

# 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  $(V, q)$ . This yields a good algorithm to enumerate a system of representatives of proper isometry classes of lattices in genera of maximal lattices in  $(V, q)$ .

## 1. INTRODUCTION

Small dimensional lattices over algebraic number fields  $K$  have been related to ideals in étale  $K$ -algebras by various authors. In his *Disquisitiones Arithmeticae* Gauß relates proper isometry classes of binary lattices to ideal classes in quadratic extensions of  $K$ . For ternary quadratic forms a similar relation between lattices and quaternion orders has been investigated by Peters ([14]) and Brzezinski ([2], [3]) based on results from Eichler and Brandt, for a functorial correspondence see Voight ([28]).

Quaternary lattices have been investigated by Ponomarev ([15, 16, 17, 18]), who relates the proper isometry classes of lattices in a quaternary quadratic space to certain equivalence classes of ideals in a quaternion algebra, where he is particularly interested in the case where  $K = \mathbb{Q}$ . The present paper generalises Ponomarev's results to arbitrary totally real number fields  $K$  and develops a fast algorithm to enumerate proper isometry classes in certain genera of quaternary lattices.

To state our results let  $(V, q)$  be a totally definite quaternary quadratic space over  $K$  of square discriminant and let  $Q$  be the totally definite quaternion algebra representing its Clifford invariant. Then Theorem 4.1 shows that 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  $\mathfrak{a}$ . This correspondence is used to relate the mass formulas of Siegel and Eichler in Section 6. Section 7 develops an algorithm to enumerate a system of representatives of proper isometry classes of  $\mathfrak{a}$ -maximal lattices in  $(V, q)$  based on the method of [10]. Algorithm 7.1 is much more efficient than the usual Kneser neighbour method (see for instance [20] for a description of a good implementation of this method). This is illustrated in a small and a somewhat larger example in the end of the paper. A further application to the classification of binary Hermitian lattices is given in [9].

**Acknowledgements** The authors thank the anonymous referee for many helpful comments largely improving the exposition of the results. The research is supported by the DFG within the framework of the SFB TRR 195.

## 2. QUADRATIC LATTICES OVER NUMBER FIELDS

In this section, we set up basic notation for quadratic lattices. Let  $K$  be a number field and let  $(V, q)$  be a non-degenerate quadratic space over  $K$ . The most important invariants of  $(V, q)$  are the Clifford invariant  $c(V, q)$  as defined in [22, Remark 2.12] and the determinant  $\det(V, q)$ , which is the square class of the determinant of a Gram matrix of  $(V, q)$ . The interest in these two isometry invariants of quadratic spaces is mainly due to the following classical result by Helmut Hasse.

---

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.

**Theorem 2.1** ([7]). *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

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

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 superscript  $^+$  is omitted.

Certain invariants of a  $\mathbb{Z}_K$ -lattice  $(L, q)$  can be read off from the transfer to the corresponding  $\mathbb{Z}$ -lattice  $(L, \mathrm{Tr}(q))$ , where

$$\mathrm{Tr}(q) : L \rightarrow \mathbb{Q}, \ell \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(q(\ell)).$$

The  $\mathbb{Z}$ -lattice  $(L, \mathrm{Tr}(q))$  is called the *trace lattice* of  $(L, q)$ .

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 lattices  $(L, q)$  and  $(L', q)$  in  $(V, q)$  are *in the same genus*, if

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

The classification of all (proper) isometry classes of lattices in a given genus is an interesting and intensively studied problem (see [20, 23, 8]). 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. Recall that for a (fractional) ideal  $\mathfrak{a}$  of  $\mathbb{Z}_K$  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  $\mathbb{Z}_K$ -lattices  $(L', q)$  in  $(V, q)$  with  $L \subsetneq L'$ . The  $\mathbb{Z}_K$ -maximal lattices are also called *maximal*. Locally, all  $\mathfrak{a}$ -maximal lattices are isometric, see [13, Theorem 91:2]. Hence the set of all  $\mathfrak{a}$ -maximal lattices in  $(V, q)$  forms a single genus, which we denote by  $\mathcal{G}_{\mathfrak{a}}(V, q)$ .

The number of isometry classes in a genus is always finite and it is called the class number of the genus. By the strong approximation theorem, see for instance [13, Theorem 104:4], the class number of a genus can be determined by local invariants if there is an infinite place  $\sigma$  of  $K$  such that  $(V_{\sigma}, q)$  is isotropic. So the only interesting case is when  $K$  is totally real and  $(V_{\sigma}, q)$  is definite for all infinite places  $\sigma$  of  $K$ . After rescaling, we assume that  $(V, q)$  is *totally positive definite*, which means that  $(V_{\sigma}, q)$  is positive definite for all these  $\sigma$ . An element  $a$  of the totally real number field  $K$  is called *totally positive*, if  $\sigma(a) > 0$  for all infinite places  $\sigma$  of  $K$ .

### 3. SOME BASIC FACTS ABOUT QUATERNION ALGEBRAS

This section relates normal ideals in quaternion algebras to maximal lattices. A detailed discussion of the arithmetic of quaternion algebras can be found in [5], [27], and [19]. Let  $Q$  be a totally definite quaternion algebra over an algebraic number field  $K$ . Then  $K$  is totally real and  $Q$  has a basis  $(1, i, j, ij)$  with  $ij = -ji$  and  $i^2 = -a$ ,  $j^2 = -b$  for some totally positive  $a, b \in K$ . The algebra  $Q$  is also denoted by  $Q = \left(\frac{-a, -b}{K}\right)$ . It carries a canonical involution,  $\bar{\cdot} : Q \rightarrow Q$  defined by  $\overline{t + xi + yj + zij} = t - xi - yj - zij$ . The reduced norm

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

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

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

(see e.g. [4, Appendix IV, Proposition 3] or [12, Proposition 4.3]).

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

*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 [11, 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 other order.

**Proposition 3.2.** *If  $\mathcal{M}$  is a maximal order in  $Q$ , then  $(\mathcal{M}, n) \in \mathcal{G}_{\mathbb{Z}_K}(Q, n)$  is a maximal lattice.*

*Proof.* It is enough to show that for all prime ideals  $\mathfrak{p}$  of  $\mathbb{Z}_K$  the completion  $(\mathcal{M}_{\mathfrak{p}}, n)$  is a maximal lattice in  $(Q_{\mathfrak{p}}, n)$ . If  $\mathfrak{p}$  is not ramified, then  $(\mathcal{M}_{\mathfrak{p}}, n)$  is unimodular (see [19, Theorem 20.3]) and if  $\mathfrak{p}$  is ramified in  $Q$  then  $\mathcal{M}_{\mathfrak{p}} = \{x \in Q_{\mathfrak{p}} \mid n(x) \in \mathbb{Z}_{K_{\mathfrak{p}}}\}$  by [19, Theorem 12.8]. In both cases the lattice  $(\mathcal{M}_{\mathfrak{p}}, n)$  is maximal.  $\square$

A  $\mathbb{Z}_K$ -lattice  $J$  in  $Q$  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 [19, Theorem 21.2]) and  $J$  is an invertible left (right) ideal of its left (right) order. Let  $\mathcal{M}$  be a maximal order in  $Q$ . Then  $J$  is called a *two sided* ideal of  $\mathcal{M}$ , if  $O_r(J) = O_\ell(J) = \mathcal{M}$ . The two sided ideals of  $\mathcal{M}$  form an abelian group. The *normaliser* of  $\mathcal{M}$

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

acts on this group by left multiplication. This action has finitely many orbits, the number of which is called the two sided ideal class number  $H(\mathcal{M})$  of  $\mathcal{M}$ .

*Remark 3.3.* Any normal lattice  $J_{\mathfrak{p}}$  in the completion  $Q_{\mathfrak{p}} = Q \otimes_K K_{\mathfrak{p}}$  is free as a right  $O_r(J_{\mathfrak{p}})$ -module and thus of the form  $\alpha O_r(J_{\mathfrak{p}})$  for some  $\alpha \in Q_{\mathfrak{p}}^*$ . The map

$$\begin{aligned} J_{\mathfrak{p}} &\rightarrow J_{\mathfrak{p}} \\ \gamma &\mapsto \alpha \bar{\gamma} \bar{\alpha}^{-1} \end{aligned}$$

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

We call two normal lattices  $I, J$  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  $J$ .

**Proposition 3.4.** *Let  $I, J$  be normal lattices in  $Q$ .*

- (1) *If  $I$  and  $J$  are two sided equivalent, then  $O_r(I)$  and  $O_r(J)$  are conjugate.*
- (2) *Suppose  $O_r(I) = O_r(J)$ . Then  $I$  and  $J$  are two sided equivalent if and only if there exists some  $\beta \in N(O_r(I))$  such that  $I\beta$  is left equivalent to  $J$ .*

*Proof.* Suppose  $I$  and  $J$  are two sided equivalent. Then there exist  $\alpha, \beta \in Q^*$  such that  $\alpha I\beta = J$ . Then  $O_r(J) = O_r(\alpha I\beta) = \beta^{-1} O_r(I)\beta$  is conjugate to  $O_r(I)$ . This shows the first assertion. Moreover, if  $O_r(I) = O_r(J)$ , then  $\beta \in N(O_r(I))$ . The converse of the second assertion is clear.  $\square$

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

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

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

$$\{C(J) \mid J \text{ a normal lattice in } Q\} \rightarrow \text{CL}^+(K), C(J) \mapsto [n(J)]$$

from the set of equivalence classes of normal lattices 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 lattice  $J$  in  $Q$  of type  $[\mathfrak{a}]$  if  $[n(J)] = [\mathfrak{a}]$ . This generalises the notion of stably free ideals, which are the normal lattices of type  $[\mathbb{Z}_K]$ , see [19, Section 35].

**Proposition 3.5.** *Let  $J$  be a  $\mathbb{Z}_K$ -lattice in  $Q$  and let  $\mathfrak{a}$  be a fractional ideal of  $\mathbb{Z}_K$ . Then  $J$  is a normal lattice in  $Q$  with  $n(J) = \mathfrak{a}$  if and only if  $(J, n)$  lies in  $\mathcal{G}_{\mathfrak{a}}(Q, n)$ .*

*Proof.* Suppose first that  $J$  is a normal lattice in  $Q$  with  $n(J) = \mathfrak{a}$ . Then the right order  $\mathcal{O}$  of  $J$  is maximal. As in the proof of Proposition 3.2 we pass to the completions and let  $\mathfrak{p}$  be a maximal ideal of  $\mathbb{Z}_K$ . As  $J$  is locally free (see Remark 3.3), there exists  $x_{\mathfrak{p}} \in Q_{\mathfrak{p}}^*$  such that  $x_{\mathfrak{p}}J_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}$ . Assume that  $(J_{\mathfrak{p}}, n)$  is not  $\mathfrak{a}_{\mathfrak{p}}$ -maximal. Then there exists  $y_{\mathfrak{p}} \in Q_{\mathfrak{p}} \setminus J_{\mathfrak{p}}$  such that  $n(J_{\mathfrak{p}} + y_{\mathfrak{p}}\mathbb{Z}_{K_{\mathfrak{p}}}) \subseteq \mathfrak{a}_{\mathfrak{p}}$ . But then  $n(\mathcal{O}_{\mathfrak{p}} + x_{\mathfrak{p}}^{-1}y_{\mathfrak{p}}\mathbb{Z}_{K_{\mathfrak{p}}}) \subseteq \mathbb{Z}_{K_{\mathfrak{p}}}$ . This contradicts Proposition 3.2. Suppose now that  $(J, n)$  is an  $\mathfrak{a}$ -maximal lattice in  $(Q, n)$ . Let  $\mathcal{M}$  be some maximal order in  $Q$ . For each maximal ideal  $\mathfrak{p}$  of  $\mathbb{Z}_K$  there exists some  $z_{\mathfrak{p}} \in Q_{\mathfrak{p}}^*$  such that  $n(z_{\mathfrak{p}})\mathbb{Z}_{K_{\mathfrak{p}}} = \mathfrak{a}_{\mathfrak{p}}^{-1}$ . Then  $(z_{\mathfrak{p}}J_{\mathfrak{p}}, n)$  is  $\mathbb{Z}_{K_{\mathfrak{p}}}$ -maximal and by Proposition 3.2 properly isometric to  $(\mathcal{M}_{\mathfrak{p}}, n)$ . So there exist  $\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}} \in Q_{\mathfrak{p}}^*$  with  $n(\alpha_{\mathfrak{p}}) = n(\beta_{\mathfrak{p}})$  such that  $\alpha_{\mathfrak{p}}\mathcal{M}_{\mathfrak{p}}\beta_{\mathfrak{p}}^{-1} = z_{\mathfrak{p}}J_{\mathfrak{p}}$ . Hence  $O_r(J_{\mathfrak{p}}) = O_r(z_{\mathfrak{p}}^{-1}\alpha_{\mathfrak{p}}\mathcal{M}_{\mathfrak{p}}\beta_{\mathfrak{p}}^{-1}) = \beta_{\mathfrak{p}}\mathcal{M}_{\mathfrak{p}}\beta_{\mathfrak{p}}^{-1}$  is maximal. Thus  $J$  is normal. As  $n(\mathcal{M}_{\mathfrak{p}}) = \mathbb{Z}_{K_{\mathfrak{p}}}$  we conclude that  $n(J_{\mathfrak{p}}) = \mathfrak{a}_{\mathfrak{p}}$  for all maximal ideals  $\mathfrak{p}$ , so  $n(J) = \mathfrak{a}$ .  $\square$

Let  $J$  be a normal lattice of type  $[\mathfrak{a}]$ . Then  $n(J) = a\mathfrak{a}$  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 lattice  $J$  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  $\{(\alpha, \beta) \in Q^* \times Q^* \mid n(\alpha)n(\beta^{-1}) \in \mathbb{Z}_K^*\}$ . Let

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

Clearly  $\mathfrak{N}(J)$  only depends on the left and right order of  $J$ .

**Lemma 3.6.** *Let  $J$  be a normal lattice and let  $\alpha, \beta \in Q^*$ . Then  $\alpha J\beta^{-1} = J$  if and only if  $(\alpha, \beta) \in \mathfrak{N}(J)$ .*

*Proof.* Suppose first that  $\alpha J\beta^{-1} = J$ . Then  $O_r(J) = O_r(\alpha J\beta^{-1}) = \beta O_r(J)\beta^{-1}$  and hence  $\beta \in N(O_r(J))$ . Similarly  $\alpha \in N(O_{\ell}(J))$ . Moreover  $n(J) = n(\alpha J\beta^{-1}) = n(\alpha)n(\beta^{-1})n(J)$  implies that  $n(\alpha)n(\beta^{-1}) \in \mathbb{Z}_K^*$ .

Suppose now  $(\alpha, \beta) \in \mathfrak{N}(J)$  and consider the ideal  $I := J^{-1}\alpha J\beta^{-1}$ . Then  $O_{\ell}(I) = O_{\ell}(J^{-1}) = O_r(J)$  and  $O_r(I) = O_r(J\beta^{-1}) = O_r(J)$  as  $\beta \in N(O_r(J))$ . Hence  $I$  is a two sided ideal of  $O_r(J)$ . As  $\alpha \in N(O_{\ell}(J))$  and  $O_{\ell}(J) = O_r(J^{-1})$ , we have  $n(I) = n(J^{-1})n(\alpha)n(J)n(\beta^{-1}) = \mathbb{Z}_K$ . For every maximal ideal  $\mathfrak{p}$  of  $\mathbb{Z}_K$  there exists a unique maximal two sided ideal of  $\mathcal{M}$  containing  $\mathfrak{p}\mathcal{M}$  and these freely generate the group of all two sided ideals of  $\mathcal{M}$ , see [19, Theorems 22.4 and 22.10]. So  $I$  being a two sided ideal of  $O_r(J)$  of norm  $\mathbb{Z}_K$  implies that  $I = O_r(J)$  and hence

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

For a normal lattice  $J$  we set

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

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

For each coset  $u \in \mathbb{Z}_{K, > 0}^*/U(J)$ , we choose an element  $\alpha_u \in Q$  such that  $n(\alpha_u) \in u$ .

**Proposition 3.7.** *Let  $J$  be a normal lattice in  $Q$  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*

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

Moreover,

$$\text{Aut}^+(\alpha_u J, n) = \alpha_u \text{Aut}^+(J, n) \alpha_u^{-1}$$

where

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

*Proof.* Let  $I \in C_{\mathfrak{a}}(J)$ . Then there are  $\alpha, \beta \in Q^*$  with  $n(\alpha)n(\beta^{-1}) \in \mathbb{Z}_K^*$  such that  $I = \alpha J\beta^{-1}$ . Let  $u := n(\alpha)n(\beta^{-1})U(J) \in \mathbb{Z}_{K, > 0}^*/U(J)$ . By definition there are  $\alpha' \in N(O_{\ell}(J)), \beta' \in N(O_r(J))$  such that  $n(\alpha_u)n(\alpha')n(\beta'^{-1}) = n(\alpha)n(\beta^{-1})$ . As  $n(\alpha_u)$  and  $n(\alpha)n(\beta^{-1})$  lie in  $\mathbb{Z}_K^*$  we also have  $n(\alpha')n(\beta'^{-1}) \in \mathbb{Z}_K^*$ . So  $(\alpha', \beta') \in \mathfrak{N}(J)$  and thus  $\alpha'J\beta'^{-1} = J$  by Lemma 3.6. Moreover  $n(\alpha_u\alpha'\alpha^{-1}) = n(\beta\beta'^{-1})$ , hence

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

It remains to show that two different elements in  $\text{Lat}(J)$  do not represent the same proper isometry class. To this end let  $(\alpha_u J, n)$  and  $(\alpha_v J, n)$  be properly isometric elements of  $\text{Lat}(J)$ . Then there are  $\alpha, \beta \in Q^*$  such that  $n(\alpha)n(\beta^{-1}) = 1$  and  $\alpha\alpha_u J\beta^{-1} = \alpha_v J$ . Then  $(\alpha_v^{-1}\alpha\alpha_u)J\beta^{-1} = J$ . Lemma 3.6 shows that  $\alpha_v^{-1}\alpha\alpha_u \in N(O_{\ell}(J))$  and  $\beta \in N(O_r(J))$ . Moreover,  $n(\alpha_v^{-1})n(\alpha_u) = n(\alpha_v^{-1}\alpha\alpha_u)n(\beta^{-1}) \in U(J)$ . So  $u = v$ .  $\square$

#### 4. QUATERNARY LATTICES

In this section we summarise the results of the previous section in the context of a totally positive definite quadratic space  $(V, q)$  of dimension 4 over some totally real number field  $K$ . 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 [16] 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 of  $\mathbb{Z}_K$  and choose  $\mathfrak{a}$ -normalised lattices  $J_1, \dots, J_k$  in  $Q$  such that the disjoint union

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

is the set of all  $\mathfrak{a}$ -normalised normal lattices in  $Q$ . The easiest way to see that  $k$  is finite is the combination of the following theorem and the finiteness of class numbers of genera.

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

*Proof.* Let  $(J, n) \in \mathcal{G}_{\mathfrak{a}}(Q, n)$ . Proposition 3.5 shows that  $J$  is an  $\mathfrak{a}$ -normalised normal lattice in  $Q$ . The choice of  $J_1, \dots, J_k$  implies that there exists a unique index  $1 \leq i \leq k$  such that  $J \in C_{\mathfrak{a}}(J_i)$ . Proposition 3.7 shows that  $(J, n)$  is properly isometric to one and only one lattice in  $\text{Lat}(J_i)$ .  $\square$

#### 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  $Q$ . The unit group index  $[\mathcal{M}^* : \mathbb{Z}_K^*]$  is finite, see for example [27, Théorème V.1.2]. Let

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

be a system of representatives of the left equivalence classes of right ideals of  $\mathcal{M}$ . The number of these classes is finite and does not depend on the maximal order  $\mathcal{M}$ . Hence  $h$  is called the *class number* of  $Q$  and it is always bigger or equal to the *type number*  $t$  of  $Q$ , the number of conjugacy classes of maximal orders in  $Q$ , see for example [27, Théorème III.5.4] and the accompanying discussion. 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 [5]).

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

where  $h_K$  is the class number of  $K$ .

Let  $h_K^+ := |\text{CL}^+(K)|$  be the narrow class number of  $K$  and fix some narrow class  $[\mathfrak{a}] \in \text{CL}^+(K)$ . Then we define

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

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.**  $\text{Mass}(\mathcal{M}) = h_K^+ \cdot \text{Mass}(\mathcal{M}, [\mathfrak{a}])$ .

*Proof.* There exists some maximal order  $\mathcal{M}'$  in  $Q$  such that  $\mathcal{I}(\mathcal{M}, [\mathfrak{a}]) = \mathcal{I}(\mathcal{M}', [\mathbb{Z}_K])$ . The discussion after [26, Théorème 1] shows that  $\text{Mass}(\mathcal{M}, [\mathfrak{a}]) = \text{Mass}(\mathcal{M}', [\mathbb{Z}_K])$  does not depend on the maximal order  $\mathcal{M}'$ . Hence  $\text{Mass}(\mathcal{M}, [\mathfrak{a}]) = \text{Mass}(\mathcal{M}, [\mathfrak{b}])$  for all fractional ideals  $\mathfrak{b}$  of  $\mathbb{Z}_K$  and therefore

$$\text{Mass}(\mathcal{M}) = \sum_{[\mathfrak{b}] \in \text{CL}^+(K)} \text{Mass}(\mathcal{M}, [\mathfrak{b}]) = h_K^+ \cdot \text{Mass}(\mathcal{M}, [\mathfrak{a}]). \quad \square$$

## 6. THE MINKOWSKI-SIEGEL MASS FORMULA

In the spirit of our paper relating normal ideals in the quaternion algebra  $Q$  to maximal lattices in  $(Q, n)$  this section compares Eichler's mass formula for ideals to the well known Minkowski-Siegel mass formula for lattices. Whereas Eichler's formula involves the class number  $h_K$  of  $K$ , the Minkowski-Siegel formula does not. Our comparison below explains how the class number cancels out.

The quotient of the narrow class number and the class number is

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

Let  $\mathcal{P}(\mathbb{Z}_K) \cong K^* / \mathbb{Z}_K^*$  be the group of fractional principal ideals.

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

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

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

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

and

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

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 [5, p. 137], the order of the two sided ideal class group of  $\mathcal{M}_i$  is

$$H(\mathcal{M}_i) = 2^{s-f_i} h_K.$$

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

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

Let

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

where  $\mathfrak{N}(\mathcal{M}_i \mathcal{M}_j)$  is given by eq. (1) and define

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

Then the image of  $\overline{n_{ij}}$  is exactly  $\Pi_i \cap \Pi_j$  and the kernel of  $\overline{n_{ij}}$  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

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

and its kernel  $V_{ij} := \text{Ker}(\widetilde{n_{ij}})$ .

Let  $\mathcal{M}_i^{(1)} = \{\alpha \in \mathcal{M}_i^* \mid n(\alpha) = 1\}$  be the norm one subgroup of  $\mathcal{M}_i^*$ . Since  $Q$  is totally definite, the group  $\mathcal{M}_i^{(1)}$  is finite. Let  $2^{y_{ij}}$  be the index of  $\mathcal{M}_i^{(1)}/\{\pm 1\} \times \mathcal{M}_j^{(1)}/\{\pm 1\}$  in  $V_{ij}$ .

*Remark 6.1.* Let  $J$  be a normal lattice in  $Q$  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 3.7 satisfies

$$U(J)/(\mathbb{Z}_K^*)^2 = \widetilde{n_{ij}}(U_{ij}).$$

In particular

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

All the groups defined above 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  $N_i \times N_j$ .

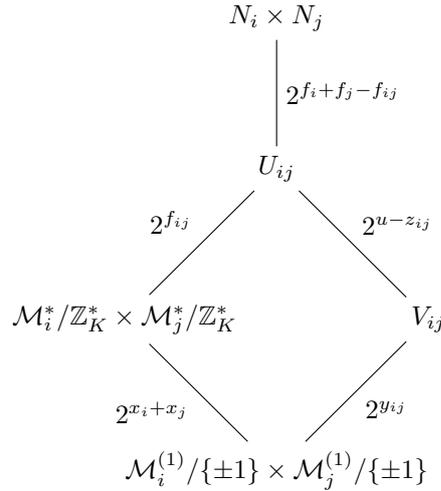


FIGURE 1. Some subgroups of  $N_i \times N_j$  and their indices.

**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 3.7 every proper automorphism of  $(J, n)$  is of the form  $x \mapsto \alpha x \beta^{-1}$  with  $\alpha \in N(\mathcal{M}_i)$ ,  $\beta \in N(\mathcal{M}_j)$  and  $n(\alpha) = n(\beta)$ . This induces an epimorphism  $\text{Aut}^+(J, n) \rightarrow V_{i,j}$  with kernel  $\{\pm \text{id}_J\}$ .  $\square$

**Lemma 6.3.** *The number of two sided equivalence classes represented by normal lattices 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 3.6 shows that the stabiliser of any ideal in  $\mathcal{S}$  is  $U_{ij}$ . 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 lattices 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  $\mathcal{G}_\mathfrak{a}(Q, n)$ . Then the mass of this genus of  $\mathfrak{a}$ -maximal lattices is defined as

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

Already Siegel gave an analytic expression for the mass of a genus of arbitrary positive definite  $\mathbb{Z}_K$ -lattices (see [24] and [25]). 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  $K$*

$$\text{Mass}(\mathcal{G}_\mathfrak{a}(Q, n)) = 2^{1-2[K:\mathbb{Q}]} \zeta_K(-1)^2 \prod_{i=1}^s \frac{(|\mathbb{Z}_K/\mathfrak{p}_i| - 1)^2}{2}.$$

*Proof.* Clearly the map  $(L, n) \mapsto (L, an)$  is an isometry preserving bijection between  $\mathcal{G}_\mathfrak{a}$  and  $\mathcal{G}_{a\mathfrak{a}}$  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 3.7 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 [6] the mass of  $\mathcal{G}_{\mathfrak{a}_i}(Q, n)$  does not depend on  $i$ , (as locally the lattices are just rescaled versions of each other) so for all  $i$

$$\text{Mass}(\mathcal{G}_{\mathfrak{a}_i}(Q, n)) = \text{Mass}(\mathcal{M})^2 h_K^{-2} 2^{-1-s}$$

and the theorem follows from the computation of  $\text{Mass}(\mathcal{M})$  in Theorem 5.1.  $\square$

## 7. PROPER ISOMETRY CLASSES IN $\mathcal{G}_\mathfrak{a}(Q, n)$

This section uses the method from [10] to develop an algorithm for determining a system of representatives of the proper isometry classes in  $\mathcal{G}_\mathfrak{a}(Q, n)$ . As explained in Remark 7.3 below, this yields a much faster algorithm to enumerate this genus than the usual neighboring algorithm.

**Algorithm 7.1.** *Given a totally definite quaternion algebra  $Q$  over  $K$  and a fractional ideal  $\mathfrak{a}$  of  $\mathbb{Z}_K$ , the following algorithm returns a system of representatives of the proper isometry classes in  $\mathcal{G}_{\mathfrak{a}}(Q, n)$ .*

- (1) *Compute a maximal order  $\mathcal{M}$  in  $Q$  using Zassenhaus' Round 2 algorithm [30] or Voight's specialised algorithm [29, Algorithm 7.10].*
- (2) *Using [10, Algorithm 7.10] compute:*
  - (a) *A system of representatives  $(\mathcal{M}_1, \dots, \mathcal{M}_t)$  of the conjugacy classes of maximal orders in  $Q$ .*
  - (b) *A system of representatives  $(I_1, \dots, I_h)$  of all invertible right ideals of  $\mathcal{M}$  up to left equivalence.*
- (3) *For  $1 \leq i \leq t$  set  $S_i := \{I_j \mathcal{M}_i \mid 1 \leq j \leq h \text{ and } [n(I_j \mathcal{M}_i)] = [\mathfrak{a}]\}$ .*
- (4) *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.*
- (5) *For  $J \in \bigcup_i T_i$  fix some totally positive generator  $a_J$  of  $n(J)^{-1}\mathfrak{a}$  and compute some  $x_J \in Q^*$  such that  $n(x_J) = a_J$ .*
- (6) *For  $u \in \mathbb{Z}_{K, >0}^*/(\mathbb{Z}_K^*)^2$  compute some  $\alpha_u \in Q^*$  such that  $n(\alpha_u) \in u$ .*
- (7) *Return  $\{(\alpha_u x_J J, n) \mid J \in \bigcup_i T_i \text{ and } u \in \mathbb{Z}_{K, >0}^*/U(J)\}$ .*

*Proof.* We only need to show that the output of the algorithm is correct. The set  $\{I_i \mathcal{M}_j \mid 1 \leq i \leq h\}$  is a system of representatives of the left equivalence classes of all invertible right ideals of  $\mathcal{M}_j$ . Thus Proposition 3.4 shows that  $\bigcup_i T_i$  is a system of representatives of the two sided equivalence classes of all normal lattices in  $(V, q)$  of type  $[\mathfrak{a}]$ . For any lattice  $J \in T_i$ , the class  $[n(J)^{-1}\mathfrak{a}]$  is trivial. Hence the scalar  $a_J$  exists. The existence of the elements  $x_J$  and  $\alpha_u$  follows from the Theorem of Hasse-Schilling-Maass. Then  $x_J J$  is  $\mathfrak{a}$ -normalised. Proposition 3.7 shows that the proper isometry classes of lattices  $(I, n)$  with  $I \in C_{\mathfrak{a}}(x_J J)$  is given by

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

Hence the set computed in (7) is a system of representatives of the proper isometry classes of all  $\mathfrak{a}$ -maximal lattices in  $(Q, n)$ .  $\square$

*Remark 7.2.* We give some remarks concerning the last three steps in the previous algorithm.

- (1) Let  $J, J' \in T_i$ . Proposition 3.7 shows that  $U(J) = U(J')$  whenever the left orders of  $J$  and  $J'$  are conjugate. This can be used to speed up the last step of the algorithm.
- (2) The norms of the ideals  $J \in \bigcup_i T_i$  will only be supported by very few prime ideals. So for the computation of  $x_J$  and  $\alpha_u$  in steps (5) and (6) one only has to solve very few norm equations of the form

$$n(x) = a \quad \text{with } a \in K_{>0}.$$

The Theorem of Hasse-Schilling-Maass (or the Hasse principle for quadratic forms) shows that any such norm equation has a solution  $x \in Q^*$  and it gives rise to the isotropic vector  $(1, x)$  of the quintic quadratic space  $\langle -a \rangle \perp (Q, n)$ . This is how it such a solution  $x \in Q^*$  can be found.

- (3) Note that left multiplication with  $(\alpha_u x_J)^{-1}$  gives an isometry between  $(\alpha_u x_J J, n)$  and  $(J, u_0 a_J n)$  where  $u_0 = n(\alpha_u)$ . So for most applications, it is not necessary to compute the elements  $x_J$  and  $\alpha_u$  in steps (5) and (6).

*Remark 7.3.* The computation of a system of representatives of the proper isometry classes in  $\mathcal{G}_{\mathfrak{a}}(Q, n)$  using Algorithm 7.1 is much faster than using Kneser's neighbour method [20] directly. There are mainly two reasons for this.

- (1) Let  $s$  be the number of finite places of  $K$  which ramify in  $Q$  and suppose that  $K$  has narrow class number 1. Section 4 of [5] shows that  $H(\mathcal{M}_i) \leq 2^s$  and  $t \leq h = \sum_{i=1}^t H(\mathcal{M}_i) \leq 2^s t$ . Moreover,  $|N(\mathcal{M}_i)/\mathcal{M}_i^* K^*| \leq 2^s$ . By Algorithm 7.1 the number of proper isometry classes in  $\mathcal{G}_{\mathfrak{a}}(Q, n)$  is at least  $ht/2^s \geq h^2/2^{2s}$ . So using Kneser's method directly requires to enumerate way more lattices than the enumeration of the  $h$  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 [8, 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 show that a certain  $\mathbb{Z}$ -lattice has minimum  $\leq [K : \mathbb{Q}] = \text{Tr}(1)$ , see [10, Algorithm 6.3]. The test for a lattice minimum is much faster than the computation of an isometry.

*Example 7.4.* 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 represented by

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

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 [10] that is implemented in Magma [1] 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

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

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  $[n(\mathcal{M}_i\mathcal{M}_j)] = [n(\mathcal{M}_i\mathcal{M}_i)] \cdot [n(\mathcal{M}_1\mathcal{M}_j)]$  can be computed from the information above. Using the information on  $z_{ij}$  given before, Proposition 3.7 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  $n(\mathcal{M}_i\mathcal{M}_j)$  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

For the four genera considered above, the trace lattices lie in the genera of even 15-modular (+ type) (see [21] 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 positive definite 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  $\{i, j\} = \{6, 8\}$ .

*Example 7.5.* Let  $K = \mathbb{Q}(\zeta_{19} + \zeta_{19}^{-1})$  be the totally real subfield of the cyclotomic field  $\mathbb{Q}(\zeta_{19})$ . Then there exists a unique prime ideal  $\mathfrak{p}$  of  $\mathbb{Z}_K$  over 19 and the narrow class group  $\text{CL}^+(K)$  is trivial. Let  $Q = \left(\frac{-1, -19}{K}\right)$  be the quaternion algebra over  $K$  ramified only at the infinite places and at  $\mathfrak{p}$ . We implemented Algorithm 7.1 in Magma and applied it to compute the maximal integral  $\mathbb{Z}_K$ -lattices in  $(Q, n)$ . The timings below were done on an Intel Core i7 7700K.

The computation of a maximal order in  $Q$  took less than a second. For the second step, [10, Algorithm 7.10] took about 9 minutes. It turns out that there are  $t = 185$  conjugacy classes of maximal orders in  $Q$ . Each of them has  $h = 356$  left equivalence classes of right ideals. The computation of the products in step (3) took 12 minutes and it took another 50 minutes to enumerate the orbit representatives in step (4). It turns out that  $\bigcup_i T_i$  consists of 63466 lattices. Since  $\mathbb{Z}_{K, > 0}^* = (\mathbb{Z}_K^*)^2$ , we can always choose  $u = 1$  in the last step of the algorithm. So there are 63466 proper isometry classes of maximal integral  $\mathbb{Z}_K$ -lattices in  $(Q, n)$ . The complete enumeration only took 71 minutes. Enumerating such a large genus with Kneser's neighbour method would take several days.

## REFERENCES

- [1] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997.
- [2] J. Brzezinski. Arithmetical quadratic surfaces of genus 0, I. *Math. Scand.*, 46:183–208, 1980.
- [3] J. Brzezinski. A characterization of Gorenstein orders in quaternion algebras. *Math. Scand.*, 50:19–24, 1982.
- [4] J. Dieudonné. *Linear algebra and geometry*. Hermann, 1969.
- [5] 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.
- [6] W. T. Gan, J. Hanke, and J.-K. Yu. On an exact mass formula of Shimura. *Duke Mathematical Journal*, 107, 2001.
- [7] H. Hasse. Äquivalenz quadratischer Formen in einem beliebigen Zahlkörper. *J. reine u. angew. Mathematik*, 153:158–162, 1924.
- [8] M. Kirschmer. *Definite quadratic and hermitian form with small class number*. Habilitation, RWTH Aachen University, 2016.
- [9] M. Kirschmer and G. Nebe. Binary hermitian lattices over number fields. In preparation.
- [10] 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>.
- [11] M. Kneser. *Quadratische Formen*. Springer-Verlag, Berlin, 2002. Revised and edited in collaboration with Rudolf Scharlau.
- [12] G. Nebe. Finite quaternionic matrix groups. *Represent. Theory*, 2:106–223, 1998.
- [13] O. T. O'Meara. *Introduction to Quadratic Forms*. Springer, 1973.
- [14] M. Peters. Ternäre und quaternäre quadratische Formen und Quaternionenalgebren. *Acta Arith.*, 15:329–365, 1968/1969.
- [15] P. Ponomarev. Class numbers of definite quaternary forms with square discriminant. *J. Number Theory*, 6:291–317, 1974.
- [16] P. Ponomarev. Arithmetic of quaternary quadratic forms. *Acta Arith.*, 29(1):1–48, 1976.
- [17] P. Ponomarev. A correspondence between quaternary quadratic forms. *Nagoya Math. J.*, 62:125–140, 1976.
- [18] P. Ponomarev. Class number formulas for quaternary quadratic forms. *Acta Arith.*, 39(1):95–104, 1981.
- [19] I. Reiner. *Maximal Orders*. Oxford Science Publications, 2003.
- [20] R. Scharlau and B. Hemkemeier. Classification of integral lattices with large class number. *Math. Comp.*, 67(222):737–749, 1998.
- [21] R. Scharlau and R. Schulze-Pillot. Extremal lattices. In *Algorithmic algebra and number theory (Heidelberg, 1997)*, pages 139–170. Springer, Berlin, 1999.
- [22] W. Scharlau. *Quadratic and Hermitian forms*, volume 270 of *Grundlehren der mathematischen Wissenschaften*. Springer, 1985.
- [23] A. Schiemann. Classification of Hermitian Forms with the Neighbor Method. *J. Symbolic Computation*, 26:487–508, 1998.
- [24] C. L. Siegel. Über die Analytische Theorie der quadratischen Formen. *Annals of Mathematics*, 36(3):527–606, 1935.
- [25] C. L. Siegel. Über die Analytische Theorie der quadratischen Formen III. *Annals of Mathematics*, 38(1):212–291, 1937.
- [26] M.-F. Vignéras. Simplification pour les ordres des corps de quaternions totalement définis. *J. Reine Angew. Math.*, 286/287:257–277, 1976.

- [27] M.-F. Vignéras. *Arithmétique des Algèbres de Quaternions*, volume 800 of *Lecture Notes in Mathematics*. Springer-Verlag, 1980.
- [28] J. Voight. Characterizing quaternion rings over an arbitrary base. *J. Reine Angew. Math.*, 657:113–134, 2011.
- [29] J. Voight. Identifying the matrix ring: Algorithms for quaternion algebras and quadratic forms. In K. Al-ladi, M. Bhargava, D. Savitt, and P. H. Tiep, editors, *Quadratic and Higher Degree Forms*, volume 31 of *Developments in Mathematics*, pages 255–298. Springer New York, 2013.
- [30] H. Zassenhaus. On the second round of the maximal order program. In *Applications of number theory to numerical analysis (Proc. Sympos., Univ. Montréal, Montreal, Que., 1971)*, pages 389–431. Academic Press, New York, 1972.

*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