

QUATERNARY QUADRATIC LATTICES OVER NUMBER FIELDS

MARKUS KIRSCHMER AND GABRIELE NEBE

ABSTRACT. We relate proper isometry classes of maximal lattices in a totally definite quaternary quadratic space (V, q) with trivial discriminant to certain equivalence classes of ideals in the quaternion algebra representing the Clifford invariant of (V, q) . We use this strategy to classify binary Hermitian lattices over CM fields.

1. INTRODUCTION

In his *Disquisitiones Arithmeticae* Gauß defines his famous composition of rational binary quadratic forms and relates proper isometry classes of binary lattices to ideal classes in quadratic number fields. Kneser generalised Gauß' composition in [13] to binary quadratic forms over arbitrary commutative base rings. Much further reaching generalisations have been given by Bhargava in his thesis and a series of subsequent papers. For ternary quadratic forms a similar relation between lattices and quaternion orders has been investigated by Peters ([20]) and Brzezinski ([3], [4]) based on results from Eichler and Brandt, for a functorial correspondence see Voight ([35]). Aeberli ([1]) used the Brandt groupoid of ideal classes in quaternion algebras to define a composition of quaternary lattices. A unified interpretation of these composition laws based on Clifford algebras is given in [15].

Quaternary lattices have further been investigated by Ponomarev ([21, 23, 22, 24]), who relates the proper isometry classes of lattices in a rational quaternary quadratic space to certain equivalence classes of ideals in a rational quaternion algebra.

The present paper generalises this correspondence to arbitrary totally real number fields K : If (V, q) is a totally definite quaternary quadratic space over K of square discriminant and Q the totally definite quaternion algebra representing its Clifford invariant, then the proper isometry classes of \mathfrak{a} -maximal lattices in (V, q) are in bijection with certain equivalence classes of normal ideals in Q of norm \mathfrak{a} (see Proposition 3.4 and Theorem 4.1). We use this correspondence to conclude Siegel's mass formula for these genera of lattices from Eichler's mass formula for quaternion algebras in Section 6. The correspondence also gives rise to an algorithm to enumerate the proper isometry classes of lattices in the genus of \mathfrak{a} -maximal lattices in (V, q) based on the method of [12]. This new algorithm is much more efficient than the usual Kneser neighbour method. As an application we study binary Hermitian lattices over totally complex quadratic extensions of K in Section 8. In particular our classification of unimodular binary $\mathbb{Z}[\zeta_{23}]$ -lattices shows that there are exactly

2010 *Mathematics Subject Classification.* 11E20; 11E41; 11E12; 11R52.

Key words and phrases. Quaternary quadratic forms, lattices over totally real fields, genera of lattices, orders in quaternion algebras, class numbers, classification algorithm.

two isometry classes of extremal even unimodular lattices of dimension 48 with an automorphism of order 23.

2. QUADRATIC LATTICES OVER NUMBER FIELDS

Let K be a number field and (V, q) a non-degenerate quadratic space over K . The most important invariants of (V, q) are its determinant, the square class of the determinant of a Gram matrix, and the Clifford invariant $c(V, q)$, which is either K or the class of a quaternion division algebra in the Brauer group of K . The interest in these two isometry invariants of quadratic spaces is mainly due to the following classical result by Helmut Hasse.

Theorem 2.1 ([9]). *Over a number field K the isometry class of a quadratic space is uniquely determined by its dimension, its determinant, its Clifford invariant and its signature at all real places of K .*

Let \mathbb{Z}_K be the ring of integers in K . A \mathbb{Z}_K -lattice L in (V, q) is a finitely generated \mathbb{Z}_K -submodule of V that contains a K -basis of V . The orthogonal group

$$O(V, q) := \{\varphi \in \mathrm{GL}(V) \mid q(\varphi(v)) = q(v) \text{ for all } v \in V\}$$

and its normal subgroup $\mathrm{SO}(V, q) := \{\varphi \in O(V, q) \mid \det(\varphi) = 1\}$ of proper isometries act on the set of all lattices in (V, q) . We call two lattices (L, q) and (L', q) in (V, q) *properly isometric*, $(L, q) \cong^+ (L', q)$, if they are in the same orbit under the action of $\mathrm{SO}(V, q)$ and denote by

$$[(L, q)]^+ = [L]^+ = L \cdot \mathrm{SO}(V, q)$$

the proper isometry class of the \mathbb{Z}_K -lattice L . The stabiliser of (L, q) in $\mathrm{SO}(V, q)$ is called the proper isometry group $\mathrm{Aut}^+(L, q)$ of (L, q) . If we refer to the coarser notion of isometry and orbits under the full orthogonal group, then the upper script $^+$ is omitted.

The two lattices L and L' are called in the same *genus*, if

$$(L_{\mathfrak{p}}, q) \cong (L'_{\mathfrak{p}}, q) \text{ for all maximal ideals } \mathfrak{p} \text{ of } \mathbb{Z}_K.$$

Here and in the following $L_{\mathfrak{p}} := L \otimes_{\mathbb{Z}_K} \mathbb{Z}_{K_{\mathfrak{p}}}$ denotes the completion of L at the finite place \mathfrak{p} of K .

The classification of all (proper) isometry classes of lattices in a given genus is an interesting and intensively studied problem (see [26, 29, 11]). One strategy is to embed an integral quadratic lattice (L, q) into a maximal one and deduce the classification of the genus of (L, q) from the one of maximal lattices. The mass formula for maximal lattices is given in [8]. Recall that for a fractional ideal \mathfrak{a} of K a lattice (L, q) in (V, q) is *\mathfrak{a} -maximal*, if $q(L) \subseteq \mathfrak{a}$ and $q(L') \not\subseteq \mathfrak{a}$ for all proper overlattices L' of L . The \mathbb{Z}_K -maximal lattices are also called *maximal*. It is well known (see [19]) that all \mathfrak{a} -maximal lattices in (V, q) are in the same genus, which we denote by $\mathcal{G}_{\mathfrak{a}}(V, q)$.

3. SOME BASIC FACTS ABOUT QUATERNION ALGEBRAS

A detailed discussion of the arithmetic of quaternion algebras can be found in [6], [34], and [25]. So let Q be a totally definite quaternion algebra whose centre K is a totally real number field. It is well known that Q has a basis $(1, i, j, ij)$ with $ij = -ji$ and $i^2 = a, j^2 = b$ for suitable totally negative $a, b \in K$. Then Q is also

denoted by $Q = \left(\frac{a,b}{K}\right)$. It carries a canonical involution, $\bar{} : Q \rightarrow Q$ defined by $\overline{t + xi + yj + zij} = t - xi - yj - zij$ such that the reduced norm

$$n : Q \rightarrow K, n(\alpha) = \alpha\bar{\alpha}$$

of Q is a quaternary totally positive definite quadratic form over K with $n(\alpha\beta) = n(\alpha)n(\beta)$ for all $\alpha, \beta \in Q$. The group of proper isometries of the quadratic space is known to be

$$(1) \quad \text{SO}(Q, n) = \{x \mapsto \alpha x \beta \mid \alpha, \beta \in Q^*, n(\alpha)n(\beta) = 1\}$$

(see e.g. [5, Appendix IV, Proposition 3] or [16, Proposition 4.3]).

The canonical involution $\bar{}$ of Q is an improper isometry of (Q, n) , so $O(Q, n) = \text{SO}(Q, n) : \langle \bar{} \rangle$.

Remark 3.1. The Gram matrix of (Q, n) with respect to the basis $(1, i, j, ij)$ from above is $\text{diag}(1, -a, -b, ab)$. Hence the determinant of (Q, n) is a square and its Clifford invariant can be computed with [14, Formula (11.12)] as the class of Q in the Brauer group of K .

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 proper overorder. A full \mathbb{Z}_K -lattice J in the vector space Q is called *normal*, if its right order

$$O_r(J) := \{\alpha \in Q \mid J\alpha \subseteq J\}$$

is a maximal order in Q . Then also its left order $O_\ell(J) := \{\alpha \in Q \mid \alpha J \subseteq J\}$ is maximal (see [25]) and J is an invertible fractional left (right) ideal of its left (right) order. J is called a two sided \mathcal{M} -ideal, if $O_r(J) = O_\ell(J) = \mathcal{M}$. The two sided \mathcal{M} -ideals form an abelian group containing the subgroup of principal two sided \mathcal{M} -ideals $\{\mathcal{M}\alpha \mid \alpha \in \mathcal{N}(\mathcal{M})\}$, where

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

is the normaliser of \mathcal{M} .

Remark 3.2. Any normal lattice $J_{\mathfrak{p}}$ in the completion $Q_{\mathfrak{p}} := Q \otimes_K K_{\mathfrak{p}}$ is free, hence of the form $\alpha O_r(J_{\mathfrak{p}})$ for some $\alpha \in Q_{\mathfrak{p}}^*$. The map

$$J_{\mathfrak{p}} \rightarrow J_{\mathfrak{p}} : \gamma \mapsto \alpha \bar{\gamma} \frac{\alpha}{n(\alpha)}$$

is an improper isometry of $(J_{\mathfrak{p}}, n)$.

We call two normal ideals I, J left-, right-, respectively two sided *equivalent*, if there are $\alpha, \beta \in Q$ such that $I = \alpha J$, $I = J\beta$, respectively $I = \alpha J\beta$. We denote by

$$C(J) := \{\alpha J\beta \mid \alpha, \beta \in Q^*\}$$

the two sided equivalence class of the normal lattice J .

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

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

Clearly $N(\alpha J\beta) = n(\alpha)n(\beta)N(J)$ so the norm gives a well defined map

$$\bar{N} : \{C(J) \mid J \text{ normal ideal}\} \rightarrow \text{CL}^+(K), C(J) \mapsto [N(J)]$$

from the set of equivalence classes of normal ideals in Q into the narrow class group $\text{CL}^+(K)$ of K .

Let \mathfrak{a} be a fractional ideal of \mathbb{Z}_K . We call a normal ideal J in Q (and also its two sided equivalence class) of *type* $[\mathfrak{a}]$ if $\overline{N}(J) = [\mathfrak{a}]$. Then the stably free ideals are exactly the ones of type $[\mathbb{Z}_K]$.

Let J be a normal ideal of type $[\mathfrak{a}]$. Then $N(J) = \mathfrak{a}\mathfrak{a}$ for some totally positive $a \in K$. By the theorem of Hasse-Schilling-Maass, there is some $\alpha \in Q$ such that $n(\alpha) = \frac{1}{a}$. Then $N(\alpha J) = \mathfrak{a}$. So any two sided equivalence class of type $[\mathfrak{a}]$ is represented by some normal ideal J with $N(J) = \mathfrak{a}$. We call such a representative \mathfrak{a} -*normalised*. Then the set of all \mathfrak{a} -normalised representatives of $C(J)$ is

$$C_{\mathfrak{a}}(J) := \{\alpha J \beta^{-1} \mid \alpha, \beta \in Q^*, n(\alpha)n(\beta^{-1}) \in \mathbb{Z}_K^*\},$$

the orbit of J under the action of $\{(\alpha, \beta) \in Q^* \times Q^* \mid n(\alpha)n(\beta^{-1}) \in \mathbb{Z}_K^*\}$. The next lemma shows that the stabiliser of J under this action is the group

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

Clearly $\mathcal{A}(J)$ does only depend on the left- and right order of J .

Lemma 3.3. *Let J be a normal ideal and let $\alpha, \beta \in Q^*$. Then $\alpha J \beta^{-1} = J$ if and only if $(\alpha, \beta) \in \mathcal{A}(J)$.*

Proof. \Rightarrow : Is $\alpha J \beta^{-1} = J$ then $O_r(\alpha J \beta^{-1}) = \beta O_r(J) \beta^{-1} = O_r(J)$ and hence $\beta \in \mathcal{N}(O_r(J))$. Similarly $\alpha \in \mathcal{N}(O_{\ell}(J))$. Moreover $N(J) = N(\alpha J \beta^{-1}) = n(\alpha)n(\beta^{-1})N(J)$ implies that $n(\alpha)n(\beta^{-1}) \in \mathbb{Z}_K^*$.

\Leftarrow : Consider the ideal $I := J^{-1}\alpha J \beta^{-1}$. Then $O_{\ell}(I) = O_r(I) = O_r(J)$, so I is a two sided $O_r(J)$ -ideal. Moreover $N(I) = \mathbb{Z}_K$. Therefore $I = O_r(J)$ and hence

$$J = JO_r(J) = JI = JJ^{-1}\alpha J \beta^{-1} = \alpha J \beta^{-1}.$$

□

For a normal ideal J we denote by

$$U(J) := \{n(\alpha)n(\beta^{-1}) \mid (\alpha, \beta) \in \mathcal{A}(J)\}.$$

As the norm of an element of Q is always totally positive, the group $U(J)$ is a subgroup of the group $\mathbb{Z}_{K, > 0}^*$ of totally positive units of \mathbb{Z}_K . It always contains $(\mathbb{Z}_K^*)^2$.

Proposition 3.4. *Let J be a normal lattice with $N(J) = \mathfrak{a}$. A system of representatives of all proper isometry classes of lattices (I, n) where $I \in C_{\mathfrak{a}}(J)$ is*

$$\text{Lat}(J) := \{(J, un) \mid u \in \mathbb{Z}_{K, > 0}^*/U(J)\} = \{(\alpha_u J, n) \mid u \in \mathbb{Z}_{K, > 0}^*/U(J)\}$$

where $\alpha_u \in Q$ is chosen such that $n(\alpha_u) = u$.

All these lattices have the same proper automorphism group

$$\text{Aut}^+(J, un) = \{\gamma \mapsto \alpha \gamma \beta^{-1} \mid (\alpha, \beta) \in \mathcal{A}(J), n(\alpha) = n(\beta)\}.$$

Proof. Let $(\alpha_u J, n)$ be properly isometric to $(\alpha_v J, n)$. Then there are $\alpha, \beta \in Q^*$, $n(\alpha)n(\beta^{-1}) = 1$ such that $\alpha \alpha_u J \beta^{-1} = \alpha_v J$, so $(\alpha_v^{-1} \alpha \alpha_u) J \beta^{-1} = J$. In particular $\alpha' := (\alpha_v^{-1} \alpha \alpha_u) \in \mathcal{N}(O_{\ell}(J))$ and $\beta \in \mathcal{N}(O_r(J))$, satisfy $v^{-1}u = n(\alpha_v^{-1})n(\alpha_u) = n(\alpha')n(\beta^{-1}) \in U(J)$. So $uU(J) = vU(J)$.

Now let $I = \alpha J \beta^{-1} \in C_{\mathfrak{a}}(J)$, so $n(\alpha)n(\beta^{-1}) \in \mathbb{Z}_K^*$. Let $uU(J) = n(\alpha)n(\beta^{-1})U(J)$. Then there are $\alpha' \in \mathcal{N}(O_{\ell}(J))$, $\beta' \in \mathcal{N}(O_r(J))$ such that $un(\alpha')n(\beta'^{-1}) = n(\alpha)n(\beta^{-1})$.

In particular $n(\alpha')n(\beta'^{-1}) \in \mathbb{Z}_K^*$ and hence $\alpha'J\beta'^{-1} = J$ by Lemma 3.3. Moreover $n(\alpha_u\alpha'\alpha^{-1}) = n(\beta\beta'^{-1})$ so

$$(I, n) = (\alpha J\beta^{-1}, n) \cong^+ (\alpha_u\alpha'\alpha^{-1}(\alpha J\beta^{-1})\beta\beta'^{-1}, n) = (\alpha_u\alpha'J\beta'^{-1}, n) = (\alpha_u J, n).$$

□

For $a \in \mathbb{Z}_K^*$ the elements $(\alpha a, \beta a)$ and (α, β) in $\mathcal{A}(J)$ induce the same isometry between (J, n) and $(J, n(\alpha)n(\beta^{-1})n)$. So we have the following short exact sequence

$$\{1\} \rightarrow \text{Aut}^+(J, n) \rightarrow \mathcal{A}(J)/\mathbb{Z}_K^* \rightarrow U(J) \rightarrow \{1\}.$$

4. QUATERNARY LATTICES

In this section we fix a totally real number field K and a totally positive definite quadratic space (V, q) of dimension 4 over K . To apply the theory of the previous section, we assume that $\det(V, q)$ is a square in K . Then the Clifford invariant $c(V, q) = [Q]$ is the class of a totally definite quaternion algebra Q in the Brauer group of K and by Theorem 2.1 we have that

$$(V, q) \cong (Q, n).$$

So without loss of generality, we may assume that $(V, q) = (Q, n)$. If $K = \mathbb{Q}$ it is shown in [22] that the proper isometry classes of lattices in the genus $\mathcal{G}_{\mathbb{Z}}(Q, n)$ of maximal lattices in (Q, n) correspond to two sided equivalence classes of normal lattices J in Q . To extend this correspondence to our more general situation let \mathfrak{a} be a fractional ideal in K and choose \mathfrak{a} -normalised ideals J_1, \dots, J_k in Q such that

$$\biguplus_{i=1}^k C_{\mathfrak{a}}(J_i)$$

is the set of all \mathfrak{a} -normalised normal lattices in Q .

Theorem 4.1. $\biguplus_{i=1}^k \text{Lat}(J_i)$ is a system of representatives of the proper isometry classes of lattices in $\mathcal{G}_{\mathfrak{a}}(Q, n)$.

Proof. Let $1 \leq i, j \leq k$ and $\alpha_u, \alpha_v \in Q^*$, $n(\alpha_u) = u \in \mathbb{Z}_K^*$, $n(\alpha_v) = v \in \mathbb{Z}_K^*$ such that $(\alpha_u J_i, n)$ and $(\alpha_v J_j, n)$ are properly isometric. Then there are $\alpha, \beta \in Q^*$, $n(\alpha)n(\beta) = 1$, $\alpha_v J_j = \alpha \alpha_u J_i \beta \in C(J_i)$ so also $\alpha_v J_j \in C_{\mathfrak{a}}(J_i)$ and hence $i = j$. Applying Proposition 3.4 we see that the lattices in $\biguplus_{i=1}^k \text{Lat}(J_i)$ are pairwise not properly isometric.

$\text{Lat}(J_i) \subseteq \mathcal{G}_{\mathfrak{a}}(Q, n)$:

Let $J := J_i$ for some $1 \leq i \leq k$. We need to show that the completions $(\alpha_u J_{\mathfrak{p}}, n)$ are $\mathfrak{a}_{\mathfrak{p}}$ -maximal for all maximal ideals \mathfrak{p} of \mathbb{Z}_K . So after rescaling, we may assume that $\mathfrak{a} = \mathbb{Z}_K$ and only show that $(\alpha_u J_{\mathfrak{p}}, n) \cong (\mathcal{M}_{\mathfrak{p}}, n)$. But $J_{\mathfrak{p}} = \beta_{\mathfrak{p}} O_r(J_{\mathfrak{p}})$ for some $\beta_{\mathfrak{p}} \in Q_{\mathfrak{p}}^*$ is a principal ideal. Since $N(J) = \mathbb{Z}_K$ it follows that $n(\beta_{\mathfrak{p}}) \in \mathbb{Z}_{K_{\mathfrak{p}}}^*$ so $(\alpha_u J_{\mathfrak{p}}, n) = (\alpha_u \beta_{\mathfrak{p}} O_r(J_{\mathfrak{p}}), n)$ is maximal integral, since $(O_r(J_{\mathfrak{p}}), n)$ is maximal integral. Hence $(\alpha_u J, n) \in \mathcal{G}_{\mathbb{Z}_K}(Q, n)$.

$\mathcal{G}_{\mathfrak{a}}(Q, n) \subseteq \bigcup_{i=1}^k \bigcup \{[L]^+ \mid L \in \text{Lat}(J_i)\}$:

Fix some $1 \leq i \leq k$ and put $J := J_i$. Suppose $(I, n) \in \mathcal{G}_{\mathfrak{a}}(Q, n)$ is in the genus of (J, n) . As J is locally free it locally admits improper automorphisms (see Remark 3.2). So the lattices (I, n) and (J, n) are properly isometric at all places of K . So

for each maximal ideal \mathfrak{p} of \mathbb{Z}_K there exist $\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}} \in Q_{\mathfrak{p}}^*$ such that $n(\alpha_{\mathfrak{p}})n(\beta_{\mathfrak{p}}) = 1$ and $I_{\mathfrak{p}} = \alpha_{\mathfrak{p}}J_{\mathfrak{p}}\beta_{\mathfrak{p}}$. In particular, I is a normal lattice in Q and $N(I) = N(J) = \mathfrak{a}$. \square

5. EICHLER'S MASS FORMULA.

As above let Q be a totally definite quaternion algebra over the totally real number field K . Denote by $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ the maximal ideals of \mathbb{Z}_K that ramify in Q (i.e. where the completion $Q_{\mathfrak{p}_i}$ is a division algebra). Let \mathcal{M} be a maximal order in Q . It is well known, that the unit group index $[\mathcal{M} : \mathbb{Z}_K]$ is finite, see for example [34, Théorème V.1.2]. This can also be seen as follows. Let $\mathcal{M}^{(1)} = \{x \in \mathcal{M} \mid n(x) = 1\}$ be the norm one subgroup of \mathcal{M}^* . Note that the group $\mathcal{M}^{(1)}$ is finite since the norm form n is totally positive definite. By Dirichlet's Unit Theorem, the quotient $n(\mathcal{M}^*)/(\mathbb{Z}_K^*)^2$ is also finite. Hence we have an exact sequence of finite groups

$$1 \rightarrow \mathcal{M}^{(1)}/\{\pm 1\} \rightarrow \mathcal{M}^*/\mathbb{Z}_K^* \rightarrow n(\mathcal{M}^*)/(\mathbb{Z}_K^*)^2 \rightarrow 1.$$

Let

$$\mathcal{I}(\mathcal{M}) := \{I_1, \dots, I_h\}$$

be a system of representatives of the left equivalence classes of right ideals of \mathcal{M} . Then h is called the *class number* of Q . It does not depend on the chosen maximal order \mathcal{M} and it is always bigger or equal to the *type number* t of Q , the number of conjugacy classes of maximal orders in Q . The *mass* of \mathcal{M} is

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

Theorem 5.1 (Eichler [6]).

$$\text{Mass}(\mathcal{M}) = 2^{1-[K:\mathbb{Q}]} |\zeta_K(-1)| h_K \prod_{i=1}^s (|\mathbb{Z}_K/\mathfrak{p}_i| - 1)$$

where h_K is the class number of K .

To obtain the mass of the stably free ideal classes, let $h_K^+ := |\text{CL}^+(K)|$ be the narrow class number of K and fix some narrow class $[\mathfrak{a}]$. Then we define

$$\mathcal{I}(\mathcal{M}, [\mathfrak{a}]) := \{I \in \mathcal{I}(\mathcal{M}) \mid \overline{N}(I) = [\mathfrak{a}]\}$$

and

$$\text{Mass}(\mathcal{M}, [\mathfrak{a}]) := \sum_{I \in \mathcal{I}(\mathcal{M}, [\mathfrak{a}])} [O_{\ell}(I)^* : \mathbb{Z}_K^*]^{-1}.$$

Theorem 5.2. $\text{Mass}(\mathcal{M}, [\mathfrak{a}]) = \frac{1}{h_K^+} \text{Mass}(\mathcal{M})$.

Proof. We define

$$Q_A^* = \{(\alpha_{\mathfrak{p}})_{\mathfrak{p}} \in \prod_{\mathfrak{p}} Q_{\mathfrak{p}}^* \mid \alpha_{\mathfrak{p}} \text{ is a unit almost everywhere}\}$$

the idele group of Q^* . Similarly, we define \mathcal{M}_A^* and K_A^* . Given $\alpha \in Q_A^*$, there exists a unique normal lattice I in Q such that $I_{\mathfrak{p}} = \alpha_{\mathfrak{p}}\mathcal{M}_{\mathfrak{p}}$ locally everywhere. More precisely, the left equivalence classes of fractional right ideals of \mathcal{M} are in bijection with $Q^* \backslash Q_A^* / \mathcal{M}^*$. The theorem of Hasse-Schilling-Maass shows that any

totally positive element of K is a norm, $n(Q^*) = K_{>0}^*$. Further, the reduced norm induces an epimorphism

$$n_A: Q^* \backslash Q_A^* / \mathcal{M}^* \rightarrow K_A^* / K_{>0}^* \cong \text{CL}^+(K), \quad Q^* \alpha \mathcal{M}^* \mapsto (n(\alpha_p))_p.$$

Hence the kernel of n_A is $Q^* \backslash Q^* Q_A^1 / \mathcal{M}^*$ where Q_A^1 denotes the elements $(\alpha_p)_p \in Q_A$ with $n(\alpha_p) = 1$ everywhere.

By [34, Chapitre 5] $\text{Mass}(\mathcal{M})$ is the volume of $Q^* \backslash Q_A^* / \mathcal{M}^*$ with respect to the canonical Tamagawa measure μ on Q_A^* . Similarly, $\text{Mass}(\mathcal{M}, [\mathfrak{a}])$ is the volume of a coset of $Q^* \backslash Q^* Q_A^1 / \mathcal{M}^*$ with respect to μ . It follows from the fact that μ is invariant under translations, that the quotient $\text{Mass}(\mathcal{M}) / \text{Mass}(\mathcal{M}, [\mathfrak{a}])$ is the index of $Q^* \backslash Q^* Q_A^1 / \mathcal{M}^*$ in $Q^* \backslash Q_A^* / \mathcal{M}^*$. But this index is the narrow class number of K . \square

6. THE MINKOWSKI-SIEGEL MASS FORMULA

From Eichler's mass formula we may deduce the Minkowski-Siegel mass formula for lattices in our special case. Let $\mathcal{P}(\mathbb{Z}_K) \cong K^* / \mathbb{Z}_K^*$ be the group of fractional principal ideals. The index $|\mathbb{Z}_{K,>0}^* / (\mathbb{Z}_K^*)^2|$ is clearly the quotient of the narrow class number and the class number of K ,

$$|\mathbb{Z}_{K,>0}^* / (\mathbb{Z}_K^*)^2| = \frac{h_K^+}{h_K} =: 2^u.$$

Let $\mathcal{M}_1, \dots, \mathcal{M}_t$ represent the isomorphism classes of maximal orders in Q and let

$$N_i := \mathcal{N}(\mathcal{M}_i) / K^* \quad (1 \leq i \leq t).$$

For $1 \leq i, j \leq t$ we define the following maps:

$$\bar{n}_i: N_i \rightarrow \mathcal{P}(\mathbb{Z}_K) / \mathcal{P}(\mathbb{Z}_K)^2, \quad \alpha K^* \mapsto (n(\alpha)) \mathcal{P}(\mathbb{Z}_K)^2$$

and

$$\bar{n}_i \times \bar{n}_j: N_i \times N_j \rightarrow \mathcal{P}(\mathbb{Z}_K) / \mathcal{P}(\mathbb{Z}_K)^2, \quad (\alpha K^*, \beta K^*) \mapsto (n(\alpha)n(\beta^{-1})) \mathcal{P}(\mathbb{Z}_K)^2.$$

Let $\Pi_i := \bar{n}_i(N_i)$ be the image of \bar{n}_i and $2^{f_i} := |\Pi_i|$ denote its order. The kernel of \bar{n}_i is $\mathcal{M}_i K^* / K^* \cong \mathcal{M}_i / \mathbb{Z}_K^*$. Thus $2^{f_i} = |N_i| / |\mathcal{M}_i : \mathbb{Z}_K^*|$. By [6, p. 137], the order of the two sided class group of \mathcal{M}_i is

$$H(\mathcal{M}_i) := |\text{CL}_2(\mathcal{M}_i)| = 2^{s-f_i} h_K.$$

Moreover the image of $\bar{n}_i \times \bar{n}_j$ is $\Pi_i \Pi_j$ of order $2^{f_i+f_j-f_{ij}}$ where

$$|\Pi_i \cap \Pi_j| = 2^{f_{ij}}.$$

We denote by

$$\begin{aligned} \mathcal{U}_{ij} &:= \text{Ker}(\bar{n}_i \times \bar{n}_j) = \{(\alpha K^*, \beta K^*) \in N_i \times N_j \mid n(\alpha\beta^{-1})(K^*)^2 \in \mathbb{Z}_K^*(K^*)^2\} \\ &= \{(\alpha K^*, \beta K^*) \mid (\alpha, \beta) \in \mathcal{A}(\mathcal{M}_i \mathcal{M}_j)\} \end{aligned}$$

and define

$$\bar{n}_{ij}: \mathcal{U}_{ij} \rightarrow \mathcal{P}(\mathbb{Z}_K) / \mathcal{P}(\mathbb{Z}_K)^2, \quad (\alpha K^*, \beta K^*) \mapsto (n(\alpha)) \mathcal{P}(\mathbb{Z}_K)^2.$$

Then the image of \bar{n}_{ij} is exactly $\Pi_i \cap \Pi_j$ and the kernel of \bar{n}_{ij} is

$$\begin{aligned} &\{(\alpha K^*, \beta K^*) \in N_i \times N_j \mid n(\alpha) \in \mathbb{Z}_K^*(K^*)^2, n(\beta) \in \mathbb{Z}_K^*(K^*)^2\} \\ &= \mathcal{M}_i^* K^* / K^* \times \mathcal{M}_j^* K^* / K^* \cong \mathcal{M}_i^* / \mathbb{Z}_K^* \times \mathcal{M}_j^* / \mathbb{Z}_K^*. \end{aligned}$$

We need one more map

$$\widetilde{n}_{ij} : \mathcal{U}_{ij} \rightarrow \mathbb{Z}_{K,>0}^*(K^*)^2 / (K^*)^2 \cong \mathbb{Z}_{K,>0}^* / (\mathbb{Z}_K^*)^2, (\alpha K^*, \beta K^*) \mapsto n(\alpha\beta^{-1})(K^*)^2$$

and its kernel $\mathcal{V}_{ij} := \text{Ker}(\widetilde{n}_{ij})$. Let $2^{y_{ij}}$ be the index of $\mathcal{M}_i^{(1)} / \{\pm 1\} \times \mathcal{M}_j^{(1)} / \{\pm 1\}$ in \mathcal{V}_{ij} .

Remark 6.1. Let J be a normal ideal with right order $O_r(J) = \mathcal{M}_j$ and left order $O_\ell(J) = \mathcal{M}_i$. Then the subgroup $U(J) \leq \mathbb{Z}_{K,>0}^*$ from Proposition 3.4 satisfies

$$U(J) / (\mathbb{Z}_K^*)^2 = \widetilde{n}_{ij}(\mathcal{U}_{ij}).$$

In particular

$$|\mathbb{Z}_{K,>0}^* / U(J)| =: 2^{z_{ij}} \text{ with } 2^{u-z_{ij}} = |\mathcal{U}_{ij} / \mathcal{V}_{ij}|.$$

All the groups defined before contain

$$\mathcal{M}_i^{(1)} K^* / K^* \times \mathcal{M}_j^{(1)} K^* / K^* \cong \mathcal{M}_i^{(1)} / \{\pm 1\} \times \mathcal{M}_j^{(1)} / \{\pm 1\}.$$

For further computations we define

$$2^{x_i} := |\mathcal{M}_i^* / \mathcal{M}_i^{(1)} \mathbb{Z}_K^*| = |n(\mathcal{M}_i^*) / (\mathbb{Z}_K^*)^2|.$$

Figure 1 illustrates the various subgroups of the group $N_i \times N_j$.

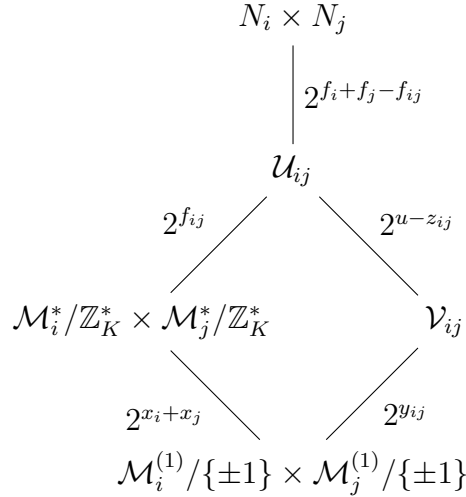


FIGURE 1. Some subgroups of $N_i \times N_j$ and their indices.

Lemma 6.2. *Let J be as in Remark 6.1. Then the proper isometry group of the lattice (J, n) only depends on the left and right orders of J and*

$$|\text{Aut}^+(J, n)| = \frac{1}{2} |\mathcal{M}_i^{(1)}| |\mathcal{M}_j^{(1)}| 2^{y_{ij}}.$$

Proof. By Proposition 3.4 every proper automorphism of (J, n) is of the form $x \mapsto axb^{-1}$ with $a \in \mathcal{N}(\mathcal{M}_i)$, $b \in \mathcal{N}(\mathcal{M}_j)$ and $n(a) = n(b)$. This induces an epimorphism $\text{Aut}^+(J, n) \rightarrow \mathcal{V}_{i,j}$ with kernel $\{\pm \text{id}_J\}$. \square

We now fix an order \mathcal{M}_j and some $1 \leq i \leq t$.

Lemma 6.3. *The number of two sided equivalence classes represented by normal ideals in Q having left order \mathcal{M}_i and right order \mathcal{M}_j is*

$$h_K 2^{s-f_i-f_j+f_{ij}}.$$

Proof. Let $(T_1, \dots, T_{2^s h_K})$ be a transversal of $\{x\mathcal{M}_i \mid x \in K^*\}$ in the abelian group of two sided ideals of \mathcal{M}_i . We consider the set $\mathcal{S} := \{T_\ell \mathcal{M}_i \mathcal{M}_j \mid 1 \leq \ell \leq 2^s h_K\}$. The group $N_i \times N_j$ acts on \mathcal{S} via

$$(N_i \times N_j) \times \mathcal{S} \rightarrow \mathcal{S}, ((aK^*, bK^*), I) \mapsto a\lambda I b^{-1}$$

where $\lambda \in K^*$ is chosen such that $a\lambda I b^{-1} \in \mathcal{S}$. Lemma 3.3 shows that the stabiliser of any ideal in \mathcal{S} is \mathcal{U}_{ij} . In particular, \mathcal{S} consists of $h_K 2^{s-f_i-f_j+f_{ij}}$ orbits. The result follows since the number of orbits is also the number of two sided equivalence classes represented by normal ideals in Q having left order \mathcal{M}_i and right order \mathcal{M}_j . \square

To state the Minkowski-Siegel mass formula let L_1, \dots, L_k be a system of representatives of proper isometry classes of lattices in $\mathcal{G}_a(Q, n)$. Then the mass of this genus of \mathfrak{a} -maximal lattices is defined as

$$\text{Mass}(\mathcal{G}_a(Q, n)) := \sum_{i=1}^k \frac{1}{|\text{Aut}^+(L_i)|}.$$

Already Siegel gave an analytic expression for the mass of a genus of arbitrary positive definite \mathbb{Z}_K -lattices (see [31] and [32]). In our special situation, this expression can also be derived from Eichler's mass formula:

Theorem 6.4. *For any fractional ideal \mathfrak{a} of K*

$$\text{Mass}(\mathcal{G}_a(Q, n)) = \text{Mass}(\mathcal{M})^2 / (h_K^2 2^{s+1})$$

where $\text{Mass}(\mathcal{M})$ is as in Theorem 5.1.

Proof. Clearly the map $(L, n) \mapsto (L, an)$ is an isometry preserving bijection between \mathcal{G}_a and \mathcal{G}_{aa} for any totally positive $a \in K$. So it is enough to show the theorem for representatives $\mathfrak{a}_1, \dots, \mathfrak{a}_{h_K^+}$ of $\text{CL}^+(K)$.

We fix an order \mathcal{M}_j and some $1 \leq i \leq t$. Remark 6.3 gives the number of right ideals in $\mathcal{I}(\mathcal{M}_j)$ having left order isomorphic to \mathcal{M}_i as $h_K 2^{s-f_i-f_j+f_{ij}}$. By Proposition 3.4 these right ideals give rise to $2^{z_{ij}}$ proper isometry classes of lattices (see Remark 6.1), all having the same proper isometry group which has order $2|\mathcal{M}_i^{(1)}/\{\pm 1\}||\mathcal{M}_j^{(1)}/\{\pm 1\}|2^{y_{ij}}$ by Lemma 6.2. So

$$\begin{aligned} \sum_{i=1}^{h_K^+} \text{Mass}(\mathcal{G}_{\mathfrak{a}_i}(Q, n)) &= \sum_{i,j=1}^t 2^{z_{ij}} \frac{h_K 2^{s-f_i-f_j+f_{ij}}}{2|\mathcal{M}_i^{(1)}/\{\pm 1\}||\mathcal{M}_j^{(1)}/\{\pm 1\}|2^{y_{ij}}} \\ &= \sum_{i,j=1}^t h_K 2^{s-f_i} 2^{s-f_j} 2^{u-s} \frac{2^{f_{ij}}}{2|\mathcal{M}_i^{(1)}/\{\pm 1\}||\mathcal{M}_j^{(1)}/\{\pm 1\}|2^{y_{ij}-z_{ij}+u}} \end{aligned}$$

using $y_{ij} - z_{ij} + u = f_{ij} + x_i + x_j$ we conclude

$$\begin{aligned} &= \sum_{i,j=1}^t \frac{H(\mathcal{M}_i)H(\mathcal{M}_j)}{h_K} \frac{h_K^+}{h_K} 2^{-s} \frac{1}{2|\mathcal{M}_i^*/\mathbb{Z}_K^*||\mathcal{M}_j^*/\mathbb{Z}_K^*|} \\ &= \text{Mass}(\mathcal{M})^2 \frac{h_K^+}{h_K^2} 2^{-1-s}. \end{aligned}$$

Now by [8] all the masses of $\mathcal{G}_a(Q, n)$ are the same (as locally the lattices are just rescaled versions of each other), so the theorem follows. \square

7. PROPER ISOMETRY CLASSES IN $\mathcal{G}_a(Q, n)$

To determine the proper isometry classes in $\mathcal{G}_a(Q, n)$, we first fix a maximal order \mathcal{M} in Q and determine

$$\mathcal{I}(\mathcal{M}) = \bigsqcup_{[\mathfrak{b}] \in \text{CL}^+(K)} \mathcal{I}(\mathcal{M}, [\mathfrak{b}])$$

using the algorithm described in [12]. In particular this algorithm also gives a set

$$\{\mathcal{M} = \mathcal{M}_1, \dots, \mathcal{M}_t\}$$

representing the isomorphism classes of maximal orders in Q . Then right multiplication by $X_i := \mathcal{M}\mathcal{M}_i$ gives a bijection

$$(2) \quad \mathcal{I}(\mathcal{M}_i, [\mathfrak{b}]) = \mathcal{I}(\mathcal{M}, [\mathfrak{b}]\overline{N}(X_i)^{-1})X_i.$$

In particular

$$\mathcal{I}([\mathfrak{a}]) := \bigsqcup_{i=1}^t \mathcal{I}(\mathcal{M}_i, [\mathfrak{a}])$$

contains representatives for all two sided equivalence classes of normal ideals in Q whose norm is in $[\mathfrak{a}]$.

Proposition 7.1. *Two lattices I, J in $\mathcal{I}([\mathfrak{a}])$ are two sided equivalent if and only if $I, J \in \mathcal{I}(\mathcal{M}_i, [\mathfrak{a}])$ for some i and there is some $\beta \in \mathcal{N}(\mathcal{M}_i)$ such that $I\beta$ is left equivalent to J .*

Proof. \Leftarrow : Clear.

\Rightarrow : Assume that there are $\alpha, \beta \in Q^*$, such that $\alpha I \beta = J$. Then $O_r(I) = \beta O_r(J) \beta^{-1}$ and $O_r(J)$ are isomorphic. By construction they must be equal, $O_r(J) = O_r(I) = \mathcal{M}_i$, say and hence $\beta \in \mathcal{N}(\mathcal{M}_i)$ and $I, J \in \mathcal{I}(\mathcal{M}_i, [\mathfrak{a}])$ \square

Let \mathcal{J}_i be a set of \mathfrak{a} -normalised orbit representatives of the action of $\mathcal{N}(\mathcal{M}_i)$ on $\mathcal{I}(\mathcal{M}_i, [\mathfrak{a}])$ for all $i = 1, \dots, t$ and denote by $\mathcal{J}_{ji} := \{J \in \mathcal{J}_i \mid O_\ell(J) \cong \mathcal{M}_j\}$. All J in \mathcal{J}_{ji} define the same group $U(J) \leq \mathbb{Z}_{K, >0}^*$ (cf. Proposition 3.4).

Corollary 7.2. *Let $\text{Lat}_{ji}(\mathfrak{a}) := \{(J, un) \mid J \in \mathcal{J}_{ji}, u \in \mathbb{Z}_{K, >0}^*/U(J)\}$. Then*

$$\bigsqcup_{j,i=1}^t \text{Lat}_{ji}(\mathfrak{a})$$

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

Remark 7.3. The computation of a system of representatives of the proper isometry classes in $\mathcal{G}_a(Q, n)$ using Corollary 7.2 is much faster than using Kneser's neighbour method [26] directly. There are mainly two reasons for this.

- (1) For the computation of $\biguplus_{j,i=1}^t \text{Lat}_{ji}(\mathbf{a})$ one only has to enumerate the set $\mathcal{I}(\mathcal{M})$ using the algorithm described in [12]. The size of the set $\mathcal{I}(\mathcal{M})$ is the class number h of Q . From eq. (2), one then immediately obtains the sets $\mathcal{I}(\mathcal{M}_i, [\mathbf{b}])$ for $1 \leq i \leq t$.

If K has narrow class number 1, then Corollary 7.2 shows that the number of proper isometry classes in $\mathcal{G}_a(Q, n)$ is at least $ht/2^s \geq t^2/2^{2s}$. So using Kneser's method directly requires to enumerate way more lattices than the enumeration of the $h \leq 2^s t$ ideal classes in \mathcal{M} .

- (2) The bottleneck of Kneser's method is the computation of many isometries between \mathbb{Z}_K -lattices. The computation of such an isometry is usually done by computing a suitable isometry of the corresponding trace lattices, see for example [11, Remark 2.4.4]. Since the trace lattices have rank $4[K : \mathbb{Q}]$, this method is limited to $[K : \mathbb{Q}]$ being small.

Computing a system of representatives for the right ideal classes of \mathcal{M} does not require the computations of isometries, since isomorphism tests for normal ideals amount only to the computation of minima of \mathbb{Z} -lattices, see [12, Algorithm 6.3]. The computation of a lattice minimum is much faster than the computation of an isometry.

7.1. Example: Unimodular lattices over $\mathbb{Z}[\sqrt{15}]$. As an example we take $K = \mathbb{Q}[\sqrt{15}]$. Then $\mathbb{Z}_K = \mathbb{Z}[\sqrt{15}]$, $h_K = 2$, $h_K^+ = 4$. The narrow class group of K is

$$\{[\mathbb{Z}_K], [(3, \sqrt{15}) = \mathfrak{p}_3], [(5, \sqrt{15}) = \mathfrak{p}_5], [(\sqrt{15}) = \mathfrak{p}_3\mathfrak{p}_5]\}$$

and the fundamental unit $\epsilon = 4 + \sqrt{15}$ of \mathbb{Z}_K is totally positive.

We take $Q = \left(\frac{-1, -1}{K}\right)$ to be the quaternion algebra over K ramified only at the two infinite places. With the algorithm from [12] that is implemented in Magma [2] we compute that Q has 8 maximal orders each of class number 8. We list these maximal orders \mathcal{M}_i ($1 \leq i \leq 8$) by giving the structure of their unit group:

i	$\mathcal{M}_i^*/\mathbb{Z}_K^*$	$\mathcal{M}_i^{(1)}/\{\pm 1\}$	$n(\mathcal{M}_i^*)/(\mathbb{Z}_K^*)^2$	$n(N_i)/(\mathbb{Z}_K^*)^2$
1	$C_2 \times C_2$	$C_2 \times C_2$	1	$\langle 2 \rangle$
2	$C_2 \times C_2$	C_2	$\langle \epsilon \rangle$	$\langle 2, 2\epsilon \rangle$
3	A_4	A_4	1	$\langle 2 \rangle$
4	C_2	1	$\langle \epsilon \rangle$	$\langle 2, 2\epsilon \rangle$
5	S_3	C_3	$\langle \epsilon \rangle$	$\langle 2, 2\epsilon \rangle$
6	S_3	S_3	1	$\langle 2\epsilon \rangle$
7	$C_2 \times C_2$	C_2	$\langle \epsilon \rangle$	$\langle 2, 2\epsilon \rangle$
8	C_3	C_3	1	$\langle 2\epsilon \rangle$

From this information we get

$$\Pi_i = \langle (2) \rangle, f_i = f_{ij} = 1 \text{ for all } i, j$$

and $z_{ij} = 1$ if $\{i, j\} \in \{\{1, 1\}, \{3, 3\}, \{1, 3\}, \{6, 6\}, \{8, 8\}, \{6, 8\}\}$ and $z_{ij} = 0$ in all other cases. We compute that

$$\overline{N}(\mathcal{M}_1\mathcal{M}_j) = \begin{cases} [\mathbb{Z}_K] & \text{for } j \in \{1, 7\} \\ [\mathfrak{p}_3] & \text{for } j \in \{4\} \\ [\mathfrak{p}_5] & \text{for } j \in \{2, 3, 6\} \\ [\mathfrak{p}_3\mathfrak{p}_5] & \text{for } j \in \{5, 8\}. \end{cases}$$

As the class number is equal to the type number, all normal ideals are equivalent to $\mathcal{M}_i\mathcal{M}_j$ for some $1 \leq i, j \leq 8$. Moreover $\overline{N}(\mathcal{M}_i\mathcal{M}_j) = \overline{N}(\mathcal{M}_1\mathcal{M}_i)\overline{N}(\mathcal{M}_1\mathcal{M}_j)$ can be computed from the information above. Using the information on z_{ij} given before, Proposition 3.4 now allows to deduce the number of proper isometry classes of \mathbb{Z}_K -lattices in each of the four genera as listed in the next table. The columns are headed by a set of indices i whereas the entries in the table give the set of values of j such that $\overline{N}(\mathcal{M}_i\mathcal{M}_j)$ lies in the narrow ideal class of the respective row. The entries below the # gives the number of proper isometry classes of lattices obtained by these values (i, j) . Summing up these entries in each row gives the proper class number h^+ of the genus as displayed in the first column of the table:

h^+	\mathfrak{a}	$\{1, 7\}$	#	$\{2, 3, 6\}$	#	$\{4\}$	#	$\{5, 8\}$	#
22	\mathbb{Z}_K	$\{1, 7\}$	5	$\{2, 3, 6\}$	11	$\{4\}$	1	$\{5, 8\}$	5
18	\mathfrak{p}_3^{-1}	$\{4\}$	2	$\{5, 8\}$	7	$\{1, 7\}$	2	$\{2, 3, 6\}$	7
18	\mathfrak{p}_5^{-1}	$\{2, 3, 6\}$	7	$\{1, 7\}$	7	$\{5, 8\}$	2	$\{4\}$	2
14	\mathfrak{p}_{15}^{-1}	$\{5, 8\}$	4	$\{4\}$	3	$\{2, 3, 6\}$	3	$\{1, 7\}$	4

To analyse the lattices we consider the 4-dimensional \mathbb{Z}_K -lattices as \mathbb{Z} -lattices of dimension 8 with the trace of the quadratic form:

Definition 7.4. *Let K be a totally real number field and (L, q) be a totally positive definite \mathbb{Z}_K -lattice in (Q, n) . Then the \mathbb{Z} -trace lattice of (L, q) is the \mathbb{Z} -lattice L equipped with the quadratic form $\text{Tr}(q) : L \rightarrow \mathbb{Q}, \ell \mapsto \text{Tr}_{K/\mathbb{Q}}(q(\ell))$.*

For the four genera considered above, the \mathbb{Z} -trace lattices lie in the genera of even 15-modular (+ type) (see [27] for basic facts on modular lattices), 5-modular, 3-modular resp. unimodular lattices of dimension 8. Of course the latter 14 lattices are as \mathbb{Z} -lattices all isometric to the \mathbb{E}_8 -lattice, the unique even unimodular \mathbb{Z} -lattice of dimension 8. One finds 2 extremal 15-modular lattices (minimum 6 as \mathbb{Z} -lattices): $(\mathcal{M}_3, \epsilon n)$ and $(\mathcal{M}_3\mathcal{M}_6, n) \cong (\mathcal{M}_6\mathcal{M}_3, n)$. There is a unique extremal even 5-modular lattice of dimension 8 (minimum 4 as \mathbb{Z} -lattice), so all the \mathbb{Z} -trace lattices in $\mathcal{G}_{\mathfrak{p}_3^{-1}}(Q, n)$ of minimum 4 are isometric to this lattice. These are $(\mathcal{M}_i\mathcal{M}_j, n)$ for $\{i, j\} = \{2, 5\}, \{3, 8\}$ or $(\mathcal{M}_i\mathcal{M}_j, \epsilon n)$ for $\{i, j\} = \{6, 8\}$.

8. BINARY HERMITIAN FORMS

Assume that we have a CM-field extension E/K with $\text{Gal}(E/K) =: \langle \sigma \rangle$. Then $E = K(\alpha)$ for some $\alpha \in E$ with $\alpha^2 =: \delta \in K$ and $\sigma(\alpha) = -\alpha$. Any non-degenerate Hermitian space (V, h) of dimension n over E gives rise to a non-degenerate quadratic space (V, q_h) of dimension $2n$ over K where $q_h : V \rightarrow K, v \mapsto h(v, v)$. Then the associated symmetric bilinear form b_q (with $b_q(x, y) := q(x + y) - q(x) - q(y)$) satisfies

$$b_q(x\alpha, y) = h(x\alpha, y) + h(y, x\alpha) = h(x, y\sigma(\alpha)) + h(y\sigma(\alpha), x) = b_q(x, y\sigma(\alpha))$$

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

$$h_\varphi := h : V \times V \rightarrow E, h(x, y) := \frac{1}{2}b_q(x, y) + \frac{1}{2\bar{\delta}}b_q(x\varphi(\alpha), y)\alpha$$

is a Hermitian form on V such that $q = q_h$. In this case we call the embedding φ *Hermitian* with respect to q .

Clearly the unitary group $U(V, h)$ embeds into the orthogonal group $O(V, q_h)$. Even more is true: If $g \in U(V, h)$ then $h(xg, yg) = h(x, y)$ for all $x, y \in V$. So the norm of the determinant of $g \in \text{End}_E(V)$, which is the determinant of $g \in \text{End}_K(V)$, is equal to 1 (see [28, Theorem 10.1.5]) and hence

$$U(V, h) \hookrightarrow SO(V, q_h).$$

On the other hand, given a Hermitian embedding $\varphi : E \rightarrow \text{End}_K(V)$ with respect to q , then the unitary group is

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

In this section we want to combine this point of view with the methods developed before to classify binary Hermitian \mathbb{Z}_E -lattices: Given a 2-dimensional totally positive definite Hermitian space (V, h) over E , the associated quadratic space (V, q_h) is a quaternary totally positive definite quadratic space over K . By [28, Chapter 10, Remark 1.4] the determinant of (V, q_h) is a square in K and $c(V, q_h) = [\frac{(\delta, -\det(h))}{K}]$, where $E = K(\alpha)$ with $\alpha^2 = \delta \in K$. So $(V, q_h) \cong (Q, n)$ for the quaternion algebra $Q = \frac{(\delta, -\det(h))}{K}$, in particular E is a maximal subfield of Q and Q is a 2-dimensional vector space over E . As the restriction of the canonical involution of Q to E is the non-trivial Galois automorphism σ of E/K , the norm form n gives rise to a Hermitian form h_n on the 2-dimensional E -vector space Q , such that $(Q, h_n) \cong (V, h)$.

To classify all Hermitian embeddings of E with respect to n we identify $\text{End}_K(Q)$ with $Q^{op} \otimes Q$.

Lemma 8.1. *Let $\varphi : E \rightarrow \text{End}_K(Q)$ be a Hermitian embedding with respect to n . Then*

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

Proof. Write $E = K(\alpha)$ with $\sigma(\alpha) = -\alpha$ and $\alpha^2 \in K$ and let $Q^0 := \{x \in Q \mid x + \bar{x} = 0\}$ be the 3-dimensional K -subspace of trace 0 elements in Q . The restriction of the adjoint involution of n to $Q^{op} \otimes K$ and to $K \otimes Q$ is the canonical involution of Q resp. $Q^{op} \cong Q$. In particular the 6-dimensional space $(Q^{op})^0 \otimes K \oplus K \otimes Q^0$ 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 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 $x \in Q^0, y \in (Q^0)^{op}$. 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 $\varphi(\alpha) = 1 \otimes x \in K \otimes Q$ or $\varphi(\alpha) = y \otimes 1 \in Q^{op} \otimes K$. \square

Clearly the orthogonal group acts on the set of Hermitian embeddings by conjugation.

Proposition 8.2. *Up to the action of $O(Q, n)$ there is a unique Hermitian embedding $\varphi : E \rightarrow \text{End}_K(Q)$.*

Proof. Recall that all proper isometries of (Q, n) are of the form $\tau_{a,b} : x \mapsto axb$ with $a, b \in Q, n(a)n(b) = 1$ and that the canonical involution $x \mapsto \bar{x}$ is an improper isometry $\bar{}$. Given a Hermitian embedding $\varphi : E \rightarrow \text{End}_K(Q)$ with values $\varphi(E) \subseteq Q^{op} \otimes K$, the conjugate by $\bar{}$ yields a Hermitian embedding with values in $K \otimes Q$. By the Theorem of Skolem and Noether any two embeddings φ_1, φ_2 of E into $Q \cong K \otimes Q$ are conjugate in Q^* . So there is some $a \in Q^*$ such that $a\varphi_1a^{-1} = \varphi_2$. The proper isometry $\tau_{a^{-1}, a}$ hence conjugates φ_1 into φ_2 . \square

Note that Proposition 8.2 gives, for the special case of binary Hermitian forms, a more explicit way to show [28, Theorem (10.1.1)] that two Hermitian spaces are isometric, if and only if the corresponding quadratic spaces are isometric over K . However, this is in general not true for lattices: The ring of integers \mathbb{Z}_E also embeds into Q , so there is some maximal order \mathcal{M} in Q containing \mathbb{Z}_E . The lattice (\mathcal{M}, n) is hence a Hermitian \mathbb{Z}_E -lattice L in (V, h) , maximal with respect to the condition that $n(\ell) = h(\ell, \ell) \in \mathbb{Z}_K$ for all $\ell \in L$. Again these maximal Hermitian \mathbb{Z}_E -lattices form a genus ([30]). As before we generalise this notion for an arbitrary fractional \mathbb{Z}_K -ideal \mathfrak{a} and call a hermitian \mathbb{Z}_E -lattice $L \leq (V, h)$ \mathfrak{a} -maximal, if $q_h(L) \subseteq \mathfrak{a}$ and $q_h(L') \not\subseteq \mathfrak{a}$ for all proper \mathbb{Z}_E -overlattices L' of L . We denote by

$$\mathcal{G}_{\mathfrak{a}}(V, h) := \{L \leq (V, h) \mid L \text{ is } \mathfrak{a}\text{-maximal}\}$$

the genus of \mathfrak{a} -maximal \mathbb{Z}_E -lattices in (V, h) . We want to use the techniques explained in the previous section to compute a system of representatives of Hermitian isometry classes of lattices in $\mathcal{G}_{\mathfrak{a}}(V, h)$. For all fractional \mathbb{Z}_K -ideals \mathfrak{a} there is a right \mathcal{M} -ideal J such that $N(J) = \mathfrak{a}$. So there are \mathfrak{a} -maximal \mathbb{Z}_K -lattices in (V, h) that are Hermitian \mathbb{Z}_E -lattices. Therefore $\{(L, q_h) \mid (L, h) \in \mathcal{G}_{\mathfrak{a}}(V, h)\} \subseteq \mathcal{G}_{\mathfrak{a}}(V, q_h)$ and we obtain the following remark.

Remark 8.3. Let \mathfrak{a} be a fractional \mathbb{Z}_K -ideal. Let $L \leq (V, h)$ be an \mathfrak{a} -maximal \mathbb{Z}_E -lattice in (V, h) . Then (L, q_h) is an \mathfrak{a} -maximal \mathbb{Z}_K -lattice in (V, q_h) and there is a Hermitian embedding $\varphi : \mathbb{Z}_E \rightarrow \text{End}_{\mathbb{Z}_K}(L)$.

The reverse direction is dealt with in the next lemma.

Lemma 8.4. *Given an \mathfrak{a} -maximal \mathbb{Z}_K -lattice (L, q) then the set of all isometry classes of Hermitian \mathbb{Z}_E -lattices (L, h_i) such that $q_{h_i} = q$ is in bijection with the set of $\text{Aut}_{\mathbb{Z}_K}(L, q)$ -orbits on the set of all Hermitian embeddings $\varphi_i : \mathbb{Z}_E \rightarrow \text{End}_{\mathbb{Z}_K}(L)$.*

Proof. By the remarks above the set of all Hermitian \mathbb{Z}_E -structures on (L, q) is in bijection to the set of all Hermitian embeddings $\varphi_i : \mathbb{Z}_E \rightarrow \text{End}_{\mathbb{Z}_K}(L)$. If we put $h_i := h_{\varphi_i}$ for short, then we need to show that $(L, h_i) \cong (L, h_j)$ if and only if there is an automorphism $g \in \text{Aut}_{\mathbb{Z}_K}(L, q)$ such that $\varphi_j(e)g = g\varphi_i(e)$ for all $e \in \mathbb{Z}_E$. Clearly any such g yields

$$\begin{aligned} h_i(xg, yg) &= \frac{1}{2}b_q(xg, yg) - \frac{1}{2\delta}b_q(xg\varphi_i(\alpha), yg)\alpha = \\ &= \frac{1}{2}b_q(xg, yg) - \frac{1}{2\delta}b_q(x\varphi_j(\alpha)g, yg)\alpha = \\ &= \frac{1}{2}b_q(x, y) - \frac{1}{2\delta}b_q(x\varphi_j(\alpha), y)\alpha = h_j(x, y) \end{aligned}$$

for all $x, y \in L$. On the other hand, any isometry between (L, h_i) and (L, h_j) is an automorphism of L , preserving the quadratic form $q(x) = h_i(x, x) = h_j(x, x)$. \square

By Lemma 8.1 the image $\varphi(\mathbb{Z}_E)$ of a hermitian embedding into $\text{End}_{\mathbb{Z}_K}(L)$ is either contained in the left or in the right order of the normal lattice L . After conjugation with the improper isometry given by the canonical involution of Q we may assume without loss of generality that $\varphi(\mathbb{Z}_E) \subseteq O_r(L)$.

8.1. An algorithm to determine $\mathcal{G}_a(V, h)$. To determine $\mathcal{G}_a(V, h)$ we start with the system of representatives of \mathbb{Z}_K -isometry classes of lattices in $\mathcal{G}_a(V, q)$ given in Section 7.

Remark 8.5. To compute all Hermitian embeddings $\varphi : \mathbb{Z}_E \hookrightarrow \mathcal{M}$ 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 $\bar{x} = -x$. These elements lie in the sublattice \mathcal{M}^0 of trace 0 elements in \mathcal{M} . The map $\text{Tr}(n) : y \mapsto \text{Tr}_{K/\mathbb{Q}}(n(y))$ defines a positive definite quadratic form on the \mathbb{Z} -lattice \mathcal{M}^0 . Clearly $\text{Tr}(n)(x) = \text{Tr}_{K/\mathbb{Q}}(-\delta) =: a \in \mathbb{Z}_{>0}$. Using the shortest vector algorithm [7] we enumerate the vectors v of norm a in the \mathbb{Z} -lattice $(\mathcal{M}^0, \text{Tr}(n))$ and then check whether $v^2 = \delta$. For these v the map $\alpha \mapsto v$ then defines an embedding φ of E into Q . It yields an embedding of \mathbb{Z}_E into \mathcal{M} if and only if $\varphi(\mathbb{Z}_E) \subseteq \mathcal{M}$.

For $1 \leq i, j \leq t$ let

$$\mathcal{N}_{ij} := \{a \in \mathcal{N}(\mathcal{M}_j) \mid \exists b \in \mathcal{N}(\mathcal{M}_i), n(a) = n(b)\}$$

be the projection of the proper automorphism group of $\mathcal{M}_i \mathcal{M}_j$ onto the second component and let Φ_{ij} be a system of representatives of the \mathcal{N}_{ij} orbits of the Hermitian embeddings of \mathbb{Z}_E into \mathcal{M}_j .

Theorem 8.6. *The set $\{(L, h_\varphi) : L \in \text{Lat}_{ij}(\mathfrak{a}), \varphi \in \Phi_{ij}\}$ is a system of representatives of isometry classes of lattices in $\mathcal{G}_a(V, h)$.*

Proof. Assume that (L, h_φ) and $(L', h_{\varphi'})$ are isometric as Hermitian lattices. Then also the underlying \mathbb{Z}_K -lattices (L, q_{h_φ}) and $(L', q_{h_{\varphi'}})$ are isometric, so $L = L'$ and Lemma 8.4 implies that there is $g \in \text{Aut}(L, q)$ such that $g\varphi g^{-1} = \varphi'$. As the images of φ and φ' are both contained in $\mathbb{Z}_K \otimes O_r(L) \subset \text{End}_{\mathbb{Z}_K}(L)$, and the improper automorphisms interchange $O_\ell(L) \otimes \mathbb{Z}_K$ and $\mathbb{Z}_K \otimes O_r(L)$, the element g is a proper isometry. By Proposition 3.4 there is some $a \in \mathcal{N}_{ij}$ such that $a\varphi a^{-1} = \varphi'$, so $\varphi = \varphi'$ by definition of Φ_{ij} .

Now let $(L, h) \in \mathcal{G}_a(V, h)$. Then the \mathbb{Z}_K -lattice $(L, q_h) \in \mathcal{G}_a(V, q_h)$ so by Corollary 7.2 there are $i, j \in \{1, \dots, t\}$ and some $(L, q) \in \text{Lat}_{ij}(\mathfrak{a})$ such that (L, q_h) is properly isometric to (L, q) . Moreover Lemma 8.4 tells us that there is a Hermitian embedding $\varphi : \mathbb{Z}_E \rightarrow \text{End}_{\mathbb{Z}_K}(L)$. After conjugation with the improper isometry given by the canonical involution of Q we may assume without loss of generality that $\varphi(\mathbb{Z}_E) \subseteq O_r(L) = \mathcal{M}_j$. By definition of Φ_{ij} there is some automorphism of (L, q) conjugating φ into Φ_{ij} . Now the theorem follows from Lemma 8.4. \square

8.2. Example: Hermitian unimodular lattices over $\mathbb{Z}[\sqrt{15}][\sqrt{-\epsilon}]$. To continue with Example 7.1 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 from 7.1, giving rise to a Hermitian structure (Q, h) . To find representatives of the isometry classes of Hermitian lattices in $\mathcal{G}_{(\sqrt{15}-1)}(Q, h)$ we first compute all $\mathcal{M}_i^{(1)}$ -orbits of embeddings $\varphi : \mathbb{Z}_E \hookrightarrow \mathcal{M}_i$ for $i = 1, \dots, 8$. We find two such orbits for $i = 2, 4, 5, 7$ and no

embedding for the other values of i . The $(\sqrt{15}^{-1})$ -normalised representatives for the ideals

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

each yield one isometry class of Hermitian lattices in $\mathcal{G}_{(\sqrt{15}^{-1})}(Q, h)$. So this genus has class number 8.

9. BINARY UNIMODULAR LATTICES OVER CERTAIN CYCLOTOMIC FIELDS

In this last 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 of order $4p$ as

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

where $\sigma^2 = -1$, $\sigma \zeta_p \sigma^{-1} = \zeta_p^{-1}$ (see for example [16, Theorem 6.1]). The Hermitian lattice (\mathcal{M}, 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 $A_{p-1} \perp A_{p-1}$. Because of its meaning for the classification of extremal even unimodular lattices, we denote by $D(L, h)$ the dual of the \mathbb{Z} -lattice (L, q) where $q(\ell) = \frac{1}{p} \text{Tr}_{K/\mathbb{Q}}(h(\ell, \ell))$.

Remark 9.1. Let $p \equiv 3 \pmod{4}$ and let (L, h) be a binary unimodular Hermitian $\mathbb{Z}[\zeta_p]$ -lattice. Let $Q' = \left(\frac{-1, -p}{\mathbb{Q}}\right)$ be the quaternion algebra with centre \mathbb{Q} ramified only at p and the infinite place and let \mathcal{M}' be some maximal order in Q' . Then for any lattice (L', q') in the genus of (\mathcal{M}', n) there are exactly $2(p+1)$ even unimodular \mathbb{Z} -lattices (of dimension $2(p+1)$) containing $D(L, h) \perp (L', q')$ of index p^2 . All these even unimodular lattices have an automorphism g of order p with characteristic polynomial $\chi_g = (X^p - 1)^2(X - 1)^2$.

9.1. Class number of Hermitian lattices. It is quite interesting that in the very special case where additionally $h_K^+ = 1$ we can compute the class number of the genus of Hermitian unimodular \mathbb{Z}_E -lattices from the type number t of Q . A formula for t can be found in [34, Corollaire V.2.6].

Proposition 9.2. *Let $p \equiv 3 \pmod{4}$, $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ and $E = \mathbb{Q}(\zeta_p)$ 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 $Q := \left(\frac{-1, -p}{K}\right)$.*

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 Proposition 3.4 equals $\mathbb{Z}_{K, > 0}^*$.

Let $\mathcal{M}_1, \dots, \mathcal{M}_t$ 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 $\mathcal{M}_2, \dots, \mathcal{M}_a$ be the other maximal orders \mathcal{M}_i into which

\mathbb{Z}_E embeds. Then by [33] $\mathcal{M}_i^{(1)} \cong C_{2p}$ for $i = 2, \dots, a$. For all these $i = 1, \dots, a$ the normaliser is

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

It acts on the set of \mathbb{Z}_K -linear embeddings $\varphi : \mathbb{Z}_E \rightarrow \mathcal{M}_i$ with the same orbits as $\mathcal{M}_i^{(1)}$. In particular there is one such orbit for $i = 1$ and two orbits for $i = 2, \dots, a$ and the total number of embeddings is $1 + 2(a - 1) = 2a - 1$. By [34, Corollaire III.5.12] this number is exactly the class number of E , so $h_E = 2a - 1$ is odd. By Corollary 7.2 we need to compute a set of representatives J_i or the $\mathcal{N}(\mathcal{M}_i)$ -orbits on the left-equivalence classes $\mathcal{I}(\mathcal{M}_i)$ of \mathcal{M}_i -right ideals. For $1 \leq i \leq a$ these orbits are of the form $\{[I], [I(1 - \zeta_p)]\}$ and have length 1, if and only if there is some $b \in Q^*$ such that

$$bI = I(1 - \zeta_p).$$

Of course the left order of I is

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

so b normalises $O_\ell(I)$. Moreover the norm of b is the norm of $(1 - \zeta_p)$, so $bO_\ell(I)$ generates the maximal ideal of $O_\ell(I)$ of norm p . By the assumption $h_K = 1$ this condition is equivalent to the fact that the two sided class number $H(O_\ell(I)) = 1$. As $h = \sum_{i=1}^t H(\mathcal{M}_i)$ we compute that the number of $\mathcal{N}(\mathcal{M}_i)$ -orbits on $\mathcal{I}(\mathcal{M}_i)$ is exactly t for all $1 \leq i \leq a$ and a system of representatives is given by

$$\{\mathcal{M}_j \mathcal{M}_i \mid 1 \leq j \leq t\}.$$

So by Theorem 8.6 the number of isometry classes of Hermitian \mathbb{Z}_E -lattices in the genus of (\mathcal{M}, h_n) is $h_E t$. \square

Remark 9.3. The conclusion that h_E is odd follows from the much more general result due to Hasse [10, Satz 42]. There Hasse gives necessary and sufficient conditions for h_E/h_K being odd.

9.2. Examples for small primes p . Due to the growth of 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 9.2.

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 class number of the genus of (\mathcal{M}', n) from Remark 9.1 is 1 and the even unimodular \mathbb{Z} -lattices obtained in Remark 9.1 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 [34, 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}, h_n) has dual trace lattice of minimum 4. Also the genus of the even 4-dimensional 11-modular lattices, the genus of (\mathcal{M}', n) from Remark 9.1, contains a unique lattice 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.

9.2.1. $p = 19$. For $p = 19$ again $h_E = 1$ and hence by [34, 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}, h_n) is 185 by Proposition 9.2. As we are mainly interested in the trace lattices, we group these 185 lattices into orbits under the Galois group $\text{Gal}(E/\mathbb{Q}) \cong C_{18}$ 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, 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 $L \perp L'$ where L is one of these 22 lattices and L' the unique 4-dimensional 19-modular lattice of minimum 4 (cf. Remark 9.1). As $(L^\# / L, q_L) \cong ((L')^\# / L', q_{L'})$ are anisotropic quadratic spaces, the lattice M is of the form

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

for an isometry φ between $-q_{L'}$ and q_L . The automorphism group of L' has 5 orbits on the set of these isometries, so each of the 22 lattices L gives rise to 5 lattices M . Among the 110 lattices M , 12 come in isometric pairs, hence we have shown:

Corollary 9.4. *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 $L \perp L'$ of index 19 such that L 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 $L \cong \mathbb{A}_{18}$ has minimum 2. \square

9.2.2. $p = 23$. 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 ([18, Table 2]). If 23 divides the order of the automorphism group of such a lattice, then by [17, Theorem 4.4] the elements of order 23 have characteristic polynomial $(X^{23} - 1)^2(X - 1)^2$ and these lattices are constructed as in Remark 9.1. Our computations described below in particular show the following corollary.

Corollary 9.5. *There are exactly two isometry classes of extremal even unimodular lattices of dimension 48 that admit an automorphism of order 23.*

So let $p = 23$ and $K = \mathbb{Q}(\zeta_{23} + \zeta_{23}^{-1})$ be the maximal totally real subfield of $E = \mathbb{Q}(\zeta_{23})$. Then the narrow class number $h_K^+ = 1$ 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 9.2 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 $\text{Aut}(P_{48q}) \cong \text{SL}_2(47)$ and the other one to the

respective sublattice of P_{48p} with $\text{Aut}(P_{48p}) \cong (\text{SL}_2(23) \times S_3).2$. Computing the overlattices from Remark 9.1 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 9.5 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.

REFERENCES

- [1] G. Aeberli. Der Zusammenhang zwischen quaternären quadratischen Formen und Idealen in Quaternionenringen. *Comment. Math. Helv.*, 33:212–239, 1959.
- [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] J. Brzezinski. Arithmetical quadratic surfaces of genus 0, I. *Math. Scand.*, 46:183–208, 1980.
- [4] J. Brzezinski. A characterization of Gorenstein orders in quaternion algebras. *Math. Scand.*, 50:19–24, 1982.
- [5] J. Dieudonné. *Linear algebra and geometry*. Hermann, 1969.
- [6] 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.
- [7] 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.
- [8] W. T. Gan, J. Hanke, and J.-K. Yu. On an exact mass formula of Shimura. *Duke Mathematical Journal*, 107, 2001.
- [9] H. Hasse. Äquivalenz quadratischer Formen in einem beliebigen Zahlkörper. *J. reine u. angew. Mathematik*, 153:158–162, 1924.
- [10] H. Hasse. *Über die Klassenzahl abelscher Zahlkörper*. Akademie-Verlag, Berlin, 1952.
- [11] M. Kirschmer. *Definite quadratic and hermitian form with small class number*. Habilitation, RWTH Aachen University, 2016.
- [12] 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>.
- [13] M. Kneser. Composition of binary quadratic forms. *J. Number Theory*, 15(3):406–413, 1982.
- [14] M. Kneser. *Quadratische Formen*. Springer-Verlag, Berlin, 2002. Revised and edited in collaboration with Rudolf Scharlau.
- [15] M. Kneser, M. Ojanguren, M.-A. Knus, R. Parimala, and R. Sridharan. Composition of quaternary quadratic forms. *Compositio Math.*, 60(2):133–150, 1986.
- [16] G. Nebe. Finite quaternionic matrix groups. *Represent. Theory*, 2:106–223, 1998.
- [17] G. Nebe. On automorphisms of extremal even unimodular lattices. *Int. J. Number Theory*, 9(8):1933–1959, 2013.
- [18] G. Nebe. A fourth extremal even unimodular lattice of dimension 48. *Discrete Math.*, 331:133–136, 2014.
- [19] O. T. O'Meara. *Introduction to Quadratic Forms*. Springer, 1973.
- [20] M. Peters. Ternäre und quaternäre quadratische Formen und Quaternionenalgebren. *Acta Arith.*, 15:329–365, 1968/1969.
- [21] P. Ponomarev. Class numbers of definite quaternary forms with square discriminant. *J. Number Theory*, 6:291–317, 1974.
- [22] P. Ponomarev. Arithmetic of quaternary quadratic forms. *Acta Arith.*, 29(1):1–48, 1976.
- [23] P. Ponomarev. A correspondence between quaternary quadratic forms. *Nagoya Math. J.*, 62:125–140, 1976.
- [24] P. Ponomarev. Class number formulas for quaternary quadratic forms. *Acta Arith.*, 39(1):95–104, 1981.
- [25] I. Reiner. *Maximal Orders*. Oxford Science Publications, 2003.

- [26] R. Scharlau and B. Hemkemeier. Classification of integral lattices with large class number. *Math. Comp.*, 67(222):737–749, 1998.
- [27] R. Scharlau and R. Schulze-Pillot. Extremal lattices. In *Algorithmic algebra and number theory (Heidelberg, 1997)*, pages 139–170. Springer, Berlin, 1999.
- [28] W. Scharlau. *Quadratic and Hermitian forms*, volume 270 of *Grundlehren der mathematischen Wissenschaften*. Springer, 1985.
- [29] A. Schiemann. Classification of Hermitian Forms with the Neighbor Method. *J. Symbolic Computation*, 26:487–508, 1998.
- [30] G. Shimura. Arithmetic of unitary groups. *Ann. Math.*, 79:269–409, 1964.
- [31] C. L. Siegel. Über die Analytische Theorie der quadratischen Formen. *Annals of Mathematics*, 36(3):527–606, 1935.
- [32] C. L. Siegel. Über die Analytische Theorie der quadratischen Formen III. *Annals of Mathematics*, 38(1):212–291, 1937.
- [33] M.-F. Vignéras. Simplification pour les ordres des corps de quaternions totalement définis. *J. Reine Angew. Math.*, 286/287:257–277, 1976.
- [34] M.-F. Vignéras. *Arithmétique des Algèbres de Quaternions*, volume 800 of *Lecture Notes in Mathematics*. Springer-Verlag, 1980.
- [35] J. Voight. Characterizing quaternion rings over an arbitrary base. *J. Reine Angew. Math.*, 657:113–134, 2011.

E-mail address: markus.kirschmer@math.rwth-aachen.de

E-mail address: nebe@math.rwth-aachen.de

LEHRSTUHL D FÜR MATHEMATIK, RWTH AACHEN UNIVERSITY, 52056 AACHEN, GERMANY