Advances in Mathematics **148**, 75–104 (1999)
Article ID aima.1999.1846, available online at http://www.idealibrary.com on IDEAL®

Pieces of Eight: Semiselfdual Lattices and a New Foundation for the Theory of Conway and Mathieu Groups

Robert L. Griess, Jr.[1]

Department of Mathematics, University of Michigan, Ann Arbor, Michigan 48109
E-mail: rlg@math.lsa.umich.edu

Received December 13, 1996; accepted March 8, 1999

Contents.

1. INTRODUCTION

We give a new and easy construction of the largest groups of Mathieu and Conway, as the full automorphism groups of the Golay code and Leech lattice, respectively. In addition we get a new uniqueness proof for the Leech lattice and the Golay code. The main technique is intensive use of semiselfdual sublattices: instead of rank 1 lattices as the basis for coordinate concepts, we use scaled versions of L_{E_8}, the E_8 root lattice; the semiselfdual lattices we use most of the time are isometric to $\sqrt{2}\, L_{E_8}$. While it has been recognized for decades that one can use copies of L_{E_8} to describe the Leech lattice (see [23, 33, 34]), our uses of it to *create the theory* of Conway and Mathieu groups are new. Using these "smarter coordinates," properties of their automorphism groups and appropriate uniqueness theorems, we get a compact foundation of this theory (see Section 3, esp. (3.7) and (3.19)).

[1] We thank Dan Frohardt, George Glauberman, and Jacques Tits for useful comments. For financial support during work on this article, we acknowledge NSF Grant DMS 9623038 and University of Michigan Faculty Recognition Grant (1993-96).

0001-8708/99 $30.00

The logical order of our steps is new. We first take a Leech lattice (*any* rank 24 even integral unimodular lattice without vectors of squared length 2) then deduce its uniqueness and properties of its automorphism group, the large Conway group. We use our uniqueness theorems to get transitivity of $\Lambda_2, \Lambda_3, \Lambda_4$ and other configurations of vectors and sublattices *without listing members of these sets or even knowing* $|\mathrm{Aut}(\Lambda)|$, in contrast with earlier treatments (some of our transitivity results may not be in the literature). Next, we deduce existence and uniqueness of the Golay code, then existence and order of the Mathieu group, M_{24}. Simple observations of the Golay code then give immediate results about permutation representations of M_{24}. Only minimal examination of particular codes is ever done, in contrast with [5, 8, 1, 16]. Our logical sequence of *first* obtaining the Conway group, *then* the Mathieu groups, is in defiance of the classical theories for these groups. Our characterization. Of the Leech lattice is a logical improvement over that of [6], which *depends on* the characterization of the Golay code because we *deduce* its characterization.

The construction of the Leech lattice we give (3.3)(i) is not really new (see [21, 33, 34]), but our treatment of uniqueness and analysis of the automorphism group is different, notably in avoidance of Conway's characterization [6] and avoidance of displaying explicit "extra automorphisms" with respect to a frame basis [5, 7, 16]. Furthermore, our foundation of the theory of Conway and Mathieu groups is "elementary," if one takes the structure of the E_8 lattice, its automorphism group, and basic lattice management (2.1) for granted. We emphasize that the present article contains a complete proof of this foundation (modulo standard background material about lattices and finite groups in Section 2 and the Appendixes), a fact which should be taken into account in making comparisons.

Our break with the past is not complete since we still rely on the theta series of an E_8 lattice and a Leech lattice and in (3.4), (3.7), (3.17), (3.18), we have to use a few elementary properties of a code associated to a frame (A.4), (A.8) (this code turns out to be the Golay code, but we do not need to quote its characterization). Possibly, reliance on the theta series can be lessened; for instance, one would like a direct, elementary proof of the fact that in a Leech lattice, Λ, the orthogonal of a sublattice isometric to $\sqrt{2}\, L_{E_8}$ contains a copy of $\sqrt{2}\, L_{E_8}$ (and even $\sqrt{2}\, L_{E_8} \perp \sqrt{2}\, L_{E_8}$). Even the weaker statement that a vector x in the Leech lattice contains a copy of $\sqrt{2}\, L_{E_8}$ in the sublattice $\{ y \in \Lambda \mid (x, y) \in 2\mathbb{Z} \}$ (the "annihilator of $x \bmod 2$") would be useful (and seems hard to prove without using theta series).

We introduce *semiselfdual involutions* in (2.5), a concept with potential for wider applications. In case one wishes to follow the spirit of an earlier construction, one can choose an extra automorphism from our family of semiselfdual involutions (2.5), (3.6), (5.3).

2. BASIC NOTATIONS AND DEFINITIONS

Throughout this article, $(\cdot, \cdot)$ denotes a positive definite bilinear form on a lattice of finite rank or a finite dimensional rational vector space. If L is a lattice, we write $\mathbb{Q}L$ for the ambient rational vector space, which may be identified with $\mathbb{Q} \otimes L$. Groups act on the right. The notation $A.B$ stands for a group extension, with extension kernel A and quotient B, with $A:B$ and $A \cdot B$ denoting split and nonsplit extensions, respectively. If m is an integer, m^n denotes the direct product of n cyclic groups of order n and $m^{n+\cdots+q+r}$ denotes a compound extension $(m^{n+\cdots+q})\, m^r$.

(2.1) DEFINITION. We recall a few things about lattices and free abelian groups. The *invariants* or *invariant factors* of an integral lattice, L, are the invariant factors of the integral matrix $((x_i, x_j))$, where $x_1, ..., x_n$ is a basis. For example, L_{E_8} has invariants (1^8) and $\sqrt{2}\, L_{E_8}$ has invariants (2^8). All our lattices are positive definite, so invariants are nonzero; N.B., *for brevity, we may list only the invariants greater than* 1 (so, e.g. (2^2) denotes the invariants of the D_8-lattice, which is more compact than the complete list $(2^2 1^6)$). The *determinant* of L (not necessarily integral) is the determinant of the matrix $((x_i, x_j))$. If M is a sublattice of finite index, $\det(M) = \det(L)\, |L:M|^2$. If L is a lattice in the rational vector space V (L is not necessarily integral and does not necessarily span V), the *dual of* L is $L^* := \{x \in \mathbb{Q}L \mid (L, x) \leqslant \mathbb{Z}\}$. Then L^* is a lattice, called the *dual lattice*; we have $(\det L^*)^{-1} = \det L$, so if L is integral, L^* need not be. A *root* is a lattice vector of squared length 2. The *radical mod n* of L is the sublattice $\{x \in L \mid (x, L) \leqslant n\mathbb{Z}\} = nL^* \cap L$.

(2.2) DEFINITION. We use the abbreviations EL, EUL for an even lattice, respectively, even unimodular lattice. An integral lattice L is called a *scaled unimodular lattice* (SUL) if and only if there is a unimodular lattice U and a scalar s so that $L \cong sU$. In other words, there is an isomorphism of abelian groups θ: $L \cong U$ so that for all $x, y \in L$, $(x, y)_L = s^2 (x^\theta, y^\theta)_U$. We call s the *scale* or *scale factor* of L; clearly, s is the square root of an integer, and we take it to be positive.

(2.3) LEMMA. (i) *If L is integral and unimodular and M is a direct summand (as abelian groups), the natural map $L \to \mathrm{Hom}(M, \mathbb{Z})$ is onto; the nontrivial invariants of M and $M^\perp \cap L$ are the same.*

(ii) *If M is a sublattice of the integral lattice L, and M is SUL with scale factor s, then $\{x \in L \mid (x, M) \leqslant s^2\mathbb{Z}\} = [M^\perp \cap L] \perp M$.*

(2.4) DEFINITION. Call an integral lattice L *semiselfdual* (SSD) if and only if $2L^* \leqslant L$; in this case, $2L^* = L \cap 2L^*$ is the *radical mod* 2 (2.1).

The following idea seems to be new.

(2.5) PROPOSITION (Semiselfdual Involutions). *If L is an integral lattice and M a semiselfdual lattice* (2.4) *contained in L, then the linear map on the ambient rational vector space which is -1 on M and 1 on $M^{\perp}$ is an automorphism of the lattice L.*

Proof. Let t be the linear map on $V := \mathbb{Q}L$. Let $V^{\pm}$ denote the eigenspaces for ± 1. Then t acts on the abelian group $V/M \cong V^{+} \oplus (V^{-}/M)$ by $+1$ on the first summand and -1 on the second. The second summand contains the subgroup M^{*}/M, left invariant by t, and on it t acts as $+1$ since M is SSD. Since L lies between M and $V^{+} \oplus M^{*}$, L is t-invariant since t acts as $+1$ on $V^{+} \oplus (M^{*}/M)$. ∎

(2.6) LEMMA. *If the lattice L is even and integral, has no roots, and $M \cong \sqrt{2}\, L_{E_8}$ is a sublattice, it is a direct summand of L, as an abelian group. Its image in $L/2L$ is a totally singular subspace, of dimension* 8.

Proof. Since $\det(M) = 2^8$, the only torsion in L/M occurs for the prime 2. If M is not a summand, there is an element $u \in L$ so that $u \in L \backslash M$ and $2u \in M$. Then we may assume that $2u$ is a shortest element in the coset $2u + 2M$, whence $(2u, 2u) = 4$ or 8 (A.2). Since L is an even unimodular lattice, we get $(u, u) = 2$, a contradiction since L has no roots. The last statement follows easily. ∎

(2.7) LEMMA. *Suppose that the lattice L is generated by the subset S. Then L is integral if $(S, S) \subseteq \mathbb{Z}$ and it is even if it is integral and $(x, x) \in 2\mathbb{Z}$ for all $x \in S$.*

(2.8) *Remark.* For basic coding concepts, see [22, 16]. Binary codewords may be interpreted as subsets of the alphabet, the index set for coordinates. The only special codes we refer to will be the (*extended*) *Hamming code* (A.3), with parameters (length, dimension, minimum weight) [8, 4, 4], and the *binary Golay code*, with parameters [24, 12, 8]. Existence and uniqueness proofs for the Hamming code are elementary exercises, but not so for the Golay code. We will study a *Golay code*, any binary code with parameters [24, 12, 8], and deduce its existence and uniqueness in (4.2).

(2.9) PROPOSITION (Tower of Scaled E_8-Lattices). *Let $L \cong L_{E_8}$ and $M \leqslant L$, $M \cong \sqrt{2}\, L_{E_8}$ (so we have a tower $\cdots 2L < M < L < \frac{1}{2}M \cdots$). Let $G := \mathrm{Aut}(L) \cong W_{E_8}$ and let $P := \mathrm{Stab}_G(M)$.*

(i) $P \cong 2_{+}^{1+6} GL(4, 2)$.

(ii) *$O_2(P)/\langle -1\rangle$ operates regularly on $\mathcal{K}$, the set of sublattices K of L such that $K \cong \sqrt{2}\, L_{E_8}$ and $K/2L$ complements $M/2L$ in $L/2L$. If $K \in \mathcal{K}$, $\mathrm{Stab}_G(M) \cap \mathrm{Stab}_G(K) = \mathrm{Stab}_P(K) \cong 2 \cdot GL(4, 2)$ (nonsplit).*

Proof. Parts (i) and (ii) follow from basic properties of $O^+(8, 2)$; see (A.3) and Appendix B, also (3.1). ▮

3. THE AUTOMORPHISM GROUP OF THE LEECH LATTICE

Thoughout this article, we let Λ be a *Leech lattice*, that is, an EUL lattice in dimension 24 with no vectors of squared length 2. Such lattices are easily seen to exist. The standard description involves the Golay code (A.4), but this can be avoided; we give a version in (3.2), (3.3)(i); this is not new [21, 33, 34]. *Assuming only existence of Λ, we prove its uniqueness* (3.7) *and get significant information about its automorphism group.*

(3.1) LEMMA. *Let s be the positive square root of a positive integer.* (i) *Given a lattice $L \cong sL_{E_8}$, there are* 135 *sublattices M of L such that $M \cong \sqrt{2}\, sL_{E_8}$; if M is such, M contains $2L$ and the invariant factors of M are $((2s^2)^8)$. The set of such M forms an orbit under* Aut(L). *For the* natural nonsingular bilinear form *on $L/2L$ (which takes the pair $(x + 2L, y + 2L)$ to $s^{-2}(x, y) + 2\mathbb{Z}$), $M/2L$ may be interpreted as a maximal totally singular subspace.*

(ii) *Given a lattice $L \cong sL_{E_8}$, there are* 135 *overlattices M of L such that $M \cong (s/\sqrt{2})\, L_{E_8}$; the set of such forms an orbit under* Aut(L); *if M is such and $s^2 \in 2\mathbb{Z}$, the invariant factors of M are $((\frac{1}{2}s^2)^8)$.*

Proof. Write f for the given bilinear form: $f(x, y) = (x, y)$. Without loss, we may assume $s = 1$.

(i) If M is between L and $2L$ and corresponds to a maximal totally singular subspace, we deduce $\det(M) = 2^8$ from $|L : M| = 16$. Since $(x, x) \in 4\mathbb{Z}$, for all $x \in M$, we get $(M, M) \leqslant 2\mathbb{Z}$ and so M is an even unimodular integral lattice for the bilinear form $\frac{1}{2} f$. From (A.9), we get $M \cong L_{E_8}$.

Let M be any such a sublattice of L. Then $M^*/M \cong 2^8$ and L/M is a subspace. Then $(M^*, 2f)$ has determinant 1 and so in the nonsingular space M^*/M with quadratic form $x + M \mapsto f(x, x) \pmod 2$, L maps to a totally singular subspace. Since $\det(L) = 1$ and $\det(M^*) = 2^{-8}$, $M^*/L \cong 2^4$. This forces L to contain $2M^* = M$ and $L/2M^*$ to be a maximal totally singular subspace of $M^*/2M^*$. Since the action of Aut(L) on $L_{E_8}/2L_{E_8}$ is that of $O^+(8, 2)$, we have transitivity.

(ii) Take dual lattices and apply (i). ▮

We next give results, (3.3)(ii) and (3.7), which characterize Leech lattices by certain internal data. Note that we ignore 1*s* when referring to the invariants of a lattice (2.1), e.g., T below has rank 16 and invariants (2^8) (the full set of 16 invariants is $(2^8 1^8)$ but we drop the 1*s* (2.1)).

(3.2) DEFINITION. Consider the 6-tuple $(M_1, M_2, M_3, \theta, N_1, \zeta)$, which satisfies the following conditions:

The $M_i \cong \sqrt{2}\, L_{E_8}$, for $i = 1, 2, 3$, are pairwise orthogonal sublattices in $\mathbb{Q}^{24}$; for each i, we let p_i be the orthogonal projection to $\mathbb{Q}M_i$; $W_i := \mathrm{Aut}(M_i)$.

θ: $M_1 \to M_2$ is an isometry (this is independent of the identifications fixed in the previous line).

$M_{12} := M_{12,\theta} := \{(x, x^\theta) \mid x \in M_1\} \cong 2L_{E_8}$.

N_1 is a sublattice of M_1; $N_1 \cong 2L_{E_8}$.

$N_2 := N_{2,\theta} := N_1^\theta$; $N_{12} := N_{12,\theta} := \{(x, x^\theta) \mid x \in N_1\} \cong 2\sqrt{2}\, L_{E_8}$.

$T := M_1 + M_2 + \frac{1}{2}N_{12}$; its invariants are (2^8) and the radical mod 2 (2.1) of T is $U := N_1 + N_2 + M_{12}$; $U/2T \cong 2^8$ and $U \cong \sqrt{2}\, T$ (to see this, just replace M_i, N_i by N_i, $2M_i$, respectively, in the definition of T and (3.1)(ii)); we remark that $T^* = \frac{1}{2}U \cong (1/\sqrt{2})\, T$).

ζ: $T^*/T \to M_3^*/M_3$ is an isometry with respect to the nonsingular quadratic forms $x + T \mapsto (x, x) + 2\mathbb{Z}$ and $x + M_3 \mapsto (x, x) + 2\mathbb{Z}$.

L is the sublattice between $T \perp M_3$ and $T^* \perp M_3^* = \frac{1}{2}U \perp \frac{1}{2}M_3$ which is diagonal with respect to the isometry ζ (note, for all i, $L^{p_i} = M_i^* \cong (1/\sqrt{2})\, L_{E_8}$).

Call such an 6-tuple a *Leech 6-tuple*. An ordered triple of pairwise orthogonal rank 8 lattices $M_i \cong \sqrt{2}\, L_{E_8}$, for $i = 1, 2, 3$, in $\mathbb{Q}^{24}$ is called a *Leech two*. We extend above maps on lattices to the ambient rational vector spaces.

(3.3) THEOREM. (i) *L is a Leech lattice.*

(ii) *Any Leech lattice containing a Leech trio comes from a Leech 6-tuple as above.*

(iii) *The set of Leech 6-tuples which extends a given Leech trio forms a single orbit under the natural action of* $\mathrm{Aut}(M_1) \times \mathrm{Aut}(M_2) \times \mathrm{Aut}(M_3)$. *A stabilizer has the shape* $[2 \times 2^{1+6}]\, GL(4, 2)$; *the first factor is* $\langle -1 \rangle$ *and the second factor is a diagonal embedding of the stabilizer of a maximal totally singular subspace for the action of* $\mathrm{Aut}(M_i)$ *on* $M_i/2M_i$, *for* $i = 1, 2$. *Its projection to* $\mathrm{Aut}(M_i)$ *is* $2_+^{1+6} GL(4, 2)$, *for* $i = 1, 2$, *and its projection to* $\mathrm{Aut}(M_3)$ *is* $2 \cdot GL(4, 2)$.

Proof. We begin by observing that T is the sublattice $T := M_1 + M_2 + \frac{1}{2}N_{12}$ of $\frac{1}{2}N_1 \perp \frac{1}{2}N_2 \cong L_{E_8} \perp L_{E_8}$. Since $M_i \cong \sqrt{2}\, L_{E_8}$ and $T/M_1 \perp M_2$ is diagonal in $M_1^*/M_1 \oplus M_2^*/M_2$, it is clear that the minimum squared length in T is 4, so T has no roots.

(i) Use (2.1) (applied to $T \perp M_3 \leqslant L \leqslant T^* \perp M_3^*$) to get that L is unimodular. Since $T^* \cong (1/\sqrt{2})\, T$, every vector has squared length an integer, even though T^* is not an integral lattice. Similarly, $M_3^* \cong (1/\sqrt{2})\, L_{E_8}$, whence every vector has squared length an integer. We must show that L has no roots.

Suppose that $r \in L$ is a root. Let $r_i := r^{p_i}$, for $i = 1, 2, 3$. Then $n_i := (r_i, r_i) \in \mathbb{Z}$ and $n_1 + n_2 + n_3 = 2$. For all i, $n_i < 2$ (else $r = r_i \in M_i^* \cap L = M_i$, which has no roots). So, $n_i \in \{0, 1\}$, for all i.

Suppose that $n_3 = 1$ and $\{n_1, n_2\} = \{0, 1\}$. The latter forces T to have a root since $r_1, r_2 \in L^{p_1 + p_2} = T^* \cong (1/\sqrt{2})\, T$, a contradiction to the first paragraph.

Suppose that $n_3 = 0$. Then $r \in M_3^{\perp} \cap L = T$, again a contradiction to the first paragraph.

(ii) Let L be a Leech lattice. We are given a trio and identifications $M_1 \cong M_2 \cong M_3$. Define $J := M_3^{\perp} \cap L$; then $\det(J) = \det(M_3) = 2^8$ (2.1). For $i = 1, 2$, $M_i \leqslant J \cap \mathbb{Q}M_i \leqslant M_i^*$. Since L has no roots and $M_i \cong \sqrt{2}\, L_{E_8}$, we have $M_i = J \cap \mathbb{Q}M_i = L \cap \mathbb{Q}M_i$ (2.6). Since the invariants for $K := M_1 \perp M_2$ are (2^{16}), J lies between K and $\frac{1}{2}K$, and it follows that J has invariants (2^8) and J/K corresponds to a 4-dimensional subspace of $K^*/K \cong 2^8$ which is diagonally embedded with respect to the decomposition $K^*/K \cong M_1^*/M_1 \times M_2^*/M_2$. We claim that $J^{p_i} \cong L_{E_8}$ for $i = 1, 2$, which is the same as saying (3.1) that for the natural nonsingular quadratic form on M_i^*/M_i, J^{p_i} corresponds to a maximal totally isotropic subspace. If not, there is $x \in J$ which maps to a nonsingular vector of M_i^*/M_i; write $x_j := x^{p_j}$ for $j = 1, 2$. Then (x_i, x_i) is an odd integer, which means that both x_1 and x_2 correspond to nonsingular vectors since $(x, x) \in 2\mathbb{Z}$. Since both cosets $x_j + M_j$ contain vectors of squared length 1 (A.2), we deduce that J contains a root, a contradiction. So, $J^{p_j} \cong L_{E_8}$. Define $N_j := 2J^{p_j} \leqslant M_j$, for $j = 1, 2$. It follows that $J = M_1 + M_2 + D$, where $2D$ is a diagonal subgroup of $N_1 \perp N_2$ defined by an isometry, θ, which carries M_1 to M_2 and N_1 to N_2 (use (3.1)(ii)). We have $D \cong \sqrt{2}\, L_{E_8}$.

Define $N := J \perp M_3$; $\det(N) = 2^{16}$. Since M_3 is a direct summand of L (2.6) and its invariants are (2^8), the same is true for $M_3^{\perp} \cap L$. Since $J \leqslant M_3^{\perp} \cap L$, $J = M_3^{\perp} \cap L$.

Since the invariants of $M_1 \perp M_2 \perp M_3$ are (2^{24}) and those of J are (2^8), L/N corresponds to a subgroup of $N^*/N \cong 2^{16}$ of dimension 8 which is

diagonally embedded with respect to the decomposition $N^*/N \cong J^*/J \times M_3^*/M_3$. In fact, with respect to the natural nonsingular bilinear form on N^*/N, defined by $x + N \mapsto (x, x) + 2\mathbb{Z}$, L/N is diagonally embedded with respect to an isometry $\zeta: J^*/J \to M_3^*/M_3$ since L is even.

(iii) We consider the proof of (ii). Fix identifications $M_1 \cong M_2 \cong M_3$ and corresponding copies of $W_i := \mathrm{Aut}(M_i) \cong W_{E_8}$. The choices for θ form an orbit under the natural action of W_1 or of W_2; its stabilizer is a diagonal subgroup W_{12} of $W_1 \times W_2$.

The subgroup S_{12} of W_{12} stabilizing the sublattice T is isomorphic to a subgroup of W_{E_8} of shape $2^{1+6}GL(4, 2)$, (A.3); S_{12} acts on T^*/T as $GL(4, 2)$ (since $[M_i, O_2(S_{12})] = N_i$ and $[N_i, O_2(S_{12})] = 2M_i$, for $i = 1, 2$; see (3.2)). The set of isometries $T^*/T \to M_3^*/M_3$ forms a single orbit under the natural action of W_3. It follows that the isometry of (ii) has stabilizer S contained in $S_{12} \times W_3$ and is isomorphic to $[2 \times 2_+^{1+6}]\, GL(4, 2)$; the projection of S to $W_1 \times W_2$ is S_{12} and the projection to W_3 is isomorphic to $2.GL(4, 2)$ since the normal subgroup of shape 2^{1+6} acts trivially on T^*/T. ∎

(3.4) COROLLARY. *If L is a Leech lattice and M is a sublattice isometric to $\sqrt{2}\, L_{E_8}$, then isomorphism type of $M^\perp$ is determined.*

Proof. Since L is unimodular and M is a direct summand, $\det(M^\perp) = \det(M) = 2^8$. We finish with (3.3)(ii) if we find a sublattice of $M^\perp$ isometric to $\sqrt{2}\, L_{E_8} \perp \sqrt{2}\, L_{E_8}$. This follows from (A.6)–(A.8). ∎

(3.5) PROPOSITION. *Choose a quadratic form on $\mathbb{Q}^{24}$ so that $\mathbb{Q}^{24}$, endowed with this form, contains a Leech lattice, say Λ. Then $\mathbb{Q}^{24} = \mathbb{Q}\Lambda$ and $O(\mathbb{Q}^{24})$ acts transitively on the following sets*:

(i) *pairs (L, M), where L is a Leech lattice in $\mathbb{Q}\Lambda$ and M is a sublattice of L isometric to $\sqrt{2}\, L_{E_8}$;*

(ii) *triples (L, M_1, M_2), where L is a Leech lattice in $\mathbb{Q}\Lambda$ and M_1, M_2 is a pair of orthogonal sublattices, each isometric to $\sqrt{2}\, L_{E_8}$;*

(iii) *quadruples (L, M_1, M_2, M_3), where L is a Leech lattice in $\mathbb{Q}\Lambda$ and (M_1, M_2, M_3) is a Leech trio in L.*

Proof. For (iii), use (3.3)(iii).

(i) A proof may be obtained from the ideas in the proofs of (3.3)(ii),(iii) and (3.4).

(ii) It suffices, by (iii), to prove that this ordered pair is part of a Leech trio. Define $Q := M_1 \perp M_2$, $M_3 := Q^\perp \cap L$. Since the invariants of Q

are (2^{16}), the invariants of both M_3 and $R := M_3^{\perp} \cap L$ are (2^a), for some $a \leqslant 16$. Since $\operatorname{rank}(M_3) = 8$, $a \leqslant 8$. We have $|R : Q| = 2^{8-a/2}$ (2.1). If $a < 8$, then for some $k \in \{1, 2\}$, $R_k := R \cap \mathbb{Q}M_k > M_k$. Since L is an even lattice, R_k/M_k must be a totally singular subspace with respect to the natural non-singular bilinear form on M_k^*/M_k; by (A.2)(i) (applied to $M_k^* \cong (1/\sqrt{2})\, L_{E_8}$), $R_k \backslash M_k$, hence L, contains a root, a contradiction. So, $a = 8$, whence $M_3 = 2M_3^*$ is doubly even and so $M_3 \cong \sqrt{2}\, L_{E_8}$ (A.9). ▮

(3.6) COROLLARY. $\operatorname{Aut}(\Lambda)$ *acts transitively on the set of sublattices isometric to* $\sqrt{2}\, L_{E_8}$. *We also have a conjugacy class of involutions in* $\operatorname{Aut}(\Lambda)$, *the SSD involutions* (2.5) *associated to these sublattices.*

(3.7) COROLLARY. *Any two Leech lattices are isometric.*

Proof. Any Leech lattice has a Leech trio (A.7). Now use (3.5). ▮

At this point, we know little about $\operatorname{Aut}(L)$ beyond some transitivity properties. We need to study the sublattices which occur as $M^{\perp}$, for a sublattice $M \cong \sqrt{2}\, L_{E_8}$.

(3.8) THEOREM. (i) *In a Leech lattice,* Λ, *let* M *be a sublattice isometric to* $\sqrt{2}\, L_{E_8}$ *and set* $T := M^{\perp}$. *Then* $\operatorname{Aut}(T)$ *is an extension* $2^{1+8}\Omega^+(8, 2)$.

(ii) *The noncentral involutions of* $\operatorname{Aut}(T)$ *which lie in* $O_2(\operatorname{Aut}(T))$ *form a single* $\operatorname{Aut}(T)$ *conjugacy class. For such an involution, the sum of the fixed point sublattice and the negated sublattice is isometric to* $\sqrt{2}\, L_{E_8} \perp \sqrt{2}\, L_{E_8}$.

(iii) *There is a bijection between the involutions of* (ii) *and ordered pairs of orthogonal sublattices of* T, *each isometric to* $\sqrt{2}\, L_{E_8}$. *If* $M_1 \cong M_2 \cong \sqrt{2}\, L_{E_8}$ *are orthogonal sublattices of* T, *then* $\operatorname{Stab}_{\operatorname{Aut}(T)}(M_1) \cap \operatorname{Stab}_{\operatorname{Aut}(T)}(M_2) \cong 2 \times 2^{1+6}GL(4, 2)$ *and the image of this group in* $\operatorname{Aut}(M_i)$, *for* $i = 1, 2$, *is of the form* $2^{1+6}GL(4, 2)$.

(iv) *The set of unordered pairs of sublattices as in* (ii) *is in bijection with the set of maximal totally singular subspaces of* $T/2T$ (*all of which have dimension* 12 *and contain the* 8*-dimensional radical*).

(v) $T \cap 2\Lambda = 2M_1 + 2M_2 + N_{12} = 2T$ *and* $T/T \cap 2\Lambda \cong 2^{16}$; *also* $T + M + 2\Lambda = T + 2\Lambda$.

(vi) *The actions of* $\operatorname{Stab}(M)$ *on* T^*/T *and* $M^*/M = \frac{1}{2}M/M \cong M/2M$ *are equivalent and may be identified with the action of* $\Omega^+(8, 2)$ *on the space* $\mathbb{F}_2^8$ *stabilizing a nondegenerate quadratic form.*

(We remark that these actions are equivalent to the irreducible action on $U/U \cap 2\Lambda \cong U + 2\Lambda/2\Lambda$ but not to T/U, where U is the radical modulo 2 of T.)

Proof. First, we show that $B := \{a \in \mathrm{Aut}(T) \mid [T, a] \leqslant U\} \cong 2_+^{1+8}$.

Take the sublattice $Q := M_1 \perp M_2$ of T, with $M_j \cong \sqrt{2}\, L_{E_8}$, for $j = 1, 2$, as in (3.2). Note that $U = N_1 + N_2 + M_{12}$. Let A be the stabilizer in $\mathrm{Aut}(T)$ of Q. Note that A lies in a wreath product $[\mathrm{Aut}(M_1) \times \mathrm{Aut}(M_2)]\, 2$ and that A has the form $[2_+^{1+6} \times 2_+^{1+6}].[GL(4, 2) \times 2]$; see (A.3) and consider the subgroup of the above wreath product which stabilizes N_1 and N_2. In more detail, let $R_i \cong 2_+^{1+6}$, for $i = 1, 2$ be the normal subgroup of $\mathrm{Stab}_{\mathrm{Aut}(M_i)}(N_i)$ as in (A.3); then $B \leqslant A$ has the form $R_{12} \circ E$, a central product, where R_{12} is diagonally embedded in $R_1 \times R_2$, E is dihedral of order 8, $E \cap O_2(A) \cong 2 \times 2$, and E contains an involution which interchanges R_1 and R_2 under conjugation. The statement about B follows.

Since B acts absolutely irreducibly on T, $C(B)$ consists of scalar matrices and so the quotient $\mathrm{Aut}(T)/BC(B)$ embeds in $\mathrm{Out}(B) \cong O^+(8, 2)$ (C.3). Our subgroup A contains B and maps onto a parabolic subgroup P of $\mathrm{Out}(B)'$ of the form $2^6 : GL(4, 2)$.

We may do the above for any sublattice of T which is isometric to $M_1 \perp M_2$. One such sublattice is $\frac{1}{2}N_{12;\theta} \perp \frac{1}{2}N_{12;-\theta}$, and we thereby get a subgroup isomorphic to P and distinct from P. Since P is a maximal parabolic subgroup of $\mathrm{Out}(B)' = \Omega^+(8, 2)$ [4], these two subgroups generate $\mathrm{Out}(B)'$. It follows that $\mathrm{Aut}(T)/B \cong O^+(8, 2)$ or $\Omega^+(8, 2)$.

There are several ways to see that $\mathrm{Aut}(T)/B \ncong O^+(8, 2)$: (a) a subgroup H of $GL(\mathbb{C} \otimes T)$ which contains B as a normal subgroup and with quotient $O^+(8, 2)$ has the property that certain elements of $H \backslash H'$ have traces of the form $\varepsilon 2^{c/2}$, where ε is a root of unity and c is an odd integer (C.4); since the representation of $\mathrm{Aut}(T)$ on T is rational, this does not happen; (b) study the centralizer in A of B_1, a 2_+^{1+6} subgroup of B; $C(B_1)$ lies in $GL(2, \mathbb{Q})$ and contains a copy of $C_B(B_1) \cong Dih_8$, which is a maximal finite 2-subgroup in $GL(2, \mathbb{Q})$; (c) in case $\mathrm{Aut}(T)/B$ were $O^+(8, 2)$, we would get a contradiction when we examine the structure of the frame group; see (A.5).

We now have (i). For (ii), it is clear since $\mathrm{Aut}(T)$ has index 2 in a holomorph of an extraspecial group (Appendix C), that the noncentral involutions in $O_2(\mathrm{Aut}(T))$ form a single conjugacy class. Since two such involutions are the central involutions of R_1 and R_2, the connection with the stated sublattices follows. For (iii), note that such a decompostion (with ordered summands) leads to a SSD involution t (-1 on M_1, 1 on M_2) which preserves T. It remains to show that t satisfies $[T, t] \leqslant U$. It is clear from the proof of (3.3)(ii) that there are appropriate sublattices $N_k \leqslant M_k$ and exactly two isometries $\pm\theta$: $M_1 \to M_2$ so that $T = M_1 + M_2 + \frac{1}{2}N_{12}$ as in (3.2). Then we get $[T, t] = N_1 \leqslant U = N_1 + N_2 + M_{12}$, as required.

For (iv), note that $\mathrm{Aut}(T)$ induces $\Omega^+(8, 2)$ on $T/U \cong 2^8$ and that $M_1 \perp M_2/U$ represents a maximal totally singular subspace.

The first part of (v) follows since T is a direct summand of Λ. From (2.3), we get that $T+M \geqslant 2\Lambda$ and $T+M/2\Lambda$ has codimension 8 in $\Lambda/2\Lambda$. Since the image of T in $\Lambda/2\Lambda$ has dimension 16, $T+2\Lambda = T+M+2\Lambda$.

For the first part of (vi), just note that Λ projects onto each of M^*/M and T^*/T. Since $T^* = \frac{1}{2}U$ and $U \cap 2\Lambda = T \cap \Lambda = 2T$, $U/2T \cong T^*/T$ as modules for $\mathrm{Stab}(M)$; these modules are selfdual. Clearly, $\Lambda/2\Lambda$ has a composition series with factors $U/2T \cong U+2\Lambda/2\Lambda$, T/U ($T+2\Lambda/2\Lambda$ is the annihilator of $U+2\Lambda/2\Lambda$) and finally Λ/T (isomorphic to $\Lambda/2\Lambda$ modulo the annihilator of $U+2\Lambda/2\Lambda$). The first and third are dual, hence isomorphic. The middle factor turns out to be not isomorphic to these, but the proof is perhaps not easy (this fact is not a necessary part of our theory; anyway, here is a nonelementary proof: we take an element x of order 3 in $\mathrm{Stab}(M)$ for which 1 occurs as an eigenvalue in the first and third factor with multiplicity 6; so, on Λ, the multiplicity of 1 is at least 12; since we know the classes of elements of order 3 in $\mathrm{Aut}(\Lambda)$ [16, 1]), we deduce that x has 1 with multiplicity exactly 12 and so on the middle composition factor, x does not have 1 as an eigenvalue). ▮

(3.9) COROLLARY. *With notation as in* (3.8)(i), *the group* $\mathrm{Stab}_{\mathrm{Aut}(\Lambda)}(M) = \mathrm{Stab}_{\mathrm{Aut}(\Lambda)}(M^\perp)$ *is of the form* $2_+^{1+8}.W'_{E_8}$ (*though we do not need it, we mention that this is a nonsplit extension* (C.3)) *and it induces* W'_{E_8} *on* M *and* $\mathrm{Aut}(T) \cong 2_+^{1+8}\Omega^+(8,2)$ *on* $M^\perp$.

Proof. Because of the decompositon (3.2), it is clear that $\mathrm{Stab}(M) = \mathrm{Stab}(M^\perp)$ induces exactly W'_{E_8} on M (3.8). The normal extraspecial group is generated by its involutions. By (3.8)(ii) and how the involutions may be interpreted as SSD maps that act trivially on M, the normal subgroup of $\mathrm{Stab}(M)$ of shape 2_+^{1+8} acts trivially on M. ▮

(3.10) COROLLARY. *If* (M_1, M_2, M_3) *is a Leech trio in* Λ, *its stabilizer in* $\mathrm{Aut}(\Lambda)$ *is of the form* $2^{3+12}GL(4,2)$, *of order* $2^{21}3^2 5.7$. *The stabilizer of the unordered trio has the form* $2^{3+12}[GL(4,2) \times \mathrm{Sym}_3]$, *a group of order* $2^{22}3^3 5.7$. *This subgroup determines the Leech trio by the three nontrivial linear characters of the normal eights group which occur in* $\mathbb{Q}^{24} = \mathbb{Q}\Lambda$ (*each with multiplicity* 8).

Proof. Let B and A be these respective subgroups. We have $A/B \cong \mathrm{Sym}_3$ (3.5)(iii) and $C_B(M_3) \cong 2 \times 2^{1+6}$ which acts on M_1, M_2 with respective kernels the two direct factor of order 2; see the proofs of (3.5)(iii) and (3.8). The result follows since A embeds in the subgroup $H \cong [2_+^{1+6}GL(4,2)] \wr \mathrm{Sym}_3$ of $\mathrm{Aut}(M_1 \perp M_2 \perp M_3)$, where the wreathing is done with the natural degree 3 action; in other words, B is forced to have shape 2^{3+12} and be the unique normal subgroup of A of index 2^6 in $O_2(H)$. The last statement is trivial. ▮

(3.11) DEFINITION. Write $\Lambda_n := \{x \in \Lambda \mid (x, x) = 2n\}$, the set of lattice vectors of *type n*.

(3.12) LEMMA. (i) $\mathrm{Aut}(\Lambda)$ *acts transitively on the set of pairs* (x, M), *where* M *is a sublattice isometric to* $\sqrt{2}\, L_{E_8}$ *and* $x \in M$ *has type* 4;

(ii) $\mathrm{Stab}((x, M)) \cong [2^{1+8+6}]\, \mathrm{Alt}_7 (\leqslant 2^{1+1+8+6}\Omega^+(6, 2))$ *and its order is* $2^{18}3^2 5.7$;

(iii) $\Omega^+(6, 2) \cong \mathrm{Alt}_8$.

Proof. By (3.6), it suffices for (i) to prove transitivity of $\mathrm{Stab}(M)$ on $M \cap \Lambda_4$. Define an equivalence relation on $M \cap \Lambda_4$ by congruence modulo $2M$. Each class consists of 16 vectors, two of which are orthogonal or opposite (A.2). Now, $\mathrm{Stab}(M)$ induces W'_{E_8} on M (3.9), which is transitive on the set of equivalence classes since they correspond to singular points in $M/2M$. Let K be a class and a, b, c, d linearly independent vectors in K. Then $\frac{1}{2}(a-b)$ and $\frac{1}{2}(c-d)$ are roots and the product of the corresponding reflections interchanges a and b. Transitivity follows since all "even" transformations on M come from the action of $\mathrm{Stab}(M)$ (3.9). Note that the group $\mathrm{Stab}(M)$ has a permutation representation of degree 8 on $K/\{\pm 1\}$ and that the simple group $\Omega^+(6, 2)$ has order $8!/2$. ∎

(3.13) PROPOSITION. *Let* $T_n := \{x \in T \mid (x, x) = 2n\}$. *Then*

(i) $\mathrm{Aut}(T)$ *has one orbit on* T_2 (*length* $4320 = 2^5 3^3 5$, *stabilizer of shape* $2^{4+6}\Omega^+(6, 2)$) *and it has two orbits on* T_4, *size* 522720; *one orbit in* U, *the radical modulo* 2 (*length* $4320 = 2^5 3^3 5$, *stabilizer of shape* $2^{4+6}\Omega^+(6, 2)$), *and the second orbit outside* U (*length* $518400 = 2^8 3^4 5^2$, *stablizer of shape* $2^{4+3+3}GL(3, 2)$).

(ii) $\mathrm{Aut}(T)$ *has one orbit on* T_3 (*length* $61440 = 2^{12} 3.5$). *A stabilizer is isomorphic to* $Sp(6, 2)$.

(iii) *The theta series for* T *begins* $1 + 4320q^2 + 61440q^3 + 522720q^4 + \cdots$.

Proof. (i) Since $\mathrm{Aut}(T)$ induces $\Omega^+(8, 2)$ on T/U (3.8)(vi), any singular coset in T/U lies in a natural sublattice of the form $M_1 \perp M_2$, with $M_i \cong \sqrt{2}\, L_{E_8}$. Since $U \cap M_i \cong 2L_{E_8}$, (3.5)(iii), (3.10), and (A.3)(ii) imply the statement about elements of type 2 and show that the elements x of type 4 in $M_i \backslash N_i$ lie in one $\mathrm{Aut}(T)$-orbit. To get the cardinality of the first orbit, count ordered triples (x, M_1, M_2), where $x \in T_2 \cap M_1$, $M_1 \cong M_2 \cong \sqrt{2}\, L_{E_8}$, $(M_1, M_2) = 0$. Such ordered pairs M_1, M_2 correspond to the $2 \cdot 135 = 2.3^3 5$ noncentral involutions of $O_2(\mathrm{Aut}(T))$. Given M_1, there are $240 = 2^4 3.5$ such x, hence $2^5 3^4 5^2$ such triples. In T/U, there are 15 totally

singular subspaces containing the singular vector $x+U$, and such subspaces have the form M_1+M_2/U. So the number of such x is $2^5 3^4 5^2/15 = 2^5 3^3 5 = 4320$. Since $U \cong \sqrt{2}\, T$, we get the same count for the orbit $T_4 \cap U$. Now, let S be a stabilizer for this orbit, $|S| = 2^{21}3^5 5^2 7/2^5 3^3 5 = 2^{16}3^2 5.7$. Since $-1_T \notin S$, $S \cap O_2(\mathrm{Aut}(T))$ is elementary abelian of rank at most 4. Since $S/S \cap O_2(\mathrm{Aut}(T))$ embeds in a subgroup of shape $2^6 : \Omega^+(6,2)$, this embedding is onto and $S \cap O_2(\mathrm{Aut}(T)) \cong 2^4$.

For $T_4 \backslash U$, we have transitivity if we show that every element is in the $\mathrm{Aut}(T)$-orbit of an element of $M_i \backslash N_i$. Clearly every element of type 4 in $M_1 \perp M_2$ has the form $x = x_1 + x_2$, $x_i \in M_i$, where (a) one of the summands is 0 (whence x has the desired form), or (b) each x_i has type 2. Assume the latter for x and, by way of contradiction, assume that (*) x is not in the orbit of an element from (a). Then by (3.8)(ii), no involution of $O_2(\mathrm{Aut}(T))$ fixes x, so the orbit of x under $O_2(\mathrm{Aut}(T))$ has length 2^9 and lies in a single coset of U. Because U is the radical modulo 2, if L is the span of the orbit of $\frac{1}{2}x$, L is an even integral lattice containing at least 512 roots. Since the action of $\mathrm{Aut}(T)$ on $\mathbb{Q}T$ is an absolutely irreducible representation, the action of $\mathrm{Aut}(Q)$ on the orthogonally indecomposable summands of L is transitive, so all have the same isometry type and are generated by roots. So, the roots of L form a system of type D_m^n, A_m^n, or E_8^2, for $mn = 16$. No such lattice has 512 roots, a contradiction. We count pairs $(x, M_1 + M_2)$ with M_1, M_2 as above, with x a type 4 vector in $M_1 + M_2 \backslash U$; in each M_i, there are $2160 - 240 = 1920 = 2^7 3.5$ such x, and the remaining x have the form $x_1 + x_2$, where $x_i \in M_i$ has type 2. The number of such pairs is 240^2, but the requirement $x \notin U$ requires us to remove 240.2^4 such pairs. Given $M_1 + M_2$, there are $2^7 3.5 + 2^7 3.5 + 2^8 3^2 5^2 - 2^8 3.5 = 2^8 3^2 5^2$ such x. The number of such $M_1 + M_2$ is $135 = 3^3 5$, so the number of such pairs is $2^8 3^5 5^3$. Since these pairs form an orbit under $\mathrm{Aut}(T)$ and there are 15 such $M_1 + M_2$ containing a given x, the cardinality of $T_4 \backslash U$ is $2^8 3^5 5^3/15 = 2^8 3^4 5^2$.

A stabilizer S for x in this orbit has order $2^{21}3^5 5^2 7/2^8 3^4 5^2 = 2^{13}3.7$. Since -1_T does not stabilize S, $S \cap Z(\mathrm{Aut}(T)) = 1$ and $S \cap O_2(\mathrm{Aut}(T))$ is an elementary abelian group of rank at most 4. We may take x to have the form (b) as above. Then, since $S/S \cap O_2(\mathrm{Aut}(T))$ embeds in a subgroup of shape $Sp(6,2)$, the order forces $S/S \cap O_2(\mathrm{Aut}(T)) \cong 2^{3+3}GL(3,2)$ because the index prime to 2 means the subgroup is a parabolic [4], and the order allows one parabolic, up to conjugacy.

(ii) An element x of T_3 maps to a nonsingular vector in T/U, where $\mathrm{Aut}(T)$ acts as $\Omega^+(8,2)$, so is transitive on such vectors with the stabilizer of $x+U$ an $Sp(6,2)$-subgroup. We claim that the only element of $O_2(\mathrm{Aut}(T)) \cong 2_+^{1+8}$ which stabilizes $\{x, -x\}$, for $x \in T_3$, is $\{\pm 1\}$. But this is clear from (3.8)(ii) where it is shown that the noncentral involutions of $O_2(\mathrm{Aut}(T))$

have, for their action on T, fixed point sublattices isometric to $\sqrt{2}\,L_{E_8}$; these contain no vectors of odd type. We next claim that $O_2(\mathrm{Aut}(T))$ acts transitively on $\Lambda_3 \cap (x+U)$. Since two elements of type 3 are congruent modulo 2Λ if and only if they are equal or negatives (an easy exercise), for any $y \in \Lambda_3 \cap (x+U)$, the map $O_2(\mathrm{Aut}(T))/Z(O_2(\mathrm{Aut}(T)) \to U/2T$ derived from $g \mapsto y - y^g + 2T$ is injective, and this proves the claim since $U/2T \cong 2^8$. Therefore, $|T_3| = 2^9 \cdot 120 = 2^{12} 3 \cdot 5 = 61440$. A stabilizer for this orbit meets $O_2(\mathrm{Aut}(T))$ trivially and embeds in $Sp(6, 2)$ since these vectors have odd type. Since this $|\Omega^+(8, 2)|/|Sp(6, 2)| = 120$, we deduce that this embedding is onto.

(iii) This follows frown (i) and (ii). Also, see (A.10) and (A.11). ∎

(3.14) LEMMA. *If* $x \in \Lambda_2 \cup \Lambda_3$, $A(x) := \{ y \in \Lambda \mid (x, y) \in 2\mathbb{Z} \}$, *the "annihilator mod* 2," *contains a sublattice isometric to* $\sqrt{2}\,L_{E_8}$.

Proof. Let (M_1, M_2, M_3) be a Leech triple and let $x = x_1 + x_2 + x_3$, where x_i is the projection of x to the rational span of M_i. Then each $x_i \in M_i^* = \frac{1}{2} M_i$, whence $n_i := (x_i, x_i)$ is a nonnegative integer. If some n_i is 0, we are done, so assume all are positive.

Since Λ is even, we may reindex to assume $n_3 > 0$ is even. Let $y := x_1 + x_2$. Each x_i is nonzero. If x has type 2, $(y, y) = 2$ and $y \in T^* \cong (1/\sqrt{2})\,T$; we quote (3.13)(i) to transform x by $\mathrm{Stab}(M_3)$ to an element where some n_i is 0. If x has type 3, y has type 1 or 2 and a similar use of transitivity (3.13) works (there are cases: $y \in T$ implies $x_3 \in M_3$ and this is impossible since minimum squared lengths in T and M_3 are 4; if $y \notin T$, then x_3 has type 1 or 2 and y has type 2 or 1). ∎

(3.15) LEMMA. (i) *Suppose that* $x \in \Lambda_n$ *and* $M \leqslant \Lambda$, $M \cong \sqrt{2}\,L_{E_8}$ *satisfies* $(M, x) \leqslant 2\mathbb{Z}$ (*such* M *exist if* $n \leqslant 3$, *by* (3.14)). *Then* $x \in M \perp (M^\perp \cap \Lambda)$, *so we write* $x = u + v$, $u \in M$, $v \in M^\perp$.

(ii) *If* $n = 2$, $u = 0$ *or* $v = 0$. *In case* $u = 0$, *there is a sublattice* $M_1 \perp M_2$ *of* $M^\perp$ *as in* (3.2) *containing* x.

(iii) *If* $n = 3$, $x = v \in M^\perp$.

Proof. For (i), use (2.3)(ii). The remaining statements follow from (3.13). ∎

(3.16) THEOREM. $\mathrm{Aut}(\Lambda)$ *is transitive on* Λ_2.

Proof. From (3.13)(ii), a type 2 vector lies in a $\sqrt{2}\,L_{E_8}$ sublattice, say M, of Λ. From (3.9), we know that $\mathrm{Stab}(M)$ induces W'_{E_8} on M, so all vectors of type 2 in M lie in a single orbit under $\mathrm{Stab}(M)$. ∎

(3.17) THEOREM. $\mathrm{Aut}(\Lambda)$ *is transitive on*

(i) *pairs* (M, x), *where* $M \cong L_{E_8}$ *is a sublattice and* $x \in \Lambda_3 \cap M^{\perp}$;

(ii) Λ_3;

(iii) *quadruples* (M_1, M_2, M_3, x), *where* (M_1, M_2, M_3) *is a Leech trio and* $x \in \Lambda_3 \cap M_3^{\perp}$.

The stabilizer of a pair as in (i) *has the form* $2.Sp(6, 2)$, *order* $2^{10}3^45.7$, *and the stabilizer of a quadruple as in* (iii) *has the form* $2.2^{3+3}.GL(3, 2)$, *order* $2^{10}3.7$.

Proof. Part (i) follows from (3.13). Note that (3.15) tells us that any type 3 vector is part of a pair as in (i), so (ii) follows from (i). For (iii), use Witt's theorem to see that H, the stabilizer in $\mathrm{Aut}(T)$ of a maximal totally singular subspace in T/U, is transitive on nonsingular vectors. As in the proof of (3.13), we know that if $x \in T$ has type 3, $O_2(\mathrm{Aut}(T))$ is transitive on the type 3 vectors in $x + U$, so we get the stabilizer for (i). The stabilizer for (iii) has index 135 in the stabilizer for (i), so by surveying the maximal parabolics for $Sp(6, 2)$, we get the indicated subgroup. ∎

(3.18) LEMMA. *Let* $x \in \Lambda_4$. *Then the set of sublattices* $M \cong \sqrt{2}\, L_{E_8}$ *which contain* x *form an orbit of length* 253 *under* $\mathrm{Stab}_{\mathrm{Aut}(\Lambda)}(x)$.

Proof. See (A.4), (A.7), (3.12)(i). ∎

(3.19) THEOREM. $\mathrm{Aut}(\Lambda)$ *is transitive on frames* (A.4) *and on* Λ_n, *for* $n = 0, 2, 3, 4$; $|\mathrm{Aut}(\Lambda)| = 2^{22}3^95^47^211.13.23$.

Proof. By (3.16) and (3.17), it suffices to prove transitivity on Λ_4. Let $G := \mathrm{Aut}(\Lambda)$. Any type 4 element lies in a frame and any frame gives rise to a Golay code (A.4) and so we may take our element x of type 4 and embed it in a pair (M, x) as in (A.7), (3.12)(i). Transitivities on Λ_4 and frames follow (3.12). The number of such pairs containing x is 253 (3.18). Then, we have $|G : G_{(M, x)}| = |G : G_x|\, |G_x : G_{(M, x)}|$. The first factor on the right side is $u_4 = 2^43^75^37.13$ (A.1)(ii) and the second is 253 (A.6). We conclude that $|G : G_{(M, x)}| = 2^43^75^37.11.13.23$, whence (3.12)(ii), $|G| = 2^{22}3^95^47^211.13.23$. ∎

(3.20) THEOREM. *Let* Λ *be any Leech lattice. Then, for any frame* Σ, *there is an ordered basis* $\Sigma^+ \subset \Sigma$ *and a code so that* Λ *is as described in* (A.4). *The stabilizer* Σ *in* $\mathrm{Aut}(\Lambda)$ *has the form* $D : P$ (A.4.1), (A.5).

(3.21) *Remark.* The preceding statement is not trivial. Moving from a frame plus Golay code to a containing Leech lattice involves work over

$\mathbb{Z}/4\mathbb{Z}$, where the sign problems are harder to deal with than over $\mathbb{Z}/2\mathbb{Z}$, e.g., [16, Appendix 9A].

(3.22) *Remark* (The TU-tower). We call attention to the chain $\cdots < 2T < U < T \leq \frac{1}{2}U < \cdots$ whose every member is a scaled copy of T by a power of $\sqrt{2}$ (3.2). This is an analogue of (2.9).

We get another nice uniqueness result, which makes the Barnes–Wall lattice a member of the Broué–Enguehard series; see (A.10) and (A.11).

(3.23) THEOREM. *There is a unique even integer lattice which has rank* 16, *theta series which begins like* $1 + 4320q^2 + \cdots$, *and has no vectors of type* 2 *in its radical modulo* 2.

Proof. Let T be such a lattice and $U := \{x \in T \mid (x, T) \leq 2\mathbb{Z}\}$, the radical modulo 2. As usual, for an even integral lattice, L, we write L_n for $\{x \in L \mid (x, x) = 2n\}$. Our assumption may be expressed $T_1 = \varnothing = U_2$ and $\operatorname{rank}(T) = 16$.

The main thing we have to establish is that the relation "congruence modulo U" is an equivalence relation on T_2 whose classes consist of "frames," that is, 16-sets of type 2 vectors, two of which are proportional or orthogonal. So, let x, y be nonproportional members of T_2 such that $x + U = y + U$. Then, $x + y = u \in U$ and so $(x, x + y) \in 2\mathbb{Z}$, whence $(x, y) \in 2\mathbb{Z}$. We want $(x, y) = 0$. If nonzero, we may replace y by $-y$ if necessary to arrange $(x, y) < 0$. Then $(x, y) \leq -2$ and $0 < (x + y, x + y) \leq 4 + 4 - 4 = 4$, whence $x + y \in U_2 = \varnothing$, a contradiction. So, each class has at most 16 vectors.

Since $4320/16 = 135 > 2^7$, it follows that the finite abelian 2-group T/U is elementary abelian and that the nonsingular quadratic form on it inherited from T has maximal Witt index (the other possibility, a quadratic form of nonmaximal Witt index, would have exactly 119 singular points). It follows that the 4320 elements of T_2 are distributed among these 135 singular cosets of U in T, whence each class has exactly 16 members.

In case $\frac{1}{2}U/T$ has maximal Witt index (for its form taking values in $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$), we follow an idea from Section 3. Let $Q \cong \sqrt{2}\, L_{E_8}$. There is an isometry of $\frac{1}{2}Q/Q$ and $\frac{1}{2}U/T$, so can take Λ to be the preimage in $\frac{1}{2}Q \perp \frac{1}{2}U$ of the diagonal subgroup of $\frac{1}{2}Q/Q \times \frac{1}{2}U/T$. Then, Λ is an even unimodular lattice with no roots (since the minimum norm in T is 4), so L is isometric to the standard Leech lattice (3.7). From (3.4), we deduce that our T is isometric to the lattice T of (3.2), and we are done.

The isometry type of $\frac{1}{2}U/T$ has not been established. However, we did prove that T/U has maximal Witt index, so if we use $(1/\sqrt{2})\, T$, $(1/\sqrt{2})\, U$ for $\frac{1}{2}U$, T, respectively, in the argument of the last paragraph, we get a rootless even unimodular lattice since the minimum norm in T is 4 and we

deduce from (3.4) that the isometry type of $(1/\sqrt{2})\,U$ is determined. Uniqueness of T then follows from (3.22). ▮

4. THE MATHIEU GROUP, WITH THE GOLAY CODE (FINALLY!)

(4.1) Definition. A *Golay code*, $\mathscr{G}$, is a binary code of length 24, dimension 12, and minimum weight *at least* 8. A group M_{24} is the automorphism group of a binary Golay code. We use the notations of (A.4), (A.5).

(4.2) Theorem (Uniqueness of the Binary Golay Code). *There is a unique* (*up to equivalence*, *i.e.*, *coordinate permutations*) *binary code of length* 24, *dimension* 12, *and minimum weight at least* 8 (*hence equal to* 8).

Proof. Existence of such codes comes from (A.4.3) and existence of a Leech lattice. To prove uniqueness, we suppose that $\mathscr{C}$ is any Golay code. We define a lattice, L with $\mathscr{C}$ following the recipe in (A.4). Let $\Omega := \{1, ..., 24\}$ be an index set and $\{x_i \mid i \in \Omega\}$ be a basis of Euclidean space $\mathbb{R}^\Omega$ such that $(x_i, x_j) = 2\delta_{i,j}$. For $A \subseteq \Omega$, define $x_A := \sum_{i \in A} x_i$, $v_i := -x_i + \frac{1}{4}x_\Omega$. Let L be the span of all $2x_i$, $\pm x_i \pm x_j$, v_i and all $\frac{1}{2}x_A$, $A \in \mathscr{C}$. Then L is a EUL without vectors of type 2, hence is isometric to Λ (3.7). By transitivity of $\mathrm{Aut}(\Lambda)$ on frames (3.19), we may assume that $\{\pm 2x_i \mid i \in \Omega\}$ corresponds by our isometry to the standard frame (A.4), whence $\mathscr{C} \cong \mathscr{G}$. ▮

(4.3) Proposition. $\mathrm{Aut}(\mathscr{G}) = P$ *and* $|P| = 2^{10}3^3 5.7.11.23$ (*see* (A.5) *for the definition of* P; *the big Mathieu group* M_{24} *is* defined *to be* $\mathrm{Aut}(\mathscr{G})$, *so we get* $|M_{24}| = 2^{10}3^3 5.7.11.23$).

Proof. See (A.5), (3.19). ▮

(4.4) Proposition. P *acts transitively* (i) *on the set of octads*; (ii) *and on* Ω.

Proof. (i) If $\mathscr{O}$ and $\mathscr{O}'$ are octads, then $M(\mathscr{O})$ (A.6) contains some $x \in \Sigma$, the standard frame (A.4), and $M(\mathscr{O}')$ contains some $x' \in \Sigma$. Now use (3.12)(i) and note that an element of $\mathrm{Aut}(\Lambda)$ which carries the first pair to the second stabilizes Σ.

(ii) Given $i, j \in \Omega$, expand each to an octad to create pairs $(M(\mathscr{O}), 2\alpha_i)$ and $(M(\mathscr{O}'), 2\alpha_j)$. Now use (3.12)(i) and (3.19). ▮

(4.5) Proposition. *The stabilizer in* P *of an octad is isomorphic to* $AGL(4, 2)$, *the affine general linear group*, *which is a semidirect product of the general linear group* $GL(4, 2)$ *by the group of translations*, *isomorphic to* 2^4.

Proof. Let H be the stabilizer in P of the octad $\mathcal{O}$; form the sublattice $M(\mathcal{O})$ (A.6) and use (3.9) and (A.5) to conclude that the stabilizer of $(M(\mathcal{O}), F)$, where F is a frame in the sense of (A.2)(i), has the form DH, order $2^{16}|GL(4, 2)|$, whence $|D| = 2^{12}$ implies that $|H| = 2^4 |GL(4, 2)| = |AGL(4, 2)|$. It is clear from (3.3)(iii) that H has a normal 2-subgroup R of order 16 whose quotient is $\Omega^+(6, 2)$. We now display $R \cong 2^4$.

The involutions of R can be associated to semiselfdual sublattices (2.4) as follows: the space W of Golay sets disjoint from $\mathcal{O}$ consist of 30 octads, $\varnothing$ and $\mathcal{O} + \Omega$ (A.7). Given a codimension 1 subspace, W_0 of W which contains $\langle \Omega \rangle$, we define an involution $t \in P$ as follows. Let $\mathcal{O}_i$, $i = 1, 2, 3$ be octads in W_0 which are linearly independent modulo $\mathcal{O} + \Omega$. Define an associated *TI* (*triple intersection*) as a set of the form $\mathcal{O}'_1 \cap \mathcal{O}'_2 \cap \mathcal{O}'_3$, where $\mathcal{O}'_i$ represents $\mathcal{O}_i$ or its complement $\mathcal{O}_i + [\mathcal{O} + \Omega]$ in $\mathcal{O} + \Omega$; a TI is a 2-set. Similarly, call a set a *DI*, a *double intersection*, if it has the form $\mathcal{O}'_1 \cap \mathcal{O}'_2$, notation as above; a DI is a 4-set. The intersection of any two octads disjoint from $\mathcal{O}$ is a 0-, 4-, or 8-set. Define $M := M(\mathcal{O}_1, \mathcal{O}_2, \mathcal{O}_3)$ as the span of all $\alpha_i - \alpha_j$, where $\{i, j\}$ is an associated TI and all $\frac{1}{2}[\alpha_i - \alpha_j + \alpha_k - \alpha_\ell]$, where $\{i, j\}$ and $\{k, \ell\}$ are TIs whose union forms a DI. (It is easy to check that the definition of M depends just on W_0.) For such an M, we have a SSD involution, $t = t_M \in P$. Its effect on the α_i is to interchange two whose indices form a TI. If W_0, W_1, and W_2 are three such subspaces of W with associated involutions t_0, t_1, t_2, then $t_0 t_1 t_2 = 1$ if $W_0 \cap W_1 = W_1 \cap W_2 = W_2 \cap W_0$.

It is clear that we have 15 involutions which have cycle shape $1^8 2^8$ and which, with the identity, form an elementary abelian group, R, which acts regularly on $\mathcal{O} + \Omega$. At once, H splits over R. Let K be a complement. Since the action of K on T is faithful (because the action of $\mathrm{Stab}(M)$ on $M^\perp \cap \Lambda = \Lambda \cap [\mathbb{Q}\Lambda, R]$ has kernel $\{\pm 1\}$ (3.8)), we are done. ∎

(4.6) *Remark* (A Trio of Sporadic Isomorphism). We note that the sporadic isomorphisms $\Omega^+(6, 2) \cong GL(4, 2) \cong \mathrm{Alt}_8$ follow from our analysis (C.3), (A.3), (3.12), (4.5); this says more than $GL(4, 2) \cong \mathrm{Alt}_8$, which is observed in the traditional course of studying M_{24} and the octad stabilizer [8, 16].

(4.7) *Remark*. It follows from (3.13) that if $x = 2\alpha_i \in \Lambda_4$ is in the standard frame, there are two orbits of $\mathrm{Stab}(x)$ on the set of $M \cong \sqrt{2}\, L_{E_8}$ in $x^\perp \cap \Lambda$. One is the set of all $M(\mathcal{O})$ (A.4), (4.6), where $\mathcal{O}$ is an octad avoiding i, and a sublattice from the other orbit contains no vectors from the standard frame and is a sublattice of $\Lambda \cap \sum_{i \notin \mathcal{O}'} \mathbb{Q}\alpha_i$, where $\mathcal{O}'$ is an octad containing i. ∎

Next, we will give a uniqueness argument for the ternary Golay code. We use existence of a ternary Golay code to prove uniqueness. If $\mathcal{TG}$ is

such a code, namely, a $[12, 6, 6]$ code over $\mathbb{F}_3$, then we use a lattice M which is the orthogonal direct sum of 12 lattices isometric to L_{A_2}. Using rational linear combinations of elements of the M_i related to the elements of $\mathscr{TG}$, we will get a rootless even unimodular rank 24 lattice, Λ, which by our characterization (3.7), must be unique up to isomorphism. We give our version here (cf. [8, 16]).

(4.8) *Ternary Construction of the Leech Lattice.* Let $\mathscr{TG}$ be a ternary Golay code, a $[12, 6, 6]$ code. One may imitate the analogous construction of the E_8-lattice, described in [16, (8.22)]. For $i = 1, ..., 12$, take a base α_i, β_i of the A_2 root system in $M_i \cong L_{A_2}$, define $v_i := \frac{1}{3}[\alpha_i - \beta_i]$. Then $M_i^* = M_i + \mathbb{Z}v_i$. Define M_0 as the span of all $3M_i^*$ and all $\sum c_i\alpha_i$, where $c_i \in \mathbb{Z}$ and $\sum_i c_i \in 3\mathbb{Z}$. For $c = (c_i) \in \mathbb{F}_3^6$ and x one of the symbols α, β, v, define $x_S := \sum_{i \in S} c_i x_i$, where we think of $\mathbb{F}_3$ as the subset $\{-1, 0, 1\}$ of $\mathbb{Z}$. Finally, define $\gamma_i := \frac{1}{3}[4\alpha_i + \sum_{j \neq i} \alpha_j]$. We define the lattice $\Lambda_0 := M_0 + \sum_{c \in \mathscr{TG}} \mathbb{Z}v_c$; then $L_0/M_0 \cong \mathscr{TG}$. We take $\Lambda := L_0 + \mathbb{Z}\gamma_i$ (the definition of Λ is independent of i since $\gamma_i - \gamma_j = \alpha_i - \alpha_j \in M_0$); see (2.7). Since $\det(M_i) = 3$ and $\det(M) = 3^{12}$, we get $\det(M_0) = 3^{14}$, $\det(L_0) = 3^2$, and $\det(\Lambda) = 1$ by repeated use of the formula $\det(K) = \det(J)\,|J : K|^2$, for lattices $K \leqslant J$ (2.1). The rootless property of Λ is easy to verify. Though the code is not described explicitly, we may still construct a group of automorphisms of Λ which is isomorphic to $\mathscr{TG}$ and preserves M, namely the maps $\varepsilon_s := \prod_i \varepsilon_i^{s_i}$, where $s = (s_i) \in \mathscr{TG}$ is a codeword and ε_i is the identity on M_j if $j \neq i$ and

$$\varepsilon_i : \begin{cases} \alpha_i \\ \beta_i \end{cases} \mapsto \begin{cases} \beta_i \\ -\alpha_i - \beta_i, \end{cases}$$

a rotation by $2\pi/3$ on M_i. Note that $\alpha_i^{\varepsilon_i} = \alpha_i - 3v_i$, $\beta_i^{\varepsilon_i} = \beta_i - 3\beta_i - 3v_i$, and $v_i^{\varepsilon_i} = v_i - \beta_i$, whence ε_i satisfies $|M_i : M_i(\varepsilon_i - 1)^k| = 3^k$. Proof that the ε_c preserve Λ is routine (one must use the property that all inner products in $\mathscr{TG}$ are zero mod 3). Obviously, $\mathrm{Aut}(\mathscr{TG})$ is a group of lattice automorphisms (by coordinate permutations) and it normalizes the above group of order 3^6.

From this particular way of constructing Λ, we can see an important property of the Sylow 3-group of $\mathrm{Aut}(\Lambda)$, which has order 3^9.

(4.9) Lemma. *A Sylow* 3*-group contains exactly one elementary abelian subgroup of order* 3^6. *Such a subgroup is therefore weakly closed in a Sylow* 3*-subgroup.*

Proof. This follows from the fact that an element of order 3 in $\mathrm{Aut}(\mathscr{TG}) \cong 2 \cdot M_{12}$ acts with Jordan canonical form $2J_3$ or $J_1J_2J_3$. Proof of this fact is an exercise using Section 7 of [16, (7.37)]. ▮

This lemma can be proved with much less work than a general analysis of $\mathscr{T}\mathscr{G}$ and $\mathrm{Aut}(\mathscr{T}\mathscr{G})$. Since we deduce that $|\mathrm{Aut}(\mathscr{T}\mathscr{G})|_3 = 3^3$ from our knowledge of $|\mathrm{Aut}(\Lambda)|$, it would suffice to display a group of automorphisms of order 3^3 (this Sylow 3-group is nonabelian) and just observe the Jordan canonical forms of its elements; this may be done by selective use of Section 7 of [16].

(4.10) THEOREM. *There is a unique ternary code with parameters of the form* [12, 6, 6].

Proof. Any such code may be used with a lattice $M := M_1 \perp \cdots \perp M_{12}$, where $M_i \cong L_{A_2}$, to construct a Leech lattice, Λ, as above.

This group of shape 3^6 is isomorphic to $\mathscr{T}\mathscr{G}$ by the inverse of $c \mapsto \varepsilon_c$ (4.8) and may be used to recover the lattices $M_0 \cap M_i$ (in the notation of (4.8)) as the sublattices affording 12 distinct rational characters of 3^6; one gets M_i from $M_0 \cap M_i$ as $M_i = 3[M_0 \cap M_i]^*$.

The weak closure property of such a group in a Sylow 3-subgroup of $\mathrm{Aut}(\Lambda)$ (4.9) then implies that any two such lattices M are in a single orbit under the action of $\mathrm{Aut}(\Lambda)$. From this, it follows that the associated code in M^*/M is unique up to equivalence. ∎

5. OTHER CONSEQUENCES FOR THE LEECH LATTICE AND ITS AUTOMORPHISM GROUP

We make no attempt to systematically derive the standard results about Mathieu groups and Conway groups using SDD theory, but merely give a sample to illustrate use of our theory. The next result analyzes an entry from the list of triangle stabilizers in $\mathrm{Aut}(\Lambda)$ [5, 16].

(5.1) PROPOSITION. *G is transitive on triangles of type* 222. *Let a, b, c form a triangle of type* 222, *that is, a triple of vectors of type* 2 *which sum to* 0. *Let $H := \mathrm{Stab}_G(a, b, c)$. Then, H contains* 2*-central involutions with centralizers of shapes* $2_-^{1+6}\Omega^-(6, 2)$.

Proof. Note that the image mod 2Λ of any triangle with edges of even type lies in a maximal totally singular subspace. By (3.16), we may assume that $a \in M_3$, where (M_1, M_2, M_3) is a Leech triple. If $b \in M_1 \perp M_2 \perp M_3$, we are done since $(b, b) = 4$, $(b, a) \neq 0$, and $M_i \cong \sqrt{2}\, L_{E_8}$ imply that $b \in M_3$. It is therefore enough, by (3.6) to show that any triangle of type 222 lies in a sublattice isometric to $\sqrt{2}\, L_{E_8} \perp \sqrt{2}\, L_{E_8} \perp \sqrt{2}\, L_{E_8}$ since $\mathrm{Stab}(M_3)$ induces W'_{E_8} on M_3.

For an index k, define $T = T_k := \Lambda \cap M_k^{\perp}$ and let $U = U_k/2T$ be the radical mod 2 of T (2.3). For an index k and $x \in \Lambda$, define $A_k(x) := \{ y \in T_k \mid (x, y) \in 2\mathbb{Z} \}$, a sublattice of T_k of index 1 or 2.

If there is an index $i \neq 3$ so that $(M_i, b) = 0$, (3.8)(ii) and the first paragraph imply that we are also done because the images of a, b in $T_i/2T_i$ lie in a common maximal totally singular subspace, we are done. So, we may assume that there is no such i.

We let b_i be the projection of b to $\mathbb{Q}M_i$; each (b_i, b_i) is a positive integer. Since $4 = (b, b) = (b_1, b_1) + (b_2, b_2) + (b_3, b_3)$, we conclude that the three summands on the right side are $(1, 1, 2)$, in some order.

If $(b_3, b_3) = 2$, $b' := b_1 + b_2 \in T_3^* \backslash T^3$. By transitivity (3.13)(i), (3.8)(ii), and the singularity of $b + T_3 \in T_3^*/T_3$, we may assume that $b' \in \frac{1}{2}[N_1 + N_2]$, whence b' lies in one of the $\frac{1}{2}N_j$. If i is the remaining index, we have $\{a, b\} \in M_i^\perp \cap \Lambda = T_i$, and we are done by another use of (3.8) and the first paragraph of this proof.

Finally, we assume that $(b_3, b_3) = 1$; let j be the index so that $(b_j, b_j) = 2$ and set $b' := b - b_j \in T_j^* \backslash T_j$; $b' + T_j$ is a singular vector in T_j^*/T_j. Then the image in T_j^*/T_j lies in a totally singular subspace, say R/T_j, where $R = R' \perp R'' \cong L_{E_8} \perp L_{E_8}$. By transitivity (3.13)(i), we may assume that a lies in one summand, say R'. Since $(b', b') = 2$, b' lies in one summand, and since $(a, b') = (a, b) = -2 \neq 0$, this summand must be R'. Therefore, $\{a, b\}^\perp \geqslant R'' \cap \Lambda \cong \sqrt{2}\, L_{E_8}$. Now, $\mathrm{Stab}(R'' \cap \Lambda)$ will transform the set $\{a, b\}$ into a sublattice of $(R'' \cap \Lambda)^\perp$ which is isometric to $\sqrt{2}\, L_{E_8} \perp \sqrt{2}\, L_{E_8}$, and finally we are done.

The structure of the centralizer of an involution follows from making the choice of triangle of type 222 in the sublattice M of (3.9). ∎

(5.2) *Remark*. The proof of (5.1) can be adapted to show that the group Co_2 has an involution with centralizer of the form $2_+^{1+8} Sp(6, 2)$ and by looking in $\frac{1}{2}N_{12}$ (2.3), we can find another with centralizer of the form $2^{1+6}2^4.GL(4, 2)$. The stabilizer H of a triangle of type 222 should be isomorphic to $PSU(6, 2)$, but I am not aware of any proof in the literature; indeed, in [5], the table of stabilizers had a question mark at 222 (removed in later versions). Centralizer of involution characterizations of $PSU(6, 2)$ in the literature seem to require more than the centralizer shape in (5.1). One can identify H by verifying that it has the 3-transposition property [12, 13].

(5.3) *Remark*. There are four classes of involutions in $\mathrm{Aut}(\Lambda)$ [1, 16]. All may be interpreted as SSD involutions. We know already (3.6) about involutions associated to $M \cong \sqrt{2}\, L_{E_8}$; their negatives are also SSD, associated to $M^\perp \cap \Lambda$. The involutions of trace 0 are associated to the sublattice of Λ consisting of vectors supported at a dodecad; it is isometric to the halfspin lattice for D_{12} [16] and has invariants (2^{12}). Finally, the involution -1 is the SSD involution associated to Λ itself.

(5.4) *Remark*. Something like SSD theory should work for elements of order greater than 2. We would expect a theory of existence and uniqueness of other codes used in other descriptions of the Leech lattice [16], e.g., the ternary Golay code which is associated to the subgroup $3^{12}2 \cdot M_{12}$.

(5.5) PROPOSITION. *A Leech trio stabilizer is a* 2*-local in* $\mathrm{Aut}(\Lambda)$ *of shape* $2^{1+2+12}[\mathrm{Sym}_3 \times GL(4,2)]$ (3.10) *and it acts absolutely irreducibly on* $\Lambda/p\Lambda$, *for all odd primes* p.

Proof. If M is any sublattice isomorphic to $\sqrt{2}\,L_{E_8}$, $O_2(\mathrm{Stab}_{\mathrm{Aut}(\Lambda)}(M))$ acts on $\Lambda/p\Lambda$ with an irreducible direct summand of dimension 16. Also, $O_2(\mathrm{Stab}_{\mathrm{Aut}(\Lambda)}(M))$ stabilizes any Leech trio containing M (the other two sublattices of a trio are just the fixed points of x and xz, where z is the SSD involution associated to M and x is a noncentral involution in $O_2(\mathrm{Stab}_{\mathrm{Aut}(\Lambda)}(M))$ (3.8)(ii). If we let M range over members of a Leech trio, it follows that the trio stabilizer acts irreducibly on $\Lambda/p\Lambda$. ∎

(5.6) COROLLARY. $\Lambda/p\Lambda$ *is an absolutely irreducible* G*-module, for all prime numbers* p.

Proof. If p is odd, we use (5.5). Suppose that $p=2$. Let $Q/2\Lambda$ be a proper submodule of $\Lambda/2\Lambda$, of dimension $d>0$. By transitivity of G on vectors of type 3 (3.17) and $d<24$, we have $Q \cap \Lambda_3 = \varnothing$ (A.2)(ii). Then, $Q/2\Lambda$ is totally singular, whence $d \leqslant 12$. But then $2^d < \min\{u_2/2, u_4/24\}$, a contradiction to transitivity on Λ_2 and Λ_4. So, we have irreducibility. Suppose that we do not have absolute irreducibility. Then we have a nontrivial centralizer algebra and an integer $e>1$ so that when $\Lambda/2\Lambda$ is extended to a splitting field, every irreducible for $\mathrm{Aut}(\Lambda)$ occurs with multiplicity divisible by e. If we take an element x of order 23 in $\mathrm{Aut}(\Lambda)$ and note that $x^{23}-1$ has a single nontrivial irreducible factor, we see that $e>1$ is impossible, a contradiction. ∎

(5.7) *Remark*. We have absolutely irreducible action modulo all primes for W_{E_8} on L_{E_8} (easy to prove) and also that of the sporadic simple group F_3 on a 248 dimensional lattice. For other examples, see [10, 11, 27–32].

APPENDIXES: BACKGROUND

Appendix A. Elementary Lattice Theory

(A.1) PROPOSITION. *Theta functions. For an even integral lattice* L, *the theta function is* $\sum_{k \geqslant 0} u_k q^k$, *where* u_k *is the number of lattice vectors of squared length* $2k$.

(i) *The theta series for* L_{E_8} *begins* $1 + 240q + 2160q^2 + \cdots$.

(ii) *The theta series for a Leech lattice,* Λ, *begins* $1 + 196560q^2 + 16773120q^3 + 398034000q^4 + \cdots$.

Proof. See [24], for instance; or [8, p. 135]. ∎

(A.2) Proposition (The E_8 Lattice and Leech Lattice mod 2). *Let* L *be* L_{E_8} *or a Leech lattice* Λ *and let* $L_n := \{x \in L \mid (x, x) = 2n\}$.

(i) *For* $L = L_{E_8}$, *a coset of* $2L$ *meets* L_n *for exactly one value of* $n \in \{0, 1, 2\}$ *and such a nonempty intersection has the form* $\{\pm x\}$, *except for* $n = 2$ *for which it is a "frame," a set of* 16 *vectors, two of which are equal, opposite, or orthogonal.*

(ii) *For* $L = \Lambda$, *a coset of* $2L$ *meets* L_n *for exactly one value of* $n \in \{0, 2, 3, 4\}$ *and such a nonempty intersection has the form* $\{\pm x\}$, *except for* $n = 4$ *for which it is a "frame," a set of* 48 *vectors, two of which are equal, opposite, or orthogonal.*

Proof. Part (i) is trivial. For (ii), which is almost as trivial, see [5, 16]. ∎

(A.3) Lemma. (i) *In* W_{E_8}, *the stabilizer* P *of a maximal totally singular subspace in* L_{E_8} *mod* 2 *has the form* $2_+^{1+6}GL(4, 2) \cong 2_+^{1+6}\Omega^+(6, 2)$; P *splits over* $O_2(P)/Z(P)$ *but not over* $O_2(P)$, *i.e.,* P *contains a perfect group of the form* $2.GL(4, 2)$ *but does not contain* $GL(4, 2)$. *Also, the nontrivial cosets of this subspace each contain* 16 *roots.*

(ii) W_{E_8} *acts transitively on*

(a) *pairs* (M, x) *where* $M \cong \sqrt{2}\, L_{E_8}$ *is a sublattice of* $L = L_{E_8}$ *and* $x \in M$, $(x, x) = 2$;

(b) *pairs* (M, x) *where* $M \cong \sqrt{2}\, L_{E_8}$ *is a sublattice of* $L = L_{E_8}$ *and* $x \in L \backslash M$, $(x, x) = 4$;

(c) *pairs* (M, x) *where* $M \cong \sqrt{2}\, L_{E_8}$ *is a sublattice of* $L = L_{E_8}$ *and* $x \in M$, $(x, x) = 4$.

Proof. (i) Since all such stabilizers are conjugate, it suffices to examine a convenient one. The chief factors of such a group P are clear; the only issue is the structure of the maximal normal 2-subgroup. Use the following description of L_{E_8}. Let $v_1, ..., v_8$ be a basis of 8-dimensional Euclidean space such that $(v_i, v_j) = 2\delta_{i,j}$ and let $\mathcal{H}$ be a dimension 4, length 8, minimum weight 4 extended binary Hamming code, e.g., the span in $\mathbb{F}_2^8$ of (11110000), (11001100), (10101010), (11111111). Its group is a subgroup $S \cong AGL(3, 2)$ of the full group Sym_8 of coordinate permutations. We may and do identify

the index set with the normal eights group $E := O_2(S)$ of S; the codewords of weight 4 may be identified with affine subspaces of dimension 3 in E. For $A \subseteq E$, define $v_A := \sum_{i \in A} v_i$. Define the lattice L to be the $\mathbb{Z}$-span of all $\pm v_i \pm v_j$, $\frac{1}{2} v_A$ for $A \in \mathscr{H}$ and all $-v_i + \frac{1}{4} v_E$. This lattice is even and unimodular so is isometric to L_{E_8}. Denote by M the sublattice spanned by all $\pm v_i \pm v_j$ and $\frac{1}{2} v_E$. Both L and M admit the group S by coordinate permutations and admit the group of sign changes consisting of maps ε_A, $A \subseteq E$, which are defined by

$$v_i \mapsto \begin{cases} -v_i, & i \in A; \\ v_i, & i \notin A. \end{cases}$$

The group $\langle E, F \rangle$ is extraspecial (C.1) and acts trivially on both L/M and $M/2L$. For a discussion of a related family of lattices, see [2] (A.11). For the statement about splittings in P, we observe that P has a subgroup of the form $2.GL(4, 2)$ which occurs as the stabilizer of a maximal totally singular subspace complementary to the one stablized by P.

To show that any subgroup $2.GL(4, 2)$ of P is nonsplit, we note that, if split, the ambient 8 dimensional complex representation would have irreducible constituents of degrees 1 and 7 [1]; on any invariant lattice taken modulo 2 therefore we would have the trivial module, which is not the case (we have two 4-dimensional irreducible constituents).

(ii) Let $L_n := \{x \in L \mid (x, x) = 2n\}$. By Witt's Theorem and the fact that W_{E_8} induces the full orthogonal group on $L/2L$, there is a single orbit of W_{E_8} on singular vectors outside the subspace $M/2L$ of $L/2L$ and a single orbit on nonsingular vectors outside this subspace. These nonsingular vectors are the images in $L/2L$ of L_1 and a nonsingular vector corresponds to a pair $\{x, -x\}$ in L_1. Since $-1 \in P$, the stabilizer in W_{E_8} of M, we clearly have one orbit, whence (a).

(b) Now, let $X := M \cap L_2$. A singular vector outside $M/2L$ corresponds via $L \to L/2L$ to a subset R of X of 16 vectors, two of which are equal, negatives, or orthogonal. It suffices to show that $\mathrm{Stab}_P(R)$ is transitive on R. Since P induces $GL(4, 2)$ on L/M, it suffices to take R to contain an "odd" vector, say $-v_i + \frac{1}{4} v_E$, and show R is contained in a single K-orbit. Since membership in R is determined by congruence modulo $2L$, every vector in R is odd. Finally, it suffices to show that K has a single orbit on Y, the set of all odd vectors of squared length 4. It is easy to see that Y consists of $[-v_i + \frac{1}{4} v_E]^{\varepsilon_A}$, for all indices $i \in E$ and all even subsets $A \subseteq E$. Since S is transitive on E and K contains D, the group of all ε_A, transitivity is clear.

(c) We can view the action of P as that of the stabilizer in $\mathrm{Aut}(M)$ of $2L$, so the preceding argument applies here since $M \cong \sqrt{2}\, L_{E_8}$ and $2L/2M$ is a maximal totally isotropic in the sense of the associated non-singular quadratic form (3.1) on $M/2M$. We deduce (c) from (b). ▮

(A.4) (*Frames, Codes and a Description of the Leech Lattice*).

(A.4.1) (Frame and code concepts). Given a Leech lattice, Λ, a *frame* is a set of 48 vectors in Λ of squared length 8, two of which are opposite or orthogonal; a frame is an equivalence class of sets of vectors of type 4 in which x and y are equivalent if and only if $x - y \in 2\Lambda$. An *oriented frame* or a *frame basis* is a subset of a frame which is a basis of $\mathbb{Q}\Lambda$.

(A.4.2) (Standard frame and standard description of a Leech lattice). We now assume the existence of a Golay code, $\mathscr{G}$, and its use in describing a Leech lattice, Λ, in the standard way with a basis consisting of an orthogonal set of roots $\{\alpha_i \mid i \in \Omega\}$. The *standard frame* is $\Sigma := \{\pm 2\alpha_i \mid i \in \Omega\}$ and the *standard oriented frame* is $\Sigma^+ := \{2\alpha_i \mid i \in \Omega\}$. We define $\Lambda := \mathrm{span}_{\mathbb{Z}}\{2\alpha_i,\ \pm\alpha_i \pm \alpha_j,\ \frac{1}{2}\alpha_S,\ v_i \mid i, j \in \Omega, S \in \mathscr{G}\}$, where, for $S \subseteq \Omega$, $\alpha_S := \sum_{i \in S} \alpha_i$ and $v_i := \frac{1}{4}\alpha_\Omega - \alpha_i\}$ (this set of generators is unnecessarily large, but shows symmetry). The *frame group* is the stabilizer of a given frame in $\mathrm{Aut}(\Lambda)$. Clearly, in the standard frame group $\mathrm{Stab}(\Sigma)$, there is a natural subgroup of the form $D : P$, where D acts diagonally with respect to the frame and where P is the group of permutation matrices identified with the automorphism group of the code $\mathscr{G}$. The orthogonal transformations which stabilize each 1-space spanned by elements of Σ have the form ε_A, $A \in \Omega$, which are defined by

$$\alpha_i \mapsto \begin{cases} -\alpha_i, & i \in A; \\ \alpha_i, & i \notin A. \end{cases}$$

(A.4.3) (Deduction of a code from a Leech lattice). Conversely, given a Leech lattice, Λ, and a frame, F (which exists, by (A.1)(ii)), we find that a code occurs naturally. We define $\Lambda(4) := \mathrm{span}\{\frac{1}{2}(x - y) \mid x, y \in F\}$, $\Lambda(2) := \{x \in L \mid 2x \in \Lambda(4)\}$. Then, by using the 24 coordinate spaces $\frac{1}{2}\mathbb{Z}x \bmod \mathbb{Z}F$, $x \in F$, $\Lambda(2)/\Lambda(4)$ gives a binary code $\mathscr{C}$ and, since Λ is a Leech lattice, it is straightforward to see that the code is doubly even of dimension 12 (whence the universe set is in $\mathscr{C}$, making it closed under complementation), the code has minimum weight at least eight and that $|\Lambda : \Lambda(2)| = 2$.

We now prove that the minimum weight is eight. Let $S \in \mathscr{C}$ have minumum weight, say $w \geqslant 8$. Since $\mathscr{C}$ is closed under complementation, we may assume that $w \leqslant 12$. We suppose that $w \geqslant 9$ and obtain a contradiction. Consider the map $\psi: \mathscr{C} \to P(S)$, the power set, defined by $A \mapsto A \cap S$. Since Λ is integral, all intersections of pairs of sets in $\mathscr{C}$ are even, so

$\dim(\mathrm{Im}(\psi)) \leqslant w-1$ and $\dim(\mathrm{Ker}(\psi)) \geqslant 13-w$. Assuming that $\dim(\mathrm{Ker}(\psi)) \geqslant 2$, we have $A \in \mathrm{Ker}(\psi)$, $A \neq 0$, $\Omega + S$. Since $|A| \geqslant 9$, $18 \leqslant |A+S| < 24$, whence $0 < |A+S+\Omega| \leqslant 6$, a contradiction. We have $\dim(\mathrm{Ker}(\psi)) = 1$ and $w = 12$ and so every set in $\mathscr{C}$ is 0, Ω or a 12-set. Since $\mathrm{Im}(\psi)$ is the codimension 1 space of even sets in $P(S)$, there is $A \in \mathscr{C}$ so that $A \cap S$ is a 2-set. Since A is a 12-set, $A+S$ is a 20-set, our final contradiction.

(A.4.4) (The Steiner system, octads, and dodecads). Let $S(5, 8, 24)$ denote a Steiner system with parameters (5, 8, 24), that is, a family of 8-sets in a fixed 24-set such that any 5-set is contained in a unique member of this family. Sets of weight 8 in $\mathscr{C}$ are called *octads* (4.4). The octads in a Golay code as above form such a Steiner system. Sets of weight 12 in $\mathscr{C}$ are called *dodecads*; their stabilizers are, by definition, the group M_{12}.

(A.5) PROPOSITION. $\mathrm{Stab}_{\mathrm{Aut}(\Lambda)}(\Sigma) = D : P$ *and* $D := \{\varepsilon_A \mid A \in \mathscr{G}\} \cong 2^{12}$ (*see* (A.4.2)).

Proof. Since the code $\mathscr{G}$ is its annihilator in the power set $P(\Omega)$ (with addition the symmetric difference and bilinear form $(A, B) \mapsto |A \cap B| \bmod 2$), application of ε_A to lattice elements of the form $\frac{1}{2}\alpha_S$, $S \in \mathscr{G}$, shows that if it stabilizes Λ, then $A \in \mathscr{G}$. Trivially, $\varepsilon_A \in \mathrm{Aut}(\Lambda)$ if $A \in \mathscr{G}$.

Now, let $g \in \mathrm{Stab}(\Sigma)$; then g is a product dp, where d is diagonal and p is a permutation matrix. Applying g to a vector of the form $\frac{1}{2}\alpha_S$, $S \in \mathscr{G}$ gives a vector of the form $\frac{1}{2}\sum_{i \in T} \pm \alpha_i$ in Λ, for some $T \subseteq \Omega$. Since its inner product with every $\frac{1}{2}\alpha_S$, $S \in \mathscr{G}$ is an integer, we get $|T \cap S|$ even, for every $S \in \mathscr{G}$, which implies that $T \in \mathscr{G}$. This means that p is in the group of the code, whence both p and d stabilize Σ. ∎

(A.6) *Notation.* $M(\mathcal{O})$ is the set of lattice vectors supported at the octad $\mathcal{O}$ (A.4). From (A.4.3), it is clear that $\Lambda \cap M(\mathcal{O})$ is just the $112 \pm \alpha_i \pm \alpha_j$ and all 128 $\frac{1}{2}\alpha_{\mathcal{O}}\varepsilon_A$, for all $A \in \mathscr{G}$.

(A.7) LEMMA. *For* $x \in \Sigma$ (A.4.2), *the set of* $M \cong \sqrt{2}\, L_{E_8}$ *containing* x *is just the set of lattices of the form* $M(\mathcal{O})$ *where* $\mathcal{O}$ *is an octad containing the index* i, *where* $x = \pm 2\alpha_i$. (*There are* $253 = 11.23$ *such.*)

Proof. It is clear from (3.6) that the stabilizer of x is transitive on the set of such M which contain it. Since $\mathrm{Stab}(x) \leqslant \mathrm{Stab}(\Sigma)$, which acts monomially with respect to the double basis Σ, it follows that every such M has the form $M(\mathcal{O})$. (The count $253 = \binom{23}{4}/\binom{7}{4}$ follows from (A.4.4).) ∎

(A.8) PROPOSITION. *The Golay sets disjoint from an octad consist of* 30 *octads, the empty set, and the octad complement. Any octad is part of a trio* (*a partition of* Ω *into three octads*).

Proof. Let $\mathcal{O}$ be an octad. Study the map $\mathcal{G} \to P(\mathcal{O})$, as in (A.4). ∎

(A.9) THEOREM (Classifications of EULs). *An EUL has rank divisible by* 8. *In rank* 8, *there is, up to isometry, just one EUL,* L_{E_8} [36]. *In rank* 16, *there are two, the halfspin lattice of rank* 16 *and the direct sum of two copies of* L_{E_8} [36]. *In rank* 24, *there are* 24, *and they are distinguished by the systems formed by their sets of roots; the empty root system corresponds to the Leech lattice* [23]. *See also* [35, 24, 22].

(A.10) [2] (*The Lattices of Broué–Enguehard*). Given an integer $n \geqslant 3$, there is a lattice L_n of rank 2^n with the following properties:

(i) $\det(L_n) = \begin{cases} 1, & n \text{ odd;} \\ 2^8, & n \text{ even;} \end{cases}$

(ii) $\mathrm{Aut}(L_3) \cong W_{E_8} \cong 2 \cdot O^+(8, 2)$;

$\mathrm{Aut}(L_n) \cong 2^{1+2n}_+ \Omega^+(2n, 2)$ if $n \geqslant 4$;

(iii) the minimum squared length is $2^{[n/2]}$.

(iv) $\mathrm{Aut}(L_n)$ is transitive on minimal vectors.

(A.11) *Remark.* (i) These lattices are beautifully described by an error correcting code of length 2^n based on the action of $GL(n, 2)$ on $\mathbb{F}_2^n$ and the minimal vectors are listed. In case $n = 3$, the expected group of automorphisms $2^{1+6}_+ \Omega^+(6, 2)$ is proper in the full group of automorphisms, the Weyl group for E_8.

(ii) The Barnes–Wall lattice [3] is a rank 16 lattice with determinant 256 and minimum squared length 4; the theta series begins $1 + 4320q^2 + 61440q^3 + 522720q^4 + \cdots$. In [8, p. 131], its occurrence as our lattice T (3.2) and certain other properties are asserted but no reference or proof is given. This lattice turns out to be a member of the Broué–Enguehard series, by (3.23); in [8, 2] it is mentioned but there seems to be no explanation of its relationship to the Barnes–Wall lattice.

Appendix B. Orthogonal Groups in Characteristic 2

For basic theory, see [9, 1]. We summarize what we need.

(B.1) *The Groups.* We are in even dimension $2n \geqslant 2$ over the field F, which is perfect of characteristic 2 (this includes finite fields). There are two equivalence classes of quadratic forms, according to the Witt index, the dimension of a maximal totally singular subspace; the possibilities for the

Witt index are n (plus type) and $n-1$ (minus type) and the isomorphism types of the isometry groups are denoted $O^\varepsilon(2n, F)$, $\varepsilon = \pm$. This group is not simple since it has a normal subgroup $\Omega^\varepsilon(2n, F)$ of index 2, the kernel of the Dickson invariant [9], which is a simple group except in the case $(n, \varepsilon) = (2, +)$.

(B.2) *Permutation Representations.* By Witt's theorem, which says that in V, a finite dimensional vector space with a nonsingular quadratic form, an isometry between subspaces extends to an isometry on V, the groups $O^\varepsilon(2n, F)$ are transitive on the totally singular subspaces of a given dimension $d \leqslant n$; when restricted to $\Omega^\varepsilon(2n, F)$ we still have transitivity, except for $d = n$, where we have two orbits. For one of these subspaces, the stabilizer in $\Omega^\varepsilon(2n, F)$ or $O^\varepsilon(2n, F)$ is a parabolic subgroup of the form $F(\binom{n}{2}) : GL(n, F)$. The stabilizer in $\Omega^\varepsilon(2n, F)$ of a singular, resp. nonsingular vector, has the shape $F^{2n-2}\Omega^\varepsilon(2n-2, F)$, $\Omega^\varepsilon(2n-1, F) \cong Sp(2n-2, F)$.

(B.3) *Weyl Group of E_8.* The Weyl group $W := W_{E_8}$ satisfies $Z(W) = \{\pm 1\}$, $W/Z(W) \cong O^+(8, 2)$, and $|W| = 2^{14}3^5 5^2 7$.

Appendix C. Extraspecial p-Groups

(C.1) DEFINITION [14, 19]. Given a prime number p, an extraspecial p-group is a finite p-group P such that $Z(P) = P'$ has order p. It follows that $\Phi(P) = Z(P)$ and that $P/Z(P)$ is a vector space of dimension $2n$ over $\mathbb{F}_p$, for some integer $n \geqslant 1$ and that the map $P/Z(P) \times P/Z(P) \to Z(P)$ based on commutation may be interpreted as a nonsingular alternating bilinear form. When $p = 2$, the squaring map induces a map $P/Z(P) \to Z(P)$ which may be interpreted as a nonsingular quadratic form.

(C.2) THEOREM. *Given P as in* (C.1), *the irreducible representations consist of p^{2n} linear characters and an algebraically conjugate family of $p-1$ irreducibles of dimension p^n; the latter are faithful.*

(C.3) DEFINITION. A *holomorph* of P, as in (C.1), is a group G so that $P \lhd G$ and the natural map $G \to \mathrm{Aut}(P)$ has kernel $Z(P)$ and image $C_{\mathrm{Aut}(P)}(Z(P))$; if the image is a proper subgroup, the G is a *partial holomorph.* A holomorph is *standard* if it exists as a subgroup of $GL(2^m, \mathbb{C})$; otherwise it is a *twisted holomorph.* For $p = 2$ extensions are generally nonsplit [17, 18] but are split for p odd. In any holomorph, G, the conjugacy classes within P consist of the p elements of $Z(P)$, plus one or two further ones, distinguished by their orders, p and p^2 (either one or both orders may occur).

(C.4) THEOREM. *Let G be a standard holomorph and χ the character of G in the p^n dimensional irreducible representation. For $g \in G$, define P_g by $P_g/Z(P) := C_{P/Z(P)}(g)$ and $d_g := \dim(P_g/Z(P))$. We say that g acts* cleanly *on P if and only if $P_g = C_P(g)$ (the other possibility, left unnamed, is $|P_g : C_P(g)| = p$). Then $\chi(g) = \varepsilon p^{d_g/2}$ for some root of unity ε, if g acts cleanly; and $\chi(g) = 0$ otherwise.*

Proof. See [15]. ∎

REFERENCES

1. Conway, Curtis, Norton, Parker, and Wilson, "An Atlas of Finite Groups," Oxford, Clarendon, 1985.
2. M. Broué and M. Enguehard, Une famillie infinie de formes quadratiques entière; leurs groupes d'automorphismes, *C. R. Acad. Sci. Paris Sér. A* **274** (1972).
3. E. S. Barnes and G. E. Wall, Some extreme forms defined in terms of Abelian groups, *J. Amer. Math. Soc.* **1** (1959), 47–63.
4. R. Carter, "Simple Groups of Lie Type," Wiley, London, 1972, 1989.
5. J. Conway, A group of order 8, 315, 553, 613, 086, 720, 000, *Bull. London Math. Soc.* **1** (1969), 79–88.
6. J. Conway, A characterization of Leech's lattice, *Invent. Math.* **7** (1969), 137–142.
7. J. Conway, Three lectures on exceptional groups in Higman–Powell, *in* "Finite Simple Groups," pp. 215–247, Academic Press, London, 1971.
8. J. Conway and N. Sloane, "Sphere Packings, Lattices and Groups," Springer-Verlag, Berlin, 1988.
9. J. Dieudonne, "La Géométrie des Groups Classiques," Springer-Verlag, Berlin/Heidelberg/New York, 1971.
10. N. Dummigan and P. H. Tiep, Congruences for certain theta series, *J. Number Theory* **71** (1998), 86–105.
11. N. Dummigan and P. H. Tiep, Lower bounds for certain symplectic group and unitary group lattices, *Amer. J. Math.*, in press.
12. B. Fischer, Finite groups generated by 3-transpositions, notes, University of Warwick, 1969.
13. B. Fischer, Finite groups generated by 3-transpositions, *Invent. Math.* **13** (1971), 232–246.
14. D. Gorenstein, "Finite Groups," Harper & Row, New York, 1968; 2nd ed., Chelsea, New York, 1980.
15. R. L. Griess, Jr., The monster and its nonassociative algebra, *in* "Finite Groups—Coming of Age" (J. McKay, Ed.), Contemp. Math., Vol. 45, Amer. Math. Soc., Providence, 1985.
16. R. L. Griess, Jr., "Twelve Sporadic Groups," Springer Mathematical Monographs, Springer-Verlag, New York/Berlin, 1998.
17. R. L. Griess, Jr., Automorphisms of extra special groups and nonvanishing degree 2 cohomology, *Pacific J. Math.* **48** (1973), 403–422.
18. R. L. Griess, Jr., On a subgroup of order $2^{15}\,|GL(5, 2)|$ in $E_8(\mathbb{C})$, the Dempwolff group and $\mathrm{Aut}(D_8 \circ D_8 \circ D_8)$, *J. Algebra* **40** (1976), 271–279.
19. B. Huppert, "Endliche Gruppen, I," Springer-Verlag, New York/Berlin, 1967.
20. J. Milnor and D. Husemoller, "Symmetric Bilinear Forms," Springer-Verlag, Berlin/Heidelberg/New York, 1973.

21. J. Lepowsky and A. Meurman, An E_8 approach to the Leech lattice and the Conway group, *J. Algebra* **77** (1982), 484–504.
22. J. MacWilliams and N. Sloane, "The Theory of Error-Correcting Codes," North-Holland, Amsterdam, 1983.
23. H.-V. Niemeyer, "Definite Quadratische Formen der Diskriminante 1 und Dimension 24," Doctoral Dissertation, Göttingen, 1968.
24. J.-P. Serre, "A Course in Arithmetic," Graduate Texts in Mathematics, Vol. 7, Springer-Verlag, New York/Berlin, 1973.
25. N. Sloane, review of [21], *in* "Mathematical Reviews."
26. J. G. Thompson, A simple subgroup of $E_8(3)$, *in* "Finite Groups Symposium" (N. Iwahori, Ed.), pp. 113–116, Japan Soc. for Promotion of Sci., Tokyo, 1976.
27. P. H. Tiep, Globally irreducible representations of the finite symplectic group $Sp_4(q)$, *Comm. Algebra* **22** (1994), 6439–6457.
28. P. H. Tiep, Basic spin representations of $2\mathbb{S}_n$ and $2\mathbb{A}_n$ as globally irreducible representations, *Arch. Math.* **64** (1995), 103–112.
29. P. H. Tiep, Weil representations as globally irreducible representations, *Math. Nachr.* **184** (1997), 313–327.
30. P. H. Tiep, Globally irreducible representations of finite groups and integral lattices, *Geom. Dedicata* **64** (1997), 85–123.
31. P. H. Tiep, Globally irreducible representations of $SL_3(q)$ and $SU_3(q)$, *Israel J. Math.*, in press.
32. P. H. Tiep and A. E. Zalesskii, Reduction modulo p of unramified representations, in preparation.
33. J. Tits, Four presentations of Leech's lattice, *in* "Finite Simple Groups, II, Proceedings, London Math. Soc. Research Symposium, Durham, 1978" (M. J. Collins, Ed.), pp. 306–307, Academic Press, London/New York, 1980.
34. J. Tits, Quaternions over $\mathbb{Q}(\sqrt{5})$, Leech's lattice and the sporadic group of Hall–Janko, *J. Algebra* **63** (1980), 56–75.
35. B. B. Venkov, The classification of integral even unimodular 24-dimensional quadratic forms, *Trudy Mat. Inst. Steklov.* **148** (1978), 65–76; *Proc. Steklov Inst. Math.* **4** (1980), 1967–1974.
36. E. Witt, Theorie der quadratischen Formen in beliebigen Körpern, *J. Reine Angew. Math.* **176** (1937), 31–44.