On automorphisms of extremal even unimodular lattices.

GABRIELE NEBE

Lehrstuhl D für Mathematik, RWTH Aachen University, 52056 Aachen, Germany
nebe@math.rwth-aachen.de

The automorphism groups of the three known extremal even unimodular lattices of dimension 48 and the one of dimension 72 are determined using the classification of finite simple groups. Restrictions on the possible automorphisms of 48-dimensional extremal lattices are obtained. We classify all extremal lattices of dimension 48 having an automorphism of order m with $\varphi(m) > 24$. In particular the lattice P_{48n} is the unique extremal 48-dimensional lattice that arises as an ideal lattice over a cyclotomic number field.

Keywords: extremal even unimodular lattice, automorphism group, ideal lattices.

Mathematics Subject Classification 2010: 11H56, 11H06, 11H31

1. Introduction

Let L be an even unimodular lattice in Euclidean n-space $(\mathbb{R}^n, (,))$, so $(x, x) \in 2\mathbb{Z}$ for all $x \in L$ and $L = L^{\#} = \{x \in \mathbb{R}^n \mid (x, L) \subseteq \mathbb{Z}\}$. Then the theory of modular forms allows to upper bound the minimum

$$\min(L) := \min\{(x, x) \mid 0 \neq x \in L\} \leq 2 + 2\lfloor \frac{n}{24} \rfloor.$$

Extremal lattices are those even unimodular lattices L that achieve equality. Of particular interest are extremal even unimodular lattices L in the jump dimensions, the multiples of 24. There are only five extremal lattices known in jump dimensions: The Leech lattice Λ_{24} of dimension 24, three lattices P_{48p}, P_{48q}, P_{48n} of dimension 48 and one lattice Γ_{72} of dimension 72 ([10], [20], [22]). These five lattices realise the maximal known sphere packing density in these dimensions.

Up to dimension 24 one knows all even unimodular lattices, in particular the Leech lattice is the unique extremal lattice in dimension 24. A complete classification of all even unimodular lattices in dimension 48 seems to be impossible. The present paper narrows down the possible automorphisms of extremal 48-dimensional lattices L. It turns out that all primes that can occur as an order of some automorphism already occur for one of the three known examples. These primes are 47, 23 and all primes ≤ 13. Explicit computations allow to find all extremal lattices L with

an automorphism σ of order m such that $\varphi(m) > 24$ as well as those, where σ has order 46 and $\sigma^{23} \neq -1$. Section 3.2 uses the classification of finite simple groups to prove the structure of the automorphism groups of the three known 48-dimensional extremal lattices, Section 6 deals with Γ_{72}. Section 4 determines all possible primes p that might occur as the order of some automorphism σ of L together with their fixed lattice $F = \mathrm{Fix}_L(\sigma)$. It turns out that $\dim(F) \leq 22$ for odd primes p. For $p = 2$ either $F = 0$ or a rescaled version of a 24-dimensional unimodular lattice without roots, so $F \cong \sqrt{2}\Lambda_{24}$, or $F \cong \sqrt{2}O_{24}$, where O_{24} denotes the odd Leech lattice, the unique odd unimodular lattice of dimension 24 with minimum 3. This allows to conclude that the minimal polynomial of any automorphism $\sigma \in \mathrm{Aut}(L)$ of order m is divisible by the m-th cyclotomic polynomial Φ_m of degree $\varphi(m)$. Using ideal lattices as introduced in [5] extensive number theoretic computations in MAGMA [6] are applied to find all lattices L that have some automorphism $\sigma \in \mathrm{Aut}(L)$ of order m with $\varphi(m) > 24$. This proves the following theorem.

Theorem 1.1. *Let L be an extremal even unimodular lattice of dimension* 48 *and* $\sigma \in \mathrm{Aut}(L)$ *of order m such that $\varphi(m) > 24$. Then one of the following six possibilities occurs.*

- *$m = 120$ and $L \cong P_{48n}$*
- *$m = 132$ and $L \cong P_{48p}$*
- *$m = 69$ or $m = 138$ and $L \cong P_{48p}$*
- *$m = 47$ or $m = 94$ and $L \cong P_{48q}$*
- *$m = 65$ or $m = 130$ and $L \cong P_{48n}$*
- *$m = 104$ and $L \cong P_{48n}$*

2. Bounds on the Hermite function

This section recalls some basic notions in the geometric theory of lattices. For more details the reader is referred to the textbook [18]. The main purpose is to state the table displaying the bounds on the Hermite function obtained from [8].

Let $L = \bigoplus_{i=1}^{n} \mathbb{Z}B_i$ be a lattice in Euclidean space $(\mathbb{R}^n, (,))$ for some basis $B := (B_1, \ldots, B_n)$ with Gram matrix $G(B) := ((B_i, B_j))_{i,j=1}^{n}$. The determinant of L is the determinant of any of its Gram matrices, $\det(L) := \det(G(B))$. We denote by

$$\mathrm{Min}(L) := \{\ell \in L \mid (\ell, \ell) = \min(L)\}.$$

the set of minimal vectors of L. Its cardinality is known as the kissing number, as this is the number of spheres in the lattice sphere packing that touch one fixed sphere. The density of this sphere packing is maximal, if $\gamma(L)$ is maximal, where the Hermite function γ on the space of similarity classes of n-dimensional lattices assigns to L the value

$$\gamma(L) := \frac{\min(L)}{\det(L)^{1/n}}$$

The **Hermite constant** is

$$\gamma_n := \max\{\gamma(L) \mid L \text{ is an } n\text{-dimensional lattice}\}.$$

Explicit values for γ_n are only known for $n \leq 8$ and $n = 24$. The best known upper bounds on γ_n are given in [8]. Note that Cohn and Elkies work with the center density δ_n. One gets $\gamma_n = 4\delta_n^{2/n}$.

Table 1. Upper bounds b_n for γ_n.

n	b_n	n	b_n	n	b_n	n	b_n	n	b_n
7	1.8115	13	2.6494	19	3.3975	25	4.1275	31	4.8484
8	2	14	2.7759	20	3.5201	26	4.2481	32	4.9681
9	2.1327	15	2.9015	21	3.6423	27	4.3685	33	5.0877
10	2.2637	16	3.0264	22	3.7641	28	4.4887	34	5.2072
11	2.3934	17	3.1507	23	3.8855	29	4.6087	35	5.3267
12	2.5218	18	3.2744	24	4.0067	30	4.7286	36	5.4462

The **automorphism group** $\mathrm{Aut}(L) := \{\sigma \in O(\mathbb{R}^n, (,)) \mid \sigma(L) = L\}$ acts on $\mathrm{Min}(L)$. Taking matrices with respect to the lattice basis B, we obtain $\mathrm{Aut}(L) \leq \mathrm{GL}_n(\mathbb{Z})$ is a finite integral matrix group.

3. Extremal even unimodular lattices of dimension 48

3.1. *Ternary codes and unimodular lattices of dimension* 48

Two of the known extremal even unimodular lattices of dimension 48 are have a canonical construction as 2-neighbors of code lattices of extremal ternary codes. Let me recall Sloane's construction A:

Definition 3.1. *(see for instance [10, Chapter 7]) Let $(e_1, \ldots, e_n)$ be a p-frame in $\mathbb{R}^n$, i.e. $(e_i, e_j) = p\delta_{ij}$. For any code $C \leq (\mathbb{Z}/p\mathbb{Z})^n$ the code lattice is $A_p(C) := \{\frac{1}{p}\sum c_i e_i \mid (\bar{c}_1, \ldots, \bar{c}_n) \in C\}$ where $\bar{x} := x + p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z}$.*

Note that $A_p(C)$ contains the vectors e_i of norm p. To increase the minimum of the lattice one usually passes to a neighbor lattice as follows:

Definition 3.2. *([16]) Let L be an integral lattice and $v \in L \setminus 2L^{\#}$ such that (v, v) is a multiple of 4. Then*

$$L^{(v),2} := \langle \{\ell \in L \mid (v, \ell) \text{ even } \} \cup \{\frac{v}{2}\}\rangle_{\mathbb{Z}}$$

is called the 2-neighbor *of L defined by v.*

Note that the 2-neighbor is an integral lattice with the same determinant as L. If L is unimodular, then any unimodular lattice N such that $[L : N \cap L] = 2$ is obtained as some 2-neighbor of L (see [16]).

Recall that the minimum weight of a self-dual ternary code C of length 48 cannot exceed 15. C is called *extremal*, if this minimum weight is equal to 15 (see for instance

4   *Gabriele Nebe*

[17]). Extremal codes always contain a vector of weight 48, so we may replace C by some equivalent code to obtain that the all-ones vector $\mathbf{1} = (1, \ldots, 1) \in C$.

Theorem 3.3. *[17] Let C be an extremal self-dual ternary code of length 48 containing the all-ones vector. Then $\Lambda(C) := A_3(C)^{(v),2}$ is an extremal even unimodular lattice, where $v = \frac{1}{3}(e_1 + \ldots + e_{48}) \in A_3(C)$.*

The extremal ternary self-dual codes of length 48 are not completely classified yet. One knows two equivalence classes of such codes (see [10]): the Pless code P_{48} and the extended quadratic residue code Q_{48}. In fact [21] shows that these are the only such codes that have an automorphism of prime order $p \geq 5$:

Theorem 3.4. *[21] Let C be an extremal self-dual ternary code of length 48 such that $|\operatorname{Aut}(C)|$ is divisible by some prime $p \geq 5$. Then $C \cong Q_{48}$ or $C \cong P_{48}$. The monomial automorphisms groups are $\operatorname{Aut}(Q_{48}) \cong \operatorname{SL}_2(47)$ and $\operatorname{Aut}(P_{48}) \cong (\operatorname{SL}_2(23) \times C_2) : 2$.*

The extremal lattices obtained from extremal ternary codes can be characterized as follows:

Theorem 3.5. *An extremal even unimodular lattice L of dimension 48 is of the form $L = \Lambda(C)$ for some extremal ternary code C if and only if there is some $\beta \in L$ with $(\beta, \beta) = 12$ such that $N_6(\beta) := \{x \in \operatorname{Min}(L) \mid (x, \beta) = 6\}$ has cardinality 94.*

Proof. It is well known that any 2-neighbor M of L has minimum ≥ 3 and that the pairs of vectors $\pm v$ of norm 3 in M are pairwise orthogonal: This follows because any two vectors $v, w \in M \setminus L$ satisfy that both vectors $v \pm w \in M \cap L$ and hence

$$(v \pm w, v \pm w) = (v, v) + (w, w) \pm 2(v, w) \geq 6 \text{ or } v \pm w = 0.$$

Assume that there is such a $\beta \in L$. Then the neighbor $M := L^{(\beta),2}$ contains a 3-frame

$$\operatorname{Min}(M) = \{\pm \frac{\beta}{2}\} \cup \{x - \frac{\beta}{2} \mid x \in N_6(\beta)\}$$

and so M is a code lattice, $M = A_3(C)$ for some $C = C^{\perp} \leq \mathbb{F}_3^{48}$. Clearly M is an odd unimodular lattice with even sublattice $M \cap L$. Since $\min(M \cap L) \geq \min(L) = 6$, the code C contains no words of weight ≤ 12, so C is extremal.
For $L = \Lambda(C)$ the vector $\beta = 2e_1 \in L$ satisfies $(\beta, \beta) = 12$ and $N_6(\beta) = \{e_1 \pm e_j \mid j = 2, \ldots, 48\}$. $\qquad \square$

3.2. *The automorphism groups of the three known lattices*

In the literature one finds three extremal even unimodular lattices of dimension 48. Two of them (P_{48p} and P_{48q}) are constructed from the two known extremal ternary codes of length 48 as described in [17] (see Theorem 3.3). They appear in [10, Chapter 7, Example 9], where the authors refer to personal communications

with J. Thompson for the structure of the automorphism group of these lattices. Since the description there is slightly incorrect and no explicit construction of the automorphism groups is available in the literature, the construction of the automorphism groups is given in the next theorem. A third lattice (named P_{48n} by Neil Sloane) has been found by the author in [20], where it was proved that the normalizer of the subgroup $\mathrm{SL}_2(13)$ in $\mathrm{Aut}(P_{48n})$ is $(\mathrm{SL}_2(13) \mathsf{Y} \mathrm{SL}_2(5)).2^2$. Here Y denotes the central product, $\times$ the direct product, : a split extension, and . an extension that might be split or non-split. The elementary abelian group of order 2^a is abbreviated by 2^a. Using the classification of finite simple groups one may obtain the full automorphism group of these three lattices:

Theorem 3.6. $\mathrm{Aut}(P_{48p}) \cong \mathrm{SL}_2(23) \times S_3) : 2$ *of order* $72864 = 2^5 3^2 11 \cdot 23$.
$\mathrm{Aut}(P_{48q}) \cong \mathrm{SL}_2(47)$ *of order* $103776 = 2^5 3 \cdot 23 \cdot 47$.
$\mathrm{Aut}(P_{48n}) \cong (\mathrm{SL}_2(13) \mathsf{Y} \mathrm{SL}_2(5)).2^2$ *of order* $524160 = 2^7 3^2 5 \cdot 7 \cdot 13$.

Proof. Let L be one of the three 48-dimensional extremal even unimodular lattices from the theorem and let $G := \mathrm{Aut}(L)$ be its automorphism group. Then by construction G contains the corresponding group U from above as a subgroup. Explicit matrices generating these subgroups can be obtained from the database of lattices [23] and are used in the MAGMA computations below. Let $q = 23, 47, 13$ be the largest prime divisor of $|U|$. Then U contains a normal subgroup $\mathrm{SL}_2(q)$.
(A) We first show that $U = N_G(\mathrm{SL}_2(q))$ is the full normalizer in G of $\mathrm{SL}_2(q)$:
For $L = P_{48n}$, $q = 13$ this is [20, Theorem 5.3].
So let $L = P_{48q}$, $q = 47$. Then $N := \mathrm{SL}_2(47)$ acts on L with endomorphism ring $\mathbb{Z}[\frac{1+\sqrt{-47}}{2}]$. Using the sublattice algorithm [25] in MAGMA one computes that L has a unique $\mathbb{Z}N$-sublattice X of index 2. Since N is perfect it fixes all lattices between $X^{\#}$ and X and we obtain 3 invariant unimodular lattices

$$X < L, L', M < X^{\#}$$

with L' even of minimum 4 and M odd with $\min(M) = 3$. The minimal vectors of M form a 3-frame and hence $M = A_3(C)$ for some extremal ternary self-dual code C. With MAGMA we compute $\mathrm{Aut}(C) \cong \mathrm{SL}_2(47)$. Since $\mathrm{Aut}(M)$ permutes the 48 pairs of minimal vectors of M we obtain

$$\mathrm{Aut}(M) = \mathrm{Stab}_{C_2 \wr S_{48}}(M) = \mathrm{Aut}(C) \cong \mathrm{SL}_2(47).$$

The normalizer in $G = \mathrm{Aut}(L)$ of N has to act on the unique sublattice X and hence permutes the lattices $\{L, L', M\}$. These are pairwise non-isometric, so $N_G(N)$ stabilizes all three lattices, so $N_G(N) = \mathrm{Aut}(M) = N \cong \mathrm{SL}_2(47)$.
Now let $L = P_{48p}$. Let $N := \mathrm{SL}_2(23) \le \mathrm{Aut}(L)$. Then L has three $\mathbb{Z}N$-sublattices X_i of index 2, which are computed using the sublattice algorithm in MAGMA. The group U permutes these three lattices X_i transitively, so it is enough to show that $\mathrm{Stab}_{N_G(N)}(X_1) \le U$. As before there are three unimodular lattices $X_1 \le L, L', M \le X_1^{\#}$ between X_1 and its dual lattice. $L = P_{48p}$ is even of minimum 6, L' is even of minimum 4, and M is an odd lattice containing a 3-frame

6   *Gabriele Nebe*

of minimal vectors. Again $M = A_3(C)$ for some extremal ternary self-dual code C. With MAGMA we compute $\operatorname{Aut}(C) \cong (\operatorname{SL}_2(23) \times C_2) : 2$. This group is isomorphic to $\operatorname{Aut}(M)$, fixes the even sublattice X_1 of M and hence is isomorphic to $\operatorname{Stab}_{N_G(N)}(X_1)$.

(B) We now show that U (and hence also $G = \operatorname{Aut}(L)$) is a primitive rational matrix group if $L = P_{48p}$ or $L = P_{48n}$ and $U = \operatorname{SL}_2(47)$ has a unique system of imprimitivity whose stabiliser in $\operatorname{Aut}(P_{48q})$ is equal to U:

First assume that $L = P_{48q}$. Then $U = \operatorname{SL}_2(47)$ has a unique maximal subgroup of index ≤ 48, this is $C_{47} : C_{46}$ and of index 48 in U. The U-invariant 3-frame constructed above gives rise to the corresponding monomial representation of U. So if $G = \operatorname{Aut}(L)$ is imprimitive, then $U \leq G \leq C_2 \wr S_{48} = \operatorname{Aut}(F)$, where $F \cong \sqrt{3}\mathbb{Z}^{48}$ is the lattice generated by the U-invariant 3-frame. As before this implies that $G \leq \operatorname{Aut}(Q_{48}) \cong U$.

We now show that $U = (\operatorname{SL}_2(23) \times S_3) : 2 \leq \operatorname{Aut}(P_{48p})$ is a primitive matrix group by investigating the restriction of the natural representation $\Delta_{|S}$ to all subgroups S of index dividing 48. The restriction of Δ to the derived subgroup $\operatorname{SL}_2(23) \times C_3$ of U is rational irreducible, so the representation is not induced from a 24-dimensional representation of a (normal) subgroup of index 2. The rational constituents of $\Delta_{|\operatorname{SL}_2(23)}$ are of dimension 24 (see [9] or explicit MAGMA computation), so if the representation of U is rational imprimitive, then it is induced from a subgroup of U not containing $\operatorname{SL}_2(23)$. The unique such subgroup of index ≤ 24 has index 24 and is the normalizer N in U of a 23-Sylow subgroup of U, $N \cong (C_{46} : C_{11} \times S_3).2$. The restriction of of Δ to N has no composition factor of degree 2, so finally this shows that U is a primitive subgroup of $\operatorname{GL}_{48}(\mathbb{Q})$.

The group $\operatorname{SL}_2(13)$ has no maximal subgroup of index dividing 48. From this one easily concludes that the group $U = (\operatorname{SL}_2(13) \mathsf{Y} \operatorname{SL}_2(5)).2^2$ is a primitive rational matrix group and so is $\operatorname{Aut}(P_{48n})$.

(C) Now assume that $G = \operatorname{Aut}(L)$ is a primitive subgroup of $\operatorname{GL}_{48}(\mathbb{Q})$:

Then all abelian normal subgroups of G are cyclic. A theorem of Ph. Hall (see [15, p. 357]) classifies all p-groups whose abelian characteristic subgroups are cyclic (these are central products of extraspecial p-groups with cyclic, dihedral, quaternion or quasidihedral groups). The relevant 2-groups (resp. 3-groups) that have a rational representation of dimension dividing 16 (resp. 6) do not allow a non-trivial $\operatorname{SL}_2(q)$ action by automorphisms ($q = 13, 23, 47$). Therefore we know that $O_2(G) = \langle -I_{48} \rangle$ and $O_3(G) = O_3(U)(= C_3$ or $1)$ centralise $\operatorname{SL}_2(q)$. If $G \neq U$ then G has to contain a quasisimple proper overgroup of $\operatorname{SL}_2(q)$. The tables in Hiss and Malle [14] (which use the classification of finite simple groups) exclude such overgroups inside $\operatorname{GL}_{48}(\mathbb{Q})$. □

Remark 3.7. The rational normaliser of the group $G = (\operatorname{SL}_2(13) \mathsf{Y} \operatorname{SL}_2(5)).2^2 = \operatorname{Aut}(P_{48n})$ acts transitively on the G-invariant lattices in $\mathbb{Q}P_{48n}$ (see [19]). So all $\mathbb{Z}G$-lattices in this space are similar to P_{48n}, therefore G is maximal finite in $\operatorname{GL}_{48}(\mathbb{Q})$.

3.3. *Identifying new lattices*

It is very hard, if not impossible with the present computing power, to check isometry of two extremal 48-dimensional even unimodular lattices, if nothing else but the Gram matrix is given. In this subsection I describe the computation of an explicit isometry between such lattices using a given subgroup U of order 48 of the automorphism group.

In [13] the authors construct two extremal even unimodular lattices $A_{14}(C_{14,48})$ and $A_{46}(C_{46,48})$ of dimension 48 as code lattices of self-dual codes of length 48. From the construction of the codes with weighing matrices one also obtains a group U of order 48 (the monomial automorphism group of the codes $C_{2p,48} \leq (\mathbb{Z}/2p\mathbb{Z})^{48}$, with monomial entries ± 1).

Theorem 3.8. $A_{14}(C_{14,48}) \cong P_{48n}$ *and* $A_{46}(C_{46,48}) \cong P_{48p}$.

Proof. Let L be one of the code lattices $A_{14}(C_{14,48})$ or $A_{46}(C_{46,48})$ and U be the known subgroup of $\mathrm{Aut}(L)$ coming from the construction with codes. The group U determines a sublattice $M \leq L$ as the full preimage of the fixed space $\mathrm{Fix}_U(L/2L)$ of the action of U on $L/2L$. The lattice M contains $2L$ of index 2^2, it has minimum norm 16 and kissing number 7200 and it is spanned by its minimal vectors. The automorphism group of M has order 96.

The group U has a normal subgroup $\langle\sigma\rangle$ of order 3. For both lattices $\mathrm{Fix}_L(\sigma) \cong \sqrt{3}(E_8 \perp E_8)$ and the orthogonal lattice is a 32-dimensional lattice of determinant 3^{16} and minimum norm 6. Its automorphism group has order $2^8 3^9$ for $A_{14}(C_{14,48})$ and $2^8 3^6 5$ for $A_{46}(C_{46,48})$.

To find candidates among the three known lattices that might be isometric to L we first find suitable elements of order 3 in the known automorphism groups. To this aim we compute representatives of all conjugacy classes of elements in G with Magma together with their minimal polynomial and their fixed lattice: The group $G := \mathrm{Aut}(P_{48p})$ contains 2 conjugacy classes of elements σ of order 3 with a 16-dimensional fixed lattice. In both cases the automorphism group of the orthogonal lattice has order $2^8 3^6 5$. The elements σ may be distinguished by the order of the normaliser $N_G(\langle\sigma\rangle)$ with is either 288 or 144. In the second case this normalizer contains a unique subgroup U_p with $\sigma \in U_p$ such that U_p is isomorphic (as an abstract group) to U. We take this group U_p compute the lattice M_p as full preimage of the fixed space $\mathrm{Fix}_{U_p}(P_{48p}/2P_{48p})$. We compute an isometry between this lattice M_p and the sublattice M of $A_{46}(C_{46,48})$. This isometry turns out to map P_{48p} onto the lattice $A_{46}(C_{46,48})$.

Also the group $G := \mathrm{Aut}(P_{48n})$ contains 2 conjugacy classes of elements σ of order 3 with a 16-dimensional fixed lattice. Here the automorphism groups of the orthogonal lattices have order $2^8 3^9$ respectively $2^{15} 3^9 5^2$. The normaliser $N_G(\langle\sigma\rangle)$ of the first element σ contains two subgroups U_n with $\sigma \in U_n$ such that U_n is isomorphic (as an abstract group) to U. Only for one of these groups U_n the lattice M_n (the full preimage of the fixed space $\mathrm{Fix}_{U_n}(P_{48n}/2P_{48n})$) is isometric to the lattice M

constructed from $A_{14}(C_{14,48})$. Again the isometry turns out to map P_{48n} onto the lattice $A_{14}(C_{14,48})$. □

4. Automorphisms of unimodular lattices

Let $\sigma \in \mathrm{GL}_n(\mathbb{Q})$ be some element of prime order p. Let $K := \ker(\sigma - 1)$ and $I := \mathrm{im}(\sigma - 1)$. Then K is the fixed space of σ and the action of σ on I gives rise to a vector space structure of I over the p-th cyclotomic number field $\mathbb{Q}[\zeta_p]$. In particular $n = d + z(p-1)$, where $d := \dim_{\mathbb{Q}}(K)$ and $z = \dim_{\mathbb{Q}[\zeta_p]}(I)$.

If L is some σ-invariant $\mathbb{Z}$-lattice, then L contains a sublattice M with

$$L \geq M := (L \cap K) \oplus (L \cap I) = L_K(\sigma) \oplus L_I(\sigma) \geq pL$$

of finite index $[L : M] = p^s$ where $s \leq \min(d, z)$. The fixed lattice $L_K(\sigma)$ is sometimes also denoted by $\mathrm{Fix}(\sigma) = \mathrm{Fix}_L(\sigma)$.

Definition 4.1. *The tuple* $p - (z, d) - s$ *is called the* type *of the element* $\sigma \in \mathrm{GL}(L)$.

Remark 4.2. The type is an invariant of the $\mathbb{Z}_p[\sigma]$-module $\mathbb{Z}_p L$. The group ring $\mathbb{Z}_p[\sigma]$ has three indecomposable lattices, the trivial module $\mathbb{Z}_p$, the regular module $\mathbb{Z}_p[\sigma]$ and the irreducible lattice $\mathbb{Z}_p[\zeta_p]$ of degree $p - 1$ (see for instance [26]). If σ is of type $p - (z, d) - s$ then $\mathbb{Z}_p L \cong \mathbb{Z}_p[\sigma]^s \oplus \mathbb{Z}_p^{d-s} \oplus \mathbb{Z}_p[\zeta_p]^{z-s}$.

We now assume that we fix some σ-invariant positive definite symmetric bilinear form F. Since there are no non-zero σ-invariant homomorphisms between K and I, the decomposition above is orthogonal with respect to F, $\mathbb{Q}^n = K \perp I$.

Lemma 4.3. *Let* $L = L^{\#}$ *be a unimodular lattice and* $\sigma \in \mathrm{Aut}(L)$ *be of type* $p - (z, d) - s$. *Then*

    a) $0 \leq s \leq \min(z, d)$.
    b) *If* $s = 0$ *then* L *is the orthogonal sum* $L = L_K(\sigma) \perp L_I(\sigma)$.
    c) $L_K(\sigma)^{\#}/L_K(\sigma) \cong L_I(\sigma)^{\#}/L_I(\sigma) \cong (\mathbb{Z}/p\mathbb{Z})^s$ *as abelian groups.*
    d) $z \equiv s \pmod 2$.

Proof. b) is trivial and c) is well known, see for instance [18, Prop. 1.9.8].
To see the upper bound in a) put $L_K := L_K(\sigma)$ and $L_I := L_I(\sigma)$. Let $\pi_K := \frac{1}{p}(1 + \sigma + \ldots + \sigma^{p-1})$ denote the orthogonal projection onto K and $\pi_I = 1 - \pi_K$ the one onto I. Then π_I and π_K commute with σ, $\sigma\pi_K = \pi_K$ and hence $(1 - \sigma)\pi_I = (1 - \sigma)(1 - \pi_K) = 1 - \sigma$. The lattice $L_I = I \cap L$ contains $(1 - \sigma)L$. We show that $(1 - \sigma)$ annihilates the quotient $L_I^{\#}/L_I$. Since $L = L^{\#}$ the dual lattice of L_I is $L_I^{\#} = \pi_I(L)$. Therefore

$$(1 - \sigma)L_I^{\#} = (1 - \sigma)\pi_I(L) = (1 - \sigma)L \subseteq L_I.$$

Therefore $L_I^{\#}/L_I$ is a quotient of $L_I^{\#}/(1 - \sigma)L_I^{\#} \cong \mathbb{F}_p^z$, so $s \leq z$. Similarly

$$L_K^{\#} = \pi_K(L) \supseteq L_K = \pi_K(L) \cap L \supseteq p\pi_K(L)$$

and hence $s \leq d$.

To obtain d) we consider the image $I = \mathrm{im}(\sigma - 1)$. This is of dimension z over $\mathbb{Q}[\zeta_p]$ and $L_I := L_I(\sigma)$ is a $\mathbb{Z}[\zeta_p]$-lattice in I. Since F is σ-invariant, there is some positive definite Hermitian form $h : I \times I \to \mathbb{Q}[\zeta_p]$ so that $F(x,y) = \mathrm{trace}_{\mathbb{Q}[\zeta_p]/\mathbb{Q}}(h(x,y))$ for all $x, y \in I$. Choose some orthogonal basis $(b_1, \ldots, b_z)$, so that $h(b_i, b_j) = a_i \delta_{ij}$ with $a_i \in \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ and put $\mathcal{M} := \langle b_1, \ldots, b_z \rangle_{\mathbb{Z}[\zeta_p]}$ the $\mathbb{Z}[\zeta_p]$-lattice spanned by this basis. Let M be $\mathcal{M}$ viewed as a $\mathbb{Z}$-lattice together with the positive definite symmetric bilinear form F. Then the $\mathbb{Z}$-dual lattice $M^{\#}$ with respect to F is

$$M^{\#} = \langle \frac{1}{a_1 (1 - \zeta_p)^{p-2}} b_1, \ldots, \frac{1}{a_z (1 - \zeta_p)^{p-2}} b_z \rangle_{\mathbb{Z}[\zeta_p]}$$

and in particular $\det(M, F) = |M^{\#}/M| = p^{z(p-2)} \prod_{i=1}^{z} N_{\mathbb{Q}[\zeta_p]/\mathbb{Q}}(a_i)$. Since the norm $N_{\mathbb{Q}[\zeta_p]/\mathbb{Q}}(a_i) = N_{\mathbb{Q}[\zeta_p + \zeta_p^{-1}]/\mathbb{Q}}(a_i)^2$ is a rational square, the square class of the determinant of F is $p^z (\mathbb{Q}^*)^2$. In particular $\det(L_I) p^z = p^{s+z}$ is a square so $s \equiv z$ (mod 2). $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Note that for odd primes p there is at most one genus of even p-elementary lattices of given dimension and determinant ([10, Theorem 13, p. 386]). So the type of σ uniquely determines the genus of $L_K(\sigma)$ and $L_I(\sigma)$.

4.1. *Prime order automorphisms of 48-dimensional extremal lattices*

In this section, L is always an extremal even unimodular lattice of dimension 48. We list the possible types of automorphisms $\sigma \in \mathrm{Aut}(L)$ of prime order.

Theorem 4.4. *Let L be an extremal even unimodular lattice of dimension 48. Assume that $\sigma \in \mathrm{Aut}(L)$ is of prime order $p \geq 11$. Then σ is of type*

$$47 - (1,2) - 1, \; 23 - (2,4) - 2, \; 13 - (4,0) - 0, \; 11 - (4,8) - 4$$

and the fixed lattice $L_K(\sigma)$ is the unique extremal p-modular lattice of dimension $2, 4, 0,$ and 8. Its Gram matrix is F_p with

$$F_{47} = \begin{pmatrix} 6 & 1 \\ 1 & 8 \end{pmatrix}, \; F_{23} = \begin{pmatrix} 6 & 3 & 2 & 2 \\ 3 & 6 & 2 & 0 \\ 2 & 2 & 6 & 3 \\ 2 & 0 & 3 & 6 \end{pmatrix}, \; F_{11} = \begin{pmatrix} 6 & \text{-}2 & 1 & 3 & 2 & 0 & 3 & \text{-}1 \\ \text{-}2 & 6 & 3 & 1 & \text{-}2 & 1 & 1 & 0 \\ 1 & 3 & 6 & 3 & 0 & 3 & 3 & 2 \\ 3 & 1 & 3 & 6 & 2 & 3 & 3 & 2 \\ 2 & \text{-}2 & 0 & 2 & 6 & 3 & 3 & 3 \\ 0 & 1 & 3 & 3 & 3 & 6 & 3 & 3 \\ 3 & 1 & 3 & 3 & 3 & 3 & 6 & 2 \\ \text{-}1 & 0 & 2 & 2 & 3 & 3 & 2 & 6 \end{pmatrix}.$$

All these automorphisms occur for one of the three known extremal even unimodular lattices.

Proof. Clearly $\varphi(p) = p - 1 \leq 48$ implies that the prime p is at most 47. We abbreviate $L_K := L_K(\sigma)$, $L_I := L_I(\sigma)$ and denote the type of σ by $p - (z, d) - s$. Since L is not an orthogonal sum we have $s > 0$ if $d \neq 0$.

$\underline{p = 47}$: Then $d = 2$ and $z = 1$. The fixed lattice L_K is a 2-dimensional even lattice of minimum ≥ 6, determinant 47. This immediately implies that L_K has Gram matrix F_{47}.

$\underline{43 \geq p \geq 29}$: Since $p - 1 > 24$ we obtain $z = 1$ in all cases, $d = 48 - (p - 1)$, and L_K is a d-dimensional lattice of determinant p (see Lemma 4.3 d)). In all cases ($p = 43, 41, 37, 31$, and 29) the density of L_K validates the bounds from [8] given in Section 2.

$\underline{p = 23}$: Then the type of σ is either $23 - (2, 4) - 2$ or $23 - (1, 26) - 1$. The latter case easily gives a contradiction to the bounds in Section 2. In the other case, $\dim(L_K) = 4$, $\min(L_K) \geq 6$, and $\det(L_K) = 23^2$, so L_K is in the genus of the even 23-modular lattices. By [27] this genus contains a unique lattice of minimum ≥ 6. This lattice has Gram matrix F_{23} as claimed.

$\underline{p = 19}$: Then the type of σ is either $19 - (2, 12) - 2$ and L_K is a 12-dimensional lattice of determinant 19^2 and minimum 6 or σ has type $19 - (1, 30) - 1$ and L_I is an 18-dimensional lattice of determinant dividing 19 and minimum 6. Both cases validate the bound in [8] given in Section 2.

$\underline{p = 17}$: Since the kissing number of L is $2^9 3^2 5^3 7 \cdot 13$ which is not a multiple of 17, the automorphism σ can not act fixed point freely. This also follows from Lemma 4.3. So the type of σ is either $17 - (2, 16) - 2$ or $17 - (1, 32) - 1$. In the first case L_K and in the second case L_I is a 16-dimensional lattice of determinant dividing 17^2 and minimum ≥ 6 contradicting the bound in [8] given in Section 2.

$\underline{p = 13}$: Then the type of σ is either $13 - (4, 0) - 0$ (which occurs as an element of $\mathrm{Aut}(P_{48n})$), or $13 - (3, 12) - s$ with $s \leq 3$ and L_K is a 12-dimensional lattice of determinant dividing 13^3 and minimum 6, or $13 - (2, 24) - 2$ and L_K is a 24-dimensional lattice of determinant 13^2 and minimum 6, or $13 - (1, 36) - 1$ and L_I is a 12-dimensional lattice of determinant 13 and minimum 6. The latter three cases contradict the bounds in [8] given in Section 2.

$\underline{p = 11}$: Then the type of σ is either $11 - (4, 8) - s$ with $s \leq 4$, or $11 - (3, 18) - s$ with $s \leq 3$ and L_K is a 18-dimensional lattice of determinant dividing 11^3 and minimum 6, or $11 - (2, 28) - 2$ and L_K is a 22-dimensional lattice of determinant 11^2 and minimum 6, or $11 - (1, 38) - 1$ and L_I is a 10-dimensional lattice of determinant 11 and minimum 6. The latter three cases contradict the bounds in [8] given in Section 2. In the first case, these bounds imply that $s = 4$. Hence L_K is in the genus of 11-modular 8-dimensional lattices. By [27] this genus contains a unique lattice of minimum ≥ 6. This lattice has Gram matrix F_{11} as claimed. $\qquad\square$

Proposition 4.5. *Let $\sigma \in \mathrm{Aut}(L)$ be of order 7. Then either the type of σ is $7 - (8, 0) - 0$ or the type is $7 - (7, 6) - 5$ with fixed lattice $L_K(\sigma) \cong \sqrt{7} A_6^{\#}$.*

Proof. Clearly the type of σ is $7 - (8 - a, 6a) - s$ with $s \leq 8 - a$. For $a \geq 3$ one

obtains a contradiction since the density of one of the lattices $L_K := L_K(\sigma)$ or $L_I := L_I(\sigma)$ exceeds the bounds in [8]. For $a = 2$ these bounds allow the possibility that $\det(L_K) = 7^6$. Then L_K is a 12-dimensional even 7-elementary lattice in the genus of the 7-modular lattices. The complete enumeration of this genus in [27] has proved that all such lattices have minimum ≤ 4. In the case $a = 1$ the lattice L_K is of dimension 6, even, 7-elementary. One concludes that $s = 5$ and $L_K \cong \sqrt{7} A_6^{\#}$ because A_6 is the only even 6-dimensional lattice of determinant 7.   □

Using the bounds in [8] and Lemma 4.3 we get the following possible types for automorphisms of order 5.

Remark 4.6. Let $\sigma \in \mathrm{Aut}(L)$ be of order 5. Then the type of σ is either $5 - (12,0) - 0$, $5 - (10,8) - 8$, $5 - (10,8) - 6$, $5 - (9,12) - 9$, $5 - (9,12) - 7$, $5 - (8,16) - 8$, or $5 - (7,20) - 7$.

Excluding some cases in this remark we obtain the following proposition:

Proposition 4.7. *Let* $\sigma \in \mathrm{Aut}(L)$ *be of order 5. Then the type of* σ *is either* $5 - (12,0) - 0$, $5 - (10,8) - 8$ *with* $L_K(\sigma) \cong \sqrt{5} E_8$ *or* $5 - (8,16) - 8$ *with* $L_K(\sigma) \cong [2.\,\mathrm{Alt}_{10}]_{16}$.

Proof. For the type $5 - (10,8) - 8$, the fixed lattice is $\sqrt{5} U$ for some 8-dimensional even unimodular lattice U, so $L_K(\sigma) \cong \sqrt{5} E_8$. A MAGMA computation shows that no overlattice of index 5 of this lattice has minimum ≥ 6 ($\mathrm{Aut}(E_8)$ has 8 orbits on the one-dimensional subspaces of $E_8 / 5 E_8$), which excludes type $5 - (10,8) - 6$.
For the type $5 - (8,16) - 8$, the fixed lattice is in the genus of the even 5-modular 16-dimensional lattices. By [4, Theorem 8.1] this genus contains a unique lattice of minimum 6, denoted by $[2.\,\mathrm{Alt}_{10}]_{16}$ in [24].
To exclude the types $5 - (9,12) - a$ for $a = 9, 7$, it is enough to enumerate the genus of $\sqrt{5}(A_4 \perp A_4 \perp A_4)^{\#}$ (determinant 5^9, dimension 12) and note that all 15 isometry classes of lattices in this genus have minimum ≤ 4.
In the last case $5 - (7,20) - 7$ the lattice $L_I(\sigma)$ is the dual of some unimodular Hermitian $\mathbb{Z}[\zeta_5]$-lattice of dimension 7. A complete enumeration of the genus shows that the class number is 20 and all lattices have minimum ≤ 4.   □

Proposition 4.8. *Let* $\sigma \in \mathrm{Aut}(L)$ *be of order 3. Then the type of* σ *is either* $3 - (24,0) - 0$, $3 - (20,8) - 8$ *with* $L_K(\sigma) \cong \sqrt{3} E_8$, $3 - (18,12) - 12$ *with* $L_K(\sigma) \cong \sqrt{3} D_{12}^{+}$, $3 - (16,16) - 16$ *with* $L_K(\sigma) \cong \sqrt{3}(E_8 \perp E_8)$ *or* $L_K(\sigma) \cong \sqrt{3} D_{16}^{+}$, *type* $3 - (15,18) - 15$ *(two possibilities for* L_I, L_K *is unique), type* $3 - (14,20) - 14$ *(* L_I *unique), or type* $3 - (13,22) - 13$ *(* L_I *unique).*

Proof. Put $L_K := L_K(\sigma)$, $L_I := L_I(\sigma)$. Most of the possible types are excluded from the bounds in [8] using Lemma 4.3. So I only comment on the cases, where these bounds do allow lattices of minimum 6. These are
$\underline{3 - (19,10) - 9}$: Then L_K is in the genus of $\sqrt{3} E_8 \perp A_2$. This genus contains only

$\sqrt{3}E_8 \perp A_2$, so $\min(L_K) = 2 < 6$ is a contradiction.

$\underline{3 - (18, 12) - 10}$: Then the lattice L_K is an overlattice of index 3 of $\sqrt{3}D_{12}^+$. One computes that the automorphism group of D_{12}^+ has 13 orbits on these lattices, none of them has minimum 6.

$\underline{3 - (17, 14) - 13}$: Then the lattice L_K is in the genus of $\sqrt{3}(E_8 \perp E_6^\#)$. This genus contains 2 isometry classes, both lattices have minimum 4. This also excludes the type $3 - (17, 14) - 11$, since then L_K contains one of the latter two lattices.

To exclude the cases $\underline{3 - (16, 16) - s}$ for $s = 14, 12, 10$ we need to compute overlattices of index 3 of the rescaled unimodular lattices $\sqrt{3}(E_8 \perp E_8)$ and $\sqrt{3}D_{16}^+$. The automorphism group of the first lattice has 14 orbits, the other one 17 orbits on the overlattices of index 3, none of the lattices has minimum 6.

$\underline{\text{types}}$: $3 - (15, 18) - a$, $a = 15, 13, 11$, $3 - (14, 20) - a$, $a = 14, 12, 10$, $3 - (13, 22) - a$, $a = 13, 11$, $3 - (12, 24) - a$, $a = 12, 10$, $3 - (11, 26) - 11$, and $3 - (10, 28) - 10$:

In all cases the lattice L_I is or contains an Hermitian unimodular lattice of dimension $z = 10, \ldots, 15$. These lattices have been classified by Feit, Abdukhalikov, and Scharlau [11], [1], [2]. For lattices of minimum 6 one obtains one lattice, L_{13}, of dimension $2z = 26$, one lattice, L_{14}, of dimension $2z = 28$, and two such lattices, L_{15}, M_{15}, of dimension $2z = 30$.

This excludes the cases $z = 10, 11, 12$.

The group $\mathrm{Aut}(L_{13})$ has 2 orbits on the set of integral overlattices of index 3 of L_{13}, one has minimum 2 and the other minimum 4. So $L_I = L_{13}$ and only the type $3 - (13, 22) - 13$ is possible here.

The group $\mathrm{Aut}(L_{14})$ has 5 orbits on the set of integral overlattices of index 3 of L_{14}, one with minimum 2, the other 4 with minimum 4. So $L_I = L_{14}$ and only the type $3 - (14, 22) - 14$ is possible here.

The group $\mathrm{Aut}(L_{15}) \cong \pm 3.U_4(3).2$ has 13 orbits on the set of integral overlattices of index 3 of L_{15}, again none of these overlattices has minimum ≥ 6.

The group $\mathrm{Aut}(M_{15}) \cong \pm(3_+^{1+2} \times 3_+^{1+2}).\mathrm{SL}_2(3).2$ has 174 orbits on the set of integral overlattices of index 3 of M_{15}, again none of these overlattices has minimum ≥ 6. $\square$

Lemma 4.9. *Let M be an even lattice such that $M^\#/M$ has exponent 2. Then M contains a sublattice isometric to $\sqrt{2}U$ where $U = U^\#$ is an (even or odd) unimodular lattice.*

Proof. Since this is a statement about 2-adic lattices, we pass to $M_2 := \mathbb{Z}_2 \otimes M$. This lattice has a 2-adic Jordan decomposition $M_2 = f_{II} \oplus \sqrt{2}f$ where f_{II} is even and unimodular of dimension, say, $2m$, and f is unimodular. If $m = 0$, then $M \cong \sqrt{2}U$ for some unimodular U and we are done. So assume $m \geq 1$. Then f_{II} contains a vector v such that $(v, v) \in 2\mathbb{Z}_2^*$. Therefore f_{II} contains the sublattice $v \perp v^\perp$ of index 2, and $v \perp v^\perp \perp \sqrt{2}f$ has a Jordan decomposition $g_{II} \oplus \sqrt{2}g$ with $\dim(g) = \dim(f) + 2$ and $\dim(g_{II}) = 2(m-1)$. Since g_{II} is again even and unimodular, we may proceed by induction. $\square$

Note that the possible genera of such lattices are given in [10, Table 15.5, p. 388] and one can easily find lattices representing these genera and also give a case by case proof of the lemma.

Theorem 4.10. *Let* $-1 \neq \sigma \in \mathrm{Aut}(L)$ *be of order* 2. *Then* σ *is of type* $2-(24,24)-24$ *and*

$$\mathrm{Fix}_L(\sigma) \perp \mathrm{Fix}_L(-\sigma) \cong \sqrt{2}(\Lambda_{24} \perp \Lambda_{24}) \ or \ \sqrt{2}(O_{24} \perp O_{24}).$$

Both cases occur.

Proof. Both lattices $L_K := L_K(\sigma)$ and $L_I := L_K(-\sigma)$ satisfy that

$L_K^{\#}/L_K \cong L_I^{\#}/L_I$ has exponent $2, \min(L_K) \geq 6, \min(L_I) \geq 6, L_I$ and L_K even.

By Lemma 4.9 all such lattices contain some lattice $\sqrt{2}U$ with $U = U^{\#}$. Since there is no unimodular lattice U of dimension $n \leq 22$ or of dimension 25 (see [10, Table 16.7, p. 416-417] and [7]) with $\min(U) \geq 3$ this implies that $\dim(L_K) = 24$ and that L_K is an overlattice of either $\sqrt{2}\Lambda_{24}$ or $\sqrt{2}O_{24}$ where Λ_{24} and O_{24} denote the Leech lattice respectively the odd Leech lattice of dimension 24 (see [10, Table 16.1, p. 407] and [10, Table 17.1, p. 424-426]). All non-zero classes of $\frac{1}{\sqrt{2}}\Lambda_{24}/\sqrt{2}\Lambda_{24}$ are represented by vectors of norm 2,3,4, (see e.g. [10, Chapter 10, Theorem 28]) so $\sqrt{2}\Lambda_{24}$ has no overlattice of index 2 with minimum ≥ 6. The automorphism group of the odd Leech lattice has 16 orbits on the 1-dimensional subspaces of $\frac{1}{\sqrt{2}}O_{24}/\sqrt{2}O_{24}$. The minima of the corresponding overlattices are

$$\frac{3}{2}, 2 \ (2 \ \text{lattices}), \frac{5}{2}, 3 \ (2 \ \text{lattices}), \frac{7}{2} \ (2 \ \text{lattices}), 4 \ (5 \ \text{lattices}), \frac{9}{2} \ (2 \ \text{lattices}), 5.$$

In particular no proper overlattice of index 2 has minimum ≥ 6.
The case $\mathrm{Fix}_L(\sigma) \perp \mathrm{Fix}_L(-\sigma) \cong \sqrt{2}(O_{24} \perp \Lambda_{24})$ cannot occur, since the quadratic spaces $\frac{1}{\sqrt{2}}O_{24}/\sqrt{2}O_{24}$ and $\frac{1}{\sqrt{2}}\Lambda_{24}/\sqrt{2}\Lambda_{24}$ are not isometric. $\qquad\square$

From the previous discussion we found that the maximal dimension of the fixed lattice of an automorphism of L of odd prime order is ≤ 22. The nontrivial automorphism of order 2 have fixed lattices of dimension 24. From this fact we obtain the following corollary which is essentially for the computational approach in the next section.

Corollary 4.11. *Let* L *be an extremal even unimodular lattice of dimension* 48 *and* $\sigma \in \mathrm{Aut}(L)$ *of order* m. *Then the* m-*th cyclotomic polynomial* Φ_m *divides the minimal polynomial of* σ.

Proof. Assume that Φ_m does not divide the minimal polynomial of σ. Write $m = \prod_{i=1}^{s} p_i^{n_i}$ with pairwise distinct primes p_i and $n_i \in \mathbb{N}$. If Φ_m does not divide μ_σ, then $\Phi_{\prod_{i=1}^{s} p_i}$ does not divide the minimal polynomial of $\sigma^{\prod_{i=1}^{s} p_i^{n_i-1}}$ so we may restrict to automorphisms σ of square free order $m := \prod_{i=1}^{s} p_i$.

Table 2. The possible types of automorphisms of prime order p.

p	dim $L_K(\sigma)$	det($L_K(\sigma)$)	$L_K(\sigma)$	example
47	2	47	unique	P_{48q}
23	4	23^2	unique	P_{48q}, P_{48p}
13	0		$\{0\}$	P_{48n}
11	8	11^4	unique	P_{48p}
7	0		$\{0\}$	P_{48n}
7	6	7^5	$\sqrt{7}A_6^\#$	not known
5	0		$\{0\}$	P_{48n}
5	8	5^8	$\sqrt{5}E_8$	not known
5	16	5^8	$[2.\,\mathrm{Alt}_{10}]_{16}$	not known
3	0		$\{0\}$	P_{48p}, P_{48n}
3	8	3^8	$\sqrt{3}E_8$	not known
3	12	3^{12}	$\sqrt{3}D_{12}^+$	not known
3	16	3^{16}	$\sqrt{3}(E_8 \perp E_8)$	$P_{48p}, P_{48q}, P_{48n}$
3	16	3^{16}	$\sqrt{3}D_{16}^+$	not known
3	18	3^{15}	unique	not known
3	20	3^{14}	$L_I(\sigma)$ unique	not known
3	22	3^{13}	$L_I(\sigma)$ unique	not known
2	0		$\{0\}$	$\sigma = -1$
2	24	2^{24}	$\sqrt{2}\Lambda_{24}$	P_{48n}
2	24	2^{24}	$\sqrt{2}O_{24}$	P_{48n}, P_{48p}

We proceed by induction on the number of prime divisors s and assume that s is minimal, i.e. for all i the minimal polynomial of σ^{p_i} is a multiple of Φ_{m/p_i}.

If $s = 1$, there is nothing to show.

If $s = 2$, then $\Phi_{p_1}\Phi_{p_2}\Phi_1$, in particular $\mathrm{Fix}(\sigma^{p_1}) + \mathrm{Fix}(\sigma^{p_2})$ generates $\mathbb{R}^{48}$. By the results in this section the maximal dimension of a fixed space of any element in $\mathrm{Aut}(L)$ (of prime order) is 24, and for all elements of odd prime order the dimension of the fixed space is at most 22. So $\dim(\mathrm{Fix}(\sigma^{p_1}) + \mathrm{Fix}(\sigma^{p_2})) \leq 46$, a contradiction. So assume that $s \geq 3$. Write $\sigma = \sigma_1 \ldots \sigma_s$ so that σ_i has order p_i. Clearly for all i the restriction γ_i of $\prod_{j \neq i} \sigma_j$ to $L_I(\sigma_i)$ has a minimal polynomial that is not divisible by $\Phi_{\prod_{j \neq i} p_j}$. By the minimality of s the order of γ_i is $\prod_{j \neq i} p_j$. As neither the Leech lattice Λ_{24} nor the odd Leech lattice O_{24} admit such an automorphism (of odd order) this shows that m is odd. As the possible fixed lattices of the elements of order $q = 23, 11, 7$ do not admit an automorphism of order $p \neq q$ with $p \geq 7$, only one of these primes can occur in $\{p_1, \ldots, p_s\}$ which shows that $s = 3$, $\{p_1, p_2, p_3\} = \{3, 5, q\}$ and Φ_{5q} of degree $4(q-1) \geq 24$ divides μ_σ. But then the fixed lattice of the element σ^{5q} (which has order 3) has dimension ≥ 24, which is a contradiction.   □

Corollary 4.12. *Let L be an extremal even unimodular lattice of dimension 48. Then any element σ of order 2^5 in $\mathrm{Aut}(L)$ acts with irreducible minimal polynomial and $\mathrm{Aut}(L)$ contains no elements of order 2^6, $2^5 3$, $2^4 5$, or $2^3 11$.*

Proof. First assume that $\sigma \in \mathrm{Aut}(L)$ has order 2^5. Since $\varphi(2^5) = 16$ and also $\dim(L) = 48$ is a multiple of 16, also the dimension of the fixed lattice $\mathrm{Fix}_L(\sigma^{2^4})$

is a multiple of 16. By Theorem 4.10 this is only possible, if $\operatorname{Fix}_L(\sigma^{2^4}) = \{0\}$ so $\sigma^{2^4} = -1$.

Now assume that $\sigma \in \operatorname{Aut}(L)$ has order 2^6. Then σ^2 acts with irreducible minimal polynomial, contradicting the fact that $\varphi(2^6) = 32$ does not divide $\dim(L) = 48$.

Now let $|\langle\sigma\rangle| = 2^5 3$. Then σ^3 acts with an irreducible minimal polynomial on L, so the type of σ^{2^5} is $3 - (z,d) - s$ with z and d both divisible by 16. By Proposition 4.8 this yields that this type is $3 - (16,16) - 16$ and $\operatorname{Fix}_L(\sigma^{2^5})$ is either $\sqrt{3}(E_8 \perp E_8)$ or $\sqrt{3}D_{16}^+$. With Magma we check that both lattices admit no automorphism of order 32.

Now let $|\langle\sigma\rangle| = 2^4 5$ and put $\tau := \sigma^{2^3 5}$. Then τ is an element of order 2 in $\operatorname{Aut}(L)$. If $\tau \neq -1$ then by Theorem 4.10 both lattices $\operatorname{Fix}_L(\tau)$ and $\operatorname{Fix}_L(-\tau)$ are either similar to Λ_{24} or to O_{24}. By Proposition 4.7 one sees that σ acts as an element of order 80 on $\operatorname{Fix}_L(-\tau)$. Neither $\operatorname{Aut}(\Lambda_{24})$ nor $\operatorname{Aut}(O_{24})$ contain elements of order 80.

Therefore $\tau = -1$, so σ^5 acts with irreducible minimal polynomial. As above this implies that the type of σ^{2^4} is $5 - (z,d) - s$ with z and d both divisible by 8. By Proposition 4.7 this implies that $\operatorname{Fix}_L(\sigma^{2^4}) = L_K \cong [2.\operatorname{Alt}_{10}]_{16}$. With Magma one checks that $\operatorname{Aut}(L_K) \cong 2.\operatorname{Alt}_{10}$ does not contain an element of order 16.

Finally let σ be of order $2^3 11$, $L_K := L_K(\sigma^8)$ and $L_I := L_I(\sigma^8)$. Since $\operatorname{Aut}(L_K)$ does not contain an element of order 8, the element σ acts with an irreducible minimal polynomial on L_I (which is hence an ideal lattice in the 88-th cyclotomic number field). But then $L_K = L_K(\sigma^{44})$ contradicting Theorem 4.10 (and also the fact that L_K has determinant 11^4). $\qquad\qquad\square$

5. Lattices with a given automorphism

This section describes some explicit Magma computations enumerating all extremal even unimodular lattices that admit a certain automorphism. In particular we classify all extremal even unimodular lattices L of dimension 48 that admit an automorphism σ of order m with $\varphi(m) > 24$.

5.1. *Certain automorphisms of order* 46

Theorem 5.1. *Let L be an extremal even unimodular lattice of dimension 48 such that $\operatorname{Aut}(L)$ contains an element σ of order 46 such that $\sigma^{23} \neq -1$. Then $L \cong P_{48p}$.*

Proof. Let $L_K := L_K(\sigma^{23})$ and $L_I := L_K(-\sigma^{23})$. From Theorem 4.10 one concludes that $L_K \cong L_I \cong \sqrt{2}\Lambda_{24}$ or $L_K \cong L_I \cong \sqrt{2}O_{24}$. The automorphism group of the Leech lattice $\operatorname{Aut}(\Lambda_{24}) = 2.Co_1$ and the odd Leech lattice $\operatorname{Aut}(O_{24}) \cong 2^{12}.M_{24}$ both contain two conjugacy classes of elements of order 23 represented by g and g^{-1}, say. By Theorem 4.4 the element σ^2 acts on $L_K \perp L_I$ as an automorphism of type $23 - (2,4) - 2$. So the conjugacy classes of such subgroups $\langle\sigma^2\rangle$ of order 23 in $\operatorname{Aut}(L_K \perp L_I)$ are represented by $\langle(g,g)\rangle$ and $\langle(g,g^{-1})\rangle$. With Magma we

compute the $\langle \sigma^2 \rangle$-invariant unimodular overlattices L of $L_K \perp L_I$ of minimum 6 for all 4 cases. Note that $\frac{1}{2}(L_K \perp L_I)/(L_K \perp L_I)$ is a semisimple $\mathbb{F}_2\langle \sigma^2 \rangle$-module isomorphic to $S^4 \oplus V_1^2 \oplus V_2^2$ where $S \cong \mathbb{F}_2$ and $V_1, V_2 \cong \operatorname{Hom}_{\mathbb{F}_2}(V_1, \mathbb{F}_2)$ are the two non-isomorphic simple 11-dimensional $\mathbb{F}_2\langle \sigma^2 \rangle$-modules. Then $L/(L_K \perp L_I) \cong S^2 \oplus V_1 \oplus V_2$ can be reached in 2 steps: First we compute the unique lattice Y of minimum 6 with $Y/(L_K \perp L_I) \cong S^2$, by going through all 35 two-dimensional subspaces of $S^4 \cong \mathbb{F}_2^4$. We then go through the $(2^{11}-1)/23+2 = 91$ orbits of one-dimensional subspaces of $V_1 \perp V_1$ under the action of $\langle (1, g) \rangle \leq C_{\operatorname{Aut}(L_K \perp L_I)}(\sigma^2)$ to obtain candidates for the lattices Z of minimum 6 such that $Z/Y \cong V_1$. Then $Z^\#/Z \cong V_1 \oplus V_2$ and there is a unique unimodular overlattice W of Z with $W/Z \cong V_2$. Only for the case $L_K \cong \sqrt{2}O_{24}$ and $\langle \sigma^2 \rangle \cong \langle (g, g^{-1}) \rangle$ there is such a lattice W with $\min(W) = 6$. We check that $W \cong P_{48p}$ by computing a vector $\beta \in W$ fixed by σ^2 and of norm $(\beta, \beta) = 12$ such that the 2-neighbor $W^{(\beta),2}$ contains a 3-frame. The corresponding extremal ternary code is easily checked to be isometric to the Pless code P_{48}. $\qquad\square$

5.2. *Ideal lattices*

This section classifies all 48-dimensional extremal even unimodular lattices L that have an automorphism σ of order m such that $\varphi(m) = 48$. By Corollary 4.11 the minimal polynomial of σ is the m-th cyclotomic polynomial and hence L is an ideal lattice in the m-th cyclotomic number field $F = \mathbb{Q}[\zeta_m]$.

Remark 5.2. (see [5]) Let $\sigma \in \operatorname{Aut}(L)$ be an automorphism of the lattice L with characteristic polynomial Φ_m, the m-th cyclotomic polynomial. Then the action of σ on $\mathbb{Q}L$ turns the vector space $\mathbb{Q}L$ into a one-dimensional vector space over the m-th cyclotomic number field $F = \mathbb{Q}[\zeta_m]$ which we identify with F. Then the lattice L is a $\mathbb{Z}[\zeta_m]$-submodule, hence isomorphic to a fractional ideal J in F. The symmetric positive definite bilinear form $B : L \times L \to \mathbb{Q}$ is ζ_m-invariant, since $B(x\sigma, y\sigma) = B(x, y)$ for all $x, y \in L$. It hence corresponds to some trace form on the ideal J,

$$B(x, y) = \operatorname{trace}_{F/\mathbb{Q}}(\alpha x \overline{y}) = b_\alpha(x, y), \quad \text{for all } x, y \in J$$

where $\overline{}$ is the complex conjugation on F, the involution with fixed field $F^+ := \mathbb{Q}[\zeta_m + \zeta_m^+]$, and $\alpha \in F^+$ is totally positive, i.e. $\iota(\alpha) > 0$ for all embeddings $\iota : F^+ \to \mathbb{R}$. Let

$$\Delta := \{x \in F \mid \operatorname{trace}_{F/\mathbb{Q}}(x\overline{y}) \in \mathbb{Z} \text{ for all } y \in \mathbb{Z}[\zeta_m]\}$$

denote the inverse different of the ring of integers $\mathbb{Z}_F = \mathbb{Z}[\zeta_m]$ of F. Then the dual lattice of (J, b_α) is

$$(J, b_\alpha)^\# = (\overline{J}^{-1}\Delta\alpha^{-1}, b_\alpha).$$

So (J, b_α) is unimodular, if and only if $(J\overline{J})^{-1}\Delta\alpha^{-1} = \mathbb{Z}_F$. For all fields $F = \mathbb{Q}[\zeta_m]$ considered below it turns out that that there is some totally positive $\alpha_0 \in F^+$

such that $\Delta\alpha_0^{-1} = \mathbb{Z}_F$, so $(\mathbb{Z}_F, b_{\alpha_0})$ is unimodular. Then the isometry classes of unimodular (positive definite) ideal lattices are represented by

$$(J, b_{\alpha_J u \alpha_0})$$

where $[J]$ runs through all ideal classes in F such that $J\overline{J} = \alpha_J \mathbb{Z}_F$ is generated by some totally positive element $\alpha_J \in F^+$ and

$$[u] \in \{u \in \mathbb{Z}_{F^+}^* \mid u \text{ totally positive }\}/\{v\overline{v} \mid v \in \mathbb{Z}_F^*\}.$$

Definition 5.3. *Let $F = \mathbb{Q}[\zeta_m]$ with maximal real subfield $F^+ := \mathbb{Q}[\zeta_m + \zeta_m^{-1}]$. Let $\mathrm{Cl}(F)$ denote the ideal class group of F and $\mathrm{Cl}^+(F^+)$ the ray class group of F^+, where two ideals I, J are equal in $\mathrm{Cl}^+(F^+)$ if there is some totally positive $\alpha \in F^+$ with $I = \alpha J$. Since $x\overline{x}$ is totally positive for any $0 \neq x \in F$, the norm induces a group homomorphism*

$$N : \mathrm{Cl}(F) \to \mathrm{Cl}^+(F^+), \ [J] \mapsto [J\overline{J} \cap F^+].$$

*The **positive class group** $\mathrm{Cl}^+(F)$ is the kernel of this homomorphism and $h^+(F) := |\mathrm{Cl}^+(F)|$.*

Remark 5.4. In the appendix of [29] lists all $m \not\equiv 2 \pmod 4$ such that $\varphi(m) = 48$ as well as the class numbers of F. These coincide with the results of a computation with MAGMA which also shows that the class number of F^+ is 1 in all cases. In particular the positive class group $\mathrm{Cl}^+(F)$ contains $\mathrm{Cl}(F)^2$. However the computation of the unit group $\mathbb{Z}_{F^+}^*$ is too involved to be performed automatically with MAGMA. Instead we compute a system S of independent units in $\mathbb{Z}_{F^+}^*$ and a system of representatives U of all totally positive products of elements in S modulo squares. To show that U is a system of representatives of totally positive units $\mathbb{Z}_{F^+}^*$ modulo squares we check that none of the elements in U has a square root in F^+.
I thank Claus Fieker for helping me with the MAGMA calculations.

Table 3. The class group and the positive class group of $\mathbb{Q}[\zeta_m]$.

m	65	104	105	112	140	144	156	168	180
h_F	$2 \cdot 2 \cdot 4 \cdot 4$	$3 \cdot 117$	13	$3 \cdot 156$	39	$13 \cdot 39$	156	84	$5 \cdot 15$
h_F^+	$2 \cdot 2$	$3 \cdot 117$	13	$6 \cdot 39$	39	$13 \cdot 39$	78	42	$5 \cdot 15$

Theorem 5.5. *Let L be an extremal even unimodular lattice such that $\mathrm{Aut}(L)$ contains some element σ of order $m \not\equiv 2 \pmod 4$ with $\varphi(m) = 48$. Then $m = 65$ or $m = 104$ and $L \cong P_{48n}$.*

Proof. We briefly describe the MAGMA computations that led to this result. They are similar for all cases. In all cases there is some totally positive $\alpha \in F^+$ such that $(\mathbb{Z}_F, b_\alpha)$ is unimodular. Let $I_1, \ldots, I_k$ be ideals of $\mathbb{Z}_F$ such that their classes

generate the positive class group of F, so that $[I_j]$ has order a_j with $a_1 \cdots a_k = h_F^+$. Choose totally positive $\alpha_1, \ldots, \alpha_k \in F^+$ such that $N(I_j) = (\alpha_j)$. Then the isometry classes of unimodular ideal lattices are all represented by some ideal lattice of the form

$$(I_1^{i_1} \cdots I_k^{i_k}, b_{u\alpha\alpha_1^{-i_1} \cdots \alpha_k^{-i_k}}) \text{ where } u \in U \text{ and } 0 \le i_l \le a_l - 1 \text{ for } l = 1, \ldots k$$

where U is computed as described in Remark 5.4.

m=65: Here $|U| = 32$, $\mathrm{Cl}^+(F) = \mathrm{Cl}(F)^2 = \langle [I_1], [I_2] \rangle \cong C_2 \times C_2$, $\alpha = \frac{1}{65}\alpha_{5a}\alpha_{5b}\alpha_{5c}\alpha_{13}$, so there are $4 \cdot 32$ ideal lattices to be considered. Only two of them are extremal, both are principal ideal lattices. To obtain an isometry with the lattice P_{48n} we compute a lattice M such that $M/13L$ is the (4-dimensional) fixed space of the action of σ^5 on $L/13L$. The dual D of M (rescaled to be integral) is a lattice of determinant 13^8, minimum 6 and kissing number 6240 and automorphism group of order $2^6 3^2 65$. The automorphism group of P_{48n} contains a unique conjugacy class of elements of order 65. We compute the corresponding sublattice D_0 of P_{48n} and an isometry between D_0 and D. For both ideal lattices the isometry maps the ideal lattice to P_{48n}.

m=104: Now $|U| = 2$, $\mathrm{Cl}^+(F) = \mathrm{Cl}(F) = \langle [I_1], [I_2] \rangle \cong C_3 \times C_{117}$, $\alpha = \frac{1}{52}\alpha_{13}$, so there are $2 \cdot 3 \cdot 117$ ideal lattices to be considered. Only four of them are extremal, the underlying ideal is a suitable ideal of order 3 and its inverse and all $u \in U$. To obtain an isometry with the lattice P_{48n} we compute a lattice M such that $M/13L$ is the (4-dimensional) fixed space of the action of σ^8 on $L/13L$. As in the case $m = 65$ the dual D of M (rescaled to be integral) is isometric to the corresponding sublattice D_0 of P_{48n} and an isometry between D_0 and D maps the ideal lattice L to P_{48n} in all four cases.

m=105: Again $|U| = 2$, $\mathrm{Cl}^+(F) = \mathrm{Cl}(F) = \langle [I_1] \rangle \cong C_{13}$, where I_1 is some prime ideal dividing 29. $\alpha = \frac{1}{105}\alpha_3\alpha_{5a}\alpha_{5b}\alpha_7$, so there are $2 \cdot 13$ ideal lattices to be considered. In all these lattices reduction algorithms find elements of norm 4.

m=112: Then $|U| = 4$, $\mathrm{Cl}^+(F) = \mathrm{Cl}(F)^2 = \langle [I_1], [I_2] \rangle \cong C_6 \times C_{39}$, where I_1 is some prime ideal dividing 7 and I_2 an ideal dividing 113. $\alpha = \frac{1}{56}\alpha_{7a}\alpha_{7b}$, so there are $4 \cdot 6 \cdot 39$ ideal lattices to be considered. In all these lattices reduction algorithms find elements of norm 4.

m=140: Here $|U| = 2$, $\mathrm{Cl}^+(F) = \mathrm{Cl}(F) = \langle [I_1] \rangle \cong C_{39}$. $\alpha = \frac{1}{70}\alpha_5\alpha_7$, so there are $2 \cdot 39$ ideal lattices to be considered. In all these lattices reduction algorithms find elements of norm 4.

m=144: Again $|U| = 2$, $\mathrm{Cl}^+(F) = \mathrm{Cl}(F)^2 = \langle [I_1], [I_2] \rangle \cong C_{13} \times C_{39}$, $\alpha = \frac{1}{72}\alpha_3^3$, so there are $2 \cdot 13 \cdot 39$ ideal lattices to be considered. In all these lattices reduction algorithms find elements of norm 4.

m=156: Now $|U| = 4$, $\mathrm{Cl}^+(F) = \mathrm{Cl}(F)^2 = \langle [I_1]^2 \rangle \cong C_{78}$, $\alpha = \frac{1}{78}\alpha_{3a}\alpha_{3b}\alpha_{13a}\alpha_{13b}$, so there are $4 \cdot 78$ ideal lattices to be considered. In all these lattices reduction algorithms find elements of norm 4.

m=168: Again $|U| = 4$, $\mathrm{Cl}^+(F) = \mathrm{Cl}(F)^2 = \langle [I_1]^2 \rangle \cong C_{42}$, $\alpha = \frac{1}{84}\alpha_{3a}\alpha_{3b}\alpha_{7a}\alpha_{7b}$, so there are $4 \cdot 42$ ideal lattices to be considered. In all these lattices reduction

algorithms find elements of norm 4.

m=180: Now $|U| = 2$, $\mathrm{Cl}^+(F) = \mathrm{Cl}(F) = \langle [I_1], [I_2] \rangle \cong C_5 \times C_{15}$. $\alpha = \frac{1}{90} \alpha_3^3 \alpha_5$, so there are $2 \cdot 5 \cdot 15$ ideal lattices to be considered. In all these lattices reduction algorithms find elements of norm 4. $\qquad\square$

5.3. *Subideal lattices*

This section classifies all extremal even unimodular lattice L that have an automorphism σ of order m such that $24 < \varphi(m) < 48$. By Corollary 4.11 we know that Φ_m divides μ_σ. We have a unique decomposition

$$\mathbb{Q}L = V \oplus W \text{ into } \sigma \text{ invariant subspaces}$$

so that σ acts as a primitive m-th root of unity on V. Since $\varphi(m) > 24$, the action of σ turns V into a 1-dimensional vector space over $F := \mathbb{Q}[\zeta_m]$, the m-th cyclotomic number field, and the lattice $M := L \cap V = (J, b_\alpha)$ is an ideal lattice in F. The lattice M is integral, if $J\overline{J}\alpha \subseteq \Delta$ and then

$$M^\#/M \cong \Delta(J\overline{J}\alpha)^{-1}/\mathbb{Z}[\zeta_m] \text{ as a } \mathbb{Z}[\zeta_m] - \text{module.}$$

For our computations it turns out that $M = L_I(\sigma^d)$ for some element σ^d of prime order p with $pd = m$, so we know $\det(M)$ (more precisely the abelian group $M^\#/M$ from Section 4. We also know the fixed lattice $K = \mathrm{Fix}_L(\sigma^d)$ and the possible actions of σ on K, by computing the conjugacy classes of automorphisms of K of order d. The even unimodular lattice L is a subdirect product of $M^\#$ and $K^\#$ with kernel $M \perp K$. Therefore the $\mathbb{Z}[\zeta_m]$-module $M^\#/M$ is isomorphic to $K^\#/K$.

Table 4. The values $m \not\equiv 2 \pmod 4$ such that $48 > \varphi(m) > 24$.

m	29	31	37	41	43	47	49	51	55	57	63	64
$\varphi(m)$	28	30	36	40	42	46	42	32	40	36	46	32
thm	4.4	4.4	4.4	4.4	4.4	5.6	5.9	4.4	5.8	4.4	5.9	4.12
m	68	69	75	76	80	88	92	96	100	108	120	132
$\varphi(m)$	32	44	40	36	32	40	44	32	40	36	32	40
thm	4.4	5.9	5.9	4.4	4.12	4.12	5.9	4.12	5.9	5.9	5.9	5.9

Again in all cases the class number of the maximal real subfield of the cyclotomic field is 1 and we use the MAGMA computations described in Remark 5.4. To explain the strategy we will give two proofs in detail.

Theorem 5.6. *(see also [12, Section 4.5.4]) Let L be an extremal even unimodular lattice of dimension 48 such that $\mathrm{Aut}(L)$ contains an element σ of order 47. Then $L \cong P_{48q}$.*

Proof. Let $L_K := L_K(\sigma)$ and $L_I := L_I(\sigma)$. Then L_K has Gram matrix F_{47} from Theorem 4.4 and $[L : L_K \perp L_I] = 47$. Moreover L_I is an ideal lattice in the 47-th cyclotomic number field $F = \mathbb{Q}[\zeta_{47}]$. So there is some fractional ideal J

in F and some totally positive $a \in F^+ := \mathbb{Q}[\zeta_{47} + \zeta_{47}^{-1}]$ such that $L_I = J$ and $(x, y) = \text{trace}(ax\overline{y})$ for all $x, y \in J$. The class number of F is $695 = 5 \cdot 139$ ([29]) and one computes with MAGMA, that the class group is generated by any prime ideal $\wp$ that divides 283 (e.g. $\wp = (283, \zeta_{47} + 279)$). Again with MAGMA one computes a system of independent units in the ring of integers $\mathbb{Z}_{F^+} = \mathbb{Z}[\zeta_{47} + \zeta_{47}^{-1}]$ of which the 23 real embeddings (together with -1) generate all 2^{23} possible sign combinations. In particular any totally positive unit in $\mathbb{Z}_{F^+}$ is a square. Since F^+ has class number one, any ideal in $\mathbb{Z}_{F^+}$ has some totally positive generator. In particular the ideal $\wp\overline{\wp} \cap \mathbb{Z}_{F^+}$ has some totally positive generator α that may be computed explicitly in MAGMA. Therefore the lattice L_I is isometric to one of the 695 ideal lattices

$$J_j := (\Delta\wp^j, (x, y) \mapsto 47 \, \text{trace}(\alpha^{-j} x\overline{y})) \text{ for some } j = 0, \ldots, 694.$$

Here $\Delta = (1 - \zeta_{47})^{-45}$ is the inverse different of the lattice $\mathbb{Z}_F$, which has the desired property that $\det(\Delta, (x, y) \mapsto 47 \, \text{trace}(x\overline{y})) = 47$. With a combination of lattice reduction algorithms we find vectors of norm 4 in all these lattices but in one pair; only J_{139} and its complex conjugate have minimum norm 6. The quadratic space $(L_K \perp J_{139})^\# / (L_K \perp J_{139})$ is a hyperbolic plane over $\mathbb{F}_{47}$. The two isotropic subspaces correspond to isometric even unimodular extremal lattices (the isometry is given by $\text{diag}(-I_2, I_{46})$). Let L be one of these lattices. By the uniqueness of L it is clear that L is isometric to P_{48q}. To establish an explicit isometry one may consider a vector $\beta \in L_K \leq L$ of norm 12 and compute the neighbor $L^{(\beta),2}$. This lattice contains a 3-frame, so $L = \Lambda(C)$ for some ternary extremal code with an automorphism of order 47. $\square$

Remark 5.7. Theorem 5.6 has already been obtained in the diploma thesis [12] supervised by Skoruppa. Similar, but much more involved, computations allowed Skoruppa also to construct all even unimodular lattices of dimension 72 with an automorphism of order 71. A combination of reduction algorithms finds vectors of norm 4 or 6 in all these lattices, so there is no extremal even unimodular lattice of dimension 72 that has an automorphism of order 71 (see [28]).

Theorem 5.8. *There is no extremal even unimodular lattice L of dimension* 48 *such that* $\text{Aut}(L)$ *contains an element* σ *of order* 55.

Proof. Then $d = 5, p = 11$, the type of σ^5 is $11 - (4, 8) - 4$, $\det(M) = 11^4$, σ^5 acts trivially on $M^\#/M$ so $M^\#/M \cong \mathbb{Z}[\zeta_{55}]/(1 - \zeta_{55}^5)$ and the minimal polynomial for the action of σ on $M^\#/M$ is $x^4 + x^3 + x^2 + x + 1 = \Phi_5$. The automorphism group of the fixed lattice K of σ^5 contains 3 conjugacy classes a_1, a_2, a_3 of elements of order 5 with irreducible minimal polynomial. These are the possible candidates for the action of σ on K. They act on the dual quotient $K^\#/K$ with minimal polynomial

$$\mu_1 := x^2 + 8x + 1, \ \mu_2 := x^2 + 4x + 1, \ \mu_3 = x^4 + x^3 + x^2 + x + 1.$$

So σ acts on $M \perp K$ as $\text{diag}(\zeta_{55}, a_3)$.
The class group of F is generated by $\wp = (11, \zeta_{55} + 8)$, $h_F = 10$ and the classes of

totally positive units in $\mathbb{Z}_{F^+}$ are represented by $U = \{1 = u_1, u_2, u_3, u_4\}$. The ideal $\overline{\wp}\wp \cap \mathbb{Z}_{F^+} = \beta\mathbb{Z}_{F^+}$ has no totally positive generator but its square is generated by the totally positive element β^2. Also there is some prime element $p_5 \in \mathbb{Z}_{F^+}$ dividing 5 such that $p_{55} := \beta p_5$ is totally positive. Therefore the lattice M is isometric to one of the $4 \cdot 5$ ideal lattices

$$J_{j,i} := (\Delta\wp^{2j+1}, (x,y) \mapsto \operatorname{trace}(u_i\beta^{-2j}p_{55}^{-1}x\overline{y})) \text{ for some } j = 0, \ldots, 4, i = 1, \ldots, 4.$$

$4 \cdot 4$ of these lattices ($j = 0, 1, 3, 4$ and all u_i) have minimum 6.
With MAGMA compute the unimodular overlattices L of $J_{j,i} \perp L_K$ that are invariant under $\operatorname{diag}(\sigma, a_3)$. None of these lattices has minimum 6. $\qquad\square$

Similar as in Theorem 5.6 and 5.8 we obtain the following theorem.

Theorem 5.9. *Let L be an extremal even unimodular lattice such that $\operatorname{Aut}(L)$ contains some element σ of order m with $24 < \varphi(m) < 48$. Then either $m = 47$ and $L \cong P_{48q}$, $m = 69$ and $L \cong P_{48p}$, $m = 120$ and $L \cong P_{48n}$, or $m = 132$ and $L \cong P_{48p}$.*

Proof. The MAGMA computations are similar for all cases and follow the ones described above for the case $m = 47$ and $m = 55$. We will always denote by $F := \mathbb{Q}[\zeta_m]$ the m-th cyclotomic number field, $F^+ := \mathbb{Q}[\zeta_m + \zeta_m^{-1}]$ its maximal real subfield. The class number of F^+ turns out to be 1, the class group of F is cyclic in all cases, $\wp$ will denote some prime ideal of $\mathbb{Z}_F$ whose class generates the class group of F and h_F its order, the class number of F. As before, Δ will denote the inverse different of $\mathbb{Z}_F$, this is always a principal ideal. The ideal lattice M will always be of the form $M = L_I(\sigma^d)$ with $dp = m$ for some prime p. In particular we know the $\mathbb{Z}_F$-module $M^\#/M$ from the computations of the possible fixed lattices of prime order automorphisms in Section 4.1 as explained above. The set $U \subset \mathbb{Z}_{F^+}^*$ of totally positive units is obtained as described in Remark 5.4.

m=49: Then $d = p = 7$, the type of σ^7 is $7 - (7,6) - 5$, $\det(M) = 7^5$ $\wp = (197, \zeta_{49} + 4)$, $h_F = 43$, $\overline{\wp}\wp \cap F^+ = \alpha\mathbb{Z}_{F^+}$ for some totally positive α, all totally positive units in $\mathbb{Z}_{F^+}$ are squares, so $U = \{1\}$. A combination of lattice reduction algorithms we find vectors of norm 4 in all 43 lattices

$$J_j := (\Delta(1 - \zeta_{49})^{-1}\wp^j, b_{\alpha^{-j}}) \text{ for } j = 0, \ldots, 42.$$

m=63: By Theorem 4.5 there is no automorphism of Type $7 - (6,12) - s$, so $d = 21$ and $p = 3$ and the type of σ^{21} is $3 - (18,12) - 12$ and M is an ideal lattice in the 63-th cyclotomic number field with $\det(M) = 3^{12}$. The class group of F has order 7 and is generated by any prime ideal dividing 2, e.g. $\wp = (2, 1 + \zeta_{63} + \zeta_{63}^4 + \zeta_{63}^5 + \zeta_{63}^6)$. In the maximal real subfield F^+ there are unique prime ideals $\wp_7$ and $\wp_3$ dividing 7 resp. 3. As the class number of F^+ is 1, both ideals are principal, $\wp_7$ has some totally positive generator, α_7, but $\wp_3$ doesn't. So the norms of the totally positive elements in $\mathbb{Z}_{F^+}$ that divide 3 are powers of 3^{12}. The lattice $(\mathbb{Z}_F, b_{\alpha_7/21})$ has determinant

3^{18}, so there is no ideal lattice in the 63rd cyclotomic number field of determinant 3^{12}.

m=69: Then $d = 3$, $p = 23$ and σ^3 has type $23 - (2, 4) - 2$. $\det(M) = 23^2$, $h_F = 69$, $\wp = (139, \zeta_{69} + 135)$. $U = \{1, u_0\}$ and $\overline{\wp}\wp \cap \mathbb{Z}_{F^+} = \alpha\mathbb{Z}_{F^+}$ for some totally positive element $\alpha \in F^+$. So M is isometric to one of the $2 \cdot 69$ ideal lattices

$$J_j := (\Delta\wp^j, (x, y) \mapsto \mathrm{trace}(23p_3u\alpha^{-j}x\overline{y})) \text{ for some } j = 0, \dots, 68, u \in \{1, u_0\},$$

where p_3 is some totally positive prime element dividing 3. 2 of these lattices ($j = 0$ and both u) have minimum 6.

The automorphism group of the fixed lattice K of σ^3 contains a unique conjugacy class of elements of order 3, say represented by a_1. We compute the unimodular overlattices L of $M \perp K$ that are invariant under $\mathrm{diag}(\sigma, a_1)$ and find 24 lattices of minimum 6. For all these 24 lattices L we compute the norm 12-vectors v in the fixed lattice K. For all lattices there is at least one v for which the neighbor $L^{(v),2}$ contains a 3-frame. So $L = \Lambda(C)$ for some extremal ternary code which turns out to be equivalent to the Pless code P_{48}.

m=75: Then $d = 15$, $p = 5$, the type of σ^{15} is $5 - (10, 8) - 8$, $\det(M) = 5^8$, $h_F = 11$, $\wp = (151, 146 + \zeta_{75})$, $U = \{1, u_0\}$ and $\overline{\wp}\wp \cap \mathbb{Z}_{F^+} = \alpha\mathbb{Z}_{F^+}$ Therefore the lattice M is isometric to one of the $2 \cdot 11$ ideal lattices

$$J_j := (\Delta\wp^j, (x, y) \mapsto \mathrm{trace}(75u\alpha^{-j}\alpha_{3,5}^{-1}x\overline{y})) \text{ for some } j = 0, \dots, 10, u \in \{1, u_0\}$$

where $\alpha_{3,5}$ is a totally positive element generating the product of some prime ideal over 3 and some prime ideal over 5. All 20 non-principal ideal lattices have minimum 6. The element σ acts on $M^{\#}/M$ as a primitive 15th root of 1. The automorphism group of the fixed lattice $K = \sqrt{5}E_8$ contains a unique conjugacy class of automorphisms that act as primitive 15th root of 1, say represented by a_1. We compute the unimodular overlattices L of $M \perp K$ that are invariant under $\mathrm{diag}(\sigma, a_1)$. None of these lattices has minimum 6.

m=92: Then $d = 4$, $p = 23$, the type of σ^4 is $23 - (2, 4) - 2$, $\det(M) = 23^2$, $h_F = 201$, $\wp = (277, \zeta_{92} + 275)$. $U = \{1, u_0\}$ and $\overline{\wp}\wp \cap \mathbb{Z}_{F^+} = \alpha\mathbb{Z}_{F^+}$ for some totally positive element $\alpha \in F^+$. Therefore the lattice M is isometric to one of the $2 \cdot 201$ ideal lattices

$$J_j := (\Delta\wp^j, (x, y) \mapsto \mathrm{trace}(46u\alpha^{-j}x\overline{y})) \text{ for some } j = 0, \dots, 200, u \in \{1, u_0\}.$$

None of these lattices has minimum 6.

m=100: Then $d = 20$, $p = 5$, the type of σ^{20} is $5 - (10, 8) - 8$, $\det(M) = 5^8$, $h_F = 5 \cdot 11$, $\wp_5 = (5, 6 + \zeta_{100})$ is an element of order 5 and $\wp_7 = (7, 1 + \zeta_{100} + \zeta_{100}^2 - \zeta_{100}^3 + \zeta_{100}^4)$ an element of order 11 in the class group of F.

Again there are two square classes of totally positive units, so $U = \{1, u_0\}$. Both ideals $\overline{\wp_5}\wp_5 \cap \mathbb{Z}_{F^+} = \alpha_5\mathbb{Z}_{F^+}$ and $\overline{\wp_7}\wp_7 \cap \mathbb{Z}_{F^+} = \alpha_7\mathbb{Z}_{F^+}$ have totally positive generators. Therefore the lattice M is isometric to one of the $2 \cdot 5 \cdot 11$ ideal lattices

$$(\Delta\wp_5^j\wp_7^k, (x, y) \mapsto \mathrm{trace}(50\alpha_5^{-1}u\alpha_5^{-j}\alpha_7^{-k}x\overline{y}))$$

for some $j = 0, \ldots, 4, k = 0, \ldots, 10, u \in \{1, u_0\}$. All 40 ideal lattices for $j = 1, 4$ and $k \neq 0$ have minimum 6. The element σ acts on $M^{\#}/M$ as a primitive 20th root of 1. The automorphism group of the fixed lattice $K = \sqrt{5}E_8$ contains a unique conjugacy class of automorphisms that act as primitive 20th root of 1, say represented by a_1. We compute the unimodular overlattices L of $M \perp K$ that are invariant under $\mathrm{diag}(\sigma, a_1)$. None of these lattices has minimum 6.

m=108: Here $d = 36$ and $p = 3$ and the type of σ^{36} is $3 - (18, 12) - 12$ and M is an ideal lattice in the 108-th cyclotomic number field F with $\det(M) = 3^{12}$. The class group of F has order 19 and is generated by any prime ideal dividing 109, e.g. $\wp = (109, 106 + \zeta_{108})$. In the maximal real subfield F^+ there are unique prime ideals $\wp_2$ and $\wp_3$ dividing 2 resp. 3. As the class number of F^+ is 1, both ideals are principal, but none of them has a totally positive generator. However $\wp_2 \wp_3 = (\alpha_{2,3})$ has some totally positive generator as well as $\wp_3^2 = (\alpha_3^2)$. So the norms of the totally positive elements in $\mathbb{Z}_{F^+}$ that divide 3 are powers of 3^4. The lattice $(\mathbb{Z}_F, b_{1/18})$ has determinant 3^{18}, so there is no ideal lattice in the 108-th cyclotomic number field of determinant 3^{12}.

m=120: The classnumber is $h_F = 4$ and the class group is generated by some prime ideal dividing 5, e.g. $\wp_5 = (5, 2 + 4\zeta_{120} + \zeta_{120}^2)$. In $\mathbb{Z}_F^+$ both prime ideals dividing 3 have totally positive generators, α_{3a}, α_{3b}. Also the unique prime ideal that divides 2 has a totally positive generator, α_2, whereas the two prime ideals dividing 5 are not generated by totally positive elements, their product and their squares are generated by the totally positive elements $\alpha_{5ab}, \alpha_{5a}^2$ and α_{5b}^2. In particular $\overline{\wp_5}\wp_5 \cap F^+$ is not generated by some totally positive element, so there are only two ideal classes to be considered. The totally positive units lie in the classes of $1 = u_0, u_1, u_2, u_3$.

Now we have two possibilities for $\det(M)$:

a) $d = 40$, $p = 3$, type of σ^{40} is $3 - (16, 16) - 16$, $\det(M) = 3^{16}$. Since σ^{40} acts trivially on $K^{\#}/K$ the $\mathbb{Z}_F$-module $M^{\#}/M$ is isomorphic to $\mathbb{Z}_F/(1 - \zeta_{120}^{40})$ and σ acts on $M^{\#}/M$ with minimal polynomial Φ_{40}. So M is one of the 8 ideal lattices

$$(\Delta \wp_5^{2j}, (x, y) \mapsto \mathrm{trace}(60\alpha_5^{-2j} u \alpha_{5ab}^{-1} x \overline{y})) \text{ for some } j = 0, 1, u \in \{1, u_1, u_2, u_3\}.$$

Only the lattices for $j = 0$ and $u = u_1, u_3$ have minimum 6. Both lattices are isometric to the Eisenstein lattice described by Christine Bachoc [3].

In principle we have two possibilities for the fixed lattice K, $K \cong \sqrt{3}D_{16}^+$ or $K \cong \sqrt{3}(E_8 \perp E_8)$. The automorphism group of D_{16}^+ does not contain elements with minimal polynomial Φ_{40}, so $K \cong \sqrt{3}(E_8 \perp E_8)$. For this lattice $\mathrm{Aut}(E_8 \perp E_8)$ contains a unique conjugacy class of such elements, represented by, say, a_1. We now need to compute the (σ, a_1)-invariant unimodular overlattices of $M \perp K$ for the two possibilities for M. A straight forward approach is too memory consuming, as we now need to handle invariant submodules of $\mathbb{F}_3^{32}$. The lattices L are of the form

$$L_{\varphi} = \{(x, y) \in M^{\#} \perp K^{\#} \mid \varphi(x + M) = y + K\}$$

for some isometry $\varphi : (M^{\#}/M, F_M) \to (K^{\#}/K, -F_K)$ so that $\sigma \varphi = \varphi a_1$. For any $c \in C_{\mathrm{Aut}(K)}(a_1) = \langle a_1 \rangle$ the lattices L_{φ} and $L_{\varphi c}$ are isometric. Fixing one such isome-

try φ_0, we hence obtain all L_φ by letting φ vary in $\{\varphi_0 u \mid u \in C_{O(K^\#/K)}(a_1)/\langle a_1 \rangle\}$. To compute the centralizer in the orthogonal group $O(K^\#/K)$ we compute the orthogonal elements in the endomorphism algebra $\mathrm{End}_{K^\#/K}(a_1) \cong \bigoplus_{i=1}^{4} \mathbb{F}_{3^4} e_i$. As the involution $x \mapsto \overline{x} = (F_K x^{tr} F_K^{-1})$ on $\mathrm{End}_{K^\#/K}(a_1)$ interchanges the idempotents, say, $\overline{e_1} = e_2$, $\overline{e_3} = e_4$, the orthogonal elements are of the form $x e_1 + \overline{x}^{-1} e_2 + y e_3 + \overline{y}^{-1} e_4$, so $|C_{O(K^\#/K)}(a_1)| = 80^2$ and $C_{O(K^\#/K)}(a_1)/\langle a_1 \rangle$ has 160 coset representatives. For each lattice M there are exactly 4 lattices L_φ that have minimum norm 6.

To obtain an isometry between L_φ and P_{48n} we observe that $\mathrm{Aut}(P_{48n})$ has a unique conjugacy class of automorphism of order 120, say represented by τ. We compute a lattice Λ such that $\Lambda/2L_\varphi$ is the (4-dimensional) fixed space of the action of σ^5 on $L_\varphi/2L_\varphi$. The dual D of Λ (rescaled to be integral) is a lattice of determinant 2^8, minimum 6 and kissing number 3264000 and automorphism group of order 5760. We compute the corresponding sublattice D_0 of P_{48n} and an isometry between D_0 and D. For all eight lattices L_φ the isometry maps L_φ to P_{48n}.

b) $d = 24$, $p = 5$, type of σ^{24} is $5 - (8, 16) - 8$, $\det(M) = 5^8$. Again $M^\#/M \cong \mathbb{Z}_F/(1 - \zeta_{120}^{24})$ as σ^{24} acts trivially on K and σ acts on $M^\#/M$ as a primitive 24-th root of unity. So M is one of the 8 ideal lattices

$$(\Delta \wp_5^{2j}, (x,y) \mapsto \mathrm{trace}(60 \alpha_5^{-2j} u \alpha_{3a}^{-1} \alpha_{3b}^{-1} x \overline{y})) \text{ for some } j = 0, 1, u \in \{1, u_1, u_2, u_3\}.$$

None of these lattices has minimum ≥ 6.

m=132: Then $d = 12$, $p = 11$, σ^{12} has type $11 - (4, 8) - 4$, $\det(M) = 11^4$, $\wp = (23, \zeta_{132}^2 + 22\zeta_{132} + 8)$, $h_F = 11$. $U = \{1, u_0\}$ and $\overline{\wp}\wp \cap \mathbb{Z}_{F^+} = \alpha \mathbb{Z}_{F^+}$ for some totally positive element $\alpha \in F^+$. Therefore the lattice M is isometric to one of the $2 \cdot 11$ ideal lattices

$$J_j := (\Delta \wp^j, (x,y) \mapsto \mathrm{trace}(u \alpha^{-j} x \overline{y})) \text{ for some } j = 0, \ldots, 10, u \in \{1, u_0\}.$$

$10 \cdot 2$ of these lattices ($j = 1, \ldots, 10$ and all u) have minimum 6.

The automorphism group of the fixed lattice K of σ^{12} contains a unique conjugacy class of elements of order 12 with irreducible minimal polynomial, say represented by a_1. We compute the unimodular overlattices L of $M \perp K$ that are invariant under $\mathrm{diag}(\sigma, a_1)$ and find 240 lattices of minimum 6. For all these 240 lattices L we compute the 50 orbits of $\langle a_1 \rangle$ on the norm 12-vectors v in the fixed lattice L_K and find one orbit for which the neighbor $L^{(v),2}$ contains a 3-frame. So $L = \Lambda(C)$ for some extremal ternary code which turns out to be equivalent to the Pless code P_{48}. $\square$

6. The automorphism group of the 72-dimensional extremal lattice

In the paper [22] I describe the construction of some extremal even unimodular lattice Γ of dimension 72 such that $G := \mathrm{Aut}(\Gamma)$ contains the subgroup $\mathcal{U} \cong (\mathrm{SL}_2(25) \times \mathrm{PSL}_2(7)) : 2$. As in Section 3.2 we may prove that $\mathcal{U}$ is indeed the full automorphism group of Γ. With the same strategy as in the proof of [20, Theorem 5.3] one shows the following lemma.

Lemma 6.1. $\mathcal{U} = N_G(\mathrm{SL}_2(25))$.

Proof. Let $N := \mathrm{SL}_2(25)$ be the normal subgroup of $\mathcal{U}$ that is isomorphic to $\mathrm{SL}_2(25)$. With MAGMA one computes that the endomorphism algebra of N is

$$A := \{x \in \mathbb{Q}^{72\times 72} \mid xg = gx \text{ for all } g \in N\} \cong \mathcal{Q}^{3\times 3}_{\infty,5}$$

so the natural character of N is a multiple of one of the two irreducible characters of degree 12 ([9]) with real Schur index 2. The outer automorphism group of $\mathrm{SL}_2(25)$ has order 4, but only a subgroup of order 2 stabilises this character. Since $\mathcal{U}$ contains an element inducing this non-trivial outer automorphism, it is enough to show that $\mathcal{U}$ contains the centraliser $C := C_G(N)$. Then C is a subgroup of the unit group A^*; moreover C stabilizes Γ and the $\mathcal{U}$-invariant quadratic form. Let $v \neq 0$ be any vector in Γ and let $L_v := vA \cap \Gamma \leq \Gamma$. The dimension of L_v divides $\dim(A) = 36$ and C is a subgroup of $\mathrm{Aut}(L_v)$. Computations in MAGMA find a vector v such that $\dim(L_v) = 36$ and $\mathrm{Aut}(L_v) \cong \pm \mathrm{PSL}_2(7)$. Therefore $C \cong \pm \mathrm{PSL}_2(7) \leq \mathcal{U}$.   □

Using the classification of finite simple groups and in particular the tables in [14] we now conclude as in Section 3.2 that $\mathcal{U} = \mathrm{Aut}(\Gamma)$.

Theorem 6.2. *Let Γ be the extremal even unimodular 72-dimensional lattice constructed in [22]. Then $\mathrm{Aut}(\Gamma) \cong (\mathrm{SL}_2(25) \times \mathrm{PSL}_2(7)) : 2$.*

Proof. Explicit generators for the subgroup $\mathcal{U} \cong (\mathrm{SL}_2(25) \times \mathrm{PSL}_2(7)) : 2$ of $G := \mathrm{Aut}(\Gamma)$ have been constructed in [22]. Remark 2.4 of this paper also shows that $\mathcal{U}$ is absolutely irreducible and that all $\mathcal{U}$-invariant lattices are similar to Γ. In particular $\mathcal{U}$ does not fix an orthogonally decomposable lattice and therefore $\mathcal{U}$ and hence also G is a primitive maximal finite rational matrix group. In particular the maximal normal p-subgroups of G are given in the Theorem of Ph. Hall on [15, p. 357]. None of the possible groups contains $\mathrm{SL}_2(25)$ as an automorphism group. The tables in [14] show that there are no finite quasisimple groups in $\mathrm{GL}_{72}(\mathbb{Q})$ that contain the group $\mathcal{U}$. Therefore one concludes that $\mathrm{SL}_2(25)$ is normal in G, so by Lemma 6.1 we obtain $G = \mathcal{U}$.   □

References

[1] K. Abdukhalikov, *Unimodular Hermitian lattices in dimension* 13. J. Algebra 272 (2004) 186–190.

[2] K. Abdukhalikov, R. Scharlau, *Unimodular lattices in dimensions* 14 *and* 15 *over the Eisenstein integers.* Math. Comp. 78 (2009) 387–403.

[3] C. Bachoc, *Applications of coding theory to the construction of modular lattices.* J. Comb. Th A 78-1 (1997) 92–119

[4] C. Bachoc, B. Venkov, *Modular forms, lattices and spherical designs.* in Réseaux euclidiens, designs sphériques et formes modulaires, 87–111, Monogr. Enseign. Math., 37, Enseignement Math., Geneva, 2001

[5] E. Bayer-Fluckiger, *Ideal lattices.* A panorama of number theory or the view from Baker's garden (Zürich, 1999), 168–184, Cambridge Univ. Press, Cambridge, 2002.

26   *Gabriele Nebe*

[6] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language.* J. Symbolic Comput. 24 (1997) 235–265.

[7] R. E. Borcherds, *The Leech Lattice and Other Lattices.* Ph. D. Dissertation, University of Cambridge, 1984.

[8] H. Cohn, N. Elkies, *New upper bound on sphere packings I.* Ann. of Math. 157 (2003) 689–714.

[9] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, *Atlas of finite groups.* Oxford University Press 1985.

[10] J.H. Conway, N.J.A. Sloane, *Sphere packings, lattices and groups.* Grundlehren der Mathematischen Wissenschaften 290. Springer-Verlag, New York, 1988.

[11] W. Feit, *Some lattices over $\mathbb{Q}(\sqrt{-3})$.* J. Algebra 52 (1978) 248–263.

[12] L. Fischer, *Die Berechnung extremaler Gitter vom Rang $\ell + 1$ mit einem Automorphismus von Primzahlordnung ℓ mittels der Theorie der Kreisteilungskörper.* Diplomarbeit, Universität Siegen 2008.

[13] M. Harada, T. Miezaki, *On the Existence of Extremal Type II $\mathbb{Z}_{2k}$-Codes.* Math. Comp. (to appear)

[14] G. Hiß, G. Malle, *Low-dimensional representations of quasi-simple groups.* LMS J. Comput. Math. 4 (2001), Corrigenda: LMS J. Comput. Math. 5 (2002)

[15] B. Huppert, *Endliche Gruppen I.* Die Grundlehren der Mathematischen Wissenschaften, Band 134 Springer-Verlag, Berlin-New York 1967

[16] M. Kneser, *Klassenzahlen definiter quadratischer Formen.* Arch. Math. 8 (1957) 241–250.

[17] H. Koch, *The 48-dimensional analogues of the Leech lattice.* Trudy Mat. Inst. Steklov. 208 (1995) 193–201.

[18] J. Martinet, *Perfect lattices in Euclidean spaces.* Grundlehren der Mathematischen Wissenschaften 327. Springer-Verlag, Berlin, 2003.

[19] G. Nebe, *The normaliser action and strongly modular lattices.* L'Ens. Math., 43 (1997) 67–76.

[20] G. Nebe, *Some cyclo-quaternionic lattices.* J. Algebra 199 (1998) 474–498.

[21] G. Nebe, *On extremal self-dual ternary codes of length 48.* Int. J. Comb. 2012.

[22] G. Nebe, *An even unimodular 72-dimensional lattice of minimum 8.* J. Reine und Angew. Math. 673 (2012) 237–247.

[23] G. Nebe, N.J.A. Sloane, *A database of lattices.* published electronically, http://www.math.rwth-aachen.de/∼Gabriele.Nebe/LATTICES/

[24] G. Nebe, W. Plesken, *Finite rational matrix groups.* Mem. Amer. Math. Soc. 116 (1995)

[25] W. Plesken, M. Pohst, *On maximal finite irreducible subgroups of GL(n,**Z**). II. The six dimensional case.* Math. Comp. 31 (1977) 552–573.

[26] I. Reiner, *Integral Representations of Cyclic Groups of Prime Order.* Proc. AMS 8 (1957) 142–146.

[27] R. Scharlau, R. Schulze-Pillot, *Extremal lattices.* Algorithmic algebra and number theory (Heidelberg, 1997), 139–170, Springer, Berlin, 1999.

[28] N.P. Skoruppa, *The Rubens-project 72*, Preprint 2007, 2013.

[29] L.C. Washington, *Introduction to cyclotomic fields.* Graduate Texts in Mathematics 83, Springer-Verlag, New York, 1982.