uniserial module.

Proof. The determinant of $h - 1$ is $p$. Therefore the series $(h - 1)^iM$ for $i = 0, 1, \ldots r$ forms a chain from $M$ down to $N$ such that each term has index $p$ in the previous. Since $h$ has order $p$ and $M/N$ is a finite $p$-group, there are no other $h$-submodules of $M$ which contain $N$. □

Lemma A.2. Suppose that $p$ is an odd prime and that $L$ is a rank $p-1$ integral lattice with an automorphism $h$ of order $p$. Suppose that $D(L)$ is elementary abelian $p$-group of rank $r \in \{1, 2, \ldots, p-1\}$. Let $i, j \in \{0, 1, \ldots, r\}$. Then $((h - 1)^ix, (h - 1)^y) = 0$ for all $x, y \in L$ if and only if $i + j \geq r$.

Proof. Consider the descending chain $(h - 1)^iD(L)$ for $i \geq 0$ and its ascending chain of annihilators (A.1). □

Lemma A.3. Suppose that $p$ is an odd prime and that $L$ is a rank $p-1$ integral lattice with an automorphism $h$ of order $p$. Suppose that $(L, L) \not< p\mathbb{Z}$ and that $D(L)$ is elementary abelian $p$-group of rank $r \in \{0, 1, \ldots, p-1\}$. Then the nonsingular quadratic space $L/pL^*$ is isometric to $(h - 1)L/p((h - 1)L)^* \perp U$, where $U$ has Gram matrix $\frac{1}{p} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ (mod $\mathbb{Z}$).

Proof. The commutator space $(h - 1)^{r-1}D(L)$ is 1-dimensional and consists of singular vectors. Let $W$ complement $(h - 1)^{r-1}D(L)$ in $\text{ann}((h - 1)^{r-1}D(L)) = (h - 1)D(L)$. Then $W$ is nonsingular and $\text{ann}(W)$ is a 2-dimensional space containing a singular vector, so is split. By (A.1) and determinant considerations, $((h - 1)L)^*$ contains $L^*$ with index $p$ and $p((h - 1)L)^*/pL$ is the 1-space $(h - 1)^{r-1}D(L)$. □

Corollary A.4. The discriminant group of $A_4(1)$ is isometric to the orthogonal direct sum of the discriminant group of $A_4$ and the $\mathbb{F}_5$-space with Gram matrix $\frac{1}{5} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ (mod $\mathbb{Z}$). Also, the minimum norm in $A_4^*$ is $\frac{4}{5}$. 

17
Proof. (A.3). $\square$

Lemma A.5. Let $h$ be an isometry of order 5 on $A_4$. Define $A(i) := (h - 1)^i A_4$, for $i \in \mathbb{Z}$. The lattices in the chain below have the indicated minimum norms (note that $A_4(1) \cong (h - 1)A_4$ and that if $X$ is an $h$-invariant lattice in $\mathbb{Q}A_4$, then $(h - 1)^2 X \cong \sqrt{5}X$ and $(h - 1)^4 X = 5X$).

\[\cdots A(4) A(3) A(2) A(1) A(0) A(-1) A(-2) A(-3) A(-4) \cdots\]

\[\cdots 50 \quad 20 \quad 10 \quad 4 \quad 2 \quad \frac{4}{5} \quad \frac{8}{5} \quad \frac{4}{25} \quad \frac{2}{25} \cdots\]

Proof. Note that $(h - 1)$ has determinant 5 and so $|X : (h - 1)X| = 5$. Also, $(h - 1)^i$ has determinant $5^i$ and $(h - 1)^4$ induces the 0-map on $X/5X$, so $(h - 1)^4 X = 5X$.

The adjoint of $h$ is $h^{-1}$ and so $((h - 1)x, (h - 1)y) = (x, (h^{-1} - 1)(h - 1)y) = (x, (h - 1)^2(-h^{-1}y)$. It follows that $A(2)$ satisfies $(A(2), A(2)) \leq 5\mathbb{Z}$. Therefore $\frac{1}{\sqrt{5}} A(2)$ is an even integral lattice of determinant 5. By [19, 21], this lattice is isometric to $A_4$.

Finally, recall that $A_4(1)$ is isometric to $(h - 1)A_4$ [19, 21]. Since $A(3) = (h - 1)A(2)$, the previous paragraph and the definition of $A_4(1)$ and $(h - 1)A_4$ implies that $A(3) \cong \sqrt{5}A_4(1)$.

The first statement follows. The table of minimum norms is a consequence of the known minimum norms in $A_4$ and $A_4(1)$, respectively. $\square$

Lemma A.6. Suppose that $L$ is a lattice invariant under an isometry $g$ of prime order $p$ and that the minimal polynomial of $g$ is the cyclotomic polynomial $(x^p - 1)/(x - 1)$.

(i) Let $n = \text{rank}(L)$. There exists an integer $m$ so that $n = (p - 1)m$.

(ii) If $K$ is a rank $n$ $g$-invariant lattice in $\mathbb{Q} \otimes L$, then $(g - 1)^{p-1}K = pK$ and the action of $g$ on $K/pK$ has Jordan canonical form the sum of $m$ blocks of degree $p - 1$.

Proof. By [29], we may write $L$ as a direct sum of indecomposable modules $L_i$, $i = 1, \ldots, q$, for $g$. Each $L_i$ is isomorphic to an ideal in $\mathbb{Z}[(g)]/(1 + g + \cdots + g^{p-1})$ [29] and so has rank $p - 1$ as an abelian group and on it the minimal polynomial of $g$ is $(x^p - 1)/(x - 1)$. Therefore $q = m$ and the elementary divisors for $g - 1$ on $L$ are $(1, \ldots, 1, p, \ldots, p)$, where $p$ has multiplicity $m$. It follows that $K/(g - 1)K \cong p^m$ (elementary abelian). Since $(g - 1)^{p-1} \equiv 1 + g + \cdots + g^{p-1} \equiv 0 \mod{p}$, $(g - 1)^{p-1}(K) \leq pK$. Since $|K : (g - 1)^{p-1}K| = p^{m(p-1)} = p^n = |K : pK|$, we have $(g - 1)^{p-1}(K) = pK$. Each Jordan block for the action of $p - 1$ on $K/pK$ has degree at most
Lemma A.7. (i) The minimum norm for glue vectors of $A_4$ in $A_4^*$ is $\frac{4}{5}$; the nontrivial cosets have minimum norms $\frac{6}{5}$ and $\frac{9}{5}$.

(ii) Norms of vectors in the lattice $A_4(1)^*$ have the form $\frac{k}{5}$ where $k$ is an even integer. The minimum norm for nonzero glue vectors of $A_4(1)$ in $A_4(1)^*$ are $\frac{2}{5}, \frac{4}{5}, \frac{6}{5}, \frac{8}{5}, 2$ [21].

Proof. (i) A vector in $A_4^* \setminus A_4$ has norm of the form $\frac{k}{5}$, where $k$ is an even integer. The vector $\pm \frac{1}{5}(1,1,1,1,-4)$ in the standard model of $A_4$ has norm $\frac{4}{5}$ and it is easy to prove that there is no smaller norm and that a minimum norm vector in $A_4^* \setminus A_4$ is just this vector, up to negation and coordinate permutation. For details, see [21]. For if $u \in A_4^*$ has the minimum, $u$ has form $\pm \frac{1}{5}(1,1,1,1,-4)$ in the standard model of $A_4$. The coset $2u + A_4$ contains the vector $\pm \frac{1}{5}(2,2,2,-3,-3)$, which has norm $\frac{6}{5}$ and no smaller norm is possible in this coset.

(ii) The first statement follows from the fact that $D(A_4(1))$ is an elementary abelian group of exponent 5 and that $A_4(1)$ is an even lattice.

For a singular coset, the minimum is norm 2 since $A_4$ is properly between $A_4(1)$ and $A_4(1)^*$. The vectors mentioned in (i) and in $A_4$ are in the dual of $A_4(1)^*$. Therefore, minimum norms $\frac{4}{5}, \frac{6}{5}, 2$ occur. It remains to deal with the cosets of $A_4(1)$ in $A_4(1)^*$ where the norm of a vector has the form $\frac{k}{5}$ where $k \in \pm 2 + 10\mathbb{Z}$.

In the notation of (A.5), $A_4(1)^* = A(-2)$ and we get minimum norm in $A(-2)$ is $\frac{8}{5}$. If $v$ is such a minimal vector, we have $(2v, 2v) = \frac{8}{5}$ and no vector in $2v + A_4(1)$ has lesser norm since $|\frac{8}{5}| < 2$. □

Lemma A.8. For an integer $k$ and a finite abelian group $A$, denote by $A_k$ the subgroup of all elements of $A$ whose order is a number relatively prime to $k$.

Let $L$ be an integral lattice and $M$ a sublattice of finite index $n$. The natural map $L^* \to M^* \to D(M) \to D(M)_{n'}$ induces an isometry $D(L)_{n'} \cong D(M)_{n'}$.

Proof. We have the containments $M \leq L \leq L^* \leq M^*$. Since $n = |L : M| = |M^* : L|$, the natural map $\varphi$ of $M^*$ onto $D(M)_{n'}$ remains onto when restricted to $L^*$. If $\varphi|_{L^*}$ has kernel $K$, then $K/M$ has the property that every
element of it is annihilated by a power of $n$. Since $L^*/K$ has order prime to $n$, we have a splitting $L^*/M = K/M \oplus J/M$, for a sublattice $J$, where $M \leq J \leq L^*$ and $(|J/M|, n) = 1$. Clearly, $J$ is uniquely determined and $J$ maps isomorphically onto $\mathcal{D}(M)_{n'}$. Since $K \cap J = M$, $J/M \cong \mathcal{D}(M)_{n'}$, as required. Since $M \leq J \leq M^*$, the isomorphism of groups $J/M \cong \mathcal{D}(M)_{n'}$ is an isometry. □

**Lemma A.9.** Let $L$ be an integral lattice and $M$ an SSD sublattice. The involution associated to $M$ acts trivially on $\mathcal{D}(L)$.

**Proof.** Let $P^\varepsilon$ be the orthogonal projection to the $\varepsilon$-eigenspace of $t = t_M$, $\varepsilon = \pm$. For $x \in L$, $x = P^+(x) + P^-(x)$ and $tx = P^+(x) - P^-(x)$. Therefore, $x - tx = 2P^-(x)$.

Now take $x \in L^*$. Since $L$ is integral, $P^-(x) \in M^* \leq \frac{1}{2}M$. Therefore, $x - tx = 2P^-(x) \in M \leq L$, proving the result. □

**Proposition A.10.** (i) Suppose that we have a pair of $EE_8$-lattices $M, N$. Let $t, u$ be the associated involutions. Suppose that $t', u'$ are involutions of $\langle t, u \rangle$ such that both $t'u'$ are associated to $EE_8$-sublattices $M', N'$ and that $\langle t, u \rangle = \langle t', u' \rangle$. Then there exists an isometry $g \in O(M + N)$ so that $t^g = t'$ and $u^g = u'$.

(ii) This property (i) holds whenever $t', u'$ are generators and $n > 1$ is an odd prime.

**Proof.** This follows from the main theorem of [19]. □

**Proposition A.11.** Suppose that $L = L_1 \perp L_2$ where the $L_i$ are orthogonally indecomposable lattices. Let $M$ be a nonzero RSSD sublattice of $L$ which is a direct summand of $L$ as an abelian group and let $t = t_M$ be the associated involution.

(i) If $t$ fixes some $L_i$, then $t$ fixes both $L_i$ and $M = M \cap L_1 \perp M \cap L_2$.

(ii) If $M$ is orthogonally indecomposable and $t$ fixes each $L_i$, then $t$ is 1 on one of the $L_i$ and $M$ is contained in the other.

(iii) If each $L_i$ has roots, $\text{rank}(L_1) = \text{rank}(L_2) = \text{rank}(M)$ and $M$ is rootless, then $t$ does not fix any of the $L_i$.

**Proof.** (i): This is clear since $O(L)$ permutes the set of indecomposable orthogonal summands.

(ii): This is immediate from (i).
(iii): From (ii) we get $M$ contained in $L_j$ for some $j$. Since $M$ is a direct summand of $L$, it is a direct summand of $L_j$. Since $M$ and $L_j$ have the same rank, $M = L_j$. This is a contradiction since $L_j$ has roots and $M$ does not. □

Lemma A.12. Suppose that $X, Y$ are integral lattices such that
(a) $D(X) \cong D(Y)$ has squarefree exponent; and
(b) $O(X)$ acts on $D(X)$ as the full orthogonal group of the quadratic space $D(X)$.

Then for each divisor $d > 0$ of $\det(X)$, $O(X)$ has one orbit on $O := \{ J \mid X \perp Y \leq J \leq X^* \perp Y^*, J$ is integral and $|J : X \perp Y| = d\}$, provided that this set is nonempty.

Proof. A finite quadratic space is the orthogonal direct sum of its $p$-primary parts, for all primes $p$. If $J \in O$, $J/(X \perp Y)$ corresponds to a totally singular subspace of $D(X \perp Y)$.

If $W := D(X \perp Y)$ and $W = \oplus_p W_p$ is the primary decomposition, we have $O(W) \cong \prod_p O(W_p)$. Each $W_p$ is a vector space. Now use Witt’s theorem on extensions of isometries. □

Lemma A.13. Let $V$ be a quadratic space which is finite dimensional over a field and split. Let $W$ be a totally singular subspace. Then $\text{Stab}_{O(V)}(W)$ induces $O(W/\text{Rad}(W))$ on $W/\text{Rad}(W)$.

Proof. Witt’s theorem on extensions of isometries. □

Lemma A.14. Let $M, N$ be sublattices of the lattice $Q$ where $N$ is a direct summand of $Q$, $Q = M + N$ and $(\det(N), \det(Q)) = 1$. Then the natural map of $M$ to $D(N)$ is onto.

Proof. By an elementary lemma, the natural map of $Q^*$ to $N^*$ is onto (for example, [17] or [21]. The image under this map of $Q$ has index relatively prime to $\det(N)$. Consequently, the natural map $\phi$ of $Q$ to $D(N)$ is onto. Since $\text{Ker}(\phi) = N \perp \text{ann}_Q(N)$ and $Q = M + N$, the natural map of $M$ to $D(N)$ is onto. □

Lemma A.15. Let $L$ be the $E_8$-lattice and $M$ and $A_1^2$-sublattice. Let $M = M_1 \perp M_2$ be the orthogonal decomposition of $M$ into indecomposable summands. We let $W_1 \times W_2$ be the Weyl group of $M$, where $W_i$ is the Weyl group on $M_i$. 

21
(i) If \( h \in W \) has order 5, the action of \( h \) on \( L/5L \) has Jordan canonical form the sum of a single degree 5 block and three degree 1 blocks.

(ii) If \( h \in W_1 \times W_2 \) has order 5 and \( h \notin W_1 \cup W_2 \), then the action of \( h \) on \( L/5L \) has Jordan canonical form the sum of a single degree 5 block and a single degree 3 block.

\textbf{Proof.} (i) Suppose \( h \in W_1 \). This follows since when \( v \in L \setminus M_1 \perp M_2 \), then \( \mathbb{Z}(h)v \) is a free module for \( \mathbb{Z}(h) \) and it maps in \( L/5L \) to a free submodule, which is an injective module. Since \( h \) fixes the rank 4 module \( M_2 \) pointwise and \( M_2 \) is a direct summand of \( L \), (i) follows.

(ii) The actions of \( h \) on \( L/M_2 \) and on \( M_2 \) have minimum polynomial \( x^4 + x^3 + x^2 + x + 1 \). Therefore, the action of \( h \) on \( L/5L \) has fixed point dimension at most 2. As in (i), we get a 5-dimensional free module in \( L/5L \) and (ii) follows. \( \square \)

\textbf{Lemma A.16.} Suppose that \( Z \) is a lattice which contains orthogonal sublattices \( X \) and \( Y \) such that \( X \perp Y \) has finite index in \( Z \) and both \( X \) and \( Y \) are direct summands of \( Z \).

We interpret \( O(X) \) as a subgroup of \( O(\mathbb{Q} \otimes Z) \) by extending with trivial action on \( \text{ann}(X) \). Similarly, we interpret \( O(Y) \) as a subgroup of \( O(\mathbb{Q} \otimes Z) \) by extending with trivial action on \( \text{ann}(Y) \).

Define \( S := \text{Stab}_{O(X) \times O(Y)}(Z) \) and define \( T \) to be the kernel of the action of \( \text{Stab}_{O(X)}(E) \) on \( E \) and \( U \) to be the kernel of the action of \( \text{Stab}_{O(Y)}(F) \) on \( F \). These are normal subgroups of \( S \).

The overlattice \( Z \) corresponds to the following data: subspaces \( E \) of \( D(X) \) and \( F \) of \( D(Y) \) and a linear \( S \)-isomorphism \( \psi : E \rightarrow F \) which is a similitude of the quadratic spaces.

(i) \( S/(T \times U) \) embeds as a diagonal subgroup of \( O(E) \times O(F) \), i.e., a subgroup which meets each direct factor \( O(E) \) and \( O(F) \) trivially.

(ii) The image of \( S \) in \( O(F) \) is \( A \cap B \) where \( A \) is the image of \( \text{Stab}_{O(Y)}(F) \) in \( O(F) \) and \( B \) is the subgroup obtained from \( \psi \) of the image \( C \) of \( \text{Stab}_{O(X)}(E) \) in \( O(E) \), i.e., \( B = \psi C \psi^{-1} \). (A similar description applies to the projection to \( O(\mathcal{D}(X)) \)).

(iii) We use the notations of (i, ii). Suppose that \( E = D(X) \) and \( F = D(Y) \). If \( O(X) \) induces \( O(D(X)) \) on \( D(X) \) and \( O(Y) \) induces \( O(D(Y)) \) on \( D(Y) \), then \( S/(T \times U) \cong O(D(X)) \cong O(D(Y)) \).

\textbf{Proof.} Straightforward. \( \square \)
A.1 About the centralizer of an $EE_8$ dihedral group of order 10 in $O(N(A_4^6))$

Let $\mathcal{N} := \mathcal{N}(A_4^6)$ be the Niemeier lattice with the root system $A_4^6$. Then $\mathcal{N} \supset A_4^6$. Since $A_4^6/A_4 \cong \mathbb{Z}_5$, $\mathcal{N}/A_4^6 < \mathbb{Z}_5^6$ is a self-dual linear code over $\mathbb{Z}_5$ and it is generated by

$$(1, 0, 1, -1, -1, 1), \quad (1, 1, 0, 1, -1, -1), \quad (1, -1, 1, 0, 1, -1)$$

(see [4], [8]).

Let $H$ be the automorphism group of the glue code $C = \mathcal{N}/A_4^6$. Then $H < \mathbb{Z}_2^6.Sym_6$. Now use $\{\infty, 0, 1, 2, 3, 4\}$ to label the 6 coordinates. Then $H$ has shape $2.PGL(2, 5)$ and generated by

$$(01234), \quad \varepsilon_2 \varepsilon_3 (\infty 0)(23), \quad \varepsilon_\infty (1243), \quad \varepsilon_\infty \varepsilon_0 \varepsilon_1 \varepsilon_2 \varepsilon_3 \varepsilon_4,$$

where $\varepsilon_i$ is the multiplication of $-1$ on the $i$-th coordinate and a permutation denotes a permutation matrix (cf. [4], [8] and [23]). Note that a cycle $(i_1 i_2 \ldots i_\ell)$ acts on $\{\infty, 0, 1, 2, 3, 4\}$ from the left and maps $i_1$ to $i_2$, $i_2$ to $i_3$, \ldots, $i_\ell$ to $i_1$.

Note that $H$ also acts on $\mathcal{N}$ and the isometry group $O(\mathcal{N})$ is isomorphic to the semidirect product $W \rtimes H$, where $W = Weyl(A_4^6) \cong Sym_6^6$ and $H \cong 2.PGL(2, 5)$ is the automorphism group of the glue code (cf. [4], [8]).

Let $h$ be a fixed point free order 5 element in $O(A_4)$ and define

$$M := \text{span}\{(0, 0, \alpha, \beta, -\beta, -\alpha) \mid \alpha, \beta \in A_4\} \cup \{(0, 0, \gamma, \gamma', -\gamma', -\gamma)\}$$

and

$$N := \text{span}\{(0, 0, h\alpha, h\beta, -\beta, -\alpha) \mid \alpha, \beta \in A_4\} \cup \{(0, 0, h\gamma, h\gamma', -\gamma', -\gamma)\},$$

where $\gamma = \frac{1}{5}(1, 1, 1, 1, -4)$ and $\gamma' = \frac{1}{5}(2, 2, 2, -3, -3)$. Then $M \cong N \cong EE_8$. Notice that the word $(0, 0, 1, 2, -2, -1)$ is in the glue code.

The corresponding SSD involutions are given by

$$t_M = (14)(23)$$

and

$$t_N = (1, 1, h, h, h^{-1}, h^{-1})(14)(23).$$
Thus, \(t_N t_M = (1, 1, h, h, h^{-1}, h^{-1})\) has order 5 and the dihedral group \(\langle t_M, t_N \rangle\) is isomorphic to \(Dih_{10}\) and is generated by

\[\tilde{h} := (1, 1, h, h, h^{-1}, h^{-1})\quad \text{and} \quad t_M = (14)(23).\]

We define \(Q := M + N, \) and \(R' := \ann_N(Q) \) and \(Q' := \ann_N(R')\). Since \(t\) and \(u\) act on the six coordinate spaces for the glue code as permutations of cycle shape \(1^22^2\), \(R'\) contains the sum of two \(A_4\) indecomposable orthogonal components of the root sublattice. Then \(Q' \perp R'\) contains a copy of \(Q \perp R\) and \(N\) is an overlattice of \(Q \perp R\) as described in (5.2), the case \(e = 1\). In particular \(R' \cong A_4^2\), \(\mathcal{D}(R') \cong 5^2 \cong \mathcal{D}(Q')\) and the root sublattice of \(Q'\) is isometric to \(A_4^4\).

If \(L\) is an integral lattice, we let \(\text{Weyl}(L)\) denote the group generated by reflections at the roots of \(L\).

Clearly, \(C_{\text{Weyl}(Q' \perp R')}(\tilde{h}) \cong \text{Weyl}(A_4^2) \times 5^4\). Also, \(C_{O(N)}(\tilde{h})\) is contained in the subgroup of index \(\binom{6}{2}\) of \(O(N)\) which fixes the two orthogonal direct summands of \(Q' \perp R'\) which are in \(R'\). The group \(C_{O(N)}(\tilde{h})\) therefore has the property that its image in \(O(N)/\text{Weyl}(Q' \perp R') \cong 2.PGL(2, 5)\) has order \(240/\binom{6}{2} = 16\). It follows that \(C_{O(N)}(\tilde{h})^{(\infty)}\), the terminal member of the derived series of \(C_{O(N)}(\tilde{h})\), is just \(\text{Weyl}(R')' \cong Alt_5 \times Alt_5\). This is contained in \(C_{O(N)}(D)\) and in fact equals \(C_{O(N)}(D)^{(\infty)}\).

We have proved:

**Proposition A.17.** We let \(N := N(A_6^4)\) and let \(D\) be a dihedral group of order 10 generated by a pair of \(E E_8\)-involutions in \(O(N)\) which give permutations of cycle shape \(1^22^2\) on the six coordinate space for the glue code (equivalently, on the six indecomposable orthogonal components of the root sublattice). Then \(C_{O(N)}(D)^{(\infty)} = C_{O(N)}(O_{2^2}D)^{(\infty)} \cong Alt_5 \times Alt_5\).

### B The finite orthogonal groups

We give formulas for the orders of the orthogonal groups over finite fields.

**Theorem B.1.** We let \(q\) be an odd prime power, \(\varepsilon = \pm\).

(i) \(|SO^\varepsilon(2n, q)| = q^{n(n-1)}(q^n - \varepsilon) \prod_{i=1}^{n-1}(q^{2i} - 1)\)

(ii) \(|SO(2n + 1, q)| = q^{n^2} \prod_{i=1}^{n}(q^{2i} - 1)\)

(ii) The orders of the corresponding orthogonal groups are twice the above numbers.
Proof. (i) This is taken from [1], pages 126-147. (ii) In characteristic not 2, an orthogonal group contains the special orthogonal group with index 2. □

Corollary B.2. The stabilizer in $O^+(2n,q)$ of a maximal totally singular subspace has the form $q^2:GL(n,q)$. The number of such subspaces is $2\prod_{i=1}^{n-1}(q^i + 1)$.

Proof. The form of the stabilizer follows by considering a direct sum decomposition of the space by a pair of totally singular subspaces. The second statement follows from Witt's transitivity result and the formulas of (B.1). □

Corollary B.3. Suppose that $q$ is odd and that $\varepsilon = +$. The orthogonal group has structure $(SL(2,q) \circ SL(2,q))\langle (2 \times 2) \rangle$. The normalizer of either $SL(2,q)$ central factor is the special orthogonal group.

Proof. By order considerations (B.1), it suffices to show that the orthogonal group contains such a subgroup.

For $i = 1, 2$, let $U_i$ be $\mathbb{F}_q^2$ with a nonsingular alternating form. The group of similitudes is $GL(U_i)$. The wreath product $(GL(U_1) \times GL(U_2))(t)$, where $t$ is the usual involution which switches arguments of tensors, acts on $V := U_1 \otimes U_2$, as similitudes of the nonsingular quadratic form obtained by tensor product from the forms on the $U_i$. Call this homomorphism $\varphi$. The kernel $K$ of $\varphi$ is a central subgroup isomorphic to $\mathbb{Z}_{q-1}$. The subgroup $H$ of $GL(U_1) \times GL(U_2)$ preserving the form is normal and gives a quotient isomorphic to $\mathbb{Z}_{q-1}$. Obviously, $K \leq H$.

Let $D_i$ be the diagonal subgroup of $GL(U_i)$, $i = 1, 2$. Write $h_i(a,b)$ for the diagonal matrix $\left( \begin{array}{cc} a & 0 \\ 0 & b \end{array} \right)$ of $D_i$.

Define $D = D_1 \times D_2$. Then $D \cap H = \{(h_1(a,b),h_2(c,d)) \mid abcd = 1\}$ so $H$ is just the kernel of the map $\psi : GL(U_1) \times GL(U_2) \to \mathbb{F}_q^\times$ which takes $(g_1,g_2)$ to $\text{det}(g_1)\text{det}(g_2)$.

The intersection $Z$ of $Z(GL(U_1)) \times Z(GL(U_2))$ with $H$ is $Z = \{h_1(a,a)h_2(b,b) \mid (ab)^2 = 1, \text{i.e.}, ab = \pm 1\}$ and $K = \{h_1(a,a)h_2(b,b) \mid ab = 1\}$.

Fix a nonsquare $n \in \mathbb{F}_q^\times$. Observe that, given $a, b$, there is $e$ so that $abe^2 \in \{1, n\}$. It follows that if $(h_1(a,b),h_2(c,d)) \in D \cap H$, it is congruent modulo $K$ to $(h_1(1,1),h_2(1,1))$ or $(h_1(n,1),h_2(n^{-1},1))$. Therefore, $\text{Im}(\varphi)$ contains $\varphi(SL(U_1) \times SL(U_2))$ with index 2. By order considerations, $\text{Im}(\varphi) = SO(V)$.

Finally, note that the action of $t$ has determinant $-1$ and that it interchanges the groups $\varphi(SL(U_1))$ and $\varphi(SL(U_2))$ under conjugation. □
Corollary B.4. Let $q$ be an odd prime power. A subgroup $S$ of index 2 in $O^+(4,q)$ contains $Z := Z(O^+(4,q)) = \{\pm 1\}$ and $S/Z$ is isomorphic to either $PSL(2,q) \wr 2$ or the even subgroup of $PGL(2,q) \times PGL(2,q)$, i.e., the subgroup of index 2 which intersects each direct factor in its unique subgroup of index 2.

Proof. The containment $Z \leq S$ follows since $Z$ is in the commutator subgroup of $O^+(4,q)$.

We use the fact that $PSO^+(4,q)$ embeds as a subgroup $T$ of index 2 in $U := PGL(2,q) \wr 2$. We have $U'' \cong PSL(2,q) \times PSL(2,q)$ and $U/U'' \cong \text{Dih}_8$, in which $T/U''$ is a four-group. In $\text{Dih}_8$, there are just two conjugacy classes of four-groups. Our group $T$ is not the subgroup $PGL(2,q) \times PGL(2,q)$. Furthermore, the two subgroups of order 2 in $T/U''$ which are not central in $U/U''$ are conjugate. Therefore, the isomorphism types for $S$ are limited to two possibilities. Now use (B.3). □

Lemma B.5. Let $q$ be an odd prime power. Then $O(3,q) \cong 2 \times PGL(2,q)$.

Proof. Since the dimension is odd, $O(3,q) = (-1) \times SO(3,q)$. It suffices to show that $SO(3,q) \cong PGL(2,q)$.

We take the natural actions of $GL(2,q)$ on the space of $2 \times 2$ matrices over $\mathbb{F}_q$ and observe that it leaves invariant the trace 0 matrices for which the form $A, B \mapsto \text{Tr}(A,B)$ is nonsingular and symmetric. The kernel of this action is the group of scalar matrices. Consequently, $PGL(2,q)$ embeds in $SO(3,q)$. The order formula (B.1) shows that this embedding is onto. □

Lemma B.6. Let $q$ be an odd prime power. There are five orbits of $O^+(4,q)$ on 2-spaces, and these orbits are distinguished by these properties of their members (in the notation $\text{Orbit}(a, \cdots)$, the parameter $a$ means the dimension of the radical of the 2-space):

- $\text{Orbit}(2)$: totally singular;  
- $\text{Orbit}(1,s), \text{Orbit}(1,n)$: nullity 1; two kinds, according to whether norms are squares or nonsquares  
- $\text{Orbit}(0,1)$: nonsingular, maximal Witt index;  
- $\text{Orbit}(0,0)$: nonsingular, nonmaximal Witt index.

Proof. This is a consequence of Witt’s theorem and the theory of nonsingular quadratic spaces. □
Lemma B.7. Let $p$ be an odd prime and let $\langle g \rangle$ be a group of order $p$. Suppose that for $i = 1, 2$, $U_i$ is a 2-dimensional $\mathbb{F}_p \langle g \rangle$-module on which $g$ acts with a single degree 2 indecomposable Jordan block. The action of $g$ on $U_1 \otimes U_2$ has Jordan canonical form the sum of a degree 1 and degree 3 indecomposable Jordan block.

Proof. For $U_i$, choose a basis $e_i, f_i$ so that $g$ fixes $f_i$ and $ge_i = e_i + f_i$. Consider the $\mathbb{F}_p \langle g \rangle$-submodules $\text{span}\{e_1 \otimes e_2, f_1 \otimes e_2 + e_1 \otimes f_2, f_1 \otimes f_2\}$ and $\text{span}\{f_1 \otimes e_2 - e_1 \otimes f_2\}$. □

Remark B.8. Tensor products of indecomposables for cyclic $p$-groups in characteristic $p$ were studied in [33, 25].

Lemma B.9. In $O^+(4, q)$, for $q$ a power of the odd prime $p$, the elements of order $p$ in each $SL(2, q)$-component of $O^+(4, q)$ have Jordan canonical form a direct sum of two indecomposable degree 2 blocks. The other elements of order $p$ in $O^+(4, q)$ have Jordan canonical form a sum of indecomposable blocks of degrees 1 and 3.

Proof. (B.7). □

Lemma B.10. We use the hypotheses and notations of (B.6). Suppose that $v_1, v_2, v_3, v_4$ is a basis of the nonsingular quadratic space $V := \mathbb{F}_q^4$ of maximal Witt index which has Gram matrix

$$
\begin{pmatrix}
0 & 0 & 0 & 1 \\
0 & a & 0 & 0 \\
0 & 0 & b & 0 \\
1 & 0 & 0 & 0
\end{pmatrix}, a \neq 0, b \neq 0.
$$

Let $W := \text{span}\{v_1, v_2\} \in \text{Orbit}(1, s) \cup \text{Orbit}(1, n)$. The stabilizer in $O^+(4, q)$ of $W$ has the form $S = UH$, where $U$ is a normal subgroup of order $q^2$ which acts trivially on the factors of the chain $0 < W < \text{ann}(v_1) < V$ and where $H$ is diagonal with respect to the above basis, acting as matrices of the form

$$
\begin{pmatrix}
c & 0 & 0 & 0 \\
0 & d & 0 & 0 \\
0 & 0 & e & 0 \\
0 & 0 & 0 & c^{-1}
\end{pmatrix}, c \in \mathbb{F}_q^\times, d, e \in \{\pm 1\}.
$$

In particular, $H \cong \mathbb{Z}_{q-1} \times 2 \times 2$. The order of $S$ is $2^2(q - 1)q^2$. The kernel of the action of $S$ on $W$ is a subgroup of order $q$. 

27
Proof. It is clear from the proof of (B.7) and (B.9) that $S$ contains a maximal unipotent group, $U$, and that $U$ acts trivially on the factors of such a chain. Furthermore, any orthogonal transformation which acts trivially on the factors of such a chain is unipotent so is in $U$.

We have $S \leq Y$, the stabilizer of $F_qv_1$. The group $Y$ splits over $U$ by coprimeness. A complement $H$ to $U$ in $Y$ has a direct product decomposition $H = H_1 \times H_2$ where $H_1$ acts trivially on $W' := \text{span}\{v_2, v_3\}$ and faithfully on $W'' := \text{span}\{v_1, v_4\}$ and such that $H_2$ acts trivially on $W''$ and faithfully on $W'$. We have $H_1 \cong \mathbb{F}_q^\times$ and $H_2 \cong O^+(2, q) \cong \mathbb{F}_q^\times : 2$, a dihedral group.

Thus $S$ contains $UH_1$ and $S \cap H_2$ is just the subgroup fixing a nonsingular 1-space in the natural 2-dimensional orthogonal representation of this group. Therefore, $S \cap H_2 \cong 2 \times 2$. Our matrix representation of $S$ follows since $H_2$ fixes a complement to $W'$ in $V$ and we may as well assume that it is $W''$ by replacing $H$ with a $U$-conjugate. The final two statements are easy. □

C Finite subgroups of $E_8(\mathbb{C})$

Lemma C.1. A sublattice in $E_8$ of index 5 contains roots.

Proof. Such a sublattice corresponds to a cyclic group of order 5 in $E_8(\mathbb{C})$. The list of elements of order 5 shows that every one fixes root spaces. See [3, 11]. □

Lemma C.2. Let $h \in O(E_8)$ be an isometry of order 5 without eigenvalue 1. Then $(h - 1)E_8$ is rootless.

Proof. Let $E_8$ contain a sublattice $M_1 \perp M_2$, where $M_1 \cong M_2 \cong A_4$. Then we may take $h = h_1h_2$, where $h_i \in \text{Weyl}(M_i)$ and $|h_i| = 5$. Then $E_8$ contains $M_1 \perp M_2$ with index 5 and is represented by a nontrivial gluing. The action of $(h - 1)$ carries $E_8$ to a sublattice of $M_1 \perp M_2$ which intersects $M_i$ in the rootless sublattice $(h_i - 1)M_i$, for $i = 1, 2$ (A.5). □

Lemma C.3. We use the notation of [3] for conjugacy classes in $E_8(\mathbb{C})$.

(i) $E_8(\mathbb{C})$ has one conjugacy class of subgroups $F$ such that $F \cong 5^2$ and $\dim(C(F)) = 8$, i.e., $C(F)^0$ is a torus. In fact, $C(F) \cong \mathbb{T} \cdot 5$. If $g \in C(F) \setminus C(F)^0$, the action of $g$ on the root lattice modulo 5 has Jordan canonical form the sum of two degree 4 Jordan blocks.

(ii) There is one $E_8(\mathbb{C})$-orbit on ordered pairs $(x, y)$ of class 5$C$-elements which generate an elementary abelian group of order 25 whose centralizer is 8-dimensional.

28
(iii) In the lattice $Y := E_8$, there is one equivalence class of rootless sublattices $X$ so that $Y/X \cong 5^2$. We have $\text{Stab}_{O(Y)}(X) \cong 5:GL(2,5) \cong (5 \times SL(2,5)):4$, a group with trivial center, and the normal subgroup of order 5 is the kernel of the action on $Y/X$.

(iv) An $X$ as in (iii) contains a sublattice isometric to $A_4(1) \perp A_4(1)$. Furthermore, an isometry $g$ of order 5 in $O(X) \cap O(Y)$ acts nontrivially on $D(X)$, with Jordan canonical form a sum of two degree 2 Jordan blocks. The Smith invariants of $g - 1$ on $X$ are $(1,1,1,1,1,1,5,5)$.

**Proof.** The arguments use techniques from the theory of finite subgroups of Lie groups. See [15, 16] for references and examples. Let $Tr$ be the trace function for a linear transformation on the adjoint module for the Lie group of type $E_8$.

(i) and (ii) A survey of the elements of finite order (e.g., [15, 16]) shows that for a cyclic group $H$ of order 5 in $E_8(\mathbb{C})$, $\sum_{g \in H} Tr(g) \geq 240$, with equality occurring only at the case where nonidentity elements of $H$ are in class $5C$ (recall that this sum is the $|H|$ times the dimension of the fixed point subalgebra). Consequently, if $E$ is any elementary abelian group of order 25, $\sum_{g \in E} Tr(g) \geq 200$, with equality holding only when all nonidentity elements of $E$ are in the class $5C$.

(iii) This follows from the proof of (ii), which shows that if $x$ has type $5C$, it corresponds to a sublattice $Z$ of $Y$ of type $A_4^2$. A rootless index 5 sublattice of this may be obtained as follows. Let $Z_1$ and $Z_2$ be the pair of $A_4$ direct summands. For $i = 1, 2$, let $g_i$ be an element of order 5 from the Weyl group of $Z_i$. Any sublattice between $(g_1-1)Z_1 \perp (g_2-1)Z_2$ and $Z_1 \perp Z_2$ is stable under the action of $g_1 g_2$. In particular, a sublattice $J$ of index 5 in $Z_1 \perp Z_2$ which meets $Z_i$ in $(g_i-1)Z_i$, for $i = 1, 2$, is rootless and is left invariant by $g_1 g_2$. There are four such lattices $J$, and this set of four lattices forms an orbit under $W(Z_1) \times W(Z_2)$, where $W(Z_i) \cong Sym_5$ denotes the Weyl group. Since $W(Z_1) \times W(Z_2) \leq O(Y)$, it follows that $g_1 g_2$ is conjugate to all of its nontrivial powers in $O(J) \cap O(Y)$.

Such a sublattice $J$ corresponds to an elementary abelian group of order 25 which fixes no root spaces, hence whose connected centralizer is a maximal torus. By (ii), its normalizer in $E_8(\mathbb{C})$ induces on $Y/X$ the group $GL(2,5)$ and so the kernel of the action has shape $\mathbb{T}.5$, whose component group is cyclic of order 5. Now apply (ii) to $J$ and the action of $g_1 g_2$ on $J$.

(iv) We use the notation of (iii). Let $P_i$ be the orthogonal projection to $\mathbb{Q}Z_i$, $i = 1, 2$. 

29
Since \( g \) has minimum polynomial \((x^5 - 1)/(x - 1) \in \mathbb{Q}[x] \) on \( Z_i \), it has minimum polynomial \((x - 1)^4 \in \mathbb{F}_5[x] \) on \( A/5A \), where \( A \) is any nonzero \( g_i \)-submodule of \( Z_i \) (C.1)(iii).

Now set \( g := g_1g_2 \). Then the minimum polynomial of \( g \) on any nonzero invariant lattice \( B \) in \( \mathbb{Q}R \) is \((x^5 - 1)/(x - 1) \in \mathbb{Q}[x] \). By reasoning as above, we get that the minimum polynomial of \( g \) on \( B/5B \) is \((x - 1)^4 \in \mathbb{F}_5[x] \).

The central involution of \( \text{Stab}_0(Y)(X) \sim 5 \times GL(2,5) \) acts as \(-1\) so acts on \( \mathcal{D}(B) \) with irreducible constituents of even degree. Since, by minimal polynomial considerations, \( g \) acts nontrivially on \( \mathcal{D}(B) \), it follows that the commutator space of \( g \) on \( \mathcal{D}(B) \) has dimension 2 and so \( g \) acts with Jordan canonical form the sum of two indecomposable degree 2 blocks.

By (A.6), we see that \((g - 1)^4X = 5X\), which implies that \( 5^2 \) does not divide any Smith invariants. Since \( \det(g - 1) = 25 \), the result follows. □

**Lemma C.4.** If \( g \) is an element of \( E_8(\mathbb{C}) \) of finite order and \( \dim(C(g)) = 8 \), then \(|g| \geq 30\).

**Proof.** See [3, 11, 15, 16] for background on finite subgroups of Lie groups. An element of finite order is conjugate to one which corresponds to a labeling of the extended \( E_8 \)-diagram [22]. The condition \( \dim(C(g)) = 8 \) implies that each label is positive, whence \(|g| \geq 30\). □

**Lemma C.5.** Let \( U_1 \perp U_2 \) be an orthogonal direct sum of \( E_8 \)-lattices. Suppose that \( Q \leq U_1 \perp U_2 \) and \( Q \) is a rootless lattice of index \( 5^2 \). Then \( Q \leq U_1 \perp U_2 \) corresponds to an elementary abelian group \( E \cong 5^2 \) in the Lie group \( G = E_8(\mathbb{C}) \times E_8(\mathbb{C}) \) whose connected centralizer in \( G \) is a torus. Such a group \( E \) is unique in \( G \) up to conjugacy.

**Proof.** Let \( G_i, i = 1, 2 \) be the two direct factors of \( G \) and let \( E_i \) be the projection of \( E \) to \( G_i \). Then the connected centralizer of \( E_i \) in \( G_i \) is a torus, \( i = 1, 2 \). By (3.2), \( E_i \) is unique up to conjugacy in \( G_i \) and its normalizer \( N_i \) induces \( \text{Aut}(E_i) \cong GL(2,5) \) on \( E_i \), for \( i = 1, 2 \). The action of \( N_1 \times N_2 \) on \( E_1 \times E_2 \) has one orbit on its subgroups of order \( 5^2 \) which meet each of \( E_1 \) and \( E_2 \) trivially. The lemma follows. □

**D Finite subgroups of \( O(n, \mathbb{F}) \) which centralize root groups**

Let \( \mathbb{F} \) be an algebraically closed field.
Lemma D.1. Let $A$ be an odd order finite abelian subgroup of $GL(V)$ where $V$ is a $2m$ dimensional vector space over $\mathbb{F}$, an algebraically closed field of characteristic not dividing $|A|$. We suppose that $A$ leaves invariant a split, nondegenerate quadratic form. Denote by $O(V)$ the isometry group of this form.

(i) If there exists a nontrivial linear character of $A$ which occurs with multiplicity at least $2$, then $C(A)$ contains a root group.

(ii) If the trivial character occurs with multiplicity at least $4$, then $C(A)$ contains a root group.

Proof. (i) For a linear character $\mu$ of $A$, let $V(\mu)$ be the eigenspace for $\mu$ in $V$.

Let $\lambda \neq 1$ be a character which occurs with multiplicity $k \geq 2$. Then $V(\lambda)$ and $V(\lambda^{-1})$ each have dimension $k$ and intersect trivially. Furthermore, since $|A|$ is odd, the spaces $V(\lambda)$ and $V(\lambda^{-1})$ are each totally singular and the associated bilinear form pairs them nonsingularly.

Let $W$ be an $m$-dimensional totally singular subspace which is invariant under $A$ and which contains $V(\lambda)$. Let $W'$ be an $m$-dimensional totally singular subspace which is invariant under $A$ and which contains $V(\lambda^{-1})$. We may arrange for $W \cap W' = 0$. The subgroup $H$ of $O(V)$ which leaves both $W$ and $W'$ invariant acts faithfully on each of $W$ and $W'$ as $GL(W), GL(W')$, respectively.

Since $k \geq 2$, $A$ centralizes a natural $GL(k, \mathbb{F})$-subgroup of $H$ and so centralizes a root group of $O(V)$.

(ii) This is immediate since a natural $4$-dimensional orthogonal group contained in $O(V)$ contains a root group. □

Corollary D.2. Let $p$ be an odd prime and let $A$ be an elementary abelian group of order $p^2$ in $O(2m, \mathbb{F})$, where $\mathbb{F}$ is an algebraically closed field of characteristic not dividing $|A|$. If $p^2 < 4m - 3$, then $C(A)$ contains a root group.

Proof. By (D.1), we may assume that the fixed point space has dimension at most $2$. We may partition the nontrivial linear characters into inverse pairs. If one such pair occurs with multiplicity at least $2$, we are done by (D.1). Denying this, we get $\frac{p^2 - 1}{2} \geq 2m - 2$, or $p^2 \geq 1 + 4m - 4 = 4m - 3$. □

Corollary D.3. Let $A$ be an abelian group of order $25$ in $O(16, F)$, where $F$ is an algebraically closed field of characteristic not $5$. Then $A$ centralizes a root group.
Proof. We note that $25 < 32 - 3$ then use (D.2). □

References

[1] E. Artin, Geometric Algebra, Wiley Interscience, 1957 (fourth printing 1965).

[2] R. Carter, Simple groups of Lie type, John Wiley & Sons, 1989.

[3] A. M. Cohen and R. L. Griess, Jr., On finite simple subgroups of the complex Lie group of type $E_8$, Proc. Symp. Pure Math., 47, 1987, 367-405.

[4] J. H. Conway and N. J. A. Sloane, Sphere packings, lattices and groups, Third edition. With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 290. Springer-Verlag, New York, 1999.

[5] P. J. Costello and J. S. Hsia, Even unimodular 12-dimensional quadratic forms over $Q(\sqrt{5})$, Adv. in Math. 64 (1987), no. 3, 241–278.

[6] J. Dieudonne, La géométrie des groupes classiques, Ergebniss der Mathematik und ihrer Grenzgebiete, Neue Folge, Heft 5, Springer, Berlin, 1955.

[7] C. Dong, H. Li, G. Mason and S. P. Norton, Associative subalgebras of Griess algebra and related topics, Proc. of the Conference on the Monster and Lie algebra at the Ohio State University, May 1996, ed. by J. Ferrar and K. Harada, Walter de Gruyter, Berlin – New York, 1998.

[8] V. A. Erokhin, Groups of automorphisms of 24-dimensional even unimodular lattices, J. Math. Sci., Vol. 6, No.3, 1876–1879, 1984.

[9] I. B. Frenkel, J. Lepowsky and A. Meurman, Vertex Operator Algebras and the Monster, Academic Press, New York, 1988.
[10] G. Glauberman and S. P. Norton, On McKay’s connection between the affine $E_8$ diagram and the Monster, Proceedings on Moonshine and related topics (Montreal, QC, 1999), 37–42, CRM Proc. Lecture Notes, 30, Amer. Math. Soc., Providence, RI, 2001.

[11] R. L. Griess, Jr., Elementary Abelian $p$-subgroups of algebraic groups, Geom. Dedicata 39, 1991, 253-305.

[12] R. L. Griess, Jr., A vertex operator algebra related to $E_8$ with automorphism group $O^+(10,2)$. The Monster and Lie algebras (Columbus, OH, 1996), 43–58, Ohio State Univ. Math. Res. Inst. Publ., 7, de Gruyter, Berlin, 1998.

[13] R. L. Griess, Jr., Pieces of Eight, Advances in Mathematics, 148, 75-104 (1999).

[14] R. L. Griess, Jr., Twelve Sporadic Groups, Springer Monographs in Mathematics, 1998, Springer-Verlag.

[15] R. L. Griess, Jr., and A. J. E. Ryba, Finite simple groups which projectively embed in an exceptional Lie group are classified!, Bulletin Amer. Math. Soc. 36 (1), 1999, 75-93.

[16] R. L. Griess, Jr., and A. J. E. Ryba, Quasisimple finite subgroups of exceptional algebraic groups, with Alex Ryba, Journal of Group Theory, 2002, 1-39.

[17] R. L. Griess, Jr., Positive definite lattices of rank at most 8, Journal of Number Theory, 103 (2003), 77-84.

[18] R. L. Griess, Jr., Pieces of $2^d$: existence and uniqueness for Barnes-Wall and Ypsilanti lattices. Advances in Mathematics, 196 (2005) 147-192. math.GR/0403480; Corrections and additions to “Pieces of $2^d$: existence and uniqueness for Barnes-Wall and Ypsilanti lattices.” [Adv. Math. 196 (2005) 147-192], Advances in Mathematics 211 (2007) 819-824. See item [Gr05.1].

[19] R. L. Griess, Jr. and C. H. Lam, Dihedral groups and $EE_8$ lattices, preprint 87 pages; to appear in Pure and Applied Math Quarterly (special issue for Jacques Tits).
[20] R. L. Griess, Jr. and C. H. Lam, A moonshine path from $E_8$ to the monster, preprint.

[21] R. L. Griess, Jr., “An introduction to groups and lattices: finite groups and positive definite rational lattices”; to be published simultaneously by Higher Education Press (in China) and by the International Press for the rest of the world.

[22] V. G. Kac, Automorphisms of finite order of semisimple Lie algebras, Funkcional. Anal. i Prilozen, 3 (1969), 94-96 (announcement); for proofs, see Section 5, Chapter 10 of the book Helgason, Sigurdur, Differential geometry and symmetric spaces. Pure and Applied Mathematics, Vol. XII. Academic Press, New York-London 1962 xiv+486.

[23] J. S. Leon, V. Pless, N. J. A. Sloane, Self-dual codes over GF(5), J. Combin. Theory Ser. A 32 (1982), no. 2, 178–194.

[24] C. H. Lam and H. Shimakura, Ising vectors in the vertex operator algebra $V_\Lambda^+$ associated with the Leech lattice $\Lambda$, Int. Math. Res. Not. (2007), Vol. 2007: article ID rnm132, 21 pages.

[25] J. H. Lindsey, Groups with a t. i. cyclic Sylow subgroup, J. Algebra 30 (1974), 181–235.

[26] H. Maass, Modulformen und quadratische Formenber dem quadratischen Zahlkrper $R(\sqrt{5})$ (German), Math. Ann. 118, (1941). 65–84.

[27] J. McKay, Graphs, singularities, and finite groups, Proc. Symp. Pure Mathe., Vol.37, Amer. Math. Soc., Providence, RI, 1980, 183-186.

[28] W. Pleskin and G. Nebe, Finite Rational Matrix Groups, American Mathematical Society, vol. 116, number 556, 1995.

[29] D. S. Rim, Modules over finite groups. Ann. of Math. (2) 69 1959 700–712.
[30] R. Scharlau and B. Hemkemeier, Mathematics of Computation, Volume 67, Number 222, April 1998, Pages 737749 S 0025-5718(98)00938-7 (an identical preprint appeared in December 1994 in the Bielefeld preprint series of SFB 343).

[31] R. Scharlau and R. Schulze-Pillot, Extremal Lattices, (English summary) Algorithmic algebra and number theory (Heidelberg, 1997), 139–170, Springer, Berlin, 1999.

[32] H. Shimakura, The automorphism group of the vertex operator algebra $V_L^+$ for an even lattice $L$ without roots, J. Algebra 280 (2004): 29V57.

[33] B. Srinivasan, The modular representation ring of a cyclic $p$-group. Proc. London Math. Soc. (3) 14 1964 677–688.

[34] B. Hemkemeier, “tn” (two neighbors), software available at http://twoneighbours.origo.ethz.ch/wiki/twoneighbours

[35] B. B. Venkov, On the classification of integral even unimodular 24-dimensional quadratic forms, Trudy Matematicheskogo Institut a imeni V. A Steklova 148 (1978) 65-76, 273; also Chapter 18 of [4].

[36] E. Witt, Theorie der quadratischen Formen in beliebigen K¨orpern JRAM, 176 (1937) 31-44.