Definite quadratic and hermitian forms with small class number

Der Fakultät für Mathematik, Informatik und Naturwissenschaften der RWTH Aachen University vorgelegte Habilitationsschrift

von

Dr.rer.nat

Markus Kirschmer

aus Giengen

Contents

1 Introduction

1.1 The local-global principle

This Habilitation thesis investigates the local-global principle for quadratic and hermitian forms over the ring of integers in number fields. Let K be a number field with ring of integers $\mathfrak{o}$. The local-global principle shows up in various situations, for example:

- The Hasse-Minkowski theorem states that a quadratic form over K is isotropic, i.e. it represents 0, if and only if it is isotropic over every completion of K. As a consequence, two quadratic forms over K are isometric if and only if their completions are isometric at every place of K.
- The same result also holds for (quaternionic) hermitian spaces over number fields. More generally it extends to simply-connected algebraic groups defined over K.
- The Hasse-Brauer-Noether-Albert theorem (c.f. [Rei03, Theorem 32.11]) states that a central-simple K-algebra is split, i.e. isomorphic to a full matrix ring $K^{m \times m}$ if and only if it splits over every completion of K. As a consequence, two central simple K-algebras are isomorphic if and only if their completions are isomorphic at every place of K.
- The Local-Square theorem states that an element $a \in K$ is a square if and only if a is a square in every completion of K. Note that the result is not completely true for higher powers as the Grunwald-Wang theorem shows.
- The Hasse norm theorem states that given a cyclic field extension F/K, then $a \in K$ is a global norm in F/K if and only if for each place v of K and a place w of F over v, a is a local norm in F_w/K_v. Again, the result does not hold for arbitrary extensions F/K, not even for abelian ones.
- Two $\mathfrak{o}$-lattices, i.e. finitely generated $\mathfrak{o}$-submodules of a vector space over K are equal if and only if their completions are equal at every place of K.

For arithmetic structures, the local-global principle usually fails. For example, let $\mathcal{I}(\mathfrak{o})$ be the group of fractional ideals of $\mathfrak{o}$. Every element in $\mathcal{I}(\mathfrak{o})$ is locally principal, but not necessarily principal itself. If the local-global principle fails, it is interesting to know 'by how much it fails'. So in the case of fractional ideals, one investigates the class group $\mathrm{Cl}(\mathfrak{o}) := \mathcal{I}(\mathfrak{o})/\{a\mathfrak{o}\,;\, a \in K^*\}$.

1.2 Hermitian lattices and genera

Let E/K be a field extension of degree at most 2 or let E be a quaternion skewfield over K. The canonical involution of E/K will be denoted by $\overline{}\colon E \to E$. A hermitian space over E is a (left) vector space V over E equipped with a sesquilinear form $\Phi\colon V \times V \to E$ such that

- $\Phi(x + x', y) = \Phi(x, y) + \Phi(x', y)$ for all $x, x', y \in V$.
- $\Phi(\alpha x, \beta y) = \alpha\Phi(x, y)\overline{\beta}$ for all $x, y \in V$ and $\alpha, \beta \in E$.
- $\Phi(y, x) = \overline{\Phi(x, y)}$ for all $x, y \in V$.

If $E = K$ the above setting simply gives a quadratic space over K.

Let $\mathcal{O}$ be a maximal order in E. An $\mathcal{O}$-lattice in V is a finitely generated $\mathcal{O}$-submodule of V that contains an E-basis of V. The local-global principle does not hold for $\mathcal{O}$-lattices in general. As in the case of fractional ideals of $\mathfrak{o}$, this immediately leads to the definition of the *genus*. Two $\mathcal{O}$-lattices L, M in V are said to be in the same genus if and only if the completions $L_\mathfrak{p} := L \otimes_\mathcal{O} \mathcal{O}_\mathfrak{p}$ and $M_\mathfrak{p}$ are isometric for every prime ideal $\mathfrak{p}$ of $\mathfrak{o}$. Each genus is a disjoint union of (finitely many) isometry classes. The number of isometry classes in a genus is called its class number. So again, the class number measures 'by how much' the local global principle fails. In particular, the one-class genera consist precisely of those lattices for which the local-global principle does hold.

The class number of a lattice in an indefinite hermitian space is known a priori thanks to strong approximation, see Chapter 5 for details. It only depends on some local data as well as some quotient of a ray class group. For lattices in definite spaces, such local considerations do not yield the class number of a lattice. It has to be worked out explicitly, for example using Kneser's neighbour method.

The goal of this Habilitation project is to provide a complete classification of all definite hermitian lattices with class number one or two. It should be stressed that the field K, the extension E and the rank m of V over E are not fixed a priori. However, it is well known that up to a suitable equivalence relation, there are only finitely many such genera.

The enumeration of one-class genera actually dates back to C. F. Gauß. He relates the class numbers of definite binary quadratic lattices to relative ideal class numbers of CM-fields. In particular, the complete, unconditional classification of binary quadratic lattices with class number one is out of reach with current methods.

The classification of all rational quadratic lattices with class number one and rank at least three is originally due to G. L. Watson who classified these lattices by hand in a long series of papers [Wat63, Wat72, Wat74, Wat78, Wat82, Wat84, Wat]. In [KL13], D. Lorch and the author checked Watson's computations using the algorithms given in Chapter 6 and found them to be largely correct. They also enumerate all one-class genera in dimensions four and five, for which G. Watson only produced partial results. Very recently, D. Lorch in his thesis [Lor] (supervised by the author) successfully extends this classification to all one-class genera over totally real number fields.

For $E \neq K$, no complete classifications were previously known.

1.3 Limitations

The main strategy of the classification of all genera of definite hermitian lattices with given class number is as follows.

1. Enumerate the possible totally real number fields K, the possible K-algebras E and the possible ranks m.

2. Enumerate the possible similarity classes of hermitian spaces of rank m over E.

3. Enumerate the genera of square-free lattices with class number at most B. Square-free (or almost unimodular lattices as they are called by some authors) are those lattices that are endpoints under some reduction operators which do not increase class numbers, see Section 6.1 for details.

4. Enumerate the similarity classes of all genera with class number at most B by inspecting inverse images under these reduction operators.

Steps 2–4 never pose a problem. However, the first step might simply be impossible to do in practice. The reason is as follows. Siegel's mass formula yields upper bounds on the root discriminant of the possible totally real base fields K. Then one looks up these fields in tables such as [Voi08]. However, these tables are only complete up to root discriminant 14 (without further additional information like the number of primes ideals of norm 2). Already this classification needed about 200 days of CPU time. Since the search space for these fields grows exponentially with the degree of the fields, already the enumeration of all fields with slightly larger root discriminant say 15, is completely out of reach. This is the only reason why the classification of all definite hermitian lattices with class number at most two is impossible in case of some unary and binary lattices. More precisely, the following problems occur.

1. Suppose $E = K$. As mentioned before, the binary quadratic lattices lead to relative class number problems of CM-extensions, see Section 7.2 for details. Hence this case is out of reach. However the rational binary quadratic lattices with class number at most two can be enumerated assuming the Generalized Riemann Hypothesis, see Section 7.2.2.

   All definite quadratic lattices with class number at most two and rank different from two have been completely classified. A summary of the results is presented in Chapter 7.

   It is worth mentioning, that the ternary quadratic case is especially challenging. Pfeuffer's bounds on the local factors in Siegel's mass formula show that the root discriminant of K is at most 24.21, see Corollary 6.3.2. As mentioned above, this bound is useless for practical purposes.

   However, there is a different way of enumerating the ternary quadratic lattices with class number at most B using quaternion orders, see [KL16] and Section 7.3. The idea is as follows. The local global principle for quaternion orders also fails.

Thus it is natural to define what is (for historical reasons) called the type of a quaternion order. Two orders in a quaternion algebra are said to be of the same type if and only if their completions are isomorphic (i.e. conjugate) at every prime ideal of $\mathfrak{o}$. Again, each type of orders is a finite union of conjugacy classes and the number of such classes is called the type number. Now there are correspondences by Brzezinski-Peters-Eichler-Brandt or J. Voight between definite, ternary quadratic lattices over K and definite Gorenstein quaternion orders over K which maps genera and isometry classes to types and conjugacy classes. Hence, instead of classifying the definite quadratic $\mathfrak{o}$-lattices with class number at most two one can also classify the Gorenstein quaternion orders over K with type number at most two. The latter has the advantage, that one can bring Eichler's mass formula into the game. It yields a much better bound on the root discriminant of K, see Theorem 7.3.4 for details. Using this bound, one can indeed enumerate all possible base fields K that might admit one-class genera of definite quadratic forms.

It is also worth mentioning that the type number of a quaternion order agrees with the type number of its Gorenstein closure. Thus the above classification actually yields all definite quaternion orders with type number one or two, whether they are Gorenstein or not. From this result, one can then enumerate all definite quaternion orders with ideals class number one or two, see [KL16] for details.

2. Suppose E/K is a CM-extension. The unary hermitian case is directly related to the binary quadratic case. So a complete classification is again impossible. In the binary hermitian case, the situation is very similar. In this case, the possible totally real base fields K that might occur can be worked out completely, see Section 8.2. However, for some fixed field K, the enumeration of all possible extensions E/K turns out to be the problem. In this case, Siegel's mass formula does not involve the relative discriminant $\mathrm{d}_{E/K}$ but merely the relative class number $\#\operatorname{Cl}(E)/\#\operatorname{Cl}(K)$. So again, the enumeration of all definite binary hermitian lattices is a relative class number problem, see Section 8.2 for details. However, for $K = \mathbb{Q}$ it turns out that one needs to know the imaginary quadratic number fields E with class number at most 48. These have been computed by M. Watkins in his thesis [Wat04]. So for $K = \mathbb{Q}$, the enumeration of all definite, binary hermitian lattices with class number at most 2 is indeed feasible, see Table 8.1 for a summary of the results.

   For all lattices of rank at least 3, the classification of all definite hermitian lattices with class number at most two given in Chapter 8 is complete.

3. For quaternion algebras E over K, Chapter 9 provides a complete classification of all definite hermitian lattices with class number at most two.

1.4 Results

Chapters 7 to 9 report on the classification of all definite quadratic, hermitian and quaternionic hermitian lattices respectively. Below are short summaries of the results in each case.

Theorem 1.4.1 *Let K be a totally real number field with maximal order $\mathfrak{o}$. Let L be a definite quadratic $\mathfrak{o}$-lattice of rank $m \geq 3$.*

1. *If $K = \mathbb{Q}$ and L has class number one, then $m \leq 10$. Up to similarity, there are* 1884 *definite, rational quadratic lattices with class number one and rank at least* 3*. This result is due to G. Watson, see also [KL13].*

2. *If $K = \mathbb{Q}$ and L has class number two, then $m \leq 16$. Up to similarity, there exist* 7283 *genera of definite, rational quadratic lattices with class number one and rank at least* 3*.*

3. *If $K \neq \mathbb{Q}$ and L has class number one, then $m \leq 6$. Further, if $m \in \{5, 6\}$ then $K = \mathbb{Q}(\sqrt{5})$ and for each rank m there are two similarity classes. Up to similarity, there exist* 4019 *definite quadratic lattices over* 29 *different fields $K \neq \mathbb{Q}$ with class number one and rank at least* 3*. The largest field has degree* 5*. This result is due to D. Lorch, see [Lor].*

4. *If $K \neq \mathbb{Q}$ and L has class number two, then $m \leq 8$. Up to similarity, there are* 17.064 *genera of definite quadratic lattices over* 75 *different fields $K \neq \mathbb{Q}$ with class number two and rank at least* 3*. The largest field has degree* 6*.*

Details are given in Chapter 7.

Theorem 1.4.2 *Let E/K be a CM-extension and let $\mathcal{O}$ be the maximal order of E. If L is a definite hermitian $\mathcal{O}$-lattice of rank $m \geq 3$ and class number one (two), then $m \leq 8$ ($m \leq 9$). Moreover, there are* 164 (406) *similarity classes of genera of such lattices over* 10 (19) *different fields E. The largest field E has degree* 6 (8)*. A complete classification is given in Chapter 8.*

Theorem 1.4.3 *Let E be a definite quaternion algebra over some totally real number field K. Further let $\mathcal{O}$ be a maximal order in E and let L be a hermitian $\mathcal{O}$-lattice of rank m. If L has class number one (two), then $m \leq 4$ ($m \leq 5$). Further, there are only* 69 (148) *different algebras E over* 29 (60) *different centers K that admit genera of definite lattices of class number one (two). A complete list of these lattices in given in Chapter 9.*

Note that counting similarity classes of quaternionic hermitian lattices does not make much sense since two different maximal orders yield genera which can never be similar. However, these genera can be described uniformly using genus symbols, see Chapter 9 for details.

Since some enumerations produced large numbers of genera, not all of these genera could be described in the thesis explicitly. Thus all the results are also electronically available from [Kir16] in a text-based format which can be processed easily by any computer algebra system.

The enumeration of all genera with given class number relies heavily on calculations (like computing automorphism groups, isometry tests, unit and class groups of orders, ideals and orders in quaternion algebras, computing with modules over Dedekind rings, ...) that require the use of a computer algebra system. The author has chosen to implement the classification in `Magma` [BCP97] as it covers most of the required basic algorithms and it is easily extensible through packages. The code for performing the classification as well as certain intermediate steps (like constructing hermitian spaces and lattices from local data, deciding (local) isometry, Kneser's neighbour method, ...) is available upon request.

1.5 Outline

The Habilitation thesis is organized as follows. The second chapter gives a short introduction to lattices in quadratic and hermitian spaces. Chapter 3 recalls the classification of quadratic and hermitian spaces over local fields. It also discusses the structure of lattices in such spaces, i.e. Jordan decompositions.

The fourth chapter presents Siegel's mass formula, which is the most important tool for classifying all genera with a given class number. The local factors that appear in the mass formula were not known in all cases. Especially local factors at even prime ideals are notoriously difficult to handle. Thus, in Sections 4.4 and 4.5 the local factors of unimodular quadratic lattices as well as the local factors of square-free hermitian lattices at ramified prime ideals over 2 are worked out completely using a method of M. Eichler.

In Chapter 5, Kneser's Neighbour method is presented. It allows the complete enumeration of all isometry classes in a given genus. The description given here works for quadratic as well as (quaternionic) hermitian lattices. It is very explicit, in the sense that it provides generators for every single neighbour. Also the number of neighbours is worked out in all cases.

Chapter 6 explains how to classify all definite hermitian lattices with a given class number. As mentioned before, Chapters 7 to 9 report on the classification of all one- and two-class genera of lattices in definite quadratic, hermitian and quaternionic hermitian spaces respectively.

The concept of genera and isometry classes can be generalized to algebraic groups over K. In that sense, the first nine chapters dealt with classical (i.e. orthogonal and unitary) groups. The last chapter then discusses the parahoric subgroups of exceptional algebraic groups over K having class number one.

2 Basic definitions

2.1 Quadratic and hermitian spaces

In this work, K always denotes some field of characteristic 0. Further, $(E, \overline{})$ will be one of the following K-algebras with involution:

1. $E = K$ and $\overline{}$ is the identity on K.
2. $E \cong K[X]/(X^2 - a)$ and $\overline{}$ is the nontrivial K-linear automorphism of E.
3. E is a *quaternion algebra* with center K, i.e. a 4-dimensional, central simple K-algebra. By the Artin-Wedderburn theorem, E is either a skew field or isomorphic to the full matrix ring $K^{2\times 2}$. In any case, it admits a K-basis $(1, i, j, ij)$ such that

   $$a := i^2 \in K, \quad b := j^2 \in K \quad \text{and} \quad ij = -ji\,.$$

   The quaternion algebra over K with these multiplication rules will be denoted by $\left(\frac{a,b}{K}\right)$. Further,

   $$\overline{} \colon E \to E,\ x + yi + zj + wij \mapsto x - yi - zj - wij \quad \text{with } x, y, z, w \in K$$

   is called the *canonical involution* of E. It satisfies $\{\alpha \in E\,;\, \alpha = \overline{\alpha}\} = K$. In particular, the *reduced norm* and *reduced trace*

   $$\mathrm{nr}_{E/K} \colon E \to K,\ \alpha \mapsto \alpha\overline{\alpha} \quad \text{and} \quad \mathrm{tr}_{E/K} \colon E \to K,\ \alpha \mapsto \alpha + \overline{\alpha}$$

   take values in K.

In any of these three cases, let

$$\mathrm{N} \colon E \to K,\ \alpha \mapsto \alpha\overline{\alpha} \quad \text{and} \quad \mathrm{T} \colon E \to K, \alpha \mapsto \alpha + \overline{\alpha}\,.$$

If $E = K$ these maps are simply squaring and multiplication by 2 respectively. In the other two cases these are the (reduced) norm and (reduced) trace of E over K. Also note that since E is a separable K-algebra, the bilinear form

$$E \times E \to K,\ (\alpha, \beta) \mapsto \mathrm{T}(\alpha\beta)$$

associated to T is non-degenerate.

Definition 2.1.1 A *hermitian space* (V, Φ) over E is a finitely generated, free left E-module V equipped with a map $\Phi \colon V \times V \to E$ such that

- $\Phi(x+x',y)=\Phi(x,y)+\Phi(x',y)$ for all $x,x',y\in V$.
- $\Phi(\alpha x,\beta y)=\alpha\Phi(x,y)\overline{\beta}$ for all $x,y\in V$ and $\alpha,\beta\in E$.
- $\Phi(y,x)=\overline{\Phi(x,y)}$ for all $x,y\in V$.

For a hermitian space (V,Φ) over E, the map

$$Q_\Phi\colon V\to K,\ x\mapsto\Phi(x,x)$$

defines a quadratic form on the K-vector space V, i.e.

1. $Q_\Phi(ax)=a^2Q_\Phi(x)$ for all $a\in K$ and $x\in V$,
2. $b_\Phi\colon V\times V\to K,\ (x,y)\mapsto Q_\Phi(x+y)-Q_\Phi(x)-Q_\Phi(y)$ is bilinear.

In particular, if $E=K$, then $2\Phi=b_\Phi$. So in this case it makes sense to call (V,Φ) a *quadratic space*. Since the characteristic of K is different from 2, the bilinear form Φ can be recovered from Q_Φ or b_Φ and vice versa. So in the sequel, the space (V,Φ) will also be denoted by (V,Q_Φ) whenever convenient.

Definition 2.1.2 The hermitian spaces (V,Φ) and (V',Φ') over E are said to be *isometric* (denoted by $(V,\Phi)\cong(V',\Phi')$), if there exists some isomorphism $\sigma\colon V\to V'$ of E-modules such that $\Phi(x,y)=\Phi'(\sigma(x),\sigma(y))$ for all $x,y\in V$. Any such isomorphism is then called an *isometry* between (V,Φ) and (V',Φ'). The group of all isometries of (V,Φ) itself, i.e.

$$\mathbf{U}(V,\Phi):=\{\sigma\in\mathrm{GL}(V)\,;\,\Phi(\sigma(x),\sigma(y))=\Phi(x,y)\text{ for all }x,y\in V\}$$

is called the *unitary group* of (V,Φ). If (V,Φ) is quadratic, then $\mathbf{U}(V,\Phi)$ is also called the *orthogonal group* of (V,Φ) and will sometimes be denoted by $\mathbf{O}(V,\Phi)$.

Definition 2.1.3 Let (V,Φ) be a hermitian space over E of rank m with basis B.

1. The space (V,Φ) is called *regular*, if $\Phi(x,V)\neq\{0\}$ for all nonzero $x\in V$.
2. The space (V,Φ) is said to *represent* $a\in K$, if $a=Q_\Phi(x)$ for some non-zero $x\in V$. A vector $x\in V$ is called *isotropic* if $Q_\Phi(x)=0$. Similarly, (V,Φ) is said to be *isotropic*, if Φ represents zero, i.e. it contains a nonzero isotropic vector.
3. Two vectors $x,y\in V$ are called *perpendicular* or *orthogonal* if $\Phi(x,y)=0$. Let V_1,V_2 be E-submodules of V. Then V is the *orthogonal sum* of the V_i, denoted by $V=V_1\perp V_2$, if $V=V_1\oplus V_2$ and $\Phi(V_1,V_2)=\{0\}$.
4. The *Gram matrix* of any tuple $S=(x_1,\dots,x_m)\in V^m$ is

$$\mathrm{G}(S):=(\Phi(x_i,x_j))_{i,j}\in E^{m\times m}\ .$$

5. The *determinant* $\det(V,\Phi)$ is the class of the Dieudonné determinant $\det(\mathrm{G}(B))$ in $K/\,\mathrm{N}(E^*)$ whenever E is a skew field. If E contains zero divisors, then $\det(V,\Phi)$ is defined to be the neutral element in the trivial group $K^*/\,\mathrm{N}(E^*)$. In any case,

$$\operatorname{disc}(V,\Phi) := (-1)^{m(m-1)/2}\cdot\det(V,\Phi)$$

is called the *discriminant* of (V,Φ).

6. Given square matrices $G_1,\ldots,G_s$ over E such that $G_i = \overline{G_i}^{\mathrm{tr}}$, then $\langle G_1,\ldots,G_s\rangle$ denotes a hermitian space over E which has a block diagonal Gram matrix $\mathrm{Diag}(G_1,\ldots,G_s)$.

7. The space (V,Φ) is said to be *hyperbolic*, if $(V,\Phi)\cong\langle\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right),\ldots,\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)\rangle$.

The fact that the bilinear form associated to T is non-degenerate has several important consequences.

Theorem 2.1.4 *Let (V,Φ) be a regular hermitian space over E. Then (V,Φ) admits an orthogonal E-basis, i.e. $(V,\Phi)\cong\langle a_1,\ldots,a_m\rangle$ for some $a_i\in K^*$.*

Proof. Let $(b_1,\ldots,b_m)$ be any basis of V. The result is trivial if $m=1$. Suppose now $m\geq 2$ and $Q_\Phi(b_i)=0$ for all i. Since (V,Φ) is non-degenerate there exists $i>1$ such that $\Phi(b_1,b_i)\neq 0$. Since the trace bilinear form associated to T non-degenerate, there exists some $\lambda\in E$ such that $\mathrm{T}(\Phi(b_1,b_i)\overline{\lambda})=1$. Then $Q_\Phi(b_1+\lambda b_i)=\mathrm{T}(\Phi(b_1,\lambda b_2))=1$. So without loss of generality one may assume that $a_1 := Q_\Phi(b_1)\neq 0$. But then $V = Eb_1\perp\sum_{j=2}^m E(b_j-\frac{\Phi(b_j,b_1)}{a_1}b_1)$. Hence the result follows by induction on m. □

Proposition 2.1.5 *Let (V,Φ) be a regular hermitian space over E of rank m. Let $\mathbb{H}=\left(\frac{-1,-1}{\mathbb{R}}\right)$ be Hamilton's quaternions.*

1. *If $K=\mathbb{R}$ and $E\in\{\mathbb{R},\mathbb{C},\mathbb{H}\}$ then the isomorphism type of a regular hermitian space over E is uniquely determined by its rank and $n_{(V,\Phi)} := \#\{b\in B\,;\,Q_\Phi(b)<0\}$ where B denotes any orthogonal basis of V over E.*

2. *If $\mathrm{N}(E^*)=K^*$, then $(V,\Phi)\cong\langle 1,\ldots,1\rangle$. Note that this holds whenever $K=\mathbb{C}$.*

Proof. The first assertion is Sylvester's law of inertia. The second assertion follows from the previous theorem and the fact that $\Phi(\alpha x,\alpha x)=\mathrm{N}(\alpha)\Phi(x,x)$ for all $\alpha\in E$ and $x\in V$. □

Remark 2.1.6 Let (V,Φ) be a hermitian space over E. For any E-linear map $\sigma\colon V\to V$, the following statements are equivalent:

1. $\sigma\in\mathbf{U}(V,\Phi)$.

2. $Q_\Phi(\sigma(x))=Q_\Phi(x)$ for all $x\in V$.

Proof. Clearly 1. implies 2. Conversely, suppose σ satisfies the second condition. If $E = K$, then 1. holds thanks to the polarization identity

$$2\Phi(x,y) = b_\Phi(x,y) = Q_\Phi(x+y) - Q_\Phi(x) - Q_\Phi(y) \quad \text{for all } x, y \in V\ .$$

Suppose now $E \neq K$. Let $x, y \in V$ and $\alpha \in E$. By assumption

$$\begin{aligned} &Q_\Phi(\sigma(x)) + Q_\Phi(\sigma(y)) + \mathrm{T}(\Phi(\sigma(x), \sigma(y))) \\ &= Q_\Phi(\sigma(x+y)) = Q_\Phi(x+y) \\ &= Q_\Phi(x) + Q_\Phi(y) + \mathrm{T}(\Phi(x,y))\ . \end{aligned}$$

and therefore

$$\mathrm{T}(\alpha\Phi(\sigma(x), \sigma(y))) = \mathrm{T}(\alpha\Phi(x,y)) \quad \text{for all } \alpha \in E\ .$$

The bilinear form associated to T is non-degenerate and thus $\Phi(x,y) = \Phi(\sigma(x), \sigma(y))$.□

2.2 Lattices over maximal orders

In this section, some well known facts about finitely generated, torsion free modules over maximal orders are recalled.

Definition 2.2.1 Let $\mathfrak{o}$ be a Dedekind ring, i.e. an integrally closed Noetherian ring of Krull dimension 1. Further, let K be the field of fractions of $\mathfrak{o}$ and let E be a separable K-algebra.

1. An $\mathfrak{o}$-*lattice* $I \subset E$ is a finitely generated $\mathfrak{o}$-submodule of E. It is said to be *full*, if the ambient K-space KI equals E.
2. A full $\mathfrak{o}$-lattice in E which is also a subring of E is called an $\mathfrak{o}$-*order* (or simply an *order*) in E. An order is called maximal, if it is not properly contained in another order.
3. Let I be a full $\mathfrak{o}$-lattice in E. Then
$$\mathcal{O}_\ell(I) := \{x \in E\,;\, xI \subseteq I\} \quad \text{and} \quad \mathcal{O}_r(I) := \{x \in E\,;\, Ix \subseteq I\}$$
are $\mathfrak{o}$-orders in E, the so-called *left* and *right orders* of I. The lattice I is *integral*, if $I \subseteq \mathcal{O}_\ell(I)$ (or equivalently $I \subseteq \mathcal{O}_r(I)$).
4. Let $\mathcal{O}$ be an order in E. An $\mathfrak{o}$-lattice I is called a *fractional left ideal* of $\mathcal{O}$, if $\mathcal{O}_\ell(I) \subseteq \mathcal{O}$. Similarly, one defines fractional right ideals. If I as a fractional left and right ideal of $\mathcal{O}$, it is called a *fractional twosided ideal* of $\mathcal{O}$.
5. A fractional left ideal I of $\mathcal{O}$ is said to be *invertible*, if $IJ = \mathcal{O}$ for some $\mathfrak{o}$-lattice J. If J exists, then $\mathcal{O} = \mathcal{O}_\ell(I)$ and $JI = \mathcal{O}_r(I)$. So there is no need to distinguish between left, right and twosided invertible ideals. Also note that if $\mathcal{O}$ is maximal, then every (left/right/twosided) ideal of $\mathcal{O}$ is invertible.

Definition 2.2.2 Let $\mathcal{O}$ be a maximal order in some separable K-algebra E and let V be a finitely generated, free left module over E.

1. An $\mathcal{O}$-lattice $L \subset V$ is a finitely generated $\mathcal{O}$-module in V. The rank of an $\mathcal{O}$-lattice L is the rank of the ambient space EL over E and will be denoted by $\operatorname{rank}(L)$. The lattice L is said to be full, if the ambient space EL equals V, i.e. L contains an E-basis of V.

2. Let L be an $\mathcal{O}$-lattice. Suppose there exists an E-basis $(x_1, \ldots, x_n)$ of EL and fractional left ideals $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$ of $\mathcal{O}$ such that
$$L = \bigoplus_{i=1}^{n} \mathfrak{A}_i x_i \, .$$
Then the sequence of pairs $(\mathfrak{A}_i, x_i)_{1 \leq i \leq n}$ is called a *pseudo-basis* of L.

The existence of pseudo-bases over Dedekind rings is due to E. Steinitz and is well known.

Theorem 2.2.3 (Steinitz) *Let $\mathfrak{o}$ be a Dedekind ring with fields of fractions K and let M be an $\mathfrak{o}$-lattice in a finite dimensional K-space V.*

1. *The $\mathfrak{o}$-module M is projective and admits some pseudo-basis $(\mathfrak{a}_i, x_i)_{1 \leq i \leq r}$.*

2. *Let M' be an $\mathfrak{o}$-lattice in KM of rank s. Then $s \leq r$ and there exists a pseudo-basis $(\mathfrak{a}_i, x_i)_{1 \leq i \leq r}$ of M and fractional ideals $\mathfrak{b}_1, \ldots, \mathfrak{b}_s$ of $\mathfrak{o}$ such that*
$$M' = \bigoplus_{j=1}^{s} \mathfrak{b}_j \mathfrak{a}_j x_j \quad \text{and} \quad \mathfrak{b}_1 \supseteq \mathfrak{b}_2 \supseteq \ldots \supseteq \mathfrak{b}_s \, .$$
The ideals $\mathfrak{b}_1, \ldots, \mathfrak{b}_s$ are called the invariant factors *of M and M'; they are uniquely determined. In particular, the* index ideal *of M' in M*
$$[M : M']_{\mathfrak{o}} := \prod_{i=1}^{s} \mathfrak{b}_i$$
is well defined.

Proof. See for example [O'M73, Chapter 81]. □

Using pseudo-bases, `Magma` can perform a wide range of operations for finitely generated modules over Dedekind rings like addition, intersection, comparison, invariant factors, etc. Hence, for algorithmic purposes, lattices over Dedekind rings will always be assumed to be given by a pseudo-basis.

For the remainder of this section let $\mathfrak{o}$ be the ring of integers of some number field K and let $\mathcal{O}$ be a maximal order in some separable K-algebra E. Then every $\mathcal{O}$-lattice admits a pseudo-basis, see for example [Rei03, Theorem 2.44 and Remark 2.45]. However, I do not know of a constructive proof of this fact in the literature or even an implementation in some computer algebra system. Hence a constructive proof will be given below. The algorithm is based on the corresponding algorithm for finitely generated modules over Dedekind rings by W. Bosma and M. Pohst [BP91].

First, one needs special two-element generators for (left) ideals of $\mathcal{O}$:

Lemma 2.2.4 *Let $\mathfrak{A}$ be an integral left ideal of $\mathcal{O}$. Let $a \in \mathbb{N}$ be a generator of $\mathfrak{A} \cap \mathbb{Z}$. Then there exists some $\alpha \in \mathfrak{A}$ such that*

$$\mathfrak{A} = \mathcal{O}a + \mathcal{O}\alpha \quad \text{and} \quad \mathcal{O}\alpha \cap \mathbb{Z} = \mathbb{Z}ab \text{ where } b \in \mathbb{N} \text{ is coprime to } a\,.$$

Further, if a and α satisfy the above conditions, then $\mathfrak{A}^{-1} = \mathcal{O} + \alpha^{-1}b\mathcal{O}$.

Proof. If $a = 1$, then $\mathfrak{A} = \mathcal{O}$ and one can take $\alpha = 1$. Suppose now $a > 1$. By [Rei03, Corollary 27.7], there exists some $\alpha \in E^*$ such that $\mathfrak{A}^{-1}a^2 + \mathfrak{A}^{-1}\alpha = \mathfrak{A}^{-1}\mathfrak{A}$. Hence $\mathfrak{A} = \mathcal{O}a^2 + \mathcal{O}\alpha = \mathcal{O}a + \mathcal{O}\alpha$. By induction it follows that $\mathfrak{A} = \mathcal{O}a^n + \mathcal{O}\alpha$ for all $n \in \mathbb{N}$. Let $\mathcal{O}\alpha \cap \mathbb{Z}$ be generated by $ab \in \mathbb{N}$. Suppose there exists some prime divisor p of $\gcd(a, b)$. Then there exists some prime ideal $\mathfrak{p}$ of $\mathfrak{o}$ over p such that a is not contained in $\mathcal{O}_\mathfrak{p}\alpha$. Further, there exists some $n \in \mathbb{N}$ such that $\mathcal{O}_\mathfrak{p}a^n \subseteq \mathcal{O}_\mathfrak{p}\alpha$ and therefore $\mathfrak{A}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}\alpha$. But then $a \in \mathcal{O}_\mathfrak{p}\alpha$ gives the desired contradiction. Hence a and b are coprime.
Suppose now $\alpha \in \mathcal{O}$ satisfies the conditions of the lemma. Let $\mathfrak{B} = \mathcal{O} + \alpha^{-1}b\mathcal{O}$. Then $\mathfrak{B}\mathfrak{A} = \mathcal{O}a + \mathcal{O}b + \mathcal{O}\alpha\mathcal{O} + \mathcal{O}\alpha^{-1}ab\mathcal{O}$. It follows that $\mathfrak{B}\mathfrak{A} = \mathcal{O}$ since a and b are coprime integers and α, $\alpha^{-1}ab \in \mathcal{O}$. Thus $\mathfrak{B} = \mathfrak{A}^{-1}$ as claimed. □

Note that, an element α satisfying the conditions of Lemma 2.2.4 is usually found as a small linear combination of some $\mathbb{Z}$-basis of $\mathfrak{A}$.

Corollary 2.2.5 *If $\mathfrak{A}$ is a left ideal of $\mathcal{O}$, then there exist $\alpha_1, \alpha_2 \in \mathfrak{A}$ and $\beta_1, \beta_2 \in \mathfrak{A}^{-1}$ such that $\alpha_1\beta_1 + \alpha_2\beta_2 = \beta_1\alpha_1 + \beta_2\alpha_2 = 1$.*

Proof. Without loss of generality, $\mathfrak{A}$ is integral. Let a, b, α be as in Lemma 2.2.4. Since a and b are coprime integers, there exist $r, s \in \mathbb{Z}$ such that $ra + sb = 1$. Then for example $\beta_1 = 1$, $\alpha_1 = ra$, $\beta_2 = sb\alpha^{-1}$ and $\alpha_2 = \alpha$ will do the trick. □

Algorithm 2.2.6 PseudoBasis$(m_1, \dots, m_r)$
Input: Generators $m_1, \dots, m_r$ of some left $\mathcal{O}$-module M.
Output: Some pseudo-basis $(\mathfrak{A}_i, x_i)_i$ of M.

```
Let $(v_1, \dots, v_n)$ be an $E$-basis of the ambient space $EM$.
if $n = 0$ then return $\emptyset$ end if
Write $m_i = \nu_{i,1}v_1 + \cdots + \nu_{i,n}v_n$ for $1 \le i \le r$.
Set $\mathfrak{A}_1 = \sum_{i=1}^r \mathcal{O}\nu_{i,1}$.
Compute $\alpha_1, \alpha_2 \in \mathfrak{A}_1$ and $\beta_1, \beta_2 \in \mathfrak{A}_1^{-1}$ such that $\beta_1\alpha_1 + \beta_2\alpha_2 = 1$.
Using linear algebra over $\mathfrak{o}$ or $\mathbb{Z}$, compute $h_1, h_2 \in M$ and $w_1, w_2 \in \bigoplus_{j \ge 2} Ev_j$ such
  that $\alpha_i v_1 = h_i + w_i$.
```

```
Set $x_1 = v_1 - (\beta_1 w_1 + \beta_2 w_2) = \beta_1 h_1 + \beta_2 h_2$.
For $1 \leq i \leq r$ set $m_i' = m_i - \nu_{i,1} x_1$.
Let $(\mathfrak{A}_2, x_2), \dots, (\mathfrak{A}_s, x_s)$ be the output of PseudoBasis$(m_1', \dots, m_r')$.
return $(\mathfrak{A}_1, x_1), \dots, (\mathfrak{A}_s, x_s)$.
```

Proof. By construction, $m_i' \in M$ and $m_i' - m_i = \nu_{i,1} x_i \in \mathfrak{A}_1 x_1 \subseteq M$. Thus M equals $\mathfrak{A}_1 x_1 \oplus \sum_{j=1}^{r} \mathcal{O} m_j'$. By induction on rank$(M)$, the algorithm terminates and returns a pseudo-basis of M. □

Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{o}$. Given an $\mathfrak{o}$-module M, let $M_\mathfrak{p}$ denote its completion at $\mathfrak{p}$. Using pseudo-bases, one can not only perform the obvious operations like taking sums, intersections, etc., but also various 'local' manipulations of a given $\mathcal{O}$-module M. Usually, one proceeds in three steps:

1. Construct a free $\mathcal{O}$-submodule (or supermodule) M' of M such that $M_\mathfrak{p} = M'_\mathfrak{p}$ for some prime ideal $\mathfrak{p}$ of $\mathfrak{o}$.

2. Using the $\mathcal{O}$-basis of M' (which is also a $\mathcal{O}_\mathfrak{p}$-basis for $M_\mathfrak{p}$) perform the wanted local operation on $M_\mathfrak{p}$.

3. By adding the module $\mathfrak{p}M$ and intersecting with $\mathfrak{p}^{-1}M$, one ensures that the places different from $\mathfrak{p}$ are not affected by the manipulations performed in step 2.

For example, the construction of maximal submodules can be done as follows.

Algorithm 2.2.7 MaximalSubmodules$(M, \mathfrak{p})$

Input: An $\mathcal{O}$-module M given by some pseudo-basis $(\mathfrak{A}_1, x_1), \dots, (\mathfrak{A}_s, x_s)$ and some prime ideal $\mathfrak{p}$ of $\mathfrak{o}$.

Output: The set of all maximal $\mathcal{O}$-sublattices of M that contain $\mathfrak{p}M$.

```
For $1 \leq i \leq s$ compute $\alpha_i \in \mathfrak{A}_i$ such that $(\mathfrak{A}_i)_\mathfrak{p} = \mathcal{O}_\mathfrak{p} \alpha_i$ (for example by inspecting
    small linear combinations of elements in a $\mathbb{Z}$-basis of $\mathfrak{A}_i$).
Let $M' := \sum_{i=1}^{s} \mathcal{O} \alpha_i x_i \subseteq M$.
Let $\varphi \colon M' \to (\mathcal{O}/\mathfrak{p}\mathcal{O})^s$, $\sum_i \lambda_i x_i \mapsto (\lambda_1 + \mathfrak{p}\mathcal{O}, \dots, \lambda_1 + \mathfrak{p}\mathcal{O})$.
Let $X_1, \dots, X_r$ be the maximal $\mathcal{O}/\mathfrak{p}\mathcal{O}$-submodules of $(\mathcal{O}/\mathfrak{p}\mathcal{O})^s$.
return $\{\varphi^{-1}(X_i) + \mathfrak{p}M \,;\, 1 \leq i \leq r\}$.
```

Proof. From $M_\mathfrak{p} = M'_\mathfrak{p}$, it follows that $(\varphi^{-1}(X_i) + \mathfrak{p}M)_\mathfrak{p} = (\varphi^{-1}(X_i))_\mathfrak{p}$ with $1 \leq i \leq r$ are the maximal $\mathcal{O}_\mathfrak{p}$-submodules of $M_\mathfrak{p}$ that contain $\mathfrak{p}M$. Let $\mathfrak{q}$ be a prime ideal of $\mathfrak{o}$ different from $\mathfrak{p}$. Then $M' \subseteq M$ implies that $(\varphi^{-1}(X_i) + \mathfrak{p}M)_\mathfrak{q} = M_\mathfrak{q}$. Hence the result is correct. □

2.3 Hermitian lattices over Dedekind rings

Let $\mathfrak{o}$ be a Dedekind ring with field of fractions K. Further let (V, Φ) be a regular hermitian space over E and fix some maximal $\mathfrak{o}$-order $\mathcal{O}$ in E.

To ease notation, the term '$\mathcal{O}$-lattice in (V, Φ)' from now on means an $\mathcal{O}$-lattice in V of full rank.

Definition 2.3.1 Let $\mathfrak{A}$ be a fractional left ideal of $\mathcal{O}$. Then $\mathrm{N}(\mathfrak{A})$ and $\mathrm{T}(\mathfrak{A})$ denote the $\mathfrak{o}$-ideals generated by $\{\alpha\overline{\alpha}\,;\, \alpha \in \mathfrak{A}\}$ and $\{\alpha + \overline{\alpha}\,;\, \alpha \in \mathfrak{A}\}$ respectively.

Definition 2.3.2 Let L be a free $\mathcal{O}$-lattice in (V, Φ) with basis B. Suppose E is a skew field. Then

$$\begin{aligned} \det(L) &:= \det(\mathrm{G}(B)) \in K^* / \, \mathrm{N}(\mathcal{O}^*) \\ \operatorname{disc}(L) &:= (-1)^{m(m-1)/2} \cdot \det(L) \end{aligned}$$

are called the *determinant* and *discriminant* of L respectively. Given square matrices $G_1, \dots, G_s$ over E such that $G_i = \overline{G_i}^{\mathrm{tr}}$, then $\langle G_1, \dots, G_s \rangle$ denotes a free hermitian $\mathcal{O}$-lattice with Gram matrix $\mathrm{Diag}(G_1, \dots, G_s)$.

Definition 2.3.3 Let L be an $\mathcal{O}$-lattice in (V, Φ).

1. Then $L^\# := \{x \in V\,;\, \Phi(x, L) \subseteq \mathcal{O}\}$ is called the *dual* of L.

2. L is called *integral* if $L \subseteq L^\#$.

3. If there exists some fractional twosided ideal $\mathfrak{A}$ of $\mathcal{O}$ such that $\mathfrak{A}L^\# = L$, then L is said to be $\mathfrak{A}$-*modular*. The $\mathcal{O}$-modular lattices are also called *unimodular*.

4. If E is commutative, then the index ideal $[L^\# : L]_{\mathcal{O}}$ is called the *volume* of L and will be denoted by $\mathfrak{v}(L)$.

5. The *scale* $\mathfrak{s}(L)$ is the set $\Phi(L, L) = \{\Phi(x, y)\,;\, x, y \in L\}$.

6. The $\mathfrak{o}$-ideal generated by $\{Q_\Phi(x)\,;\, x \in L\}$ is the *norm* $\mathfrak{n}(L)$.

7. Let $\mathfrak{a}$ be a fractional ideal of $\mathfrak{o}$. Then L is said to be $\mathfrak{a}$-*maximal*, if $\mathfrak{n}(L) \subseteq \mathfrak{a}$ and whenever $L \subsetneq L'$ for some $\mathcal{O}$-lattice L' then $\mathfrak{n}(L') \not\subseteq \mathfrak{a}$.

8. Given a fractional left ideal $\mathfrak{A}$ of $\mathcal{O}$, let
$$L^{\mathfrak{A}} := \{x \in L\,;\, \Phi(x, L) \subseteq \mathfrak{A}\}\,.$$

9. For $a \in K^*$, the *rescaled lattice* L^a denotes the module L in the hermitian space $(V, a\Phi)$.

10. Suppose $L = L_1 \oplus L_2$ with some $\mathcal{O}$-submodules L_i such that $\Phi(L_1, L_2) = \{0\}$. Then L is called the *orthogonal sum* of L_1 and L_2. This will be denoted by $L = L_1 \perp L_2$.

Remark 2.3.4 Let L be an $\mathcal{O}$-lattice in (V, Φ) with pseudo-basis $(\mathfrak{A}_i, x_i)_{1 \le i \le m}$.

1. Let $(x_1^*, \dots, x_m^*)$ be the basis of V, which is dual to $(x_1, \dots, x_m)$ with respect to Φ. Then
$$L^\# = \bigoplus_{i=1}^{m} \overline{\mathfrak{A}_i}^{-1} x_i^*\,.$$
In particular, $L^\#$ is an $\mathcal{O}$-lattice with pseudo-basis $(\overline{\mathfrak{A}_i}^{-1}, x_i^*)_{1 \le i \le m}$ and $(L^\#)^\# = L$.

2. The scale $\mathfrak{s}(L)$ is a twosided ideal of $\mathcal{O}$. Moreover, the scale and norm of L can be computed as follows:

$$\mathfrak{s}(L) = \sum_{1\le i,j\le m} \mathfrak{A}_i \Phi(x_i, x_j)\overline{\mathfrak{A}_j}\ ,$$

$$\mathfrak{n}(L) = \sum_{i=1}^{m} \mathrm{N}(\mathfrak{A}_i)\Phi(x_i, x_i) + \sum_{1\le i<j\le m} \mathrm{T}(\mathfrak{A}_i \Phi(x_i, x_j)\overline{\mathfrak{A}_j})\ .$$

3. If E is a field, then the volume $\mathfrak{v}(L)$ is the fractional ideal of E generated by

$$\{\det(\mathrm{G}(b))\, ;\, b \subset L \text{ is linearly independent}\}\ .$$

4. Suppose L is $\mathfrak{A}$-modular. Then $\mathfrak{A} = \mathfrak{s}(L)$, in particular, it make sense to call L a modular lattice, since the ideal $\mathfrak{A}$ can be recovered easily from L.

Proof. After taking completions, one may assume that L is a free $\mathcal{O}$-module. The proofs are then routine. □

Definition 2.3.5 Let (V', Φ') be a hermitian space over E. Let L and L' be $\mathcal{O}$-lattices in (V, Φ) and (V', Φ') respectively.

1. The lattices L and L' are *isometric*, denoted by $L \cong L'$, if $\sigma(L) = L'$ for some isometry $\sigma\colon (V, \Phi) \to (V', \Phi')$. Then σ is called a *isometry* from L to L'.

2. The lattices L and L' are said to be *similar*, if $L' \cong L^a$ for some $a \in K^*$.

3. The *automorphism group* of L is the group

$$\mathrm{Aut}(L) := \{\sigma \in \mathbf{U}(V, \Phi)\, ;\, \sigma(L) = L\}$$

of all isometries from L on itself.

2.4 Hermitian lattices over number fields

Let K be a number field with maximal order $\mathfrak{o}$. Further, let (V, Φ) be a hermitian space over E and fix some maximal order $\mathcal{O}$ in E.

For the remainder of this work, some more notation will be needed.

1. The space (V, Φ) is called (totally positive) *definite*, if K is totally real and $Q_\Phi(x)$ is totally positive for all nonzero $x \in V$.

2. The set of all places of K will be denoted by $\Omega(K)$. For $v \in \Omega(K)$, let K_v be the completion of K at v. Similarly $V_v := V \otimes_K K_v$ is the completion of V at v. By linearity, the form Φ extends to V_v. Hence (V_v, Φ) is a hermitian space over $E_v := E \otimes_K K_v$.

3. The set of all prime ideals of $\mathfrak{o}$ will be denoted by $\mathbb{P}(\mathfrak{o})$. The prime ideals are identified with the finite places of K. Hence it makes sense to write $\mathbb{P}(\mathfrak{o}) \subset \Omega(K)$. Further, for $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$ let $\operatorname{ord}_{\mathfrak{p}} \colon K_{\mathfrak{p}} \to \mathbb{Z} \cup \{\infty\}$ be the usual $\mathfrak{p}$-adic valuation.

4. Let $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$. The completion of $\mathfrak{o}$ at $\mathfrak{p}$ will be denoted by $\mathfrak{o}_{\mathfrak{p}}$. Moreover, if M is an $\mathfrak{o}$-module, then $M_{\mathfrak{p}} := M \otimes_{\mathfrak{o}} \mathfrak{o}_{\mathfrak{p}}$ is the completion of M at $\mathfrak{p}$. In particular, given an $\mathcal{O}$-lattice L in (V, Φ), then $L_{\mathfrak{p}}$ is an $\mathcal{O}_{\mathfrak{p}}$-lattice in $(V_{\mathfrak{p}}, \Phi)$.

5. Let $K_{>0} = \{a \in K^* \,;\, \sigma(a) > 0 \text{ for all real embeddings } \sigma \colon K \to \mathbb{R}\}$ be the subset of totally positive elements. Further, let $\mathfrak{o}_{>0} := K_{>0} \cap \mathfrak{o}$.

6. The free abelian group of all fractional ideals of $\mathfrak{o}$ will be denoted by $\mathcal{I}(\mathfrak{o})$ and

$$\begin{aligned} \operatorname{Cl}(K) := \operatorname{Cl}(\mathfrak{o}) &:= \mathcal{I}(\mathfrak{o})/\{a\mathfrak{o} \,;\, a \in K^*\} \\ \operatorname{Cl}^+(K) := \operatorname{Cl}^+(\mathfrak{o}) &:= \mathcal{I}(\mathfrak{o})/\{a\mathfrak{o} \,;\, a \in K_{>0}\} \end{aligned}$$

   denote the *class group* and *narrow class group* of K (or $\mathfrak{o}$) respectively.

7. The group of roots of unity in a number field F will be denoted by $\mu(F)$.

Theorem 2.4.1 (Local-Global Principle) *Two hermitian spaces (V, Φ) and (V', Φ') over E are isometric, if and only if their completions (V_v, Φ) and (V'_v, Φ') are isometric at every place $v \in \Omega(K)$.*

Proof. The problem was solved by H. Minkowski, H. Hasse, W. Landherr, M. Kneser and T. Springer. For a proof, see for example [Sch85, Chapter 10]. □

In particular, the classification of hermitian spaces over E follows immediately from the classification of hermitian spaces over $\mathbb{R}, \mathbb{C}$ and non-Archimedean local fields. The latter classification will be discussed in Chapter 3 while the first two cases are handled by Proposition 2.1.5. For $\mathcal{O}$-lattices, the Local-Global Principle does not hold in general. This leads to the following definition.

Definition 2.4.2 Let L be an $\mathcal{O}$-lattice in (V, Φ). The *class* and *genus* of L are

$$\begin{aligned} \operatorname{cls}(L) &:= \{L' \subset V \,;\, L' \text{ is an } \mathcal{O}\text{-lattice isometric to } L\}\,, \\ \operatorname{gen}(L) &:= \{L' \subset V \,;\, L' \text{ is an } \mathcal{O}\text{-lattice such that } L_{\mathfrak{p}} \cong L'_{\mathfrak{p}} \text{ for all } \mathfrak{p} \in \mathbb{P}(\mathfrak{o})\}\,. \end{aligned}$$

So it makes sense to say that the Local-Global Principle holds for some $\mathcal{O}$-lattice L in (V, Φ) if and only if $\operatorname{gen}(L) = \operatorname{cls}(L)$. In the indefinite case, one can usually tell a priori for which lattices the Local-Global Principle holds, see Chapter 5 for details. If (V, Φ) is definite, such a classification is much more difficult and it is actually the goal of this work. First, an algorithm to compute isometries will be given. This allows to decide if any $\mathcal{O}$-lattice L' lies in the same class as L.

Lemma 2.4.3 *Let L and L' be $\mathcal{O}$-lattices in (V, Φ). Further, let the $\mathbb{Q}$-algebra E be generated by the subset $\mathcal{B} \subset E$. Given $\alpha \in E$, the map*

$$F_\alpha \colon V \times V \to \mathbb{Q},\ (x, y) \mapsto \mathrm{T}_{K/\mathbb{Q}}(\mathrm{T}(\alpha\Phi(x, y)))\,.$$

defines a rational bilinear form on the $\mathbb{Q}$-vector space V. For any $\mathbb{Q}$-linear map $\sigma \colon V \to V$, the following statements are equivalent:

1. *σ is an isometry of the $\mathcal{O}$-lattices L and L'.*
2. *$\sigma(L) = L'$ and $F_\alpha(\sigma(x), \sigma(y)) = F_\alpha(x, y)$ for all $x, y \in V$ and all $\alpha \in \mathcal{B} \cup \{1\}$.*

Proof. Clearly, 1. implies 2. Suppose now 2. holds and let $\mathrm{T}_{E/K} := \mathrm{T}_{K/\mathbb{Q}} \circ \mathrm{T}$ denote the reduced trace of the $\mathbb{Q}$-algebra E. Since the algebra E is separable over $\mathbb{Q}$, the bilinear form

$$E \times E \to \mathbb{Q},\ (\alpha, \beta) \mapsto \mathrm{T}_{E/\mathbb{Q}}(\alpha\beta)$$

associated to $\mathrm{T}_{E/\mathbb{Q}}$ is non-degenerate, see [Rei03, Section 7c] for details. In particular, F_1 is non-degenerate. For $\alpha \in \mathcal{B}$ and $x, y \in V$ it follows that

$$F_1(\sigma(\alpha x), \sigma(y)) = F_1(\alpha x, y) = F_\alpha(x, y) = F_\alpha(\sigma(x), \sigma(y)) = F_1(\alpha\sigma(x), \sigma(y))\,.$$

Hence $\sigma(\alpha x) = \alpha\sigma(x)$. But then σ is E-linear, since $\mathcal{B}$ generates E as a $\mathbb{Q}$-algebra. Thus

$$\mathrm{T}_{E/\mathbb{Q}}(\alpha\Phi(x, y)) = F_\alpha(x, y) = F_\alpha(\sigma(x), \sigma(y)) = \mathrm{T}_{E/\mathbb{Q}}(\alpha\Phi(\sigma(x), \sigma(y)))$$

for all $x, y \in V$ and all $\alpha \in E$. Since the bilinear form of $\mathrm{T}_{E/\mathbb{Q}}$ is non-degenerate, it follows that $\sigma \in \mathbf{U}(V, \Phi)$. □

Remark 2.4.4 Suppose (V, Φ) is definite. Then:

1. The form F_1 of Lemma 2.4.3 is positive definite. Hence the number of isometries between two $\mathcal{O}$-lattices in (V, Φ) is finite.
2. In [PS97], W. Plesken and B. Souvignier present an algorithm to compute all isometries between two $\mathbb{Z}$-lattices preserving several rational bilinear forms, provided at least one of the forms is positive definite. Hence one can compute isometries and automorphism groups of $\mathcal{O}$-lattices in (V, Φ) using this algorithm and Lemma 2.4.3.
3. Let L be an $\mathcal{O}$-lattice in V. If E is commutative, then

$$\mu(E) \to \mathrm{Aut}(L),\ \varepsilon \mapsto (v \mapsto \varepsilon v)$$

is a monomorphism. Hence $\#\mu(E)$ divides $\#\,\mathrm{Aut}(L)$.

Theorem 2.4.5 *Let L be an $\mathcal{O}$-lattice in (V, Φ). Then there exist finitely many lattices $L_1, \dots, L_h \in \mathrm{gen}(L)$ such that $\mathrm{gen}(L) = \biguplus_{i=1}^{h} \mathrm{cls}(L_i)$. The number h is called the* class number *of $\mathrm{gen}(L)$ (or L) and will be denoted by $h(\mathrm{gen}(L))$ or $h(L)$.*

Proof. The theorem is a special case of a much more general result of A. Borel on algebraic groups [Bor63, Theorem 5.1]. Alternatively, it can also be deduced as follows. The assertion is true for indefinite spaces due to strong approximation, for details see Chapter 5. For definite spaces, the sum $\sum_{\mathrm{cls}(M)\in\mathrm{gen}(L)} \frac{1}{\#\operatorname{Aut}(M)}$ is a rational number by Siegel's Mass formula, c.f. Theorem 4.2.3. Further, the previous result shows that $\operatorname{Aut}(M)$ can be viewed as a finite subgroup of $\mathrm{GL}_{mn}(\mathbb{Q})$ and thus its order is bounded from above by some constant depending only of nm by a result of H. Minkowski [Min87]. Hence the class number is finite. □

Remark 2.4.6 Two genera G and G' of hermitian $\mathcal{O}$-lattices are said to be *similar*, if $G' = \{L^a\,;\, L \in G\}$ for some $a \in K^*$. Since similar genera necessarily share the same class number, the classification of all genera with a given class number reduces to the enumeration of all similarity classes of such genera. This will turn out to be a finite problem, provided that the rank of the lattices it not tiny, see Chapter 6 for details.

The concept of definite indecomposable lattices was introduced by M. Kneser for quadratic lattices over $\mathbb{Z}$. It readily generalizes to definite $\mathcal{O}$-lattices in (V,Φ). This is the last goal for this section.

Definition 2.4.7 Let L be an $\mathcal{O}$-lattice in (V,Φ). The lattice L is said to be *indecomposable*, if it cannot be written as an orthogonal sum $L = L_1 \perp L_2$ with $L_i \neq \{0\}$. A vector $v \in L$ is called *indecomposable*, if v cannot be written in the form $v = v_1 + v_2$ with $v_i \in L - \{0\}$ and $\Phi(v_1, v_2) = 0$.

Lemma 2.4.8 *Let L be an $\mathcal{O}$-lattice in (V,Φ). If (V,Φ) is definite, then every $x \in L$ is a sum of indecomposable vectors.*

Proof. Without loss of generality, L is integral. If x is indecomposable, there is nothing to show. If x is decomposable, then $x = x_1 + x_2$ with $x_i \in L - \{0\}$ and $\Phi(x_1, x_2) = 0$. In particular, $0 < \mathrm{T}_{K/\mathbb{Q}}(Q_\Phi(x_i)) < \mathrm{T}_{K/\mathbb{Q}}(Q_\Phi(x))$. The result follows by induction. □

Theorem 2.4.9 *Let L be an $\mathcal{O}$-lattice in (V,Φ). If (V,Φ) is definite, then L admits a unique orthogonal decomposition $L = \perp_{i=1}^r L_i$ into indecomposable lattices $L_1,\dots,L_r$.*

Proof. The proof follows [Kne02, Satz (27.2)]. Let $L = \perp_{i=1}^{\ell} L_i'$ be any orthogonal decomposition. If $x \in L$ is indecomposable, then $x \in L_i'$ for some i. Thus two indecomposable elements x and y with $\Phi(x,y) \neq 0$ are necessarily in the same summand L_i'. Two indecomposable elements $x, y \in L$ are said to be equivalent if and only if there exists some indecomposable elements $x = x_1, \dots, x_r = y \in L$ such that $\Phi(x_i, x_{i+1}) \neq 0$ for all $1 \le i < r$. This defines an equivalence relation on the set of indecomposable elements of L. Since the equivalence classes give rise to an orthogonal decomposition of (V,Φ) there are at most $m := \dim_E(V)$ such classes $K_1,\dots,K_k$ say. Denote by L_i the $\mathcal{O}$-submodule of L generated by K_i. Then $L = \perp_{i=1}^k L_i$ since each vector in L is a sum of indecomposable ones. Moreover, each component L_i is indecomposable and contained

in L'_j for some j.
To prove the uniqueness, assume that all L'_j are also indecomposable. For $1 \leq j \leq \ell$ let $I_j = \{1 \leq i \leq k \mid L_i \subseteq L'_j\}$ and set $M_j := \oplus_{i \in I_j} L_i \subseteq L'_j$. It suffices to show that $L'_j = M_j$ for all j since then $|I_j| = 1$. Let $x \in L'_j$. Write $x = \sum_{i=1}^{l} x_i$ with $x_i \in M_i \subseteq L'_i$ for all i. Since $\oplus_{i=1}^{\ell} L'_i = L$ this implies $x_i = 0$ for all $i \neq j$. So $M_j = L'_j$ as claimed. □

3 Hermitian lattices over complete discrete valuation rings

The aim of this chapter is to give a brief overview on the classification of hermitian forms over complete discrete valuation rings.

Unless stated otherwise, the field K will be complete with respect to a surjective, discrete valuation $\operatorname{ord}\colon K \to \mathbb{Z} \cup \{\infty\}$. Let $\mathfrak{o} = \{a \in K\,;\, \operatorname{ord}(a) \geq 0\}$ be the corresponding valuation ring and let $\mathfrak{p} = p\mathfrak{o} = \{a \in K\,;\, \operatorname{ord}(a) > 0\}$ be the maximal ideal of $\mathfrak{o}$. Further, the residue class field $\mathfrak{o}/\mathfrak{p}$ is always assumed to be finite.

3.1 Local fields

Let q be the order of the residue class field $\mathfrak{o}/\mathfrak{p}$. The order of the quotient group $\mathfrak{o}/(\mathfrak{o}^*)^2$ equals $2q^{\operatorname{ord}(2)}$, see [O'M73, 63:9] for details. In particular, if K is *non-dyadic*, i.e. $2 \in \mathfrak{o}^*$, then $\mathfrak{o}/(\mathfrak{o}^*)^2$ is isomorphic to C_2. If K is *dyadic* however, the quotient $\mathfrak{o}^*/(\mathfrak{o}^*)^2$ is much larger. In this case an additional invariant, the so called quadratic defect, will be needed for the classification of hermitian lattices. However, there is no need to make a general assumption on the characteristic of $\mathfrak{o}/\mathfrak{p}$ right now since most of the results in this section hold whether K is dyadic or not.

Definition 3.1.1 Let $a \in K$. The *quadratic defect* $\mathfrak{d}(a)$ of a is

$$\mathfrak{d}(a) := \bigcap_{b \in K} (a - b^2)\mathfrak{o}\ .$$

Lemma 3.1.2 *Let $a, b \in K$.*

1. *Then $\mathfrak{d}(ab^2) = b^2\mathfrak{d}(a)$ and $\mathfrak{d}(a) = (0)$ if and only if a is a square.*

2. *If $a \in \mathfrak{o}$, then $\mathfrak{d}(a)$ is the smallest ideal $\mathfrak{a}$ of $\mathfrak{o}$ such that a is a square modulo $\mathfrak{a}$.*

3. *If $\operatorname{ord}(a)$ is odd or ∞, then $\mathfrak{d}(a) = a\mathfrak{o}$. The converse is true for dyadic fields K.*

4. *If $a \in \mathfrak{o}^*$, then $\mathfrak{d}(a)$ is one of the ideals*

$$(0) \subsetneq 4\mathfrak{o} \subsetneq 4\mathfrak{p}^{-1} \subsetneq 4\mathfrak{p}^{-3} \cdots \subsetneq \mathfrak{p}^3 \subsetneq \mathfrak{p}\ .$$

Conversely, every such ideal is the quadratic defect of some element in $\mathfrak{o}^*$. More precisely, if $1 \leq v < \operatorname{ord}(4)$ is odd and $u \in \mathfrak{o}^*$, then $\mathfrak{d}(1 + p^v u) = \mathfrak{p}^v$. The existence of a unit of quadratic defect $4\mathfrak{o}$ follows from Theorem 3.1.7 and the fact that K admits an unramified quadratic field extension.

Proof. A proof of these assertions is given in [O'M73, Section 63]. □

Quadratic defects can be computed efficiently using the following lifting argument.

Algorithm 3.1.3 QUADRATICDEFECT(a)

Input: Some element $a \in K$.
Output: The quadratic defect $\mathfrak{d}(a)$.

```
 1: if $\operatorname{ord}(a)$ is odd or $\infty$ then return $a\mathfrak{o}$.
 2: if $\operatorname{ord}(a) \neq 0$ then return $a \cdot$ QUADRATICDEFECT($a/p^{\operatorname{ord}(a)}$).
 3: if $\operatorname{ord}(2) = 0$ then return $(0)$ if $a$ is a square mod $\mathfrak{p}$ and return $\mathfrak{o}$ otherwise.
 4: Compute $s \in \mathfrak{o}^*$ such that $s^2 a \equiv 1 \pmod{\mathfrak{p}}$. Replace $a$ by $as^2$.
 5: Set $v = \operatorname{ord}(a-1) \geq 1$.
 6: while $v < \operatorname{ord}(4)$ and $v$ is even do
 7:     Compute $s \in \mathfrak{o}^*$ such that $s^2 \equiv (a-1)/p^v \pmod{\mathfrak{p}}$.
 8:     Replace $a$ by $a/(1+sp^{v/2})^2$ and set $v = \operatorname{ord}(a-1)$.
 9: end while
10: if $v < \operatorname{ord}(4)$ is odd then
11:     return $\mathfrak{p}^v$.
12: else if $v = \operatorname{ord}(4)$ and $X^2 + X + (a-1)/4 \in (\mathfrak{o}/\mathfrak{p})[X]$ is irreducible then
13:     return $4\mathfrak{o}$.
14: else
15:     return $(0)$.
16: end if
```

Proof. By Lemma 3.1.2, the first three steps are correct. So one may suppose that K is dyadic and $a \in \mathfrak{o}^*$. Lines 6–9 replace a with some element in the same square class (which does not affect the quadratic defect) such that $\operatorname{ord}(a-1)$ gets larger in each iteration. In particular, the algorithm terminates. By Hensel's Lemma, $\mathfrak{d}(a) = (0)$ whenever $v > \operatorname{ord}(4)$ and Lemma 3.1.2 shows that $\mathfrak{d}(a) = \mathfrak{p}^v$ whenever $v < \operatorname{ord}(4)$ is odd. This leaves only the case $a = 1 - 4\delta$ with $\delta \in \mathfrak{o}^*$. Again, the previous Lemma shows that $\mathfrak{d}(a) = 4\mathfrak{o}$ or a is a square. By Hensel's Lemma, the latter condition holds if and only if $(1-4\delta) \equiv (1+2x)^2 \pmod{4\mathfrak{p}}$ has a solution $x \in \mathfrak{o}$. But this is equivalent to $X^2 + X + \delta \in (\mathfrak{o}/\mathfrak{p})[X]$ being reducible. □

Remark 3.1.4 The proof of Algorithm 3.1.3 shows the following.

1. Let $a \in \mathfrak{o}^*$. Then there exists some $u \in \mathfrak{o}^*$ such that $u^2 a = 1 + d$ for some $d \in \mathfrak{o}$ with $d\mathfrak{o} = \mathfrak{d}(x)$.

2. Let $\Delta = 1 + 4\varrho \in \mathfrak{o}^*$ such that $\mathfrak{d}(\Delta) = \varrho\mathfrak{o} = 4\mathfrak{o}$. Let $f(X) = X^2 + uX + u^2\varrho \in \mathfrak{o}[X]$ with $u \in \mathfrak{o}^*$. Then the image of f under the canonical epimorphism $\mathfrak{o}[X] \to (\mathfrak{o}/\mathfrak{p})[X]$ is irreducible. By Hensel's Lemma, f itself must be irreducible.

Lemma 3.1.5 *Let F be a field such that*

- *F is finite or*

- *F is a non-dyadic local field which is complete with respect to a disrete valuation and whose residue class field is finite.*

Then $F = \{x^2 + y^2\,;\, x, y \in F\}$.

Proof. By Hensel's Lemma, one may assume that $q := |F|$ is finite. The case that q is even is trivial. Suppose now that q is odd. If F^2, the set of squares in F, is closed under addition, it would be a subgroup of $(F, +)$. But this is impossible, since $\#F^2 = \frac{q+1}{2}$ does not divide q. □

Definition 3.1.6 For non-zero elements a, b in a local field F, the *Hilbert symbol* is defined as

$$(a, b) := \begin{cases} +1 & \text{if } ax^2 + by^2 = z^2 \text{ has a non-zero solution } (x, y, z) \in F^3, \\ -1 & \text{otherwise.} \end{cases}$$

So $(a, b) = +1$ if and only if the quadratic form $\langle a, b\rangle$ represents 1. Hence $(a, b) = +1$ for all $a, b \in \mathbb{C}$. Similarly, if $F = \mathbb{R}$, then $(a, b) = -1$ if and only if a, b are both negative.

Theorem 3.1.7 *Let $\Delta \in \mathfrak{o}^*$ be an element of quadratic defect $4\mathfrak{o}$.*

1. $(a, \Delta) = (-1)^{\operatorname{ord}(a)}$ *for all $a \in K^*$.*

2. *If K is non-dyadic and $a, b \in K$ such that* $\operatorname{ord}(a) \equiv \operatorname{ord}(b) \equiv 0 \pmod 2$, *then* $(a, b) = +1$.

3. *The Hilbert symbol is a symmetric, non-degenerate bilinear form on the $\mathbb{F}_2$-vector space $K^*/(K^*)^2$. Non-degenerate means that if $a \in K^* - (K^*)^2$ then $(a, b) = -1$ for some $b \in K^*$.*

4. *If $E \cong K[x]/(x^2 - a)$ for some $a \in K^*$, then $b \in \mathrm{N}(E^*)$ if and only if $(a, b) = 1$.* *In particular,* $K^*/\,\mathrm{N}(E^*) \cong \begin{cases} C_1 & \text{if } a \in (K^*)^2, \\ C_2 & \text{if } a \notin (K^*)^2. \end{cases}$

5. *The field $E = K(\sqrt{\Delta})$ is the unique unramified quadratic extension of K and* $\mathrm{N}(E^*) = \{a \in K^*\,;\, \operatorname{ord}(a) \in 2\mathbb{Z}\}$. *In particular,* $\{a \in \mathfrak{o}^*\,;\, \mathfrak{d}(a) = 4\mathfrak{o}\} = \Delta(\mathfrak{o}^*)^2$.

Proof. For a proof the first assertion, see [O'M73, 63.11a]. For the second, one may assume that $a, b \in \mathfrak{o}^*$. Moreover, there is nothing to show if a or b is a square. So without loss of generality $a = b$. But then $\langle a, b\rangle$ represents 1 by Lemma 3.1.5.
3. The Hilbert symbol is certainly symmetric and depends only on the square classes of a and b. The linearity follows from the characterization in 4. using relative norms. The proof on the non-degeneracy is more involved. By 1. one may assume that $a \in \mathfrak{o}^*$. Without loss of generality, $\Delta \equiv 1 \pmod{4\mathfrak{o}}$ and $a = 1 + c$ such that $c\mathfrak{o} = \mathfrak{d}(a)$. Again by 1., the case $c\mathfrak{o} \subsetneq 4\mathfrak{o}$ is trivial. So only the case that K is dyadic and $\operatorname{ord}(c)$ is odd remains. Let $b := \Delta - a$. Then $\langle a, b\rangle \cong \langle \Delta, \Delta ab\rangle$ shows that

$$(a, b) = (\Delta, \Delta ab) = (-1)^{\operatorname{ord}(\Delta ab)} = (-1)^{\operatorname{ord}(b)} = (-1)^{\operatorname{ord}(c)} = -1\,.$$

The fourth assertion is now clear. Further, $E = K(\sqrt{a})$ is unramified over K if and only if $\mathrm{N}(E^*) = \{a \in K^* \,;\, \mathrm{ord}(a) \in 2\mathbb{Z}\}$. By 1. and 3. the latter condition is equivalent to $a \in \Delta(K^*)^2$. This proves the last part. □

Theorem 3.1.8 *Let* $E = \left(\frac{a,b}{F}\right)$ *be a quaternion algebra over some local field* F *of characteristic* 0 *and let* $E^0 := \{\alpha \in E \,;\, \mathrm{tr}_{E/F}(\alpha) = 0\}$ *be its trace zero subspace.*

1. *The following statements are equivalent:*

   a) E *is a skewfield.*

   b) *The quaternary quadratic space* $(E, \mathrm{nr}_{E/F})$ *over* F *is anisotropic.*

   c) *The ternary quadratic space* $(E^0, \mathrm{nr}_{E/F})$ *over* F *is anisotropic.*

   d) $(a, b) = -1$.

2. *If* $F = \mathbb{R}$*, then* E *is a skewfield if and only if* $E \cong \left(\frac{-1,-1}{\mathbb{R}}\right)$.

3. *If* $F = K$*, then the quadratic space* $(E, \mathrm{nr}_{E/K})$ *is universal, i.e.* $\mathrm{nr}_{E/K}(E^*) = K^*$*. Moreover,* E *is a skewfield if and only if* $E \cong \left(\frac{\Delta,p}{K}\right)$.

Proof. 1. The Structure Theorem of Artin-Wedderburn implies that the F-algebra E is either a skewfield or isometric to $F^{2\times 2}$. Hence a), b) and c) are certainly equivalent. Further, $(E^0, \mathrm{nr}_{E/F}) \cong \langle -a, -b, ab\rangle$ is anisotropic if and only if $\langle b, a, 1\rangle$ is so. But the latter condition is equivalent to $(a, b) = -1$.
2. The first assertion shows that $E = \left(\frac{a,b}{\mathbb{R}}\right)$ is a skewfield if and only if $a, b < 0$. If this is the case, then $E \cong \left(\frac{-1,-1}{\mathbb{R}}\right)$.
3. The previous theorem and part 1d) show that $\left(\frac{\Delta,p}{K}\right)$ is a skewfield. The fact that all quaternion skewfields over K are isometric follows from the structure of the Brauer group of K, see for example [Rei03, Theorem 31.8]. Finally, if $E \cong K^{2\times 2}$ then clearly $\mathrm{nr}_{E/K}(E^*) = K^*$ and if $E \cong \left(\frac{\Delta,p}{K}\right)$ then $\mathrm{nr}_{E/K}(E^*)$ contains $-p$ as well as $\{x \in K^* \,;\, \mathrm{ord}(x) \in 2\mathbb{Z}\}$. Thus $\mathrm{nr}_{E/K}(E^*) = K^*$ for any quaternion algebra E over K. □

Note that Hilbert symbols can be evaluated efficiently as explained in [Voi13]. Thus, given $b \in K^*$, one can constructively decide if $b \in \mathrm{N}(E^*)$ as follows.

1. If $E = K$, then $b \in \mathrm{N}(E^*) = (K^*)^2$ if and only if $\mathfrak{d}(a) = (0)$.

2. If $E = K[x]/(x^2 - a)$ then $b \in \mathrm{N}(E^*)$ if and only if $(a, b) = 1$.

3. If E is a quaternion algebra over K, then $b \in \mathrm{N}(E^*)$.

3.2 Hermitian spaces over local fields

This section recalls the well known classification of hermitian spaces over K.

Definition 3.2.1 Let $(V,\Phi) \cong \langle a_1,\dots,a_m\rangle$ be a regular quadratic space over $E = K$.

1. The *Hasse invariant* $\mathrm{c}(V,\Phi) := \prod_{i<j}(a_i,a_j) \in \{\pm 1\}$ is independent of the chosen orthogonal basis.
2. The *Witt invariant* is defined by

$$\omega(V,\Phi) := \begin{cases} \mathrm{c}(V,\Phi) & \text{if } m \equiv 1,2 \pmod 8, \\ \mathrm{c}(V,\Phi)\cdot(-1,-\det(\Phi)) & \text{if } m \equiv 3,4 \pmod 8, \\ \mathrm{c}(V,\Phi)\cdot(-1,-1) & \text{if } m \equiv 5,6 \pmod 8, \\ \mathrm{c}(V,\Phi)\cdot(-1,\det(\Phi)) & \text{if } m \equiv 7,0 \pmod 8. \end{cases}$$

Theorem 3.2.2 *The isometry type of any regular quadratic space (V,Φ) over K is uniquely determined by its rank m, its determinant d and its Hasse invariant* c. *Further, (V,Φ) is isotropic if and only if either*

- $m = 2$ *and* $-d \in (K^*)^2$.
- $m = 3$ *and* $\mathrm{c} = (-1,-d)$.
- $m = 4$ *and* ($d \notin (K^*)^2$ *or* $\mathrm{c} = (-1,-1)$).
- $m \geq 5$.

Proof. See for example [O'M73, Chapter 63]. □

The previous result shows that there is a unique anisotropic, quaternary quadratic space over K (up to isometry). By Theorem 3.1.8, this space must be a quaternion skew field over K equipped with its reduced norm form and it is universal.

Theorem 3.2.3 *Let (V,Φ) be a regular hermitian form over $E \neq K$ of rank m and determinant d.*

1. *If* $\dim_K(E) = 2$, *then* $(V,\Phi) \cong \langle 1,\dots,1,d\rangle$.
2. *If* $\dim_K(E) = 4$, *then* $(V,\Phi) \cong \langle 1,\dots,1\rangle$.

In particular, the isometry type of (V,Φ) is uniquely determined by m and $d \in K^*/\,\mathrm{N}(E^*)$.

Proof. By Theorem 2.1.4, $(V,\Phi) \cong \langle a_1,\dots,a_m\rangle$ for some $a_i \in K^*$. Thus the result is certainly true whenever $\mathrm{N}(E^*) = K^*$. So only the case that E/K is a quadratic field extension remains. Without loss of generality one may assume that $m = 2$. It suffices to show that Φ represents 1. This is certainly the case if Φ is isotropic. If Φ and thus Q_Φ are non-isotropic, then Φ is universal by the comment just before this theorem. So Φ represents 1 in any case. □

Corollary 3.2.4 *Let (V, Φ) be a regular hermitian form over $E \neq K$ of rank m and determinant d.*

1. *If $\dim_K(E) = 2$, then (V, Φ) is isotropic if and only if either*
   - *$m = 2$ and $-d \in \mathrm{N}(E^*)$ or*
   - *$m \geq 3$.*
2. *If $\dim_K(E) = 4$, then (V, Φ) is isotropic if and only if $m \geq 2$.*

Proof. This follows immediately from the previous theorem. □

3.3 Jordan decompositions

Let $\Delta = 1 - 4\varrho \in \mathfrak{o}^*$ such that $\mathfrak{d}(\Delta) = 4\varrho\mathfrak{o} = 4\mathfrak{o}$. In this section, the following conventions will be used.

- If E/K is an unramified quadratic field extension, then $E = K(\sqrt{\Delta})$.
- If E is a quaternion skewfield over K, then $E = \left(\frac{\Delta, p}{K}\right)$.
- If E is a (skew-)field, then $\mathcal{O}$ denotes the maximal $\mathfrak{o}$-order in E and Ord is the usual surjective, discrete valuation of E with valuation ring $\mathcal{O}$.
- If $E = K \oplus K$, let $\mathcal{O} = \mathfrak{o} \oplus \mathfrak{o}$ and let $\mathrm{Ord}\colon E \to \mathbb{Z} \cup \{\infty\}$, $(a, b) \mapsto \min(\mathrm{ord}(a), \mathrm{ord}(b))$.
- If $E = K^{2\times 2}$, let $\mathcal{O} = \mathfrak{o}^{2\times 2}$ and let

$$\mathrm{Ord}\colon E \to \mathbb{Z} \cup \{\infty\},\ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \min(\mathrm{ord}(a), \mathrm{ord}(b), \mathrm{ord}(c), \mathrm{ord}(d))\ .$$

Let $\mathfrak{P} = \pi\mathcal{O}$ be the largest integral twosided ideal of $\mathcal{O}$ that contains $\mathfrak{p}\mathcal{O}$ and that is invariant under the involution $\overline{}$.

- Given $a, b \in K$, let $A(a, b)$ denote the matrix $\left(\begin{smallmatrix} a & 1 \\ 1 & b \end{smallmatrix}\right)$.
- For any integer i, let $H(i)$ be a binary hermitian $\mathcal{O}$-lattice with Gram matrix $\left(\begin{smallmatrix} 0 & \pi^i \\ \overline{\pi}^i & 0 \end{smallmatrix}\right)$. Further, for any non-negative integer r, let $H(i)^r$ denote the orthogonal sum of r copies of $H(i)$.

Finally, (V, Φ) denotes some regular hermitian space over E.

3.3.1 The generic case

Definition 3.3.1 An orthogonal sum $\perp_{i=1}^{t} L_i$ of $\mathcal{O}$-lattices in (V, Φ) is called a *Jordan decomposition* if the sublattices L_i are $\mathfrak{P}^{s_i}$-modular such that $s_1 < s_2 < \ldots < s_t$. Two Jordan decompositions $\perp_{i=1}^{t} L_i$ and $\perp_{i=1}^{t'} L'_i$ are said to be of the same *Jordan type* if $t = t'$ and for $1 \leq i \leq t$ the following conditions hold:

1. $\operatorname{rank}(L_i) = \operatorname{rank}(L'_i)$.
2. $\mathfrak{s}(L_i) = \mathfrak{s}(L'_i)$.
3. $\mathfrak{n}(L_i)\mathcal{O} = \mathfrak{s}(L_i)$ if and only if $\mathfrak{n}(L'_i)\mathcal{O} = \mathfrak{s}(L'_i)$.

The fact that every $\mathcal{O}$-lattice in (V, Φ) has some Jordan decomposition follows from the following algorithm.

Algorithm 3.3.2 JordanDecomposition(L)
Input: An $\mathcal{O}$-lattice L in (V, Φ).
Output: An orthogonal decomposition of L into modular sublattices of rank at most 2.

```
Let $(e_1, \ldots, e_m)$ be an $\mathcal{O}$-basis of $L$.
Set $o := \min\{\mathrm{Ord}(\Phi(e_k, e_\ell))\,;\, 1 \leq k, \ell \leq m\}$.
Let $(i, j) \in \{1, \ldots, m\}^2$ with $i = j$ if possible, such that $\mathrm{Ord}(\Phi(e_i, e_j)) = o$.
if $i \neq j$ and there exists some $\lambda \in \mathcal{O}$ such that $\mathrm{Ord}(\mathrm{T}(\lambda\Phi(e_i, e_j))) = o$ then
    Replace $e_i$ by $e_i + \overline{\lambda} e_j$
    Set $j := i$.
end if
if i=j then
    Swap $e_1$ with $e_i$.
    for $2 \leq k \leq m$ do
        Replace $e_k$ by $e_k - \frac{\Phi(e_k, e_1)}{\Phi(e_1, e_1)} e_1$.
    end for
    Set $r := 1$.
else
    Swap $e_1$ with $e_{\min\{i,j\}}$ and $e_2$ with $e_{\max\{i,j\}}$.
    for $3 \leq k \leq m$ do
        Replace $e_k$ by
            $$e_k - \frac{\Phi(e_k, e_2)\Phi(e_2, e_1) - \Phi(e_k, e_1)\Phi(e_2, e_2)}{\mathrm{N}(\Phi(e_1, e_2)) - \Phi(e_1, e_1)\Phi(e_2, e_2)} e_1 - \frac{\Phi(e_k, e_1)\Phi(e_1, e_2) - \Phi(e_k, e_2)\Phi(e_1, e_1)}{\mathrm{N}(\Phi(e_1, e_2)) - \Phi(e_1, e_1)\Phi(e_2, e_2)} e_2 \,.$$
    end for
    Set $r := 2$.
end if
return $\sum_{i \leq r} \mathcal{O} e_i \perp$ JordanDecomposition($\sum_{i > r} \mathcal{O} e_i$).
```

Theorem 3.3.3 *Every $\mathcal{O}$-lattice L in (V,Φ) admits a Jordan decomposition. Further, any two Jordan decompositions of L are of the same Jordan type.*

Proof. The existence follows from Algorithm 3.3.2. For the uniqueness, note that the proof given by O'Meara in [O'M73, Theorem 91.9] for the quadratic case carries over unchanged. □

In most cases, such an element λ from line 4 of Algorithm 3.3.2 exists. Below are some partial results.

Lemma 3.3.4 *Let $\alpha \in E$ such that* $\mathrm{Ord}(\alpha) = o$.

1. *If $E = K$ is non-dyadic, then* $\mathrm{Ord}(\mathrm{T}(1 \cdot \alpha)) = o$.
2. *If E/K is an unramified quadratic field extension, then* $\mathrm{Ord}(\mathrm{T}(\lambda\alpha)) = o$ *for*
$$\lambda = p^o/\alpha \cdot \begin{cases} 1 & \textit{if } K \textit{ is non-dyadic,} \\ \frac{1+\sqrt{\Delta}}{2} & \textit{if } K \textit{ is dyadic.} \end{cases}$$
3. *If E/K is a ramified quadratic extension, K is non-dyadic and i is even, then* $\mathrm{Ord}(\mathrm{T}(\lambda\alpha)) = o$ *for* $\lambda = p^{\frac{o}{2}}/\alpha \in \mathcal{O}^*$.
4. *If $E \cong K \times K$ or $E \cong K^{2\times 2}$, then* $\mathrm{Ord}(\mathrm{T}(\lambda\alpha)) = o$ *for some idempotent $\lambda \in \mathcal{O}$.*
5. *If E is a quaternion skewfield and o is even, then* $\mathrm{Ord}(\mathrm{T}(\lambda\alpha)) = o$ *for*
$$\lambda = p^{\frac{o}{2}} \cdot \begin{cases} \alpha^{-1} & \textit{if } K \textit{ is non-dyadic,} \\ \frac{1+\sqrt{\Delta}}{2}\alpha^{-1} & \textit{if } K \textit{ is dyadic.} \end{cases}$$

Proof. This follows from direct verifications. □

The above result immediately yields a classification of modular lattices in almost all cases.

Proposition 3.3.5 *Let L be a $\mathfrak{P}^i$-modular $\mathcal{O}$-lattice in (V,Φ).*

1. *If $E = K$ is non-dyadic, then $L \cong \langle p^i, \dots, p^i, \det(L)p^{i(1-m)}\rangle$.*
2. *If $E \cong K \times K$ or $E \cong K^{2\times 2}$ or E/K is an unramified quadratic field extension then $L \cong \langle p^i, \dots, p^i\rangle$.*
3. *If E/K is a ramified quadratic field extension, K is non-dyadic and i is even, then $L \cong \langle p^{i/2}, \dots, p^{i/2}, \det(L)p^{i(1-r)/2}\rangle$.*
4. *If E is a quaternion skewfield and i is even, then $L \cong \langle p^{i/2}, \dots, p^{i/2}\rangle$.*
5. *If E/K is a ramified quadratic field extension, K is non-dyadic and i is odd, then m is even and $L \cong H(i)^{m/2}$.*

6. *If E is a quaternion skewfield over K and i is odd, then m is even and $L \cong H(i)^{m/2}$.*

Proof. 1.–4.: From Algorithm 3.3.2 and Lemma 3.3.4 it follows that L admits an orthogonal basis. Thus 2. and 4. follow immediately from $\mathrm{N}(\mathcal{O}^*) = \mathfrak{o}^*$. For the proof of 1. and 3., it suffices to show that the form $\langle \varepsilon, \varepsilon \rangle$ represents 1 where $\varepsilon \in \mathfrak{o}^*$ denotes some non-square. But this follows immediately from Lemma 3.1.5.
5.–6.: Since i is odd, no rank-one submodule of L has an orthogonal complement in L. From Algorithm 3.3.2 it follows that m is even. So it suffices to discuss the case $m = 2$. After rescaling, one may also assume that $i = 1$. Thus L has a Gram matrix $\left(\begin{smallmatrix} a & \pi \\ \overline{\pi} & b \end{smallmatrix}\right)$ for some $a, b \in \mathfrak{p}$. But then $\det(V, \Phi) = ab - \mathrm{N}(\pi) = -\mathrm{N}(\pi)(1 + c)$ for some $c \in \mathfrak{p}$. Corollary 3.2.4 shows that (V, Φ) must be isotropic. Let x be some primitive, isotropic vector of L. Then L admits some $\mathcal{O}$-basis (x, y) with corresponding Gram matrix $\left(\begin{smallmatrix} 0 & \pi \\ \overline{\pi} & d \end{smallmatrix}\right)$ for some $d \in \mathfrak{p}$. Let

$$\lambda = \begin{cases} \frac{(1+\sqrt{\Delta})}{2} d\pi^{-1} & \text{if } \dim_K(E) = 4 \text{ and } K \text{ is dyadic,} \\ \frac{1}{2} d\pi^{-1} & \text{otherwise.} \end{cases}$$

Then $\lambda \in \mathcal{O}$ and the $\mathcal{O}$-basis $(x, y - \lambda x)$ of L has Gram matrix $\left(\begin{smallmatrix} 0 & \pi \\ \overline{\pi} & 0 \end{smallmatrix}\right)$. □

The previous result allows a classification of hermitian $\mathcal{O}$-lattices in all but two cases.

Theorem 3.3.6 *Let (V, Φ) and (V', Φ') be hermitian spaces over E. Let $L = \perp_{i=1}^{t} L_i$ and $L' = \perp_{i=1}^{t'} L'_i$ be Jordan decompositions of $\mathcal{O}$-lattices in (V, Φ) and (V', Φ') respectively. Suppose that E does* not *satisfy any of the following two conditions.*

- *$E = K$ is dyadic.*
- *E is a ramified quadratic field extension of the dyadic field K.*

Then the following statements are equivalent.

1. *The lattices L and L' are isometric.*
2. *The lattices L_i and L'_i are isometric for all $1 \le i \le t = t'$.*
3. *The hermitian spaces (EL_i, Φ_i) and (EL'_i, Φ'_i) are isometric for all $1 \le i \le t = t'$. Here Φ_i and Φ'_i denote the restrictions of Φ and Φ' to EL_i and EL'_i respectively.*
4. *The hermitian spaces (V, Φ) and (V', Φ') are isometric, L and L' are of the same Jordan type and the following assertions hold.*
   - *If $E = K$ then $\det(L_i)/\det(L'_i) \in (\mathfrak{o}^*)^2$ for all $1 \le i \le t$.*
   - *If E/K is a ramified field extension then $\det(L_i)/\det(L'_i) \in \mathrm{N}(\mathcal{O}^*)$ for all $1 \le i \le t$ with $\mathfrak{s}(L_i)$ is even.*

Proof. Proposition 3.3.5 and the classification of hermitian spaces over local fields given in Section 3.2 show that 2., 3. and 4. are equivalent. Moreover, 2. certainly implies 1. Suppose now 1. holds. Let $\varphi \colon L \to L'$ be an isometry. By Theorem 3.3.3, isometric lattices are of the same Jordan type. Hence Proposition 3.3.5 shows that L and L' are isometric whenever $E \neq K$ and E/K is a not a ramified quadratic field extension. Suppose now $E = K$ or E/K is a ramified quadratic field extension. Then $L_1/\mathfrak{P}L_1$ and $L_1'/\mathfrak{P}L_1'$ are hermitian spaces over $\mathcal{O}/\mathfrak{P}$ of the same rank. Let $\tau \colon L' \to L_1'$ be the canonical projection. Then

$$L_1/\mathfrak{P}L_1 \to L_1'/\mathfrak{P}L_1,\ x + \mathfrak{p}L_1 \mapsto \tau(\varphi(x)) + \mathfrak{p}L_1'$$

induces an isometry of hermitian spaces and thus $\det(L_1) \equiv \det(L_1) \pmod{\mathfrak{p}}$. Hence $\det(L_1)/\det(L_1) \in \mathrm{N}(\mathcal{O}^*)$. The same argument applied to $L^{\mathfrak{s}(L_i)}$ and $(L')^{\mathfrak{s}(L_i)}$ shows that $\det(L_i)/\det(L_i) \in \mathrm{N}(\mathcal{O}^*)$ for all $2 \le i \le t$. □

The two remaining cases are much more involved. They will be discussed in the next sections.

3.3.2 The quadratic, dyadic case

In this section, let $E = K$ be dyadic. The classification of quadratic lattices over K is due to T. O'Meara. In this case, more invariants are needed to distinguish the isometry classes of $\mathfrak{o}$-lattices.

Definition 3.3.7 Let L be an $\mathfrak{o}$-lattice in (V, Φ) and let $\mathfrak{a}$ be a fractional ideal of $\mathfrak{o}$.

1. For $a, b \in K^*$, the equivalence relation $a \cong b \mod \mathfrak{a}$ is defined as
$$a/b \in \mathfrak{o}^* \quad \text{and} \quad \mathfrak{d}(a/b) \subseteq \mathfrak{a}/b\,.$$
2. The *norm group* $\mathfrak{g}(L)$ is the additive subgroup $Q_\Phi(L) + 2\mathfrak{s}(L)$ of $(K, +)$. An element $\alpha \in \mathfrak{g}(L)$ is called a *norm generator* of L if $\alpha\mathfrak{o} = \mathfrak{n}(L)$.
3. Since $2\mathfrak{s}(L) \subseteq \mathfrak{g}(L)$, there exists a maximal fractional ideal $\mathfrak{m}(L)$ contained in $\mathfrak{g}(L)$. Then the *weight* $\mathfrak{w}(L)$ is the fractional ideal $2\mathfrak{s}(L) + \mathfrak{p}\mathfrak{m}(L)$.

Proposition 3.3.8 *The scale, norm and weight of an $\mathfrak{o}$-lattice L in (V, Φ) satisfy the following conditions.*

1. $2\mathfrak{s}(L) \subseteq \mathfrak{w}(L) \subseteq \mathfrak{g}(L) \subseteq \mathfrak{n}(L) \subseteq \mathfrak{s}(L)$.
2. $\mathfrak{w}(L) = \mathfrak{n}(L)$ *if and only if* $\mathfrak{n}(L) = 2\mathfrak{s}(L)$.
3. *If* $\mathrm{ord}(\mathfrak{n}(L)) + \mathrm{ord}(\mathfrak{w}(L))$ *is even, then* $\mathfrak{w}(L) = 2\mathfrak{s}(L)$.

Proof. See [O'M73, Section 93]. □

Norm generators and weights can be computed easily using the following result.

Lemma 3.3.9 *Let L be a $\mathfrak{o}$-lattice in (V, Φ) with basis $(x_1, \dots, x_m)$.*

1. *If $\mathfrak{n}(L) = 2\mathfrak{s}(L)$ let α be any generator of $\mathfrak{n}(L)$; otherwise let $\alpha = Q_\Phi(x_i)$ for some $1 \leq i \leq m$ that makes $\alpha\mathfrak{o}$ maximal. Then α is a norm generator of L.*

2. *If α' is any norm generator of L, then*

$$\mathfrak{w}(L) = 2\mathfrak{s}(L) + \sum_{j=1}^{m} \alpha' \mathfrak{d}(Q_\Phi(x_j)/\alpha') \,.$$

3. *$\gamma \in K$ is a norm generator of L if and only if $\alpha \cong \gamma \mod \mathfrak{w}(L)$.*

Proof. See [O'M73, Section 93]. □

Norm generators and weights are enough to distinguish isometry classes of modular lattices.

Theorem 3.3.10 *Let $i \in \mathbb{Z}$. Let L and L' be $\mathfrak{p}^i$-modular $\mathfrak{o}$-lattices in (V, Φ) with norm generators α and α' respectively. Then the following statements are equivalent:*

1. *L and L' are isometric.*

2. *L and L' represent the same numbers, i.e. $\mathfrak{g}(L) = \mathfrak{g}(L')$.*

3. *$\mathfrak{w}(L) = \mathfrak{w}(L')$ and $\alpha \cong \alpha' \mod \mathfrak{w}(L)$.*

Proof. See [O'M73, Theorem 93:16 and 93:4]. □

Proposition 3.3.11 *Let L be a unimodular lattice in (V, Φ) with determinant $d \in \mathfrak{o}^*$ and weight $\mathfrak{w}(L) = \mathfrak{p}^b$. Let $\Delta = 1 - 4\varrho \in \mathfrak{o}^*$ such that $\mathfrak{d}(\Delta) = 4\varrho\mathfrak{o} = 4\mathfrak{o}$.*

1. *If $m = \dim_K(V) = 2r + 1$ is odd, then either $b = e$ or $b < e$ is odd.*

   a) *If $\omega(V, \Phi) = +1$, then*

   $$L \cong \langle A(p^b, 0) \rangle \perp \langle (-1)^r d \rangle \perp H(0)^{r-1} \,.$$

   b) *If $\omega(V, \Phi) = -1$, then $b < e$ and*

   $$L \cong \langle A(p^b, 4\varrho p^{-b}) \rangle \perp \langle \Delta^{-1}(-1)^r d \rangle \perp H(0)^{r-1} \,.$$

2. *Suppose $m = \dim_K(V) = 2r$ is even. Let α be a norm generator of L and let $\gamma \in \mathfrak{o}$ such that $\operatorname{disc}(L) = (1 + \gamma) \cdot (\mathfrak{o}^*)^2$ and $\mathfrak{d}(1 + \gamma) = \gamma\mathfrak{o}$. Then $\gamma \in \mathfrak{n}(L)\mathfrak{w}(L)$ and L is isometric to one of the following lattices.*

   a) *If $\operatorname{ord}(\alpha) + b$ is even, then $b = e$ and*

   $$L \cong \langle A(\alpha, -\gamma\alpha^{-1}) \rangle \perp H(0)^{r-1} \,. \tag{I}$$

b) If $r = 1$ *and* $\operatorname{ord}(\alpha) + b$ *is odd, then*

$$L \cong \langle A(\alpha, -\gamma\alpha^{-1})\rangle \,. \tag{II}$$

Further, either $e = b$ *or* $e > b = \operatorname{ord}(\gamma) - \operatorname{ord}(\alpha)$.

c) If $r \geq 2$ *and* $\operatorname{ord}(\alpha) + b$ *is odd, then* L *is isometric to either*

$$\langle A(\alpha, -\gamma\alpha^{-1})\rangle \perp \langle A(p^b, 0)\rangle \perp H(0)^{r-2} \quad \textit{or} \tag{IIIa}$$

$$\langle A(\alpha, -(\gamma - 4\varrho)\alpha^{-1})\rangle \perp \langle A(p^b, 4\varrho p^{-b})\rangle \perp H(0)^{r-2} \,. \tag{IIIb}$$

Proof. This is a consequence of Theorem 3.3.10. See [O'M73, Examples 93:17–18] for details. □

Remark 3.3.12 Suppose the notation of Proposition 3.3.11. Witt symbols can be used to distinguish between lattices of type (IIIa) and (IIIb). More precisely, suppose $\dim_K(V) = 2r \geq 4$. Then any unimodular $\mathfrak{o}$-lattice L in (V, Φ) with $\operatorname{ord}(\mathfrak{n}(L)\mathfrak{w}(L))$ odd is of type (IIIa) if and only if $\omega(V, \Phi)$ equals the Hilbert symbol $(\alpha, 1 + \gamma)$.

Let $L = \perp_{j=1}^{s} L_i$ be a Jordan decomposition. Let $\mathfrak{s}_i := \mathfrak{s}(L_i)$ and $\mathfrak{w}_i = \mathfrak{w}(L^{\mathfrak{s}_i})$. Further pick some norm generator α_i of $L^{\mathfrak{s}_i}$. Then

$$(t, \mathfrak{s}_1, \ldots, \mathfrak{s}_t, \alpha_1, \ldots, \alpha_t, \mathfrak{w}_1, \ldots, \mathfrak{w}_t)$$

are called the *fundamental invariants* of L. Using the fundamental invariants of L, one defines the ideals $\mathfrak{f}_1, \ldots, \mathfrak{f}_{t-1}$ by

$$\mathfrak{f}_i \mathfrak{s}_i^2 = \begin{cases} \alpha_i\alpha_{i+1}\mathfrak{o} & \text{if } \operatorname{ord}(\alpha_i\alpha_{i+1}) \text{ is odd} \\ \mathfrak{d}(\alpha_i\alpha_{i+1}) + \alpha_i\mathfrak{w}_{i+1} + \alpha_{i+1}\mathfrak{w}_i + 2\mathfrak{s}_i\mathfrak{p}^{\operatorname{ord}(\alpha_i\alpha_{i+1})/2} & \text{otherwise.} \end{cases}$$

Suppose that the lattices L and L' have the fundamental invariants $(t, \mathfrak{s}_i, \alpha_i, \mathfrak{w}_i)$ and $(t', \mathfrak{s}_i', \alpha_i', \mathfrak{w}_i')$ respectively. The lattices L and L' are said to have the same fundamental invariants if $t = t'$ and for all $1 \leq i \leq t$:

$$\mathfrak{s}_i = \mathfrak{s}_i', \quad \mathfrak{w}_i = \mathfrak{w}_i' \quad \text{and} \quad \alpha_i \cong \alpha_i' \mod \mathfrak{w}_i \,.$$

Isometric lattices have the same fundamental invariants. Conversely, T. O'Meara proved the following classification.

Theorem 3.3.13 ([O'M73, Theorem 93:28]) *Let* L *and* L' *be lattices in* (V, Φ)*. Let* $L_1 \perp \ldots \perp L_t$ *and* $L_1' \perp \ldots \perp L_t'$ *be Jordan decompositions of* L *and* L' *respectively. Suppose that* L *and* L' *have the same fundamental invariants* $(t, \mathfrak{s}_i, \alpha_i, \mathfrak{w}_i)$*. Then* L *and* L' *are isometric if and only if the following conditions hold for all* $1 \leq i \leq t - 1$*:*

1. $\det L_{(i)} / \det L_{(i)}' \cong 1 \mod \mathfrak{f}_i$.

2. *The quadratic space* $KL_{(i)}$ *embeds into* $KL_{(i)}' \perp \langle \alpha_{i+1}\rangle$ *when* $\mathfrak{f}_i \subsetneq 4\alpha_{i+1}\mathfrak{w}_{i+1}^{-1}$.

3. *The quadratic space* $KL_{(i)}$ *embeds into* $KL_{(i)}' \perp \langle \alpha_i\rangle$ *when* $\mathfrak{f}_i \subsetneq 4\alpha_i\mathfrak{w}_i^{-1}$.

Here $L_{(i)} = L_1 \perp \ldots \perp L_i$ *and* $L_{(i)}' = L_1' \perp \ldots \perp L_i'$.

3.3.3 The hermitian, ramified dyadic case

Let E/K be a ramified quadratic field extension and suppose that K is dyadic. Let π be a generator of $\mathfrak{P}$. Then $p := \pi\overline{\pi}$ is a generator of $\mathfrak{p}$.

Further, let $\mathfrak{D}^{-1} := \{\alpha \in E\,;\, \mathrm{T}(\alpha\mathcal{O}) \subseteq \mathfrak{o}\}$ be the inverse different of E/K. Then $\mathfrak{D} = \pi^e\mathcal{O}$ for some $e \geq 2$ and

$$\mathrm{T}(\mathfrak{D}^{-1}) = \mathrm{T}(\pi\mathfrak{D}^{-1}) = \mathfrak{o}\,.$$

Thus for any $i \in \mathbb{Z}$

$$\mathrm{T}(\pi^i\mathcal{O}) = \mathrm{T}(\pi^{i+e}\mathfrak{D}^{-1}) = \mathfrak{p}^{\lfloor \frac{i+e}{2} \rfloor}\,.$$

Similar to the quadratic defect, is the concept of the normic defect.

Definition 3.3.14 The *normic defect* of $a \in K$ is defined by

$$\mathfrak{d}_E(a) := \bigcap_{\beta \in E} (a - \mathrm{N}(\beta))\mathfrak{o}\,.$$

For any fractional ideal $\mathfrak{a}$ of $\mathfrak{o}$, there is an equivalence relation on K^* defined by

$$a \cong b \mod \mathfrak{a} :\iff a/b \in \mathfrak{o}^* \text{ and } a - b\,\mathrm{N}(\alpha) \in \mathfrak{a} \text{ for some } \alpha \in E^*\,.$$

Remark 3.3.15 Let $a, b \in K$. Then

1. $a \in \mathrm{N}(E)$ if and only if $\mathfrak{d}_E(a) = (0)$.
2. $\mathfrak{d}_E(a) \subseteq a\mathfrak{o}$.
3. $\mathfrak{d}_E(na) = n\mathfrak{d}_E(a)$ for all $n \in \mathrm{N}(E)$.
4. $a = \mathrm{N}(\alpha) + b$ for some $\alpha \in E$ and $b\mathfrak{o} = \mathfrak{d}_E(a)$.
5. If a, b are non-zero, then $a \cong b \mod \mathfrak{a}$ if and only if $a/b \in \mathfrak{o}^*$ and $\mathfrak{d}_E(a/b) \subseteq \mathfrak{a}/b$.

In view of Remark 3.3.15/3 it suffices to discuss the normic defect of elements in the non-trivial coset of $\mathfrak{o}^*/\,\mathrm{N}(\mathcal{O}^*) \cong C_2$.

Lemma 3.3.16 *If $a \in \mathfrak{o}^* - \mathrm{N}(\mathcal{O}^*)$, then $\mathfrak{d}_E(a) = \mathfrak{p}^{e-1}$.*

Proof. See for example [Joh68, Proposition 6.1]. □

Corollary 3.3.17 *There exists some $u = 1 + u_0 \in \mathfrak{o}^*$ such that $\mathfrak{d}_E(u) = \mathfrak{p}^{e-1} = u_0\mathfrak{o}$ and $\mathfrak{o}^* = \mathrm{N}(\mathcal{O}^*) \uplus u\,\mathrm{N}(\mathcal{O}^*)$.*

Using methods similar to [O'M73, Chapter 93], R. Jacobowitz proved the following classification.

Theorem 3.3.18 ([Jac62, Theorem 11.4]) *Let (V, Φ) and (V', Φ') be two hermitian spaces over E. Let $L = \perp_{i=1}^{t} L_i$ and $L' = \perp_{i=1}^{t'} L'_i$ be Jordan decompositions of $\mathcal{O}$-lattices in (V, Φ) and (V', Φ') respectively. Then L and L' are isometric if and only if the following conditions hold:*

1. *L and L' are of the same Jordan type.*
2. *$\det(L)/\det(L') \in \mathrm{N}(\mathcal{O}^*)$.*
3. *$\mathfrak{n}_i := \mathfrak{n}(L^{\mathfrak{s}(L_i)}) = \mathfrak{n}(L^{\mathfrak{s}(L'_i)})$ for all $1 \le i \le t$.*
4. *$\det(L_1 \perp \ldots \perp L_i)/\det(L'_1 \perp \ldots \perp L'_i) \cong 1 \mod \mathfrak{o} \cap \mathfrak{n}_i \mathfrak{n}_{i+1} \mathfrak{s}(L_i)^{-2}$ for all $1 \le i < t$.*

Corollary 3.3.19 *Let L and L' be $\mathfrak{P}^i$-modular $\mathcal{O}$-lattices in (V, Φ) for some $i \in \mathbb{Z}$. Then the following statements are equivalent:*

1. *L and L' are isometric.*
2. *L and L' represent the same numbers.*
3. *$\mathfrak{n}(L) = \mathfrak{n}(L')$.*

Corollary 3.3.20 *Let L be a $\mathfrak{P}^i$-modular $\mathcal{O}$-lattice in (V, Φ) and let m be the rank of V over E.*

1. *If $m = 2r + 1$ is odd, then i is even and*
   $$L \cong \langle u p^{i/2} \rangle \perp H(i)^r \quad \textit{where} \quad u\,\mathrm{N}(\mathcal{O}^*) = \mathrm{disc}(L) p^{-mi/2} \in \mathfrak{o}^* / \mathrm{N}(\mathcal{O}^*)\,.$$
   In particular, $\mathfrak{n}(L)\mathcal{O} = \mathfrak{s}(L)$.
2. *Suppose $m = 2r + 2$ is even and (V, Φ) is hyperbolic. Let $\mathfrak{n}(L) = \mathfrak{p}^k$. Then*
   $$\pi^i \mathfrak{D} \subseteq \mathfrak{p}^k \mathcal{O} \subseteq \pi^i \mathcal{O} \quad \textit{and} \quad L \cong \langle \begin{pmatrix} p^k & \pi^i \\ \overline{\pi}^i & 0 \end{pmatrix} \rangle \perp H(i)^r$$
   Conversely, any $\mathcal{O}$-lattice with such a Gram matrix is $\mathfrak{P}^i$-modular with norm $\mathfrak{p}^k$. In particular, $L \cong H(i)^{r+1}$ if and only if $\mathfrak{p}^k = \mathrm{T}(\pi^i \mathcal{O})$.
3. *Suppose $m = 2r + 2$ is even and (V, Φ) is not hyperbolic. Let $\mathfrak{n}(L) = \mathfrak{p}^k$ and let u_0 be as in Corollary 3.3.17. Then*
   $$\pi^i \mathfrak{D} \subsetneq \mathfrak{p}^k \mathcal{O} \subseteq \pi^i \mathcal{O} \quad \textit{and} \quad L \cong \langle \begin{pmatrix} p^k & \pi^i \\ \overline{\pi}^i & -p^{i-k} u_0 \end{pmatrix} \rangle \perp H(i)^r$$
   Conversely, any $\mathcal{O}$-lattice with such a Gram matrix is $\mathfrak{P}^i$-modular with norm $\mathfrak{p}^k$.

3.4 Construction of global hermitian spaces defined by local invariants

In this section, let K be a number field. The goal of this section is the following: Given local invariants which determine a unique isometry class of hermitian spaces over E, compute a Gram matrix of such a space.

For any place $v \in \Omega(K)$, the Hilbert symbol of K_v will be denoted by $(\_,\_)_v$. The real embeddings of K will be denoted by $\sigma_1, \dots, \sigma_r \colon K \to \mathbb{R}$.

Given $a, b \in K^*$, Theorem 3.1.7 shows that the set $\{v \in \Omega(K)\,;\, (a,b)_v = -1\}$ is finite. The product formula for Hilbert symbols (c.f. [O'M73, Theorem 71.18]) states that

$$\prod_{v \in \Omega(K)} (a,\, b)_v = 1\,.$$

In other words, the set $\{v \in \Omega(K)\,;\, (a,b)_v = -1\}$ has even cardinality.

The construction of global hermitian spaces with given local invariants can be reduced to the following important sub-problem.

Algorithm 3.4.1

Input: A finite subset $S \subset \Omega(K)$ of even cardinality and some $b \in K^*$ such that $b \notin (K_v^*)^2$ for all $v \in S$.

Output: Some $a \in \mathfrak{o}$ such that $\{v \in \Omega(K)\,;\, (a,b)_v = -1\} = S$.

```
Set $S' := \{\sigma_i \notin S\,;\, \sigma_i(b) < 0\} \cup \{\mathfrak{p} \in \mathbb{P}(\mathfrak{o}) - S\,;\, \mathfrak{p} \mid 2 \text{ or } \operatorname{ord}_{\mathfrak{p}}(b) \neq 0\}$.
Set $P := (S \cup S') \cap \mathbb{P}(\mathfrak{o})$.
Let $G$ be the elementary abelian 2-group $C_2^{\#S} \times C_2^{\#S'}$ and let
    $$\varphi\colon K^* \to G,\ a \mapsto [((a,b)_v)_{v \in S}, ((a,b)_v)_{v \in S'}]\,.$$
Set $v := [(-1)_{v \in S}, (+1)_{v \in S'}] \in G$.
Let $\{g_1, \dots, g_e\}$ be a set of generators of $\mathfrak{o}^*$.
repeat
    Pick a random prime ideal $\mathfrak{q} \in \mathbb{P}(\mathfrak{o}) - P$.
    Let $\{g_{e+1}\mathfrak{o}, \dots, g_f\mathfrak{o}\}$ with $g_i \in \mathfrak{o}$ generate the kernel of the homomorphism
        $$\langle P \cup \{\mathfrak{q}\}\rangle \le \mathcal{I}(\mathfrak{o}) \to \mathrm{Cl}(\mathfrak{o}),\ \mathfrak{a} \mapsto [\mathfrak{a}]\,.$$
until $v \in \langle \varphi(g_1), \dots, \varphi(g_f)\rangle \le G$
Write $v = \prod_{j \in J} \varphi(g_j)$ for some index set $J \subseteq \{1, \dots, f\}$.
return $a := \prod_{j \in J} g_j \in \mathfrak{o}$.
```

Proof. Provided that the algorithm terminates, its output is correct, since by construction

- $(a,b)_v = -1$ for all $v \in S$.
- $(a,b)_v = +1$ for all $v \in S' - \{\mathfrak{q}\}$.

- $(a, b)_v = +1$ for all $v \in \Omega(K) - (S \cup S' \cup \{\mathfrak{q}\})$.

Hence $(a, b)_v$ is correct at all but possibly one place. Thus it is correct everywhere by the product formula for Hilbert symbols.

Also note that there exists some solution $a' \in \mathfrak{o}$ by [O'M73, Theorem 71.19]. Let D be the divisor $4 \prod_{\mathfrak{p} \in P} \mathfrak{p} \cdot \prod_i \sigma_i$ of K. By Chebotarev's density theorem, the prime ideals of $\mathfrak{o}$ are equally distributed over the classes of the ray class group modulo D. In particular, the class of $a'\mathfrak{o}$ is represented by some prime ideal $\mathfrak{q}$. Conversely, any such ideal $\mathfrak{q}$ yields a solution $a \in \mathfrak{o}$ which is supported at $P \cup \{\mathfrak{q}\}$. So the algorithm terminates. □

The following remark shows that the above algorithm allows the construction of quaternion algebras with given ramification as well as hermitian spaces over $E \neq K$ defined by local invariants.

Remark 3.4.2

1. Algorithm 3.4.1 requires the computation of the unit and class groups of $\mathfrak{o}$. But other than that, it only makes use of linear algebra over $\mathbb{F}_2$.

2. A quaternion algebra $E = \left(\frac{a,b}{K}\right)$ is said to be *ramified* at $v \in \Omega(K)$ if and only if E_v is a skew field. By Theorem 3.1.8, this is equivalent to $(a,\, b)_v = -1$. In particular, the set of all places at which E is ramified is finite, of even cardinality and contains no complex places. Conversely, let $S \subset \Omega(K)$ be a finite subset of even cardinality which contains no complex infinite place. By weak approximation, there exists some $b \in K^*$ such that $b \notin (K_v^*)^2$. Let $a \in \mathfrak{o}$ such that $\{v \in \Omega(K)\, ;\, (a, b)_v = -1\} = S$ as computed by the Algorithm 3.4.1. Then $\left(\frac{a,b}{K}\right)$ is ramified exactly at the places in S.
   Note that the set S uniquely determines the isomorphism class of $\left(\frac{a,b}{K}\right)$ by the theorem of Hasse-Brauer-Noether-Albert, see [Rei03, Theorem 32.11] for details.

3. Suppose $E = K(\sqrt{b})$ is a quadratic field extension of K. Let (V, Φ) be a regular hermitian space over E of rank $m \geq 1$ and determinant $d\,\mathrm{N}(E^*) \in K^* / \mathrm{N}(E^*)$. Let $v_1, \dots, v_s$ be the real places of K at which b is negative and let $n_i = n_{(V_{v_i}, \Phi)}$, c.f. Proposition 2.1.5. Loc. cit., the Local-Global Principle 2.4.1 and Theorem 3.2.3 show that
$$(V, \Phi) \cong \langle a_1, \dots, a_{m-1}, d \cdot \prod_{i=1}^{m-1} a_i \rangle$$
   for any $a_1, \dots, a_{m-1} \in K^*$ such that $v_i(a_j) < 0 \iff j \leq n_i$. In particular, if (V, Φ) is definite, then $(V, \Phi) \cong \langle 1, \dots, 1, d \rangle$.
   By Hasse's norm theorem, $\det(V, \Phi) = d\,\mathrm{N}(E^*)$ is uniquely determined by the set
$$\begin{aligned} S &= \{v \in \Omega(K)\, ;\, d \notin \mathrm{N}(E_v^*)\} \\ &= \{v \in \Omega(K)\, ;\, (d, b)_v = -1\}\,. \end{aligned}$$
   In particular, the set S is finite, of even cardinality and consists only of places which are non-split in E. Conversely, given $n_1, \dots, n_r$ and S, one can recover $\det(V, \Phi)$ and thus a Gram matrix of (V, Φ) using weak approximation and Algorithm 3.4.1.

4. Suppose E is a quaternion algebra with center K and let (V, Φ) be a regular hermitian space over E of rank $m \geq 1$. Let $v_1, \ldots, v_s$ be the real places of K at which E is ramified and let $n_i = n_{(V_{v_i}, \Phi)}$, c.f. Proposition 2.1.5. Loc. cit., the Local-Global Principle 2.4.1 and Theorem 3.2.3 show that
$$(V, \Phi) \cong \langle a_1, \ldots, a_m \rangle$$
for any $a_1, \ldots, a_m \in K^*$ such that $v_i(a_j) < 0 \iff j \leq n_i$. In particular, if (V, Φ) is definite, then $(V, \Phi) \cong \langle 1, \ldots, 1 \rangle$.

Constructing a quadratic space defined by local invariants is more difficult. The Local-Global Principle 2.4.1, Proposition 2.1.5 and Theorem 3.2.3 show that any regular quadratic space over K is uniquely determined by the following invariants:

1. Its rank m.
2. Its determinant $d \in K^*/(K^*)^2$.
3. The finite set $\{\mathfrak{p} \in \mathbb{P}(\mathfrak{o})\,;\, \mathrm{c}(V_\mathfrak{p}, \Phi) = -1\}$.
4. The numbers $n_{(V_{\sigma_i}, \Phi)}$ for $1 \leq i \leq r$ from Proposition 2.1.5.

Given the space (V, Φ), these invariants are easy to compute. Conversely, given these invariants, the computation of a quadratic space (V, Φ) with these invariants (provided it exists) is more involved. The algorithm given below to solve this problem is inspired by Section 6.7 of J. Cassels' book on rational quadratic forms [Cas78].

Algorithm 3.4.3 QuadraticFormFromInvariants$(m, d, P, (n_1, \ldots, n_r))$

Input: Some integer $m \geq 1$, some nonzero element $d \in \mathfrak{o}$, some finite subset $P \subset \mathbb{P}(\mathfrak{o})$ and some integers $n_1, \ldots, n_r \in \{0, \ldots, m\}$.

Output: A Gram matrix of a quadratic space (V, Φ) over K of rank m and determinant d such that $\{\mathfrak{p} \in \mathbb{P}(\mathfrak{o})\,;\, \mathrm{c}(V_\mathfrak{p}, \Phi) = -1\} = P$ and $n_{(V_{\sigma_i}, \Phi)} = n_i$ for all $1 \leq i \leq r$.

```
Raise an error if $\mathrm{sign}(\sigma_i(d)) \neq (-1)^{n_i}$ for some $i$.
Raise an error if $m = 1$ and $P \neq \emptyset$.
Raise an error if $m = 2$ and $-d \in (K_\mathfrak{p}^*)^2$ for some $\mathfrak{p} \in P$.
Raise an error if $\#\{1 \leq i \leq r\,;\, n_i \equiv 2, 3 \pmod 4\} + \#P$ is odd.
Initialiase the list $D = ()$.
while $m \geq 2$ do
    if $m \geq 4$ then
        By weak approximation, compute $a \in \mathfrak{o}$ such that for all $1 \leq i \leq r$:
            $$\begin{cases} \sigma_i(a) < 0 & \text{if } n_i > 0, \\ \sigma_i(a) > 0 & \text{otherwise.} \end{cases} \qquad (3.4.1)$$
    else if $m = 3$ then
        Set $P' := \{\mathfrak{p} \in P;\ (-1, -d)_\mathfrak{p} = 1\} \cup \{\mathfrak{p} \in \mathbb{P}(\mathfrak{o}) - P;\ \mathfrak{p} \mid 2d \text{ and } (-1, -d)_\mathfrak{p} = -1\}$.
```

```
11:         By weak approximation, compute $a \in \mathfrak{o}$ satisfying Eq. (3.4.1) such that
                $$\mathrm{ord}_{\mathfrak{p}}(ad) \equiv 1 \pmod 2 \quad \text{for all } \mathfrak{p} \in P' .$$
12:     else if $m = 2$ then
13:         Set $S := P \cup \{\sigma_i \,;\, n_i = 2\}$.
14:         Using Algorithm 3.4.1, compute some $a \in \mathfrak{o}$ such that
                $$\{v \in \Omega(K) \,;\, (a, -d)_v = -1\} = S .$$
15:     end if
16:     Set $P := \{\mathfrak{p} \in P \,;\, (a, -d)_{\mathfrak{p}} = 1\} \cup \{\mathfrak{p} \in \mathbb{P}(\mathfrak{o}) - P \,;\, \mathfrak{p} \mid 2ad \text{ and } (a, -d)_{\mathfrak{p}} = -1\}$.
17:     For $1 \leq i \leq r$ replace $n_i$ by $\max\{0, n_i - 1\}$.
18:     Replace $m$ by $m - 1$ and $d$ by $ad$.
19:     Append $a$ to $D$.
20: end while
21: Append $d$ to $D$.
22: return the diagonal matrix $\mathrm{Diag}(D)$.
```

Proof. The conditions imposed by lines 1–4 are both necessary and sufficient for the existence of a quadratic space with the given invariants, c.f. [O'M73, Theorems 63.23 and 72.1]. The returned answer is certainly correct if $m = 1$. If $m > 1$, the algorithm chooses some $a \in \mathfrak{o}$ that is represented by (V, Φ) thanks to the Local-Global Principle and Theorem 3.2.2. Hence $(V, \Phi) \cong \langle a \rangle \perp (V', \Phi')$ for some quadratic space (V', Φ') of dimension $m - 1$. The invariants of (V', Φ') are computed in lines 15–17 from a and the corresponding invariants of (V, Φ). Hence by induction, the result is correct. □

3.5 Construction of global hermitian lattices defined by local invariants

Let K be a number field and let (V, Φ) be a hermitian space over E of rank m. Further, let $\mathfrak{o}$ and $\mathcal{O}$ be maximal orders of K and E respectively.

Definition 3.5.1 A prime ideal $\mathfrak{p}$ of $\mathfrak{o}$ is called *bad*, if $\mathfrak{p} \mid 2$ and one of the following conditions holds:

- $E = K$.
- $E_{\mathfrak{p}}/K_{\mathfrak{p}}$ is a ramified quadratic field extension.

In all other cases, $\mathfrak{p}$ is said to be *good*.

In Section 3.3, it is shown that Jordan decompositions are unique at the good but not at the bad prime ideals.

The goal of this section is to describe an algorithm which computes a representative of some genus G of $\mathcal{O}$-lattices in (V, Φ), which is given by local invariants. First an algorithm for computing $\mathfrak{o}$-maximal $\mathcal{O}$-lattices in (V, Φ) is presented. It is based on the following two lemmata.

Lemma 3.5.2 *Let $\mathfrak{a}$ be some fractional ideal of $\mathfrak{o}$. The set of all $\mathfrak{a}$-maximal $\mathcal{O}$-lattices in (V, Φ) forms a single genus.*

Proof. See [O'M73, Theorem 91:2] and [Shi64, Proposition 4.13]. □

Lemma 3.5.3 *Let M be an $\mathcal{O}$-lattice in (V, Φ). Suppose that $M_\mathfrak{p}$ is $\mathfrak{o}_\mathfrak{p}$-maximal for some $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$. Then the valuation $v = \operatorname{ord}_\mathfrak{p}([M^\# : M]_\mathfrak{o})$ is given by the following local invariants.*

1. *Suppose $E = K$. Let $d \in K^*$ be a representative of the discriminant $\operatorname{disc}(V_\mathfrak{p}, \Phi)$ such that $\operatorname{ord}_\mathfrak{p}(d) \in \{0, 1\}$ and let $e = \operatorname{ord}_\mathfrak{p}(2)$. Then v is given by the following table.*

m	d	$\omega(V_\mathfrak{p}, \Phi)$	*extra condition*	v
odd	–	$+1$		$\operatorname{ord}_\mathfrak{p}(d) - e(m-1)$
odd	–	-1		$2 - \operatorname{ord}_\mathfrak{p}(d) - e(m-1)$
even	*square*	$+1$		$-em$
even	*square*	-1		$2 - em$
even	*non-square*	$+1$		$\operatorname{ord}_\mathfrak{p}(\mathrm{d}_{K(\sqrt{d})/K}) - e(m-2)$
even	*non-square*	-1	$K_\mathfrak{p}(\sqrt{d})/K_\mathfrak{p}$ *ramified*	$\operatorname{ord}_\mathfrak{p}(\mathrm{d}_{K(\sqrt{d})/K}) - e(m-2)$
even	*non-square*	-1	$K_\mathfrak{p}(\sqrt{d})/K_\mathfrak{p}$ *unramified*	$2 - em$

2. *Suppose $E \neq K$ and $\mathfrak{p}$ is unramified in E. Then $v = 0$ if $\det(V_\mathfrak{p}, \Phi) \in \mathrm{N}(E^*)$ and $v = 1$ otherwise.*

3. *Suppose $\dim_K(E) = 2$ and $\mathfrak{p}$ is ramified in E. Let $e = \operatorname{ord}_\mathfrak{p}(\mathrm{d}_{E/K})$. Then v is given by the following table.*

m	$\operatorname{disc}(V_\mathfrak{p}, \Phi)$	v
odd	–	$-e(m-1)/2$
even	*norm*	$-em/2$
even	*non-norm*	$1 - em/2$

4. *Suppose $\dim_K(E) = 4$ and $\mathfrak{p}$ is ramified in E. Then $v = -2\lfloor \frac{m}{2} \rfloor$.*

Proof. This follows from a case by case discussion using the classification of $\mathfrak{o}_\mathfrak{p}$-maximal $\mathcal{O}_\mathfrak{p}$-lattices in $(V_\mathfrak{p}, \Phi)$, c.f. for example [GHY01]. □

Algorithm 3.5.4 LocalMaximalLattice$(L, \mathfrak{p}, v)$

Input: Some $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$ and some $\mathcal{O}$-lattice L in (V, Φ) such that $\operatorname{ord}_\mathfrak{p}(\mathfrak{n}(L)) \geq v$.

Output: A chain of minimal $\mathcal{O}$-overlattices $L_0 = L \subsetneq L_1 \subsetneq \cdots \subsetneq L_r$ in (V, Φ) such that $(L_r)_\mathfrak{p}$ is $\mathfrak{p}^v$-maximal and $(L_i)_\mathfrak{q} = L_\mathfrak{q}$ for all $\mathfrak{q} \in \mathbb{P}(\mathfrak{o}) - \{\mathfrak{p}\}$.

```
1: Let $a \in K^*$ such that $\operatorname{ord}_\mathfrak{p}(a) = -v$.
2: Let $w = \operatorname{ord}_\mathfrak{p}([M^\# : M]_{\mathfrak{o}_\mathfrak{p}})$ where $M$ denotes an $\mathfrak{o}_\mathfrak{p}$-maximal $\mathcal{O}_\mathfrak{p}$-lattice in $(V_\mathfrak{p}, a\Phi)$,
   c.f. Lemma 3.5.3.
```

```
3:  Let $\mathfrak{P}$ be a maximal left ideal of $\mathcal{O}$ that contains $\mathfrak{p}$.
4:  Let $\mathfrak{D}^{-1} := \{\alpha \in E\,;\, \mathrm{T}(\alpha\mathcal{O}) \subseteq \mathfrak{o}\}$.
5:  Initialiase $i = 0$ and let $L_0$ be the lattice $L^a$ in $(V, a\Phi)$.
6:  while $\mathrm{ord}_{\mathfrak{p}}([L_i^{\#} : L_i]_{\mathfrak{o}}) > w$ do
7:      Set $L_{i+1} := L_i + \mathcal{O}x$ for some $x \in (\mathfrak{D}^{-1}L_i^{\#} \cap \mathfrak{P}^{-1}L_i) - L_i$ with $\mathrm{ord}_{\mathfrak{p}}(Q_{a\Phi}(x)) \geq 0$.
8:      Increment $i$.
9:  end while
10: return the chain $L_0^{1/a}, \dots, L_i^{1/a}$ of $\mathcal{O}$-lattices in $(V, \Phi)$.
```

Proof. By construction, every lattice L_i satisfies $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{n}(L_i)) \geq v$ and $(L_i)_{\mathfrak{q}} = L_{\mathfrak{q}}$ for all $\mathfrak{q} \neq \mathfrak{p}$. Further, $\mathrm{ord}_{\mathfrak{p}}([L_i^{\#} : L_i]_{\mathfrak{o}})$ decreases in each step. So provided the element x in line 6 always exists, the algorithm eventually returns some chain and Lemmata 3.5.2 and 3.5.3 show that the last lattice in this chain is $\mathfrak{p}^v$-maximal in (V, Φ).
To see that the element x exists, suppose that $(L_i)_{\mathfrak{p}}$ is not $\mathfrak{o}_{\mathfrak{p}}$-maximal. If $\mathfrak{p}$ is non-split in E, then $\mathfrak{P}$ is the unique maximal left ideal of $\mathcal{O}$ over $\mathfrak{p}$. Thus the assumption on L_i implies that there exists some minimal overlattice X over L_i which is contained in $\mathfrak{P}^{-1}L_i$ such that $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{n}(X)) \geq 0$. This result also holds if $\mathfrak{p}$ splits in E, although for different reasons. If $\mathfrak{p}$ splits in E, then $(L_i)_{\mathfrak{p}}$ has a an orthogonal basis $(b_1, \dots, b_m)$. By assumption, $a\Phi(b_i, b_i) \in \mathfrak{p}$ for some i. Let $\mathfrak{P}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}\pi$. Let X be the $\mathcal{O}$-lattice with $X_{\mathfrak{q}} = L_{\mathfrak{q}}$ for all $\mathfrak{q} \in \mathbb{P}(\mathfrak{o}) - \{\mathfrak{p}\}$ and $X_{\mathfrak{p}} = (L_i)_{\mathfrak{p}} + \pi^{-1}b_i$. So whether $\mathfrak{p}$ splits or not, the lattice X is a minimal overlattice over L_i, it is contained in $\mathfrak{P}^{-1}L_i$ and $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{n}(X)) \geq 0$. In particular, X is of the form $L_i + \mathcal{O}x$ for some $x \in \mathfrak{P}^{-1}L_i - L_i$. The condition $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{n}(X)) \geq 0$ readily translates into $\mathrm{ord}_{\mathfrak{p}}(a\Phi(x, x)) \geq 0$ and $\mathrm{T}(a\Phi(x, (L_i)_{\mathfrak{p}})) \subseteq \mathfrak{o}_{\mathfrak{p}}$. The latter condition is equivalent to $x \in \mathfrak{D}_{\mathfrak{p}}^{-1}(L_i^{\#})_{\mathfrak{p}}$. Hence in line 6, an element x always exists. □

Calling the above algorithm with different prime ideals yields a method for computing $\mathfrak{a}$-maximal lattices:

Algorithm 3.5.5 MaximalLattice$(L, \mathfrak{a})$

Input: Some fractional ideal $\mathfrak{a}$ of $\mathfrak{o}$ and some $\mathcal{O}$-lattice L in (V, Φ) such that $\mathfrak{n}(L) \subseteq \mathfrak{a}$.
Output: An $\mathcal{O}$-lattice M in (V, Φ) that is $\mathfrak{a}$-maximal and contains L.

```
Let $P = \{\mathfrak{p} \in \mathbb{P}(\mathfrak{o})\,;\, \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) \neq 0$ or $\mathfrak{p} \mid \mathrm{d}_{E/K}$ or $\mathfrak{p}$ is bad or $L_{\mathfrak{p}}$ is not unimodular$\}$.
Initialiase $M = L$.
for $\mathfrak{p} \in P$ do
    Replace $M$ by the last lattice returned by LocalMaximalLattice$(M, \mathfrak{p}, \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}))$.
end for
return $M$.
```

Starting from a maximal lattice, one can construct a representative of any given genus as follows.

Algorithm 3.5.6 LatticeInGenus(G)

Input: A genus G of hermitian $\mathcal{O}$-lattices in (V, Φ) given by local invariants (for example by Gram matrices) at the places in

$$P := \{\mathfrak{p} \in \mathbb{P}(\mathfrak{o})\,;\, \mathfrak{p} \mid \mathrm{d}_{E/K} \text{ or } \mathfrak{p} \text{ is bad or } L_{\mathfrak{p}} \text{ is not modular for } L \in G\}\,.$$

```
Output: Some lattice $L \in G$.
1: From the given local invariants compute the norm ideal $\mathfrak{a}$ of the lattices in $G$.
2: Compute an $\mathfrak{a}$-maximal lattice $L$ in $(V, \Phi)$ using Algorithm 3.5.5.
3: for $\mathfrak{p} \in P$ do
4:     Compute an $\mathcal{O}$-sublattice $X$ of $L$ such that $X_\mathfrak{p}$ has the correct invariants at $\mathfrak{p}$ and $X_\mathfrak{q} = L_\mathfrak{p}$ for all $\mathfrak{q} \neq \mathfrak{p}$.
5:     Replace $L$ by $X$.
6: end for
7: return $L$.
```

Clearly, step 4 is the crucial step. Suppose $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$ is good. Given any Jordan decomposition of $L_\mathfrak{p}$ it is easy (c.f. Algorithm 2.2.7) to write down a random sublattice X of L such that

- $L_\mathfrak{q} = X_\mathfrak{q}$ for all $\mathfrak{q} \in \mathbb{P}(\mathfrak{o}) - \{\mathfrak{p}\}$.
- The blocks of any Jordan decomposition of $X_\mathfrak{p}$ have the correct scales and ranks.

By Theorem 3.3.6, the number of local isometry classes represented by such lattices $X_\mathfrak{p}$ is at most 2^{m-1} and the classes are equally distributed. So one quickly finds a lattice X that does the trick. At bad primes however, the task can be quite challenging since the number of isometry classes can be fairly large and they are not equally distributed. In this case, one can fall back to the following deterministic procedure which makes use of the fact that bad primes usually have small norms.

Algorithm 3.5.7 SUBLATTICE$(M, M', \mathfrak{p},)$

```
Input: Some prime ideal $\mathfrak{p}$ of $\mathfrak{o}$, an $\mathcal{O}$-lattice $M'$ in a hermitian space $(V', \Phi')$ over $E$ such
    that $(V'_\mathfrak{p}, \Phi') \cong (V_\mathfrak{p}, \Phi)$ and an $\mathcal{O}$-lattice $M$ in $(V, \Phi)$ such that $M_\mathfrak{p}$ is $\mathfrak{n}(M')_\mathfrak{p}$-maximal.
Output: Some $\mathcal{O}$-lattice $L \subseteq M$ such that $L_\mathfrak{p} \cong M'_\mathfrak{p}$ and $L_\mathfrak{q} = M_\mathfrak{q}$ for all $\mathfrak{q} \in \mathbb{P}(\mathfrak{o}) - \{\mathfrak{p}\}$.
1: Let $M'_0 \subsetneq \ldots \subsetneq M'_r$ be the output of LOCALMAXIMALLATTICE$(M', \mathfrak{p}, \mathrm{ord}_\mathfrak{p}(\mathrm{nr}(M')))$.
2: Initialiase $L = M$.
3: for $i = r-1, \ldots, 1, 0$ do
4:     repeat
5:         Compute a random maximal $\mathcal{O}$-sublattice $X$ of $L$ containing $\mathfrak{p}L$.
6:     until $X_\mathfrak{p} \cong (M'_i)_\mathfrak{p}$
7:     Replace $L$ by $X$.
8: end for
9: return $L$.
```

Proof. If the algorithm terminates, it certainly yields an $\mathcal{O}$-lattice L with the desired properties. By induction, $(M'_{i+1})_\mathfrak{p}$ is isometric to $L_\mathfrak{p}$. Hence there exists at least one maximal $\mathcal{O}$-sublattice X between L and $\mathfrak{p}L$ such that $X_\mathfrak{p} \cong (M'_i)_\mathfrak{p}$. □

Note that if (V, Φ) is definite, the above search can be improved considerably. The finite group $\mathrm{Aut}(L)$ acts on the maximal $\mathcal{O}$-subspaces of L that contain $\mathfrak{p}L$. Thus one only needs to consider orbit representatives X in step 5. This is extremely useful since the local isometry classes represented by the maximal $\mathcal{O}$-sublattices of L are not always equally distributed at bad primes.

4 The mass formula of Siegel

In this chapter, K is a totally real number field of degree n with ring of integers $\mathfrak{o}$. Let (V, Φ) be a definite hermitian space over E of rank m. If $E = K$, then m is assumed to be at least 2.

Let $\mathcal{O}$ denote some fixed maximal order in E. Then the *inverse different*

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

of $\mathcal{O}$ is an invertible twosided ideal of $\mathcal{O}$. Moreover, the *relative discriminant ideal* $\mathrm{d}_{E/K} := \mathrm{N}(\mathfrak{D})$ does not depend on chosen maximal order $\mathcal{O}$. Note that, if E is a quaternion algebra over K, ramified only at the prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ of $\mathfrak{o}$, then $\mathrm{d}_{E/K} = \prod_{i=1}^{s} \mathfrak{p}_i^2$. Hence $\mathrm{d}_{E/K}$ is the square of the reduced discriminant as defined in [Rei03, Chapter 25].

Given an algebraic number field F, let $\mathrm{Nr}_{F/\mathbb{Q}} \colon F \to \mathbb{Q}$ be the usual norm of F and the absolute value of the discriminant of F will be denoted by d_F.

4.1 Some properties of L-series

In this section, some well-known results of L-series of number fields are recalled. For a proof of these results and more information, see for example [Neu06, Chapter VII].

Definition 4.1.1 The *Dedekind zeta function* ζ_F of an algebraic number field F is defined by the Dirichlet series

$$\zeta_F(s) = \sum_{\mathfrak{a}} \frac{1}{\mathrm{Nr}_{F/\mathbb{Q}}(\mathfrak{a})^s} \,.$$

Here the sum ranges over all ideals $\mathfrak{a}$ of the ring of integers of F.

Theorem 4.1.2 *Let F be a number field. The series $\zeta_F(s)$ converges absolutely and uniformly on $\{s \in \mathbb{C}\,;\, \Re(s) \geq 1 + \varepsilon\}$ for every $\varepsilon > 0$. For $\Re(s) > 1$, the series $\zeta_F(s)$ has an Euler product expansion*

$$\zeta_F(s) = \prod_{\mathfrak{p}} \frac{1}{1 - \mathrm{Nr}_{F/\mathbb{Q}}(\mathfrak{p})^{-s}}$$

where $\mathfrak{p}$ ranges over the prime ideals of the ring of integers of F.

E. Hecke showed that ζ_F admits a meromorphic continuation on $\mathbb{C}$, with a single pole at 1 and it satisfies a functional equation relating $\zeta_F(s)$ with $\zeta_F(1-s)$.

Theorem 4.1.3 (Hecke, Functional equation) *Let F be a number field with signature (r_1, r_2) and degree $n = r_1 + 2r_2$. The* completed Dedekind zeta function

$$\Lambda_F(s) := \left(\frac{\mathrm{d}_F}{4^{r_2}\pi^n}\right)^{s/2} \Gamma(s/2)^{r_1}\Gamma(s)^{r_2}\zeta_F(s) \qquad (\Re(s) > 1)$$

has an analytic continuation on $\mathbb{C} - \{0, 1\}$ and satisfies the functional equation

$$\Lambda_F(s) = \Lambda_F(1 - s)\,.$$

Here Γ denotes the usual Gamma function.

The Dedekind zeta function has a unique pole at $s = 1$ and this pole is simple. The residue $\mathrm{Res}_1(\zeta_F)$ at $s = 1$ gives a beautiful relation between important invariants of F.

Theorem 4.1.4 (Class number formula) *Let F be a number field with signature (r_1, r_2). The Dedekind zeta function ζ_F has an analytic continuation on $\mathbb{C} - \{1\}$. It has a simple pole at $s = 1$ with residue*

$$\mathrm{Res}_1(\zeta_F) = \lim_{s\to 1}(s-1)\zeta_F(s) = \frac{2^{r_1}(2\pi)^{r_2}\,\mathrm{Reg}(F)\cdot \#\,\mathrm{Cl}(F)}{\#\mu(F)\cdot \mathrm{d}_F^{1/2}}$$

where d_F, $\mathrm{Cl}(F)$, $\mu(F)$ and $\mathrm{Reg}(F)$ denote the absolute value of the discriminant, the class group, the roots of unity and the regulator of F respectively.

Let F/K be a quadratic extension of the totally real number field K. The Galois group $\mathrm{Gal}(F/K)$ has two irreducible characters (i.e. homomorphisms $\mathrm{Gal}(F/K) \to \{\pm 1\}$). To each character χ of $\mathrm{Gal}(F/K)$, one associates the so-called *Artin map*, which will also be denoted by χ. It is the multiplicative function $\chi\colon \mathcal{I}(\mathfrak{o}) \to \{-1, 0, +1\}$ on the group of fractional ideals $\mathcal{I}(\mathfrak{o})$ of $\mathfrak{o}$ defined by

$$\chi(\mathfrak{p}) = \begin{cases} 0 & \text{if } \chi \neq 1 \text{ and } \mathfrak{p} \text{ ramifies in } F, \\ -1 & \text{if } \chi \neq 1 \text{ and } \mathfrak{p} \text{ is inert in } F, \\ +1 & \text{otherwise,} \end{cases}$$

for all prime ideals $\mathfrak{p}$ of $\mathfrak{o}$. The Artin map χ gives rise to the L-series

$$\mathfrak{L}_K(\chi, s) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \frac{1}{1 - \chi(\mathfrak{p})\,\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})^{-s}} \qquad (\Re(s) > 1)$$

where $\mathfrak{a}$ and $\mathfrak{p}$ range over the integral and prime ideals of $\mathfrak{o}$ respectively. Clearly $\mathfrak{L}_K(1, s) = \zeta_K(s)$ for $\Re(s) > 1$.

Suppose now $\chi \neq 1$. From the decomposition of prime ideals of $\mathfrak{o}$ in F it follows that

$$\mathfrak{L}_K(\chi, s) = \frac{\zeta_F(s)}{\zeta_K(s)} \qquad (\Re(s) > 1)\,. \tag{4.1.1}$$

In particular, $\mathfrak{L}_K(\chi)$ has a meromorphic continuation on $\mathbb{C}$ and Theorem 4.1.3 yields a functional equation for $\mathfrak{L}_K(\chi)$ relating $\mathfrak{L}_K(\chi, s)$ with $\mathfrak{L}_K(\chi, 1 - s)$. Below, some of these identities are collected that will be used later on.

Corollary 4.1.5 *Let F be a quadratic field extension of the totally real number field K. Let R be the ring of integers of F and let χ be the non-trivial character of* $\mathrm{Gal}(F/K)$. *Further, let $n = [K : \mathbb{Q}]$ and set $d := \frac{\mathrm{d}_F}{\mathrm{d}_K} = \mathrm{d}_K \operatorname{Nr}_{K/\mathbb{Q}}(\mathrm{d}_{F/K})$.*

1. *If $s \geq 2$ is an even integer, then*

$$\zeta_K(1-s) = \left((-1)^{s/2} \cdot \frac{2 \cdot (s-1)!}{(2\pi)^s} \right)^n \cdot \mathrm{d}_K^{s-1/2} \cdot \zeta_K(s)\,.$$

2. *If F is totally real and $s \geq 2$ is an even integer, then*

$$\mathfrak{L}_K(\chi, 1-s) = \left((-1)^{s/2} \cdot \frac{2 \cdot (s-1)!}{(2\pi)^s} \right)^n \cdot d^{s-1/2} \cdot \mathfrak{L}_K(\chi, s)\,.$$

3. *If F is totally complex and $s \geq 1$ is an odd integer, then*

$$\mathfrak{L}_K(\chi, 1-s) = \left((-1)^{(s-1)/2} \cdot \frac{2 \cdot (s-1)!}{(2\pi)^s} \right)^n \cdot d^{s-1/2} \cdot \mathfrak{L}_K(\chi, s)\,.$$

4. *If F is totally complex, then*

$$\mathfrak{L}_K(\chi, 1) = \frac{\#\,\mathrm{Cl}(F)}{\#\,\mathrm{Cl}(K)} \cdot \frac{(2\pi)^n}{Q \cdot \#\mu(F) \cdot d^{1/2}}$$

where $Q := [R^* : \mu(F)\mathfrak{o}^*] \in \{1, 2\}$ denotes the Hasse unit index of F/K.

Proof. 1. This is an immediate consequence of Theorem 4.1.3. Further, 2. follows from 1. and equation (4.1.1).

3. Let $\ell := \frac{\Lambda_F(s)}{\Lambda_K(s)} = \left(\frac{d}{(4\pi)^n}\right)^{s/2} \frac{\Gamma(s)^n}{\Gamma(s/2)^n} \mathfrak{L}_K(\chi, s) = \left(\frac{d}{(4\pi)^n}\right)^{s/2} \left(\frac{2^{s-1}(\frac{s-1}{2})!}{\sqrt{\pi}}\right)^n \mathfrak{L}_K(\chi, s)$. Using the functional equation 4.1.3, one obtains

$$\begin{aligned}
\ell = \lim_{z \to 1-s} \frac{\Lambda_F(z)}{\Lambda_K(z)} &= \left(\frac{d}{(4\pi)^n}\right)^{(1-s)/2} \mathfrak{L}_K(\chi, 1-s) \cdot \left(\frac{1}{2} \lim_{z \to 1-s} \frac{\Gamma(z)}{\Gamma(z/2)} \cdot \frac{1-s-z}{\frac{1-s}{2} - \frac{z}{2}} \right)^n \\
&= \left(\frac{d}{(4\pi)^n}\right)^{(1-s)/2} \mathfrak{L}_K(\chi, 1-s) \cdot \left(\frac{1}{2} \frac{\mathrm{Res}_{1-s}(\Gamma)}{\mathrm{Res}_{(1-s)/2}(\Gamma)} \right)^n \\
&= \left(\frac{d}{(4\pi)^n}\right)^{(1-s)/2} \mathfrak{L}_K(\chi, 1-s) \cdot \left(\frac{1}{2} \cdot (-1)^{(s-1)/2} \frac{(\frac{s-1}{2})!}{(s-1)!} \right)^n .
\end{aligned}$$

4. Follows from Theorem 4.1.4 and equation (4.1.1). □

Quite surprising, the values $\zeta_K(1-s)$ and $\mathfrak{L}_K(\chi, 1-s)$ in the previous corollary are in fact rational numbers:

Theorem 4.1.6 (Klingen-Siegel, Shintani) *Let F/K be a quadratic field extension of a totally real number field K. Let χ be the non-trivial character of* $\mathrm{Gal}(F/K)$. *Then ζ_K and $\mathfrak{L}_K(\chi)$ are rational valued at non-positive integers.*

To simplify the presentation later on, the following notation will be used.

Definition 4.1.7 Suppose $d \in K^*$. If $d \notin (K^*)^2$, then χ_d denotes the non-trivial character of $\mathrm{Gal}(K(\sqrt{d})/K)$ otherwise set $\chi_d = 1$.

4.2 Siegel's Mass formula

Suppose K is a totally real number field of degree n. Let (V, Φ) be a definite hermitian space over E of dimension m.

Let G be the reductive algebraic group defined by

$$G(A) = \{\varphi \in \mathrm{End}_A(A \otimes_K V)\,;\, \Phi(\varphi(x), \varphi(y)) = \Phi(x, y) \text{ for all } x, y \in A \otimes_K V\}$$

for every K-algebra A. The connected component of the identity will be denoted by G^0. The algebraic group G is a form of an orthogonal, hermitian or symplectic group, depending on $\dim_K(E) = 1$, 2 or 4. For convenience, Table 4.1 lists some invariants of G, which will be needed later on.

$\dim_K(E)$	m	type	$[G : G^0]$	$\dim(G)$	degrees of G
1	odd	O_m	2	$m(m-1)/2$	$2, 4, 6, \ldots, m-1$
1	even	O_m	2	$m(m-1)/2$	$2, 4, 6, \ldots, m-2, m/2$
2	–	U_m	1	m^2	$1, 2, 3, \ldots, m$
4	–	Sp_{2m}	1	$m(2m+1)$	$2, 4, 6, \ldots, 2m$

Table 4.1: Invariants of G

Definition 4.2.1 Let L be an $\mathcal{O}$-lattice in (V, Φ) and let $L_1, \ldots, L_h$ represent the isometry classes in $\mathrm{gen}(L)$. Then

$$\mathrm{Mass}(L) := \mathrm{Mass}(\mathrm{gen}(L)) := \sum_{i=1}^{h} \frac{1}{\#\,\mathrm{Aut}(L_i)}$$

is called the *mass* of (the genus of) L.

Since the mass is invariant under scaling, it suffices to discuss the mass of integral lattices only.

Definition 4.2.2 Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{o}$ of norm q and let L be an integral $\mathcal{O}$-lattice in (V, Φ). Given a commutative $\mathfrak{o}$-algebra R, the map Φ extends to some bilinear map on $L_\mathfrak{p} \otimes_{\mathfrak{o}_\mathfrak{p}} R$. Thus $L_\mathfrak{p}$ defines a local integral group scheme H via

$$H(R) = \{\varphi \in \mathrm{End}_{\mathcal{O}_\mathfrak{p} \otimes_{\mathfrak{o}_\mathfrak{p}} R}(L_\mathfrak{p} \otimes_{\mathfrak{o}_\mathfrak{p}} R)\,;\, \Phi(x, y) = \Phi(\varphi(x), \varphi(y)) \text{ for all } x, y \in L_\mathfrak{p} \otimes_{\mathfrak{o}_\mathfrak{p}} R\}$$

for every commutative $\mathfrak{o}$-algebra R. The local density of L at $\mathfrak{p}$ is defined by

$$\beta(L_\mathfrak{p}) := \frac{1}{[G : G^0]} \cdot \lim_{N\to\infty} \frac{\#H(\mathfrak{o}_\mathfrak{p}/\mathfrak{p}^N)}{q^{N\dim(G)}} \,.$$

The above limit $\beta(L_\mathfrak{p})$ is known to stabilize for some N, see for example [Sie35, Satz 2] for the case $E = K$. However, if H is not smooth over $\mathfrak{o}$, it does not have to stabilize at $N = 1$.

Theorem 4.2.3 (Siegel) *Let L be an integral $\mathcal{O}$-lattice in (V, Φ). Then* $\operatorname{Mass}(L)$ *equals*

$$(\mu/\gamma_m)^n \cdot \tau(G) \cdot \mathrm{d}_K^{\dim(G)/2} \cdot \mathrm{Nr}_{K/\mathbb{Q}}(\mathrm{d}_{E/K})^{m(m+1)/4} \cdot [L^\# : L]_\mathbb{Z}^{m(V)/2} \cdot \prod_\mathfrak{p} \beta(L_\mathfrak{p})^{-1}$$

where the product runs over all prime ideals of $\mathfrak{o}$ and

$$\tau(G) = \begin{cases} 2 & \textit{if } \dim_K(E) = 2\,, \\ 1 & \textit{otherwise,} \end{cases} \qquad \textit{is the Tamagawa number of } G.$$

$$m(V) = \begin{cases} m+1 & \textit{if } E = K\,, \\ m & \textit{if } \dim_K(E) = 2\,, \\ m - 1/2 & \textit{if } \dim_K(E) = 4\,. \end{cases}$$

$$\mu = \begin{cases} 2^m & \textit{if } E = K \textit{ and } m \textit{ is even,} \\ 2^{(m+1)/2} & \textit{if } E = K \textit{ and } m \textit{ is odd,} \\ 1 & \textit{otherwise.} \end{cases}$$

$$\gamma_m = \prod_{i=1}^r \frac{(2\pi)^{d_i}}{(d_i - 1)!} \qquad \textit{where } d_1, \ldots, d_r \textit{ are the degrees of } G.$$

Proof. The proof in the quadratic case is due to Siegel [Sie35, Sie37]. For a proof of the general case, see [GY00, Section 10]. □

The local factors $\beta(L_\mathfrak{p})$ are known in many cases. For example

- if $E = K$ and $2 \notin \mathfrak{p}$ by work of C.-L. Siegel [Sie35, Sie37] and H. Pfeuffer [Pfe71a].
- if $E = K = \mathbb{Q}$ and $\mathfrak{p} = 2\mathbb{Z}$ by work of G. L. Watson [Wat76].
- if $L_\mathfrak{p}$ is maximal by work of G. Shimura [Shi97, Shi99a, Shi99b], see also [GHY01].
- if $\mathfrak{p}$ is good by work of W. T. Gan & J.-K. Yu [GY00].
- if $\mathfrak{p}$ is bad and $K_\mathfrak{p}/\mathbb{Q}_2$ is unramified by work of S. Cho [Cho].

Suppose $\mathfrak{p}$ is good and let L be an $\mathcal{O}$-lattice in (V, Φ). Then Gan and Yu associate to $L_\mathfrak{p}$ several group schemes as follows. Let

$$L_\mathfrak{p} = L_1 \perp \ldots \perp L_t$$

be a Jordan decomposition of $L_\mathfrak{p}$, which is essentially unique by Theorem 3.3.6. Let $\mathfrak{P}$ be the largest twosided $\mathcal{O}$-ideal over $\mathfrak{p}$ that is invariant under the involution $^-$ and let $s_i \in \mathbb{Z}$ such that $\mathfrak{s}(L_i) = \mathfrak{P}^{s_i}$. Further, let $\pi \in \mathfrak{P}$ such that $\mathfrak{P}_\mathfrak{p} = \pi\mathcal{O}_\mathfrak{p}$. For $1 \le i \le t$, the rescaled Gram matrix $\pi^{-s_i}\,\mathrm{G}(L_i) \pmod{\mathfrak{P}}$ defines a (skew-) hermitian form on $L_i/\mathfrak{P}L_i$ and hence a group scheme G_i over $\mathfrak{o}/\mathfrak{p}$. The local factor $\beta(L_\mathfrak{p})$ can now be expressed in terms of these schemes:

Theorem 4.2.4 *In the above situation, let $m_i = \operatorname{rank}(L_i)$ and $m_i' = \sum_{j>i} m_j$. If $\mathfrak{p}$ is a good prime ideal of $\mathfrak{o}$ of norm $q = \mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})$, then*

$$\beta(L_\mathfrak{p}) = [G : G^0]^{-1} \cdot q^N \cdot \prod_{i=1}^{t} q^{-\dim(G_i)} \# G_i(\mathfrak{o}/\mathfrak{p})\,.$$

Here $N = \sum_{i=1}^t d_i + d s_i m_i m_i'$ where $d = \dim_{\mathfrak{o}/\mathfrak{p}}(\mathcal{O}/\mathfrak{P})$ and

$$d_i = \begin{cases} t m_i^2 & \text{if } \dim_K(E) = 2,\ \mathfrak{p} \text{ is ramified in } E \text{ and } s_i = 2t \text{ is even,}\\ t m_i^2 + \dim G_i & \text{if } \dim_K(E) = 2,\ \mathfrak{p} \text{ is ramified in } E \text{ and } s_i = 2t+1 \text{ is odd,}\\ t m_i(2m_i - 1) & \text{if } \dim_K(E) = 4,\ \mathfrak{p} \text{ is ramified in } E \text{ and } s_i = 2t \text{ is even,}\\ t m_i(2m_i - 1) + m_i^2 & \text{if } \dim_K(E) = 4,\ \mathfrak{p} \text{ is ramified in } E \text{ and } s_i = 2t+1 \text{ is odd,}\\ s_i(d m_i^2 - \dim G_i) & \text{otherwise.} \end{cases}$$

Proof. See [GY00, Theorem 7.3]. □

For convenience, the dimension d, the type of G_i and the cardinality of $G_i(\mathfrak{o}/\mathfrak{p})$ are given explicitly below.

Lemma 4.2.5 *In the situation of Theorem 4.2.4, the dimension d and the type of G_i are given by the following table.*

$\dim_K(E)$	$\mathfrak{p}$ *in* E	m_i	s_i	$\operatorname{disc}(L_i)$	d	G_i
1	–	*odd*	–	–	1	O_{m_i}
1	–	*even*	–	*square*	1	O_{m_i}
1	–	*even*	–	*non-square*	1	$\mathrm{O}^-_{m_i}$
2	*split*	–	–	–	2	GL_{m_i}
2	*inert*	–	–	–	2	U_{m_i}
2	*ramified*	–	*odd*	–	1	Sp_{m_i}
2	*ramified*	*odd*	*even*	–	1	O_{m_i}
2	*ramified*	*even*	*even*	*square*	1	O_{m_i}
2	*ramified*	*even*	*even*	*non-square*	1	$\mathrm{O}^-_{m_i}$
4	*unramified*	–	–	–	4	Sp_{2m_i}
4	*ramified*	–	*even*	–	2	U_{m_i}
4	*ramified*	–	*odd*	–	2	$\mathrm{Res}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mathrm{Sp}_{m_i})$

Here GL_r, Sp_r, U_r, O_r and O^-_r denote the general linear group, the unitary group as well as the split and non-split orthogonal groups over $\mathbb{F}_q \cong \mathfrak{o}/\mathfrak{p}$ in r variables respectively.

Further, $\mathrm{Res}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mathrm{Sp}_r)$ *denotes the symplectic group in r variables over $\mathbb{F}_{q^2}$ viewed as an algebraic group over $\mathbb{F}_q$ via Weil restriction of scalars. The dimensions and numbers of $\mathbb{F}_q$-valued points of these algebraic groups are given below.*

G	$\dim(G)$	$\#G(\mathbb{F}_q)$
GL_m	m^2	$q^{m(m-1)/2}\prod_{j=1}^{m}(q^j-1)$
U_m	m^2	$q^{m(m-1)/2}\prod_{j=1}^{m}(q^j-(-1)^j)$
O_{2k}	$(2k-1)k$	$2(q^k-1)q^{k(k-1)}\prod_{j=1}^{k-1}(q^{2j}-1)$
O_{2k}^-	$(2k-1)k$	$2(q^k+1)q^{k(k-1)}\prod_{j=1}^{k-1}(q^{2j}-1)$
O_{2k+1}	$(2k+1)k$	$2q^{k^2}\prod_{j=1}^{k}(q^{2j}-1)$
Sp_{2k}	$(2k+1)k$	$q^{k^2}\prod_{j=1}^{k}(q^{2j}-1)$
$\mathrm{Res}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mathrm{Sp}_{2k})$	$2(2k+1)k$	$q^{2k^2}\prod_{j=1}^{k}(q^{4j}-1)$

If $\mathfrak{p}$ is bad, the computation of the local factors is much more involved. For example, [Cho] discusses the case $\mathfrak{p}$ is bad and $K_\mathfrak{p}/\mathbb{Q}_2$ is unramified, see also [Cho15].

Theorem 4.2.3 states Siegel's mass formula as an infinite product of real numbers. Almost all factors are different from 1 and some are not even rational.

Both issues make the evaluation of the mass formula algorithmically difficult. These problems can be addressed by reorganizing the mass formula. For this, different local factors $\lambda(L_\mathfrak{p}) \in \mathbb{Q}$ have to defined such that $\lambda(L_\mathfrak{p}) = 1$ for all but finitely many prime ideals $\mathfrak{p}$ of $\mathfrak{o}$.

Definition 4.2.6 Let L be an $\mathcal{O}$-lattice in (V,Φ) and let $\mathfrak{p}$ be a prime ideal of $\mathfrak{o}$ of norm q. Further, let $H_\mathfrak{p}$ be the quasi-split inner form of G over $K_\mathfrak{p}$. The local factor $\lambda(L_\mathfrak{p})$ is defined as

$$\lambda(L_\mathfrak{p}) = q^{\mathrm{ord}_\mathfrak{p}([L_\mathfrak{p}^\# : L_\mathfrak{p}]_{\mathfrak{o}_\mathfrak{p}})m(V)/2+a_\mathfrak{p}} \cdot \frac{q^{-\dim H_\mathfrak{p}} \cdot \#H_\mathfrak{p}(\mathfrak{o}/\mathfrak{p})}{[H_\mathfrak{p} : H_\mathfrak{p}^0]\cdot \beta(L_\mathfrak{p})}$$

where $m(V)$ is as is Theorem 4.2.3 and $a_\mathfrak{p}$ is determined by the following conditions:

- If $E = K$ and m is even, then

  $$a_\mathfrak{p} = \mathrm{ord}_\mathfrak{p}(\mathrm{d}_{K(\sqrt{d})/K})\cdot(1-m)/2 + \mathrm{ord}_\mathfrak{p}(2)\cdot m$$

  where $\mathrm{disc}(L) = d\cdot (K^*)^2$.

- If $E = K$ and m is odd then $a_\mathfrak{p} = \mathrm{ord}_\mathfrak{p}(2)\cdot(m+1)/2$.

- If $E_\mathfrak{p}/K_\mathfrak{p}$ is a ramified quadratic field extension and m is even, then

  $$a_\mathfrak{p} = \mathrm{ord}_\mathfrak{p}(\mathrm{d}_{E/K})\cdot m/2\,.$$

- If $E_\mathfrak{p}/K_\mathfrak{p}$ is a quaternion skew field, then $a_\mathfrak{p} = m(m+1)/2$.

- In all other cases, $a_\mathfrak{p} = 0$.

By [GHY01], the type of $H_\mathfrak{p}$ is given by the following table.

$\dim_K(E)$	m	condition	$H_\mathfrak{p}$
1	odd	–	O_m
1	even	$\operatorname{disc}(L_\mathfrak{p}) \in (K_\mathfrak{p}^*)^2$	O_m
1	even	$\operatorname{disc}(L_\mathfrak{p}) \notin (K_\mathfrak{p}^*)^2$ and $K_\mathfrak{p}(\sqrt{\operatorname{disc}(L_\mathfrak{p})})/K_\mathfrak{p}$ unramified	O_m^-
1	even	$\operatorname{disc}(L_\mathfrak{p}) \notin (K_\mathfrak{p}^*)^2$ and $K_\mathfrak{p}(\sqrt{\operatorname{disc}(L_\mathfrak{p})})/K_\mathfrak{p}$ ramified	O_{m-1}
2	–	$E_\mathfrak{p}/K_\mathfrak{p}$ split	GL_m
2	–	$E_\mathfrak{p}/K_\mathfrak{p}$ inert	U_m
2	odd	$E_\mathfrak{p}/K_\mathfrak{p}$ ramified	O_m
2	even	$E_\mathfrak{p}/K_\mathfrak{p}$ ramified	Sp_m
4	–	–	Sp_{2m}

A case by case discussion immediately yields the following version of the mass formula in terms of the $\lambda(L_\mathfrak{p})$.

Proposition 4.2.7 (Siegel's mass formula) *Let L be an $\mathcal{O}$-lattice in (V, Φ) and let γ_m be as in Theorem 4.2.3.*

1. *If $E = K$ and m is odd, then*

$$\operatorname{Mass}(L) = \gamma_m^{-n} \cdot \mathrm{d}_K^{m(m-1)/4} \cdot \prod_{i=1}^{(m-1)/2} \zeta_K(2i) \cdot \prod_\mathfrak{p} \lambda(L_\mathfrak{p})$$
$$= \frac{1}{2^{n(m-1)/2}} \cdot \prod_{i=1}^{(m-1)/2} |\zeta_K(1-2i)| \cdot \prod_\mathfrak{p} \lambda(L_\mathfrak{p}) \,.$$

2. *Suppose $E = K$ and m is even. Let $\operatorname{disc}(V, \Phi) = d \cdot (K^*)^2$ and let χ_d be as in Definition 4.1.7. Then*

$$\operatorname{Mass}(L)$$
$$= \gamma_m^{-n} \cdot \mathrm{d}_K^{m(m-1)/4} \cdot \operatorname{Nr}_{K/\mathbb{Q}}(\mathrm{d}_{F/K})^{(m-1)/2} \prod_{i=1}^{m/2-1} \zeta_K(2i) \cdot \mathfrak{L}_K(\chi_d, m/2) \cdot \prod_\mathfrak{p} \lambda(L_\mathfrak{p})$$
$$= \frac{1}{2^{nm/2}} \cdot \prod_{i=1}^{m/2-1} |\zeta_K(1-2i)| \cdot |\mathfrak{L}_K(\chi_d, 1-m/2)| \cdot \prod_\mathfrak{p} \lambda(L_\mathfrak{p}) \,.$$

3. *Suppose* $\dim_K(E) = 2$. *Let* χ *be the non-trivial character of* $\mathrm{Gal}(E/K)$. *Then*

$$\begin{aligned}\mathrm{Mass}(L) &= 2\gamma_m^{-n} \cdot \mathrm{d}_K^{m^2/2} \cdot \mathrm{Nr}_{K/\mathbb{Q}}(\mathrm{d}_{E/K})^{m(m-(-1)^m)/4} \prod_{i=1}^{m} \mathfrak{L}_K(\chi^i, i) \cdot \prod_{\mathfrak{p}} \lambda(L_\mathfrak{p}) \\ &= \frac{2}{2^{n(m-1)}} \cdot \frac{\#\,\mathrm{Cl}(E)}{\#\,\mathrm{Cl}(K) \cdot \#\mu(E) \cdot Q} \cdot \prod_{i=2}^{m} |\mathfrak{L}_K(\chi^i, 1-i)| \cdot \prod_{\mathfrak{p}} \lambda(L_\mathfrak{p}) \\ &= \frac{2}{2^{nm}} \cdot \prod_{i=1}^{m} |\mathfrak{L}_K(\chi^i, 1-i)| \cdot \prod_{\mathfrak{p}} \lambda(L_\mathfrak{p})\end{aligned}$$

where $Q = [\mathcal{O}^* : \mu(E)\mathfrak{o}^*] \in \{1, 2\}$ *denotes the Hasse unit index of* E/K.

4. *If* $\dim_K(E) = 4$, *then*

$$\begin{aligned}\mathrm{Mass}(L) &= \gamma_m^{-n} \cdot \mathrm{d}_K^{m(m+1/2)} \cdot \prod_{i=1}^{m} \zeta_K(2i) \cdot \prod_{\mathfrak{p}} \lambda(L_\mathfrak{p}) \\ &= \frac{1}{2^{nm}} \cdot \prod_{i=1}^{m} |\zeta_K(1-2i)| \cdot \prod_{\mathfrak{p}} \lambda(L_\mathfrak{p})\,.\end{aligned}$$

For the remainder of this section, some properties of $\lambda(L_\mathfrak{p})$ are collected, that will be useful later on.

Definition 4.2.8 For integers n, m, q such that $0 \le m \le n$, let

$$\binom{n}{m}_q := \frac{\prod_{i=1}^{n}(1-q^i)}{\prod_{i=1}^{m}(1-q^i) \cdot \prod_{i=1}^{n-m}(1-q^i)}$$

be the *Gaußian binomial coefficient*. Note that $\binom{n}{m}_q$ is always an integer. For example if q is a prime power, then $\binom{n}{m}_q$ is simply the number of m-dimensional subspaces of a n-dimensional vector space over $\mathbb{F}_q$.

For good prime ideals $\mathfrak{p}$, the factors $\beta(L_\mathfrak{p})$ are given by Theorem 4.2.4. Hence the computation of $\lambda(L_\mathfrak{p})$ at good prime ideals is straight forward. Below are some local factors that will be needed later on.

Lemma 4.2.9 *Let* $\mathfrak{p}$ *be a good prime ideal of* $\mathfrak{o}$ *and let* $\mathfrak{P}$ *be the largest twosided ideal of* $\mathcal{O}$ *over* $\mathfrak{p}$ *that is invariant under* $^-$. *Let* $L_\mathfrak{p} = L_0 \perp L_1$ *be an* $\mathcal{O}$*-lattice in* $(V_\mathfrak{p}, \Phi)$ *such that* L_i *is* $\mathfrak{P}^i$*-modular. Write* $m_i = \mathrm{rank}(L_i)$ *and set* $q = \mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})$. *Then* $\lambda(L_\mathfrak{p})$ *is given by the following table:*

$\dim_K(E)$	m	$E_\mathfrak{p}/K_\mathfrak{p}$	$\lambda(L_\mathfrak{p})$
1	*odd*	–	$\begin{cases} \frac{1}{2}(q^{m_0/2}+\varepsilon_0)\binom{(m-1)/2}{m_0/2}_{q^2} & \textit{if } m_0 \textit{ is even,} \\ \frac{1}{2}(q^{m_1/2}+\varepsilon_1)\binom{(m-1)/2}{m_1/2}_{q^2} & \textit{if } m_1 \textit{ is even} \end{cases}$
1	*even*	–	$\begin{cases} \frac{1}{2}\binom{m/2-1}{(m_0-1)/2}_{q^2} & \textit{if } m_0 \textit{ and } m_1 \textit{ are odd,} \\ \frac{(q^{m_0/2}+\varepsilon_0)(q^{m_1/2}+\varepsilon_1)}{2(q^{m/2}+\varepsilon_0\varepsilon_1)}\binom{m/2}{m_0/2}_{q^2} & \textit{otherwise} \end{cases}$
2	–	*split*	$\binom{m}{m_0}_q$
2	–	*inert*	$\lvert\binom{m}{m_0}_{-q}\rvert$
2	*odd*	*ramified*	$\frac{1}{2}\binom{(m-1)/2}{m_1/2}_{q^2}$
2	*even*	*ramified*	$\frac{1}{2}(q^{m_0/2}+\varepsilon_0)\binom{m/2}{m_1/2}_{q^2}$
4	–	*unramified*	$\binom{m}{m_0}_{q^2}$
4	–	*ramified*	$\prod_{j=1}^{m_0}(q^j+(-1)^j)\cdot\prod_{j=1}^{m_1/2}(q^{4j-2}-1)\cdot\binom{m}{m_1}_{q^2}$

Here $\varepsilon_i = +1$ *if* $\operatorname{disc}(L_i) \in (K_\mathfrak{p}^*)^2$ *and* $\varepsilon_i = -1$ *otherwise.*

Proposition 4.2.10 *Let L and M be $\mathcal{O}$-lattices in (V, Φ) and let $\mathfrak{p}$ be a prime ideal of $\mathfrak{o}$. Then*

1. $\lambda(L_\mathfrak{p}) \in \mathbb{Q}$.
2. *The set* $\{\mathfrak{p} \in \mathbb{P}(\mathfrak{o})\,;\, \lambda(L_\mathfrak{p}) \neq 1\}$ *is finite.*
3. $\lambda(L_\mathfrak{p}) = \lambda(L_\mathfrak{p}^c)$ *for all* $c \in K_\mathfrak{p}^*$.
4. *Suppose* $E \neq K$. *Then* $\lambda(L_\mathfrak{p}) \in \frac{1}{2}\mathbb{Z}$. *Further, if* $\lambda(L_\mathfrak{p}) \notin \mathbb{Z}$, *then m is odd and $E_\mathfrak{p}/K_\mathfrak{p}$ is a ramified quadratic field extension.*
5. *If* $L_\mathfrak{q} = M_\mathfrak{q}$ *for all* $\mathfrak{q} \in \mathbb{P}(\mathfrak{o}) - \{\mathfrak{p}\}$, *then*
$$\operatorname{Mass}(M) = \operatorname{Mass}(L) \cdot \frac{\lambda(M_\mathfrak{p})}{\lambda(L_\mathfrak{p})}\,.$$

Proof. The first assertion is Corollary 4.3.6, while the second follows immediately from Lemma 4.2.9. The last statement is trivial and the fourth follows from a case by case discussion using Lemma 4.2.9 and Theorems 4.5.2 and 4.5.5.
The third assertion is clear if $c \in \mathfrak{o}_\mathfrak{p}^*$. Hence one only has to discuss the case that $\operatorname{ord}_\mathfrak{p}(c) = 1$. But then, one may assume that $c \in K^*$ is totally positive and $c\mathfrak{o} = \mathfrak{p}\mathfrak{q}$ for some good prime ideal $\mathfrak{q}$ of $\mathfrak{o}$ such that $L_\mathfrak{q}$ is unimodular. Then $\lambda(L_\mathfrak{a}^c) = \lambda(L_\mathfrak{a})$ for all $\mathfrak{a} \in \mathbb{P}(\mathfrak{o}) - \{\mathfrak{p}, \mathfrak{q}\}$ and also for $\mathfrak{a} = \mathfrak{q}$ by Lemma 4.2.9. Moreover, L and L^c have the same mass. But then the formulation of Siegel's mass formula given in Proposition 4.2.7 shows that $\lambda(L_\mathfrak{p}) = \lambda(L_\mathfrak{p}^c)$. □

4.3 Comparing local factors

The purpose of this section is to present a practical method to compare the local factors of two $\mathfrak{o}$-lattices in (V, Φ). This result will be employed later to compute the missing local factors of square-free lattices whenever $\dim_K(E) = 2$. The method is taken from the article [BN97] of Ch. Bachoc and G. Nebe and it can also be deduced from Section 17 of M. Eichler's book [Eic52]. I would like to thank R. Schulze-Pillot for pointing out this reference.

In this section, $\mathfrak{p}$ always denotes a prime ideal of $\mathfrak{o}$.

Definition 4.3.1 Given $\mathcal{O}_\mathfrak{p}$-lattices M and L in $(V_\mathfrak{p}, \Phi)$ the following two sets of lattices are defined:

$$\begin{aligned} D(L, M) &= \{X \subseteq L \mid X \text{ an } \mathcal{O}_\mathfrak{p}\text{-lattice isometric to } M\}, \\ U(L, M) &= \{X \supseteq M \mid X \text{ an } \mathcal{O}_\mathfrak{p}\text{-lattice isometric to } L\}. \end{aligned}$$

Remark 4.3.2 Let $M \subseteq L$ be $\mathcal{O}_\mathfrak{p}$-lattices in $(V_\mathfrak{p}, \Phi)$. Taking duals induces bijections

$$D(L, M) \longleftrightarrow U(M^\#, L^\#) \quad \text{and} \quad U(L, M) \longleftrightarrow D(M^\#, L^\#)\,.$$

Hence, the computation of D can be turned into the computation of some suitable set U. The latter is usually more convenient to compute.

Definition 4.3.3 Let $\mathfrak{a}$ be a fractional ideal of $\mathfrak{o}$. Given any $\mathcal{O}$-lattice L in (V, Φ), let

$$^{\mathfrak{a}}L := \{x \in L\,;\, \Phi(x, x) \in \mathfrak{a}\}\,.$$

A similar definition is made for $\mathcal{O}_\mathfrak{p}$-lattices in $(V_\mathfrak{p}, \Phi)$.

Remark 4.3.4 Let $\mathfrak{a}$ be a fractional ideal of $\mathfrak{o}$ and let L be an $\mathcal{O}$-lattice L in (V, Φ). Then $^{\mathfrak{a}}L$ is an $\mathcal{O}$-lattice if and only if $\mathrm{T}(\mathfrak{s}(L)) \subseteq \mathfrak{a}$. If this is the case, then $^{\mathfrak{a}}L$ is the maximal $\mathcal{O}$-sublattice of L with norm contained in $\mathfrak{a}$ and thus $\#D(L_\mathfrak{p}, {}^{\mathfrak{a}}L_\mathfrak{p}) = 1$ for all $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$.

Proposition 4.3.5 *Let L and M be $\mathcal{O}$-lattices in (V, Φ) such that $M_\mathfrak{p} \subseteq L_\mathfrak{p}$. Then*

$$\lambda(M_\mathfrak{p}) \cdot \#U(L_\mathfrak{p}, M_\mathfrak{p}) = \lambda(L_\mathfrak{p}) \cdot \#D(L_\mathfrak{p}, M_\mathfrak{p})\,.$$

Proof. The proof follows [BN97] and [Eic52, S. 111]. Without loss of generality, $L_\mathfrak{q} = M_\mathfrak{q}$ for all prime ideals $\mathfrak{q} \neq \mathfrak{p}$ of $\mathfrak{o}$. So by Proposition 4.2.10/5, it suffices to show that

$$\mathrm{Mass}(M) \cdot \#U(L_\mathfrak{p}, M_\mathfrak{p}) = \mathrm{Mass}(L) \cdot \#D(L_\mathfrak{p}, M_\mathfrak{p})\,.$$

Let $L_1, \ldots, L_h$ and $M_1, \ldots, M_s$ represent the isometry classes in $\mathrm{gen}(L)$ and $\mathrm{gen}(M)$ respectively. Further, let

$$\begin{aligned} a_{ij} &= \#\{X \subseteq L_i \mid X \text{ an } \mathcal{O}\text{-lattice isometric to } M_j\}\,, \\ b_{ji} &= \#\{X \supseteq M_j \mid X \text{ an } \mathcal{O}\text{-lattice isometric to } L_i\}\,. \end{aligned}$$

Then $\sum_j a_{ij} = \#D(L_\mathfrak{p}, M_\mathfrak{p})$ and similarly $\sum_i b_{ji} = \#U(L_\mathfrak{p}, M_\mathfrak{p})$. Suppose $\varphi, \varphi' \in U(V, \Phi)$ such that $\varphi(M_j), \varphi'(M_j) \subseteq L_i$ with $\varphi(M_j) = \varphi'(M_j)$. Then $\varphi^{-1} \circ \varphi' \in \operatorname{Aut}(M_j)$ and thus

$$\begin{aligned} a_{ij} \cdot \# \operatorname{Aut}(M_j) &= \#\{\varphi \in U(V, \Phi) \mid \varphi(M_j) \subseteq L_i\} \\ &= \#\{\psi \in U(V, \Phi) \mid M_j \subseteq \psi(L_i)\} = b_{ji} \cdot \# \operatorname{Aut}(L_i)\,. \end{aligned}$$

Putting everything together, one obtains

$$\begin{aligned} \#D(L_\mathfrak{p}, M_\mathfrak{p}) \cdot \operatorname{Mass}(L) &= \sum_{j=1}^{s} \sum_{i=1}^{h} \frac{a_{ij}}{\# \operatorname{Aut}(L_i)} \\ &= \sum_{j=1}^{s} \sum_{i=1}^{h} \frac{b_{ji}}{\# \operatorname{Aut}(M_j)} = \#U(L_\mathfrak{p}, M_\mathfrak{p}) \cdot \operatorname{Mass}(M) \end{aligned}$$

as claimed. □

Corollary 4.3.6 *Let L be an $\mathcal{O}$-lattice in (V, Φ). Then $\lambda(L_\mathfrak{p}) \in \mathbb{Q}$ for all $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$.*

Proof. By Proposition 4.2.10 one may assume that L is integral. So L is contained in some $\mathfrak{o}$-maximal lattice M. Then $\lambda(M_\mathfrak{p}) \in \mathbb{Q}$ by work of G. Shimura [Shi97, Shi99a, Shi99b], see also [GHY01]. But then $\lambda(L_\mathfrak{p}) \in \mathbb{Q}$ by Proposition 4.3.5. □

4.4 Local factors of unimodular quadratic lattices

Let (V, Φ) be a definite quadratic space of dimension m over $E = K$. The local factors of (unimodular) $\mathfrak{o}$-lattices in (V, Φ) are known at all good primes, c.f. Lemma 4.2.9. The purpose of this section is to work out the local factors of unimodular lattices at any prime ideal $\mathfrak{p}$ over 2.

The norm and the ramification index of $\mathfrak{p}$ will be denoted by q and e respectively. Further, let p be a uniformiser of $\mathfrak{p}$. Let M be a $2\mathfrak{o}_\mathfrak{p}$-maximal $\mathfrak{o}_\mathfrak{p}$-lattice in $(V_\mathfrak{p}, \Phi)$. Given any unimodular $\mathfrak{o}_\mathfrak{p}$-lattice L in $(V_\mathfrak{p}, \Phi)$, let

$$\lambda'(L) := \lambda(L)/\lambda(M)\,.$$

The factor $\lambda(M)$ is well known by the work of G. Shimura and only depends on the isometry type of $(V_\mathfrak{p}, 2\Phi)$:

Theorem 4.4.1 *Let M be an $\mathfrak{o}_\mathfrak{p}$-lattice in $(V_\mathfrak{p}, \Phi)$ and let $d = \operatorname{disc}(V_\mathfrak{p}, \Phi)$. If M is $\mathfrak{p}^k$-maximal, then $\lambda(M)$ is given by the following table.*

m	$\omega(V_\mathfrak{p}, p^k\Phi)$	*additional condition*	$\lambda(M)$
$2r+1$	-1	$k + \operatorname{ord}_\mathfrak{p}(d)$ *even and* $m > 1$	$\frac{q^{m-1}-1}{2(q+1)}$
$2r+1$	± 1	$k + \operatorname{ord}_\mathfrak{p}(d)$ *odd and* $m > 1$	$\frac{q^r+\omega(V_\mathfrak{p}, p^k\Phi)}{2}$
$2r$	-1	$d \in (K_\mathfrak{p}^*)^2$	$\frac{(q^{r-1}-1)(q^r-1)}{2(q+1)}$
$2r$	-1	$d \notin (K_\mathfrak{p}^*)^2$ *and* $\mathfrak{p}$ *does not ramify in* $K_\mathfrak{p}(\sqrt{d})$	$\frac{(q^{r-1}+1)(q^r+1)}{2(q+1)}$
$2r$	± 1	$d \notin (K_\mathfrak{p}^*)^2$ *and* $\mathfrak{p}$ *ramifies in* $K_\mathfrak{p}(\sqrt{d})$	$\frac{1}{2}$
all other cases			1

Proof. See Shimura [Shi99a] or Gan-Hanke-Yu [GHY01]. □

Proposition 4.4.2 *Let $L = L_0 \perp L_1$ be an integral $\mathfrak{o}_\mathfrak{p}$-lattice in $(V_\mathfrak{p}, \Phi)$ such that L_0 is unimodular, $\mathfrak{n}(L_0) = 2\mathfrak{o}_\mathfrak{p}$ and $\mathfrak{n}(L_1) \subseteq 2\mathfrak{p}$.*

1. *The map*

$$Q\colon L_0/\mathfrak{p}L_0,\ x + \mathfrak{p}L_0 \mapsto Q_\Phi(x)/2 + \mathfrak{p}$$

is a well-defined quadratic form on the $\mathfrak{o}/\mathfrak{p}$-space $L_0/\mathfrak{p}L_0$.

2. *For any primitive vector $w \in L_0$, set $L_w := \{x \in L\,;\, \Phi(x,w) \in \mathfrak{p}\}$. Let $v \in L_0$ be a fixed primitive vector. If $\operatorname{ord}_\mathfrak{p}(Q_\Phi(v)) = e$, let X denote the set of anisotropic lines in $(L_0/\mathfrak{p}L_0, Q)$, otherwise let X denote the set of all isotropic lines. Then*

$$\sigma\colon X \to D(L, L_v),\ \langle w + \mathfrak{p}L_0\rangle \mapsto L_w$$

is a bijection.

Proof. The first assertion is clear. For the proof of the second, note that σ does not depend on the representative w. Suppose now that $\langle w + \mathfrak{p}L_0\rangle \in X$. There exists some isometry in $\mathbf{O}(L_0/\mathfrak{p}L_0, Q)$ that maps $\langle v + \mathfrak{p}L_0\rangle$ to $\langle w + \mathfrak{p}L_0\rangle$. By [Kne02, Satz 15.6], it lifts to some isometry of L_0 and therefore to some element $\varphi \in \operatorname{Aut}(L)$. Thus $L_w = L_{\varphi(v)} = \varphi(L_v) \in D(L, L_v)$. Hence σ is well-defined. Since L_0 is unimodular, the map σ is also one to one. It remains to show that it is onto. Let $M \in D(L, L_v)$. Then there exists some $\varphi \in \mathbf{O}(V_\mathfrak{p}, \Phi)$ such that $\varphi(L_v) = M$. Let $w := \varphi(v)$. From $v \in L_v$ it follows that $w \in M \subseteq L$. Hence, $w = w_0 + w_1$ for some $w_i \in L_i$. Then $M = \varphi(L_v) = L_w = L_{w_1}$. Further, $Q_\Phi(v) \in 2\mathfrak{p} \iff Q_\Phi(w_0) \in 2\mathfrak{p}$. Thus $\langle w_0 + \mathfrak{p}L_0\rangle \in X$. □

Since the number of (an)isotropic lines in regular quadratic spaces over finite fields are well known (see for example [Kne02, Section IV.13]), the above proposition can be made effective.

Corollary 4.4.3 *Suppose the notation of Proposition 4.4.2. Let m_0 be the rank of L_0 and let $r = \lfloor \frac{m_0}{2} \rfloor$. Then*

$$\begin{aligned}\#D(L, L_v) &= (q-1)^{-1} \cdot \begin{cases} (q^r - \varepsilon)(q^{m_0 - r - 1} + \varepsilon) & \text{if } \operatorname{ord}_\mathfrak{p}(Q_\Phi(v)) > e,\\ q^{m_0} - 1 - (q^r - \varepsilon)(q^{m_0 - r - 1} + \varepsilon) & \text{if } \operatorname{ord}_\mathfrak{p}(Q_\Phi(v)) = e,\end{cases}\\ &= \begin{cases} (q-1)^{-1}(q^r - \varepsilon)(q^{m_0 - r - 1} + \varepsilon) & \text{if } \operatorname{ord}_\mathfrak{p}(Q_\Phi(v)) > e,\\ q^{r-1}(q^r - \varepsilon) & \text{if } \operatorname{ord}_\mathfrak{p}(Q_\Phi(v)) = e \text{ and } m_0 \text{ is even},\\ q^{m_0 - 1} & \text{if } \operatorname{ord}_\mathfrak{p}(Q_\Phi(v)) = e \text{ and } m_0 \text{ is odd},\end{cases}\end{aligned}$$

where $\varepsilon = -1$ if $(L_0/\mathfrak{p}L_0, Q)$ is non-hyperbolic of even degree, and $\varepsilon = +1$ otherwise.

Theorem 4.4.4 *Let L be a unimodular $\mathfrak{o}_\mathfrak{p}$-lattice in $(V_\mathfrak{p}, \Phi)$ of weight $\mathfrak{p}^b$. Suppose that $m = \dim_K(V) = 2r+1$ is odd. Then*

$$\lambda'(L) = \begin{cases} 1 & \text{if } b = e, \\ (q^r - \omega(V_\mathfrak{p}, \Phi))q^{r(e-b-1)} & \text{if } e > b \text{ and } e \text{ is odd}, \\ \frac{1}{2}(q^{2r}-1)q^{r(e-b-1)} & \text{if } e > b,\ e \text{ is even and } \omega(V_\mathfrak{p}, \Phi) = +1, \\ (q+1)q^{r(e-b-1)} & \text{if } e > b,\ e \text{ is even and } \omega(V_\mathfrak{p}, \Phi) = -1. \end{cases}$$

Proof. Let $\Delta = 1 - 4\varrho \in \mathfrak{o}^*$ such that $\mathfrak{d}(\Delta) = 4\varrho\mathfrak{o} = 4\mathfrak{o}$. If $\omega(V_\mathfrak{p}, \Phi) = 1$ set $\delta = 0$, otherwise set $\delta = \varrho$. There exists some Jordan decomposition $L = \langle x, y\rangle \perp \langle z\rangle \perp H$ where $\mathrm{G}(x, y) = A(p^b, 4\delta p^{-b})$ and $Q_\Phi(z) \in \mathfrak{o}^*$ and $H \cong H(0)^{r-1}$.
Suppose first that $b = e$. Then ${}^{2\mathfrak{o}_\mathfrak{p}}L \subseteq L \subseteq ({}^{2\mathfrak{o}_\mathfrak{p}}L)^\#$ and the quotient $({}^{2\mathfrak{o}_\mathfrak{p}}L)^\# / {}^{2\mathfrak{o}_\mathfrak{p}}L$ is cyclic. Thus $\lambda'(L) = \lambda'({}^{2\mathfrak{o}_\mathfrak{p}}L) = 1$ since ${}^{2\mathfrak{o}_\mathfrak{p}}L$ is $2\mathfrak{o}_\mathfrak{p}$-maximal.
From now on, it is assumed that $b < e$. By Proposition 3.3.8 this implies that b is odd. Let $M_1 = {}^{\mathfrak{p}^b}L$ and $M_2 = {}^{\mathfrak{p}^{b+1}}L$. Then again $\lambda'(L) = \lambda'(M_1)$ since $M_1^\#/M_1$ is cyclic. Suppose $X \in U(M_1, M_2) - \{M_1\}$. Then $X = \langle M_2, v\rangle$ for some $v \in M_2^\# \cap p^{-1}M_2$. Together with $Q_\Phi(v)\mathfrak{o} = \mathfrak{n}(M_1) = \mathfrak{p}^b$ this shows that one can assume $v = \mu x + p^{-1}y$ for some $\mu \in \mathfrak{o}$. Further, $Q_\Phi(v)\mathfrak{o} = \mathfrak{p}^b$ shows that $\mu \notin \mathfrak{p}$ if $b \le e-2$ and $\mu + 2p^{-e} \notin \mathfrak{p}$ if $b = e-1$ and $\omega(V_\mathfrak{p}, \Phi) = 1$. Conversely, Theorem 3.3.13 shows that all parameters μ satisfying these conditions yield a lattice X isometric to M_1. Hence

$$\lambda'(L) = \lambda'(M_2) \cdot \begin{cases} q - \omega(V_\mathfrak{p}, \Phi) & \text{if } b = e-1, \\ q & \text{if } b \le e-2. \end{cases}$$

If $b = e-1$ and $\omega(V_\mathfrak{p}, \Phi) = -1$ then Remark 3.1.4/2 shows that M_2 is $2\mathfrak{o}_\mathfrak{p}$-maximal and therefore $\lambda'(L) = q+1$. Suppose now $b = e-1$ and $\omega(V_\mathfrak{p}, \Phi) = +1$. Then $N := \langle M_2, p^{-1}y\rangle$ is $2\mathfrak{o}_\mathfrak{p}$-maximal. Let $X \supseteq M_2$ be an integral lattice of norm $\mathfrak{p}^{b+1}$ not isometric to M_1 such that $[X : M_2]_\mathfrak{o} = \mathfrak{p}$. As seen before, there are only two such lattices, namely N and $X' = \langle M_2, -2p^{-e}x + p^{-1}y\rangle$. Hence $U(N, M_2) = \{N, X'\}$. Further, $\#D(N, M_2) = (q-1)^{-1}(q^{2r}-1)$ by Corollary 4.4.3 and N is $2\mathfrak{o}_\mathfrak{p}$-maximal. Hence

$$\lambda'(L) = (q-1) \cdot \lambda'(M_2) = (q-1) \cdot \frac{1}{2}\frac{q^{2r}-1}{q-1} \cdot \lambda'(N) = \frac{q^{2r}-1}{2}\,.$$

So only the case $b \le e-2$ remains. Let $\tilde{L} = \langle px, p^{-1}y, z\rangle \perp H$. Then $\tilde{L}$ is unimodular with weight $\mathfrak{p}^{b+2}$. Let $\tilde{M} = {}^{\mathfrak{p}^{b+2}}\tilde{L}$. Then $\lambda'(\tilde{L}) = \lambda'(\tilde{M})$ as seen before. Let $M_3 = {}^{\mathfrak{p}^{b+2}}L$. Using similar arguments as before, one obtains $\#U(M_2, M_3) = 1 = \#U(\tilde{M}, M_3)$. Thus

$$\lambda'(L) = q \cdot \lambda'(M_3) = q \cdot \#D(\tilde{M}, M_3) \cdot \lambda'(\tilde{L})\,.$$

So it remains to compute $\#D(\tilde{M}, M_3) = \#U(M_3^\#, \tilde{M}^\#)$. If $b = e-2$, then $\#D(\tilde{M}, M_3) = q^{r-1}(q^r - \omega(V_\mathfrak{p}, \Phi))$ by Corollary 4.4.3. Suppose now $b < e-2$ and $X \in U(M_3^\#, \tilde{M}^\#)$. The conditions $\mathfrak{n}(X) = \mathfrak{n}(M_3^\#) = \mathfrak{p}^{-b-3}$ and $\mathfrak{n}(X^{\mathfrak{p}^{-1}}) = \mathfrak{n}((M_3^\#)^{\mathfrak{p}^{-1}}) = \mathfrak{p}^b$ imply that

$X = \langle \tilde{M}^\#, v\rangle$ with $v = x + \mu p^{-1}y + p^{-1}h$ where $\mu \in \mathfrak{o}$ and $h \in H$. Conversely, by Theorem 3.3.13, each such vector v yields some lattice in $U(M_3^\#, \tilde{M}^\#)$. Hence $\#D(\tilde{M}, M_3) = q^{2r-1}$ and therefore $\lambda'(L) = q^{2r} \cdot \lambda'(\tilde{L})$. The result now follows by induction on b. □

To simplify the presentation of the local factors, the following symbol will be used:

Definition 4.4.5 Given a unimodular lattice L in $(V_\mathfrak{p}, \Phi)$ let

$$\varepsilon(L) = \begin{cases} +1 & \text{if } \mathfrak{d}(\operatorname{disc}(L)) = (0), \\ -1 & \text{if } \mathfrak{d}(\operatorname{disc}(L)) = 4\mathfrak{o}_\mathfrak{p}, \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 4.4.6 *Let L be a unimodular $\mathfrak{o}_\mathfrak{p}$-lattice in $(V_\mathfrak{p}, \Phi)$. Further, let $\mathfrak{n}(L) = \mathfrak{p}^a$, $\mathfrak{w}(L) = \mathfrak{p}^b$ and $\mathfrak{d}(-\det(L_\mathfrak{p})) = \mathfrak{p}^c$. If $m = \dim_K(V) = 2$, then*

$$\lambda'(L) = \begin{cases} q^{\lfloor \frac{e-a-1}{2} \rfloor}(q - \varepsilon(L)) & \textit{if } a < b = e \le c/2, \\ 2q^{\lfloor \frac{c-e-a}{2} \rfloor} & \textit{if } b = e \textit{ and } a + e + 1 \le c < 2e, \\ 1 & \textit{otherwise.} \end{cases}$$

Proof. Propositions 3.3.8 and 3.3.11 show that $c \ge a + b \ge 2a$. Moreover, if $a = b$ then $a = e$. So L is $2\mathfrak{o}_\mathfrak{p}$-maximal in that case and therefore $\lambda'(L) = 1$. Similarly, if $c = 2a + 1$, then $b = a + 1$ and L is $\mathfrak{p}^a$-maximal. In any of these two cases, Theorem 4.4.1 shows that L has the same local density then any $2\mathfrak{o}_\mathfrak{p}$-maximal lattice in $(V_\mathfrak{p}, \Phi)$. Hence $\lambda'(L) = 1$.

Suppose now $a \le e - 1$ and $c \ge 2a + 2$. Let α, γ be as in Proposition 3.3.11 and fix some basis (x, y) of L with Gram matrix $A(\alpha, -\gamma\alpha^{-1})$. Let $M := {}^{\mathfrak{p}^{a+1}}L = \langle px, y\rangle$. Remark 4.3.4 shows

$$\lambda'(L) = \#U(L, M) \cdot \lambda'(M)\,.$$

The rescaled lattice $M^{p^{-1}}$ has norm generator $p\alpha$, determinant $-(1+\gamma)$ and weight $\mathfrak{p}^{b'}$ where $b' = b - 1$ if $c = a + b$ and $b' = e$ otherwise. So once $\#U(L, M)$ has been worked out, one can finish the proof by induction on a.

Suppose first $a = e - 1$. Then $b = e$ and the case $c = 2e - 1$ has already been discussed above, which leaves $c \ge 2e$. Then $(M^\#)^p$ is unimodular and Corollary 4.4.3 shows that

$$\#U(L, M) = \#D((M^\#)^p, L^p) = q - \omega(V_\mathfrak{p}, \Phi)\,.$$

So only the case where $a \le e - 2$ and $c \ge 2a + 2$ remains. Let $L' \in U(L, M)$. Then $L' = \langle M, v/p\rangle$ for some $v \in M$. Write $v = \mu x p + \nu y$ with $\mu, \nu \in \mathfrak{o}$. Then $\mathfrak{n}(L') = \mathfrak{p}^a$ implies $\mu \in \mathfrak{o}^*$ and so one may assume that $\mu = 1$. Then L and L' are both unimodular, have weight $\mathfrak{p}^b$ and norm generators α and $\alpha' := \Phi(x + \nu y/p, x + \nu y/p)$ respectively. Theorem 3.3.13 shows that $L \cong L'$ if and only if the quadratic defect of

$$\alpha'/\alpha = 1 + 2\nu\alpha^{-1}/p - \nu^2\gamma\alpha^{-2}/p^2$$

is contained in $\mathfrak{p}^{b-a}$. A case by case discussion yields

$$\#U(L,M) = \begin{cases} 2 & \text{if } b = e \text{ and } c = e+a+1, \\ q & \text{if } b = e \text{ and } e-a \text{ is odd and } c > e+a+1, \\ 1 & \text{otherwise.} \end{cases}$$

The result now follows by induction on a. □

As a consequence of the previous result, one obtains the mass factors for unimodular lattices L where $\operatorname{ord}_\mathfrak{p}(\mathfrak{n}(L)\mathfrak{w}(L))$ is even.

Lemma 4.4.7 *Let $L = L_1 \perp L_2$ be an $\mathfrak{o}_\mathfrak{p}$-lattice in $(V_\mathfrak{p}, \Phi)$. Suppose that L_2 is unimodular with $\mathfrak{n}(L_2) = 2\mathfrak{o}_\mathfrak{p}$ and L_1 is a $\mathfrak{p}^s$-modular binary lattice such that $s < 0$ and $\mathfrak{d}(-\det(L_1)) \subseteq 2\mathfrak{p}^{2s+1}\mathfrak{n}(L)$. Further let $x \in L_1$ such that $Q_\Phi(x)\mathfrak{o} = \mathfrak{n}(L_1)$ and let $z \in L_2$. Let $M_1 := \langle (x+z)/p, L_1\rangle$ and $M := \langle (x+z)/p, L\rangle$. Then there exists some splitting $M = M_1 \perp M_2$. Moreover, $M_2 \cong L_2$ and $M_1 \cong \langle x/p, y\rangle$.*

Proof. The condition $s < 0$ implies that M_2 exists, c.f. [O'M73, 82:15] for details. Let $\alpha = Q_\Phi(x) \cdot p^{-2s}$ and write $-\det(L_1) = p^{2s}(1+\gamma)$ where $\gamma\mathfrak{p}^{2s} = \mathfrak{d}(-\det(L))$. By [O'M73, Example 93:17], there exists some $y \in L_1$ such that $L_1 = \langle x, y\rangle$ and $\mathrm{G}(x,y) = p^s A(\alpha, -\gamma\alpha^{-1})$. The lattices $X := \langle x/p, y\rangle$ and L_1 are both $\mathfrak{p}^{s-1}$-modular. The assumption on $\mathfrak{d}(-\det(L_1))$ implies that $\det(M_1) = \det(X)$ and thus $\det(M_2) = \det(L_2)$. In particular, the quadratic spaces KL_1 and KM_1 are isometric. Thus KM_2 is isometric to KL_2. From the description

$$M_2 = \left\{ \left. m\gamma\alpha^{-1}(x+z) + my + v \;\right|\; v \in L_2 \text{ and } m = \tfrac{-\Phi(v,z)}{\gamma\alpha^{-1}Q_\Phi(z) + (1+\gamma)p^s} \right\}$$

and the condition on $\mathfrak{d}(-\det(L_1))$ it is easy to check that M_2 is integral and $\mathfrak{n}(M_2) \subseteq 2\mathfrak{o}_\mathfrak{p}$. Thus M_2 and L_2 are both unimodular lattices of norm $2\mathfrak{o}_\mathfrak{p}$ in isometric spaces. Proposition 3.3.11 shows that $M_2 \cong L_2$ as claimed.
It remains to show that $X \cong M_1$. Both lattices have weight $2\mathfrak{p}^{s-1} + \alpha^{-1}\gamma\mathfrak{p}^s$ and norm generators $\alpha_1 := \alpha p^{s-2}$ and $\alpha_2 := (\alpha p^s + Q_\Phi(z))p^{-2}$ respectively. A case by case discussion shows that the quadratic defect of $\alpha_2/\alpha_1 = 1 + p^{-s}\alpha^{-1}Q_\Phi(z)$ is contained in $2\mathfrak{n}(L_1)^{-1} \subseteq \mathfrak{w}(L_1)/\mathfrak{n}(L_1)$. Hence $X \cong M_1$ by Theorem 3.3.13. □

Lemma 4.4.8 *Let L be a unimodular $\mathfrak{o}_\mathfrak{p}$-lattice in $(V_\mathfrak{p}, \Phi)$. Suppose $m = \dim_K(V) = 2r$ is even and L admits a splitting $L = \tilde{L} \perp M$ where $\tilde{L}$ has rank 2 and $\mathfrak{n}(M) = 2\mathfrak{o}_\mathfrak{p}$. Let $a = \operatorname{ord}_\mathfrak{p}(\mathfrak{n}(L))$, $c = \operatorname{ord}_\mathfrak{p}(\mathfrak{d}(-\det(\tilde{L})))$, $i = \lceil \frac{e-a}{2} \rceil$ and $j = \min\{i, \max\{0, \lfloor \frac{c-e-a}{2} \rfloor\}\}$. Then*

$$\lambda'(L) = \begin{cases} q^{2ir-i-r}(q^r - \varepsilon(L)) & \textit{if } c \geq 2e \textit{ and } a+e \textit{ is even,} \\ \frac{1}{2}q^{(2r-1)(i-1)}(q^r - \varepsilon(L))(q^{r-1} + \varepsilon(L)) & \textit{if } c = \infty \textit{ and } a+e \textit{ is odd,} \\ q^{(i-1)(2r-1)}(q+1) & \textit{if } c = 2e \textit{ and } a+e \textit{ is odd,} \\ 2q^{j(2r-1)} & \textit{if } a+e+1 \leq c < 2e, \\ q^{2j(r-1)} & \textit{otherwise.} \end{cases}$$

Proof. Let α be a norm generator of $\tilde{L}$ and write $-\det(\tilde{L}) = 1 + \gamma$ with $\gamma \in \mathfrak{o}$ such that $\gamma\mathfrak{o} = \mathfrak{d}(-\det(\tilde{L}))$. There exists some basis (x, y) of $\tilde{L}$ with $\mathrm{G}(x, y) = A(\alpha, -\gamma\alpha^{-1})$.
If $X \in U(L, {}^{2\mathfrak{o}_\mathfrak{p}}L)$ then $X \subseteq ({}^{2\mathfrak{o}_\mathfrak{p}}L)^{\#} = ({}^{2\mathfrak{o}_\mathfrak{p}}\tilde{L})^{\#} \perp M$. Thus $\#U(L, {}^{2\mathfrak{o}_\mathfrak{p}}L) = \#U(\tilde{L}, {}^{2\mathfrak{o}_\mathfrak{p}}\tilde{L})$.
For $0 \leq t \leq j$ let $\tilde{L}_t = \langle p^i x, p^{-t} y\rangle$ and $L_t := \tilde{L}_t \perp M$. Then $L_0 = {}^{2\mathfrak{o}_\mathfrak{p}}L$ and L_j is $2\mathfrak{o}_\mathfrak{p}$-maximal, i.e. $\lambda'(L_j) = 1$. Suppose first that $X \in U(L_t, L_{t-1})$ for some $1 \leq t \leq j$. Then $X = \langle L_{t-1}, v/p\rangle$ for some $v \in L_{t-1}$. From $\Phi(v/p, L_{t-1}) \subseteq \Phi(v/p, L_t) \subseteq \mathfrak{o}$, it follows that $v \in \mathfrak{p}L_{t-1}^{\#} \cap L_{t-1}$. Hence one may assume that $v \in \tilde{L}_{t-1}$.
One checks that unless $c = \infty$, $i = t$ and $e - a$ is odd, the condition $\mathfrak{n}(X) = \mathfrak{n}(L_t) \subseteq 2\mathfrak{o}$ implies $X = L_t$ and thus $\#U(L_t, L_{t-1}) = 1$. In the special case that $c = \infty$ and $e - a$ is odd, $L_{i-1} \cong H(1)$ and L_{i-1} has two overlattices isometric to $L_i \cong H(0)$. Hence $\#U(L_i, L_{i-1}) = 2$ in this exceptional case.
If $i = j \geq 1$, then $c \geq 2e$ and Corollary 4.4.3 shows that

$$\#D(L_i, L_{i-1}) = \begin{cases} q^{r-1}(q^r - \varepsilon(L)) & \text{if } a + e \text{ is even,} \\ (q-1)^{-1}(q^r - \varepsilon(L))(q^{r-1} + \varepsilon(L)) & \text{if } a + e \text{ is odd.} \end{cases}$$

Suppose now $1 \leq t \leq \min\{i-1, j\}$. Then every element in $U(L_{t-1}^{\#}, L_t^{\#})$ is of the form $\langle (v+w)/p, L_t\rangle$ with $w \in M$ and v a norm generator of $\tilde{L}_t$. In particular, $\#U(L_{t-1}^{\#}, L_t^{\#}) = q^{2(r-1)} \cdot \#U(\tilde{L}_{t-1}^{\#}, \tilde{L}_t^{\#})$ by Lemma 4.4.7.
Putting everything together yields

$$\lambda'(L) = \lambda'(\tilde{L}) \cdot \begin{cases} q^{2(r-1)(i-1)} \frac{q^{r-1}(q^r - \varepsilon(L))}{q - \varepsilon(\tilde{L})} & \text{if } i = j \geq 1 \text{ and } a + e \text{ is even,} \\ q^{2(r-1)(i-1)} \frac{(q^r - \varepsilon(L))(q^{r-1} + \varepsilon(L))}{2(q-1)} & \text{if } i = j \geq 1 \text{ and } a + e \text{ is odd,} \\ q^{2j(r-1)} & \text{otherwise.} \end{cases}$$

Note that the second case can only occur of $\varepsilon(\tilde{L}) = 1$. The result now follows from Theorem 4.4.6. □

As an immediate consequence from the previous result, one obtains the mass factors of forms of type (II), c.f. Proposition 3.3.11.

Theorem 4.4.9 *Let L be a unimodular $\mathfrak{o}_\mathfrak{p}$-lattice in $(V_\mathfrak{p}, \Phi)$ such that $\mathrm{ord}_\mathfrak{p}(\mathfrak{n}(L)\mathfrak{w}(L))$ is even. Let $a = \mathrm{ord}_\mathfrak{p}(\mathfrak{n}(L))$ and $c = \mathrm{ord}_\mathfrak{p}(\mathfrak{d}(\mathrm{disc}(L)))$. If $m = \dim_K(V) = 2r$ is even, then*

$$\lambda'(L) = \begin{cases} 1 & \text{if } e = a, \\ q^{(e-a)(r-1/2)-r}(q^r - \varepsilon(L)) & \text{if } a < e \leq c/2, \\ 2q^{(c-e-a-1)(r-1/2)} & \text{if } a + e + 1 \leq c < 2e, \\ q^{(c-e-a-1)(r-1)} & \text{otherwise.} \end{cases}$$

Proof. By Proposition 3.3.11, there exists some splitting $L = \tilde{L} \perp M$ where $M \cong H(0)^{r-1}$. The result follows by applying Lemma 4.4.8 to this splitting. □

Theorem 4.4.10 *Let L be an unimodular $\mathfrak{o}_\mathfrak{p}$-lattice in $(V_\mathfrak{p}, \Phi)$ such that $\operatorname{ord}_\mathfrak{p}(\mathfrak{n}(L)\mathfrak{w}(L))$ is odd. Let $a = \operatorname{ord}_\mathfrak{p}(\mathfrak{n}(L))$, $b = \operatorname{ord}_\mathfrak{p}(\mathfrak{w}(L))$, $c = \operatorname{ord}_\mathfrak{p}(\mathfrak{d}(\operatorname{disc}(L)))$ and*

$$c' = \begin{cases} \infty & \textit{if } c = 2e \textit{ and } L \textit{ is of type } (\text{IIIb}) \textit{ c.f. Proposition 3.3.11},\\ 2e & \textit{if } c = \infty \textit{ and } L \textit{ is of type } (\text{IIIb}),\\ c & \textit{otherwise.} \end{cases}$$

If $m = dim_K(V) = 2r \geq 4$ is even, then

$$\lambda'(L) = \begin{cases} \frac{1}{2}q^{(e-a-1)(r-\frac{1}{2})}(q^r - \varepsilon(L))(q^{r-1} + \varepsilon(L)) & \textit{if } b = e \textit{ and } c' = \infty,\\ q^{(e-a-1)(r-\frac{1}{2})}(q+1) & \textit{if } b = e \textit{ and } c' = 2e,\\ \frac{1}{2}q^{s(r-\frac{1}{2})+r}(q^r - \varepsilon(L))(q^{2r-2} - \varepsilon(L)) & \textit{if } b < e \textit{ and } c = c' = \infty,\\ q^{s(r-\frac{1}{2})+r}(q+1) & \textit{if } b < e \textit{ and } c \neq c' = \infty,\\ \frac{1}{2}q^{s(r-\frac{1}{2})+r}(q^{r-1}+1)(q^r - \varepsilon(L))(q^{r-1} + \varepsilon(L)) & \textit{if } b < e \textit{ and } c = c' = 2e\\ q^{s(r-\frac{1}{2})+r}(q^{r-1}+1)(q+1) & \textit{if } b < e \textit{ and } c \neq c' = 2e,\\ 1 & \textit{if } c = a+b,\\ 2q^{(c-e-a)(r-\frac{1}{2})} & \textit{if } a+b < c < 2b = 2e,\\ q^{(c-a-b-2)(r-\frac{1}{2})+1}(q^{2r-2}-1) & \textit{otherwise} \end{cases}$$

where $s = 2e - b - a - 3$.

Proof. Let $\Delta = 1 - 4\varrho \in \mathfrak{o}^*$ such that $\mathfrak{d}(\Delta) = 4\varrho\mathfrak{o} = 4\mathfrak{o}$. If $e = b$ or $c = a + b$, then $L \cong L_1 \perp L_2$ where L_1 is binary and L_2 is unimodular with $\mathfrak{n}(L_2) = 2\mathfrak{o}_\mathfrak{p}$. These cases have been already discussed in Lemma 4.4.8.

Suppose now $b < e$ and $a + b < c$. Let α be a norm generator of L. If L is of type (IIIa), let $\delta = 0$, otherwise let $\delta = \varrho$. There exists some splitting $L = \langle x, y\rangle \perp \langle z, w\rangle \perp H$ where $\mathrm{G}(x, y) = A(\alpha, -(\gamma - 4\delta)\alpha^{-1})$, $\mathrm{G}(z, w) = A(p^b, 4\delta p^{-b})$ and $H \cong H(0)^{r-2}$. Let $M = {}^{\mathfrak{p}^{b+1}}L$ and $\tilde{L} = \langle px, p^{-1}y, z, w\rangle \perp H$. One verifies that $\#U(L, M) = q$ and $\#U(\tilde{L}, M) = 1$. Hence $\lambda'(L) = q \cdot \#U(M^\#, \tilde{L}) \cdot \lambda'(\tilde{L})$.

So it remains to compute $\#U(M^\#, \tilde{L})$. The result then follows by induction on a since $\mathfrak{n}(\tilde{L}) = \mathfrak{p}^{a+2} + \mathfrak{p}^b$. Any element $X \in \#U(M^\#, \tilde{L})$ is of the form $X = \langle \tilde{L}, v\rangle$ with $v = \mu x + \nu p^{-2} y + \eta p^{-1} z + \tau p^{-1} w + p^{-1} h$ where $h \in H$ and $\mu, \nu, \eta, \tau \in \mathfrak{o}$.

Suppose first that $a < e - 2$ and $c > a + b + 2$. The conditions $\operatorname{ord}_\mathfrak{p}(Q_\Phi(v)) = a$ and $\mathfrak{w}(X) = \mathfrak{p}^b$ show that one can assume $\mu = 1$ and $\eta = 0$. Conversely, it follows from Theorem 3.3.13 that any vector v satisfying these two conditions yields some lattice in $U(M^\#, \tilde{L})$. Hence $\#U(M^\#, \tilde{L}) = q^{2(r-1)}$ in this case.

Suppose now $e = a + 2 = b + 1$ and $c \geq 2e$. The condition $\operatorname{ord}_\mathfrak{p}(Q_\Phi(v)) = a$ shows that one can assume $\eta = 0$. Let $W := \langle x, p^{-2}y, H\rangle$. Then $W/\mathfrak{p}W$ equipped with the quadratic form $w + \mathfrak{p}W \mapsto Q_\Phi(w) + \mathfrak{p}^a$ is a regular quadratic space over $\mathfrak{o}/\mathfrak{p}$ and (μ, ν, h) yields an anisotropic line in this space. Conversely, every such line yields some vector $v \in \mathfrak{p}^{-1}\tilde{L}$ with $\operatorname{ord}_\mathfrak{p}(Q_\Phi(v)) = a$ and thus a lattice $X \in U(M^\#, \tilde{L})$ as Theorem 3.3.13 shows. Further, $W/\mathfrak{p}W$ is hyperbolic if and only if $\gamma = 4\delta$. Hence [Kne02, Section IV.13] shows that $\#U(M^\#, \tilde{L}) = q^{r-1}(q^{r-1} - \varepsilon')$ where $\varepsilon' = 1$ if $\gamma = 4\delta$ and -1 otherwise. Finally, suppose $c = a + b + 2$. There exists some splitting $\tilde{L} = \langle \tilde{x}, \tilde{y} \rangle \perp \langle \tilde{z}, \tilde{w} \rangle \perp \tilde{H}$ where $\mathrm{G}(\tilde{x}, \tilde{y}) = A(\alpha p^2, -(\gamma - 4\delta)\alpha^{-1}p^{-2})$, $\mathrm{G}(\tilde{z}, \tilde{w}) = A(p^e, 4\delta p^{-e})$ and $\tilde{H} \cong H(0)^{r-2}$. Any element $X \in U(M^\#, \tilde{L})$ is of the form $\langle \tilde{L}, v/p \rangle$ with $v = \mu\tilde{x} + \nu\tilde{y} + \eta\tilde{w} + \tau\tilde{z} + h$ where $\mu, \nu, \eta, \tau \in \mathfrak{o}$ and $h \in \tilde{H}$. The conditions $\mathfrak{n}(X) = \mathfrak{n}(L)$ and $\mathfrak{w}(X) = \mathfrak{w}(L)$ imply that one may assume $\mu = 1$ and $\nu = 0$. This leaves at most $q^{2(r-1)}$ possibilities for X. All of these lattices except $\langle \tilde{L}, \tilde{x}/p \rangle$ are isometric to $M^\#$ as a direct computation using Theorem 3.3.13 shows. Hence $\#U(M^\#, \tilde{L}) = q^{2(r-1)} - 1$. □

4.5 Local factors of square-free hermitian lattices over ramified dyadic field extensions

Let E/K be a CM-extension of number fields and let (V, Φ) be a definite hermitian space of dimension m over E.

Suppose $\mathfrak{p}$ is a bad prime ideal of $\mathfrak{o}$, i.e. $\mathfrak{p} \mid 2$ and $e := \mathrm{ord}_{\mathfrak{p}}(\mathrm{d}_{E/K}) \geq 2$. Let $\mathfrak{P}$ be the prime ideal of $\mathcal{O}$ above $\mathfrak{p}$ and set $q = \mathrm{Nr}_{E/K}(\mathfrak{p}) = \#\mathfrak{o}/\mathfrak{p}$. As before, π denotes a uniformiser of $\mathfrak{P}$. Then $p := \pi\overline{\pi}$ is a uniformiser of $\mathfrak{p}$.

An $\mathcal{O}$-lattice L in (V, Φ) will be called square-free, if $L_{\mathfrak{p}} = L_0 \perp L_1$ where L_i is $\mathfrak{P}^i$-modular. These lattices will play an important role in the classification of all lattices with given class number, see Chapter 6 for details.

The purpose of this section is to compare the local density of any square-free $\mathcal{O}_{\mathfrak{p}}$-lattice in $(V_{\mathfrak{p}}, \Phi)$ with the local density of some maximal lattice. The latter densities have been worked out by G. Shimura [Shi97] and also by W. Gan, J. Hanke and J.-K. Yu [GHY01]:

Theorem 4.5.1 *Let M be a $\mathfrak{p}^i$-maximal $\mathcal{O}_{\mathfrak{p}}$-lattice in $(V_{\mathfrak{p}}, \Phi)$ for some $i \in \mathbb{Z}$. Then*

$$\lambda(M) = \begin{cases} \frac{1}{2} & \textit{if } m \textit{ is odd,} \\ 1 & \textit{if } (V_{\mathfrak{p}}, \Phi) \textit{ is hyperbolic,} \\ \frac{q^m - 1}{2(q+1)} & \textit{otherwise.} \end{cases}$$

Proof. See Propositions 4.4 and 4.5 of [GHY01]. □

If m is odd, the computation of the local factor $\lambda(L_{\mathfrak{p}})$ is fairly easy.

Theorem 4.5.2 *Let $L := L_0 \perp L_1$ be an $\mathcal{O}_{\mathfrak{p}}$-lattice in $(V_{\mathfrak{p}}, \Phi)$ such that L_i is $\mathfrak{P}^i$-modular. Let $m_i = \mathrm{rank}(L_i)$. If $m = m_0 + m_1$ is odd, then*

$$\lambda(L) = \frac{1}{2} \binom{(m-1)/2}{m_1/2}_{q^2} .$$

Proof. For $0 \leq r \leq (m-1)/2$ let L_r be an $\mathcal{O}_{\mathfrak{p}}$-lattice in $(V_{\mathfrak{p}}, \Phi)$ such that

$$L_r \cong \langle 1 \rangle \perp H(0)^r \perp H(1)^s \quad \text{where } s = (m-1)/2 - r\,. \tag{4.5.1}$$

Theorem 3.3.18 shows that L is similar to $L_{(m_0-1)/2}$. Let

$$(x_0, x_1, y_1, \dots, x_r, y_r, x_1', y_1', \dots, x_s', y_s')$$

be a basis of L_r corresponding to the orthogonal decomposition given in equation (4.5.1). First the local factors $\lambda(L_r)$ and $\lambda(L_{r+1})$ will be compared. The lattices in $U(L_{r+1}, L_r)$ are precisely the lattices of the form $\langle L_r, x/\pi\rangle$ where x is a primitive vector in $\langle x_1', x_2', \dots, x_s', y_s'\rangle$. Thus $\#U(L_{r+1}, L_r) = (q-1)^{-1}(q^{(m-1)-2r} - 1)$. Similarly, one checks that

$$\#D(L_{r+1}, L_r) = \#U(L_r^\#, L_{r+1}^\#) = (q-1)^{-1}(q^{2(r+1)} - 1)\,.$$

Thus

$$\lambda(L_r) = \lambda(L_{(m-1)/2}) \cdot \prod_{i=r}^{(m-3)/2} \frac{q^{2(i+1)} - 1}{q^{(m-1)-2i} - 1} = \lambda(L_{(m-1)/2}) \cdot \binom{(m-1)/2}{(m-1)/2 - r}_{q^2}$$

and

$$\lambda(L_r) = \lambda(L_0) \cdot \prod_{i=0}^{r-1} \frac{q^{(m-1)-2i} - 1}{q^{2i+2} - 1} = \lambda(L_0) \cdot \binom{(m-1)/2}{(m-1)/2 - r}_{q^2}\,.$$

Hence it suffices to show that $\lambda(L_0) = 1/2$ or $\lambda(L_{(m-1)/2}) = 1/2$.
Suppose first that e is even and set $f = e/2$. To ease notation, write M for $L_{(m-1)/2}$. Then ${}^{\mathfrak{p}^f}M$ is $\mathfrak{p}^f$-maximal and $\#D(M, {}^{\mathfrak{p}^f}M) = 1$ as explained in Remark 4.3.4. Conversely, $\#U(M, {}^{\mathfrak{p}^f}M) = 1$ since $({}^{\mathfrak{p}^f}M)^\#/{}^{\mathfrak{p}^f}M$ is cyclic. Thus $\lambda(L_{(m-1)/2}) = \lambda({}^{\mathfrak{p}^f}M) = 1/2$ by Theorem 4.5.1.
Suppose now that e is odd and set $f = (e+1)/2$. Using the basis of L_0 from above, let $M_1 := \langle x_0, x_1'y_1', \dots, x_s', y_s'\rangle$ and $M = \langle \pi^f x_0\rangle \perp M_1$. Then $\#D(L_0, M) = 1$ as M is the unique maximal sublattice of L_0 with norm $\mathfrak{p}^f$. Conversely, for $0 \le i < f$, $\langle \pi^i x_0\rangle \perp M_1$ is the only superlattice of $\langle \pi^{i+1} x_0\rangle \perp M_1$ which is isometric to $(\pi^i\overline{\pi}^i) \perp H(1)^{(m-1)/2}$. Whence $\lambda(L_0) = \lambda(M)$. Further, M is $\mathfrak{p}^f$-maximal and therefore $\lambda(L_0) = \lambda(M) = 1/2$ by Theorem 4.5.1. This finishes the proof. □

If m is even, the computation of local densities is much more involved. First, an analogue to Proposition 4.4.2 is given.

Theorem 4.5.3 *Let $i \in \mathbb{Z}$ such that $e+i$ is odd and set $f = \frac{e+i-1}{2}$. Let $L = L_0 \perp L_1$ be an $\mathcal{O}_\mathfrak{p}$-lattice in $(V_\mathfrak{p}, \Phi)$ such that L_0 is $\mathfrak{P}^i$-modular and $\operatorname{rank}(L_0) \ge 2$ is even. Suppose $\mathfrak{n}(L_0) = \mathfrak{p}^f$ and $\mathfrak{n}(L_1) \subseteq \mathfrak{p}^{f+1}$.*

1. *Let L_0' denote the $\mathfrak{o}/\mathfrak{p}$-space $L_0/\mathfrak{P}L_0$. Then*

$$Q\colon L_0' \to \mathfrak{o}/\mathfrak{p},\ x + \mathfrak{P}L_0 \mapsto p^{-f}Q_\Phi(x) + \mathfrak{p}$$

is a well defined quadratic form on L_0'.

2. *Given any primitive vector $w \in L_0$, set $L_w := \{x \in L\,;\, \Phi(x,w) \in \mathfrak{P}^{i+1}\}$. Let v be a fixed primitive vector of L_0. If $Q(v+\mathfrak{P}L_0) = 0$ let X denote the set of all isotropic lines in (L_0', Q). Otherwise let X denote the set of all anisotropic lines of (L_0', Q). Then*
$$\sigma\colon X \to D(L, L_v),\ \langle w + \mathfrak{P}L_0\rangle \mapsto L_w$$
is a bijection.

Proof. 1. The map Q is well defined since $\mathrm{T}(\pi\Phi(x,y)) \in \mathrm{T}(\mathfrak{P}^{i+e+1}) = \mathfrak{p}^{f+1}$ for all $x, y \in L$. Further,
$$(x+\mathfrak{P}L_0, y+\mathfrak{P}L_0) \mapsto Q(x+y+\mathfrak{P}L_0) - Q(x+\mathfrak{P}L_0) - Q(y+\mathfrak{P}L_0) = p^{-f}\,\mathrm{T}(\Phi(x,y)) + \mathfrak{p}$$
is bilinear and thus Q is a quadratic form.

2. The most difficult part is to show that σ is well defined. Let $\langle w + \mathfrak{P}L_0\rangle \in X$. The map σ does not depend on the chosen representative w. By Witt's theorem, there exists some automorphism $\varphi' \in \mathrm{Aut}(L_0', Q)$ such that $\varphi'(v+\mathfrak{P}L_0) = w + \mathfrak{P}L_0$, see for example [Kne02, Satz 3.4] for details. Hence there exists some $\mathcal{O}$-linear map $\varphi_1\colon L_0 \to L_0$ such that $\varphi_1(v) + \mathfrak{P}L_0 = w + \mathfrak{P}L_0$ and $\Phi(\varphi_1(x), \varphi_1(x)) - \Phi(x,x) \in \mathfrak{p}^{1+f}$ for all $x \in L_1$. To show that $L_w \in D(L, L_v)$, the map φ' will be lifted to some (hermitian) automorphism of L_0 using arguments similar to [Kne02, Section V.15]. Suppose there exists some $\mathcal{O}$-linear lift $\varphi_k\colon L_0 \to L_0$ of φ' such that
$$Q_\Phi(\varphi_k(x)) - Q_\Phi(x) \in \mathfrak{p}^{k+f} \quad \text{for all } x \in L_0\,.$$
Define
$$Q_k\colon L_0' \to \mathfrak{o}/\mathfrak{p},\ x + \mathfrak{P}L_0 \mapsto p^{-k-f}(Q_\Phi(\varphi_k(x)) - Q_\Phi(x)) + \mathfrak{p}\,.$$
As before, the map Q_k is well-defined since $e+i$ is odd. Further,
$$Q_k(x+y) - Q_k(x) - Q_k(y) = p^{-k-f}\,\mathrm{T}(\Phi(\varphi_k(x), \varphi_k(y)) - \Phi(x,y)) + \mathfrak{p} \quad \text{for all } x, y \in L_0$$
defines a bilinear form on L_0'. Hence Q_k is a quadratic form on L_0'. So there exists some (not necessarily symmetric) bilinear form $\Psi\colon L_0' \times L_0' \to \mathfrak{o}/\mathfrak{p}$ such that
$$Q_k(x+\mathfrak{P}L_0) = \Psi(x+\mathfrak{P}L_0, x+\mathfrak{P}L_0) \quad \text{for all } x \in L_0\,.$$
The assumption that L_0 is $\mathfrak{P}^i$-modular implies that
$$L_0' \times L_0' \to \mathfrak{o}/\mathfrak{p},\ (x+\mathfrak{P}L_0, y+\mathfrak{P}L_0) \mapsto p^{-f}\,\mathrm{T}(\Phi(x,y)) + \mathfrak{p}$$
is bilinear and non-degenerate. In particular, given any element b in some $\mathcal{O}$-basis B of L_0, there exists some $v_b \in L_0$ such that
$$\Psi(x+\mathfrak{P}L_0, b+\mathfrak{P}L_0) = -p^{-f}\,\mathrm{T}(\Phi(x, v_b)) + \mathfrak{p} \quad \text{for all } x \in L_0\,. \tag{4.5.2}$$
Let $v\colon L_0 \to L_0$ be the $\mathcal{O}$-linear map defined by $v(b) = v_b$ and set $\varphi_{k+1} := \varphi_k + p^k v$. Equation (4.5.2) shows that
$$Q_\Phi(\varphi_k(x)) - Q_\Phi(x) + p^k\,\mathrm{T}(\Phi(x, v(x)) \in \mathfrak{p}^{k+1+f} \quad \text{for all } x \in L_0\,.$$

But this is equivalent to

$$Q_\Phi(\varphi_{k+1}(x)) - Q_\Phi(x) \in \mathfrak{p}^{k+1+f} \quad \text{for all } x \in L_0\,.$$

Proceeding in this way, one obtains a sequence (φ_k) of $\mathcal{O}$-linear maps on L_0. Remark 2.1.6 shows that $\varphi := \lim_{k\to\infty} \varphi_k$ is an isometry of EL_0 and thus injective. It is surjective since $\varphi(L_0)$ and L_0 are both unimodular. Let $\varphi' \in \operatorname{Aut}(L)$ be any extension of $\varphi \in \operatorname{Aut}(L_0)$. Then $\langle \varphi'(v) + \mathfrak{P}L_0\rangle = \langle w + \mathfrak{P}L_0\rangle$ and therefore $L_w = \varphi'(L_v) \in D(L, L_v)$ as claimed.
Further, σ is injective since L_0 is $\mathfrak{P}^i$-modular. If $M \in D(L, L_v)$, there exist some isometry $\tau \in U(V, \Phi)$ with $M = \tau(L_v)$. Write $\tau(v) = v_0 + v_1$ with $v_i \in L_i$. Then $M = L_{\tau(v)} = L_{v_0}$. The assumption on $\mathfrak{n}(L_1)$ implies that $Q(v + \mathfrak{P}L_0) = Q(v_0 + \mathfrak{P}L_0)$ and therefore $\langle v_0 + \mathfrak{P}L_0\rangle \in X$. So σ is surjective. □

Again, using [Kne02, Section IV.13], the previous result can be made effective.

Corollary 4.5.4 *In the situation of Theorem 4.5.3, one has*

$$\#D(L, L_v) = \begin{cases} q^{k-1}(q^k - \varepsilon) & \text{if } \operatorname{ord}_\mathfrak{p}(Q_\Phi(v)) = \frac{e+i-1}{2},\\ (q-1)^{-1}(q^k - \varepsilon)(q^{k-1} + \varepsilon) & \text{otherwise,}\end{cases}$$

where $k = \frac{1}{2}\operatorname{rank}(L_0)$, $\varepsilon = +1$ if EL_0 is hyperbolic and $\varepsilon = -1$ otherwise.

Theorem 4.5.5 *Let $L_\mathfrak{p} = L_0 \perp L_1$ be an $\mathcal{O}_\mathfrak{p}$-lattice in $(V_\mathfrak{p}, \Phi)$ such that L_i is $\mathfrak{P}^i$-modular. Write $\ell_0 := \operatorname{ord}_\mathfrak{p}(\mathfrak{n}(L))$, $\ell_1 := \operatorname{ord}_\mathfrak{p}(\mathfrak{n}(\mathfrak{P}L_0 \perp L_1))$ and $m_i := \operatorname{rank}(L_i)$. If $m = m_0 + m_1$ is even, then*

$$\lambda(L) = \frac{c}{2} \cdot \binom{m/2}{m_0/2}_{q^2}$$

where $c \in \mathbb{N}$ is given as follows:

1. *If $L_\mathfrak{p} \cong H(0)^{m_0/2} \perp H(1)^{m_1/2}$, then* $c = \begin{cases} q^{\frac{m_1}{2}} + 1 & \text{if } e \text{ is even,}\\ q^{\frac{m_0}{2}} + 1 & \text{if } e \text{ is odd.}\end{cases}$

2. *If $(V_\mathfrak{p}, \Phi)$ is hyperbolic and $L_\mathfrak{p} \not\cong H(0)^{m_0/2} \perp H(1)^{m_1/2}$, then*
$$c = \begin{cases} q^{m(e/2-\ell_1)-m_1/2}(q^{m_1} - 1) & \text{if } \ell_0 = \ell_1 \text{ and } e \text{ is even,}\\ q^{m(e/2-1-\ell_0)+m_1/2}(q^{m_0} - 1) & \text{if } \ell_0 \neq \ell_1 \text{ and } e \text{ is even,}\\ q^{m((e-1)/2-\ell_1)+m_0/2}(q^{m_1} - 1) & \text{if } \ell_0 = \ell_1 \text{ and } e \text{ is odd,}\\ q^{m((e-1)/2-\ell_0)-m_0/2}(q^{m_0} - 1) & \text{if } \ell_0 \neq \ell_1 \text{ and } e \text{ is odd.}\end{cases}$$

3. *If $(V_\mathfrak{p}, \Phi)$ is non-hyperbolic, then*
$$c = \begin{cases} q^{m_1/2} - 1 & \text{if } \ell_0 = \ell_1 = e/2 \text{ and } e \text{ is even,}\\ q^{m(e/2-\ell_1)-m_1/2}(q^{m_1} - 1) & \text{if } \ell_0 = \ell_1 < e/2 \text{ and } e \text{ is even,}\\ q^{m(e/2-1-\ell_0)+m_1/2}(q^{m_0} - 1) & \text{if } \ell_0 \neq \ell_1 \text{ and } e \text{ is even,}\\ q^{m((e-1)/2-\ell_1)+m_0/2}(q^{m_1} - 1) & \text{if } \ell_0 = \ell_1 \text{ and } e \text{ is odd,}\\ q^{m_0/2} - 1 & \text{if } \ell_0 \neq \ell_1,\ \ell_0 = (e-1)/2 \text{ and } e \text{ is odd,}\\ q^{m((e-1)/2-\ell_0)-m_0/2}(q^{m_0} - 1) & \text{if } \ell_0 \neq \ell_1,\ \ell_0 < (e-1)/2 \text{ and } e \text{ is odd.}\end{cases}$$

Proof. Let u_0 be as in Corollary 3.3.17. If (V, Φ) is hyperbolic, let $u = 0$; otherwise let $u = -u_0$. For $0 \le r \le \frac{m}{2}$, let $L_{k,r}$ and $M_{k,r}$ be $\mathcal{O}_{\mathfrak{p}}$-lattices in $(V_{\mathfrak{p}}, \Phi)$ such that

$$\begin{aligned} L_{k,r} &\cong \langle \begin{pmatrix} p^k & 1 \\ 1 & up^{-k} \end{pmatrix} \rangle \perp H(0)^r \perp H(1)^s \quad \text{with } 0 \le k \le \begin{cases} \lfloor \frac{e}{2} \rfloor & \text{if } u = 0\,, \\ \lfloor \frac{e-1}{2} \rfloor & \text{if } u \neq 0\,, \end{cases} \\ M_{k,r} &\cong \langle \begin{pmatrix} p^k & \pi \\ \overline{\pi} & up^{1-k} \end{pmatrix} \rangle \perp H(0)^r \perp H(1)^s \quad \text{with } 1 \le k \le \begin{cases} \lfloor \frac{e+1}{2} \rfloor & \text{if } u = 0\,, \\ \lfloor \frac{e}{2} \rfloor & \text{if } u \neq 0 \end{cases} \end{aligned} \tag{4.5.3}$$

where $s = \frac{m}{2} - r - 1$. Note that, if $\ell_0 \neq \ell_1$, then $L \cong L_{\ell_0, \frac{m_0}{2}-1}$. Conversely, if $\ell_0 = \ell_1$, then $L \cong M_{\ell_1, \frac{m_0}{2}}$.

First, the following claim will be established:

$$\begin{aligned} \#D(L_{k,r}, M_{k+1,r}) &= \begin{cases} q^r(q^{r+1} - 1) & \text{if } k = \frac{e-1}{2}, \\ 1 & \text{otherwise.} \end{cases} \\ \#U(L_{k,r}, M_{k+1,r}) &= \begin{cases} q^s(q^{s+1} - 1) & \text{if } k = \frac{e}{2} - 1 \text{ and } u = 0, \\ q^s(q^{s+1} + 1) & \text{if } k = \frac{e}{2} - 1 \text{ and } u \neq 0, \\ (q-1)^{-1}(q^{2s+2} - 1) & \text{if } k = \frac{e-1}{2}, \\ q^{1+2s} & \text{otherwise.} \end{cases} \end{aligned} \tag{4.5.4}$$

The quantities $\#D(L_{k,r}, M_{k+1,r})$ have already been worked out in Remark 4.3.4 and Corollary 4.5.4. Also, the first two cases of $\#U(L_{k,r}, M_{k+1,r}) = \#D(M_{k+1,r}^{\#}, L_{k,r}^{\#})$ follow from Corollary 4.5.4. So only the last two cases of $\#U(L_{k,r}, M_{k+1,r})$ need to be discussed. Let $M_{k+1,r} = \langle x, y \rangle \perp M_0 \perp M_1$ where $\mathrm{G}(x, y) = \left(\begin{smallmatrix} p^{k+1} & \pi \\ \overline{\pi} & up^{-k} \end{smallmatrix}\right)$, $M_0 \cong H(0)^r$ and $M_1 \cong H(1)^s$. Every element of $U(L_{k,r}, M_{k+1,r})$ is of the form $M_{k+1,r} + \mathfrak{P}^{-1}v$ where $v = \alpha x + \beta y + v_0 + v_1$ with $\alpha, \beta \in \mathcal{O}$ and $v_i \in M_i$. Comparing norms and scales shows that one may assume $v_0 = 0$. Further, $k \neq \frac{e-1}{2}$ implies $\alpha \notin \mathfrak{P}$. By Theorem 3.3.18, each such v yields a lattice in $U(L_{k,r}, M_{k+1,r})$.

Similarly, one shows that

$$\begin{aligned} \#U(L_{k,r}, M_{k,r}) &= \begin{cases} (q-1)^{-1}(q^{s+1} - 1)(q^s + 1) & \text{if } k = \frac{e}{2}, \\ 1 & \text{otherwise.} \end{cases} \\ \#D(L_{k,r}, M_{k,r}) &= \begin{cases} q^r(q^{r+1} - 1) & \text{if } u = 0 \text{ and } k = \frac{e-1}{2}, \\ q^r(q^{r+1} + 1) & \text{if } u \neq 0 \text{ and } k = \frac{e-1}{2}, \\ (q-1)^{-1}(q^{2r+2} - 1) & \text{if } k = \frac{e}{2}, \\ q^{1+2r} & \text{otherwise.} \end{cases} \end{aligned} \tag{4.5.5}$$

In particular, for any fixed r, one can compare the local factors of any pair of lattices defined in equation (4.5.3). In the following, only the cases where e is even will be discussed. The cases where e is odd are proved similarly.

1. Since e is assumed to be even, the lattice $L_{e/2,m/2-1} \cong H(0)^{m/2}$ is $\mathfrak{p}^{e/2}$-maximal and therefore $\lambda(L_{e/2,m/2-1}) = 1$. If $1 \leq r < m/2$, then equation (4.5.5) shows that

$$\lambda(L_{e/2,r-1}) = \lambda(M_{e/2,r}) = \lambda(L_{e/2,r}) \cdot \frac{q^{2r+2}-1}{(q^{m/2-r}-1)(q^{m/2-r-1}+1)}$$

and therefore

$$\begin{aligned}\lambda(H(0)^r \perp H(1)^{m/2-r}) = \lambda(L_{e/2,r-1}) &= \prod_{i=r}^{m/2-1} \frac{q^{2i+2}-1}{(q^{m/2-i}-1)(q^{m/2-i-1}+1)} \\ &= \frac{q^{m/2-r}+1}{2} \cdot \binom{m/2}{r}_{q^2}, \\ \lambda(H(1)^{m/2}) = \lambda(M_{e/2,0}) = \lambda(L_{e/2,0}) \cdot \frac{q^2-1}{(q^{m/2}-1)(q^{m/2-1}+1)} &= \frac{q^{m/2}+1}{2} .\end{aligned}$$

This proves part 1.

2. Suppose $k < e/2$. From equations (4.5.4) and (4.5.5) it follows that

$$\lambda(L_{k,r}) = \lambda(L_{k+1,r}) \cdot \begin{cases} \frac{(q^{2r+2}-1)q^{m/2-1-r}}{(q^{m/2-1-r}+1)} & \text{if } k = \frac{e}{2}-1, \\ q^m & \text{otherwise.} \end{cases}$$

Hence

$$\lambda(L_{k,r}) = q^{m(e/2-1-k)+m/2-1-r} \frac{q^{2r+2}-1}{q^{m/2-1-r}+1} \cdot \lambda(L_{e/2,r}) .$$

Equation (4.5.5) also yields

$$\lambda(M_{k,r}) = \lambda(L_{k,r}) \cdot q^{1+2r} = q^{m(e/2-1-k)+m/2+r} \frac{q^{2r+2}-1}{q^{m/2-1-r}+1} \cdot \lambda(L_{e/2,r}) .$$

Part 2. now follows immediately by plugging in the explicit value of $\lambda(L_{e/2,r})$ into the previous two equations.

3. The lattice $M_{e/2,m/2-1}$ is $\mathfrak{p}^{e/2}$-maximal and therefore $\lambda(M_{e/2,m/2-1}) = \frac{q^m-1}{2(q+1)}$. Corollary 4.5.4 gives

$$\#U(M_{e/2,r+1}, M_{e/2,r}) = \#D(M^{\#}_{e/2,r}, M^{\#}_{e/2,r+1}) = \frac{(q^{m/2-r-1}-1)(q^{m/2-r}+1)}{q-1} .$$

Conversely, let $M^{\#}_{e/2,r+1} = M_0 \perp M_{-1}$ where $M_0 \cong H(0)^{r+1}$ and M_{-1} is $\mathfrak{P}^{-1}$-modular. The lattices in $U(M^{\#}_{e/2,r}, M^{\#}_{e/2,r+1})$ are precisely the lattices $M^{\#}_{e/2,r+1} + \mathfrak{P}^{-1}v$ where v denotes a primitive vector in M_0. Thus $\#D(M_{e/2,r+1}, M_{e/2,r}) = (q-1)^{-1}(q^{2r+2}-1)$.

Hence

$$\begin{aligned}\lambda(M_{e/2,r}) &= \lambda(M_{e/2,e/2-1}) \cdot \prod_{i=r}^{m/2-2} \frac{q^{2i+2}-1}{(q^{m/2-i-1}-1)(q^{m/2-i}+1)} \\ &= \frac{q^{m/2-r}-1}{2} \binom{m/2}{r}_{q^2} , \\ \lambda(L_{e/2-1,r}) &= \lambda(M_{e/2,r}) \cdot q^{m/2-r-1}(q^{m/2-r}+1) = q^{m/2-r-1} \frac{q^{2r+2}-1}{2} \binom{m/2}{r+1}_{q^2} .\end{aligned}$$

Finally, suppose $0 \leq k \leq \frac{e}{2} - 2$. Equations (4.5.4) and (4.5.5) show that

$$\begin{aligned}\lambda(L_{k,r}) &= q^m \cdot \lambda(L_{k+1,r}) = q^{m(e/2-1-k)} \cdot L_{e/2-1,r} , \\ \lambda(M_{k+1,r}) &= q^{2r+1-m} \cdot \lambda(L_{k,r}) = q^{m(e/2-2-k)+2r+1} \cdot L_{e/2-1,r} .\end{aligned}$$

This finishes the proof of part 3. □

5 Kneser's Neighbour method

Let K be a number field and let (V, Φ) be a regular hermitian space over E.

In this chapter, an algorithm to compute representatives of the isometry classes in the genus of some given $\mathcal{O}$-lattice in (V, Φ) will be presented. The algorithm is originally due to M. Kneser, who introduced it in [Kne57] for quadratic lattices over the integers. It has then been adopted for number fields by R. Scharlau & B. Hemkemeier [SH98], for hermitian forms by A. Schiemann [Sch98] using ideas of D. Hoffmann [Hof91], and for quaternionic hermitian forms by C. Bachoc [Bac95]. The exposition given here follows [Sch98] and provides a uniform approach which works in all three cases.

5.1 Strong approximation

If E is commutative, some problems arise. In such a case, the orthogonal or unitary group of (V, Φ) does not have the strong approximation property. Luckily there exist finite-index subgroups which have that property. Depending on $\dim_K(E)$, the following notation will be assumed in this chapter.

The case $E = K$

Let $v \in V$ be anisotropic. The *reflection* along $\langle v \rangle^\perp$

$$\tau_v \colon V \to V,\ w \mapsto w - 2\frac{\Phi(w,v)}{\Phi(v,v)}v$$

defines an isometry in $\mathbf{O}(V, \Phi)$. Conversely, any isometry $\varphi \in \mathbf{O}(V, \Phi)$ can be expressed as a finite product $\varphi = \tau_{v_1} \circ \ldots \circ \tau_{v_r}$ of reflections. Using Clifford algebras, one can show that $\prod_{i=1}^r Q_\Phi(v_i) \in K^*/(K^*)^2$ does not the depend on the chosen factorization (c.f. [O'M73, 54:6]). Hence there exists a unique group homomorphism $\theta \colon \mathbf{O}(V, \Phi) \to K^*/(K^*)^2$ such that $\theta(\tau_v) = Q_\Phi(v)(F^*)^2$ for all anisotropic vectors $v \in V$. The map θ is called the *spinor norm* of (V, Φ). In [Zas62], H. Zassenhaus gives an equivalent definition of spinor norms in terms of determinants. His characterization yields a different proof for the fact that the spinor norm is a well defined group homomorphism.

Definition 5.1.1 The *special orthogonal group* of (V, Φ) is the kernel

$$\mathbf{SO}(V, \Phi) = \{\sigma \in \mathbf{O}(V, \Phi)\,;\, \det(\sigma) = +1\}$$

of $\det \colon \mathbf{O}(V, \Phi) \to \{\pm 1\}$. Further, let

$$\mathbf{S}(V, \Phi) = \{\sigma \in \mathbf{SO}(V, \Phi)\,;\, \theta(\sigma) = +1\}$$

be the kernel of θ, when restricted to $\mathbf{SO}(V,\Phi)$. Similarly, one defines $\mathbf{SO}(V_{\mathfrak{p}},\Phi)$ and $\mathbf{S}(V_{\mathfrak{p}},\Phi)$ for all $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$.
Two $\mathfrak{o}$-lattices L and M in (V,Φ) are said to be in the same *spinor genus* if there exists an isometry $\sigma \in \mathbf{O}(V,\Phi)$ such that $L_{\mathfrak{p}} = \sigma(\varphi_{\mathfrak{p}}(M_{\mathfrak{p}}))$ with $\varphi_{\mathfrak{p}} \in \mathbf{S}(V_{\mathfrak{p}},\Phi)$ for all $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$. The spinor genus of L will be denoted by $\operatorname{sgen}(L)$.

The case that E/K is a quadratic field extension

Definition 5.1.2 The *special unitary group* of (V,Φ) is the kernel

$$\mathbf{S}(V,\Phi) := \{\sigma \in \mathbf{U}(V,\Phi)\,;\, \det(\sigma) = +1\}$$

of $\det\colon \mathbf{U}(V,\Phi) \to \{\pm 1\}$. Similarly, one defines $\mathbf{S}(V_{\mathfrak{p}},\Phi)$ for all $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$.
Two $\mathcal{O}$-lattices L and M in (V,Φ) are said to be in the same *special genus* if there exists an isometry $\sigma \in \mathbf{U}(V,\Phi)$ such that $L_{\mathfrak{p}} = \sigma(\varphi_{\mathfrak{p}}(M_{\mathfrak{p}}))$ with $\varphi_{\mathfrak{p}} \in \mathbf{S}(V_{\mathfrak{p}},\Phi)$ for all $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$. The special genus of L will be denoted by $\operatorname{sgen}(L)$.

The case that E/K is a quaternion algebra

To be able to present the theory in a uniform way, set $\mathbf{S}(V,\Phi) = \mathbf{U}(V,\Phi)$ and let the *special genus* $\operatorname{sgen}(L)$ of any $\mathcal{O}$-lattice L in (V,Φ) be the usual genus $\operatorname{gen}(L)$.

By Theorem 2.4.5, every genus is a disjoint union of finitely many spinor/special genera which in turn are disjoint unions of finitely many isometry classes. As promised before, the group $\mathbf{S}(V,\Phi)$ usually does have the strong approximation property.

Theorem 5.1.3 (Strong approximation) *Suppose* $\dim_K(V) \geq 3$. *Let* $S \subseteq \mathbb{P}(\mathfrak{o})$ *be a set of prime ideals of* $\mathfrak{o}$ *and let* $T \subseteq S$ *be a finite subset. Suppose that there exists a place* v *of* K*, not corresponding to an ideal in* S*, such that* (V_v,Φ) *is isotropic. Further, let* L *be an* $\mathcal{O}$*-lattice in* (V,Φ) *and for* $\mathfrak{p} \in T$ *fix some* $\sigma_{\mathfrak{p}} \in \mathbf{S}(V_{\mathfrak{p}},\Phi)$. *Then for every* $k \in \mathbb{N}$ *there exists some* $\sigma \in \mathbf{S}(V,\Phi)$ *such that*

$$\begin{aligned} (\sigma - \sigma_{\mathfrak{p}})(L_{\mathfrak{p}}) &\subseteq \mathfrak{p}^k L_{\mathfrak{p}} \quad \textit{for all } \mathfrak{p} \in T \textit{ and} \\ \sigma(L_{\mathfrak{p}}) &= L_{\mathfrak{p}} \quad \textit{for all } \mathfrak{p} \in S - T\,. \end{aligned}$$

Proof. See for example the article of M. Kneser [Kne66]. □

Corollary 5.1.4 *Suppose* $\dim_K(V) \geq 3$ *and let* L *be an* $\mathcal{O}$*-lattice in* (V,Φ).

1. *If* (V,Φ) *is indefinite, then* $\operatorname{sgen}(L) = \operatorname{cls}(L)$.
2. *If* (V,Φ) *is definite, let* $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$ *such that* $(V_{\mathfrak{p}},\Phi)$ *is isotropic. Then there exists some* $M \in \operatorname{sgen}(L)$ *such that* $M_{\mathfrak{q}} = L_{\mathfrak{q}}$ *for all* $\mathfrak{q} \in \mathbb{P}(\mathfrak{o}) - \{\mathfrak{p}\}$.

Proof. Let $M \in \operatorname{sgen}(L)$. There exist some $\sigma \in \mathbf{U}(V,\Phi)$ such that for all $\mathfrak{q} \in \mathbb{P}(\mathfrak{o})$ one has $M_{\mathfrak{q}} = \sigma(\tau_{\mathfrak{q}}(L_{\mathfrak{q}}))$ for some $\tau_{\mathfrak{q}} \in \mathbf{S}(V_{\mathfrak{q}},\Phi)$. Set $S = \mathbb{P}(\mathfrak{o})$ if (V,Φ) is indefinite, otherwise set $S = \mathbb{P}(\mathfrak{o}) - \{\mathfrak{p}\}$. Let $T = \{\mathfrak{q} \in \mathbb{P}(\mathfrak{o})\,;\, M_{\mathfrak{q}} \neq \sigma(L_{\mathfrak{q}})\}$ and fix some $k \in \mathbb{N}$ such that $\mathfrak{q}^k L_{\mathfrak{q}} \subseteq \tau_{\mathfrak{q}}(L_{\mathfrak{q}})$ for all $\mathfrak{q} \in T$. By strong approximation, there exists some $\varphi \in \mathbf{S}(V,\Phi)$ such that $\varphi(L_{\mathfrak{q}}) = \tau_{\mathfrak{q}}(L_{\mathfrak{q}})$ for all $\mathfrak{q} \in S$. Hence $M_{\mathfrak{q}} = \sigma(\varphi(L_{\mathfrak{q}}))$ for all $\mathfrak{q} \in S$. □

In particular, if E is a quaternion algebra, then every genus in (V,Φ) has class number one whenever (V,Φ) is indefinite.

5.2 Neighbours of a lattice

Let L be an $\mathcal{O}$-lattice in (V,Φ) and let $\mathfrak{p}$ be a good prime ideal of $\mathfrak{o}$ such that $L_\mathfrak{p}$ is modular. Further, let $\mathfrak{P}$ be some maximal left ideal of $\mathcal{O}$ that contains $\mathfrak{p}$. After rescaling Φ, one can make the following assumptions:

- If $\mathfrak{p}$ is unramified in E, then $L_\mathfrak{p}$ is unimodular.
- If $\mathfrak{p}$ is ramified in E, then $L_\mathfrak{p}$ is either unimodular or $\mathfrak{P}^{-1}$-modular.
- $L_\mathfrak{q}$ is integral for all $\mathfrak{q} \in \mathbb{P}(\mathfrak{o}) - \{\mathfrak{p}\}$.

Definition 5.2.1 In the above situation, one defines:

1. An $\mathcal{O}$-lattice L' in (V,Φ) is a $\mathfrak{P}$-*neighbour* of L if $L'_\mathfrak{p}$ is $\mathfrak{s}(L_\mathfrak{p})$-modular and there exist $\mathcal{O}$-module isomorphisms
$$L/(L\cap L') \cong \mathcal{O}/\mathfrak{P} \quad \text{and} \quad L'/(L\cap L') \cong \overline{\mathfrak{P}}^{-1}/\mathcal{O}\,.$$
2. a) If $L_\mathfrak{p}$ is unimodular, then $x \in L$ is said to be $\mathfrak{P}$-*admissible*, if $x \notin \overline{\mathfrak{P}}L$ and $Q_\Phi(x) \in \mathfrak{P}\overline{\mathfrak{P}}$. If this is the case, let
$$L^x_\mathfrak{P} := \{y \in L\,;\, \Phi(x,y) \in \overline{\mathfrak{P}}\} \text{ and } L_{x,\mathfrak{P}} := L^x_\mathfrak{P} + \overline{\mathfrak{P}}^{-1}x\,.$$
   b) If $L_\mathfrak{p}$ is $\mathfrak{P}^{-1}$-modular, then $x \in L$ is said to be $\mathfrak{P}$-*admissible*, if $x \notin \mathfrak{P}L$ and $Q_\Phi(x) \in \mathfrak{p}$. If this is the case, let
$$L^x_\mathfrak{P} := \{y \in L\,;\, \Phi(x,y) \in \mathcal{O}\} \text{ and } L_{x,\mathfrak{P}} := L^x_\mathfrak{P} + \mathfrak{P}^{-1}x\,.$$

   The lattice $L_{x,\mathfrak{P}}$ is called the $\mathfrak{P}$-*neighbour* of L at x.

Remark 5.2.2 Let $x \in L$ be $\mathfrak{P}$-admissible.

1. Let M be a $\mathfrak{P}$-neighbour of L. Then $L_\mathfrak{q} = M_\mathfrak{q}$ for all $\mathfrak{q} \in \mathbb{P}(\mathfrak{o}) - \{\mathfrak{p}\}$. Further, $L_\mathfrak{p}$ and $M_\mathfrak{p}$ are both $\mathfrak{s}(L_\mathfrak{p})$-modular. Hence M and L are in the same genus.
2. By the same argument, L and $L_{x,\mathfrak{P}}$ are in the same genus.
3. $\sigma(L_{x,\mathfrak{P}}) = L_{\sigma(x),\mathfrak{P}}$ for all $\sigma \in \operatorname{Aut}(L)$.

Lemma 5.2.3 *Let $M \neq L$ be an $\mathcal{O}$-lattice in (V,Φ) such that $L_\mathfrak{q} = M_\mathfrak{q}$ for all $\mathfrak{q} \in \mathbb{P}(\mathfrak{o})$ different from $\mathfrak{p}$. If E is a quadratic extension of K which is split at $\mathfrak{p}$, it is further assumed that $\overline{\mathfrak{P}}^e M \subseteq L$ for some $e \geq 1$. Then $\overline{\mathfrak{P}}M \cap L \not\subseteq \overline{\mathfrak{P}}L$.*

Proof. Suppose first that $\mathfrak{P}$ is a twosided $\mathcal{O}$-ideal. Then there exists a minimal $e \geq 0$ such that $\overline{\mathfrak{P}}^e M \subseteq L$. Note that $e \geq 1$ since $L \neq M$. The minimality of e implies that $\overline{\mathfrak{P}}M \cap L \not\subseteq \overline{\mathfrak{P}}L$.
Suppose now that $\mathfrak{P}$ is not a twosided $\mathcal{O}$-ideal. Then E is a quaternion algebra which is unramified at $\mathfrak{p}$. Further $\mathfrak{A} := \{\alpha \in E\,;\, \alpha M \subseteq L\}$ is a proper, integral, twosided ideal of $\mathcal{O}$. Hence $\mathfrak{A} = \mathcal{O}\mathfrak{p}^e$ for some $e \geq 1$, c.f. [KV10, Lemma 3.1]. Assume that $\overline{\mathfrak{P}}M \cap L \subseteq \overline{\mathfrak{P}}L$. Then

$$\mathcal{O}\mathfrak{p}^e M \subseteq \overline{\mathfrak{P}}M \cap L \subseteq \overline{\mathfrak{P}}L$$

and therefore $\overline{\mathfrak{P}}^{-1}\mathcal{O}\mathfrak{p}^e \subseteq \mathfrak{A} = \mathcal{O}\mathfrak{p}^e$. But then $\overline{\mathfrak{P}}^{-1} \subseteq \mathcal{O}$ yields the desired contradiction.□

Note that if M is a $\mathfrak{P}$-neighbour of L and $E_\mathfrak{p}/K_\mathfrak{p} \cong K_\mathfrak{p} \oplus K_\mathfrak{p}$ then $M/(L \cap M) \cong \mathcal{O}/\overline{\mathfrak{P}}$ shows that $\overline{\mathfrak{P}}M \subseteq L$. Hence M satisfies the conditions of the previous lemma.

Proposition 5.2.4 *The set of all $\mathfrak{P}$-neighbours of L is given by*

$$\{L_{x,\mathfrak{P}}\,;\, x \in L \text{ is } \mathfrak{P}\text{-admissible}\}\,.$$

Proof. Let $x \in L$ be $\mathfrak{P}$-admissible. Then

$$L_{x,\mathfrak{P}}/(L \cap L_{x,\mathfrak{P}}) \cong (L_{x,\mathfrak{P}} + L)/L = (\overline{\mathfrak{P}}^{-1}x + L)/L \cong \overline{\mathfrak{P}}^{-1}x/(L \cap \overline{\mathfrak{P}}^{-1}x) \cong \overline{\mathfrak{P}}^{-1}/\mathcal{O}\,.$$

If $L_\mathfrak{p}$ is unimodular, the $\mathcal{O}$-module morphism

$$L \to \mathcal{O}/\mathfrak{P},\ y \mapsto \Phi(y,x) + \mathfrak{P}$$

has kernel $L \cap L_{x,\mathfrak{P}} = L^x_\mathfrak{P}$ and is surjective since $\mathcal{O}/\mathfrak{P}$ is a simple $\mathcal{O}$-module. Similarly, if $L_\mathfrak{p}$ is $\mathfrak{P}^{-1}$-modular, then

$$L \to \mathfrak{P}^{-1}/\mathcal{O} \cong \mathcal{O}/\mathfrak{P},\ y \mapsto \Phi(y,x) + \mathcal{O}$$

is surjective with kernel $L \cap L_{x,\mathfrak{P}} = L^x_\mathfrak{P}$. Thus $L_{x,\mathfrak{P}}$ is a $\mathfrak{P}$-neighbour of L in any case.
Conversely, let M be any $\mathfrak{P}$-neighbour of L. Lemma 5.2.3 shows that there exists some $x \in (\overline{\mathfrak{P}}M \cap L) - \overline{\mathfrak{P}}L$. Then x is $\mathfrak{P}$-admissible. The claim is that $M = L_{x,\mathfrak{P}}$. First note that $L \cap M \subseteq L^x_\mathfrak{P}$ since M is modular. Further, $L_\mathfrak{p}$ is also modular, so $L^x_\mathfrak{p} \subsetneq L$. Since $L/(L \cap M)$ is a simple $\mathcal{O}$-module it follows that $L^x_\mathfrak{P} = L \cap M$. Thus $L^x_\mathfrak{P} \subseteq M$ and therefore $L_{x,\mathfrak{P}} \subseteq M$. But then $L_{x,\mathfrak{P}} = M$ by modularity. □

Proposition 5.2.5 (Kneser) *Let $M \in \operatorname{gen}(L)$ such that $L_\mathfrak{q} = M_\mathfrak{q}$ for all $\mathfrak{q} \in \mathbb{P}(\mathfrak{o}) - \{\mathfrak{p}\}$. If E/K is a quadratic extension which is split at $\mathfrak{p}$, it is further assumed that $\overline{\mathfrak{P}}^e M \subseteq L$ for some $e \geq 1$. Then there exists a sequence of $\mathcal{O}$-lattices $L = L_0, L_1, \ldots, L_r = M$ such that L_i is a $\mathfrak{P}$-neighbour of L_{i-1} for all $1 \leq i \leq r$.*

Proof. Let $e \geq 0$ such that $[L/(L \cap M)]_\mathfrak{o} = \mathfrak{p}^e$. There is nothing to show if $e = 0$, so suppose $e \geq 1$. By Lemma 5.2.3 there exists some $x \in (\overline{\mathfrak{P}}M \cap L) - \overline{\mathfrak{P}}L$. Then x is $\mathfrak{P}$-admissible. Further, $L_{x,\mathfrak{P}} \cap M$ properly contains $L \cap M$ since $\overline{\mathfrak{P}}^{-1}x \subseteq M$ but $\overline{\mathfrak{P}}^{-1}x \not\subseteq L$. Thus $[L/(L_{x,\mathfrak{P}} \cap M)]_\mathfrak{o} = \mathfrak{p}^f$ for some $f < e$. The result follows by induction on e. □

Definition 5.2.6 The set of all $\mathcal{O}$-lattices M in (V, Φ) such that there exists some $\sigma \in \mathbf{U}(V, \Phi)$ and a sequence $L = L_0, L_1, \dots, L_r = \sigma(M)$ where L_i is a $\mathfrak{P}$-neighbour of L_{i-1} will be denoted by $\mathcal{N}(L, \mathfrak{P})$.

Proposition 5.2.7 *The set* $\mathcal{N}(L, \mathfrak{P})$ *coincides with*

$$\{M \in \operatorname{gen}(L)\,;\ \textit{there exists } M' \in \operatorname{cls}(M) \textit{ such that } L_{\mathfrak{q}} = M'_{\mathfrak{q}} \textit{ for all } \mathfrak{q} \in \mathbb{P}(\mathfrak{o}) - \{\mathfrak{p}\}\}\,.$$

Proof. In view of Proposition 5.2.5, only the case that $E_{\mathfrak{p}} \cong K_{\mathfrak{p}} \oplus K_{\mathfrak{p}}$ requires proof. Let $M \in \mathcal{N}(L, \mathfrak{P})$. By loc. cit. it suffices to show that there exists some $M' \in \operatorname{cls}(M)$ such that $\overline{\mathfrak{P}}^e M' \subseteq L$ for some $e \geq 0$. There exists some $f \geq 0$ such that $(\overline{\mathfrak{P}}\mathfrak{P})^f M \subseteq L$. Without loss of generality, $\mathfrak{P}^f$ is principal, say generated by $\alpha \in E^*$. But then $M' := \alpha\overline{\alpha}^{-1} M \in \operatorname{cls}(M)$ satisfies $\overline{\mathfrak{P}}^{2f} M' = \overline{\mathfrak{P}}^{2f}(\overline{\mathfrak{P}}^{-1}\mathfrak{P})^f M = (\overline{\mathfrak{P}}\mathfrak{P})^f M \subseteq L$. □

Corollary 5.2.8 *Suppose* $\dim_K(V) \geq 3$. *If* $(V_{\mathfrak{p}}, \Phi)$ *is isotropic, then*

$$\operatorname{sgen}(L) \subseteq \mathfrak{N}(L, \mathfrak{P})\,.$$

Proof. This follows immediately from Proposition 5.2.7 and Corollary 5.1.4. □

Note that $(V_{\mathfrak{p}}, \Phi)$ is isotropic at almost all prime ideals $\mathfrak{p}$, c.f. Theorem 3.2.2 and Corollary 3.2.4 for details.

5.3 Computing the neighbours

The space (V, Φ), the lattice L as well as the prime ideals $\mathfrak{p}$ and $\mathfrak{P}$ are as before. This section explains the neighbour algorithm to compute a system of representatives of the isometry classes in $\mathfrak{N}(L, \mathfrak{P})$ whenever (V, Φ) is definite. Let $\mathcal{O}' = \mathcal{O} \cap \mathcal{O}_r(\mathfrak{P})$ be the intersection of the left and right orders of $\mathfrak{P}$. Then $L/\overline{\mathfrak{P}}L$ is a vector space over the finite field $\mathcal{O}'/\overline{\mathfrak{P}}$. For $x \in L - \overline{\mathfrak{P}}L$, the class of $x + \overline{\mathfrak{P}}L$ in the projective $\mathcal{O}'/\overline{\mathfrak{P}}$-space $L/\overline{\mathfrak{P}}L$ will be denoted by $[x]$. Note that $\mathcal{O}' = \mathcal{O}$ unless E is a quaternion algebra which is unramified at $\mathfrak{p}$. In this special case, $\overline{\mathfrak{P}}$ is a non-invertible twosided ideal of $\mathcal{O}'$ and $\mathcal{O}'/\overline{\mathfrak{P}} \cong \mathfrak{o}/\mathfrak{p}$.

The first question one has to answer is: ‘Which projective classes yield $\mathfrak{P}$-neighbours of L and if so, how many?’ The exposition below follows A. Schiemann [Sch98, Section 3] who discusses the case that $\dim_K(E) = 2$.

Lemma 5.3.1 *For* $\mathfrak{P}$*-admissible vectors* $x, y \in L$*, the following statements are equivalent:*

1. $L_{x,\mathfrak{P}} = L_{y,\mathfrak{P}}$
2. $[x] = [y]$ *and* $\Phi(x, y) \in \overline{\mathfrak{P}}\mathfrak{s}(L)\mathfrak{P}$.

Proof. 1. → 2. From

$$\overline{\mathfrak{P}}^{-1}\Phi(x, y)\mathfrak{P}^{-1} = \Phi(\overline{\mathfrak{P}}^{-1}x, \overline{\mathfrak{P}}^{-1}y) \subseteq \Phi(L_{x,\mathfrak{P}}, L_{x,\mathfrak{P}})$$

it follows that $\Phi(x,y) \in \overline{\mathfrak{P}}\mathfrak{s}(L)\mathfrak{P}$ and

$$\underbrace{\overline{\mathfrak{P}}L^x_{\mathfrak{P}}}_{\subset \overline{\mathfrak{P}}L} + \mathcal{O}_r(\mathfrak{P})x = \overline{\mathfrak{P}}L_{x,\mathfrak{P}} = \overline{\mathfrak{P}}L_{y,\mathfrak{P}} = \underbrace{\overline{\mathfrak{P}}L^y_{\mathfrak{P}}}_{\subset \overline{\mathfrak{P}}L} + \mathcal{O}_r(\mathfrak{P})y$$

shows that $y \equiv \alpha x \pmod{\overline{\mathfrak{P}}L}$ for some $\alpha \in \mathcal{O}_r(\mathfrak{P})$. It remains to show that $\alpha \in \mathcal{O}$. Thus one may assume that E is a quaternion algebra which is unramified at $\mathfrak{p}$. Since $\mathcal{O}$ and $\mathcal{O}_r(\mathfrak{P})$ agree at all places of K different from $\mathfrak{p}$, it suffices to show that $\alpha \in \mathcal{O}_{\mathfrak{p}}$. Without loss of generality, $\mathcal{O}_{\mathfrak{p}} = \mathfrak{o}_{\mathfrak{p}}^{2\times 2}$ and $\mathfrak{P} = \mathcal{O}_{\mathfrak{p}} \cdot \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$ where p denotes some uniformizer of $\mathfrak{p}$. Then $\mathcal{O}_r(\mathfrak{P})_{\mathfrak{p}} = \begin{pmatrix} \mathfrak{o}_{\mathfrak{p}} & p\mathfrak{o}_{\mathfrak{p}} \\ p^{-1}\mathfrak{o}_{\mathfrak{p}} & \mathfrak{o}_{\mathfrak{p}} \end{pmatrix}$ and $\alpha = \begin{pmatrix} a & pb \\ p^{-1}c & d \end{pmatrix}$ for some $a,b,c,d \in \mathfrak{o}_{\mathfrak{p}}$. Suppose $c \notin p\mathfrak{o}_{\mathfrak{p}}$. Let $(b_1,\dots,b_m)$ be any $\mathcal{O}_{\mathfrak{p}}$-basis of $L_{\mathfrak{p}}$. Then $x = \sum_{i=1}^m \lambda_i b_i$ for some $\lambda_i = \left(\begin{smallmatrix} a_i & b_i \\ c_i & d_i \end{smallmatrix}\right) \in \mathcal{O}_{\mathfrak{p}}$. The condition $\alpha x \in L$ shows that $\alpha\lambda_i \in \mathcal{O}_{\mathfrak{p}}$ for all i. This is equivalent to $a_i, b_i \in \mathfrak{p}$, i.e. $\lambda_i \in \overline{\mathfrak{P}}_{\mathfrak{p}}$. But this contradicts the assumption $x \notin \overline{\mathfrak{P}}L$. Hence $c \in p\mathfrak{o}_{\mathfrak{p}}$ and therefore $\alpha \in \mathcal{O}$.

2. → 1. If $L_{\mathfrak{p}}$ is unimodular, let $\mathfrak{A} = \overline{\mathfrak{P}}$, otherwise let $\mathfrak{A} = \mathcal{O}$. There exist $\alpha, \beta \in \mathcal{O}' - \overline{\mathfrak{P}}$ and $v, w \in \overline{\mathfrak{P}}L$ such that $x = \alpha y + v$ and $y = \beta x + w$. Let $\gamma x + z \in L_{x,\mathfrak{P}}$ where $\gamma \in \overline{\mathfrak{P}}^{-1}$ and $z \in L^x_{\mathfrak{P}}$. To show that $\gamma x + z = \gamma\alpha y + \gamma v + z \in L_{y,\mathfrak{P}}$, it suffices to show that $\gamma v + z \in L^y_{\mathfrak{P}}$:

$$\Phi(y, \gamma v + z) \equiv \Phi(\beta x, \gamma v + z) \equiv \Phi(\beta x, \gamma v) \equiv \beta \underbrace{\Phi(x, x - \alpha y)}_{\in \overline{\mathfrak{P}}\mathfrak{P}} \overline{\gamma} \equiv 0 \pmod{\mathfrak{A}} .$$

Hence $L_{x,\mathfrak{P}} \subseteq L_{y,\mathfrak{P}}$. The converse inclusion follows the same way. □

Using the previous result, one can write down minimal subsets $R(L,\mathfrak{P}) \subset L$ such that $\{L_{x,\mathfrak{P}} \,;\, x \in R(L,\mathfrak{P})\}$ are the $\mathfrak{P}$-neighbours of L. This generalizes [Sch98, Section 3].

Proposition 5.3.2 *Let S be a system of representatives of the projective $\mathcal{O}'/\overline{\mathfrak{P}}$-space $L/\overline{\mathfrak{P}}L$. Define a subset $R(L,\mathfrak{P}) \subset L$ as follows:*

1. *If $E = K$, fix some $p \in \mathfrak{p} - \mathfrak{p}^2$. For any $x \in S$ with $Q_\Phi(x) \in \mathfrak{p}$, there exists some $z_x \in L$ such that $\Phi(z_x, x) \notin \mathfrak{p}$. Set*

   $$R(L,\mathfrak{P}) := \{x + p b_x z_x \,;\, x \in S,\ Q_\Phi(x) \in \mathfrak{p}\}$$

   where $b_x \in \mathfrak{o}$ such that $b_x \equiv -\frac{Q_\Phi(x)}{2p\Phi(z_x,x)} \pmod{\mathfrak{p}}$.

2. *If $E_{\mathfrak{p}} \cong K_{\mathfrak{p}} \oplus K_{\mathfrak{p}}$, set $R(L,\mathfrak{P}) := \{\pi x \,;\, x \in S\}$ where $\pi \in \mathfrak{P} - \overline{\mathfrak{P}}$.*

3. *If $E_{\mathfrak{p}} \cong K_{\mathfrak{p}}^{2\times 2}$, let $\pi \in \mathfrak{P} - \overline{\mathfrak{P}}$. For any $x \in S$, there exist some $z_x \in L$ such that $\Phi(z_x, \pi x) \notin \mathfrak{P}$. Further, there exists some $\beta_x \in \mathfrak{p}\mathcal{O}$ such that $\beta_x \Phi(z_x, \pi x) \notin \overline{\mathfrak{P}}\mathfrak{P}$. Set*

   $$R(L,\mathfrak{P}) := \{\pi x + b\beta_x z_x \,;\, x \in S, b + \mathfrak{p} \in \mathfrak{o}/\mathfrak{p}\} .$$

4. *Suppose E is ramified at $\mathfrak{p}$ and $L_\mathfrak{p}$ is unimodular. For any $x \in S$ with $Q_\Phi(x) \in \mathfrak{p}$, there exists some $z_x \in L$ such that $\Phi(z_x, x) \notin \mathfrak{P}$. Set*

$$R(L, \mathfrak{P}) := \{x + \beta z_x \,;\, x \in S,\ Q_\Phi(x) \in \mathfrak{p},\ \beta + \mathfrak{P}^2 \in \mathfrak{P}/\mathfrak{P}^2\}\,.$$

5. *Suppose E is ramified at $\mathfrak{p}$ and $L_\mathfrak{p}$ is $\mathfrak{P}^{-1}$-modular. For any $x \in S$, there exists some $z_x \in L$ such that $\Phi(z_x, x) \notin \mathcal{O}$. Set*

$$R(L, \mathfrak{P}) := \{x + \beta z_x \,;\, x \in S,\ \beta + \mathfrak{P}^2 \in \mathfrak{P}/\mathfrak{P}^2 \textit{ and } Q_\Phi(x) + \mathrm{T}(\Phi(\beta z_x, x)) \in \mathfrak{p}\}\,.$$

6. *If $\dim_K(E) = 2$ and $\mathfrak{p}$ is inert in E, let $p \in \mathfrak{p} - \mathfrak{p}^2$. For any $x \in S$ with $Q_\Phi(x) \in \mathfrak{p}$, there exists some $z_x \in L$ such that $\Phi(z_x, x) \notin \mathfrak{P}$. Let $R(L, \mathfrak{P})$ denote the set*

$$\{x + \beta p z_x \,;\, x \in S,\ Q_\Phi(x) \in \mathfrak{p},\ \beta + \mathfrak{P} \in \mathcal{O}/\mathfrak{P} \textit{ and } Q_\Phi(x)/p + \mathrm{T}(\beta\Phi(z_x, x)) \in \mathfrak{p}\}\,.$$

Then $\{L_{x,\mathfrak{P}} \,;\, x \in R(L, \mathfrak{P})\}$ are the $\mathfrak{P}$-neighbours of L and no proper subset of $R(L, \mathfrak{P})$ has this property.

Proof. 1. Let $x \in L - \mathfrak{p}L$. Then $Q_\Phi(x) \equiv Q_\Phi(y) \pmod{\mathfrak{p}}$ for all $y + \mathfrak{p}L \in [x]$. Hence the projective lines $[x]$ with $Q_\Phi(x) \notin \mathfrak{p}$ never yield $\mathfrak{p}$-neighbours. If $Q_\Phi(x) \in \mathfrak{p}$, then z_x exists since $L_\mathfrak{p}$ is unimodular. Further $x + p\lambda_x z_x$ is $\mathfrak{p}$-admissible. So after replacing x with $x + p\lambda_x z_x$, one may suppose that x is $\mathfrak{p}$-admissible. Let $y \in L$ with $[x] = [y]$ also be $\mathfrak{p}$-admissible. Then $y = ax + bz$ for some $a \in \mathfrak{o} - \mathfrak{p}$, $b \in \mathfrak{p}$ and $z \in L$. Thus

$$Q_\Phi(y) = a^2 Q_\Phi(x) + 2ab\Phi(x, z) + b^2 Q_\Phi(z) \in \mathfrak{p}^2$$

and therefore $\Phi(x, y) \equiv b\Phi(x, z) \equiv 0 \pmod{\mathfrak{p}^2}$. Hence Lemma 5.3.1 shows that $[x]$ yields a single neighbour.

2. and 3. Let $x \in L - \overline{\mathfrak{P}}L$. Then $Q_\Phi(\pi x) \in \overline{\mathfrak{P}}\mathfrak{P}$. Note that this implies that $\pi x \notin \overline{\mathfrak{P}}L$. This is clearly true if E is commutative and in the quaternion case one can argue as in the proof of Lemma 5.3.1. Hence $R(L, \mathfrak{P})$ contains only $\mathfrak{P}$-admissible vectors. Let $y = \alpha\pi x + \beta z$ be $\mathfrak{P}$-admissible where $\alpha \in \mathcal{O}' - \overline{\mathfrak{P}}$, $\beta \in \overline{\mathfrak{P}}$ and $z \in L$. Then

$$\underbrace{Q_\Phi(y)}_{\in\mathfrak{p}} = \alpha\overline{\alpha}\underbrace{\pi\overline{\pi}}_{\in\mathfrak{p}} Q_\Phi(x) + \underbrace{\beta\overline{\beta}}_{\in\mathfrak{p}} Q_\Phi(z) + \alpha\Phi(\pi x, z)\underbrace{\overline{\beta}}_{\in\mathfrak{P}} + \beta\Phi(z, \pi x)\overline{\alpha}$$

shows that $\beta\Phi(z, \pi x)\overline{\alpha} \in \mathfrak{P}$. From $\beta\Phi(z, \pi x) \in \overline{\mathfrak{P}} \subseteq \mathcal{O}'$ and $\overline{\alpha} \notin \mathfrak{P}$ it follows that $\beta\Phi(z, \pi x) \in \mathfrak{P} \cap \overline{\mathfrak{P}}$. If E is commutative, then $\mathfrak{P} \cap \overline{\mathfrak{P}} = \overline{\mathfrak{P}}\mathfrak{P}$ and therefore $\Phi(y, x) \equiv \beta\Phi(z, \pi x) \equiv 0 \pmod{\overline{\mathfrak{P}}\mathfrak{P}}$. So by Lemma 5.3.1, the line $[x]$ only yields a single neighbour. This finishes the proof of part 2.

Suppose now E is a quaternion algebra. The element z_x exists since $\pi x \notin \overline{\mathfrak{P}}L$ and L is unimodular. To show that β_x exists, one may suppose that $\mathcal{O}_\mathfrak{p} = \mathfrak{o}_\mathfrak{p}^{2\times 2}$ and $\mathfrak{P} = \mathcal{O}_\mathfrak{p} \cdot \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$ where p denotes some uniformiser of $\mathfrak{p}$. Then $\Phi(z_x, \pi x) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $a, b, c, d \in \mathfrak{o}_\mathfrak{p}$. Set $\beta_x = p\left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right)$ with $e, f, g, h \in \mathfrak{o}_\mathfrak{p}$. Then $\beta_x\Phi(z_x, \pi x) \in (\overline{\mathfrak{P}}\mathfrak{P})_\mathfrak{p}$ if and only if $eb + hd \in \mathfrak{p}$.

The condition $\Phi(z_x, \pi x) \notin \mathfrak{P}$ implies that b and d cannot both lie in $\mathfrak{p}$. Hence there exists $\beta_x \in \mathfrak{p}\mathcal{O}$ such that $\beta_x \Phi(z_x, \pi x) \notin \overline{\mathfrak{P}}\mathfrak{P}$. Let $y' = \alpha' \pi x + \beta' z'$ be $\mathfrak{P}$-admissible where $\alpha' \in \mathcal{O}' - \overline{\mathfrak{P}}$, $\beta' \in \overline{\mathfrak{P}}$ and $z' \in L$. By Lemma 5.3.1,

$$L_{y,\mathfrak{P}} = L_{y',\mathfrak{P}} \iff \beta\Phi(z, \pi x)\overline{\alpha} + \alpha\Phi(\pi x, z')\overline{\beta'} \in \overline{\mathfrak{P}}\mathfrak{P}\,.$$

Since $(\mathfrak{P} \cap \overline{\mathfrak{P}})/\overline{\mathfrak{P}}\mathfrak{P}$ is an one-dimensional $\mathfrak{o}/\mathfrak{p}$-space, the line $[x]$ gives rise to no more than $\#(\mathfrak{o}/\mathfrak{p})$ neighbours. Conversely, the set $\{\pi x + b\beta_x z_x\,;\, b + \mathfrak{p} \in \mathfrak{o}/\mathfrak{p}\}$ yields $\#(\mathfrak{o}/\mathfrak{p})$ different neighbours.

4. If $x \in L - \mathfrak{P}L$ and $Q_\Phi(x) \in \mathfrak{p}$ then $Q_\Phi(y) \in \mathfrak{p}$ for all $y + \mathfrak{P}L \in [x]$. Hence one only has to consider the projective lines $[x]$ such that $Q_\Phi(x) \in \mathfrak{p}$ and then every representative of $[x]$ is $\mathfrak{P}$-admissible. The existence of z_x follows from the fact that L is unimodular and $x \notin \mathfrak{P}L$. Suppose now $y = \alpha x + \beta z$ for some $\alpha \in \mathcal{O} - \mathfrak{P}$, $\beta \in \mathfrak{P}$ and $z \in L$. By Lemma 5.3.1, x and y yield the same neighbour if and only if $\beta\Phi(z, x) \in \mathfrak{P}^2$. Since $\beta \in \mathfrak{P}$, the line $[x]$ can yield no more than $\#(\mathcal{O}/\mathfrak{P})$ different neighbours. Conversely, different vectors from $\{x + \beta z_x\,;\, \beta + \mathfrak{P}^2 \in \mathfrak{P}/\mathfrak{P}^2\}$ never give the same neighbours.

5. A vector $x + \beta z_x$ with $\beta \in \mathfrak{P}$ is $\mathfrak{P}$-admissible if and only if $Q_\Phi(x) + \mathrm{T}(\beta\Phi(z_x, x)) \in \mathfrak{p}$. Let $x' := x + \beta z_x$ and $y = \alpha x' + \gamma z$ with $\alpha \in \mathcal{O} - \mathfrak{P}$, $\beta, \gamma \in \mathfrak{P}$ and $z \in L$ be $\mathfrak{P}$-admissible. After rescaling y with some element in $\mathcal{O} - \mathfrak{P}$, one may assume that $\alpha = 1$. The assumption that y is $\mathfrak{P}$-admissible yields that $\Phi(y, y) \equiv \mathrm{T}(\gamma\Phi(z, x')) \equiv 0 \pmod{\mathfrak{p}}$. By Lemma 5.3.1, x' and y yield the same neighbour if and only if $0 \equiv \Phi(y, x') \equiv \gamma\Phi(z, x')$ $\pmod{\mathfrak{P}}$. Now the relative field extension $(\mathcal{O}/\mathfrak{P})/(\mathfrak{o}/\mathfrak{p})$ is either trivial or quadratic, depending on $\dim_K(E)$. So $[x]$ yields a single neighbour if E is commutative but $\#(\mathfrak{o}/\mathfrak{p})$ different neighbours if E is a quaternion algebra. Conversely, the set

$$\{x + \beta z_x\,;\, \beta + \mathfrak{P}^2 \in \mathfrak{P}/\mathfrak{P}^2 \text{ and } Q_\Phi(x) + \mathrm{T}(\Phi(\beta z_x, x)) \in \mathfrak{p}\}$$

consists of $\mathfrak{P}$-admissible representatives of $[x]$ that yield the correct number of neighbours.

6. If $x \in L - \mathfrak{P}L$ such that $Q_\Phi(x) \notin \mathfrak{p}$, then $[x]$ contains no admissible vector. Suppose now $x \in L - \mathfrak{P}L$ and $Q_\Phi(x) \in \mathfrak{p}$. Let $y = \alpha x + p\beta z$ with $\alpha \in \mathcal{O} - \mathfrak{P}$, $\beta \in \mathcal{O}$ and $z \in L$ by any representative of $[x]$. If y is $\mathfrak{P}$-admissible, so is αy and the two vectors give the same neighbour. Hence one may assume that $\alpha = 1$. Then y is $\mathfrak{P}$-admissible if and only if $Q_\Phi(x)/p + \mathrm{T}(\beta\Phi(y, x)) \in \mathfrak{p}$. If $\Phi(y, x) \in \mathfrak{P}$ and y is $\mathfrak{P}$-admissible, then x is $\mathfrak{P}$-admissible and $L_{x,\mathfrak{P}} = L_{y,\mathfrak{P}}$. Suppose $\Phi(y, x) \notin \mathfrak{P}$. The trace bilinear form of the relative extension $(\mathcal{O}/\mathfrak{P})/(\mathfrak{o}/\mathfrak{p})$ is non-degenerate, hence there are $\#(\mathfrak{o}/\mathfrak{p})$ classes $\beta + \mathfrak{P} \in \mathcal{O}/\mathfrak{P}$ such that y is $\mathfrak{P}$-admissible. From Lemma 5.3.1 it follows that the projective line $[x]$ yields no more than $\#(\mathfrak{o}/\mathfrak{p})$ different neighbours. Conversely, the vectors in

$$\{x + p\beta z_x\,;\, \beta + \mathfrak{P} \in \mathcal{O}/\mathfrak{P} \text{ and } Q_\Phi(x)/p + \mathrm{T}(\beta\Phi(z_x, x)) \in \mathfrak{p}\}$$

are $\mathfrak{P}$-admissible and they give rise to different neighbours. □

Using the previous result, one can count the number of $\mathfrak{P}$-neighbours of L, see [Sch98, Lemma 3.3].

Corollary 5.3.3 *In the situation of Lemma 5.3.1 let $q = \mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})$ and $\mathfrak{s}(L_\mathfrak{p}) = \mathfrak{P}^i$. The number $\#R(L, \mathfrak{P})$ of $\mathfrak{P}$-neighbours of L is given by the following table:*

$\dim_K(E)$	m	$E_\mathfrak{p}/K_\mathfrak{p}$	i	$\#R(L, \mathfrak{P})$
1	*odd*	–	–	$(q^{m-1} - 1)/(q - 1)$
1	*even*	–	–	$(q^{m/2} - \varepsilon)(q^{m/2-1} + \varepsilon)/(q - 1)$
2	–	*split*	–	$(q^m - 1)/(q - 1)$
2	–	*inert*	–	$q(q^m - (-1)^m)(q^{m-1} + (-1)^m)/(q^2 - 1)$
2	*odd*	*ramified*	*even*	$q(q^{m-1} - 1)/(q - 1)$
2	*even*	*ramified*	*even*	$q(q^{m/2} - \varepsilon)(q^{m/2-1} + \varepsilon)/(q - 1)$
2	–	*ramified*	*odd*	$(q^m - 1)/(q - 1)$
4	–	*unramified*	–	$q(q^{2m} - 1)/(q - 1)$
4	–	*ramified*	*even*	$q^2(q^m - (-1)^m)(q^{m-1} + (-1)^m)/(q^2 - 1)$
4	–	*ramified*	*odd*	$q(q^{2m} - 1)/(q^2 - 1)$

where $\varepsilon = +1$ if $\mathrm{disc}(V, \Phi) \in \mathrm{N}(E_\mathfrak{p}^*)$ and $\varepsilon = -1$ otherwise.

Proof. If $E = K$, one may assume that $i = 0$. Then $\#R(L, \mathfrak{P})$ is the number of isotropic lines in the $\mathfrak{o}/\mathfrak{p}$-space $L' := L/\mathfrak{P}L$ equipped with the quadratic form

$$Q' \colon L' \to \mathfrak{o}/\mathfrak{p},\ x + \mathfrak{P}L \mapsto Q_\Phi(x) + \mathfrak{p}\,.$$

These numbers have been worked out for example in [Kne02, Section V.13]. Suppose $\dim_K(E) = 2$. The split case as well as the ramified case with i odd are obvious. In the remaining cases, one may assume that $i = 0$ and again, it boils down to work out the number of isotropic lines in (L', Q'). Note that if $\mathfrak{p}$ is inert in E, then (L', Q') is of dimension $2m$ and hyperbolic if and only if m is even, see [Sch98, Lemma 3.3] for details. Suppose now $\dim_K(E) = 4$. If $\mathfrak{p}$ is ramified in E and i is even, one may assume that $i = 0$. Then $\#R(L, \mathfrak{P})(q^2 - 1)/q^2$ is the number of anisotropic vectors in the $2m$-dimensional $\mathfrak{o}/\mathfrak{p}$-space $L' := L/\mathfrak{P}L$ equipped with the quadratic form

$$Q' \colon L' \to \mathfrak{o}/\mathfrak{p},\ x + \mathfrak{P}L \mapsto Q_\Phi(x) + \mathfrak{p}\,.$$

The quadratic space (L', Q') is again hyperbolic if and only if m is even. All other cases are again trivial. □

Lemma 5.3.1 yields a method to enumerate the set of all isometry classes in $\mathrm{gen}(L)$ which are represented by $\mathcal{N}(L, \mathfrak{P})$.

Algorithm 5.3.4 IteratedNeighbours$(L, \mathfrak{P})$

Input: An $\mathcal{O}$-lattice L in a definite hermitian space (V, Φ) over E of dimension m and some maximal left ideal $\mathfrak{P}$ of $\mathcal{O}$ such that $\mathfrak{p} := \mathfrak{P} \cap \mathfrak{o}$ satisfies the assumptions made in the beginning of Section 5.2.

Output: A set S of representatives of the isometry classes in $\mathcal{N}(L, \mathfrak{P})$.

```
If $L_\mathfrak{p}$ is unimodular, set $\mathfrak{A} = \overline{\mathfrak{P}}$; otherwise set $\mathfrak{A} = \mathcal{O}$.
```

```
 2: Initialise the sets $S = T = \{L\}$.
 3: while there exists some $M \in T$ do
 4:     Exclude $M$ from $T$.
 5:     Let $(x_1, \dots, x_m)$ be a basis of a free $\mathcal{O}$-submodule $M'$ of $M$ such that $M_\mathfrak{p} = M'_\mathfrak{p}$.
 6:     for $x \in R(M, \mathfrak{P})$ do
 7:         Set $I := \{1 \le i \le m \,;\, \Phi(x, x_i) \notin \mathfrak{A}\}$ and $i := \min(I)$.
 8:         For $j \in I - \{i\}$ let $\lambda_j \in \mathcal{O}$ such that $\Phi(x, x_j) - \Phi(x, x_i)\overline{\lambda_j} \in \mathfrak{A}$.
 9:         Set $L' := \sum_{j \notin I} \mathcal{O}x_j + \sum_{j \in I - \{i\}} \mathcal{O}(x_j - \lambda_j x_i) + \overline{\mathfrak{A}}x_i + \overline{\mathfrak{P}}^{-1}x + \mathfrak{p}M$.
10:         if $L'$ is not isometric to any element in $S$ then
11:             Include $L'$ to both $S$ and $T$.
12:         end if
13:     end for
14: end while
15: return $S$.
```

Proof. Note that by induction, the lattice M is always modular at $\mathfrak{p}$. Hence I is nonempty. Further, the lattice L' in line 9 equals $M_{x,\mathfrak{P}}$. So the algorithm does enumerate some lattices in $\mathcal{N}(L, \mathfrak{P})$. The algorithm terminates since the number of isometry classes in $\operatorname{gen}(L)$ is finite. The fact that the algorithm reaches every isometry class in $\mathcal{N}(L, \mathfrak{P})$ follows from Proposition 5.2.5 and Remark 5.2.2. □

5.4 Enumerating all isometry classes in a given genus

In this section, algorithms to compute a system of representatives of all isometry classes of an $\mathcal{O}$-lattice L in (V, Φ) are given. In view of Corollary 5.1.4 and Algorithm 5.3.4, it suffices to answer the question, which spinor/special genera have to be joined to cover a given genus completely. If E is a quaternion algebra, then $\operatorname{gen}(L) = \operatorname{sgen}(L)$. So only the two cases where E is commutative remain. They will be discussed individually below.

5.4.1 The quadratic case

Suppose $E = K$ is a number field and let (V, Φ) be a regular quadratic space over K of rank $m \ge 3$. The question how the genus of some lattice decomposes into spinor genera is answered by M. Kneser in [Kne56] using the spinor norms introduced by M. Eichler. It turns out that a description using proper isometry classes is more suitable.

Definition 5.4.1 Let L, L' be $\mathfrak{o}$-lattices in (V, Φ).

1. The lattices L and L' are said to be *properly isometric*, if $L' = \varphi(L)$ for some $\varphi \in \mathbf{SO}(V, \Phi)$. The *proper isometry class* $\operatorname{cls}^+(L)$ is the set of all $\mathfrak{o}$-lattices properly isometric to L and $\operatorname{Aut}^+(L) := \operatorname{Aut}(L) \cap \mathbf{SO}(V, \Phi)$ is the *proper automorphism group* of L. Similarly one defines $\operatorname{Aut}^+(L_\mathfrak{p})$ for $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$.

2. The lattices L and L' are said to be in the same *proper spinor genus*, if there exists some $\varphi \in \mathbf{SO}(V, \Phi)$ such that $\varphi(L)_\mathfrak{p} = \sigma_\mathfrak{p}(L'_\mathfrak{p})$ with $\sigma_\mathfrak{p} \in \mathbf{S}(V_\mathfrak{p}, \Phi)$ for all $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$. The proper spinor genus of L will be denoted by $\operatorname{sgen}^+(L)$.

The following remark explains how classes, spinor genera and genera differ from their 'proper' counterparts, see also Corollary 5.4.8.

Remark 5.4.2 Let L be an $\mathfrak{o}$-lattice in (V, Φ) and let $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$.

1. $\mathrm{cls}(L) = \mathrm{cls}^+(L)$ if and only if $\mathrm{Aut}(L) \neq \mathrm{Aut}^+(L)$. In particular, if m is odd, then $-\mathrm{id}_V \in \mathrm{Aut}(L) - \mathrm{Aut}^+(L)$, so $\mathrm{cls}(L) = \mathrm{cls}^+(L)$.

2. If $\mathrm{Aut}(L) = \mathrm{Aut}^+(L)$, then $\mathrm{cls}(L) = \mathrm{cls}^+(L) \uplus \mathrm{cls}^+(\tau(L))$ where τ denotes any isometry in $\mathbf{O}(V, \Phi) - \mathbf{SO}(V, \Phi)$. For example one can take τ to be a reflection.

3. Let $x \in L_\mathfrak{p}$ such that $Q_\Phi(x)\mathfrak{o} = \mathfrak{n}(L_\mathfrak{p})$. The reflection τ_x fixes L. In particular, $[\mathrm{Aut}(L_\mathfrak{p}) : \mathrm{Aut}^+(L_\mathfrak{p})] = 2$. Moreover, if $L' \in \mathrm{gen}(L)$, then for all $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$ there exists some $\sigma_\mathfrak{p} \in \mathbf{SO}(V_\mathfrak{p}, \Phi)$ such that $L_\mathfrak{p} = \sigma_\mathfrak{p}(L'_\mathfrak{p})$.

For the remainder of this section let L be a fixed $\mathfrak{o}$-lattice in (V, Φ).

Definition 5.4.3 Given a prime ideal $\mathfrak{p}$ of $\mathfrak{o}$, the *group of spinor norms* of $L_\mathfrak{p}$ is

$$\theta(L_\mathfrak{p}) := \theta(\mathrm{Aut}^+(L_\mathfrak{p})) = \{\theta(\sigma)\,;\, \sigma \in \mathrm{Aut}^+(L)\}\,.$$

For odd prime ideals, the computation of spinor norms was also solved by M. Kneser.

Theorem 5.4.4 *Suppose $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$ is odd. Let $L_\mathfrak{p} = \perp_{i=1}^r L_i$ be a Jordan decomposition and let*

$$F = \bigcup_{1 \le i \le r} \{Q_\Phi(x)\,;\, x \in L_i \text{ and } Q_\Phi(x) \notin \mathfrak{p}\mathfrak{s}(L_i)\}\,.$$

Then $\theta(L_\mathfrak{p}) = \{(\prod_{i=1}^{2\ell} f_i)(K_\mathfrak{p}^*)^2\,;\, f_i \in F \text{ and } \ell \in \mathbb{N}\}$. In particular, $\mathfrak{o}_\mathfrak{p}^*(K_\mathfrak{p}^*)^2 \subseteq \theta(L_\mathfrak{p})$ if $\mathrm{rank}(L_i) > 1$ for some i and $\theta(L_\mathfrak{p}) = \mathfrak{o}_\mathfrak{p}^*(K_\mathfrak{p}^*)^2$ if L is modular.

Proof. See [Kne56, Satz 3]. □

If $\mathfrak{p}$ is a prime ideal over 2, then $\mathfrak{o}_\mathfrak{p}^*(K_\mathfrak{p}^*)^2 \subseteq \theta(L_\mathfrak{p})$ if $L_\mathfrak{p}$ has a Jordan block of rank at least 3, c.f. [O'M73, Example 93:20]. The explicit computation of $\theta(L_\mathfrak{p})$ is quite involved and was only solved recently by C. Beli in [Bel03].

The question, whether $M \in \mathrm{gen}(L)$ is in the same proper spinor genus as L can be answered using idèles. The presentation given here follows T. O'Meara [O'M73, Section 102]. For the remainder of this section, the following notation will be used.

- The group of *idèles* of K will be denoted by

  $$J = \{(x_v)_v \in \prod_{v \in \Omega(K)} K_v^*\,;\, x_\mathfrak{p} \in \mathfrak{o}_\mathfrak{p}^* \text{ for all but finitely many } \mathfrak{p} \in \mathbb{P}(\mathfrak{o})\}\,.$$

  Note that K^* can be regarded as a subgroup of J via the diagonal embedding.

- Given a prime ideal $\mathfrak{p}$ of $\mathfrak{o}$ and some $x \in K_\mathfrak{p}^*$, let $j(\mathfrak{p}, x)$ be the idèle satisfying $j(\mathfrak{p}, x)_\mathfrak{p} = x$ and $j(\mathfrak{p}, x)_v = 1$ for all places v different from $\mathfrak{p}$.

- Let $J^L = \{j \in J\,;\, j_\mathfrak{p} \in \theta(L_\mathfrak{p}) \text{ for all } \mathfrak{p} \in \mathbb{P}(\mathfrak{o})\}$.
- Let S be the set of all infinite places v of K such that (V_v, Φ) is anisotropic. For any subgroup X of J, let X_S be the subgroup $\{x \in X\,;\, x_v > 0 \text{ for all } v \in S\}$ of X.
- Let $P = \{\mathfrak{p} \in \mathbb{P}(\mathfrak{o})\,;\, \theta(L_\mathfrak{p}) \neq \mathfrak{o}_\mathfrak{p}^*(K_\mathfrak{p}^*)^2\}$, which can be computed using Theorem 5.4.4 and [Bel03]. Further, let D be the divisor $\prod_{v \in S} v \cdot \prod_{\mathfrak{p} \in P} \mathfrak{p}^{1+\operatorname{ord}_\mathfrak{p}(4)}$. The ray class group of $\mathfrak{o}$ with respect to D will be denoted by $\mathrm{Cl}_D(\mathfrak{o})$.
- Let $J_D = \{j \in J_S\,;\, j_\mathfrak{p} \equiv 1 \pmod{\mathfrak{p}^{1+\operatorname{ord}_\mathfrak{p}(4)}} \text{ for } \mathfrak{p} \in P \text{ and } j_\mathfrak{p} \in \mathfrak{o}_\mathfrak{p}^* \text{ for } \mathfrak{p} \notin P\}$.
- Given a fractional ideal $\mathfrak{a}$ of K which is not supported at P, let $[\mathfrak{a}]$ be its class in $\mathrm{Cl}_D(\mathfrak{o})$. Similarly, given an idèle $j \in J$ with $j_\mathfrak{p} \in \mathfrak{o}_\mathfrak{p}^*$ for all $\mathfrak{p} \in P$, then $[j]$ denotes the class of $\prod_{\mathfrak{p} \in \mathbb{P}(\mathfrak{o})} \mathfrak{p}^{\operatorname{ord}_\mathfrak{p}(j_\mathfrak{p})}$ in $\mathrm{Cl}_D(\mathfrak{o})$.

Using idèle groups and spinor norms it is possible to answer which lattices in $\operatorname{gen}(L)$ are contained in the same proper spinor genus.

Theorem 5.4.5 *Let $M \in \operatorname{gen}(L)$. Define some idèle $j \in J$ as follows. If $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$ with $L_\mathfrak{p} \neq M_\mathfrak{p}$ set $j_\mathfrak{p} = \theta(\sigma_\mathfrak{p})$ where $\sigma_\mathfrak{p} \in \mathbf{SO}(V_\mathfrak{p}, \Phi)$ such that $M_\mathfrak{p} = \sigma_\mathfrak{p}(L_\mathfrak{p})$. On all other places v of K set $j_v = 1$. Then $M \in \operatorname{sgen}^+(L)$ if and only if $j \in K_S^* J^L$. In particular, the number of proper spinor genera in $\operatorname{gen}(L)$ is $[J : K_S^* J^L] < \infty$.*

Proof. See for example [O'M73, Section 102]. □

So the above theorem tells exactly, which (proper) spinor genera have to be joined in order to cover all isometry classes of $\operatorname{gen}(L)$. However, the group $J/K_S^*J^L$, being a quotient of two infinite groups, is difficult to handle algorithmically. Thus an explicit isomorphism between $J/K_S^*J^L$ and some quotient of the ray class group $\mathrm{Cl}_D(\mathfrak{o})$ will be given below. I learned this description from Wai Kiu Chan [Cha13] on the AIM conference on *Algorithms for lattices and algebraic automorphic forms*.

Theorem 5.4.6

1. *The map $J/K^* \to J/K_S^*J^L$, $jK^* \mapsto cjK_S^*J^L$ with $c \in K^*$ such that $cj \in J_S$ is a well defined, surjective homomorphism of groups with kernel $K^*J_S^L/K^*$. Hence it induces an isomorphism*

$$\psi_1 \colon J/K^*J_S^L \to J/K_S^*J^L\,.$$

2. *The map $\psi \colon J/K^* \to \mathrm{Cl}_D(\mathfrak{o})$, $jK^* \mapsto [cj]$ where $c \in K^*$ such that $cj \in J_S$ and $cj_\mathfrak{p} \equiv 1 \pmod{\mathfrak{p}^{1+\operatorname{ord}_\mathfrak{p}(4)}}$ for all $\mathfrak{p} \in P$ is a well defined, surjective homomorphism of groups with kernel K^*J_D/K^*. Hence it induces an isomorphism*

$$\psi_2 \colon J/K^*J_D \to \mathrm{Cl}_D(\mathfrak{o})\,.$$

3. *For $\mathfrak{p} \in P$ let $X_\mathfrak{p}$ be a set of generators of $\theta(L_\mathfrak{p})/(K_\mathfrak{p}^*)^2$. Then*

$$U = \langle \{\psi(j(\mathfrak{p}, x)K^*)\,;\, x(K_\mathfrak{p}^*)^2 \in X_\mathfrak{p},\ \mathfrak{p} \in P\},\ \mathrm{Cl}_D(\mathfrak{o})^2 \rangle$$

does not depend the chosen representatives. Further,

$$\phi\colon J/K_S^* J^L \to \mathrm{Cl}_D(\mathfrak{o})/U,\ jK_S^*J^L \mapsto \psi(jK^*)U$$

is an isomorphism.

Proof. The first two parts are verified directly. The choice of D implies that $J^2 J_D \subseteq J_S^L$. Further, ψ maps $K^*J^2J_D/K^*$ onto $\mathrm{Cl}_D(\mathfrak{o})^2$. Since $\mathrm{Cl}_D(\mathfrak{o})/\mathrm{Cl}_D(\mathfrak{o})^2$ is an elementary abelian 2-group, the subgroup U does not depend on the sets $X_\mathfrak{p}$. The elements in $K^*J_S^L/K^*J^2J_D$ are generated by idèles of the form $\{j(\mathfrak{p},x)\,;\,\mathfrak{p}\in P \text{ and } x \in X_\mathfrak{p}\}$. So the image of $K_S^*J^L/K^*J_D$ under ψ_2 is U. Thus ϕ is an isomorphism. □

Theorems 5.4.5 and 5.4.6 yield the following results, including an algorithm for computing representatives of the isometry classes in $\mathrm{gen}(L)$ in the definite case.

Corollary 5.4.7 *Let $M \in \mathrm{gen}(L)$ and let j be the idèle from Theorem 5.4.5. Then the following statements are equivalent.*

1. $M \in \mathrm{sgen}^+(L)$.
2. $j \in K_S^*J^L$.
3. $\phi(j) = 1$ *where ϕ is as in Theorem 5.4.6.*

Corollary 5.4.8 *Let $x \in V$ be anisotropic and let $Q = \{\mathfrak{p} \in \mathbb{P}(\mathfrak{o})\,;\, Q_\Phi(x)\mathfrak{o}_\mathfrak{p} \neq \mathfrak{n}(L)_\mathfrak{p}\}$. For $\mathfrak{p} \in P \cup Q$ let $x_\mathfrak{p} \in L_\mathfrak{p}$ such that $Q_\Phi(x_\mathfrak{p})\mathfrak{o}_\mathfrak{p} = \mathfrak{n}(L)_\mathfrak{p}$. Let $j \in J$ be defined by*

$$j_v = \begin{cases} 1 & \text{if } v \notin P \cup Q,\\ Q_\Phi(x)Q_\Phi(x_v) & \text{if } v \in P\cup Q. \end{cases}$$

Then the following statements are equivalent:

1. $\mathrm{sgen}^+(L) = \mathrm{sgen}(L)$.
2. $\mathrm{sgen}^+(L') = \mathrm{sgen}(L')$ *for all* $L' \in \mathrm{gen}(L)$.
3. $\phi(j) = 1$ *where ϕ is as in Theorem 5.4.6.*

In particular, if these conditions hold, then the number of proper spinor genera in $\mathrm{gen}(L)$ *equals the number of spinor genera in* $\mathrm{gen}(L)$*. Otherwise it is twice that number.*

Proof. The equality $\mathrm{sgen}^+(L) = \mathrm{sgen}(L)$ holds if and only if $\tau_x(L) \in \mathrm{sgen}^+(L)$. The latter condition is equivalent to $\phi(j) = 1$ by Theorems 5.4.5 and 5.4.6. Further, j only depends on $\mathrm{gen}(L)$ by construction. □

In view of Proposition 5.2.7, let $\mathcal{N}^+(L,\mathfrak{p})$ be the set

$$\{M \in \mathrm{gen}(L)\,;\, \text{there exists } M' \in \mathrm{cls}^+(M) \text{ such that } L_\mathfrak{q} = M'_\mathfrak{q} \text{ for all } \mathfrak{q} \in \mathbb{P}(\mathfrak{o}) - \{\mathfrak{p}\}\}\,.$$

The decomposition of $\mathcal{N}^+(L,\mathfrak{p})$ into proper spinor genera is explained by the following result which strengthens Corollary 5.2.8/3.

Lemma 5.4.9 *Let U be the subgroup of $\mathrm{Cl}_D(\mathfrak{o})$ as in Theorem 5.4.6. Let $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$ be odd such that $L_\mathfrak{p}$ is modular. Further, let M be a $\mathfrak{p}$-neighbour of L and let p denote a uniformiser of $\mathfrak{p}$.*

1. *There exists some $\sigma \in \mathbf{SO}(V_\mathfrak{p}, \Phi)$ such that $M_\mathfrak{p} = \sigma(L_\mathfrak{p})$ and $\theta(\sigma) = p(K^*)^2$.*
2. *The set $\mathcal{N}^+(L, \mathfrak{p})$ consists of at most two proper spinor genera. More precisely, if $[\mathfrak{p}] \in U$, then $\mathcal{N}^+(L, \mathfrak{p}) = \mathrm{sgen}^+(L)$. Otherwise $\mathcal{N}^+(L, \mathfrak{p}) = \mathrm{sgen}^+(L) \uplus \mathrm{sgen}^+(M)$.*

Proof. 1. There exists some $\mathfrak{p}$-admissible $x \in L$ such that $M = L_{x,\mathfrak{p}}$. Let $y \in L_\mathfrak{p}$ such that $\Phi(x, y) = 1$. In particular, $L_\mathfrak{p} = \langle x, y\rangle \perp L'$ for some suitable sublattice L' of $L_\mathfrak{p}$. Then $M_\mathfrak{p} = \langle p^{-1}x,\, py\rangle \perp L'$. Hence it suffices to discuss the case that $\mathrm{rank}(L) = 2$. After replacing x with $x + upy$ for some $u \in \mathfrak{o}_\mathfrak{p}$, one may assume that $Q_\Phi(x) = 0$. So without loss of generality, the Gram matrix of (x, y) is $H(0)$. But then $\sigma := \tau_{x-py} \circ \tau_{x-y}$ does the trick.
2. This is an immediate consequence of the previous corollary and the first part. □

Corollary 5.4.10 *Suppose (V, Φ) is indefinite. Let ϕ, U be as in Theorem 5.4.6 and let j be as in Corollary 5.4.8. Then*

1. $\mathrm{sgen}(L) = \mathrm{cls}(L)$ *and* $\mathrm{sgen}^+(L) = \mathrm{cls}^+(L)$*. Moreover,* $\mathrm{cls}^+(L) = \mathrm{cls}(L)$ *if and only if* $\phi(j) = 0$*.*
2. *Let $\mathfrak{p}_1, \dots, \mathfrak{p}_{h^+}$ be odd prime ideals of $\mathfrak{o}$ such that $L_{\mathfrak{p}_i}$ is modular and $[\mathfrak{p}_1], \dots, [\mathfrak{p}_{h^+}]$ is a transversal of U in $\mathrm{Cl}_D(\mathfrak{o})$. Let L_i be a $\mathfrak{p}_i$-neighbour of L. Then $L_1, \dots, L_{h^+}$ represent the proper isometry classes (proper spinor genera) in* $\mathrm{gen}(L)$*.*
3. *Let $\mathfrak{p}_1, \dots, \mathfrak{p}_h$ be odd prime ideals of $\mathfrak{o}$ such that $L_{\mathfrak{p}_i}$ is modular and $[\mathfrak{p}_1], \dots, [\mathfrak{p}_h]$ is a transversal of $\langle U, \phi(j)\rangle$ in $\mathrm{Cl}_D(\mathfrak{o})$. Let L_i be a $\mathfrak{p}_i$-neighbour of L. Then $L_1, \dots, L_h$ represent the isometry classes (spinor genera) in* $\mathrm{gen}(L)$*.*

Proof. The first assertion is a consequence of strong approximation, c.f. Corollary 5.1.4 and the second follows immediately from Corollary 5.4.7 and Lemma 5.4.9. The last assertion follows from the first two parts and Corollary 5.4.8. □

So the above result solves the indefinite case. The definite case is handled by the following algorithm.

Algorithm 5.4.11 GenusRepresentatives(L)
Input: An $\mathfrak{o}$-lattice L in the definite quadratic space (V, Φ) over K.
Output: A set of representatives of the isometry classes in $\mathrm{gen}(L)$.

```
1: Let $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$ of minimal norm such that $2 \notin \mathfrak{p}$ and $L_\mathfrak{p}$ is modular.
2: Let $U$ be the subgroup of $\mathrm{Cl}_D(\mathfrak{o})$ as in Theorem 5.4.6.
3: Replace $U$ by $\langle U, [\mathfrak{p}]\rangle \le \mathrm{Cl}_D(\mathfrak{o})$.
4: Compute a set $G$ of prime ideals, coprime to $2\mathfrak{o}$, such that $L_\mathfrak{q}$ is modular for all $\mathfrak{q} \in G$
   and $\{[g]U \,;\, g \in G\}$ generates $\mathrm{Cl}_D(\mathfrak{o})/U$.
```

```
 5: Let $S$ be the output of IteratedNeighbours($L$, $\mathfrak{p}$) and initialize the list $\mathcal{S} = [S]$.
 6: Initialise $i = 1$.
 7: while $i \le \#\mathcal{S}$ do
 8:     for $\mathfrak{q} \in G$ do
 9:         Let $M$ be a $\mathfrak{q}$-neighbour of $L'$ where $L' \in \mathcal{S}[i]$.
10:         if there exists no lattice in $\bigcup_{S \in \mathcal{S}} S$ isometric to $M$ then
11:             Let $S$ be the output of IteratedNeighbours($M$, $\mathfrak{p}$).
12:             Append $S$ as the last element of $\mathcal{S}$.
13:         end if
14:     end for
15:     Increment $i$.
16: end while
17: return $\bigcup_{S \in \mathcal{S}} S$.
```

Proof. Theorems 5.4.5 and 5.4.6 show that the group $\mathrm{Cl}_D(\mathfrak{o})/U$ acts transitively on the spinor genera in the genus of L via

$$([g]U, \operatorname{sgen}(L')) \mapsto \operatorname{sgen}(M') \quad \text{where } M' \text{ denotes some } g\text{-neighbour of } L'.$$

The algorithm simply implements the standard orbit enumeration of the orbit of $\operatorname{sgen}(L)$ under this action. Note that Algorithm 5.3.4 computes representatives of the isometry classes of one or two spinor genera. Hence the check in line 10 ensures that each spinor genus is only visited once. □

5.4.2 The hermitian case

Suppose E/K is a quadratic extension of number fields. The question how the genus of a given $\mathcal{O}$-lattice L decomposes into special genera was answered by G. Shimura in [Shi64]. To state the result, some more notation is required.

- Let $C_0 = \{[\mathfrak{A}] \in \mathrm{Cl}(\mathcal{O})\,;\, \overline{\mathfrak{A}} = \mathfrak{A}\} \trianglelefteq \mathrm{Cl}(\mathcal{O})$. The group C_0 is generated by
$$\{[\mathfrak{P}] \in \mathrm{Cl}(\mathcal{O})\,;\, \mathfrak{P} \text{ a ramified prime ideal of } \mathcal{O}\} \cup \{[\mathfrak{a}\mathcal{O}] \in \mathrm{Cl}(\mathcal{O})\,;\, [\mathfrak{a}] \in \mathrm{Cl}(\mathfrak{o})\}\,.$$
- Further, let J and J_0 be the subgroups of the group $\mathcal{I}(\mathcal{O})$ of fractional ideals of $\mathcal{O}$ defined by
$$J = \{\mathfrak{A} \in \mathcal{I}(\mathcal{O})\,;\, \mathfrak{A}\overline{\mathfrak{A}} = \mathcal{O}\} \text{ and}$$
$$J_0 = \{\alpha\mathcal{O}\,;\, \alpha \in E^*,\ \alpha\overline{\alpha} = 1\} \trianglelefteq J\,.$$
- Given a prime ideal $\mathfrak{q}$ of $\mathfrak{o}$, set
$$\mathcal{E}_{\mathfrak{q},0} = \{\varepsilon \in \mathcal{O}_{\mathfrak{q}}^*\,;\, \varepsilon\overline{\varepsilon} = 1\}\,,$$
$$\mathcal{E}_{\mathfrak{q},1} = \{\overline{\varepsilon}\varepsilon^{-1}\,;\, \varepsilon \in \mathcal{O}_{\mathfrak{q}}^*\} \trianglelefteq \mathcal{E}_{\mathfrak{q},0}\,,$$
$$\mathcal{E}(L_{\mathfrak{q}}) = \{\det(\sigma)\,;\, \sigma \in \mathrm{Aut}(L_{\mathfrak{q}})\} \trianglelefteq \mathcal{E}_{\mathfrak{q},0}\,.$$

Remark 5.4.12 Let $\mathfrak{q}$ be a prime ideal of $\mathfrak{o}$ that is ramified in E.

1. The homomorphism $C \to J/J_0$, $[\mathfrak{A}] \mapsto \mathfrak{A}\overline{\mathfrak{A}}^{-1} \cdot J_0$ is well-defined and surjective with kernel C_0. In particular, $[C : C_0] = [J : J_0]$.
2. The homomorphism $E_{\mathfrak{q}}^* \to \mathcal{E}_{\mathfrak{q},0}/\mathcal{E}_{\mathfrak{q},1}$, $\alpha \mapsto \alpha\overline{\alpha}^{-1}\mathcal{E}_{\mathfrak{q},1}$ is surjective by Hilbert's Theorem 90 and has kernel $K_{\mathfrak{q}}^*\mathcal{O}_{\mathfrak{q}}^*$. In particular, $[\mathcal{E}_{\mathfrak{q},0} : \mathcal{E}_{\mathfrak{q},1}] = [E_{\mathfrak{q}}^* : K_{\mathfrak{q}}^*\mathcal{O}_{\mathfrak{q}}^*] = 2$.
3. The homomorphism $\varphi \colon E_{\mathfrak{q}}^* \to \mathcal{E}_{\mathfrak{q},0}/\mathcal{E}_{\mathfrak{q},0}^2$, $\alpha \mapsto \alpha\overline{\alpha}^{-1}$ is surjective by Hilbert's Theorem 90 and has kernel $K_{\mathfrak{q}}^*\mathcal{E}_{\mathfrak{q},0} = K_{\mathfrak{q}}^*(E_{\mathfrak{q}}^*)^2$. Therefore
$$\mathcal{E}_{\mathfrak{q},0}/\mathcal{E}_{\mathfrak{q},0}^2 \cong E_{\mathfrak{q}}^*/K_{\mathfrak{q}}^*\mathcal{E}_{\mathfrak{q},0} = E_{\mathfrak{q}}^*/K_{\mathfrak{q}}^*(E_{\mathfrak{q}}^*)^2 .$$
This isomorphism also gives a method of computing representatives of $\mathcal{E}_{\mathfrak{q},0}/\mathcal{E}_{\mathfrak{q},0}^2$ of the form $\lambda/\overline{\lambda}$ with $\lambda \in \mathcal{O}$.

Proof. The first two assertions are obvious. The last one can be seen as follows. The groups $K_{\mathfrak{q}}^*\mathcal{E}_{\mathfrak{q},0}$ and $K_{\mathfrak{q}}^*(E_{\mathfrak{q}}^*)^2$ are clearly contained in $\operatorname{Ker}(\varphi)$. Conversely, let $\alpha \in \operatorname{Ker}(\varphi)$. Thus $\alpha/\overline{\alpha} = \varepsilon^2$ with $\varepsilon \in \mathcal{E}_{\mathfrak{q},0}$. Hence $\alpha\overline{\varepsilon} = \overline{\alpha}\varepsilon \in K^*$ and $\alpha = (\alpha\overline{\varepsilon})\varepsilon \in K^*\mathcal{E}_{\mathfrak{q},0}$. Further, $\varepsilon = \varphi(\lambda)$ for some $\lambda \in E^*$. Hence $\alpha = (\alpha\overline{\varepsilon})\lambda/\overline{\lambda} = (\alpha\overline{\varepsilon}\lambda\overline{\lambda}) \cdot \overline{\lambda}^{-2} \in K^*(E^*)^2$. □

The exact value of $\mathcal{E}(L_{\mathfrak{q}})$ is known in almost all cases. The following result is due to G. Shimura. However, a simpler proof is given below.

Proposition 5.4.13 *Let $\mathfrak{Q}$ be a prime ideal of $\mathcal{O}$ and set $\mathfrak{q} := \mathfrak{Q} \cap \mathfrak{o}$.*

1. *If $\mathfrak{Q}$ is unramified or $L_{\mathfrak{q}}$ has a Jordan block of odd rank, then*
$$\mathcal{E}(L_{\mathfrak{q}}) = \mathcal{E}_{\mathfrak{q},0} .$$
2. *If $\mathfrak{Q}$ is ramified and $2 \notin \mathfrak{q}$ then*
$$\mathcal{E}(L_{\mathfrak{q}}) = \begin{cases} \mathcal{E}_{\mathfrak{q},0} & \text{if } L_{\mathfrak{q}} \text{ has a } \mathfrak{Q}^i\text{-modular Jordan block with } i \text{ even,} \\ \mathcal{E}_{\mathfrak{q},1} & \text{otherwise.} \end{cases}$$
3. *If $\mathfrak{Q}$ is ramified and $2 \in \mathfrak{q}$ then*
$$\mathcal{E}_{\mathfrak{q},0}^2 \subseteq \mathcal{E}(L_{\mathfrak{q}}) \subseteq \mathcal{E}_{\mathfrak{q},0} .$$
If the rank of some Jordan block of $L_{\mathfrak{q}}$ is different from 2, then $\mathcal{E}_{\mathfrak{q},1} \subseteq \mathcal{E}(L_{\mathfrak{q}})$.

Proof. By Algorithm 3.3.2, L splits into $L_1 \perp L_2$ with $\operatorname{rank}(L_1) \le 2$. If $\operatorname{rank}(L_1) = 1$, then $\mathcal{E}(L_{\mathfrak{q}}) = \mathcal{E}_{\mathfrak{q},0}$. If $\operatorname{rank}(L_2) = 2$, then $\mathcal{E}_{\mathfrak{q},0}^2 \subseteq \mathcal{E}(L_{\mathfrak{q}})$. Further, the hyperbolic planes $H(i)$ admit the isometries $\{\operatorname{Diag}(\overline{\varepsilon}, \varepsilon^{-1})\,;\, \varepsilon \in \mathcal{O}_{\mathfrak{p}}^*\}$. In view of Proposition 3.3.5 and Corollary 3.3.20, this only leaves the case that $\mathfrak{Q}$ is ramified, $2 \notin \mathfrak{q}$ and the scales of all Jordan blocks of $L_{\mathfrak{q}}$ have odd valuation. Under these assumptions, Proposition 3.3.5 shows that $(V_{\mathfrak{q}}, \Phi)$ is hyperbolic and has a skew-symmetric Gram matrix. But determinants of isometries of such spaces lie in $\mathcal{E}_{\mathfrak{q},1}$, see for example [Sch85, Theorem 7.6]. □

Theorem 5.4.14 *Let P be the set of all primes ideals $\mathfrak{q}$ of $\mathfrak{o}$ (ramified in E) such that $\mathcal{E}_{\mathfrak{q},0} \neq \mathcal{E}(L_\mathfrak{q})$. Set*

$$\begin{aligned} \mathcal{E}(L) &= \prod_{\mathfrak{q}\in P} \mathcal{E}_{\mathfrak{q},0}/\mathcal{E}(L_\mathfrak{q})\,, \\ R &= \{(\varepsilon\mathcal{E}(L_\mathfrak{q}))_{\mathfrak{q}\in P} \in \mathcal{E}(L)\,;\, \varepsilon \in \mathcal{O}^* \text{ such that } \varepsilon\overline{\varepsilon} = 1\}\,, \\ H &= \{(\varepsilon\mathcal{O},\, (\varepsilon\mathcal{E}(L_\mathfrak{q}))_{\mathfrak{q}\in P}) \in J \times \mathcal{E}(L)\,;\, \varepsilon \in E \text{ such that } \varepsilon\overline{\varepsilon} = 1\}\,. \end{aligned}$$

Consider the map

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

where $\sigma_\mathfrak{q} \in \mathbf{U}(V_\mathfrak{q},\Phi)$ such that $M_\mathfrak{q} = \sigma_\mathfrak{q}(L_\mathfrak{q})$ for all $\mathfrak{q} \in P$.

1. *The map Ψ induces a bijection between the special genera in* gen(L) *and*

$$(J \times \mathcal{E}(L))/H\,.$$

2. *Let $(\mathfrak{a}_1,\dots,\mathfrak{a}_r)$ and $(\gamma_1,\dots,\gamma_s)$ be systems of representatives of J/J_0 and $\mathcal{E}(L)/R$ respectively. Then $\{(\mathfrak{a}_i,\gamma_j)H\,;\, 1 \le i \le r,\ 1 \le j \le r\}$ is a system of representatives of $(J \times \mathcal{E}(L))/H$. Thus, the number of special genera in* gen(L) *is*

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

Proof. See [Shi64, Theorems 5.24 and 5.27]. □

The above theorem immediately gives an algorithm to compute representatives of the isometry classes in a given genus, see [Sch98].

Algorithm 5.4.15 GenusRepresentatives(L)
Input: An $\mathcal{O}$-lattice L in the definite hermitian space (V,Φ) over E.
Output: A system $\mathcal{S}$ of representatives of the isometry classes in gen(L).

```
Let $\mathcal{B}$ be the set of all prime ideals $\mathfrak{Q}$ of $\mathcal{O}$ such that $L_{\mathfrak{Q}\cap\mathfrak{o}}$ is not modular or $\mathfrak{Q}$ is a ramified prime ideal over 2.
Let $\mathfrak{P} \notin \mathcal{B}$ be a prime ideal of $\mathcal{O}$ of minimal norm.
Let $\mathcal{A} = \{\mathfrak{A}_1,\dots,\mathfrak{A}_r\}$ be a set of ideals of $\mathcal{O}$, not supported at $\mathcal{B}$, such that
    $$\{[\mathfrak{A}_i]C_0\,;\, 1 \le i \le r\} \cup \{[\mathfrak{P}]C_0\}$$
    generates $C/C_0$.
Let $P$ be the set of prime ideals $\mathfrak{q}$ of $\mathfrak{o}$ such that $\mathcal{E}(L_\mathfrak{q})$ is not (known to be) $\mathcal{E}_{\mathfrak{q},0}$.
Let $\Lambda$ be a generating set of $\mathcal{E}(L)/R$ where $R$ is as in Theorem 5.4.14.
for $\gamma R \in \Lambda$ do
    For $\mathfrak{q} \in P$ let $\beta_\mathfrak{q} \in \mathcal{O}$ with $\mathrm{ord}_\mathfrak{P}(\beta_\mathfrak{q}) \in \{0,1\}$ such that $\gamma_\mathfrak{q}\mathcal{E}_{\mathfrak{q},0}^2 = \beta_\mathfrak{q}/\overline{\beta_\mathfrak{q}}\mathcal{E}_{\mathfrak{q},0}^2$.
```

```
 8:     Compute some $\alpha \in E$ such that
            $\alpha\beta_{\mathfrak{q}} - 1 \in 4\mathfrak{q}\mathcal{O}_{\mathfrak{q}}$ for all $\mathfrak{q} \in P$
            $\alpha \in \mathcal{O}_{\mathfrak{Q}}^*$ for all split ideals $\mathfrak{Q} \in \mathcal{B}$
 9:     Include $\alpha\mathcal{O}$ to $\mathcal{A}$.
10: end for
11: Initialiase the list $\mathcal{S} = [S]$ where $S$ is the output of IteratedNeighbours($L$, $\mathfrak{P}$).
12: Initialise $i = 1$.
13: while $i \le \#\mathcal{S}$ do
14:     for $\mathfrak{A} \in \mathcal{A}$ do
15:         Compute a lattice $M \in \operatorname{gen}(L)$ such that $[L' : M]_{\mathcal{O}} = \mathfrak{A}\overline{\mathfrak{A}}^{-1}$ where $L' \in \mathcal{S}[i]$.
16:         if there exists no lattice in $\bigcup_{S \in \mathcal{S}} S$ isometric to $M$ then
17:             Append the output of IteratedNeighbours($M$, $\mathfrak{P}$) at the end of $\mathcal{S}$.
18:         end if
19:     end for
20:     Increment $i$.
21: end while
22: return $\bigcup_{S \in \mathcal{S}} S$.
```

Proof. Suppose the notation of Theorem 5.4.14 and let $\mathcal{L} = \bigcup_{S \in \mathcal{S}} S$. Corollary 5.2.8 shows that $\bigcup_{L \in \mathcal{L}} \operatorname{cls}(L)$ is a union of special genera and line 16 ensures that $\mathcal{L}$ represents no isometry class twice. In particular, since $h(L)$ is finite, the algorithm terminates. It remains to show that $\mathcal{L}$ represents every special genus in $\operatorname{gen}(L)$. For this, let $\mathfrak{q} \in P$ and write $\mathfrak{q}\mathcal{O} = \mathfrak{Q}^2$. The element α from line 8 satisfies that $\alpha\beta_q$ is a square in $\mathcal{O}_{\mathfrak{Q}}^*$. Thus $(\beta_{\mathfrak{q}}/\overline{\beta_{\mathfrak{q}}})(\alpha/\overline{\alpha}) \in \mathcal{E}_{\mathfrak{q},0}^2 \subseteq \mathcal{E}(L_{\mathfrak{q}})$. Hence $\alpha\gamma = 1 \in \mathcal{E}(L)$ and therefore $(\mathcal{O}, \gamma)H = (\alpha\mathcal{O}, 1)H$. Theorem 5.4.14 shows that $\{(\mathfrak{A}, 1)H\,;\, \mathfrak{A} \in \mathcal{A}\}$ generates $(J \times \mathcal{E}(L))/H$ and that $(J \times \mathcal{E}(L))/H$ acts transitively on the set of special genera in $\operatorname{gen}(L)$ via

$$(J \times \mathcal{E}(L))/H \times \operatorname{gen}(L) \to \operatorname{gen}(L),\ ((\mathfrak{A}, 1)H, \operatorname{sgen}(L')) \mapsto \operatorname{sgen}(M)$$

where $[L' : M]_{\mathcal{O}} = \mathfrak{A}\overline{\mathfrak{A}}^{-1}$. Thus the standard orbit enumeration in line 13 eventually reaches every special genus in $\operatorname{gen}(L)$. □

Remark 5.4.16 Here are some hints, how the individual steps of the previous algorithm can be performed in practise.

1. A (non-minimal) generating set Λ as in line 5 can be obtained from Remark 5.4.12 if one replaces $\mathcal{E}(L)/R$ by $\prod_{\mathfrak{q} \in P} \mathcal{E}_{\mathfrak{q},0}/\mathcal{E}_{\mathfrak{q},0}^2$. This does not change the validity of the algorithm.

2. The lattice M from line 15 can be obtained as follows. The choice of $\mathfrak{A}$ implies that $\mathfrak{A} = \mathfrak{P}_1, \ldots, \mathfrak{P}_t\mathfrak{B}$ with split prime ideals $\mathfrak{P}_i \notin \mathcal{B}$ and some fractional ideal $\mathfrak{B} \in C_0$. Consider the sequence

   $$L' = L_0, L_1, \ldots, L_t \quad \text{where } L_i \text{ is a } \mathfrak{P}_i\text{-neighbour of } L_{i-1}\,.$$

   Then $M := L_t$ satisfies $[L' : M]_{\mathcal{O}} = \mathfrak{A}\overline{\mathfrak{A}}^{-1}$.

6 Enumerating genera with small class number

The purpose of this chapter is to present an algorithm which classifies the definite hermitian lattices of rank m and class number at most B over any totally real number field. The algorithm proceeds in four steps.

1. Enumerate the possible totally real number fields K, the possible K-algebras E and the possible ranks m.
2. Enumerate the possible similarity classes of hermitian spaces of rank m over E.
3. Enumerate the genera of square-free lattices with class number at most B.
4. Enumerate the similarity classes of all genera with class number at most B.

Throughout this chapter, let K be a totally real number field of degree n and let (V, Φ) be a definite hermitian space over E of rank m. Further, let $\mathfrak{o}$ and $\mathcal{O}$ be maximal orders in K and E respectively.

Note that D. Lorch in [Lor] uses a slightly different approach for enumerating the one-class genera of definite quadratic lattices.

6.1 Square-free lattices

This section defines the so-called square-free lattices and shows that every integral lattice can be reduced to a square-free lattice by reduction operators that do not increase class numbers.

Definition 6.1.1 Let $\mathfrak{L}$ denote the set of all $\mathcal{O}$-lattices in (V, Φ) and let $L \in \mathcal{L}$. Let $\mathfrak{P}$ be a maximal twosided ideal of $\mathcal{O}$ and set $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{o}$. Further, let $\mathfrak{A}$ be an integral twosided ideal of $\mathcal{O}$ such that $\mathfrak{A} = \overline{\mathfrak{A}}$.

1. If $E_\mathfrak{p} \cong K_\mathfrak{p} \oplus K_\mathfrak{p}$, then $L_\mathfrak{p}$ is said to be *square-free*, if $L_\mathfrak{p}$ is unimodular. In all other cases, $L_\mathfrak{p}$ is called square-free, if
$$\mathfrak{P} L_\mathfrak{p}^\# \subseteq L_\mathfrak{p} \subseteq L_\mathfrak{p}^\# \,.$$
Moreover, $L_\mathfrak{p}$ is called $\mathfrak{A}_\mathfrak{p}$*-square-free*, if $L_\mathfrak{p}$ is square-free and $\mathfrak{A}_\mathfrak{p} \subseteq \mathfrak{s}(L_\mathfrak{p}) \subseteq \mathcal{O}_\mathfrak{p}$.
2. The lattice L is said to be *square-free* or $\mathfrak{A}$*-square-free*, if $L_\mathfrak{p}$ is square-free or $\mathfrak{A}_\mathfrak{p}$-square-free for all $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$.

3. Let $\rho_{\mathfrak{P}}$ be the map defined by

$$\rho_{\mathfrak{P}} \colon \mathfrak{L} \to \mathfrak{L},\ L \mapsto \begin{cases} L + (\mathfrak{P}^{-1}L \cap L^{\#}) & \text{if } E_{\mathfrak{p}} \cong K_{\mathfrak{p}} \oplus K_{\mathfrak{p}}, \\ L + (\mathfrak{P}^{-1}L \cap \mathfrak{P}L^{\#}) & \text{otherwise.} \end{cases}$$

Clearly, if a genus contains some $\mathfrak{A}$-square-free $\mathcal{O}$-lattice, then all lattices in the genus have that property. It is worthwhile to mention that square-free lattices are also called almost or nearly unimodular by some authors.

The maps $\rho_{\mathfrak{P}}$ generalize the maps defined by L. Gerstein in [Ger72] to hermitian spaces. They are similar in nature to the *p-mappings* introduced by G. Watson in [Wat62]. Below is a summary of some important properties of these maps $\rho_{\mathfrak{P}}$, which will be used later on.

Remark 6.1.2 Let L be an $\mathcal{O}$-lattice in (V, Φ). Let $\mathfrak{P}$ be a maximal twosided ideal of $\mathcal{O}$ and set $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{o}$.

1. If $\mathfrak{q} \in \mathbb{P}(\mathfrak{o}) - \{\mathfrak{p}\}$, then $(\rho_{\mathfrak{P}}(L))_{\mathfrak{q}} = L_{\mathfrak{q}}$.
2. Suppose $E_{\mathfrak{p}} \not\cong K_{\mathfrak{p}} \oplus K_{\mathfrak{p}}$ and let $L_{\mathfrak{p}} = \perp_{i\in\mathbb{Z}} L_i$ be a Jordan decomposition where $L_i = (0)$ or $\mathfrak{P}^i$-modular. Then
$$(\rho_{\mathfrak{P}}(L))_{\mathfrak{p}} = \mathop{\perp}_{i\in\mathbb{Z}} L_i' \quad \text{where} \quad L_i' = \begin{cases} L_i & \text{if } i \le 1, \\ \mathfrak{P}^{-1}L_i & \text{if } i > 1. \end{cases}$$
3. Suppose $E_{\mathfrak{p}} \cong K_{\mathfrak{p}} \oplus K_{\mathfrak{p}}$ and let $L_{\mathfrak{p}} = \perp_{i\in\mathbb{Z}} L_i$ be a Jordan decomposition where $L_i = (0)$ or $\mathfrak{p}^i\mathcal{O}$-modular. Then
$$(\rho_{\mathfrak{P}}(L))_{\mathfrak{p}} = \mathop{\perp}_{i\in\mathbb{Z}} L_i' \quad \text{where} \quad L_i' = \begin{cases} L_i & \text{if } i < 1, \\ \mathfrak{P}^{-1}L_i & \text{if } i \ge 1. \end{cases}$$
In particular, $\rho_{\mathfrak{P}}(L)$ and $\rho_{\overline{\mathfrak{P}}}(L)$ are in the same genus.
4. If $L_{\mathfrak{p}}$ is integral, then $(\rho_{\mathfrak{P}}(L))_{\mathfrak{p}} = L_{\mathfrak{p}} \iff L_{\mathfrak{p}}$ is square-free.
5. If $\mathfrak{Q}$ is a maximal twosided ideal of $\mathcal{O}$, then $\rho_{\mathfrak{P}} \circ \rho_{\mathfrak{Q}} = \rho_{\mathfrak{Q}} \circ \rho_{\mathfrak{P}}$.
6. If L is integral, there exist some maximal twosided ideals $\mathfrak{P}_1, \dots, \mathfrak{P}_s$ of $\mathcal{O}$ such that
$$L' := (\rho_{\mathfrak{P}_1} \circ \dots \circ \rho_{\mathfrak{P}_s})(L)$$
is square-free. Moreover, the genus of L' is uniquely determined by L.

Proof. The first five assertions are obvious and the last follows from the second and third by induction on the largest valuation of the scales of the non-zero Jordan blocks. □

Lemma 6.1.3 *Let L, M be $\mathcal{O}$-lattices in (V, Φ) and let $\mathfrak{P}$ be a maximal twosided ideal of $\mathcal{O}$.*

1. *If L and M are (locally) isometric, then so are $\rho_{\mathfrak{P}}(L)$ and $\rho_{\mathfrak{P}}(M)$. In particular, $\rho_{\mathfrak{P}}(\mathrm{gen}(L)) = \mathrm{gen}(\rho_{\mathfrak{P}}(L))$.*
2. *Suppose $\rho_{\mathfrak{P}}(M) = L$. Then $\mathrm{Aut}(M)$ is the stabilizer of M under $\mathrm{Aut}(L)$.*
3. *Suppose $\rho_{\mathfrak{P}}(M) = L$ and let $L_1, \dots, L_h$ represent the isometry classes in $\mathrm{gen}(L)$. The group $\mathrm{Aut}(L_i)$ acts on $\rho_{\mathfrak{P}}^{-1}(L_i) \cap \mathrm{gen}(M)$. Let $M_{i,1}, \dots, M_{i,h_i}$ represent the orbits of this action. Then*
$$\{M_{i,j}\,;\, 1 \le i \le h,\ 1 \le j \le h_i\}$$
represents the isometry classes of $\mathrm{gen}(M)$. In particular, $h(M) \ge h(L)$.
4. *If $\rho_{\mathfrak{P}}(M) = L$, then $\mathrm{Mass}(M) = |\rho_{\mathfrak{P}}^{-1}(L) \cap \mathrm{gen}(M)| \cdot \mathrm{Mass}(L) \ge \mathrm{Mass}(L)$.*

Proof. The lattice $\rho_{\mathfrak{P}}(L)$ is constructed from L by taking sums and intersections of (rescaled copies of) L and its dual. All these operations commute with (local) isometries. This shows the first and the second assertions. The third is an immediate consequence of the previous ones: Let $M' \in \mathrm{gen}(M)$. Then $\rho_{\mathfrak{p}}(M') \cong L_i$ for some i. Without loss of generality $\rho_{\mathfrak{p}}(M') = L_i$. Hence M' lies in some orbit under $\mathrm{Aut}(L_i)$, whence $M' \cong M_{i,j}$ for some j. So the claimed set represents each isometry class at least once. Suppose $M_{i,j}$ and $M_{r,s}$ are isometric, then so are L_i and L_r. This shows $i = r$. But any isometry from $M_{i,j}$ to $M_{i,s}$ induces an isometry on L_i. Hence $j = s$. So the claimed set represents each isometry class in $\mathrm{gen}(M)$ uniquely. The last assertion follows from Proposition 4.3.5. Alternatively it can also be deduced from the second and third parts. □

Definition 6.1.4 Let G be a genus of integral $\mathcal{O}$-lattices and let G' be a genus of square-free $\mathcal{O}$-lattices. The genus G can be *reduced to* G', if there exists some maximal twosided ideals $\mathfrak{P}_1, \dots, \mathfrak{P}_s$ of $\mathcal{O}$ and $L \in G$ such that
$$(\rho_{\mathfrak{P}_1} \circ \ldots \circ \rho_{\mathfrak{P}_s})(L) \in G'\ .$$
Lemma 6.1.3 shows that G' is uniquely determined by G.

Lemma 6.1.3 also shows that if (V, Φ) admits an $\mathcal{O}$-lattice with class number h, it must admit a square-free $\mathcal{O}$-lattice L with class number at most h. However, there are infinitely many genera of square-free lattices similar to $\mathrm{gen}(L)$ which necessarily all have the same class number. This is where the $\mathfrak{A}$-square-free lattices come into the game.

Remark 6.1.5 Let L be a square-free $\mathcal{O}$-lattice in (V, Φ). Let $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ be the prime ideals of $\mathfrak{o}$ that divide $\mathrm{d}_{E/K}$ and let $\mathfrak{p}_i\mathcal{O} = \mathfrak{P}_i^2$. Further, let $\mathfrak{a}$ be an integral ideal of $\mathfrak{o}$ such that $\{\mathfrak{b} \in \mathcal{I}(\mathfrak{o})\,;\, \mathfrak{a} \subseteq \mathfrak{b} \subseteq \mathfrak{o}\}$ represents the classes of the narrow class group $\mathrm{Cl}^+(\mathfrak{o})$. Then $\mathfrak{A} = \mathfrak{a}\mathcal{O} \cdot \prod_{i=1}^r \mathfrak{P}_i$ satisfies $\mathfrak{A} = \overline{\mathfrak{A}}$ and there exists some totally positive $a \in K^*$ such that L^a is $\mathfrak{A}$-square-free. Moreover, a is unique up to multiplication with elements from $\mathfrak{o}^*_{>0}$.

Proof. The construction of $\mathfrak{A}$ implies that $\mathfrak{A} = \overline{\mathfrak{A}}$. Let $\mathfrak{s}(L) = \mathfrak{c}\mathcal{O} \cdot \prod_{i=1}^r \mathfrak{P}^{e_i}$ with $e_i \in \{0, 1\}$ and some integral ideal $\mathfrak{c}$ of $\mathfrak{o}$. The choice of $\mathfrak{a}$ guarantees that there exists a totally positive $a \in K^*$, unique up to multiplication by totally positive units, such that $a^{-1}\mathfrak{c} \subseteq \mathfrak{o}$ is a divisor of $\mathfrak{a}$. □

6.2 Partial duals

The maps $\rho_{\mathfrak{P}}$ from the previous section act on the (genera of all) $\mathcal{O}$-lattices in (V, Φ) such that class numbers are not increased. This section describes similar maps which actually do preserve class numbers.

Definition 6.2.1 Let L be an $\mathcal{O}$-lattice in (V, Φ) and let $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$ be a prime ideal of $\mathfrak{o}$. The *partial dual* of L at $\mathfrak{p}$ is the unique $\mathcal{O}$-lattice $L^{\#,\mathfrak{p}}$ in (V, Φ) that satisfies

$$(L^{\#,\mathfrak{p}})_{\mathfrak{q}} = \begin{cases} L_{\mathfrak{q}} & \text{if } \mathfrak{q} \neq \mathfrak{p}, \\ L_{\mathfrak{p}}^{\#} & \text{if } \mathfrak{q} = \mathfrak{p} \end{cases}$$

for all $\mathfrak{q} \in \mathbb{P}(\mathfrak{o})$.

Remark 6.2.2 Let L, M be $\mathcal{O}$-lattices in (V, Φ) and let $\mathfrak{p}, \mathfrak{q} \in \mathbb{P}(\mathfrak{o})$.

1. The partial dual $L^{\#,\mathfrak{p}}$ can be computed explicitly as follows. From the Jordan decomposition of $L_{\mathfrak{p}}$ one obtains integers i and j such that $\mathfrak{p}^i L_{\mathfrak{p}} \subseteq L_{\mathfrak{p}}^{\#} \subseteq \mathfrak{p}^j L_{\mathfrak{p}}$. Then $L^{\#,\mathfrak{p}} = (\mathfrak{p}^i L + L^{\#}) \cap \mathfrak{p}^j L$.
2. $(L^{\#,\mathfrak{p}})^{\#,\mathfrak{q}} = (L^{\#,\mathfrak{q}})^{\#,\mathfrak{p}}$ and $(L^{\#,\mathfrak{p}})^{\#,\mathfrak{p}} = L$.
3. If L and M are (locally) isometric, then so are $L^{\#,\mathfrak{p}}$ and $M^{\#,\mathfrak{p}}$.
4. $\mathrm{Aut}(L) = \mathrm{Aut}(L^{\#,\mathfrak{p}})$ and $h(L) = h(L^{\#,\mathfrak{p}})$.

Proof. The claimed identity in the first part holds locally at every place of $\mathfrak{o}$. Hence it holds globally. The second assertion follows from the definition of partial duals. The lattice $L^{\#,\mathfrak{p}}$ is constructed from L by taking sums and intersections of rescaled copies of L. These constructions are preserved under isometries. This shows the third part, the inclusion $\mathrm{Aut}(L) \subseteq \mathrm{Aut}(L^{\#,\mathfrak{p}})$ as well as $h(L) \geq h(L^{\#,\mathfrak{p}})$. The fact that $(L^{\#,\mathfrak{p}})^{\#,\mathfrak{p}} = L$ now finishes the proof of the last assertion. □

Definition 6.2.3 Two hermitian $\mathcal{O}$-lattices L and M are said to be *equivalent*, if there exists some chain of $\mathcal{O}$-lattices $L = L_0, L_1, \ldots, L_r = M$ and some prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of $\mathfrak{o}$ such that L_i is similar to the partial dual $L_{i-1}^{\#,\mathfrak{p}_i}$ for all $1 \leq i \leq r$. Note that this induces an equivalence relation on the set of all hermitian $\mathcal{O}$-lattices, which preserves automorphism groups.
This equivalence relation induces an equivalence relation on the similarity classes of genera of $\mathcal{O}$-lattices, which preserves class numbers.

6.3 Enumerating the possible definite hermitian spaces

The purpose of this section is to enumerate all similarity classes of definite hermitian spaces over number fields that could possibly contain lattices of class number at most B for some fixed integer B.

Let K be a totally real number field of degree n and let (V, Φ) be a definite hermitian space of rank m over E.

6.3.1 The quadratic case

Suppose $E = K$ and $m \geq 3$. The local densities of square-free $\mathfrak{o}$-lattices at a prime ideal $\mathfrak{p}$ over 2 are not known in all cases. For a given $\mathfrak{o}$-lattice L, the local factor $\lambda(L_\mathfrak{p})$ can be computed explicitly using Proposition 4.3.5, see also Remark 6.3.3 below. But this does not help in enumerating the possible base fields. For that one needs a bound that only depends on $\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})$ and m. Such a bound was provided by H. Pfeuffer in his thesis [Pfe71a]:

Theorem 6.3.1 *Let $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$ be a prime ideal of norm q over 2 and let $e = \mathrm{ord}_\mathfrak{p}(2)$ its ramification index. Further let L be an $\mathfrak{o}$-lattice in (V, Φ) such that $L_\mathfrak{p}$ is square-free. If $m = \dim_K(V) \geq 3$, then*

$$\beta(L_\mathfrak{p}) \cdot q^{-\mathrm{ord}_\mathfrak{p}(\mathfrak{v}(L))(m+1)/2} \leq q^{em} \cdot \begin{cases} 3/2 & \text{if } m = 3 \text{ and } q = 2, \\ 9/8 & \text{if } m = 4 \text{ and } q = 2, \\ 1 & \text{otherwise.} \end{cases}$$

Proof. See Korollar 1a, Theorem 2 and Hilfssatz 8 of [Pfe71a]. □

Corollary 6.3.2 *Suppose (V, Φ) admits an $\mathfrak{o}$-lattice with class number at most 2. If $K = \mathbb{Q}$, then $m \leq 30$. If $K \neq \mathbb{Q}$, then $m \leq 14$ and the* root discriminant $\mathrm{d}_K^{1/n}$ *is bounded as follows:*

m	3	4	5	6	7	8	9	10	11	12	13	14
$\mathrm{d}_K^{1/n} <$	24.12	12.06	8.37	6.52	5.33	4.50	3.89	3.42	3.06	2.76	2.52	2.31

If $m \geq 4$, a complete list of the possible fields K is available from [Voi08]. For example, there are only 361 totally real fields K whose root discriminant is below 12.06. The largest one has degree 8.

Proof. Let γ_m be as in Theorem 4.2.3 and let L be a square-free $\mathfrak{o}$lattice in (V, Φ) with class number at most 2. Siegel's mass formula and Theorem 6.3.1 show that

$$\begin{aligned} 1 &\geq \mathrm{Mass}(L) \\ &\geq \gamma_m^{-n} \cdot \mathrm{d}_K^{m(m-1)/4} \cdot \mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{v}(L))^{(m+1)/2} \cdot \prod_{\mathfrak{p} \in \mathbb{P}(\mathfrak{o})} \beta(L_\mathfrak{p})^{-1} \cdot \begin{cases} 2^{nm} & \text{if } m \text{ is even,} \\ 2^{n(m+1)/2} & \text{if } m \text{ is odd} \end{cases} \\ &\geq \gamma_m^{-n} \cdot \mathrm{d}_K^{m(m-1)/4} \cdot \begin{cases} (8/9)^n & \text{if } m = 4, \\ 1 & \text{if } m \geq 6 \text{ is even,} \\ 2^{-n} \cdot (2/3)^n & \text{if } m = 3, \\ 2^{-n(m-1)/2} & \text{if } m \geq 5 \text{ is odd.} \end{cases} \end{aligned}$$

In particular, the root discriminant $\mathrm{d}_K^{1/n}$ satisfies

$$\mathrm{d}_K^{1/n} \le \gamma_m^{4/m(m-1)} \cdot \begin{cases} (9/8)^{1/3} & \text{if } m = 4, \\ 1 & \text{if } m \ge 6 \text{ is even}, \\ 3^{2/3} & \text{if } m = 3, \\ 2^{2/m} & \text{if } m \ge 5 \text{ is odd}. \end{cases}$$

The right hand side of the above inequality is less that 1 for $m > 30$ and less than $\sqrt{5}$ for $m \ge 15$. It also yields the claimed bounds on $\mathrm{d}_K^{1/n}$. □

The enumeration of all totally real number fields with root discriminants at most 24.12 is out of reach with current methods and computers. Thus, for the ternary quadratic lattices, different methods are needed which will yield better bounds on $\mathrm{d}_K^{1/n}$. This case will be discussed in detail in Section 7.3.

Remark 6.3.3 Let $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$ be a prime ideal over 2 and let L be an $\mathfrak{o}$-lattice in (V, Φ). If $\mathfrak{p}$ is unramified, the local factor $\lambda(L_\mathfrak{p})$ is given by results of S. Cho, see [Cho15]. In general, one can compute $\lambda(L_\mathfrak{p})$ as follows:

1. Compute a chain of minimal $\mathfrak{o}_\mathfrak{p}$-overlattices $L_\mathfrak{p} = L_0 \subsetneq L_1 \subsetneq \ldots \subsetneq L_r$ where L_r is $\mathfrak{n}(L_\mathfrak{p})$-maximal, c.f. Algorithm 3.5.4.
2. Look up $\lambda(L_r)$ from Theorem 4.4.1.
3. Compute $\lambda(L_\mathfrak{p})$ by a successive comparison of $\lambda(L_i)$ with $\lambda(L_{i-1})$ for $i = r, \ldots, 1$ using Proposition 4.3.5.

Note that one can speed up this method considerably as follows. As explained in Section 3.4, construct a definite hermitian space (V', Φ') such that $(V_\mathfrak{p}, \Phi) \cong (V'_\mathfrak{p}, \Phi')$. Using Algorithm 3.5.4, construct an $\mathfrak{o}$-lattice L'_r in (V', Φ) such that $(L'_r)_\mathfrak{p}$ is $\mathfrak{n}(L_\mathfrak{p})$-maximal. Then $(L'_r)_\mathfrak{p} \cong L_r$ and thus $\lambda(L_r) = \lambda((L'_r)_\mathfrak{p})$. The maximal $\mathfrak{o}$-sublattices between L'_r and $\mathfrak{p}L'_r$ correspond to the projective lines of the $\mathfrak{o}/\mathfrak{p}$-space $L'_r/\mathfrak{p}L'_r$. The finite group $\mathrm{Aut}(L'_r)$ acts on these sublattices and hence on the projective lines. From orbit representatives and the orbit lengths, one obtains a sublattice L'_{r-1} of L'_r such that $(L'_{r-1})_\mathfrak{p} \cong L_{r-1}$ as well as the cardinality $\#D((L'_r)_\mathfrak{p}, (L'_{r-1})_\mathfrak{p})$. Similarly, one can then use the finite group $\mathrm{Aut}(L'_{r-1})$ to speed up the enumeration of $\#U((L'_r)_\mathfrak{p}, (L'_{r-1})_\mathfrak{p})$. This immediately gives $\lambda((L'_{r-1})_\mathfrak{p}) = \lambda(L_{r-1})$. Iterating this procedure finally yields $\lambda(L_\mathfrak{p})$.

Algorithm 6.3.4

Input: An integral ideal $\mathfrak{a}$ of $\mathfrak{o}$ and some integers $m \ge 3$ and $B \ge 1$.

Output: A set $\mathcal{L}$ of quadratic spaces over K such that every genus of $\mathfrak{a}$-square-free $\mathfrak{o}$-lattices of rank m and class number at most B is represented by some lattice in exactly one of the spaces in $\mathcal{L}$.

```
Set $M_0 = \gamma_m^{-n} \cdot \mathrm{d}_K^{m(m-1)/4}$ where $\gamma_m$ is given by Theorem 4.2.3.
Let $P_2 := \{\mathfrak{p} \in \mathbb{P}(\mathfrak{o}) \,;\, \mathfrak{p} \mid 2\}$.
```

```
3: Enumerate the finite set $D := \{S \subset \mathbb{P}(\mathfrak{o})\,;\, M_0 \cdot \prod_{\mathfrak{p}\in S\cup P_2} \lambda'_\mathfrak{p} \le B/2\}$ where
   $$\lambda'_\mathfrak{p} = \begin{cases} \min\{\lambda(L)\,;\, L \text{ is a square-free } \mathfrak{o}_\mathfrak{p}\text{-lattice of rank } m\} & \text{if } \mathfrak{p} \mid 2 \\ 1 & \text{if } \mathfrak{p} \mid \mathfrak{a} \text{ and } \mathfrak{p} \nmid 2, \\ \frac{\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})^{m-1}-1}{2(\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})+1)} & \text{if } \mathfrak{p} \nmid 2\mathfrak{a} \text{ and } m \text{ is odd,} \\ \frac{1}{2}\cdot \mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})^{(m-1)/2} & \text{if } \mathfrak{p} \nmid 2\mathfrak{a} \text{ and } m \text{ is even.} \end{cases}$$
4: Initialiase $\mathcal{L} = \emptyset$.
5: Let $(u_1, \dots, u_s)$ be a transversal of $(\mathfrak{o}^*)^2$ in $\mathfrak{o}^*_{>0}$.
6: for $S \in D$ and $[\mathfrak{b}] \in \mathrm{Cl}(\mathfrak{o})$ do
7:     Let $g$ be a totally positive generator of $\mathfrak{b}^2 \cdot \prod_{\mathfrak{p}\in S} \mathfrak{p}$. If none exists, go to step 6.
8:     for $1 \le i \le s$ do
9:         Set $M_1 := 2^{-n\lfloor \frac{m}{2} \rfloor} \cdot \begin{cases} \prod_{j=1}^{\frac{m-1}{2}} |\zeta_K(1-2j)| & \text{if } m \text{ is odd,} \\ \prod_{j=1}^{\frac{m}{2}-1} |\zeta_K(1-2j)| \cdot |\mathfrak{L}_K(\chi_{(-1)^{m/2}u_i g}, \frac{2-m}{2})| & \text{if } m \text{ is even.} \end{cases}$
10:        Set $D' := \{C \subset \mathbb{P}(\mathfrak{o})\,;\, \#C \text{ is even and } M_1 \cdot \prod_{\mathfrak{p}\in S\cup C\cup P_2} \lambda''_\mathfrak{p} \le B/2\}$ where
           $$\lambda''_\mathfrak{p} = \begin{cases} \frac{1}{2} & \text{if } m \text{ is even, } \mathfrak{p} \nmid 2\mathfrak{a} \text{ and } \mathfrak{p} \in S \\ \frac{(\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})^{m/2}-1)(\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})^{m/2-1}-1)}{2(\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})+1)} & \text{if } m \text{ is even, } \mathfrak{p} \nmid 2\mathfrak{a} \text{ and } \mathfrak{p} \notin S, \\ \lambda'_\mathfrak{p} & \text{otherwise.} \end{cases}$$
11:        for $C \in D'$ do
12:            Let $(V, \Phi) :=$ QuadraticFormFromInvariants$(m, u_i g, C, (0, \dots, 0))$.
13:            Include $(V, \Phi)$ to $\mathcal{L}$.
14:        end for
15:    end for
16: end for
17: return $\mathcal{L}$.
```

Proof. First note that for any rational number c, the set $\{\mathfrak{p} \in \mathbb{P}(\mathfrak{o})\,;\, \lambda'_\mathfrak{p} \le c\}$ is finite. Thus the set D is finite. Similarly one sees that D' is always finite. Hence the algorithm terminates. Let L be an $\mathfrak{a}$-square-free lattice of rank $m \ge 3$ and $h(L) \le B$. Let (V, Φ) be its ambient quadratic space and set $S := \{\mathfrak{p} \in \mathbb{P}(\mathfrak{o})\,;\, \mathrm{ord}_\mathfrak{p}(\det(V, \Phi)) \text{ is odd}\}$. It remains to show that $\mathcal{L}$ contains a unique space isometric to (V, Φ). If m is even, let $F := K(\sqrt{\mathrm{disc}(V, \Phi)})$. By construction, $\lambda(L_\mathfrak{p}) \ge \lambda'_\mathfrak{p}$ for all $\mathfrak{p} \mid 2$. Lemma 4.2.9 shows that $\lambda(L_\mathfrak{p}) \ge 1$ for all $\mathfrak{p} \nmid 2$. Let $\mathfrak{p} \in S$ be a prime ideal of norm q such that $\mathfrak{p} \nmid 2\mathfrak{a}$. Again, Lemma 4.2.9 shows that

$$q^{\mathrm{ord}_\mathfrak{p}(\mathfrak{d}_{F/K})(m-1)/2} \cdot \lambda(L_\mathfrak{p}) \ge \frac{1}{2} q^{(m-1)/2}$$

whenever m is even. Similarly, if m is odd, then

$$\lambda(L_\mathfrak{p}) \ge \frac{1}{2}(q^{m_0/2} - 1)\binom{(m-1)/2}{m_0/2}_{q^2} \ge \frac{q^{m-1}-1}{2(q+1)}$$

where m_0 denotes the rank of a unimodular Jordan component of $L_\mathfrak{p}$. Hence Siegel's mass formula shows that

$$B/2 \geq \operatorname{Mass}(L) \geq M_0 \cdot \prod_{\mathfrak{p} \in S \cup P_2} \lambda'_\mathfrak{p}$$

and therefore $S \in D$. In particular, there exists some fractional ideal $\mathfrak{b}$ of K such that $\det(V, \Phi)\mathfrak{o} = \mathfrak{b}^2 \cdot \prod_{\mathfrak{p} \in S} \mathfrak{p}$ has a totally positive generator and $\mathfrak{b}^2$ is unique up to multiplication by elements in $(K^*)^2$. Whence the class $\det(V, \Phi)(K^*)^2$ is eventually represented by some unique product $u_i g$.
Let $C := \{\mathfrak{p} \in \mathbb{P}(\mathfrak{o})\,;\, \mathrm{c}(V_\mathfrak{p}, \Phi) = -1\}$. A case by case discussion using Lemma 4.2.9 shows that $\lambda(L_\mathfrak{p}) \geq \lambda''_\mathfrak{p}$ for all $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$. Again by Siegel's mass formula, shows that

$$B/2 \geq \operatorname{Mass}(L) \geq M_1 \cdot \prod_{\mathfrak{p} \in S \cup C \cup P_2} \lambda''_\mathfrak{p}\,.$$

Thus $C \in D'$ and the algorithm therefore constructs a space isometric to (V, Φ) in line 12 at some point. The fact that the spaces in $\mathcal{L}$ are pairwise non-isometric follows from the Local-Global Principle. □

Remark 6.3.5 Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{o}$ over 2. Then $\lambda'_\mathfrak{p}$ in Algorithm 6.3.4 can be computed from Remark 6.3.3 and the description of all square-free $\mathfrak{o}_\mathfrak{p}$-lattices, c.f. Proposition 3.3.11.

6.3.2 The hermitian case

Suppose E/K is a CM-extension of number fields and $m \geq 2$. From Lemma 4.2.9 and Theorems 4.5.2 and 4.5.2 it follows that $\lambda(L_\mathfrak{p}) \in \frac{1}{2}\mathbb{Z}$ and $\lambda(L_\mathfrak{p}) = \frac{1}{2}$ is only possible if $\mathfrak{p}$ is ramified in E and m is odd. This result combined with Siegel's mass formula immediately yields the following bounds.

Proposition 6.3.6 *Let L be an $\mathcal{O}$-lattice in (V, Φ) and let γ_m be as in Theorem 4.2.3.*

1. *The root discriminant $\mathrm{d}_K^{1/n}$ of K is bounded by*

$$\mathrm{d}_K^{1/n} < \left(h(L)^{1/n} \frac{\gamma_m}{2\pi}\right)^{2/(m^2-1)}\,.$$

2. *If $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$ is ramified in E, then*

$$h(L) \geq \left(\frac{2\pi}{\gamma_m}\right)^n \cdot \mathrm{d}_K^{(m^2-1)/2} \cdot \mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})^{m(m-(-1)^m)/4-1/2} \cdot \begin{cases} 1 & \text{if } m \text{ is even,} \\ 1/2 & \text{if } m \text{ is odd}\,. \end{cases}$$

3. *If $K = \mathbb{Q}$, then $h(L) > \frac{\pi}{\gamma_m} 3^{m(m-(-1)^m)/4-1/2}$.*

Proof. Let χ be the non-trivial character of $\mathrm{Gal}(E/K)$ and let $Q = [\mathcal{O}^* : \mathfrak{o}^*\mu(E)]$ be the Hasse unit index of E/K. Siegel's mass formula 4.2.7 shows that

$$\frac{h(L)}{\#\mu(E)} \ge \mathrm{Mass}(L) = 2\gamma_m^{-n}\, \mathrm{d}_K^{m^2/2}\, \mathrm{Nr}_{K/\mathbb{Q}}(\mathrm{d}_{E/K})^{m(m-(-1)^m)/4} \prod_{i=1}^{m} \mathfrak{L}_K(\chi^i, i) \prod_{\mathfrak{p}} \lambda(L_\mathfrak{p})\,.$$

If $t \ge 1$, then $\mathfrak{L}_K(\chi^{2t}, 2t) \cdot \mathfrak{L}_K(\chi^{2t+1}, 2t+1) = \zeta_K(2t)\frac{\zeta_E(2t+1)}{\zeta_K(2t+1)} > \zeta_E(2t+1) > 1$. Thus

$$\begin{aligned} h(L) &> 2\gamma_m^{-n} \cdot \#\mu(E) \cdot \mathfrak{L}_K(\chi, 1) \cdot \mathrm{d}_K^{m^2/2} \cdot \mathrm{Nr}_{K/\mathbb{Q}}(\mathrm{d}_{E/K})^{m(m-(-1)^m)/4} \cdot \prod_{\mathfrak{p}} \lambda(L_\mathfrak{p}) \\ &= \left(\frac{2\pi}{\gamma_m}\right)^n \underbrace{\frac{2 \cdot \#\,\mathrm{Cl}(E)}{Q \cdot \#\,\mathrm{Cl}(K)}}_{\ge 1} \cdot \mathrm{d}_K^{(m^2-1)/2} \cdot \mathrm{Nr}_{K/\mathbb{Q}}(\mathrm{d}_{E/K})^{m(m-(-1)^m)/4-1/2} \cdot \prod_{\mathfrak{p}} \lambda(L_\mathfrak{p}) \\ &\ge \left(\frac{2\pi}{\gamma_m}\right)^n \cdot \mathrm{d}_K^{(m^2-1)/2} \cdot \underbrace{\mathrm{Nr}_{K/\mathbb{Q}}(\mathrm{d}_{E/K})^{m(m-(-1)^m)/4-1/2} \cdot \prod_{\mathfrak{p}} \lambda(L_\mathfrak{p})}_{\ge 1}\,. \end{aligned}$$

This shows the first two assertions. The last assertion follows from the fact that if $K = \mathbb{Q}$, then $\mathrm{d}_E \ge 3$. □

Corollary 6.3.7 *Suppose that $m \ge 3$ and (V, Φ) admits an $\mathcal{O}$-lattice of class number at most 2. If $K = \mathbb{Q}$, then $m \le 16$. If $K \ne \mathbb{Q}$, then $m \le 12$ and the root discriminant $\mathrm{d}_K^{1/n}$ is bounded as indicated below.*

m	3	4	5	6	7	8	9	10	11	12
$\mathrm{d}_K^{1/n} <$	9.13	6.83	5.49	4.59	3.95	3.47	3.09	2.79	2.54	2.33

A complete list of these fields K is given in [Voi08].

Proof. If $K = \mathbb{Q}$, the previous result shows that $\frac{\pi}{\gamma_m} 3^{m(m-(-1)^m)/4-1/2} < 2$ which only holds for $m \le 16$. If $K \ne \mathbb{Q}$, then loc. cit. implies that

$$\sqrt{5} \le \mathrm{d}_K^{1/n} < \left(2^{1/2}\frac{\gamma_m}{2\pi}\right)^{2/(m^2-1)}\,.$$

This is only satisfied for $m \le 12$ and the above table lists the values of the right hand side for $3 \le m \le 12$. □

Remark 6.3.8 Suppose that $m \ge 3$ and (V, Φ) admits an $\mathcal{O}$-lattice of class number $\le B$. For any fixed field K, Proposition 6.3.6/2 effectively bounds the possible candidates for the relative discriminant $\mathrm{d}_{E/K}$. The set of all quadratic extensions E/K with given relative discriminant $\mathrm{d}_{E/K}$ can then be obtained from (`Magma`'s interface to) Class Field Theory.

So for $m \geq 3$ and $B \leq 2$, one can easily write down all CM-extensions E/K which might yield a hermitian $\mathcal{O}$-lattice of class number at most B. It remains to be discussed, which ambient hermitian spaces (V, Φ) over E might occur. This is achieved by the following algorithm.

Algorithm 6.3.9

Input: Some integral ideal $\mathfrak{A}$ of $\mathcal{O}$ such that $\mathfrak{A} = \overline{\mathfrak{A}}$ and integers $m \geq 2$, $B \geq 1$.

Output: A set $\mathcal{L}$ of hermitian spaces of dimension m over E such that every genus of $\mathfrak{A}$-square-free $\mathcal{O}$-lattices of rank and class number at most B is represented by some $\mathcal{O}$-lattice in exactly one of the spaces in $\mathcal{L}$.

```
Let $M_0 = 2^{1-nm} \cdot \prod_{j=1}^{m} |\mathfrak{L}_K(\chi^j, 1-j)|$ where $\chi$ is the non-trivial character of $\mathrm{Gal}(E/K)$.
Enumerate the finite set
    $$D = \{C \subset \mathbb{P}(\mathfrak{o}) \,;\, E_\mathfrak{p} \ncong K_\mathfrak{p} \oplus K_\mathfrak{p} \text{ for all } \mathfrak{p} \in C \text{ and } M_0 \cdot \prod_{\mathfrak{p} \in C \cup P} \lambda'_\mathfrak{p} \leq B/\#\mu(E)\}$$
where $P = \{\mathfrak{p} \in \mathbb{P}(\mathfrak{o}) \,;\, \mathfrak{p} \mid \mathrm{d}_{E/K}\}$ and
    $$\lambda'_\mathfrak{p} = \begin{cases} \frac{1}{2} & \text{if } m \text{ is odd and } \mathfrak{p} \text{ is ramified in } E, \\ \frac{1}{2}\,\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})^{m-1} & \text{if } \mathfrak{p} \text{ is inert in } E \text{ and } \mathfrak{p}\mathcal{O} \nmid \mathfrak{A}, \\ 1 & \text{otherwise.} \end{cases}$$
Initialiase $\mathcal{L} = \emptyset$.
for $C \in D$ such that $\#C$ is even do
    As explained in Remark 3.4.2, construct some definite, $m$-dimensional hermitian space $(V, \Phi)$ over $E$ such that
        $$\{\mathfrak{p} \in \mathbb{P}(\mathfrak{o}) \,;\, \det(V_\mathfrak{p}, \Phi) \notin \mathrm{N}(E_\mathfrak{p}^*)\} = C\,.$$
    Include $(V, \Phi)$ to $\mathcal{L}$.
end for
return $\mathcal{L}$.
```

Proof. First note that for every rational number c, the set

$$\{\mathfrak{p} \in \mathbb{P}(\mathfrak{o}) \,;\, E_\mathfrak{p} \ncong K_\mathfrak{p} \oplus K_\mathfrak{p} \text{ for all } \mathfrak{p} \in C \text{ and } \lambda'_\mathfrak{p} \leq c\}$$

is finite. Thus the set D is finite and so the algorithm terminates. Suppose L is a $\mathfrak{A}$-square-free $\mathcal{O}$-lattice of rank m and class number at most B. Let (V, Φ) be its ambient hermitian space and set $C = \{\mathfrak{p} \in \mathbb{P}(\mathfrak{o}) \,;\, \det(V_\mathfrak{p}, \Phi) \notin \mathrm{N}(E_\mathfrak{p}^*)\}$. It remains to show that (V, Φ) is isometric to some unique space in $\mathcal{L}$. First, $\#C$ is even by the product formula for Hilbert symbols. If m is odd and $\mathfrak{p}$ ramifies in E, then $\lambda(L_\mathfrak{p}) \geq 1/2$. In all other cases, $\lambda(L_\mathfrak{p}) \geq 1$. Suppose now $\mathfrak{p} \in C$ is not unramified in E. Then $\mathfrak{p}$ is inert in E. Let q be the norm of $\mathfrak{p}$. If $\mathfrak{p}\mathcal{O}$ is coprime to $\mathfrak{A}$, then $\lambda(L_\mathfrak{p}) \geq \left|\binom{m}{1}_{-q}\right| \geq q^{m-1}/2$ by Lemma 4.2.9. So Siegel's mass formula shows that

$$B/\#\mu(E) \geq \operatorname{Mass}(L) \geq M_0 \cdot \prod_{\mathfrak{p}\in C\cup P} \lambda_\mathfrak{p} \,.$$

Hence $C \in D$ and thus (V,Φ) is isometric to a unique space in $\mathcal{L}$ by the Local-Global Principle 2.4.1. □

6.3.3 The quaternionic hermitian case

Let E be a definite quaternion algebra over some totally real number field K. Further, let (V,Φ) be a definite hermitian space of rank m over E.

Proposition 6.3.10 *Let L be an $\mathcal{O}$-lattice in (V,Φ) and let γ_m be as in Theorem 4.2.3. Then*

$$\mathrm{d}_K^{1/n} \leq \left((h(L)/2)^{1/n} \cdot \gamma_m \cdot \prod_{\mathfrak{p}|\mathrm{d}_{E/K}} \prod_{j=1}^{m} (\operatorname{Nr}_{K/\mathbb{Q}}(\mathfrak{p})^j + (-1)^j)^{-1/n} \right)^{\frac{2}{m(2m+1)}} \,.$$

Proof. Without loss of generality, L is square-free. Proposition 4.2.7 shows that

$$\begin{aligned} h(L)/2 \geq \operatorname{Mass}(L) &\geq \gamma_m^{-n}\, \mathrm{d}_K^{m(m+1/2)} \prod_{\mathfrak{p}|\mathrm{d}_{E/K}} \lambda(L_\mathfrak{p}) \\ &\geq \gamma_m^{-n}\, \mathrm{d}_K^{m(m+1/2)} \prod_{\mathfrak{p}|\mathrm{d}_{E/K}} \prod_{j=1}^{m} (\operatorname{Nr}_{K/\mathbb{Q}}(\mathfrak{p})^j + (-1)^j) \,. \end{aligned} \tag{6.3.1}$$

□

Corollary 6.3.11 *Suppose (V,Φ) admits an $\mathcal{O}$-lattice of class number 1 or 2 and let γ_m be as Theorem 4.2.3. Then $m \leq 9$ and the following holds:*

1. *If $m = 1$, then $\mathrm{d}_K^{1/n} \leq 11.60$. For a complete list of these fields, see [Voi08].*
2. *If $m = 2$, then $\mathrm{d}_K^{1/n} \leq 6.34$.*
3. *If $m = 3$, then $K = \mathbb{Q}$ or $K = \mathbb{Q}(\sqrt{d})$ where $d \in \{2,3,5,13,17\}$.*
4. *If $m = 4$, then $K = \mathbb{Q}$ or $K = \mathbb{Q}(\sqrt{d})$ where $d \in \{2,5\}$.*
5. *If $m \in \{5,6\}$, then $K = \mathbb{Q}$ or $K = \mathbb{Q}(\sqrt{5})$.*
6. *If $m \in \{7,8,9\}$, then $K = \mathbb{Q}$.*
7. *The algebra E satisfies*

$$\prod_{\mathfrak{p}|\mathrm{d}_{E/K}} \prod_{j=1}^{m} (\operatorname{Nr}_{K/\mathbb{Q}}(\mathfrak{p})^j + (-1)^j) \leq \gamma_m^n \cdot \mathrm{d}_K^{-m(m+1/2)} \,.$$

Proof. The last assertion is simply equation (6.3.1). If $K = \mathbb{Q}$, then E/K is ramified and thus $1 \geq \gamma_m^{-1} \prod_{j=1}^m (2^j + (-1)^j)$. This inequality only holds for $m \leq 9$. Suppose now $K \neq \mathbb{Q}$. By Proposition 6.3.10, shows that $\sqrt{5} \leq \mathrm{d}_K^{1/n} \leq \gamma_m^{\frac{2}{m(2m+1)}}$. This only holds for $m \leq 6$. The right hand side is maximal for $m = 1$, in which case it yields the upper bound $\mathrm{d}_K^{1/n} \leq 11.60$. In particular, K is contained in the list [Voi08]. The result now follows by enumerating all fields K for which

$$1 \geq \mathrm{Mass}(L) \geq \gamma_m^{-n} \cdot \mathrm{d}_K^{m(m+1/2)} \cdot \begin{cases} 1 & \text{if } n \text{ is even,} \\ \prod_{j=1}^m (q^j + (-1)^j) & \text{if } n \text{ is odd,} \end{cases}$$

where q denotes the norm of the smallest prime ideal of ring of integers of K. □

Remark 6.3.12 Suppose (V, Φ) contains an $\mathcal{O}$-ideal with class number at most 2. Conditions 1.–6. of Corollary 6.3.11 and [Voi08] provide a finite list of candidates for (K, m). For any such pair, the last condition of Corollary 6.3.11 is only satisfied by finitely discriminants $\mathrm{d}_{E/K}$. The corresponding quaternion algebras E can be constructed explicitly as explained in Remark 3.4.2. Since there is only one isometry class of definite hermitian spaces of rank m over E, one immediately obtains a finite list of candidates (V, Φ) that can possibly admit genera of class number one or two.

6.4 Enumerating the square-free genera with bounded class number

The previous section showed how to compute all definite hermitian spaces (V, Φ) that can possibly admit square-free lattices with a certain class number, provided the rank of the space is sufficiently large. Next is an algorithm to enumerate representatives of the genera of these square-free lattices in (V, Φ) explicitly.

Algorithm 6.4.1 AllASquarefreeLattices$((V, \Phi), B, \mathfrak{A})$

Input: Some definite hermitian space (V, Φ) over E of rank $m \geq 2$ and $\dim_K(V) \geq 3$. Some positive integer B and some integral ideal $\mathfrak{A}$ of $\mathcal{O}$ such that $\mathfrak{A} = \overline{\mathfrak{A}}$.

Output: A set $\mathcal{S}$ representing the genera of all $\mathfrak{A}$-square-free $\mathcal{O}$-lattices in (V, Φ) with class number at most B.

```
if $E = K$ then
    Set $c_0 := \prod_{\mathfrak{p} | 2} \min\{\lambda(L) ; L$ a $\mathfrak{A}_\mathfrak{p}$-square-free $\mathcal{O}_\mathfrak{p}$-lattice in $(V_\mathfrak{p}, \Phi)\}$.
    if $m$ is odd then
        Set $c := 2^{-n(m-1)/2} \cdot \prod_{i=1}^{(m-1)/2} |\zeta_K(1-2i)| \cdot c_0$.
        Set $P_0 := \{\mathfrak{p} \in \mathbb{P}(\mathfrak{o}) ; \mathfrak{p} \mid 2$ or $\frac{\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})^{m-1}-1}{\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})+1} \leq B\}$.
    else
        Set $d := \mathrm{disc}(V, \Phi)$ and $r := \{\mathfrak{p} \in \mathbb{P}(\mathfrak{o}) ; \mathrm{ord}_\mathfrak{p}(d) \notin 2\mathbb{Z}$ and $\mathfrak{p} \nmid 2\}$.
        Set $c := 2^{-nm/2-r} \cdot \prod_{i=1}^{m/2-1} |\zeta_K(1-2i)| \cdot |\mathfrak{L}_K(\chi_d, 1-m/2)| \cdot c_0$.
        Set $P_0 := \{\mathfrak{p} \in \mathbb{P}(\mathfrak{o}) ; \mathfrak{p} \mid 2$ or $\frac{(\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})^{m-1}-1)(\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})^{m/2}-1)}{\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})+1} \leq B\}$.
```

```
10:     end if
11: else if $E/K$ is a quadratic field extension then
12:     Set $P_0 := \{\mathfrak{p} \in \mathbb{P}(\mathfrak{o})\,;\, \mathfrak{p}$ ramifies in $E\}$.
13:     Set $c := 2^{-nm} \cdot \prod_{i=1}^{m} |\mathfrak{L}_K(\chi^i, 1-i)|$ where $\chi$ is the non-trivial character of
    Gal$(E/K)$.
14:     if $m$ is odd then replace $c$ by $c/2^{\#P_0}$ end if
15:     Set $P_0 := P_0 \cup \{\mathfrak{p} \in \mathbb{P}(\mathfrak{o})\,;\, \mathfrak{p}$ is inert in $E$ and $\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})^{m-1} \le \frac{2B}{c\cdot\#\mu(E)}\}$.
16: else
17:     Set $c := 2^{-nm} \cdot \prod_{i=1}^{m} |\zeta_K(1-2i)|$.
18:     Set $P_0 := \{\mathfrak{p} \in \mathbb{P}(\mathfrak{o})\,;\, E_\mathfrak{p}$ is ramified or $\frac{\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})^{2m}-1}{\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})^{2}-1} \le \frac{B}{2c}\}$.
19: end if
20: Let $\{\mathfrak{p}_1, \dots, \mathfrak{p}_s\} = P_0 \cup \{\mathfrak{p} \in \mathbb{P}(\mathfrak{o})\,;\, M_\mathfrak{p}$ is not unimodular or $\mathfrak{A}_\mathfrak{p} \neq \mathcal{O}_\mathfrak{p}\}$.
21: Compute some $\mathfrak{o}$-maximal $\mathcal{O}$-lattice $M$ in $(V, \Phi)$ using Algorithm 3.5.5.
22: For $1 \le i \le s$ let $S_i$ be be a set of $\mathcal{O}$-sublattices of $M$ such that:
      • $\{L_\mathfrak{p}\,;\, L \in S_i\}$ represents the isometry classes of $\mathfrak{A}_\mathfrak{p}$-square-free $\mathcal{O}_{\mathfrak{p}_i}$-lattices in
        $(V_{\mathfrak{p}_i}, \Phi)$.
      • $L_\mathfrak{q} = M_\mathfrak{q}$ for all $L \in S$ and $\mathfrak{q} \in \mathbb{P}(\mathfrak{o}) - \{\mathfrak{p}_i\}$.
23: return $\mathcal{S} := \{\bigcap_i L_i\,;\, L_i \in S_i$ and $h(\bigcap_i L_i) \le B\}$.
```

Proof. Let w be the number of roots of unity of the center of E. Further, let L be an $\mathfrak{A}$-square-free $\mathcal{O}$-lattice in (V, Φ). Then $\mathrm{Mass}(L) \le c$ by Lemma 4.2.9. Moreover, if $\mathfrak{p} \in \mathbb{P}(\mathfrak{o}) - \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}$ and $L_\mathfrak{p}$ is not unimodular, then $\mathrm{Mass}(L) > B/w$ and so $h(L) > B$. Hence $h(L) \le B$ implies that $L_{\mathfrak{p}_i}$ is isometric to some lattice in S_i and $M_\mathfrak{p} \cong L_\mathfrak{p}$ for all $\mathfrak{p} \in \mathbb{P}(\mathfrak{o}) - \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}$. In particular, $\mathrm{gen}(L)$ is represented by some lattice in $\mathcal{S}$. □

Remark 6.4.2 Here are some hints how the individual steps ofAlgorithm 6.4.1 can be performed in practise:

1. The constant c_0 in line 2 of the previous algorithm can be computed using Proposition 3.3.11 and Remark 6.3.3.

2. The sets S_i from line 22 can be computed using the results of Section 3.3 and Algorithm LatticeInGenus 3.5.6.

3. The check $h(\bigcap_i L_i) \le B$ in the last line can be done using Kneser's neighbour method, see Section 5.4. But of course, one should check $\mathrm{Mass}(\bigcap_i L_i) \le B/w$ first, where w denotes the number of roots of unity of the center of E. Note that the needed local factors are given by Lemma 4.2.9 and Section 4.5 or can be computed using Remark 6.3.3.

6.5 Enumerating all genera with bounded class number

The previous section showed how to compute the definite hermitian, square-free $\mathcal{O}$-lattices of rank m and class number at most B. Given these lattices, one can enumerate all similarity classes of genera of definite hermitian $\mathcal{O}$-lattices of rank m and class number at most B by computing preimages under the reduction operators $\rho_{\mathfrak{P}}$ successively. Before this procedure can be stated explicitly, one needs to know how the local factors change under $\rho_{\mathfrak{P}}$ as well as whether this procedure actually terminates. These questions are answered by the following two results.

Lemma 6.5.1 *Let L and M be $\mathcal{O}$-lattices in (V, Φ) and let $\mathfrak{P}$ be a maximal twosided ideal of $\mathcal{O}$ such that $\mathfrak{p} := \mathfrak{P} \cap \mathfrak{o}$ is good and unramified in E. Suppose that $L_{\mathfrak{p}}$ is unimodular and $\rho_{\mathfrak{P}}(M) = L$. Then $\lambda(L_{\mathfrak{p}}) = 1$.*
If $F_{\mathfrak{p}} \cong K_{\mathfrak{p}} \oplus K_{\mathfrak{p}}$, then $\lambda(M_{\mathfrak{p}})$ is given by Lemma 4.2.9. In all other cases, $M_{\mathfrak{p}} = M_0 \perp M_2$ where M_i is $\mathfrak{P}^i$-modular and the local factor $\lambda(M_{\mathfrak{p}})$ is given by the following table.

$\dim_K(E)$	m_0	m_2	$\lambda(M_{\mathfrak{p}})$
1	*even*	*odd*	$q^{m_0 m_2/2} \cdot \frac{1}{2}(q^{m_0/2} + \varepsilon_0) \cdot \binom{(m-1)/2}{m_0/2}_{q^2}$
1	*odd*	*even*	$q^{m_0 m_2/2} \cdot \frac{1}{2}(q^{m_2/2} + \varepsilon_1) \cdot \binom{(m-1)/2}{m_2/2}_{q^2}$
1	*odd*	*odd*	$q^{(m_0 m_2 - 1)/2} \cdot \frac{1}{2} \cdot \binom{m/2-1}{(m_0-1)/2}_{q^2}$
1	*even*	*even*	$q^{m_0 m_2/2} \cdot \frac{(q^{m_0/2}+\varepsilon_0)(q^{m_2/2}+\varepsilon_1)}{2(q^{m/2}+\varepsilon_0\varepsilon_1)} \cdot \binom{m/2}{m_0/2}_{q^2}$
2	–	–	$q^{m_0 m_2} \cdot \left\lvert\binom{m}{m_0}_{-q}\right\rvert$
4	–	–	$q^{2 m_0 m_2} \cdot \binom{m}{m_0}_{q^2}$

Here q denotes the norm of $\mathfrak{p}$, $m_i = \operatorname{rank}(M_i)$ and $\varepsilon_i = +1$ if $\operatorname{disc}(M_i) \in (K_{\mathfrak{p}}^*)^2$ and $\varepsilon = -1$ otherwise.

Proof. This follows immediately from Theorem 4.2.4. □

Theorem 6.5.2 *Let $\mathfrak{P}$ be a maximal twosided ideal of $\mathcal{O}$ and let $\mathfrak{A}$ be an integral ideal of $\mathcal{O}$ such that $\mathfrak{A} = \overline{\mathfrak{A}}$. Let $(L_i)_{i \in \mathbb{N}}$ be a sequence of $\mathcal{O}$-lattices in (V, Φ) such that $\mathfrak{A} \subseteq \mathfrak{s}(L_i) \subseteq \mathcal{O}$ and $L_{i+1} \in \rho_{\mathfrak{P}}^{-1}(L_i) - \{L_i\}$ for all i. Then $\# \{i \in \mathbb{N} ;\, h(L_i) = h(L_{i+1})\}$ is bounded from above by some number which only depends on $\mathfrak{p} := \mathfrak{P} \cap \mathfrak{o}$ and L_0.*

Proof. The group $\operatorname{Aut}(L_i)$ is a subgroup of $\operatorname{Aut}(L_{i-1})$ and $(h(L_i))_{i \in \mathbb{N}}$ is monotonic increasing by Lemma 6.1.3. Loc. cit. also shows that $h(L_i) = h(L_{i-1})$ implies that $\rho_{\mathfrak{P}}^{-1}(L_{i-1}) \cap \operatorname{gen}(L_i) = \{L_{i-1}\}$ or $\operatorname{Aut}(L_i) \subsetneq \operatorname{Aut}(L_{i-1})$. Note that since $\operatorname{Aut}(L_i)$ is a subgroup of $\operatorname{Aut}(L_0)$, the latter case can only happen finitely many times. Hence is suffices to show that there exists some integer $N \geq 2$, depending only on $\mathfrak{p}$, such that $\rho_{\mathfrak{P}}^{-1}(L_{i-1}) \cap \operatorname{gen}(L_i)$ contains some lattice X different from L_i for all $i \geq N$. Let $\pi \in \mathcal{O}$ such that $\mathfrak{P} = \pi\mathcal{O}$ and let $i \geq 2$. Then $(L_i)_{\mathfrak{p}} = M_1 \perp M_2$ where M_1 is square-free and $\mathfrak{s}(M_2) \subseteq \mathfrak{P}^2$. Note that neither M_1 or M_2 are zero as $(\mathfrak{s}(L_i))_{i \in \mathbb{N}}$ is bounded and $L_i \neq L_{i+1}$. By Algorithm 3.3.2, M_1 and M_2 have orthogonal decompositions into modular lattices of rank at most 2. For showing the existence of such a lattice X, one may assume that the M_i itself are modular lattices of rank one or two. Let $x \in M_1$ and $z \in M_2$ such that $Q_\Phi(x)\mathfrak{o} = \mathfrak{n}(M_1)$ and $Q_\Phi(z)\mathfrak{o} = \mathfrak{n}(M_2)$. If M_1 has rank 2, let $y \in M_1$ such that (x, y) is a basis of M_1; otherwise set $y = 0$. Similarly, if M_2 has rank 2, let $w \in M_2$ such that (z, w) is a basis of M_2; otherwise set $w = 0$. Let X_1 and X_2 be the $\mathcal{O}_{\mathfrak{p}}$-lattices generated by $(x - \pi^{-1}z, y)$ and $(z + \frac{\Phi(z,z)}{\pi Q_\Phi(x,x)}, w + \frac{\Phi(z,w)}{\pi Q_\Phi(x,x)})$ respectively. Let X be the $\mathcal{O}$-lattice which coincides with L_i at all places of $\mathfrak{o}$ different from $\mathfrak{p}$ and $X_{\mathfrak{p}} = X_1 \perp X_2$. Note that $\mathfrak{s}(M_2) \subseteq \mathfrak{P}^i$. So if i is large enough, then $X_1 \perp X_2$ is an $\mathcal{O}_{\mathfrak{p}}$-sublattice of L_{i-1} different, yet isometric to $M_1 \perp M_2$ and $\rho_{\mathfrak{P}}(X) = \rho_{\mathfrak{P}}(L_{i-1})$. Explicit bounds for i depend on whether $\mathfrak{p}$ is good or bad and can be worked out case by case. □

The computation of all $\mathcal{O}$-lattices in (V, Φ) with a given class number B, can be reduced to the enumeration of square-free lattices as follows.

Algorithm 6.5.3 InverseSearch$(L, B, \mathfrak{A})$

Input: Some positive integer B, some twosided ideal of $\mathcal{O}$ such that $\mathfrak{A} = \overline{\mathfrak{A}}$ and some $\mathfrak{A}$-square-free $\mathcal{O}$-lattice L in (V, Φ) such that $h(L) \le B$.

Output: A sequence $\mathcal{L}$ of $\mathcal{O}$-lattices representing the genera G of all $\mathcal{O}$-lattices in (V, Φ) that satisfy the following conditions:

- $h(G) \le B$.
- G is reducible to $\mathrm{gen}(L)$.
- $\mathfrak{A} \subseteq \mathfrak{s}(M) \subseteq \mathcal{O}$ for all $M \in G$.

```
Initialiase the list $\mathcal{L} = (L)$ and let $w$ be the number of roots of unity in the center of $E$.
Let $P = \{\mathfrak{p} \in \mathbb{P}(\mathfrak{o})\,;\, \mathfrak{p}$ is bad or ramified in $E$ or $L_{\mathfrak{p}}$ is not unimodular or $\mathfrak{A}_{\mathfrak{p}} \ne \mathcal{O}_{\mathfrak{p}}\}$.
Let $P = P \cup \left\{\mathfrak{p} \in \mathbb{P}(\mathfrak{o})\,;\, \begin{array}{l}\mathrm{Mass}(M) \le B/w \text{ for some } M \in \rho_{\mathfrak{P}}^{-1}(L) \text{ where } \mathfrak{P} \\ \text{denotes a maximal twosided ideal of } \mathcal{O} \text{ over } \mathfrak{p}\end{array}\right\}$.
for $\mathfrak{p} \in P$ do
    Set $i = 1$ and fix some maximal twosided ideal $\mathfrak{P}$ of $\mathcal{O}$ over $\mathfrak{p}$.
    while $i \le \#\mathcal{L}$ do
        Let $\mathcal{M} = \{M \in \rho_{\mathfrak{P}}^{-1}(\mathcal{L}_i)\,;\, M \ne \mathcal{L}_i$ and $\mathfrak{A} \subseteq \mathfrak{s}(M)\}$.
        Let $S$ be a set of lattices that represent $\{\mathrm{gen}(M)\,;\, M \in \mathcal{M}$ and $h(M) \le B\}$.
        Append the lattices in $S$ at the end of the list $\mathcal{L}$.
        Increment $i$.
    end while
end for
return $\mathcal{L}$.
```

Proof. The set P is finite by Lemma 6.5.1. Hence Theorem 6.5.2 shows that the algorithm terminates. Also $\mathcal{L}$ does not contain two representatives in the same genus. It remains to show that the lattices in $\mathcal{L}$ represent any given genus G of integral $\mathcal{O}$-lattices in (V, Φ) that satisfies the three conditions specified at the beginning of the algorithm. By definition, there exist some $M \in G$ and maximal twosided ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ of $\mathcal{O}$ and some integer $e_i \ge 1$ such that $(\rho_{\mathfrak{P}_r}^{e_r} \circ \ldots \circ \rho_{\mathfrak{P}_1}^{e_1})(M) = L$. By Lemmata 6.1.3 and 6.5.1 one has $\mathfrak{P}_i \cap \mathfrak{o} \in P$ for all i. If $e := \sum_i e_i$ is zero, then $M = L$. Suppose now $e > 0$. The algorithm runs through the list P in a given order. Since the reduction operators $\rho_{\mathfrak{P}_i}$ commute, one may suppose that $\mathfrak{P}_r \cap \mathfrak{o}$ comes after $\mathfrak{P}_i \cap \mathfrak{o}$ for all $i < r$. Hence by induction, the list $\mathcal{L}$ represents $\mathrm{gen}(\rho_{\mathfrak{P}}(M))$. But then, the list $\mathcal{L}$ also represents $\mathrm{gen}(M) = G$. □

Again, the check $h(M) \leq B$ in line 8 of Algorithm 6.5.3 can be done using Kneser's neighbour method, see Section 5.4. Finally, the way to enumerate all similarity classes of genera of $\mathcal{O}$-lattices of rank m and class number at most B is paved:

```
Algorithm 6.5.4 ENUMERATE($K, \mathcal{O}, m, B$)
Input: A totally real number field $K$ and some maximal order $\mathcal{O}$ of a $K$-algebra $E$ such
    that either $E = K$ or $E/K$ is a CM-extension or $E$ is a definite quaternion algebra
    with center $K$. Integers $B \geq 1$ and $m \geq 2$ such that $m \geq 3$ whenever $E = K$.
Output: A set $\mathcal{L}$ representing the similarity classes of all genera of $\mathcal{O}$-lattices in hermitian
    spaces of rank $m$ over $E$ having class numbers at most $B$.
1: Let $\mathfrak{A}$ be the integral ideal of $\mathcal{O}$ from Remark 6.1.5.
2: Compute representatives $(V_1, \Phi_1), \dots, (V_t, \Phi_t)$ of the isometry classes of all definite
    hermitian spaces over $E$ of rank $m$, that might admit $\mathfrak{A}$-square-free $\mathcal{O}$-lattices with
    class numbers at most $B$, see Algorithms 6.3.4 and 6.3.9 and Remark 6.3.12.
3: For $1 \leq i \leq t$ let $\mathcal{L}_i$ be the output of ALLASQUAREFREELATTICES($(V_i, \Phi_i), B, \mathfrak{A}$).
4: Compute the set
       $\mathcal{L} = \bigcup_{i=1}^{t} \bigcup_{L \in \mathcal{L}_i} \textsc{InverseSearch}(L, B, \mathfrak{A})\,.$
5: Eliminate duplicate entries from $\mathcal{L}$, i.e. lattices that represent similar genera.
6: return $\mathcal{L}$.
```

Proof. The algorithm terminates since it only makes finitely many calls to algorithms that are already known to terminate. Let M be an $\mathcal{O}$-lattice in some hermitian space (V, Φ) of rank m such that $h(L) \leq B$. It remains to show that $\mathcal{L}$ represents a genus similar to $\mathrm{gen}(M)$. By the choice of $\mathfrak{A}$, there exists some totally positive element $a \in K$ such that the rescaled lattice M^a satisfies $\mathfrak{A} \subseteq \mathfrak{s}(M^a) \subseteq \mathcal{O}$. Thus $(V, a\Phi)$ is isometric to (V_i, Φ_i) for some i and one may assume that $M \subseteq V_i$. Now $\mathrm{gen}(M)$ reduces to some unique $\mathfrak{A}$-square-free genus G. Hence G is represented by some lattice L in $\mathcal{L}_i$ and thus $\mathrm{gen}(M)$ is represented by some lattice in $\textsc{InverseSearch}(L, B, \mathfrak{A})$. □

Remark 6.5.5 In the end, Algorithm 6.5.4 only returns similarity classes of genera. Thus it can be optimized in two ways.

1. The group $\mathfrak{o}^*_{>,0}$ acts on the the isometry classes of all definite hermitian spaces over E of rank m, that might admit $\mathfrak{A}$-square-free $\mathcal{O}$-lattices with class numbers at most B via rescaling. It suffices to let $(V_1, \Phi), \dots, (V_t, \Phi_t)$ in step 2 of Algorithm 6.5.4 represent the orbits of that action.

2. One can replace step 3 by the following steps.

```
1:  Change Algorithm 6.4.1 to only return a set $\mathcal{L}'_i$ representing the $\mathfrak{A}$-square-free
    $\mathcal{O}$-lattices in $(V_i, \Phi_i)$ of class number at most $B$ such that the rank of the
    unimodular component of a Jordan composition of $L_\mathfrak{p}$ has rank at least $m/2$
    for all $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$ such that $\mathfrak{A}_\mathfrak{p} \neq \mathcal{O}_\mathfrak{p}$.
2:  for $1 \leq i \leq t$ do
3:      Let $P = \{\mathfrak{p} \in \mathbb{P}(\mathfrak{o})\,;\, \mathfrak{A}_\mathfrak{p} \neq \mathcal{O}_\mathfrak{p}$ and $L_\mathfrak{p}$ is not unimodular for some $L \in \mathcal{L}'_i\}$.
4:      for $\mathfrak{p} \in P$ do
5:          for $L \in \mathcal{L}'_i$ such that $L_\mathfrak{p}$ is not unimodular do
6:              Let $a \in K^*$ be totally positive such that $(L^{\#,\mathfrak{p}})^a$ is $\mathfrak{A}$-square-free.
7:              Insert $(L^{\#,\mathfrak{p}})^a$ into $\mathcal{L}'_i$.
8:          end for
9:      end for
10:     Set $\mathcal{L}_i := \mathcal{L}'_i$.
11: end for
```

Note that an element a as above always exists, by the choice of $\mathfrak{A}$. Further, $(L^{\#,\mathfrak{p}})^a$ and L share the same class number. Also note that the set $\mathcal{L}'_i$ is usually much smaller than the set $\mathcal{L}_i$ from Algorithm 6.5.4 and thus can be computed much quicker. Now after step 11, the set $\bigcup_i \mathcal{L}_i$ will represent each genus of definite hermitian $\mathfrak{A}$-square-free $\mathcal{O}$-lattices. Hence it is save to replace the sets $\mathcal{L}_i$ in Algorithm 6.4.1 by the ones from above.

7 Quadratic lattices with class number at most 2

The purpose of this chapter is to report on the classification of all definite quadratic lattices over totally real number fields of rank at least 3 and class number at most 2.

The classification of all rational quadratic forms with class number 1 is originally due to G. L. Watson who classified these lattices by hand in a long series of papers [Wat63, Wat72, Wat74, Wat78, Wat82, Wat84, Wat]. In [KL13], D. Lorch and the author checked Watson's computations using the algorithms given in Chapter 6 and found them to be largely correct. They also enumerate all one-class genera in dimensions 4 and 5, for which G. Watson only produced partial results.

In [Kir14], the author classifies the one-class genera of maximal quadratic lattices over totally real number fields having rank at least 3. Very recently, D. Lorch in his thesis successfully extends this classification to all one-class genera over totally real number fields, see [Lor] for details. Prior to that, the literature mostly discussed unimodular lattices over number fields, see [Sch94] and the references therein.

Throughout this chapter, let $E = K$ be a totally real number field of degree n and let (V, Φ) be a definite quadratic space over K of rank m. Further, let $\mathfrak{o}$ be the maximal order in K.

7.1 The unary case

Suppose $m = 1$ and let L, L' be $\mathfrak{o}$-lattices in (V, Φ) in the same genus. For any prime ideal $\mathfrak{p}$ of $\mathfrak{o}$, there exists some $x_\mathfrak{p} \in K_\mathfrak{p}^*$ such that $L'_\mathfrak{p} = L_\mathfrak{p} x_\mathfrak{p}$ and $x_\mathfrak{p}^2 = 1$. Whence $x_\mathfrak{p} \in \{\pm 1\}$ and $L_\mathfrak{p} = L'_\mathfrak{p}$. But then $L' = L$. In particular, any unary $\mathfrak{o}$-lattice has class number one.

7.2 The binary case

7.2.1 Definite binary quadratic lattices over totally real number fields

Suppose that $m = 2$. In his seminal book 'Disquisitiones Arithmeticae' [Gau01], C. F. Gauß introduces (among many other things) the composition of binary, rational quadratic forms and the notion of (proper) isometry classes and genera. He relates the proper isometry classes in a given genus with the so called ambiguous ideal classes of some quadratic extension of $\mathbb{Q}$. A similar result holds for any totally real number field K. The following approach is taken from H. Pfeuffer [Pfe81] and O. Körner [Kör81].

The discriminant $\operatorname{disc}(V,\Phi) = -\det(V,\Phi)$ is a non-square, as (V,Φ) is anisotropic. Hence $F = K(\sqrt{\operatorname{disc}(V,\Phi)})$ is a quadratic field extension of K. Let σ be the non-trivial Galois automorphism of F/K and let $\mathfrak{f}$ denote the ring of integers of F. For any subset S of (a completion of) F, let $S^1 = \{x \in S\,;\, x\sigma(x) = 1\}$ be the elements of relative norm 1 in S.

By [Kne02, (6.15)], the even part of the Clifford algebra of (V,Φ) is isomorphic to the field F. Further, the space (V,Φ) is similar to the field F equipped with the trace bilinear form

$$F \times F \to E,\ (x,y) \mapsto \frac{1}{2}\operatorname{T}_{F/K}(x\sigma(y)) = \frac{x\sigma(y)+\sigma(x)y}{2}\,.$$

So for the classification of all definite binary quadratic lattices with a given class number, one may assume that $V = F$ and Φ is the bilinear form from above. Then the quadratic form Q_Φ associated to Φ is the usual relative norm $\operatorname{Nr}_{F/K}\colon F \to K$, $x \mapsto x\sigma(x)$.

Lemma 7.2.1 *The map $\Psi\colon F^1 \to \mathbf{SO}(F,\Phi)$, $\alpha \mapsto (x \mapsto \alpha x)$ is an isomorphism of groups and $\sigma \in \mathbf{O}(F,\Phi)$ is an isometry of determinant -1. Similarly, $F_\mathfrak{p}^1 \cong \mathbf{SO}(F_\mathfrak{p},\Phi)$ for all $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$.*

Proof. Only the surjectivity of Ψ requires proof. Let $\varphi \in \mathbf{SO}(F,\Phi)$. Then $\alpha := \varphi(1) \in F^1$. Let $x \in F^*$ be such that $\operatorname{T}_{F/K}(x) = 0$. Then $(1,x)$ is an orthogonal basis of (F,Φ). Hence its image under φ must also be such a basis. Thus $\varphi(x) = \alpha s x$ for some $s \in K^*$. Comparing norms shows that $s^2 = 1$. Together with $\det(\varphi) = +1$ this implies that $s = 1$ and therefore $\varphi = \Psi(\alpha)$. □

Given any $\mathfrak{o}$-lattice L in (F,Φ), let $h^+(L)$ denote the proper class number of L, i.e. the number of proper isometry classes in the genus of L. Let $\Lambda = \mathcal{O}_r(L)$ be the (right) order of L. The previous lemma shows that $\operatorname{Aut}^+(L) = \Lambda^1$ is finite. Thus $\Lambda^1 = \mu(F) \cap \Lambda$ is the group of roots of unity in Λ^*. Moreover, $\sigma \in \operatorname{Aut}(\Lambda) - \operatorname{Aut}^+(\Lambda)$ shows that $\operatorname{cls}(\Lambda) = \operatorname{cls}^+(\Lambda)$. Hence

$$h(\Lambda) \le h^+(\Lambda) \le 2h(\Lambda) - 1\,. \tag{7.2.1}$$

In particular, $h(\Lambda) = 1 \iff h^+(\Lambda) = 1$.

Lemma 7.2.2 *Let L be an $\mathfrak{o}$-lattice in (F,Φ) and let $\Lambda = \mathcal{O}_r(L)$.*

1. *L is an invertible, fractional ideal of Λ.*
2. *The set $\operatorname{gen}(\Lambda)$ forms a group with respect to the usual multiplication of ideals and $\operatorname{cls}^+(\Lambda)$ is a subgroup.*
3. *The map $\Psi\colon \operatorname{gen}(\Lambda) \to \operatorname{gen}(L)$, $M \mapsto LM$ is a bijection, which preserves proper isometry classes.*
4. *$h^+(L) = h^+(\Lambda) = [\operatorname{gen}(\Lambda) : \operatorname{cls}^+(\Lambda)]$.*

Proof. The product $L\sigma(L)$ is generated as Λ-module by $\{x\sigma(x)\,;\, x \in L\}$. But then $L\sigma(L) = \mathrm{Nr}_{F/K}(L) \cdot \Lambda$. Thus $\mathrm{Nr}_{F/K}(L)^{-1}\sigma(L)$ is the inverse of L. An $\mathfrak{o}$-lattice X is in $\mathrm{gen}(\Lambda)$ if and only if for all $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$ such that $X_\mathfrak{p} \neq \Lambda_\mathfrak{p}$, there exists some $x_\mathfrak{p} \in F_\mathfrak{p}^1$ with $X_\mathfrak{p} = \Lambda_\mathfrak{p} x_\mathfrak{p}$. The second part follows immediately from this characterization. Similarly, one characterizes the elements in $\mathrm{gen}(L)$. This shows that Ψ is well-defined. It is a bijection, since L is invertible. Two lattices $L_1, L_2 \in \mathrm{gen}(L)$ are properly isometric if and only if $L_1 = L_2 c$ for some $c \in F^1$. This is equivalent to $L^{-1}L_1 = L^{-1}L_2 c$, i.e. $\Psi^{-1}(L_1) = \Psi^{-1}(L_2)c$. Hence $L_1 \in \mathrm{cls}^+(L_2) \iff \Psi^{-1}(L_1) \equiv \Psi^{-1}(L_2) \pmod{\mathrm{cls}^+(\Lambda)}$. So Ψ^{-1} and thus Ψ preserve proper isometry classes and the number of such classes is equal to the index $[\mathrm{gen}(\Lambda) : \mathrm{cls}^+(\Lambda)]$. □

The previous lemma shows that the classification of all $\mathfrak{o}$-lattices in (F, Φ) with a certain proper class number boils down to classification of all $\mathfrak{o}$-orders Λ in F with that proper class number. The latter number can be related to $h^+(\mathfrak{f})$ as follows.

Theorem 7.2.3 *Let Λ be an $\mathfrak{o}$-order in F with conductor $\mathfrak{c}$. Then $h^+(\Lambda) \geq h^+(\mathfrak{f})$ and*

$$h^+(\Lambda) \cdot [\mathfrak{f}^1 : \Lambda^1] = h^+(\mathfrak{f}) \cdot \prod_{\mathfrak{p}|\mathfrak{c}} [\mathfrak{f}_\mathfrak{p}^1 : \Lambda_\mathfrak{p}^1]\,.$$

Proof. The proof follows [Kör81, Lemma 3]. The case $\mathfrak{c} = \mathfrak{o}$ is trivial, so suppose $\mathfrak{c} \neq \mathfrak{o}$. The map $\varphi\colon \mathrm{gen}(\Lambda) \to \mathrm{gen}(\mathfrak{f})$, $L \mapsto L\mathfrak{f}$ is a group homomorphism. Let $M \in \mathrm{gen}(\mathfrak{f})$. For every prime ideal $\mathfrak{p}$ of $\mathfrak{o}$, there exists some $x_\mathfrak{p} \in F_\mathfrak{p}^1$ such that $M_\mathfrak{p} = \mathfrak{f}_\mathfrak{p} x_\mathfrak{p}$ and one can choose $x_\mathfrak{p} = 1$ at all but finitely many places. Hence there exists some $\mathfrak{o}$-lattice L such that $L_\mathfrak{p} = \Lambda_\mathfrak{p} x_\mathfrak{p}$ everywhere. This shows that φ is onto with kernel

$$\mathrm{Ker}(\varphi) = \{\bigcap_{\mathfrak{p}|\mathfrak{c}} (F \cap \Lambda_\mathfrak{p} x_\mathfrak{p})\,;\, x_\mathfrak{p} \in \mathfrak{f}_\mathfrak{p}^1\}\,.$$

This yields the first assertion and an epimorphism $\psi\colon \mathrm{gen}(\Lambda)/\mathrm{cls}^+(\Lambda) \to \mathrm{gen}(\mathfrak{f})/\mathrm{cls}^+(\mathfrak{f})$ such that

$$\mathrm{Ker}(\psi) \cong \mathrm{Ker}(\varphi)/(\mathrm{Ker}(\varphi) \cap \mathrm{cls}^+(\Lambda))\,.$$

Further,

$$\prod_{\mathfrak{p}|\mathfrak{c}} \mathfrak{f}_\mathfrak{p}^1 \to \mathrm{Ker}(\varphi),\ (x_\mathfrak{p}) \mapsto \bigcap_{\mathfrak{p}|\mathfrak{c}} (F \cap \Lambda_\mathfrak{p} x_\mathfrak{p})$$

is a group epimorphism with kernel $\prod_{\mathfrak{p}|\mathfrak{c}} \Lambda_\mathfrak{p}^1$ and therefore

$$\mathrm{Ker}(\varphi) \cong \prod_{\mathfrak{p}|\mathfrak{c}} \mathfrak{f}_\mathfrak{p}^1/\Lambda_\mathfrak{p}^1\,.$$

Finally, note that $\mathrm{Ker}(\varphi) \cap \mathrm{cls}^+(\Lambda) = \{x\Lambda\,;\, x \in \mathfrak{f}^1\} \cong \mathfrak{f}^1/\Lambda^1$. Combining the above indices shows that $h^+(\Lambda) = h^+(\mathfrak{f}) \cdot \#\mathrm{Ker}(\psi) = h^+(\mathfrak{f}) \cdot [\mathfrak{f}^1 : \Lambda^1]^{-1} \cdot \prod_{\mathfrak{p}|\mathfrak{c}} [\mathfrak{f}_\mathfrak{p}^1 : \Lambda_\mathfrak{p}^1]$. □

In particular, there are only finitely many conductors $\mathfrak{c}$ such that $h^+(\Lambda) \leq B$ for any given bound B. It is worth mentioning that, O. Körner expresses $[\mathfrak{f}^1 : \Lambda^1]^{-1} \cdot \prod_{\mathfrak{p}} [\mathfrak{f}_{\mathfrak{p}}^1 : \Lambda_{\mathfrak{p}}^1]$ in terms of some invariants of $\operatorname{gen}(L)$ making the above theorem even more explicit, see [Kör81, Theorem 2] for details.

What remains is a study of the proper class number of $\mathfrak{f}$, which is classical. Let $\mathcal{I}(\mathfrak{f})$ be the group of fractional $\mathfrak{f}$-ideals and consider the following subgroups.

- $\mathcal{P} := \{x\mathfrak{f}\,;\, x \in F^*\}$ and $\mathcal{P}_0 := \{x\mathfrak{f}\,;\, x \in K^*\}$.
- $\mathcal{A} := \{\mathfrak{a} \in \mathcal{I}(\mathfrak{f})\,;\, \mathfrak{a} = \sigma(\mathfrak{a})\}$ the subgroup of *ambiguous ideals*.
- $\mathcal{I}_0 := \{\mathfrak{a}\mathfrak{f}\,;\, \mathfrak{a} \in \mathcal{I}(\mathfrak{o})\}$ the image of $\mathcal{I}(\mathfrak{o})$ in $\mathcal{I}(\mathfrak{f})$.

Hilbert's Theorem 90 shows that the group homomorphism

$$\mathcal{I}(\mathfrak{f}) \to \operatorname{gen}(\mathfrak{f}),\ \mathfrak{a} \mapsto \mathfrak{a}\sigma(\mathfrak{a})^{-1}$$

is actually onto. Hence it induces an group epimorphism $\mathcal{I}(\mathfrak{f}) \to \operatorname{gen}(\mathfrak{f})/\operatorname{cls}^+(\mathfrak{f})$. The kernel of this epimorphism is $\mathcal{A}\mathcal{P}$ and thus

$$\operatorname{gen}(\mathfrak{f})/\operatorname{cls}^+(\mathfrak{f}) \cong \mathcal{I}(\mathfrak{f})/\mathcal{A}\mathcal{P}\,.$$

To evaluate the index $h^+(\mathfrak{f}) = [\mathcal{I}(\mathfrak{f}) : \mathcal{A}\mathcal{P}]$, consider the diagram

$$\begin{tikzcd}
\mathcal{I}(\mathfrak{f}) \arrow[d, dash] & & \\
\mathcal{A}\mathcal{P} \arrow[dr, dash] \arrow[dd, dash] & & \\
& \mathcal{A} \arrow[dr, dash, "2^r"] \arrow[dd, dash] & \\
\mathcal{P} \arrow[dr, dash] & & \mathcal{I}_0 \arrow[dd, dash, "\#\operatorname{Cl}(K)"] \\
& \mathcal{A} \cap \mathcal{P} \arrow[dr, dash] & \\
& & \mathcal{P}_0
\end{tikzcd}$$

were r denotes the number of prime ideals of $\mathfrak{o}$ that ramify in F.

By Hilbert's Theorem 90, $\varphi\colon F^* \to F^1,\ x \mapsto x\sigma(x)^{-1}$ is an epimorphism of groups with kernel K^*. For $x \in F^*$, the ideal $x\mathfrak{f}$ is ambiguous if and only if $\varphi(x) \in \mathfrak{f}^1$. Let $U = \{x \in F^*\,;\, \varphi(x) \in \mathfrak{f}^1\}$. Then $U \to (\mathcal{A} \cap \mathcal{P})/\mathcal{P}_0,\ x \mapsto x\mathfrak{f}$ is a group epimorphism with kernel $K^*\mathfrak{f}^*$. Hence

$$(\mathcal{A} \cap \mathcal{P})/\mathcal{P}_0 \cong U/K^*\mathfrak{f}^*\,.$$

Further, φ induces isomorphisms $U/K^*\mathfrak{f}^* \cong \mathfrak{f}^1/\varphi(\mathfrak{f}^*)$ and $\mathfrak{f}^*/\mathfrak{o}^*\mathfrak{f}^1 \cong \varphi(\mathfrak{f}^*)/(\mathfrak{f}^1)^2$. From $[\mathfrak{f}^1 : (\mathfrak{f}^1)^2] = 2$, its follows that

$$[\mathcal{A} \cap \mathcal{P} : \mathcal{P}_0] = 2/Q$$

where $Q = [\mathfrak{f}^* : \mu(F)\mathfrak{o}^*] \in \{1, 2\}$ denotes the Hasse unit index of F/K. Comparing indices yields the following theorem.

Theorem 7.2.4 *Let r be the number of prime ideals of $\mathfrak{o}$ that ramify in F and let $Q = [\mathfrak{f}^* : \mu(F)\mathfrak{o}^*]$ be the Hasse unit index of F/K. Then*

$$h^+(\mathfrak{f}) = [\mathcal{I}(\mathfrak{f}) : \mathcal{A}\mathcal{P}] = \frac{\#\operatorname{Cl}(F)}{\#\operatorname{Cl}(K)} \cdot \frac{1}{Q \cdot 2^{r-1}} \,.$$

In particular, any CM-extension F/K with relative class number $\frac{\#\operatorname{Cl}(F)}{\#\operatorname{Cl}(K)}$ equal to 1 yields definite, binary quadratic $\mathfrak{o}$-lattices with class number one. However, the exact list of all CM-fields with relative class number one is currently unknown. See [LK06] for an overview of the problem. Thus the classification of all definite, binary quadratic forms with class number one is out of reach with current methods.

Provided that there are infinitely many real quadratic fields of class number one, [Kör81, Theorem 1] shows that there are infinitely many indefinite, binary quadratic lattices with class number one over the integers.

Despite the fact that Theorem 7.2.4 is ineffective, the enumeration of all definite binary quadratic lattices is still a finite problem. The result is due to A. Earnest and D. Estes [EE81].

Theorem 7.2.5 *Given any positive integer B, there are only finitely many similarity classes of definite binary quadratic forms over totally real number fields with class number at most B.*

Proof. See [EE81, Section 5]. □

7.2.2 Definite binary quadratic lattices over the rationals

While Theorem 7.2.4 does not allow a classification of all binary quadratic forms of class number one in general, it does so for $K = \mathbb{Q}$ under the assumption of the Generalized Riemann Hypothesis (GRH). The discriminants of the maximal orders corresponding to these forms are L. Euler's well known 65 idoneal numbers. The classification is based on the following observation and Louboutin's bound which will be recalled in Theorem 7.2.7.

Remark 7.2.6 Let Λ be an imaginary quadratic $\mathbb{Z}$-order. Then

1. $h(\Lambda) = 1 \iff h^+(\Lambda) = 1$.
2. $h(\Lambda) = 2 \iff h^+(\Lambda) \in \{2, 3\}$.

Proof. By equation 7.2.1, only the implication $h^+(\Lambda) = 3 \implies h(\Lambda) = 2$ requires proof. Let I be a fractional ideal of Λ such that $\operatorname{cls}^+(I)$ generates $\operatorname{gen}(\Lambda)/\operatorname{cls}^+(\Lambda) \cong C_3$. Suppose $h(\Lambda) \neq 2$. Then $h(\Lambda) = 3$ and thus $\operatorname{cls}(L) = \operatorname{cls}^+(L)$ for all $L \in \operatorname{gen}(\Lambda)$. In particular, $\sigma(I) \in \operatorname{cls}^+(I)$. By Hilbert's Theorem 90, one may assume that $\sigma(I) = I$ is ambiguous. Since $\mathbb{Q}$ has class number one, this implies that aI is a product of ramified ideals of Λ for some $a \in \mathbb{Q}^*$. But then $\operatorname{cls}^+(I)$ has order at most 2 which yields the desired contradiction. □

Theorem 7.2.7 ([Lou90, Theorem 1]) *Let F be an imaginary quadratic number field. Assuming (GRH), one has*

$$\#\operatorname{Cl}(F) \geq \frac{\pi}{3\exp(1)} \frac{\sqrt{\mathrm{d}_F}}{\ln \mathrm{d}_F}\,.$$

Suppose now F is an imaginary quadratic number field with maximal order $\mathfrak{f}$ such that $h^+(\mathfrak{f}) \leq B$. If (GRH) holds, then Theorems 7.2.4 and 7.2.7 imply that

$$\frac{\sqrt{d_F}}{\ln \mathrm{d}_F} \leq \frac{3\exp(1)}{\pi} 2^{r-1} B < 2.6 \cdot 2^{r-1} B \tag{7.2.2}$$

where r denotes the number of primes that ramify in F. Thus d_F is a product of r coprime integers from

$$\{4, 8\} \cup \{p \in \mathbb{Z}\,;\, p \text{ an odd prime}\}\,.$$

In particular, the left hand side of equation 7.2.2 tends to ∞ as $r \to \infty$. For example in the case $B = 3$, one checks that $r \leq 9$ and 9973 is the largest possible prime divisor of d_F. An explicit search using `Magma` yields the following result. The first part is due to P. Weinberger [Wei73].

Theorem 7.2.8 *Assuming (GRH), the following holds.*

1. *There are 65 maximal, imaginary quadratic $\mathbb{Z}$-orders $\mathfrak{f}$ such that $h^+(\mathfrak{f}) = 1$. The discriminants of these orders are Euler's idoneal numbers. They are listed in Table 7.1.*
2. *There are 161 maximal, imaginary quadratic $\mathbb{Z}$-orders $\mathfrak{f}$ such that $h^+(\mathfrak{f}) = 2$.*
3. *There are 338 maximal, imaginary quadratic $\mathbb{Z}$-orders $\mathfrak{f}$ such that $h^+(\mathfrak{f}) = 3$.*

A list of these orders is available from [Kir16].

Suppose now Λ is a $\mathbb{Z}$-suborder of $\mathfrak{f}$ with conductor $c \neq 1$ such that $h^+(\Lambda) \leq B$. Theorem 7.2.3 shows that $h^+(\mathfrak{f}) \leq h^+(\Lambda) \leq B$. Hence for all orders $\mathfrak{f}$ from Theorem 7.2.8, one simply has to compute the possible conductors that yield orders with proper ideal class number at most B. If $p \mid c$ and $p \nmid 2\,\mathrm{d}_F$, then $\mathfrak{f}_p^1$ is mapped to the elements of $\mathfrak{f}_p/p\mathfrak{f}_p$ of norm one and Λ_p^1 is mapped to $\{\pm 1\}$. Hence $[\mathfrak{f}_p^1 : \Lambda_p^1] \geq \frac{p-1}{2}$. Thus c is supported at

$$\{p\,;\, p \mid 2\,\mathrm{d}_F \;\text{ or }\; p \leq 1 + 2B[\mathfrak{f}^1 : \{\pm 1\}]/h^+(\mathfrak{f})\}\,.$$

This yields all possible prime divisors of c. The same argument as used in Theorem 7.2.3 actually shows that $h^+(\Lambda') \geq h^+(\Lambda)$ for any suborder Λ' of Λ. Thus for any prospective prime divisor p of c one can test the $\mathfrak{o}$-suborders of $\mathfrak{f}$ having conductor $p, p^2, p^3, \ldots$ until one reaches an order Λ with $h^+(\Lambda) > B$. This gives an upper bound for the p-adic valuation of c and thus all possible conductors c. If one applies this strategy to all orders given by Theorem 7.2.8, one obtains the result below.

Theorem 7.2.9 *Assuming (GRH), the following holds.*

1. *There are* 101 *imaginary quadratic* $\mathbb{Z}$*-orders* Λ *such that* $h^+(\Lambda) = 1$*. They are listed in Table 7.1.*
2. *There are* 324 *imaginary quadratic* $\mathbb{Z}$*-orders* Λ *such that* $h^+(\Lambda) = 2$*.*
3. *There are* 683 *imaginary quadratic* $\mathbb{Z}$*-orders* Λ *such that* $h^+(\Lambda) = 3$*.*

A list of these orders is available from [Kir16].

The above result and Remark 7.2.6 immediately yield a classification of all definite binary quadratic lattices of class number at most 2 over the rationals.

Corollary 7.2.10 *Assuming (GRH), there are* 101 *imaginary quadratic* $\mathbb{Z}$*-orders* Λ *such that* $h(\Lambda) = 1$ *and* 1007 *imaginary quadratic* $\mathbb{Z}$*-orders* Λ *such that* $h(\Lambda) = 2$*.*

Table 7.1: Fundamental discriminants $-\mathrm{d}_F$ and conductors c of orders with $h^+ = 1$.

d_F	c	d_F	c	d_F	c	d_F	c	d_F	c	d_F	c
3	$1,2,3,4,5,7,8$	43	1	148	1	340	1	595	1	1320	$1,2$
4	$1,2,3,4,5$	51	1	163	1	372	1	627	1	1380	1
7	$1,2,4,8$	52	1	168	$1,2$	403	1	660	1	1428	1
8	$1,2,3,6$	67	1	187	1	408	$1,2$	708	1	1435	1
11	$1,3$	84	1	195	1	420	1	715	1	1540	1
15	$1,2,4,8$	88	$1,2$	228	1	427	1	760	$1,2$	1848	$1,2$
19	1	91	1	232	$1,2$	435	1	795	1	1995	1
20	$1,3$	115	1	235	1	483	1	840	$1,2$	3003	1
24	$1,2$	120	$1,2$	267	1	520	$1,2$	1012	1	3315	1
35	$1,3$	123	1	280	$1,2$	532	1	1092	1	5460	1
40	$1,2$	132	1	312	$1,2$	555	1	1155	1		

7.3 The ternary case

Suppose $m = 3$. The bound given in Corollary 6.3.2 is simply not good enough to be able to write down all possible base fields K that might admit one-class genera of definite, ternary quadratic forms. However, there is a well known correspondence between ternary quadratic forms and quaternion orders due to J. Brzezinski [Brz80, Brz82] and M. Peters [Pet69]. It is based on work of M. Eichler [Eic52] and H. Brandt [Bra43]. In [KL16], D. Lorch and the author used this correspondence to classify all ternary quadratic forms of class number at most 2. The section at hand gives a summary of the method used.

By [Kne02, Section 6], the even part of the Clifford algebra of (V, Φ) is a definite quaternion algebra $\mathcal{Q}$. Let $\sigma\colon \mathcal{Q} \to \mathcal{Q}$ be its canonical involution and let $\mathrm{nr}_{\mathcal{Q}/K}$ and $\mathrm{tr}_{\mathcal{Q}/K}$ denote the reduced norm and trace of $\mathcal{Q}$. By [Kne02, (6.20)], the trace zero subspace $\mathcal{Q}^0 := \{x \in \mathcal{Q}\,;\, \mathrm{tr}_{\mathcal{Q}/K}(x) = 0\}$ equipped with the trace bilinear form

$$\mathcal{Q}^0 \times \mathcal{Q}^0 \to K,\ (x, y) \mapsto \frac{1}{2}\,\mathrm{tr}(x\sigma(y))$$

is similar to (V, Φ). So for the classification of all definite ternary quadratic lattices with a given class number, one may assume that $V = \mathcal{Q}^0$ and Φ is the bilinear form from above. Its associated quadratic form Q_Φ is then the reduced norm $\mathrm{nr}_{\mathcal{Q}/K}$.

An $\mathfrak{o}$-order $\mathcal{O}$ in $\mathcal{Q}$ is called *Gorenstein*, if the inverse reduced different

$$\mathcal{O}^\# := \{x \in \mathcal{Q}\,;\, \mathrm{tr}_{\mathcal{Q}/K}(x\mathcal{O}) \subseteq \mathfrak{o}\}$$

is an invertible twosided ideal of $\mathcal{O}$. For example maximal or more generally hereditary orders are Gorenstein. For any order $\mathcal{O}$, the ideal $\mathcal{D}(\mathcal{O}) := \mathrm{nr}_{\mathcal{Q}/K}(\mathcal{O}^\#)^{-1}$ of $\mathfrak{o}$ is called the reduced discriminant of $\mathcal{O}$. If $\mathcal{O}$ is a maximal order in $\mathcal{Q}$, then $\mathcal{D}(\mathcal{O}) = \mathrm{d}_{\mathcal{Q}/K}^{1/2}$ is the product of all prime ideals of $\mathfrak{o}$ that ramify in $\mathcal{Q}$. Two $\mathfrak{o}$-orders $\mathcal{O}, \mathcal{O}'$ in $\mathcal{Q}$ are said to be of the same type, if $\mathcal{O}_\mathfrak{p}$ and $\mathcal{O}'_\mathfrak{p}$ are isomorphic (i.e. conjugate) for all $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$. The set of all orders in $\mathcal{Q}$ which are of the same type as $\mathcal{O}$ is a union of finitely many isomorphism classes. The number of the classes is called the type number of $\mathcal{O}$. Note that any order is contained in some canonical Gorenstein order, the so-called *Gorenstein closure*. Further the type number of an order always agrees with the type number of it Gorenstein closure, see Section 2 of [KL16] for details. Hence the classification of all orders with given type number boils down to the enumeration of all Gorenstein orders with that type number.

If L is an $\mathfrak{o}$-lattice in $(\mathcal{Q}^0, \Phi)$, then

$$\mathfrak{O}(L) := 1\mathfrak{o} + \sum_{x,y \in L} \mathfrak{n}(L)^{-1} \cdot xy$$

is a Gorenstein order in $\mathcal{Q}$ (see [Pet69, Satz 7] and [Brz82, Proposition 2.3]). Conversely, if $\mathcal{O}$ is a Gorenstein order in $\mathcal{Q}$ then

$$\mathfrak{L}(\mathcal{O}) := \mathcal{D}(\mathcal{O}) \cdot (\mathcal{O}^\# \cap \mathcal{Q}^0)$$

is an $\mathfrak{o}$-lattice in $(\mathcal{Q}^0, \Phi)$.

Theorem 7.3.1 *Let $\mathcal{Q}$ be a quaternion algebra over some number field K and let L, L' be $\mathfrak{o}$-lattices in $(\mathcal{Q}^0, \Phi)$.*

1. *Each Gorenstein order $\mathcal{O}$ in $\mathcal{Q}$ satisfies $\mathcal{O} = \mathfrak{O}(\mathfrak{L}(\mathcal{O}))$.*
2. *There exists a fractional ideal $\mathfrak{a}$ of $\mathfrak{o}$ such that $\mathfrak{a}L = \mathfrak{L}(\mathfrak{O}(L))$.*
3. *$\mathfrak{O}(L)$ and $\mathfrak{O}(L')$ are isomorphic if and only if L' is isometric to $\mathfrak{a}L$ for some fractional ideal $\mathfrak{a}$ of $\mathfrak{o}$.*

Proof. The first assertion follows from [Brz82, Proposition 3.2] and it implies $\mathfrak{O}(L) = \mathfrak{O}(\mathfrak{L}(\mathfrak{O}(L)))$. Hence L and $\mathfrak{L}(\mathfrak{O}(L))$ differ by some fractional ideal as [Eic52, Satz 14.1] shows. The last part is proven in [Brz80, Corollary 3.10]. □

The two constructions $\mathfrak{O}$ and $\mathfrak{L}$ are compatible with taking completions. This shows the following result.

Corollary 7.3.2 *Let L be a ternary $\mathfrak{o}$-lattice in $(\mathcal{Q}, \Phi)$. Then the class number of* $\operatorname{gen}(L)$ *coincides with the type number of $\mathfrak{O}(L)$.*

Recently J. Voight came up with a functorial correspondence between ternary quadratic forms and quaternion orders which preserves class numbers [Voi11]. Using either correspondence shows that the classification of all definite ternary quadratic forms over K with class number h is equivalent to the enumeration of all definite quaternion Gorenstein orders over K with type number h.

Let $\mathcal{O}$ be a Gorenstein order in $\mathcal{Q}$ and let $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$. There exists some twosided ideal I of $\mathcal{O}$ such that $I/\mathfrak{p}\mathcal{O}$ is the radical of the $\mathfrak{o}/\mathfrak{p}$-algebra $\mathcal{O}/\mathfrak{p}\mathcal{O}$. The *radical idealizer process* $\operatorname{Id}_{\mathfrak{p}}(\mathcal{O})$ of $\mathcal{O}$ is the Gorenstein closure of the right order of I. The radical idealizer process is similar to the reduction operators $\rho_{\mathfrak{p}}$ from Definition 6.1.1, as it satisfies the following conditions.

- $(\operatorname{Id}_{\mathfrak{p}}(\mathcal{O}))_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}$ if and only if $\mathcal{O}_{\mathfrak{p}}$ is hereditary, c.f. [Rei03, Chapter 39].
- $\operatorname{Id}_{\mathfrak{q}}(\operatorname{Id}_{\mathfrak{p}}(\mathcal{O})) = \operatorname{Id}_{\mathfrak{p}}(\operatorname{Id}_{\mathfrak{q}}(\mathcal{O}))$ for all $\mathfrak{q} \in \mathbb{P}(\mathfrak{o})$.
- The type number of $\mathcal{O}$ is at least the type number of $\operatorname{Id}_{\mathfrak{p}}(\mathcal{O})$, c.f. [KL16, Lemma 5.4].

In particular, if K admits a definite, ternary quadratic $\mathfrak{o}$-lattice with class number h, it also admits a definite, hereditary, quaternion order with type number at most h.

Theorem 7.3.3 (Eichler's Mass formula) *Let $\mathcal{O}$ be a hereditary order in $\mathcal{Q}$. Write $\mathcal{D}(\mathcal{O}) = \mathrm{d}_{\mathcal{Q}/K}^{1/2} \cdot \mathfrak{l}$ for some integral ideal $\mathfrak{l}$ of $\mathfrak{o}$. Further let $\mathcal{O}_1, \dots, \mathcal{O}_t$ represent the isomorphism classes of all orders in $\mathcal{Q}$ that are of the same type as $\mathcal{O}$. Then*

$$\begin{aligned} \mathcal{M}(\mathcal{O}) &:= \sum_{i=1}^{t} \frac{h(\mathcal{O}_i)}{[\mathcal{O}_i^* : \mathfrak{o}^*]} \\ &= 2^{1-n} \cdot |\zeta_K(-1)| \cdot \# \operatorname{Cl}(K) \cdot \prod_{\mathfrak{p} | \mathrm{d}_{\mathcal{Q}/K}^{1/2}} (\operatorname{Nr}_{K/\mathbb{Q}}(\mathfrak{p}) - 1) \cdot \prod_{\mathfrak{p} | \mathfrak{l}} (\operatorname{Nr}_{K/\mathbb{Q}}(\mathfrak{p}) + 1) \, . \end{aligned}$$

Here $h(\mathcal{O}_i)$ denotes the number of isomorphism classes of invertible, twosided ideals of $\mathcal{O}_i$.

Proof. See for example [Eic55, Section 4]. □

If $\mathcal{O}$ is an order in $\mathcal{Q}$, let $\mathcal{N}_{\mathcal{Q}^*}(\mathcal{O}) = \{x \in \mathcal{Q}^* \,;\, x\mathcal{O}x^{-1} = \mathcal{O}\}$ be its normalizer in $\mathcal{Q}^*$. If $\mathcal{O}$ is hereditary, [Eic55, Section 4] shows that the number $h(\mathcal{O})$ occurring in Eichler's mass formula is given by

$$h(\mathcal{O}) = \frac{2^r \cdot \#\,\mathrm{Cl}(K)}{[\mathcal{N}_{\mathcal{Q}^*}(\mathcal{O}) : \mathcal{O}^* K^*]} = 2^r \cdot \#\,\mathrm{Cl}(K) \cdot \frac{[\mathcal{O}^* : \mathfrak{o}^*]}{[\mathcal{N}_{\mathcal{Q}^*}(\mathcal{O}) : K^*]} \tag{7.3.1}$$

where r denotes the number of prime ideals dividing $\mathcal{D}(\mathcal{O})$.

Combining equation (7.3.1) with Eichler's mass formula yields a major improvement over Corollary 6.3.2.

Theorem 7.3.4 *If $\mathcal{O}$ is a hereditary order in $\mathcal{Q}$ with type number t, then*

$$\mathrm{d}_K^{1/n} < ((t/2)^{1/n} \cdot 4\pi^2 \cdot (3/2)^{\omega_2(K)/n})^{2/3}\,.$$

Here $\omega_2(K)$ denotes the number of prime ideals in $\mathfrak{o}$ of norm 2.

Proof. Let r and $\{\mathcal{O}_1, \dots, \mathcal{O}_t\}$ be as in Theorem 7.3.3. Eichler's mass formula and equation (7.3.1) show that

$$\begin{aligned} t &\geq \sum_{i=1}^{t} \frac{1}{[\mathcal{N}_{\mathcal{Q}^*}(\mathcal{O}_i) : K^*]} = \frac{\mathcal{M}(\mathcal{O})}{2^r \cdot \#\,\mathrm{Cl}(K)} \\ &\geq 2^{1-n} \cdot |\zeta_K(-1)| \prod_{\mathfrak{p} \mid \mathrm{d}_{\mathcal{Q}/K}^{1/2}} \frac{\mathrm{N}(\mathfrak{p}) - 1}{2} \\ &\geq 2^{1-n} \cdot |\zeta_K(-1)| \cdot 2^{-\omega_2(K)} \geq \frac{2\,\mathrm{d}_K^{3/2}}{(2\pi)^{2n}} \cdot \zeta_K(2) \cdot 2^{-\omega_2(K)} \\ &> \frac{2\,\mathrm{d}_K^{3/2}}{(2\pi)^{2n}} \cdot (4/3)^{\omega_2(K)} \cdot 2^{-\omega_2(K)} \geq \frac{2\,\mathrm{d}_K^{3/2}}{(2\pi)^{2n}} \cdot (2/3)^{\omega_2(K)} \end{aligned}$$

as claimed. □

Corollary 7.3.5 *If $\mathcal{O}$ is a hereditary order in $\mathcal{Q}$ with type number $t \leq 2$, then*

$$\mathrm{d}_K^{1/n} < (4\pi^2 \cdot (3/2)^{\omega_2(K)/n})^{2/3}\,. \tag{7.3.2}$$

There are 358 totally real number fields K that satisfy equation (7.3.2). The largest one has degree 8.

Proof. Let K be a totally real number field that satisfies equation (7.3.2) and let n be its degree. Then $\mathrm{d}_K^{1/n} < (6\pi^2)^{2/3} < 15.20$. The bounds from [BD08] imply that $n \leq 10$. If $n = 10$, then [BD08] shows that $\mathrm{d}_K^{1/n} < 15.20$ is only possible if $\omega_2(K) \leq 1$. But $\mathrm{d}_K^{1/n} < (4\pi^2 \cdot (3/2)^{1/10})^{2/3} < 11.92$ is impossible by [Voi08]. The case $n = 9$ is ruled out similarly. The tables [Voi08] list all totally real number fields K with $\mathrm{d}_K^{1/n} \leq 15.5$ and degree at most 8. The result follows from an explicit search. □

With the possible base fields at hand, the enumeration of all ternary quadratic $\mathfrak{o}$-lattices with class number at most 2 can now proceed as in Chapter 6. However, enumerating the quaternion orders of type number 2 directly as it is done in [KL16], is much more efficient:

Suppose a hereditary order $\mathcal{O}$ in $\mathcal{Q}$ has type number $t \leq 2$. Let $\mathcal{D}(\mathcal{O}) = \mathrm{d}_{\mathcal{Q}/K}^{1/2} \cdot \mathfrak{l}$ for some integral, square-free ideal $\mathfrak{l}$ of $\mathfrak{o}$. As in the proof of Theorem 7.3.4 it follows that

$$2 \geq t \geq 2^{1-n} |\zeta_K(-1)| \cdot \prod_{\mathfrak{p} \mid \mathrm{d}_{\mathcal{Q}/K}^{1/2}} (\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p}) - 1) \cdot \prod_{\mathfrak{p} \mid \mathfrak{l}} (\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p}) + 1) \,.$$

For any field K from Corollary 7.3.5, there are only finitely many pairs of integral, square-free coprime ideals $(\mathrm{d}_{\mathcal{Q}/K}^{1/2}, \mathfrak{l})$ of $\mathfrak{o}$ that satisfy this inequality. From $\mathrm{d}_{\mathcal{Q}/K}$ one obtains the quaternion algebra $\mathcal{Q}$ as explained in Remark 3.4.2. Every order $\mathcal{O}$ in $\mathcal{Q}$ with discriminant $\mathcal{D}(\mathcal{O}) = \mathrm{d}_{\mathcal{Q}/K}^{1/2} \mathfrak{l}$ is hereditary and of the same type. The construction of such an order can be done as follows.

1. Start with a maximal order $\mathcal{O}$ in $\mathcal{Q}$ which can be computed using Zassenhaus' Round2 algorithm, see [Zas72].

2. For $\mathfrak{p} \mid \mathfrak{l}$ find an isomorphism $\varphi_\mathfrak{p} \colon \mathcal{O}/\mathfrak{p}\mathcal{O} \to (\mathfrak{o}/\mathfrak{p})^{2\times 2}$. This boils down to find some nonzero element in $\mathcal{O}/\mathfrak{p}\mathcal{O}$ with reducible minimal polynomial over $\mathfrak{o}/\mathfrak{p}$.

3. For $\mathfrak{p} \mid \mathfrak{l}$ replace $\mathcal{O}$ by the preimage of the upper triangular matrices under $\varphi_\mathfrak{p}$.

Once $\mathcal{O}$ is constructed, a set of representatives of the conjugacy classes of hereditary orders with discriminant $\mathcal{D}(\mathcal{O})$ can be obtained from [KV10, Algorithm 7.10]. This yields the type number of $\mathcal{O}$. So the enumeration of all definite, hereditary quaternion orders with type number 2 is now clear, see also [KL16, Algorithm 4.5]. The non-hereditary orders with type number at most 2 can be gotten by successively taking preimages under $\mathrm{Id}_\mathfrak{p}$ but two questions still remain:

- At which places $\mathfrak{p}$ does one have to compute preimages of $\mathrm{Id}_\mathfrak{p}$ to reach all Gorenstein orders of type number 2?

- How to compute the type number of such a preimage.

These two questions are answered by the following lemma.

Lemma 7.3.6 *Let $\Lambda, \mathcal{O}$ be Gorenstein orders in $\mathcal{Q}$ such that $\mathrm{Id}_\mathfrak{p}(\Lambda) = \mathcal{O}$ for some $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$. Let $(\mathcal{O}_1, \dots, \mathcal{O}_t)$ represent the conjugacy classes of all orders in $\mathcal{Q}$ which are of the same type as $\mathcal{O}$.*

1. The normalizer $\mathcal{N}_{\mathcal{Q}^*}(\mathcal{O}_i)$ acts on

$$X_i := \{\Lambda' \subset \mathcal{Q}\,;\, \Lambda' \textit{ is of the same type as } \Lambda \textit{ and } \mathrm{Id}_\mathfrak{p}(\Lambda') = \mathcal{O}_i\}$$

by conjugation. Let $\{\Lambda_{i,1}, \dots, \Lambda_{i,n_i}\}$ represent the orbits of this action. Then

$$\{\Lambda_{i,j} \mid 1 \leq j \leq n_i,\ 1 \leq i \leq t\}$$

is a complete set of representatives of the conjugacy classes of all orders in $\mathcal{Q}$ which are of the same type as Λ.

2. *Suppose $\mathfrak{p} \nmid \mathcal{D}(\mathcal{O})$ and $\Lambda_\mathfrak{p}$ is not hereditary. Then $\# X_i \geq \mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})(\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})-1)/2$. In particular, the type number of Λ is at least*

$$\sum_{i=1}^{t} \left\lceil \frac{\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})(\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})-1)}{2 \cdot \# \mathcal{N}_{\mathcal{Q}^*}(\mathcal{O}_i)} \right\rceil .$$

Proof. See [KL16, Lemmata 5.4 and 5.5]. □

A complete description of the method to compute all definite Gorenstein quaternion orders with a given type number is presented in [KL16, Algorithms 4.5 and 5.6]. If one applies these algorithms to the fields K given by Corollary 7.3.5, one finally obtains the following result.

Theorem 7.3.7

1. *There are 4194 types of definite Gorenstein quaternion orders of type number one over 30 different base fields. The largest field has degree 5.*

2. *There are 18 538 types of definite Gorenstein quaternion orders of type number two over 75 different base fields. The largest field has degree 6.*

A complete list of representatives is available electronically from [Kir16].

Note that since the type number of an quaternion order agrees with the type number of its Gorenstein closure, the above result actually classifies all definite quaternion orders with type number at most 2. From that classification it is fairly easy to enumerate all definite quaternion orders which ideal class number (i.e. the number of isomorphism classes of invertible left ideals) at most 2. See [KL16, Section 6] for details.

7.4 The general case

As mentioned in the beginning of this chapter, the enumeration of all one-class genera of definite quadratic lattices is due to G. Watson, see also [KL13]. D. Lorch very recently extends this classification to arbitrary totally real number fields in his thesis [Lor].

Applying Algorithm 6.5.4 to the fields K and ranks $m \geq 4$ given by Corollary 6.3.2 yields the following results.

Theorem 7.4.1 *The number of similarity classes of genera of definite quadratic $\mathbb{Z}$-lattices with rank $m \geq 4$ and class number $h \leq 2$ is given by the following table.*

m	4	5	6	7	8	9	10	11	12	13	14	15	16	≥ 17
$h = 1$	481	295	186	86	36	4	2	0	0	0	0	0	0	0
$h = 2$	1717	967	581	302	131	52	16	7	6	0	2	2	1	0

A complete list of representatives is available electronically from [Kir16].

To state the results for $K \neq \mathbb{Q}$, two specific lattices over $\mathbb{Q}(\sqrt{5})$ will be needed. Let $V_1 := \mathbb{Q}(\zeta_5)$ and let $\sigma_1 \colon \mathbb{Q}(\zeta_5) \to \mathbb{Q}(\zeta_5)$ the field morphism which maps ζ_5 to ζ_5^{-1}. Similarly, let $V_2 := \left(\frac{-1,-1}{\mathbb{Q}(\sqrt{5})}\right)$ and let σ_2 be the canonical involution of V_2. Any maximal order M_i of V_i equipped with the trace bilinear form

$$\Phi_i \colon V_i \times V_i \to V_i,\ (x,y) \mapsto \frac{x\sigma_i(y) + y\sigma_i(x)}{2}$$

yields an indecomposable, definite binary or quaternary quadratic $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$-lattice having class number one. Using the notation of [Neb98], the automorphism groups of M_1 and M_2 are $\pm D_{10}$ and $(\mathrm{SL}_2(5) \circ \mathrm{SL}_2(5))$:2. Note that the lattice M_2 is similar to the lattice H_4 of [Sch94].

Theorem 7.4.2 *Suppose L is a definite quadratic lattice over $K \neq \mathbb{Q}$ of rank $m \geq 4$.*

1. *There are 607 similarity classes of one-class genera of quaternary lattices over 22 different base fields. The largest field has degree 5.*
2. *There are 1737 similarity classes of two-class genera of quaternary lattices over 32 different base fields. The largest field has degree 6.*
3. *If $m \geq 5$ and $h(L) = 1$, then $m \leq 6$ and $K = \mathbb{Q}(\sqrt{5})$. Moreover, either L or $L^\#$ is similar to $\langle 1 \rangle \perp M_2$ or $M_1 \perp M_2$.*
4. *If $m \geq 5$ and $h(L) = 2$, then K is either $\mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{13})$ or the maximal totally real subfield $\mathbb{Q}(\theta_7)$ of the seventh cyclotomic field $\mathbb{Q}(\zeta_7)$. The number of similarity classes of such genera is as follows.*

m	5	6	7	8	≥ 9
$\mathbb{Q}(\sqrt{5})$	40	11	2	1	0
$\mathbb{Q}(\sqrt{2})$	10	0	0	0	0
$\mathbb{Q}(\sqrt{13})$	2	0	0	0	0
$\mathbb{Q}(\theta_7)$	4	2	0	0	0

A complete list of representatives is available electronically from [Kir16].

The first and third part of the previous theorem are due to D. Lorch, see also [Lor].

7.5 Unimodular lattices with mass at most 1/2

Let L be a unimodular $\mathfrak{o}$-lattice in a definite quadratic space (V, Φ) over K such that $\mathrm{Mass}(L) \leq 1/2$.

Lemma 7.5.1 *Let K be a totally real number field of degree n. Suppose L is a unimodular, definite quadratic $\mathfrak{o}$-lattice of rank $m \geq 3$ and mass at most $1/2$. Then*

$$\mathrm{d}_K^{1/n} \leq (2^{-\frac{1}{n}} \cdot \gamma_m \cdot c_m)^{\frac{4}{m(m-1)}}$$

where γ_m is given by Theorem 4.2.3 and

$$c_m = \begin{cases} 3/2 & \text{if } m = 3, \\ 9/8 & \text{if } m = 4, \\ 1 & \text{otherwise.} \end{cases}$$

In particular, $m \le 28$ and $m \le 14$ whenever $K \neq \mathbb{Q}$.

Proof. Suppose first m is odd. Then $\lambda(L_\mathfrak{p}) \ge 1$ unless $m = 3$ and $\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p}) = 2$, see Section 4.4 for details. Hence Siegel's mass formula states that

$$\begin{aligned} 1/2 \ge \mathrm{Mass}(L) &= \gamma_m^{-n}\, \mathrm{d}_K^{m(m-1)/4} \cdot \prod_{i=1}^{(m-1)/2} \zeta_K(2i) \cdot \prod_{\mathfrak{p}} \lambda(L_\mathfrak{p}) \\ &\ge \gamma_m^{-n}\, \mathrm{d}_K^{m(m-1)/4} \cdot \begin{cases} (2/3)^n & \text{if } m = 3, \\ 1 & \text{otherwise.} \end{cases} \end{aligned}$$

Suppose now that m is even. Let $\mathrm{disc}(L) = d \cdot (K^*)^2$. Then $\lambda(L_\mathfrak{p}) \ge 1$ unless $\mathfrak{p}$ ramifies in $K(\sqrt{d})$ or all of the following conditions hold: $m = 4$, $\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p}) = 2$ and $d \in (K_\mathfrak{p}^*)^2$. Hence

$$\begin{aligned} &1/2 \ge \mathrm{Mass}(L) \\ &= \gamma_m^{-n}\, \mathrm{d}_K^{m(m-1)/4} \cdot \mathrm{Nr}_{K/\mathbb{Q}}(\mathrm{d}_{K(\sqrt{d})/K})^{(m-1)/2} \cdot \prod_{i=1}^{m/2-1} \zeta_K(2i) \cdot \mathfrak{L}_K(\chi_d, m/2) \cdot \prod_{\mathfrak{p}} \lambda(L_\mathfrak{p}) \\ &\ge \gamma_m^{-n}\, \mathrm{d}_K^{m(m-1)/4} \cdot \begin{cases} (8/9)^n & \text{if } m = 4, \\ 1 & \text{otherwise.} \end{cases} \end{aligned}$$

This yields the claimed bounds on $\mathrm{d}_K^{1/n}$. Note that this bound becomes less than 1 (or less than $\sqrt{5}$) if $m \ge 29$ (or $m \ge 15$). □

The previous lemma shows that there are only finitely many pairs (K, m) such that K admits unimodular lattices of rank m and mass at most $1/2$. Further, all possible base fields K are listed in the tables [Voi08].

The assumption that L is unimodular, forces $\mathrm{c}(V_\mathfrak{p}, \Phi) = +1$ for all odd prime ideals $\mathfrak{p}$ of $\mathfrak{o}$. Hence one can easily adopt Algorithms 6.3.4 and 6.4.1 to just enumerate the genera of unimodular $\mathfrak{o}$-lattices with mass at most $1/2$ and rank m.

Let $I_m(K)$ denote the lattice $\mathfrak{o}^m$ equipped with the standard bilinear form. The isometry classes of all unimodular $\mathbb{Z}$-lattices are enumerated in J. Conway and N. Sloane in [CS99] up to rank 25. It turns out that $\mathrm{gen}(I_{26}(\mathbb{Q}))$ and $\mathrm{gen}(I_{27}(\mathbb{Q}))$ are the only genera of unimodular lattices with rank $m \ge 26$. However, I was unable to split these two genera into isometry classes using Kneser's method since the class numbers and ranks of the lattices are simply too large.

For $K \neq \mathbb{Q}$, splitting the genera was not much of a problem. The numbers of isometry classes, genera and base fields K are given by the following table.

rank	# genera	# isometry classes	# base fields K
3	158	574	86
4	235	1760	131
5	19	191	11
6	19	295	10
7	7	252	3
8	15	544	7
9	2	43	2
10	3	261	2
11	1	100	1
12	1	15	1
≥ 13	0	0	0

In each case, after splitting the genera into isometry classes, the Mass of the genus was compared with Siegel's mass formula using the local factors given in Section 4.4. They agreed in all cases, which is a good indicator that the results in Section 4.4 are correct.

Finding the pairs (K, m) such that $I_m(K)$ has class number one, has been studied extensively by various authors. The case $m \geq 4$ was settled by J. Dzewas and K. Barner [Dze60, Bar68]. In [Pfe71b], H. Pfeuffer gives a list of 6 fields K such that $I_3(K)$ has class number one, but he could not prove the completeness of this list. The enumeration of all unimodular lattices with mass at most 1/2 or [KL16] show that Pfeuffer's list is in fact complete. More precisely, the following result holds.

Theorem 7.5.2 *Let K be a totally real number field and let $m \geq 3$ be an integer. Then $I_m(K)$ has class number one if and only if one of the following conditions holds.*

- *$m = 3$ and K is one of*

$$\mathbb{Q},\ \mathbb{Q}(\sqrt{2}),\ \mathbb{Q}(\sqrt{5}),\ \mathbb{Q}(\sqrt{17}),\ \mathbb{Q}(\theta_7),\ \mathbb{Q}[x]/(x^3 - x^2 - 3x + 1)$$

  where $\mathbb{Q}(\theta_7)$ denotes the maximal totally real subfield of the seventh cyclotomic field $\mathbb{Q}(\zeta_7)$.

- *$m = 4$ and $K \in \{\mathbb{Q},\ \mathbb{Q}(\sqrt{2}),\ \mathbb{Q}(\sqrt{5})\}$.*

- *$5 \leq m \leq 8$ and $K = \mathbb{Q}$.*

8 Hermitian lattices with class number at most 2

Let E/K be a CM-extension of number fields and let (V, Φ) be a definite hermitian space over E of rank m. The maximal orders of K and E will be denoted by $\mathfrak{o}$ and $\mathcal{O}$ respectively.

In this chapter a complete classification of definite hermitian lattices over E of rank $m \geq 3$ with class number at most 2 will be given.

8.1 The unary case

Suppose $m = 1$. Up to similarity, the space $V = E$ carries only one definite hermitian form, which is its trace bilinear form

$$\Phi\colon E \times E \to K,\ (x, y) \mapsto \frac{x\overline{y} + y\overline{x}}{2}$$

with the relative norm of E/K as associated quadratic form Q_Φ.

Every $\mathcal{O}$-lattice L in (E, Φ) is a binary quadratic $\mathfrak{o}$-lattice (but not vice versa). By Lemma 7.2.1, this identification preserves genera and maps isometry classes to proper isometry classes. So the class number of L is given by Theorem 7.2.4. As mentioned in the comment after Theorem 7.2.4, every CM-extension E/K with relative class number one admits unary hermitian lattices with class number one. However, already the list of all such extensions E/K is currently unknown, see [LK06] for an overview of that problem.

8.2 The binary case

In this section, suppose that $m = 2$. If (V, Φ) admits an $\mathcal{O}$-lattice L of class number at most 2, then Proposition 6.3.6 shows that

$$\mathrm{d}_K^{1/n} \leq \left(2^{1/n} \cdot 4\pi^2\right)^{2/(m^2-1)} \leq \begin{cases} 14.61 & \text{if } n = 2, \\ 13.53 & \text{if } n \geq 3. \end{cases}$$

A complete list of all such fields K is available from [Voi08].

Let χ be the non-trivial character of $\mathrm{Gal}(E/K)$. Siegel's mass formula 4.2.7 shows that

$$\begin{aligned} h(L) &\geq \#\mu(E) \cdot \mathrm{Mass}(L) = \#\mu(E) \cdot 2(8\pi^3)^{-n} \cdot \mathrm{d}_K^2 \cdot \mathfrak{L}_K(\chi, 1) \cdot \zeta_K(2) \prod_{\mathfrak{p} \in \mathbb{P}(\mathfrak{o})} \lambda(L_\mathfrak{p}) \\ &\geq \#\mu(E) \cdot 2(8\pi^3)^{-n} \cdot \mathrm{d}_K^2 \cdot \mathfrak{L}_K(\chi, 1) \cdot \zeta_K(2) \qquad (8.2.1) \\ &= (2\pi)^{-2n} \frac{2 \cdot \#\,\mathrm{Cl}(E)}{Q \cdot \#\,\mathrm{Cl}(K)} \cdot \mathrm{d}_K^{3/2} \cdot \zeta_K(2)\,. \end{aligned}$$

where $Q \in \{1, 2\}$ denotes the Hasse unit index of E/K. In particular, the above inequality (which is sharp for some lattices L) does not involve the relative discriminant $\mathrm{d}_{E/K}$. So for $m = 2$, the enumeration of all possible CM-fields E/K that might occur is a relative class number problem. Even the most recent bounds on relative class numbers do not allow the enumeration of all possible fields E in practise (although they show that it is indeed a finite problem).

To see how bad the situation is, let $K = \mathbb{Q}(\sqrt{5})$. By [Has85, Satz 25], the Hasse unit index of E/K is always 1. Thus equation 8.2.1 shows that

$$\#\,\mathrm{Cl}(E) \leq \frac{16\pi^4}{\zeta_K(2) \cdot 5^{3/2}} = 120\,.$$

Assuming for a moment that $E/\mathbb{Q}$ is cyclic, [Lou06, Corollary 20] shows that

$$120 \geq \#\,\mathrm{Cl}(E) \geq \frac{2}{3\exp(1)\pi^2} \cdot \frac{\sqrt{\mathrm{d}_E/5}}{(\log(\mathrm{d}_E/5)/2 + 2 + \gamma - \log(4\pi))^2}$$

where γ denotes the Euler-Mascheroni constant. Hence $\sqrt{\mathrm{d}_E/5} < 9.163 \cdot 10^5$ and thus $\mathrm{d}_E < 4.198 \cdot 10^{12}$. So a complete enumeration of all such extensions E/K is simply impossible. Also note that without the assumption that $E/\mathbb{Q}$ is cyclic, the bounds on d_E get much worse, see for example [Lou06, Theorems 28 and 31].

However for $K = \mathbb{Q}$, the classification of all possible extension $E/\mathbb{Q}$ is indeed possible. In this case, equation 8.2.1 shows that

$$\#\,\mathrm{Cl}(E) \leq 4\pi^2/\zeta_\mathbb{Q}(2) = 48\,.$$

The imaginary quadratic number fields of class number at most 48 have been enumerated by M. Watkins in his thesis [Wat04]. He shows that $\mathrm{d}_E \leq 462\,883$. An explicit search in `Magma` shows that there are 10 153 such fields.

If one applies Algorithm 6.5.4 to all these fields E, one obtains the genera of binary definite hermitian forms with class number one or two. Table 8.1 gives the absolute value of the discriminants d_E as well as the number of similarity classes of genera with class number one or two over E. A complete list is available from [Kir16].

Table 8.1: The imaginary quadratic fields E that admit definite, binary hermitian lattices with class number one or two.

d_E	$\#h = 1$	$\#h = 2$	d_E	$\#h = 1$	$\#h = 2$	d_E	$\#h = 1$	$\#h = 2$
3	19	36	4	17	34	7	14	18
8	18	28	11	18	20	15	13	24
19	16	38	20	15	21	24	25	32
35	11	29	39	0	8	40	18	35
43	18	44	51	16	55	52	17	39
55	0	4	56	0	9	67	18	52
68	0	13	84	12	45	88	14	38
91	3	31	115	9	40	120	17	42
123	16	58	132	15	36	136	0	10
148	16	43	155	0	9	163	18	52
168	14	40	184	0	11	187	2	20
195	0	49	203	0	2	219	0	10
228	12	41	232	13	34	235	9	44
259	0	2	260	0	5	264	0	13
267	16	55	276	0	14	280	5	31
291	0	10	292	0	15	308	0	1
312	14	32	328	0	13	340	5	30
355	0	9	372	12	44	388	0	14
403	1	23	408	12	29	420	0	30
427	2	32	435	0	40	456	0	14
483	0	28	520	5	26	532	0	27
552	0	12	555	0	46	564	0	14
568	0	14	580	0	5	595	0	13
616	0	1	627	0	19	660	0	25
708	14	42	715	0	12	723	0	10
760	5	23	763	0	2	772	0	15
795	0	40	820	0	5	840	0	28
852	0	14	955	0	9	1012	1	17
1027	0	1	1032	0	14	1060	0	5
1092	0	16	1128	0	12	1227	0	10
1240	0	5	1243	0	2	1320	0	27
1380	0	24	1428	0	17	1435	0	13
1507	0	2	1540	0	7	1555	0	9
1672	0	1	1752	0	14	1780	0	5
1848	0	16	1992	0	12	2020	0	5

8.3 The general case

Finally suppose that the rank m of (V, Φ) is at least 3.

Definition 8.3.1 Let G be a genus of $\mathcal{O}$-lattices in (V, Φ) and let $L \in G$.

1. Suppose $L_\mathfrak{p} = \perp_{i=1}^t L_i$ is a Jordan decomposition of L at some prime ideal $\mathfrak{p}$ of $\mathfrak{o}$. Let $\mathfrak{P}$ be the largest ideal of $\mathcal{O}$ over $\mathfrak{p}$ that is invariant under the involution $\overline{}$. Then $\mathfrak{s}(L_i) = \mathfrak{P}^{s_i}$ for some integers $s_1 < s_2 < \ldots < s_t$.

   a) If $\mathfrak{p}$ is good, the *local genus symbol* of $L_\mathfrak{p}$ is the tuple

   $$({s_1}_{\pm}^{\mathrm{rank}(L_1)}, \ldots, {s_t}_{\pm}^{\mathrm{rank}(L_t)})$$

   where the i-th subscript is determined as follows: If $\mathrm{disc}(L_i) \in \mathrm{N}(E_\mathfrak{p}^*)$, then $+$ is written, otherwise $-$ is written.
   Proposition 3.3.5 and Theorem 3.3.6 show that the local genus symbol is well defined and it determines the isomorphism class of $L_\mathfrak{p}$ is uniquely. For example, (0_-^m) denotes a unimodular lattice $L_\mathfrak{p}$ of rank m such that $\mathrm{disc}(L_\mathfrak{p})$ is not a local norm (at a place $\mathfrak{p}$ that is necessarily ramified in E). Note that if $E_\mathfrak{p}/K_\mathfrak{p}$ is unramified, then the subscripts can be recovered from $\mathfrak{s}(L_i)$ and $\mathrm{rank}(L_i)$. Hence they can be safely omitted at such places.

   b) If $\mathfrak{p}$ is bad, then the local genus symbol of $L_\mathfrak{p}$ is the tuple

   $$({s_1}_{\pm,\mathrm{ord}_\mathfrak{p}(\mathfrak{n}(L_1))}^{\mathrm{rank}(L_1)}, \ldots, {s_t}_{\pm,\mathrm{ord}_\mathfrak{p}(\mathfrak{n}(L_t))}^{\mathrm{rank}(L_t)})$$

   where the sign is chosen depending on $\mathrm{disc}(L_i)$ just as before. Note that in these cases, the local genus symbol is *not* well defined, i.e. it does depend on the chosen Jordan splitting. However, given any local genus symbol, Corollary 3.3.20 allows the reader to write down an $\mathcal{O}_\mathfrak{p}$-lattice locally isometric to $L_\mathfrak{p}$ explicitly. Further, Theorem 3.3.18 can be used to decide whether two local genus symbols define the same isometry class.

   In both cases, superscripts being equal to 1 will be omitted.

2. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be the prime ideals of $\mathfrak{o}$ which ramify in E or at which L is locally not unimodular. Let g_i be a local genus symbol of L at $\mathfrak{p}_i$. Then the *genus symbol* $[{g_1}_{\mathfrak{p}_1}; \ldots; {g_s}_{\mathfrak{p}_s}]$ determines G.

Corollary 6.3.7 and Remark 6.3.8 list all possible fields E and ranks $m \geq 3$ such that E could admit a definite $\mathcal{O}$-lattice of rank m and class number at most 2. Applying Algorithm 6.5.4 to the possible combinations (E, m), yields the following result.

Theorem 8.3.2 *Let E/K be a CM-extension of number fields. If G is a genus of definite hermitian lattices over E of rank $m \geq 3$ and class number at most two, then $m \leq 9$. A complete list of all such genera is given below and is also electronically available [Kir16].*

For any similarity class of genera as in Theorem 8.3.2, the table below lists the following information.

- The rank m.
- The extension E/K. For any positive integer r, let $\zeta_r \in \mathbb{C}$ denote some primitive r-th root of unity. So $\mathbb{Q}(\theta_r)$ with $\theta_r := \zeta_r + \zeta_r$ is the maximal totally real subfield of the r-th cyclotomic field $\mathbb{Q}(\zeta_r)$.
- A genus symbol of some genus G in the similarity class. Here $\mathfrak{p}_p$ denotes a prime ideal of $\mathfrak{o}$ over p. This ideal will be unique, except if $p = 11$ and $K = \mathbb{Q}(\sqrt{5})$. In this case the two prime ideals over 11 are labeled $\mathfrak{p}_{11,1}$ and $\mathfrak{p}_{11,2}$.
- The last column lists the factored orders of $\mathrm{Aut}(L)$ where L ranges over a system of representatives of the isometry classes of G. Thus this column tells the class number and the mass of G.

The similarity classes of genera are grouped by equivalence classes with respect to the equivalence relation from Definition 6.2.3.

m	E/K	genus symbol of G	$\#\,\mathrm{Aut}(L_i)$
3	$\mathbb{Q}(\sqrt{-2})$	$[(0_+, 1^2_{-,2})_2] \sim [(1^2_{-,2}, 2_+)_2]$	2^5
		$[(0_-, 3^2_{+,6})_2] \sim [(1^2_{+,4}, 4_-)_2]$	2^5
		$[(0_-, 5^2_{+,8})_2] \sim [(1^2_{+,4}, 6_-)_2]$	2^3
		$[(0_-, 7^2_{+,10})_2] \sim [(1^2_{+,4}, 8_-)_2]$	2
		$[(0^3_-)_2]$	$2^4 \cdot 3$ & $2^5 \cdot 3$
		$[(0^2_{-,0}, 2_+)_2] \sim [(0_+, 2^2_{-,2})_2]$	2^4 & 2^5
		$[(0^2_{-,2}, 2_+)_2] \sim [(0_+, 2^2_{-,4})_2]$	$2^4 \cdot 3$ & $2^5 \cdot 3$
		$[(0^2_{+,2}, 4_-)_2] \sim [(0_-, 4^2_{+,6})_2]$	2^4 & 2^5
		$[(0^2_{-,2}, 4_+)_2] \sim [(0_+, 4^2_{-,6})_2]$	$2^4 \cdot 3$ & $2^5 \cdot 3$
		$[(0^2_{+,2}, 6_-)_2] \sim [(0_-, 6^2_{+,8})_2]$	2^2 & 2^3
		$[(0_+, 3^2_{-,4})_2] \sim [(1^2_{-,2}, 4_+)_2]$	2^4 & 2^5
		$[(0_-, 5^2_{+,6})_2] \sim [(1^2_{+,2}, 6_-)_2]$	2^3 & 2^4
	$\mathbb{Q}(\sqrt{-1})$	$[(0^3_-)_2]$	$2^7 \cdot 3$
		$[(0_-, 1^2_{+,2})_2] \sim [(1^2_{-,2}, 2_+)_2]$	$2^7 \cdot 3$
		$[(0^2_{+,2}, 2_-)_2] \sim [(0_-, 2^2_{+,4})_2]$	$2^7 \cdot 3$
		$[(0^2_{-,0}, 2_+)_2] \sim [(0_+, 2^2_{-,2})_2]$	2^7

m	E/K	genus symbol of G	$\# \operatorname{Aut}(L_i)$
		$[(0^2_{+,2}, 4_-)_2] \sim [(0_-, 4^2_{+,6})_2]$	$2^5 \cdot 3$
		$[(0^2_{+,0}, 4_-)_2] \sim [(0_-, 4^2_{+,4})_2]$	2^6
		$[(0^2_{+,2}, 6_-)_2] \sim [(0_-, 6^2_{+,8})_2]$	$2^3 \cdot 3$
		$[(0_-, 3^2_{+,4})_2] \sim [(1^2_{+,2}, 4_-)_2]$	2^7
		$[(0_+, 3^2_{-,4})_2] \sim [(1^2_{-,2}, 4_+)_2]$	$2^7 \cdot 3$
		$[(0_-, 5^2_{+,6})_2] \sim [(1^2_{+,2}, 6_-)_2]$	2^5
		$[(0^3_-)_2; (0, 1^2)_3] \sim [(0^3_+)_2; (0^2, 1)_3]$	$2^5 \cdot 3$ & 2^7
		$[(0_-, 1^2_{+,2})_2; (0, 1^2)_3] \sim [(0_+, 1^2_{+,2})_2; (0^2, 1)_3] \sim$ $[(1^2_{-,2}, 2_+)_2; (0, 1^2)_3] \sim [(1^2_{+,2}, 2_+)_2; (0^2, 1)_3]$	2^6 & $2^7 \cdot 3$
		$[(0^2_{-,0}, 4_+)_2] \sim [(0_+, 4^2_{-,4})_2]$	2^7 & 2^7
		$[(0_+, 2_+, 4_+)_2]$	2^6 & 2^6
		$[(0^2_{+,0}, 6_-)_2] \sim [(0_-, 6^2_{+,6})_2]$	2^5 & 2^5
		$[(0^2_{+,2}, 8_-)_2] \sim [(0_-, 8^2_{+,10})_2]$	2^3 & $2^3 \cdot 3$
		$[(0_+, 5^2_{-,6})_2] \sim [(1^2_{-,2}, 6_+)_2]$	2^7 & $2^7 \cdot 3$
		$[(0_-, 7^2_{+,8})_2] \sim [(1^2_{+,2}, 8_-)_2]$	2^4 & 2^4
		$[(0^2_{+,2}, 2_-)_2; (0, 1^2)_3] \sim [(0_-, 2^2_{+,4})_2; (0, 1^2)_3] \sim$ $[(0^2_{+,2}, 2_+)_2; (0^2, 1)_3] \sim [(0_+, 2^2_{+,4})_2; (0^2, 1)_3]$	$2^5 \cdot 3$ & 2^7
		$[(0_+, 3^2_{-,4})_2; (0, 1^2)_3] \sim [(1^2_{-,2}, 4_+)_2; (0, 1^2)_3] \sim$ $[(0_-, 3^2_{-,4})_2; (0^2, 1)_3] \sim [(1^2_{-,2}, 4_-)_2; (0^2, 1)_3]$	2^6 & $2^7 \cdot 3$
	$\mathbb{Q}(\sqrt{-3})$	$[(0^3_-)_3]$	$2^4 \cdot 3^4$
		$[(0_-, 1^2_+)_3] \sim [(1^2_+, 2_-)_3]$	$2^4 \cdot 3^4$
		$[(0, 1^2)_2; (0^3_-)_3] \sim [(0^2, 1)_2; (0^3_+)_3]$	$2^4 \cdot 3^3$
		$[(0, 1^2)_2; (0_-, 1^2_+)_3] \sim [(0^2, 1)_2; (0_+, 1^2_+)_3] \sim [(0, 1^2)_2; (1^2_+, 2_-)_3] \sim$ $[(0^2, 1)_2; (1^2_+, 2_+)_3]$	$2^4 \cdot 3^3$
		$[(0_+, 2^2_-)_3] \sim [(0^2_-, 2_+)_3]$	$2^4 \cdot 3^3$
		$[(0_-, 2^2_+)_3] \sim [(0^2_+, 2_-)_3]$	$2^3 \cdot 3^3$
		$[(0_-, 2_+, 4_-)_3]$	$2^3 \cdot 3^2$
		$[(0, 2^2)_2; (0_-, 1^2_+)_3] \sim [(0^2, 2)_2; (0_-, 1^2_+)_3] \sim [(0, 2^2)_2; (1^2_+, 2_-)_3] \sim$ $[(0^2, 2)_2; (1^2_+, 2_-)_3]$	$2^2 \cdot 3^3$

m	E/K	genus symbol of G	$\#\operatorname{Aut}(L_i)$
		$[(0_-,3^2_+)_3] \sim [(1^2_+,4_-)_3]$	$2^4\cdot 3^2$
		$[(0,1,2)_2;(0^3_+)_3]$	$2^3\cdot 3^3$
		$[(0^3_-)_3;(0,1^2)_5] \sim [(0^3_+)_3;(0^2,1)_5]$	$2^3\cdot 3^2$ \& $2^4\cdot 3^3$
		$[(0_-,1^2_+)_3;(0,1^2)_5] \sim [(0_+,1^2_+)_3;(0^2,1)_5] \sim [(1^2_+,2_-)_3;(0,1^2)_5] \sim$ $[(1^2_+,2_+)_3;(0^2,1)_5]$	$2^2\cdot 3^3$ \& $2^4\cdot 3^2$
		$[(0,2^2)_2;(0^3_-)_3] \sim [(0^2,2)_2;(0^3_-)_3]$	$2^4\cdot 3^2$ \& $2^4\cdot 3^3$
		$[(0_-,4^2_+)_3] \sim [(0^2_+,4_-)_3]$	$2^2\cdot 3^2$ \& $2^3\cdot 3^2$
		$[(0_+,2_+,4_+)_3]$	$2^2\cdot 3^3$ \& $2^3\cdot 3^3$
		$[(0_-,2_-,4_+)_3] \sim [(0_+,2_-,4_-)_3]$	$2^2\cdot 3^3$ \& $2^3\cdot 3^3$
		$[(0,2,4)_2;(0_-,1^2_+)_3] \sim [(0,2,4)_2;(1^2_+,2_-)_3]$	$2\cdot 3^2$ \& $2\cdot 3^3$
		$[(0,2^2)_2;(0_-,3^2_+)_3] \sim [(0^2,2)_2;(0_-,3^2_+)_3] \sim [(0,2^2)_2;(1^2_+,4_-)_3] \sim$ $[(0^2,2)_2;(1^2_+,4_-)_3]$	$2\cdot 3^2$ \& $2^2\cdot 3^2$
		$[(0_-,5^2_+)_3] \sim [(1^2_+,6_-)_3]$	$2\cdot 3^2$ \& $2^4\cdot 3^2$
		$[(0,1,3)_2;(0^3_-)_3] \sim [(0,2,3)_2;(0^3_+)_3]$	$2^3\cdot 3^2$ \& $2^3\cdot 3^3$
		$[(0,1^2)_2;(0_+,2^2_-)_3] \sim [(0,1^2)_2;(0^2_-,2_+)_3] \sim [(0^2,1)_2;(0_-,2^2_-)_3] \sim$ $[(0^2,1)_2;(0^2_-,2_-)_3]$	$2^3\cdot 3^3$ \& $2^4\cdot 3^3$
		$[(0,1^2)_2;(0_-,2^2_+)_3] \sim [(0,1^2)_2;(0^2_+,2_-)_3] \sim [(0^2,1)_2;(0_+,2^2_+)_3] \sim$ $[(0^2,1)_2;(0^2_+,2_+)_3]$	$2^2\cdot 3^3$ \& $2^3\cdot 3^3$
		$[(0,3^2)_2;(0_-,1^2_+)_3] \sim [(0,3^2)_2;(1^2_+,2_-)_3] \sim [(0^2,3)_2;(0_+,1^2_+)_3] \sim$ $[(0^2,3)_2;(1^2_+,2_+)_3]$	$2^2\cdot 3^2$ \& $2^2\cdot 3^3$
		$[(0,1^2)_2;(0_-,3^2_+)_3] \sim [(0,1^2)_2;(1^2_+,4_-)_3] \sim [(0^2,1)_2;(0_+,3^2_+)_3] \sim$ $[(0^2,1)_2;(1^2_+,4_+)_3]$	$2\cdot 3^3$ \& $2^4\cdot 3^3$
		$[(0,1,2)_2;(0_-,2^2_-)_3] \sim [(0,1,2)_2;(0^2_-,2_-)_3]$	$2^2\cdot 3^3$ \& $2^3\cdot 3^3$
		$[(0,1,2)_2;(0_+,1^2_+)_3] \sim [(0,1,2)_2;(1^2_+,2_+)_3]$	$2^4\cdot 3^3$ \& $2^4\cdot 3^3$
	$\mathbb{Q}(\sqrt{-5})$	$[(0^3_-)_2;(0_+,1^2_+)_5] \sim [(0^3_+)_2;(0_-,1^2_+)_5] \sim [(0^3_-)_2;(1^2_+,2_+)_5] \sim$ $[(0^3_+)_2;(1^2_+,2_-)_5]$	2^2 \& 2^4
		$[(0^2_{+,2},2_-)_2;(0_+,1^2_+)_5] \sim [(0_-,2^2_{+,4})_2;(0_+,1^2_+)_5] \sim$ $[(0^2_{+,2},2_-)_2;(1^2_+,2_+)_5] \sim [(0_-,2^2_{+,4})_2;(1^2_+,2_+)_5] \sim$ $[(0^2_{+,2},2_+)_2;(0_-,1^2_+)_5] \sim [(0_+,2^2_{+,4})_2;(0_-,1^2_+)_5] \sim$ $[(0^2_{+,2},2_+)_2;(1^2_+,2_-)_5] \sim [(0_+,2^2_{+,4})_2;(1^2_+,2_-)_5]$	2^2 \& 2^4

m	E/K	genus symbol of G	$\#\,\mathrm{Aut}(L_i)$
	$\mathbb{Q}(\sqrt{-15})$	$[(0_-,1^2_+)_3;(0_+,1^2_+)_5] \sim [(0_+,1^2_+)_3;(0_-,1^2_+)_5] \sim [(1^2_+,2_-)_3;(0_+,1^2_+)_5] \sim [(0_-,1^2_+)_3;(1^2_+,2_+)_5] \sim [(1^2_+,2_-)_3;(1^2_+,2_+)_5] \sim [(1^2_+,2_+)_3;(0_-,1^2_+)_5] \sim [(0_+,1^2_+)_3;(1^2_+,2_-)_5] \sim [(1^2_+,2_+)_3;(1^2_+,2_-)_5]$	$2\cdot 3$
		$[(0^3_-)_3;(0_+,1^2_+)_5] \sim [(0^3_+)_3;(0_-,1^2_+)_5] \sim [(0^3_-)_3;(1^2_+,2_+)_5] \sim [(0^3_+)_3;(1^2_+,2_-)_5]$	2^3 & $2^3\cdot 3$
		$[(0_-,1^2_+)_3;(0^3_+)_5] \sim [(0_+,1^2_+)_3;(0^3_-)_5] \sim [(1^2_+,2_-)_3;(0^3_+)_5] \sim [(1^2_+,2_+)_3;(0^3_-)_5]$	$2^2\cdot 3$ & $2^2\cdot 3$
	$\mathbb{Q}(\sqrt{-7})$	$[(0_-,1^2_+)_7] \sim [(1^2_+,2_-)_7]$	$2\cdot 3\cdot 7$
		$[(0,1^2)_2;(0_-,1^2_+)_7] \sim [(0^2,1)_2;(0_-,1^2_+)_7] \sim [(0,1^2)_2;(1^2_+,2_-)_7] \sim [(0^2,1)_2;(1^2_+,2_-)_7]$	$2\cdot 3$
		$[(0^3_-)_7]$	$2^4\cdot 3$ & $2^4\cdot 3\cdot 7$
		$[(0,1^2)_3;(0_-,1^2_+)_7] \sim [(0^2,1)_3;(0_+,1^2_+)_7] \sim [(0,1^2)_3;(1^2_+,2_-)_7] \sim [(0^2,1)_3;(1^2_+,2_+)_7]$	2^3 & $2^3\cdot 3$
		$[(0,2^2)_2;(0_-,1^2_+)_7] \sim [(0^2,2)_2;(0_-,1^2_+)_7] \sim [(0,2^2)_2;(1^2_+,2_-)_7] \sim [(0^2,2)_2;(1^2_+,2_-)_7]$	2 & $2\cdot 3$
		$[(0,1,2)_2;(0_-,1^2_+)_7] \sim [(0,1,2)_2;(1^2_+,2_-)_7]$	2 & 2
	$\mathbb{Q}(\sqrt{-11})$	$[(0_-,1^2_+)_{11}] \sim [(1^2_+,2_-)_{11}]$	2^4
		$[(0^3_-)_{11}]$	$2^3\cdot 3$ & $2^4\cdot 3$
		$[(0,1^2)_2;(0_-,1^2_+)_{11}] \sim [(0^2,1)_2;(0_+,1^2_+)_{11}] \sim [(0,1^2)_2;(1^2_+,2_-)_{11}] \sim [(0^2,1)_2;(1^2_+,2_+)_{11}]$	$2\cdot 3$ & $2^4\cdot 3$
		$[(0,2^2)_2;(0_-,1^2_+)_{11}] \sim [(0^2,2)_2;(0_-,1^2_+)_{11}] \sim [(0,2^2)_2;(1^2_+,2_-)_{11}] \sim [(0^2,2)_2;(1^2_+,2_-)_{11}]$	2 & 2^2
	$\mathbb{Q}(\sqrt{-19})$	$[(0_-,1^2_+)_{19}] \sim [(1^2_+,2_-)_{19}]$	$2\cdot 3$ & 2^4
	$\mathbb{Q}(\sqrt{5})(\sqrt{-1})$	$[(0_+,1^2_{+,2})_{\mathfrak{p}_2}] \sim [(1^2_{+,2},2_+)_{\mathfrak{p}_2}]$	$2^6\cdot 3$ & $2^7\cdot 3$
	$\mathbb{Q}(\sqrt{5})(\sqrt{(\sqrt{5}-5)/2})$	$[(0^3_+)_{\mathfrak{p}_5}]$	$2^4\cdot 3\cdot 5^3$
		$[(0_+,1^2_+)_{\mathfrak{p}_5}] \sim [(1^2_+,2_+)_{\mathfrak{p}_5}]$	$2^4\cdot 3\cdot 5^3$
		$[(0,1^2)_{\mathfrak{p}_2};(0^3_+)_{\mathfrak{p}_5}] \sim [(0^2,1)_{\mathfrak{p}_2};(0^3_-)_{\mathfrak{p}_5}]$	$2^3\cdot 3\cdot 5^2$ & $2^4\cdot 5^3$

m	E/K	genus symbol of G	$\#\operatorname{Aut}(L_i)$
		$[(0,1^2)_{\mathfrak{p}_2};(0_+,1^2_+)_{\mathfrak{p}_5}] \sim [(0^2,1)_{\mathfrak{p}_2};(0_-,1^2_+)_{\mathfrak{p}_5}] \sim$ $[(0,1^2)_{\mathfrak{p}_2};(1^2_+,2_+)_{\mathfrak{p}_5}] \sim [(0^2,1)_{\mathfrak{p}_2};(1^2_+,2_-)_{\mathfrak{p}_5}]$	$2^2\cdot 5^3$ & $2^4\cdot 3\cdot 5^3$
		$[(0_+,2^2_+)_{\mathfrak{p}_5}] \sim [(0^2_+,2_+)_{\mathfrak{p}_5}]$	$2^2\cdot 5^3$ & $2^4\cdot 5^3$
		$[(0_-,2^2_-)_{\mathfrak{p}_5}] \sim [(0^2_-,2_-)_{\mathfrak{p}_5}]$	$2^3\cdot 5^3$ & $2^2\cdot 3\cdot 5^3$
		$[(0_+,3^2_+)_{\mathfrak{p}_5}] \sim [(1^2_+,4_+)_{\mathfrak{p}_5}]$	$2\cdot 5^3$ & $2^4\cdot 3\cdot 5^3$
	$\mathbb{Q}(\sqrt{5})(\sqrt{-3})$	$[(0^3_+)_{\mathfrak{p}_3}]$	$2^4\cdot 3^4$ & $2^4\cdot 3^3\cdot 5$
		$[(0_+,1^2_+)_{\mathfrak{p}_3}] \sim [(1^2_+,2_+)_{\mathfrak{p}_3}]$	$2^4\cdot 3^4$ & $2^4\cdot 3^3\cdot 5$
	$\mathbb{Q}(\sqrt{2})(\sqrt{-1})$	$[(0_+,1^2_{+,2})_{\mathfrak{p}_2}] \sim [(1^2_{+,2},2_+)_{\mathfrak{p}_2}]$	2^{10}
		$[(0_-,3^2_{-,4})_{\mathfrak{p}_2}] \sim [(1^2_{-,2},4_-)_{\mathfrak{p}_2}]$	2^{10}
		$[(0_-,5^2_{-,6})_{\mathfrak{p}_2}] \sim [(1^2_{-,2},6_-)_{\mathfrak{p}_2}]$	2^8
		$[(0^3_+)_{\mathfrak{p}_2}]$	$2^9\cdot 3$ & $2^{10}\cdot 3$
		$[(0^2_{-,0},2_-)_{\mathfrak{p}_2}] \sim [(0_-,2^2_{-,2})_{\mathfrak{p}_2}]$	2^9 & 2^{10}
		$[(0^2_{+,2},2_+)_{\mathfrak{p}_2}] \sim [(0_+,2^2_{+,4})_{\mathfrak{p}_2}]$	$2^9\cdot 3$ & $2^{10}\cdot 3$
		$[(0^2_{-,0},4_-)_{\mathfrak{p}_2}] \sim [(0_-,4^2_{-,4})_{\mathfrak{p}_2}]$	2^8 & 2^9
		$[(0_+,3^2_{+,4})_{\mathfrak{p}_2}] \sim [(1^2_{+,2},4_+)_{\mathfrak{p}_2}]$	2^9 & 2^{10}
		$[(0_-,7^2_{-,8})_{\mathfrak{p}_2}] \sim [(1^2_{-,2},8_-)_{\mathfrak{p}_2}]$	2^7 & 2^7
	$\mathbb{Q}(\sqrt{3})(\sqrt{-1})$	$[]$	$2^7\cdot 3^4$
		$[(0,1^2)_{\mathfrak{p}_2}] \sim [(1^2,2)_{\mathfrak{p}_2}]$	$2^7\cdot 3^3$
		$[(1,2,3)_{\mathfrak{p}_2}]$	$2^6\cdot 3^3$
		$[(0,1^2)_{\mathfrak{p}_3}] \sim [(1^3)_{\mathfrak{p}_2};(0^2,1)_{\mathfrak{p}_3}]$	$2^5\cdot 3^4$ & $2^7\cdot 3^3$
		$[(0,1^2)_{\mathfrak{p}_2};(0,1^2)_{\mathfrak{p}_3}] \sim [(0^2,1)_{\mathfrak{p}_2};(0^2,1)_{\mathfrak{p}_3}] \sim [(1^2,2)_{\mathfrak{p}_2};(0,1^2)_{\mathfrak{p}_3}] \sim$ $[(1,2^2)_{\mathfrak{p}_2};(0^2,1)_{\mathfrak{p}_3}]$	$2^6\cdot 3^2$ & $2^7\cdot 3^3$
		$[(0,2^2)_{\mathfrak{p}_2}] \sim [(0^2,2)_{\mathfrak{p}_2}]$	$2^7\cdot 3^2$ & $2^7\cdot 3^3$
		$[(0,1,3)_{\mathfrak{p}_2}] \sim [(1,3,4)_{\mathfrak{p}_2}]$	$2^6\cdot 3^2$ & $2^6\cdot 3^3$
		$[(1,4,5)_{\mathfrak{p}_2}] \sim [(1,2,5)_{\mathfrak{p}_2}]$	$2^4\cdot 3^2$ & $2^4\cdot 3^3$
		$[(1,2,3)_{\mathfrak{p}_2};(0,1^2)_{\mathfrak{p}_3}] \sim [(0,1,2)_{\mathfrak{p}_2};(0^2,1)_{\mathfrak{p}_3}]$	$2^5\cdot 3^2$ & $2^6\cdot 3^3$
		$[(1^3)_{\mathfrak{p}_2};(0,1,2)_{\mathfrak{p}_3}]$	$2^4\cdot 3^3$ & $2^6\cdot 3^2$
	$\mathbb{Q}(\sqrt{21})(\sqrt{(\sqrt{21}-5)/2})$	$[]$	$2^4\cdot 3^2\cdot 7$ & $2^4\cdot 3^4$
	$\mathbb{Q}(\sqrt{6})(\sqrt{2\sqrt{6}-5})$	$[(0,1^2)_{\mathfrak{p}_2}] \sim [(1^2,2)_{\mathfrak{p}_2}]$	$2^4\cdot 3^2$ & $2^5\cdot 3^2$

m	E/K	genus symbol of G	$\#\operatorname{Aut}(L_i)$
	$\mathbb{Q}(\theta_7)(\sqrt{\theta_7-2})$	$[(0_-,1^2_+)_{\mathfrak{p}_7}] \sim [(1^2_+,2_-)_{\mathfrak{p}_7}]$	$2\cdot 3\cdot 7^3$
		$[(0^3_-)_{\mathfrak{p}_7}]$	$2^4\cdot 3\cdot 7^2$ & $2^4\cdot 3\cdot 7^3$
	$\mathbb{Q}(\theta_9)(\sqrt{\theta_9-2})$	$[(0^3_-)_{\mathfrak{p}_3}]$	$2^2\cdot 3^6$ & $2^4\cdot 3^7$
		$[(0_-,1^2_+)_{\mathfrak{p}_3}] \sim [(1^2_+,2_-)_{\mathfrak{p}_3}]$	$2^4\cdot 3^5$ & $2^2\cdot 3^7$
		$[(0_+,2^2_-)_{\mathfrak{p}_3}] \sim [(0^2_-,2_+)_{\mathfrak{p}_3}]$	$2^2\cdot 3^5$ & $2^4\cdot 3^6$
	$\mathbb{Q}(\theta_{15})(\sqrt{\theta_{15}-2})$	$[]$	$2^4\cdot 3^3\cdot 5^2$ & $2^4\cdot 3^4\cdot 5^3$
4	$\mathbb{Q}(\sqrt{-2})$	$[(0^2_{+,2},1^2_{+,4})_2] \sim [(1^2_{+,4},2^2_{+,4})_2]$	2^9
		$[(1^4_{+,4})_2]$	$2^8\cdot 3\cdot 5$
		$[(1^4_{+,2})_2]$	2^9
		$[(0^2_{+,2},3^2_{+,6})_2] \sim [(1^2_{+,4},4^2_{+,6})_2]$	2^5
		$[(1^2_{+,4},3^2_{+,6})_2]$	$2^6\cdot 3$
		$[(1^2_{+,4},5^2_{+,8})_2]$	$2^2\cdot 3$
		$[(1^4_{+,4})_2;(0,1^3)_3] \sim [(1^4_{+,4})_2;(0^3,1)_3]$	$2^5\cdot 3$
		$[(1^2_{+,4},3^2_{+,4})_2] \sim [(1^2_{+,2},3^2_{+,6})_2]$	2^7
		$[(0^4_{+,2})_2]$	$2^8\cdot 3^2$ & $2^9\cdot 3^2$
		$[(0^2_{+,2},1^2_{+,2})_2] \sim [(1^2_{+,2},2^2_{+,4})_2]$	$2^7\cdot 3$ & $2^8\cdot 3$
		$[(0^2_{+,0},1^2_{+,2})_2] \sim [(1^2_{+,2},2^2_{+,2})_2]$	2^7 & 2^7
		$[(0^2_{+,2},2^2_{+,4})_2]$	2^7 & 2^8
		$[(0^2_{-,2},2^2_{-,4})_2]$	$2^7\cdot 3^2$ & $2^8\cdot 3^2$
		$[(0^2_{+,2},5^2_{+,8})_2] \sim [(1^2_{+,4},6^2_{+,8})_2]$	2^2 & 2^2
		$[(0^2_{+,2},1^2_{+,4})_2;(0,1^3)_3] \sim [(0^2_{+,2},1^2_{+,4})_2;(0^3,1)_3] \sim$ $[(1^2_{+,4},2^2_{+,4})_2;(0,1^3)_3] \sim [(1^2_{+,4},2^2_{+,4})_2;(0^3,1)_3]$	2^4 & 2^6
		$[(1^2_{+,4},3^2_{+,6})_2;(0,1^3)_3] \sim [(1^2_{+,4},3^2_{+,6})_2;(0^3,1)_3]$	2^3 & $2^2\cdot 3$
		$[(1^4_{+,4})_2;(0,2^3)_3] \sim [(1^4_{+,4})_2;(0^3,2)_3]$	2^2 & 2^5
		$[(0_-,1^2_{+,2},2_+)_2]$	2^6 & 2^6
		$[(1^2_{+,4},5^2_{+,6})_2] \sim [(1^2_{+,2},5^2_{+,8})_2]$	2^4 & 2^4
		$[(1^4_{+,2})_2;(0,1^3)_3] \sim [(1^4_{+,2})_2;(0^3,1)_3]$	2^4 & 2^6
	$\mathbb{Q}(\sqrt{-1})$	$[(0^4_{+,2})_2]$	$2^{10}\cdot 3^2\cdot 5$
		$[(0^2_{+,2},1^2_{+,2})_2] \sim [(1^2_{+,2},2^2_{+,4})_2]$	$2^{11}\cdot 3$

m	E/K	genus symbol of G	$\# \operatorname{Aut}(L_i)$
		$[(1^4_{+,2})_2]$	$2^{11} \cdot 3^2$
		$[(0^4_{+,0})_2]$	$2^{11} \cdot 3$
		$[(0^2_{+,0}, 1^2_{+,2})_2] \sim [(1^2_{+,2}, 2^2_{+,2})_2]$	$2^{10} \cdot 3$
		$[(1^4_{-,2})_2; (0^3, 1)_3] \sim [(1^4_{-,2})_2; (0, 1^3)_3]$	$2^9 \cdot 3$
		$[(0^2_{+,2}, 2^2_{+,4})_2]$	$2^8 \cdot 3^2$
		$[(0^2_{+,2}, 4^2_{+,6})_2]$	$2^4 \cdot 3^2$
		$[(0^2_{+,2}, 3^2_{+,4})_2] \sim [(1^2_{+,2}, 4^2_{+,6})_2]$	$2^7 \cdot 3$
		$[(1^2_{+,2}, 3^2_{+,4})_2]$	2^{10}
		$[(1^2_{-,2}, 3^2_{-,4})_2]$	$2^{10} \cdot 3^2$
		$[(0^2_{+,2}, 2^2_{+,2})_2] \sim [(0^2_{+,0}, 2^2_{+,4})_2]$	$2^9 \cdot 3$
		$[(0_+, 1^2_{+,2}, 2_-)_2]$	$2^9 \cdot 3$
		$[(0^4_{+,2})_2; (0^2, 1^2)_3]$	$2^7 \cdot 3^2$ & $2^9 \cdot 3$
		$[(0^2_{+,2}, 1^2_{-,2})_2; (0^3, 1)_3] \sim [(0^2_{+,2}, 1^2_{-,2})_2; (0, 1^3)_3] \sim$ $[(1^2_{-,2}, 2^2_{+,4})_2; (0^3, 1)_3] \sim [(1^2_{-,2}, 2^2_{+,4})_2; (0, 1^3)_3]$	$2^9 \cdot 3$ & $2^8 \cdot 3^2$
		$[(0^4_{+,2})_2; (0, 2^3)_3] \sim [(0^4_{+,2})_2; (0^3, 2)_3]$	$2^5 \cdot 3$ & $2^8 \cdot 3$
		$[(0^4_{+,2})_2; (0, 1^3)_5] \sim [(0^4_{+,2})_2; (0^3, 1)_5]$	$2^5 \cdot 3 \cdot 5$ & $2^8 \cdot 3$
		$[(0^2_{+,2}, 5^2_{+,6})_2] \sim [(1^2_{+,2}, 6^2_{+,8})_2]$	2^5 & $2^5 \cdot 3$
		$[(1^2_{+,2}, 5^2_{+,6})_2]$	2^7 & 2^7
		$[(1^4_{+,2})_2; (0, 1^3)_5] \sim [(1^4_{+,2})_2; (0^3, 1)_5]$	2^7 & $2^9 \cdot 3$
		$[(0^3_+, 2_-)_2] \sim [(0_-, 2^3_+)_2]$	$2^9 \cdot 3$ & $2^9 \cdot 3$
		$[(0^2_{+,0}, 2^2_{+,2})_2]$	2^{10} & 2^{10}
		$[(0_-, 2^2_{+,4}, 4_+)_2] \sim [(0_+, 2^2_{+,4}, 4_-)_2]$	$2^9 \cdot 3$ & $2^9 \cdot 3$
		$[(0^2_{+,2}, 4^2_{+,4})_2] \sim [(0^2_{+,0}, 4^2_{+,6})_2]$	2^7 & $2^7 \cdot 3$
		$[(0^2_{+,0}, 3^2_{+,4})_2] \sim [(1^2_{+,2}, 4^2_{+,4})_2]$	2^9 & 2^9
		$[(0^2_{-,0}, 3^2_{-,4})_2] \sim [(1^2_{-,2}, 4^2_{-,4})_2]$	2^{10} & $2^{10} \cdot 3$
		$[(0_-, 2_+, 3^2_{+,4})_2] \sim [(1^2_{+,2}, 2_+, 4_-)_2]$	2^9 & $2^9 \cdot 3$
		$[(0_+, 1^2_{+,2}, 4_-)_2] \sim [(0_-, 3^2_{+,4}, 4_+)_2]$	2^9 & $2^9 \cdot 3$
		$[(0_+, 1^2_{-,2}, 4_+)_2] \sim [(0_+, 3^2_{+,4}, 4_-)_2]$	2^9 & $2^9 \cdot 3$
		$[(0_-, 3^2_{-,4}, 6_-)_2]$	2^8 & $2^8 \cdot 3$

m	E/K	genus symbol of G	$\# \operatorname{Aut}(L_i)$
	$\mathbb{Q}(\sqrt{-3})$	$[(0^4_+)_3]$	$2^7 \cdot 3^5$
		$[(0^2_+, 1^2_+)_3] \sim [(1^2_+, 2^2_+)_3]$	$2^5 \cdot 3^5$
		$[(1^4_+)_3]$	$2^7 \cdot 3^5 \cdot 5$
		$[(0^2, 1^2)_2; (1^4_+)_3]$	$2^7 \cdot 3^4$
		$[(0^3, 1)_2; (0^4_-)_3] \sim [(0, 1^3)_2; (0^4_-)_3]$	$2^5 \cdot 3^5$
		$[(0_-, 2^3_+)_3] \sim [(0^3_+, 2_-)_3]$	$2^5 \cdot 3^4$
		$[(0_-, 2_+, 3^2_+)_3] \sim [(1^2_+, 2_+, 4_-)_3]$	$2^5 \cdot 3^3$
		$[(0_+, 1^2_+, 2_-)_3] \sim [(0_-, 1^2_+, 2_+)_3]$	$2^5 \cdot 3^5$
		$[(0, 2^3)_2; (1^4_+)_3] \sim [(0^3, 2)_2; (1^4_+)_3]$	$2^4 \cdot 3^5$
		$[(0^2, 2^2)_2; (1^4_+)_3]$	$2^3 \cdot 3^4$
		$[(1^2_+, 3^2_+)_3]$	$2^6 \cdot 3^3$
		$[(0, 1^2, 2)_2; (1^4_+)_3]$	$2^6 \cdot 3^4$
		$[(0^2, 1^2)_2; (0^4_+)_3]$	$2^7 \cdot 3^3$ & $2^6 \cdot 3^4$
		$[(0^2, 1^2)_2; (0^2_+, 1^2_+)_3] \sim [(0^2, 1^2)_2; (1^2_+, 2^2_+)_3]$	$2^3 \cdot 3^4$ & $2^5 \cdot 3^4$
		$[(0^3, 1)_2; (0^2_-, 1^2_+)_3] \sim [(0, 1^3)_2; (0^2_-, 1^2_+)_3] \sim [(0^3, 1)_2; (1^2_+, 2^2_-)_3] \sim$ $[(0, 1^3)_2; (1^2_+, 2^2_-)_3]$	$2^6 \cdot 3^4$ & $2^5 \cdot 3^5$
		$[(0, 2^3)_2; (0^4_+)_3] \sim [(0^3, 2)_2; (0^4_+)_3]$	$2^5 \cdot 3^3$ & $2^5 \cdot 3^5$
		$[(0_+, 2^3_-)_3] \sim [(0^3_-, 2_+)_3]$	$2^4 \cdot 3^5$ & $2^5 \cdot 3^5$
		$[(0^2_-, 2^2_-)_3]$	$2^5 \cdot 3^4$ & $2^6 \cdot 3^4$
		$[(0^2_+, 2^2_+)_3]$	$2^3 \cdot 3^4$ & $2^4 \cdot 3^4$
		$[(0_+, 2_-, 3^2_+)_3] \sim [(1^2_+, 2_-, 4_+)_3]$	$2^2 \cdot 3^5$ & $2^5 \cdot 3^5$
		$[(0^2_+, 3^2_+)_3] \sim [(1^2_+, 4^2_+)_3]$	$2^2 \cdot 3^3$ & $2^5 \cdot 3^3$
		$[(0_+, 1^2_+, 4_-)_3] \sim [(0_-, 3^2_+, 4_+)_3]$	$2^4 \cdot 3^3$ & $2^5 \cdot 3^3$
		$[(0, 2^2, 4)_2; (1^4_+)_3]$	$2^2 \cdot 3^3$ & $2^2 \cdot 3^4$
		$[(1^4_+)_3; (0, 1^3)_7] \sim [(1^4_+)_3; (0^3, 1)_7]$	$2^4 \cdot 3^3$ & $2^4 \cdot 3^5$
		$[(0, 1^2, 2)_2; (0^4_+)_3]$	$2^6 \cdot 3^3$ & $2^5 \cdot 3^4$
		$[(0^2, 1^2)_2; (0_+, 1^2_+, 2_-)_3] \sim [(0^2, 1^2)_2; (0_-, 1^2_+, 2_+)_3]$	$2^3 \cdot 3^4$ & $2^5 \cdot 3^4$
		$[(0, 2, 3^2)_2; (1^4_+)_3] \sim [(0^2, 1, 3)_2; (1^4_+)_3]$	$2^4 \cdot 3^3$ & $2^4 \cdot 3^4$
		$[(0, 1, 2^2)_2; (0^4_-)_3] \sim [(0^2, 1, 2)_2; (0^4_-)_3]$	$2^5 \cdot 3^3$ & $2^5 \cdot 3^4$

m	E/K	genus symbol of G	$\#\operatorname{Aut}(L_i)$
		$[(0^3,1)_2;(0_+,2_+^3)_3] \sim [(0^3,1)_2;(0_+^3,2_+)_3] \sim [(0,1^3)_2;(0_-,2_-^3)_3] \sim$ $[(0,1^3)_2;(0_-^3,2_-)_3]$	$2^3\cdot 3^4$ & $2^5\cdot 3^4$
		$[(0^3,1)_2;(0_+,1_+^2,2_+)_3] \sim [(0,1^3)_2;(0_-,1_+^2,2_-)_3]$	$2^5\cdot 3^4$ & $2^4\cdot 3^5$
	$\mathbb{Q}(\sqrt{-5})$	$[(0_{+,2}^2,1_{+,2}^2)_2;(1_+^4)_5] \sim [(1_{+,2}^2,2_{+,4}^2)_2;(1_+^4)_5]$	2^5 & 2^7
		$[(0_{+,0}^4)_2;(1_+^4)_5]$	2^5 & 2^7
		$[(1_{-,2}^4)_2;(0_-^4)_5]$	2^4 & 2^5
		$[(0_{+,2}^2,2_{+,2}^2)_2;(1_+^4)_5] \sim [(0_{+,0}^2,2_{+,4}^2)_2;(1_+^4)_5]$	2^3 & 2^5
	$\mathbb{Q}(\sqrt{-15})$	$[(0_+^2,1_+^2)_3;(1_+^4)_5] \sim [(1_+^2,2_+^2)_3;(1_+^4)_5]$	$2\cdot 3^2$
		$[(0_+,1_+^2,2_-)_3;(1_+^4)_5] \sim [(0_-,1_+^2,2_+)_3;(1_+^4)_5]$	$2\cdot 3^2$
		$[(0_+^4)_3;(1_+^4)_5]$	$2^5\cdot 3$ & $2^5\cdot 3^2$
		$[(1_+^4)_3;(1_+^4)_5]$	$2^4\cdot 3^2\cdot 5$ & $2^4\cdot 3^2\cdot 5$
		$[(0,1^3)_2;(1_+^4)_3;(1_+^4)_5] \sim [(0^3,1)_2;(1_+^4)_3;(1_+^4)_5]$	$2^4\cdot 3$ & $2^4\cdot 3$
		$[(0,2^3)_2;(1_+^4)_3;(1_+^4)_5] \sim [(0^3,2)_2;(1_+^4)_3;(1_+^4)_5]$	$2\cdot 3$ & $2\cdot 3$
	$\mathbb{Q}(\sqrt{-7})$	$[(1_+^4)_7]$	$2^4\cdot 3^2\cdot 5\cdot 7$
		$[(0,1^3)_2;(1_+^4)_7] \sim [(0^3,1)_2;(1_+^4)_7]$	$2^4\cdot 3\cdot 7$
		$[(0^2,1^2)_2;(1_+^4)_7]$	$2^4\cdot 3^2$
		$[(0,2^3)_2;(1_+^4)_7] \sim [(0^3,2)_2;(1_+^4)_7]$	$2\cdot 3\cdot 7$
		$[(0,1,2^2)_2;(1_+^4)_7] \sim [(0^2,1,2)_2;(1_+^4)_7]$	$2^2\cdot 3$
		$[(0,1^2,2)_2;(1_+^4)_7]$	$2^3\cdot 3$
		$[(0_+^2,1_+^2)_7] \sim [(1_+^2,2_+^2)_7]$	$2^2\cdot 3^2$ & $2^2\cdot 3\cdot 7$
		$[(0^2,1^2)_3;(1_+^4)_7]$	$2^5\cdot 3$ & $2^5\cdot 3^2$
		$[(0^2,2^2)_2;(1_+^4)_7]$	$2^2\cdot 3$ & $2^2\cdot 3^2$
		$[(0,3^3)_2;(1_+^4)_7] \sim [(0^3,3)_2;(1_+^4)_7]$	$2\cdot 3$ & $2\cdot 3\cdot 7$
		$[(0,2,3^2)_2;(1_+^4)_7] \sim [(0^2,1,3)_2;(1_+^4)_7]$	2 & $2\cdot 3$
		$[(0,2^2,3)_2;(1_+^4)_7] \sim [(0,1^2,3)_2;(1_+^4)_7]$	$2\cdot 3$ & $2\cdot 3$
		$[(0,2^3)_3;(1_+^4)_7] \sim [(0^3,2)_3;(1_+^4)_7]$	$2^2\cdot 3$ & $2\cdot 3\cdot 7$
	$\mathbb{Q}(\sqrt{-11})$	$[(1_+^4)_{11}]$	$2^7\cdot 3\cdot 5$
		$[(0,2^3)_2;(1_+^4)_{11}] \sim [(0^3,2)_2;(1_+^4)_{11}]$	$2^4\cdot 3$
		$[(0,1^3)_3;(1_+^4)_{11}] \sim [(0^3,1)_3;(1_+^4)_{11}]$	$2^4\cdot 3$

m	E/K	genus symbol of G	$\#\operatorname{Aut}(L_i)$
		$[(0^2, 1^2)_2; (1^4_+)_{11}]$	$2^4 \cdot 3^2$ & $2^7 \cdot 3^2$
		$[(0^2, 2^2)_2; (1^4_+)_{11}]$	$2^2 \cdot 3$ & $2^3 \cdot 3$
		$[(0, 2^3)_3; (1^4_+)_{11}] \sim [(0^3, 2)_3; (1^4_+)_{11}]$	2 & 2^4
		$[(0, 1^3)_5; (1^4_+)_{11}] \sim [(0^3, 1)_5; (1^4_+)_{11}]$	$2^2 \cdot 5$ & 2^5
		$[(0, 1^2, 2)_2; (1^4_+)_{11}]$	$2^3 \cdot 3^2$ & $2^6 \cdot 3^2$
	$\mathbb{Q}(\sqrt{-19})$	$[(1^4_+)_{19}]$	$2^4 \cdot 3^2 \cdot 5$ & $2^7 \cdot 3 \cdot 5$
		$[(0, 2^3)_2; (1^4_+)_{19}] \sim [(0^3, 2)_2; (1^4_+)_{19}]$	$2 \cdot 3^2$ & $2^4 \cdot 3$
	$\mathbb{Q}(\sqrt{5})(\sqrt{(\sqrt{5}-5)/2})$	$[(1^4_+)_{\mathfrak{p}_5}]$	$2^7 \cdot 3^2 \cdot 5^4$
		$[(0^4_+)_{\mathfrak{p}_5}]$	$2^6 \cdot 3^2 \cdot 5^3$ & $2^7 \cdot 3 \cdot 5^4$
		$[(0^2_+, 1^2_+)_{\mathfrak{p}_5}] \sim [(1^2_+, 2^2_+)_{\mathfrak{p}_5}]$	$2^4 \cdot 5^4$ & $2^6 \cdot 3 \cdot 5^4$
		$[(0_+, 1^2_+, 2_+)_{\mathfrak{p}_5}]$	$2^3 \cdot 5^4$ & $2^5 \cdot 3 \cdot 5^4$
		$[(0_-, 1^2_+, 2_-)_{\mathfrak{p}_5}]$	$2^3 \cdot 5^4$ & $2^5 \cdot 3 \cdot 5^4$
		$[(1^4_+)_{\mathfrak{p}_5}; (0, 1^3)_{\mathfrak{p}_{11,1}}] \sim [(1^4_+)_{\mathfrak{p}_5}; (0^3, 1)_{\mathfrak{p}_{11,1}}]$	$2^2 \cdot 5^3$ & $2^4 \cdot 3 \cdot 5^4$
		$[(1^4_+)_{\mathfrak{p}_5}; (0, 1^3)_{\mathfrak{p}_{11,2}}] \sim [(1^4_+)_{\mathfrak{p}_5}; (0^3, 1)_{\mathfrak{p}_{11,2}}]$	$2^2 \cdot 5^3$ & $2^4 \cdot 3 \cdot 5^4$
	$\mathbb{Q}(\sqrt{5})(\sqrt{-3})$	$[(1^4_+)_{\mathfrak{p}_3}]$	$2^7 \cdot 3^5 \cdot 5$ & $2^7 \cdot 3^4 \cdot 5^2$
	$\mathbb{Q}(\sqrt{2})(\sqrt{-1})$	$[(1^4_{+,2})_{\mathfrak{p}_2}]$	$2^{12} \cdot 3$ & 2^{15}
		$[(1^2_{-,2}, 3^2_{-,4})_{\mathfrak{p}_2}]$	$2^{11} \cdot 3$ & 2^{14}
	$\mathbb{Q}(\sqrt{3})(\sqrt{-1})$	$[]$	$2^{10} \cdot 3^3 \cdot 5$ & $2^{11} \cdot 3^5$
		$[(1^4)_{\mathfrak{p}_2}]$	$2^{11} \cdot 3^4$ & $2^8 \cdot 3^5 \cdot 5$
	$\mathbb{Q}(\theta_7)(\sqrt{\theta_7^2 - 4})$	$[(1^4_+)_{\mathfrak{p}_7}]$	$2^4 \cdot 3^2 \cdot 5 \cdot 7^2$ & $2^3 \cdot 3 \cdot 7^4$
5	$\mathbb{Q}(\sqrt{-1})$	$[(0_-, 1^4_{-,2})_2] \sim [(1^4_{+,2}, 2_+)_2]$	$2^{13} \cdot 3^2$
		$[(0_-, 3^4_{-,4})_2] \sim [(1^4_{-,2}, 4_-)_2]$	$2^{12} \cdot 3$
		$[(0^5_+)_2]$	$2^{13} \cdot 3 \cdot 5$ & $2^{12} \cdot 3^2 \cdot 5$
		$[(0^3_-, 1^2_{-,2})_2] \sim [(1^2_{-,2}, 2^3_-)_2]$	$2^{13} \cdot 3$ & $2^{12} \cdot 3^2$
		$[(0^4_{+,2}, 2_+)_2] \sim [(0_+, 2^4_{+,4})_2]$	$2^{13} \cdot 3 \cdot 5$ & $2^{12} \cdot 3^2 \cdot 5$
		$[(0^2_{+,2}, 1^2_{-,2}, 2_-)_2] \sim [(0_-, 1^2_{-,2}, 2^2_{+,4})_2]$	$2^{13} \cdot 3$ & $2^{12} \cdot 3^2$
		$[(0^2_{-,0}, 1^2_{-,2}, 2_+)_2] \sim [(0_+, 1^2_{-,2}, 2^2_{-,2})_2]$	2^{13} & $2^{12} \cdot 3$
		$[(0_-, 2^2_{+,4}, 3^2_{-,4})_2] \sim [(1^2_{-,2}, 2^2_{+,4}, 4_-)_2]$	$2^{13} \cdot 3$ & $2^{12} \cdot 3^2$
		$[(0^2_{+,2}, 1^2_{-,2}, 4_-)_2] \sim [(0_-, 3^2_{-,4}, 4^2_{+,6})_2]$	$2^{11} \cdot 3$ & $2^{10} \cdot 3^2$

m	E/K	genus symbol of G	$\# \operatorname{Aut}(L_i)$
		$[(0_-, 1^2_{+,2}, 3^2_{-,4})_2] \sim [(1^2_{-,2}, 3^2_{-,4}, 4_+)_2]$	2^{12} & $2^{12} \cdot 3^2$
		$[(1^2_{-,2}, 2_-, 3^2_{+,4})_2]$	2^{12} & $2^{12} \cdot 3^2$
		$[(0_+, 3^4_{+,4})_2] \sim [(1^4_{+,2}, 4_+)_2]$	2^{13} & $2^{13} \cdot 3^2$
		$[(0_-, 5^4_{-,6})_2] \sim [(1^4_{-,2}, 6_-)_2]$	2^{10} & $2^{10} \cdot 3$
	$\mathbb{Q}(\sqrt{-3})$	$[(0^5_+)_3]$	$2^8 \cdot 3^6 \cdot 5$
		$[(0^3_+, 1^2_+)_3] \sim [(1^2_+, 2^3_+)_3]$	$2^7 \cdot 3^6$
		$[(0_+, 1^4_+)_3] \sim [(1^4_+, 2_+)_3]$	$2^8 \cdot 3^6 \cdot 5$
		$[(1^2_+, 2_+, 3^2_+)_3]$	$2^7 \cdot 3^4$
		$[(0^3, 1^2)_2; (0^5_+)_3] \sim [(0^2, 1^3)_2; (0^5_-)_3]$	$2^8 \cdot 3^4$ & $2^7 \cdot 3^6$
		$[(0^3, 1^2)_2; (0_+, 1^4_+)_3] \sim [(0^2, 1^3)_2; (0_-, 1^4_+)_3] \sim$ $[(0^3, 1^2)_2; (1^4_+, 2_+)_3] \sim [(0^2, 1^3)_2; (1^4_+, 2_-)_3]$	$2^5 \cdot 3^6$ & $2^8 \cdot 3^5$
		$[(0, 1^4)_2; (0^5_+)_3] \sim [(0^4, 1)_2; (0^5_-)_3]$	$2^7 \cdot 3^5 \cdot 5$ & $2^8 \cdot 3^6$
		$[(0, 1^4)_2; (0_+, 1^4_+)_3] \sim [(0^4, 1)_2; (0_-, 1^4_+)_3] \sim [(0, 1^4)_2; (1^4_+, 2_+)_3] \sim$ $[(0^4, 1)_2; (1^4_+, 2_-)_3]$	$2^7 \cdot 3^6$ & $2^8 \cdot 3^6 \cdot 5$
		$[(0_+, 2^4_+)_3] \sim [(0^4_+, 2_+)_3]$	$2^5 \cdot 3^6$ & $2^8 \cdot 3^6$
		$[(0_-, 2^4_-)_3] \sim [(0^4_-, 2_-)_3]$	$2^6 \cdot 3^6$ & $2^4 \cdot 3^6 \cdot 5$
		$[(0_+, 1^2_+, 2^2_+)_3] \sim [(0^2_+, 1^2_+, 2_+)_3]$	$2^5 \cdot 3^6$ & $2^6 \cdot 3^6$
		$[(0_-, 1^2_+, 2^2_-)_3] \sim [(0^2_-, 1^2_+, 2_-)_3]$	$2^6 \cdot 3^6$ & $2^7 \cdot 3^6$
		$[(0_+, 3^4_+)_3] \sim [(1^4_+, 4_+)_3]$	$2^4 \cdot 3^6$ & $2^8 \cdot 3^6 \cdot 5$
		$[(0_+, 1^2_+, 3^2_+)_3] \sim [(1^2_+, 3^2_+, 4_+)_3]$	$2^4 \cdot 3^4$ & $2^7 \cdot 3^4$
		$[(0, 1^3, 2)_2; (0^5_-)_3]$	$2^7 \cdot 3^4$ & $2^6 \cdot 3^6$
		$[(0, 1^3, 2)_2; (0_-, 1^4_+)_3] \sim [(0, 1^3, 2)_2; (1^4_+, 2_-)_3]$	$2^4 \cdot 3^6$ & $2^7 \cdot 3^5$
	$\mathbb{Q}(\sqrt{-7})$	$[(0_+, 1^4_+)_7] \sim [(1^4_+, 2_+)_7]$	$2^5 \cdot 3 \cdot 7$ & $2^5 \cdot 3^2 \cdot 5 \cdot 7$
	$\mathbb{Q}(\sqrt{5})(\sqrt{(\sqrt{5}-5)/2})$	$[(0_+, 1^4_+)_{\mathfrak{p}_5}] \sim [(1^4_+, 2_+)_{\mathfrak{p}_5}]$	$2^3 \cdot 5^6$ & $2^8 \cdot 3^2 \cdot 5^5$
6	$\mathbb{Q}(\sqrt{-1})$	$[(0^2_{+,2}, 1^4_{-,2})_2] \sim [(1^4_{-,2}, 2^2_{+,4})_2]$	$2^{16} \cdot 3^2$
		$[(1^6_{-,2})_2]$	$2^{16} \cdot 3^4$
		$[(0^4_{+,2}, 1^2_{-,2})_2] \sim [(1^2_{-,2}, 2^4_{+,4})_2]$	$2^{16} \cdot 3^2 \cdot 5$ & $2^{15} \cdot 3^3 \cdot 5$
		$[(0^2_{-,0}, 1^4_{+,2})_2] \sim [(1^4_{+,2}, 2^2_{-,2})_2]$	$2^{16} \cdot 3$ & $2^{16} \cdot 3^2$
		$[(1^6_{+,2})_2; (0^5, 1)_3] \sim [(1^6_{+,2})_2; (0, 1^5)_3]$	$2^{13} \cdot 3$ & $2^{15} \cdot 3^2$

m	E/K	genus symbol of G	$\#\,\mathrm{Aut}(L_i)$
		$[(0^2_{+,2}, 1^2_{-,2}, 2^2_{+,4})_2]$	$2^{14} \cdot 3^2$ & $2^{13} \cdot 3^3$
		$[(0_+, 1^4_{+,2}, 2_+)_2]$	$2^{15} \cdot 3$ & $2^{15} \cdot 3^2$
		$[(1^4_{-,2}, 3^2_{+,4})_2] \sim [(1^2_{+,2}, 3^4_{-,4})_2]$	2^{15} & $2^{15} \cdot 3$
	$\mathbb{Q}(\sqrt{-3})$	$[(0^5, 1)_2; (1^6_+)_3] \sim [(0, 1^5)_2; (1^6_+)_3]$	$2^{10} \cdot 3^7 \cdot 5$
		$[(0^6_-)_3]$	$2^{10} \cdot 3^8 \cdot 5$ & $2^9 \cdot 3^7 \cdot 5 \cdot 7$
		$[(0^4_-, 1^2_+)_3] \sim [(1^2_+, 2^4_-)_3]$	$2^5 \cdot 3^8 \cdot 5$ & $2^8 \cdot 3^8$
		$[(0^2_-, 1^4_+)_3] \sim [(1^4_+, 2^2_-)_3]$	$2^9 \cdot 3^8$ & $2^{10} \cdot 3^7 \cdot 5$
		$[(0^5, 1)_2; (0^6_+)_3] \sim [(0, 1^5)_2; (0^6_+)_3]$	$2^8 \cdot 3^6 \cdot 5$ & $2^9 \cdot 3^7 \cdot 5$
		$[(0^3, 1^3)_2; (1^6_+)_3]$	$2^7 \cdot 3^8$ & $2^{10} \cdot 3^7$
		$[(1^6_+)_3; (0^5, 1)_5] \sim [(1^6_+)_3; (0, 1^5)_5]$	$2^7 \cdot 3^6$ & $2^8 \cdot 3^7 \cdot 5$
		$[(0_+, 1^4_+, 2_+)_3]$	$2^8 \cdot 3^8$ & $2^9 \cdot 3^7 \cdot 5$
		$[(0_-, 1^4_+, 2_-)_3]$	$2^8 \cdot 3^8$ & $2^9 \cdot 3^7 \cdot 5$
7	$\mathbb{Q}(\sqrt{-1})$	$[(0_-, 1^6_{+,2})_2] \sim [(1^6_{-,2}, 2_+)_2]$	$2^{17} \cdot 3 \cdot 7$ & $2^{18} \cdot 3^4$
	$\mathbb{Q}(\sqrt{-3})$	$[(0_-, 1^6_+)_3] \sim [(1^6_+, 2_-)_3]$	$2^{11} \cdot 3^9 \cdot 5$
		$[(0^7_-)_3]$	$2^{10} \cdot 3^8 \cdot 5 \cdot 7$ & $2^{11} \cdot 3^9 \cdot 5 \cdot 7$
		$[(0, 1^6)_2; (0_-, 1^6_+)_3] \sim [(0^6, 1)_2; (0_+, 1^6_+)_3] \sim [(0, 1^6)_2; (1^6_+, 2_-)_3] \sim$ $[(1^6, 2)_2; (1^6_+, 2_-)_3]$	$2^8 \cdot 3^9$ & $2^{11} \cdot 3^8 \cdot 5$
		$[(0_-, 3^6_+)_3] \sim [(1^6_+, 4_-)_3]$	$2^7 \cdot 3^7$ & $2^{11} \cdot 3^7 \cdot 5$
8	$\mathbb{Q}(\sqrt{-3})$	$[(1^8_+)_3]$	$2^{15} \cdot 3^{10} \cdot 5^2$
		$[(0^2_+, 1^6_+)_3] \sim [(1^6_+, 2^2_+)_3]$	$2^9 \cdot 3^{10}$ & $2^{12} \cdot 3^{10} \cdot 5$
		$[(0, 2^7)_2; (1^8_+)_3] \sim [(0^7, 2)_2; (1^8_+)_3]$	$2^{11} \cdot 3^7$ & $2^{11} \cdot 3^{10} \cdot 5$
		$[(0_+, 1^6_+, 2_-)_3] \sim [(0_-, 1^6_+, 2_+)_3]$	$2^9 \cdot 3^{10}$ & $2^{12} \cdot 3^{10} \cdot 5$
9	$\mathbb{Q}(\sqrt{-3})$	$[(0_+, 1^8_+)_3] \sim [(1^8_+, 2_+)_3]$	$2^{11} \cdot 3^{13}$ & $2^{16} \cdot 3^{11} \cdot 5^2$

9 Quaternionic hermitian lattices with class number at most 2

This chapter gives a complete classification of all definite quaternionic hermitian lattices with class number at most two.

Throughout the chapter, let E be a definite quaternion algebra over some totally real number field K of degree n and (V, Φ) denotes a definite hermitian space of rank m over E. Further, let $\mathfrak{o}$ and $\mathcal{O}$ be maximal orders of K and E respectively.

9.1 Two remarks

The maximal orders in E are not unique. The following remark deals with this nuisance.

Remark 9.1.1 Let $\mathcal{O}$ and $\mathcal{O}'$ be maximal orders in E. There exists some left ideal $\mathfrak{A}$ of $\mathcal{O}$ with right order $\mathcal{O}'$, for example $\mathfrak{A} := \mathcal{O}\mathcal{O}'$. The bijection

$$\{L' \subset E\,;\, L' \text{ is an } \mathcal{O}'\text{-lattice in } (V,\Phi)\} \to \{L \subset E\,;\, L \text{ is an } \mathcal{O}\text{-lattice in } (V,\Phi)\}$$
$$L' \mapsto \mathfrak{A}L'$$

preserves genera, isometry classes and thus class numbers. Note that this map does not necessarily preserve norms and scales. However, if the narrow class group of K is trivial, the situation can be remedied. In that case, $\mathfrak{A}\overline{\mathfrak{A}} = a^{-1}\mathcal{O}$ for some totally positive scalar $a \in K^*$. Then

$$\{L' \subset E\,;\, L' \text{ is an } \mathcal{O}'\text{-lattice in } (V,\Phi)\} \to \{L \subset E\,;\, L \text{ is an } \mathcal{O}\text{-lattice in } (V,a\Phi)\}$$
$$L' \mapsto (\mathfrak{A}L')^a$$

not only preserves genera, isometry classes and class numbers, but also norms and scales.

So Remark 9.1.1 shows that for the classification of all genera of lattices over E with given class number, it suffices to consider only $\mathcal{O}$-lattices for some maximal order $\mathcal{O}$ of E, which will be fixed now once and for all.

The unique decomposition of definite lattices into indecomposable ones is extremely powerful in the case of quaternionic hermitian lattices since there are no obstructions on which hermitian spaces over E exist.

Remark 9.1.2 Let G be a genus of $\mathcal{O}$-lattices in (V, Φ).

1. There exists some $\mathcal{O}$-lattice $L_1 \perp \ldots \perp L_s \in G$ such that L_i is indecomposable and $\operatorname{rank}(L_i) \leq 2$.

2. $h(G) \geq h(\perp_{j\in I} L_j)$ for all nonempty subsets $I \subseteq \{1,\dots,s\}$.

Proof. 1. Let $L \in G$ and $P = \{\mathfrak{p} \in \mathbb{P}(\mathfrak{o})\,;\, E_\mathfrak{p}$ is ramified or $L_\mathfrak{p}$ is not unimodular$\}$. Given $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$, Algorithm 3.3.2 shows that $L_\mathfrak{p} \cong L_{\mathfrak{p},1} \perp \cdots \perp L_{\mathfrak{p},r}$ with $\operatorname{rank}(L_{\mathfrak{p},i}) = 2$ for all $i < s := \lceil m/2 \rceil$. Since there exists only one hermitian space over $E_\mathfrak{p}$ of a given rank, there exists some definite $\mathcal{O}$-lattice L_i such that $(L_i)_\mathfrak{q}$ is unimodular for all $\mathfrak{q} \notin P$ and $(L_i)_\mathfrak{p} \cong L_{\mathfrak{p},i}$ for all $\mathfrak{p} \in P$. The result now follows by splitting each lattice L_i into indecomposable ones, c.f. Theorem 2.4.9.
2. Let $X = \perp_{j\in I} L_j$ and $Y = \perp_{j\notin I} L_j$. Further let $X_1,\dots,X_h$ represent the isometry classes of $\operatorname{gen}(X)$. Then $X_i \perp Y \in G$ and the unique decomposition of $\mathcal{O}$-lattices into irreducible ones shows that $X_i \perp Y \cong X_j \perp Y$ implies $X_i \cong X_j$. So $h(G) \geq h$. □

In particular, if the algebra E admits definite hermitian lattices with class number at most B and rank $m \geq 3$, it must also admit such lattices of rank $m-1$ or $m-2$. This usually rules out a lot of candidates for E.

9.2 The unary case

Suppose $m = 1$. Up to similarity, $V = E$ carries only one definite hermitian form, which is its trace bilinear form

$$\Phi\colon E \times E \to K,\ (x,y) \mapsto \frac{x\overline{y} + y\overline{x}}{2}\ .$$

The corresponding quadratic form Q_Φ is the reduced norm $\operatorname{nr}_{E/K} = \mathrm{N}$. Let $\mathcal{L}$ denote the set of all $\mathcal{O}$-lattices in (E,Φ), i.e. left ideals of $\mathcal{O}$. It is well known that the map

$$\Psi\colon \mathcal{L} \to \mathrm{Cl}^+(\mathfrak{o}),\ [\mathfrak{A}] \mapsto [\mathfrak{n}(\mathfrak{A})]$$

is surjective, see for example [Rei03, Theorem (35.14)]. The set $\operatorname{gen}(\mathfrak{A})$ consists of all $\mathfrak{n}(\mathfrak{A})$-modular $\mathcal{O}$-lattices in (E,Φ). A system of representatives of the isometry classes in $\operatorname{gen}(\mathfrak{A})$ is given by the following theorem.

Theorem 9.2.1 *Let $\mathfrak{a}$ be an ideal of $\mathfrak{o}$ and let $\mathfrak{A}_1,\dots,\mathfrak{A}_h$ represent the isomorphism classes of the fibre $\Psi^{-1}(\{[\mathfrak{a}]\})$. For $1 \leq i \leq h$ let $\Lambda_i := \mathcal{O}_r(\mathfrak{A}_i)$ denote the right order of $\mathfrak{A}_i$ and let $\{u_{i,1},\dots,u_{i,r_i}\}$ be a system of representatives of $\mathfrak{o}^*_{>0}/\,\mathrm{N}(\Lambda_i^*)$.*

1. *There exists $x_i \in E^*$ such that $\mathfrak{n}(\mathfrak{A}_i)x_i\overline{x}_i = \mathfrak{a}$ and there exists $y_{i,j} \in E^*$ such that $y_{i,j}\overline{y}_{i,j} = u_{i,j}$.*
2. *$(\mathfrak{A}_i y_{i,j} x_i\,;\, 1 \leq j \leq r_i,\ 1 \leq i \leq h)$ represents the isometry classes in the genus of all $\mathfrak{a}$-modular lattices in (E,Φ). In particular, the class number of this genus is $\sum_{i=1}^h [\mathfrak{o}^*_{>0} : \mathrm{N}(\Lambda_i^*)]$.*

Proof. The first assertion follows from the Norm Theorem of Hasse-Schilling-Maass, see [Rei03, Theorem (33.15)]. For a proof of the second note that the $\mathcal{O}$-lattices $\mathfrak{A}_i y_{i,j} x_i$

all have rank 1 and they are $\mathfrak{a}$-modular. Hence they form a single genus. Suppose first that $\mathfrak{A}_i y_{i,j} x_i$ is isometric to $\mathfrak{A}_k y_{k,\ell} x_k$. Isometries in (E, Φ) are given by right multiplication with elements of E having norm one. Hence there exists some $x \in E^*$ such that $\mathfrak{A}_i y_{i,j} x_i x = \mathfrak{A}_k y_{k,\ell} x_k$ and $x\overline{x} = 1$. Thus $\mathfrak{A}_i$ is isomorphic to $\mathfrak{A}_k$ which shows $i = k$ and further $y_{i,j} x_i x x_i^{-1} y_{i,\ell}^{-1} \in \Lambda_i$. Therefore $\mathrm{N}(y_{i,j})\,\mathrm{N}(y_{i,\ell})^{-1} = \mathrm{N}(y_{i,j} x_i x x_i^{-1} y_{i,\ell}^{-1}) \in \mathrm{N}(\Lambda_i)$ implies that $j = \ell$.
Suppose now $\mathfrak{B} \in \mathrm{gen}(\mathfrak{A})$. Then $\mathfrak{B}$ is also $\mathfrak{a}$-modular, i.e. $\mathfrak{n}(\mathfrak{B}) = \mathfrak{a}$. Hence $\mathfrak{B}$ is isomorphic to some $\mathfrak{A}_i$ say $\mathfrak{A}_i x x_i = \mathfrak{B}$ with $x \in E^*$. Comparing reduced norms shows that $\mathrm{N}(x)$ is a totally positive unit of $\mathfrak{o}$. Whence $\mathrm{N}(x) = \mathrm{N}(u) u_{i,j}$ for some $1 \le j \le r_i$ and some $u \in \Lambda_i^*$. Hence $\mathrm{N}(x) = \mathrm{N}(u y_{i,j})$, say $x = u y_{i,j} e$ for some $e \in E^*$ of norm 1. Therefore $x_i^{-1} e x_i$ also has reduced norm 1 and induces an isometry between $\mathfrak{B} = \mathfrak{A}_i x x_i = \mathfrak{A}_i y_{i,j} e x_i = \mathfrak{A}_i y_{i,j} x_i (x_i^{-1} e x_i)$ and $\mathfrak{A}_i y_{i,j} x_i$. □

The previous algorithm and Remark 9.1.1 immediately show how to decide if (E, Φ) admits $\mathcal{O}$-lattices with a given class number:

Algorithm 9.2.2

Input: Some definite quaternion algebra E and some integer $h \ge 1$.
Output: True if and only if E admits unary hermitian lattices of class number h.

```
Let $\mathcal{O}$ be a maximal order in $E$.
Let $\mathfrak{A}_1, \dots, \mathfrak{A}_\ell$ represent the isomorphism classes of left ideals of $\mathcal{O}$.
for $[\mathfrak{a}] \in \mathrm{Cl}^+(\mathfrak{o})$ do
    Let $I = \{1 \le i \le \ell ;\, \Psi(\mathfrak{A}_i) = [\mathfrak{a}]\}$.
    if $\sum_{i \in I} [\mathfrak{o}_{>0}^* : \mathrm{N}(\mathcal{O}_r(\mathfrak{A}_i)^*)] = h$ then return true end if
end for
return false.
```

Note that all algorithms for quaternion algebras needed in Algorithm 9.2.2 have been implemented by J. Voight, S. Donnelly and the author in `Magma`. For example, a maximal order can be computed using the Round2 algorithm of H. Zassenhaus [Zas72] or the more specialized algorithm [Voi13, Algorithm 7.10]. The computation of left ideal class representatives and unit groups is explained in the author's paper with J. Voight [KV10].

The remainder of this section answers the question which definite quaternion algebras admit hermitian lattices of rank 1 and class number at most 2. By Corollary 6.3.11 such an algebra E over K satisfies

$$\mathrm{d}_K^{1/n} \le 11.6 \quad \text{and} \quad \prod_{\mathfrak{p} \mid \mathrm{d}_{E/K}} (\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p}) - 1) \le 2^n \cdot |\zeta_K(-1)|^{-1} .$$

This leaves only finitely many candidates, which can easily be worked out using [Voi08] and Remark 3.4.2. Applying Algorithm 9.2.2 to these candidates with $h \in \{1, 2\}$, yields the following result.

Theorem 9.2.3 *There are* 69 (148) *definite quaternion algebras E over* 29 (60) *different base fields K that admit unary hermitian lattices of class number one (two).*

Tables 9.1 and 9.2 list the degree n of the center K, the discriminant d_K as well as $D = \mathrm{Nr}_{K/\mathbb{Q}}(\mathrm{d}_{E/K})^{1/2}$ for these algebras. A complete list is available from [Kir16].

The information given by Tables 9.1 and 9.2 usually does not define the algebra E or even a genus uniquely, but it is certainly enough to recover all genera of class number at most 2 quickly using `Magma`.

Table 9.1: Quaternion algebras that admit one-class genera of hermitian forms

n	d_K	D	n	d_K	D	n	d_K	D	n	d_K	D	n	d_K	D
1	1	2	2	12	1	2	33	1	3	148	2	4	1957	1
		3			6		60	1			5		2000	1
		5			26	3	49	7			13			20
		7		13	1			8		169	5		2304	1
		13			12			13			13			18
2	5	1		17	1			29		229	4		2777	1
		20		21	1			43		316	2		3600	1
		44		24	1		81	3		321	3		4352	1
	8	1			6			19	4	725	1		4752	1
		14		28	1			37		1125	1		10512	1
		18										5	24217	5
		50												

9.3 The general case

In this section the rank m of (V, Φ) over E is assumed to be at least 2.

To be able to write down genera in a unique and efficient way, the following notation will be used.

Definition 9.3.1 Let G be a genus of $\mathcal{O}$-lattices in (V, Φ) and let $L \in G$.

1. Suppose $L_\mathfrak{p} = \perp_{i=1}^t L_i$ is a Jordan decomposition of L at some prime ideal $\mathfrak{p}$ of $\mathfrak{o}$. Let $\mathfrak{P}$ be the maximal twosided ideal of $\mathcal{O}$ over $\mathfrak{p}$. Then $\mathfrak{s}(L_i) = \mathfrak{P}^{s_i}$ for some integers $s_1 < \ldots < s_t$. The *local genus symbol* of $L_\mathfrak{p}$ is
$$(s_1^{\mathrm{rank}(L_1)}, \ldots, s_t^{\mathrm{rank}(L_t)}) .$$
Note that the superscripts $\mathrm{rank}(L_i)$ will be omitted whenever they are 1. For example, (0^m) describes a unimodular lattice of rank m. By Proposition 3.3.5 and Theorem 3.3.6, the local genus symbol is well defined, i.e. independent from the Jordan decomposition chosen. Moreover, the isomorphism class of $L_\mathfrak{p}$ is uniquely determined by the local genus symbol.

Table 9.2: Quaternion algebras that admit two-class genera of hermitian forms

n	d_K	D	n	d_K	D	n	d_K	D	n	d_K	D	n	d_K	D
1	1	11	2	17	4	2	69	1	3	321	3	4	6125	1
		17			18	3	49	27			7		6809	1
		19			26			41		361	7		7056	1
		30		21	1			71		404	2		7488	1
		42			12			97		469	4		7537	1
		70			15			113		568	2		9909	1
		78			20			127	4	1125	1	5	14641	11
2	5	36		24	1		81	8			45			23
		45			15			17			80		24217	17
		55		28	1			73		1600	1		36497	3
		95			6		148	17		1957	21			13
		99			14			25		2048	1		38569	7
		124		29	1		169	8		2225	1			13
		155		33	1		229	2		2525	1	6	300125	1
		164			6			7		2624	1		371293	1
	8	34		37	1			13		3981	1		434581	1
		62		40	1		257	3			15		453789	1
		63		41	1			5		4205	1		485125	1
	12	39		44	1			7		4352	14		592661	1
		50		57	1			9		4752	12		1397493	1
	13	9		60	6		316	2		5125	1	8	324000000	1
		39												

2. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ be the prime ideals of $\mathfrak{o}$ such that $L_{\mathfrak{p}_i}$ is not unimodular and let g_i be the local genus symbol of L at $\mathfrak{p}_i$. Then the *genus symbol*
$$[g_{1\mathfrak{p}_1}; \dots; g_{s\mathfrak{p}_s}]$$
is well defined and it uniquely determines the genus G. For example, G consists of unimodular lattices if and only if its genus symbol is the empty list $[]$.

Corollary 6.3.11 lists finitely many pairs (E, m) of quaternion algebras E and integers $m \geq 2$ such that E might admit definite hermitian lattices of rank m of class number at most 2. Applying Algorithm 6.5.4 to these candidates, immediately yields the following result.

Theorem 9.3.2 *Let (V, Φ) be a definite hermitian space over a definite quaternion algebra E of rank $m \geq 2$. Let $\mathcal{O}$ be a maximal order of E and let G be a genus of $\mathcal{O}$-lattices in (V, Φ). If $h(G) = 1$, then $m \leq 4$ and $h(G) = 2$ implies $m \leq 5$. The complete list of all genera with class number at most 2 is given at the end of this section.*

For each similarity class of genera as in Theorem 9.3.2, the table below lists the following information:

- The rank m of the lattices.
- The quaternion algebra E. Here $\mathcal{Q}_{\alpha,\infty,\mathfrak{p}_1,\dots,\mathfrak{p}_r}$ denotes the definite quaternion algebra over $K = \mathbb{Q}(\alpha)$ ramified only at the finite places $\mathfrak{p}_1, \dots, \mathfrak{p}_r$. The subscript α will be omitted if $K = \mathbb{Q}$. Further, $\theta_7 = \zeta_7 + \zeta_7^{-1}$ for some primitive 7-th root of unity $\zeta_7 \in \mathbb{C}$.
- The genus symbol of a genus G in the similarity class. Here $\mathfrak{p}_p$ denotes a prime ideal over p, which will be unique in all cases. The classification shows that the center of E always has narrow class number one. By Remark 9.1.1, this means that the genus symbols are independent from the maximal order $\mathcal{O}$. So there is no need to list $\mathcal{O}$ itself.
- The class number $h(G)$ of the genus.
- The automorphism groups $\mathrm{Aut}(L)$ where L ranges over representatives of the isometry classes in G. The naming conventions for the groups are the same as used by G. Nebe in [Neb98] with the exception that the subscripts expressing the quaternion algebras are omitted.
- The factored orders of these automorphism groups.
- Maximal finite subgroups of $\mathrm{GL}_m(E)$ that contain these automorphism groups.

The similarity classes are grouped according to equivalence classes with respect to the equivalence relation from Definition 6.2.3.

m	E	genus symbol of G	$h(G)$	$\{\mathrm{Aut}(L)\,;\,[L]\in G\}$	$\#\,\mathrm{Aut}(L)$	maximal finite?
2	$\mathcal{Q}_{\infty,2}$	$[]$	1	$[\mathrm{SL}_2(3)]_1^2$	$2^7\cdot 3^2$	m.f.
		$[(0,2)_2]$	1	$[\mathrm{SL}_2(3)]_1\times[\mathrm{SL}_2(3)]_1$	$2^6\cdot 3^2$	$[\mathrm{SL}_2(3)]_1^2$
		$[(1^2)_2]$	1	$[2_-^{1+4}.\,\mathrm{Alt}_5]$	$2^7\cdot 3\cdot 5$	m.f.
		$[(1^2)_2;(0,1)_3]$	1	$(Q_8\times Q_8){:}C_3$	$2^6\cdot 3$	G_1
		$[(0,1)_3]$	2	G_1	$2^6\cdot 3^2$	m.f.
				$[\mathrm{SL}_2(3)]_1\otimes A_2$	$2^4\cdot 3^2$	m.f.
		$[(1^2)_2;(0,2)_3]$	2	$(Q_8\times Q_8){:}C_3$	$2^6\cdot 3$	$[\mathrm{SL}_2(3)]_1^2$
				$\mathrm{SL}_2(3)$	$2^3\cdot 3$	$[\mathrm{SL}_2(3)]_1^2$
		$[(0,4)_2]$	2	$[\mathrm{SL}_2(3)]_1\times[\mathrm{SL}_2(3)]_1$	$2^6\cdot 3^2$	$[\mathrm{SL}_2(3)]_1^2$
				$(Q_8\times Q_8){:}C_3$	$2^6\cdot 3$	$[\mathrm{SL}_2(3)]_1^2$
		$[(0,1)_5]$	2	G_1	$2^6\cdot 3^2$	m.f.
				$C_2\times\mathrm{SL}_2(3)$	$2^4\cdot 3$	G_1
		$[(1^2)_2;(0,1)_5]$	2	$(Q_8\times Q_8){:}C_3$	$2^6\cdot 3$	G_1
				$[\mathrm{SL}_2(5)]_2$	$2^3\cdot 3\cdot 5$	m.f.
		$[(1^2)_2;(0,1)_7]$	2	$(Q_8\times Q_8){:}C_3$	$2^6\cdot 3$	G_1
				$[\mathrm{SL}_2(3).2]_2$	$2^4\cdot 3$	m.f.
	$\mathcal{Q}_{\infty,3}$	$[]$	1	$[\tilde{S}_3]_1^2$	$2^5\cdot 3^2$	m.f.
		$[(1^2)_3]$	1	$[\mathrm{SL}_2(9)]_2$	$2^4\cdot 3^2\cdot 5$	m.f.
		$[(0,1)_2;(1^2)_3]$	1	$[\mathrm{SL}_2(3)\overset{2}{\square}C_3]_2$	$2^4\cdot 3^2$	m.f.
		$[(0,2)_2;(1^2)_3]$	1	$(\pm C_3\times C_3).2$	$2^2\cdot 3^2$	$[\mathrm{SL}_2(9)]_2,\ [\mathrm{SL}_2(3)\overset{2}{\square}C_3]_2$
		$[(0,1)_2]$	2	G_2	$2^4\cdot 3^2$	m.f.
				$(D_8\curlyvee_{C_2}C_4).S_3$	$2^5\cdot 3$	m.f.
		$[(0,2)_2]$	2	$[\tilde{S}_3]_1\times[\tilde{S}_3]_1$	$2^4\cdot 3^2$	$[\tilde{S}_3]_1^2$
				$C_4\times C_4$	2^4	$[\tilde{S}_3]_1^2$
		$[(0,2)_3]$	2	$[\tilde{S}_3]_1\times[\tilde{S}_3]_1$	$2^4\cdot 3^2$	$[\tilde{S}_3]_1^2$
				$(\pm C_3\wr S_2).2$	$2^3\cdot 3^2$	$[\tilde{S}_3]_1^2$
		$[(0,3)_2;(1^2)_3]$	2	$(\pm C_3\times C_3).2$	$2^2\cdot 3^2$	$G_2,\ [\mathrm{SL}_2(3)\overset{2}{\square}C_3]_2$
				$\tilde{S}_3$	$2^2\cdot 3$	$G_2,\ [\mathrm{SL}_2(3)\overset{2}{\square}C_3]_2$

m	E	genus symbol of G	$h(G)$	$\{\mathrm{Aut}(L)\,;\,[L]\in G\}$	$\#\,\mathrm{Aut}(L)$	maximal finite?
		$[(1^2)_3;(0,1)_5]$	2	$(\pm C_3\times C_3).2$ $[\mathrm{SL}_2(5)]_2$	$2^2\cdot 3^2$ $2^3\cdot 3\cdot 5$	G_2 m.f.
	$\mathcal{Q}_{\infty,5}$	$[(1^2)_5]$	1	$[\mathrm{SL}_2(5).2]_2$	$2^4\cdot 3\cdot 5$	m.f.
		$[(0,1)_2;(1^2)_5]$	1	$[\tilde{S}_4]_2$	$2^4\cdot 3$	m.f.
		$[(0,2)_2;(1^2)_5]$	1	$[\tilde{S}_3]_2$	$2^2\cdot 3$	$[\mathrm{SL}_2(5).2]_2$
		$[(0,1)_3;(1^2)_5]$	1	$[\mathrm{SL}_2(3)]_2$	$2^3\cdot 3$	m.f.
		$[]$	2	$[C_6]_1^2$ $[\mathrm{SL}_2(5){:}2]_2$	$2^3\cdot 3^2$ $2^4\cdot 3\cdot 5$	m.f. m.f.
		$[(0,1)_2]$	2	$[C_6]_1\times[C_6]_1$ QD_{16}	$2^2\cdot 3^2$ 2^4	m.f. $[\mathrm{SL}_2(5){:}2]_2$
		$[(0,1)_2,(0,1)_3,(1^2)_5]$	2	C_6 Q_{24}	$2\cdot 3$ $2^3\cdot 3$	$[\tilde{S}_4]_2$ m.f.
	$\mathcal{Q}_{\infty,7}$	$[(1^2)_7]$	1	$[\mathrm{SL}_2(5)]_2$	$2^3\cdot 3\cdot 5$	m.f.
		$[(0,1)_2;(1^2)_7]$	1	Q_{24}	$2^3\cdot 3$	m.f.
		$[]$	2	$[C_4]_1^2$ $[\mathrm{GL}_2(3)]_2$	2^5 $2^4\cdot 3$	m.f. m.f.
		$[(0,2)_1;(1^2)_7]$	2	Q_{12}	$2^2\cdot 3$	$[\mathrm{SL}_2(5)]_2$
		$[(0,1)_3;(1^2)_7]$	2	$[\mathrm{SL}_2(3)]_2$ $[Q_{24}]_2$	$2^3\cdot 3$ $2^3\cdot 3$	m.f. m.f.
	$\mathcal{Q}_{\infty,11}$	$[(1^2)_{11}]$	1	$[\tilde{S}_4]_2$	$2^4\cdot 3$	m.f.
		$[(0,1)_2;(1^2)_{11}]$	2	$[Q_{12}]_2$ $[\tilde{S}_4]_2$	$2^2\cdot 3$ $2^4\cdot 3$	m.f. m.f.
	$\mathcal{Q}_{\infty,13}$	$[(1^2)_{13}]$	2	$[\tilde{S}_4]_2$ $[\mathrm{SL}_2(5)]_2$	$2^4\cdot 3$ $2^3\cdot 3\cdot 5$	m.f. m.f.
		$[(0,1)_2;(1^2)_{13}]$	2	$[\tilde{S}_4]_2$ Q_8	$2^4\cdot 3$ 2^3	m.f. $[\mathrm{SL}_2(5)]_2$
	$\mathcal{Q}_{\infty,17}$	$[(1^2)_{17}]$	2	$[Q_{24}]_2$ $[\mathrm{SL}_2(5)]_2$	$2^3\cdot 3$ $2^3\cdot 3\cdot 5$	m.f. m.f.
	$\mathcal{Q}_{\sqrt{5},\infty}$	$[]$	1	$[\mathrm{SL}_2(5)]_1^2$	$2^7\cdot 3^2\cdot 5^2$	m.f.

m	E	genus symbol of G	$h(G)$	$\{\mathrm{Aut}(L)\,;\,[L]\in G\}$	$\#\,\mathrm{Aut}(L)$	maximal finite?
		$[(0,1)_{\mathfrak{p}_2}]$	2	$[\mathrm{SL}_2(5)]_1 \times [\mathrm{SL}_2(5)]_1$	$2^6\cdot 3^2\cdot 5^2$	m.f.
				$[2_-^{1+4}.\,\mathrm{Alt}_5]$	$2^7\cdot 3\cdot 5$	m.f.
		$[(0,1)_{\mathfrak{p}_5}]$	2	$[\mathrm{SL}_2(5)]_1 \times [\mathrm{SL}_2(5)]_1$	$2^6\cdot 3^2\cdot 5^2$	m.f.
				$[\mathrm{SL}_2(5) \underset{\sqrt{5}}{\otimes} D_{10}]_2$	$2^4\cdot 3\cdot 5^2$	m.f.
		$[(0,1)_{\mathfrak{p}_{11}}]$	2	$[\mathrm{SL}_2(5)]_1 \times [\mathrm{SL}_2(5)]_1$	$2^6\cdot 3^2\cdot 5^2$	m.f.
				$\mathrm{SL}_2(5){:}2$	$2^4\cdot 3\cdot 5$	$[\mathrm{SL}_2(5)]_1 \times [\mathrm{SL}_2(5)]_1$
	$\mathcal{Q}_{\sqrt{5},\infty,\mathfrak{p}_2\mathfrak{p}_5}$	$[(1^2)_{\mathfrak{p}_2};(1^2)_{\mathfrak{p}_5}]$	2	$[\mathrm{SL}_2(5)]_2$	$2^3\cdot 3\cdot 5$	m.f.
				$[C_5 \overset{2(2)}{\underset{5}{\boxtimes}} \mathrm{SL}_2(3)]_2$	$2^4\cdot 3\cdot 5$	m.f.
	$\mathcal{Q}_{\sqrt{2},\infty}$	$[]$	2	$[\tilde{S}_4]_1^2$	$2^9\cdot 3^2$	m.f.
				$[2_-^{1+4}.S_5]_2$	$2^8\cdot 3\cdot 5$	m.f.
		$[(0,1)_{\mathfrak{p}_2}]$	2	$[\tilde{S}_4]_1 \times [\tilde{S}_4]_1$	$2^8\cdot 3^2$	m.f.
				$Q_{16} \wr S_2$	2^9	$[\tilde{S}_4]_1^2$
	$\mathcal{Q}_{\sqrt{13},\infty}$	$[]$	2	$[\mathrm{SL}_2(3)]_1^2$	$2^7\cdot 3^2$	m.f.
				$[\mathrm{SL}_2(5){:}2]_2$	$2^4\cdot 3\cdot 5$	m.f.
	$\mathcal{Q}_{\theta_7,\infty,\mathfrak{p}_7}$	$[(1^2)_{\mathfrak{p}_7}]$	2	$(\pm C_7 \times C_7){:}2$	$2^2\cdot 7^2$	$[Q_{28}]_1^2$
				$[\mathrm{SL}_2(5)]_2$	$2^3\cdot 3\cdot 5$	m.f.
3	$\mathcal{Q}_{\infty,2}$	$[]$	1	$[\mathrm{SL}_2(3)]_1^3$	$2^{10}\cdot 3^4$	m.f.
		$[(0,1^2)_2] \sim [(1,2^2)_2]$	1	$[\mathrm{SL}_2(3)]_1 \times [2_-^{1+4}.\,\mathrm{Alt}_5]_2$	$2^{10}\cdot 3^2\cdot 5$	m.f.
		$[(0^2,2)_2] \sim [(0,2^2)_2]$	2	$[\mathrm{SL}_2(3)]_1 \times [\mathrm{SL}_2(3)]_1^2$	$2^{10}\cdot 3^3$	$[\mathrm{SL}_2(3)]_1^3$
				$(Q_8 \wr S_3){:}C_3$	$2^{10}\cdot 3^2$	$[\mathrm{SL}_2(3)]_1^3$
		$[(0,3^2)_2] \sim [(1^2,4)_2]$	2	$[\mathrm{SL}_2(3)]_1 \times [2_-^{1+4}.\,\mathrm{Alt}_5]_2$	$2^{10}\cdot 3^2\cdot 5$	m.f.
				$(Q_8 \times (Q_8 \wr S_2)){:}C_3$	$2^{10}\cdot 3$	$\mathrm{Aut}(L_1)\,;\,[\mathrm{SL}_2(3)]_1^3$
	$\mathcal{Q}_{\infty,3}$	$[]$	2	$[\tilde{S}_3]_1^3$	$2^7\cdot 3^4$	m.f.
				$[\pm\mathrm{U}_3(3)]_3$	$2^6\cdot 3^3\cdot 7$	m.f.
		$[(0,1^2)_3] \sim [(1^2,2)_3]$	2	$[\tilde{S}_3]_1 \times [\mathrm{SL}_2(9)]_2$	$2^6\cdot 3^3\cdot 5$	m.f.
				$[\pm 3_+^{1+2}.\,\mathrm{GL}_2(3)]_3$	$2^5\cdot 3^4$	m.f.
	$\mathcal{Q}_{\infty,5}$	$[(0,1^2)_5] \sim [(1^2,2)_5]$	2	$[C_6]_1 \times [\mathrm{SL}_2(5).2]_2$	$2^5\cdot 3^2\cdot 5$	m.f.

m	E	genus symbol of G	$h(G)$	$\{\mathrm{Aut}(L)\,;\,[L] \in G\}$	$\#\,\mathrm{Aut}(L)$	maximal finite?
				$C_2 \times \mathrm{SL}_2(3)$	$2^4 \cdot 3$	$C_6 \times (\mathrm{SL}_2(3).2)$
	$\mathcal{Q}_{\sqrt{5},\infty}$	$[]$	2	$[\mathrm{SL}_2(5)]_1^3$	$2^{10} \cdot 3^4 \cdot 5^3$	m.f.
				$[2.\mathrm{J}_2]_3$	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7$	m.f.
4	$\mathcal{Q}_{\infty,2}$	$[(1^4)_2]$	1	$[2_-^{1+4}.\,\mathrm{Alt}_5]_2^2$	$2^{15} \cdot 3^2 \cdot 5^2$	m.f.
		$[]$	2	$[\mathrm{SL}_2(3)]_1^4$	$2^{15} \cdot 3^5$	m.f.
				$[2_-^{1+6}.\mathrm{O}_6^-(4)]_4$	$2^{13} \cdot 3^4 \cdot 5$	m.f.
		$[(0^2,1^2)_2] \sim$	2	$[\mathrm{SL}_2(3)]_1^2 \times [2_-^{1+4}.\,\mathrm{Alt}_5]_2$	$2^{14} \cdot 3^3 \cdot 5$	m.f.
		$[(1^2,2^2)_2]$		$(Q_8 \wr S_4){:}C_3$	$2^{15} \cdot 3^2$	$[\mathrm{SL}_2(3)]_1^4$
		$[(0,1^2,2)_2]$	2	$[\mathrm{SL}_2(3)]_1 \times [\mathrm{SL}_2(3)]_1 \times [2_-^{1+4}.\,\mathrm{Alt}_5]_2$	$2^{13} \cdot 3^3 \cdot 5$	$[\mathrm{SL}_2(3)]_1^2 \times [2_-^{1+4}.\,\mathrm{Alt}_5]_2$
				$(Q_8 \wr \mathrm{Alt}_4){:}C_3$	$2^{14} \cdot 3^2$	$[\mathrm{SL}_2(3)]_1^4$
		$[(1^4)_2;\,(0^3,1)_3] \sim$	2	$(Q_8 \times Q_8){:}C_3 \times [2_-^{1+4}.\,\mathrm{Alt}_5]_2$	$2^{13} \cdot 3^2 \cdot 5$	$G_1 \times [2_-^{1+4}.\,\mathrm{Alt}_5]_2$
		$[(1^4)_2;\,(0,1^3)_3]$		$(Q_8 \times Q_8 \times Q_8).(S_3 \times C_3)$	$2^{10} \cdot 3^2$	$[S_3 \otimes \mathrm{SL}_2(3)]_2 \times [\mathrm{SL}_2(3)]_1^2$
	$\mathcal{Q}_{\infty,3}$	$[(1^4)_3]$	2	$[\mathrm{SL}_2(9)]_2^2$	$2^9 \cdot 3^4 \cdot 5^2$	m.f.
				$[\mathrm{Sp}_4(3) \overset{2}{\square} C_3]_2$	$2^8 \cdot 3^5 \cdot 5$	m.f.
	$\mathcal{Q}_{\infty,5}$	$[(1^4)_5]$	2	$[\mathrm{SL}_2(5):2]_2^2$	$2^9 \cdot 3^2$	m.f.
				$[2_-^{1+4}.S_5]_4$	$2^8 \cdot 3 \cdot 5$	m.f.
5	$\mathcal{Q}_{\infty,2}$	$[(0,1^4)_2] \sim$	2	$[2_-^{1+4}.\,\mathrm{Alt}_5]_2^2 \times [\mathrm{SL}_2(3)]_1$	$2^{18} \cdot 3^3 \cdot 5^2$	m.f.
		$[(1^4,2)_2]$		$(Q_8 \times Q_8 \times Q_8 \times Q_8 \times Q_8).(\mathrm{Alt}_5 \times C_3)$	$2^{17} \cdot 3^2 \cdot 5$	$[\mathrm{SL}_2(3)]_1^5$

Here $\tilde{S}_3 \cong Q_{12}$ is the generalized quaternion group with 12 elements and $G_1 := {}_{\infty,2}[\mathrm{SL}_2(3)]_1 \times {}_{\infty,2}[\mathrm{SL}_2(3)]_1$. Further, $\theta_7 = \zeta_7 + \zeta_7$ where $\zeta_7 \in \mathbb{C}$ denotes some primitive seventh root of unity.

10 Exceptional groups

In the previous chapters, only classical (i.e. orthogonal and hermitian) groups have been studied. This final chapter discusses the problem of enumerating one-class genera of some special subgroups of exceptional algebraic groups. The exposition below is taken from the author‘s recent preprint [Kir].

10.1 Preliminaries

In this chapter, let K be a number field of degree n with ring of integers $\mathfrak{o}$. The infinite places of K will be denoted by $\Omega_\infty(K)$.

Let G be an absolutely quasi-simple, simply connected algebraic group defined over K such that $\prod_{v\in\Omega_\infty(K)} G(K_v)$ is compact. Then K is totally real. Most of the time, G will be exceptional, i.e. a K-form of G_2, F_4, E_6, E_7, E_8 or a triality form of D_4. By fixing a presentation of G, one one may assume that G is a subgroup of GL_m for some m.

As described in [Bor63, CNP98] any full $\mathfrak{o}$-lattice L in K^m describes an integral group scheme $\underline{G}$ as follows. For each extension (or completion) E of K with ring of integers $\mathcal{O}$, let $\underline{G}(\mathcal{O})$ be the stabilizer of $L\otimes_{\mathfrak{o}}\mathcal{O}$ in $G(E)$.

Let $A = \{(\alpha_v)_{v\in\Omega(K)} \mid \alpha_\mathfrak{p} \notin \mathfrak{o}_\mathfrak{p}$ for only finitely many $\mathfrak{p}\in\mathbb{P}(\mathfrak{o})\}$ be the adele ring of K. Suppose $\alpha\in G(A)$. Then $L\cdot\alpha$ denotes the $\mathfrak{o}$-lattice L' with $L'_\mathfrak{p} = L_\mathfrak{p}\alpha_\mathfrak{p}$ for all $\mathfrak{p}\in\mathbb{P}(\mathfrak{o})$. Similarly, one defines $\underline{G}\cdot\alpha$ to be the stabilizer of $L\cdot\alpha$ in $G(K)$. Then $(\underline{G}\cdot\alpha)(\mathfrak{o}_\mathfrak{p}) = \alpha_\mathfrak{p}^{-1}\underline{G}(\mathfrak{o}_\mathfrak{p})\alpha_\mathfrak{p}$ for all $\mathfrak{p}\in\mathbb{P}(\mathfrak{o})$.

Definition 10.1.1 Two integral forms $\underline{G}$ and $\underline{G}'$ of G are *isomorphic* if $\underline{G}\cdot\alpha = \underline{G}'$ for some $\alpha\in G(K)$. Similarly, they are said to be in the same *genus* if $\underline{G}\cdot\alpha = \underline{G}'$ for some $\alpha\in G(A)$.

Let $C = \prod_{v\in\Omega_\infty(K)} G(K_v)\times\prod_{\mathfrak{p}\in\mathbb{P}(\mathfrak{o})}\underline{G}(\mathfrak{o}_\mathfrak{p})$. Note that $\alpha^{-1}\underline{G}\alpha$ is the stabilizer of $\underline{G}\cdot\alpha$ in $G(A)$. Thus

$$C\alpha G(K)\mapsto \underline{G}\cdot\alpha$$

induces a bijection between the double cosets $C\backslash G(A)/G(K)$ and the isomorphism classes in the genus of $\underline{G}$.

Lemma 10.1.2 ([CNP98, Proposition 3.3]) *Let $\underline{G}$ be an integral group scheme as above. Then $\underline{G}(\mathfrak{o}_\mathfrak{p})$ is a subgroup of finite index in a maximal compact subgroup of $G(K_\mathfrak{p})$ and $\underline{G}(\mathfrak{o}_\mathfrak{p})$ is a hyperspecial maximal compact subgroup at all but finitely many places $\mathfrak{p}\in\mathbb{P}(\mathfrak{o})$.*

The most important integral group schemes $\underline{G}$ are those for which $\underline{G}(\mathfrak{o}_\mathfrak{p})$ is a parahoric subgroup $P_\mathfrak{p}$ of $G(K_\mathfrak{p})$ at each prime ideal $\mathfrak{p}$ of $\mathfrak{o}$. The genus of such a scheme is uniquely determined by the family $P = (P_\mathfrak{p})_{\mathfrak{p}\in\mathbb{P}(\mathfrak{o})}$. By the previous lemma, $P_\mathfrak{p}$ is hyperspecial almost everywhere. Such a family P is called *coherent* in [Pra89].

It is well known ([Bor63, Theorem 5.1]) that the genus of integral forms corresponding to P decomposes into finitely many isomorphism classes represented by $\underline{G}_1, \dots, \underline{G}_{h(P)}$ say. Then the rational number

$$\operatorname{Mass}(P) = \sum_{i=1}^{h(P)} \frac{1}{\#\underline{G}_i(\mathfrak{o})}$$

is called the *mass* of P. Clearly, $h(P) \geq \operatorname{Mass}(P)$ and $h(P) = 1$ implies $\operatorname{Mass}(P)^{-1} \in \mathbb{Z}$.

10.2 The mass formula of Prasad

Let P be a coherent family of parahoric subgroups of G and let $\mathcal{G}$ be the unique quasi-split inner K-form of G. If $\mathcal{G}$ is of type ${}^6D_4$, let F/K be a cubic extension contained in the Galois extension of K over which $\mathcal{G}$ splits. In all other cases let F be the minimal extension of K over which $\mathcal{G}$ splits. If $\mathcal{G}$ splits over K, let $s(\mathcal{G}) = 0$, if $\mathcal{G}$ is a triality form of D_4, set $s(\mathcal{G}) = 7$ and if $\mathcal{G}$ is an outer form of E_6 let $s(\mathcal{G}) = 6$.

Fix a family $\mathcal{P} = (\mathcal{P}_\mathfrak{p})_{\mathfrak{p}\in\mathbb{P}(\mathfrak{o})}$ of maximal parahoric subgroups of $\mathcal{G}$ such that $\mathcal{P}_\mathfrak{p}$ is hyperspecial (special) if $\mathcal{G}$ splits (does not split) over the maximal unramified extension of $K_\mathfrak{p}$ and $\prod_{v\in V_\infty} \mathcal{G}(K_v) \times \prod_{\mathfrak{p}\in\mathbb{P}(\mathfrak{o})} \mathcal{P}_\mathfrak{p}$ is an open subgroup of $G(A)$. See [Pra89, Section 1.2] for more details.

Let $\overline{\mathcal{G}}_\mathfrak{p}$ and $\overline{G}_\mathfrak{p}$ be the groups $\mathcal{G}_\mathfrak{p} \otimes_{\mathfrak{o}_\mathfrak{p}} \mathfrak{o}_\mathfrak{p}/\mathfrak{p}$ and $G_\mathfrak{p} \otimes_{\mathfrak{o}_\mathfrak{p}} \mathfrak{o}_\mathfrak{p}/\mathfrak{p}$. By [Tit79, Section 3.5], both these groups admit a Levi decomposition over $\mathfrak{o}_\mathfrak{p}/\mathfrak{p}$. Hence there exists some maximal connected reductive $\mathfrak{o}_\mathfrak{p}/\mathfrak{p}$-subgroups $\mathcal{M}_\mathfrak{p}$ and $\overline{\mathrm{M}}_\mathfrak{p}$ such that $\overline{\mathcal{G}}_\mathfrak{p} = \mathcal{M}_\mathfrak{p}.R_u(\overline{\mathcal{G}}_\mathfrak{p})$ and $\overline{G}_\mathfrak{p} = \overline{\mathrm{M}}_\mathfrak{p}.R_u(\overline{G}_\mathfrak{p})$. Here R_u denotes the unipotent radical.

Further, let r be the rank of G and $(d_1, \dots, d_r)$ denote the degrees of $\mathcal{G}$. Then the dimension of G can be expressed as $\dim(G) = 2\sum_{i=1}^r d_i - r$.

In his seminal paper [Pra89], Prasad gave the following explicit formula for $\operatorname{Mass}(P)$.

Theorem 10.2.1 ([**Pra89**])

$$\operatorname{Mass}(P) = \mathrm{d}_K^{\dim G/2} \cdot \mathrm{Nr}_{K/\mathbb{Q}}(\mathrm{d}_{F/K})^{s(\mathcal{G})/2} \cdot \left(\prod_{i=1}^r \frac{(d_i - 1)!}{(2\pi)^{d_i}} \right)^n \cdot \prod_{\mathfrak{p}\in\mathbb{P}(\mathfrak{o})} \beta(P_\mathfrak{p}) \qquad (10.2.1)$$

where $\beta(P_\mathfrak{p}) = \dfrac{\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})^{(\dim \overline{\mathrm{M}}_\mathfrak{p} + \dim \mathcal{M}_\mathfrak{p})/2}}{\#\overline{\mathrm{M}}_\mathfrak{p}(\mathfrak{o}/\mathfrak{p})} > 1.$

For computational purposes, it is usually more convenient to express $\operatorname{Mass}(P)$ in terms of $\operatorname{Mass}(\mathcal{P})$ which is a product of special values of certain L-series of K. For $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$ let

$$\lambda(P_\mathfrak{p}) := \beta(P_\mathfrak{p})/\beta(\mathcal{P}_\mathfrak{p}) = \mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})^{(\dim \overline{\mathrm{M}}_\mathfrak{p} - \dim \mathcal{M}_\mathfrak{p})/2} \frac{\#\mathcal{M}_\mathfrak{p}(\mathfrak{o}/\mathfrak{p})}{\#\overline{\mathrm{M}}_\mathfrak{p}(\mathfrak{o}/\mathfrak{p})} .$$

Then $\mathrm{Mass}(P) = \mathrm{Mass}(\mathcal{P}) \cdot \prod_{\mathfrak{p} \in \mathbb{P}(\mathfrak{o})} \lambda(P_{\mathfrak{p}})$. Moreover, there is the following empirical fact.

Lemma 10.2.2 ([PY12, 2.5]) *The local factors $\lambda(P_{\mathfrak{p}})$ are integral.*

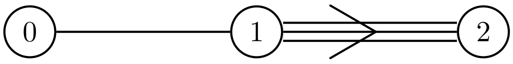
Proof. This follows from explicit computations using Bruhat-Tits theory. In most cases however, these computations can be avoided, see [PY12, 2.5] for details. □

10.3 The exceptional groups

10.3.1 The case G_2

Let $\mathbb{O}$ be the octonion algebra over K with totally definite norm form and denote by $\mathbb{O}^0$ its trace zero subspace. The automorphism group $\mathrm{Aut}(\mathbb{O})$ of $\mathbb{O}$, i.e. the stabilizer of the octonion multiplication in the special orthogonal group of $\mathbb{O}$ yields an algebraic group of type G_2 and $\mathbb{O}^0$ is an invariant subspace (cf. [SV00, Chapter 2]). Thus it yields an algebraic group $G < \mathrm{GL}_7$ of type G_2. Further, the construction shows that $G(K_{\mathfrak{p}})$ is of type G_2 for all prime ideals $\mathfrak{p}$ of $\mathfrak{o}$.

The extended Dynkin diagram of G_2 is as follows.



By [Tit79, 3.5.2], the parahoric subgroups $P_{\mathfrak{p}}$ of $G(K_{\mathfrak{p}})$ are in one-to-one correspondence with the non-empty subsets of $\{0, 1, 2\}$. For any non-empty subset T of $\{0, 1, 2\}$ let $P_{\mathfrak{p}}^{T}$ be the parahoric subgroup of $G(K_{\mathfrak{p}})$ whose Dynkin diagram is obtained from the extended Dynkin diagram of G_2 by omitting the vertices in T. For example, $P_{\mathfrak{p}}^{\{0\}}$ is hyperspecial and $P_{\mathfrak{p}}^{\{2\}}$ is of type A_2.

Theorem 10.3.1 *Suppose P is a coherent family of parahoric subgroups of G such that $h(P) = 1$. Then $K = \mathbb{Q}$ and P_p is hyperspecial for all primes $p \notin \{2, 3, 5\}$. The possible combinations (T_2, T_3, T_5) such that $P_p = P_p^{T_p}$ for $p \in \{2, 3, 5\}$ are given below.*

T_2	T_3	T_5	$\mathrm{Mass}(P)^{-1}$	$\underline{G}(\mathbb{Z})$	*sgdb*
$\{0\}$	$\{0\}$	$\{0\}$	$2^6 \cdot 3^3 \cdot 7$	$G_2(2)$	–
$\{0\}$	$\{0\}$	$\{2\}$	$2^5 \cdot 3$	$(C_4 \times C_4).S_3$	64
$\{0\}$	$\{2\}$	$\{0\}$	$2^4 \cdot 3^3$	$3_+^{1+2}.\mathrm{QD}_{16}$	520
$\{2\}$	$\{0\}$	$\{0\}$	$2^6 \cdot 3 \cdot 7$	$2^3.\,\mathrm{GL}_3(2)$	814
$\{2\}$	$\{2\}$	$\{0\}$	$2^4 \cdot 3$	$\mathrm{GL}_2(3)$	29
$\{1\}$	$\{0\}$	$\{0\}$	$2^6 \cdot 3^2$	$2_+^{1+4}.((C_3 \times C_3).2)$	8282[1]
$\{1, 2\}$	$\{0\}$	$\{0\}$	$2^6 \cdot 3$	$2_+^{1+4}.S_3$	1494
$\{0, 2\}$	$\{0\}$	$\{0\}$	$2^6 \cdot 3$	$((C_4 \times C_4).2).S_3$	956
$\{0, 1\}$	$\{0\}$	$\{0\}$	$2^6 \cdot 3$	$2_+^{1+4}.S_3$	988
$\{0, 1, 2\}$	$\{0\}$	$\{0\}$	2^6	$\mathrm{Syl}_2(G_2(2))$	134

The last column gives the label of the group $\underline{G}(\mathbb{Z})$ in the list of all groups of order $\mathrm{Mass}(P)^{-1} = \#\underline{G}(\mathbb{Z})$ *as defined by the small group database ([BEO01]).*

[1] The group is isomorphic to a index 2 subgroup of the automorphism group of the root lattice $\mathbb{F}_4$.

Proof. If G is of type G_2, then $F = K$, $r = 2$ and $(d_1, d_2) = (2, 6)$. In particular, $\dim G = 2(d_1 + d_2) - r = 14$. Thus Theorem 10.2.1 shows

$$h(P) \geq \mathrm{d}_K^7 \left(\frac{15}{32\pi^8}\right)^n .$$

Hence $h(P) = 1$ implies

$$\mathrm{d}_K^{1/n} \leq \left(\frac{32\pi^8}{15}\right)^{1/7} < 4.123 .$$

The tables [Voi08] show that K is one of $\mathbb{Q}$, $\mathbb{Q}(\sqrt{d})$ with $d \in \{2, 3, 5, 13\}$ or the maximal totally real subfield $\mathbb{Q}(\theta_7)$ of the seventh cyclotomic field $\mathbb{Q}(\zeta_7)$. The assumption $h(P) = 1$ forces $\mathrm{Mass}(P)^{-1} \in \mathbb{Z}$. Hence $\mathrm{Mass}(\mathcal{P})^{-1} \in \mathbb{Z}$ by Lemma 10.2.2. The exact values of $\mathrm{Mass}(\mathcal{P}) = 2^{-2n}|\zeta_K(-1)\zeta_K(-5)|$ for the various possible base fields K is given in the following table.

K	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{2})$	$\mathbb{Q}(\sqrt{3})$	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}(\sqrt{13})$	$\mathbb{Q}(\theta_7)$
$\mathrm{Mass}(\mathcal{P})$	$\frac{1}{2^6\cdot 3^3\cdot 7} = \frac{1}{\#G_2(2)}$	$\frac{361}{48384}$	$\frac{1681}{12096}$	$\frac{67}{302400}$	$\frac{33463}{157248}$	$\frac{7393}{84672}$

This shows that $K = \mathbb{Q}$ as claimed. For any given prime p, the local factor $\lambda(P_p)$ is given by the following table.

root system of P_p	$\emptyset$	A_1	A_2	$A_1 \times A_1$	G_2
$\lambda(P_p)$	$p^8 - p^6 - p^2 + 1$	$p^6 - 1$	$p^3 + 1$	$p^4 + p^2 + 1$	1

If $p \geq 23$ then $\#G_2(2) \cdot (p^3 + 1) > 1$ and therefore P_p is hyperspecial. For $p < 23$ one can simply check all possible combinations of P_p which yield $\mathrm{Mass}(P)^{-1} \in \mathbb{Z}$. This yields precisely the claimed combinations.

Let B be an Iwahori subgroup of G. The set of all $\mathbb{Z}_p B$-invariant lattices in $\mathbb{O}_p^0$ have been worked out in [CNP98]. For each candidate P one finds some lattice L such that the stabilizer $\underline{G}(\mathbb{Z})$ of L in $G_2 < \mathrm{GL}(\mathbb{O}^0)$ is of type P. It turns out that $\mathrm{Mass}(P)^{-1} = \#\underline{G}(\mathbb{Z})$ in all cases. □

10.3.2 The case F_4

Proposition 10.3.2 *Suppose G is of type F_4. Then there exists no coherent family P of parahoric subgroups of G with class number one.*

Proof. If G is of type F_4, then $r = 4$ and $(d_1, \dots, d_4) = (2, 6, 8, 12)$. In particular, $\dim G = 2\sum_i d_i - r = 52$ and Theorem 10.2.1 shows that

$$h(P) \geq \mathrm{d}_K^{26} \left(\frac{736745625}{8192\pi^{28}}\right)^n .$$

Hence $h(P) = 1$ implies

$$\mathrm{d}_K^{1/n} \leq \left(\frac{8192\pi^{28}}{736745625}\right)^{1/26} < 2.213 < \sqrt{5} .$$

Thus $K = \mathbb{Q}$ and

$$\mathrm{Mass}(\mathcal{P}) = \frac{736745625}{8192\pi^{28}} \cdot \prod_{i=1}^{4} \zeta_{\mathbb{Q}}(d_i) = \frac{1}{4}\prod_{i=1}^{4} |\zeta_{\mathbb{Q}}(1-d_i)| = \frac{691}{2^{15}3^{6}5^{2}7^{2}13}\,.$$

In particular, $\mathrm{Mass}(P)^{-1} \notin \mathbb{Z}$. □

Note that if $K = \mathbb{Q}$, then $\mathcal{P}$ is the model in the sense of Gross and it actually has class number 2 (see [Gro96, Proposition 5.3]).

10.3.3 Triality of D_4

Let G be of type ${}^3D_4$ or ${}^6D_4$. The field F is a totally real cubic extension of K. The extension is normal (and thus cyclic) if and only if G is of type ${}^3D_4$.

Lemma 10.3.3 *Suppose G is a K-form of D_4 and P a parahoric family of G with class number one. Then the base field K is either $\mathbb{Q}$, $\mathbb{Q}(\sqrt{d})$ with $d \in \{2, 3, 5, 13, 17\}$ or the maximal totally real subfield $\mathbb{Q}(\theta_e)$ of $\mathbb{Q}(\zeta_e)$ for $e \in \{7, 9\}$.*

Proof. If G is any form of D_4, then $r = 4$ and $(d_1, \ldots, d_4) = (2, 4, 4, 6)$. Hence $\dim G = 2\sum_i d_i - r = 28$. Thus Theorem 10.2.1 shows that

$$h(P) \geq \mathrm{Mass}(P) \geq \mathrm{d}_K^{14}\left(\frac{135}{2^{11}\pi^{16}}\right)^n .$$

So $h(P) = 1$ implies

$$\mathrm{d}_K^{1/n} \leq \left(\frac{2^{11}\pi^{16}}{135}\right)^{1/14} < 4.493\,.$$

The result now follows from the tables of totally real number fields [Voi08]. □

Let $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$ be a prime ideal of norm q. By [Tit79, Section 4], the type of G at $\mathfrak{p}$ is (using the notation of [Tit79, Tables 4.2 and 4.3])

$$\begin{cases} {}^1D_4 & \text{if } \mathfrak{p} \text{ is completely split in } F, \\ {}^3D_4 & \text{if } F_\mathfrak{p}/K_\mathfrak{p} \text{ is an unramified cubic field extension,} \\ G_2^1 & \text{if } F_\mathfrak{p}/K_\mathfrak{p} \text{ is a ramified cubic field extension,} \\ {}^2D_4 & \text{if } F_\mathfrak{p} \cong K_\mathfrak{p} \oplus F'_\mathfrak{p} \text{ for some unramified quadratic extension } F'_\mathfrak{p}/K_\mathfrak{p}, \\ B\!-\!C_3 & \text{if } F_\mathfrak{p} \cong K_\mathfrak{p} \oplus F'_\mathfrak{p} \text{ for some ramified quadratic extension } F'_\mathfrak{p}/K_\mathfrak{p}. \end{cases}$$

Therefore $\beta(\mathcal{P}_\mathfrak{p}) = \left(1 - \frac{1}{q^2}\right)\left(1 - \frac{1}{q^6}\right) \cdot \beta'_\mathfrak{p}$ where $\beta'_\mathfrak{p}$ is given by

$$\begin{cases} \left(1 - \frac{1}{q^4}\right)^2 & \text{if } \mathfrak{p} \text{ is completely split in } F, \\ 1 + \frac{1}{q^4} + \frac{1}{q^8} & \text{if } F_\mathfrak{p}/K_\mathfrak{p} \text{ is an unramified cubic field extension,} \\ 1 & \text{if } F_\mathfrak{p}/K_\mathfrak{p} \text{ is a ramified cubic field extension,} \\ \left(1 + \frac{1}{q^4}\right)\left(1 - \frac{1}{q^4}\right) & \text{if } F_\mathfrak{p} = K_\mathfrak{p} \oplus F'_\mathfrak{p} \text{ for some unramified extension } F'_\mathfrak{p}/K_\mathfrak{p}, \\ 1 - \frac{1}{q^4} & \text{if } F_\mathfrak{p} = K_\mathfrak{p} \oplus F'_\mathfrak{p} \text{ for some ramified extension } F'_\mathfrak{p}/K_\mathfrak{p}. \end{cases}$$

The functional equation for L-series shows that

$$\mathrm{Mass}(\mathcal{P}) = 2^{-4n} \cdot |\zeta_K(-1) \cdot \mathfrak{L}_K(\chi, -3) \cdot \zeta_K(-5)| \tag{10.3.1}$$

where χ denotes the non-trivial character of $\mathrm{Gal}(F/K)$, see also [PY12, Section 2.8].

Proposition 10.3.4 *If G is of type ${}^3D_4$ or ${}^6D_4$ then there exists no coherent parahoric family of class number one.*

Proof. If G admits a one-class parahoric family P, then

$$1 \geq \mathrm{Mass}(P) \geq \mathrm{Mass}(\mathcal{P}) > \mathrm{d}_K^{7/2}\, \mathrm{d}_F^{7/2} \left(\frac{135}{2^{11}\pi^{16}} \right)^n$$

or equivalently, $\mathrm{d}_F \leq \mathrm{d}_K^{-1} \cdot \left(\frac{2^{11}\pi^{16}}{135}\right)^{2n/7}$. By Lemma 10.3.3, there are only finitely many candidates for K. For each such field K, [Voi08] lists all possible cubic extensions F that satisfy the previous inequality. It turns out that $K = \mathbb{Q}$ and $F = \mathbb{Q}[x]/(f(x))$ where $f(x)$ is one of the ten polynomials given below. In each case, $\mathrm{Mass}(\mathcal{P})$ can be evaluated explicitly using equation (10.3.1).

$f(x)$	$\mathrm{Mass}(\mathcal{P})$
$x^3 - x^2 - 2x + 1$	$79/84672$
$x^3 - 3x - 1$	$199/36288$
$x^3 - x^2 - 3x + 1$	$577/12096$
$x^3 - x^2 - 4x - 1$	$11227/157248$
$x^3 - 4x - 1$	$1333/6048$
$x^3 - x^2 - 4x + 3$	$1891/6048$
$x^3 - x^2 - 4x + 2$	$2185/3024$
$x^3 - x^2 - 4x + 1$	$925/1344$
$x^3 - x^2 - 6x + 7$	$4087/4032$
$x^3 - x^2 - 5x - 1$	$19613/12096$

The result now follows from the fact that $\mathrm{Mass}(P)$ is an integral multiple of $\mathrm{Mass}(\mathcal{P})$ and therefore never the reciprocal of an integer. □

10.3.4 The case E_6

Let G be a form of E_6. The assumption that $GK_v)$ is anisotropic for all infinite places v of K forces G to be of type ${}^2E_6$. Thus the splitting field F of G is a totally complex quadratic extension of K.

Proposition 10.3.5 *There exists no coherent family P of parahoric subgroups of G with class number one.*

Proof. If G is of type ${}^2E_6$, then $r = 6$, $(d_1, \dots, d_6) = (2, 5, 6, 8, 9, 12)$, $s(\mathcal{G}) = 26$ and $\dim G = 78$. Suppose P is a parahoric family of class number one. Then Theorem 10.2.1 implies

$$1 = h(P) \geq \mathrm{Mass}(P) > \mathrm{d}_K^{39} \cdot \mathrm{Nr}_{K/\mathbb{Q}}(\mathrm{d}_{F/K})^{13} \cdot \gamma^n \geq \mathrm{d}_K^{39} \cdot \gamma^n \text{ where } \gamma := \prod_{i=1}^{6} \frac{(d_i - 1)!}{(2\pi)^{d_i}}$$

and therefore $\mathrm{d}_K^{1/n} < \gamma^{-1/39} < 2.31$. Hence K is either $\mathbb{Q}$ or $\mathbb{Q}(\sqrt{5})$.
If $K = \mathbb{Q}(\sqrt{5})$, then $\mathrm{Nr}_{K/\mathbb{Q}}(\mathrm{d}_{F/K}) \geq 4$. Hence $h(P) > 5^{39} \cdot 4^{13} \cdot \gamma^2 > 1$. So $K = \mathbb{Q}$ and $1 = h(P) > \mathrm{d}_F^{13} \cdot \gamma$ implies that $\mathrm{d}_F \leq 12$. Thus F is $\mathbb{Q}(\sqrt{-d})$ for some $d \in \{1, 2, 3, 7, 11\}$. For any $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$, the group G is quasi-split over $K_\mathfrak{p}$. Moreover, the type of G over $K_\mathfrak{p}$ is ${}^1E_6$, ${}^2E_6$ or F_4^I (using the notation of [Tit79, Section 4]) depending on whether $\mathfrak{p}$ is split, inert or ramified in F. Thus $\beta(\mathcal{P}_\mathfrak{p})^{-1}$ equals

$$(1 - q^{-2})(1 - q^{-6})(1 - q^{-8})(1 - q^{-12}) \cdot \begin{cases} (1 - q^{-5})(1 - q^{-9}) & \text{if } \mathfrak{p} \text{ is split in } F, \\ (1 + q^{-5})(1 + q^{-9}) & \text{if } \mathfrak{p} \text{ is inert in } F, \\ 1 & \text{if } \mathfrak{p} \text{ is ramified in } F, \end{cases}$$

where $q = \mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})$. Let χ be the nontrivial character of $\mathrm{Gal}(F/\mathbb{Q})$. The functional equation for L-series shows that

$$\mathrm{Mass}(\mathcal{P}) = 2^{-6} \cdot |\zeta_\mathbb{Q}(-1) \cdot \mathfrak{L}_\mathbb{Q}(\chi, -4) \cdot \zeta_\mathbb{Q}(-5) \cdot \zeta_\mathbb{Q}(-7) \cdot \mathfrak{L}_\mathbb{Q}(\chi, -8) \cdot \zeta_\mathbb{Q}(-11)| \,.$$

The values for $\mathrm{Mass}(\mathcal{P})$ for all possible fields $F = \mathbb{Q}(\sqrt{-d})$ are

d	1	2	3	7	11
$\mathrm{Mass}(\mathcal{P})$	$\frac{191407}{243465191424}$	$\frac{1097308691}{169073049600}$	$\frac{559019}{30813563289600}$	$\frac{6102221}{5200977600}$	$\frac{7340406625}{18598035456}$

In particular, there exists no parahoric family P such that $\mathrm{Mass}(P)^{-1} \in \mathbb{Z}$. □

10.3.5 The case E_7

Proposition 10.3.6 *If G is of type E_7 then there exists no coherent family P of parahoric subgroups of G with class number one.*

Proof. If G is of type E_7 then $r = 7$, $(d_1, \dots, d_7) = (2, 6, 8, 10, 12, 14, 18)$ and $\dim G = 133$. If $h(P) = 1$, then Theorem 10.2.1 implies that

$$\mathrm{d}_K^{1/n} < \left(\prod_{i=1}^{7} \frac{(2\pi)^{d_i}}{(d_i - 1)!} \right)^{2/133} < 1.547 < \sqrt{5}\,.$$

Thus $K = \mathbb{Q}$ and then

$$\mathrm{Mass}(\mathcal{P}) = 2^{-7} \prod_{i=1}^{7} |\zeta_\mathbb{Q}(1 - d_i)| = \frac{691 \cdot 43867}{2^{24} 3^{11} 5^2 7^3 11^1 13^1 19^1}$$

shows that $h(P) > 1$ for all parahoric families P. □

10.3.6 The case E_8

Proposition 10.3.7 *If G is of type E_8 and P is a coherent family of parahoric subgroups of G then $h(P) \geq 8435$.*

Proof. If G is of type E_8 then $r = 8$ and $(d_1, \ldots, d_8) = (2, 8, 12, 14, 18, 20, 24, 30)$. Thus Theorem 10.2.1 implies that

$$h(P) \geq \mathrm{Mass}(P) > \prod_{i=1}^{8} \frac{(d_i - 1)!}{(2\pi)^{d_i}} > 8434\,.$$

□

Bibliography

[Bac95] C. Bachoc. Voisinage au sens de Kneser pour les réseaux quaternioniens. *Comment. Math. Helv.*, 70(3):350–374, 1995.

[Bar68] K. Barner. Über die quaternäre Einheitsform in total reellen algebraischen Zahlkörpern. *J. Reine Angew. Math.*, 229:194–208, 1968.

[BCP97] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997.

[BD08] S. Brueggeman and D. Doud. Local corrections of discriminant bounds and small degree extensions of quadratic base fields. *Int. J. Number Theory*, 4:349–361, 2008. See also http://www.math.byu.edu/~doud/DiscBound.html.

[Bel03] C. N. Beli. Integral spinor norm groups over dyadic local fields. *J. Number Theory*, 102(1):125–182, 2003.

[BEO01] H. U. Besche, B. Eick, and E. A. O'Brien. The groups of order at most 2000. *Electron. Res. Announc. Amer. Math. Soc.*, 7:1–4, 2001.

[BN97] C. Bachoc and G. Nebe. Classification of two genera of 32-dimensional lattices over the Hurwitz order. *Exp. Math.*, 6(2):151–162, 1997.

[Bor63] A. Borel. Some finiteness properties of adele groups over number fields. *Publ. Math. I.H.E.S.*, 16:5–30, 1963.

[BP91] W. Bosma and M. Pohst. Computations with Finitely Generated Modules over Dedekind Rings. In *Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation*, ISSAC '91, pages 151–156, New York, NY, USA, 1991. ACM.

[Bra43] H. Brandt. Zur Zahlentheorie der Quaternionen. *Jber. Deutsch. Math. Verein.*, 53:23–57, 1943.

[Brz80] J. Brzezinski. Arithmetical quadratic surfaces of genus 0, I. *Math. Scand.*, 46:183–208, 1980.

[Brz82] J. Brzezinski. A characterization of Gorenstein orders in quaternion algebras. *Math. Scand.*, 50:19–24, 1982.

[Cas78] J. W. S. Cassels. *Rational Quadratic Forms*, volume 13 of *LMS Monographs*. LMS, 1978.

[Cha13] W. K. Chan. Spinor genera, 2013. Personal communication.

[Cho] S. Cho. A uniform construction of smooth integral models and a recipe for computing local densities. submitted.

[Cho15] S. Cho. Group schemes and local densities of quadratic lattices in residue characteristic 2. *Compositio Math*, 151:793–827, 2015.

[CNP98] A. Cohen, G. Nebe, and W. Plesken. Maximal integral forms of the algebraic group G_2 defined by finite subgroups. *J. Number Theory*, 72(2):282–308, 1998.

[CS99] J. H. Conway and N. J. A. Sloane. *Sphere packings, lattices and groups*, volume 290 of *Grundlehren der Mathematischen Wissenschaften.* Springer-Verlag, New York, third edition, 1999.

[Dze60] J. Dzewas. Quadratsummen in reellquadratischen Zahlkörpern. *Math. Nachr*, 21:233–284, 1960.

[EE81] A. G. Earnest and D. R. Estes. An algebraic approach to the growth of class numbers of binary quadratic lattices. *Mathematika*, 28(2):160–168 (1982), 1981.

[Eic52] M. Eichler. *Quadratische Formen und orthogonale Gruppen.* Springer, 1952.

[Eic55] M. Eichler. Zur Zahlentheorie der Quaternionen-Algebren. *J. Reine u. Angew. Math.*, 195:127–151, 1955. Berichtigung in: *J. Reine u. Angew. Math.* 197 (1957), S. 220.

[Gau01] C.-F. Gauß. *Disquisitiones Arithmeticae.* G. Fleischer (Leipzig), 1801.

[Ger72] L. Gerstein. The growth of class numbers of quadratic forms. *Amer. J. Math.*, 94(1):221–236, 1972.

[GHY01] W. T. Gan, J. Hanke, and J.-K. Yu. On an exact mass formula of Shimura. *Duke Mathematical Journal*, 107, 2001.

[Gro96] B. H. Gross. Groups over $\mathbb{Z}$. *Invent. Math.*, 124(1-3):263–279, 1996.

[GY00] W. T. Gan and J.-K. Yu. Group schemes and local densities. *Duke Math. J.*, 105(3):497–524, 12 2000.

[Has85] H. Hasse. *Über die Klassenzahl abelscher Zahlkörper.* Springer Verlag, 1985.

[Hof91] D. W. Hoffmann. On positive definite hermitian forms. *Manuscripta Math.*, 71:399–429, 1991.

[Jac62] R. Jacobowitz. Hermitian forms over local fields. *Amer. J. Math.*, 84:441–465, 1962.

[Joh68] A. A. Johnson. Integral representations of hermitian forms over local fields. *J. Reine Angew. Math.*, 229:57–80, 1968.

[Kir] M. Kirschmer. One-class genera of exceptional groups. submitted.

[Kir14] M. Kirschmer. One-class genera of maximal integral quadratic forms. *J. Number Theory*, 136:375–393, 2014.

[Kir16] M. Kirschmer. Hermitian forms with small class number. see http://www.math.rwth-aachen.de/~kirschme/forms/, 2016.

[KL13] M. Kirschmer and D. Lorch. Single-class genera of positive integral lattices. *LMS J. Comput. Math.*, 16:172–186, 2013.

[KL16] M. Kirschmer and D. Lorch. Ternary quadratic forms over number fields with small class number. *J. Number Theory*, 161:343–361, 2016.

[Kne56] M. Kneser. Klassenzahlen indefiniter quadratischer Formen in drei oder mehr Veränderlichen. *Arch. Math. (Basel)*, 7:323–332, 1956.

[Kne57] M. Kneser. Klassenzahlen definiter quadratischer Formen. *Archiv d. Math.*, 8:241–250, 1957.

[Kne66] M. Kneser. Strong approximation. In *Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965)*, pages 187–196. Amer. Math. Soc., Providence, R.I., 1966.

[Kne02] M. Kneser. *Quadratische Formen*. Springer-Verlag, Berlin, 2002. Revised and edited in collaboration with Rudolf Scharlau.

[Kör81] O. Körner. Class numbers of binary quadratic lattices over algebraic number fields. *Acta Arith.*, 39(3):269–279, 1981.

[KV10] M. Kirschmer and J. Voight. Algorithmic enumeration of ideal classes for quaternion orders. *SIAM J. Comput. (SICOMP)*, 39(5):1714–1747, 2010.

[LK06] G.-N. Lee and S.-H. Kwon. CM-fields with relative class number one. *Math. Comp.*, 75(254):997–1013 (electronic), 2006.

[Lor] D. Lorch. Einklassige Geschlechter orthogonaler Gruppen. In preparation.

[Lou90] S. Louboutin. Minorations (sous l'hypothèse de Riemann généralisée) des nombres de classes des corps quadratiques imaginaires. Application. *C. R. Acad. Sci. Paris Sér. I Math.*, 310(12):795–800, 1990.

[Lou06] S Louboutin. Lower bounds for relative class numbers of imaginary abelian number fields and CM-fields. *Acta Arith.*, 121(3):199–220, 2006.

[Min87] H. Minkowski. Zur Theorie der Positiven Quadratischen Formen. *J. Reine u. Angew. Math.*, 101:196–202, 1887.

[Neb98] G. Nebe. Finite quaternionic matrix groups. *Represent. Theory*, 2:106–223, 1998.

[Neu06] J. Neukirch. *Algebraische Zahlentheorie.* Springer, 2006.

[O'M73] O. T. O'Meara. *Introduction to Quadratic Forms.* Springer, 1973.

[Pet69] M. Peters. Ternäre und quaternäre quadratische Formen und Quaternionenalgebren. *Acta Arith.*, 15:329–365, 1968/1969.

[Pfe71a] H. Pfeuffer. Einklassige Geschlechter totalpositiver quadratischer Formen in totalreellen algebraischen Zahlkörpern. *J. Number Theory*, 3:371–411, 1971.

[Pfe71b] H. Pfeuffer. Quadratsummen in totalreellen algebraischen Zahlkörpern. *J. Reine Angew. Math.*, 249:208–216, 1971.

[Pfe81] H. Pfeuffer. Komposition und Klassenzahlen binärer quadratischer Formen. *Acta Arith.*, 39:323–337, 1981.

[Pra89] G. Prasad. Volumes of S-arithmetic quotients of semi-simple groups. *Institut des Hautes Études Scientifiques. Publications Mathématiques*, 69:91–117, 1989.

[PS97] W. Plesken and B. Souvignier. Computing Isometries of Lattices. *Journal of Symbolic Computation*, 24:327–334, 1997.

[PY12] G. Prasad and S.-K. Yeung. Nonexistence of arithmetic fake compact Hermitian symmetric spaces of type other than A_n $(n \leq 4)$. *J. Math. Soc. Japan*, 64(3):683–731, 2012.

[Rei03] I. Reiner. *Maximal Orders.* Oxford Science Publications, 2003.

[Sch85] W. Scharlau. *Quadratic and Hermitian forms*, volume 270 of *Grundlehren der mathematischen Wissenschaften.* Springer, 1985.

[Sch94] R. Scharlau. Unimodular lattices over real quadratic fields. *Mathematische Zeitschrift*, 216:437–452, 1994.

[Sch98] A. Schiemann. Classification of Hermitian Forms with the Neighbor Method. *J. Symbolic Computation*, 26:487–508, 1998.

[SH98] R. Scharlau and B. Hemkemeier. Classification of integral lattices with large class number. *Math. Comp.*, 67(222):737–749, 1998.

[Shi64] G. Shimura. Arithmetic of unitary groups. *Ann. Math.*, 79:269–409, 1964.

[Shi97] G. Shimura. Euler products and Eisenstein series. In *CBMS Reg. Conf. Ser. Math.*, volume 93. AMS, 1997.

[Shi99a] G. Shimura. An exact mass formula for orthogonal groups. *Duke Mathematical Journal*, 97(1):1–66, 1999.

[Shi99b] G. Shimura. Some exact formulas on quaternion unitary groups. *J. Reine Angew. Math.*, 509:67–102, 1999.

[Sie35] C. L. Siegel. über die Analytische Theorie der quadratischen Formen. *Annals of Mathematics*, 36(3):527–606, 1935.

[Sie37] C. L. Siegel. über die Analytische Theorie der quadratischen Formen III. *Annals of Mathematics*, 38(1):212–291, 1937.

[SV00] T. A. Springer and F. D. Veldkamp. *Octonions, Jordan Algebras and Exceptional Groups*. Springer Monographs in Mathematics. Springer-Verlag, 2000.

[Tit79] J. Tits. Reductive groups over local fields. In *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math.*, volume 33, pages 29–69. Amer. Math. Soc., Providence, R.I., 1979.

[Voi08] J. Voight. Enumeration of totally real number fields of bounded root discriminant. In A. van der Poorten and A. Stein, editors, *Algorithmic number theory (ANTS VIII, Banff, 2008)*, volume 5011 of *Lecture Notes in Comp. Sci.*, pages 268–281. Springer, 2008. See also https://math.dartmouth.edu/~jvoight/nf-tables/index.html.

[Voi11] J. Voight. Characterizing quaternion rings over an arbitrary base. *J. Reine Angew. Math.*, 657:113–134, 2011.

[Voi13] J. Voight. Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms. In K. Alladi, M. Bhargava, D. Savitt, and P. H. Tiep, editors, *Quadratic and higher degree forms*, volume 31 of *Developments in Mathematics*. Springer, 2013.

[Wat] G. L. Watson. One-class genera of positive quadratic forms in six variables. unpublished.

[Wat62] G. L. Watson. Transformations of a quadratic form which do not increase the class-number. *Proc. London Math. Soc. (3)*, 12:577–587, 1962.

[Wat63] G. L. Watson. The class-number of a positive quadratic form. *Proc. London Math. Soc. (3)*, 13:549–576, 1963.

[Wat72] G. L. Watson. One-class genera of positive ternary quadratic forms. *Mathematika*, 19:96–104, 1972.

[Wat74] G. L. Watson. One-class genera of positive quaternary quadratic forms. *Acta Arith.*, 24:461–475, 1974. Collection of articles dedicated to Carl Ludwig Siegel on the occasion of his seventy-fifth birthday, V.

[Wat76] G. L. Watson. The 2-adic density of a quadratic form. *Mathematika*, 23:94–106, 1976.

[Wat78] G. L. Watson. One-class genera of positive quadratic forms in nine and ten variables. *Mathematika*, 25(1):57–67, 1978.

[Wat82] G. L. Watson. One-class genera of positive quadratic forms in eight variables. *J. London Math. Soc. (2)*, 26(2):227–244, 1982.

[Wat84] G. L. Watson. One-class genera of positive quadratic forms in seven variables. *Proc. London Math. Soc. (3)*, 48(1):175–192, 1984.

[Wat04] M. Watkins. Class numbers of imaginary quadratic fields. *Math. Comp.*, 73(246):907–938 (electronic), 2004.

[Wei73] P. Weinberger. Exponents of the class groups of complex quadratic fields. *Acta Arith.*, 22:117–124, 1973.

[Zas62] H. Zassenhaus. On the spinor norm. *Arch. Math.*, 13:434–451, 1962.

[Zas72] 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.

Index