2014-10-08

Algorithmic enumeration of quaternionic lattices

Chisholm, Sarah

UNIVERSITY OF CALGARY

Algorithmic enumeration of quaternionic lattices

by

Sarah Chisholm

A DISSERTATION

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF DOCTOR OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS AND STATISTICS

CALGARY, ALBERTA

September, 2014

Abstract

In this thesis, we develop and implement an algorithm in Magma for enumerating isometry classes of quaternionic lattices. This algorithm can be viewed as a higher rank generalization of that used for enumerating equivalence classes of left-ideals of quaternionic orders. Our key technical innovation is an adaptation of Kneser's method of neighbours to the setting of quaternionic lattices. Central to this adaptation is the Morita equivalence between Hermitian spaces over the split quaternion algebra $\mathrm{M}_2(F)$ and symplectic spaces over F.

Acknowledgements

I am indebted to my advisors Mark Bauer and Matthew Greenberg. Matt – thank you for suggesting this incredible project and leading me along the way. Mark – you were so unbelievably helpful and supportive throughout this entire process, for which I will be eternally grateful.

Thank you to the wonderful members of the number theory group at University of Calgary for inspiration and being a great community to be apart of. Especially Clifton Cunningham, Renate Scheidler, Richard Guy, Michael Jacobson, Diane Fenton, Jean-François Biasse, Marie-Andrée Langlois, Colin Weir, Jason Nicholson and many, many others. Thank you John Voight for numerous helpful discussions. I would like to extend a thank you to the examining committee for the all of the wonderful feedback: Wayne Eberly and Sebastian Pauli.

Thanks to the lovely Preceptor group at Harvard for being so supportive. Especially Robin Gottlieb, Peter Garfield, Jameel Al-Aidroos, Janet Chen, Oliver Knill and Susan Milano. Also thanks to Kate Penner.

Finally, thank you to my amazing family: Karen, Bernie and Steve Chisholm. Thanks to my dearest friends Susan Harvey, Luda Korobenko, Tanya Bukharina, Jennifer Park, Jennifer Balakrishnan, Alyson Deines, Jennifer Boivin and Mindy MacDonald. Lastly, thank you Christopher Tabone for your support during the final stages of this work.

Table of Contents

Chapter 1

Introduction

1.1 Objective

Let F be the field of fractions of the Dedekind[1] domain $\mathfrak{o}_F$. Let V be an F-vector space of dimension n.

Definition 1. *An $\mathfrak{o}_F$-lattice in V is a finitely generated $\mathfrak{o}_F$-submodule $L \subset V$ such that $FL = V$. We write $\mathcal{L}(V)$ for the set of lattices in V.*

$$\begin{array}{ccc} L & \overset{\subset}{\longrightarrow} & V \\ \vdots & & \vdots\ n \\ \mathfrak{o}_F & \overset{\subset}{\longrightarrow} & F \end{array}$$

$\mathcal{L}(V)$ and some of its distinguished subsets are the main objects of study in this thesis.

Let $L \in \mathcal{L}(V)$. Since L is an $\mathfrak{o}_F$-submodule of V and V is F-torsion free, L is a fortiori $\mathfrak{o}_F$-torsion free. Therefore, by the structure theory of finitely generated modules over Dedekind domains [4, §1.2], L is locally free (equivalently, projective). Moreover, by the structure theorem, there is a basis $(v_1, \ldots, v_n)$ of V and a fractional ideal $\mathfrak{a}$ of $\mathfrak{o}_F$ such that

$$L = \mathfrak{a}v_1 + \mathfrak{o}_F v_2 + \cdots \mathfrak{o}_F v_n.$$

The ideal $\mathfrak{a}$ clearly depends on the basis $(v_1, \ldots, v_n)$. If $t \in F^\times$ then

$$L = (t\mathfrak{a})(t^{-1}v_1) + \mathfrak{o}_F v_2 + \cdots \mathfrak{o}_F v_n.$$

The ideal class

$$a_L := [\mathfrak{a}] \in \mathrm{Cl}(\mathfrak{o}_F),$$

[1] We begin with the general setting of the field of fractions of a Dedekind domain, to keep the theory as general as possible. When the field taken must be a number field, it will be specified.

however, does not depend on the chosen basis. In particular, L is a free $\mathfrak{o}_F$-module if and only if a_L is the trivial class in $\mathrm{Cl}(\mathfrak{o}_F)$.

Definition 2. *Two lattices $L, M \in \mathcal{L}(V)$ are* $\mathrm{GL}(V)$-equivalent *if there is a transformation $\sigma \in \mathrm{GL}(V)$ such that*[2] *$M = L\sigma$.*

Lemma 3.

1. *L and M are $\mathrm{GL}(V)$-equivalent if and only if $a_L = a_M$.*
2. *$L \mapsto a_L$ descends to isomorphism $\mathcal{L}(V)/\mathrm{GL}(V) \xrightarrow{\sim} \mathrm{Cl}(\mathfrak{o}_F)$.*

Proof.

1. Write $L = \mathfrak{a}v_1 + \mathfrak{o}_F v_2 + \cdots + \mathfrak{o}_F v_n$ and $M = \mathfrak{b}v_1' + \mathfrak{o}_F v_2' + \cdots + \mathfrak{o}_F v_n'$. Suppose that $a_L = a_M$, i.e. $[\mathfrak{a}] = [\mathfrak{b}]$. Then there exists an element $x \in F$ such that $x\mathfrak{a} = \mathfrak{b}$. Let σ be the unique map satisfying

$$\begin{aligned} v_1 &\mapsto xv_1' \\ v_i &\mapsto v_i', \quad i = 2, \ldots, n. \end{aligned}$$

   Then

$$\begin{aligned} L\sigma &= (\mathfrak{a}v_1 + \mathfrak{o}_F v_2 + \cdots + \mathfrak{o}_F v_n)\sigma \\ &= \mathfrak{b}v_1' + \mathfrak{o}_F v_2' + \cdots + \mathfrak{o}_F v_n' \\ &= M. \end{aligned}$$

   Following this argument in reverse gives the converse.

2. The statement follows from part 1.

□

[2] *We write vector in F^n as* row *vectors and represent linear transformations $F^m \to F^n$ by multiplication on the* right *by $m \times n$ matrices. This will prove convenient when working with* left *modules over noncommutative rings. Additionally,* Magma *uses these conventions.*

The situation becomes significantly richer if we restrict the notion of equivalence, requiring that it respect additional structure. The prototypical situation is as follows: Suppose that

$$f : V \times V \longrightarrow F$$

is a nondegenerate, symmetric, bilinear form, making (V, f) a *quadratic F-space*. Let $G^0(V, f)$ be the *orthogonal group of* (V, f):

$$G^0(V, f) = \{\varphi \in \mathrm{GL}(V) : f(x\varphi, y\varphi) = f(x, y) \text{ for all } x, y \in V\}.$$

The notion of $G^0(V, f)$-equivalence – analogous with Definition 2 – of $\mathfrak{o}_F$-lattices in V is very subtle indeed. In fact, even the simpler[3] problem of characterizing $G^0(V_\mathfrak{p}, f)$-equivalence of $\mathfrak{o}_{F,\mathfrak{p}}$-lattices in $V_\mathfrak{p}$ is nontrivial.[4] Here, $\mathfrak{p}$ is a prime ideal of $\mathfrak{o}_F$ and subscript $\mathfrak{p}$ indicates completion at $\mathfrak{p}$. Although nontrivial, the problem of classifying $G^0(V_\mathfrak{p}, f)$-equivalence classes of lattices in $V_\mathfrak{p}$ is doable – and included in this thesis. One can define a system of explicitly computable $\mathfrak{p}$-adic invariants[5] (discriminant, Witt invariant, etc.) that solve the classification problem in this local situation. For an $\mathfrak{o}_F$-lattice L in V, let

$$\mathrm{gen}_{G^0(V,f)}(L)$$

be the set of lattices that are $G^0(V_\mathfrak{p}, f)$-equivalent to $L_\mathfrak{p}$ for every $\mathfrak{p}$. This set is called the *$G^0(V, f)$-genus of L*. Although the $G^0(V, f)$-equivalence of two $\mathfrak{o}_F$-lattices L and M implies the $G^0(V_\mathfrak{p}, f)-$equivalence of $L_\mathfrak{p}$ and $M_\mathfrak{p}$ for every $\mathfrak{p}$, the converse need not be true – see, for example, §3.8.3. In other words, the *class set of L*, for $G = G^0(V, f)$

$$\mathrm{cl}_G(L) := \mathrm{gen}_{G^0(V,f)}(L)/G^0(V, f)$$

is typically nontrivial. Understanding $\mathrm{cl}_G(L)$ is a component of understanding classical modular forms, as these form the domain of the functions [9]. One may also view understanding

[3]The problem is simpler in the sense that we can restrict our attention to a single prime.

[4]Even the classification problem for quadratic spaces (V, f) themselves is nontrivial! Hence the impetus for Kneser's work with the $\mathfrak{p}-$neighbours algorithm.

[5]I.e. specific features of lattices that one would like to preserve among equivalent lattices.

$\mathrm{cl}_G(L)$ as a fundamental arithmetic problem in Number Theory. Much effort has been expended in devising and implementing algorithms for computing it. Kneser [12] computed the genus of a positive definite quadratic form over $\mathbb{Z}$. Schulze-Pillot [18] enumerated the genus of ternary and quaternary quadratic forms over $\mathbb{Z}$. Iyanaga [11] worked out the class number of unimodular positive definite Hermitian forms over $\mathbb{Z}[i]$ with dimension at most 7. Hoffman [10] later generalized this work to imaginary quadratic fields with discriminant -3 and -20. Schiemann [17] took this further for imaginary quadratic fields up to discriminant -455. An efficient algorithm for computing the genus is based on Kneser's method [12] of $\mathfrak{p}$-neighbours. Two $\mathfrak{o}_F$-lattices L and M in V are called $\mathfrak{p}$-neighbours if[6]

$$L/(L \cap M) \approx \mathbb{F}_\mathfrak{p} \quad \text{and} \quad M/(L \cap M) \approx \mathbb{F}_\mathfrak{p}$$

where $\mathbb{F}_\mathfrak{p} := \mathfrak{o}_F/\mathfrak{p}$ is the residue class field of $\mathfrak{p}$. Write $\mathcal{N}_\mathfrak{p}(L)$ for the set of $\mathfrak{p}$-neighbours of L. Due to the symmetry in the definition, L is a $\mathfrak{p}$-neighbour of M if and only if M is a $\mathfrak{p}$-neighbour of L. Also, it is easy to see that $\mathcal{N}_\mathfrak{p}(L)$ is stable under the natural action of $G^0(V, f)$; see Corollary 77. Let M be a $\mathfrak{p}$-neighbour of L.

Then:

- $L_\mathfrak{q} = M_\mathfrak{q}$ for all $\mathfrak{q} \neq \mathfrak{p}$ (equality as subsets of $V_\mathfrak{q}$).
- $L_\mathfrak{p}$ and $M_\mathfrak{p}$ are $G^0(V_\mathfrak{p}, f)$-equivalent.

Thus,

$$\mathcal{N}_\mathfrak{p}(L) \subset \mathrm{gen}_{G^0(V,f)}(L).$$

To compute representatives for the class set, we have implemented a quaternionic generalization of Kneser's neighbour method in the setting of orthogonal groups, with inspiration from Bachoc's work with vector spaces over Hamilton's quaternions [2] and modifications coming from Symplectic groups described by Shimura who observed a relationship between Hermitian and symplectic spaces [19] and Cunningham and Dembélé [6] who worked with

[6]The isomorphism is an isomorphism of additive groups.

the symplectic group GSp_4 to compute Siegel modular forms and constructed examples using the field $\mathbb{Q}(\sqrt{5})$.

Computations of algebraic modular forms have have been done with other algebraic groups – Lansky and Pollack [13] worked with the projective symplectic group PGSp_4 and the Lie group G_2, both over the rational field. Loeffler [14] computed with the unitary groups $\mathrm{U}(2)$ over $\mathbb{Q}(\sqrt{-11})$ and $\mathrm{U}(3)$ over $\mathbb{Q}(\sqrt{-7})$ and Greenberg and Voight [8] with definite orthogonal and unitary groups over totally real number fields.

The algorithm for computing $\mathrm{cl}_G(L)$ proceeds as follows. Assume (V, f) is *totally positive-definite*, i.e., that F is totally real and (V_w, f) is positive-definite for each infinite place w of F.

1. Generate a set S of prime ideals of $\mathfrak{o}_F$ of small norm.
2. For each $\mathfrak{p} \in S$, compute $\mathcal{N}_{\mathfrak{p}}(L)$.
3. Test for isometry, i.e., compute representatives for
$$\mathcal{R}_S := \left(\bigcup_{\mathfrak{p} \in S} \mathcal{N}_{\mathfrak{p}}(L) \right) / G^0(V, f) \subset \mathrm{cl}_G(L).$$
4. Use Siegel's mass formula [7, 20] to determine whether $\mathcal{R}_S = \mathrm{cl}_G(L)$. If not, go back to step 1. and choose a larger set S.

Thanks to the Theorem of Strong Approximation, it has been made possible to fill up the class set in step 3. See Greenberg and Voight for details [8, Theorem 5.8 & Corollary 5.10].

We give some details regarding step 4. Since (V, f) is assumed to be positive-definite,

$$\Gamma_L := \{\varphi \in G^0(V, f) : L\varphi = L\}$$

is finite. (A positive definite lattice contains only finitely many vectors of any given norm – the set of lattice vectors of a given norm is discrete and bounded and hence finite.) Siegel's

mass formula gives an explicit formula for what is called the *mass of* $\mathrm{gen}_{G^0(V,f)}(L)$, a measure of the size of the automorphism groups of lattices in the class set,

$$m := \sum_{[L]\in \mathrm{cl}_G(L)} \frac{1}{|\Gamma_L|},$$

in terms of special values of the Dedekind zeta function of F at negative integers. Thus, $\mathcal{R}_S = \mathrm{cl}_G(L)$ if and only if

$$\sum_{[L]\in \mathcal{R}_S} \frac{1}{|\Gamma_L|} = m.$$

Thus, Siegel's mass formula serves as a stopping criterion for the algorithm described above.

To put this algorithm into practice, we need to be able to:

1. Compute $\mathcal{N}_{\mathfrak{p}}(L)$.

2. Test two $\mathfrak{o}_F$-lattices in V for $G^0(V,f)$-equivalence.

3. Compute Γ_L.

The computation of $\mathcal{N}_{\mathfrak{p}}(L)$ was implemented by Scharlau and Hemkemeier [16]. The problems of testing totally positive-definite lattices for isometry and computing automorphism groups was taken up in a beautiful paper of Plesken and Souvignier [15]. They utilize a partial basis of the lattices being compared and their corresponding partial Gram matrices. The idea is to reject, as quickly as possible, those partial automorphisms that don't extend to full automorphisms – among other savvy tricks.

In thesis, we adapt Kneser's neighbour method for $\mathbb{Z}-$lattices in a quadratic space and the above algorithm to the context of *quaternionic lattices*. The motivation behind lattices of these sorts is driven by a classical approach for defining algebraic groups of compact forms of symplectic groups.

We now describe the setting of moldules over certain noncommutative algebras. Let E be a quaternion F-algebra and let V be a free, left E-module of rank n. In particular, V is an F-vector space (of dimension $4n$) and it makes sense to consider $\mathfrak{o}_F$-lattices in V. We do

not study all $\mathfrak{o}_F$-lattices in V, though. We restrict ourselves to those that are closed under scalar multiplication from any fixed maximal order $\mathfrak{o}_E$ in E, and are *maximal* (see Definition 65). These are the quaternionic lattices of the title. Let

$$h : V \times V \longrightarrow E$$

be a Hermitian form – see §2.2 for the definition – and let $G^0(V,h)$ be the unitary group of the Hermitian space (V,h):

$$G^0(V,h) = \{\varphi \in \mathrm{GL}(V) : \varphi \text{ is (left) } E\text{-linear and } h(v\varphi, w\varphi) = h(v,w) \text{ for all } v,w \in V\}.$$

If $\mathfrak{p}$ is a prime ideal of $\mathfrak{o}_F$, then $(V_\mathfrak{p}, h)$ is a Hermitian $E_\mathfrak{p}$-space. Also, if L is an $\mathfrak{o}_E$-lattice in V then $L_\mathfrak{p}$ is an $\mathfrak{o}_{E,\mathfrak{p}}$-lattice in $V_\mathfrak{p}$. We call two $\mathfrak{o}_E$-lattices L and M in V *locally* $G^0(V,h)$-*equivalent* if $L_\mathfrak{p}$ and $M_\mathfrak{p}$ are $G^0(V_\mathfrak{p},h)$-equivalent for all $\mathfrak{p}$. As in the quadratic $F-$space setting, global equivalence implies local equivalence, but the converse need not be true. Once again, let $\mathrm{gen}_{G^0(V,h)}(L)$ denote the set of $\mathfrak{o}_E$-lattices in V that are locally $G^0(V,h)$-equivalent to L and set

$$\mathrm{cl}_G(L) := \mathrm{gen}_{G^0(V,h)}(L)/G^0(V,h).$$

Our goal is to compute representatives for $\mathrm{cl}_G(L)$. To achieve this, we adapt methods from the context of quadratic spaces. Specifically, when $\mathfrak{p}$ is split in E, i.e. $E_\mathfrak{p} := F_\mathfrak{p} \otimes_F E \cong \mathrm{M}_2(F_\mathfrak{p})$, we introduce the notion of $\mathfrak{p}$-neighbour in the setting of quaternionic lattices. To do this, we seek to localize the notion of $\mathfrak{p}$-neighbour. That is we define a $\mathfrak{p}$-neighbour relation on the set of $\mathfrak{o}_{E,\mathfrak{p}}$-lattices in the completed space $V_\mathfrak{p}$. This is in contrast to the usual neighbour construction which is defined in the global space V. We are able to do this thanks to the following two facts:

1. Since $\mathfrak{p}$ is split in E, there is natural bijection between the $\mathfrak{o}_{E,\mathfrak{p}}$-lattices in $V_\mathfrak{p}$ and lattices in a functorially associated *symplectic space* $(V_{\mathfrak{p},1}, h_{12})$.

2. The set of maximal lattices in $V_{\mathfrak{p},1}$ has the structure of a directed graph. (It is a

covering of the 1-skeleton of the Bruhat-Tits building of a group of symplectic similitudes of V [1, 3].)

We define the $\mathfrak{p}$-neighbour relation on lattices in $V_{\mathfrak{p},1}$ to be the edge-relation on the associated graph, and transfer this notion back to $V_{\mathfrak{p}}$ itself using the first fact above. Reglobalizing to the space V, we say that two $\mathfrak{o}_E$-lattices in V are $\mathfrak{p}$-neighbours if:

- $L_{\mathfrak{q}} = M_{\mathfrak{q}}$ for all $\mathfrak{q} \neq \mathfrak{p}$ (equality as subsets of $V_{\mathfrak{p}}$).
- $L_{\mathfrak{p}}$ and $M_{\mathfrak{p}}$ are $\mathfrak{p}$-neighbours.

Having defined this crucial notion, we then treat the problems of computing the set of $\mathfrak{p}$-neighbours of a given quaternionic lattice, of testing quaternionic lattices for isometry and of computing automorphism groups of quaternionic lattices. Isometry testing is accomplished by defining a categorical equivalence between Hermitian spaces over E and quadratic spaces over F with "extra structure". This allows us to use the algorithm of Plesken and Souvignier – and its wonderfully flexible implementation in Magma – to test for isometry in the quaternionic setting. Computing automorphism groups is done using the same ideas. A mass formula due to Siegel serves as a stopping criterion for our algorithm. To illustrate our methods, we computed representatives for $\mathrm{cl}_G(\mathfrak{o}_E \times \mathfrak{o}_E)$ for all definite $E/\mathbb{Q}$ of discriminant < 100.

1.2 Organization of this thesis

The second chapter contains background material on Hermitian and symplectic spaces and their associated algebraic groups. We give details, sufficiently explicit for our computational needs, regarding the Morita equivalence relating two different spaces: Hermitian spaces over $\mathrm{M}_2(F)$ and symplectic spaces over F itself – see §2.4. This equivalence allows one to convert from the setting of modules over quaternion algebras over a field, to honest vector spaces

over the same field – do all necessary work in that space – then send the information back to the original space we have sought out to do computations in originally.

The third chapter is the heart of this thesis – it further develops the Morita equivalence in the context of lattices and encapsulates all matters pertaining to the construction of neighbours as outlined above. The final sections of Chapter 3 are devoted to algorithmic details and to our implementation. We conclude with future directions to take with the results of this thesis.

Chapter 2

Hermitian and symplectic spaces

2.1 Quaternion algebras

Let F be a field of characteristic other than 2 and let $a, b \in F^\times$. In this section we provide the necessary background pertaining to quaternion algebras.

Definition 4. *The* quaternion F-algebra $(a,b)_F$ *is the* 4*-dimensional* F*-algebra*

$$F + Fi + Fj + Fk$$

in which multiplication is performed according to the rules

$$i^2 = a, \quad j^2 = b, \quad k = ij = -ji. \tag{2.1.1}$$

It follows that $k^2 = -ab$.

One can verify easily that the multiplication law so defined is associative and that the center of $(a,b)_F$ is F.

Example 5. *Let*

$$i = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \quad \textit{and} \quad j = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Then i *and* j *satisfy* (2.1.1) *with* $a = b = 1$. *Therefore,*

$$\begin{aligned}(1,1)_F &= F + Fi + Fj + Fij \\ &= F\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + F\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} + F\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + F\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\end{aligned}$$

is a 4*-dimensional* F*-subalgebra*[1] *of* $\mathrm{M}_2(F)$ *and, hence is equal to* $\mathrm{M}_2(F)$*:*

$$(1,1)_F = \mathrm{M}_2(F).$$

[1] *Here* $M_2(F)$ *denotes the usual matrix algebra – the ring of* 2×2 *matrices with entries in the commutative ring* F.

$\mathrm{M}_2(F)$ *is called the* split *quaternion F-algebra.*

Let $u = w + xi + yj + zk \in (a,b)_F$. We define the *conjugate*, *reduced norm* and *reduced trace* of u by

$$\begin{aligned} \bar{u} &= w - xi - yj - zk, \\ N(u) &= u\bar{u} = \bar{u}u = w^2 - ax^2 - by^2 + abz^2, \\ T(u) &= u + \bar{u} = 2w, \end{aligned}$$

respectively.

Lemma 6. *Suppose N is anisotropic, i.e., $N(u) = 0$ if and only if $u = 0$. Then $(a,b)_F$ is a division F-algebra. If $N(u)$ is isotropic, i.e., $N(u) = 0$ for some $u \neq 0$, then $(a,b)_F$ is isomorphic to $\mathrm{M}_2(F)$ as F-algebras.*

Proof. The familiar computation shows that if $N(u) \neq 0$ then u^{-1} exists and equals $\frac{1}{N(u)}\bar{u}$, proving the first statement. For the second, see Vigneras [21]. □

Example 7. *There is no quaternion division $\mathbb{C}$-algebra, for if $(a,b)_F$ were such then*

$$\mathbb{C}[X]/(X^2 - b) \xrightarrow{\sim} \mathbb{C}(j)$$

would be a quadratic field extension of $\mathbb{C}$.

Example 8. *$(-1,-1)_F$ is Hamilton's quaternion F-algebra when $F = \mathbb{Q}$ or $F = \mathbb{R}$ or, more generally when $w^2 + x^2 + y^2 + z^2$ does not represent 0 nontrivially with $w, x, y, z \in F$ (and at least one element nonzero).*

Let $\mathfrak{p}$ be a prime of F and write $F_\mathfrak{p}$ for the completion of F at $\mathfrak{p}$. Then the canonical map

$$F_\mathfrak{p} \otimes_F (a,b)_F \xrightarrow{\sim} (a,b)_{F_\mathfrak{p}}$$

is an isomorphism of scalars. Thus, we may regard $(a,b)_{F_\mathfrak{p}}$ as the completion of $(a,b)_F$ at $\mathfrak{p}$.

The following fundamental theorem classifies quaternion algebras over local and global fields, up to isomorphism.

Theorem 9.

1. *Let F be a local field, $F \neq \mathbb{C}$. Then there is a unique quaternion division F-algebra D_F, up to isomorphism.*
2. *Let F be a global field and let E be a quaternion F-algebra. Then*

$$S_E := \{\mathfrak{p} \subset F : E_{\mathfrak{p}} \text{ is a division algebra}\}$$

is a finite set of even size. Conversely, if S is a finite set of places of F with even size then, up to F-algebra isomorphism, there is a unique quaternion F-algebras E with $S_E = S$.

Proof. See Vigneras [21]. □

2.2 Hermitian spaces and unitary groups

Let F be a field of characteristic $\neq 2$, let E be a quaternion F-algebra and let V be a free, left E-module of rank n. In this section we describe Hermitian vector spaces and their associated unitary groups. Our particular interest pertains to those Hermitian spaces over quaternion algebras. Essential computational tools described here are explicit symplectic subspaces in Example 25 and the method of computing a symplectic basis for a symplectic space with a modified Gram-Schmidt algorithm in Lemma 27.

Definition 10. *A* Hermitian form *on V is an F-bilinear map*

$$h : V \times V \longrightarrow E$$

such that

1. $h(ax, y) = ah(x, y)$ *for all* $a \in E$ *and all* $x, y \in V$.

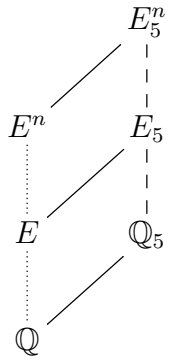
2. $\overline{h(x, y)} = h(y, x)$ *for all* $x, y \in V$.

We say that h *is* nondegenerate *if* $h(x, V) = \{0\}$ *if and only if* $x = 0$. *A* Hermitian E-space *is a pair* (V, h) *of a free* E*-module* V *of finite rank and Hermitian form* h *on* V. *We say that* (V, h) *is nondegenerate if* h *is.*

Example 11. *The* standard n-dimensional Hermitian space E *is* (E^n, h) *with*

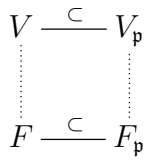
$$h(x, y) = x_1\bar{y}_1 + \cdots + x_n\bar{y}_n.$$

Example 12. *Denote by* $E = (-2, -5)_{\mathbb{Q}}$, *the quaternion algebra over* $\mathbb{Q}$ *with discriminant 5. Then* E_5 *remains a division algebra. The space* (E^n, h) *is a* Hermitian space *and the completed space* (E_5^n, h) *is a* Hermitian space *which is not equivalent to a symplectic space.*



2.2.1 Completions

Let (V, h) be a left Hermitian E-space and let $V_{\mathfrak{p}} = F_{\mathfrak{p}} \otimes_F V$ be the completion of V at $\mathfrak{p}$.



We may extend h by $F_{\mathfrak{p}}$-linearity to a map

$$h_{\mathfrak{p}} : V_{\mathfrak{p}} \times V_{\mathfrak{p}} \longrightarrow E_{\mathfrak{p}}$$

making $(V_{\mathfrak{p}}, h_{\mathfrak{p}})$ into a left Hermitian $E_{\mathfrak{p}}$-space.

2.2.2 Similarity and isometry

Let (V, h) be a Hermitian E-space. Define

$$G^0(V,h) := \{\varphi \in \mathrm{GL}(V) : h(x\varphi, y\varphi) = h(x,y) \text{ for all } x, y \in V\},$$

$$G(V,h) := \{\varphi \in \mathrm{GL}(V) : h(x\varphi, y\varphi) = s_\varphi h(x,y) \text{ for some } s_\varphi \in F^\times \text{ and all } x, y \in V\}$$

as the *unitary group of* (V, h) and the *similitude group of* (V, h), respectively.

When (V, h) is the standard Hermitian E-space, these groups take the usual form:

$$G^0(V,h) = \{A \in \mathrm{GL}_n(E) : AA^* = I\},$$

$$G(V,h) = \{A \in \mathrm{GL}_n(E) : AA^* = s_A I \text{ for some } s_A \in F^\times\}.$$

Here, A^* is the (entrywise) conjugate of the transpose of A. The groups $G^0(V,h)$ and $G(V,h)$ are often denoted $\mathrm{U}_n(E)$ and $\mathrm{GU}_n(E)$, respectively.

2.3 Digression on symplectic vector spaces

Let V be an F-vector space of dimension $2n$. As we shall utilize symplectic spaces as a significant tool for understanding Hermitian spaces, we give some background for these spaces in this section.

Definition 13. *A* symplectic form $g : V \times V \to F$ *is an* $F-$*bilinear form such that*[2]*:*

$$g(x,y) = -g(y,x)$$

for every $x, y \in V$*. Furthermore, we require that* g *is nondegenerate, i.e. if* $g(x,y) = 0$ *for every* $y \in V$ *then* $x = 0$*. Attaching the form* g *to a vector space* V *over* F *gives the* symplectic space (V, g)*.*

Example 14. *Let* $V = F^{2n}$ *and*

$$J = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} \in \mathrm{GL}_{2n}(F). \tag{2.3.1}$$

[2] *Equivalently, for* $\mathrm{char}(F) \neq 2$*, a symplectic form is totally isotropic:* $g(x,x) = 0$ *for all* $x \in V$

Define an $F-$linear form

$$g : V \times V \longrightarrow F;\ g(x, y) = xJy^t.$$

The form g is symplectic as $J^t = -J$:

$$g(y, x) = yJx^t = xJ^ty^t = -xJy^t = -g(x, y).$$

This is the standard symplectic space *of dimension* $2n$.

Remark 15. *If J is any skew-symmetric matrix, $g(x, y) := xJy^t$ is a symplectic pairing by the same argument.*

Definition 16. *A* symplectic basis, $(e_1, \ldots, e_n, f_1, \ldots, f_n)$, *of a symplectic space (V, g) is a basis which satisfies*

$$g(e_i, f_j) = \delta_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j \end{cases}$$

$$g(e_i, e_j) = g(f_i, f_j) = 0.$$

Definition 17. *A vector v in V is called an* isotropic vector *if $g(v, v) = 0$. A subspace $W \subset V$ is called an* isotropic subspace *if $g(W, W) = \{0\}$.*

Denote the perpendicular subspace in (V, g) of W by

$$W^\perp := \{x \in V \mid g(x, y) = 0\ \forall\ y \in W\}.$$

Let (V, g) be a nondegenerate symplectic space of dimension $2n$ and $X \subset V$ an isotropic subspace.

Lemma 18. *There exists an isotropic subspace $Y \subset V$ such that* $\dim X = \dim Y$, $X \cap Y^\perp = 0$ *and* $X^\perp \cap Y = 0$.

Proof. Here we sketch the idea behind the proof – this statement is rephrased in Lemma 27 where the full details of the proof are given. By induction on $\dim X$ and due to the nondegeneracy of V there exists a basis $(e_1, \ldots, e_{\dim X})$ of X and elements $f_1, \ldots, f_{\dim X}$ in V such that $g(e_i, f_j) = \delta_{ij}$. Let Y be the span of $(f_1, \ldots, f_{\dim X})$. □

Corollary 19. $\dim X \leq n$.

Proof. By Lemma 18, there exists a subspace Y such that $X \cap Y \subset X \cap Y^{\perp} = 0$. Then $2n = \dim X + \dim Y \leq \dim X + \dim Y^{\perp}$ which implies that $\dim X$ is at most $n/2$. □

Lemma 20. *Let Y be a subspace of the form in Lemma 18 and $Z = X+Y$. Then $Z \cap Z^{\perp} = 0$.*

Proof. Let $z \in Z$. Then there exists $x \in X$, $y \in Y$ such that $z = x + y$. Suppose that $x \neq 0$. Since $X^{\perp} \cap Y = 0$ there exists $y' \in Y$ such that $g(x, y') \neq 0$. Then $g(z, y') = g(x, y') + g(y, y') = g(x, y') \neq 0$. If $x = 0$, then $X^{\perp} \cap Y = 0$ implies that $y \neq 0$. The previous argument runs through with the role of x and y interchanged. Then $z \notin Y^{\perp} \supset Z^{\perp}$. □

Corollary 21. $V = (X + Y) \oplus (X + Y)^{\perp}$.

Corollary 22. *Maximal isotropic subspaces have dimension n.*

Proof. Suppose that X is a maximal isotropic subspace but that $\dim X \leq n - 1$. Let Y be defined as in Lemma 18 and let $Z = (X + Y)^{\perp}$. As $V = X \oplus Y \oplus Z$ then

$$\dim Z = \dim V - \dim X - \dim Y = \dim V - 2\dim X \geq 2$$

as we have assumed that $\dim X \leq n - 1$. There exists a $0 \neq z \in Z$. However $X' = X + \langle z \rangle$ is isotropic and has $\dim X' > \dim X$. Therefore the dimension is n. □

Definition 23. *Let (V, g) be a* symplectic space*, of dimension $2n$. The isotropic subspaces X with maximal dimension, n, are called* Lagrangians*. Moreover, $X = X^{\perp}$.*

Example 24. *Consider the standard symplectic space (V, g) of dimension $2n = 2$. Then the Lagrangians are the $1-$dimensional subspaces.*

Example 25. *Let (V, g) be the standard symplectic space with dimension $2n = 4$ with a symplectic basis (e_1, e_2, f_1, f_2). Consider the set of four linearly independent vectors in reduced Echelon form:*

$$v_1 = \begin{pmatrix} 1 & a & b & c \end{pmatrix} \; v_2 = \begin{pmatrix} 0 & 1 & d & e \end{pmatrix}, \; v_3 = \begin{pmatrix} 0 & 0 & 1 & f \end{pmatrix}, \; v_4 = \begin{pmatrix} 0 & 0 & 0 & 1 \end{pmatrix}.$$

The possible isotropic planes spanned by the vectors v_i are as follows.

1. *X spanned by* (v_1, v_2) :

$$g(v_1, v_2) = \begin{pmatrix} 1 & a & b & c \end{pmatrix} \begin{pmatrix} 0 & I_2 \\ -I_2 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & d & e \end{pmatrix}^t = -c + d + ae.$$

Isotropy requires that $d = c - ae$. *Then* (v_1, v_2) *is in bijection with* $\begin{pmatrix} 1 & a & b & c \\ 0 & 1 & c-ae & e \end{pmatrix}$ *which in row reduced Echelon form corresponds to*

$$(v_1, v_2) = \begin{pmatrix} 1 & 0 & * & \alpha \\ 0 & 1 & \alpha & * \end{pmatrix}.$$

2. *X spanned by* (v_1, v_3) :

$$g(v_1, v_3) = \begin{pmatrix} 1 & a & b & c \end{pmatrix} \begin{pmatrix} 0 & I_2 \\ -I_2 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 & f \end{pmatrix}^t = 1 + af.$$

For an isotropic plane, $f = -1/a$. *Then* (v_1, v_3) *is in bijection with* $\begin{pmatrix} 1 & a & * & * \\ 0 & 0 & 1 & -1/a \end{pmatrix}$ *which in row reduced Echelon form, for* $\beta \neq 0$, *corresponds to*

$$(v_1, v_3) = \begin{pmatrix} 1 & \beta & 0 & * \\ 0 & 0 & \beta & -1 \end{pmatrix}.$$

3. *X spanned by* (v_1, v_4) :

$$g(v_1, v_4) = \begin{pmatrix} 1 & a & b & c \end{pmatrix} \begin{pmatrix} 0 & I_2 \\ -I_2 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 \end{pmatrix}^t = a.$$

Then $a = 0$ *and* (v_1, v_4) *is in bijection with* $\begin{pmatrix} 1 & 0 & * & * \\ 0 & 0 & 0 & 1 \end{pmatrix}$ *which in row reduced Echelon form corresponds to*

$$(v_1, v_4) = \begin{pmatrix} 1 & 0 & * & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

4. *X spanned by* (v_2, v_3) :

$$g(v_2, v_3) = \begin{pmatrix} 0 & 1 & d & e \end{pmatrix} \begin{pmatrix} 0 & I_2 \\ -I_2 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 & f \end{pmatrix}^t = f.$$

Then $f = 0$ *and* (v_2, v_3) *is in bijection with* $\begin{pmatrix} 0 & 1 & * & * \\ 0 & 0 & 1 & 0 \end{pmatrix}$ *which in row reduced Echelon form corresponds to*

$$(v_2, v_3) = \begin{pmatrix} 0 & 1 & 0 & * \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

5. *X spanned by (v_2, v_4) :*

$$g(v_2, v_4) = \begin{pmatrix} 0 & 1 & d & e \end{pmatrix} \begin{pmatrix} 0 & I_2 \\ -I_2 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 \end{pmatrix}^t = 1.$$

As this pairing is nonzero for all vectors, there are no isotropic planes spanned by (v_2, v_4).

6. *X spanned by (v_3, v_4) :*

$$g(v_3, v_4) = \begin{pmatrix} 0 & 0 & 1 & f \end{pmatrix} \begin{pmatrix} 0 & I_2 \\ -I_2 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 \end{pmatrix}^t = 0.$$

As this pairing is zero for all vectors, (v_3, v_4) is in bijection with $\begin{pmatrix} 0 & 0 & 1 & * \\ 0 & 0 & 0 & 1 \end{pmatrix}$ which in row reduced Echelon form corresponds to

$$(v_3, v_4) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

The isotropic planes are summarized below:

$$\begin{pmatrix} 1 & 0 & * & \alpha \\ 0 & 1 & \alpha & * \end{pmatrix}, \begin{pmatrix} 1 & \beta & 0 & * \\ 0 & 0 & \beta & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & * & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & * \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

For $|F| = p$, there are $p^3 + p(p-1) + p + p + 1 = p^3 + p^2 + p + 1 = (p^2+1)(p+1)$ total Lagrangians.

Remark 26. *The result of the calculation in Example 25 can then be applied to compute neighbours of neighbours giving $(p^2+1)(p+1)$ at each iteration. Interestingly, the directed graph of these lattices is regular!*

The following Lemma is a rephrasing of Lemma 18, outlining the construction of the basis.

Lemma 27 (The Gram-Schmidt algorithm adapted to symplectic space)**.** *Every symplectic space (V, g) has a symplectic basis.*

Proof. Let $(e_1, \ldots, e_n)$ be a basis for a Lagrangian X. Complete $(e_1, \ldots, e_n)$ to any basis of $V : (e_1, \ldots, e_n, f_1, \ldots, f_n)$. Assume that $g(e_1, f_1) \neq 0$. This is feasible as X is a Lagrangian,

hence a maximal isotropic space, and g is nondegenerate. For e_i, with $i > 1$, the same argument holds that $g(e_i, f_i) \neq 0$ as e_i is in the span of X and due to the nondegeneracy of the pairing. To satisfy the property that $g(e_i, f_i) = 1$, replace

$$f_i \leftarrow \frac{f_i}{g(e_i, f_i)}.$$

To ensure that the pairing of $g(f_i, f_j) = 0$, for $i \geq 1$, iteratively replace

$$f_{i+1} \leftarrow f_{i+1} - \frac{g\left(f_i, f_{i+1}\right)}{g(f_i, e_i)} e_i.$$

When pairing e_i and f_j with distinct indices, if $g(e_i, f_j) \neq 0$, replace

$$f_j \leftarrow f_j - \frac{g\left(e_i, f_j\right)}{g(e_i, f_i)} f_i.$$

This process is repeated iteratively across all indices of e_i and f_j resulting in a symplectic basis of V. □

Definition 28. *A* symplectic map $\varphi : (V, g) \longrightarrow (V', g')$ *is an* $F-$*linear map*[3] $\varphi : V \longrightarrow V'$ *such that*

$$g'(x\varphi, y\varphi) = g(x, y).$$

A symplectic similitude $\varphi : (V, g) \longrightarrow (V', g')$ *is an* $F-$*linear map* $\varphi : V \longrightarrow V'$ *such that there exists* $N(\varphi) \in F^\times$ *and*

$$g'(x\varphi, y\varphi) = N(\varphi) g(x, y)$$

for every $x, y \in V$.

Definition 29. *The set* $G^0(V, g)$ *of symplectic automorphisms of* (V, g) *is called the* symplectic group *of* (V, g) :

$$G^0(V, g) := \{\varphi \in \mathrm{GL}(V) \mid g(x\varphi, y\varphi) = g(x, y)\ \forall x, y \in V\}.$$

[3] *For* $x \in V$ *we denote* $\varphi(x)$ *by* $x\varphi$. *This is convenient when representing the linear map* φ *as matrix multiplication – which acts on the* right.

The set $G(V,g)$ of symplectic similitude automorphisms of (V,g) is called the symplectic similitude group *of (V,g) :*

$$G(V,g) := \{\varphi \in \mathrm{GL}(V) \mid \exists\, N(\varphi) \in F^\times \text{ s.t. } g(x\varphi, y\varphi) = N(\varphi)g(x,y)\ \forall x,y \in V\}.$$

Lemma 30. *If $X, Y \subset V$ are Lagrangians in V, then there exists a symplectic map $\varphi \in G^0(V,g)$ such that $Y = X\varphi$.*

Proof. Let X' and Y' be Lagrangians such that

$$X + X' = V$$
$$Y + Y' = V.$$

Let e and f be bases of X and X' such that (e,f) is a symplectic basis of V. Likewise, suppose that e' and f' are bases of Y and Y' with (e',f') another symplectic basis of V. There exists a unique $F-$linear map φ taking $e\varphi = e'$ and $f\varphi = f'$. As φ takes a symplectic basis to another symplectic basis (by definition of φ and the nature of pairings of symplectic bases elements described by the Kronecker delta, Definition 16), it is a symplectic map. □

In the following Lemma, let (V,g) be the standard symplectic space describe in Example 14.

Lemma 31. *The following are equivalent:*

1. *A is the matrix of a symplectic map (respectively similutude) $\varphi \in G^0(V,g)$ (respectively $\varphi \in G(V,g)$) with respect to a symplectic basis (e,f) of V.*
2. *$AJA^t = J$ (respectively $AJA^t = N(A)J$ for some $N(A) \in F^\times$), where J is given in equation 2.3.1.*

Proof. Let J be the matrix corresponding to the bilinear map $g(x,y)$ and A the matrix representing the automorphism $\varphi : V \to V$. Then

$$g(x\varphi, y\varphi) = (x\varphi)J(y\varphi)^t = (xA)J(yA)^t = x(AJA^t)y^t$$

and AJA^t is the matrix corresponding to he map $(x, y) \mapsto g(x\varphi, y\varphi)$. If φ is a symplectic map, then $g(x\varphi, y\varphi) = g(x, y)$. Equating the corresponding matrices gives $J = AJA^t$. The reverse implication is clear. □

Definition 32. *A matrix satisfying the equivalent conditions of Lemma 31 is called symplectic (respectively a symplectic similitude). The group of $2n \times 2n$ matrices is denoted $\mathrm{Sp}_{2n}(F)$ (respectively $\mathrm{GSp}_{2n}(F)$).*

2.3.1 The case $n = 1$

The special case $n = 1$ warrants a few extra remarks. Let V be a 2-dimensional F-vector space. Given a basis (e, f) of V there is a unique symplectic form g on V satisfying

$$g_{e,f}(e, f) = 1$$

which is defined by

$$g_{e,f}(ae + bf, ce + df) = \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} = ad - bc.$$

Let $\sigma \in \mathrm{GL}(V)$ and let

$$\begin{pmatrix} w & x \\ y & z \end{pmatrix}$$

be the matrix of σ in the basis (e, f), so that

$$e\sigma = we + yf, \quad f\sigma = xe + zf.$$

Then

$$g_{e,f}(e\sigma, f\sigma) = g_{e,f}(we + yf, xe + zf) = wz - xy = \det(\sigma) = \det(\sigma) g_{e\sigma, f\sigma}(e\sigma, f\sigma).$$

Thus, $g_{e,f} = g_{e\sigma, f\sigma}$ if and only if $\det(\sigma) = 1$.

Lemma 33. *Let C be an $\mathrm{SL}_2(V)$-equivalence class[4] of bases of V. Then there is a unique nondegenerate, symplectic form g on V such that C consists of the set of g-symplectic bases of*

[4] *Here $\mathrm{SL}_2(V)$ is the usual set of 2×2 matrices with determinant 1.*

V. Conversely, if g is a nondegenerate, symplectic form on V then the set C of g-symplectic bases of V forms an $\mathrm{SL}_2(V)$-equivalence class (in the set of all bases of V).

Proof. The explicit bijection is given by $(e, f) \leftrightarrow g_{e,f}$, outlined in the remarks preceding the Lemma. □

The set of bases of V admits a simply transitive action of $\mathrm{GL}(V)$ that descends to a simply transitive action of $F^\times = \mathrm{GL}(V)/\mathrm{SL}(V)$ on the set of $\mathrm{SL}(V)$-equivalence classes of bases of V. On the other hand, $\mathrm{GL}(V)$ acts from the left on the set nondegenerate, symplectic forms on V by the rule $(\sigma g)(x, y) = g(x\sigma, y\sigma)$. But this action is merely $\sigma g = \det(\sigma)g$, so this action factors through the natural action of $F^\times = \mathrm{GL}(V)/\mathrm{SL}(V)$. Thus, we conclude that the bijection

$$\{\mathrm{SL}(V)\text{-equiv. classes of bases of } V\} \xrightarrow{\sim} \{\text{nondegenerate, symplectic forms on } V\}$$

is $\mathrm{GL}(V)$-equivariant, the action of $\mathrm{GL}(V)$ on both sides factoring through $F^\times$.

If $\dim_F(V) = 2$ then the canonical inclusion $G(V, g) \hookrightarrow \mathrm{GL}(V)$ is an isomorphism. It restricts to an isomorphism of $G^0(V, g)$ with $\mathrm{SL}(V)$.

The techniques described in this section allow the computational magic to take place in the simpler setting – symplectic space. We then can send back the computations done in this space to Hermitian space – the space in which we are interested in.

2.4 The split case $E = \mathrm{M}_2(F)$

The goal of this section is to establish the Morita equivalence in Proposition 36 and its explicit Corollaries 37 and 38. We assume, in this section, that $E = \mathrm{M}_2(F)$. I.e. The algebra has been completed at a split prime. Recall that h is a Hermitian form for the Hermitian space (V, h).

Define e_{ij} to be the standard F-basis of E :

$$e_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad e_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad e_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad e_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}. \tag{2.4.1}$$

Let

$$V_1 = e_{11}V \quad \text{and} \quad V_2 = e_{22}V.$$

As e_{11} and e_{22} are orthogonal idempotents with $e_{11} + e_{22} = I_2$, we see that $V = V_1 \oplus V_2$ and $V_1 \perp V_2$ as $E-$vector spaces. Let

$$\tau = e_{12} + e_{21}.$$

Then τ is an F-linear involution of V interchanging V_1 and V_2. Let $h_{ij}(v, w)$ be the entries of the matrix $h(v, w) \in \mathrm{M}_2(F)$. Observe that if $v, w \in V$, then

$$h(e_{11}v, e_{11}w) = e_{11}h(v, w)\bar{e}_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} h_{11}(v, w) & h_{12}(v, w) \\ h_{21}(v, w) & h_{22}(v, w) \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = h_{12}(v, w)e_{12}.$$

Thus,

$$h_{12} : V_1 \times V_1 \longrightarrow F$$

is an F-bilinear map. Observe that

$$h_{12}(v, w)e_{12} = h(e_{11}v, e_{11}w) = e_{11}h(x, v)\bar{e}_{11} = e_{11}h(v, w)e_{22}. \tag{2.4.2}$$

Lemma 34. *The pairing h_{12} is symplectic, i.e., $h_{12}(v, v) = 0$ for all $v \in V_1$. Additionally, it is nondegenerate.*

Proof. If $v \in V_1$ then $h(v, v) \in F(e_{11} + e_{22})$ and $h(v, v) \in Fe_{12}$. Thus, $h(v, v) \in F(e_{11} + e_{22}) \cap Fe_{12} = \{0\}$. Since V_1 and V_2 are orthogonal, if $v \in V_1$ and $v \perp w$ for all $w \in V_1$, then $v \perp w$ for all $w \in V$. The nondegeneracy of h_{12} now follows from that of h. □

Thus, a nondegenerate, Hermitian E-space (V, h) with $\dim_E(V) = n$ gives rise[5] to a nondegenerate, symplectic F-space (V_1, h_{12}) with $\dim_F(V_1) = 2n$. Conversely, (V, h) can be recovered from (V_1, h_{12}): If $v \in V$, then

$$v = e_{11}v + e_{22}v = e_{11}v + \tau e_{12}v.$$

[5]Although we have treated $n = 1$ as a special case, the statement still holds in general – in this case lattices and ideals happen to coincide.

Notice that both $e_{11}v$ and $e_{12}v$ are in V_1. Therefore,

$$\begin{aligned}
h(v,w) &= h(e_{11}v + \tau e_{12}v, e_{11}w + \tau e_{12}w) \\
&= h(e_{11}v, e_{11}w) + h(e_{11}v, \tau e_{12}w) + h(\tau e_{12}v, e_{11}w) + h(\tau e_{12}v, \tau e_{12}w) \\
&= h(e_{11}v, e_{11}w) + h(e_{11}v, e_{12}w)\bar{\tau} + \tau h(e_{12}v, e_{11}w) + \tau h(e_{12}v, e_{12}w)\bar{\tau} \\
&= h_{12}(e_{11}v, e_{11}w)e_{12} + h_{12}(e_{11}v, e_{12}w)e_{12}\bar{\tau} + h_{12}(e_{12}v, e_{11}w)\tau e_{12} + h(e_{12}v, e_{12}w)\tau e_{12}\bar{\tau} \\
&= h_{12}(e_{11}v, e_{11}w)e_{12} - h_{12}(e_{11}v, e_{12}w)e_{11} + h_{12}(e_{12}v, e_{11}w)e_{22} - h_{12}(e_{12}v, e_{12}w)e_{21} \\
&= \begin{pmatrix} -h_{12}(e_{11}v, e_{12}w) & h_{12}(e_{11}v, e_{11}w) \\ -h_{12}(e_{12}v, e_{12}w) & h_{12}(e_{12}v, e_{11}w) \end{pmatrix}.
\end{aligned}$$

More is true – this extends to an equivalence of categories. To see this, let $\varphi : (V,h) \to (V',h')$ be a morphism of E-Hermitian spaces and let (V_1, h_{12}) and (V_1', h_{12}') be the corresponding symplectic F-spaces. Then

$$V_1\varphi = (e_{11}V)\varphi = e_{11}(V\varphi) \subset e_{11}V' = V_1',$$

so φ restricts to a map $V_1 \to V_1'$. It is easy to see that φ respects the symplectic forms h_{12} and h_{12}'.

Conversely, suppose $\varphi_1 : (V_1, h_{12}) \to (V_1', h_{12}')$ is a symplectic map. Define

$$\varphi : V \to V' \quad \text{by} \quad v\varphi = (e_{11}v)\varphi_1 + \tau(e_{12}v)\varphi_1. \tag{2.4.3}$$

This is well-defined as $e_{11}v$ and $e_{12}v$ are in V_1. Suppose $v \in V_1$. Then $v = e_{11}v$ and

$$v\varphi = (e_{11}v)\varphi_1 + \tau(e_{12}v)\varphi_1 = v\varphi_1 + \tau(e_{12}e_{11}v)\varphi_1 = v\varphi_1 \tag{2.4.4}$$

as $e_{12}e_{11} = 0$. Thus, φ extends φ_1.

Lemma 35.

1. *φ is left E-linear.*
2. *$h'(x\varphi, y\varphi) = h(x,y)$ for all $x, y \in V$.*

Proof. We consider the action of e_{ij} to vectors $v \in V$ and $v\varphi \in V'$. First, notice the the action of e_{11} to $v\varphi$: Then

$$e_{11}(v\varphi) = e_{11}(e_{11}v)\varphi_1 + e_{11}\tau(e_{12}v)\varphi_1 = (e_{11}v)\varphi_1 + e_{12}(e_{12}v)\varphi_1 = (e_{11}v)\varphi_1$$

as $(e_{11}v)\varphi_1 \in V_1', e_{11}\tau = e_{12}$ and $e_{12}V_1' = 0$. Next consider the action of φ to $e_{11}v$:

$$(e_{11}v)\varphi = (e_{11}e_{11}v)\varphi_1 + \tau(e_{12}e_{11}v)\varphi_1 = (e_{11}v)\varphi_1.$$

Then $e_{11}(v\varphi) = (e_{11}v)\varphi$.

Likewise, for e_{12} :

$$e_{12}(v\varphi) = e_{12}(e_{11}v)\varphi_1 + e_{12}\tau(e_{12}v)\varphi_1 = e_{11}(e_{12}v)\varphi_1 = (e_{12}v)\varphi_1$$

as $e_{12}V_1' = 0$ in the second equality and $(e_{12}v)\varphi_1 \in V_1'$ in the third. Also,

$$(e_{12}v)\varphi = (e_{11}e_{12}v)\varphi_1 + \tau(e_{12}e_{12}v)\varphi_1 = (e_{12}v)\varphi_1$$

as $e_{12}e_{12} = 0$ and $e_{11}e_{12} = e_{12}$. Then $e_{12}(v\varphi) = (e_{12}v)\varphi$.

Now, for e_{21} :

$$e_{21}(v\varphi) = e_{21}(e_{11}v)\varphi_1 + e_{21}\tau(e_{12}v)\varphi_1 = e_{21}(e_{11}v)\varphi_1 + 0.$$

Additionally,

$$\begin{aligned}(e_{21}v)\varphi &= (e_{11}e_{21}v)\varphi_1 + \tau(e_{12}e_{21}v)\varphi_1 = 0 + \tau(e_{11}v)\varphi_1 = \tau(e_{11}e_{11}v)\varphi_1 \\ &= \tau e_{11}(e_{11}v)\varphi_1 = e_{21}(e_{11}v)\varphi_1\end{aligned}$$

and so $e_{21}(v\varphi) = (e_{21}v)\varphi$.

We obtain the last case for free! Since $e_{21}e_{12} = e_{22}$, the preceding statements imply that $e_{22}(v\varphi) = (e_{22}v)\varphi$.

As the e_{ij} span E over F and φ is $F-$linear, it follows that φ is $E-$linear. The fact that $h'(x\varphi, y\varphi) = h(x, y)$ follows from the fact that $h'_{12}(x\varphi, y\varphi) = h_{12}(x, y)$ and the reconstruction of h from h_{12}.

□

The reader may verify that $\varphi \mapsto \varphi_1$ respects composition. Thus, we have established:

Proposition 36. *The correspondence $(V,h) \mapsto (V_1, h_{12})$ is a Morita equivalence that is an equivalence from the category of Hermitian E-spaces to the category of symplectic F-spaces.*

Corollary 37. *The map $\varphi \mapsto \varphi_1$ is an isomorphism*

$$G(V,h) \xrightarrow{\sim} G(V_1, h_{12}).$$

It restricts to an isomorphism of

$$G^0(V,h) \xrightarrow{\sim} G^0(V_1, h_{12}).$$

Proof. Let $x, y \in V_1$ and $\varphi_1 \in G(V_1, h_{12})$. Then

$$h(x\varphi, y\varphi) = h(x\varphi_1, y\varphi_1) = h_{12}(x\varphi_1, y\varphi_1)e_{12} = s_{\varphi_1} h_{12}(x,y)e_{12} = s_{\varphi_1} h(e_{11}x, e_{11}y) = s_{\varphi_1} h(x,y)$$

where the first equality follows from the identity (2.4.4) and $s_{\varphi_1} \in F^\times$. Then $\varphi_1 \in G(V_1, h_{12})$ gives rise to $\varphi \in G(V,h)$ via the map (2.4.3). □

We conclude this chapter giving an explicit description of the morphisms arising from the Morita equivalence described in Proposition 36. In particular, the maps can be described in matrix notation, which are collected in Corollary 38.

Let $v = (v_1, \ldots, v_n)$ and $v' = (v'_1, \ldots, v'_n)$ be orthonormal bases of V and V', respectively. Let $\varphi : V \to V'$ be a homomorphism of Hermitian E-spaces and let (Φ_{ij}) be the matrix of φ in the bases v and v':

$$v_i\varphi = \sum_{r=1}^{n} \varphi_{ri} v'_r.$$

In matrix notation,

$$\begin{pmatrix} v_1\varphi & \ldots & v_n\varphi \end{pmatrix} = \begin{pmatrix} v'_1 & \ldots & v'_n \end{pmatrix} \begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1n} \\ \vdots & \ddots & \vdots \\ \varphi_{n1} & \cdots & \varphi_{nn} \end{pmatrix} = \begin{pmatrix} v'_1 & \ldots & v'_n \end{pmatrix} (\Phi_{ij})$$

where $\varphi_{ij} \in \mathrm{M}_2(F)$. Let

$$e_i = e_{12}v_i, \qquad f_i = e_{11}v_i, \qquad e'_j = e_{12}v'_j, \qquad f'_j = e_{11}v'_j$$

and write

$$\varphi_{ij} = \begin{pmatrix} a_{ij} & b_{ij} \\ c_{ij} & d_{ij} \end{pmatrix} \tag{2.4.5}$$

where $a_{ij}, b_{ij}, c_{ij}, d_{ij} \in F$. Explicitly, we construct the space $V_1 = e_{11}V$ with the basis:

$$(e_{12}v_1, \ldots, e_{12}v_n, e_{11}v_1, \ldots, e_{11}v_n) = (e_1, \ldots, e_n, f_1, \ldots, f_n) \tag{2.4.6}$$

and likewise for $V_1' = e_{11}V'$:

$$(e_{12}v_1', \ldots, e_{12}v_n', e_{11}v_1', \ldots, e_{11}v_n') = (e_1', \ldots, e_n', f_1', \ldots, f_n'). \tag{2.4.7}$$

Observe that

$$\begin{aligned} h'(e_j\varphi, e_i') &= h'(e_{12}v_j\varphi, e_{12}v_i') \\ &= e_{12}h'(v_j\varphi, v_i')\bar{e}_{12} \\ &= e_{12}\sum_{r=1}^{n} \varphi_{rj}h'(v_r', v_i')(-e_{12}) && \text{by linearity} \\ &= -e_{12}\varphi_{ij}e_{12} && \text{by orthonomality} \\ &= -c_{ij}e_{12}. \end{aligned}$$

Similarly, the same properties applied to all combinations of bases elements yields:

$$h'(e_j\varphi, f_i') = d_{ij}e_{12}, \qquad h'(f_j\varphi, e_i') = -a_{ij}e_{12}, \qquad h'(f_j\varphi, f_i') = b_{ij}e_{12}.$$

Let $a = (a_{ij})$, $b = (b_{ij})$, $c = (c_{ij})$ and $d = (d_{ij})$. For the ease of computation, let $(x_1, \ldots, x_{2n}) = (e_1, \ldots, e_n, f_1, \ldots, f_n)$ and $(x_1', \ldots, x_{2n}') = (e_1', \ldots, e_n', f_1', \ldots, f_n')$. Again, applying the map h_{12}' to all combinations of bases elements we see that:

$$
\begin{aligned}
-c_{ij} &= h'_{12}(e_j\varphi, e'_i) \\
&= h'_{12}(x_j\varphi, e'_i) \\
&= \sum_{r=1}^{2n} \varphi_{rj} h'_{12}(x'_r, e'_i) \\
&= \sum_{r=1}^{n} \varphi_{rj} h'_{12}(e'_r, e'_i) + \sum_{r=n+1}^{2n} \varphi_{rj} h'_{12}(f'_{r-n}, e'_i) \\
&= 0 + \varphi_{n+i,j} h'_{12}(f'_i, e'_i) \\
&= -\varphi_{n+i,j}.
\end{aligned}
$$

Then $\varphi_{n+i,j} = c_{ij}$ for $1 \leq i, j \leq n$. Apply h'_{12} to all other bases combinations we obtain the relations for $1 \leq i, j \leq n$,

$$
d_{ij} = h'_{12}(e_j\varphi, f'_i) = \varphi_{ij}, \qquad a_{ij} = h'_{12}(f_j\varphi, e'_i) = \varphi_{i+n,j+n}, \qquad b_{ij} = h'_{12}(f_j\varphi, f'_i) = \varphi_{i,j+n}
$$

We conclude that the matrix of $\varphi_1 : V_1 \to V'_1$ in the bases $\{e_i, f_j\}$ and $\{e'_i, f'_j\}$ is

$$
\varphi_1 = \begin{pmatrix} \varphi_{ij} & \varphi_{i,n+j} \\ \varphi_{n+i,j} & \varphi_{n+i,n+j} \end{pmatrix} = \begin{pmatrix} d & b \\ c & a \end{pmatrix}.
$$

Conversely, if $\left(\begin{smallmatrix} d & b \\ c & a \end{smallmatrix}\right)$ is the matrix of φ_1 in the bases $\{e_i, f_j\}$ and $\{e'_i, f'_j\}$ with $a, b, c, d \in \mathrm{M}_n(F)$, then the matrix of φ in the bases $\{v_i\}$ and $\{v'_i\}$ is $(\varphi_{ij}) \in \mathrm{M}_n(F)$, where φ is given by (2.4.5).

Corollary 38. *An explicit isomorphism between* $\mathrm{GU}_n(F) \longrightarrow \mathrm{GSp}_{2n}(F)$ *is given by the matrices used in the above calculations, where* $1 \leq i, j \leq n$*:*

$$
\varphi = \begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1n} \\ \vdots & \ddots & \vdots \\ \varphi_{n1} & \cdots & \varphi_{nn} \end{pmatrix} \quad \longleftrightarrow \quad \varphi_1 = \begin{pmatrix} d & b \\ c & a \end{pmatrix}
$$

$$
\varphi_{ij} = \left(\begin{smallmatrix} a_{ij} & b_{ij} \\ c_{ij} & d_{ij} \end{smallmatrix}\right) \qquad d = (d_{ij}), b = (b_{ij}), c = (c_{ij}), a = (a_{ij}).
$$

The precise description of the isomorphism described in Corollary 38 is essential for computational purposes. The relation between the Hermitian maps and symplectic maps makes it feasible to transfer information from one space to the other.

Chapter 3

Lattices in Hermitian vector spaces

3.1 Lattices, orders and ideals

This section contains relevant background information about lattices related to orders and ideals. Let F be the field of fractions of a Dedekind domain $\mathfrak{o}_F$. Let V be an n-dimensional F-vector space. Recall that an $\mathfrak{o}_F$-submodule $L \subset V$ is an $\mathfrak{o}_F$-*lattice* if L is a finitely-generated $\mathfrak{o}_F$-module and $V = FL$. The following result is a "relative version" of the structure theorem for modules over Dedekind domains:

Proposition 39. *[Elementary divisors theorem for modules over Dedekind domains] Let $\mathfrak{o}_F$ be a Dedekind domain and let F be its field of fractions. Let V be an n-dimensional F-vector space and let L and M be $\mathfrak{o}_F$-lattices in V. Then there is an F-basis $(v_1, \ldots, v_n)$ of V and sequences of fractional $\mathfrak{o}_F$-ideals $\mathfrak{a}_1 \supset \cdots \supset \mathfrak{a}_n$ and $\mathfrak{b}_1 \supset \cdots \supset \mathfrak{b}_n$ such that*

$$L = \mathfrak{a}_1 v_1 + \cdots + \mathfrak{a}_n v_n \quad \textit{and}$$

$$M = \mathfrak{b}_1\mathfrak{a}_1 v_1 + \cdots + \mathfrak{b}_n\mathfrak{a}_n v_n.$$

The sequence $\mathfrak{b}_1 \supset \cdots \supset \mathfrak{b}_n$ depends only on the ordered pair (L, M).

Proof. See Cohen [4, Theorem 1.2.35]. □

Definition 40. *The sequence*

$$\{L : M\} := (\mathfrak{b}_1, \ldots, \mathfrak{b}_n)$$

is called the sequence of elementary divisors of M with respect to L.

Lemma 41. *Let V be a finite-dimensional F-vector space and let L and M be $\mathfrak{o}_F$-lattices in V. Then there is an element $a \in \mathfrak{o}_F$ such that $aL \subset M$.*

Proof. Let $(\mathfrak{b}_1, \ldots, \mathfrak{b}_n)$ be the elementary divisors of M with respect to L. Since $\mathfrak{b}_i$ is a fractional $\mathfrak{o}_F$-ideal there is an element $a \in \mathfrak{o}_F$ such that $a\mathfrak{b}_i \subset \mathfrak{o}_F$ for all i. It follows immediately that $aL \subset M$. □

Let L be an $\mathfrak{o}_F$-lattice in V and let

$$E \subset \mathrm{End}_F(V)$$

be an F-subalgebra.

Definition 42. *An $\mathfrak{o}_F$-subalgebra $O \subset E$ is an* $\mathfrak{o}_F$-order *if it is also an $\mathfrak{o}_F$-lattice in E.*

Definition 43. *The* order of L in E *is*

$$O_E(L) := \{x \in E : xL \subset L\}.$$

Clearly, $O_E(L)$ is an $\mathfrak{o}_F$-subalgebra of E.

Lemma 44. *$O_E(L)$ is an $\mathfrak{o}_F$-order in E.*

Proof. Let $x \in E$. Then xL is also an $\mathfrak{o}_F$-lattice in V. Therefore, by Lemma 41, there is an element $a \in \mathfrak{o}_F$ such that $axL \subset L$. It follows that $ax \in O_E(L)$. Therefore, $x \in a^{-1}O_E(L) \subset FO_E(L)$ and we conclude that $E \subset FO_E(L)$.

It remains to show that $O_E(L)$ is a finitely-generated $\mathfrak{o}_F$-module. To see this, note that the *faithful* left action of $O_E(L)$ on L gives rise to an inclusion

$$O_E(L) \hookrightarrow \mathrm{End}_{\mathfrak{o}_F}(L).$$

By the structure theory of finitely-generated modules over Dedekind domains, there are fractional $\mathfrak{o}_F$-ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ and an F-basis $(v_1, \ldots, v_n)$ of V such that

$$L = \mathfrak{a}_1 v_1 + \cdots \mathfrak{a}_n v_n.$$

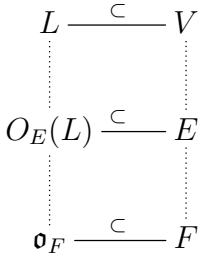
Therefore, we have

$$\mathrm{End}_{\mathfrak{o}_F}(L) \xrightarrow{\sim} \mathrm{Hom}_{\mathfrak{o}_F}\left(\bigoplus_{i=1}^{n} \mathfrak{a}_i, \bigoplus_{j=1}^{n} \mathfrak{a}_j\right) = \bigoplus_{i,j=1}^{n} \mathrm{Hom}_{\mathfrak{o}_F}(\mathfrak{a}_i, \mathfrak{a}_j) = \bigoplus_{i,j=1}^{n} \mathfrak{a}_i^{-1}\mathfrak{a}_j.$$

Since fractional ideals in Dedekind domains are, by definition, finitely generated, it follows that $\mathrm{End}_{\mathfrak{o}_F}(L)$ is a finitely-generated $\mathfrak{o}_F$-module. Since $\mathfrak{o}_F$ is a Noetherian ring (it's a Dedekind domain), $\mathrm{End}_{\mathfrak{o}_F}(L)$ is a Noetherian $\mathfrak{o}_F$-module by the Hilbert Basis Theorem. Therefore, the $\mathfrak{o}_F$-submodule $O_E(L)$ of $\mathrm{End}_{\mathfrak{o}_F}(L)$ is a finitely-generated $\mathfrak{o}_F$-module. □

Remark 45. *Since $\mathfrak{o}_F$-lattices in E exist – take $\mathfrak{o}_F x_1 + \cdots \mathfrak{o}_F x_n$ where $(x_1, \ldots, x_n)$ is an F-basis of E, for instance – it follows that $\mathfrak{o}_F$-orders in E exist. Your standard Zorn's Lemma argument shows that every $\mathfrak{o}_F$-order is contained in a maximal $\mathfrak{o}_F$-order.*

Definition 46. *Let O be an $\mathfrak{o}_F$-order in E. We say that an $\mathfrak{o}_F$-lattice L in V is an* O-lattice *if $O = O_E(L)$.*



Definition 47. *L is E-*normal *if $O_E(L)$ is maximal among $\mathfrak{o}_F$-orders in E.*

The F-algebras $E \subset \mathrm{End}_F(V)$ we will consider will arise from the following simple construction: Let E be a quaternion F-algebra and let V be a free E-module of finite rank. Then V is also a finite dimensional F-vector space and the action of E on V by scalar multiplication is F-linear, yielding an inclusion of F-algebras $E \hookrightarrow \mathrm{End}_F(V)$.

3.1.1 Ideal classes

Let E be a finite dimensional F-algebra and let O be an $\mathfrak{o}_F$-order in E.

Definition 48. *A left $\mathfrak{o}_F$-lattice in E is called a* left O-ideal.

Trivially, O itself is a left O-ideal. Let I be a left O-ideal and let $x \in E^\times$. Then it is easy to see that Ix is also a left O-ideal. In particular, Ox is a left O-ideal for all $x \in E^\times$; these ideals are called *principal*.

Lemma 49. *Let $I, J \subset E$ be left O-ideals. Then the following are equivalent:*

1. *I and J are isomorphic as left O-modules.*
2. *There is an element $a \in E^\times$ such that $J = Ia$.*

Proof. It is clear that (2) implies (1). To prove the converse, let $\varphi : I \to J$ be an isomorphism of left O-modules. In particular, φ is a homomorphism of $\mathfrak{o}_F$-modules. Extend φ by scalars to an F-linear isomorphism

$$\widetilde{\varphi} : F \otimes_{\mathfrak{o}_F} I \longrightarrow F \otimes_{\mathfrak{o}_F} J.$$

Since I and J are $\mathfrak{o}_F$-lattices in E, we have canonical isomorphisms

$$F \otimes_{\mathfrak{o}_F} I \xrightarrow{\sim} FI = E \quad \text{and} \quad F \otimes_{\mathfrak{o}_F} J \xrightarrow{\sim} FJ = E.$$

Therefore, we may view $\widetilde{\varphi}$ as an F-linear automorphism of E. Since φ is left O-linear, so is $\widetilde{\varphi}$. Therefore, $\widetilde{\varphi}$ is left E-linear as $E = FO$. Letting $a = 1\widetilde{\varphi}$, we see that

$$x\widetilde{\varphi} = (x \cdot 1)\widetilde{\varphi} = x(1\widetilde{\varphi}) = xa.$$

Since $\varphi = \widetilde{\varphi}|_I$ and φ maps I isomorphically onto J, the result follows. □

Definition 50. *We say that two left O-ideals $I, J \subset E$ are* right equivalent *if either (equivalently, both) of the conditions of Lemma 49 are satisfied. The set of right equivalence classes of left O-ideals is called the left ideal class set of O and is denoted* $\mathrm{Cl}_\ell(O)$.

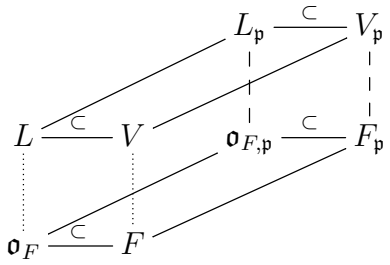
Let Ox be a principal, left O-ideal and let I be any left O-ideal. Then Ox and I are right equivalent if and only if I is principal. Thus, the set of principal, left O-ideals forms a right equivalence class. This class gives a distinguished element of $\mathrm{Cl}_\ell(O)$ and, thus, $\mathrm{Cl}_\ell(O)$ is naturally a "pointed" set.

3.2 Completions

Let V be an n-dimensional F-vector space and $\mathfrak{p}$ be a prime ideal of $\mathfrak{o}_F$. We describe lattices in their corresponding completed space a a prime $\mathfrak{p}$. Let L be an $\mathfrak{o}_F$-lattice in V and set

$$L_{\mathfrak{p}} := \mathfrak{o}_{F,\mathfrak{p}} \otimes_{\mathfrak{o}_F} L.$$

Then $L_{\mathfrak{p}}$ can be viewed naturally as a subset of $F_{\mathfrak{p}} \otimes_F V = V_{\mathfrak{p}}$.



Lemma 51.

1. *If L is an $\mathfrak{o}_F$-lattice in V then $L_{\mathfrak{p}}$ is an $\mathfrak{o}_{F,\mathfrak{p}}$-lattice in $V_{\mathfrak{p}}$.*

2. *If L and M are $\mathfrak{o}_F$-lattices in V,*

$$\{L : M\} = (\mathfrak{b}_1, \ldots, \mathfrak{b}_n) \quad \textit{and}$$

$$\{L_{\mathfrak{p}} : M_{\mathfrak{p}}\} = (\mathfrak{b}_{1,\mathfrak{p}}, \ldots, \mathfrak{b}_{n,\mathfrak{p}})$$

where $\mathfrak{b}_{i,\mathfrak{p}} = \mathfrak{b}_i \mathfrak{o}_{F,\mathfrak{p}}$.

Proof.

1. The lattice $L_{\mathfrak{p}}$ is an extension of L by scalars from $\mathfrak{o}_{F,\mathfrak{p}}$. Then $L_{\mathfrak{p}}$ is also finitely generated and $F_{\mathfrak{p}} L_{\mathfrak{p}} = V_{\mathfrak{p}}$. Therefore, $L_{\mathfrak{p}}$ is an $\mathfrak{o}_{F,\mathfrak{p}}$-lattice in $V_{\mathfrak{p}}$.

2. Here we extend Proposition 39 to the completed space $V_{\mathfrak{p}}$ where the $\mathfrak{o}_{F,\mathfrak{p}}-$ideals satisfy $\mathfrak{a}_{1,\mathfrak{p}} \supset \cdots \supset \mathfrak{a}_{n,\mathfrak{p}}$, $\mathfrak{b}_{1,\mathfrak{p}} \supset \cdots \supset \mathfrak{b}_{n,\mathfrak{p}}$ and

$$L_{\mathfrak{p}} = \mathfrak{a}_{1,\mathfrak{p}} v_1 + \cdots + \mathfrak{a}_{n,\mathfrak{p}} v_n$$

$$M_{\mathfrak{p}} = \mathfrak{b}_{1,\mathfrak{p}} \mathfrak{a}_{1,\mathfrak{p}} v_1 + \cdots + \mathfrak{b}_{n,\mathfrak{p}} \mathfrak{a}_{n,\mathfrak{p}} v_n.$$

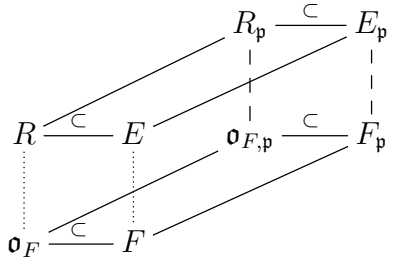
□

Let E be a finite-dimensional F-algebra. Then $E_\mathfrak{p}$ is a finite-dimensional $F_\mathfrak{p}$-algebra.

Lemma 52.

1. *If R is an $\mathfrak{o}_F$-order in E then $R_\mathfrak{p}$ is an $\mathfrak{o}_{F,\mathfrak{p}}$-order in $E_\mathfrak{p}$.*
2. *R is a maximal $\mathfrak{o}_F$-order if and only if $R_\mathfrak{p}$ is a maximal $\mathfrak{o}_{F,\mathfrak{p}}$-order for all $\mathfrak{p}$.*

Proof. (Sketch.) Again, we extend the global objects into the completed space. Here $R_\mathfrak{p} = \mathfrak{o}_{F,\mathfrak{p}} \otimes_{\mathfrak{o}_F} R$. Like the lattices described previously, the relevant objects can be organized in the diagram below.

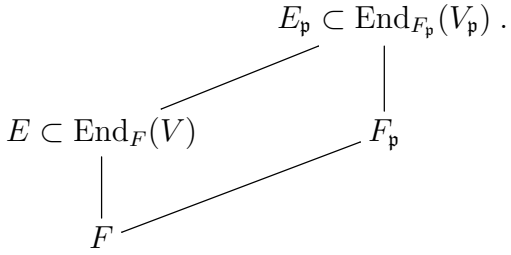


□

Suppose now that E is an F-subalgebra of $\mathrm{End}_F(V)$.

Lemma 53. *$E_\mathfrak{p}$ is canonically identified with the closure of E in $\mathrm{End}_{F_\mathfrak{p}}(V_\mathfrak{p})$.*

Proof. Identifying a completion of $F_\mathfrak{p}$ and in turn $V_\mathfrak{p}$, we can correspondingly embed $E \hookrightarrow E_\mathfrak{p}$,



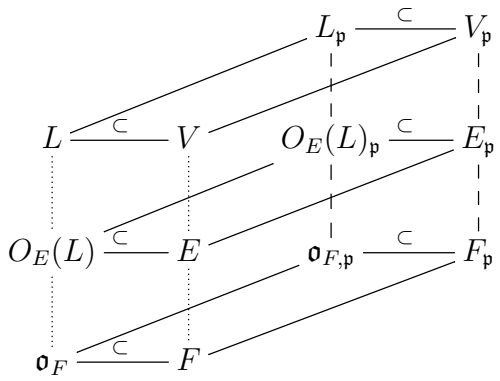
□

Let L be an $\mathfrak{o}_F$-lattice in V.

Lemma 54.

1. *The canonical map $O_E(L)_\mathfrak{p} \to O_E(L_\mathfrak{p})$ is an isomorphism.*
2. *L is E-normal if and only if $L_\mathfrak{p}$ is $E_\mathfrak{p}$-normal for all $\mathfrak{p}$.*

Proof. (Sketch.) Again we define $O_E(L)_\mathfrak{p} = \mathfrak{o}_{F,\mathfrak{p}} \otimes_{\mathfrak{o}_F} O_E(L) = \mathfrak{o}_{F,\mathfrak{p}} \otimes_{\mathfrak{o}_F} \{x \in E : xL \subset L\}$ and $O_E(L) = \{x \in E : xL_\mathfrak{p} \subset L_\mathfrak{p}\}$. We can either extend L by scalars first and compute its order or extend the order $O_E(L)$ by scalars. In either case we arrive at two isomorphically equivalent sets.



□

Therefore, if $I \subset E$ is a left O-ideal then $I_\mathfrak{p} \subset E_\mathfrak{p}$ is a left $O_\mathfrak{p}$-ideal. If O is a Dedekind Domain then $O_\mathfrak{p}$ is a discrete valuation ring and we can state the following [22, Ch. 3, §2].

Proposition 55. *Suppose $O_\mathfrak{p}$ is a maximal order in $E_\mathfrak{p}$. Then every left $O_\mathfrak{p}$-ideal in $E_\mathfrak{p}$ is principal.*

Thus, the notion of right-equivalence of ideals is trivial in the situation of the proposition.

3.3 Quaternionic lattices

In this section we focus our attention to those lattices in quaternionic vector spaces. Of particular note – essential for our terminable algorithm – is Theorem 59.

Let F be the field of quotients of a Dedekind domain $\mathfrak{o}_F$ and let E be a quaternion F-algebra. Let O, a subalgebra of E that is also a lattice, be an $\mathfrak{o}_F$-order in E. Let V be a free, left E-module of finite rank and let

$$h : V \times V \longrightarrow E$$

be a nondegenerate, Hermitian form. Let G be $G(V,h)$ or $G^0(V,h)$.

Definition 56. *Two O-lattices L and M in V are* G-equivalent *if there is a transformation $\varphi \in G$ such that $M = L\varphi$.*

For a prime $\mathfrak{p}$ of F, let $G_\mathfrak{p}$ be the appropriate completion $G(V_\mathfrak{p}, h_\mathfrak{p})$ or $G^0(V_\mathfrak{p}, h_\mathfrak{p})$.

Definition 57. *Two O-lattices L and M in V are* locally G-equivalent *if for every prime $\mathfrak{p}$ of $\mathfrak{o}_F$ there is a transformation $\varphi_\mathfrak{p} \in G_\mathfrak{p}$ such that $M_\mathfrak{p} = L_\mathfrak{p}\varphi_\mathfrak{p}$. The* G-genus *of L, written* $\mathrm{gen}_G(L)$*, is set of all lattices M locally G-equivalent to L.*

Lattices which are G-equivalent are obviously locally G-equivalent: if two lattices are equivalent globally, then it follows that they are equivalent at every prime.

Definition 58. *The* G-class set *of L is the quotient*

$$\mathrm{cl}_G(L) := \mathrm{gen}_G(L)/G. \tag{3.3.1}$$

In other words, $\mathrm{cl}_G(L)$ is the set of G-equivalence classes of lattices contained in the local G-equivalence class of G.

The following finiteness theorem is an adaptation of Gross' Proposition [9, Proposition 4.3] and is fundamental.

Theorem 59. *Suppose F is a global field. Then $\mathrm{cl}_G(L)$ is finite.*

Proof. Recall that $G = G(F)$ denotes either $G(V,h)$ or $G^0(V,h)$. The group G is of type $\mathrm{C}(n)$, where $\dim V = n$, as described by Gross [9]. Assume that $G(F_\infty) = G(\mathbb{R} \otimes_\mathbb{Q} F)$ is

compact. This will ensure that the conditions of Gross' hypothesis are satisfied. For primes $\mathfrak{p}$ such that $E_{\mathfrak{p}}$ splits, $G_{\mathfrak{p}}$ is the unitary group $G(V_{\mathfrak{p}}, h)$ or the similitude group $G^0(V_{\mathfrak{p}}, h)$. By the explicit Morita equivalence in Corollary 37, $G_{\mathfrak{p}}$ is equivalent to the symplectic similitude group and the symplectic group, $G(V_1, h_{12})$ and $G^0(V_1, h_{12})$, respectively.

Let L and M be lattices over $\mathfrak{o}_F$. We can consider if the are equivalent adèlically. I.e., we gather up all of the local information pertaining to lattices for every prime via adèlization. We can represent local equivalence between two lattices L and M by:

$$\widehat{L}\widehat{\varphi} = \widehat{M}$$

where $\widehat{\varphi} = (\varphi_{\mathfrak{p}})_{\mathfrak{p}} \in G(\widehat{F})$ and for a lattice L, $\widehat{L} = (L_{\mathfrak{p}})_{\mathfrak{p}}$. Define a right action on L by

$$(L, \widehat{\varphi}) \mapsto M = L\widehat{\varphi}.$$

Then $G(\widehat{F})$ acts on $\mathrm{gen}_G(L)$ from the right. Let $\widehat{K}_L$ be the stabilizer of $\widehat{L}$ in $G(\widehat{F})$:

$$\widehat{K}_L = \{\widehat{\varphi} \in G(\widehat{F}) \mid \widehat{L}\widehat{\varphi} = \widehat{L}\}.$$

Then

$$\begin{aligned} \widehat{K}_L\backslash G(\widehat{F}) &\to \mathrm{gen}_G(L) \\ \widehat{K}_L\widehat{\varphi} &\mapsto L\widehat{\varphi} \end{aligned}$$

gives a bijection of G sets[1]. The set $\widehat{K}_L\backslash G(\widehat{F})$ is the domain of an algebraic modular form ([9, Equation 4.2], [8, Definition 2.2]) of level $\widehat{K}_L$, which makes the genus an interesting object to calculate! Moreover,

$$\widehat{K}_L\backslash G(\widehat{F})/G(F) \leftrightarrow \mathrm{gen}_G(L)/G = \mathrm{cl}_G(L)$$

describes the class set of a lattice via a double coset space. Then the (equivalent) conditions of Gross' Proposition 1.4 [9] are satisfied. This adaptation of Gross' Proposition [9, Proposition 4.3] now follows. □

[1]Pardon the unconventional convention! While in the literature, it is standard to write this as a right coset, for our purposes it is more convenient to work with the left.

We call the size of $\mathrm{cl}_G(L)$ the *G-class number of L* and denote it by $h_G(L)$.

Remark 60. *What is especially interesting about the algebraic modular forms described in the proof of Theorem 59, is that one may use a* lattice *to define a* level *for a modular form on a group.*

Remark 61. *The study of the groups of type $C(n)$ described in the proof of Theorem 59 is analogous to those considered by Greenberg and Voight [8] which correspond to the types $A(n)$, $B(n)$ and $D(n)$. Again, see Gross [9].*

Example 62. *Consider the standard 1-dimensional Hermitian E-space (E, h), where $h(x, y) = x\bar{y}$. Let φ be a left E-linear automorphism of E. By the same reasoning as in the proof of Lemma 49, φ is given by right-multiplication by an element $a \in E^\times$:*

$$x\varphi = xa \quad \textit{for all } x \in E.$$

Then

$$h(x\varphi, y\varphi) = N(a)h(x, y).$$

In other words, φ is automatically in $G := G(V, h)$ and it follows that $\varphi \mapsto a$ is an isomorphism

$$G \xrightarrow{\sim} E^\times.$$

Thus, two O-lattices $I, J \subset E$ are G-equivalent if and only if they are right-equivalent as O-ideals. Now suppose O is a maximal $\mathfrak{o}_F$-order in E. Then by Proposition 55, any two left O-ideals in E are automatically locally equivalent. Therefore, there is a canonical identification

$$\mathrm{cl}_G(O) = \mathrm{Cl}_\ell(O).$$

In other words, when $n = 1$ and O is maximal, (3.3.1) *recovers the notion of left ideal class set.*

3.3.1 Norm and maximality

Let L be an $\mathfrak{o}_F$-lattice in V.

Definition 63. *The h-norm of L, denoted $N(L)$, is the $\mathfrak{o}_F$-submodule of E generated by the Hermitian form on all of L, i.e. $h(L, L)$.*

We list some properties of the norm:

Lemma 64.

1. *$N(L)$ is a two-sided $O_E(L)$-ideal.*
2. *Let $\mathfrak{p}$ be a prime of $\mathfrak{o}_F$. Then $N(L_\mathfrak{p}) = N(L)_\mathfrak{p}$.*
3. *Let $\varphi \in G(V, h)$. Then $N(L\varphi) = N(L)N(\varphi)$.*

Proof.

1. For $x, y \in L$, note that $\overline{h(x, y)} = h(y, x) \in N(L)$ and so $\overline{N(L)} = N(L)$. For $\alpha \in O_E(L)$ consider $\alpha h(x, y) = h(\alpha x, y) \in N(L)$ and $h(x, y)\alpha = h(x, \overline{\alpha} y) \in N(L)$, i.e. $N(L)$ is a two-sided $O_E(L)-$ideal.
2. We complete the $O_E(L)-$ideal $N(L)$ at $\mathfrak{p}$ to arrive at $N(L)_\mathfrak{p}$ or first complete L to $L_\mathfrak{p}$ and then compute its norm $N(L_\mathfrak{p})$ generated by $h(L_\mathfrak{p}, L_\mathfrak{p})$; in either direction, we arrive at the same set.
3. The $O_E(L)-$ideal $N(L\varphi)$ is generated by

$$h(L\varphi, L\varphi) = N(\varphi)h(L, L) = h(L, L)N(\varphi),$$

as $N(\varphi) \in E^\times$ and so it follows that $N(L\varphi) = N(L)N(\varphi)$.

□

Definition 65. *We say that a normal $\mathfrak{o}_F$-lattice L in V is* maximal *if L is maximal among lattices M with $O_E(M) = O_E(L)$ and $N(M) = N(L)$.*

3.4 Digression on lattices in symplectic vector spaces

To facilitate our computations related to lattices in Hermitian space, we provide the relevant details for lattices in symplectic space, which is ultimately transferred back to describe Hermitian lattices. In particular, we give an adaptation of the elementary divisor theorem for symplectic lattices in Proposition 73 and the Corollaries 78 and 77 which follow from this result.

Let (V, g) be a nondegenerate symplectic vector space over F of dimension $2n$ and let L be an $\mathfrak{o}_F$-lattice in V.

Definition 66. *The* norm of L, *denoted* $N(L)$, *is the fractional* $\mathfrak{o}_F$*-ideal generated by* $g(L, L)$.

Let $\mathfrak{o}_F$ be a discrete valuation ring.[2]

Proposition 67 (Invariant factors theorem)**.** *There is a symplectic basis* $(e_1, \ldots, e_n, f_1, \ldots, f_n)$ *of* V *and fractional* $\mathfrak{o}_F$*-ideals* $\mathfrak{a}_1 \supset \cdots \supset \mathfrak{a}_n$ *such that*

$$L = \mathfrak{o}_F e_1 + \cdots + \mathfrak{o}_F e_n + \mathfrak{a}_1 f_1 + \cdots + \mathfrak{a}_n f_n.$$

The ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ *depend only on* L *(and* g*).*

Proof. Let $\mathfrak{p} = \mathfrak{o}_F \pi$ be the maximal ideal of $\mathfrak{o}_F$ and let v be the valuation on F normalized so that $v(\pi) = 1$. Let L be an $\mathfrak{o}_F$-lattice in V. We give a construction for computing the invariant factors $\mathfrak{a}_1 \supset \cdots \supset \mathfrak{a}_n$ of L together with a symplectic basis of V as specified in Proposition 67.

Define $k_1 \in \mathbb{Z}$ by $N(L) = \mathfrak{o}_F \pi^{k_1}$, i.e.,

$$k_1 = \min_{x,y \in L} v(g(x, y)).$$

Find $e_1, f_1' \in L$ such that $g(e_1, f_1') = \pi^{k_1}$. The basis elements e_1 and f_1' can be taken to be of the form ux_i for some $u \in \mathfrak{o}_F^\times$ if $(x_1, \ldots, x_m)$ generates L as an $\mathfrak{o}_F$-module. Set $f_1 = \pi^{-k_1} f_1'$.

[2]It can be shown that Proposition 67 holds more generally, but the case of $\mathfrak{o}_F$ a DVR is sufficient for our purposes.

Then it is easy to see that $g(e_1, L) = \pi^{k_1}\mathfrak{o}_F$ and $g(L, f_1) = \mathfrak{o}_F$. Set

$$V' = (Fe_1 + Ff_1)^{\perp}$$

and let

$$L' = V' \cap L = \{x \in L : g(x, e_1) = g(x, f_1) = 0\}.$$

Claim: We have the direct sum decomposition

$$L = \mathfrak{o}_F e_1 + \mathfrak{o}_F \pi^{k_1} f_1 + L'.$$

We clearly have containment of the right hand side in the left. To prove the opposite containment, let $x \in L$. Then we can write

$$x = \alpha e_1 + \beta \pi^{k_1} f_1 + y,$$

where $\alpha, \beta \in F$ and $y \in V'$. Then

$$\mathfrak{o}_F \ni g(\pi^{-k_1} e_1, x) = \beta \pi^{k_1} g(\pi^{-k_1} e_1, f_1) = \beta$$

and

$$\mathfrak{o}_F \ni g(x, f_1) = \alpha g(e_1, f_1) = \alpha.$$

If follows that

$$y = x - \alpha e_1 - \beta \pi^{k_1} f_1 \in L$$

and the claim follows. Proceeding by induction, we may assume that there are integers $v(N(L')) = k_2 \leq \cdots \leq k_n$ and a symplectic basis $(e_2, \ldots, e_n, f_2, \ldots, f_n)$ of V' such that

$$L' = \mathfrak{o}_F e_2 + \cdots \mathfrak{o}_F e_n + \mathfrak{o}_F \pi^{k_2} f_2 + \cdots \mathfrak{o}_F \pi^{k_n} f_n.$$

Since $N(L) \supset N(L')$ it follows that $k_1 \leq k_2$, as required. Therefore, $\mathfrak{o}_F \pi^{k_1}, \ldots, \mathfrak{o}_F \pi^{k_n}$ are the invariant factors of L and (e, f) is a symplectic basis of V adapted to L. □

Definition 68. *The ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ are called the* invariant factors of L. *A symplectic basis (e, f) as in Proposition 67 is said to be* adapted to L.

Observe that

$$N(L) = \mathfrak{a}_1.$$

Definition 69. *L is* maximal *if it is maximal among lattices M in V with $N(M) = N(L)$. Write $\mathcal{L}(V, g)$ for the set of maximal lattices in V.*

Corollary 70. *L is maximal if and only if $\mathfrak{a}_1 = \ldots = \mathfrak{a}_n$.*

Proof. This follows directly from Proposition 67. □

For example, consider the case $n = 2$ and the dimension of the symplectic space is $2n = 4$. Let $L = \mathfrak{o}_F e_1 + \mathfrak{o}_F e_2 + \mathfrak{a} f_1 + \mathfrak{a} f_2$, which has norm $N(L) = \mathfrak{a}$. Consider now the lattice $L' = \mathfrak{o}_F e_1 + \mathfrak{o}_F e_2 + \mathfrak{a} f_1 + \mathfrak{a}^2 f_2$. The norm of L' is also $N(L') = \mathfrak{a}$, but $L' \subset L$. Then L' gives an example of a nonmaximal lattice.

Let $\sigma \in \mathrm{G}(V, g)$. Then one verifies easily that $N(L\sigma) = N(L)N(\sigma)$ and that $L\sigma$ is maximal if and only if L is. For instance, suppose that L and M are $\mathrm{G}(V, g)-$equivalent but that only L is a maximal lattice. Then there is some $\sigma \in \mathrm{G}(V, g)$ such that $L\sigma = M$. Taking norms, $N(L\sigma) = N(M)$ and $N(L)N(\sigma) = \mathfrak{a}_1 t = N(M)$ for some $t \in F^\times$. Which implies that M is maximal, contradicting the assumption.

Corollary 71. *Suppose L and M are maximal. Then L and M are $\mathrm{G}(V, g)$-equivalent if and only if $N(L)$ and $N(M)$ define the same element in $\mathrm{Cl}(\mathfrak{o}_F)$. L and M are $\mathrm{G}^0(V, g)$-equivalent if and only if $N(L) = N(M)$. In other words, the mapping $L \mapsto N(L)$ induces a canonical bijection*

$$\mathcal{L}(V, g)/G(V, g) \xrightarrow{\sim} \mathrm{Cl}(\mathfrak{o}_F).$$

Proof. Let (e, f) and (e', f') be symplectic bases of V adapted to L and M, respectively, and let $t \in F^\times$ be such that $N(L)t = N(M)$. Let $\sigma \in \mathrm{GL}(V)$ be unique transformation such that

$$e_i\sigma = e'_i \quad \text{and} \quad f_i\sigma = tf'_i \quad \text{where} \quad 1 \leq i \leq n.$$

Then $\sigma \in \mathrm{G}(V,g)$ and $N(\sigma) = t$. By the definition of t and the maximality of L and M we have $L\sigma = M$. □

Remark 72. *In particular,* for our purposes*, Corollary 71 says that the arithmetic of maximal lattices in symplectic spaces is no more interesting than the arithmetic of the underlying field. For this reason, we do not devote study to genera or class sets in the symplectic setting. For us, the theory of maximal lattices in symplectic spaces is a* tool *for understanding class sets of maximal lattices in Hermitian E-spaces where E is a nonsplit quaternion F-algebra – see §3.7 and §3.8 for details.*

Proposition 73 (Elementary divisors theorem)**.** *Suppose $\mathfrak{o}_F$ is a PID. Let L and M be maximal lattices in V and set $\mathfrak{a} = N(L)$. Then there is a symplectic basis (e,f) of V adapted to L and elements $a_1,\dots,a_n,b_1,\dots,b_n$ of $F^\times$ such that*

$$a_1b_1 = \cdots = a_nb_n,$$

$$\mathfrak{o}_Fa_1 \supset \cdots \supset \mathfrak{o}_Fa_n \supset \mathfrak{o}_Fb_n \supset \cdots \supset \mathfrak{o}_Fb_1$$

and

$$M = \mathfrak{o}_Fa_1e_1 + \cdots + \mathfrak{o}_Fa_ne_n + \mathfrak{a}b_1f_1 + \cdots + \mathfrak{a}b_nf_n.$$

The ideals $\mathfrak{o}_Fa_1,\cdots,\mathfrak{o}_Fa_n,\mathfrak{a}b_1,\cdots,\mathfrak{a}b_n$ are uniquely determined by L and M.

Proof. This follows from the more general setting of the elementary divisors theorem for modules over Dedekind domains, Proposition 39, and the structure of lattices in symplectic space given by the invariant factors theorem, Proposition 67. □

Definition 74. *The sequence of ideals*

$$\{L : M\} := (\mathfrak{o}_Fa_1,\cdots,\mathfrak{o}_Fa_n,\mathfrak{a}b_1,\cdots\mathfrak{a}b_n)$$

is called the sequence[3] *of* elementary divisors of M relative to L*. It will be useful to call a*

[3] *In the context of Proposition 39, the sequence of ideals $(\mathfrak{b}_1,\dots,\mathfrak{b}_{2n})$ is given by $\mathfrak{b}_i = \mathfrak{o}_Fa_i$ for $1 \le i \le n$ and $\mathfrak{b}_j = \mathfrak{a}b_j$ for $n+1 \le j \le 2n$.*

sequence

$$(a, b) = (a_1, \ldots, a_n, b_1, \ldots, b_n)$$

of elements of $F^\times$ *an* elementary sequence.

Assumption 75. *For the remainder of Chapter 3 we assume that* $\mathfrak{o}_F$ *is a PID.*

Remark 76. *In our applications to enumeration of quaternionic lattices, we will be applying the theory of maximal lattices in symplectic spaces only when* F *is a local field. Thus, Assumption 75 will be satisfied.*

Fix a "base lattice" Λ in V with $N(\Lambda) = \mathfrak{o}_F$ and let (e, f) be a symplectic basis of V adapted to Λ. Since $N(\Lambda) = \mathfrak{o}_F$, (e, f) is also an $\mathfrak{o}_F$-basis of Λ. Set

$$K = K_\Lambda = \{\sigma \in G(V, g) : \Lambda\sigma = \Lambda\}$$

and let

$$\Delta = \Delta(e, f) = \{\sigma \in G(V, g) : \exists \text{ elem. seq. } (a, b) \text{ s.t. } e_i\sigma = a_i e_i \text{ and } f_i\sigma = b_i f_i\}.$$

Equivalently, Δ is the subset of $G(V, g)$ consisting of elements that are diagonal when written as a matrix in the basis (e, f).

Corollary 77.

1. *Let* L *be a maximal lattice in* V*. Then there are elements* $d \in \Delta$ *and* $k \in K$ *such that*

   $$L = \Lambda dk.$$

   In particular, $G(V, g)$ *acts transitively on* $\mathcal{L}(V, g)$*.*

2. *The* singular value decomposition $G(V, g) = K\Delta K$ *holds.*

3. *The mapping* $dk \mapsto \Lambda dk$ *descends to a bijection*

   $$K\backslash G(V, g) \xrightarrow{\sim} \mathcal{L}(V, g).$$

Proof. (Sketch.)

1. By the theorem of elementary divisors, Proposition 73, there exists an elementary sequence, corresponding to a map $d \in \Delta$ such that

$$L' = \Lambda d = \mathfrak{o}_F a_1 e_1 + \cdots + \mathfrak{o}_F a_n e_n + \mathfrak{o}_F b_1 f_1 + \cdots + \mathfrak{o}_F b_n f_n$$

(which in general need not be L itself.) Applying an appropriate stabilizer $k \in K$ of Λ takes Λd to $L = \Lambda dk$.

2. As every lattice L can be found in this way (part 1) the action by $G(V, g)$ can be decomposed as $K\Delta K$ since for $k'dk \in K\Delta K$, $\Lambda k'dk = \Lambda dk$.

3. The action by the left most K (part 2) fixes Λ and so we shall count it only once. Then $K\backslash K\Delta K = K\backslash G(V, g) \cong \mathcal{L}(V, g)$.

□

We record one more consequence of the Elementary Divisors Theorem that will be useful later.

Corollary 78. *Suppose $k \in G^0(V, g)$ is such that $Lk = L$. Then $\{L : M\} = \{L : Mk\}$ for all $M \in \mathcal{L}(V, g)$. Conversely, if $M, M' \in \mathcal{L}(V, g)$ satisfy $\{L : M\} = \{L : M'\}$ then there exists a map $k \in G^0(V, g)$ such that $Lk = L$ and $M' = Mk$.*

Proof. Applying the map $k \in G^0(V, g)$ to both L and M means that their invariant factors remain unchanged. Then $\{L : M\} = \{Lk : Mk\} = \{L : Mk\}$ for all $M \in \mathcal{L}(V, g)$. The converse is clear. □

It is from Corollaries 78 and 77 that we are able to construct a notion of lattice neighbours in a systematic way.

3.5 Neighbours of symplectic lattices

This section includes details on the particular type of $\mathfrak{p}-$neighbours that we have described. The motivation behind our take on neighbours – differing from the original version described by Knesser [12] – is so that the construction can be done in a systematic way, thanks to the transitive action of $G(V,g)$ on maximal symplectic lattices. We can describe all neighbours explicitly via Lemma 83.

Let F be a local field with ring of integers $\mathfrak{o}_F$, maximal ideal $\mathfrak{p} = \mathfrak{o}_F\pi$ and residue class field $\mathbb{F}_\mathfrak{p}$. Let (V,g) be a nondegenerate symplectic space of dimension $2n$. The following notion plays a central role in the computations to come:

Definition 79. *Let $L, M \in \mathcal{L}(V,g)$. We say that M* is a $\mathfrak{p}-$neighbour of L *if*

$$\{L : M\} = (\mathfrak{o}_F, \ldots, \mathfrak{o}_F, \mathfrak{p}, \ldots, \mathfrak{p}).$$

We write $\mathcal{N}_\mathfrak{p}(L)$ for the set of $\mathfrak{p}$-neighbours of L.

In particular, if M is a $\mathfrak{p}$-neighbour of L then $M \subset L$.

Definition 80. *An $\mathfrak{o}_F$-lattice L in V is* integral *if $g(L,L) \subset \mathfrak{o}_F$.*

Let L be the $n-$dimensional standard lattice over $\mathfrak{o}_F$: $L = \mathfrak{o}_F^n$. Consider $M = \frac{1}{2}L$, which is a finitely generated $\mathfrak{o}_F-$module and $FM = V$, however $g(M,M) = \frac{1}{4}g(L,L) \not\subset \mathfrak{o}_F$. I.e. M is a *nonintegral* lattice. On the other hand, a lattice can be integral but not maximal. For example, take $M' = \mathfrak{o}_F^{n-1} \oplus 2\mathfrak{o}_F$. Then $N(M') = N(L) \subset \mathfrak{o}_F$ but M' is not maximal.

Lemma 81. *The following are equivalent for an $\mathfrak{o}_F$-lattice L in V:*

1. *L is maximal and $N(L) = \mathfrak{o}_F$.*
2. *L is integral and the induced pairing $\bar{g} : L/\mathfrak{p}L \times L/\mathfrak{p}L \to \mathbb{F}_\mathfrak{p}$ is nondegenerate.*
3. *L has a symplectic basis.*

Proof. By the Invariant Factors Theorem, there is a symplectic basis (e, f) of V and integers $k_1 \leq \cdots \leq k_n$ such that

$$L = \mathfrak{o}_F e_1 + \cdots + \mathfrak{o}_F e_n + \mathfrak{p}^{k_1} f_1 + \cdots + \mathfrak{p}^{k_n} f_n.$$

Then $N(L) = \mathfrak{p}^{k_1}$. Suppose L is maximal and $N(L) = \mathfrak{o}_F$. Then $k_1 = \cdots = k_n = 0$ and (e, f) is actually a symplectic $\mathfrak{o}_F$-basis of L. It follows that L is integral and that $\bar{g}$ is nondegenerate, so (1) $\Rightarrow$ (2). Now suppose that L is integral and $\bar{g}$ is nondegenerate. By integrality, $k_i \geq 0$ for all i. Suppose $k_i \geq 1$ for some i. Let $y = \pi^{k_i} f_i$. Then $y \in L$, $y \notin \mathfrak{p}L$, and $g(L, \pi^{k_i} f_i) \in \mathfrak{p}^{k_i} \subset \mathfrak{p}$. This contradicts the nondegeneracy of $\bar{g}$. Therefore, we must have $k_i = 0$ for all i, proving (2) $\Rightarrow$ (3). The implication (3) $\Rightarrow$ (1) is clear. □

Definition 82. *A lattice satisfying the equivalent conditions of Lemma 81 is called* primitive.

Let $L \in \mathcal{L}(V, g)$ be primitive and let $\bar{L} = L/\mathfrak{p}L$, so that g induces a nondegenerate, symplectic pairing

$$\bar{g} : \bar{L} \times \bar{L} \longrightarrow \mathbb{F}_\mathfrak{p}.$$

In other words, $(\bar{L}, \bar{g})$ is a nondegenerate, symplectic $\mathbb{F}_\mathfrak{p}$-space of dimension $2n$. If M is a sublattice of L we write X_M for the image of M in $\bar{L}$ by the reduction modulo $\mathfrak{p}$ map.

Lemma 83. *If M is a $\mathfrak{p}$-neighbour of the primitive lattice L, then X_M is a maximal, isotropic subspace of $\bar{L}$. Conversely, if X is a maximal isotropic subspace of $\bar{L}$ then there is a unique $\mathfrak{p}$-neighbour M of L such that $X = X_M$.*

Proof. That X_M is isotropic and has dimension n follows from the Elementary Divisors Theorem. Having dimension n, it is maximal. Conversely, let $X = \langle x_1, \ldots, x_n \rangle$ be a maximal isotropic subspace of $\bar{L}$ and let M be its preimage in L. Explicitly, if $\xi_1, \ldots, \xi_n$ are lifts to L of $x_1, \ldots, x_n$, then

$$M = \mathfrak{o}_F \xi_1 + \cdots \mathfrak{o}_F \xi_n + \mathfrak{p}L. \qquad \square \quad (3.5.1)$$

Thus, we have established a canonical, explicit bijection

$$\mathcal{N}_{\mathfrak{p}}(L) \xrightarrow{\sim} \{\text{Maximal isotropic } X \subset \bar{L}\}.$$

We can also describe these sets as coset spaces. By Corollary 77, $G(V,g)$ acts transitively on $\mathcal{N}_{\mathfrak{p}}(L)$. Thus, if M is any $\mathfrak{p}$-neighbour of L then $k \mapsto Mk$ induces a bijection

$$G(V,g)/P_{L,M} \xrightarrow{\sim} \mathcal{N}_{\mathfrak{p}}(L) \quad \text{where} \quad P_{L,M} := \mathrm{stab}_K(M).$$

Note also that

$$P_{L,M} = K_L \cap \mathrm{stab}_{G^0(V,g)}(M) = K_L \cap K_M.$$

In other words, $P_{L,M}$ is the stabilizer in $G^0(V,g)$ of the pair (L,M).

By the Elementary Divisors Theorem, there is a basis (e,f) of V adapted to L such that

$$M = \mathfrak{o}_F e_1 + \cdots \mathfrak{o}_F e_n + \mathfrak{p} f_1 + \cdots \mathfrak{p} f_n = \mathfrak{o}_F e_1 + \cdots \mathfrak{o}_F e_n + \mathfrak{o}_F \pi f_1 + \cdots \mathfrak{o}_F \pi f_n$$

where π is a generator of $\mathfrak{p}$ – recall that Assumption 75 is in force. (Since we assume $N(L) = \mathfrak{o}_F$, (e,f) is actually an $\mathfrak{o}_F$-basis of L.) Let $\delta \in \Delta$ be such that the matrix of δ in the basis (e,f) is

$$\begin{pmatrix} I_n & \\ & \pi I_n \end{pmatrix}.$$

Then $M = L\delta$ and $K_M = \delta^{-1} K_L \delta$. Thus, the mapping $k \mapsto M\delta k$ gives a bijection

$$K^\delta \backslash K \xrightarrow{\sim} \mathcal{N}_{\mathfrak{p}}(L) \quad \text{where} \quad K = K_L \quad \text{and} \quad K^\delta := \delta^{-1} K \delta \cap K.$$

Of course, we are not only interested in computing neighbours of primitive lattices, so suppose now that $L \in \mathcal{L}(V,g)$ is arbitrary. Observe that if $a \in F^\times$ then $N(aL) = a^2 N(L)$. Therefore, there is a unique integer k so that

$$\mathrm{ord}_{\mathfrak{p}} N(\pi^k L) \in \{0,1\}.$$

(It is easy to see that $\mathrm{ord}_{\mathfrak{p}} N(\pi^k L) = 0$ if and only if $\mathrm{ord}_{\mathfrak{p}} N(L)$ is even.) If $\mathrm{ord}_{\mathfrak{p}} N(\pi^k L) = 0$, then $\pi^k L$ is primitive and $\mathcal{N}_{\mathfrak{p}}(\pi^k L)$ can be described as above. But obviously,

$$\mathcal{N}_{\mathfrak{p}}(L) = \{\pi^{-k} M : M \in \mathcal{N}_{\mathfrak{p}}(\pi^k L)\}.$$

Thus, we can explicitly describe the $\mathfrak{p}$-neighbours of L for any $L \in \mathcal{L}(V,g)$ with $\mathrm{ord}_{\mathfrak{p}}N(L)$ even.

By the above reasoning, to describe the $\mathfrak{p}$-neighbours of L with $\mathrm{ord}_{\mathfrak{p}}N(L)$ odd, it suffices to consider the case when $\mathrm{ord}_{\mathfrak{p}}N(L) = 1$, i.e., $N(L) = \mathfrak{p}$. Then there is a symplectic basis (e, f) of V such that

$$L = \mathfrak{o}_F e_1 + \cdots + \mathfrak{o}_F e_n + \mathfrak{p} f_1 + \cdots + \mathfrak{p} f_n.$$

Let

$$M = \mathfrak{o}_F e_1 + \cdots + \mathfrak{o}_F e_n + \mathfrak{o}_F f_1 + \cdots + \mathfrak{o}_F f_n.$$

Then, by construction, M is primitive and L is a $\mathfrak{p}$-neighbour of M. Let $\sigma \in \mathrm{GL}(V)$ be the unique transformation such that

$$e_i\sigma = \pi f_i \quad \text{and} \quad f_i\sigma = -e_i, \quad (1 \leq i \leq n). \tag{3.5.2}$$

Then $M\sigma = L$. Therefore, $M \mapsto M\sigma = L$ gives a bijection

$$\mathcal{N}_{\mathfrak{p}}(M) \xrightarrow{\sim} \mathcal{N}_{\mathfrak{p}}(L).$$

Thus, we have described the $\mathfrak{p}$-neighbours of L in terms of the $\mathfrak{p}$-neighbours of a primitve superlattice M that, in turn, can be described explicitly as above.

Example 84 (Neighbours of the standard lattice when $n = 1$)**.** *Recall that $\mathfrak{p}$ is a split prime. Let $n = 1$ and let (V, g) be the standard symplectic space of dimension $2n = 2$, so that $V = F^2$ and*

$$g((a,b),(c,d)) = ad - bc.$$

Let $L = \mathfrak{o}_F^2$. Then

$$K = K_L = \mathrm{GSp}_2(\mathfrak{o}_F) = \mathrm{GL}_2(\mathfrak{o}_F).$$

In this case,

$$\delta = \begin{pmatrix} 1 & 0 \\ 0 & \pi \end{pmatrix}.$$

and $M_0 = L\delta$ is a $\mathfrak{p}$-neighbour of L. Moreover, we have

$$K_{M_0} = \delta^{-1} K_L \delta = \mathrm{GL}_2(F) \cap \begin{pmatrix} \mathfrak{o}_F & \mathfrak{p} \\ \mathfrak{p}^{-1} & \mathfrak{o}_F \end{pmatrix}$$

and

$$K^\delta = K_L \cap K_{M_0} = \left\{ \left(\begin{smallmatrix} d & b \\ c & a \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathfrak{o}_F) : b \in \mathfrak{p} \right\}.$$

Letting $R \subset \mathfrak{o}_F$ be a systems of representatives for the residue class field $\mathfrak{o}_F/\mathfrak{p}$ with $0 \in R$, we get

$$K^\delta \backslash K = K^\delta k_\infty \cup \bigcup_{a \in R} K^\delta k_a,$$

where

$$k_\infty = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \textit{and} \quad k_a = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \quad a \in R.$$

Recall that $\mathfrak{p}$ is a split prime in E. Therefore, the $\mathfrak{p}$-neighbours of L are the $p+1$ lattices

$$M_a := L\delta k_a, \quad a \in \{\infty\} \cup R \tag{3.5.3}$$

Since every primitive lattice has a symplectic basis and is therefore isomorphic to the standard lattice, this example is fairly general.

Example 85 (Neighbours of the standard lattice when $n = 2$)**.**

$$K = \bigcup K^\delta \begin{pmatrix} 1 & 0 & * & \alpha \\ 0 & 1 & \alpha & * \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cup \bigcup_{\beta \neq 0} K^\delta \begin{pmatrix} 1 & \beta & 0 & * \\ 0 & 0 & \beta & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & * & 0 \end{pmatrix} \cup \bigcup K^\delta \begin{pmatrix} 1 & 0 & * & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}$$
$$\cup \bigcup K^\delta \begin{pmatrix} 0 & 1 & 0 & * \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \end{pmatrix} \cup K^\delta \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

We arrive at this list of $(p^2+1)(p+1)$ neighbours via the computation from Example 25. Here K^δ is given by

$$K^\delta = \{M \in \mathrm{GL}_4(\mathfrak{o}_F) : \text{for } M = \left(\begin{smallmatrix} D & B \\ C & A \end{smallmatrix}\right),\ B \in \mathrm{M}_2(\mathfrak{p})\}.$$

Completing the planes to span V with symplectic bases gives the desired result.

The results of this section are integral to the construction of our algorithm. With the explicit description of $\mathfrak{p}-$neighbours, we are equipped to construct the class set of a Hermitian lattice.

3.6 The split case $E = \mathrm{M}_2(F)$

In this section we connect the notion of fractional coefficient ideals of lattices in Hermitian space to the associated fractional coefficient ideals of lattices in symplectic space. The main results of this section are Proposition 88 and Corollary 89.

Let $E = \mathrm{M}_2(F)$ and let (V, h) be a nondegenerate, Hermitian E-space of dimension n. In particular, V is a free left E-module. Let $\mathfrak{o}_E = \mathrm{M}_2(\mathfrak{o}_F)$ and let $L \subset V$ be an $\mathfrak{o}_E$-lattice. The prototypical example to keep in mind is the following:

Example 86. *Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be fractional ideals of $\mathfrak{o}_F$ and let*

$$\mathfrak{A}_i = \begin{pmatrix} \mathfrak{a}_i & \mathfrak{o}_F \\ \mathfrak{a}_i & \mathfrak{o}_F \end{pmatrix}.$$

Then $\mathfrak{A}_i$ is a left $\mathfrak{o}_E$-ideal. Let $(v_1, \ldots, v_n)$ be an orthonormal E-basis of V. Then

$$L = \mathfrak{A}_1 v_1 + \cdots + \mathfrak{A}_n v_n \tag{3.6.1}$$

is an $\mathfrak{o}_E$-lattice in V. It is easy to check that $\mathfrak{A}_i \bar{\mathfrak{A}}_i = \mathrm{M}_2(\mathfrak{a}_i)$:

$$\mathfrak{A}_i \bar{\mathfrak{A}}_i = \begin{pmatrix} \mathfrak{a}_i & \mathfrak{o}_F \\ \mathfrak{a}_i & \mathfrak{o}_F \end{pmatrix} \begin{pmatrix} \mathfrak{o}_F & -\mathfrak{o}_F \\ -\mathfrak{a}_i & \mathfrak{a}_i \end{pmatrix} = \begin{pmatrix} \mathfrak{a}_i & \mathfrak{a}_i \\ \mathfrak{a}_i & \mathfrak{a}_i \end{pmatrix} = \mathrm{M}_2(\mathfrak{a}_i).$$

This implies that

$$h(\mathfrak{A}_i v_i, \mathfrak{A}_j v_j) = \begin{cases} \mathrm{M}_2(\mathfrak{a}_i) & \text{if } i = j, \\ \{0\} & \text{if } i \neq j. \end{cases}$$

Therefore,

$$N(L) = \mathrm{M}_2(\mathfrak{a}_1) + \cdots \mathrm{M}_2(\mathfrak{a}_n) = \mathrm{M}_2(\mathfrak{a}_1 + \cdots + \mathfrak{a}_n).$$

(Recall that $N(L)$ is the two-sided $\mathfrak{o}_E$-ideal generated by $h(L, L)$.) In particular, it happens to be that $\mathfrak{a}_1 \supset \cdots \supset \mathfrak{a}_n$ and then $N(L) = \mathrm{M}_2(\mathfrak{a}_1)$.

Lemma 87. *Let $\mathfrak{A} \subset E = \mathrm{M}_2(F)$ be a two-sided $\mathfrak{o}_E = \mathrm{M}_2(\mathfrak{o}_F)$-ideal. Then there is a fractional $\mathfrak{o}_F$-ideal $\mathfrak{a} \subset F$ such that $\mathfrak{A} = \mathrm{M}_2(\mathfrak{a})$. In other words, the mapping*

$$\mathfrak{a} \mapsto \mathrm{M}_2(\mathfrak{a})$$

is a bijection

$$\{\textit{two-sided } \mathfrak{o}_E\textit{-ideals of } E\} \xrightarrow{\sim} \{\textit{fractional } \mathfrak{o}_F\textit{-ideals of } F\}.$$

Proof. Along the lines of Example 86, we can take a fractional $\mathfrak{o}_F-$ideal $\mathfrak{a}$ in F and

$$\mathfrak{A}' = \begin{pmatrix} \mathfrak{a} & \mathfrak{o}_F \\ \mathfrak{a} & \mathfrak{o}_F \end{pmatrix}.$$

Then $\mathfrak{A}'\bar{\mathfrak{A}}' = \mathrm{M}_2(\mathfrak{a})$. Therefore we can take $\mathfrak{A} = \mathfrak{A}'\bar{\mathfrak{A}}'$ and the desired bijection follows. □

Thus, we are justified in identifying these two sets without further comment.

Let $e_{ij} \in E$ be the matrices defined in (2.4.1). Define

$$L_1 := e_{11}L \subset V_1.$$

Then L_1 is an $\mathfrak{o}_F$-lattice in V_1.

Proposition 88. *The mapping $L \mapsto L_1$ is an inclusion-preserving bijection*

$$\mathcal{L}(V, h) \xrightarrow{\sim} \mathcal{L}(V_1, h_{12}).$$

Moreover, we have $N(L_1) = N(L)$ and L_1 is maximal if and only if L is.

Proof. Let $L_2 = e_{22}L$. Then since $e_{11} + e_{22} = 1$, we have $L = L_1 + L_2$. Let $\tau = e_{12} + e_{21}$. Since $e_{22} = \tau e_{12}$, $e_{11} = e_{12}\tau$ and $\tau L = L$, we have

$$L_2 = e_{22}L = \tau e_{12}L = \tau e_{11}\tau L = \tau e_{11}L = \tau L_1.$$

In other words, we can recover L from L_1:

$$L = L_1 + \tau L_1.$$

The claimed bijection follows.

We now argue the equality of norms – i.e. that $N(L) = N(L_1)$ in the construction above. By Lemma 87 there is a fractional $\mathfrak{o}_F$-ideal $\mathfrak{a}$ such that $N(L) = \mathrm{M}_2(\mathfrak{a})$. Let $\mathfrak{b} = N(L_1)$, meaning that

$$h(L_1, L_1) = \mathfrak{b}e_{12}.$$

Now $N(L) = \mathrm{M}_2(\mathfrak{a})$ is the two-sided $\mathfrak{o}_E$-ideal generated by $h(L, L)$ and, thus, contains the two-sided ideal generated by $h(L_1, L_1) = \mathfrak{b}e_{12}$. One checks easily that the two-sided $\mathfrak{o}_E$-ideal generated by $\mathfrak{b}e_{12}$ is $\mathrm{M}_2(\mathfrak{b})$. Therefore, $\mathrm{M}_2(\mathfrak{b}) \subset \mathrm{M}_2(\mathfrak{a})$. On the other hand,

$$\begin{aligned} h(L, L) &= h(L_1 + \tau L_1, L_1 + \tau L_1) \\ &\subset h(L_1, L_1) + h(L_1, \tau L_1) + h(\tau L_1, L_1) + h(\tau L_1, \tau L_1) \\ &= h(L_1, L_1) + h(L_1, L_1)\tau + \tau h(L_1, L_1) + \tau h(L_1, L_1)\tau \\ &= \mathfrak{b}e_{12} + \mathfrak{b}e_{11} + \mathfrak{b}e_{22} + \mathfrak{b}e_{21} \\ &= \mathrm{M}_2(\mathfrak{b}). \end{aligned}$$

Therefore, $\mathrm{M}_2(\mathfrak{a}) \subset \mathrm{M}_2(\mathfrak{b})$. □

3.6.1 Translation of results of §3.4

Let L be as in (3.6.1). Observe that

$$e_{11}\mathfrak{A}_i = e_{11}\begin{pmatrix} \mathfrak{a}_i & \mathfrak{o}_F \\ \mathfrak{a}_i & \mathfrak{o}_F \end{pmatrix} = \mathfrak{a}_i e_{11} + \mathfrak{o}_F e_{12}.$$

Therefore,

$$\begin{aligned} L_1 &= e_{11}L \\ &= e_{11}\mathfrak{A}_1 v_1 + \cdots e_{11}\mathfrak{A}_n v_n \\ &= \mathfrak{a}_1 e_{11} v_1 + \mathfrak{o}_F e_{12} v_1 + \cdots + \mathfrak{a}_n e_{11} v_n + \mathfrak{o}_F e_{12} v_n \\ &= \mathfrak{o}_F e_1 + \cdots + \mathfrak{o}_F e_n + \mathfrak{a}_1 f_1 + \cdots \mathfrak{a}_n f_n, \end{aligned}$$

where

$$e_i = e_{12}v_i \quad \text{and} \quad f_i = e_{11}v_i$$

as in (2.4.6).

Corollary 89.

1. *Let L be an $\mathfrak{o}_E$-lattice in V. Then there is an orthonormal basis $(v_1, \ldots, v_n)$ of V and there are fractional $\mathfrak{o}_F$-ideals $\mathfrak{a}_1 \supset \cdots \supset \mathfrak{a}_n$ such that*

$$L = \mathfrak{A}_1 v_n + \cdots + \mathfrak{A}_n v_n, \quad \text{where} \quad \mathfrak{A}_i = \begin{pmatrix} \mathfrak{a}_i & \mathfrak{o}_F \\ \mathfrak{a}_i & \mathfrak{o}_F \end{pmatrix}.$$

   The ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ depend only on L.

2. *Let L and M be maximal $\mathfrak{o}_E$-lattices in V. Let $\eta \in F^\times$ be such that $N(L) = \mathrm{M}_2(\eta\mathfrak{o}_F)$. Then there is an orthonormal basis $(v_1, \ldots, v_n)$ of V and elements $a_1, \ldots, a_n, b_1, \ldots, b_n$ of $F^\times$ with*

$$\mathfrak{o}_F a_1 \supset \cdots \supset \mathfrak{o}_F a_n \supset \mathfrak{o}_F b_n \supset \cdots \supset \mathfrak{o}_F b_1 \quad \text{and} \quad a_1 b_1 = \cdots = a_n b_n$$

   such that

$$L = \mathfrak{o}_E \eta v_1 + \cdots + \mathfrak{o}_E \eta v_n$$

   and

$$M = \mathfrak{o}_E \begin{pmatrix} b_1 & 0 \\ 0 & a_1 \end{pmatrix} \eta v_1 + \cdots + \mathfrak{o}_E \begin{pmatrix} b_n & 0 \\ 0 & a_n \end{pmatrix} \eta v_n.$$

   The ideals $\mathfrak{o}_F a_1, \ldots, \mathfrak{o}_F a_n, \mathfrak{o}_F b_1, \ldots, \mathfrak{o}_F b_n$ depend only on L and M.

Proof.

1. By the Morita equivalence, in particular Proposition 88, the $\mathfrak{o}_E-$lattice L in V is isomorphic to the $\mathfrak{o}_F$-lattice L_1 in V_1. The lattice L_1 takes the form

$$L_1 = \mathfrak{o}_F e_1 + \cdots \mathfrak{o}_F e_n + \mathfrak{a}_1 f_1 + \cdots + \mathfrak{a}_n f_n$$

   by the invariant factors theorem, Proposition 67. In order to preserve the coefficient ideal structure, then we have that L takes the form $L = \mathfrak{A}_1 v_n + \cdots + \mathfrak{A}_n v_n$ with $\mathfrak{A}_i = \begin{pmatrix} \mathfrak{a}_i & \mathfrak{o}_F \\ \mathfrak{a}_i & \mathfrak{o}_F \end{pmatrix}$.

2. By the invariant factors theorem (Proposition 67), there is a lattice L_1 of the form

$$L_1 = \mathfrak{o}_F\eta e_1 + \cdots + \mathfrak{o}_F\eta e_n + \mathfrak{o}_F\eta f_1 + \cdots + \mathfrak{o}_F\eta f_n.$$

Again, by the Morita equivalence (Proposition 88) there is a lattice L isomorphic to L_1. Here L corresponds to $L = \mathrm{M}_2(\eta\mathfrak{o}_F)v_1 + \cdots + \mathrm{M}_2(\eta\mathfrak{o}_F)v_n = \mathfrak{o}_E\eta v_1 + \cdots + \mathfrak{o}_E\eta v_n$. By the elementary divisors theorem (Proposition 73), there exists a lattice M_1 with the appropriate ideal containment conditions of the form

$$M_1 = \mathfrak{o}_F a_1\eta e_1 + \cdots + \mathfrak{o}_F a_n\eta e_n + \mathfrak{o}_F b_1\eta f_1 + \cdots + \mathfrak{o}_F b_n\eta f_n.$$

Then $e_{11}L = L_1$ and $e_{11}M = M_1$. Explicitly,

$$\begin{aligned} L &= \begin{pmatrix} \mathfrak{o}_F & \mathfrak{o}_F \\ \mathfrak{o}_F & \mathfrak{o}_F \end{pmatrix} \eta v_1 + \cdots + \begin{pmatrix} \mathfrak{o}_F & \mathfrak{o}_F \\ \mathfrak{o}_F & \mathfrak{o}_F \end{pmatrix} \eta v_n \\ &= \mathfrak{o}_E\eta v_1 + \cdots + \mathfrak{o}_E\eta v_n \\ M &= \begin{pmatrix} \mathfrak{o}_F b_1 & \mathfrak{o}_F a_1 \\ \mathfrak{o}_F b_1 & \mathfrak{o}_F a_1 \end{pmatrix} \eta v_1 + \cdots + \begin{pmatrix} \mathfrak{o}_F b_n & \mathfrak{o}_F a_n \\ \mathfrak{o}_F b_n & \mathfrak{o}_F a_n \end{pmatrix} \eta v_n \\ &= \mathfrak{o}_E \begin{pmatrix} b_1 & 0 \\ 0 & a_1 \end{pmatrix} \eta v_1 + \cdots + \mathfrak{o}_E \begin{pmatrix} b_n & 0 \\ 0 & a_n \end{pmatrix} \eta v_n. \end{aligned}$$

□

Corollary 90. *Let L and M be maximal $\mathfrak{o}_E$-lattices in V. Then there is a transformation $\varphi \in G(V,h)$ such that $M = L\varphi$. There is a transformation $\varphi \in G^0(V,h)$ such that $M = L\varphi$ if and only if $N(L) = N(M)$.*

Definition 91. *We say that M is a $\mathfrak{p}$-neighbour of L if $M_1 = e_{11}M$ is a $\mathfrak{p}$-neighbour of $L_1 = e_{11}L$ in the sense of Definition 79.*

Lemma 92. *If M is a $\mathfrak{p}$-neighbour of L then M is $G(V_\mathfrak{p}, h_\mathfrak{p})$-equivalent to L.*

Proof. Lemma 92 follows immediately from Corollary 77. □

3.6.2 The case $n = 1$

Let F be a local field with ring of integers $\mathfrak{o}_F$ and maximal ideal $\mathfrak{p} = \mathfrak{o}_F\pi$.

$$V = E = \mathrm{M}_2(F), \quad L = O = \mathrm{M}_2(\mathfrak{o}_F).$$

If I is an O-ideal in V, then $N(I) = I\bar{I}$, obviously a two-sided O-ideal. We want to write down the $\mathfrak{p}$-neighbours of L, i.e., the left O-ideals $I \subset L$ of norm $\mathrm{M}_2(\mathfrak{p})$. By the theory developed above, these are in bijection with the $\mathfrak{p}$-neighbours of $L_1 := e_{11}L = \mathfrak{o}_F^2$. As in (3.5.3) the $\mathfrak{p}$-neighbours of L_1 are the $p+1$ lattices

$$M_1^a := L_1\delta k_a, \quad a \in \{\infty\} \cup R.$$

Let

$$j_a \in G(V,h) = E^\times = \mathrm{GL}_2(F)$$

be the unique transformation mapping to $\delta k_a \in G(V_1, h_{12})$ under the isomorphism

$$G(V,h) \xrightarrow{\sim} G(V_1, h_{12}).$$

Then the $\mathfrak{p}$-neighbours of L are given by

$$M^a := Lj_a, \quad a \in \{\infty\} \cup \mathbb{F}_\mathfrak{p},$$

where

$$j_\infty = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad j_a = \begin{pmatrix} p & 0 \\ a & 1 \end{pmatrix}, \quad a \in R$$

and again $R = \mathfrak{o}_F/\mathfrak{p}$.

3.7 Constructing elements of $\mathrm{gen}_G(L)$: Kneser's neighbour method

This section contains a description of the algorithm we have used to compute $\mathfrak{p}-$neighbours of a Hermitian lattice. The setting begins in Hermitian space, then moves to symplectic space where the heart of the computations take place and the results are sent back to Hermitian space.

In this section, we let F be a number field and let $\mathfrak{o}_F$ be its ring of integers. Let E be a quaternion, division F-algebra, let (V,h) be a nondegenerate, Hermitian E-space and set

$$G = G(V,h) \quad \text{and} \quad G^0 = G^0(V,h).$$

Let $\mathfrak{o}_E$ be a maximal order in E and let L be a maximal $\mathfrak{o}_E$-lattice in V. Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{o}_F$ such that E is split at $\mathfrak{p}$. Then $E_\mathfrak{p} \approx \mathrm{M}_2(\mathfrak{o}_{E,\mathfrak{p}})$.

Definition 93. *We say that a lattice $M \in \mathcal{L}(V,h)$ is a* $\mathfrak{p}$-neighbour of L *if*

1. $M_\mathfrak{q} = L_\mathfrak{q}$ *for all* $\mathfrak{q} \neq \mathfrak{p}$ *(equality inside $V_\mathfrak{p}$).*
2. $M_\mathfrak{p}$ *is a* $\mathfrak{p}$*-neighbour of* $L_\mathfrak{p}$ *in the sense of Definition 79.*

We write $\mathcal{N}_\mathfrak{p}(L)$ for the set of $\mathfrak{p}$*-neighbours of L.*

Remark 94. *To ensure that condition 1 is satisfied, we first suppose that condition 2 is satisfied. Then $M \subset L$. Let $n \in \mathbb{Z}$ be such that $\mathfrak{p}^n L \subset M$ and take $N = M + \mathfrak{p}^n L$. Then $N_\mathfrak{q} = M_\mathfrak{q} + L_\mathfrak{q}$ and $N_\mathfrak{p} = M_\mathfrak{p} + \mathfrak{p}^n L_\mathfrak{p} = M_\mathfrak{p}$. Replacing M by N gives the necessary condition.*

Suppose M is a $\mathfrak{p}$-neighbour of L. By Lemma 92, $M_\mathfrak{p}$ is $G(V_\mathfrak{p}, h_\mathfrak{p})$-equivalent to $L_\mathfrak{p}$. For $\mathfrak{q} \neq \mathfrak{p}$ we have $M_\mathfrak{q} = L_\mathfrak{q}$, so they are certainly $G(V_\mathfrak{q}, h_\mathfrak{q})$-equivalent. Therefore, $M \in \mathrm{gen}_G(L)$ and

$$\mathcal{N}_\mathfrak{p}(L) \subset \mathrm{gen}_G(L).$$

Here we state the version of the approximation theorem [8, Theorem 5.8] that we require for our computations.

Proposition 95 (Approximation theorem)**.** *Let L be an $\mathfrak{o}_F$-lattice in V. Let S be a finite set of prime ideals of $\mathfrak{o}_F$ and let $M^\mathfrak{p}$ be an $\mathfrak{o}_{F,\mathfrak{p}}$-lattice in $V_\mathfrak{p}$ for all $\mathfrak{p} \in S$. Then there is a unique lattice M in V such that $M_\mathfrak{p} = L_\mathfrak{p}$ for all $\mathfrak{p} \notin S$ and $M_\mathfrak{p} = M^\mathfrak{p}$ for all $\mathfrak{p} \in S$.*

Proof. See Greenberg-Voight [8]. □

Corollary 96. *The mapping $M \mapsto M_{\mathfrak{p}}$ is a bijection*

$$\mathcal{N}_{\mathfrak{p}}(M) \xrightarrow{\sim} \mathcal{N}_{\mathfrak{p}}(M_{\mathfrak{p}}).$$

Our strategy for computing G-equivalence class representatives for the class set $\mathrm{cl}_G(L) = \mathrm{gen}_G(L)/G$ is to compute lots of $\mathfrak{p}$-neigbors of L and to test them for equivalence. More precisely, we try to find a finite set S of prime ideals of $\mathfrak{o}_F$ such that the composite

$$\bigcup_{\mathfrak{p}\in S} \mathcal{N}_{\mathfrak{p}}(L) \hookrightarrow \mathrm{gen}_G(L) \twoheadrightarrow \mathrm{cl}_G(L)$$

is surjective. Such a set S exists due to the theory of Strong Approximation [8].

3.7.1 Computing $\mathcal{N}_{\mathfrak{p}}(L)$

Let (V, h) be the standard Hermitian E-space of rank n, so that $V = E^n$ and

$$h(x, y) = \sum_{i=1}^{n} x_i \bar{y}_i.$$

Let $\mathfrak{o}_E$ be a maximal $\mathfrak{o}_F$-order in E and let L be an $\mathfrak{o}_E$-lattice in V. In this subsection, we describe how to explicitly compute $\mathcal{N}_{\mathfrak{p}}(L)$. Assume, for simplicity,[4] that $\mathfrak{o}_F$ is a PID. Since L need not be free over $\mathfrak{o}_E$, it is more convenient to represent L explicitly by giving an $\mathfrak{o}_F$-basis $(v_1, \ldots, v_{4n})$, which exists since $\mathfrak{o}_F$ is a PID.

Input: A lattice $L \in \mathcal{L}(V, h)$, a set of lifts[5] $\{k_i\} \subset G(V, g)$ of representatives[6] for the coset space $G^0(\bar{L}, \bar{g})/P_{L,M_i}$.

Output: $\mathcal{N}_{\mathfrak{p}}(L)$.

- Fix an F-linear splitting

$$j : E \to \mathrm{M}_2(F_{\mathfrak{p}})$$

[4] To avoid having to introduce pseudobases.
[5] Lifts of elements from the symplectic space $\bar{L} = L/\mathfrak{p}L$ to L.
[6] Specifically, the similitudes are integral – $N(k_i) \in \mathfrak{o}_{F,\mathfrak{p}}$.

such that $\mathfrak{o}_E \to \mathrm{M}_2(\mathfrak{o}_{F,\mathfrak{p}})$. (The MAGMA command `pMatrixRing` takes care of this.) Then j induces a corresponding splitting

$$j^n : E^n \to \mathrm{M}_2(F_\mathfrak{p})^n.$$

Let $(u_1, \ldots, u_n)$ be the standard orthonormal basis of E^n. Then $(j(u_1), \ldots, j(u_n))$ is the standard basis of $\mathrm{M}_2(F_\mathfrak{p})^n$.

- Identify $e_{11}\mathrm{M}_2(F_\mathfrak{p})^n$ with $F_\mathfrak{p}^{2n}$ as in §3.6.1. If

$$e_i := e_{12}j(u_i) \quad \text{and} \quad f_i := e_{11}j(u_i)$$

then $\{e, f\}$ is a symplectic basis of $e_{11}\mathrm{M}_2(F_\mathfrak{p})^n$.

- Let $(v_1, \ldots, v_{4n})$ be the $\mathfrak{o}_F$-basis of L which has been given to us. Let

$$x_i = e_{12}j(v_i) \quad \text{and} \quad y_i = e_{11}j(v_i).$$

and let

$$\Lambda := \mathfrak{o}_{F,\mathfrak{p}}x_1 + \cdots + \mathfrak{o}_{F,\mathfrak{p}}x_{n4} + \mathfrak{o}_{F,\mathfrak{p}}y_1 + \cdots + \mathfrak{o}_{F,\mathfrak{p}}y_{4n}$$

be the $\mathfrak{o}_{F,\mathfrak{p}}$-span of $e_{11}j^n(L)$.

- Compute $N(\Lambda)$ and let ℓ be the unique integer such that

$$\mathrm{ord}_\pi N(\Lambda') \in \{0, 1\} \quad \text{where} \quad \Lambda' = \pi^\ell \Lambda.$$

Let $\{\varepsilon', \varphi'\}$ be a symplectic basis of $F_\mathfrak{p}^{2n}$ adapted to Λ'. Define

$$\Lambda'' = \begin{cases} \Lambda' & \text{if } \Lambda' \text{ is primitive,} \\ \Lambda'\sigma^{-1} & \text{if } \Lambda' \text{ is imprimitive and } \sigma \text{ is as in (3.5.2).} \end{cases}$$

Then Λ'' is primitive and $\{\varepsilon, \varphi\}$ is a symplectic basis[7] of Λ''.

[7] In the primitive case, $\{\varepsilon, \varphi\} = \{\varepsilon', \varphi'\}$ and the imprimitive case $\{\varepsilon, \varphi\} = \{\varepsilon'\sigma^{-1}, \varphi'\sigma^{-1}\}$.

- Let
$$\delta = \begin{pmatrix} I_n & 0 \\ 0 & \pi I_n \end{pmatrix}.$$
and, for each i, let Π_i'' be the $\mathfrak{o}_{F,\mathfrak{p}}$-sublattice of Λ'' spanned by
$$\xi_j := \varepsilon_j \delta k_i \quad \text{and} \quad \eta_j := \varphi_j \delta k_i, \quad j = 1, \ldots, n.$$
Let
$$\Pi_i' = \begin{cases} \Pi_i'' & \text{if } \Lambda' \text{ is primitive,} \\ \Pi_i''\sigma & \text{if } \Lambda' \text{ is imprimitive and } \sigma \text{ is as in (3.5.2)} \end{cases}$$
and let $\Pi_i = \pi^{-\ell}\Pi_i'$. Then Π_i is a $\mathfrak{p}$-neighbour of Λ.

- Let
$$\widetilde{\Pi}_i = \Pi_i + \tau\Pi_i \subset M_2(F_\mathfrak{p})^n$$
be the $M_2(\mathfrak{o}_{F,\mathfrak{p}})$-lattice corresponding to $\Pi_i \subset F_\mathfrak{p}^{2n}$.

- Let M_i be the $\mathfrak{o}_F$-submodule of E^n such that
$$j^n(M_{i,\mathfrak{p}}) = \widetilde{\Pi}_i \quad \text{and} \quad M_{i,\mathfrak{q}} = L_\mathfrak{q} \quad \text{for all } \mathfrak{q} \neq \mathfrak{p}.$$
Then $\mathcal{N}_\mathfrak{p}(L) = \{M_i\}$.

3.8 Computing the class set

The class set of a lattice L is computed using the set of neighbours, constructed in §3.7.1. Isometry relations, if any, are determined between the neighbours, described in §3.8.1. All representatives in the class set have been obtained when the sum of the reciprocals of the size of the automorphism groups of the class set of representatives matches the mass formula, described in §3.8.2. If the expected mass is not obtained, neighbours at other primes can be computed until all representatives for the class set are found. The table in §3.8.3 demonstrates the number of primes needed for neighbour computation to fill the class set for the lattice $\mathfrak{o}_E \times \mathfrak{o}_E$.

3.8.1 Isometry testing

For computational purposes, it is convenient to have vector spaces over $\mathbb{Q}$. To impose this condition upon a quaternionic vector space, one may view the Hermitian space over F as the space $V = E^n \sim F^{4n}$ *with* additional information attached which serves the role of maintaining the quaternionic structure.

$$\begin{array}{c} V = E^n \sim F^{4n} \\ \vdots \\ n \\ \vdots \\ E = (a,b)_F \sim F^4 \end{array}$$

Let $\{a_1 = 1, a_2 = i, a_3 = j, a_4 = ij\}$ be a basis of E over F. The extra data is stored by four quadratic forms, h_ℓ, associated to each basis element of E, taking vectors in V down to F,

$$h_\ell : V \times V \to F; \quad h_\ell(x,y) = T(h(a_\ell x, y)) \quad \text{for} \quad 1 \leq \ell \leq 4.$$

Key in this implementation is to note that

$$h(a_\ell x, y) = a_\ell x \cdot \overline{y} = a_\ell \, h(x,y),$$

a feature which effectively shifts the coefficient of a_ℓ from $h(x,y)$ to a scalar in the base field. The effect is that under the reduced trace map, the coefficient is preserved.

The auxiliary forms have the property that, despite being in F, they can be used to recover the original form $h(x,y) \in E$ as follows

$$\begin{aligned} h(x,y) &= \frac{1}{2a_1^2} T(h(a_1 x, y)) + \frac{1}{2a_2^2} T(h(a_2 x, y))i \\ &\quad + \frac{1}{2a_3^2} T(h(a_3 x, y))j + \frac{1}{2a_4^2} T(h(a_4 x, y))ij \\ &= \frac{1}{2a_1^2} h_1(a_1 x, y) + \frac{1}{2a_2^2} h_2(a_2 x, y)i + \frac{1}{2a_3^2} h_3(a_3 x, y)j + \frac{1}{2a_4^2} h_4(a_4 x, y)ij. \end{aligned}$$

From the above relation, the following equivalence can be claimed.

Lemma 97. *Assume that h_1 is nondegenerate. Let $\varphi : V \to V$ be an $F-$linear surjection. Then for all $v, w \in V$ the following are equivalent:*

1. *The map φ is $E-$linear and* $h(x\varphi, y\varphi) = h(x, y)$.

2. *For each* $i = 1, \ldots, 4$, $h_i(x\varphi, y\varphi) = h_i(x, y)$.

Proof. See Greenberg and Voight [8, Lemma 6.2]. ∎

Note that the form h_1 has particularly nice feature (for $a, b < 0$), it is symmetric positive-definite (i.e. $h_1(z, z)$ is positive for non-zero vectors z). As a matrix,

$$\frac{1}{2}h_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -a & 0 & 0 \\ 0 & 0 & -b & 0 \\ 0 & 0 & 0 & ab \end{pmatrix}$$

for dimension 1 and for dimension $n > 1$, n copies of h_1 form the diagonal $4n \times 4n$ matrix. It is also the inner product matrix for the vector space E^n. Our computations involved the setting with $F = \mathbb{Q}$. For algebras over a number field $F \neq \mathbb{Q}$ an additional layer of trace map can be utilized to have a space over $\mathbb{Q}$. Boiling lattices down to $\mathbb{Z}$ one may capitalize on lattice algorithms of Plesken and Souvignier [15] to compute the automorphism group respecting the quadratic forms h_i to test for isometry. This powerful machinery functions quite efficiently by matching up short vectors to rule out isometries early.

3.8.2 Stopping criterion – The mass formula

For each $(p^2 + 1)(p + 1)$ neighbour (see Example 25), isometry testing[8] determines which neighbours which are redundant. The list of distinct lattices form representatives for the classes in the genus of the lattice.

The mass of the genus of a lattice L comes from the class set. Let $h = h_G(L)$ and define

$$\Gamma_L := \{\varphi \in G^0(V, g) \mid L\varphi = L\}.$$

The mass of the genus is defined as

$$\sum_{[L_i] \in \mathrm{cl}_G(L)} \frac{1}{|\Gamma_{L_i}|} = \sum_{i=1}^{h} \frac{1}{|\Gamma_{L_i}|}.$$

[8] In Magma the function IsIsometric() can test quickly if two lattices are isometric and can also be set to preserve the attached forms describing the quaternionic structure. This feature is necessary to work with lattices over $\mathbb{Z}$ while maintaining the quaternionic structure described in the auxiliary forms.

The mass can be precomputed as formulas for the mass involving Bernoulli numbers have been made explicit [5]. For example – the simplest case – for unimodular even lattices of dimension $n = 2k$, divisible by 8 is given by:

$$\sum_{[L_i]\in \mathrm{cl}_G(L)} \frac{1}{|\Gamma_{L_i}|} = \prod_{1\leq j<n/2} \frac{|B_{n/2}|}{n}\frac{|B_{2j}|}{4j}.$$

When running through the neighbours of L, each new similar lattice obtained is accounted for in the sum $\sum_{[L_i]\in \mathrm{cl}_G(L)} \frac{1}{|\Gamma_{L_i}|}$ until the expected value is reached.

3.8.3 Tables

For a fixed, square free discriminant[9], less than 100, the following tables include the class number for the standard lattice $L = \mathfrak{o}_E \times \mathfrak{o}_E$ in the quaternionic vector space V of dimension 2 over the quaternion algebra E. As well, the mass decomposition is given beside the precomputed mass – each denominator in the sum counts the number of locally similar lattices which are globally similar, i.e. the number of lattices in each isomorphism class of the class set.[10] The last column gives the time[11] required to compute the class set.

Example 98. *The first nontrivial class number occurs for with the quaternion algebra with discriminant 5, i.e.* $E = (-2,-5)_{\mathbb{Q}}$. *In this case the class number* $h_G(L)$ *is 2. Let* $cl_G(L) = \{[L_1],[L_2]\}$. *Representative lattices in the class set are given by:*

[9] A square free discriminant is either strictly prime or the product of an odd number of primes. The criterion is due to the fact that a quaternion algebra is ramified at a finite set of primes, which has even cardinality. As the quaternion algebras under consideration are definite, one of the places of ramification is ∞ leaving an odd number of finite primes for possible ramification.

[10] The computations were performed on a Lenovo Thinkpad X230, with an Intel core i5 processor, with 3.1 GHz, using 8 megabytes of RAM.

[11] The time is given is seconds.

1. L_1 with Gram matrix:

$$\begin{pmatrix} 2 & 1 & 1 & -1 & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & -1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 4 & 1 & 0 & 0 & 0 & 0 \\ -1 & -1 & 1 & 4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 & 2 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 4 & 1 \\ 0 & 0 & 0 & 0 & -1 & -1 & 1 & 4 \end{pmatrix}$$

2. L_2 with Gram matrix:

$$\begin{pmatrix} 6 & -1 & 0 & 2 & -3 & 4 & -3 & -3 \\ -1 & 4 & -2 & 0 & 3 & 1 & 2 & 2 \\ 0 & -2 & 4 & 1 & -3 & 0 & -1 & 0 \\ 2 & 0 & 1 & 6 & -1 & 3 & -3 & -2 \\ -3 & 3 & -3 & -1 & 6 & -2 & 2 & 2 \\ 4 & 1 & 0 & 3 & -2 & 6 & -2 & -2 \\ -3 & 2 & -1 & -3 & 2 & -2 & 4 & 2 \\ -3 & 2 & 0 & -2 & 2 & -2 & 2 & 4 \end{pmatrix}$$

$\mathrm{disc}(E)$	$h_G(L)$	primes	mass	mass decomposition	time
2	1	-	$\frac{1}{1152}$	$\frac{1}{1152}$	0.030
3	1	-	$\frac{1}{288}$	$\frac{1}{288}$	0.020
5	2	2	$\frac{13}{720}$	$\frac{1}{72}+\frac{1}{240}$	0.180
7	2	2	$\frac{5}{96}$	$\frac{1}{32}+\frac{1}{48}$	0.150
11	5	2	$\frac{61}{288}$	$\frac{1}{12}+2\cdot\frac{1}{24}+\frac{1}{32}+\frac{1}{72}$	0.210
13	4	2	$\frac{17}{48}$	$2\cdot\frac{1}{8}+\frac{1}{12}+\frac{1}{48}$	0.200
17	8	2, 3, 5	$\frac{29}{36}$	$\frac{1}{4}+2\cdot\frac{1}{8}+3\cdot\frac{1}{12}+\frac{1}{24}+\frac{1}{72}$	6.230
19	10	2, 3, 5	$\frac{181}{160}$	$\frac{1}{4}+4\cdot\frac{1}{8}+\frac{1}{10}+3\cdot\frac{1}{12}+\frac{1}{32}$	5.550
23	17	2, 3, 5, 7	$\frac{583}{288}$	$5\cdot\frac{1}{4}+3\cdot\frac{1}{8}+3\cdot\frac{1}{12}+3\cdot\frac{1}{24}$ $+\frac{1}{32}+\frac{1}{48}+\frac{1}{72}$	9.760
29	24	2, 3, 5, 7	$\frac{2497}{720}$	$\frac{1}{2}+10\cdot\frac{1}{4}+4\cdot\frac{1}{8}+\frac{1}{10}+5\cdot\frac{1}{12}$ $+\frac{1}{24}+\frac{1}{48}+\frac{1}{72}$	8.450
$30=2\cdot3\cdot5$	13	7	$\frac{65}{36}$	$\frac{1}{2}+2\cdot\frac{1}{4}+3\cdot\frac{1}{6}+2\cdot\frac{1}{8}+2\cdot\frac{1}{12}$ $+\frac{1}{36}+2\cdot\frac{1}{72}$	7.300
31	26	2, 3, 5, 7	$\frac{481}{96}$	$2\cdot\frac{1}{2}+11\cdot\frac{1}{4}+7\cdot\frac{1}{8}+4\cdot\frac{1}{12}$ $+\frac{1}{32}+\frac{1}{48}$	8.040
37	37	2, 3, 5	$\frac{137}{16}$	$5\cdot\frac{1}{2}+19\cdot\frac{1}{4}+7\cdot\frac{1}{8}+5\cdot\frac{1}{12}+\frac{1}{48}$	8.800
41	47	2, 3, 5, 7	$\frac{841}{72}$	$10\cdot\frac{1}{2}+24\cdot\frac{1}{4}+4\cdot\frac{1}{8}+7\cdot\frac{1}{12}+\frac{1}{24}$ $+\frac{1}{72}$	17.650
$42=2\cdot3\cdot7$	20	5, 11	$\frac{125}{24}$	$7\cdot\frac{1}{2}+4\cdot\frac{1}{4}+3\cdot\frac{1}{6}+\frac{1}{8}+\frac{1}{16}$ $+2\cdot\frac{1}{32}+2\cdot\frac{1}{48}$	6.310
43	52	2, 3, 5, 7	$\frac{1295}{96}$	$11\cdot\frac{1}{2}+27\cdot\frac{1}{4}+8\cdot\frac{1}{8}+5\cdot\frac{1}{12}+\frac{1}{32}$	8.580
47	62	2, 3, 5, 7	$\frac{5083}{288}$	$17\cdot\frac{1}{2}+31\cdot\frac{1}{4}+8\cdot\frac{1}{8}+4\cdot\frac{1}{12}$ $+\frac{1}{24}+\frac{1}{32}$	11.150

disc(E)	$h_G(L)$	primes	mass	mass decomposition	time
53	87	2, 3, 5, 7, 11	$\frac{3653}{144}$	$25 \cdot \frac{1}{2} + 46 \cdot \frac{1}{4} + 7 \cdot \frac{1}{8} + 7 \cdot \frac{1}{12} + \frac{1}{24} + \frac{1}{72}$	51.120
59	108	2, 3, 5, 7	$\frac{50489}{1440}$	$43 \cdot \frac{1}{2} + 51 \cdot \frac{1}{4} + 7 \cdot \frac{1}{8} + \frac{1}{10} + 2 \cdot \frac{1}{12}$ $+2 \cdot \frac{1}{24} + \frac{1}{32} + \frac{1}{72}$	15.870
61	124	2, 3, 5, 7	$\frac{1861}{48}$	$41 \cdot \frac{1}{2} + 66 \cdot \frac{1}{4} + 12 \cdot \frac{1}{8} + 5 \cdot \frac{1}{12}$	17.470
$66 = 2 \cdot 3 \cdot 11$	63	5, 7	$\frac{1525}{72}$	$33 \cdot \frac{1}{2} + 15 \cdot \frac{1}{4} + 4 \cdot \frac{1}{6} + \frac{1}{8} + \frac{1}{12} + \frac{1}{16}$ $+4 \cdot \frac{1}{24} + \frac{1}{32} + \frac{1}{48} + 2 \cdot \frac{1}{72}$	11.600
67	161	2, 3, 5, 7, 11	$\frac{4939}{96}$	$59 \cdot \frac{1}{2} + 78 \cdot \frac{1}{4} + 14 \cdot \frac{1}{8} + 9 \cdot \frac{1}{12} + \frac{1}{32}$	44.680
$70 = 2 \cdot 5 \cdot 7$	71	3, 11	$\frac{325}{12}$	$43 \cdot \frac{1}{2} + 21 \cdot \frac{1}{4} + 4 \cdot \frac{1}{8} + 3 \cdot \frac{1}{12}$	6.160
71	177	2, 3, 5, 7, 11	$\frac{17647}{288}$	$85 \cdot \frac{1}{2} + 64 \cdot \frac{1}{4} + 17 \cdot \frac{1}{8} + 7 \cdot \frac{1}{12} + 2 \cdot \frac{1}{24}$ $+\frac{1}{32} + \frac{1}{72}$	43.890
73	191	2, 3, 5, 7	$\frac{533}{8}$	$87 \cdot \frac{1}{2} + 86 \cdot \frac{1}{4} + 13 \cdot \frac{1}{8} + 5 \cdot \frac{1}{12}$	22.270
$78 = 2 \cdot 3 \cdot 13$	89	5, 7	$\frac{425}{12}$	$57 \cdot \frac{1}{2} + 22 \cdot \frac{1}{4} + 6 \cdot \frac{1}{6} + 4 \cdot \frac{1}{8}$	10.510
79	245	2, 3, 5, 7, 11	$\frac{40573}{480}$	$113 \cdot \frac{1}{2} + 100 \cdot \frac{1}{4} + 20 \cdot \frac{1}{8} + \frac{1}{10} + 9 \cdot \frac{1}{12}$ $+\frac{1}{32} + \frac{1}{48}$	54.440
83	271	2, 3, 5, 7, 11	$\frac{28249}{288}$	$137 \cdot \frac{1}{2} + 110 \cdot \frac{1}{4} + 13 \cdot \frac{1}{8} + 9 \cdot \frac{1}{12} + \frac{1}{24}$ $+\frac{1}{32}$	69.730
89	327	2, 3, 5, 7, 11	$\frac{43571}{360}$	$179 \cdot \frac{1}{2} + 113 \cdot \frac{1}{4} + 16 \cdot \frac{1}{8} + 17 \cdot \frac{1}{12} + \frac{1}{24}$ $+\frac{1}{72}$	212.020
97	416	2, 3, 5, 7, 11	$\frac{941}{6}$	$223 \cdot \frac{1}{2} + 173 \cdot \frac{1}{4} + 14 \cdot \frac{1}{8} + 6 \cdot \frac{1}{12}$	103.360

Chapter 4

Future work

4.1 Algebraic modular forms

A substantial motivator for the work done in this thesis is to apply the class sets of lattices to the construction of algebraic modular forms. Modular forms are notoriously difficult to construct. However, it is feasible to view an algebraic modular form as a counting function on the genus of a lattice.

Let F be the field of fractions of a Dedekind domain and $G = G(F)$ either the group $G(V,h)$ or $G^0(V,h)$ and W a finite dimension representation of G. An *algebraic modular form* on a group G with values in $\mathrm{GL}(W)$ is a locally constant function, f, from the finite adèlic points $G(\widehat{F})$ of G quotiented by a particular subgroup, such that $f(\gamma x) = \gamma f(x)$ for all global elements $\gamma \in G$ and $x \in \widehat{K}_L \backslash G(\widehat{F})$. That is,

$$\begin{aligned} f : \widehat{K}_L \backslash G(\widehat{F}) &\rightarrow \mathrm{GL}(W) \\ \gamma x &\mapsto \gamma f(x). \end{aligned}$$

Let $M(G,W)$ denote the space of all such functions.

Alternatively, an interpretation of the genus may be made from the bijection in §3.3

$$\widehat{K}_L \backslash G(\widehat{F})/G(F) \leftrightarrow \mathrm{gen}(L)/G(F) = cl_G(L).$$

Consider the form f now as

$$f : \mathrm{gen}(L) \rightarrow \mathrm{GL}(W),$$

coming from the bijection stated in the remarks preceding Theorem 59. The space of algebraic modular forms can be decomposed into pieces

$$M(\mathrm{G}, W) \cong \oplus_{i=1}^{h} H^0(\Gamma_i, \mathrm{GL}(W)) = \mathrm{GL}(W)^{\Gamma_1} \oplus \cdots \oplus \mathrm{GL}(W)^{\Gamma_h}$$

where $f \mapsto (f(x_1), \ldots, f(x_h))$ is given by a basis of characteristic functions $f = (f_1, \ldots, f_h)$ for the decomposed space and $\Gamma_i = \mathrm{G}(\widehat{F}) \cap \widehat{x_i}\widehat{K}_L\widehat{x_i}^{-1}$ for x_i representatives in the class set [8]. In the language of lattices, $f \mapsto (f([L_1]), \ldots, f([L_h]))$ is a description of an algebraic modular form which counts the number of neighbours in an isometry class of the genus.

The Langlands philosophy predicts connections between automorphic forms and their Galois representations. It is our desire that the algorithmic technique for computing class sets of quaternionic lattices will lead to interesting Galois representations.

4.2 Ramified primes

We have neglected the case of neighbours at ramified primes, but not with haste. This setting is worthy of investigation and can be treated using the classic Kneser method. The associated procedure should follow in line with vector spaces over number fields, modulo extra complication related to the quaternionic structure.

4.3 Alternative fields and orders

Our computations have been with quaternion algebras over the rationals. The theory is in place to insert the algebras over more general number fields. Slight alterations via the trace maps must be made to take the vector spaces down to the rationals, for ease of computation. Alternatively, another approach could involve varying the order which the lattices live over – say non-maximal – which orders could result in other interesting patterns.

Appendix A

Appendix

The file called "run.m" in §A.1 is used to run the program. Attaching the files "local.m" and "global.m" in §A.2 and §A.3 is required as well.

A.1 run.m

```
filename := "data1to100.txt";

Q := Rationals();
Attach("local.m");
Attach("global.m");
n := 2;
M := MatrixAlgebra(Q,2*n);

//Discriminants for quaternion algebras
discs := [n : n in [1..100] | IsSquarefree(n) and IsOdd(#PrimeDivisors(n))];

for d in discs do

    //The quaternion algebra, a maximal order, the Hermitian space
    //and standard lattice, respectively
    E := QuaternionAlgebra(d);
    EO := MaximalOrder(E);
    V := HermSpace(E,n);
    L0 := StandardLattice(V);
    mass := 1/(6*30*32)*&*[(q-1)*(q^2+1) : q in PrimeDivisors(d)];

    //Primes beneath a small bound: 40
    primes := [p : p in PrimesUpTo(40) | GCD(p,d) eq 1];
    prime_counter := 0;

    //Representatives of the class set and the associated mass
    reps := [L0];
    mass_so_far := 1/#aut_group(L0);

    //While the mass is less than the expected mass,
    //p-neighbours are constructed one prime at a time
```

```
    while mass_so_far lt mass do
        prime_counter := prime_counter + 1;
        p := primes[prime_counter];
        _,splitting,_ := pMatrixRing(OE,p);
        P := M!DiagonalMatrix([1/p,1,p,1]);
        S := M![0,0,1,0,0,0,0,1,-1,0,0,0,0,-1,0,0];

        //Lagrangians:
        A := [M![1,x,y+p*b,z,0,1,z,0,0,0,1,0,0,0,-x,1] : x,y,z,b in {0..p-1}];
        B := [M![0,1,y,z+p*b,0,0,-1,0,0,0,0,1,1,0,0,y] : y,z,b in {0..p-1}];
        C := [M![-p*b,0,1,z,0,0,0,1,-1,0,0,0,z,-1,0,0] : z,b in {0..p-1}];
        D := [M![0,-p*b,0,1,1,0,0,0,0,-1,0,0,0,0,1,0] : b in {0..p-1}];
        F := A cat B cat C cat D;

        //For each Lagrangian, construct the associated neighbour
        for f in F do
            L := Neighbour(L0,splitting,P*f);
            if not exists{LL : LL in reps | is_isom(L,LL)} then
                Append(~reps,L);
                mass_so_far := mass_so_far + 1/#aut_group(L);
            end if;
            if mass_so_far gt mass then break;
            end if;
        end for;
    end while;

    print "d =",d;
    print "Primes used: ",primes[1..prime_counter];
    print "Size of genus:", #reps;
    print "automorphism group sizes:", [#aut_group(L) : L in reps];
    print "mass =",mass;

    Write(filename,d);
    Write(filename,primes[1..prime_counter]);
    Write(filename,#reps);
    Write(filename,[#aut_group(L) : L in reps]);
    Write(filename,mass);
    Write(filename,"");
    Write(filename,"");
end for;
```

A.2 local.m

```
intrinsic GramMatrices(LambdaZBasis)->.
{Computes the Gram matrix of a given lattice.
The lattice Lambda must be integral.}
    n := # Eltseq(LambdaZBasis[1]);
    E := BaseRing(Parent(LambdaZBasis[1]));
    Q := BaseRing(E);
    Z := Integers(Q);
    pair := function(x,y)
    return &+[x[i]*Conjugate(y[i]) : i in [1..n]];
    end function;
    X := [&+[x[i]*Conjugate(y[i]) : i in [1..n]] : x,y in LambdaZBasis];
    XX := [[Z!Trace(pair(b*x,y)) : x,y in LambdaZBasis] : b in Basis(E)];
    M := MatrixAlgebra(Z,4*n);
    return [M!xx : xx in XX];
end intrinsic;

intrinsic ZCoords(x)->.
{Converts the vector to its Z-coordinates}
    return Vector(&cat[Eltseq(y) : y in Eltseq(x)]);
end intrinsic;

intrinsic LeftReg(x)->.
{}
    E := Parent(x);
    rows := [Eltseq(x*b) : b in Basis(E)];
    return Transpose(Matrix(rows));
end intrinsic;

intrinsic StandardOmega(n)->.
{Returns the 2nx2n matrix J=Omega=(0 I; -I 0)}
    Q := Rationals();
    I := MatrixAlgebra (Q,n)!1;
    Z := MatrixAlgebra (Q,n)!0;
    Omega := VerticalJoin([HorizontalJoin([Z,I]),HorizontalJoin([-I,Z])]);
    return Omega;
end intrinsic;

intrinsic Adjoint(x::AlgQuatElt)->.
{Returns the conjugate of an element from a quaternion algebra}
    return Conjugate(x);
end intrinsic;

intrinsic ConjTrans(G)->.
```

```
{}
    return Transpose(Parent (G)![Adjoint(x) : x in Eltseq(G)]);
end intrinsic;

intrinsic SympGS(X,Y,Omega)->.
{Applies the Gram-Schmidt algorithm to subspaces X and Y}
    n := #X;
    XX := X;
    YY := Y;

    pair := function(x,y)
        return DotProduct(x*Omega,y);
    end function;

    XX[1] := X[1]/pair(X[1],Y[1]);

    for i in [2..n] do
        // make XX[i] orthogonal to XX[j] for j < i.
        // make YY[i] orthogonal to YY[j] for j > i.
        v := X[i];
        w := Y[i];

        for j in [1..i-1] do
            x := XX[j];
            y := YY[j];
            XX[i] := XX[i] - pair (x,v)/pair(x,y)*y - pair (y,v)/pair(y,x)*x;
            YY[i] := YY[i] - pair (x,w)/pair(x,y)*y - pair (y,w)/pair(y,x)*x;
        end for;

        XX[i] := XX[i]/pair(XX[i],YY[i]);
    end for;

    return XX,YY;
end intrinsic;

intrinsic RandSympMat(Omega,N)->.
{A random matrix X of rational numbers in [0,1] with denominators bounded by N
such that X*Omega*X^t = Omega.}
    M := Parent(Omega);
    n := Nrows(Omega) div 2;
    A := M![Random(Rationals(),N) : i in [1..(2*n)^2]];
    if Determinant(A) eq 0 then print "You have chosen poorly."; end if;
    X := A[1..n];
    Y := A[n+1..2*n];
    XX,YY := SympGS(X,Y,Omega);
```

```
    B := Matrix(XX cat YY);
    return B;
end intrinsic;

intrinsic RandSymppIntMat(Omega,p,e)->.
{}
    M := Parent(Omega);
    n := Nrows(Omega) div 2;
        while true do
    A := M![Random([x : x in [-p^e+1..p^e-1] | x mod p ne 0]) : i in [1..(2*n)^2]];
    X := A[1..n];
    Y := A[n+1..2*n];
    XX,YY := SympGS(X,Y,Omega);
    B := Matrix(XX cat YY);
    if Valuation(Determinant(B),p) eq 0 then break; end if;
    end while;
    return B;
end intrinsic;

intrinsic UtoSp(g)->.
{Given an nxn unitary matrix g over M_2(F), UtoSp computes the symplectic matrix
G over a field F associated to g via the isomorphism e11*M_2(F) --> F^2n.
This intrinsic assumes that g*Omega*g^t=Omega where Omega is the standard 2nx2n
symplectic matrix [0 I; -I 0].}
    Q := BaseRing(BaseRing(Parent(g)));
    n := Nrows(g);
    V := RSpace(Q,2*n);
    I := MatrixAlgebra (Q,n)!1;
    Z := MatrixAlgebra (Q,n)!0;
    Omega := VerticalJoin([HorizontalJoin([Z,I]),HorizontalJoin([-I,Z])]);
    E := BaseRing(g);
    V := RModule(E,n);
    e11 := E![1,0,0,0];
    e12 := E![0,1,0,0];
    w := E![0,1,1,0];
    B := Basis(V);

    pairX := function(x,y)
        yy := Parent (y)!Vector([Adjoint(z) : z in Eltseq(y)]);
        return &+[x[i]*yy[i] : i in [1..n]];
    end function;

    pairY := function(x,y)
        return DotProduct(x*Omega,y);
    end function;
```

```
    function Ycoords(x);
        ans := V!([x[i][1,2] : i in [1..n]] cat [x[i][1,1] : i in [1..n]]);
        return ans;
    end function;

    YtoX := function(y)
        return &+[y[i]*e12*B[i] + y[n+i]*e11*B[i] : i in [1..n]];
    end function;

    XtoY := function(x)
        return [x[i][1,2] : i in [1..n]] cat [x[i][1,1] : i in [1..n]];
    end function;

    rows := [];

    for i in [1..2*n] do
        r := XtoY(YtoX(V.i)*g);
        Append(~rows,r);
    end for;

    ans := Matrix(rows);
    print "Check symplectic:", ans*Omega*Transpose(ans) eq Omega;
    G := Matrix(rows);
    return G;
end intrinsic;

intrinsic SptoU(g)->.
{Given a symplectic matrix g over a field F, SptoU computes the unitary matrix
G over M_2(F) associated to g via the isomorphism e11*M_2(F) --> F^2n.
This intrinsic assumes that g*Omega*g^t=Omega where Omega is the standard
2nx2n symplectic matrix [0 I; -I 0].}
    V := Parent(g[1]);
    Q := BaseRing(V);
    n := Dimension(V) div 2;
    I := MatrixAlgebra (Q,n)!1;
    Z := MatrixAlgebra (Q,n)!0;
    Omega := Parent (g)!VerticalJoin([HorizontalJoin([Z,I]),HorizontalJoin([-I,Z])]);
    gOgt := g*Omega*Transpose(g);
    Nm := gOgt[1,n+1];
    require gOgt eq Nm*Omega : "g is not a symplectic similitude.";

    E := MatrixAlgebra(Q,2);
    e11 := E![1,0,0,0];
    e12 := E![0,1,0,0];
```

```
    tau := E![0,1,1,0];

    V := RModule(E,n);
    B := Basis(V);

    MnE := MatrixAlgebra(E,n);

    pairX := function(x,y)
        yy := Parent (y)!Vector([Adjoint(z) : z in Eltseq(y)]);
        return &+[x[i]*yy[i] : i in [1..n]];
    end function;

    pairY := function(x,y)
        return DotProduct(x*Omega,y);
    end function;

    function Ycoords(x);
        ans := V!([x[i][1,2] : i in [1..n]] cat [x[i][1,1] : i in [1..n]]);
        return ans;
    end function;

    YtoX := function(y)
        return &+[y[i]*e12*B[i] + y[n+i]*e11*B[i] : i in [1..n]];
    end function;

    XtoY := function(x)
        return Vector([x[i][1,2] : i in [1..n]] cat [x[i][1,1] : i in [1..n]]);
    end function;

    rows := [];

    for i in [1..n] do
        u := Ycoords(e11*B[i]);
        v := Ycoords(e12*B[i]);
        r := YtoX(u*g) + tau*YtoX(v*g);
        Append(~rows,r);
    end for;

    G := Matrix(rows);
    print "Hermitian check:", G*ConjTrans(G) eq Nm*Parent (G)!1;
    return G;
end intrinsic;
```

A.3 global.m

```
declare attributes Lat: HermSpace, ZBasis, ZBasisMatrix, forms, splitting;
declare attributes ModRng: QBasis, forms;

intrinsic HermSpace(E::AlgQuat, n::RngIntElt)->.
{Computes the standard Hermitian space E^n over Q with the auxiliary forms
attached which maintain the quaternionic structure}
    Q := BaseRing(E);
    pair := function(x,y)
        return &+[x[i]*Conjugate(y[i]) : i in [1..n]];
    end function;
    V := RModule(E,n);
    VQBasis := [b*V.j : b in Basis(E), j in [1..n]];
    M := MatrixAlgebra(Q,4*n);
    X := [[Trace(pair(b*x,y)) : x,y in VQBasis] : b in Basis(E)];
    forms := [M!x : x in X];

    V`QBasis := VQBasis;
    V`forms := forms;
    return V;
end intrinsic;

intrinsic QCoords(x)->.
{Converts the vector to its Q-coordinates}
    return Vector(&cat[Eltseq(y) : y in Eltseq(x)]);
end intrinsic;

intrinsic LeftReg(x)->.
{}
    E := Parent(x);
    rows := [Eltseq(x*b) : b in Basis(E)];
    return Transpose(Matrix(rows));
end intrinsic;

intrinsic StandardLattice(V::ModRng)->.
{Computes the standard lattice in the standard Hermitian space}
    E := BaseRing(V);
    n := Dimension(V);
    Z := Integers();

    require assigned V`forms: "V`forms must be assigned";
    require assigned E`MaximalOrder: "E`MaximalOrder needs to be assigned.";
    require assigned V`forms: "V`forms must be assigned";
```

```
    forms := V`forms;
    OE := E`MaximalOrder;

    ZBasis := [OE.i*V.j : i in [1..4], j in [1..n]];
    ZBasisMatrix := Matrix([QCoords(x) : x in ZBasis]);
    Lforms := [ZBasisMatrix*F*Transpose(ZBasisMatrix) : F in forms];
    if &and[&and[x in Z : x in Eltseq(y)] : y in Lforms] then
        M := MatrixAlgebra(Z,4*n);
        Lforms := [M!x : x in Lforms];
        else
            print "Warning: Lattice is not integral!";
    end if;

    L := LatticeWithGram(Lforms[1]);
    L`HermSpace := V;
    L`ZBasis := ZBasis;
    L`ZBasisMatrix := ZBasisMatrix;
    L`forms := Lforms;
    return L;
end intrinsic;

intrinsic Lattice(ZBasis::SeqEnum)->.
{Given a Z-basis, computes the lattice in the standard Hermitian space}
    V := Parent(ZBasis[1]);
    E := BaseRing(V);
    n := Dimension(V);
    Z := Integers();

    require assigned V`forms: "V`forms must be assigned";
    require assigned E`MaximalOrder: "E`MaximalOrder needs to be assigned.";
    require assigned V`forms: "V`forms must be assigned";

    forms := V`forms;
    OE := E`MaximalOrder;

    ZBasisMatrix := Matrix([QCoords(x) : x in ZBasis]);
    Lforms := [ZBasisMatrix*F*Transpose(ZBasisMatrix) : F in forms];
    if &and[&and[x in Z : x in Eltseq(y)] : y in Lforms] then
        M := MatrixAlgebra(Z,4*n);
        Lforms := [M!x : x in Lforms];
        else
            print "Warning: Lattice is not integral!";
    end if;
```

```
    L := LatticeWithGram(Lforms[1]);
    L`HermSpace := V;
    L`ZBasis := ZBasis;
    L`ZBasisMatrix := ZBasisMatrix;
    L`forms := Lforms;
    return L;
end intrinsic;

intrinsic abs(L::Lat)->.
{}
    LabsBasis := [QCoords(x) : x in L`ZBasis];
    return LatticeWithBasis(Matrix(LabsBasis));
end intrinsic;

intrinsic IsOEStable(L::Lat)->.
{}
    V := L`HermSpace;
    E := BaseRing(V);
    OE := E`MaximalOrder;
    Labs := abs(L);
    X := [Vector(ZCoords(x*y)) : x in Basis(OE), y in L`ZBasis];
    return &and[x in Labs: x in X];
end intrinsic;

intrinsic check_lattice(L::Lat)->.
{}
    V := L`HermSpace;
    VForms := V`forms;
    LForms := L`forms;
    Labs := abs(L);
    M := Parent(VForms[1]);
    X := [[DotProduct(Vector(Eltseq(x))*F,Vector(Eltseq(y))) :
            x,y in Basis(Labs)] : F in VForms];
    ans1 := &and[M!X[i] eq LForms[i] : i in [1..4]];
    ans2 := IsOEStable(L);
    return ans1 and ans2, ans1, ans2;
end intrinsic;

intrinsic Neighbour(L::Lat, splitting, P::AlgMatElt)->.
{}
    n := Dimension(L) div 4;
    E := Domain(splitting);
    V := L`HermSpace;
    Ep := Codomain(splitting);
    p := Prime(BaseRing(Ep));
```

```
    MnEp := MatrixAlgebra(Ep,n);
    Epn := RSpace(Ep,n);
    LpBasis := [];

    for i in [1..4*n] do
    x :=  [splitting(y) : y in Eltseq(L`ZBasis[i])];
    Append(~LpBasis, &+[x[i]*Epn.i : i in [1..n]]);
    end for;
    PP := MnEp!SptoU(P);

    Y := [x*PP : x in LpBasis];
    YY := [&+[(y[i]@@splitting)*V.i : i in [1..n]] :y in Y];
    Labs := LatticeWithBasis(L`ZBasisMatrix);

    quat := function(v)
        vv := Eltseq(v);
        n := # vv div 4;
        ans := &+[(E!vv[4*(i-1)+1..4*i])*V.i : i in [1..n]];
        return ans;
    end function;

    MZGens := [Vector(QCoords(yy)) : yy in YY] cat [p*v : v in Basis(Labs)];
    MZabs := sub<(1/p)*Labs|MZGens>;
    MZabsBasis := [quat(x) : x in Basis(MZabs)];
    M := Lattice(MZabsBasis);
    print "";
    print "Does the neighbour pass consistency checks?", check_lattice(M);
    print "";
    return M;
end intrinsic;

intrinsic aut_group(L::Lat)->.
{}
    V := L`HermSpace;
    n := Dimension(V);
    E := BaseRing(V);
    forms := L`forms;
    G := AutomorphismGroup(L,forms[2..4]);
    print "Paranoid check:",
            &and[g*F*Transpose(g) eq F : g in Generators(G), F in forms];
    A := L`ZBasisMatrix;

    quat := function(v)
        vv := Eltseq(v);
```

```
        n := # vv div 4;
        ans := &+[(E!vv[4*(i-1)+1..4*i])*V.i : i in [1..n]];
        return ans;
    end function;

    GgensCOE := [A^-1*Matrix(g)*A : g in Generators(G)];
    formsCOE := [A^-1*F*Transpose(A^-1) : F in forms];

    Emats := [Matrix([quat(QCoords(V.i)*g) : i in [1..n]]) : g in GgensCOE];
    return G,Emats;
end intrinsic;

intrinsic is_isom(L,M)->.
{Determines of two lattices, with their associated auxiliary forms carrying the
quaternionic structure, are isometric}
    V := L`HermSpace;
    n := Dimension(V);
    E := BaseRing(V);
    Lforms := L`forms;
    Mforms := M`forms;
    bl,g := IsIsometric(L,Lforms[2..4], M,Mforms[2..4]);
    if not bl then return false; end if;

    print "Paranoid check:", &and[g*Lforms[i]*Transpose(g) eq Mforms[i] : i in [1..4]];
    gg := (M`ZBasisMatrix)^-1*Matrix(g)*L`ZBasisMatrix;
    print "Paranoid check #2:", &and[gg*f*Transpose(gg) eq f : f in Bn`forms];

    quat := function(v)
        vv := Eltseq(v);
        n := # vv div 4;
        ans := &+[(E!vv[4*(i-1)+1..4*i])*V.i : i in [1..n]];
        return ans;
    end function;

    mat := Matrix([quat(QCoords(V.i)*gg) : i in [1..n]]);
    return bl, mat;
end intrinsic;
```

Bibliography

[1] Peter Abramenko and Gabriele Nebe. Lattice chain models for affine buildings of classical type. *Mathematische Annalen*, 322(3):537–562, 2002.

[2] Christine Bachoc. Voisinage au sens de Kneser pour les réseaux quaternioniens. *Comment. Math. Helv.*, 70(3):350–374, 1995.

[3] F. Bruhat and J. Tits. Groupes réductifs sur un corps local. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 60(1):5–184, 1984.

[4] Henri Cohen. *Advanced Topics in Computational Algebraic Number Theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 2000.

[5] John Conway and Neil Sloane. The unimodular lattices of dimension up to 23 and the Minkowski-Siegel mass constants. *European Journal of Combinatorics*, 3(3):219 – 231, 1982.

[6] Clifton Cunningham and Lassina Dembélé. Computing genus-2 Hilbert-Siegel modular forms over $\mathbb{Q}(\sqrt{5})$ via the Jacquet-Langlands correspondence. *Experiment. Math.*, 18(3):337–345, 2009.

[7] Wee Teck Gan and Jiu-Kang Yu. Group schemes and local densities. *Duke Mathematical Journal*, 105(3):497–524, 12 2000.

[8] Matthew Greenberg and John Voight. Lattice methods for algebraic modular forms on classical groups. In Gebhard Böckle and Gabor Wiese, editors, *Computations with Modular Forms*, volume 6 of *Contributions in Mathematical and Computational Sciences*, pages 147–179. Springer International Publishing, 2014.

[9] Benedict Gross. Algebraic modular forms. *Israel Journal of Mathematics*, 113(1):61–93, 1999.

[10] Detlev Hoffmann. On positive definite hermitian forms. *Manuscripta Mathematica*, 71(1):399–429, 1991.

[11] Kenichi Iyanaga. Class numbers of definite hermitian forms. *Journal of the Mathematical Society of Japan*, 21(3):359–374, 07 1969.

[12] Martin Kneser. Klassenzahlen definiter quadratischer Formen. *Arch. Math.*, 8:241–250, 1957.

[13] Joshua Lansky and David Pollack. Hecke algebras and automorphic forms. *Compositio Math.*, 130(1):21–48, 2002.

[14] David Loeffler. Explicit calculations of automorphic forms for definite unitary groups. *LMS J. Comput. Math.*, 11:326–342, 2008.

[15] Wilhelm Plesken and Bernd Souvignier. Computing isometries of lattices. *J. Symbolic Comput.*, 24(3-4):327–334, 1997. Computational algebra and number theory (London, 1993).

[16] Rudolf Scharlau and Boris Hemkemeier. Classification of integral lattices with large class number. *Math. Comput.*, 67(222):737–749, 1998.

[17] Alexander Schiemann. Classification of Hermitian forms with the neighbour method. *J. Symbolic Comput.*, 26(4):487–508, 1998.

[18] Rainer Schulze-Pillot. An algorithm for computing genera of ternary and quaternary quadratic forms. In *Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation*, ISSAC '91, pages 134–143, New York, NY, USA, 1991. ACM.

[19] Goro Shimura. Arithmetic of alternating forms and quaternion hermitian forms. *J. Math. Soc. Japan*, 15:33–65, 1963.

[20] Carl Ludwig Siegel. On the theory of indefinite quadratic forms. *Annals of Mathematics*, 45(3):pp. 577–622, 1944.

[21] Marie-France Vignéras. *Arithmétique des Algèbres de Quaternions*. Lecture Notes in Mathematics. Springer-Verlag, New York, 1980.

[22] John Voight. *The arithmetic of quaternion algebras*. preprint.