BINARY HERMITIAN LATTICES OVER NUMBER FIELDS

MARKUS KIRSCHMER AND GABRIELE NEBE

ABSTRACT. In a previous paper the authors developed an algorithm to classify certain quaternary quadratic lattices over totally real fields. The present paper applies this algorithm to the classification of binary Hermitian lattices over totally imaginary fields. We use it in particular to classify the 48-dimensional extremal even unimodular lattices over the integers that admit a semilarge automorphism.

1. INTRODUCTION

Our main motivation for the research leading to the present paper is the classification of extremal even unimodular lattices using automorphisms. For a short overview of this long term project of the second author we refer to Section 2. The overall strategy is as follows: Let L be a lattice and $g \in \mathrm{Aut}(L)$ some automorphism of L of finite order o. The minimal polynomial μ_g divides the separable polynomial $X^o - 1 \in \mathbb{Q}[X]$ and hence splits into a product $\mu_g = p_1 \cdot \ldots \cdot p_s$ of pairwise distinct monic irreducible polynomials p_i. This gives rise to a g-invariant sublattice

$$M_1 \perp \ldots \perp M_s \leq L$$

of finite index in L, such that g acts on M_i with minimal polynomial p_i. The idea to classify all lattices L with a given automorphism g is to first classify the smaller lattices M_i and then construct L as a suitable g-invariant overlattice of $M_1 \perp \ldots \perp M_s$. Each lattice M_i can be seen as a lattice over the ring of integers $\mathbb{Z}[g_{|M_i}] \cong \mathbb{Z}[X]/(p_i)$ in some cyclotomic number field $E_i = \mathbb{Q}[X]/(p_i)$ of dimension $m_i = \dim_{\mathbb{Z}}(M_i)/\deg(p_i)$. The automorphism g is called *large*, if there is one i such that $\deg(p_i) > \frac{\dim(L)}{2}$. Then $m_i = 1$ and the lattice M_i is an ideal lattice in the sense of [1]. The classification of all extremal even unimodular lattices of dimension 48 and 72 admitting a large automorphism has been obtained in [23] and [25] using algorithms for number fields. The present paper classifies all extremal even unimodular lattices of dimension 48 that admit a semilarge automorphism (see Definition 9.1), where g as above is called *semilarge*, if there is one i such that $\deg(p_i) > \frac{\dim(L)}{4}$ and $m_i = 2$. In this case the lattice M_i is a binary Hermitian lattice over E_i. It turns out that we may use the algorithms for quaternion algebras developed in [16] to classify binary Hermitian lattices over CM-fields.

So let E be a totally complex quadratic extension of a totally real number field K and denote by $\mathbb{Z}_E$ and $\mathbb{Z}_K$ the ring of integers in E and K respectively. Then there is $\alpha \in E$ such that

$$E = K[\alpha] \text{ and } -\alpha^2 =: \delta \in K \text{ is totally positive.}$$

Let $(W, \mathbf{h})$ be a positive definite m-dimensional Hermitian space over E. Restriction of scalars turns $(W, \mathbf{h})$ into a $2m$-dimensional positive definite quadratic space $(W_{|K}, \mathbf{q_h})$ over K where $\mathbf{q_h}(x) = \mathbf{h}(x, x) \in K$ for all $x \in W$. Our interest lies in the case $m = 2$, as we aim to classify binary Hermitian lattices. Then $(W_{|K}, \mathbf{q_h})$ is a quaternary quadratic space over K of square determinant.

In [15] we developed an algorithm to enumerate the isometry classes in the genus of maximal $\mathbb{Z}_K$-lattices in a positive definite quaternary quadratic space $(V, \mathbf{q})$ over K of square discriminant. The underlying idea is that $(V, \mathbf{q})$ is isometric to (Q, n), where Q is a well determined definite quaternion algebra with centre K and $n: Q \to K$ is the norm form of Q. In our special case,

where $(V, q) = (W_{|K}, \mathbf{q_h})$ is the restriction of scalars of a Hermitian space as above, the quaternion algebra

$$Q = \left(\frac{-\delta, -\det(\mathbf{h})}{K} \right) = K[i, j : i^2 = -\delta, j^2 = -\det(\mathbf{h}), ij = -ji]$$

is uniquely determined by E and the determinant of the Hermitian form $\mathbf{h}$.

For any fractional ideal $\mathfrak{a}$ in K the $\mathfrak{a}$-maximal $\mathbb{Z}_K$-lattices in (Q, n) correspond to normal ideals of norm $\mathfrak{a}$ and the notion of (proper) isometry corresponds to a certain notion of equivalence of these ideals, for more details see Theorem 6.2 and [15]. The $\mathfrak{a}$-maximal $\mathbb{Z}_E$-lattices in $(W, \mathbf{h})$ are those $\mathfrak{a}$-maximal $\mathbb{Z}_K$-lattices that are stable under multiplication by $\mathbb{Z}_E$ (see Proposition 4.1). The central part of this paper is Section 7, where we apply the algorithm from [15] to enumerate the isometry classes of positive definite $\mathfrak{a}$-maximal Hermitian $\mathbb{Z}_E$-lattices in $(W, \mathbf{h})$. In particular Theorem 7.5 shows how to obtain a system of representatives. We apply this algorithm to the special situation where E is a cyclotomic number field. Our more general computations result in a nice formula in the particular case where $E = \mathbb{Q}[\zeta_p]$ for a prime $p \equiv 3 \pmod 4$ and the narrow class number of K is 1. Under these assumptions the class number of the Hermitian unimodular binary $\mathbb{Z}_E$-lattices is the product of the type number of Q and the class number of E (see Proposition 8.1). The quite involved computations that yield a classification of all extremal even unimodular lattices of dimension 48 admitting a semilarge automorphism are described in Section 9 (see Theorem 9.5 for the statement of the result). The last section applies our methods to the question of existence of extremal even 3-modular lattices in dimension 36. Building upon the results of the thesis [14] we show that there is no such lattice admitting an automorphism of prime order > 7.

2. EXTREMAL MODULAR $\mathbb{Z}$-LATTICES

Our main motivation to consider Hermitian lattices stems from a long term project of the second author to classify automorphisms of extremal unimodular and modular lattices. Let $(V, \mathbf{q})$ be a positive definite rational quadratic space, so V is a vector space over $\mathbb{Q}$ and $\mathbf{q} : V \to \mathbb{Q}$ is a positive definite quadratic form with associated bilinear form $\mathbf{b_q} : V \times V \to \mathbb{Q}, \mathbf{b_q}(x, y) := \mathbf{q}(x + y) - \mathbf{q}(x) - \mathbf{q}(y)$. The dimension of V is denoted by m. Then a $\mathbb{Z}$-lattice L in $(V, \mathbf{q})$ is the integral span $L = \oplus_{i=1}^m \mathbb{Z}b_i$ of a basis $(b_1, \ldots, b_m)$ of V.

The *dual lattice* is

$$L^\# := \{v \in V \mid \mathbf{b_q}(v, \ell) \in \mathbb{Z} \text{ for all } \ell \in L\}.$$

We call L *unimodular* if $L = L^\#$ and *even* if $\mathbf{q}(L) \subseteq \mathbb{Z}$. For an even lattice L the quadratic form $\mathbf{q}$ defines a $\mathbb{Q}/\mathbb{Z}$-valued quadratic form $\mathbf{q}_L$ on the *discriminant group* $L^\#/L$ as

$$\mathbf{q}_L : L^\#/L \to \mathbb{Q}/\mathbb{Z}, \mathbf{q}_L(x + L) := \mathbf{q}(x) + \mathbb{Z}.$$

The *density* of the sphere packing associated to L can be read of from the two most important invariants of the lattice, its *minimum*

$$\min(L) := 2\min\{\mathbf{q}(\ell) \mid 0 \neq \ell \in L\} = \min\{\mathbf{b_q}(\ell, \ell) \mid 0 \neq \ell \in L\}$$

and its *determinant*

$$\det(L) = \mathrm{vol}((V \otimes \mathbb{R})/L)^2 = \det(\mathbf{b_q}(b_i, b_j)_{1 \leq i,j \leq m})$$

for any lattice basis $(b_1, \ldots, b_m)$ of L. The value of the *Hermite function* $\gamma(L) := \frac{\min(L)}{\det(L)^{1/m}}$ yields the density of the associated sphere packing as $\frac{V_m}{2^m}\sqrt{\gamma(L)}$ where V_m is the volume of the m-dimensional unit sphere. So the densest lattices in a given dimension are those that maximise the Hermite function. The densest lattices are known in dimensions up to 8 and in dimension 24 [3]. In particular in dimension 8 and 24 the densest lattices are even unimodular lattices. Even unimodular lattices are not only of interest as they often yield dense lattices, but also because of their relations to various other mathematical theories. The most important for us here is the relation to modular forms: The theta series of an even unimodular lattice is a modular form for the full modular group (see for instance [7] for an easily accessible reference). The theory of modular forms allows to bound the density of an even unimodular lattice:

Theorem 2.1. [34] *Let L be an even unimodular lattice. Then $m := \dim(L)$ is a multiple of 8 and $\min(L) \leq 2 + 2\lfloor\frac{m}{24}\rfloor$. If $\min(L) = 2 + 2\lfloor\frac{m}{24}\rfloor$ then L is called* extremal.

Of particular interest are the extremal even unimodular lattices of dimension a multiple of 24. There are 6 such extremal lattices known: The Leech lattice of dimension 24, which is the densest lattice of dimension 24 [3], four lattices of dimension 48, P_{48p}, P_{48q} [5], P_{48n} [21], and P_{48m} [24], and one extremal even unimodular lattice of dimension 72 [22]. These lattices are the densest known lattices in their dimension. Table 1 lists these lattices L and gives the group theoretic structure of their automorphism group

$$\text{Aut}(L) = \text{Aut}(L, \mathbf{q}) := \{g \in \text{GL}(V) \mid g(L) = L \text{ and } \mathbf{q}(g(\ell)) = \mathbf{q}(\ell) \text{ for all } \ell \in L\}$$

and the order $|\text{Aut}(L, \mathbf{q})|$ together with references for a construction of L and $\text{Aut}(L, \mathbf{q})$.

TABLE 1. The known extremal even unimodular lattices in the jump dimensions

L	$\text{Aut}(L)$	$\lvert\text{Aut}(L)\rvert$	ref.
Λ_{24}	$2.\text{Co}_1$	8315553613086720000	
		$= 2^{22}3^9 5^4 7^2 11\ 13\ 23$	[18, 4]
P_{48p}	$(\text{SL}_2(23) \times S_3){:}2$	$145728 = 2^6 3^2 11\ 23$	[5, 23]
P_{48q}	$\text{SL}_2(47)$	$103776 = 2^5 3\ 23\ 47$	[5, 23]
P_{48n}	$(\text{SL}_2(13)\text{Y}\text{SL}_2(5)).2^2$	$524160 = 2^7 3^2 5\ 7\ 13$	[21, 23]
P_{48m}	$(C_5 \times C_5 \times C_3){:}(D_8\text{Y}C_4)$	$1200 = 2^4 3\ 5^2$	[24]
Γ_{72}	$(\text{SL}_2(25) \times \text{PSL}_2(7)){:}2$	$5241600 = 2^8 3^2 5^2 7\ 13$	[22, 23]

Note that the a factor of 2 is missing in the order of the automorphism group of P_{48p} given in [23] and [24], whereas the structure of the group is printed correctly.

In dimension 24 all even unimodular lattices are classified in [27] and the Leech lattice is the unique extremal lattice. The classification of all even unimodular lattice in dimension 48 is not possible (there are more than $3 \cdot 10^{121}$ isometry classes of such lattices). Therefore the second author started a long term project to classify extremal lattices $(L, \mathbf{q})$ with a given automorphism $g \in \text{Aut}(L, \mathbf{q})$ (see [23, 24]). If the characteristic polynomial of g has an irreducible factor $f(X) \in \mathbb{Q}[X]$ of degree $> \frac{m}{2}$, then one can use ideals in the cyclotomic number field $\mathbb{Q}[X]/(f(X))$ (more precisely unary Hermitian lattices) to construct the extremal lattices L with $g \in \text{Aut}(L, \mathbf{q})$.

The general method is described in [23]: Let L be an even unimodular lattice in $(V, \mathbf{q})$ and let $g \in \text{Aut}(L)$ be of prime order p. Then $V = V_1 \oplus V_z$ is an orthogonal sum of two g-invariant subspaces, namely

$$V_1 = \ker(g - 1) = \{v \in V \mid g(v) = v\}$$

the eigenspace of g to the eigenvalue 1 and its orthogonal complement V_z. If $\Phi_p := (X^p - 1)/(X - 1)$ is the p-th cyclotomic polynomial, then g acts on V_z with characteristic polynomial $\chi_g = \Phi_p^{\dim(V_z)/(p-1)}$. Put $z := \dim(V_z)/(p-1)$ and $f := \dim(V_1)$.

Definition 2.2. *In the above situation the lattices $Z(g) := L \cap V_z$ and $F(g) := L \cap V_1$ are called the g-cyclotomic lattice and the g-fixed lattice of L respectively.*

Proposition 2.3. *(see [24, Section 2]) Let $Z = Z(g)$ and $F = F(g)$ be as in Definition 2.2. Then $|Z^\#/Z| = |F^\#/F| = p^s$ with*

$$s \leq \min(z, f) \text{ and } s \equiv z \pmod 2$$

The tuple $p - (z, f) - s$ is called the type of g.

To classify the lattices L with a given automorphism g we first find all candidates for lattices Z and F and then compute L as an even unimodular lattice with

$$Z \perp F \subseteq L = L^\# \subseteq Z^\# \perp F^\#.$$

Definition 2.4. *Let Z and F be even lattices in rational quadratic spaces $(V_1, \mathbf{q}_1)$ and $(V_2, \mathbf{q}_2)$ with automorphisms $\gamma \in \text{Aut}(Z)$ and $\gamma' \in \text{Aut}(F)$. Then a group isomorphism*

$$\varphi \colon Z^\#/Z \to F^\#/F$$

is called a (γ, γ')-anti-isometry if the following conditions hold:

(a) $\mathbf{q}_Z(z + Z) + \mathbf{q}_F(\varphi(z + Z)) = 0 \in \mathbb{Q}/\mathbb{Z}$ *for all* $z \in Z^\#$.

(b) *If* $\varphi(z + Z) = f + F$ *then* $\varphi(\gamma(z) + Z) = \gamma'(f) + F$ *for all* $z \in Z^\#$, *i.e.* φ *is a* $\mathbb{Z}[\gamma]$-$\mathbb{Z}[\gamma']$-*module isomorphism.*

Then the gluing procedure (see for instance [24]) is described in the following remark.

Remark 2.5. (a) In the situation of Definition 2.4 the lattice
$$L := L_\varphi := \{(z, f) \in Z^\# \perp F^\# \mid \varphi(z + Z) = f + F\}$$
is an even unimodular lattice in $(V_1, \mathbf{q}_1) \perp (V_2, \mathbf{q}_2)$ with $V_1 \cap L = Z$ and $V_2 \cap L = F$ and $(\gamma, \gamma') \in \mathrm{Aut}(L)$.
(b) Let $L = L^\#$ be an even unimodular lattice in $(V, \mathbf{q})$, $g \in \mathrm{Aut}(L)$ such that $V = V_1 \perp V_2$ is the orthogonal sum of two g-invariant subspaces. Put $Z := L \cap V_1$, $F := L \cap V_2$, $\gamma := g_{|Z}$, $\gamma' := g_{|F}$. Then there is a (γ, γ')-anti-isometry $\varphi \colon Z^\#/Z \to F^\#/F$ such that $L = L_\varphi$.

Let g, L, F, Z be as in Proposition 2.3. Then g acts trivially on F, hence on $F^\#/F$ and on the isomorphic module $Z^\#/Z$ so we obtain the following corollary.

Corollary 2.6. *Let* g, L, F, Z *be as in Proposition 2.3. Then* $(1 - g)(Z^\#) \subseteq Z$.

The notion of extremality has been generalized by H.G. Quebbemann [29] to modular lattices: Unimodular lattices L satisfy $L = L^\#$. Quebbemann calls an even lattice L *modular* of level p (for short p-*modular*) if there is an isomorphism $f \colon L^\# \to L$ of $\mathbb{Z}$-modules such that $\mathbf{q}(f(\ell)) = p\mathbf{q}(\ell)$ for all $\ell \in L^\#$. Such a map f is called a similarity of norm p and it satisfies $\det(f) = p^{n/2} = |L^\#/L|$. The following theorem transfers the result of Theorem 2.1 to p-modular lattices, putting $p = 1$ one obtains the bound in Theorem 2.1.

Theorem 2.7. [29] *Let* p *be a prime such that* $p + 1$ *divides* 24 *and let* L *be an even* p-*modular lattice of dimension* m. *Then* m *is even if* $p \equiv 3 \pmod 4$ *and* m *is a multiple of* 4 *if* $p = 2$ *or* $p \equiv 1 \pmod 4$. *Moreover*
$$\min(L) \le 2 + 2\lfloor \tfrac{m(p+1)}{48} \rfloor.$$
Even p-*modular lattices achieving equality are called* extremal.

For the current status of the classification of extremal modular lattices we refer to [14].

3. Hermitian forms

Let K be an algebraic number field, i.e. a finite extension field of $\mathbb{Q}$ and denote by $\mathbb{Z}_K$ its ring of integers. A *fractional ideal* I in K is a non-zero finitely generated $\mathbb{Z}_K$-submodule of K. The set of all fractional ideals forms a group $J(K)$ under ideal multiplication. It contains the subgroup
$$P(K) := \{\alpha\mathbb{Z}_K \mid 0 \ne \alpha \in K\}$$
of principal ideals and a famous theorem by Minkowski (see [19, Chapter V]) shows that the *ideal class group*
$$\mathrm{CL}(K) := J(K)/P(K)$$
is a finite abelian group. Its cardinality is called the *class number*
$$h_K := |\mathrm{CL}(K)|$$
of K.

If $d := [K : \mathbb{Q}] = \dim_\mathbb{Q}(K)$ denotes the degree of K over $\mathbb{Q}$ then there are d distinct embeddings
$$\sigma_1, \ldots, \sigma_d \colon K \hookrightarrow \mathbb{C}.$$
The number field K is called *totally real*, if $\sigma_i(K) \subseteq \mathbb{R}$ for all $1 \le i \le d$ and *totally complex* if $\sigma_i(K) \not\subseteq \mathbb{R}$ for all $1 \le i \le d$.

In this paper K will always denote a totally real number field. An element $a \in K$ is called *totally positive*, if $\sigma_i(a) > 0$ for all i. The group $P(K)$ of principal ideals contains a subgroup
$$P^+(K) := \{\alpha\mathbb{Z}_K \mid \alpha \in K \text{ totally positive}\}$$
of finite index (dividing 2^d). Hence the *narrow class group*
$$\mathrm{CL}^+(K) := J(K)/P^+(K)$$

is also finite. Its cardinality

$$h_K^+ := |\mathrm{CL}^+(K)|$$

is called the *narrow class number* of the totally real field K.

Let V be a finite dimensional vector space over K. A map $\mathbf{q}\colon V \to K$ is called a *quadratic form*, if

- $\mathbf{q}(av) = a^2\mathbf{q}(v)$ for all $a \in K$, $v \in V$ and
- $\mathbf{b_q}\colon V \times V \to K$, $\mathbf{b_q}(v,w) := \mathbf{q}(v+w) - \mathbf{q}(v) - \mathbf{q}(w)$ is a K-bilinear form on V.

The form $\mathbf{b_q}$ is called the associated symmetric bilinear form of the quadratic form $\mathbf{q}$. The quadratic form is called *non-degenerate*, if $\mathbf{b_q}$ is non-degenerate, i.e. $\mathbf{b_q}(x,v) = 0$ for all $v \in V$ implies that $x = 0$. The quadratic form $\mathbf{q}$ is called *positive definite* if $\mathbf{q}(v)$ is totally positive for all nonzero $v \in V$. In particular positive definite quadratic forms are non-degenerate.

Any non-degenerate quadratic form $\mathbf{q}$ defines an involution $\sigma_{\mathbf{q}}$ on $\mathrm{End}_K(V)$, the *adjoint involution*, where for $\varphi \in \mathrm{End}_K(V)$ the endomorphism $\sigma_{\mathbf{q}}(\varphi)$ is defined by

$$\mathbf{b_q}(w, \sigma_{\mathbf{q}}(\varphi)(v)) = \mathbf{b_q}(\varphi(w), v) \text{ for all } v, w \in V.$$

Clearly $\det(\sigma_{\mathbf{q}}(\varphi)) = \det(\varphi)$ for all $\varphi \in \mathrm{End}_K(V)$.

The *orthogonal group* of a non-degenerate quadratic space

$$\mathrm{O}(V, \mathbf{q}) := \{g \in \mathrm{End}_K(V) \mid \mathbf{q}(g(v)) = \mathbf{q}(v) \text{ for all } v \in V\}$$

is the set of all $g \in \mathrm{End}_K(V)$ satisfying $\sigma_{\mathbf{q}}(g)g = \mathrm{id}_V$. In particular $\det(g) \in \{-1, 1\}$ for all $g \in \mathrm{O}(V, \mathbf{q})$ and the special orthogonal group

$$\mathrm{SO}(V, \mathbf{q}) := \{g \in \mathrm{O}(V, \mathbf{q}) \mid \det(g) = 1\}$$

is a normal subgroup of $\mathrm{O}(V, \mathbf{q})$ of index 2. Two quadratic spaces $(V, \mathbf{q})$ and $(W, \mathbf{q}')$ are *isometric* if there is an isomorphism $\varphi\colon V \to W$ of K-vector spaces such that

$$\mathbf{q}'(\varphi(v)) = \mathbf{q}(v) \text{ for all } v \in V.$$

To define Hermitian forms we let E/K be a CM extension of number fields, so K is a totally real number field and E is a totally complex quadratic extension of K. Let $\mathrm{Gal}(E/K) =: \langle \sigma \rangle$.

Remark 3.1. With the notation above $E = K[\alpha]$ for some $\alpha \in E$ with $\sigma(\alpha) = -\alpha$ and $\delta := -\alpha^2 \in K$ is totally positive.

A Hermitian space $(V, \mathbf{h})$ over E consists of a vector space V over E together with a *Hermitian form* $\mathbf{h}\colon V \times V \to E$ such that

$$\mathbf{h}(v, w) = \sigma(\mathbf{h}(w, v)) \text{ and}$$
$$\mathbf{h}(\lambda v + \mu w, u) = \lambda \mathbf{h}(v, u) + \mu \mathbf{h}(w, u) \text{ for all } v, w, u \in V, \lambda, \mu \in E.$$

Two Hermitian spaces $(V, \mathbf{h})$ and $(W, \mathbf{h}')$ are *isometric*, if there is an isomorphism of E-vector spaces $\varphi\colon V \to W$ such that

$$\mathbf{h}'(\varphi(v), \varphi(v')) = \mathbf{h}(v, v') \text{ for all } v, v' \in V.$$

If $(V, \mathbf{h})$ is an m-dimensional Hermitian space, then V is a $2m$-dimensional vector space over K, which we denote by V_K, and $\mathbf{q_h}\colon V_K \to K, v \mapsto \mathbf{h}(v, v)$ is a quadratic form. For the associated bilinear form $\mathbf{b_{q_h}}$ we compute for $v, w \in V$

$$\mathbf{b_{q_h}}(v, w) = \mathbf{h}(v+w, v+w) - \mathbf{h}(v, v) - \mathbf{h}(w, w) = \mathbf{h}(v, w) + \mathbf{h}(w, v) = \mathbf{h}(v, w) + \sigma(\mathbf{h}(v, w))$$

so

$$\text{(1)} \qquad\qquad\qquad \mathbf{b_{q_h}} = \mathrm{Tr}_{E/K} \circ \mathbf{h}$$

where $\mathrm{Tr}_{E/K}\colon E \to K, \lambda \mapsto \lambda + \sigma(\lambda)$ is the trace of the Galois extension E/K. The Hermitian form $\mathbf{h}$ is called *positive definite* if $\mathbf{q_h}$ is positive definite and *non-degenerate*, if $\mathbf{b_{q_h}}$ is non-degenerate.

Starting with a non-degenerate Hermitian space $(V, \mathbf{h})$ we hence obtain a quadratic K-vector space $(V_K, \mathbf{q_h})$ together with an embedding $\nu\colon E \to \mathrm{End}_K(V)$. As

$$\mathbf{b_{q_h}}(\nu(\lambda)w, v) = \mathbf{h}(\lambda w, v) + \mathbf{h}(w, \lambda v) = \mathbf{h}(w, \sigma(\lambda)v) + \mathbf{h}(\sigma(\lambda)w, v) = \mathbf{b_{q_h}}(w, \nu(\sigma(\lambda))v)$$

for all $\lambda \in E$, $v, w \in V$ we see that the restriction of the involution $\sigma_{\mathbf{q_h}}$ to E coincides with the Galois automorphism σ, more precisely

$$\sigma_{\mathbf{q_h}}(\nu(\lambda)) = \nu(\sigma(\lambda)) \text{ for all } \lambda \in E.$$

On the other hand, starting with a non-degenerate quadratic space $(V, \mathbf{q})$ over K then any embedding $\varphi \colon E \hookrightarrow \mathrm{End}_K(V)$ defines an E-linear structure on V. If the restriction of the adjoint involution $\sigma_{\mathbf{q}}$ to $\varphi(E)$ is σ then

$$(2) \qquad \mathbf{h}_\varphi := \mathbf{h} \colon V \times V \to E, \mathbf{h}(x, y) := \frac{1}{2}\mathbf{b_q}(x, y) + \frac{1}{2\delta}\alpha\mathbf{b_q}(\varphi(\alpha)x, y)$$

is a Hermitian form on V with $\mathbf{q} = \mathbf{q_h}$. Here δ and α are as in Remark 3.1.

Definition 3.2. *Let $(V, \mathbf{q})$ be a non-degenerate quadratic space over K. A K-algebra homomorphism $\varphi \colon E \to \mathrm{End}_K(V)$ is called a* Hermitian embedding *if*

$$\varphi(\sigma(\lambda)) = \sigma_{\mathbf{q}}(\varphi(\lambda)) \text{ for all } \lambda \in E.$$

Clearly the *unitary group*

$$U(V, \mathbf{h}) = \{g \in \mathrm{End}_E(V) \mid \mathbf{h}(g(v), g(w)) = \mathbf{h}(v, w) \text{ for all } v, w \in V\}$$

of a non-degenerate Hermitian space embeds into the orthogonal group $\mathrm{O}(V_K, \mathbf{q_h})$. Even more is true: If $g \in U(V, \mathbf{h})$ then $\mathbf{h}(g(v), g(w)) = \mathbf{h}(v, w)$ for all $v, w \in V$. In particular the norm of the determinant of $g \in \mathrm{End}_E(V)$, which is the determinant of $g \in \mathrm{End}_K(V_K)$, is equal to 1 (see [31, Theorem 10.1.5]) and hence

$$U(V, \mathbf{h}) \hookrightarrow \mathrm{SO}(V, \mathbf{q_h}).$$

On the other hand, given a quadratic space $(V, \mathbf{q})$ over K and a Hermitian embedding $\varphi \colon E \to \mathrm{End}_K(V)$, then the unitary group is

$$U(V, \mathbf{h}_\varphi) = \{g \in \mathrm{O}(V, \mathbf{q}) \mid g\varphi(e) = \varphi(e)g \text{ for all } e \in E\}.$$

Theorem 3.3. *Let $(V, \mathbf{q})$ be a quadratic space over K. Then $\mathrm{O}(V, \mathbf{q})$ acts transitively on the set of all Hermitian embeddings $\varphi \colon E \to \mathrm{End}_K(V)$.*

Proof. By [31, Theorem (10.1.1)] two Hermitian spaces $(V, \mathbf{h})$ and $(V', \mathbf{h}')$ are isometric, if and only if the quadratic spaces $(V_K, \mathbf{q_h})$ and $(V'_K, \mathbf{q_{h'}})$ are isometric. As any Hermitian embedding $\varphi \colon E \to \mathrm{End}_K(V)$ defines a Hermitian space $(V, \mathbf{h}_\varphi)$ with $\mathbf{q}_{\mathbf{h}_\varphi} = \mathbf{q}$ the statement follows. □

4. Hermitian lattices

Let $(V, \mathbf{h})$ be a Hermitian space over E, where E and K are as in the previous section. By $\mathbb{Z}_E$ and $\mathbb{Z}_K$ we denote their respective rings of integers. The *different* of E/K is

$$D_{E/K} := \{x \in E \mid \mathrm{Tr}_{E/K}(x\mathbb{Z}_E) \subseteq \mathbb{Z}_K\}^{-1} \subseteq \mathbb{Z}_E,$$

which is always an ideal in $\mathbb{Z}_E$. The extension E/K is *unramified* if and only if $D_{E/K} = \mathbb{Z}_E$.

Let R be one of $\mathbb{Z}_E$ or $\mathbb{Z}_K$. An R-*lattice* L in V is a finitely generated R-submodule of V that contains a K-basis of V, i.e. $KL = V$. For a fractional ideal $\mathfrak{a}$ in K an R-lattice L is said to be $\mathfrak{a}$-*integral*, if

$$\mathbf{q_h}(L) = \{\mathbf{q_h}(\ell) \mid \ell \in L\} \subseteq \mathfrak{a}.$$

An $\mathfrak{a}$-integral lattice L is called $\mathfrak{a}$-*maximal* if L is not contained in any other $\mathfrak{a}$-integral lattice. We call a lattice L *maximal* if it is $\mathfrak{a}$-maximal for some ideal $\mathfrak{a}$. Denote by $\mathcal{G}_\mathfrak{a}(V, \mathbf{h})$ the set of all $\mathfrak{a}$-maximal $\mathbb{Z}_E$-lattices in $(V, \mathbf{h})$. For a quadratic space $(V, \mathbf{q})$ over K let $\mathcal{G}_\mathfrak{a}(V, \mathbf{q})$ the set of all $\mathfrak{a}$-maximal $\mathbb{Z}_K$-lattices in $(V, \mathbf{q})$ in $(V, \mathbf{q})$.

Proposition 4.1. *Any $\mathfrak{a}$-maximal $\mathbb{Z}_E$-lattice in $(V, \mathbf{h})$ is an $\mathfrak{a}$-maximal $\mathbb{Z}_K$-lattice in $(V, \mathbf{q_h})$. So $\mathcal{G}_\mathfrak{a}(V, \mathbf{h}) \subseteq \mathcal{G}_\mathfrak{a}(V_K, \mathbf{q_h})$.*

Proof. Let L be an $\mathfrak{a}$-maximal $\mathbb{Z}_E$-lattice. Then L is an $\mathfrak{a}$-integral $\mathbb{Z}_K$-lattice. Assume that L is not $\mathfrak{a}$-maximal as $\mathbb{Z}_K$-lattice. Then there is some $x \in V \setminus L$ such that $L + \mathbb{Z}_K x$ is $\mathfrak{a}$-integral. It suffices to show the $\mathbb{Z}_E$-lattice $L + \mathbb{Z}_E x$ is $\mathfrak{a}$-integral. To see this let $\lambda \in \mathbb{Z}_E$ and $\ell \in L$. Then

$$(3) \qquad \mathbf{h}(\ell + \lambda x, \ell + \lambda x) = \mathbf{h}(\ell, \ell) + \lambda\sigma(\lambda)\mathbf{h}(x, x) + \lambda\mathbf{h}(x, \ell) + \sigma(\lambda)\mathbf{h}(\ell, x).$$

Putting $\ell' = \sigma(\lambda)\ell \in L$, the sum of the last two summands in (3) is

(4)
$$\lambda\mathbf{h}(x,\ell) + \sigma(\lambda)\mathbf{h}(\ell,x) = \mathbf{h}(x,\ell') + \sigma(\mathbf{h}(x,\ell')) = \mathrm{Tr}_{E/K}(\mathbf{h}(x,\ell')) = \mathbf{b_{q_h}}(x,\ell')$$
$$= \mathbf{q_h}(\ell' + x) - \mathbf{q_h}(\ell') - \mathbf{q_h}(x).$$

The right hand side of Equation (4) lies in $\mathfrak{a}$ because $L + \mathbb{Z}_K x$ is $\mathfrak{a}$-integral. For the same reason $\mathbf{h}(\ell, \ell) = \mathbf{q_h}(\ell)$ and $\mathbf{h}(x,x) = \mathbf{q_h}(x)$ also lie in $\mathfrak{a}$. As $\lambda\sigma(\lambda) \in \mathbb{Z}_K$ and one sees that the right hand side of Equation (3) lies in $\mathfrak{a}$ so $L + \mathbb{Z}_E x$ is an $\mathfrak{a}$-integral $\mathbb{Z}_E$-lattice. $\square$

For a $\mathbb{Z}_K$-lattice $L \leq (V, \mathbf{q})$ we define the *dual lattice*

$$L^* := (L, \mathbf{q})^* := \{v \in V \mid \mathbf{b_q}(v,\ell) \in \mathbb{Z}_K \text{ for all } \ell \in L\}.$$

Lemma 4.2. *Let $L \leq (V, \mathbf{q})$ be such that $\mathbf{q}(L) \subseteq \mathbb{Z}_K$ and $L^* = L$. Then $L \in \mathcal{G}_{\mathbb{Z}_K}(V, \mathbf{q})$.*

Proof. Clearly $(L, \mathbf{q})$ is $\mathbb{Z}_K$-integral, so it is enough to show its maximality. Assume that there exists some $x \in V$, such that $L + \mathbb{Z}_K x$ is $\mathbb{Z}_K$-integral. Then for all $\ell \in L$

$$\mathbf{q}(x + \ell) = \mathbf{q}(x) + \mathbf{q}(\ell) + \mathbf{b_q}(x,\ell) \in \mathbb{Z}_K$$

hence also $\mathbf{b_q}(x, L) \subseteq \mathbb{Z}_K$ and therefore $x \in L^* = L$. $\square$

Similarly, given a $\mathbb{Z}_E$-lattice L in $(V, \mathbf{h})$ then the *Hermitian dual lattice* is

$$L^* := (L, \mathbf{h})^* := \{v \in V \mid \mathbf{h}(v, \ell) \in \mathbb{Z}_E \text{ for all } \ell \in L\}.$$

Then by Equation (1) $(L, \mathbf{h})^* = D_{E/K}(L, \mathbf{q_h})^*$. The lattice L is called *Hermitian unimodular* if $L = (L, \mathbf{h})^*$. Note that Hermitian unimodular lattices are $\mathbb{Z}_K$-integral, but in general not maximal.

Lemma 4.3. *If E/K is unramified at all finite places then any Hermitian unimodular lattice in $(V, \mathbf{h})$ is $\mathbb{Z}_K$-maximal.*

Proof. Assume that there exists some $x \in V$, such that $L + \mathbb{Z}_E x$ is $\mathbb{Z}_K$-integral. Then for all $\ell \in L$ and all $\alpha \in \mathbb{Z}_E$

$$\mathbf{q_h}(\alpha x + \ell) = \mathbf{q_h}(\alpha x) + \mathbf{q_h}(\ell) + \mathrm{Tr}_{E/K}\mathbf{h}(\alpha x, \ell) \in \mathbb{Z}_K$$

hence $\mathbf{h}(x, L) \subseteq D_{E/K}$. As E/K is unramified we have $D_{E/K} = \mathbb{Z}_E$ so $x \in L^* = L$. $\square$

Two $\mathbb{Z}_K$-lattices $(L, \mathbf{q})$ and $(L', \mathbf{q}')$ are called *isometric*, if there is an isomorphism $\varphi \colon L \to L'$ of $\mathbb{Z}_K$-modules such that $\mathbf{q}'(\varphi(\ell)) = \mathbf{q}(\ell)$ for all $\ell \in L$. The *isometry group* $\mathrm{Aut}(L, \mathbf{q})$ is the group of all self isometries $\varphi \colon (L, \mathbf{q}) \to (L, \mathbf{q})$. It contains the group of proper automorphisms

$$\mathrm{Aut}^+(L, \mathbf{q}) := \mathrm{Aut}(L, \mathbf{q}) \cap \mathrm{SO}(KL, \mathbf{q}) = \{g \in \mathrm{Aut}(L, \mathbf{q}) \mid \det(g) = 1\}$$

as a normal subgroup of index at most 2.

Similarly we define isometries of Hermitian $\mathbb{Z}_E$-lattice $(L, \mathbf{h})$ and $(L', \mathbf{h}')$ as the $\mathbb{Z}_E$-module isomorphisms $\varphi \colon L \to L'$ that are compatible with the Hermitian forms i.e. $\mathbf{h}'(\varphi(\ell_1), \varphi(\ell_2)) = \mathbf{h}(\ell_1, \ell_2)$ for all $\ell_1, \ell_2 \in L$ and the *Hermitian isometry group* is denoted by $\mathrm{Aut}_{\mathbb{Z}_E}(L, \mathbf{h})$.

Remark 4.4. Let $L \leq (V, \mathbf{h})$ be a $\mathbb{Z}_E$-lattice. Then $(L, \mathbf{q_h})$ is a $\mathbb{Z}_K$-lattice in $(V_K, \mathbf{q_h})$ and the natural embedding defines a Hermitian embedding $\nu \colon \mathbb{Z}_E \to \mathrm{End}_{\mathbb{Z}_K}(L)$.

The $\mathbb{Z}_K$-isometry group $\mathrm{Aut}_{\mathbb{Z}_K}(L, \mathbf{q})$ of a $\mathbb{Z}_K$-lattice in a quadratic space $(V, \mathbf{q})$ over K acts on the set of all Hermitian embeddings $\varphi \colon \mathbb{Z}_E \to \mathrm{End}_{\mathbb{Z}_K}(L)$ by conjugation.

Proposition 4.5. *Given a $\mathbb{Z}_K$-lattice $(L, \mathbf{q}) \leq (V, \mathbf{q})$ then the set of all isometry classes of Hermitian $\mathbb{Z}_E$-lattices $(L, \mathbf{h})$ such that $\mathbf{q_h} = \mathbf{q}$ is in bijection with the set of $\mathrm{Aut}_{\mathbb{Z}_K}(L, \mathbf{q})$-orbits on the set of all Hermitian embeddings $\varphi \colon \mathbb{Z}_E \to \mathrm{End}_{\mathbb{Z}_K}(L)$.*

Proof. By the remark above the set of all Hermitian $\mathbb{Z}_E$-structures on $(L, \mathbf{q})$ is in bijection to the set of all Hermitian embeddings $\varphi \colon \mathbb{Z}_E \to \mathrm{End}_{\mathbb{Z}_K}(L)$. Let φ and ψ be two such embeddings. We

need to show that $(L, \mathbf{h}_\varphi) \cong (L, \mathbf{h}_\psi)$ if and only if there is an automorphism $g \in \mathrm{Aut}_{\mathbb{Z}_K}(L, \mathbf{q})$ such that $\varphi(e)g = g\psi(e)$ for all $e \in \mathbb{Z}_E$. By the definition of h_φ in Equation (2) any such g yields

$$
\begin{aligned}
\mathbf{h}_\varphi(g(x), g(y)) &= \tfrac{1}{2}\mathbf{b}_\mathbf{q}(g(x), g(y)) + \tfrac{1}{2\delta}\alpha\mathbf{b}_\mathbf{q}(\varphi(\alpha)g(x), g(y)) \\
&= \tfrac{1}{2}\mathbf{b}_\mathbf{q}(g(x), g(y)) + \tfrac{1}{2\delta}\alpha\mathbf{b}_\mathbf{q}(g(\psi(\alpha)x), g(y)) \\
&= \tfrac{1}{2}\mathbf{b}_\mathbf{q}(x, y) + \tfrac{1}{2\delta}\alpha\mathbf{b}_\mathbf{q}(\psi(\alpha)x, y)\alpha \\
&= \mathbf{h}_\psi(x, y)
\end{aligned}
$$

for all $x, y \in L$. On the other hand, any isometry between $(L, \mathbf{h}_\varphi)$ and $(L, \mathbf{h}_\psi)$ is an automorphism of L, preserving the quadratic form $\mathbf{q}(x) = \mathbf{h}_\varphi(x, x) = \mathbf{h}_\psi(x, x)$ so it defines an element of $\mathrm{Aut}_{\mathbb{Z}_K}(L, \mathbf{q})$. $\qquad\square$

For a $\mathbb{Z}_K$-lattice $(L, \mathbf{q})$ in the quadratic space $(V, \mathbf{q})$ let

$$[(L, \mathbf{q})] := \{(g(L), \mathbf{q}) \mid g \in \mathrm{O}(V, \mathbf{q})\} \text{ and } [(L, \mathbf{q})]^+ := \{(g(L), \mathbf{q}) \mid g \in \mathrm{SO}(V, \mathbf{q})\}$$

denote its *isometry class* respectively *proper isometry class* in $(V, \mathbf{q})$.

The following theorem summarizes the results of this section and will yield a 2-step method to determine all isometry classes of $\mathfrak{a}$-maximal Hermitian $\mathbb{Z}_E$-lattices in a Hermitian space $(V, \mathbf{h})$. We first determine a set

$$\{(L_1, \mathbf{q_h}), \ldots, (L_s, \mathbf{q_h})\}$$

of representatives of isometry classes in the set $\mathcal{G}_\mathfrak{a}(V_K, \mathbf{q_h})$. For each $1 \leq i \leq s$ we compute a set

$$\{\varphi_{ij} \mid 1 \leq j \leq k_i\}$$

of representatives of $\mathrm{Aut}_{\mathbb{Z}_K}(L_i, \mathbf{q_h})$-orbits on the set of Hermitian embeddings $\mathbb{Z}_E \to \mathrm{End}_{\mathbb{Z}_K}(L_i)$. By Theorem 3.3 there are $g_{ij} \in \mathrm{O}(V_K, \mathbf{q_h})$ such that the natural embedding ν from Remark 4.4 is of the form

$$\nu = g_{ij} \circ \varphi_{ij} \circ g_{ij}^{-1}.$$

Theorem 4.6. *The set*

$$\{(g_{ij}(L_i), \mathbf{h}) \mid 1 \leq i \leq s, 1 \leq j \leq k_i\}$$

is a set of representatives of the isometry classes in the set $\mathcal{G}_\mathfrak{a}(V, \mathbf{h})$ of $\mathfrak{a}$-maximal Hermitian $\mathbb{Z}_E$-lattices in $(V, \mathbf{h})$.

Example 4.7. To illustrate the theorem in an easy example let $(V, \mathbf{q})$ be the rational quadratic space of dimension 8 with an orthonormal basis. Up to isometry there exists a unique $\mathbb{Z}$-maximal lattice $(L, \mathbf{q})$ in $(V, \mathbf{q})$. This lattice is the even unimodular lattice $\mathbb{E}_8$ from Section 2. We consider the field $E = \mathbb{Q}[\sqrt{-5}]$, so $\mathbb{Z}_E = \mathbb{Z}[\sqrt{-5}]$. To determine all Hermitian embeddings $\varphi \colon \mathbb{Z}_E \to \mathrm{End}_\mathbb{Z}(L)$ up to conjugation by $G := \mathrm{Aut}(L, \mathbf{q})$ we first note that it is enough to find all $y = \varphi(\sqrt{-5}) \in \mathrm{End}_\mathbb{Z}(L)$ such that $y^2 = -5$ and $\mathbf{q}(y\ell) = 5\mathbf{q}(\ell)$ for all $\ell \in L$. For such y the sublattice yL maps onto a maximal isotropic subspace of $(L/5L, \overline{\mathbf{q}})$, where $\overline{\mathbf{q}}(\ell+5L) = \mathbf{q}(\ell)+5\mathbb{Z} \in \mathbb{Z}/5\mathbb{Z} = \mathbb{F}_5$. Hence we start to compute representatives of the G-orbits on the set of all 39312 such maximal isotropic spaces. There are two such orbits of length 15120 and 24192 represented by the sublattices L_1 and L_2 say. We then determine for each lattice L_i one endomorphism $x_i \in \mathrm{End}(V)$ that yields an isometry $x_i \colon (L, \mathbf{q}) \to (L_i, \tfrac{1}{5}\mathbf{q})$. Any other such isometry is of the form $x_i \circ g$ for some $g \in G$. By a random search we found $g_i \in G$ such that $y_i = x_i \circ g_i$ satisfies $y_i^2 = -5$. For $i = 1, 2$ let

$$Y_i := \{y_i \circ g \mid g \in G, \; (y_i \circ g)^2 = -5\}.$$

If $y_i \circ g \in Y_i$ then $g \in \mathrm{Stab}_G(L_i)$ because $(y_i \circ g)^2 = y_i^2$ implies that $g \circ y_i \circ g = y_i$ and hence

$$g(L_i) = g(y_i(L)) = (g \circ y_i \circ g)(L) = y_i(L) = L_i.$$

This allows to compute the set Y_i on which $\mathrm{Stab}_G(L_i)$ acts by conjugation with 2 resp. 1 orbits represented by, say, $y_1, y_1' \in Y_1$ and $y_2 \in Y_2$. So we get three orbits of Hermitian embeddings with $|\mathrm{Aut}(L, \mathbf{h}_1)| = 384$, $|\mathrm{Aut}(L, \mathbf{h}_1')| = 1920$ and $|\mathrm{Aut}(L, \mathbf{h}_2)| = 480$.

An important coarser equivalence relation than isometry is provided by genera of lattices: Given a place $\mathfrak{p}$ of K, let $K_{\mathfrak{p}}$ and $V_{\mathfrak{p}} := V \otimes_K K_{\mathfrak{p}}$ be the completions of K and V at $\mathfrak{p}$. If $\mathfrak{p}$ is finite, we denote by $\mathbb{Z}_{K_{\mathfrak{p}}}$ and $L_{\mathfrak{p}} := L \otimes_{\mathbb{Z}_K} \mathbb{Z}_{K_{\mathfrak{p}}}$ the completions of $\mathbb{Z}_K$ and L at $\mathfrak{p}$.

Two $\mathbb{Z}_E$-lattices $(L, \mathbf{h})$ and $(L', \mathbf{h})$ in $(V, \mathbf{h})$ are *in the same genus*, if $(L_{\mathfrak{p}}, \mathbf{h}) \cong (L'_{\mathfrak{p}}, \mathbf{h})$ for every maximal ideal $\mathfrak{p}$ of $\mathbb{Z}_K$. More details can be found for instance in [13].

It is well known that a genus always consists of finitely many isometry classes of Hermitian lattices, the number of which is called the *class number* of the genus. In our situation, $\mathbf{q_h}$ is positive definite and so $\mathrm{Aut}_{\mathbb{Z}_E}(L, \mathbf{h})$ is a finite group. Then the *mass of the genus* is

$$\mathrm{mass}(L, \mathbf{h}) := \sum_{i=1}^{h} |\mathrm{Aut}_{\mathbb{Z}_E}(L_i, \mathbf{h})|^{-1}$$

where the L_i represent the isometry classes of lattices in the genus of $(L, \mathbf{h})$. There are analytic formulas to compute the mass of a genus, see for instance [10].

If two (quadratic or Hermitian) lattices lie in the same genus, then, by the Hasse principle, the underlying (quadratic or Hermitian) spaces are isometric. For a complete discrete valuation ring, any two maximal lattices in a quadratic or Hermitian space are isometric (see [28, Theorem 91:2] and [33, Proposition 4.13]). Hence the set $\mathcal{G}_{\mathfrak{a}}(V, \mathbf{h})$ forms a genus of Hermitian lattices.

There is a well known method to enumerate representatives of isometry classes of lattices in a genus, the Kneser neighbouring method [17]. In Example 4.7 it would be easier to apply this method directly (see for instance [32]). In Section 7 below and the following examples however, we are facing situations where this method fails due to the fact that the class number of the genus is quite large and the usual isometry tests of Hermitian lattices are too expensive.

5. DUALITY AND TRANSFER

As in the previous section let $(V, \mathbf{h})$ be a totally positive definite Hermitian space over E. Then V is also a vector space over $\mathbb{Q}$ of dimension $\dim_{\mathbb{Q}}(V) = \dim_E(V) \cdot [E : \mathbb{Q}]$ and the composition of the quadratic form $\mathbf{q_h}$ with the trace of K over $\mathbb{Q}$ defines a positive definite quadratic form

$$\mathrm{Tr}(\mathbf{q_h}) := \mathrm{Tr}_{K/\mathbb{Q}} \circ \mathbf{q_h} \colon V \to \mathbb{Q}, v \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(\mathbf{q_h}(v)).$$

On the other hand starting with a positive definite rational quadratic space $(V, \mathbf{q})$ the adjoint defines an involution

$$^{-} \colon \mathrm{End}_{\mathbb{Q}}(V) \to \mathrm{End}_{\mathbb{Q}}(V), \alpha \mapsto \overline{\alpha} \text{ with } \mathbf{b_q}(\alpha(x), y) = \mathbf{b_q}(x, \overline{\alpha}(y)) \text{ for all } x, y \in V.$$

Remark 5.1. Let $(V, \mathbf{q})$ be a positive definite rational quadratic space of dimension m. Assume that $\alpha \in \mathrm{End}_{\mathbb{Q}}(V)$ has an irreducible minimal polynomial, i.e. $E := \mathbb{Q}[\alpha] = \langle 1, \alpha, \alpha^2, \dots \alpha^{e-1} \rangle_{\mathbb{Q}}$ is a field of degree $e := [E : \mathbb{Q}]$, say. If $\alpha \neq \overline{\alpha} \in \mathbb{Q}[\alpha]$ then $^{-} \colon E \to E$ is a field automorphism of order 2 and $K := \{x \in E \mid \overline{x} = x\}$ is a subfield of index 2 in E. The embedding of E into $\mathrm{End}_{\mathbb{Q}}(V)$ turns V into a vector space of dimension m/e over E and there is a unique Hermitian form $\mathbf{h} \colon V \to E$ such that $\mathbf{q} = \mathrm{Tr}_{K/\mathbb{Q}}(\mathbf{q_h})$. More precisely for $x, y \in V$ we determine $\mathbf{h}(x, y) \in E$ as the unique element in E with

$$\mathrm{Tr}_{E/\mathbb{Q}}(\alpha^i \mathbf{h}(x, y)) = \mathbf{b_q}(\alpha^i(x), y) \text{ for all } 0 \leq i \leq e - 1.$$

Any $\mathbb{Z}_E$-lattice L in $(V, \mathbf{h})$ is a $\mathbb{Z}$-lattice in the quadratic space $(V, \mathrm{Tr}_{K/\mathbb{Q}}(\mathbf{q_h}))$. This $\mathbb{Z}$-lattice $(L, \mathrm{Tr}(\mathbf{q_h}))$ is called the *trace lattice* of $(L, \mathbf{h})$.

The following relation between the Hermitian dual lattice L^* and the dual of the trace lattice is well known.

Lemma 5.2. *For a $\mathbb{Z}_E$-lattice L in $(V, \mathbf{h})$ we have*

$$D_{E/\mathbb{Q}} \cdot (L, \mathrm{Tr}_{K/\mathbb{Q}}(\mathbf{q_h}))^{\#} = (L, \mathbf{h})^*.$$

Proof. For $x \in V$ we compute

$$
\begin{aligned}
x \in (L, \mathrm{Tr}_{K/\mathbb{Q}}(\mathbf{q_h}))^{\#} &\iff \mathrm{Tr}_{E/\mathbb{Q}}(\mathbf{h}(x, L)) \subseteq \mathbb{Z} \\
&\iff \mathbf{h}(x, L) \subseteq D_{E/\mathbb{Q}}^{-1} \\
&\iff D_{E/\mathbb{Q}} \cdot x \subseteq (L, \mathbf{h})^* .
\end{aligned}
$$
$\square$

Similarly as for vector spaces in Remark 5.1 certain automorphisms of lattices define a unique Hermitian structure:

Remark 5.3. Let $(L, \mathbf{q})$ be a positive definite $\mathbb{Z}$-lattice and suppose that $g \in \mathrm{Aut}(L, \mathbf{q})$ has an irreducible minimal polynomial. Then $E := \mathbb{Q}[g] \subseteq \mathrm{End}_{\mathbb{Q}}(\mathbb{Q}L)$ is a cyclotomic field with maximal totally real subfield $K := \mathbb{Q}[\alpha]$ where $\alpha = g + g^{-1} = g + \bar{g}$ and $^-$ is as in Remark 5.1. With respect to $\mathbf{h}$ from Remark 5.1, the lattice $(L, \mathbf{h})$ hence becomes a Hermitian $\mathbb{Z}_E$-lattice such that $(L, \mathrm{Tr}_{K/\mathbb{Q}}(\mathbf{q_h})) = (L, \mathbf{q})$.

Let $(L, \mathbf{q})$ be an even unimodular $\mathbb{Z}$-lattice and $g \in \mathrm{Aut}(L)$ be an element of odd prime order p. Let $p - (z, f) - s$ be the type of g and let Z, F be as in Proposition 2.3. Then by Remark 5.3 the lattice Z is a $\mathbb{Z}_E$-lattice in a totally positive definite Hermitian space $(V, \mathbf{h})$, where $E = \mathbb{Q}[\zeta_p]$. By Corollary 2.6 as a $\mathbb{Z}_E$-lattice

$$(1 - \zeta_p)Z^\# \underbrace{\subseteq}_{p^{z-s}} Z \underbrace{\subseteq}_{p^s} Z^\# \underbrace{\subseteq}_{p^{z-s}} (1 - \zeta_p)^{-1}Z.$$

Put $T := (1 - \zeta_p)^{(p-3)/2}Z$. With respect to the Hermitian form $\mathbf{h}$ from Remark 5.1 we compute

$$(1 - \zeta_p)T \underbrace{\subseteq}_{p^s} (T, \mathbf{h})^* \underbrace{\subseteq}_{p^{z-s}} T$$

in particular $M := T^*$ is an integral Hermitian $\mathbb{Z}_E$-lattice in $(V, \mathbf{h})$. To determine $\det(\mathbf{h})$, we compute the Jordan decomposition of M as described in [13]. Let $\pi := (1 - \zeta_p)(1 - \zeta_p^{-1})$ and $\mathfrak{p} := \pi\mathbb{Z}_K$ be the prime ideal of $\mathbb{Z}_K$ over p where $K := \mathbb{Q}[\zeta_p + \zeta_p^{-1}]$. The lattice M has a Jordan decomposition $M_\mathfrak{p} = M_0 \perp M_1$ where $M_0 = M_0^*$ is a unimodular lattice of rank s, M_1 has rank $z - s$ and $(1 - \zeta_p)M_1^* = M_1$. Hence M_1 is isometric to an orthogonal sum of $(z - s)/2$ copies of a rescaled hyperbolic plane $\begin{pmatrix} 0 & 1-\zeta_p \\ 1-\zeta_p^{-1} & 0 \end{pmatrix}$ and M_0 has an orthogonal basis, $M_0 \sim \langle 1, \ldots, 1, u \rangle$ for some unit $u \in \mathbb{Z}_{K_\mathfrak{p}}^*$ such that $u(-\pi)^{(z-s)/2}$ represents the class of $\det(\mathbf{h})$ modulo norms. Note that this provides an alternative proof of the fact that $z \equiv s \pmod 2$ (see [23, Lemma 4.3]).

Lemma 5.4. *In the situation above $(V, \mathbf{h})$ contains a Hermitian unimodular lattice and $\det(\mathbf{h}) = 1$.*

Proof. A unimodular lattice $\tilde{M}$ in $(V, \mathbf{h})$ can be constructed as the lattice that coincides with M at all finite places $\neq \mathfrak{p}$ and is a unimodular overlattice of $M_0 \perp M_1$ in $(V_\mathfrak{p}, \mathbf{h})$. To compute the determinant we note that E/K is ramified only at the place $\mathfrak{p}$ and at the infinite places of K. Moreover $\mathbf{h}$ is totally positive definite. Hence $\det(\mathbf{h})$ is a norm at all infinite places of K. Since $\tilde{M}$ is Hermitian unimodular at all finite places, the determinant $\det(\mathbf{h})$ is a norm at all places different from $\mathfrak{p}$. By the Hasse Norm Theorem, $\det(\mathbf{h})$ must be a norm of some element of E. □

6. Quaternion algebras and quaternary quadratic lattices

In this section we state the results of [15] and the necessary background that is needed in the next section to develop an algorithm for the classification of binary Hermitian lattices. A detailed discussion of the arithmetic of quaternion algebras can be found in [8], [36] and [30]. Let K be a totally real number field as before. For totally positive $a, b \in K$ the *quaternion algebra*

$$Q = \left(\frac{-a, -b}{K}\right)$$

has a basis $(1, i, j, ij)$ with $ij = -ji$ and $i^2 = -a$, $j^2 = -b$. It carries a canonical involution, $^- \colon Q \to Q$ defined by $\overline{t + xi + yj + zij} = t - xi - yj - zij$. The reduced norm

$$n \colon Q \to K, n(\alpha) = \alpha\overline{\alpha}$$

of Q is a quaternary positive definite quadratic form over K such that $n(\alpha\beta) = n(\alpha)n(\beta)$ for all $\alpha, \beta \in Q$. In particular $\alpha^{-1} = \overline{\alpha}/n(\alpha)$ for $\alpha \in Q \setminus \{0\} =: Q^*$ shows that Q is a division algebra.

For $\alpha, \beta \in Q^*$ the map

$$\tau_{\alpha, \beta} \colon Q \to Q, x \mapsto \alpha x \beta^{-1}$$

is an isometry, if and only if $n(\alpha) = n(\beta)$. It is well known, see e.g. [6, Appendix IV, Proposition 3] or [20, Proposition 4.3] that the group of proper isometries of the quadratic space (Q, n) is

$$\mathrm{SO}(Q, n) = \{\tau_{\alpha,\beta} \mid \alpha, \beta \in Q^*, \ n(\alpha) = n(\beta)\}$$

The canonical involution $^-$ of Q is an improper isometry of (Q, n), so the full orthogonal group $\mathrm{O}(Q, n)$ is generated by the normal subgroup $\mathrm{SO}(Q, n)$ and the canonical involution $^-$.

An *order* in Q is a $\mathbb{Z}_K$-lattice that is a subring of Q. An order $\mathcal{M}$ is called *maximal* if it is not contained in any other order. The unit group Q^* of Q acts on the set of all maximal orders in Q by conjugation with finitely many orbits. We fix a system of representatives

$$\mathcal{M}_1, \ldots, \mathcal{M}_t$$

of the conjugacy classes of maximal orders in Q. The number t is called the *type number* of Q.

The stabilizer of a maximal order $\mathcal{M}$ in Q under this action is

$$N(\mathcal{M}) := \{\alpha \in Q^* \mid \alpha \mathcal{M} \alpha^{-1} = \mathcal{M}\}$$

the *normaliser* of $\mathcal{M}$ in Q^*.

For a $\mathbb{Z}_K$-lattice J in Q we define the *left* and *right orders* of J as

$$O_\ell(J) := \{\alpha \in Q \mid \alpha J \subseteq J\} \text{ and } O_r(J) := \{\alpha \in Q \mid J\alpha \subseteq J\}.$$

A *right ideal* J of the maximal order $\mathcal{M}$ is a $\mathbb{Z}_K$-lattice J in Q such that $O_r(J) = \mathcal{M}$. Then also the left order $O_\ell(J)$ is a maximal order, hence there is some $i := i(J) \in \{1, \ldots, t\}$ such that $O_\ell(J)$ is conjugate to $\mathcal{M}_i$.

Proposition 6.1. *(see* [15, Proposition 3.7]*)*

$$\mathrm{Aut}^+(J, n) = \{\tau_{\alpha,\beta} \mid (\alpha, \beta) \in N(O_\ell(J)) \times N(O_r(J)), n(\alpha) = n(\beta)\}.$$

The *norm* $n(J)$ of a $\mathbb{Z}_K$-lattice J is the fractional ideal of $\mathbb{Z}_K$ generated by the norms of the elements in J,

$$n(J) := \sum_{\gamma \in J} \mathbb{Z}_K n(\gamma).$$

Two right ideals I, J of $\mathcal{M}$ are called *left-equivalent*, if there is some $\alpha \in Q^*$ such that $I = \alpha J$. We denote by $[J] = \{\alpha J \mid \alpha \in Q^*\}$ the left equivalence class of the right ideal J. Clearly $n(\alpha J) = n(\alpha)n(J)$ and hence the map $[n]$ from the set of left-equivalence classes of right ideals of $\mathcal{M}$ into the narrow class group $\mathrm{CL}^+(K)$, defined by $[n]([J]) = n(J)P^+(K)$ is well defined. Also the left orders of two left-equivalent right ideals of $\mathcal{M}$ are conjugate.

Any right ideal J defines a certain subgroup $U(J)$ of finite (2-power) index in the group $\mathbb{Z}_{K,>0}^*$ of totally positive units of $\mathbb{Z}_K$ (see [15, Proposition 3.7]) more precisely

$$U(J) := \{n(\alpha)n(\beta^{-1}) \mid \alpha \in N(O_\ell(J)), \beta \in N(O_r(J)), n(\alpha)n(\beta^{-1}) \in \mathbb{Z}_K^*\}.$$

We note that $(\mathbb{Z}_K^*)^2 \subseteq U(J) \subseteq \mathbb{Z}_{K,>0}^*$ and that $U(J)$ only depends on the conjugacy classes of the left and right orders of J.

Let $\mathfrak{a} \in J(K)$ be some fractional $\mathbb{Z}_K$-ideal. A system of representatives of proper isometry classes of lattices in $\mathcal{G}_\mathfrak{a}(Q, n)$ can be obtained by [15, Algorithm 7.1] as follows.

Let $\mathcal{M}$ be some maximal order in Q and let $(I_1, \ldots, I_h)$ be a system of representatives of left-equivalence classes of right ideals of $\mathcal{M}$. For $1 \leq i \leq t$ set

$$S_i := \{I_j \mathcal{M}_i \mid 1 \leq j \leq h \text{ and } [n][I_j\mathcal{M}_i] = \mathfrak{a}P^+(K)\}.$$

If $g \in N(\mathcal{M}_i)$ and $I \in S_i$ then there exists a unique lattice $J \in S_i$ such that J is left-equivalent to Ig^{-1}. This yields an action of the normaliser $N(\mathcal{M}_i)$ on S_i. For $1 \leq i \leq t$ compute a system of orbit representatives T_i of this action. For $J \in \bigcup_i T_i$ fix some totally positive generator a_J of $n(J)^{-1}\mathfrak{a}$. Then by the Theorem of Hasse-Schilling-Maass, there is some $x_J \in Q^*$ such that $n(x_J) = a_J$. For all $u(\mathbb{Z}_K^*)^2 \in \mathbb{Z}_{K,>0}^*/(\mathbb{Z}_K^*)^2$ compute some $\alpha_u \in Q^*$ such that $n(\alpha_u) = u$.

Theorem 6.2. [15, Algorithm 7.1] *The set*

$$R_\mathfrak{a} := \{(\alpha_u x_J J, n) \mid J \in \bigcup_i T_i \text{ and } uU(J) \in \mathbb{Z}_{K,>0}^*/U(J)\}$$

is a system of representatives of proper isometry classes of lattices in $\mathcal{G}_\mathfrak{a}(Q, n)$.

For later use we note that the *mass* of the quaternion algebra Q is defined as

$$\text{mass}(Q) := \sum_{i=1}^{h} [O_\ell(I_i)^* : \mathbb{Z}_K^*]^{-1}.$$

As for the mass of the genus of lattices there are analytic formulas (see for instance [8]) to compute the mass of Q from local invariants.

7. Binary Hermitian lattices

In this section we use Theorem 6.2 and Proposition 4.5 to classify binary Hermitian $\mathbb{Z}_E$-lattices: Given a 2-dimensional totally positive definite Hermitian space $(V, \mathbf{h})$ over E, the associated quadratic space $(V, \mathbf{q_h})$ is a quaternary totally positive definite quadratic space over K. By [31, Chapter 10, Remark 1.4] the determinant of $(V, \mathbf{q_h})$ is a square in K and the Clifford invariant is the class of the quaternion algebra

$$Q_\mathbf{h} := \left(\frac{-\delta, -\det(\mathbf{h})}{K} \right),$$

where, as in Section 4, $E = K[\alpha]$ with $\alpha^2 = -\delta \in K$. In particular E is a maximal subfield of $Q_\mathbf{h}$ and $Q_\mathbf{h}$ is a 2-dimensional vector space over E.

A Theorem of Hasse (see [11]) implies that $(V, \mathbf{q_h})$ is isometric to $(Q_\mathbf{h}, n)$. As the restriction of the canonical involution of $Q_\mathbf{h}$ to E is the non-trivial Galois automorphism σ of E/K, the natural embedding $\nu \colon E \to Q_\mathbf{h} \subseteq \text{End}_K(Q_\mathbf{h})$ is a Hermitian embedding and the norm form n gives rise to a Hermitian form $\mathbf{h}_n := \mathbf{h}_\nu$ on the 2-dimensional E-vector space $Q_\mathbf{h}$, such that $(Q_\mathbf{h}, \mathbf{h}_n) \cong (V, \mathbf{h})$.

To classify all Hermitian embeddings of E with respect to n we identify $\text{End}_K(Q_\mathbf{h})$ with $Q_\mathbf{h}^{op} \otimes Q_\mathbf{h}$ where $Q_\mathbf{h}^{op}$ denotes the opposite algebra of $Q_\mathbf{h}$.

Lemma 7.1. *Let $\varphi \colon E \to \text{End}_K(Q_\mathbf{h})$ be a Hermitian embedding with respect to n. Then*

$$\varphi(E) \subseteq Q_\mathbf{h}^{op} \otimes K \ \text{or} \ \varphi(E) \subseteq K \otimes Q_\mathbf{h}.$$

Proof. Write $E = K[\alpha]$ with $\sigma(\alpha) = -\alpha$ and $\alpha^2 \in K$ and let $Q_\mathbf{h}^0 := \{x \in Q_\mathbf{h} \mid x + \overline{x} = 0\}$ be the 3-dimensional K-subspace of trace 0 elements in $Q_\mathbf{h}$. The restriction of the adjoint involution of n to $Q_\mathbf{h}^{op} \otimes K$ and to $K \otimes Q_\mathbf{h}$ is the canonical involution of $Q_\mathbf{h}$ resp. $Q_\mathbf{h}^{op} \cong Q_\mathbf{h}$. In particular the 6-dimensional space $(Q_\mathbf{h}^{op})^0 \otimes K \oplus K \otimes Q_\mathbf{h}^0$ is contained in the space of skew symmetric elements (with respect to the adjoint involution of $K^{4 \times 4}$ induced by the symmetric bilinear form $\mathbf{b}_n$). As this space is of dimension 6, we conclude that $\varphi(\alpha)$, being skew symmetric, is of the form

$$\varphi(\alpha) = 1 \otimes x + y \otimes 1$$

for suitable $x \in Q_\mathbf{h}^0, y \in (Q_\mathbf{h}^{op})^0$. Now $\varphi(\alpha)^2 = y^2 \otimes 1 + 1 \otimes x^2 + 2y \otimes x \in K$ implies that $x = 0$ or $y = 0$, so $\varphi(\alpha) = 1 \otimes x \in K \otimes Q_\mathbf{h}$ or $\varphi(\alpha) = y \otimes 1 \in Q_\mathbf{h}^{op} \otimes K$. $\square$

By Theorem 3.3 the orthogonal group acts transitively on the set of Hermitian embeddings by conjugation. For the special case of quaternion algebras we can prove this more directly:

Proposition 7.2. *Up to the action of $\text{O}(Q_\mathbf{h}, n)$ there is a unique Hermitian embedding $\varphi \colon E \to \text{End}_K(Q_\mathbf{h})$.*

Proof. Recall that all proper isometries of $(Q_\mathbf{h}, n)$ are of the form $\tau_{\alpha,\beta} \colon x \mapsto \alpha x \beta^{-1}$ with $\alpha, \beta \in Q_\mathbf{h}^*, n(\alpha) = n(\beta)$ and that the canonical involution $x \mapsto \overline{x}$ is an improper isometry $\bar{}$. Given a Hermitian embedding $\varphi \colon E \to \text{End}_K(Q_\mathbf{h})$ with values $\varphi(E) \subseteq Q_\mathbf{h}^{op} \otimes K$, the conjugate by $\bar{}$ yields a Hermitian embedding with values in $K \otimes Q_\mathbf{h}$. By the Theorem of Skolem and Noether any two embeddings φ_1, φ_2 of E into $Q_\mathbf{h} \cong K \otimes Q_\mathbf{h}$ are conjugate in $Q_\mathbf{h}^*$. So there is some $a \in Q_\mathbf{h}^*$ such that $a\varphi_1 a^{-1} = \varphi_2$. The proper isometry $\tau_{a^{-1}, a}$ hence conjugates φ_1 into φ_2. $\square$

The ring of integers $\mathbb{Z}_E$ also embeds into $Q_\mathbf{h}$, so there is some maximal order $\mathcal{M}$ in $Q_\mathbf{h}$ containing $\mathbb{Z}_E$. The lattice $(\mathcal{M}, n)$ is hence a Hermitian $\mathbb{Z}_E$-lattice L in $(Q_\mathbf{h}, \mathbf{h}_n)$, maximal with respect to the condition that $n(\ell) = \mathbf{h}_n(\ell, \ell) \in \mathbb{Z}_K$ for all $\ell \in L$, so

$$(\mathcal{M}, n) \in \mathcal{G}_{\mathbb{Z}_K}(Q_\mathbf{h}, \mathbf{h}_n)$$

(see [15, Proposition 3.2] and Proposition 4.1).

By Lemma 7.1 the image $\varphi(\mathbb{Z}_E)$ of a Hermitian embedding into $\mathrm{End}_{\mathbb{Z}_K}(L)$ is either contained in the left or in the right order of L. After conjugation with the improper isometry given by the canonical involution of $Q_{\mathbf{h}}$ we may assume without loss of generality that $\varphi(\mathbb{Z}_E)$ is contained in the right order, so L is a right ideal of some maximal order $\mathcal{M}$ that contains $\varphi(\mathbb{Z}_E)$.

Remark 7.3. To compute all Hermitian embeddings $\varphi\colon \mathbb{Z}_E \hookrightarrow \mathcal{M}$ for a given maximal order $\mathcal{M}$ we choose some $\alpha \in \mathbb{Z}_E$ with $\sigma(\alpha) = -\alpha$ and $\alpha^2 = -\delta \in \mathbb{Z}_K$.

We first find all elements $x \in \mathcal{M}$ with $x^2 = -\delta$ and $\overline{x} = -x$. These elements lie in the sublattice $\mathcal{M}^0$ of trace 0 elements in $\mathcal{M}$. The map

$$\mathrm{Tr} \circ n\colon \mathcal{M}^0 \to \mathbb{Z}, y \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(n(y))$$

defines a positive definite quadratic form on the $\mathbb{Z}$-lattice $\mathcal{M}^0$. Clearly $\mathrm{Tr} \circ n(x) = \mathrm{Tr}_{K/\mathbb{Q}}(\delta) =: a \in \mathbb{Z}_{>0}$. Using the shortest vector algorithm [9] we enumerate the vectors v of norm a in the $\mathbb{Z}$-lattice $(\mathcal{M}^0, \mathrm{Tr}(n))$ and then check whether $v^2 = -\delta$. For these v the map $\alpha \mapsto v$ then defines an embedding φ of E into $Q_{\mathbf{h}}$. It yields an embedding of $\mathbb{Z}_E$ into $\mathcal{M}$ if and only if $\varphi(\mathbb{Z}_E) \subseteq \mathcal{M}$.

Let $\mathcal{M}_1, \ldots, \mathcal{M}_t$ be, as before, a system of representatives of the conjugacy classes of maximal orders in $Q_{\mathbf{h}}$. After rearranging the maximal orders, we assume that there is a Hermitian embedding $\varphi\colon \mathbb{Z}_E \to \mathcal{M}_i$ for $i = 1, \ldots, t_0$ and no such embedding for $i > t_0$.

For $1 \leq i \leq t$ and $1 \leq j \leq t_0$ let J be a right ideal of $\mathcal{M}_j$ such that the left order $O_\ell(J)$ is conjugate to $\mathcal{M}_i$. Then the set of all $\beta \in N(\mathcal{M}_j)$ such that there is some $\alpha \in N(O_\ell(J))$ with $\tau_{\alpha,\beta} \in \mathrm{Aut}^+(J)$ (see Proposition 6.1) is

$$N_{ij} := \{\beta \in N(\mathcal{M}_j) \mid \exists \alpha \in N(\mathcal{M}_i),\ n(\alpha) = n(\beta)\}.$$

Note that

$$\mathcal{M}_j^{(1)} := \{\beta \in \mathcal{M}^* \mid n(\beta) = 1\}$$

is always a subgroup of N_{ij}.

Let $\varphi\colon \mathbb{Z}_E \to \mathcal{M}_j$ be a Hermitian embedding. Then for $\tau_{\alpha,\beta} \in \mathrm{Aut}^+(J)$ and $x \in \mathbb{Z}_E$ we compute for all $\gamma \in J$:

$$\tau_{\alpha,\beta} \circ \varphi(x) \circ \tau_{\alpha,\beta}^{-1}(\gamma) = \tau_{\alpha,\beta}(\alpha^{-1}\gamma\beta\varphi(x)) = \gamma(\beta\varphi(x)\beta^{-1})$$

so $\tau_{\alpha,\beta} \cdot \varphi = \beta \cdot \varphi$, hence we get

Remark 7.4. The set of $\mathrm{Aut}^+(J)$-orbits on the set of all Hermitian embeddings $\varphi\colon \mathbb{Z}_E \to \mathcal{M}_j$ is in bijection to the set of all N_{ij}-orbits on the set of all Hermitian embeddings $\varphi\colon \mathbb{Z}_E \to \mathcal{M}_j$. Let Φ_{ij} be a system of representatives of these orbits.

Combining Theorem 6.2 with Proposition 4.5 we finally obtain the following Theorem.

Theorem 7.5. *Keep the notation of Theorem 6.2. The set*

$$\{(\alpha_u x_J J, \mathbf{h}_\varphi)\colon (J, \varphi) \in \bigcup_{j=1}^{t_0} (T_j, \Phi_{i_J, j}), uU(J) \in \mathbb{Z}_{K,>0}^*/U(J)\}$$

is a system of representatives of isometry classes of lattices in $\mathcal{G}_{\mathfrak{a}}(Q_{\mathbf{h}}, \mathbf{h}_n)$.

The most important case in this paper is that E is a cyclotomic number field, so $E = \mathbb{Q}[\zeta_o]$ and $K = \mathbb{Q}[\zeta_o + \zeta_o^{-1}]$ with $o \not\equiv 2 \pmod 4$. Then $\alpha := \zeta_o - \zeta_o^{-1}$ satisfies $\alpha^2 = -\delta$ with

$$\delta = 2 - \zeta_o^2 - \zeta_o^{-2} = 4 - (\zeta_o + \zeta_o^{-1})^2 \in K.$$

Suppose that o is not a prime power. Then E/K is unramified and we often can apply the following remark to obtain the quaternion algebra $Q_{\mathbf{h}} = \left(\frac{-\delta, -\det(\mathbf{h})}{K}\right)$.

Remark 7.6. Assume that E/K is unramified and that there is a $\mathbb{Z}_E$-lattice L in $(V, \mathbf{h})$ such that the $\mathbb{Z}_K$-dual $(L, \mathbf{q}_{\mathbf{h}})^* = \mathfrak{a}L$ for some fractional $\mathbb{Z}_K$-ideal $\mathfrak{a}$. Then $\det(\mathbf{h}) = a\sigma(a)$ for some $a \in E$. and $Q_{\mathbf{h}} = \left(\frac{-\delta, -1}{K}\right)$.

Proof. As E/K is unramified every fractional $\mathbb{Z}_K$-ideal is a norm, in particular there is some fractional $\mathbb{Z}_E$-ideal $\mathfrak{A}$ such that $\mathfrak{a} = \mathfrak{A}\sigma(\mathfrak{A})$. Replacing L by $\mathfrak{A}^{-1}L$ we obtain a unimodular $\mathbb{Z}_K$-lattice in $(V, \mathbf{q_h})$ and hence may assume that $\mathfrak{a} = \mathbb{Z}_K$. For all prime ideals $\mathfrak{P}$ of $\mathbb{Z}_E$ the $\mathbb{Z}_{E_{\mathfrak{P}}}$-lattice $(L_{\mathfrak{P}}, \mathbf{h})$ has an orthonormal basis (see for example [13, Proposition 4.1]). So locally everywhere $\det(\mathbf{h})$ is a norm. As $\det(\mathbf{h})$ is totally positive the Hasse norm principle ([26, Korollar VI.4.5]) shows that there exists an element $a \in E$ such that $\det(\mathbf{h}) = a\sigma(a)$. Hence $Q_{\mathbf{h}} = \left(\frac{-\delta, -1}{K} \right)$ by the usual rules for Hilbert symbols (see for instance [28, 63:10]). $\qquad\square$

Example 7.7. For illustration we apply our methods to the situation of [15, Example 7.3] for $K = \mathbb{Q}[\sqrt{15}]$ and $Q = \left(\frac{-1, -1}{K} \right)$. We take $E := K[\sqrt{-\epsilon}]$ where $\epsilon := 4 + \sqrt{15}$ is the fundamental unit of $\mathbb{Z}_K$. Then E embeds into the quaternion algebra Q giving rise to a Hermitian structure $(Q, \mathbf{h}_n)$.

[15, Example 7.3] shows that the type number of Q is 8 and lists 8 maximal orders $\mathcal{M}_i$ ($1 \leq i \leq 8$) to which we refer in the following. To find representatives of the isometry classes of Hermitian lattices in $\mathcal{G}_{(\sqrt{15}^{-1})}(Q, \mathbf{h}_n)$ we consider the 14 proper isometry classes of $\mathbb{Z}_K$-lattices in $\mathcal{G}_{(\sqrt{15}^{-1})}(Q, n)$ represented by $(\mathcal{M}_i\mathcal{M}_j, \alpha_{ij}n)$ with

$$(i, j) \in \{1, 7\} \times \{5, 8\} \cup \{2, 3, 6\} \times \{4\} \cup \{4\} \times \{2, 3, 6\} \cup \{5, 8\} \times \{1, 7\}.$$

Only those $\mathcal{M}_i\mathcal{M}_j$ are relevant, for which there is a Hermitian embedding $\varphi_j \colon \mathbb{Z}_E \hookrightarrow \mathcal{M}_j$. We compute that such an embedding exists if and only if $j \in \{2, 4, 5, 7\}$. Moreover in all cases the group N_{ij} acts transitively on these embeddings. So there are 8 isometry classes of Hermitian lattices in $\mathcal{G}_{(\sqrt{15}^{-1})}(Q, \mathbf{h})$. represented by

$$(\mathcal{M}_i\mathcal{M}_j, \alpha_{ij}h_{\varphi_j}) \text{ where } (i, j) \in \{(4, 2), (2, 4), (3, 4), (6, 4), (1, 5), (7, 5), (5, 7), (8, 7)\}.$$

8. BINARY UNIMODULAR LATTICES OVER CERTAIN CYCLOTOMIC FIELDS

In this section we restrict to the case where $E = \mathbb{Q}[\zeta_p]$ for some prime $p \equiv 3 \pmod 4$ and K is its maximal totally real subfield $\mathbb{Q}[\zeta_p + \zeta_p^{-1}]$. To classify the genus of binary unimodular Hermitian $\mathbb{Z}_E$-lattices let $Q := \left(\frac{-1, -p}{K} \right)$ be the quaternion algebra over K ramified at the $\frac{p-1}{2}$ infinite places of K and the finite place over p. Then E embeds into Q and hence there is some maximal order $\mathcal{M}$ that contains $\mathbb{Z}_E = \mathbb{Z}[\zeta_p]$. In fact, such a maximal order can be constructed as the enveloping order of the quaternion group Q_{4p} of order $4p$ as

$$\mathcal{M} = \langle 1, \zeta_p, \sigma, \sigma\zeta_p \rangle_{\mathbb{Z}_K}$$

where $\sigma^2 = -1$ and $\sigma\zeta_p\sigma^{-1} = \zeta_p^{-1}$ (see for example [20, Theorem 6.1]). The Hermitian lattice $(\mathcal{M}, \mathbf{h}_n)$ is isometric to the standard Hermitian $\mathbb{Z}_E$-lattice of dimension 2, and hence the $\mathbb{Z}$-trace lattice of the $\mathbb{Z}_K$-lattice $(\mathcal{M}, \frac{1}{p}n)$ is isometric to the dual lattice of the root lattice $\mathbb{A}_{p-1} \perp \mathbb{A}_{p-1}$.

8.1. **Class number of Hermitian lattices.** In general there are no analytic formulas for the class number of a given genus. However, for binary Hermitian unimodular $\mathbb{Z}[\zeta_p]$-lattices (p a prime $\equiv 3 \pmod 4$) this number can be obtained from the type number t of the associated quaternion algebra Q, provided that $h_K^+ = 1$ (which is the case for $p < 163$ assuming GRH (see [37, p. 421])). An analytic formula for t can be found in [36, Corollaire V.2.6].

Proposition 8.1. *Let $p \equiv 3 \pmod 4$ be a prime, $K = \mathbb{Q}[\zeta_p + \zeta_p^{-1}]$, $E = \mathbb{Q}[\zeta_p]$, and $Q := \left(\frac{-1, -p}{K} \right)$ be as above. Assume that $h_K^+ = 1$. Then h_E is odd and the class number of the genus of Hermitian unimodular binary $\mathbb{Z}_E$-lattices is $h_E t$ where t is the type number of Q.*

Proof. We first note that the condition on the narrow class number $h_K^+ = 1$ implies that $\mathbb{Z}_{K,>0}^* = (\mathbb{Z}_K^*)^2$ and hence the group $U(J)$ from Theorem 6.2 equals $\mathbb{Z}_{K,>0}^*$.

Let $\mathcal{M}_1, \ldots, \mathcal{M}_t$ represent the conjugacy classes of maximal orders in Q. We may assume $\mathcal{M}_1 = \mathcal{M}$ with $\mathcal{M}^{(1)} \cong Q_{4p}$. As the norm 1 units $\mathcal{M}^{(1)}$ generate the order $\mathcal{M}$ as a $\mathbb{Z}_K$-lattice, the order $\mathcal{M}$ is the unique maximal order in Q with norm 1 group of order $4p$. Let $\mathcal{M}_2, \ldots, \mathcal{M}_a$ be the other maximal orders $\mathcal{M}_i$ into which $\mathbb{Z}_E$ embeds. Then by [35] $\mathcal{M}_i^{(1)} \cong C_{2p}$ for $i = 2, \ldots, a$. Choose an Hermitian embedding $\varphi_i \colon \mathbb{Z}_E \to \mathcal{M}_i$ and denote by $z_i := \varphi_i(\zeta_p) \in \mathcal{M}_i$. For all these $i = 1, \ldots, a$ the normaliser is

$$N(\mathcal{M}_i) = \langle \mathcal{M}_i^{(1)}, 1 - z_i, K^* \rangle.$$

It acts on the set of $\mathbb{Z}_K$-linear embeddings $\varphi \colon \mathbb{Z}_E \to \mathcal{M}_i$ with the same orbits as $\mathcal{M}_i^{(1)}$. In particular there is one such orbit for $i = 1$ and two orbits for $i = 2, \dots, a$ represented by φ_i and $\zeta_p \mapsto \varphi_i(\zeta_p^{-1})$, and the total number of embeddings is $1 + 2(a - 1) = 2a - 1$. By [36, Corollaire III.5.12] this number is exactly the class number of E, so $h_E = 2a - 1$ is odd.

By Theorem 6.2 we need to compute for all $1 \le i \le a$ a set of representatives T_i or the $N(\mathcal{M}_i)$-orbits on the left-equivalence classes in S_i. These orbits are of the form

$$[I] \cdot N(\mathcal{M}_i) = \{[I], [I(1 - z_i)]\}.$$

We claim that $|[I] \cdot N(\mathcal{M}_i)| = H(O_\ell(I))$ is the two-sided class number of the left order of I. To see this we first remark that the fact that $h_K = 1$ implies that the classes of 2-sided ideals of any maximal order $\mathcal{M}$ are represented by $\mathcal{M}$ and its maximal ideal $\mathcal{P}$ of norm p. So $H(\mathcal{M}) = 1$ if and only if $\mathcal{P} = \beta\mathcal{M}$ with $\beta \in N(\mathcal{M})$ of norm p. On the other hand $|[I] \cdot N(\mathcal{M}_i)| = 1$, if and only if there is some $b \in Q^*$ such that

$$bI = I(1 - z_i).$$

Of course the left order of I is

$$O_\ell(I) = O_\ell(I(1 - z_i)) = O_\ell(bI)$$

so b normalizes $O_\ell(I)$. Moreover the norm of b is the norm of $1 - z_i$, so $bO_\ell(I)$ generates the maximal ideal of $O_\ell(I)$ of norm p and therefore $H(O_\ell(I)) = 1$.

The fact that $|[I] \cdot N(\mathcal{M}_i)| = H(O_\ell(I))$ shows that T_i contains exactly one ideal with left order conjugate to $\mathcal{M}_j$ for any $1 \le j \le t$. More precisely T_i can be chosen as

$$T_i = \{\mathcal{M}_j \mathcal{M}_i \mid 1 \le j \le t\}$$

and has exactly t elements. So by Theorem 7.5 the number of isometry classes of Hermitian $\mathbb{Z}_E$-lattices in the genus of $(\mathcal{M}, \mathbf{h}_n)$ is $h_E t$. $\square$

Remark 8.2. The conclusion that h_E is odd can also be derived from a much more general result due to Hasse as follows. The assumption that $h_K^+ = 1$ implies that $h_K = 1$ as well as that the units in $\mathbb{Z}_K^*$ yield every possible sign combination at the real places of K. Moreover, p is the only ramified prime in E and it is non-split in K. By [12, Satz 42] these conditions are sufficient for h_E to be odd.

8.2. **Examples for small primes** p**.** To give more meaning to our results and also because of the application to the classification of extremal unimodular lattices, we study the binary Hermitian lattices over $\mathbb{Z}[\zeta_p]$ in the context of even unimodular $\mathbb{Z}$-lattices. So let p be a prime $p \equiv 3 \pmod 4$ and let Q be the quaternion algebra as in Proposition 8.1.

Remark 8.3. Let L be an even unimodular $\mathbb{Z}$-lattice of dimension $2(p - 1) + 4$ that admits an automorphism $g \in \operatorname{Aut}(L)$ of type $p - (2, 4) - 2$. Let Z, F be as in Proposition 2.3. Then there is a Hermitian unimodular lattice $\Lambda \le (Q, \mathbf{h}_n)$ such that

$$(Z^{\#}, p\mathbf{q}) \cong (\Lambda, \operatorname{Tr}_{K/\mathbb{Q}}(n)).$$

The lattice F is a quaternary quadratic lattice over the rationals with $\det(F) = p^2$. Putting $Q' = \left(\frac{-1, -p}{\mathbb{Q}}\right)$ to be the quaternion algebra with centre $\mathbb{Q}$ ramified only at p and the infinite place then $(F, \mathbf{q}) \in \mathcal{G}_{\mathbb{Z}}(Q', n')$. So we can use our method to determine the possible F and Z. Given such F and Z, there are exactly $2(p + 1)$ even unimodular $\mathbb{Z}$-lattices containing $F \perp Z$ of index p^2. All these even unimodular lattices have an automorphism g of order p and type $p - (2, 4) - 2$.

Due to the growth of the computational complexity we only treat the primes $p = 3, 7, 11, 19, 23$. For all these p the narrow class number of K is $h_K^+ = 1$ and we may apply Proposition 8.1.

For $p = 3$ and $p = 7$ the order $\mathcal{M}$ is the unique maximal order, so the genus of the Hermitian unimodular $\mathbb{Z}_E$-lattices of dimension 2 only consists of the class of the standard lattice. Also the set $\mathcal{G}_{\mathbb{Z}}(Q', n')$ from Remark 8.3 consists of a unique isometry class and the even unimodular $\mathbb{Z}$-lattices obtained in Remark 8.3 are all isometric to the root lattice $\mathbb{E}_8$ (for $p = 3$) respectively $\mathbb{E}_8 \perp \mathbb{E}_8$ (for $p = 7$).

For $p = 11$ we compute that $h_E = 1$, so the order $\mathcal{M}$ is the unique maximal order that contains $\mathbb{Z}[\zeta_p]$ (see [36, Corollaire III.5.12]). The type number of Q is the class number of $\mathcal{M}$ and equal to 2. The other lattice in the genus of $(\mathcal{M}, \mathbf{h}_n)$ has dual trace lattice of minimum 4. Also $\mathcal{G}_{\mathbb{Z}}(Q', n')$ from Remark 8.3 contains a unique isometry class of lattices of minimum 4. One finds the Leech lattice, the unique extremal even unimodular lattice of dimension 24, as an overlattice of minimum 4 of the orthogonal sum of these two lattices.

8.2.1. $p = 19$. For $p = 19$ again $h_E = 1$ and hence by [36, Corollaire III.5.12] the order $\mathcal{M}$ from above is the unique maximal order that contains $\mathbb{Z}[\zeta_p]$. With [2] we compute the type number t of Q as $t = 185$ so also the class number of the genus of $(\mathcal{M}, \mathbf{h}_n)$ is 185 by Proposition 8.1. As we are mainly interested in the trace lattices, we group these 185 lattices into orbits under the Galois group $\mathrm{Gal}(E/\mathbb{Q}) \cong C_{18}$ and obtain in total 23 orbits, two of them have length 1, one has length 3, and the other 20 orbits have length 9. So we obtain in total 23 isometry classes of dual trace lattices Z, one of which has minimum 2 and the other 22 lattices have minimum 4.

To classify extremal even unimodular lattices of dimension 40 with an automorphism of order 19 we need to find all unimodular overlattices M of $Z \perp F$ where Z is one of these 22 lattices and F the unique 4-dimensional 19-modular lattice of minimum 4 (cf. Remark 8.3). By Remark 2.5 we hence need to classify the anti-isometries $\varphi \colon (Z^\#/Z, \mathbf{q}_Z) \to (F^\#/F, \mathbf{q}_F)$. The automorphism group of F has 5 orbits on the set of these isometries, so each of the 22 lattices Z gives rise to 5 lattices M. Among the 110 lattices M, 12 come in isometric pairs, hence we have shown:

Corollary 8.4. *There are exactly* 104 *isometry classes of extremal even unimodular lattices of dimension* 40 *that admit an automorphism of order* 19.

Proof. It just remains to show that all automorphisms of order 19 of an extremal even unimodular lattice M of dimension 40 have characteristic polynomial $(X^{19}-1)^2(X-1)^2$. The other possibility would be $(X^{19}-1)(X-1)^{21}$. Then M contains a sublattice $Z \perp F$ of index 19 such that Z has determinant 19 and is an ideal lattice in $\mathbb{Z}[\zeta_{19}]$. As this ring has class number 1 and also $h_K^+ = 1$ we conclude that Z is the root lattice $\mathbb{A}_{18}$ which has minimum 2. $\qquad\square$

8.2.2. $p = 23$. The case $p = 23$ is of particular interest in the classification of 48-dimensional extremal even unimodular lattices. In the moment one knows 4 such extremal lattices, two of which have an automorphism of order 23 (Table 3). If 23 divides the order of the automorphism group of such a lattice, then by [23, Theorem 4.4] the elements of order 23 have type $23 - (2, 4) - 2$ and these lattices are constructed as in Remark 8.3. Our computations described below show the following corollary.

Corollary 8.5. *There are exactly two isometry classes of extremal even unimodular lattices of dimension* 48 *that admit an automorphism of order* 23.

Let $K = \mathbb{Q}[\zeta_{23} + \zeta_{23}^{-1}]$ be the maximal totally real subfield of $E = \mathbb{Q}[\zeta_{23}]$. The narrow class number of K is $h_K^+ = 1$ and the class number of E is $h_E = 3$. For $Q = \left(\frac{-1, -23}{K}\right)$ we compute the type number $t = 16393$ and the class number $h = 32651$. So by Proposition 8.1 the genus of binary Hermitian unimodular $\mathbb{Z}_E$-lattices consists of exactly $3 \cdot 16393$ isometry classes. Out of these only 12 have dual trace lattices of minimum ≥ 6, all coming from lattices of the first maximal order $\mathcal{M}$. These 12 dual trace lattices fall into two isometry classes of $\mathbb{Z}$-lattices, 11 of them are isometric to the orthogonal complement of the fixed lattice of an element of order 23 in $\mathrm{Aut}(P_{48q}) \cong \mathrm{SL}_2(47)$ and the other one to the respective sublattice of P_{48p} with $\mathrm{Aut}(P_{48p}) \cong (\mathrm{SL}_2(23) \times S_3).2$. Computing the overlattices from Remark 8.3 we conclude that these two extremal even unimodular lattices are the only ones that allow an automorphism of order 23.

Note that the result of Corollary 8.5 cannot easily be established by enumerating the genus of binary Hermitian unimodular $\mathbb{Z}_E$-lattices using Kneser's neighbour method directly, simply because the computation of isometries between such lattices is very time and memory consuming.

9. SEMILARGE AUTOMORPHISMS OF 48-DIMENSIONAL EXTREMAL EVEN UNIMODULAR LATTICES

Let $(L, \mathbf{q})$ be an even unimodular $\mathbb{Z}$-lattice of dimension m as in Section 2. For $g \in \mathrm{Aut}(L)$ we say that g is *large* if its characteristic polynomial χ_g has an irreducible factor of degree $> \frac{m}{2}$. The

papers [23] and [25] use ideal lattices to classify extremal even unimodular lattices of dimension 48 and 72 that admit a large automorphism.

Definition 9.1. *An automorphism g of an m-dimensional lattice is called* semilarge, *if χ_g has an irreducible factor of degree $> \frac{m}{4}$ that occurs with multiplicity 2.*

Table 2 gives the number of conjugacy classes of semilarge elements in the automorphism group of the four known extremal even unimodular lattices of dimension 48. The summands are in bijection with the conjugacy classes of subgroups generated by the respective semilarge automorphism. So the first entry $8 + 4 + 4$ contains the information that $\mathrm{Aut}(P_{48p})$ contains 16 conjugacy classes of semilarge elements of order 48, generating subgroups that fall into 3 conjugacy classes.

TABLE 2. The semilarge automorphisms of the four known extremal lattices P_{48pqnm}.

order	48	60	33	44	23	35	39	52	56	84
P_{48p}	8+4+4	-	5	5	1	-	-	-	-	-
P_{48q}	8	-	-	-	11	-	-	-	-	-
P_{48n}	-	2	-	-	-	3	1	1	3+3	3
P_{48m}	-	-	-	-	-	-	-	-	-	-

As $\mathrm{Aut}(L)$ is a finite group, any element $g \in \mathrm{Aut}(L)$ is an element of $\mathrm{GL}_m(\mathbb{Q})$ of finite order, so χ_g is a product of cyclotomic polynomials

$$\chi_g = \prod_{i=1}^{s} \Phi_{a_i}^{e_i}$$

where the roots in $\mathbb{C}$ of the irreducible polynomial $\Phi_{a_i} \in \mathbb{Q}[X]$ are exactly the primitive a_i-th roots of unity. The order of g is the least common multiple of the a_i. If L is an extremal lattice of dimension 48 then [23, Corollary 4.11] shows that the order of g is indeed the maximum of all the a_i.

Table 3 is taken from [24]. It lists the possible types of prime order automorphisms $\sigma \neq -1$ of extremal even unimodular lattices of dimension 48 together with their fixed lattice $F(\sigma)$ and the cyclotomic lattice $Z(\sigma)$ as defined in Definition 2.2.

TABLE 3. The possible types of automorphisms $\sigma \neq -1$ of prime order.

type	$F(\sigma)$	$Z(\sigma)$	example	complete
47-(1,2)-1	unique	unique	P_{48q}	[23, Thm 5.6]
23-(2,4)-2	unique	2	P_{48q}, P_{48p}	Cor. 8.5
13-(4,0)-0	$\{0\}$	at least 1	P_{48n}	
11-(4,8)-4	unique	at least 1	P_{48p}	
7-(8,0)-0	$\{0\}$	at least 1	P_{48n}	
7-(7,6)-5	$\sqrt{7}A_6^{\#}$	not known	not known	
5-(12,0)-0	$\{0\}$	at least 2	P_{48n}, P_{48m}	
5-(10,8)-8	$\sqrt{5}\mathbb{E}_8$	at least 1	P_{48m}	
5-(8,16)-8	$[2.\mathrm{Alt}_{10}]_{16}$	Λ_{32}	P_{48m}	[24]
3-(24,0)-0	$\{0\}$	at least 3	$P_{48p}, P_{48n}, P_{48m}$	
3-(20,8)-8	$\sqrt{3}\mathbb{E}_8$	not known	not known	
3-(16,16)-16	$\sqrt{3}(\mathbb{E}_8 \perp \mathbb{E}_8)$	at least 4	$P_{48p}, P_{48q}, P_{48n}$	
3-(16,16)-16	$\sqrt{3}\mathbb{D}_{16}^{+}$	at least 4	not known	
3-(15,18)-15	unique	two	not known	
3-(14,20)-14	?	unique	not known	
3-(13,22)-13	?	unique	not known	
2-(24,24)-24	$\sqrt{2}\Lambda_{24}$	$\sqrt{2}\Lambda_{24}$	P_{48n}	
2-(24,24)-24	$\sqrt{2}O_{24}$	$\sqrt{2}O_{24}$	$P_{48n}, P_{48p}, P_{48m}$	

For the rest of this section we assume that g is a semilarge automorphism of an extremal even unimodular lattice L of dimension $m = 48$ and denote by $o := \mathrm{ord}(g)$ the order of g. Replacing g by $-g$ if necessary we may assume that $o \not\equiv 2 \pmod 4$.

Lemma 9.2. Φ_o^2 *divides* χ_g.

Proof. As g is semilarge, $\chi_g = \Phi_a^2 f$ for some a dividing $\mathrm{ord}(g)$ such that
$$\deg(\Phi_a) = \varphi(a) > m/4 = 12.$$
In particular $\deg(f) < 48 - 2 \cdot 12 = 24$. If a is a proper divisor of o, then $\varphi(o) \geq 2\varphi(a)$. The facts that Φ_o divides χ_g by [23, Corollary 4.11] and that $\deg(\Phi_o) \geq 2 \deg(\Phi_a) > 24 > \deg(f)$ contradict each other. $\qquad\square$

Lemma 9.3. *If o is even then $g^{o/2} = -1$.*

Proof. By Lemma 9.2 $\chi_g = \Phi_o^2 f$ with $\deg(f) < 24$. Then the fixed space of $g^{o/2}$ has dimension $\leq \deg(f) < 24$ and Table 3 implies that $g^{o/2} = -1$. $\qquad\square$

Going through all possible $o \in \mathbb{N}$ with $o \not\equiv 2 \pmod 4$ and $\varphi(o) \in [13, \ldots, 24]$ we arrive at the following possibilities for o:

$\varphi(o)$	o
16	$17, 32, 40, 48, 60$
18	$19, 27$
20	$25, 33, 44$
22	23
24	$35, 39, 45, 52, 56, 72, 84$

We always put
$$E := \mathbb{Q}[\zeta_o], \mathbb{Z}_E = \mathbb{Z}[\zeta_o], K := \mathbb{Q}[\zeta_o + \zeta_o^{-1}], \mathbb{Z}_K = \mathbb{Z}[\zeta_o + \zeta_o^{-1}] \text{ and } \delta := 4 - (\zeta_o + \zeta_o^{-1})^2.$$
Let $(W, \mathbf{h})$ be the 2-dimensional Hermitian E-space on which g acts as primitive o-th root ζ_o of unity,
$$Q_\mathbf{h} := \left(\frac{-\delta, -\det(\mathbf{h})}{K} \right), \text{ and } Z := L \cap W.$$
The overall strategy to find all extremal unimodular lattices L can be divided into four steps:

(i) Identify the orthogonal lattice F of Z in L as the fixed lattice (or the orthogonal sum of two fixed lattices) of an element h of order p using Table 3.

(ii) Construct the possible lattices F and classify the conjugacy classes of automorphism of order o/p that may occur as the action of g on F.

(iii) Construct the possible lattices Z as ideals in the quaternion algebra $Q_\mathbf{h}$ using Theorem 7.5 (possibly as sublattices of maximal lattices).

(iv) Construct the g-invariant extremal unimodular overlattices L of $Z \oplus F$ using Remark 2.5 and some additional structure that make the computations feasible.

Step (i) is an easy combinatorial consideration and step (ii) a fast computation in Magma using the automorphism group and conjugacy classes algorithms. Step (iii) and (iv) are computationally much more involved. Step (iii) is done using the main result Theorem 7.5 of this paper building upon sophisticated algorithms for quaternion algebras from [16]. Step (iv) is more or less linear algebra. To make the computations feasible, one needs to consider the action of the centraliser of g in $\mathrm{Aut}(Z) \times \mathrm{Aut}(F)$ in a clever way.

We treat the possibilities for o according to their Euler Phi values and structure the description of the computations according to the four steps described above.

9.1. $\varphi(o) = 16$. By Table 3 the prime $o = 17$ is not possible and [23, Corollary 4.12] shows that any automorphism g of order 32 has $\chi_g = \Phi_{32}^3$, in particular such an automorphism is not semilarge (see also Lemma 9.3).

$o = 40$. By Lemma 9.3 $\chi_g = \Phi_{40}^2 \Phi_8^4$. Let $h := g^8$. Then h is an element of order 5 with a fixed space of dimension $16 = \deg(\Phi_8^4)$. By [24, Theorem 3.2] any extremal lattice L with such an automorphism h is isometric to P_{48m}. But the automorphism group of P_{48m} does not contain an element of order 40, so this case is impossible.

$o = 48$. By Lemma 9.3 $\chi_g = \Phi_{48}^2 \Phi_{16}^2$.

(i) Let $h := g^{16}$. Then h is an element of order 3 with fixed space of dimension 16, so by Table 3 the type of h is $3 - (16, 16) - 16$ and there are two possibilities for the fixed lattice $F = F(h)$ of h in L:

$$F_1 \cong \sqrt{3}\mathbb{D}_{16}^+ \text{ or } F_2 \cong \sqrt{3}(\mathbb{E}_8 \perp \mathbb{E}_8).$$

(ii) For both lattices there is a unique conjugacy class of automorphisms with characteristic polynomial Φ_{16}^2, represented by, say,

$$\gamma_1 \in \text{Aut}(\sqrt{3}\mathbb{D}_{16}^+) \text{ respectively } \gamma_2 \in \text{Aut}(\sqrt{3}(\mathbb{E}_8 \perp \mathbb{E}_8)).$$

(iii) In both cases the lattice $Z = Z(h) = \{\ell \in L \mid (\ell, F(h)) = \{0\}\}$ is a 32-dimensional $\mathbb{Z}$-lattice of determinant 3^{16}. By Lemma 5.4 $(1-h)Z^\# = Z$ and the $\mathbb{Q}[\zeta_3]$-Hermitian space $(W_{\mathbb{Q}[\zeta_3]}, \text{Tr}_{E/\mathbb{Q}[\zeta_3]} \circ \mathbf{h})$ contains a Hermitian unimodular lattice $(M, \text{Tr}_{E/\mathbb{Q}[\zeta_3]} \circ \mathbf{h})$. As in Lemma 5.2 we compute the dual of the $\mathbb{Z}_E$-lattice M as $(M, \mathbf{h})^* = D_{E/\mathbb{Q}[\zeta_3]}M$. As E/K is unramified we are in the position to apply Remark 7.6 to obtain $\det(\mathbf{h}) = 1$ and $Q_{\mathbf{h}} = \left(\frac{-\delta, -1}{K}\right)$. Moreover $(Z^\#, \frac{1}{8}\mathbf{h})$ is a Hermitian unimodular $\mathbb{Z}_E$-lattice and Z is a $(1/8)\mathbb{Z}_K$-maximal lattice in $Q_{\mathbf{h}}$. The mass of $Q_{\mathbf{h}}$ is $\frac{365}{16}$, the class number and the type number of $Q_{\mathbf{h}}$ are both 39, and there is a unique maximal order $\mathcal{M}$ containing an element γ of order 48. The narrow class number of K is 2 but all totally positive units in $\mathbb{Z}_K$ are norms of units in $\mathbb{Z}_E$. We find that 22 of the 39 right ideal classes of $\mathcal{M}$ have trivial norm in the narrow class group of K, so there are 22 possibilities for such $\mathbb{Z}_E$-lattices Z. Only 12 of them, $Z_1, \ldots, Z_{12}$ give rise to $\mathbb{Z}$-lattices with minimum ≥ 6.

(iv) The even unimodular lattice L is of the form

$$L = \{x + y \mid x \in Z_j^\#, y \in F_i^\#, \varphi(x + Z_j) = y + F_i\}$$

for some $1 \leq j \leq 12$, $i = 1, 2$ and some (γ, γ_i)-anti-isometry φ (see Definition 2.4). To construct these φ we first note that γ acts on $Z_j^\#/Z_j$ with minimal polynomial Φ_{16} and that $\Phi_{16} \equiv p_1 p_2$ (mod 3) for two distinct irreducible polynomials p_1, $p_2 \in \mathbb{F}_3[X]$ of degree 4. We obtain the decomposition

$$Z_j^\#/Z_j = p_1(\gamma)(Z_j^\#/Z_j) \oplus p_2(\gamma)(Z_j^\#/Z_j)$$
$$\cong S^2 \oplus S^{*2}$$
$$\cong F_i^\#/F_i = p_1(\gamma_i)(F_i^\#/F_i) \oplus p_2(\gamma)(F_i^\#/F_i)$$

where S is the simple $\mathbb{F}_3[X]/(p_2(X))$-module with dual module $S^* \cong \mathbb{F}_3[X]/(p_1(X))$. Fix a basis (b_1, b_2) of $p_1(\gamma)(Z_j^\#/Z_j)$ and compute the dual basis (b_1^*, b_2^*) of $p_2(\gamma)(Z_j^\#/Z_j)$. Then φ is uniquely determined by $v_k := \varphi(b_k) \in p_1(\gamma_i)(F_i^\#/F_i)$ for $k = 1, 2$, because then $\varphi(b_k^*) = -v_k^*$ where $(v_1^*, v_2^*) \in (p_2(\gamma_i)(F_i^\#/F_i))^2$ is the dual basis of (v_1, v_2). The centralizer of $g = (\gamma, \gamma_i)$

$$C_{\text{Aut}(Z_j)}(\gamma) \times C_{\text{Aut}(F_i)}(\gamma_i)$$

in the automorphism group of $Z_j \perp F_i$ still acts on these anti-isometries φ. We only use the action of the second component to restrict the possibilities for v_1 to a system of orbit representatives of $C_{\text{Aut}(F_i)}(\gamma_i)$ on the non-zero vectors in $p_1(\gamma_i)(F_i^\#/F_i)$.

For $i = 1$ (so $F_i \cong \sqrt{3}\mathbb{D}_{16}^+$) none of the glued lattices is extremal.

For $i = 2$ (so $F_i \cong \sqrt{3}(\mathbb{E}_8 \perp \mathbb{E}_8)$) we find 160 not necessarily inequivalent extremal even unimodular lattices. We are now facing the problem to check isometry of these lattices. To this aim we first partition the 160 lattices according to the isometry class of the sublattice Z into two sets of cardinality 16 and 144.

Let L be one of the first 16 extremal lattices. Then $(Z \perp F)^\#/L \cong S^2 \oplus S^{*2}$ as an $\mathbb{F}_3\langle g \rangle$-module and we consider the $\mathbb{Z}\langle g \rangle$-lattice X with

$$3X \subseteq X^\# \subseteq L \subseteq X \subseteq (Z \perp F)^\#$$

such that $X/L \cong S^2$. The lattice X has minimum 2 and 480 shortest vectors. Its automorphism group has order 432. The $\text{Aut}(X)$-orbit O of the subspace $L/3X$ of $X/3X$ has length 9. For all other 15 lattices L' the corresponding overlattice X' is isometric to X. After applying this isometry, we hence may assume that $X' = X$ and consider the subspace $L'/3X \leq X/3X$. All these subspaces lie in O. To check isometry to one of the known lattices, we do the same

computation with the lattice P_{48q}. The automorphism group of this lattice contains 8 conjugacy classes of elements of order 48 with characteristic polynomial $\Phi_{16}^2\Phi_{48}^2$. All these elements generate conjugate subgroups, so it is enough to consider one such element $g \in \mathrm{Aut}(P_{48q})$. The lattice $Z(g^{16})$ is isometric to the lattice Z in the first part, we compute X, check isometry and recognize the subspace $P_{48q}/3X$ in O.

For the other 144 extremal lattices, one finds two isometry classes of lattices X, say X_1 and X_2, where 48 of the lattices yield an overlattice isometric to X_1 and the other 96 have overlattice X_2. The lattice X_1 has minimum 2, kissing number 576 and an automorphism group of order $2^4 3^4$. The orbit on the sublattices $L/3X$ has length 9 and all the 48 lattices L are in this orbit. We check that two of the three conjugacy classes of relevant subgroups of the lattice P_{48p} (see Table 2) yield lattices isometric to X_1 and that $P_{48p}/3X_1$ is in this orbit. In particular all the 48 lattices L are isometric to P_{48p}. The lattice X_2 has also minimum 2 and kissing number 576. The automorphism group of X_2 has order $2^5 3^6$ and the orbit of $L/3X_2$ has length 81. All 96 lattices yield subspaces in this orbit, so does the third conjugacy class of relevant subgroups in $\mathrm{Aut}(P_{48p})$. So also these 96 lattices are isometric to P_{48p}.

$o = 60$. By Lemma 9.3 we now have 3 possibilities for the characteristic polynomial of g, $\chi_g = \Phi_{60}^2 f$ where f is one of Φ_{12}^4 (case (1)), Φ_{20}^2 (case (2)), or $\Phi_{12}^2\Phi_{20}$ (case (3)).

(1) In the first case let $h := g^{12}$. Then h is an element of order 5 having a 16-dimensional fixed space (as in the case $o = 40$ above). By [24, Theorem 3.2] any extremal lattice L with such an automorphism h is isometric to P_{48m}. But the automorphism group of P_{48m} does not contain an element of order 60, so this case is impossible.

(2) The second case is very similar to the case $o = 48$.

(i) Here $h := g^{20}$ is an element of order 3 with a 16-dimensional fixed lattice $F(h)$ which is isometric to $\sqrt{3}\mathbb{D}_{16}^+$ or $\sqrt{3}(\mathbb{E}_8 \perp \mathbb{E}_8)$ as for $o = 48$.

(ii) As $\mathrm{Aut}(\mathbb{D}_{16}^+)$ does not contain an element with characteristic polynomial Φ_{20}^2 we conclude that $F \cong \sqrt{3}(\mathbb{E}_8 \perp \mathbb{E}_8)$. There are two conjugacy classes of elements γ_1, $\gamma_2 \in \mathrm{Aut}(F)$ with characteristic polynomial Φ_{20}^2.

(iii) The lattice Z is a maximal lattice in $Q_{\mathbf{h}} = \left(\frac{-\delta,-1}{K}\right)$. The mass of $Q_{\mathbf{h}}$ is 2, the class number and the type number of $Q_{\mathbf{h}}$ are both 9, and there is a unique maximal order $\mathcal{M}$ containing an element γ of order 60. The narrow class number of K is 2 but all totally positive units in $\mathbb{Z}_K$ are norms of units in $\mathbb{Z}_E$. 7 of the 9 right ideal classes of $\mathcal{M}$ have trivial norm in the narrow class group of K, so there are 7 possibilities for such $\mathbb{Z}_E$-lattices Z. 4 of them, $Z_1, \ldots, Z_4$ give rise to $\mathbb{Z}$-lattices of minimum ≥ 6.

(iv) The construction of the even unimodular lattices is completely analogous as in the case $o = 48$, as $\Phi_{20} \equiv p_1 p_2 \pmod 3$ is again the product of two irreducible polynomials of degree 4 in $\mathbb{F}_3[X]$. There are 184 glues that lead to extremal even unimodular lattices. To test that all these lattices are isometric we used the same strategy as for $o = 48$, which is a bit easier here, as we obtain a unique isometry class of lattices X. So we fix one of these 184 lattices L and compute the overlattice X with $X/L \cong S^2$ as in the case $o = 48$. The lattice X has minimum 2 and 480 shortest vectors. Its automorphism group is isomorphic to $(2.\mathrm{Alt}_6 Y (C_3^3 : C_8)).2$. The $\mathrm{Aut}(X)$-orbit O of the subspace $L/3X$ of $X/3X$ has length 54. For all other lattices L' the corresponding overlattice X' is isometric to X. After applying this isometry, we hence may assume that $X' = X$ and consider the subspace $L'/3X \leq X/3X$. All these subspaces lie in O. As for $o = 48$ we then check that the lattice P_{48m} is isometric to L.

(3) (i) In the third case $\chi_g = \Phi_{60}^2\Phi_{20}\Phi_{12}^2$ and the lattice L contains a sublattice $Z \perp F_3 \perp F_5$ of index $3^8 5^8$, where the lattices $F_p \cong \sqrt{p}\mathbb{E}_8$ are the fixed lattices of the elements of order p in $\langle g \rangle$.

(ii) For both lattices F_p there is a unique conjugacy class of automorphisms of order $o/p = 20$ resp. 12 that have an irreducible minimal polynomial.

(iii) The lattice Z is not maximal but a maximal sublattice in some maximal lattice M in the same quaternion algebra as before with $\det(M, \mathrm{Tr}_{K/\mathbb{Q}}(\mathbf{q_h})) = 5^8$ and $\det(Z, \mathrm{Tr}_{K/\mathbb{Q}}(\mathbf{q_h})) = 3^8 5^8$. As computed above there are 7 possibilities for M each having $(81^2 - 1)/(81 - 1) = 82$ maximal sublattices Z. The mass of the genus of Z is 82 times the mass of the genus of M, $\mathrm{mass}(Z) = 41/30$ and we find in total 94 isometry classes of lattices Z, 84 of which have minimum ≥ 6.

(iv) Now we compute the overlattices N of index 5^8 of $Z \perp F_5$ by computing suitable anti-isometries. We find 16 (not necessarily inequivalent) such glues N that still have minimum 6 and then continue to construct L as an overlattice of $N \perp F_3$. In this last step no extremal lattice is found.

9.2. $\varphi(o) = 18$. By Table 3 the prime $o = 19$ is not possible, so the only other possibility is $o = 27 = 3^3$. Then g^9 is an automorphism of L of order 3 whose fixed space has dimension $48 - 36 = 12$. This is impossible by Table 3.

9.3. $\varphi(o) = 20$.
$o = 25$. (i) Then $\chi_g = \Phi_{25}^2(X-1)^8$ or $\chi_g = \Phi_{25}^2\Phi_5^2$. In both cases $h = g^5$ is an automorphism of order 5 with a fixed lattice $F := F(h)$ of dimension 8. So F is isometric to $\sqrt{5}\mathbb{E}_8$ by Table 3.
(ii) The lattice F has a unique conjugacy class of automorphisms of order 1 (in the first case) resp. 5 with irreducible minimal polynomial (in the second case).
(iii) The lattice $Z := Z(h)$ is a lattice of determinant 5^8 admitting an automorphism $\gamma := g_{|Z}$ with $\chi_\gamma = \Phi_{25}^2$. Moreover, as Z and F are both pure sublattices of L, there is an isomorphism of $\mathbb{Z}[g]$-modules

$$\varphi \colon Z^\#/Z \to F^\#/F$$

such that $L = \{(z,f) \in Z^\# \times F^\# \mid \varphi(z+Z) = f+F\}$. So in the first case γ acts trivially on $Z^\#/Z$ which implies that $(1-\gamma)Z^\# \subseteq Z$. But $|Z^\#/(1-\gamma)Z^\#| = 5^2$ so this case is impossible. Hence $\chi_g = \Phi_{25}^2\Phi_5^2$ and $\Phi_5(\gamma)$ acts trivially on $Z^\#/Z$. As $5^8 = |F^\#/F| = |Z^\#/Z|$ we conclude that $Z = \Phi_5(\gamma)Z^\#$. The lattice $Z_0 := (1-\gamma)^{15}Z$ satisfies $(Z_0, \mathbf{q_h})^* = Z_0$ and hence $Z_0 \in \mathcal{G}_{\mathbb{Z}_K}(W_K, \mathbf{q_h})$ by Lemma 4.2. In particular $Q_{\mathbf{h}} = \left(\frac{-\delta, -1}{K}\right)$. As $h_K = 1$ we know that the class number of $Q_{\mathbf{h}}$ equals the type number, which we compute to be $t = 172$. There is a unique maximal order $\mathcal{M}$ in $Q_{\mathbf{h}}$ that contains an element of order 25. As $\mathcal{M}^{(1)} \cong Q_{100}$ is the quaternion group of order 100, there is a unique Hermitian embedding of $\mathbb{Z}_E$ into $\mathcal{M}$. Also the narrow class number $h_K^+ = 1$. Hence the isometry classes of lattices $Z_0 \in \mathcal{G}_{\mathbb{Z}_K}(Q_{\mathbf{h}}, \mathbf{h}_n)$ are in bijection with the 172 right ideal classes of $\mathcal{M}$. For 80 of these lattices Z_0 the integral lattice $(Z, \mathbf{q}) := ((1-\zeta_{25})^{-15}Z_0, \mathrm{Tr}_{K/\mathbb{Q}}(n))$ has minimum ≥ 6. These 80 lattices fall into 9 isometry classes represented by, say, $Z_1, \ldots, Z_9$. The $\mathbb{Z}$-automorphism groups of all these 9 lattices have a normal Sylow 5-subgroup $\langle \gamma \rangle$ that is cyclic of order 25.
(iv) The lattice F from above is isometric to $\sqrt{5}\mathbb{E}_8$ and its automorphism group contains a unique conjugacy class of elements with characteristic polynomial Φ_5^2, represented by, say, γ'. As γ' is unique up to conjugacy in $\mathrm{Aut}(F)$ and $\langle \gamma \rangle$ is unique up to conjugacy in $\mathrm{Aut}(Z_j)$ we may assume that the element $g \in \mathrm{Aut}(L, \mathbf{q})$ acts on the sublattice $Z_j \perp F$ as (γ, γ').

To classify the extremal even unimodular lattices L we hence need to compute the (γ, γ')-anti-isometries that lead to lattices of minimum 6: Now $Z_j^\#/Z_j \cong F^\#/F \cong S^2$ are modules over the chain ring

$$S = \mathbb{Z}[\zeta_{25}]/(\Phi_5(\zeta_{25})) \cong \mathbb{Z}[\zeta_5]/(5).$$

Let π be a generator of the maximal ideal of S. We find vectors $b_1, b_2 \in Z^\# \setminus Z^\#\pi$ such that $\mathbf{b_q}(b_i, b_i) \in \{12/5, 14/5\}$, the minimal possible norms, and such that the classes of

$$B := (b_1, \gamma(b_1), \gamma^2(b_1), \gamma^3(b_1), b_2, \gamma(b_2), \gamma^2(b_2), \gamma^3(b_3))$$

form a basis of $Z_j^\#/Z_j$. The classes in $(F^\#/F) \setminus (F^\#/F)\pi$ are represented by elements of norm $\leq 18/5$. So for L having minimum ≥ 6 the image $\varphi(b_i + Z) \in F^\#/F$ should have norm $18/5$ respectively $16/5$. As in the case $o = 48$ we compute orbit representatives of these classes under $C_{\mathrm{Aut}(F)}(\gamma')$ to narrow down the possibilities for $\varphi(b_1 + Z)$. No extremal lattice L is found.

By Table 3 the maximal dimension of a fixed lattices of an automorphism of order 5 of an extremal 48-dimensional unimodular lattice L is 16. In particular any automorphism of order 25 of L has to be semilarge, therefore we note:

Corollary 9.4. *There is no extremal even unimodular lattice of dimension 48 with an automorphism of order 25.*

$o = 33$. (i) Here $h := g^3$ is an element of order 11. By Table 3 the type of h is $11 - (4, 8) - 4$ and the fixed lattice F of h in L is the unique extremal 8-dimensional even 11-modular lattice.
(ii) The restriction of g to F is an automorphism γ' of order 3 of F acting as a primitive third root of unity on $F^{\#}/F \cong \mathbb{F}_{11}^4$. The automorphism group of F contains a unique conjugacy class of such elements γ' of order 3 and these have $\chi_{\gamma'} = \Phi_3^4$, so $\chi_g = \Phi_{33}^2 \Phi_3^4$.
(iii) The lattice $Z = Z(h) = \{\ell \in L \mid (\ell, F) = \{0\}\}$ is a 40-dimensional $\mathbb{Z}$-lattice of determinant 11^4 on which g acts with characteristic polynomial Φ_{33}^2. Moreover by Lemma 5.4 $Z^{\#}(1 - h) = Z$ and the $\mathbb{Q}[\zeta_{11}]$ Hermitian space $(W_{\mathbb{Q}[\zeta_{11}]}, \mathrm{Tr}_{E/\mathbb{Q}[\zeta_{11}]} \circ \mathbf{h})$ contains a Hermitian unimodular lattice $(M, \mathrm{Tr}_{E/\mathbb{Q}[\zeta_{11}]} \circ \mathbf{h})$. As in Lemma 5.2 we compute the dual of the $\mathbb{Z}_E$-lattice M as $(M, \mathbf{h})^* = D_{E/\mathbb{Q}[\zeta_{11}]}M$. As E/K is unramified we are in the position to apply Remark 7.6 to obtain $\det(\mathbf{h}) = 1$ and $Q_{\mathbf{h}} = \left(\frac{-\delta, -1}{K}\right)$. The mass of $Q_{\mathbf{h}}$ is $\frac{2105}{22}$, the class number and the type number of $Q_{\mathbf{h}}$ are both 115, and there is a unique maximal order $\mathcal{M}$ containing an element γ of order 33. The narrow class number of K is 2 but all totally positive units in $\mathbb{Z}_K$ are norms of units in $\mathbb{Z}_E$. 63 of the 115 right ideal classes of $\mathcal{M}$ have trivial norm in the narrow class group of K, so there are 63 possibilities for such $\mathbb{Z}_E$-lattices Z. 14 of them, $Z_1, \ldots, Z_{14}$ give rise to $\mathbb{Z}$-lattices of minimum ≥ 6.
(iv) The even unimodular lattice L is of the form

$$L = \{x + y \mid x \in Z_j^{\#}, y \in F^{\#}, \varphi(x + Z_j) = y + F\}$$

for some $1 \leq j \leq 14$ and some (γ, γ')-anti-isometry φ (see Definition 2.4).

Now $F^{\#}/F \cong Z_j^{\#}/Z_j$ is just the sum of two isomorphic $\mathbb{F}_{11}[g]$-modules, so there is no reduction from the representation theoretic side. Instead we use the fact that the minimum of L needs to be 6: For all j the minimum of $Z_j^{\#}$ is either $30/11$ or $32/11$. The maximal minimal norm of a class $v + F$ in $F^{\#}/F$ is $36/11$ and there are 600 classes of norm $36/11$ falling into three orbits under $C_{\mathrm{Aut}(F)}(\gamma')$ and 720 classes of norm $34/11$ falling into two such orbits. So for each j we fix a tuple $(b_1, \gamma(b_1), b_2, \gamma(b_2))$ of minimal vectors of $Z_j^{\#}$ whose classes form a basis of $Z_j^{\#}/Z_j \cong \mathbb{F}_{11}^4$. For $\varphi(b_1 + Z_j)$ we choose one of the three or two orbit representatives $v_1 + F$ of the classes of suitable norm, and for $\varphi(b_2 + Z_j)$ we run through all classes of the right norm and check that φ is an anti-isometry by testing if L is even and unimodular.

We find exactly 5 extremal lattices L, corresponding the 5 conjugacy classes of elements of order 33 in $\mathrm{Aut}(P_{48p})$, so all these lattices are isometric to P_{48p}.
$o = 44$. By Lemma 9.3 the characteristic polynomial is $\chi_g = \Phi_{44}^2 \Phi_4^4$.
(i) Now $h := g^4$ is an element of order 11 and as in the case $o = 33$ the type of h is $11 - (4, 8) - 4$ and the fixed lattice F of h in L is unique.
(ii) The restriction of g to F is an automorphism γ' of order 4 of F acting as a primitive fourth root of unity on $F^{\#}/F \cong \mathbb{F}_{11}^4$. The automorphism group of F contains a unique conjugacy class of such elements γ'.
(iii) The lattice $Z := Z(h) = \{\ell \in L \mid (\ell, F) = \{0\}\}$ is a 40-dimensional $\mathbb{Z}$-lattice of determinant 11^4 on which g acts with characteristic polynomial Φ_{44}^2. As for $o = 33$ we obtain $Q_{\mathbf{h}} = \left(\frac{-\delta, -1}{K}\right)$. The mass of $Q_{\mathbf{h}}$ is $\frac{109585}{132}$, the class number and the type number of $Q_{\mathbf{h}}$ are both 880, and there is a unique maximal order $\mathcal{M}$ containing an element γ of order 44. The narrow class number of K is 2 but all totally positive units in $\mathbb{Z}_K$ are norms of units in $\mathbb{Z}_E$. 445 of the 880 right ideal classes of $\mathcal{M}$ have trivial norm in the narrow class group of K, so there are 445 possibilities for such $\mathbb{Z}_E$-lattices Z. 14 of them, $Z_1, \ldots, Z_{14}$ give rise to $\mathbb{Z}$-lattices of minimum ≥ 6.
(iv) The gluing strategy is the same as for $o = 33$ but we additionally use the action of the stabilizer $\mathrm{Stab}_{C_{\mathrm{Aut}(F)}(\gamma')}(v_1 + F)$ to narrow down the possibilities for $\varphi(b_2 + Z_j)$. Then we find 5 extremal lattices L corresponding to the 5 conjugacy classes of elements of order 44 in $\mathrm{Aut}(P_{48p})$, which allows us to conclude that all these lattices are isometric to P_{48p}.

9.4. $\varphi(o) = 22$. Then $o = 23$ and this case has been handled in Section 8.2.2.

9.5. $\varphi(o) = 24$. In this case $F = \{0\}$ so steps (i), (ii), and (iv) are not necessary as $L = Z$ is a binary Hermitian lattice. The possibilities for o are given in Table 4 below. In all cases o is not a prime power, so the field extension E/K is unramified outside the infinite places. By Remark 5.3

$\mathbb{Z}_E = \mathbb{Z}[\zeta_o]$ and $\mathbb{Z}_K = \mathbb{Z}[\zeta_o + \zeta_o^{-1}]$ embed into $\mathrm{End}_{\mathbb{Z}}(L)$ by letting ζ_o act as g. In particular L is a 4-dimensional $\mathbb{Z}_K$-lattice with an Hermitian embedding $\nu \colon \mathbb{Z}_E \to \mathrm{End}_{\mathbb{Z}_K}(L)$. By Lemma 5.2 the $\mathbb{Z}_K$-dual lattice of L is $L^* = D_{K/\mathbb{Q}} L$ and so Remark 7.6 shows that

$$Q_{\mathbf{h}} = \left(\frac{(\zeta_o + \zeta_o^{-1})^2 - 4, -1}{K} \right).$$

As in the proof of Remark 7.6 there is a fractional $\mathbb{Z}_E$-ideal $\mathfrak{A}$ such that $D_{K/\mathbb{Q}} = \mathfrak{A}\sigma(\mathfrak{A})$ and replacing L by $\mathfrak{A}^{-1} L$ we may achieve that $L = L^*$. Lemma 4.2 shows $L \in \mathcal{G}_{\mathbb{Z}_K}(Q_{\mathbf{h}}, n)$ and we may use Theorem 7.5 to enumerate all such $\mathbb{Z}_E$-lattices L. There are three cases (see Table 4) where the type number $t(Q_{\mathbf{h}})$ is $> 10^4$, i.e. $o = 52, 56, 72$. In these cases our computations took about 3 weeks of computing time.

To describe our computation we first note that in all seven cases we compute $h_K = 1$ and $\mathbb{Z}_{K,>0}^* = \{u\sigma(u) \mid u \in \mathbb{Z}_E^*\}$. Hence for all maximal orders $\mathcal{M}$ such that $\mathbb{Z}_E$ embeds into $\mathcal{M}$ and all $\mathcal{M}$-right ideals J the group $U(J) = \mathbb{Z}_{K,>0}^*$. As seen in the proof of Lemma 8.1, there is a unique Hermitian embedding of $\mathbb{Z}_E$ into $\mathcal{M}$ if and only if $\mathcal{M}^{(1)} \cong Q_{4o}$ is the quaternion group of order $4o$; otherwise there are two such embeddings ν and $\nu \circ \sigma$. Note that there is a unique maximal order $\mathcal{M}$ with $\mathcal{M}^{(1)} \cong Q_{4o}$.

The table below summarizes our computations by listing the following information:

- The type number t of $Q_{\mathbf{h}}$ which is also the class number of $Q_{\mathbf{h}}$ in all cases.
- The narrow class number h_K^+ of K.
- The mass of the quaternion algebra $Q_{\mathbf{h}}$.
- The number t_0 of conjugacy classes of maximal orders in $Q_{\mathbf{h}}$ into which $\mathbb{Z}_E$ embeds.
- The number $\#\mathcal{G}$ of isometry classes in the genus $\mathcal{G} := \mathcal{G}_{D_{K/\mathbb{Q}}^{-1}}(Q_{\mathbf{h}}, \mathbf{h}_n)$.
- The mass of the genus $\mathcal{G}$.
- The number of isometry classes in $\mathcal{G}$ that yield an extremal even unimodular lattice of rank 48.

TABLE 4. Some details for the relevant quaternion algebras.

o	$t(Q_{\mathbf{h}})$	h_K^+	$\mathrm{mass}(Q_{\mathbf{h}})$	t_0	$\#\mathcal{G}$	$\mathrm{mass}(\mathcal{G})$	# ext.
35	1880	2	$\frac{381433}{210}$	1	952	$\frac{381433}{29400}$	3
39	6866	4	6669	2	6856	$\frac{171}{2}$	1
45	3024	2	$\frac{265501}{90}$	1	1518	$\frac{265501}{16200}$	0
52	89108	2	$\frac{1066603}{12}$	2	133842	$\frac{1066603}{416}$	1
56	48674	4	$\frac{338195}{7}$	2	48626	$\frac{338195}{392}$	6
72	75844	2	$\frac{604903}{8}$	2	113946	$\frac{604903}{384}$	0
84	3520	2	$\frac{10322}{3}$	1	1778	$\frac{5161}{252}$	3

We summarize the result of the computations described in this section in the following theorem.

Theorem 9.5. *Let L be an extremal even unimodular lattice of dimension 48 admitting a semi-large automorphism. Then L is isometric to one of P_{48p}, P_{48q}, or P_{48n}.*

10. An application to extremal 36-dimensional 3-modular lattices

The dissertation of Michael Jürgens [14] exhibits the possible automorphisms of an extremal 3-modular lattice in dimension 36, whose existence is still open. In particular [14, Section 4.2.3] shows that such an extremal lattice has no automorphisms of order 11, 13, or any prime $p \geq 23$ and specifies a unique possible type for automorphisms of order 17 and 19 . In this section we use binary Hermitian lattices to exclude these automorphisms and to achieve the following result.

Theorem 10.1. *Let L be an extremal even 3-modular lattice of dimension 36. Then all primes p dividing $|\mathrm{Aut}(L)|$ are ≤ 7.*

Proof. Most of the proof of the theorem is already contained in [14], it remains to exclude the automorphisms of order 17 and 19:

Let $g \in \mathrm{Aut}(L)$ be an automorphism of order 19. Then by [14] the characteristic polynomial $\chi_g = \Phi_{19}^2$ and hence L is a Hermitian lattice of rank 2 over $\mathbb{Z}[\zeta_{19}]$. So let $E = \mathbb{Q}[\zeta_{19}]$, $(V, \mathbf{h}) = E \otimes_{\mathbb{Z}[\zeta_{19}]} L$, and $K := \mathbb{Q}[\zeta_{19} + \zeta_{19}^{-1}]$. Then the narrow class number $h_K^+ = 1$ and $\det(\mathbf{h}) = 3$. Therefore the $\mathbb{Z}_E$-lattice L is a maximal lattice in $Q_{\mathbf{h}} := \left(\frac{-\delta, -3}{K} \right)$ with $\delta = 4 - (\zeta_{19} + \zeta_{19}^{-1})^2$ as usual. Using the algorithm in [16] we compute the type number of $Q_{\mathbf{h}}$ as $t = 189574$ and the class number is 378374. There is a unique conjugacy class of maximal orders $\mathcal{M}$ that contain an element of order 19 and there are two Hermitian embeddings of $\mathbb{Z}_E$ into $\mathcal{M}$. As the trace lattices for both embeddings are the same, we need to consider 378374 different 3-modular $\mathbb{Z}$-lattices of dimension 36. None of them has minimum 8.

Now assume that there is some $g \in \mathrm{Aut}(L)$ of order 17. Then by [14] the characteristic polynomial is $\chi_g = \Phi_{17}^2(X - 1)^4$ and L contains a g-invariant sublattice $Z \perp F \subseteq L$ of index 17^2 such that F is a unique 4-dimensional lattice of determinant $3^2 17^2$ and minimum 8 and Z is some 32-dimensional lattice of determinant $3^{16} 17^2$ admitting an automorphism $g' := g_{|Z}$ with $\chi_{g'} = \Phi_{17}^2$. More precisely $(1 - g')(Z^\# + 17Z) = Z$.

So here $E = \mathbb{Q}[\zeta_{17}]$ and $K := \mathbb{Q}[\zeta_{17} + \zeta_{17}^{-1}]$ and again $h_K^+ = 1$ and the determinant of the Hermitian form is 3. So $Q_{\mathbf{h}} := \left(\frac{-\delta, -3}{K} \right)$ with $\delta = 4 - (\zeta_{17} + \zeta_{17}^{-1})^2$ is the quaternion algebra ramified at the 8 infinite places of K and at the places above 3 and 17. The type number of $Q_{\mathbf{h}}$ is 75425 and there is a unique maximal order $\mathcal{M}$ containing an element of order 17. This order has 300478 right-ideal classes yielding $\mathbb{Z}$-lattices Z of dimension 32. Only four of these lattices have minimum ≥ 8. For each of the four lattices Z we computed the 3-modular overlattices of $Z \perp F$; none of them is extremal. □

References

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

[2] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997.

[3] H. Cohn and A. Kumar. Optimality and uniqueness of the Leech lattice among lattices. *Ann. of Math. (2)*, 170(3):1003–1050, 2009.

[4] J. H. Conway. A group of order $8, 315, 553, 613, 086, 720, 000$. *Bull. London Math. Soc.*, 1:79–88, 1969.

[5] J. H. Conway and N. J. A. Sloane. *Sphere packings, lattices and groups*, volume 290 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, New York, third edition, 1999.

[6] J. Dieudonné. *Linear algebra and geometry*. Hermann, 1969.

[7] W. Ebeling. *Lattices and codes*. Advanced Lectures in Mathematics. Springer Spektrum, Wiesbaden, third edition, 2013. A course partially based on lectures by Friedrich Hirzebruch.

[8] M. Eichler. Zur Zahlentheorie der Quaternionen-Algebren. *J. Reine u. Angew. Math.*, 195:127–151, 1955. Correction in: *J. Reine u. Angew. Math.* 197 (1957), p. 220.

[9] U. Fincke and M. Pohst. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Math. Comp.*, 44(170):463–471, 1985.

[10] W. T. Gan and J.-K. Yu. Group schemes and local densities. *Duke Math. J.*, 105(3):497–524, 2000.

[11] H. Hasse. Äquivalenz quadratischer Formen in einem beliebigen Zahlkörper. *J. reine u. angew. Mathematik*, 153:158–162, 1924.

[12] H. Hasse. *Über die Klassenzahl abelscher Zahlkörper*. Akademie-Verlag, Berlin, 1952.

[13] A. A. Johnson. Integral representations of hermitian forms over local fields. *J. Reine Angew. Math.*, 229:57–80, 1968.

[14] M. Jürgens. *Nicht-Existenz und Konstruktion extremaler Gitter*. PhD thesis, Technische Universität Dortmund, 2015. See also www.mathematik.tu-dortmund.de/sites/michael-juergens/extremal-lattices.

[15] M. Kirschmer and G. Nebe. Quaternary quadratic lattices over number fields. Advance online publication. doi:10.1142/S1793042119500131, 2018.

[16] M. Kirschmer and J. Voight. Algorithmic enumeration of ideal classes for quaternion orders. *SIAM J. Comput. (SICOMP)*, 39(5):1714–1747, 2010. See also https://arxiv.org/pdf/0808.3833.pdf.

[17] M. Kneser. *Quadratische Formen*. Springer-Verlag, Berlin, 2002. Revised and edited in collaboration with Rudolf Scharlau.

[18] J. Leech. Some sphere packings in higher space. *Canad. J. Math.*, 16:657–682, 1964.

[19] H. Minkowski. *Diophantische Approximationen; eine Einführung in die Zahlentheorie*. Teubner, 1907.

[20] G. Nebe. Finite quaternionic matrix groups. *Represent. Theory*, 2:106–223, 1998.

[21] G. Nebe. Some cyclo-quaternionic lattices. *J. Algebra*, 199(2):472–498, 1998.

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

[23] G. Nebe. On automorphisms of extremal even unimodular lattices. *Int. J. Number Theory*, 9(8):1933–1959, 2013.

[24] G. Nebe. A fourth extremal even unimodular lattice of dimension 48. *Discrete Math.*, 331:133–136, 2014.

[25] G. Nebe. Automorphisms of extremal unimodular lattices in dimension 72. *J. Number Theory*, 161:362–383, 2016.

[26] J. Neukirch. *Algebraische Zahlentheorie*. Springer-Verlag, Berlin, 1992.

[27] H.-V. Niemeier. Definite quadratische Formen der Dimension 24 und Diskriminante 1. *J. Number Theory*, 5:142–178, 1973.

[28] O. T. O'Meara. *Introduction to Quadratic Forms*. Springer, 1973.

[29] H.-G. Quebbemann. Modular lattices in Euclidean spaces. *J. Number Theory*, 54(2):190–202, 1995.

[30] I. Reiner. *Maximal Orders*. Oxford Science Publications, 2003.

[31] W. Scharlau. *Quadratic and Hermitian forms*, volume 270 of *Grundlehren der mathematischen Wissenschaften*. Springer, 1985.

[32] A. Schiemann. Classification of Hermitian Forms with the Neighbor Method. *J. Symbolic Computation*, 26:487–508, 1998.

[33] G. Shimura. Arithmetic of unitary groups. *Ann. Math.*, 79:269–409, 1964.

[34] C. L. Siegel. Berechnung von Zetafunktionen an ganzzahligen Stellen. *Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II*, 1969:87–102, 1969.

[35] M.-F. Vignéras. Simplification pour les ordres des corps de quaternions totalement définis. *J. Reine Angew. Math.*, 286/287:257–277, 1976.

[36] M.-F. Vignéras. *Arithmétique des Algebrès de Quaternions*, volume 800 of *Lecture Notes in Mathematics*. Springer-Verlag, 1980.

[37] L. C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

Email address: markus.kirschmer@math.rwth-aachen.de

Email address: nebe@math.rwth-aachen.de

Lehrstuhl D für Mathematik, RWTH Aachen University, 52056 Aachen, Germany