DETERMINANT GROUPS OF HERMITIAN LATTICES OVER LOCAL FIELDS

MARKUS KIRSCHMER

ABSTRACT. We describe the determinants of the automorphism groups of hermitian lattices over local fields. Using a result of G. Shimura, this yields an explicit method to compute the special genera in a given genus of hermitian lattices over a number field.

1. INTRODUCTION

An important method to study global fields such as algebraic number fields is to pass to the completions, which are local fields. In case of a number field, the possible completions are the fields of real or complex numbers as well as the p-adic number fields. For such fields many problems are much easier to solve. The famous local-global principle relates properties of global fields to the respective properties of all its completions.

A classical result known as the Hasse principle shows that quadratic or hermitian spaces over a global field K are isometric if and only if they are isometric over all completions of K. The Hasse principle fails to hold for the analogous arithmetic question, i.e. isometry of lattices over number rings. This motivates the definition of the genus of a quadratic or hermitian lattice L as the set of all lattices which are isometric to L locally everywhere. A genus always decomposes into finitely many isometry classes and it is an important algorithmic task to make this decomposition explicit.

To that end, one considers an equivalence relation which is finer than being in the same genus but coarser than being isometric. For quadratic lattices, these intermediate equivalence classes are called spinor genera. The analogue for hermitian lattices were dubbed special genera in [9]. For lattices in indefinite spaces, strong approximation implies that the spinor or special genera consist of a single isometry class. In the case of definite spaces, the decomposition of spinor or special genera into isometry classes can be achieved by computing iterated neighbours as defined by Kneser, cf. Remark 4.8.

So it remains to give a description of the spinor or special genera in a given genus. M. Kneser [6] answered this question for quadratic lattices. His result depends on the local spinor norm groups of these lattices, which he computed at all non-dyadic places. C. N. Beli [1] worked out the local spinor norms at the dyadic places, which makes Kneser's answer explicit.

For hermitian lattices, the question was answered by G. Shimura in [10]. For a lattice L of odd rank, his result only depends of the class group of the underlying

---

number field. If L has even rank however, the answer also depends on the determinants of the local automorphism groups of L and he worked out those groups at all but the ramified dyadic places.

Theorem 3.7, which is the main result of this note, gives these local determinant groups at all places. With Shimura's result and the local determinant groups at hand, Section 4 gives an algorithm to compute representative lattices for the special genera in any given genus of hermitian lattices.

2. Hermitian spaces

In this section, we collect some basic results and definitions on lattices in hermitian spaces. Let $\mathfrak{o}$ be a Dedekind ring with field of fractions K such that the characteristic of K is different from 2. Further, let $E = K[X]/(X^2 - a)$ be an étale K-algebra of dimension 2 and let $^-\colon E \to E$ be the K-linear automorphism of E with fixed field K. We denote by

$$\mathrm{Nr}\colon E \to K, \alpha \mapsto \alpha\overline{\alpha} \quad \text{and} \quad \mathrm{Tr}\colon E \to K, \alpha \mapsto \alpha + \overline{\alpha}$$

the norm and the trace of the K-algebra E. Let

$$\mathcal{O} = \{\alpha \in E \mid \mathrm{Tr}(\alpha) \in \mathfrak{o} \text{ and } \mathrm{Nr}(\alpha) \in \mathfrak{o}\}$$

be the integral closure of $\mathfrak{o}$ in E and denote by

$$\mathfrak{D}^{-1} = \{\alpha \in E \mid \mathrm{Tr}(\alpha\mathcal{O}) \subseteq \mathfrak{o}\}$$

the inverse different of $\mathcal{O}$ over $\mathfrak{o}$.

Let (V, Φ) be a hermitian space over E, i.e. a finitely generated free E-module V and a map $\Phi\colon V \times V \to E$ such that for all $v, v', w, w' \in V$ and $\alpha, \beta \in E$ the following conditions hold:

$$\Phi(\alpha v + \beta v', w) = \alpha\Phi(v, w) + \beta\Phi(v', w),$$
$$\Phi(v, \alpha w + \beta w') = \overline{\alpha}\Phi(v, w) + \overline{\beta}\Phi(v, w'),$$
$$\Phi(w, v) = \overline{\Phi(v, w)}.$$

The unitary and special unitary groups of (V, Φ) are

$$\mathrm{U}(V, \Phi) = \{\varphi \in \mathrm{GL}(V) \mid \Phi(\varphi(x), \varphi(y)) = \Phi(x, y) \text{ for all } x, y \in V\} \text{ and}$$
$$\mathrm{SU}(V, \Phi) = \mathrm{U}(V, \Phi) \cap \mathrm{SL}(V)$$

Given a basis $(x_1, \ldots, x_m)$ of (V, Φ) over E, let $(\Phi(x_i, x_j))_{i,j} \in E^{m \times m}$ be the associated Gram matrix and

$$\det(V, \Phi) = \det(\Phi(x_i, x_j))_{i,j} \in K^*/\mathrm{Nr}(E^*)$$

be the determinant of (V, Φ). It does not depend on the chosen basis.

An $\mathcal{O}$-lattice L in V is a finitely generated $\mathcal{O}$-submodule in V that contains a K-basis of V. The fractional $\mathcal{O}$-ideals

$$\mathrm{s}(L) = \{\Phi(x, y) \mid x, y \in L\} \quad \text{and} \quad \mathrm{n}(L) = \sum_{x \in L} \Phi(x, x)\mathcal{O}$$

are called the scale and the norm of L respectively. For $x, y \in L$ we have

$$\mathrm{Tr}(\Phi(x, y)) = \Phi(x + y, x + y) - \Phi(x, x) - \Phi(y, y) \in \mathrm{n}(L)$$

and thus $\Phi(x, y) \in \mathfrak{D}^{-1} \cdot \mathrm{n}(L)$. This shows that

$$(2.1) \qquad\qquad \mathrm{s}(L) \subseteq \mathfrak{D}^{-1} \cdot \mathrm{n}(L) \subseteq \mathfrak{D}^{-1} \cdot \mathrm{s}(L).$$

Definition 2.1. *Let L be an $\mathcal{O}$-lattice in V.*

(1) *The lattice L is called maximal if $\mathrm{n}(L) \subsetneq \mathrm{n}(M)$ for any $\mathcal{O}$-lattice $L \subsetneq M$.*
(2) *The dual of L is the $\mathcal{O}$-lattice $L^{\#} = \{x \in V \mid \Phi(x, L) \subseteq \mathcal{O}\}$.*
(3) *If $L = \mathfrak{A}L^{\#}$ for some fractional ideal $\mathfrak{A}$ of $\mathcal{O}$ with $\mathfrak{A} = \overline{\mathfrak{A}}$ then L is called $\mathfrak{A}$-modular (or simply modular).*

Definition 2.2. *The unitary group $\mathrm{U}(V, \Phi)$ acts on the set of all $\mathcal{O}$-lattices in V. Two $\mathcal{O}$-lattices L and L' in V are said to be isometric, denoted by $L \cong L'$, if they lie in the same orbit under $\mathrm{U}(V, \Phi)$. The automorphism group $\mathrm{Aut}(L)$ is the stabilizer of L in $\mathrm{U}(V, \Phi)$.*

3. Hermitian lattices over local rings

Let $K, E, \mathfrak{o}, \mathcal{O}$ and (V, Φ) be as in Section 2. We now assume $\mathfrak{o}$ to be the valuation ring of a complete discrete surjective valuation $\mathrm{ord} \colon K \to \mathbb{Z} \cup \{\infty\}$. The maximal ideal of $\mathfrak{o}$ will be denoted by $\mathfrak{p}$. The purpose of this section is to describe the determinants of the automorphisms of $\mathcal{O}$-lattices in V.

If $E \cong K \oplus K$ is split, let $\mathfrak{P} = \mathfrak{p}\mathcal{O}$ otherwise let $\mathfrak{P}$ be the maximal ideal of $\mathcal{O}$. In both cases, $\mathfrak{P}$ is the largest proper ideal of $\mathcal{O}$ over $\mathfrak{p}$ that is invariant under $^{-}$. Hence $\mathfrak{D} = \mathfrak{P}^{e}$ for some integer $e \geq 0$.

If E/K is a ramified field extension, we need to distinguish two cases:

(1) $E \cong K[X]/(X^2 - p)$ for some prime element $p \in \mathfrak{o}$. Then $\mathcal{O}$ contains a prime element π such that $\overline{\pi} = -\pi$. In this case $\mathcal{O} = \mathfrak{o} \oplus \pi\mathfrak{o}$ and $\mathfrak{D} = 2\mathfrak{P}$. In particular, $e = 2\,\mathrm{ord}(2) + 1$ is odd.
(2) $E \cong K[X]/(X^2 - u)$ for some unit $u \in \mathfrak{o}^*$. Section 63A of [7] shows that one may assume that $\mathrm{ord}(u - 1) = 2k + 1$ for some integer $1 \leq k \leq \mathrm{ord}(2)$. Then $\mathcal{O} = \mathfrak{o} \oplus \alpha\mathfrak{o}$ for some element $\alpha \in \mathcal{O}$ such that $\alpha^2 = u$. Let $p \in \mathfrak{o}$ be a prime element. Then $\pi = p^{-k}(1 + \alpha)$ is a prime element of $\mathcal{O}$ and $\mathfrak{D} = 2\mathfrak{P}^{-2k}$. In particular, $e = 2\,\mathrm{ord}(2) - 2k$ is even.

Note that the second case can only occur if E/K is wildly ramified, i.e. E/K is ramified and $\mathrm{ord}(2) > 0$.

Lemma 3.1. *Suppose E/K is ramified. Then $\mathfrak{D} = \sum_{\gamma \in \mathcal{O}} (\gamma - \overline{\gamma})\mathcal{O} = (\pi - \overline{\pi})\mathcal{O}$ for any prime element $\pi \in \mathcal{O}$.*

Proof. Suppose first that π is the prime element form the discussion just before this lemma. One checks that $\pi - \overline{\pi}$ generates $\mathfrak{D}$ in both cases. The fact that $\mathcal{O} = \mathfrak{o} \oplus \pi\mathfrak{o}$ shows that any $\gamma \in \mathcal{O}$ is of the form $\gamma = a + b\pi$ with $a, b \in \mathfrak{o}$. Then

$$\gamma - \overline{\gamma} = (a + b\pi) - (a + b\overline{\pi}) = b(\pi - \overline{\pi}) \in \mathfrak{D} .$$

Suppose now γ is a prime element of $\mathcal{O}$. Then $\mathrm{ord}(a) > \mathrm{ord}(b) = 0$ and thus $(\gamma - \overline{\gamma})\mathcal{O} = (\pi - \overline{\pi})\mathcal{O} = \mathfrak{D}$. $\qquad\square$

The isometry classes of $\mathcal{O}$-lattices in V were described by R. Jacobowitz in [3], see also [4]. This classification is not needed for our purposes. We only make use of the following two results.

Proposition 3.2. *Any $\mathcal{O}$-lattice L in V has a decomposition $L = \perp_{i=1}^{r} L_i$ into modular sublattices L_i of rank 1 or 2.*

Proof. See for example [3, Proposition 4.3]. $\qquad\square$

If E/K is ramified, let $\pi \in \mathcal{O}$ be the prime element from above. For $i \in \mathbb{Z}$, we denote by $H(i)$ a binary hermitian lattice over $\mathcal{O}$ with Gram matrix

$$\begin{pmatrix} 0 & \pi^i \\ \overline{\pi}^i & 0 \end{pmatrix}.$$

For an integer $r \geq 0$ let $H(i)^r$ denote the orthogonal sum of r copies of $H(i)$.

Proposition 3.3. *Suppose E/K is ramified and let L be a $\mathfrak{P}^i$-modular hermitian $\mathcal{O}$-lattice of rank m. Then $\mathrm{n}(L) = \mathfrak{D}\,\mathrm{s}(L)$ if and only if m is even, $i \equiv e \pmod 2$ and $L \cong H(i)^{m/2}$.*

Proof. If K is non-dyadic see [3, Proposition 8.1]. Suppose K is dyadic and write $L = \perp_j L_j$ with $\mathfrak{P}^i$-modular lattices of rank at most 2. The assumption $\mathrm{n}(L) = \mathfrak{D}\,\mathrm{s}(L)$ implies that all L_j have rank 2 and satisfy $\mathrm{n}(L_j) = \mathfrak{D}\,\mathrm{s}(L_j)$. So its suffices to discuss the case $m = 2$, which is [4, Proposition 7.1]. $\qquad\square$

Given any $\mathcal{O}$-lattice L in V, set

$$(3.1) \qquad\qquad \rho(L) = L + \left(\mathfrak{P}^{-1}L \cap \mathfrak{P}L^{\#}\right).$$

Then ρ defines a map on the set of all $\mathcal{O}$-lattices in V. It generalizes the maps defined by L. Gerstein in [2] to hermitian spaces. They are similar in nature to the *p-mappings* introduced by G. Watson in [11].

Since isometries of L also preserve $L^{\#}$ and commute with sums and intersections, we have $\mathrm{Aut}(L) \subseteq \mathrm{Aut}(\rho(L))$. Moreover, if $\perp_{i=1}^r L_i$ is a decomposition of L into modular sublattices, then $\rho(L)$ has the decomposition

$$\overset{r}{\underset{i=1}{\perp}} L_i' \quad \text{where } L_i' = \begin{cases} L_i & \text{if } \mathfrak{P} \subseteq \mathrm{s}(L_i), \\ \mathfrak{P}^{-1}L_i & \text{otherwise.} \end{cases}$$

In particular, $\rho(H(i)) \cong H(i-2)$ for $i \geq 2$ and $\rho(H(i)) = H(i)$ for $i < 2$.

We consider the following subgroups of $\mathcal{O}^*$.

$$\mathcal{E}_0 = \mathcal{E}_0(\mathcal{O}) = \{u \in \mathcal{O}^* \mid u\overline{u} = 1\}$$
$$\mathcal{E}_1 = \mathcal{E}_1(\mathcal{O}) = \{u\overline{u}^{-1} \mid u \in \mathcal{O}^*\} \subseteq \mathcal{E}_0$$

Given any $\mathcal{O}$-lattice L in V let

$$\mathcal{E}(L) = \{\det(\varphi) \mid \varphi \in \mathrm{Aut}(L)\}$$

be its determinant group. It is a subgroup of $\mathcal{E}_0$.

Remark 3.4. Suppose E/K is ramified. Hilbert 90 shows that the homomorphism $E^* \to \mathcal{E}_0/\mathcal{E}_1, x \mapsto x\overline{x}^{-1}\mathcal{E}_1$ is onto. Its kernel is $K^*\mathcal{O}^*$ and therefore $[\mathcal{E}_0 : \mathcal{E}_1] = [E^* : K^*\mathcal{O}^*] = 2$.

For an anisotropic vector $v \in (V, \Phi)$ and a scalar $\delta \in E$ of norm 1, we define the corresponding quasi-reflection

$$\tau_{x,\delta} \colon V \to V, \; y \mapsto y + (\delta - 1)\frac{\Phi(y, x)}{\Phi(x, x)}x.$$

Note that $\tau_{x,\delta}(x) = \delta x$ and $\tau_{x,\delta}$ is the identity on $\{v \in V \mid \Phi(v, x) = 0\}$. Hence $\tau_{x,\delta} \in \mathrm{U}(V, \Phi)$ and $\det(\tau_{x,\delta}) = \delta$.

Finally, we set

$$e' = \max(0, e - 1) = \begin{cases} e - 1 & \text{if } E/K \text{ is ramified,} \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 3.5. *If $\delta \in \mathcal{E}_0$, then $\delta - 1 \in \mathfrak{P}^{e'}$. If E/K is ramified then*

$$\mathcal{E}_1 = \{\delta \in \mathcal{E}_0 \mid \delta - 1 \in \mathfrak{D}\} \, .$$

Proof. Only the case that E/K is ramified requires proof. By Hilbert 90, every element of $\mathcal{E}_0$ is of the form $\beta/\overline{\beta}$ for some $\beta \in E^*$ with $v(\beta) \in \{0, 1\}$. Suppose $\gamma \in \mathcal{O}^*$ and let π be any prime element of $\mathcal{O}$. Lemma 3.1 shows that

$$(\gamma/\overline{\gamma} - 1)\mathcal{O} = (\gamma - \overline{\gamma})\mathcal{O} \subseteq \mathfrak{D} \quad \text{and} \quad (\pi/\overline{\pi} - 1)\mathcal{O} = (\pi - \overline{\pi})\mathfrak{P}^{-1} = \mathfrak{D}\mathfrak{P}^{-1} \, .$$

The result follows. $\qquad\qquad\square$

Corollary 3.6. *Let L be an $\mathcal{O}$-lattice in V. Then $\mathcal{E}_1 \subseteq \mathcal{E}(L)$. If $\mathrm{s}(L)\mathfrak{P}^{e'} \subseteq \mathrm{n}(L)$ then $\mathcal{E}(L) = \mathcal{E}_0$.*

Proof. Let $x \in L$ be a norm generator, i.e. $\Phi(x,x)\mathcal{O} = \mathrm{n}(L)$. Suppose first that $\mathrm{s}(L)\mathfrak{P}^{e'} \subseteq \mathrm{n}(L)$ and let $\delta \in \mathcal{E}_0$. Lemma 3.5 asserts that $(\delta - 1)\frac{\Phi(y,x)}{\Phi(x,x)} \in \mathcal{O}$ for all $y \in L$. Hence $\tau_{x,\delta} \in \mathrm{Aut}(L)$ and therefore $\delta = \det(\tau_{x,\delta}) \in \mathcal{E}(L)$.
Suppose now that $\mathrm{s}(L)\mathfrak{P}^{e'} \not\subseteq \mathrm{n}(L)$. Then E/K is ramified. Let $\delta \in \mathcal{E}_1$. Lemma 3.5 and Eq. (2.1) show that $(\delta - 1)\frac{\Phi(y,x)}{\Phi(x,x)} \in \mathfrak{D}\,\mathrm{s}(L)\,\mathrm{n}(L)^{-1} \subseteq \mathcal{O}$ for all $y \in L$. Hence $\tau_{x,\delta} \in \mathrm{Aut}(L)$ and thus $\delta \in \mathcal{E}(L)$. $\qquad\qquad\square$

We are now ready to give our main result.

Theorem 3.7. *Let L be an $\mathcal{O}$-lattice in V and let $m = \mathrm{rank}_E(V)$. If E/K is ramified, m is even and $L \cong \perp_{i=1}^{m/2} H(s_i)$ with $e \equiv s_i \pmod 2$ for all $1 \leq i \leq m/2$, then $\mathcal{E}(L) = \mathcal{E}_1$. In all other cases, $\mathcal{E}(L) = \mathcal{E}_0$.*

Proof. We fix a decomposition $L = \perp_{i=1}^{r} L_i$ with modular sublattices L_i of rank 1 or 2 as in Proposition 3.2. Suppose first that $\mathcal{E}(L) \neq \mathcal{E}_0$. Then $\mathcal{E}(L_i) \neq \mathcal{E}_0$ for all i. Corollary 3.6 shows that this is only possible if E/K is ramified and $\mathfrak{D}\,\mathrm{s}(L_i) = \mathrm{n}(L_i)$. By Proposition 3.3 this implies that $L_i \cong H(s_i)$ for some integer s_i with $s_i \equiv e \pmod 2$.
Conversely assume that E/K is ramified, m is even and $L \cong \perp_{i=1}^{m/2} H(s_i)$ with $e \equiv s_i \pmod 2$ for all i. After rescaling L we may assume that $s_i \geq 0$ for all i. Let $j \in \{0,1\}$ such that $j \equiv e \pmod 2$. Repeated application of the map ρ from Eq. (3.1) yields some $\mathcal{O}$-lattice M in V such that $\mathrm{Aut}(L) \subseteq \mathrm{Aut}(M)$ and $M \cong H(j)^{m/2}$. By Corollary 3.6 it suffices to show that $\mathcal{E}(M) \subseteq \mathcal{E}_1$. There exists some element $\alpha \in E$ such that $\overline{\alpha} = -\alpha$ and $\mathrm{ord}_{\mathfrak{P}}(\alpha) = j$. Then $H(j) \cong \left(\begin{smallmatrix} 0 & \alpha \\ -\alpha & 0 \end{smallmatrix}\right)$ by Proposition 3.3. Lemma 3.1 shows that

$$M/\mathfrak{D}M \times M/\mathfrak{D}M \to \mathcal{O}/\mathfrak{D}, \ (x + \mathfrak{D}M, y + \mathfrak{D}M) \mapsto \alpha^{-1}\Phi(x,y) + \mathfrak{D}$$

is a well defined symplectic form over $\mathcal{O}/\mathfrak{D}\mathcal{O}$. Since automorphisms of such forms have determinant one, we conclude that $\det(\varphi) \equiv 1 \pmod{\mathfrak{D}}$ for all $\varphi \in \mathrm{Aut}(M)$. Hence $\mathcal{E}(M) \subseteq \mathcal{E}_1$ by Lemma 3.5. $\qquad\qquad\square$

In [10, Proposition 4.18] G. Shimura works out the group $\mathcal{E}(L)$ for maximal lattices L. We recover his result from Theorem 3.7.

Corollary 3.8 (Shimura)**.** *Let L be a maximal $\mathcal{O}$-lattice in a hermitian space (V, Φ) over E of rank m. Then $\mathcal{E}(L) = \mathcal{E}_1$ if and only if E/K is ramified, m is even and $\det(V, \Phi) = (-1)^{m/2}$. In all other cases $\mathcal{E}(L) = \mathcal{E}_0$.*

Proof. Theorem 3.7 shows that $\mathcal{E}(L) = \mathcal{E}_0$ whenever E/K is unramified or m is odd. Suppose now that E/K is ramified and m is even. Let $\mathrm{n}(L) = \mathfrak{P}^{2n}$. If $\det(V, \Phi) = (-1)^{m/2}$, then $L \cong \perp_{i=1}^{m/2} H(2n-e)$, see for example [10, Propositions 4.7 and 4.8]. So in this case, $\mathcal{E}(L) = \mathcal{E}_1$. Conversely, if $\det(V, \Phi) \neq (-1)^{m/2}$, then L can not be written in the form $L \cong \perp_{i=1}^{m/2} H(s_i)$ with integers s_i. So in this case $\mathcal{E}(L) = \mathcal{E}_0$. $\hfill\square$

4. SPECIAL GENERA OF HERMITIAN LATTICES OVER NUMBER FIELDS

In this section we assume that K and E are both algebraic number fields with ring of integers $\mathfrak{o}$ and $\mathcal{O}$ respectively.

Let $\mathfrak{p}$ be a maximal ideal of $\mathfrak{o}$. The completions of K and $\mathfrak{o}$ at $\mathfrak{p}$ will be denoted by $K_\mathfrak{p}$ and $\mathfrak{o}_\mathfrak{p}$. More generally, given a vector space V over K and an $\mathfrak{o}$-module L, then $V_\mathfrak{p} = V \otimes_K K_\mathfrak{p}$ and $L_\mathfrak{p} = L \otimes_\mathfrak{o} \mathfrak{o}_\mathfrak{p}$ denote the completions of V and L at $\mathfrak{p}$.

Let (V, Φ) be a hermitian space over E of rank at least 2 and let L be an $\mathcal{O}$-lattice in V. The space (V, Φ) is called definite, if K is totally real and there exists some $a \in K^*$ such that $a\Phi(x, x)$ is totally positive for every nonzero vector $x \in V$. Otherwise (V, Φ) is called indefinite.

By linearity, Φ extends to $V_\mathfrak{p}$. This yields a hermitian space $(V_\mathfrak{p}, \Phi)$ over the étale $K_\mathfrak{p}$-algebra $E_\mathfrak{p}$ which contains the $\mathcal{O}_\mathfrak{p}$-lattice $L_\mathfrak{p}$.

Definition 4.1. *Two lattices L and L' in V are said to be in the same genus if $L_\mathfrak{p} \cong L'_\mathfrak{p}$ for every maximal ideal $\mathfrak{p}$ of K. The lattices are said to be in the same special genus, if there exists an isometry $\sigma \in \mathrm{U}(V, \Phi)$ such that $L_\mathfrak{p} = \sigma(\varphi_\mathfrak{p}(L'_\mathfrak{p}))$ with $\varphi_\mathfrak{p} \in \mathrm{SU}(V, \Phi)$ for every maximal ideal $\mathfrak{p}$ of $\mathfrak{o}$. The genus and special genus of L will be denoted by $\mathrm{gen}(L)$ and $\mathrm{sgen}(L)$ respectively.*

It is well known that the genus of L is a union of finitely many special genera and each special genus decomposes into finitely many isometry classes. The special genera in $\mathrm{gen}(L)$ were described by G. Shimura [10] in terms of the local determinant groups $\mathcal{E}(L_\mathfrak{p})$. To state his result, some more notation is needed:

- $\mathcal{I}$ denotes the group of fractional ideals of $\mathcal{O}$.
- $J = \{\mathfrak{A} \in \mathcal{I} \mid \mathfrak{A}\overline{\mathfrak{A}} = \mathcal{O}\}$ and $J_0 = \{\alpha\mathcal{O} \mid \alpha \in E^* \text{ and } \mathrm{Nr}(\alpha) = 1\} \subseteq J$.
- $C = \mathcal{I}/\{\alpha\mathcal{O} \mid \alpha \in E^*\}$ denotes the class group of $\mathcal{O}$.
- $C_0 = \{[\mathfrak{A}] \in C \mid \overline{\mathfrak{A}} = \mathfrak{A}\}$ is the subgroup of C generated by the image of the class group of $\mathfrak{o}$ in C and

$$\{[\mathfrak{P}] \in C \mid \mathfrak{P} \in \mathcal{I} \text{ a prime ideal that ramifies over } K\}.$$

- $P(L)$ is the set of all prime ideals of $\mathfrak{o}$ such that $\mathcal{E}(L_\mathfrak{p}) \neq \mathcal{E}_0(\mathcal{O}_\mathfrak{p})$. The ideals in $P(L)$ are necessarily ramified in E, cf. Theorem 3.7.
- $\mathcal{E}(L) = \prod_{\mathfrak{p} \in P(L)} \mathcal{E}_0(\mathcal{O}_\mathfrak{p})/\mathcal{E}(L_\mathfrak{p})$.
- $H(L) = \{(e\mathcal{O}, (e\mathcal{E}(L_\mathfrak{p}))_{\mathfrak{p} \in P(L)}) \in J \times \mathcal{E}(L) \mid e \in E \text{ and } \mathrm{Nr}(e) = 1\}$.
- $R(L) = \{(e\mathcal{E}(L_\mathfrak{p}))_{\mathfrak{p} \in P(L)} \in \mathcal{E}(L) \mid e \in \mathcal{O} \text{ and } \mathrm{Nr}(e) = 1\}$.
- Given a maximal ideal $\mathfrak{P}$ of $\mathcal{O}$, define an element $c(\mathfrak{P}) \in \mathcal{E}(L)$ by

$$c(\mathfrak{P})_\mathfrak{p} = \begin{cases} -1 & \text{if } \mathfrak{p} = \mathfrak{P} \cap \mathcal{O}, \\ +1 & \text{otherwise} \end{cases}$$

  for all $\mathfrak{p} \in P(L)$.
- Given an $\mathcal{O}$-lattice M in V, let $[L : M]_\mathcal{O}$ be the fractional ideal of $\mathcal{O}$ generated by $\{\det(\varphi) \mid \varphi \in \mathrm{Hom}_\mathcal{O}(L, M)\}$.

Remark 4.2. The group homomorphism $\mathcal{I} \to J/J_0$, $\mathfrak{A} \mapsto \mathfrak{A}\overline{\mathfrak{A}}^{-1}$ is onto by Hilbert 90. Hence it induces an isomorphism $C/C_0 \cong J/J_0$.

Theorem 4.3 (Shimura). *Consider the map*

$$\Psi \colon \mathrm{gen}(L) \to J \times \mathcal{E}(L), \ M \mapsto ([L:M]_{\mathcal{O}}, (\det(\sigma_{\mathfrak{p}})\mathcal{E}(L_{\mathfrak{p}}))_{\mathfrak{p} \in P(L)})$$

where $\sigma_{\mathfrak{p}} \in \mathrm{U}(V_{\mathfrak{p}}, \Phi)$ such that $\sigma_{\mathfrak{p}}(L_{\mathfrak{p}}) = M_{\mathfrak{p}}$ for all $\mathfrak{p} \in P(L)$. Then Ψ induces a bijection between the special genera in $\mathrm{gen}(L)$ and $(J \times \mathcal{E}(L))/H(L)$.

Proof. See [10, Theorem 5.24 and its proof 5.28]. $\qquad\square$

The decomposition given in Theorem 4.3 can be made explicit using Kneser's concept of neighbours, see also [9].

Definition 4.4. *Let $\mathfrak{P}$ be a maximal ideal of $\mathcal{O}$ and let $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{o}$. Further L, L' be $\mathcal{O}$-lattices in V. We say that L' is a $\mathfrak{P}$-neighbour of L if $L_{\mathfrak{p}}$ and $L'_{\mathfrak{p}}$ are both modular with $\mathrm{s}(L_{\mathfrak{p}}) = \mathrm{s}(L'_{\mathfrak{p}})$ and there exist $\mathcal{O}$-module isomorphisms*

$$L/(L \cap L') \cong \mathcal{O}/\mathfrak{P} \quad and \quad L'/(L \cap L') \cong \mathcal{O}/\overline{\mathfrak{P}}.$$

Lemma 4.5. *Let $\mathfrak{P}$ be a maximal ideal of $\mathcal{O}$ and set $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{o}$. Suppose $L_{\mathfrak{p}}$ is modular and if $\mathfrak{p}$ is ramified in E, then $2 \notin \mathfrak{p}$. Further, let Ψ denote the bijection from Theorem 4.3.*

  (1) *If $(V_{\mathfrak{p}}, \Phi)$ is isotropic (which automatically holds if $\mathrm{rank}_E(V) \geq 3$ or $\mathfrak{p}$ is unramified in E), then there exists some $\mathfrak{P}$-neighbour of L.*
  (2) *If L' is a $\mathfrak{P}$-neighbour of L then $L' \in \mathrm{gen}(L)$ and $\Psi(L') = (\mathfrak{P}\overline{\mathfrak{P}}^{-1}, c(\mathfrak{P}))$.*

Proof. Part (1) follows from [9, Lemma 2.2] and [5, Proposition 5.2.4]. Suppose now L' is a $\mathfrak{P}$-neighbour of L. The definition of $\mathfrak{P}$-neighbours yields $[L:L']_{\mathcal{O}} = \mathfrak{P}\overline{\mathfrak{P}}^{-1}$. Further, $L' \in \mathrm{gen}(L)$ by [9, Lemma 2.8] and [5, Remark 5.2.2]. If $\mathfrak{q} \in P(L)$ is different from $\mathfrak{p}$, then $L_{\mathfrak{q}} = L'_{\mathfrak{q}}$. Suppose now $\mathfrak{p} \in P(L)$. Then $E_{\mathfrak{p}}/K_{\mathfrak{p}}$ is necessarily ramified and there exists some prime element $\pi \in \mathcal{O}_{\mathfrak{p}}$ such that $\overline{\pi} = -\pi$. By [9, Lemma 2.2] and [5, Proposition 5.2.4] there exists a decomposition $L_{\mathfrak{p}} = (x\mathcal{O}_{\mathfrak{p}} \oplus y\mathcal{O}) \perp M$ such that $\Phi(x,x) = \Phi(y,y) = 0$ and $L'_{\mathfrak{p}} = (x\mathfrak{P}^{-1} \oplus y\mathfrak{P}) \perp M$. Let $\sigma \in \mathrm{End}_{E_{\mathfrak{p}}}(V_{\mathfrak{p}})$ such that $\sigma(x) = -\pi^{-1}x$, $\sigma(y) = \pi y$ and $\sigma(z) = z$ for all $z \in M$. Then $\sigma \in \mathrm{U}(V_{\mathfrak{p}}, \Phi)$ is an isometry between $L_{\mathfrak{p}}$ and $L'_{\mathfrak{p}}$ with determinant -1. $\qquad\square$

The group J is infinite, which makes Theorem 4.3 difficult to use in practice. For algorithmic purposes, there is a more convenient description of $(J \times \mathcal{E}(L))/H(L)$. To this end, fix some fractional ideals $\mathfrak{A}_1 = \mathcal{O}, \mathfrak{A}_2, \ldots, \mathfrak{A}_r$ of $\mathcal{O}$ which represent the cosets in C/C_0. For $1 \leq i, j \leq r$ let $1 \leq k(i,j) \leq r$ be the unique index such that $\mathfrak{A}_i\mathfrak{A}_j\mathfrak{A}_{k(i,j)}^{-1} \in C_0$. Remark 4.2 shows that there exists some $\alpha_{i,j} \in E^*$ with $\mathrm{Nr}(\alpha_{i,j}) = 1$ such that

$$\alpha_{i,j}\mathfrak{A}_i\overline{\mathfrak{A}_i}^{-1}\mathfrak{A}_j\overline{\mathfrak{A}_j}^{-1} = \mathfrak{A}_{k(i,j)}\overline{\mathfrak{A}_{k(i,j)}}^{-1}.$$

Then $(\alpha_{i,j})$ defines a 2-cocycle $C/C_0 \times C/C_0 \to \mathcal{E}(L)/R(L)$. Let $G(L)$ be the corresponding central extension of $\mathcal{E}(L)/R(L)$ by C/C_0, i.e. $G(L)$ is the cartesian product $C/C_0 \times \mathcal{E}(L)/R(L)$ equipped with the multiplication

$$([\mathfrak{A}_i], x) * ([\mathfrak{A}_j], y) = ([\mathfrak{A}_{k(i,j)}], \alpha_{i,j}xy).$$

The example at the end of this section shows that $G(L)$ does not need to be a split extension of $\mathcal{E}(L)/R(L)$ by C/C_0.

Lemma 4.6 (Shimura). *The map*

$$\psi \colon (J \times \mathcal{E}(L))/H(L) \to G(L),$$

$$(\alpha \mathfrak{A}_i \overline{\mathfrak{A}_i}^{-1}, x) \cdot H(L) \mapsto ([\mathfrak{A}_i] \cdot C_0, \alpha^{-1} x \cdot R(L))$$

with $\alpha \in E^*$ an arbitrary element of norm 1, is an isomorphism of groups. In particular, the number of special genera in $\mathrm{gen}(L)$ equals

$$\#G(L) = [C : C_0] \cdot [\mathcal{E}(L) : R(L)] = [J : J_0] \cdot [\mathcal{E}(L) : R(L)].$$

Proof. The map is well-defined and bijective by [10, 5.28]. It is a group homomorphism by the choice of $G(L)$. $\qquad\square$

The group $G(L)$ and the isomorphism ψ from Lemma 4.6 yield the following method to decompose a genus into its special genera.

Algorithm 4.7.
Input: *An $\mathcal{O}$-lattice L in a hermitian space (V, Φ) over E.*
Output: *A set S of $\mathcal{O}$-lattices in V representing the special genera in $\mathrm{gen}(L)$.*
 1: *Compute the groups $\mathcal{E}(L)/R(L)$ and C/C_0.*
 2: **if** $[\mathcal{E}(L) : R(L)] = [C : C_0] = 1$ **then return** $\{L\}$ **end if**
 3: *Using Lemma 4.6, find prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_t$ of $\mathcal{O}$ such that*
    (1) $\{g_1, \ldots, g_t\}$ *generates $G(L)$ where $g_i = \psi((\mathfrak{P}_i \overline{\mathfrak{P}_i}^{-1}, c(\mathfrak{P}_i)) \cdot H(L))$.*
    (2) $(V_{\mathfrak{P}_i \cap \mathfrak{o}}, \Phi)$ *is isotropic and $L_{\mathfrak{P}_i \cap \mathfrak{o}}$ is modular.*
    (3) $2 \notin \mathfrak{P}_i$ *if $\mathfrak{P}_i$ is ramified over K.*
 4: **for** $1 \le i \le t$ **do**
 5:     *Set $L_{i,-1} = L_{i,0} = L$.*
 6:     *Let o_i be the order of g_i in $G(L)/\langle g_1, \ldots, g_{i-1} \rangle$.*
 7:     **for** $1 \le j < o_i$ **do**
 8:         *Let $L_{i,j}$ be a $\mathfrak{P}_i$-neighbour of $L_{i,j-1}$ different from $L_{i,j-2}$.*
 9:     **end for**
10: **end for**
11: *Set $\mathfrak{A} = \prod_{i=1}^t \mathfrak{P}_i^{o_i - 1}$.*
12: **return** $S = \{\mathfrak{A}L + (\overline{\mathfrak{A}}^{-1} L \cap \bigcap_{i=1}^t L_{i,e_i}) \mid 0 \le e_i < o_i\}$.

Proof of correctness. The lattice $M = \mathfrak{A}L + (\overline{\mathfrak{A}}^{-1} L \cap \bigcap_{i=1}^t L_{i,e_i})$ in S satisfies

$$M_{\mathfrak{p}} = \begin{cases} (L_{i,e_i})_{\mathfrak{p}} & \text{if } \mathfrak{p} = \mathfrak{P}_i \cap \mathfrak{o}, \\ L_{\mathfrak{p}} & \text{otherwise.} \end{cases}$$

Thus $G(L) = \{\psi(\Psi(M)) \mid M \in S\}$ and $\#S = \prod_i o_i = \#G(L)$. Hence Theorem 3.7 and Lemma 4.6 imply that the lattices in S represent each special genus in $\mathrm{gen}(L)$ exactly once. $\qquad\square$

The previous algorithms shows how to split a genus into special genera. To decompose a genus into isometry classes, it remains to describe how to decompose a special genus into isometry classes:

Remark 4.8.   (1) Suppose (V, Φ) is definite. Fix a maximal ideal $\mathfrak{P}$ of $\mathcal{O}$ such that $(\mathfrak{P} \overline{\mathfrak{P}}^{-1}, c(\mathfrak{P})) \in H(L)$. Every isometry class in $\mathrm{sgen}(L)$ has a representative M such that there exists a sequence $L = M_0, M_1, \ldots, M_t = M$ where M_i is a $\mathfrak{P}$-neighbour of M_{i-1}, cf. [9, Corollary 2.7]. Conversely, any lattice in such a chain of $\mathfrak{P}$-neighbours lies in $\mathrm{sgen}(L)$ by the choice

of $\mathfrak{P}$. So one can decompose $\mathrm{sgen}(L)$ be computing iterated $\mathfrak{P}$-neighbours. One only needs a method to decide if two definite hermitian $\mathcal{O}$-lattices are isometric. The latter can be done by the Plesken-Souvignier algorithm see [8] and [9, Section 4.2].

(2) If (V, Φ) is indefinite then strong approximation shows that $\mathrm{sgen}(L)$ is a single isometry class, see for example [5, Corollary 5.1.4].

Example. Let $E = \mathbb{Q}(\sqrt{-17})$ and $K = \mathbb{Q}$. The different of $\mathcal{O} = \mathbb{Z}[\sqrt{-17}]$ is $\mathfrak{P}_2^2 \mathfrak{P}_{17}$ where $\mathfrak{P}_2$ and $\mathfrak{P}_{17}$ denote the prime ideals of $\mathcal{O}$ over 2 and 17 respectively. Fix some prime ideal $\mathfrak{P}_3$ of $\mathcal{O}$ over 3. The class group C of $\mathcal{O}$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ and the subgroup C_0 has order 2.
Let L be the free hermitian $\mathcal{O}$-lattice with basis (x, y) and associated Gram matrix

$$\begin{pmatrix} 102 & \sqrt{-17} \\ -\sqrt{-17} & 0 \end{pmatrix}.$$

Then $L_2 \cong H(0)$ and $L_{17} \cong H(1)$. Theorem 3.7 shows that $\mathcal{E}(L) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The group $R(L)$ has order 2 and is diagonally embedded into $\mathcal{E}(L)$. Hence the group $G(L)$ has order $[C : C_0] \cdot [\mathcal{E}(L) : R(L)] = 4$. Using Lemma 4.6, one checks that $G(L) \cong \mathbb{Z}/4\mathbb{Z}$ is generated by $\psi(\mathfrak{P}_3 \overline{\mathfrak{P}}_3^{-1}, 1)$.
For $0 \le i \le 3$ let $L_i = \mathfrak{P}_3^i x \oplus \overline{\mathfrak{P}}_3^{-i} y$. Then L_i is a $\mathfrak{P}_3$-neighbour of L_{i-1} such that $[L : L_i]_{\mathcal{O}} = (\mathfrak{P}_3 \overline{\mathfrak{P}}_3)^{-i}$. Thus the four special genera (or isometry classes) in the genus of L are represented by the lattices L, L_1, L_2, L_3.

REFERENCES

[1] C. N. Beli. Integral spinor norm groups over dyadic local fields. *J. Number Theory*, 102(1):125–182, 2003.
[2] L. Gerstein. The growth of class numbers of quadratic forms. *Amer. J. Math.*, 94(1):221–236, 1972.
[3] R. Jacobowitz. Hermitian forms over local fields. *Amer. J. Math.*, 84:441–465, 1962.
[4] A. A. Johnson. Integral representations of hermitian forms over local fields. *J. Reine Angew. Math.*, 229:57–80, 1968.
[5] M. Kirschmer. *Definite quadratic and hermitian forms with small class number*. Habilitation, RWTH Aachen University, 2016.
[6] M. Kneser. Klassenzahlen indefiniter quadratischer Formen in drei oder mehr Veränderlichen. *Arch. Math. (Basel)*, 7:323–332, 1956.
[7] O. T. O'Meara. *Introduction to Quadratic Forms*. Springer, 1973.
[8] W. Plesken and B. Souvignier. Computing Isometries of Lattices. *Journal of Symbolic Computation*, 24:327–334, 1997.
[9] A. Schiemann. Classification of Hermitian Forms with the Neighbor Method. *J. Symbolic Computation*, 26:487–508, 1998.
[10] G. Shimura. Arithmetic of unitary groups. *Ann. Math.*, 79:269–409, 1964.
[11] G. L. Watson. Transformations of a quadratic form which do not increase the class-number. *Proc. London Math. Soc. (3)*, 12:577–587, 1962.

LEHRSTUHL D FÜR MATHEMATIK, RWTH AACHEN UNIVERSITY, PONTDRIESCH 14/16, 52062 AACHEN, GERMANY
E-mail address: `markus.kirschmer@math.rwth-aachen.de`