Thesis for the Degree of Doctor of Philosophy

On Quaternionic Shimura Surfaces

Håkan Granath

CHALMERS | GÖTEBORG UNIVERSITY

Department of Mathematics
CHALMERS UNIVERSITY OF TECHNOLOGY
GÖTEBORG UNIVERSITY
Göteborg, Sweden 2002

On Quaternionic Shimura Surfaces
Håkan Granath
ISBN 91-7291-165-4

Doktorsavhandlingar vid Chalmers tekniska högskola
Ny serie nr 1847
ISSN 0346-718x

Department of Mathematics
Chalmers University of Technology and Göteborg University
SE-412 96 Göteborg
SWEDEN
Telephone +46 (0)31 772 1000

Chalmers University of Technology and Göteborg University
Göteborg, Sweden 2002

Abstract

Let k be a real quadratic field, and let A be a totally indefinite quaternion algebra which allows an involution of type 2, that is, an involution inducing the non-trivial automorphism on k. Let Λ be a maximal order in A. The elements of Λ with norm 1 act naturally on $\mathcal{H}\times\mathcal{H}$, where $\mathcal{H}$ is the complex upper half plane. Let Γ denote the image of Λ^1 in $\mathrm{Aut}(\mathcal{H}\times\mathcal{H})$, and X the quotient surface $\mathcal{H}\times\mathcal{H}/\Gamma$. We let Y be the minimal desingularisation of the compactification of X. If $A = M_2(k)$, then X is a so called Hilbert modular surface. Such surfaces are rather well investigated. We look at the case when A is a skew field. In this case, X is compact, so it only has quotient singularities. We also examine quotients by some extensions of Γ to larger discrete subgroups of $\mathrm{Aut}(\mathcal{H}\times\mathcal{H})$.

We construct a family of curves on Y, which corresponds to the so called modular curves in the case of Hilbert modular surfaces. The main part of the work consists of a study of various aspects of these curves. They are parametrised by the elements β of a quaternary lattice (L, q), which consists of what we call integral Λ-hermitian forms. There is a close connection between the quadratic space L and the order Λ via Clifford algebras.

To each curve F_β there is an associated quaternion order Λ_β over $\mathbb{Z}$ and a map $\mathcal{H}/\Lambda_\beta^1 \to F_\beta$, which is generically 1 to 1 or 2 to 1. We determine the genus of the order Λ_β. To do this, we study, among other things, a certain one-to-one correspondence between primitive orders and hermitian planes in the local case.

For each positive integer N, we define a curve F_N in the same way as it is done in the case of Hilbert modular surfaces. We determine the number of irreducible components of F_N. To each intersection point of curves, we associate an integral binary quadratic form. We derive a formula for the number of points on X, which are associated to a given form. This gives a possibility to completely determine the configuration of curves.

Finally, we study the particular case when $k = \mathbb{Q}(\sqrt{13})$ and the discriminant of the algebra A is (3). We construct a natural tower $\Gamma \subset \Gamma_{\mathrm{I}} \subset \Gamma_{\mathrm{II}} \subset \Gamma_{\mathrm{III}}$ of discrete subgroups of $\mathrm{Aut}(\mathcal{H}\times\mathcal{H})$, where each group extension is of degree 2, and consider the minimal desingularisation of the corresponding quotients. We prove, using the modular curves, that Y is a minimal surface of general type, Y_{I} is a $K3$-surface blown up 4 times, Y_{II} is an Enriques surface blown up 2 times, and Y_{III} is a rational surface with Euler characteristic $e = 12$. We also construct an elliptic fibration on Y_{II}, which we use to conclude that Y_{II} is a so called special Enriques surface.

Keywords: Shimura surface, quaternion order, Clifford algebra, hermitian form, Kodaira classification

2000 Mathematics Subject Classification: Primary 14G35, 16H05, 11E88. Secondary 11G18, 11R52, 11E39, 14J10.

Contents

Acknowledgement

I would like to thank my advisor Juliusz Brzezinski. Without his constant encouragement and his enthusiasm and patience, I would never have been able to finish this thesis. He has shown a great interest in my work and it has always been very inspiring to discuss problems with him.

I also want to thank Samuel Bengmark for his support.

1 Introduction

In this thesis, we consider surfaces constructed from unit groups of totally indefinite quaternion orders over the integers in real quadratic fields. Hence the thesis involves concepts from both algebraic geometry and number theory. We start with an informal introduction.

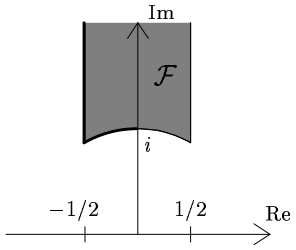
Let $\mathcal{H}$ denote the upper complex half plane

$$\mathcal{H} = \{z \in \mathbb{C} \mid \operatorname{Im} z > 0\}.$$

The group $\mathrm{SL}_2(\mathbb{R})$, consisting of real 2×2-matrices with determinant 1, acts on $\mathcal{H}$ via Moebius transformations:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} z = \frac{a_{11}z + a_{12}}{a_{21}z + a_{22}}.$$

Consider now the action of the discrete subgroup $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ of $\mathrm{SL}_2(\mathbb{R})$. In this very classical situation, it is well known that, under the action of Γ, every point of $\mathcal{H}$ is equivalent to a unique point in the set $\mathcal{F}$ indicated in the following figure:



$\mathcal{F}$ is a so called fundamental domain for the action of Γ on $\mathcal{H}$. Now the quotient of $\mathcal{H}$ by any discrete group has a natural structure of a complex curve. In this particular case, it is well known that $\mathcal{H}/\Gamma \cong \mathbb{C}$. If we add one point at the "cusp" of $\mathcal{F}$ in the direction of the imaginary axis, we get a compact curve, the projective line $\mathbb{P}^1(\mathbb{C})$.

Let now R be the ring of integers in a real quadratic field k, and $x \mapsto \overline{x}$ the non-trivial automorphism of k. Consider the group $\Gamma = \mathrm{SL}_2(R)$. Since k is a subfield of $\mathbb{R}$, we can let Γ act on $\mathcal{H} \times \mathcal{H}$ by

$$\lambda(z_1, z_2) = (\lambda z_1, \overline{\lambda} z_2).$$

Hilbert was interested in this group action. The quotient surface $X = \mathcal{H} \times \mathcal{H}/\Gamma$ is called a Hilbert modular surface. X has in general quotient singularities coming from so called elliptic elements of Γ, i.e. elements of finite order acting non-trivially on $\mathcal{H} \times \mathcal{H}$. Furthermore, X is not compact,

but as in the case of $\mathrm{SL}_2(\mathbb{Z})$, it can be compactified by adding points at the so called cusps. The cusps give rise to highly non-trivial singularities, which were first resolved by Hirzebruch.

Consider the canonical minimal resolution Y of the compactification of X. On Y we have the curves which are exceptional divisors of the singularities. There are also other important curves on Y, the so called "modular curves" F_N, for positive integers N. For example the diagonal $\{(z,z) \mid z \in \mathcal{H}\}$ in $\mathcal{H}\times\mathcal{H}$ gives the curve F_1. Using these curves, one succeeded to fit the Hilbert modular surfaces into the Kodaira classification of algebraic surfaces. For example, it was shown that Y is a rational surface for small discriminants of k.

The group $\Gamma = \mathrm{SL}_2(R)$ is a subgroup of the unit group in the ring of 2×2-matrices over R, which is a special instance of a quaternion order. However, the surfaces that we will consider are not constructed from this group, but from groups related to other quaternion orders. The classical Hamiltonian quaternion algebra is the $\mathbb{R}$-algebra $\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}ij$, where $i^2 = j^2 = -1$ and $ij = -ji$. Now, quaternion algebras can be considered over any field F. If a, b are non-zero elements of F, then we can define

$$A = F + Fi + Fj + Fij,$$

where $i^2 = a$, $j^2 = b$ and $ij = -ji$. There is a canonical multiplicative map $\mathrm{nr} : A \to F$, called the norm map, given by $\mathrm{nr}(x_0 + x_1 i + x_2 j + x_3 ij) = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2$, for $x_i \in F$. If F is a number field, then for every embedding $F \to \mathbb{R}$, we get a real quaternion algebra $\mathbb{R} \otimes_F A$, which is either isomorphic to $M_2(\mathbb{R})$ or $\mathbb{H}$. If we have the former case for all real embeddings, then we say that A is totally indefinite. Assume now that A is a totally indefinite quaternion algebra over a real quadratic field k. Let Λ be a so called R-order in A, i.e. a subring of A containing R, which is finitely generated as an R-module and such that $k\Lambda = A$. Consider now the group Λ^1, which consists of elements $\lambda \in \Lambda$ with $\mathrm{nr}(\lambda) = 1$. The two embeddings $A \to M_2(\mathbb{R})$ give two embeddings $\Lambda^1 \to \mathrm{SL}_2(\mathbb{R})$, and hence an action of Λ^1 on $\mathcal{H}\times\mathcal{H}$.

If every non-zero element of A is invertible, then we say that A is a skew field. This is the case we will consider. In this case, the quotient surfaces $\mathcal{H}\times\mathcal{H}/\Lambda^1$ are automatically compact. To be able to say something about these surfaces, we need to find a suitable construction of curves which correspond to the modular curves F_N in the case of Hilbert modular surfaces.

We can construct such a family of curves if we add one extra condition requiring that A allows a so called involution of type 2, i.e. an involution which acts non-trivially on the center k of A. The curves are parametrised

by the elements of a quaternary quadratic lattice, which is the set of what we call integral Λ-hermitian forms. There is a close connection between this quadratic space and the order Λ via Clifford algebras. This makes it possible to calculate the number of components of F_N, as well as the geometric genus of the curves. To each intersection point of the curves, we associate an integral positive definite binary form. We get a formula for the number of points of X that belong to a certain form, and using this, it is possible to determine the configuration of curves in concrete examples.

Finally, we apply this theory to a particular case when $k = \mathbb{Q}(\sqrt{13})$. We consider not only the group Γ, but also a natural family of larger discrete subgroups of $\mathrm{Aut}(\mathcal{H}\times\mathcal{H})$. We get rather detailed geometrical information about these surfaces. We prove that Y is a minimal surface of general type. The quotients with the larger groups give a $K3$-surface and a special Enriques surface. The quotient surface with respect to the largest group is rational.

1.1 Hilbert modular surfaces

Since the surfaces we will study are closely related to the Hilbert modular surfaces, we give a very brief description of what is known about these. For more information see [17].

Let k be a real quadratic field extension of $\mathbb{Q}$ and $x \mapsto \bar{x}$ its non-trivial automorphism. We have $k = \mathbb{Q}(\sqrt{d})$, where d is a positive square free integer. Let R be the ring of integers in k and let D be the discriminant of R. Hence we have $D = d$ if $d \equiv 1 \pmod 4$, and $D = 4d$ otherwise.

In its general form, the construction of Hilbert modular surfaces is as follows. Let $\mathfrak{b}$ be an R-ideal. Consider the group $\mathrm{PSL}_2(R,\mathfrak{b}) = \mathrm{SL}_2(R,\mathfrak{b})/\{\pm 1\}$, where $\mathrm{SL}_2(R,\mathfrak{b}) = \{\lambda \in \left(\begin{smallmatrix} R & \mathfrak{b}^{-1} \\ \mathfrak{b} & R \end{smallmatrix}\right) \mid \det(\lambda) = 1\}$, acting on $\mathcal{H}\times\mathcal{H}$. In the language of the rest of this thesis, the choice of $\mathfrak{b}$ corresponds to a choice of a maximal order in $M_2(k)$. For simplicity, we will in this subsection only consider the case $\mathfrak{b} = R$. We write $\Gamma = \mathrm{PSL}_2(R)$ and $X = \mathcal{H}\times\mathcal{H}/\Gamma$.

Hilbert was interested in this group action, and his student Blumenthal worked on finding a fundamental domain. Later Siegel computed the hyperbolic volume of the fundamental domain for the action of Γ on $\mathcal{H}\times\mathcal{H}$.

X has in general quotient singularities coming from elliptic elements of Γ. The number of such singularities was computed by Prestel in [33].

As we have mentioned, an important feature of the Hilbert modular surfaces is the presence of so called cusps. Maass pointed out that the number of cusps equals the class number of k. The surface X can be compactified by adding one point for each cusp, but from each cusp we get a singularity. The difficulty of resolving these singularities was for a long time a problem that

inhibited the development of the theory of Hilbert modular surfaces. Eventually, they where resolved by Hirzebruch (see [24]), and the exceptional curves of the resolutions turned out to consist of cycles of curves related to certain continued fractions expansions. Let $Y = Y(D)$ denote the minimal desingularisation of the compactification of X.

The resolution of the cusp singularities opened up new possibilities to study the Hilbert modular surfaces using methods from algebraic geometry. It is then important to find sufficiently many curves on Y. In addition to the curves coming from the resolution of the singularities, there are also the so called modular curves. These are constructed as follows. Consider the set of skew-hermitian matrices of the form

$$\beta = \begin{pmatrix} aD & \lambda\sqrt{D} \\ -\overline{\lambda}\sqrt{D} & bD \end{pmatrix}, \tag{1.1}$$

where $a, b \in \mathbb{Z}$ and $\lambda \in R$. These matrices form a $\mathbb{Z}$-lattice of rank 4, which we denote by L. An element β of L is called primitive if it is not of the form $\beta = n\beta'$, where $n \in \mathbb{Z}$, $n > 1$ and $\beta' \in L$. Consider the curve $C_\beta \subset \mathcal{H}\times\mathcal{H}$ defined by

$$C_\beta = \{(z_1, z_2) \in \mathcal{H}\times\mathcal{H} \mid \begin{pmatrix} z_2 & 1 \end{pmatrix} \beta \begin{pmatrix} z_1 \\ 1 \end{pmatrix} = 0\}. \tag{1.2}$$

The image of C_β in X is denoted by F_β. For positive integers N, we let F_N denote the union of all curves F_β where β runs over all primitive elements in L with determinant N. The curves F_N have a finite number of irreducible components. Franke computed the number of components of F_N in the case that k has prime discriminant, see [14]. Hausmann extended these results to arbitrary k in [20].

Using numerical invariants of the surfaces, which were computed by several authors, and the configurations of curves, it was possible to fit the curves into the Enriques-Kodaira classification of surfaces. The result is (see [23]) that $Y(D)$ is rational surface for $D = 5$, 8, 12, 13, 17, 21, 24, 28, 33 and 60, $Y(D)$ is a blown up $K3$-surface for 12 values of D, and a blown-up honestly elliptic surfaces for 14 values of D. For all other values of D, $Y(D)$ is of general type.

Define the curve $T_N = \cup F_{N/t^2}$, where the union is taken over all positive integers t such that $t^2 \mid N$. It was discovered by Hirzebruch and Zagier, that the intersection numbers of these curves appear as Fourier coefficients of certain modular forms of so called Nebentypus. The intersection numbers $T_N T_M$ for $N, M \in \mathbb{Z}$ were computed in [22]. This aspect of the theory Hilbert modular surfaces can also be studied for the surfaces that we will consider. It is however not treated in this thesis.

1.2 Quaternionic Shimura surfaces

We say some words on the construction of quaternionic Shimura surfaces. This is a special case of a construction of algebraic varieties introduced by Shimura (see e.g. [42]). Let A be a totally indefinite quaternion algebra over k. This implies that there exist two inequivalent real representations

$$\varrho_i : A \to M_2(\mathbb{R}), \quad i = 1, 2.$$

Let Λ be a maximal order in A, and Λ^1 the group

$$\Lambda^1 = \{\lambda \in \Lambda \mid \mathrm{nr}(\lambda) = 1\}.$$

Now ϱ_i maps Λ^1 into $\mathrm{SL}_2(\mathbb{R})$ for $i = 1, 2$, so Λ^1 acts on the $\mathcal{H}\times\mathcal{H}$ by

$$\lambda(z_1, z_2) = (\varrho_1(\lambda)z_1, \varrho_2(\lambda)z_2). \tag{1.3}$$

Notice that this action is not faithful. An element λ acts trivially on $\mathcal{H}\times\mathcal{H}$ if and only if it belongs to the center k of A, i.e. if and only if $\lambda = \pm 1$.

The image of Λ^1 in $\mathrm{Aut}(\mathcal{H}\times\mathcal{H})$ is a discrete subgroup, and we let X denote the quotient surface,

$$X = \mathcal{H}\times\mathcal{H}/\Lambda^1.$$

Note that if we choose a different set of representations ϱ_i in (1.3), then we get a quotient which is isomorphic to the original. This is clear since the two actions are just conjugated by an element in $\mathrm{Aut}(\mathcal{H}\times\mathcal{H})$.

If τ is an involution on A which restricts to the nontrivial automorphism on the center k of A, then we say that τ is an involution of type 2. Not every quaternion algebra A has such an involution. In this thesis, we will only consider quaternion algebras having an involution of type 2. We need this assumption to construct the modular curves.

We are interested in the case where A is a skew field over a real quadratic field k. In this case, the quotient surface $X = \mathcal{H}\times\mathcal{H}/\Lambda^1$ is compact (see [44], chapter 9). The only singularities of X are quotient singularities corresponding to finite cyclic subgroups of Λ^1. These surfaces have been examined by some authors.

Shavel studies, in [37], the case when X is non-singular, and determines all cases when the surfaces X have geometric genus $p_g = 0$. There are 3 such cases, one with $k = \mathbb{Q}(\sqrt{2})$ and two with $k = \mathbb{Q}(\sqrt{3})$. He also considers the corresponding question for certain extensions of the group Γ. This gives many more cases with $p_g = 0$.

Takeuchi [45] determines all cases when the corresponding construction in dimensions higher than two, with respect to the group $\Gamma = \Lambda^1/\{\pm 1\}$, gives a smooth variety of geometric genus 0.

We are rather interested in the case when X has singularities. On the other hand, we restrict to the case when the algebra allows a so called involution of type 2. With this restriction, there are for instance no cases where $p_g(X) = 0$. But, as we will see, we may get surfaces with $p_g = 0$ if we consider extensions of Γ.

We remark that the surfaces X are moduli spaces of abelian surfaces with some extra structure. This is of course an important and interesting aspect of these surfaces, but it is not treated in the thesis.

1.3 Summary of the thesis

We now give a brief overview of the contents of the thesis.

Chapters 2 and 3 are of a somewhat preparatory nature. For the convenience of the reader, we present some aspects of the theory of Clifford algebras and orders in quaternion algebras which we will need later. However, we present some minor new results that will be used later on. There is a well known connection between orders and ternary quadratic lattices. This connection can be established in a very natural way, and using this we can get for instance a natural correspondence between quadratic orders embedded in the quaternion order and rank 2 sublattices of the ternary quadratic lattice. Another thing we do, is to present an algorithm that can be used to compute minimal over-orders of a given quaternion order.

In chapter 4, we examine involutions of so called type 2, i.e. involutions on A which act non-trivially on the center k of A. We introduce the concept of special involutions with respect to a maximal order Λ. An involution τ is special if the fixed point set $\Lambda_\tau = \{\lambda \in \Lambda \mid \tau(\lambda) = \lambda\}$ satisfies $(\Lambda_\tau)_p \cong M_2(\mathbb{Z}_p)$ for all primes p that are ramified in k. We prove that there always exists a special involution, so we can without loss of generality assume that the involutions we consider are special.

In chapter 5, we consider hermitian forms in different settings. In fact, two different topics are considered. The first one is the following. We introduce the concept of A-hermitian forms, which in the 1-dimensional case simply are maps $\Phi : A \times A \to A$ which satisfy $\Phi(x+y,z) = \Phi(x,z)+\Phi(y,z)$, $\Phi(xa,y) = \Phi(x,y)a$ and $\Phi(x,y) = \tau(\Phi(y,x))^*$ for all $a,x,y,z \in A$. If Λ is a maximal order, then we define in a natural way what it means for Φ to be integral (only if 2 is ramified in k extra care has to be taken). The set of so called integral Λ-hermitian forms is what later will be the lattice that parametrises the modular curves which we construct in chapter 7. We compute the local number of classes of such forms. This computation is essentially a disguised form of the local computation of the number of classes of integral skew-hermitian forms in [20].

The second topic is the following. We consider a construction of orders from hermitian planes. This construction, but on the level of algebras instead of orders, occurs for instance in [43], section 4. Let F be a field with maximal order P, and K be a separable quadratic F-algebra with maximal P-order S. We say that a quaternion P-order Λ is an S-primitive order if there exists an embedding $f : S \to \Lambda$. Let $h : M \times M \to S$ be a hermitian form on an S-lattice M of rank 2. Define

$$\Lambda_h = \{\lambda \in \mathrm{End}_S(M) \mid h(x, \lambda y) = h(\lambda^* x, y) \text{ for all } x, y \in M\}.$$

Now, we construct a map going the other way: given an S-primitive order we construct a hermitian S-plane. We prove that, in the local case, these maps are inverses of each other. In particular, we have that Λ_h is S-primitive. A useful corollary is that the orders that we construct in chapter 7 are Bass orders. In the global case, the map $h \mapsto \Lambda_h$ is in general not bijective, but it is always surjective.

In chapter 7, we construct the curves which correspond to the so called modular curves on Hilbert modular surfaces. We construct a quaternary quadratic $\mathbb{Z}$-lattice L parametrising them, which replaces the skew-hermitian matrices (1.1). This is where we use the concept of Λ-integral forms. So, for every primitive element $\beta \in L$ with $q(\beta) > 0$, we have a curve $C_\beta \subset \mathcal{H} \times \mathcal{H}$. We let F_β denote the image of C_β in X and Γ_β the stabiliser of C_β in Λ^1, so $\Gamma_\beta = \{\lambda \in \Lambda^1 \mid \lambda C_\beta = C_\beta\}$. For every non-zero $\beta \in L$, there is a natural quaternary $\mathbb{Q}$-subalgebra A_β of A. If we let $\Lambda_\beta = \Lambda \cap A_\beta$, then Λ^1_β is a subgroup of Γ_β of index 1 or 2.

The key fact is that Λ and (L, q) are closely connected via Clifford algebras. More precisely, there is a dual quaternary space $(L^\#, q^\#)$ and an embedding of rings

$$\phi : C_0(L^\#, q^\#) \to \Lambda.$$

ϕ is not an isomorphism in our case, and, in fact, ϕ is an isomorphism if and only if A is a split algebra. But the image Θ of ϕ is rather close to being all of Λ, we have for example that $\Lambda = R\Theta$.

We use this connection to derive the following formula for the discriminant of Λ_β: $d(\Lambda_\beta) = (q(\beta)) \cap (d(\Lambda) \cap \mathbb{Z})$. If we combine this with a computation of $d(A_\beta)$ and the results of chapter 5, we get a complete description of the genus (i.e. the local isomorphism class) of the order Λ_β. This, together with the description of the group extension $\Gamma_\beta \supseteq \Lambda^1_\beta$, makes it possible to determine the genus of the curve C_β/Γ_β.

In chapter 8, we determine the number of irreducible components of the curve F_N. To do that, we exploit the fact that the problem can be formulated as a question about classes of integral Λ-hermitian forms. Then

we essentially use the ideas of Franke [14] and Hausmann [20], who solved the corresponding problem in the case of Hilbert modular surfaces. They used an approximation result of Shimura [41] on hermitian lattices (in the usual sense). This result is straightforwardly carried over to our theory of integral Λ-hermitian forms and we can just proceed in the same way to compute the number of components.

In chapter 9, we examine how the curves intersect each other. To each intersection point of modular curves, we associate a binary quadratic form. We introduce, in the same way as it is done in [22] for the case of Hilbert modular surfaces, a rational number $s(\varphi)$ which mainly depends on how many points in X that are associated to the form φ. We determine, under the assumption that neither 2 nor 3 is ramified in k, which forms φ can occur and, in particular, we describe which forms correspond to elliptic points. It turns out that it is natural to divide the elliptic points into two groups, points of type I and type II respectively, according to the associated binary form. The main result, however, is a formula for $s(\varphi)$, see theorem 9.16.

In chapter 10, we leave the surfaces for a while and consider the situation when Λ is a $\mathbb{Z}$-order in an indefinite rational quaternion algebra and Λ^1 acts on $\mathcal{H}$. Specifically, we consider discrete subgroups of $\mathrm{Aut}(\mathcal{H})$ extending the image of Λ^1 and show how one can compute the number of fixed points of the different involutions, which we get on the quotient curve. One reason to do this, is that it is needed to compute the genus of some of the curves F_β (recall that Γ_β may be an extension of Λ^1_β).

In chapter 11, we recall some well known facts about the numerical invariants of the surfaces Y. We also consider how the group Γ can be extended to a larger discrete subgroup of $\mathrm{Aut}(\mathcal{H}\times\mathcal{H})$. We show, for instance, that if k has class number 1, prime discriminant and $d(\Lambda) = (q)$ where q a prime, then there exists an extension $\widehat{\Gamma}$ of Γ such that $\widehat{\Gamma}/\Gamma \cong D_4$, the dihedral group. We also consider some of the quotient singularities that can arise on the surface $\mathcal{H}\times\mathcal{H}/\widehat{\Gamma}$. The reason that we have to make such thorough investigations in the well known area of resolutions of quotient singularities is that we do not only need to know the exceptional divisors of the minimal resolutions, but we also need to know how these divisors meet the modular curves F_β.

In chapter 12, we study an example where $k = \mathbb{Q}(\sqrt{13})$ and $d(\Lambda) = (3)$. This example is chosen since it has one of the smallest hyperbolic volumes of the fundamental domain and at the same time 2 and 3 are not ramified in k, so we can use the results of chapter 9. We choose a small number of curves F_N and using the results of the previous sections, we determine the intersection points of these curves, as well as their genus and self-intersections.

Also, we have a natural tower of discrete subgroup of $\mathrm{Aut}(\mathcal{H}\times\mathcal{H})$

$$\Gamma \subset \Gamma_{\mathrm{I}} \subset \Gamma_{\mathrm{II}} \subset \Gamma_{\mathrm{III}},$$

where each extension is of degree 2 and $\Gamma_{\mathrm{III}}/\Gamma \cong D_4$. We let Y_{I} denote the minimal desingularisation of $\mathcal{H}\times\mathcal{H}/\Gamma_{\mathrm{I}}$, and similarly for Y_{II} and Y_{III}. We prove that Y is a minimal surface of general type, Y_{I} is a $K3$-surface blown up 4 times, Y_{II} is a special Enriques surface blown up 2 times and Y_{III} is a rational surface with Euler number $e = 12$.

It would be a very nice further step if one could give explicit equations for the surface Y, as it has been done for some Hilbert modular surfaces, see for example [18]. However, we have not managed to do that.

2 Algebras and orders

In this preparatory chapter, we state mostly well known results about algebras and orders. Two things are maybe not standard. One is the formulation of corollary 2.9, which describes a natural connection between an order and its corresponding quadratic lattice. That point of view will be very important to us in the following. The other is an algorithm in section 2.7 to produce larger orders containing a given one. It will be useful, in particular, for producing maximal orders.

Throughout the chapter, we use the following conventions. If not explicitly stated otherwise, P is a Dedekind domain with quotient field F. We always assume that $\mathrm{char}\, F = 0$. If we say that F is a local field, then we mean the following: We additionally assume that P is a complete discrete valuation ring where the valuation is denoted by v. Let π be a generator of the maximal ideal of P. Let $\widehat{P}$ denote the residue class field $P/(\pi)$.

2.1 Preliminaries

Let V be a finite dimensional vector space over F. A P-lattice L on V is a finitely generated P-module such that $FL = V$.

Let L be a free lattice with basis $e_1, \ldots, e_n$. We say that an element $x \in L$ is *primitive*, if $\{r \in F \mid rx \in L\} = P$. An integral quadratic form on L is a map $q : L \to P$ such that

$$q(x_1e_1 + \cdots + x_ne_n) = \sum_{1\le i\le j\le n} a_{ij}x_ix_j,$$

where $x_i \in P$ for $i = 1, \ldots, n$, and $a_{ij} \in P$ for all i, j. The form is said to be primitive, if the P-ideal generated by all coefficients a_{ij} equals P. The form

is said to be isotropic, if there exists a non-zero element $x \in L$ such that $q(x) = 0$, otherwise it is said to be anisotropic. To the quadratic form q, we associate the bilinear form $b(x, y) = q(x + y) - q(x) - q(y)$, where $x, y \in L$. We have $q(x) = \frac{1}{2}b(x, x)$ for all $x \in L$. The matrix

$$M_q = (b(e_i, e_j)) \tag{2.1}$$

is called the matrix of q (with respect to the given basis). The discriminant $d(q)$ of q is the ideal $(\det(M_q))$ if the rank is even, and $(\frac{1}{2}\det(M_q))(\subseteq P)$ if the rank is odd (see [28], p. 208). The form q is said to be non-degenerate if $d(q) \neq 0$, and it is said to be unimodular if $d(q) = P$. Two quadratic forms q_1 and q_2 on L are said to be equivalent, or in the same class, if there exists an automorphism $g : L \to L$ such that $q_1(x) = q_2(g(x))$ for all $x \in L$. Two forms are said to be in the same genus, if they are equivalent over $P_\mathfrak{p}$ for all prime spots $\mathfrak{p}$ of F. The forms q_1 and q_2 are said to be similar, if q_1 is equivalent to cq_2 for some non-zero $c \in F$. The form q is called modular if it is similar to a unimodular form.

We recall the definition of the Hilbert symbol. Let F be a local field. If $a, b \in F^*$, then the Hilbert symbol (a, b) is defined by

$$(a, b) = \begin{cases} 1 & \text{if the form } x^2 - ay^2 - bz^2 \text{ on } F^3 \text{ is isotropic,} \\ -1 & \text{otherwise.} \end{cases}$$

If p is a prime and $F = \mathbb{Q}_p$, then we will often write the Hilbert symbol as $(a, b)_p$, for $a, b \in \mathbb{Q}_p^*$. We also write $(a, b)_\infty$, for $a, b \in \mathbb{R}^*$. Using the following proposition, it is possible to compute $(a, b)_p$ for all primes p. For a proof, see for example [2], p. 56 and [31], theorem 71:18.

Proposition 2.1. *The Hilbert symbol satisfies the following properties:*

i) *for any $a, b, c \in F^*$, we have $(a, bc) = (a, b)(a, c)$, $(ac^2, b) = (a, b)$, $(b, a) = (a, b)$ and $(a, -a) = 1$,*

ii) *if p is an odd prime and $a, b \in \mathbb{Z}_p^*$, then $(a, b)_p = 1$ and $(a, p)_p = \left(\frac{a}{p}\right)$, where $\left(\frac{a}{p}\right)$ is the Legendre symbol,*

iii) *if $a, b \in \mathbb{Z}_2^*$, then $(a, b)_2 = (-1)^{(\overline{a}-1)(\overline{b}-1)/4}$ and $(a, 2)_2 = (-1)^{(\overline{a}^2-1)/8}$, where $\overline{a}, \overline{b} \in \mathbb{Z}$ with $\overline{a} \equiv a \pmod 8$ and $\overline{b} \equiv b \pmod 8$,*

iv) *if $a, b \in \mathbb{R}^*$, then $(a, b)_\infty = -1$ if and only if $a < 0$ and $b < 0$.*

Furthermore, if a and b are non-zero rational numbers, then $(a, b)_p = 1$ for almost all primes, and we have the Hilbert product formula

$$\prod_p (a, b)_p = 1, \tag{2.2}$$

where p runs over all primes and ∞.

Consider again a general field F. Let K be a separable F-algebra of degree 2. Let $x \mapsto \overline{x}$ denote the non-trivial automorphism of K over F. Let S denote the ring of integral elements in K. Assume now that F is local. If $K \cong F \times F$, then we say that K/F is a split extension. Assume that K is a field. Let Π denote the generator of the maximal ideal of S. If $\Pi S = \pi S$, then we say that the extension is unramified, otherwise it is ramified.

2.2 Quaternion algebras

Let A be a finite dimensional F-algebra. A is *central*, if the center of A is F. A is *simple*, if A has no non-trivial two-sided ideals. The *Jacobson radical* $J(A)$ is the intersection of all maximal left (or equivalently right) ideals of A. A is *semi-simple* if $J(A) = (0)$. It is well known that a semi-simple algebra is a direct product of simple algebras (see e.g. [26], theorem 3.6).

Definition 2.2. If F is a field and A is a central simple algebra of dimension 4 over F, then A is called a *quaternion algebra*.

Let A be a quaternion algebra over F. There is a unique anti-involution $x \mapsto x^*$ on A, called the *canonical involution*, such that $\mathrm{tr}(x) = x + x^* \in F$ and $\mathrm{nr}(x) = xx^* \in F$ for all $x \in A$. The map $\mathrm{tr} : A \to F$ is called the *reduced trace* of A, and $\mathrm{nr} : A \to F$ the *reduced norm*. It is also well known that there exists an F-basis of A of the form $1, i, j, ij$, where $i^2, j^2 \in F^*$ and $ij + ji = 0$.

If A is a quaternion algebra over F, then by Wedderburn's theorem (see e.g. [26], theorem 2.5), we have that $A \cong M_2(F)$ or A is a skew field, i.e. an algebra in which every non-zero element is invertible. If F is a local field, then we say in the former case that A is *split*, and in the latter that A is *ramified*.

If F is a local field, then it is well known that there is a unique quaternion algebra over F, which is a skew field (see [46], théorème II.1.1). The unique skew field over $\mathbb{Q}_p$, where p is a prime, will be denoted by $\mathbb{H}_p$.

Definition 2.3. If A is a quaternion algebra over the field F, and $\mathfrak{p}$ is a prime spot of F, then we define

$$\left(\frac{A}{\mathfrak{p}}\right) = \begin{cases} -1 & \text{if } A_{\mathfrak{p}} \text{ is ramified,} \\ 1 & \text{if } A_{\mathfrak{p}} \text{ is split.} \end{cases}$$

The discriminant $d_F(A)$ is then defined as the formal product of all prime spots $\mathfrak{p}$ of F (including the infinite ones) such that $\left(\frac{A}{\mathfrak{p}}\right) = -1$. The

number of factors of $d_F(A)$ is even, and for any product of an even number of prime spots, there exists a quaternion algebra A having that product as its discriminant. Two quaternion algebras A_1 and A_2 are isomorphic if and only if $d_F(A_1) = d_F(A_2)$ (see [46], théorème III.3.1). We let $d(A)$ denote the product of all finite primes dividing $d_F(A)$, so $d(A)$ is an ideal in P.

If u is an invertible element in A, then the map $A \to A$ given by $x \mapsto uxu^{-1}$ is called an *inner automorphism* of A. The following result, known as the Skolem-Noether Theorem, is central in the theory of simple algebras. For a proof, see for example [35], theorem 7.21.

Proposition 2.4. *Let B be a simple F-subalgebra of A. If $\rho : B \to A$ is a non-trivial algebra homomorphism, then there exists an invertible element $u \in A$ such that $\rho(x) = uxu^{-1}$ for all $x \in B$.*

We formulate a variation of this result, which we will need later.

Lemma 2.5. *Let K be a separable maximal commutative subalgebra of A. If ρ_1 and ρ_2 are embeddings of K into A, then there exists an invertible element $u \in A$ such that $\rho_1(x) = u\rho_2(x)u^{-1}$ for all $x \in K$.*

Proof. If K is a field, then such an element u exists by the Skolem-Noether theorem. Assume therefore that $K \cong F \times F$. Since K has a zero divisors, we have $A \cong M_2(F)$. Fix an identification of K with $F \times F$. It is sufficient to show the claim in the case where ρ_2 is given by $\rho_2(x, y) = \left(\begin{smallmatrix} x & 0 \\ 0 & y \end{smallmatrix}\right)$, for $x, y \in F$. Let now $e_1 = \rho_1(1, 0)$ and $e_2 = \rho_1(0, 1)$. We have $e_1 + e_2 = 1$, $e_1^2 = e_1$, $e_2^2 = e_2$ and $e_1 e_2 = 0$. It is clear that there exists a vector v such that $e_1(v), e_2(v) \neq 0$. The vectors $e_1(v)$ and $e_2(v)$ are linearly independent, and we let u be the invertible matrix with columns given by the vectors $e_1(v)$ and $e_2(v)$. It is straightforward to check that u satisfies the claim. □

If K is a separable maximal commutative subalgebra of A, then

$$K \otimes_F A \cong M_2(K) \tag{2.3}$$

(see e.g. [26]). If K is a field, then K is called a *splitting field* of A.

Definition 2.6. A P-order Λ in A is a subring of A containing P which is a finitely generated P-lattice and such that $F\Lambda = A$.

Let $\Lambda \subset A$ be a P-order and let

$$\Lambda^{\#} = \{x \in A \mid \mathrm{tr}(x\Lambda) \subseteq P\}$$

be the dual lattice of Λ. Now it is well known (see e.g. [4]) that the P-ideal $[\Lambda^{\#} : \Lambda]$ is a square, so

$$[\Lambda^{\#} : \Lambda] = d(\Lambda)^2$$

for some P-ideal $d(\Lambda) \subseteq P$. $d(\Lambda)$ is called the *reduced discriminant* of Λ. If $P = \mathbb{Z}$, then we will for convenience let $d_0(\Lambda)$ denote the positive generator of the ideal $d(\Lambda)$. We will use the symbol $d_0(\Lambda)$ also in other situations when it makes sense, i.e. when it is known that the ideal $d(\Lambda)$ is generated by a rational integer.

2.3 Clifford algebras

We recall now the construction of Clifford algebras. Let L be a P-lattice on the F-vector space V such that $FL = V$. Let

$$q : V \to F$$

be a quadratic form such that $q(L) \subseteq P$. Define the tensor algebras

$$\mathcal{T}(L) = \bigoplus_{k=0}^{\infty} L^{\otimes k} \quad \text{and} \quad \mathcal{T}_0(L) = \bigoplus_{k=0}^{\infty} L^{\otimes 2k}.$$

Let I and I_0 be the ideals in $\mathcal{T}(L)$ and $\mathcal{T}_0(L)$ respectively, generated by all elements $x \otimes x - q(x)$, where $x \in L$. Now $C(L,q) = \mathcal{T}(L)/I$ is called the *Clifford algebra* of (L,q), and $C_0(L,q) = \mathcal{T}_0(L)/I_0$ the *even Clifford algebra* of (L,q).

We can, of course, analogously define F-algebras $C(V,q)$ and $C_0(V,q)$. We have that $C(L,q)$ is a P-order in $C(V,q)$ and that $C_0(L,q)$ is a P-order in $C_0(V,q)$.

Let us now consider ternary quadratic spaces. In this case, the F-algebras $C(V,q_1)$ and $C(V,q_2)$ are isomorphic if and only if the quadratic forms q_1 and q_2 are similar (cf. [31], theorem 58:4). It is well known that if q is a non-degenerate ternary quadratic form, then $C_0(V,q)$ is a quaternion algebra over F. Assume now that P is a principal ideal domain. Let e_1, e_3, e_3 be a P-basis of L and suppose that q is given by

$$q(x_1e_1 + x_2e_2 + x_3e_3) = \sum_{1 \le i \le j \le 3} a_{ij}x_ix_j,$$

where $x_i \in P$. We let $a_{ij} = a_{ji}$ if $i > j$. A P-basis of $C_0(L,q)$ is given by

$$E_0 = 1, \ E_1 = e_2e_3, \ E_2 = e_3e_1, \ E_3 = e_1e_2, \tag{2.4}$$

and straightforward calculations give that multiplication satisfies the rules

$$\begin{aligned} E_i^2 &= a_{jk}E_i - a_{jj}a_{kk}, \\ E_iE_j &= a_{kk}(a_{ij} - E_k), \\ E_jE_i &= a_{1k}E_1 + a_{2k}E_2 + a_{3k}E_3 - a_{ik}a_{jk}, \end{aligned} \tag{2.5}$$

where i, j, k is an even permutation of $1, 2, 3$. The first of these three equations implies that the canonical involution is given by

$$E_i^* = a_{jk} - E_i. \tag{2.6}$$

The matrix associated to the ternary quadratic form q by (2.1) is:

$$M_q = \begin{pmatrix} 2a_{11} & a_{12} & a_{13} \\ a_{12} & 2a_{22} & a_{23} \\ a_{13} & a_{23} & 2a_{33} \end{pmatrix}.$$

We have that $d(q) = (\frac{1}{2} \det M_q) = (a_{12}a_{13}a_{23} - a_{13}^2 a_{22} - a_{11}a_{23}^2 - a_{12}^2 a_{33} + 4a_{11}a_{22}a_{33})$. The following result can be shown by a direct calculation (see [32], Satz 7).

Proposition 2.7. *If $\Lambda = C_0(L, q)$, then the reduced discriminant of Λ is given by $d(\Lambda) = d(q)$.*

We also remark that $C_0(V, q) \cong M_2(F)$ if and only if $q : V \to F$ is isotropic. Assume namely that (V, q) is isotropic. We can choose an F-basis e_1, e_2, e_3 for V such that $q(e_3) = 0$. Then, by (2.5), we get that $E_1 E_2 = 0$, so $C_0(V, q)$ has zero divisors. The converse now follows since isomorphic even Clifford algebras correspond to similar quadratic forms.

2.4 Orders and Clifford algebras

Assume now that P is a principal ideal domain. In this case, any quaternion order Λ over P is isomorphic to the even Clifford algebra of some ternary quadratic form $q : L \to P$. We recall the construction of the lattice L and the form q. We show that the isomorphism $C_0(L, q) \cong \Lambda$ can be realised in a natural way.

Let d_0 be a generator of $d(\Lambda)$. Fix a P-basis $x_0 = 1, x_1, x_2, x_3$ of Λ. We have a corresponding dual basis y_0, y_1, y_2, y_3 of $\Lambda^\#$, which satisfies $tr(x_i y_j^*) = \delta_{ij}$ if $0 \leq i, j \leq 3$.

Let $A_0 = \{x \in A \mid \mathrm{tr}(x) = 0\}$. We define a P-lattice L, by

$$L = \Lambda^\# \cap A_0.$$

Since $x_0 = 1$, it follows directly that $L = \langle y_1, y_2, y_3 \rangle$ (i.e. the P-module generated by y_1, y_2, y_3). We define a quadratic form q on L, by

$$q(l) = d_0 \, \mathrm{nr}(l),$$

for $l \in L$. The following result can be found in [32], Satz 8. Note that it shows, in particular, that $q(l) \in P$ for all $l \in L$.

Proposition 2.8. $\Lambda = \langle 1, d_0 y_2^* y_3, d_0 y_3^* y_1, d_0 y_1^* y_2 \rangle = P + d(\Lambda)\Lambda^{\#}\Lambda^{\#}$.

By proposition 2.8, we can define a P-linear mapping $L \otimes L \to \Lambda$, by

$$l_1 \otimes l_2 \mapsto d_0 l_1^* l_2 \tag{2.7}$$

for $l_1, l_2 \in L$. This map can be uniquely extended to a ring homomorphism $\varphi : \mathcal{T}_0(L) \to A$. It is clear that if $l \in L$, then $\phi(l \otimes l - q(l)) = 0$. Hence ϕ factors through the Clifford algebra $C_0(L, q)$. In fact, by proposition 2.8 again, we have that ϕ is surjective. Hence we have shown:

Corollary 2.9. *The natural ring homomorphism $\phi : C_0(L, q) \to \Lambda$ induced by (2.7) is an isomorphism.*

2.5 Maximal orders in the local case

Assume that F is a local field. In this case, there are only two isomorphism classes of quaternion algebras over F. For the convenience of the reader, we will recall the description of the maximal orders in these two cases.

The following result is proved in [35], theorem 17.3.

Proposition 2.10. *If Λ is a maximal order in $M_2(F)$, then there exists an invertible element $u \in M_2(F)$ such that $\Lambda = uM_2(P)u^{-1}$.*

If $\Lambda = M_2(P)$, then clearly $\Lambda^{\#} = \Lambda$ and $d(\Lambda) = (1)$. A basis of the lattice L constructed in section 2.4 is therefore

$$y_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad y_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad y_3 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},$$

and the ternary quadratic form q is

$$q(x_1 y_1 + x_2 y_2 + x_3 y_3) = -x_1^2 - x_2 x_3,$$

where $x_i \in P$ for $i = 1, 2, 3$. The claim of corollary 2.9 can now be explicitly verified.

Now we turn to the case when A is a skew field. It appears that in this case, A has a unique maximal order. Consider the quadratic form

$$q(x_1 e_1 + x_2 e_2 + x_3 e_3) = \pi x_1^2 - \epsilon x_2^2 - x_2 x_3 - x_3^2$$

on the lattice $L = Pe_1 + Pe_2 + Pe_3$, where $\epsilon \in P$ and $1 - 4\epsilon \in P^* \setminus (P^*)^2$, i.e. the polynomial $x^2 + x + \epsilon$ is irreducible in $F[x]$. We have that q is anisotropic, so the Clifford algebra $\Lambda = C_0(L, q)$ is an order in the unique skew field over F, which we denote A. It has a P-basis $1, E_1, E_2, E_3$, where

$$E_1^2 = -\epsilon - E_1, \quad E_2^2 = \pi, \quad E_3 = E_1 E_2, \quad E_2 E_1 + (E_1 + 1)E_2 = 0, \tag{2.8}$$

by equations (2.5). The norm form can now be computed:

$$\begin{aligned} \mathrm{nr}(a_0 + a_1E_1 + a_2E_2 + a_3E_3) = \\ = a_0^2 - a_0a_1 + \epsilon a_1^2 - \pi(a_2^2 - a_2a_3 + \epsilon a_3^2) \end{aligned} \tag{2.9}$$

for $a_i \in F$.

We claim that $\Lambda = \{\alpha \in A \mid \mathrm{nr}(\alpha) \in P\}$. Take a non-zero element $\alpha \in A$ such that $\mathrm{nr}(\alpha) \in P$. We want to show that $\alpha \in \Lambda$. There is a minimal integer n such that $a = \pi^n\alpha \in \Lambda$. We have $a = \sum_{i=0}^{3} a_iE_i$, where $a_i \in P$ for all i. Assume now that $n \geq 1$. Then we have $\pi^2 \mid \mathrm{nr}(a)$ so, noting that the binary form $a_0^2 - a_0a_1 + \epsilon a_1^2$ (where a_0, $a_1 \in P$) is irreducible modulo π, we get that $\pi \mid a_0$ and $\pi \mid a_1$. But then we get, by the same reasoning, that also $\pi \mid a_2$ and $\pi \mid a_3$. Hence $a = \pi a'$ where $a' \in \Omega$. But this contradicts the minimality of n. Hence we must have $n = 0$, and our claim is proved. In fact, we have shown the following well known result (see [35], theorem 12.5):

Proposition 2.11. *If F is a local field and the quaternion algebra A over F is a skew field, then $\Lambda = \{x \in A \mid \mathrm{nr}(x) \in P\}$ is the unique maximal order in A.*

If p is a prime, then we let Ω_p denote the unique maximal order in the unique skew field $\mathbb{H}_p$ over $\mathbb{Q}_p$.

We now state some results about ideals in maximal orders. If J is a Λ-ideal, then we let $\mathrm{nr}(J)$ denote the P-ideal generated by all elements $\mathrm{nr}(j)$, where $j \in J$. The following result is theorem 18.3 in [35]:

Proposition 2.12. *If Λ is a maximal order, then Λ has a unique maximal two-sided ideal I_m. If A is split, then $I_m = \pi\Lambda$, and if A is a skew field, then $I_m = \Lambda g$ for any $g \in \Lambda$ with $v(\mathrm{nr}(g)) = v(\pi)$. Furthermore, any two-sided ideal I is a power of I_m. In particular, we get in the case $A = M_2(F)$ that $I = \mathfrak{i}\Lambda$, where $\mathfrak{i}$ is the P-ideal $\mathfrak{i} = I \cap F$.*

We immediately get the following corollary, which also holds in the global case:

Corollary 2.13. *If J is a two-sided ideal in a maximal order Λ, then J can be uniquely written in of the form $J = \mathfrak{i}J_0$, where $\mathfrak{i}$ is an ideal in P, and J_0 is a two sided ideal in Λ with $\mathrm{nr}(J_0)$ dividing $d(\Lambda)$.*

The following elementary result will be useful in the sequel. If $b \in A$ with $b \neq 0$, define the ideal

$$m_\Lambda(b) = \{x \in F \mid xb \in \Lambda\}. \tag{2.10}$$

Lemma 2.14. *If* $\Lambda \cong M_2(P)$ *and* $a, b \in \Lambda$ *with* $m_\Lambda(b) = P$, *then* $\Lambda a \Lambda \subseteq b\Lambda$ *if and only if* $a \in \mathrm{nr}(b)\Lambda$.

Proof. Assume that $m_\Lambda(b) = P$, i.e. $b \in \Lambda$ and $b \notin \pi\Lambda$. By proposition 2.12, we have $\Lambda a \Lambda = \pi^n \Lambda$ for some integer n. We get $\Lambda a \Lambda \subseteq b\Lambda$ if and only if $\pi^n \Lambda \subseteq b\Lambda$ if and only if $\pi^n b^* \Lambda \subseteq \mathrm{nr}(b)\Lambda$ if and only if $b \in \pi^{-n}\,\mathrm{nr}(b)\Lambda$. By the hypothesis on b, this is equivalent to $\pi^n \in (\mathrm{nr}(b))$. The claim follows. □

2.6 Classification of orders

In this section, we recall some concepts and results about the classification of orders in quaternion algebras.

An order Λ is said to be a *Gorenstein order* (see [9], §37), if $\Lambda^\#$ is projective as left (or equivalently right) Λ-module. If Λ is an order, then there exists a minimal Gorenstein order containing Λ, which we denote by $G(\Lambda)$. We have

$$\Lambda = P + \mathfrak{b} G(\Lambda) \tag{2.11}$$

for some P-ideal $\mathfrak{b} \subseteq P$ (see [3], prop. 1.4). The order $\Lambda = C_0(L, q)$ (see section 2.3) is a Gorenstein order if and only if (L, q) is a primitive form (see [4]).

An order Λ is called *hereditary*, if every (left) Λ-module is projective. An order is hereditary if and only if the discriminant $d(\Lambda)$ is square free (see e.g. [3], proposition 1.2). An order Λ is called *Bass order* if every order Λ' containing Λ is a Gorenstein order. If $d(\Lambda)$ is cube free, then Λ is a Bass order ([3], corollary 1.5). An order Λ is a Gorenstein (Bass) order if and only if $\Lambda_\mathfrak{p}$ is a Gorenstein (Bass) order for every prime ideal $\mathfrak{p}$ (see [9], §37). We say that being Gorenstein (Bass) is a local property.

Assume now that F is local. Recall that $J(\Lambda)$ denotes the Jacobson radical of Λ, i.e. the intersection of the maximal left (or right) ideals of Λ. Any idempotent of $\Lambda/J(\Lambda)$ can be lifted to Λ (see proposition IV.2.2 in [36]).

$\Lambda/J(\Lambda)$ is a semi-simple algebra, by lemma I.4.17 in [36]. An order Λ is said to be an *Azumaya order*, if $\Lambda/J(\Lambda)$ is a non-trivial central simple algebra over $\widehat{P}$. We have that $\pi\Lambda \subseteq J(\Lambda)$, so $\Lambda/J(\Lambda)$ is a $\widehat{P}$-vector space with $\dim_{\widehat{P}} \Lambda/J(\Lambda) \leq 4$. If Λ is Azumaya, then we must have $\Lambda/J(\Lambda) \cong M_2(\widehat{P})$, since there are no skew fields over a finite field (see theorem III.6.7 in [36]). By lifting idempotents of $\Lambda/J(\Lambda)$ to Λ, it is possible to construct an isomorphism $\Lambda \cong M_2(P)$.

Definition 2.15. If Λ is a Gorenstein order which is not Azumaya, then

the Eichler invariant $e(\Lambda)$ is defined by

$$e(\Lambda) = \begin{cases} -1 & \text{if } \Lambda/J(\Lambda) \text{ is a quadratic field extension if } \widehat{P}, \\ 1 & \text{if } \Lambda/J(\Lambda) \cong \widehat{P} \times \widehat{P}, \\ 0 & \text{if } \Lambda/J(\Lambda) \cong \widehat{P}. \end{cases}$$

One can verify that the cases in definition 2.15 in fact cover all possibilities for $\Lambda/J(\Lambda)$.

Proposition 2.16. *If Λ is an order with $e(\Lambda) = \pm 1$, then Λ is a Bass order. If $e(\Lambda) = 1$ and $d(\Lambda) = (\pi^n)$, for some integer $n \geq 1$, then Λ is isomorphic to the order*

$$\begin{pmatrix} P & P \\ \pi^n P & P \end{pmatrix}.$$

For a proof, see e.g. [3], propositions 2.1 and 3.1. The second statement follows once again from the existence of a pair of orthogonal idempotents in Λ.

2.7 Resolution of orders

Assume that F is a local field. Let (L, q) be a ternary quadratic space over P, $\Lambda = C_0(L, q)$ and d_0 a generator of the ideal $d(\Lambda)$. Let $\widehat{L} = L/\pi L$. We have that $\widehat{L} \cong \widehat{P}^3$ as a $\widehat{P}$-vector space. Consider now the reduction $\widehat{q}$ of the quadratic form q modulo (π):

$$\widehat{q} : \widehat{L} \to \widehat{P}.$$

Proposition 2.17. *The quadratic form $\widehat{q}$ gives the following information about the order Λ:*

i) *if* $\operatorname{rk} \widehat{q} = 3$, *then* $\Lambda \cong M_2(P)$,

ii) *if* $\operatorname{rk} \widehat{q} = 2$ *and* $\widehat{q}$ *is irreducible, then* $e(\Lambda) = -1$,

iii) *if* $\operatorname{rk} \widehat{q} = 2$ *and* $\widehat{q}$ *is reducible, then* $e(\Lambda) = 1$,

iv) *if* $\operatorname{rk} \widehat{q} = 1$, *then* $e(\Lambda) = 0$,

v) *if* $\widehat{q} = 0$, *then* Λ *is not Gorenstein.*

Proof. If $\widehat{q} = 0$, then (L, q) is not a primitive form, and hence $C_0(L, q)$ is not a Gorenstein order.

Assume now that $\widehat{q} \neq 0$. Let M be the null space of $\widehat{q}$, so the quadratic form $\widehat{L}/M \to \widehat{P}$ is non-degenerate. We clearly have a surjective ring homomorphism $\Lambda \to C_0(\widehat{L}/M, \widehat{q})$. Since $C_0(\widehat{L}/M, \widehat{q})$ is a simple algebra, this gives a surjection

$$\Lambda/J(\Lambda) \to C_0(\widehat{L}/M, \widehat{q}). \tag{2.12}$$

Considering the possible isomorphism classes of the two rings $\Lambda/J(\Lambda)$ and $C_0(\widehat{L}/M, \widehat{q})$, the only possible case when the map (2.12) could fail to be an isomorphism is if $\Lambda/J(\Lambda) \cong \widehat{P} \times \widehat{P}$ and $C_0(\widehat{L}/M, \widehat{q}) \cong \widehat{P}$, i.e. if $e(\Lambda) = 1$ and $\mathrm{rk}(\widehat{q}) = 1$. But from proposition 2.16, it follows directly that if $e(\Lambda) = 1$, then $\mathrm{rk}(\widehat{q}) = 2$. Hence we have that the map (2.12) is an isomorphism and the claim follows. □

The proofs of the following results can be found in [3]:

Proposition 2.18. *If $e(\Lambda) = 1$, then Λ is a Bass order. If $d(\Lambda) = (\pi^n)$, then $\Lambda \cong \left(\begin{smallmatrix} P & P \\ \pi^n P & P \end{smallmatrix}\right)$. There exists exactly two minimal over-orders Λ' of Λ. We have that $[\Lambda' : \Lambda] = (\pi)$ and $e(\Lambda_i) = 1$ if Λ' is not maximal. There are exactly 2^n chains of orders*

$$\Lambda = \Lambda_0 \subset \Lambda_1 \subset \cdots \subset \Lambda_n$$

such that Λ_{i+1} is a minimal order containing Λ_i for $i = 0, 1, \ldots, n-1$, and Λ_n a maximal order. Every maximal order containing Λ occurs in such a chain. Furthermore, Λ is the intersection of two uniquely defined maximal orders.

Proposition 2.19. *If $e(\Lambda) = -1$, then Λ is a Bass order. If Λ is not hereditary, then there is a unique minimal order Λ' containing Λ. It satisfies $[\Lambda' : \Lambda] = (\pi^2)$, and if Λ' is not maximal, then $e(\Lambda') = -1$. Furthermore $J(\Lambda) = \pi\Lambda'$.*

Corollary 2.20. *If $e(\Lambda) = -1$, then there is a unique chain of orders*

$$\Lambda = \Lambda_0 \subset \Lambda_1 \subset \cdots \subset \Lambda_n$$

such that $[\Lambda_{i+1} : \Lambda_i] = (\pi^2)$ and $e(\Lambda_i) = -1$ for $i = 0, 1, \ldots, n-1$, and Λ_n is a maximal order.

If Λ is a Gorenstein order with $e(\Lambda) = 0$, then Λ is not necessarily a Bass order.

Proposition 2.21. *If $e(\Lambda) = 0$, then Λ has a uniquely determined over-order Λ' with $[\Lambda' : \Lambda] = (\pi)$. If Λ is not hereditary and Λ' is Gorenstein, then $e(\Lambda') = 0$.*

Corollary 2.22. *If $e(\Lambda) = 0$ and Λ is a Bass order, then there is a unique chain of orders*

$$\Lambda = \Lambda_0 \subset \Lambda_1 \subset \cdots \subset \Lambda_n$$

such that $[\Lambda_{i+1} : \Lambda_i] = (\pi)$, $e(\Lambda_i) = 0$ for $i = 0, 1, \ldots, n-1$, and $d(\Lambda_n) = (\pi)$.

If Λ is a Bass order with $e(\Lambda) = -1$ or 0, then the first hereditary order in the chain of orders in corollary 2.20 or corollary 2.22 respectively, is called the *hereditary closure* of Λ and is denoted $H(\Lambda)$. We also have that $H(\Lambda)$ is the intersection of all hereditary orders containing Λ.

We now prove two results which show how the minimal over-orders of a Gorenstein order can be computed. We state the results locally for simplicity, but the point is that they can immediately be applied in the global case and hence give an algorithm to compute the maximal orders which contain a given order.

Proposition 2.23. *Let Λ be an order with $e(\Lambda) = 0$ or $e(\Lambda) = 1$. Let $l : \widehat{L} \to \widehat{P}$ be a linear factor of the reducible quadratic form $\widehat{q}$. Take 2 generators of $\ker l$, and let e_1 and e_2 be liftings of these elements to L. Then we have that*

$$\Lambda' = \Lambda + \frac{1}{\pi} d(\Lambda) e_1^* e_2$$

is an over-order of Λ with $[\Lambda' : \Lambda] = (\pi)$. This order only depends on the choice of l. If $e(\Lambda) = 1$ and $\widehat{q} = l_1 l_2$, then the two over-orders constructed using l_1 and l_2 respectively are different.

Proof. There is an element e_3 such that e_1, e_2, e_3 is a basis of L. The quadratic form q on L is given by $q(x) = d_0 \operatorname{nr}(x)$. We have $q(ae_1 + be_2) \in (\pi)$ for all $a, b \in P$. We define $L' = \langle e_1, e_2, \pi e_3 \rangle$, with quadratic form $q'(x) = \pi^{-1} d_0 \operatorname{nr}(x)$. It is clear that q' is integral. The natural images, i.e. the images of the maps ϕ given by corollary 2.9, of the orders $C_0(L, q)$ and $C_0(L', q')$ are $\Lambda = \langle 1, d_0 e_1^* e_2, d_0 e_1^* e_3, d_0 e_2^* e_3 \rangle$ and $\Lambda' = \langle 1, \pi^{-1} d_0 e_1^* e_2, d_0 e_1^* e_3, d_0 e_2^* e_3 \rangle$ respectively. The claim follows.

Consider the case $e(\Lambda) = 1$ and assume that $\widehat{q} = l_1 l_2$. We can choose a basis e_1, e_2, e_3 for L such that $l_1(e_1) = l_2(e_2) = l_1(e_3) = l_2(e_3) = 0$. The orders we get are $\Lambda + \frac{1}{\pi} d(\Lambda) e_1^* e_3$ and $\Lambda + \frac{1}{\pi} d(\Lambda) e_2^* e_3$ respectively, and these are clearly different. □

Proposition 2.24. *Let Λ be a non-hereditary order with $e(\Lambda) = -1$. If e_1 is a primitive element of L such that $q(e_1) \in (\pi)$, then we have that*

$$\Lambda' = \Lambda + \frac{1}{\pi} d(\Lambda) e_1 L$$

is the unique over-order of Λ with $[\Lambda' : \Lambda] = (\pi^2)$.

Proof. Since e_1 is a primitive element of L, we can choose a P-basis e_1, e_2, e_3 of L. Let $b(x,y) = q(x+y) - q(x) - q(y)$ be the bilinear form on L associated to q. Using that the form $\widehat{q}$ is irreducible of rank 2, it is straightforward to verify that the matrix $M = (b(e_i, e_j))$ must be of the form

$$M = \begin{pmatrix} 2q(e_1) & \pi a_{12} & \pi a_{13} \\ \pi a_{12} & 2a_{22} & a_{23} \\ \pi a_{13} & a_{23} & 2a_{33} \end{pmatrix},$$

where $a_{ij} \in P$. Since the rank of $\widehat{q}$ is 2, we get that $4a_{22}a_{33} - a_{23}^2 \in P^*$. Furthermore, we have that $2\pi^2 \mid \det(M)$, since Λ is not hereditary. Since we now have $\det M \equiv 2q(e_1)(4a_{22}a_{33} - a_{23}^2) \pmod{2\pi^2}$, we get $\pi^2 \mid q(e_1)$. Hence, if we define the lattice $L' = \langle e_1, \pi e_2, \pi e_3 \rangle$ with quadratic form $q'(x) = \pi^{-2} d_0 \operatorname{nr}(x)$, we have that q' is integral. The natural images of the orders $C_0(L,q)$ and $C_0(L',q')$ are $\Lambda = \langle 1, d_0 e_1^* e_2, d_0 e_1^* e_3, d_0 e_2^* e_3 \rangle$ and $\Lambda' = \langle 1, \pi^{-1} d_0 e_1^* e_2, \pi^{-1} d_0 e_1^* e_3, d_0 e_2^* e_3 \rangle$ respectively. Thus

$$\Lambda' = \Lambda + \frac{1}{\pi} d(\Lambda) e_1^* e_2 + \frac{1}{\pi} d(\Lambda) e_1^* e_3 = \Lambda + \frac{1}{\pi} d(\Lambda) e_1^* L = \Lambda + \frac{1}{\pi} d(\Lambda) e_1 L \qquad \square$$

2.8 Eichler orders

Definition 2.25. An order Λ is an *Eichler order* if it is an intersection of two maximal orders.

The following characterisation of Eichler orders, was first proved by Eichler in [12]. We give a proof for completeness.

Lemma 2.26. *An order Λ is an Eichler order if and only if the following holds for every prime ideal $\mathfrak{p}$ in P: $\Lambda_\mathfrak{p}$ is a maximal order or a Bass order with $e(\Lambda_\mathfrak{p}) = 1$.*

Proof. Assume that the local conditions are satisfied. Then the existence of two maximal orders Λ_1, Λ_2 such that $\Lambda = \Lambda_2 \cap \Lambda_2$ follows from proposition 2.18.

Assume that $\Lambda \subset A$ is an Eichler order and $\mathfrak{p}$ a prime ideal. If $A_\mathfrak{p}$ is a skew field, then $A_\mathfrak{p}$ contains a unique maximal order, so $\Lambda_\mathfrak{p}$ must be maximal. Assume that $A_\mathfrak{p}$ is split. Let $\Lambda = \Lambda_1 \cap \Lambda_2$, where Λ_1 and Λ_2 are maximal. We have $\Lambda_1 \cong M_2(P_\mathfrak{p})$, so we can identify Λ_1 with $M_2(P_\mathfrak{p})$. Now, by proposition 2.4, there exists $x \in A^*$ such that $\Lambda_2 = x\Lambda_1 x^{-1}$. We may assume that x is a primitive element of Λ_1, and hence $x = \epsilon_1 x_0 \epsilon_2$, where $\epsilon_1, \epsilon_2 \in \Lambda_1^*$ and $x_0 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & r \end{smallmatrix}\right)$ with $r \in P_\mathfrak{p}$. We get

$$\Lambda = \Lambda_1 \cap x\Lambda x^{-1} = \epsilon_1(\Lambda_1 \cap x_0 \Lambda_1 x_0^{-1})\epsilon_1^{-1} = \epsilon_1 \begin{pmatrix} P_\mathfrak{p} & P_\mathfrak{p} \\ rP_\mathfrak{p} & P_\mathfrak{p} \end{pmatrix} \epsilon_1^{-1}.$$

Thus $\Lambda_\mathfrak{p}$ is maximal if $\mathfrak{p} \nmid r$, and $e(\Lambda_\mathfrak{p}) = 1$ if $\mathfrak{p} \mid r$. We are done. □

Lemma 2.27. *Let Λ be an Eichler order in a quaternion algebra A and assume that $d(\Lambda) = d(A)N_0$, where $N_0 \subseteq P$ is an ideal. Let a be the number of different prime ideals dividing N_0. There are 2^a maximal orders Λ_1 containing Λ, such that there exist some maximal order Λ_2 with $\Lambda = \Lambda_1 \cap \Lambda_2$.*

Proof. Follows directly from proposition 2.18. □

Lemma 2.28. *If $\Lambda/\mathbb{Z}$ is an Eichler order in an indefinite quaternion algebra, then $\mathrm{nr} : \Lambda \to \mathbb{Z}$ is surjective.*

Proof. Consider the map $\mathrm{nr} : \Lambda \to \mathbb{Z}$ as a quaternary quadratic form. This form is then indefinite, so, by theorem 1.5 in [7] (see also theorem 3.8 in the next chapter), it is sufficient to show that $\mathrm{nr} : \Lambda_p \to \mathbb{Z}_p$ is surjective for every prime p. But this follows immediately from the local description of an Eichler order given in lemma 2.26. □

2.9 Primitive orders

Let S be a maximal order in a quadratic separable F-algebra K.

Definition 2.29. We say that an order Λ is *S-primitive* if there exists an embedding of S into Λ.

If an order is S-primitive for some S, then it is a Bass order. This follows immediately from (2.11). The following result follows from proposition 1.12 and remark 1.16 in [5]:

Proposition 2.30. *Assume that P is a local ring and that Λ is an S-primitive order which is not Azumaya. If K/F is unramified, then $e(\Lambda) = -1$. If K/F is split, then $e(\Lambda) = 1$. If K/F is ramified and Λ is not hereditary, then $e(\Lambda) = 0$. Furthermore, assume that $d(\Lambda) = (\pi^n)$, where $n \in \mathbb{Z}$. Then:*

i) If $e(\Lambda) = -1$, then $\Lambda = S + J(H(\Lambda))^m$, where $m = n/2$ if $H(\Lambda)$ is an Azumaya algebra, and $m = n - 1$ otherwise.

ii) If $e(\Lambda) = 0$, then $\Lambda = S + J(H(\Lambda))^m$, where $m = n - 1$.

If Λ_1 and Λ_2 are two S-primitive orders, then by conjugating one of these orders if necessary, we may (by lemma 2.5) arrange so that they both contain the same copy of S. Hence the situation is

$$\begin{array}{ccc} \Lambda_1 & \subset & A \\ \cup & & \cup \\ S & \subset & \Lambda_2 \,. \end{array} \tag{2.13}$$

Lemma 2.31. *Assume that F is a local field, and that K is a field. Let Λ_i be two non-maximal S-primitive orders in a quaternion algebra A. Then $H(\Lambda_1) \cong H(\Lambda_2)$.*

Proof. If A is a skew field, then there is nothing to prove since A contains a unique hereditary order. Assume that $A \cong M_2(F)$. If K/F is an unramified field extension, then $e(\Lambda_i) = -1$, for $i = 1, 2$, by proposition 2.30. Hence we get that $H(\Lambda_i) \cong M_2(P)$ by corollary 2.20 and we are done. If K is a ramified field, then we get, for $i = 1, 2$, that $e(\Lambda_i) = 0$, and hence that $H(\Lambda_i)$ is a non-maximal hereditary order by corollary 2.22. Such orders must have Eichler invariant equal to 1, and hence they are isomorphic to $\left(\begin{smallmatrix} P & P \\ \pi P & P \end{smallmatrix}\right)$. □

We have the following result, which is a version of the Eichler-Hasse-Noether-Chevalley-Schilling theorem (cf. [13], Satz 7):

Proposition 2.32. *Let S be a maximal order in a separable maximal commutative subalgebra K of A, and let Λ_1, Λ_2 be two isomorphic orders in A containing S. Then there exists a non-trivial ideal $\mathfrak{i} \subseteq S$ such that $\mathfrak{i}\Lambda_1 = \Lambda_2\mathfrak{i}$.*

Proof. We only need to check this locally. If K is split, then we may identify A with $M_2(F)$. We can assume, by lemma 2.5, that the embedding of $S \cong P \times P$ is given by $S = \left(\begin{smallmatrix} P & 0 \\ 0 & P \end{smallmatrix}\right)$. We get that the orders Λ_j are of the form $\Lambda_j = \left(\begin{smallmatrix} P & a_j P \\ b_j P & P \end{smallmatrix}\right)$, for $j = 1, 2$, where $a_j, b_j \in F$. Since $\Lambda_1 \cong \Lambda_2$, we get that $(a_1 b_1) = (a_2 b_2) \subseteq P$. It is now clear that if we choose an invertible element $g \in S$ of the form $g = x\left(\begin{smallmatrix} a_2 & 0 \\ 0 & a_1 \end{smallmatrix}\right)$, where $x \in F$, then $g\Lambda_1 = \Lambda_2 g$.

Assume now that K is a field. If the orders Λ_j are hereditary, then the claim follows by theorem 1.8 in [6] (it states that the embedding numbers $e_*(S, \Lambda_j)$ (defined therein) are equal to 1, which gives the claim).

Assume that the orders are not hereditary. By proposition 2.30, we have that $e(\Lambda_1) = e(\Lambda_2) \neq 1$. We get, by proposition 2.30, that there exists an integer m such that

$$\Lambda_j = S + J(H(\Lambda_j))^m,$$

for $i = 1, 2$. We have that $H(\Lambda_1) \cong H(\Lambda_2)$, by lemma 2.31, but we know that the assertion holds in the hereditary case, and hence we have that $gH(\Lambda_1) = H(\Lambda_2)g$ for some invertible element $g \in S$. Consequently, we get $gJ(H(\Lambda_1)) = J(H(\Lambda_2))g$, and we are done. □

Proposition 2.33. *Let F be a local field, K a separable maximal commutative subalgebra of A and S a maximal order of K. Let $\Lambda_1, \Lambda_2 \subset A$ be two S-primitive orders. If $d(\Lambda_1) = d(\Lambda_2)$, then $\Lambda_1 \cong \Lambda_2$.*

Proof. If the orders are maximal, then there is nothing to prove. Assume that the orders are non-maximal. We can assume without loss of generality that the situation is as in diagram (2.13). By lemma 2.31, we have that $H(\Lambda_1) \cong H(\Lambda_2)$, and hence there exists, by proposition 2.32, an invertible element $g \in S$ such that $gH(\Lambda_1)g^{-1} = H(\Lambda_2)$. We get, for a suitable integer m as in proposition 2.30, that $g\Lambda_1 g^{-1} = g(S + J(H(\Lambda_1))^m)g^{-1} = S + J(H(\Lambda_2))^m = \Lambda_2$. □

2.10 Automorphisms of orders

In this section, we present some results about normalisers and automorphisms of orders which we will need later. If A is a quaternion algebra, then we let ν denote the map $A^* \to \mathrm{Aut}(A)$ given by $\nu(w) = (x \mapsto wxw^{-1})$. We define the *normaliser* of Λ:

$$N(\Lambda) = \{w \in A^* \mid w\Lambda w^{-1} = \Lambda\}.$$

It is clear that $\mathrm{Aut}(\Lambda) = \nu(N(\Lambda))$. The proof of the following result can be found in [5] (see theorem 2.2).

Proposition 2.34. *Assume that F is a local field. If $\Lambda \cong M_2(P)$, then $\mathrm{Aut}(\Lambda) = \nu(\Lambda^*)$. If Λ is a Bass order with $e(\Lambda) = \pm 1$, then $[\mathrm{Aut}(\Lambda) : \nu(\Lambda^*)] = 2$, and*

$$\mathrm{Aut}(\Lambda) = \nu(\Lambda^* \cup \Lambda^* s),$$

where $s \in \Lambda$ is as follows: If $e(\Lambda) = 1$, then $\Lambda \cong \left(\begin{smallmatrix} P & P \\ \pi^n P & P \end{smallmatrix}\right)$ and we let s be the element which corresponds to the matrix $\left(\begin{smallmatrix} 0 & 1 \\ \pi^n & 0 \end{smallmatrix}\right)$ under this isomorphism. Assume now that $e(\Lambda) = -1$. If A is a skew field, then s is any generator of $J(H(\Lambda))$. If A is split, then s is a suitable element in $H(\Lambda)^* \setminus \Lambda^*$.

Lemma 2.35. *If F is a number field and Λ is a P-order, then $[N(\Lambda) : F^*\Lambda^1] < \infty$.*

Proof. From theorem 55.19 and theorem 55.22 in [10], it follows that

$$[N(\Lambda) : F^*\Lambda^*] < \infty.$$

Now we have an exact sequence of groups:

$$(1) \to P^*\Lambda^1 \to P^*\Lambda^* \to P^*/(P^*)^2,$$

where the last map is given by $x \mapsto \mathrm{nr}(x)(P^*)^2$. By Dirichlet's theorem, we have that $P^*/(P^*)^2$ is finite, and hence we get $[P^*\Lambda^* : P^*\Lambda^1] < \infty$. It follows that $[F^*\Lambda^* : F^*\Lambda^1] < \infty$, and we are done. □

3 Quadratic forms

In this chapter, we state some preparatory results on quadratic forms that we will need later. Most of the results are of course well known. One thing that can be mentioned though, is that the natural correspondence between quaternion orders and Clifford algebras described in corollary 2.9, gives a natural correspondence between quadratic orders in the quaternion order and rank 2 sublattices of the ternary quadratic lattice. This is lemma 3.4.

3.1 Oriented binary forms

Let L be a $\mathbb{Z}$-lattice. Two bases $e_1, \ldots, e_n$ and $f_1, \ldots, f_n$ of L are said to have the same orientation, if the map $g : L \to L$, induced by $g(e_i) = f_i$ for all i, satisfies $\det(g) = 1$. By an oriented $\mathbb{Z}$-lattice, we mean a lattice together with a choice of orientation, i.e. with a basis that is declared to have positive orientation. Let L_1 and L_2 be two oriented lattices. We say that an isomorphism $g : L_1 \to L_2$ is orientation preserving, if $g(e_1), \ldots, g(e_n)$ is a positive basis of L_2 for any positive basis $e_1, \ldots, e_n$ of L_1.

An oriented integral binary form on L is a pair (L, q), where L is an oriented lattice of rank 2 over $\mathbb{Z}$ with some positive basis e_1, e_2, and $q : L \to \mathbb{Z}$ is a map

$$xe_1 + ye_2 \mapsto ax^2 + bxy + cy^2 \tag{3.1}$$

for all $x, y \in \mathbb{Z}$, where $a, b, c \in \mathbb{Z}$. We say that two oriented binary forms (L_1, q_1) and (L_2, q_2) are equivalent if there exists an orientation preserving isomorphism $f : L_1 \to L_2$ such that $q_1 = q_2 \circ f$. We write $q_1 \cong q_2$. The oriented binary form obtained by reversing orientation of the underlying lattice of q is denoted by $\overline{q}$. We write $q_1 \simeq q_2$ if $q_1 \cong q_2$ or $q_1 \cong \overline{q}_2$.

If the choice of an oriented basis e_1, e_2 is clear from the context, then the oriented binary form (3.1) will be denoted by $q = [a, b, c]$. If $q \cong [a, b, c]$, then we let $d_0(q)$ denote the generator $b^2 - 4ac$ of the discriminant ideal $d(q)$. The form q is positive definite if and only if $d_0(q) < 0$ and $a > 0$. The content $m(q)$ of the form q is the ideal generated by a, b and c. If $m(q) = (1)$, then we say that q is a primitive form.

Definition 3.1. If $N < 0$, then we let $h(N)$ denote the number of equivalence classes of primitive positive definite oriented binary forms q with $d_0(q) = N$.

Now it can be shown that any positive definite binary form is equivalent to a unique form $[a, b, c]$ satisfying $-a \leq b < a$, $c \geq a$ and $c > a$ if $b > 0$

(see [48], p. 121). Hence $h(N)$ is finite for all $N < 0$, and

$$h(N) = \#\{(a,b,c) \in \mathbb{Z}^3 \,|\, N = b^2 - 4ac,\ (a,b,c) = 1, \\ -a \leq b < a,\ c \geq a \text{ and } c > a \text{ if } b > 0\}$$

Clearly $h(N) = 0$ if $N \equiv 2, 3 \pmod 4$.

3.2 Binary forms and quadratic orders

Let K be a complex quadratic field with non-trivial automorphisms $x \mapsto \overline{x}$ and with a choice of orientation. By this we mean that we have chosen a $\mathbb{Q}$-basis x_1, x_2 of K, and we say that any other $\mathbb{Q}$-basis y_1, y_2 of K is *positive* if the change of basis matrix has positive determinant. Let $\mathcal{O}$ be an order in K. Let $N = d(\mathcal{O})$ be the discriminant of $\mathcal{O}$, so N is a negative integer. We have that $K \cong \mathbb{Q}(\sqrt{N})$, and $\mathcal{O}$ is the unique order with discriminant N in K. An $\mathcal{O}$-module M is a subgroup of K such that $\mathcal{O}M = M$, M is finitely generated over $\mathcal{O}$ and $\mathbb{Q}M = K$. From now on, we only consider $\mathcal{O}$-modules which satisfy

$$\mathcal{O} = \{x \in K \mid xM = M\}.$$

We say that a $\mathbb{Z}$-basis m_1, m_2 of M is positive if it is positive as a $\mathbb{Q}$-basis of K. Note that m_1, m_2 is positive basis if and only if $1, \overline{m}_1 m_2$ is positive $\mathbb{Q}$-basis of K. We say that two $\mathcal{O}$-modules M and M' are equivalent if there exists an element $\alpha \in K$ such that $\alpha M = M'$. We let $\mathrm{cl}(\mathcal{O})$, or alternatively $\mathrm{cl}(N)$, denote the number of equivalence classes of $\mathcal{O}$-modules.

Take an oriented quadratic binary lattice (L, q), with $q(x_1 e_1 + x_2 e_2) = ax_1^2 + bx_1x_2 + cx_2^2$, where e_1, e_2 is a positive basis of L. Consider the even Clifford algebra $C_0(L,q) = \mathbb{Z}[e_1e_2]$. If we let $z = e_1e_2$, then a calculation gives that $z^2 - bz + ac = 0$ and hence the discriminant of the quadratic order $C_0(L,q)$ is $d_0(q)$. Furthermore, we can choose an orientation of $C_0(L,q)$ by declaring that $1, e_1e_2$ is a positive basis. Observe that this orientation is well defined, i.e. it only depends on the orientation of L.

A classical result by Gauss says that $h(N) = \mathrm{cl}(N)$ (see [48], p. 94). As an illustration of some techniques that will be used later in this work, we will now show this fact using Clifford algebras (cf. [27]).

Let us fix an oriented $\mathbb{Z}$-lattice L with a positive basis e_1, e_2. We will now give a one-to-one correspondence between equivalence classes of primitive forms with discriminant N on L and equivalence classes of $\mathcal{O}$-modules.

Let $q : L \to \mathbb{Z}$ be a primitive form with $d_0(q) = N$. Consider the Clifford algebra $C(L,q)$. It has a $\mathbb{Z}$-basis $1, e_1, e_2, e_1e_2$. It naturally contains a copy

of $C_0(L,q)$ and L respectively, so we have maps

$$\begin{array}{ccc} C_0(L,q) & \longrightarrow & C(L,q) \\ & & \uparrow \\ & & L \end{array}$$

It is clear, that this gives L a natural structure as a $C_0(L,q)$-module, since L is the odd part of $C(L,q)$. Furthermore, there exists a unique orientation preserving isomorphism of orders $\delta : C_0(L,q) \to \mathcal{O}$. Hence, we can associate to q the $\mathcal{O}$-module

$$M_q = \delta(e_1 L).$$

The converse mapping is the obvious one: Let M be an $\mathcal{O}$-module. Choose a positive $\mathbb{Z}$-basis m_1, m_2 of M and define a quadratic form $q_M : L \to \mathbb{Z}$ by

$$q_M(x_1 e_1 + x_2 e_2) = c\,\mathrm{nr}(x_1 m_1 + x_2 m_2),$$

where c is the unique positive rational number which makes this form primitive integral.

It is clear that these maps are also well defined on classes of binary forms and $\mathcal{O}$-modules respectively. We claim that they are inverses of each other. That the form q_{M_q} is equivalent to q is clear, since we have

$$\mathrm{nr}_{K/\mathbb{Q}}(\delta(e_1 l)) = l e_1 e_1 l = q(e_1) q(l),$$

for every $l \in L$. Conversely, we want to show that the $\mathcal{O}$-module M_{q_M} is equivalent to M. It is clear that the map $\delta : C_0(L, q_M) \to \mathcal{O}$ is induced by the map $L \otimes L \to \mathcal{O}$ given by:

$$x \otimes y \mapsto c\overline{g(x)}g(y),$$

where $g : L \to M$ is such that $g(x_1 e_1 + x_2 e_2) = x_1 m_1 + x_2 m_2$, for $x_1, x_2 \in \mathbb{Z}$. Hence, we get

$$\delta(e_1 L) = (c\overline{m}_1)M,$$

which shows the claim.

3.3 Some results on binary forms

We make a few observations about binary forms over the integers $\mathbb{Z}$ that we will need later. The following result is well known (see e.g. [7], p. 165, example 14):

Lemma 3.2. *If q is a definite oriented binary form with non-trivial automorphisms (i.e. with more than two automorphisms), then $q \cong mq_0$, where m is an integer and $q_0(x,y) = x^2 + y^2$ or $q_0(x,y) = x^2 + xy + y^2$.*

Lemma 3.3. *Let $\Delta < -4$ be an integer and r an odd prime with $r \nmid \Delta$. If (L,q) is a primitive binary form representing r and with discriminant Δ, then any other such form is equivalent to q or $\overline{q}$. Furthermore, if $q \cong \overline{q}$, then q represents r exactly four times and if $q \ncong \overline{q}$, then both q and $\overline{q}$ represent r exactly twice.*

Proof. Take $e_1 \in L$ with $q(e_1) = r$. Then it clearly exists $e_2 \in L$ such that e_1, e_2 is a basis of L and

$$q(xe_1 + ye_2) = rx^2 + bxy + cy^2, \tag{3.2}$$

where $-r < b < r$ and $c = (b_0^2 - \Delta)/(4r)$. Now we have $b^2 \equiv \Delta \pmod{4r}$, and this congruence has exactly two solutions b modulo $2r$. Hence the presentation in (3.2) is unique up to the sign of b.

Assume now that q represents r more than twice, so $q(e_1') = r$ for some $e_1' \neq \pm e_1$. Then, by the above, there exists e_2' such that $q(xe_1' + ye_2') = rx^2 + \alpha bxy + cy^2$, where $\alpha = \pm 1$. We know that q has no non-trivial automorphisms by lemma 3.2, since $\Delta < -4$. Hence we conclude that $\alpha = -1$, which means that $\overline{q} \cong q$. We also see that q cannot represent r more than four times, for otherwise we could construct a non-trivial automorphism of (L,q).

Assume now that $\overline{q} \cong q$, so there exists $g : L \to L$ such that $\det(L) = 1$ and $q(g(xe_1 + ye_2)) = rx^2 - bxy + cy^2$. Since we have $b \neq 0$ by hypothesis, it is clear that we must have $g(e_1) \neq \pm e_1$. Hence q represents r four times. □

3.4 Quadratic orders in quaternion orders

As before, we let P be a principal ideal domain and F its field of fractions. A is a quaternion algebra over F and $\Lambda \subset A$ a P-order. Let L, d and q be as in section 2.4. The isomorphism $\phi : C_0(L,q) \to \Lambda$ is as in corollary 2.9.

A lattice $M \subseteq L$ is said to be *optimally embedded* in L if $M = FM \cap L$. A P-order S in an algebra over F of dimension 2 is called a quadratic order over P. If S is a quadratic order with $S \subset \Lambda$, then S is called *optimally embedded* if $S = FS \cap \Lambda$.

Lemma 3.4. *There is a natural bijection between optimally embedded sublattices $M \subseteq L$ of rank 2 and optimally embedded quadratic orders $S \subseteq \Lambda$. It is given by*

$$M \mapsto S_M := C_0(M, q|_M),$$

where $C_0(M, q|_M)$ is naturally embedded as a subalgebra of $C_0(L, q) = \Lambda$. The inverse mapping is given by

$$S \mapsto M_S := \{x \in L \mid \mathrm{tr}(Sx^*) = (0)\}.$$

Proof. Let d_0 be a generator of $d(\Lambda)$. Take an optimally embedded sublattice $M \subseteq L$ of rank 2. We want to show that S_M is optimally embedded in Λ. Choose a P-basis m_1, m_2 of M. Since M is optimally embedded in L, we can extend it to a P-basis m_1, m_2, l of L, and hence

$$1,\ d_0 m_1^* m_2,\ d_0 m_2^* l,\ d_0 l^* m_1$$

is a P-basis of Λ. Now we have $S_M = P[\omega]$, where $\omega = d_0 m_1^* m_2$, and hence S_M is optimally embedded in Λ. Furthermore, it is clear that $\mathrm{tr}(\omega m_1^*) = \mathrm{tr}(\omega m_2^*) = 0$, so $M \subseteq M_{S_M}$. But M is optimally embedded and hence we have equality $M = M_{S_M}$.

Conversely, assume that S is optimally embedded in Λ with a generator ω_S, so $S = P[\omega_S]$. It is clear that M_S is an optimally embedded sublattice of L. Let $m_1,\ m_2$ be a basis of M_S and put $w = d_0 m_1^* m_2$. Then

$$\omega_S \omega = \omega_S d_0 m_1^* m_2 = -d_0 m_1 \omega_S^* m_2 = d_0 m_1 m_2^* \omega_S = \omega \omega_S.$$

Now $F[\omega_S]$ is a maximal commutative subalgebra of A and hence $F[\omega_S] = F[\omega]$. Since both $P[\omega_S]$ and $P[\omega]$ are optimally embedded in Λ, we get

$$P[\omega] = F[\omega] \cap \Lambda = F[\omega_S] \cap \Lambda = P[\omega_S],$$

i.e. $S = S_{M_S}$. □

3.5 Embedding numbers

Let P, F and A be as in section 3.4, and let K be a separable quadratic F-algebra. Let $\Lambda \subseteq A$ and $S \subseteq K$ be P-orders.

We say that an embedding $f : S \to \Lambda$ is *optimal* if the image of f is optimally embedded in Λ, i.e. $f(S) = (Ff(S)) \cap \Lambda$. Let

$$E = \{f \mid f : S \to \Lambda \text{ is an optimal embedding}\}.$$

The units $\lambda \in \Lambda^*$ act on E by

$$(\lambda \cdot f)(q) = \lambda f(q) \lambda^{-1}.$$

Let $e(S, \Lambda)$ denote the number of orbits in E under this action. It is called the *embedding number* of S into Λ.

Let now $F = \mathbb{Q}$ and $P = \mathbb{Z}$. If p is a prime, then for simplicity we often write $e_p(S, \Lambda)$ for $e(S_p, \Lambda_p)$. We have the following result:

Proposition 3.5. *If Λ is an Eichler order over $\mathbb{Z}$, then*

$$e(S,\Lambda) = h(S) \prod_{p \text{ prime}} e_p(S,\Lambda).$$

For a proof, see [46], théorème III.5.11. (In the formulation in [46] of that result there is a constant h, but it follows from theorem 5.2.11 in [30] that $h = 1$ in the case of Eichler orders.) To use proposition 3.5, we need to be able to compute the local embedding numbers $e_p(S,\Lambda)$. In the case of hereditary orders, they are given by:

Proposition 3.6. *Let p be a prime, $F = \mathbb{Q}_p$ and $P = \mathbb{Z}_p$.*

i) *If $\Lambda \cong M_2(\mathbb{Z}_p)$, then $e(S,\Lambda) = 1$ for every S.*

ii) *If $\Lambda \cong \begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$, then $e(S,\Lambda) = 2$ if K is split, and if K is a field we have*

$$e(S,\Lambda) = \begin{cases} 2 & \text{if } S \text{ is non-maximal,} \\ 1 & \text{if } S \text{ is maximal and } K/F \text{ is ramified,} \\ 0 & \text{if } S \text{ is maximal and } K/F \text{ is unramified.} \end{cases}$$

iii) *If $\Lambda \cong \Omega_p$, then $e(S,\Lambda) = 0$ if K is split, and if K is a field we have*

$$e(S,\Lambda) = \begin{cases} 2 & \text{if } S \text{ is maximal and } K/F \text{ is unramified,} \\ 1 & \text{if } S \text{ is maximal and } K/F \text{ is ramified,} \\ 0 & \text{if } S \text{ is non-maximal.} \end{cases}$$

For a proof of these results, we refer to [46] and [6].

The next lemma deals with a related type of embedding numbers which, in the case that we will consider, coincides with the above.

Lemma 3.7. *Let Λ be an Eichler order in an indefinite quaternion algebra over $\mathbb{Q}$, and let S be a complex quadratic order over $\mathbb{Z}$. Let the group Λ^1 act by conjugation on the set of optimally embedded orders $S' \subseteq \Lambda$ with $S' \cong S$. The number of orbits is then $e(S,\Lambda)$.*

Proof. Let

$$E' = \{S' \mid S' \subseteq \Lambda,\ S' \cong S \text{ and } S' = (\mathbb{Q}S') \cap \Lambda\}.$$

We want to show that $\#(E'/\Lambda^1) = \#(E/\Lambda^*)$.

Since Λ is an indefinite Eichler order, there exists $\lambda \in \Lambda$ with $\mathrm{nr}(\lambda) = -1$. Assume that $f : S \to \Lambda$ is an optimal embedding such that $\lambda \cdot f = f$. Then λ commutes with all elements in $f(S)$. But $\mathbb{Q}f(S)$ is a maximal commutative subalgebra of A, so we must have $\lambda \in \mathbb{Q}f(S)$. Now, $\mathbb{Q}f(S)$ is a complex field, which contradicts $\mathrm{nr}(\lambda) = -1$. Hence we have $\#(E/\Lambda^1) = 2\#(E/\Lambda^*)$

Take now $S' \in E'$ and $\lambda \in \Lambda^1$. Assume that $\lambda s \lambda^{-1} = s^*$ for every $s \in S'$. Take $j \in S'$ with $j^* = -j$ and $j \neq 0$. We have $\lambda j - j^* \lambda = 0$, but also $\lambda j + j^* \lambda^* = \mathrm{tr}(\lambda j) \in \mathbb{Z}$, so we get $j^*(\lambda + \lambda^*) \in \mathbb{Z}$. Hence $\lambda + \lambda^* = 0$, so $\lambda^2 = -1$. We get $A = \mathbb{Q}(\lambda, j)$, where $\lambda^2 < 0$, $j^2 < 0$ and $\lambda j = -j\lambda$, but this contradicts that A is indefinite. We conclude that $\#(E/\Lambda^1) = 2\#(E'/\Lambda^1)$, and we are done. □

3.6 Some results on quaternary quadratic forms

We list some results about quaternary quadratic forms for future reference. First we cite the very important result concerning the numbers represented by indefinite quaternary quadratic forms over $\mathbb{Z}$. It is theorem 1.5 in [7]:

Theorem 3.8. *Let q be a non-degenerate indefinite integral form in $n \geq 4$ variables and let $N \neq 0$ be an integer. Suppose that N is represented by q over all $\mathbb{Z}_p$. Then N is represented by q over $\mathbb{Z}$.*

Further, let P be a finite set of primes and for $p \in P$ let $\beta_p \in \mathbb{Z}_p^n$ be any representation of N. Then there is $\beta \in \mathbb{Z}^n$ representing N such that β is arbitrarily close to β_p for every $p \in P$.

We also have a simple local result:

Lemma 3.9. *Let (L, q) be a unimodular quaternary quadratic lattice over $\mathbb{Z}_p$. Let M be rank 2 sublattice of L with L/M torsion free, and let $M^\perp$ denote the orthogonal complement of M in L. Let $\varphi = q|_M$, $\varphi^\perp = q|_{M^\perp}$ and assume that φ is non-degenerate. Then we have $d(\varphi) = d(\varphi^\perp)$ and $m(\varphi) = m(\varphi^\perp)$.*

Proof. Let $q(x) = \frac{1}{2}b(x, x)$, where b is a symmetric bilinear form on L. Since φ is non-degenerate, we have that $M + M^\perp$ is a sublattice of L of rank 4. We want to show that

$$[L : M + M^\perp] = d(\varphi). \tag{3.3}$$

If (3.3) is true, then we get $d(\varphi) = d(\varphi^\perp)$ by symmetry.

Let e_1, e_2 be a $\mathbb{Z}_p$-basis of M, and extend it to a $\mathbb{Z}_p$-basis e_1, e_2, e_3, e_4 of L. Let Q be the 4×4 matrix $(b(e_i, e_j))$ and write $Q = \left(\begin{smallmatrix} A & B \\ B^t & C \end{smallmatrix}\right)$, where A, B and C are 2×2 blocks. We have $d(\varphi) = (\det(A))$. Identifying L with

column vectors, we have that M is the column space of the 4×2 matrix $\left(\begin{smallmatrix} I \\ 0 \end{smallmatrix}\right)$. Using that (L, q) is unimodular, it is straightforward to check that it is always possible to arrange so that the matrix B is invertible by changing the basis if necessary (consider the column space of the two top rows of the reduced matrix $\widehat{Q} \in M_4(\widehat{P})$). We get that $M^\perp$ is the column space of $\left(\begin{smallmatrix} -I \\ B^{-1}A \end{smallmatrix}\right)$. Hence $[L : M + M^\perp] = (\det(A))$, and we have proved (3.3).

Assume now that $m(\varphi) = (m)$, $m \in \mathbb{Z}_p$. From the description of $M^\perp$ above, we have that $M^\perp \subseteq \mathbb{Z}_p e_1 + \mathbb{Z}_p e_2 + \mathbb{Z}_p m e_3 + \mathbb{Z}_p m e_4$, and hence we get $q(x) \equiv 0 \pmod{m}$ for all $x \in M^\perp$. Therefore, $m(\varphi) \mid m(\varphi^\perp)$. But then, by symmetry, we also must have $m(\varphi^\perp) \mid m(\varphi)$, and we are done. □

4 Involutions

In this chapter, k is a quadratic field over $\mathbb{Q}$, whose non-trivial automorphism is denoted by $x \mapsto \overline{x}$, and R is the ring of integers in k. We let A be a quaternion algebra over k. We investigate under which conditions on A there exists a so called involution τ of *type* 2 on A. Let Λ be a maximal order in A. We define what we mean by τ being *optimal* respectively *special* with respect to Λ. We prove that for every maximal order Λ, there exists an involution which is special with respect to Λ.

4.1 Algebras with involutions

Definition 4.1. An *involution of type* 2 on A is a map $\tau : A \to A$ such that $\tau^2(a) = a$, $\tau(a + b) = \tau(a) + \tau(b)$, $\tau(ab) = \tau(a)\tau(b)$ and $\tau(xa) = \overline{x}\tau(a)$ for all $a, b \in A$ and $x \in k$.

First we observe that if τ is any involution of type 2, then it commutes with the canonical involution on A, i.e.

$$\tau(a^*) = \tau(a)^* \tag{4.1}$$

for all $a \in A$. To see this, note first that τ preserves the center k of A. Now, if $a \in A \setminus k$, then a^* is uniquely determined by the conditions that $a + a^* \in k$ and $aa^* \in k$. We get $\tau(a) + \tau(a^*) \in k$ and $\tau(a)\tau(a^*) \in k$ which shows that $\tau(a^*)$ satisfies the conditions which characterise $\tau(a)^*$, and hence (4.1) is proved. For completeness, we prove the following well-known result (see [39], theorem 7.4, p. 301):

Lemma 4.2. *Let τ and ν be two involutions of type 2 on A. Then there exists an invertible element $m \in A$ such that $\tau(m)^* = m$ and $\nu(a) =$*

$m^{-1}\tau(a)m$ *for all* $a \in A$. *Furthermore, if* m_1 *is another invertible element in* A *satisfying* $\tau(m_1)^* = m_1$ *and* $\nu(a) = m_1^{-1}\tau(a)m_1$ *for all* $a \in A$, *then there exists* $r \in \mathbb{Q}$ *such that* $m_1 = rm$.

Proof. Consider the map $\nu \circ \tau$. This is a k-linear automorphism of A so, by the Skolem-Noether theorem (proposition 2.4), there exists an invertible element $n \in A$ such that $\nu \circ \tau(a) = nan^{-1}$ for all $a \in A$. Since τ is an involution, we get that

$$\nu(a) = n^{-1}\tau(a)n$$

for all $a \in A$. Now if we use that $\nu \circ \nu$ is a the identity, we get that $a = (\tau(n)n)^{-1}a\tau(n)n$ for all $a \in A$, and hence that $\tau(n)n \in k$, the center of A. This implies that

$$\tau(n) = \alpha n^*$$

for some $\alpha \in k$. If we now apply τ and the canonical involution to this equality, we get $n^* = \overline{\alpha}\tau(n)$ and hence $\alpha\overline{\alpha} = 1$. By Hilbert's theorem 90 (see [26], p. 34) there exists $\rho \in k$ such that $\alpha = \rho/\overline{\rho}$. If we let $m = \rho n$, it is clear that m satisfies the claim.

Consider now an alternative element m_1. We get that $a = \nu(\nu(a)) = (\tau(m)m_1)^{-1}a\tau(m)m_1$ for all $a \in A$. Hence $\tau(m)m_1 \in k$, so $m_1 = \alpha\tau(m)^* = \alpha m$, where $\alpha \in k$. We get $m_1 = \tau(m_1)^* = \overline{\alpha}\tau(m)^* = \overline{\alpha}m$, so $\overline{\alpha} = \alpha$ and thus $\alpha \in \mathbb{Q}$. □

If there exists an involution τ of type 2 on A, then we can define

$$A_\tau = \{a \in A \mid \tau(a) = a\}.$$

It is clear that A_τ is a $\mathbb{Q}$-subalgebra of A. We have $\sqrt{d}A_\tau = \{a \in A \mid \tau(a) = -a\}$, so $A = A_\tau \oplus \sqrt{d}A_\tau$, since τ is an involution. Hence A_τ has dimension 4 over $\mathbb{Q}$. Furthermore, we have $A = kA_\tau$ and hence A_τ must be a simple algebra, since A is a simple algebra.

Conversely, suppose there exists a $\mathbb{Q}$-subalgebra $A_\mathbb{Q} \subset A$, which is a quaternion algebra. We claim that $kA_\mathbb{Q} = A$. Assume that this is not the case. Then there exist non-trivial elements $a_1, a_2 \in A_\mathbb{Q}$ such that $a_2 = \sqrt{d}a_1$. But $A_\mathbb{Q}$ is simple, hence we get $A_\mathbb{Q} = \sqrt{d}A_\mathbb{Q}$, which implies that $k \subset A_\mathbb{Q}$. Since k is the center of A, we conclude that the 2-dimensional k-algebra $A_\mathbb{Q}$ is commutative, a contradiction. Now $A = kA_\mathbb{Q}$ implies that $A \cong k \otimes_\mathbb{Q} A_\mathbb{Q}$, and we can define a natural involution on $k \otimes_\mathbb{Q} A_\mathbb{Q}$ by

$$x \otimes a \mapsto \overline{x} \otimes a.$$

Hence A has an involution of type 2.

The following lemma gives the relation between the discriminants of A and $A_\mathbb{Q}$ respectively if $A \cong k \otimes_\mathbb{Q} A_\mathbb{Q}$.

Lemma 4.3. *A is ramified at a prime spot q of k if and only if $q \neq \overline{q}$ and $p = q\overline{q}$ is a split prime spot of $\mathbb{Q}$ such that $(A_{\mathbb{Q}})_p$ is ramified.*

Proof. If p is a prime spot of $\mathbb{Q}$ such that $(A_{\mathbb{Q}})_p \cong M_2(\mathbb{Q}_p)$ and q is a prime spot of $\mathbb{Q}$ above p, then it is clear that $A_q \cong M_2(k_q)$.

Assume now that p is a prime spot such that $(A_{\mathbb{Q}})_p$ is isomorphic to the skew field $\mathbb{H}_p$ over $\mathbb{Q}_p$. If p is split, that is $p = q_1q_2$ with $q_1 \neq q_2$, then $k_{q_i} \otimes_{\mathbb{Q}} A_{\mathbb{Q}} \cong \mathbb{Q}_p \otimes_{\mathbb{Q}} A_{\mathbb{Q}} \cong \mathbb{H}_p$, so A is ramified at q_i for $i = 1, 2$. Assume now that p is an unramified or ramified prime spot. Consider first the case $p = \infty$. Then k is a complex field so $k_\infty \otimes_{\mathbb{Q}} A_{\mathbb{Q}} \cong \mathbb{C} \otimes_{\mathbb{R}} \mathbb{H} \cong M_2(\mathbb{C})$. Let p be a finite prime. Then we know that the field k_p can be embedded into $\mathbb{H}_p$ (see proposition 3.6). Hence, we have $k_p \otimes_{\mathbb{Q}_p} \mathbb{H}_p \cong M_2(k_p)$. □

If A is a quaternion algebra over k with ramification as described in the lemma, then clearly it is possible to choose a quaternion algebra $A_{\mathbb{Q}}$ over $\mathbb{Q}$ such that A and $k \otimes_{\mathbb{Q}} A_{\mathbb{Q}}$ are ramified at the same set of spots. Hence A and $k \otimes_{\mathbb{Q}} A_{\mathbb{Q}}$ are isomorphic (see [46], théorème III.3.1). We have now shown:

Proposition 4.4. *If A is a quaternion algebra over a quadratic field k, then the following properties are equivalent:*

i) *A has an involution of type 2;*

ii) *A contains a rational quaternion subalgebra;*

iii) *A is ramified at a finite number of pairs of conjugated (different) prime spots of k.*

4.2 Subalgebras corresponding to involutions

Let τ be an involution of type 2 on A. Take an invertible element $\beta \in A$ and consider the map $\theta : A \to A$ given by

$$\theta(a) = \beta^{-1}\tau(a)\beta.$$

θ satisfies $\theta(xa) = \overline{x}\theta(a)$ for all $x \in k$ and $a \in A$. Define

$$A_{\tau,\beta} = \{a \in a \mid \theta(a) = a\}.$$

It is clear that $A_{\tau,\beta}$ is a $\mathbb{Q}$-algebra.

Lemma 4.5. *The natural map $g : k \otimes_{\mathbb{Q}} A_{\tau,\beta} \to A$ is injective.*

Proof. Let $f_1, \ldots, f_t$ be a $\mathbb{Q}$-basis of $A_{\tau,\beta}$. Assume that $x = \sum x_i \otimes f_i$ is a non-trivial element of $k \otimes_{\mathbb{Q}} A_{\tau,\beta}$ which maps to 0, i.e. $g(x) = \sum x_i f_i = 0$. We can without loss of generality assume that $x_1 = 1$. Since we have $\theta(f_i) = f_i$ for all i, we get $0 = g(x) + \theta(g(x)) = \sum \mathrm{tr}_{k/\mathbb{Q}}(x_i) f_i$. This contradicts the fact that the f_i's are linearly independent over $\mathbb{Q}$, since $\mathrm{tr}_{k/\mathbb{Q}}(x_1) = 2 \neq 0$. □

If we put $B = kA_{\tau,\beta} \subseteq A$, then B is a k-subalgebra of A. By lemma 4.5, we have

$$B \cong k \otimes_{\mathbb{Q}} A_{\tau,\beta}$$

and hence $\dim_k B = \dim_{\mathbb{Q}} A_{\tau,\beta}$. Now it is clear that $\dim_{\mathbb{Q}} A_{\tau,\beta} = 4$ if and only if θ is an involution. Since $\theta^2(a) = (\tau(\beta)\beta)^{-1} a (\tau(\beta)\beta)$, we get that θ is an involution if and only if $\tau(\beta)\beta$ is an element of the center k of A.

Assume that θ is not an involution. We have that $\theta(\tau(\beta)\beta) = \tau(\beta)\beta$, so $\tau(\beta)\beta \in A_{\tau,\beta}$. Since $\tau(\beta)\beta \notin k$, we conclude that

$$\dim_{\mathbb{Q}} A_{\tau,\beta} \geq 2.$$

It is not possible to have $\dim_{\mathbb{Q}} A_{\tau,\beta} = 3$. To see this, consider the map $\theta^2 : A \to A$, which is an inner automorphism given by $a \mapsto (\tau(\beta)\beta)^{-1} a \tau(\beta)\beta$. But θ^2 acts trivially on B, so $\tau(\beta)\beta$ commutes with all elements in the 3-dimensional k-subalgebra B. But then $\tau(\beta)\beta$ must commute with all elements in A and hence $\tau(\beta)\beta \in k$, a contradiction. Thus we have proved:

Proposition 4.6. *$A_{\tau,\beta}$ is either a quaternion algebra over $\mathbb{Q}$ or a 2-dimensional $\mathbb{Q}$-subalgebra of A. The former happens if and only if $\tau(\beta)\beta \in k$.*

4.3 Orders and involutions

Let τ be an involution of type 2 on A and $\Lambda \subset A$ a maximal R-order.

Definition 4.7. We let Λ_τ denote the order consisting of elements fixed under the involution, i.e.

$$\Lambda_\tau = \{\lambda \in \Lambda \mid \tau(\lambda) = \lambda\}.$$

In other words, we have $\Lambda_\tau = \Lambda \cap A_\tau$. The situation is

$$\begin{array}{ccc} R & \longrightarrow & \Lambda \\ \uparrow & & \uparrow \\ \mathbb{Z} & \longrightarrow & \Lambda_\tau \,. \end{array}$$

It is clear that, in general, the isomorphism class of Λ_τ depends on τ. However, in the constructions that we will do it will be important to choose an

involution with certain good properties. For a given maximal order Λ, it is in general not so clear what should be considered as the best choice of involution τ. The ideal situation is if τ can be chosen to be optimal in the following sense:

Definition 4.8. We say that an involution τ on A is *optimal* with respect to a maximal order Λ if $d(\Lambda_\tau) = d(\Lambda) \cap \mathbb{Z}$.

Locally, for any maximal order there exists an optimal involution. Globally, this is in general not true. To see this, consider for example any algebra A which is ramified at an odd number of pairs of prime spots in k. But it need not be possible even if A is ramified at an even number of pairs of prime spots. Consider for example the case where $A \cong M_2(k)$, but $\Lambda \ncong M_2(R)$ (such orders exist for some fields k). If τ is optimal, then $\Lambda_\tau \cong M_2(\mathbb{Z})$, which gives that $\Lambda \supseteq R\Lambda_\tau \cong M_2(R)$, so we get a contradiction.

It turns out that it is most important to have good behaviour of Λ_τ at those prime spots that divide $D = d(k)$.

Definition 4.9. We say that an involution τ of type 2 on a maximal order Λ is *special*, if for all primes p such that $p \mid D$, we have $(\Lambda_\tau)_p \cong M_2(\mathbb{Z}_p)$.

Note that the involution is special if and only if $d(\Lambda_\tau)$ and D are relatively prime. Another way to formulate this, is to say that $\tau : A_p \to A_p$ is optimal with respect to Λ_p for all primes p, which are ramified in k.

Lemma 4.10. *Let A be a quaternion algebra over a real quadratic field and assume that it exists an involution of type 2 on A. If Λ is a maximal order in A, then there exists an involution of type 2 on A which is special with respect to Λ.*

Proof. Let τ be some involution of type 2 on A. Let p be a prime ramified in k, so $R_p = \mathbb{Z}_p + \sqrt{d}\mathbb{Z}_p$. From lemma 4.3, we know that $A_p \cong M_2(k_p)$ and hence we get that the maximal order Λ_p is isomorphic to $M_2(R_p)$ by proposition 2.10. We fix such an isomorphism. We let ι_p denote the natural involution on $M_2(k_p)$, which is given by element-wise conjugation on the entries of the matrices $x \in M_2(k_p)$. By lemma 4.2, there exists an element $m_p \in A_p$ such that $\tau(m_p)^* = m_p$ and $\iota_p(x) = m_p^{-1}\tau(x)m_p$ for all $x \in A_p$. Let t_p be an integer such that $p^{t_p}m_p^{-1} \in 2p\Lambda_p$.

If we let $W = \{x \in A \mid \tau(x)^* = x\}$, then $m_p \in W_p$ for all p. Choose now an element $\beta \in W$ such that $\beta - m_p \in p^{t_p}\Lambda_p$ for all ramified primes p. Define an involution of type 2 on A by

$$\nu(x) = \beta^{-1}\tau(x)\beta.$$

We want to show that ν is a special involution with respect to Λ. Let

$$\Lambda_\nu = \{\lambda \in \Lambda \mid \nu(\lambda) = \lambda\}.$$

Let again p be a prime ramified in k. If we let $\gamma_p = m_p^{-1}\beta$, then $\nu(\lambda) = \gamma_p^{-1}\iota_p(\lambda)\gamma_p$ for all $\lambda \in \Lambda_p$ and $\iota_p(\gamma_p)^* = \gamma_p$. Now $\gamma_p - 1 = m_p^{-1}(\beta - m_p) \in p^{t_p}m_p^{-1}\Lambda_p \subseteq 2p\Lambda_p$, so $\gamma_p = a_p + 2\sqrt{d}b_p$, where $a_p \in \mathbb{Z}_p^*$ and $b_p \in pM_2(\mathbb{Z}_p)$ with $b_p^* = -b_p$. We have $(\Lambda_\nu)_p = \{\lambda \in \Lambda_p \mid \iota_p(\lambda)\gamma_p = \gamma_p\lambda\}$. If we write $\lambda = x + \sqrt{d}y$ with $x, y \in M_2(\mathbb{Z}_p)$, then $\iota_p(\lambda)\gamma_p = \gamma_p\lambda$ if and only if $yb_p + b_py = a_py + b_px - xb_p = 0$. It is straightforward to verify that we can define a $\mathbb{Z}_p$-linear map $g_p : M_2(\mathbb{Z}_p) \to (\Lambda_\nu)_p$ by

$$g_p(x) = x + \frac{\sqrt{d}}{a_p}(xb_p - b_px).$$

We get $\mathrm{nr}_{\Lambda_p/R_p}(g_p(x)) = xx^* + da_p^{-2}\,\mathrm{nr}_{\Lambda_p/R_p}(b_px - xb_p)$, which gives that

$$\mathrm{nr}_{\Lambda_p/R_p}(g_p(x)) \equiv \det(x) \pmod{p}$$

for all $x \in M_2(\mathbb{Z}_p)$. But the determinant form on $M_2(\mathbb{Z}_p)$ has discriminant 1, and hence the norm form on $(\Lambda_\nu)_p$ has discriminant 1 too. Hence $(\Lambda_\nu)_p \cong M_2(\mathbb{Z}_p)$ and we are done. □

We formulate a local result on optimal involutions in a special case, which we will need later.

Lemma 4.11. *If p is a prime such that $p \mid d(\Lambda)$, then any involution τ on Λ_p is optimal. Furthermore, there exists an isomorphism $\Omega_p \times \Omega_p \to \Lambda_p$ such that the induced involution on $\Omega_p \times \Omega_p$ is given by $\tau(x, y) = (y, x)$ for all $(x, y) \in \Omega_p \times \Omega_p$.*

Proof. We can identify Λ_p with $\Omega_p \times \Omega_p$ and let ι be the involution given by $\iota(x, y) = (y, x)$ for all $(x, y) \in \Omega_p \times \Omega_p$. By lemma 4.2, there exists $m = (b, b^*)$ such that $\tau(\lambda) = m^{-1}\iota(\lambda)m^{-1}$ for all $\lambda \in \Lambda_p$. We get that $\Lambda_\tau = \{(x, y) \in \Omega_p \times \Omega_p \mid yb = bx\} \cong \Omega_p$, so τ is optimal.

We clearly have $R_p\Lambda_\tau \subseteq \Lambda_p$, but on the other hand we have that $R_p\Lambda_\tau$ is a maximal order, hence we get $\Lambda_p = R_p\Lambda_\tau$. The claim follows. □

We conclude this section with a result which will be used to construct involutions on the surfaces that we will study.

Lemma 4.12. *Let τ be an involution of type 2 on A such that Λ_τ is an Eichler order. Then there exists an element $s \in \Lambda_\tau$ such that $s\tau(\Lambda)s^{-1} = \Lambda$, $s^2 \in \mathbb{Z}\Lambda_\tau^1$ and $\mathrm{nr}(s) > 0$.*

Proof. We write $d_0(\Lambda_\tau) = N_0N_1N_2$, where N_0 contains those primes p which are unramified in k and satisfy $(\Lambda_\tau)_p \cong \Omega_p$, N_1 contains those primes p which are split in k and $e((\Lambda_t)_p) = 1$, and N_2 all other prime factors.

We claim that if $p \nmid N_0N_1$, then $\tau(\Lambda_p) = \Lambda_p$. If $(\Lambda_\tau)_p \cong M_2(\mathbb{Z}_p)$, then $\Lambda_p = R_p(\Lambda_\tau)_p$, so the claim follows. If k_p is a field and $e((\Lambda_\tau)_p) = 1$, then the claim follows from proposition 2.18. Namely, this result implies that we may identify A_p with $M_2(k_p)$ in such a way that τ_p is given by element-wise conjugation and $(\Lambda_\tau)_p$ is given by $\left(\begin{smallmatrix} P & P \\ \pi^n P & P \end{smallmatrix}\right)$. It follows from proposition 2.18, that every maximal R_p-order containing $(\Lambda_\tau)_p$ is invariant under τ. If p is split in k and $(\Lambda_\tau)_p \cong \Omega_p$, then the claim follows from lemma 4.11. Finally, if p is ramified in k and $(\Lambda_\tau)_p \cong \Omega_p$, then by corollary 2.20 we have that the R_p-order $R_p(\Lambda_\tau)_p$ is contained in a unique maximal R_p-order, so the claim follows.

Now we want to construct the element s. If $p \mid N_0$, choose an element $s_p \in (\Lambda_\tau)_p$ with $\nu_p(\mathrm{nr}(s_p)) = 1$. If $p \mid N_1$, let $s_p \in (\Lambda_\tau)_p$ be as in proposition 2.34. Define the $\mathbb{Z}$-lattice

$$M = \bigcap_{p \mid N_0N_1} (\Lambda_\tau \cap (\Lambda_\tau)_p s_p) \subset A_\tau.$$

Consider the integral indefinite quaternary form $\mathrm{nr} : M \to \mathbb{Z}$. It is clear that this form represents N_0N_1 locally for every prime p, and hence there exists by theorem 3.8 an element $s \in M$ such that $\mathrm{nr}(s) = N_0N_1$. We have $(N_0N_1)^{-1}s^2 \in (\Lambda_\tau)_p$ for every prime p, and hence $s^2 \in N_0N_1\Lambda^1$. We need to show that

$$s\tau(\Lambda_p)s^{-1} = \Lambda_p \tag{4.2}$$

for every prime p.

If $p \nmid N_0N_1$, then the claim follows directly by the above, since s is a unit in $(\Lambda_\tau)_p$.

Consider now the case $p \mid N_0$. We get that $R_p\Lambda_\tau$ is a hereditary R_p-order with $e(R_p\Lambda_\tau) = 1$. Hence $R_p\Lambda_\tau$ is included in exactly two maximal orders, namely Λ_p and $\tau(\Lambda_p)$. Furthermore, s does not normalise neither Λ_p nor $\tau(\Lambda_p)$, since $v_p(\mathrm{nr}(s))$ is odd. Hence (4.2) holds in this case.

Consider finally the case $p \mid N_1$. We identify Λ_p with $M_2(\mathbb{Z}_p) \times M_2(\mathbb{Z}_p)$. Let ι be the involution of type 2 on Λ_p which is given by $\iota(x, y) = (y, x)$. There is $\beta_0 \in \Lambda_p$ satisfying $\iota(\beta_0)^* = \beta_0$ such that $\tau(\lambda) = \beta_0^{-1}\iota(\lambda)\beta_0$ for all $\lambda \in \Lambda_p$. We can assume that $\beta_0 = (m, m^*)$, where $m \in M_2(\mathbb{Z}_p)$ is a primitive element. We must then have $\det(m)\mathbb{Z}_p = N_1\mathbb{Z}_p$. We can therefore

write $m = \epsilon_1 \left(\begin{smallmatrix} 1 & 0 \\ 0 & N_1 \end{smallmatrix}\right) \epsilon_2$, where $\epsilon_1, \epsilon_2 \in M_2(\mathbb{Z}_p)^*$. We get

$$\begin{aligned}(\Lambda_\tau)_p &= \{\lambda \in \Lambda_p \mid \beta_0 \lambda = \iota(\lambda)\beta_0\} = \\ &= \{(x, mxm^{-1}) \mid x \in M_2(\mathbb{Z}_p) \cap m^{-1} M_2(\mathbb{Z}_p) m\} = \\ &= \{(x, mxm^{-1}) \mid x \in \epsilon_2^{-1} \begin{pmatrix} \mathbb{Z}_p & N_1\mathbb{Z}_p \\ \mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix} \epsilon_2\}.\end{aligned}$$

Proposition 2.34 implies that s is of the form

$$s = (\epsilon_2^{-1} \begin{pmatrix} a_{11}N_1 & a_{12}N_1 \\ a_{21} & a_{22}N_1 \end{pmatrix} \epsilon_2, \epsilon_1 \begin{pmatrix} a_{11}N_1 & a_{12} \\ a_{21}N_1 & a_{22}N_1 \end{pmatrix} \epsilon_1^{-1}),$$

where $a_{ij} \in \mathbb{Z}_p$ and $a_{12}a_{21} \in \mathbb{Z}_p^*$. Now if follows that $s\beta_0^{-1} \in \Lambda_p^*$, so

$$s\tau(\Lambda_p)s^{-1} = s\beta_0^{-1}\iota(\Lambda_p)\beta_0 s^{-1} = s\beta_0^{-1}\Lambda_p(s\beta_0^{-1})^{-1} = \Lambda_p. \qquad \square$$

5 Hermitian structures

In this chapter, we consider two different questions.

We introduce the concept of an integral Λ-hermitian form, where Λ is a maximal order in a quaternion k-algebra A having an involution of type 2, where k is a real quadratic field. We compute the number of local classes of such forms in sections 5.2 to 5.5. We want to make clear that the main cases are already proved by Hausmann in [20], so this should essentially be considered as a reformulation of his results to make them better adopted to our situation.

In the sections 5.6 and 5.7, we consider a construction of orders from hermitian planes. We prove that there is a certain one-to-one correspondence in the local case. A useful corollary is that the orders that we construct in chapter 7 are Bass orders.

5.1 Preliminaries on hermitian lattices

In this section, we will recall the basic concepts on hermitian lattices. Let P, F, S and K be as in section 2.1.

Let V be a finite dimensional vector space over K. A map $h : V \times V \to K$ is called a hermitian form on V if it satisfies the following properties: $h(x+y,z) = h(x,z) + h(y,z)$, $h(ax,y) = ah(x,y)$ and $h(y,x) = \overline{h(x,y)}$ for all $x, y, z \in V$, $a \in K$.

It is well known that any hermitian form has an orthogonal basis, i.e. there exists a K-basis $e_1, \ldots, e_n$ of V such that $h(e_i, e_j) = 0$ if $i \neq j$.

Let L be a finitely generated S-lattice in V. If h restricts to an S-valued function on L, i.e. $h : L \times L \to S$, then (L, h) will be called a hermitian lattice. If L has rank 1, then we call (L, h) a *hermitian line*. If the rank of L is 2, then L is called a *hermitian plane*.

Take two hermitian lattices (L_1, h_1) and (L_2, h_2). An isomorphism $g : L_1 \to L_2$ of S-modules is called a *similarity* if there exists an element $a \in F^*$ such that $h_1(x, y) = ah_2(g(x), g(y))$ for all $x, y \in L_1$. If $a = 1$, then g is an *isometry* and we say that L_1 and L_2 are isometric.

If $e_1, \ldots, e_n$ is an S-basis of L, and $x = \sum_i x_i e_i$ and $y = \sum_i y_i e_i$ are two arbitrary elements of L, then $h(x, y) = \sum_{i,j} \overline{y}_i a_{ij} x_j$, where $a_{ij} = h(e_j, e_i)$. The matrix $H = (a_{ij}) \in M_n(S)$ satisfies $\overline{H}^t = H$. We often specify an isometry class of hermitian lattices by simply giving such a matrix. If $\det(H) \neq 0$, then we say that (L, h) is non-degenerate. From now on we will only consider non-degenerate hermitian lattices.

Let $e'_1, \ldots, e'_n$ be another basis of L with $e'_j = \sum_i \lambda_{ij} e_i$. The matrix $\lambda = (\lambda_{ij})$ is then unimodular, i.e. $\lambda, \lambda^{-1} \in M_n(S)$. If the form h is represented by the matrix H' in the basis $e'_1, \ldots, e'_n$, then H and H' are related by

$$H' = \overline{\lambda}^t H \lambda.$$

We have $\det(\lambda) \in S^*$, since λ is unimodular, and hence we get that $\det(H)$ and $\det(H')$ determine the same class in $F^*/\operatorname{nr}_{K/F}(S^*)$. This class is denoted by $d(h)$, the *discriminant* of (L, h).

If $L = M_1 \oplus M_2$ and $h(M_1, M_2) = (0)$, then we say that L is an orthogonal sum of M_1 and M_2. We write $L = M_1 \perp M_2$. Given two arbitrary hermitian lattices M_1 and M_2, it is clear how to construct a hermitian form h on $L = M_1 \oplus M_2$ such that $L = M_1 \perp M_2$.

We say that (L, h) is *isotropic* if it represents 0, i.e. there exists $x \in L$, $x \neq 0$, such that $h(x, x) = 0$. A lattice which is not isotropic is called *anisotropic*.

The so called *scale* $s(L)$ of L, is the S-ideal generated by all elements $h(x, y)$, where $x, y \in L$. The *norm* $n(L)$ is the S-ideal generated by all $h(x, x)$, $x \in L$. We clearly have $n(L) \subseteq s(L)$. If $n(L) = s(L)$, then we say that L is *normal*, otherwise *subnormal*.

Assume now that K is a local field. Let Π be a prime element of K and π a prime element of F. A vector $x \in L$ is primitive if $x \notin \Pi L$. Let $i \geq 0$ be an integer. We say that L is Π^i-*modular* if $h(x, L) = \Pi^i P$ for every primitive vector $x \in L$. An example of a Π^i-modular plane is given by the

so called *hyperbolic plane*

$$H(i) = \begin{pmatrix} 0 & \Pi^i \\ \overline{\Pi}^i & 0 \end{pmatrix}.$$

We say that L is *modular* if L is Π^i-modular for some i. Any lattice can be written as the orthogonal sum of modular lines and planes (see [25], prop. 4.3). We also have the following result, which is proposition 4.4 in [25]:

Proposition 5.1. *Let h be a hermitian plane. Then h is isometric to a sum of two lines if and only if h is normal.*

If $a \in F^*$, then we define the scaled lattice $a \circ L$, to be the lattice L together with the hermitian form $(x, y) \mapsto ah(x, y)$. We say that the hermitian lattice (L, h) is primitive if $\pi \nmid s(L)$. By suitable scaling, we can always replace a hermitian form on a lattice with a primitive hermitian form. A primitive modular plane is either Π^0- or Π^1-modular.

We finally remark that many of the concepts that we have defined for hermitian lattices also have an obvious meaning in the case of hermitian spaces. Just note that if (V, h) is a non-degenerate hermitian space, then it is natural to consider the determinant as a class in the group $F^*/\operatorname{nr}_{K/F}(K^*)$. Recall that if K is a local field, then this group is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ (see e.g. [31], corollary 63:13a). By considering an orthogonal basis, it is clear that the class $-d(h)$ is trivial if and only if the hermitian space (V, h) is isotropic.

5.2 Isometry classes of hermitian lattices over R_p

Let $k = \mathbb{Q}(\sqrt{d})$, where d is a square free integer, and R the ring of integers in k. Let p be a rational prime and assume that k_p is a field. Let $R_p = R \otimes_{\mathbb{Z}} \mathbb{Z}_p$, and let Π be a prime element in R_p, which we choose as follows: If $p \neq 2$, the *non-dyadic* case, then $\Pi = \sqrt{d}$. If $p = 2$ and $d \equiv 3 \pmod 4$, the so called *dyadic ramified unit* case, then $\Pi = 1 + \sqrt{d}$. If $p = 2$ and $d \equiv 0 \pmod 2$, the so called *dyadic ramified prime* case, then $\Pi = \sqrt{d}$.

In this section, we will, for convenience, write down a complete set of isometry classes of primitive hermitian planes over R_p. All statements in this section follow from the results in [25]. As it turns out, the isometry class of a hermitian plane is almost always determined by the discriminant class $d(h)$. Indeed, if things are reformulated in terms of integral Λ-hermitian forms instead, see section 5.4, we get a one-to-one correspondence between isometry classes and their corresponding discriminants. We remark that, in the case of Hilbert modular surfaces, the same goal was achieved by instead considering integral skew-hermitian forms in the sense of [20].

Consider first the case that k_p is unramified. In this case, we have:

Lemma 5.2. *Any hermitian plane is normal and, in fact, any primitive form is isometric to a unique form among the following*

$$\begin{pmatrix} 1 & 0 \\ 0 & p^k \end{pmatrix}, \quad k \in \mathbb{Z},\ k \geq 0. \tag{5.1}$$

We remark that the form given by (5.1) is isotropic if and only if k is even.

Assume now that k_p is ramified. Choose an element $\epsilon \in \mathbb{Z}_p^* \setminus \operatorname{nr}(R_p^*)$. The normal planes are described by the following lemma:

Lemma 5.3. *Let $l \geq 0$ be an integer, and let $\mathcal{M}(l)$ denote the set of isometry classes of normal primitive hermitian planes h over R_p with $v_p(d(h)) = l$.*

i) If $l < v_p(D)$, then $\mathcal{M}(l)$ consists of 2 classes, one class consisting of isotropic planes and one class consisting of anisotropic planes.

ii) If $l \geq v_p(D)$, then $\mathcal{M}(l)$ consists of 4 classes. In this case, a class is characterised by the following two properties: If its forms are isotropic or not, and if its forms represent trivial elements in $\mathbb{Z}_p^*/\operatorname{nr}_{k_p/\mathbb{Q}_p}(R_p^*)$ or not.

We write down representatives of all isometry classes of normal planes. The forms in part i) of lemma 5.3 are represented by

$$\begin{pmatrix} 1 & 0 \\ 0 & -\epsilon^i \operatorname{nr}(\Pi)^k \end{pmatrix}, \quad 0 \leq k < v_p(D),\ i = 0, 1. \tag{5.2}$$

The form in (5.2) is isotropic if and only if $i = 0$. The forms in part ii) of lemma 5.3 are represented by

$$\begin{pmatrix} \epsilon^i & 0 \\ 0 & -\epsilon^j \operatorname{nr}(\Pi)^k \end{pmatrix} \quad k \geq v_p(D),\ i, j = 0, 1. \tag{5.3}$$

The form in (5.3) is isotropic if and only if $i = j$. It represents trivial elements in $\mathbb{Z}_p^*/\operatorname{nr}_{k_p/\mathbb{Q}_p}(R_p^*)$ if and only if $i = 0$.

We now want to write down all the subnormal primitive planes. When we do this, we will write the planes in a particular order. The reason behind this ordering will become apparent later.

Consider first the ramified non-dyadic case. In this case, there is only one subnormal plane, namely H(1):

$$\begin{pmatrix} 0 & \sqrt{d} \\ -\sqrt{d} & 0 \end{pmatrix}. \tag{5.4}$$

Consider now the dyadic ramified unit case. In this case, we have 3 classes of subnormal primitive planes h. When $v_p(d(h)) = 0$, we have $H(0)$:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{5.5a}$$

and when $v_p(d(h)) = 1$, we have the isotropic plane $H(1)$ and one anisotropic plane:

$$\begin{pmatrix} 0 & \Pi \\ \overline{\Pi} & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 2 & \Pi \\ \overline{\Pi} & 2 \end{pmatrix}. \tag{5.5b}$$

Consider finally the dyadic ramified prime case. In this case, we have 5 classes of subnormal primitive planes h. First, we have $h = H(1)$, with $v_p(d(h)) = 1$:

$$\begin{pmatrix} 0 & \sqrt{d} \\ -\sqrt{d} & 0 \end{pmatrix}. \tag{5.6a}$$

We also have two planes h with $v_p(d(h)) = 0$, namely $H(0)$ and one plane which is anisotropic:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 2 & 1 \\ 1 & -2 \end{pmatrix}. \tag{5.6b}$$

Finally, we have two more planes h with $v_p(d(h)) = 1$:

$$\begin{pmatrix} 2 & \sqrt{d} \\ -\sqrt{d} & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 2 & \sqrt{d} \\ -\sqrt{d} & 2d \end{pmatrix}. \tag{5.6c}$$

The first plane in (5.6c) is isotropic and the second plane is anisotropic.

Now we want to compute the set of norms of automorphism of a hermitian plane h. Let k_p be a an arbitrary field extension of $\mathbb{Q}_p$ again. We let R_p^1 denote the elements of R_p with norm 1:

$$R_p^1 = \{\rho \in R_p \mid \rho\overline{\rho} = 1\}.$$

If h is a hermitian plane with matrix H, then we define

$$R_p(h) = \{\det(\lambda) \mid \lambda \in M_2(R_p),\ \overline{\lambda}^t H \lambda = H\}.$$

Clearly $R_p(h)$ is a subgroup of R_p^1, and we introduce the following concept:

Definition 5.4. We say that the hermitian plane h is *rigid* if $R_p(h) \neq R_p^1$.

We now have the following result:

Lemma 5.5. *If h is a primitive hermitian plane, then h is rigid in exactly the following cases:*

i) *in the ramified non-dyadic case and in the dyadic ramified prime case, when h is isometric to $H(1)$,*

ii) *in the dyadic ramified unit case, when h is isometric to $H(0)$.*

In these cases, we have

$$R_p(h) = \{\rho \in R_p^1 \mid \rho \equiv 1 \pmod{\sqrt{D}}\}, \tag{5.7}$$

and hence the group index $[R_p^1 : R_p(h)] = 2$.

Proof. (Compare with proposition 2.28 in [20].) Assume first that h is normal, so we may choose $H = \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$, where $a, b \in \mathbb{Z}_p$. Assume that $\rho \in R_p^1$. If we let $\lambda = \left(\begin{smallmatrix} \rho & 0 \\ 0 & 1 \end{smallmatrix}\right)$, then we have $\mathrm{nr}(\lambda) = \rho$ and $\overline{\lambda}^t H \lambda = H$. Hence $R_p(h) = R_p^1$ in this case.

We need to show that the planes given by (5.5b), (5.6b) and (5.6c) are not rigid. It is easy to see that all these planes represent 2, hence H can be chosen of the form $H = \left(\begin{smallmatrix} 2 & \alpha \\ \overline{\alpha} & b \end{smallmatrix}\right)$, where $\alpha \in R_2$, $b \in \mathbb{Z}_2$. If $\rho \in R_2$ with $\rho\overline{\rho} = 1$, then it is easy to verify that $(\rho - 1)/2 \in R_2$. If we now choose $\lambda = \left(\begin{smallmatrix} \rho & \alpha(\rho-1)/2 \\ 0 & 1 \end{smallmatrix}\right)$, then we get $\det(\lambda) = \rho$ and $\overline{\lambda}^t H \lambda = H$.

Consider now the planes, which we claim to be rigid. Observe that, in all cases, the plane is isometric to $H = \left(\begin{smallmatrix} 0 & \sqrt{d} \\ -\sqrt{d} & 0 \end{smallmatrix}\right)$. If $\lambda = (x_{ij})$, then $\overline{\lambda}^t H \lambda = H$ implies that $\overline{x}_{11}x_{22} - x_{12}\overline{x}_{21} = 1$. Hence $\det(\lambda) = x_{11}x_{22} - x_{12}x_{21} \equiv 1 \pmod{\sqrt{D}}$. Conversely, assume that $\rho \in R_p^1$ with $\rho \equiv 1 \pmod{\sqrt{D}}$. Then there exists $\epsilon \in R_p^*$ such that $\rho = \epsilon/\overline{\epsilon}$ (in fact, we may choose $\epsilon = (1+\rho)/2$ except possibly in the dyadic ramified unit case, where we may have to use $\epsilon = \sqrt{d}(1-\rho)/2$ instead). If we let $\lambda = \left(\begin{smallmatrix} \epsilon & 0 \\ 0 & 1/\overline{\epsilon} \end{smallmatrix}\right)$, then $\det(\lambda) = \rho$ and $\overline{\lambda}^t H \lambda = H$. The lemma is proved. □

In other words, the rigid planes are the ones in (5.4), (5.5a) and (5.6a).

5.3 A-hermitian forms

Let A be a quaternion algebra over k, and V a vector space over A, i.e. V is a right A-module.

Definition 5.6. A map $\Phi : V \times V \to A$ is called an A-hermitian form if

i) $\Phi(x+y, z) = \Phi(x, z) + \Phi(y, z)$,

ii) $\Phi(xa, y) = \Phi(x, y)a$,

iii) $\Phi(x, y) = \overline{\Phi(y, x)}^*$,

for all $x, y, z \in V$ and $a \in A$. The pair (V, Φ) is called an A-hermitian space.

Two A-hermitian spaces (V_1, Φ_1) and (V_2, Φ_2) are isometric, if there exists an invertible A-linear map $f : V_1 \to V_2$ such that $\Phi_2(f(x), f(y)) = \Phi_1(x, y)$ for all $x, y \in V_1$.

In the sequel, we will only consider 1-dimensional A-hermitian spaces V, which naturally will be identified with A. In this situation, an A-hermitian form is simply a map $\Phi : A \times A \to A$ of the form

$$\Phi(x, y) = \overline{y}^* \gamma x,$$

where γ is an element in A satisfying $\overline{\gamma}^* = \gamma$. If $\Phi \neq 0$, then we define the determinant of Φ by

$$\det(\Phi) = \mathrm{nr}(\gamma)\, \mathrm{nr}_{k/\mathbb{Q}}(k^*),$$

which is a class in the group $\mathbb{Q}^* / \mathrm{nr}_{k/\mathbb{Q}}(k^*)$. The following result is a special case of corollary 6.6, p. 376, in [39]:

Theorem 5.7. *Two A-hermitian spaces (A, Φ_1) and (A, Φ_2) are isometric if and only if* $\det(\Phi_1) = \det(\Phi_2)$.

We define the groups of isometries of an A-hermitian form:

Definition 5.8. The *unitary group* of an A-hermitian form Φ is

$$\mathrm{U}(A, \Phi) = \{s \in A \mid \Phi(sx, sy) = \Phi(x, y)\ \forall x, y \in A\}$$

and the *special unitary group* is

$$\mathrm{SU}(A, \Phi) = \{s \in \mathrm{U}(A, \Phi) \mid \mathrm{nr}(s) = 1\}.$$

By a (free) Λ-lattice in A, we mean a set $\mathcal{L}$ of the form $\mathcal{L} = v\Lambda$, where $v \in A$ is such that $\mathbb{Q}\mathcal{L} = A$. We say that two Λ-lattices $\mathcal{L}$ and $\mathcal{L}'$ lie in the same class with respect to $\mathrm{SU}(A, \Phi)$, if there is $\sigma \in \mathrm{SU}(A, \Phi)$ such that $\sigma\mathcal{L} = \mathcal{L}'$. We say that the lattices lie in the same genus if for all primes p there is $\sigma_p \in \mathrm{SU}(A_p, \Phi_p)$ such that $\sigma_p \mathcal{L}_p = \mathcal{L}'_p$.

5.4 Integral Λ-hermitian forms

Let Λ be a maximal order in A and let τ be a type 2 involution on A, which is special with respect to Λ. Let $\Phi : A \times A \to A$ be an A-hermitian form with respect to the involution τ. We introduce the following concept:

Definition 5.9. We say that the A-hermitian form Φ is *integral* with respect to the order Λ if it satisfies the properties

i) $\Phi(x,y) \in \Lambda$ for all $x, y \in \Lambda$,

ii) $\Phi(x,x) \in R + \sqrt{D}\Lambda$ for all $x \in \Lambda$.

Let us comment on condition ii) in definition 5.9. Since we have assumed that the involution is special, we claim that this condition only matters in the case that 2 is ramified in k. Namely, take $x \in \Lambda$. We have $\Phi(x,x) \in R + \sqrt{D}\Lambda$ if and only if $\Phi(x,x) \in (R + \sqrt{D}\Lambda)_p$ for all primes p. Now, if p is a prime not dividing D, then $(R + \sqrt{D}\Lambda)_p = \Lambda_p$, since $\sqrt{D}$ is a unit in R_p, so condition ii) follows from condition i). Let now $p \neq 2$ be a prime dividing D. Since the involution is special, Λ_p can be identified with $M_2(R_p)$, where the involution τ acts element-wise on the entries of the matrices. Let $\beta = \Phi(x,x) \in M_2(R_p)$. Since $R_p = \mathbb{Z}_p[\sqrt{D}]$, the condition $\tau(\beta)^* = \beta$ gives that

$$\beta = \begin{pmatrix} a + b\sqrt{D} & c\sqrt{D} \\ d\sqrt{D} & a - b\sqrt{D} \end{pmatrix},$$

where $a, b, c, d \in \mathbb{Z}_p$. Hence $\beta \in (R + \sqrt{D}\Lambda)_p$ as required.

It turns out that this extra condition ii), imposed if 2 is ramified in k, is essential for the computations that we will do.

We say that two integral Λ-hermitian forms Φ_1 and Φ_2 are equivalent if there exists a unit $\lambda \in \Lambda^1$ such that $\Phi_2(x,y) = \Phi_1(\lambda x, \lambda y)$, for all $x, y \in \Lambda$. We say that a Λ-hermitian form Φ is *primitive* if it is true that for any $r \in \mathbb{Q}$ such that $r\Phi$ is a integral form, we have $r \in \mathbb{Z}$. For each Λ-hermitian form $\Phi : \Lambda \times \Lambda \to \Lambda$, we define $d(\Phi) = \mathrm{nr}(\Phi(1,1)) \in \mathbb{Z}$. It is clear that $d(\Phi_1) = d(\Phi_2)$ if Φ_1 and Φ_2 are equivalent.

Definition 5.10. Let $N \in \mathbb{Z}$, $N \neq 0$. The number of equivalence classes of primitive integral Λ-hermitian forms Φ with $d(\Phi) = N$ is denoted by $n(\Lambda, \tau, N)$.

5.5 Local classification of integral Λ-hermitian forms

We remark that most of the results of this section are implicitly given in [20], but we give proofs of all statements for completeness and since we have a slightly more general setting.

Let A, Λ and τ be as in section 5.4 and take $N \in \mathbb{Z}_p$, $N \neq 0$. We want to compute the number $n(\Lambda_p, \tau, N)$ of equivalence classes, with respect to Λ_p^1, of Λ_p-hermitian forms Φ on (A_p, τ), which are primitive integral with respect to Λ_p and satisfy $\det(\Phi) = N$.

Assume first that k_p is a field. We let ι be an optimal involution on Λ_p. Then we have $(\Lambda_p)_\iota \cong M_2(\mathbb{Z}_p)$, and hence $\Lambda_p = R_p(\Lambda_p)_\iota$. We can therefore, without loss of generality, identify Λ_p with $M_2(R_p)$ and assume that the involution ι is given by element-wise conjugation on the matrices, i.e. $\iota((a_{ij})) = (\overline{a}_{ij})$. A primitive integral Λ-hermitian form Φ with respect to ι is determined by its matrix

$$\Phi(1,1) = \beta = \begin{pmatrix} \rho & a\sqrt{D} \\ b\sqrt{D} & \overline{\rho} \end{pmatrix}, \tag{5.8}$$

where $\rho \in R_p$ and $a, b \in \mathbb{Z}_p$ are such that $(a, b, \rho) = (1)$ in the unramified case and $(a, b, \rho) \supseteq (\Pi)$ in the ramified case. Two matrices β_1 and β_2 are equivalent if there exists a matrix $\lambda \in \mathrm{SL}_2(R_p)$ such that $\overline{\lambda}^* \beta_1 \lambda = \beta_2$.

In section 5.2, we studied isometry classes of hermitian planes. This is equivalent to studying the orbits of primitive matrices

$$H = \begin{pmatrix} a & \rho \\ \overline{\rho} & b \end{pmatrix}, \tag{5.9}$$

with $a, b \in \mathbb{Z}_p$, $\rho \in R_p$, where we say that H is primitive if $(a, b, \rho) = (1)$ in the unramified case and $(a, b, \rho) \supseteq (\Pi)$ in the ramified case. The group action is $\lambda \cdot H = \overline{\lambda}^t H \lambda$ for $\lambda \in \mathrm{GL}_2(R_p)$. We will now translate the classification of hermitian R_p-planes to a classification of Λ_p-hermitian forms.

Assume first that k_p is an unramified field. Recall that we have not assumed that τ is an optimal involution on Λ_p.

Lemma 5.11. *If k_p is unramified, then for every non-zero $N \in \mathbb{Z}_p$, there exists exactly one class of primitive Λ-hermitian forms Φ with $d(\Phi) = N$, i.e. $n(\Lambda_p, \tau, N) = 1$.*

Proof. First we show that the statement holds for the optimal involution ι, i.e. that $n(\Lambda_p, \iota, N) = 1$ It is clear, that for any $N \neq 0$, there exists a primitive form Φ such that $\det(\Phi) = N$. Assume that Φ_1 and Φ_2 are two primitive Λ_p-hermitian forms with respect to ι such that $\det(\Phi_1) = \det(\Phi_2)$. Let $\beta_i = \Phi_i(1,1)$ and $H_i = \left(\begin{smallmatrix} 0 & \sqrt{d} \\ -\sqrt{d} & 0 \end{smallmatrix}\right)\beta_i$ for $i = 1, 2$. It is clear that $\overline{H}_i^t = H_i$. By lemma (5.1), there exists $\gamma \in \mathrm{GL}_2(R_p)$ such that $\overline{\gamma}^t H_1 \gamma = H_2$. It is clear that $\det(\gamma) \in R_p^1$. Since H_1 is not rigid, there exists $\mu \in M_2(R_p)$ such that $\overline{\mu}^t H_1 \mu = H_1$ and $\det(\mu) = \det(\gamma)^{-1}$. If we choose $\lambda = \mu\gamma$, then we have $\overline{\lambda}^* \beta_1 \lambda = \beta_2$, so Φ_1 and Φ_2 are equivalent.

Consider now a general involution τ. By lemma 4.2, we have $\tau(x) = m^{-1}\iota(x)m$, for some invertible element $m \in A_p$ such that $m \in \Lambda_p$, $m \notin p\Lambda_p$

and $\iota(m)^* = m$. An integral Λ_p-hermitian form is given by an element β in A_p such that $\tau(\beta)^* = \beta$ and $\tau(\Lambda_p)^*\beta\Lambda_p \subseteq \Lambda_p$. We have

$$\begin{aligned}\tau(\Lambda_p)^*\beta\Lambda_p \subseteq \Lambda_p &\Leftrightarrow m^{-1}\iota(\Lambda_p)^* m\beta\Lambda_p \subseteq \Lambda_p \\ &\Leftrightarrow \Lambda_p m\beta\Lambda_p \subseteq m\Lambda_p \\ &\Leftrightarrow m\beta \in \mathrm{nr}(m)\Lambda_p \\ &\Leftrightarrow \beta \in m^*\Lambda_p,\end{aligned}$$

where the third equivalence follows from lemma 2.14. Let now $\beta = m^*x$, where $x \in \Lambda_p$. We get that $\tau(\beta)^* = \beta$ if and only if $\iota(x)^* = x$. Hence we have that the map

$$x \mapsto m^*x,$$

gives a one-to-one correspondence between the elements of A_p representing integral Λ_p-hermitian forms with respect to ι and the elements representing integral Λ_p-hermitian forms with respect to τ. □

Assume now that k_p is a ramified field. In this case, τ is by hypothesis an optimal involution on Λ_p, so we identify τ with the involution ι as above.

Lemma 5.12. *There is a one-to-one correspondence between primitive hermitian matrices H in the sense of* (5.9) *and primitive integral matrices β in the sense of* (5.8) *defined in the following way:*

$$\beta = g(H) = \alpha_H GH,$$

where the factor $\alpha_H \in k_p$ is given by

$$\alpha_H = \begin{cases} 1/\sqrt{d} & \text{if } H \text{ is rigid,} \\ \sqrt{d} & \text{if } H \text{ is subnormal but not rigid,} \\ \sqrt{D} & \text{if } H \text{ is normal,} \end{cases}$$

and G is the matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Furthermore, we have $g(\overline{\lambda}^t H\lambda) = \overline{\lambda}^* g(H)\lambda$ for every $\lambda \in \mathrm{SL}_2(R_p)$,

Proof. Straightforward calculations give that if a matrix H satisfies $\overline{H}^t = H$ and if $\lambda \in \mathrm{SL}_2(R_p)$, then $\beta = g(H)$ satisfies $\overline{\beta}^* = \beta$ and $g(\overline{\lambda}^t H\lambda) = \overline{\lambda}^*\beta\lambda$. It remains to show that the factor α_H is such that $g(H)$ is primitive if H is primitive. If H is normal, then this is clear. In the cases where H is subnormal, we can verify this claim by inspection of the matrices given in equations (5.4)–(5.6). □

Lemma 5.13. *Let k_p be ramified. Then we have the following result*

i) *if* $N \in \mathbb{Z}_p^*$ *and* $(d,N)_p = -1$, *then* $n(\Lambda_p, \iota, N) = 0$,

ii) *if* $N \in \mathbb{Z}_p^*$ *and* $(d,N)_p = 1$, *then* $n(\Lambda_p, \iota, N) = 2$, *and for any such form* Φ *we have that* $-\Phi \sim \Phi$ *if and only if* $p \nmid d$ (*i.e. in the dyadic ramified unit case*),

iii) *if* $1 \leq v_p(N) < 2v_p(D)$, *then* $n(\Lambda_p, \iota, N) = 1$.

iv) *if* $v_p(N) \geq 2v_p(D)$, *then* $n(\Lambda_p, \iota, N) = 2$. *Furthermore, for such a form* Φ, *we have that* $-\Phi \sim \Phi$ *if and only if* $(-1, D)_p = 1$.

Proof. If we write $\rho = x + dy$, $x, y \in \mathbb{Z}_p$, and β is as in (5.8), then we have

$$\det(\beta) = x^2 - dy^2 - Dab, \tag{5.10}$$

and $(x, y, a, b) = (1)$. It is clear that the form (5.10) represents N primitively if and only if the equation

$$x^2 - dy^2 \equiv N \pmod{D\mathbb{Z}_p}, \quad x, y \in \mathbb{Z}_p$$

has a solution. It is easy to see that this equation is unsolvable precisely if $N \in \mathbb{Z}_p^*$ and $(d,N)_p = -1$. In particular, we get i). To prove the rest of this lemma, we use lemma 5.12 and follow the idea in the proof of lemma 5.11.

ii) Assume that $N \in \mathbb{Z}_p^*$ and $(d,N)_p = 1$. If $\det(\beta) = N$, then we have that $H = g^{-1}(\beta)$ is a rigid hermitian matrix. Since $[R_p(H) : R_p^1] = 2$, we have 2 classes of forms. Furthermore, since for every form β there is a $\gamma \in \Lambda_p^*$ such that $\iota(\gamma)^*\beta\gamma \in \mathbb{Z}_p^*$, we see that β is equivalent to $-\beta$ if and only if there is some $\gamma \in \Lambda_p^1$ with $\iota(\gamma) = -\gamma$. This is the case if and only if $p \nmid d$.

iii) If $1 \leq v_p(N) < v_p(D)$, then $g^{-1}(\beta)$ is a subnormal non-rigid form. If $v_p(D) \leq v_p(N) < 2v_p(D)$, then $g^{-1}(\beta)$ is a normal plane h with $v_p(d(h)) < v_p(D)$. The claim now follows.

iv) In this case, we get that $g^{-1}(\beta)$ is a normal plane h with $v_p(d(h)) \geq v_p(D)$. There exist two classes of hermitian matrices with a given determinant. These two classes are distinguished by the elements in $\mathbb{Z}_p^*$ that they represent, according to lemma 5.3. Hence we get that β and $-\beta$ are equivalent if and only if $-1 \in \mathrm{nr}(R_p)$. This happens if and only if $(-1, D)_p = 1$. □

Now we turn to the split case, so assume that $k_p \cong \mathbb{Q}_p \times \mathbb{Q}_p$. We consider first the case $p \mid d(\Lambda)$. By lemma 4.11, any involution is optimal, and we can in fact identify Λ_p with $\Omega_p \times \Omega_p$ and let $\tau(x,y) = (y,x)$ for $x, y \in \Omega_p$. Consider two integral Λ_p-hermitian forms Φ_1 and Φ_2 with $d(\Phi_1) = d(\Phi_2)$. We have for $i = 1, 2$ that $\beta_i = \Phi_i(1,1) = (b_i, b_i^*)$, where $b_i \in \Omega_p$ with $\mathrm{nr}(b_1) = \mathrm{nr}(b_2)$. By proposition 2.11, we see that Φ_i is primitive if and

only if $p^2 \nmid d(\Phi_i)$. Let $c = b_2^{-1}b_1 \in \Omega_p^1$ and $\lambda = (c,1) \in \Lambda_p^1$. Then we get $\tau(\lambda)^*\beta_2\lambda = \beta_1$. Hence,

$$n(\Omega_p \times \Omega_p, \tau, N) = \begin{cases} 1 & \text{if } p^2 \nmid N \\ 0 & \text{otherwise.} \end{cases}$$

Consider now the case $p \nmid d(\Lambda)$. We have $\Lambda_p \cong M_2(\mathbb{Z}_p) \times M_2(\mathbb{Z}_p)$. Let ι be the optimal involution given by $\iota((x,y)) = (y,x)$, for all $x, y \in M_2(\mathbb{Z}_p)$. First we compute $n(\Lambda_p, \iota, N)$. A primitive integral Λ_p-hermitian form Φ with respect to ι is given by $\Phi(x,y) = \iota(y)^*\beta x$, where $\beta = (b, b^*)$ with $b \in M_2(\mathbb{Z}_p)$ and $b \notin pM_2(\mathbb{Z}_p)$. If $\lambda \in \Lambda^1$, then $\lambda = (a,c)$ where $a, c \in \mathrm{SL}_2(\mathbb{Z}_p)$, and we get $\iota(\lambda)^*\beta\lambda = (c^*ba, a^*b^*c)$. Assume now that Φ_1 and Φ_2 are two primitive forms with $d(\Phi_1) = d(\Phi_1)$. Let Φ_i be given by $\beta_i = (b_i, b_i^*)$, $i = 1, 2$. We have $\det(b_1) = \det(b_2)$ and $b_1, b_2 \in M_2(\mathbb{Z}_p) \setminus pM_2(\mathbb{Z}_p)$. It is easy to see that there exist elements $a, c \in \mathrm{SL}_2(\mathbb{Z}_p)$ such that $b_2 = c^*b_1a$, so we get that Φ_1 and Φ_2 are equivalent. Hence, we have

$$n(M_2(\mathbb{Z}_p) \times M_2(\mathbb{Z}_p), \iota, N)) = 1,$$

for all non-zero $N \in \mathbb{Z}_p$. Now, this holds in fact for any involution τ:

Lemma 5.14. *If p is split in k and $p \nmid d(\Lambda)$, then $n(\Lambda_p, \tau, N) = 1$ for every non-zero $N \in \mathbb{Z}_p$.*

Proof. Instead of changing the involution, we will change the order Λ_p in $M_2(\mathbb{Q}_p) \times M_2(\mathbb{Q}_p)$. We let $\Lambda_p = M_2(\mathbb{Z}_p) \times m^{-1}M_2(\mathbb{Z}_p)m$, where m is an invertible element in $M_2(\mathbb{Q}_p)$ such that $m \in M_2(\mathbb{Z}_p)$ and $m \notin pM_2(\mathbb{Z}_p)$. Take a Λ_p-hermitian form Φ and let $\beta = \Phi(1,1)$. By lemma 2.14, we get $\tau(\Lambda_p)^*\beta\Lambda_p \subseteq \Lambda_p$ if and only if $M_2(\mathbb{Z}_p)m^*xM_2(\mathbb{Z}_p) \subseteq m^*M_2(\mathbb{Z}_p)$ if and only if $m^*x \subseteq \mathrm{nr}(m)M_2(\mathbb{Z}_p)$ if and only if $x \in mM_2(\mathbb{Z}_p)$. The claim now follows as in the proof of lemma 5.11. □

For future reference, we now summarise the results of this section. We first introduce two functions: For every prime p dividing D, we define a character $\chi_{D,p} : \mathbb{Z}_p \to \{\pm 1, 0\}$, by

$$\chi_{D,p}(N) = \begin{cases} (D,N)_p & \text{if } p \nmid N, \\ 0 & \text{if } p \mid N. \end{cases}$$

If p is a prime such that $p \mid D$, and $N \in \mathbb{Z}_p$, $N \neq 0$, then we define

$$a_{D,p}(N) = \begin{cases} 2 & \text{if } v_p(N) \geq 2v_p(D) \\ 1 & \text{otherwise.} \end{cases}$$

Proposition 5.15. *Let τ be an involution of type 2 on A, which is special with respect to Λ. Let $N \in \mathbb{Z}_p \setminus \{0\}$. If we let $n = n(\Lambda_p, \tau, N)$, then we have*

i) *if k_p is unramified, then $n = 1$,*

ii) *if k_p is ramified, then $n = (\chi_{D,p}(N) + 1)a_{D,p}(N)$,*

iii) *if k_p is split and $p \nmid d(\Lambda)$, then $n = 1$,*

iv) *if k_p is split and $p \mid d(\Lambda)$, then $n = 1$ if $p^2 \nmid N$ and $n = 0$ otherwise.*

5.6 Hermitian spaces and quaternion algebras

The results in this section can be found in [43], p. 23–25, but are included for completeness. Let F be a field, and K a separable quadratic algebra over F with $l \mapsto \overline{l}$ the non-trivial automorphism of K over F.

Proposition 5.16. *Let (V, h) be a 2-dimensional non-degenerate hermitian space over K. Then*

$$Q_h = \{f \in \mathrm{End}_K(V) \mid h(f^*x, y) = h(x, fy)\ \forall x, y \in V\}$$

is a quaternion algebra. Furthermore, Q_h is split if and only if $-\det(h)$ is trivial in $F^*/\mathrm{nr}_{K/F}(K^*)$, i.e. if and only if h is isotropic.

Proof. It is clear that Q_h is an F-algebra. We now identify V with 2×1 K-matrices, and let h be given by

$$h(u, v) = \overline{v}^t H u,$$

where H is some 2×2 K-matrix such that $\overline{H}^t = H$. It is clear that the isomorphism class of Q_h only depends on the similarity class of h. Hence, by choosing an orthogonal basis for h, and scaling h if necessary, we may assume that H is of the form

$$H = \begin{pmatrix} 1 & 0 \\ 0 & s \end{pmatrix},$$

where $s \in F^*$. Now we get that Q_h consists of those K-matrices $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ which satisfy $\overline{\gamma}^t H = H\gamma^*$, and so by an easy calculation we get

$$Q_h = \{\gamma = \begin{pmatrix} a & -s\overline{c} \\ c & \overline{a} \end{pmatrix} \mid a, c \in K\}.$$

From this description, it is clear that $Q_h \otimes K \cong M_2(K)$. Hence Q_h is a central simple algebra of dimension 4. If we now consider the norm form on Q_h, which is given by

$$\mathrm{nr}(\gamma) = a\overline{a} + sc\overline{c},$$

we see that this form is isotropic if and only if $-s \in \mathrm{nr}(K^*)$. This shows the proposition. □

5.7 Orders and hermitian planes

Let P and F be as is chapter 2, and K as in section 5.6. Let S be the maximal order of K, so we have the following diagram of inclusions:

$$\begin{array}{ccc} F & \longrightarrow & K \\ \uparrow & & \uparrow \\ P & \longrightarrow & S\,. \end{array}$$

Let M be a projective S-module of rank 2. Any such M will be called an *S-plane*. Let $V = K \otimes_S M$, so V is a 2-dimensional vector space containing M as a lattice. If $h : M \times M \to S$ is a hermitian form, then we construct a P-order Λ_h, by

$$\Lambda_h = \{\lambda \in \mathrm{End}_S(M) \mid h(x, \lambda y) = h(\lambda^* x, y) \text{ for all } x, y \in M\}. \qquad (5.11)$$

In the notations of section 5.6, we have $\Lambda_h = Q_h \cap \mathrm{End}_S(M)$. Note that $\mathrm{End}_S(M)$ is a maximal order in $\mathrm{End}_K(V)$. It is clear that the isomorphism class of Λ_h only depends on the similarity class of h.

Recall from definition 2.29 that a quaternion P-order Λ is S-primitive if it exists an embedding of S into Λ. Recall also the fact that an S-primitive order is a Bass order. Conversely, it is true, if P is a local ring, that any Bass order Λ is S-primitive for some maximal order S in some quadratic extension of F (see proposition 1.11 in [5]). We will see later in this section that if P is a local ring, then the order Λ_h in (5.11) is in fact S-primitive. As a consequence we get, for an arbitrary base ring P, that Λ_h is a Bass order.

To a similarity class of hermitian S-planes, we have by (5.11) associated a P-order. Now we want to give a construction going in the opposite direction. Given an S-primitive order, we want to construct a similarity class of hermitian S-planes.

Let Λ be an S-primitive order with a fixed choice of an embedding of S

into Λ. Let $A = F \otimes_P \Lambda$, so we have the following diagram of embeddings:

$$\begin{array}{ccc} K & \longrightarrow & A \\ \uparrow & & \uparrow \\ S & \longrightarrow & \Lambda\,. \end{array}$$

We want to construct a hermitian form h_Λ, on some S-plane M, such that the similarity class of h_Λ is well defined. Now Λ can be naturally considered as an S-plane by multiplication from the left, so it is sufficient to construct a hermitian form on Λ. Consider now the natural embedding of Λ into $\mathrm{End}_S(\Lambda)$ given by

$$\lambda \mapsto \hat{\lambda} = (v \mapsto v\lambda^*),$$

for all $\lambda \in \Lambda$. This induces the following commutative diagram of ring embeddings

$$\begin{array}{ccc} A & \longrightarrow & \mathrm{End}_K(A) \\ \uparrow & & \uparrow \\ \Lambda & \longrightarrow & \mathrm{End}_S(\Lambda)\,. \end{array} \tag{5.12}$$

With these identifications, it is clear that we have

$$\Lambda = A \cap \mathrm{End}_S(\Lambda). \tag{5.13}$$

Now we claim that there exists a map

$$\delta : A \to K \tag{5.14}$$

satisfying $\delta(F) = F$, $\delta(la) = l\delta(a)$ for all $l \in K$, $a \in A$, and $\delta(a^*) = \overline{\delta(a)}$ for all $a \in A$. We can construct δ as follows. Let $u \in A$ be such that $\overline{l} = ulu^{-1}$ for all $l \in K$. Such an element u exists by lemma 2.5. Now we get that $A = K \oplus Ku$ and we let δ be projection on the first summand. It is straightforward to verify that this map has the required properties. The map δ is uniquely determined up to a non-zero factor of F. We choose one such map δ satisfying $\delta(\Lambda) \subseteq S$ and we define the hermitian form

$$h_\Lambda : \Lambda \times \Lambda \to S$$

by

$$h_\Lambda(x, y) = \delta(xy^*).$$

Using this construction, we get in particular:

Proposition 5.17. *If Λ is an S-primitive order, then Λ is isomorphic to Λ_h for some S-plane (M,h).*

Proof. We want to show that we can choose (M,h) as the hermitian S-plane (Λ, h_Λ), or in other words that the composition $\Lambda \mapsto h_\Lambda \mapsto \Lambda_{h_\Lambda}$ induces the identity on the set of isomorphism classes of S-orders. It is clear that $h_\Lambda(x, \hat{\lambda}(y)) = h_\Lambda(\hat{\lambda}^*(x), y)$ for all $x, y, \lambda \in \Lambda$. Furthermore, we claim that the copy of A in $\mathrm{End}_K(A)$ given by diagram (5.12), equals

$$\{f \in \mathrm{End}_K(A) \mid h_\Lambda(x, f(y)) = h_\Lambda(f^*(x), y) \text{ for all } x, y \in A\}. \qquad (5.15)$$

Namely, A is clearly an F-subalgebra of the algebra defined by (5.15). On the other hand, both these algebras are 4-dimensional vector spaces over F, and hence equal. Now, using equality (5.13), we get that $\Lambda_{h_\Lambda} = \Lambda$ as desired. □

The following lemma is the key step to prove that we get a one-to-one correspondence between similarity classes of S-planes and isomorphism classes of S-primitive orders in the local case.

Lemma 5.18. *If $v \in M$, then $\Lambda_h(v) = M$ if and only if $n(h) = (h(v,v))$.*

Proof. First we show that the condition is necessary. Assume that $\Lambda_h(v) = M$. Take an element $w \in M$. Then there exists by hypothesis an element $\lambda_w \in \Lambda_h$ such that $\lambda_w(v) = w$. We get $h(w,w) = h(\lambda_w(v), \lambda_w(v)) = h(v, \lambda_w^* \lambda_w(v)) = \mathrm{nr}(\lambda_w) h(v,v) \in (h(v,v))$. Hence $n(h) = (h(v,v))$, since w was arbitrary.

Now we want to show that the condition is sufficient. If $v \in M$ is any element with $n(h) = (h(v,v))$, then clearly $\Lambda_h(v) \subseteq M$. To show that we have equality, it is sufficient to show that we have equality for all localisations. Hence we can assume that P is a local ring. It is furthermore sufficient to show that $\Lambda_h(v) = M$ for some element v with $n(h) = (h(v,v))$. Let namely $u \in M$ be some other element satisfying $n(h) = (h(u,u))$. By hypothesis, we have $u = \lambda_u(v)$ for some element $\lambda_u \in \Lambda_h$. But then we get, as above, that $(h(u,u)) = \mathrm{nr}(\lambda_u)(h(v,v))$ and hence λ_u is a unit in Λ_h. Therefore, $\Lambda_h(u) = (\Lambda_h \lambda_u)(v) = \Lambda_h(v) = M$. Scaling h with a suitable constant, we can assume that h is a primitive hermitian form on $M = S \oplus S$. We identify M with 2×1 S-matrices, and a hermitian form h is then given by $h(x,y) = \overline{y}^t H x$, for some 2×2 matrix H with $\overline{H}^t = H$. With these identifications, we get

$$\Lambda_h = \{\lambda \in M_2(S) \mid \overline{\lambda}^t H = H \lambda^*\}.$$

We want to show that there exists an element $v \in M$ such that $\Lambda_h(v) = M$. There are several cases.

Assume that K is a split algebra, so $S = P \times P$. Let e_1 and e_2 be the orthogonal idempotents of S, so $\overline{e}_1 = e_2$. It is clear that we can find a basis of M such that h is similar to the form given by the matrix $H = \left(\begin{smallmatrix} 1 & 0 \\ 0 & x \end{smallmatrix}\right)$, $x \in P$. We get

$$\Lambda_h = \{e_1 X + e_2 Y \mid X, Y \in M_2(P) \text{ and } Y^t H = H X^*\},$$

which gives $\Lambda_h = \{e_1 \left(\begin{smallmatrix} a & -xb \\ c & d \end{smallmatrix}\right) + e_2 \left(\begin{smallmatrix} d & -xc \\ b & a \end{smallmatrix}\right) \mid a, b, c, d \in P\}$. The claim follows by choosing $v = \begin{pmatrix} 1 & 0 \end{pmatrix}^t$.

Assume now that K is a field. The valuation is denoted by $x \mapsto |x|$. Let π be a prime element of P and Π a prime element of S. We are now going to use the classification of hermitian planes in [25] to verify the claim.

Assume first that M has an orthogonal basis, so we can choose a basis such that H is given by $H = \left(\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right)$ with $|\alpha| \geq |\beta|$. We get

$$\Lambda_h = \{\begin{pmatrix} a & -\beta/\alpha\overline{c} \\ c & \overline{a} \end{pmatrix} \mid a, c \in S\},$$

so if we choose $v = \begin{pmatrix} 1 & 0 \end{pmatrix}^t$, then $\Lambda_h(v) = M$ and we are done. If K is an unramified field extension of F, then every hermitian plane has an orthogonal basis (see [25], p. 453). Hence we assume from now on that K is ramified.

Consider first the non-dyadic case. In this case, we can choose π and Π such that $\Pi = \sqrt{\pi}$. By proposition 8.1 in [25], if h does not have an orthogonal basis, then h is similar to a hyperbolic plane, which is given by the matrix

$$H(i) = \begin{pmatrix} 0 & \Pi^i \\ \overline{\Pi}^i & 0 \end{pmatrix}$$

for $i = 0, 1$. We get

$$\Lambda_h = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, d \in P,\ c, d \in S,\ \overline{\Pi}^i \overline{c} = -\Pi^i c,\ \Pi^i \overline{b} = -\overline{\Pi}^i b\}. \qquad (5.16)$$

If $i = 0$, then we get $\Lambda_h = \{\left(\begin{smallmatrix} a & \Pi b \\ \Pi c & d \end{smallmatrix}\right) \mid a, b, c, d \in P\}$, so $\Lambda_h(v) = M$ if $v = \begin{pmatrix} 1 & 1 \end{pmatrix}^t$. If $i = 1$, then we get $\Lambda_h = M_2(P)$, and we can choose $v = \begin{pmatrix} 1 & \Pi \end{pmatrix}^t$.

Now we consider the dyadic case, i.e. we assume that $|2| < |1|$. If we can choose Π and π such that $\Pi = \sqrt{\pi}$, then we have the so called ramified prime case. Otherwise Π can be chosen as $\Pi = (1 + \sqrt{1 + \pi^{2k+1}\delta})/\pi^k$, where $\delta \in P$

with $|\delta| = |1|$ and k is an integer with $|4| < |\pi|^{2k+1} < |1|$. This is the so called ramified unit case (see [25], section 5, for a discussion of these cases). According to (9.1) in [25], we have, for $i = 0, 1$, that $n(H(i)) = (2\pi^i)$ in the ramified prime case, and $n(H(i)) = (2\pi^{-k})$ in the ramified unit case. In the former case, the situation is analogous to the non-dyadic case using (5.16). In the latter case, it is straightforward to check, using (5.16), that we get $\Lambda_h(v) = M$ if we choose $v = \begin{pmatrix} 1 & \Pi \end{pmatrix}^t$ when $i = 0$ and $v = \begin{pmatrix} 1 & 1 \end{pmatrix}^t$ when $i = 1$.

There are even more subnormal planes h to consider in the dyadic case. According to propositions 9.1, 9.2 and 10.2 in [25], they are given by the following: Let $i = 0$ or $i = 1$, and assume that h is Π^i-modular. We have $n(h) \supseteq n(H(i))$. Assume that $n(h) = (\pi^m)$. Then h can be given by the matrix

$$H = \begin{pmatrix} \pi^m & \Pi^i \\ \overline{\Pi}^i & \alpha \end{pmatrix},$$

where $|\alpha| \leq |\pi^m|$. It is straightforward to verify that

$$\Lambda_h = \{ \begin{pmatrix} a & \Pi^i(a - \overline{a})/\pi^m - \alpha\overline{c}/\pi^m \\ c & \overline{a} + (\Pi^i c + \overline{\Pi}^i \overline{c})/\pi^m \end{pmatrix} \mid a, c \in S \}$$

and hence $v = \begin{pmatrix} 1 & 0 \end{pmatrix}^t$ will do. □

Assume now that there exists an element $v \in M$ satisfying $\Lambda_h(v) = M$. Then, for any element $s \in S$, there exists a unique element $\lambda_s \in \Lambda_h$ such that $\lambda_s(v) = sv$. Hence we get an embedding of S into Λ_h by the map

$$s \mapsto \lambda_s,$$

and consequently Λ_h is S-primitive. Furthermore, consider the map $\delta : \Lambda_h \to S$ defined by

$$\delta(\lambda) = h(v, \lambda(v)).$$

This map δ clearly satisfies all the requirements we made concerning the mapping (5.14). Using this, it is clear that the composition of maps $h \mapsto \Lambda_h \mapsto h_{\Lambda_h}$ is the identity on the set of similarity classes of hermitian S-planes.

If P is a local ring, then the existence of an element $v \in M$ as in lemma 5.18 is clear. As a special case of proposition 2.32, we get in the local case that if $\rho_j : S \to \Lambda$, $j = 1, 2$, are two embeddings, then there exists an element n in the normaliser $N(\Lambda)$ of Λ such that $n\rho_1(s)n^{-1} = \rho_2(s)$ for all $s \in S$. Hence we get that the two hermitian spaces constructed by using

this two choices of embeddings are isomorphic. In other words, the hermitian form h_Λ is well defined, that is, it does not depend of the embedding of S into Λ. Hence we have shown

Proposition 5.19. *If P is a local ring, then the map $h \mapsto \Lambda_h$ gives a one-to-one correspondence between similarity classes of hermitian S-planes and isomorphism classes of S-primitive orders.*

Since being Bass is a local property, and we know that S-primitive orders are Bass orders, we get the following global result:

Corollary 5.20. *The orders Λ_h are Bass orders.*

We now want to give a simple global example when the map $h \mapsto \Lambda_h$ is not injective. Let $P = \mathbb{Z}$ and $S = \mathbb{Z}[i]$. We let h_1 be the hermitian form given by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 6 \end{smallmatrix}\right)$, and h_2 the form given by $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 3 \end{smallmatrix}\right)$. We have that h_1 and h_2 do not belong to the same similarity class of hermitian forms over S. This can be seen by noting that there is no element v such that $(h_2(v,v)) = n(h_2) = (1)$, but such an element clearly exists for h_1. A straightforward calculation gives that $\Lambda_{h_1} \cong \Lambda_{h_2}$.

6 Quaternionic Shimura surfaces

6.1 Construction

We will now define the surfaces that are the main subject of this thesis. Let $k = \mathbb{Q}(\sqrt{d})$ be a real quadratic field with $R = \mathcal{O}_k$ and $d(k) = D$, as in section 1.1. Let A be a totally indefinite skew field over k which allows an involution of type 2. Let Λ be a maximal R-order in A. Assume that $a \mapsto \overline{a}$ is an involution of type 2 on A which is special with respect to Λ.

We fix a real representation

$$\varrho_0 : A \to M_2(\mathbb{R}),$$

and hence implicitly an embedding of k into $\mathbb{R}$. We note that ϱ_0 and $\lambda \mapsto \varrho_0(\overline{\lambda})$ are inequivalent representations of A. We can therefore choose the action of Λ^1 in (1.3) as

$$\lambda(z_1, z_2) = (\varrho_0(\lambda)(z_1), \varrho_0(\bar{\lambda})(z_1)),\ \lambda \in \Lambda^1,$$

or, more compactly written,

$$\lambda(z_1, z_2) = (\lambda z_1, \bar{\lambda} z_1). \tag{6.1}$$

We denote by ϱ the induced map

$$\varrho : \Lambda^1 \to \mathrm{Aut}(\mathcal{H}\times\mathcal{H}).$$

Let Γ denote the image of Λ^1 in $\mathrm{Aut}(\mathcal{H}\times\mathcal{H})$. We have $\Gamma \cong \Lambda^1/\{\pm 1\}$. Let X denote the quotient surface $X = \mathcal{H}\times\mathcal{H}/\Lambda^1$.

Now, X is a compact complex surface, since A is a skew field (see [44], proposition 9.3), and the only singularities of X are quotient singularities. In fact, it is well known (cf. [29]) that X is a projective surface. Furthermore, X is even defined over some number field (cf. [11]).

We let Y denote the canonical minimal desingularisation of X.

6.2 Elliptic points

The singularities of X come from points $z \in \mathcal{H}\times\mathcal{H}$ with non-trivial isotropy group in Λ^1. Consider an element $\alpha \in \mathrm{GL}^+(\mathbb{R})$ acting on $\mathcal{H}$. It has an isolated fixed point if and only if $(\mathrm{tr}(\alpha))^2 - 4\det(\alpha) < 0$. Hence an element $\lambda \in \Lambda^1$, which does not act trivially, has a fixed point if and only if it is a so called elliptic element, i.e. $(\mathrm{tr}\,\lambda)^2 - 4\,\mathrm{nr}\,\lambda \in k$ is negative under both the real embeddings, which we write

$$(\mathrm{tr}\,\lambda)^2 - 4\,\mathrm{nr}\,\lambda << 0. \tag{6.2}$$

For $z = (z_1, z_2) \in \mathcal{H}\times\mathcal{H}$, we define the isotropy groups

$$\Lambda^1_z = \{\lambda \in \Lambda^1 \mid \lambda z = z\}$$

and

$$\Gamma_z = \{\lambda \in \Gamma \mid \lambda z = z\}.$$

For any z we have $\{\pm 1\} \subseteq \Lambda^1_z$, and the group $\Gamma_z = \Lambda^1_z/\{\pm 1\}$ acts faithfully on $\mathcal{H}\times\mathcal{H}$. A discrete subgroup of $\mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{R})$, which fixes a point z, is necessarily finite. Furthermore, since we actually have an embedding $\varrho_0 : \Lambda^1 \to \mathrm{SL}_2(\mathbb{R})$, and finite subgroups of $\mathrm{SL}_2(\mathbb{R})$ are cyclic, we have that Λ^1_z and Γ_z are cyclic groups. If Γ_z is non-trivial, then z is called an elliptic point, and the order of Γ_z is called the order of the elliptic point z.

Since we only consider elements λ with $\mathrm{nr}\,\lambda = 1$, we have that (6.2) gives a finite set of possibilities for $\mathrm{tr}\,\lambda$, namely $\mathrm{tr}\,\lambda = 0$, ± 1, $\pm\sqrt{2}$, $\pm\sqrt{3}$ or $(\pm 1 \pm \sqrt{5})/2$. These correspond to elements of Γ of orders 2, 3, 4, 6 or 5 respectively. Hence we have the following well known result:

Proposition 6.1. *The possible orders of elliptic points are* 2, 3, 4, 5 *and* 6. *The order* 4 *is only possible if* $k = \mathbb{Q}(\sqrt{2})$, *the order* 5 *is only possible if* $k = \mathbb{Q}(\sqrt{5})$ *and the order* 6 *is only possible if* $k = \mathbb{Q}(\sqrt{3})$.

We also remark that if Λ is a $\mathbb{Z}$-order in an indefinite rational quaternion algebra, then only elliptic points of orders 2 or 3 are possible.

6.3 The two actions of Λ^1

Given a maximal order and an involution τ of type 2, one can consider the action of Λ^1 on either $\mathcal{H}\times\mathcal{H}$ or on $\mathcal{H}\times\mathcal{H}^-$, where $\mathcal{H}^-$ is the lower complex half plane, by

$$\lambda(z_1, z_2) = (\varrho_0(\lambda)z_1, \varrho_0(\tau(\lambda))z_2).$$

These two actions may or may not be holomorphically equivalent. They are holomorphically equivalent for example if there exists some $\lambda \in \Lambda$ with $\mathrm{nr}(\lambda) = -1$. If they are not, then it may happen that the corresponding quotient surfaces are not equivalent. It may even happen that they have different Kodaira dimensions (see [23]). See [19] for the complete answer to the question regarding when the two actions are holomorphically equivalent in the case $\Lambda = M_2(R)$.

Let us observe that, since we have the freedom to choose the involution τ, we can without loss of generality restrict to actions on $\mathcal{H}\times\mathcal{H}$. In fact, take an element $b \in A$ with $\tau(b)^* = b$ and $\mathrm{nr}(b) < 0$. Such elements clearly exist. Define $\sigma(x) = b\tau(x)b^{-1}$ for $x \in A$, so σ is an involution of type 2 on A. Define a biholomorphic map $\Psi : \mathcal{H}\times\mathcal{H}^- \to \mathcal{H}\times\mathcal{H}$ by $\Psi(z_1, z_2) = (z_1, \varrho_0(b)z_2)$. Consider the two maps $\Lambda^1 \to \mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{R})$ given by $\psi_\tau(\lambda) = (\varrho_0(\lambda), \varrho_0(\tau(\lambda)))$ and $\psi_\sigma(\lambda) = (\varrho_0(\lambda), \varrho_0(\sigma(\lambda)))$. We have that the diagram

$$\begin{array}{ccc} \mathcal{H}\times\mathcal{H}^- & \xrightarrow{\psi_\tau(\lambda)} & \mathcal{H}\times\mathcal{H}^- \\ \Psi\downarrow & & \downarrow\Psi \\ \mathcal{H}\times\mathcal{H} & \xrightarrow{\psi_\sigma(\lambda)} & \mathcal{H}\times\mathcal{H} \end{array}$$

commutes for every $\lambda \in \Lambda^1$. Hence the action of Λ^1 on $\mathcal{H}\times\mathcal{H}^-$ induced by the involution τ is holomorphically equivalent to the action of Λ^1 on $\mathcal{H}\times\mathcal{H}$ induced by the involution σ.

7 A family of curves

We will construct and study a family of curves on the quotient surface X. These curves will be parametrised by primitive elements in a certain quaternary $\mathbb{Z}$-lattice L. The underlying set L consists in fact of integral Λ-hermitian forms (see section 5.4).

When we construct our surface, we start with a maximal order Λ in A. Then we have to make a choice of an involution $\tau : A \to A$ of type 2, and the surface is the quotient X of $\mathcal{H}\times\mathcal{H}$ by the group action given by (6.1). For a given order Λ, we can at most get two different equivalence classes

of the surface X when we choose different involutions τ. Namely, if σ is another involution of type 2 given by $\sigma(x) = b\tau(x)b^{-1}$, where $\tau(b)^* = b$ and $\mathrm{nr}(b) > 0$, then the surfaces we get are equivalent. This fact is just a special case of the remark we made about the freedom of choice of the representations ϱ_i in (1.3). Hence, we get at most two possible equivalence classes of surfaces if we use different involutions, and they correspond to the situation discussed in section 6.3, where we fix τ and consider the action on $\mathcal{H}\times\mathcal{H}$ and $\mathcal{H}\times\mathcal{H}^-$ respectively. We now fix τ and we will from now on only consider involutions σ related to τ by an element b as above with $\mathrm{nr}(b) > 0$.

Now, by lemma 4.10, we know that there always exist special involutions, so from now on we will assume that τ is special with respect to Λ. We know, by proposition 4.4, that the R-ideal $d(\Lambda)$ is generated by a positive integer, which we denote $d_0(\Lambda)$. We also write $d_{\mathbb{Z}}(\Lambda) = d(\Lambda) \cap \mathbb{Z}$.

In section 7.2, we construct a quaternary quadratic lattice (L_τ, q_τ) which parametrises the curves. The construction can be regarded as a generalisation of the constructions made when studying modular curves on Hilbert modular surfaces using certain skew-hermitian matrices, see (1.1). In that case, the quadratic form is the determinant of the skew-hermitian matrices.

We show that we get a well-defined isometry class (L_τ, q_τ) up to what we call the *local type* of τ. The number of local types is finite. We have not been able to find an example when two involutions of different local types give non-isometric forms, but we have not ruled out the possibility. However, since the genus of the form does not depend on the local type, for our purposes this will not be a problem. Hence, we will simply fix a choice of local type and then drop the subscript τ from the notation, so we will denote the lattice by (L, q).

Following the terminology in [17], we will for convenience call the curves F_β, where $\beta \in L$, *modular curves*. Also, the curves F_N, which are finite unions of curves F_β, will be called modular curves.

7.1 Construction of curves

Consider an element $\beta \in A$. If $\mathrm{nr}(\beta) > 0$ (under the embedding $k \to \mathbb{R}$ induced by ϱ_0, which we have fixed), then we can define the following curve in $\mathcal{H}\times\mathcal{H}$:

$$C_\beta = \{(z, \beta z) \mid z \in \mathcal{H}\}.$$

This curve maps to some set $F_\beta \subset X$. We remark that the curve F_β and the group Γ_β below, do depend on the choice of involution τ. However, for easier notations we have chosen to not explicitly indicate this.

Now, F_β need not in general be an algebraic curve on X. We want to examine for which elements β it happens that F_β is a subvariety of X. This

is the case if the stabiliser group

$$\Gamma_\beta = \{\lambda \in \Lambda^1 \mid \lambda \cdot C_\beta = C_\beta\}$$

of $C_\beta \subseteq \mathcal{H} \times \mathcal{H}$ is sufficiently large in the sense that C_β/Γ_β is a compact curve. We will now examine for which elements β this holds. For $\lambda \in \Lambda^1$, we have

$$\begin{aligned} \lambda \cdot C_\beta &= \{(\lambda z, \tau(\lambda)\beta z \mid z \in \mathcal{H}\} = \\ &= \{(z, \tau(\lambda)\beta\lambda^* z) \mid z \in \mathcal{H}\} = \\ &= C_{\tau(\lambda)\beta\lambda^*}, \end{aligned} \tag{7.1}$$

and hence $\lambda \in \Gamma_\beta$ if and only if $\tau(\lambda)\beta\lambda^* = x\beta$ for some $x \in k^*$. Applying the norm form $\mathrm{nr} : A \to k$ to both sides of this equation, we get that $x^2 = 1$. Hence we have that an element $\lambda \in \Lambda^1$ belongs to Γ_β if and only if

$$\tau(\lambda)\beta\lambda^* = \pm\beta. \tag{7.2}$$

Definition 7.1. If β is an invertible element in A, then we define a $\mathbb{Q}$-subalgebra of A:

$$A_{\tau,\beta} = \{a \in A \mid \beta a = \tau(a)\beta\},$$

and an order $\Lambda_{\tau,\beta}$ in $A_{\tau,\beta}$:

$$\Lambda_{\tau,\beta} = A_{\tau,\beta} \cap \Lambda.$$

We get that the group $\Lambda^1_{\tau,\beta}$ is a subgroup of Γ_β of index 1 or 2 depending on whether the minus sign in equation (7.2) occurs for some $\lambda \in \Lambda^1$.

Proposition 7.2. *$A_{\tau,\beta}$ is either a quadratic field over $\mathbb{Q}$ or a non-split indefinite quaternion algebra over $\mathbb{Q}$, and the latter happens if and only if β is of the form $\beta = x\gamma$, where $x \in k$ and $\gamma \in A$ with $\tau(\gamma)^* = \gamma$.*

Proof. This follows directly from proposition 4.6. The condition $\tau(\beta)\beta \in k^*$ is clearly (compare with the proof of lemma 4.2) equivalent to the condition stated in the proposition. Now, if $A_{\tau,\beta}$ is 2-dimensional, then $A_{\tau,\beta}$ must be a field since A is a division algebra. If $A_{\tau,\beta}$ is a quaternion algebra, then it must be non-split and indefinite by lemma 4.3. □

We see that C_β/Γ_β is a compact curve if and only if $A_{\tau,\beta}$ is a quaternion algebra. With β and γ as in proposition 7.2, we have that $A_{\tau,\beta} = A_{\tau,\gamma}$. Hence we only need to consider elements $\beta \in A$ satisfying the equation

$$\tau(\beta)^* = \beta. \tag{7.3}$$

We define

$$W_\tau = \{\beta \in A \mid \tau(\beta)^* = \beta\}, \tag{7.4}$$

which is a 4-dimensional vector space over $\mathbb{Q}$. Consider now the norm form $\mathrm{nr} : A \to k$. If $\beta \in W_\tau$, then $\mathrm{nr}(\beta) = \mathrm{nr}(\tau(\beta)^*) = \overline{\mathrm{nr}(\beta)}$. Hence nr restricts to a quadratic form on W_τ taking rational values:

$$\mathrm{nr}\,|_{W_\tau} : W_\tau \to \mathbb{Q}. \tag{7.5}$$

Since $A_{\tau,1}$ is indefinite, there exists a $\mathbb{Q}$-basis of $A_{\tau,1}$ of the form $1, i, j, ij$, with $i^2 > 0$, $j^2 > 0$ and $ij + ji = 0$. We get that

$$1, \sqrt{d}i, \sqrt{d}j, \sqrt{d}ij$$

is a basis of W_τ. We see from this that the form (7.5), when diagonalized over $\mathbb{R}$, is of the type $++--$. Since A is a skew field, the quadratic form $\mathrm{nr} : A \to k$ is anisotropic. In particular, we get that the form (7.5) is anisotropic.

For every element $\beta \in W_\tau$ such that $\mathrm{nr}(\beta) > 0$, we consider the curve $C_\beta \in \mathcal{H} \times \mathcal{H}$ and we have that the quotient C_β/Γ_β is a compact complex curve. The subgroup $\Lambda^1_{\tau,\beta}$ of Γ_β is such that the map

$$C_\beta/\Lambda^1_{\tau,\beta} \to C_\beta/\Gamma_\beta$$

is either an isomorphism or a double cover. The map

$$C_\beta/\Gamma_\beta \to X$$

is generically one-to-one, and its image, denoted by F_β, is an irreducible complex curve on X. The map

$$C_\beta/\Gamma_\beta \to F_\beta$$

is just the normalisation map of F_β.

Assume that $[\Gamma_\beta : \Lambda^1_{\tau,\beta}] = 2$. We have $\Gamma_\beta = \Lambda^1_{\tau,\beta} \cup \gamma\Lambda^1_{\tau,\beta}$, for some element $\gamma \in \Lambda^1$ with $\tau(\gamma)\beta = -\beta\gamma$, by (7.2). Let $\gamma_d = \sqrt{d}\gamma$. It is clear that $\gamma_d \in \Lambda_{\tau,\beta}$, $\gamma_d \in N(\Lambda_{\tau,\beta})$ and $\mathrm{nr}(\gamma_d) = d$. The map $C_\beta \to C_\beta$ defined by $(z, \beta\zeta) \mapsto (\gamma_d z, \overline{\gamma}_d \beta z)$ gives an involution on $C_\beta/\Lambda^1_{\tau,\beta}$, which we denote by ι_d (compare with section 10.2):

$$\iota_d : C_\beta/\Lambda^1_{\tau,\beta} \to C_\beta/\Lambda^1_{\tau,\beta}. \tag{7.6}$$

We have that C_β/Γ_β is the quotient of $C_\beta/\Lambda^1_{\tau,\beta}$ by ι_d.

As we saw in equation (7.1), if $\lambda \in \Lambda^1$, then $\lambda \cdot C_\beta = C_{\tau(\lambda)\beta\lambda^*}$. Hence $\beta \in W_\tau$ and $\tau(\lambda)\beta\lambda^* \in W_\tau$ define the same curve on X. It is therefore natural to define an action of Λ^1 on W_τ by

$$\lambda \cdot \beta = \tau(\lambda)\beta\lambda^*, \tag{7.7}$$

so with this notation, we have $F_{\lambda\cdot\beta} = F_\beta$. In fact, two curves F_{β_1} and F_{β_2} are equal if and only if there exist $x \in \mathbb{Q}$ and $\lambda \in \Lambda^1$ such that $\beta_2 = x\lambda \cdot \beta_1$. Note also that

$$\mathrm{nr}(\lambda \cdot \beta) = \mathrm{nr}(\beta)$$

for all elements $\lambda \in \Lambda^1$ and $\beta \in W_\tau$. Hence, the action of λ is an isometry of (W_τ, nr).

7.2 The lattice parametrising the curves

In this section, we are going to construct a lattice L_τ in the vector space W_τ, which is invariant under the action (7.7) of Λ^1. We will follow the convention to always use primitive elements β of L_τ when we study the curves F_β. By a *primitive element* β in L_τ, we mean an element with the property that if $x\beta \in L_\tau$ for some $x \in \mathbb{Q}$, then $x \in \mathbb{Z}$. With this convention, we get that $F_{\beta_1} = F_{\beta_2}$ if and only if

$$\beta_2 = \pm\lambda \cdot \beta_1 \tag{7.8}$$

for some $\lambda \in \Lambda^1$. We will also define a quadratic form $q_\tau : L_\tau \to \mathbb{Z}$, where $q_\tau(l) = c\,\mathrm{nr}(l)$ for some rational number $c > 0$.

We will see (in proposition 7.13) that (L_τ, q_τ) is essentially independent of the choice of τ and therefore we will eventually drop the subscript τ from the notation.

Let ν and τ be two special involutions. By lemma 4.2, there exists an element $\gamma = \gamma_{\nu,\tau} \in A$ such that $\tau(\gamma)^* = \gamma$ and $\nu(x) = \gamma^{-1}\tau(x)\gamma$ for all $x \in A$.

Definition 7.3. We say that ν and τ are of the same *local type* if the integers $v_p(\mathrm{nr}(\gamma))$ are even for all primes p dividing $d(\Lambda)$.

Now to the construction. Let τ be a special involution. For any β in W_τ, we define a hermitian form $\Phi_{\tau,\beta} : A \times A \to A$, in the sense of section 5.3, by

$$\Phi_{\tau,\beta}(x, y) = \tau(y)^*\beta x. \tag{7.9}$$

We are interested in those elements β for which $\Phi_{\tau,\beta}$ satisfy definition 5.9:

Definition 7.4. We define a $\mathbb{Z}$-lattice L_τ of rank 4 by

$$L_\tau = \{\beta \in W_\tau \mid \Phi_{\tau,\beta} \text{ is integral}\}. \tag{7.10}$$

It is clear that L_τ is an invariant subset of W_τ under the action (7.7) of Λ^1. The following, somewhat technical, lemma relates the lattices we get if we use different involutions of the same local type.

Lemma 7.5. *If τ and ν are special involutions, which belong to the same local type, then there exists an element $\gamma \in W_\tau$ such that $\nu(x) = \gamma^{-1}\tau(x)\gamma$ for all $x \in A$ and $L_\nu = \gamma^* L_\tau$.*

Proof. By lemma 4.2, there exists an element $w \in W_\tau$ such that

$$\nu(x) = w^{-1}\tau(x)w$$

for all $x \in A$. If $x \in A$, then by a straightforward calculation, we get that $\nu(w^*x)^* = w^*x$ if and only if $\tau(x)^* = x$. Hence, we conclude that

$$W_\nu = w^* W_\tau,$$

so the two lattices L_ν and w^*L_τ span the same 4-dimensional $\mathbb{Q}$-vector space, i.e. they are commensurable. We are done if we can show that in fact there exists $r \in \mathbb{Q}$ such that

$$L_\nu = rw^* L_\tau. \tag{7.11}$$

Now we realise that we only need to check equation (7.11) locally, i.e. we need to show that for any prime p, there is a $r_p \in \mathbb{Q}_p$ such that

$$(L_\nu)_p = r_p w^* (L_\tau)_p. \tag{7.12}$$

Since for almost all primes p, we have $(L_\nu)_p = w^*(L_\tau)_p$, this would imply that there exists an element $r \in \mathbb{Q}$ such that (7.11) holds.

Fix now a prime p. We want to prove that (7.12) holds for some r_p. We examine the different cases.

We consider first the case $p \mid d(\Lambda)$. By lemma 4.11, we can make the identification $\Lambda_p = \Omega_p \times \Omega_p$ with $\tau(x, y) = (y, x)$. Consider now the involution ν given by $\nu(\lambda) = w^{-1}\tau(\lambda)w$, where $w = (c, c^*)$ with $c \in \Omega_p$. By the hypothesis that these two involutions are of the same local type, we have that $v_p(\mathrm{nr}(w)) = v_p(\mathrm{nr}(c))$ is even. This implies that c is of the form $s\epsilon$, for some $s \in \mathbb{Q}_p$ and $\epsilon \in \Omega_p^*$. We now get

$$(L_\tau)_p = \{(x, x^*) \mid x \in \Omega_p\} \tag{7.13}$$

and

$$(L_\nu)_p = \{(x, \epsilon x^* \epsilon^{-1}) \mid x \in \Omega_p\}.$$

Hence we get $(L_\nu)_p = s^{-1}w^*(L_\tau)_p$ and we are done in this case.

Assume now that $p \nmid d(\Lambda)$. We have that $\Lambda_p \cong M_2(R_p)$ and we let ι be the optimal involution on $M_2(R_p)$, which is given by element-wise conjugation, i.e.

$$\iota((a_{ij})) = (\overline{a}_{ij})$$

if $(a_{ij}) \in M_2(R)$. We now claim that it is sufficient to show the following:

Claim. *For any special involution σ on A_p, there exists $\gamma_\sigma \in W_\iota$ such that the following holds*

i) $\sigma(x) = \gamma_\sigma^{-1}\iota(x)\gamma_\sigma$ *for all* $x \in A_p$.

ii) $L_\sigma = \gamma_\sigma^* L_\iota$.

Assume namely that this claim is true. Then it is easy to check that the following holds: $\tau(\gamma_\tau^{-1}\gamma_\nu)^* = \gamma_\tau^{-1}\gamma_\nu$, $\nu(x) = (\gamma_\tau^{-1}\gamma_\nu)^{-1}\tau(x)\gamma_\tau^{-1}\gamma_\nu$ for every $x \in A_p$ and $(L_\nu)_p = (\gamma_\tau^{-1}\gamma_\nu)^*(L_\tau)_p$. By the uniqueness part of lemma 4.2, we have $\gamma_\tau^{-1}\gamma_\nu = r_p w$ for some $r_p \in \mathbb{Q}_p$, and hence we have shown that (7.12) holds if the claim holds. We will now prove the claim in the different cases.

Assume first that p is unramified in k. Let $\gamma_\sigma \in W_\iota$ be some element satisfying i) in the claim. Replacing, if necessary, γ_σ with $s\gamma_\sigma$ for some suitable $s \in \mathbb{Q}_p$, we may assume that $m_{\Lambda_p}(\gamma_\sigma) = (1)$ (see (2.10)). Now we have

$$L_\iota = \{x \in W_\iota \mid \Lambda_p x \Lambda_p \subseteq \Lambda_p\} \tag{7.14}$$

and

$$L_\sigma = \{\gamma_\sigma^* y \mid y \in W_\iota,\ \sigma(\Lambda_p)\gamma_\sigma^* y \Lambda_p \subseteq \Lambda_p\}.$$

But $\sigma(\Lambda_p)\gamma_\sigma^* y \Lambda_p \subseteq \Lambda_p$ if and only if $\gamma_\sigma^* \Lambda_p x \Lambda_p \subseteq \Lambda_p$, which, by lemma 2.14, is equivalent to $\Lambda_p x \Lambda_p \subseteq \Lambda_p$. Hence, we get $L_\sigma = \gamma_\sigma^* L_\iota$.

Assume now that p is ramified in k. By the hypothesis that σ is special, we have that $\Lambda_\sigma \cong M_2(\mathbb{Z}_p)$. We claim that this implies that, replacing γ_σ with $s\gamma_\sigma$ for some $s \in \mathbb{Q}_p$ if necessary, we can assume that γ_σ is of the form

$$\gamma_\sigma = \iota(\epsilon)^* \epsilon, \tag{7.15}$$

for some unit $\epsilon \in \Lambda_p$. To see this, fix an isomorphism $\Lambda_\iota \to \Lambda_\sigma$. Since $R_p\Lambda_\iota = R_p\Lambda_\sigma = \Lambda_p$, this map can be extended to an automorphism of Λ_p. By the Skolem-Noether theorem this automorphism is inner, and hence there exists an invertible element g in A_p such that $\Lambda_\sigma = g^{-1}\Lambda_\iota g$. Then we also get that g satisfies $g\Lambda_p = \Lambda_p g$, so $g\Lambda_p$ is a two-sided ideal. Hence $g\Lambda_p = a\Lambda_p$ for some $a \in k_p$, and therefore $g = a\epsilon$ for some $\epsilon \in \Lambda_p^*$. Thus, we get

$$\Lambda_\sigma = \epsilon^{-1}\Lambda_\iota \epsilon.$$

Now, for any $\lambda \in \Lambda_\iota$, we have $\sigma(\epsilon^{-1}\lambda\epsilon) = \epsilon^{-1}\lambda\epsilon$. Hence $\iota(\epsilon)\gamma_\sigma\epsilon^{-1} \in k_p$ and we get that γ_σ must be of the form

$$\gamma_\sigma = t\iota(\epsilon)^*\epsilon,$$

for some $t \in k_p$. Taking into account that $\mathrm{nr}(\gamma_\sigma) \in \mathbb{Q}_p$, we get $t^2 \in \mathbb{Q}_p$. Hence $t \in \mathbb{Q}_p$ or $t \in \sqrt{D}\mathbb{Q}_p$. We want to exclude the latter case. If $t \in \sqrt{D}\mathbb{Q}_p$, then $\iota(\gamma_\sigma)^* = \gamma_\sigma$ is equivalent to $\epsilon\iota(\epsilon)^* + \iota(\epsilon)^*\epsilon = 0$. Now we note that for any $\lambda \in \Lambda_p$, we have $\iota(\lambda) \equiv \lambda \pmod{\sqrt{D}\Lambda_p}$. Hence, we get $\epsilon\epsilon^* + \epsilon^*\epsilon \equiv 0 \pmod{\sqrt{D}\Lambda_p}$, i.e. $2\,\mathrm{nr}(\epsilon) \equiv 0 \pmod{\sqrt{D}R_p}$. But this contradicts that ϵ is a unit. Hence we have $t \in \mathbb{Q}_p$, so replacing γ_σ with $t^{-1}\gamma_\sigma$, we have demonstrated (7.15).

Now we get

$$L_\iota = \{x \in W_\iota \mid x \in R_p + \sqrt{D}\Lambda_p\}$$

and

$$L_\sigma = \{\gamma_\sigma^* y \mid y \in W_\iota,\ \gamma_\sigma^* x \in R_p + \sqrt{D}\Lambda_p\}.$$

With γ_σ as in (7.15), it is clear that for any $y \in \Lambda_p$, we have $y \in R_p + \sqrt{D}\Lambda_p$ if and only if $\gamma_\sigma^* y \in R_p + \sqrt{D}\Lambda_p$. It follows that $L_\sigma = \gamma_\sigma^* L_\iota$. We have now proved the claim in the case that k_p is a field.

Assume finally that p is split in k and that $p \nmid d(\Lambda)$. Then $R_p = \mathbb{Z}_p \times \mathbb{Z}_p$, and we identify Λ_p with $M_2(\mathbb{Z}_p) \times M_2(\mathbb{Z}_p)$, where $\iota(a,b) = (b,a)$. Hence

$$L_\iota = \{(x, x^*) \mid x \in M_2(\mathbb{Z}_p)\}.$$

Let $\gamma_\sigma = (b, b^*)$, where $b \in M_2(\mathbb{Z}_p)$ with $\det(b) \neq 0$. Without loss of generality, we can assume that b is primitive, i.e. $b \notin pM_2(\mathbb{Z}_p)$. We get

$$L_\sigma = \{\gamma_\sigma^* y \mid y \in W_\iota,\ \sigma(\Lambda_p)\gamma_\sigma^* y\Lambda_p \subseteq \Lambda_p\}.$$

If $y \in W_\iota$, so $y = (z, z^*)$, where $z \in M_2(\mathbb{Q}_p)$, then we have $\sigma(\Lambda_p)\gamma_\sigma^* y\Lambda_p \subseteq \Lambda_p$ if and only if $b^* M_2(\mathbb{Z}_p) z M_2(\mathbb{Z}_p) \subseteq M_2(\mathbb{Z}_p)$. According to lemma 2.14, this is equivalent to $z \in M_2(\mathbb{Z}_p)$. Hence we get $L_\sigma = \gamma_\sigma^* L_\iota$, so the claim holds in the split case too. □

Definition 7.6. Define a quadratic form q_τ on L_τ by

$$q_\tau(\beta) = \frac{d_0(\Lambda)}{d_0(\Lambda_\tau)}\,\mathrm{nr}(\beta) \tag{7.16}$$

for $\beta \in L_\tau$.

Definition 7.7. Define a dual lattice $L_\tau^\#$ to L_τ by

$$L_\tau^\# = \{l \in W_\tau \mid \mathrm{tr}(l^* L_\tau) \subseteq \mathbb{Z}\}. \tag{7.17}$$

We define a quadratic form $q_\tau^\#$ on $L_\tau^\#$ by

$$q_\tau^\#(l) = D d_0(\Lambda_\tau)\,\mathrm{nr}(l). \tag{7.18}$$

A priori we have that q_τ and $q_\tau^\#$ are quadratic forms with values in $\mathbb{Q}$, and at this point it is not obvious that they are in fact integral forms. We therefore define quadratic forms $\dot{q}_\tau : L_\tau \to \mathbb{Z}$, $\dot{q}_\tau(\beta) = x_\tau\,\mathrm{nr}(\beta)$ and $\dot{q}_\tau^\# : L_\tau^\# \to \mathbb{Z}$, $\dot{q}_\tau^\#(l) = y_\tau\,\mathrm{nr}(l)$, where x_τ and y_τ are the uniquely determined positive rational numbers such that $\dot{q}_\tau$ and $\dot{q}_\tau^\#$ are primitive integral forms. We will see later (in lemma 7.12) that $q_\tau = \dot{q}_\tau$ and $q_\tau^\# = \dot{q}_\tau^\#$.

If ι is an involution on Λ_p, which does not necessarily come from a global involution on Λ, then we can still define $\dot{q}_\iota$ and $\dot{q}_\iota^\#$. These forms will of course only be well defined up to a factor in $\mathbb{Z}_p^*$. We now write down an explicit local description of the lattices for an optimal involution ι on Λ_p. If $p \mid d(\Lambda)$, then we have

$$L_\iota = \{\beta = (x, x^*) \mid x \in \Omega_p\} \tag{7.19a}$$

and

$$L_\iota^\# = \{l = (y, y^*) \mid y \in \Omega_p^\#\}, \tag{7.19b}$$

where $\dot{q}_\iota(\beta) = \mathrm{nr}(x)$ and $\dot{q}_\iota^\#(l) = p\,\mathrm{nr}(y)$. If $p \nmid d(\Lambda)$, then we have

$$L_\iota = \{\beta = \begin{pmatrix} \alpha & a\sqrt{D} \\ b\sqrt{D} & \overline{\alpha} \end{pmatrix} \mid \alpha \in R_p,\ a, b \in \mathbb{Z}_p\} \tag{7.20a}$$

and

$$L_\iota^\# = \{l = \begin{pmatrix} \alpha & a/\sqrt{D} \\ b/\sqrt{D} & \overline{\alpha} \end{pmatrix} \mid \alpha \in R_p^\#,\ a, b \in \mathbb{Z}_p\}, \tag{7.20b}$$

where $\dot{q}_\iota(\beta) = \det(\beta)$ and $\dot{q}_\iota(l) = D\det(l)$.

Consider now the quaternary quadratic lattice $(L_\tau^\#, \dot{q}_\tau^\#)$ and the even Clifford algebra $C_0(L_\tau^\#, \dot{q}_\tau^\#)$ associated to it. Define a function

$$\phi_\tau : L_\tau^\# \otimes_{\mathbb{Z}} L_\tau^\# \to A$$

by

$$\phi_\tau(l_1 \otimes l_2) = y_\tau l_1^* l_2.$$

We can extend ϕ_τ in a natural way to the even tensor algebra, so we get a map $\phi_\tau : \mathcal{T}_0(L_\tau^\#) \to A$. This map clearly vanishes on the ideal generated by the elements $l \otimes l - \dot{q}_\tau^\#(l)$ giving an embedding of the ring $C_0(L_\tau^\#, \dot{q}_\tau^\#)$ into the algebra A.

Definition 7.8. Θ_τ will denote the image of the map

$$\phi_\tau : C_0(L_\tau^\#, \dot{q}_\tau^\#) \to A$$

Θ_τ is a subring of A, but it should be noted that it is not in general an R-order.

Definition 7.9. For a primitive element $\beta \in L_\tau$, we define the ternary quadratic lattice $(L_{\tau,\beta}^\#, q_{\tau,\beta}^\#)$, where

$$L_{\tau,\beta}^\# = \{l \in L_\tau^\# \mid \mathrm{tr}(l^*\beta) = 0\}$$

and $q_{\tau,\beta}^\#$ denotes the restriction of $q_\tau^\#$ to $L_{\tau,\beta}^\#$.

We also consider $\dot{q}_{\tau,\beta}^\#$, the restriction of $\dot{q}_\tau^\#$ to $L_{\tau,\beta}^\#$. Now, by restriction of ϕ_τ, we get an embedding of the quaternion order $C_0(L_{\tau,\beta}^\#, \dot{q}_{\tau,\beta}^\#)$ into A. The image is in fact a suborder of $A_{\tau,\beta}$.

Lemma 7.10. *The image of $C_0(L_{\tau,\beta}^\#, \dot{q}_{\tau,\beta}^\#)$ under ϕ_τ is $\Theta_\tau \cap A_{\tau,\beta}$.*

Proof. If we take $l_1, l_2 \in L_{\tau,\beta}^\#$, then $\beta l_1^* l_2 = -l_1\beta^* l_2 = l_1 l_2^* \beta = \tau(l_1^* l_2)\beta$, so $\phi_\tau(l_1 \otimes l_2) \in A_{\tau,\beta}$. We conclude that $C_0(L_{\tau,\beta}^\#, \dot{q}_{\tau,\beta}^\#) \subseteq A_{\tau,\beta}$.

To show the inverse inclusion, take $\lambda \in \Theta_\tau \cap A_{\tau,\beta}$. It follows from the definitions of the lattices and the fact that β is a primitive element of L_τ that $L_\tau^\# = L_{\tau,\beta}^\# \oplus \mathbb{Z}\omega$ for some $\omega \in L_\tau^\#$ with $\mathrm{tr}(\omega^*\beta) = 1$. Since λ belongs to Θ_τ, it can be written in the form $\lambda = \lambda_0 + y_\tau l_1^*\omega + y_\tau^2 l_2^* l_3 l_4^* \omega$, where λ_0 lies in the image of $C_0(L_{\tau,\beta}^\#, \dot{q}_{\tau,\beta}^\#)$ and $l_1, \ldots, l_4 \in L_{\tau,\beta}^\#$. A direct calculation gives now $0 = \beta\lambda - \tau(\lambda)\beta = -\tau(y_\tau l_1^* + y_\tau^2 l_2^* l_3 l_4^*)$. Hence $\lambda = \lambda_0 + (y_\tau l_1^* + y_\tau^2 l_2^* l_3 l_4^*)\omega = \lambda_0 \in \phi_\tau(C_0(L_{\tau,\beta}^\#, q_\beta^\#))$ and we are done. □

Lemma 7.11. *We have that $\Theta_\tau \subseteq \Lambda$ and $[\Lambda : \Theta_\tau] = d_\mathbb{Z}(\Lambda)^2$. In fact, we have $\Lambda/\Theta_\tau \cong (\mathbb{Z}/d_\mathbb{Z}(\Lambda))^2$.*

Proof. Let ν be another special involution of the same local type as τ, and γ as in lemma 7.5. We have $L_\nu = \gamma^* L_\tau$, so a calculation gives that

$$L_\tau^\# = \gamma L_\nu^\#,$$

and from this we clearly have that $y_\nu = |\,\mathrm{nr}(\gamma)|y_\tau$. Take arbitrary elements $\gamma l_1, \gamma l_2 \in \gamma L_\nu^\# = L_\tau^\#$. We get $\phi_\tau(\gamma l_1 \otimes \gamma l_2) = y_\tau l_1^* \gamma^* \gamma l_2 = \pm\phi_\nu(l_1 \otimes l_2)$ and hence we have

$$\Theta_\nu = \Theta_\tau,$$

i.e. Θ_τ does not depend on the choice of involution (up to the local type).

Fix a prime p and let ι be an optimal involution on Λ_p. If $p \nmid d(\Lambda)$, then we need to show that $\Theta_\iota = \Lambda_p$. This is just a straightforward calculation given the description of $L_\iota^\#$ in (7.20).

Consider now the case $p \mid d(\Lambda)$. With notations as in (7.19) and in equation (2.8) (with $\pi = p$), we have that

$$(1,1),\ (E_1, -1 - E_1),\ \frac{1}{p}(E_2, -E_2),\ \frac{1}{p}(E_3, -E_3)$$

is a basis of $L_\tau^\#$. A $\mathbb{Z}_p$-basis of $(\Theta_\tau)_p$ is hence given by: $(1,1)$, $(pE_1, -p - pE_1)$, $(E_2, -E_2)$, $(E_3, -E_3)$, $(E_2 + E_3, E_3)$, $(\epsilon E_2, \epsilon E_2 + E_3)$, $(1 + E_1, 1 + E_1)$, $(p\epsilon - p - pE_1, -p\epsilon)$. Thus $(\Theta_\tau)_p$ is a $\mathbb{Z}_p$-sublattice of Λ_p of index p^2. We also note that $(\Theta_\tau)_p$ can be written in a convenient coordinate free way:

$$\begin{aligned}(\Theta_\tau)_p &= \{(x,y) \in \Omega_p \times \Omega_p \mid \mathrm{nr}(x - y) \in (p)\} \\ &= \{\lambda \in \Lambda_p \mid \mathrm{nr}(\lambda - \tau(\lambda)) \in (p)\}.\end{aligned} \tag{7.21}$$

This follows directly from the above description and equation (2.9). □

Note that Θ_τ is not an R-algebra if A is a skew field, but from equation (7.21), we immediately get

$$R\Theta_\tau = \Lambda.$$

Lemma 7.12. *We have that $q_\tau = \dot{q}_\tau$ and $q_\tau^\# = \dot{q}_\tau^\#$. In particular, we get that q_τ and $q_\tau^\#$ are primitive integral quadratic forms.*

Proof. We need to show that

$$(x_\tau)_p = \frac{d_{\mathbb{Z}}(\Lambda)_p}{d(\Lambda_\tau)_p}$$

and

$$(y_\tau)_p = Dd(\Lambda_\tau)_p$$

for all primes p.

If $p \mid d(\Lambda)$, then $(x_\tau) = (1)$ and $(y_\tau) = (p)$ by (7.19). We also have $d_{\mathbb{Z}}(\Lambda)_p = d(\Lambda_\tau)_p = (p)$, so we are done.

If $p \mid D$, then we have by hypothesis that $d_{\mathbb{Z}}(\Lambda)_p = d(\Lambda_\tau)_p = (1)$. The claim now follows by the explicit description in (7.20).

If finally $p \nmid d(\Lambda)$ and $p \nmid D$, then we have $L_\iota^\# = L_\iota$, $d(L_\iota) \in \mathbb{Z}_p^*$ and $\Lambda_p \cong C_0(L_\iota^\#, \dot{q}_\iota^\#)$. Furthermore, we have $(L_\tau)_p = \gamma^* L_\iota$, where $\gamma \in L_\iota$ is primitive. Hence $x_\tau \in \mathrm{nr}(\gamma)^{-1}\mathbb{Z}_p^*$ and $y_\tau \in \mathrm{nr}(\gamma)\mathbb{Z}_p^*$. By lemma 7.10, we

have $\Lambda_{\iota,\gamma} \cong C_0(L^{\#}_{\iota,\gamma}, \dot{q}^{\#}_{\iota,\gamma})$. But $\Lambda_{\iota,\gamma} = (\Lambda_\tau)_p$, so we are done if we show that $d((L^{\#}_{\iota,\gamma}, \dot{q}^{\#}_{\iota,\gamma})) = (\mathrm{nr}(\gamma))$.

We have $\gamma\mathbb{Z}_p + L^{\#}_{\iota,\gamma} \subseteq L^{\#}_{\iota}$. Using the fact that γ is a primitive element of L_ι, we get $\mathrm{tr}(\gamma^* L^{\#}_{\iota}) = \mathbb{Z}_p$. On the other hand, we get $\mathrm{tr}(\gamma^*(\gamma\mathbb{Z}_p + L^{\#}_{\iota,\gamma})) = \mathrm{tr}(\gamma^*\gamma)\mathbb{Z}_p = 2\,\mathrm{nr}(\gamma)\mathbb{Z}_p$, and so we see that $[L^{\#}_{\iota} : \gamma\mathbb{Z}_p + L^{\#}_{\iota,\gamma}] = (2\,\mathrm{nr}(\gamma))$. Using this, we get

$$d(\gamma\mathbb{Z}_p + L^{\#}_{\iota,\gamma}) = (2\,\mathrm{nr}(\gamma))^2 d(L^{\#}_{\iota}).$$

We can also compute $d(\gamma\mathbb{Z}_p + L^{\#}_{\iota,\gamma})$ by noting that $\gamma\mathbb{Z}_p + L^{\#}_{\iota,\gamma}$ is an orthogonal sum, and hence we have

$$d(\gamma\mathbb{Z}_p + L^{\#}_{\iota,\gamma}) = 2\,\mathrm{nr}(\gamma) 2 d(L^{\#}_{\iota,\gamma}).$$

We conclude that $d(L^{\#}_{\iota,\gamma}) = (\mathrm{nr}(\gamma))$, since $d(L^{\#}_{\iota}) = (1)$. □

The next result is a statement of the fact that the quadratic lattice (L_τ, q_τ), together with the action of Λ^1 on L_τ is essentially independent on the choice of τ.

Proposition 7.13. *Let τ and ν be two special involutions on Λ of the same local type. Then there exists an isomorphism of $\mathbb{Z}$-lattices $f_{\nu,\tau} : L_\tau \to L_\nu$ such that $q_\nu(f_{\nu,\tau}(\beta)) = s_{\nu,\tau} q_\tau(\beta)$ for all $\beta \in L_\tau$, where $s_{\nu,\tau} = \pm 1$. The isomorphism $f_{\nu,\tau}$ also commutes with the actions of Λ^1 on L_τ and L_ν respectively, i.e. the following diagram commutes*

$$\begin{array}{ccc} \Lambda^1 \times L_\tau & \xrightarrow{(\lambda,\beta)\mapsto\tau(\lambda)\beta\lambda^*} & L_\tau \\ {\scriptstyle Id\times f_{\nu,\tau}}\downarrow & & \downarrow{\scriptstyle f_{\nu,\tau}} \\ \Lambda^1 \times L_\nu & \xrightarrow{(\lambda,\beta)\mapsto\nu(\lambda)\beta\lambda^*} & L_\nu\,. \end{array} \tag{7.22}$$

Proof. Let γ be as in lemma 7.5. Define $f_{\nu,\tau}$ by $f_{\nu,\tau}(l) = \gamma^* l$. Since the map $L_\tau \to \mathbb{Z}$ given by $\beta \mapsto q_\nu(f_{\nu,\tau}(\beta)) = \mathrm{nr}(\gamma) x_\nu / x_\tau q_\tau(\beta)$ is a primitive integral form, and q_τ is a primitive integral form, we get that $s_{\nu,\tau} = \mathrm{sign}(\mathrm{nr}(\gamma))$.

To show that the diagram commutes, we have to verify that

$$\gamma^*\tau(\lambda)\beta\lambda^* = \nu(\lambda)\gamma^*\beta\lambda^*$$

for all $\beta \in L_\tau$ and $\lambda \in \Lambda^1$. But this holds, since $\nu(\lambda) = \gamma^{-1}\tau(\lambda)\gamma$ by hypothesis. □

By proposition 7.13, we can now fix one choice of a special involution τ and we write $\tau(x) = \overline{x}$. This choice will correspond to a choice of a local type of involutions, but it will have no practical importance. We now write

$$A_{\mathbb{Q}} = A_\tau \quad \text{and} \quad \Lambda_{\mathbb{Z}} = \Lambda_\tau,$$

and furthermore we will from now on suppress the index τ from the notation, so we write for example (L, q) instead of (L_τ, q_τ), and similarly $(L^\#, q^\#)$, $(L_\beta^\#, q_\beta^\#)$, W, A_β and Λ_β.

We now formulate a result which gives a complete local description of the lattice (L, q).

Proposition 7.14. *(L, q) is an integral lattice with discriminant $d_{\mathbb{Z}}(\Lambda)^2 D^3$ and $(L^\#, q^\#)$ is an integral lattice with discriminant $d_{\mathbb{Z}}(\Lambda)^2 D$. More precisely, if p is a prime and we let $q_p : L_p \to \mathbb{Z}_p$ denote the localisations of q at p, then we have*

i) if p is split in k and $p \nmid d(\Lambda)$, then q_p is isometric to the form $xy + zw$,

ii) if p is split in k and $p \mid d(\Lambda)$, then q_p is isometric to $\mathrm{nr} : \Omega_p \to \mathbb{Z}_p$,

iii) if p is unramified in k, then q_p is isometric to $x^2 - dy^2 + zw$ if $p \neq 2$ and to $x^2 + xy + y^2 + zw$ if $p = 2$,

iv) if p is ramified in k, then q_p is isometric to $\eta(x^2 - dy^2 - Dzw)$, where η is a unit in $\mathbb{Z}_p$.

Proof. Follows directly from (7.19) and (7.20). □

Lemma 7.15. *The discriminant of the ternary quadratic lattice $(L_\beta^\#, q_\beta^\#)$ is $q(\beta) d_{\mathbb{Z}}(\Lambda)$.*

Proof. We have that $\beta\mathbb{Z} + L_\beta^\# \subseteq L^\#$. Using the fact that β is a primitive element of L, we get $\mathrm{tr}(\beta^* L^\#) = \mathbb{Z}$. On the other hand, we get $\mathrm{tr}(\beta^*(\beta\mathbb{Z} + L_\beta^\#)) = \mathrm{tr}(\beta^*\beta)\mathbb{Z} = 2\,\mathrm{nr}(\beta)\mathbb{Z}$, and so we see that $[L^\# : \beta\mathbb{Z} + L_\beta^\#] = 2\,\mathrm{nr}(\beta)$. Using this, we get

$$d(\beta\mathbb{Z} + L_\beta^\#) = (2\,\mathrm{nr}(\beta))^2 d(L^\#).$$

We can also compute $d(\beta\mathbb{Z} + L_\beta^\#)$ by noting that $\beta\mathbb{Z} + L_\beta^\#$ is an orthogonal sum, and hence we have

$$d(\beta\mathbb{Z} + L_\beta^\#) = 2q^\#(\beta) 2 d(L_\beta^\#).$$

Solving for $d(L_\beta^\#)$ gives

$$d(L_\beta^\#) = \frac{(2\,\mathrm{nr}(\beta))^2 d(L^\#)}{4q^\#(\beta)}$$

and, recalling that $d(L^\#) = d(\Lambda)_\mathbb{Z}^2 D$ and $q^\#(\beta) = d_0(\Lambda_\mathbb{Z}) D\,\mathrm{nr}(\beta)$, we get

$$d(L_\beta^\#) = \frac{d_\mathbb{Z}(\Lambda)^2}{d(\Lambda_\mathbb{Z})}\,\mathrm{nr}(\beta) = q(\beta) d_\mathbb{Z}(\Lambda). \qquad \square$$

Theorem 7.16. *The discriminant of Λ_β equals the least common multiple of $q(\beta)$ and $d_0(\Lambda)$.*

Proof. By lemma 7.10 and lemma 7.11, we know that the image of the order $C_0(L_\beta^\#, q_\beta^\#)$ is $\Lambda_\beta \cap \Theta$. If $p \nmid d(\Lambda)$, then we have by lemma 7.11 that $\Lambda_p = \Theta_p$, and hence $(\Lambda_\beta)_p \cong C_0(L_\beta^\#, q_\beta^\#)$. The claim therefore follows from lemma 7.15 and proposition 2.7. If $p \mid d(\Lambda)$, then we know that $(\Lambda_\beta)_p \cong \Omega_p$. Hence the claim follows, since by the description of q_p in part ii) of proposition 7.14, we have that $p^2 \nmid q(\beta)$. $\square$

Corollary 7.17. *The quaternary space (L, q) represents $d_0(\Lambda_\mathbb{Z})/d_0(\Lambda)$.*

Proof. We can use theorem 7.16 to determine $L \cap \mathbb{Z}$. Let $L \cap \mathbb{Z} = (b)$, where $b > 0$. We have $\Lambda_b = \Lambda_\mathbb{Z}$, and hence we get that $d_0(\Lambda_\mathbb{Z})$ is the least common multiple of $d_0(\Lambda)b^2/d_0(\Lambda_\mathbb{Z})$ and $d_0(\Lambda)$. From this we get that the only possibility is $b = d_0(\Lambda_\mathbb{Z})/d_0(\Lambda)$. We now get $q(b) = d_0(\Lambda_\mathbb{Z})/d_0(\Lambda)$ and we are done. $\square$

We remark that from corollary 7.17, it follows that the unit $\eta \in \mathbb{Z}_p^*$ occurring in part iv) of proposition 7.14 can be chosen to be $d_0(\Lambda_\mathbb{Z})/d_0(\Lambda)$.

7.3 Local description of the order Λ_β

In this section, we are going to determine the local isomorphism classes of the order Λ_β, i.e. determine the genus of Λ_β.

If $p \mid d(\Lambda)$, then we already know that $(\Lambda_\beta)_p \cong \Omega_p$ by lemma 4.11.

Assume that $p \nmid d(\Lambda)$. Then we have $A_p \cong M_2(k_p)$ by lemma 4.3. Consider the 2-dimensional k_p-module $V_p = k_p \oplus k_p$, and the R_p-module $M_p = R_p \oplus R_p \subset V_p$. We identify A_p with $\mathrm{End}_{k_p}(V_p)$, and Λ_p with $\mathrm{End}_{R_p}(M_p)$.

Lemma 7.18. *There exists a non-degenerate hermitian form $h : V_p \times V_p \to k_p$ such that*

$$h(av, u) = h(v, \overline{a}^* u) \text{ for all } a \in A_p,\ u, v \in V_p.$$

In other words, the hermitian form h has the map $a \mapsto \overline{a}^*$ as its adjoint involution. Furthermore, h is uniquely determined up to a non-zero factor in $\mathbb{Q}_p$.

Proof. Let g be a non-degenerate hermitian form on V_p. Then $g(au, v) = g(u, \widetilde{a}^* v)$ for all $u, v \in V_p$, where $a \mapsto \widetilde{a}$ is some involution of type 2 on A_p. Now, by lemma 4.2, there exists an invertible element $m \in A_p$ such that $\widetilde{m}^* = m$ and $\overline{a} = m^{-1}\widetilde{a}m$ for all $a \in A_p$. Let $h(u, v) = g(mu, v)$. We have $h(u, v) = g(mu, v) = g(u, mv) = \overline{g(mv, u)} = \overline{h(v, u)}$, so h is a hermitian form. Furthermore, we get $h(au, v) = h(u, m^{-1}\widetilde{a}^* mv) = h(u, \overline{a}^* v)$ and hence h has the required properties. The uniqueness is clear. □

Choose now one form h as in lemma 7.18. Given an element $\beta \in A$ with $\overline{\beta}^* = \beta$, we want to determine whether

$$(A_\beta)_p = \{a \in A_p \mid \beta a = \overline{a}\beta\}$$

is a skew field or not. We define

$$h_\beta(v, u) = h(\beta v, u),$$

for $v, u \in V_p$. It is readily verified that h_β is a hermitian form on V_p.

Lemma 7.19. *$\beta a = \overline{a}\beta$ if and only if $h_\beta(av, u) = h_\beta(v, a^* u)$ for all $u, v \in V_p$.*

Proof. $h_\beta(av, u) = h_\beta(v, a^* u)$ if and only if $h(\beta av, u) = h(\beta v, a^* u)$ if and only if $h(\beta av, u) = h(\overline{a}\beta v, u)$. The claim follows. □

We have thus shown that $(\Lambda_\beta)_p$ is isomorphic to the order constructed from the hermitian R_p-plane (M_p, h_β) by (5.11). In particular, we have by proposition 5.19:

Proposition 7.20. *If $p \nmid d(\Lambda)$, then $(\Lambda_\beta)_p$ is R_p-primitive.*

We remark that the orders Λ_β are not R-primitive in our case, since $d_0(\Lambda) \neq 1$. Namely, if $p \mid d(\Lambda)$, then it is impossible to embed $R_p \cong \mathbb{Z}_p \times \mathbb{Z}_p$ in $(\Lambda_\beta)_p \cong \Omega_p$.

If we apply proposition 2.30, we get the following corollary of proposition 7.20:

Corollary 7.21. *The Eichler number of the order $(\Lambda_\beta)_p$ is given by*

i) $e((\Lambda_\beta)_p) = 1$ *if p is split and $p \nmid d(\Lambda)$,*

ii) $e((\Lambda_\beta)_p) = -1$ *if p is unramified and $p \mid d(\Lambda_\beta)$,*

iii) $e((\Lambda_\beta)_p) = 0$ *if* p *is ramified and* $p^2 \mid d(\Lambda_\beta)$.

Now we want to determine whether $(A_\beta)_p$ splits or not. If p splits in k (and $p \nmid d(\Lambda)$), then we know from lemma 4.3 that $(A_\beta)_p$ splits.

Assume that p is unramified in k. Then, by corollary 2.20, we have that $(A_\beta)_p$ splits if and only if $v_p(d(\Lambda_\beta)) = v_p(q(\beta))$ is even.

Assume that p is ramified in k. According to proposition 5.16, we have that $(A_\beta)_p$ is a split algebra if and only if

$$-\det(h_\beta) = -\det(h)\,\mathrm{nr}(\beta)$$

defines a trivial class in $\mathbb{Q}_p^*/\,\mathrm{nr}_{k_p/\mathbb{Q}_p}(k_p^*)$ (recall that $\mathbb{Q}_p^*/\,\mathrm{nr}_{k_p/\mathbb{Q}_p}(k_p^*)$ is isomorphic to $\mathbb{Z}/2$ if k_p is a field). If $\beta = 1$, then $A_\beta = A_\mathbb{Q}$, so A_β splits since the involution $a \to \overline{a}$ is assumed to be special. We conclude that $-\det(h) \in \mathrm{nr}_{k_p/\mathbb{Q}_p}(k_p^*)$. We summarise:

Proposition 7.22. *Let* p *be a prime. If* p *is split in* k*, then* $(A_\beta)_p$ *is split if and only if* $p \nmid d(\Lambda)$*. If* p *is unramified in* k*, then* $(A_\beta)_p$ *is split if and only if* $v_p(q(\beta))$ *is even. If* p *is ramified in* k*, then* $(A_\beta)_p$ *is split if and only if* $\mathrm{nr}(\beta) \in \mathrm{nr}_{k_p/\mathbb{Q}_p}(k_p^*)$.

By proposition 2.33, we have now completely determined the genus of the order Λ_β. More precisely, we have:

Proposition 7.23. *If* p *is split in* k *and* $p \mid d(\Lambda)$*, then* $(\Lambda_\beta)_p \cong \Omega_p$*. Otherwise* $(\Lambda_\beta)_p$ *is the unique Bass order, which allows an embedding of* R_p*, has discriminant given by theorem* 7.16 *and splitting behaviour as described in proposition* 7.22.

7.4 The curves F_N

Definition 7.24. For every positive integer N, we define

$$F_N = \bigcup_\beta F_\beta,$$

where β runs over all primitive elements $\beta \in L$ such that $q(\beta) = N$.

The following result will also be a consequence of the calculations in chapter 8, but we present an independent proof.

Proposition 7.25. *Every curve* F_N *is a finite* (*possibly empty*) *union of irreducible curves.*

Proof. Let $O^+(L,q)$ denote the group of proper integral automorphisms of (L,q). By general theory of integral quadratic forms, we know that if N is a non-zero integer, then the set of $\beta \in L$ with $q(\beta) = N$ decomposes into finitely many orbits under the action of $O^+(L,q)$ (see [7], lemma 6.1). The group Λ^1 generates a subgroup of $O^+(L,q)$ under the action given by (7.7). We need to show that this subgroup has finite index in $O^+(L,q)$.

If w is an invertible element of A with $\mathrm{nr}(\beta) \in \mathbb{Q}$, then we define the map $g_w : W \to W$ by

$$g_w(x) = \overline{w}xw^{-1}.$$

Clearly $g_w \in O^+(W,q)$ and, in fact, every element of $O^+(W,q)$ is of the form g_w for some w (see [34], proposition 2). Hence we have

$$O^+(L,q) = \{g_w \mid w \in A,\ \ \mathrm{nr}(w) \in \mathbb{Q}^*,\ \overline{w}L = Lw\}.$$

Assume now that $\omega \in A$ with $\mathrm{nr}(\omega) \in \mathbb{Q}^*$ and $\overline{\omega}L = L\omega$. We get

$$\overline{\omega}L^{\#} = L^{\#}\omega,$$

and hence $\omega^{-1}\Theta\omega = \Theta$. By lemma 7.11, we get therefore

$$\omega^{-1}\Lambda\omega = \Lambda,$$

i.e. $\omega \in N(\Lambda)$, the normaliser of Λ. Now $[N(\Lambda) : k^*\Lambda^1] < \infty$ by lemma 2.35, so we get that

$$\{g_\lambda \mid \lambda \in \Lambda^1\}$$

is a subgroup of $O^+(L,q)$ of finite index. □

7.5 Construction of involutions on X

It is clear that there exists $\beta \in L$ such that Λ_β is an Eichler order – take for example β such that $q(\beta) = N$ is square free. Using such elements β, we can construct involutions on X by the following result:

Lemma 7.26. *Assume that Λ_β is an Eichler order. There exists a map $T = T_\beta \in \mathrm{Aut}(\mathcal{H}\times\mathcal{H}) \setminus \mathrm{Aut}(\mathcal{H}) \times \mathrm{Aut}(\mathcal{H})$ such that*

i) $\Gamma \cup T\Gamma$ *is a subgroup of* $\mathrm{Aut}(\mathcal{H}\times\mathcal{H})$,

ii) $T(C_\beta) = C_\beta$.

Proof. Let $s \in \Lambda_\beta$ be the element given by lemma 4.12, when this lemma is applied to the involution $\sigma(x) = \beta^{-1}\overline{x}\beta$. Define the map T by

$$T(z_1, z_2) = (s\beta^* z_2, \overline{s}\beta z_1),$$

for $z_1, z_2 \in \mathcal{H}$. We get, for all $z \in \mathcal{H}\times\mathcal{H}$,

$$T\lambda T(z) = (s\beta^*\overline{\lambda}\overline{s}\beta)(z) = (s\beta^{-1}\overline{\lambda}\beta s^{-1})(s^2)(z).$$

Now, by hypothesis, we have that $s\beta^{-1}\overline{\lambda}\beta s^{-1} \in \Lambda^1$ and $s^2 \in \mathbb{Z}\Lambda^1$, and this shows that $T\Gamma T = \Gamma$. Furthermore, we get that

$$\begin{aligned} T(C_\beta) &= \{(s\beta^*\beta z_0, \overline{s}\beta z_0) \mid z_0 \in \mathcal{H}\} = \\ &= \{(sz_0, \beta s z_0) \mid z_0 \in \mathcal{H}\} = \\ &= C_\beta. \end{aligned}$$

□

It may be of interest to note that we also get the following result:

Corollary 7.27. *Let A be a quaternion algebra over k and assume that σ is an involution of type 2 on A. If Λ is a maximal order in A, then we have $\sigma(\Lambda) \cong \Lambda$.*

Proof. By lemma 4.10, there exist an involution τ which is special with respect to Λ. Take $w \in A^*$ such that $\tau(x) = w\sigma(x)w^{-1}$ for all $x \in A$. Take $\beta \in L_\tau$ such that $\Lambda_{\tau,\beta}$ is an Eichler order. Let s be the element given by lemma 4.12 applied to the involution $x \mapsto \beta^{-1}\tau(x)\beta$. If we put $\gamma = s\beta^{-1}w$, then $\gamma\sigma(\Lambda)\gamma^{-1} = s\beta^{-1}\tau(\Lambda)\beta s^{-1} = \Lambda$. □

8 The number of components of F_N

In this chapter, we will determine the number of irreducible components of the curves F_N and the group index $[\Gamma_\beta : \Lambda^1_\beta]$ for $\beta \in L$. The method we will use is to relate these questions to a question about integral Λ-hermitian forms in the sense of section 5.4. In the case of Hilbert modular surfaces, Franke [14] and Hausmann [20] solved the corresponding problem using the theory of (ordinary) hermitian lattices. Hence, our proof is just a generalisation of theirs, using a suitable reformulation of the problem.

The technical tool, which we need, is an approximation result stating that every $\mathrm{SU}(A, \Phi)$-genus of Λ-lattices only contains one class (recall the definitions from section 5.3). In [41], Shimura shows that every $\mathrm{SL}(V, h)$-genus of R-lattices $M \subset V$, where $h : V \to k$ is a hermitian form (in the usual sense) of rank 2, consists of only one class. That situation can be translated to our setting in the following way.

Fix a 2-dimensional k-vector space V with a non-degenerate hermitian form h and a free R-lattice $M_0 \subset V$. Let $A = \mathrm{End}_k(V)$ be a k-algebra with the maximal R-order $\Lambda = \mathrm{End}_R(M_0)$. Define implicitly a type 2 involution $a \mapsto \overline{a}$, by

$$h(au, v) = h(u, \overline{a}^* v),$$

for all $u, v \in V$. Define an A-hermitian form Φ on A by $\Phi(x, y) = \overline{x}^* y$. We have a natural one-to-one correspondence between free R-modules $M \subset V$ and free right Λ-modules $\mathcal{L}$, given by the maps

$$M \mapsto \mathrm{End}_R(M_0, M) \subset A,$$

and

$$\mathcal{L} \mapsto \mathcal{L}(M_0) \subset V.$$

It is straightforward to check that this gives a one-to-one correspondence between $\mathrm{SL}(V, h)$-classes of free R-lattices M and $\mathrm{SU}(A, \Phi)$-classes of free Λ-lattices $\mathcal{L}$.

Hence, one can say that we extend some of the results in [41] from the case $A = M_2(k)$, to the case where A is a totally indefinite quaternion algebra over k which has a type 2 involution. As it turns out, the proofs in [41] work almost unchanged in this more general setting, but we include all modified proofs for completeness.

8.1 Approximation theory

Consider an A-hermitian space (A, Φ), where A is considered as a right A-module, and $\Phi : A \times A \to A$ is a non-degenerate A-hermitian space in the sense of section 5.3. Recall the definition of $\mathrm{SU}(A, \Phi)$-classes of Λ-lattices $\mathcal{L}$ in section 5.3. Our goal in this section is to show that each genus of Λ-lattices only contains one class.

The following lemma is well known (see lemma 5.3 in [41]):

Lemma 8.1. *Let W be a finite dimensional vector space over $\mathbb{Q}_p$ and M a $\mathbb{Z}_p$-lattice in W. If $f, g \in \mathrm{GL}(W)$ and $(f - g)(M) \subseteq pf(M)$, then $f(M) = g(M)$.*

The following result should be compared with theorem 5.12 in [41]:

Theorem 8.2. *Let P be a finite set of primes and let σ_p be an element of $\mathrm{SU}(A_p, \Phi)$ for each $p \in P$. Let $\mathcal{L}$ be a Λ-lattice in A and e a positive integer. Then there exists an element $\sigma \in \mathrm{SU}(A, \Phi)$ such that $(\sigma - \sigma_p)\mathcal{L}_p \subseteq p^e \mathcal{L}_p$ for every $p \in P$ and $\sigma \mathcal{L}_p = \mathcal{L}_p$ for all primes p not in P.*

Proof. Define the quaternion algebra

$$A_\Phi = \{\alpha \in A \mid \Phi(\alpha x, y) = \Phi(x, \alpha^* y) \text{ for all } x, y \in A\}.$$

A_Φ is an indefinite quaternion algebra, and $\mathrm{SU}(A,\Phi) = A_\Phi^1$. Take an R-order Λ' in A such that $\Lambda'_\Phi = \Lambda' \cap A_\Phi$ is a maximal order in A_Φ. Choose a positive integer f such that $f\sigma_p \in (\Lambda'_\Phi)_p$ for all $p \in P$. Let P_1 be the set of primes p such that $\mathcal{L}_p \neq \Lambda'_p$, P_2 the set of prime divisors of f and $Q = P \cup P_1 \cup P_2$. There is an integer $d > e$ such that $p^d \mathcal{L}_p \subseteq \Lambda'_p \subseteq p^{-d}\mathcal{L}_p$ for all $p \in Q$. Take $\gamma \in \Lambda'_\Phi$ such that $\gamma \equiv f\sigma_p \bmod f^3 p^{3d}(\Lambda'_\Phi)_p$ for $p \in P$ and $\gamma \equiv f \bmod f^3 p^{3d}(\Lambda'_\Phi)_p$ for $p \in Q \setminus P$. Then $\gamma\gamma^* \equiv f^2 \bmod f^3 \prod_{p\in Q} p^{3d}$. By Eichler's approximation theorem (see [30], theorem 5.2.10), there exists an element α in Λ'_Φ such that $\alpha\alpha^* = f^2$ and $\alpha \equiv \gamma \bmod f\prod_{p\in Q} p^{3d}\Lambda'_\Phi$. Putting $\sigma = f^{-1}\alpha$, we have $\sigma\sigma^* = 1$, so $\sigma \in \mathrm{SU}(A,\Phi)$. Now, for $p \in P$ we get $(\sigma - \sigma_p)\mathcal{L}_p \subseteq p^{-d}(f^{-1}\alpha - f^{-1}\gamma + f^{-1}\gamma - \sigma_p)\Lambda'_p \subseteq p^{2d}\Lambda'_p \subseteq p^d\mathcal{L}_p$. If $p \in Q \setminus P$, we get $(\sigma - 1)\mathcal{L}_p \subseteq f^{-1}p^{-d}(\alpha - \gamma + \gamma - f)\Lambda'_p \subseteq p^d\mathcal{L}_p$, so by lemma 8.1, we get $\sigma\mathcal{L}_p = \mathcal{L}_p$. Finally, if $p \notin Q$, then f is a unit in $\mathbb{Z}_p$. Hence σ is a unit in Λ'_p, so $\sigma\mathcal{L}_p = f^{-1}\alpha\Lambda'_p = \Lambda'_p = \mathcal{L}_p$. □

The following is closely related to theorem 5.19 in [41]:

Theorem 8.3. *With respect to* $\mathrm{SU}(A,\Phi)$*, every genus of* Λ*-lattices consists of only one class.*

Proof. Let $\mathcal{L}$ and $\mathcal{L}'$ be Λ-lattices in A belonging to the same genus with respect to $\mathrm{SU}(A,\Phi)$. Let P be the set of primes p such that $\mathcal{L}_p \neq \mathcal{L}'_p$. For each $p \in P$ there exists an element σ_p of $\mathrm{SU}(A_p,\Phi)$ such that $\sigma_p\mathcal{L}_p = \mathcal{L}'_p$. By theorem 8.2, there exists an element σ of $\mathrm{SU}(A,\Phi)$ such that $(\sigma - \sigma_p)\mathcal{L}_p \subseteq p\sigma\mathcal{L}_p$ for $p \in P$ and $\sigma\mathcal{L}_p = \mathcal{L}_p$ for $p \notin P$. Lemma 8.1 now gives us that $\sigma\mathcal{L}_p = \sigma_p\mathcal{L}_p = \mathcal{L}'_p$ for $p \in P$. Hence $(\sigma\mathcal{L})_p = \mathcal{L}'_p$ for all primes so we have $\sigma\mathcal{L} = \mathcal{L}'$. □

8.2 The number of components

Let $N > 0$ be an integer. Let f_N denote the number of components of the curve F_N. To be able to compute f_N, we first need some technical lemmas.

Lemma 8.4. *If* $\beta \in A$ *is an element with* $\overline{\beta}^* = \beta$ *and* $\mathrm{nr}(\beta) \neq 0$*, and if* $x \in k^*$ *with* $x\overline{x} = 1$*, then there exists* $\gamma \in A$ *with* $\overline{\gamma}^*\beta\gamma = \beta$ *and* $\mathrm{nr}(\gamma) = x$*.*

Proof. Put $A_\beta = \{\alpha \in A \mid \beta\alpha = \overline{\alpha}\beta\}$. We observe that $\mathrm{nr} : A_\beta \to \mathbb{Q}$ is surjective, since this map is an indefinite quaternary quadratic form (this follows e.g. from Meyers theorem, see [40], p. 43). Take an element $\eta \in k$

with $\eta/\overline{\eta} = x$, which exists by Hilbert's theorem 90 (see [26], p. 34), and an element $c \in A_\beta$ such that $\eta\overline{\eta}\,\mathrm{nr}(c) = 1$. Let $\gamma = \eta c$. We get that $\mathrm{nr}(\gamma) = \eta^2\,\mathrm{nr}(c) = \eta/\overline{\eta} = x$ and $\overline{\gamma}^*\beta\gamma = \eta\overline{\eta}\overline{c}^*\beta c = \eta\overline{\eta}\overline{\mathrm{nr}(c)}\beta = \beta$. □

Lemma 8.5. *Let $\beta_1, \beta_2 \in L$ with $\mathrm{nr}(\beta_1) = \mathrm{nr}(\beta_2)$. Then there exists a hermitian form $\Phi : A \times A \to A$ and elements $x_1, x_2 \in A$ such that $\mathrm{nr}(x_1) = \mathrm{nr}(x_2)$ and*

$$\beta_i = \Phi(x_i, x_i),$$

for $i = 1, 2$.

Proof. Define two forms Φ_i by $\Phi_i(x, y) = \overline{y}^*\beta_i x$, for $i = 1, 2$. According to theorem 5.7, there exists an element $s \in A$ such that $\Phi_1(sx, sy) = \Phi_2(x, y)$ for all $x, y \in A$. Thus $\beta_2 = \Phi_2(1, 1) = \Phi_1(s, s) = \overline{s}^*\beta_1 s$. Let $x = \mathrm{nr}(s)^{-1}$. Then we have that $x\overline{x} = 1$, so, by lemma 8.4, there exists $\gamma \in A$ with $\mathrm{nr}(\gamma) = x$ and $\overline{\gamma}^*\beta_1\gamma = \beta_1$. Now we get that $\beta_2 = \Phi_1(\gamma s, \gamma s)$, so we can choose $\Phi = \Phi_1$, $x_1 = 1$ and $x_2 = \gamma s$. □

Lemma 8.6. *Let Φ, β_i and x_i be as in lemma 8.5. Define the two Λ-lattices $\mathcal{L}_i = x_i\Lambda$, for $i = 1, 2$. Then there exists $\sigma \in \mathrm{SU}(A, \Phi)$ such that $\sigma\mathcal{L}_2 = \mathcal{L}_1$ if and only if there exists $\mu \in \Lambda^1$ such that $\beta_2 = \overline{\mu}^*\beta_1\mu$.*

Proof. Assume first that $\sigma\mathcal{L}_2 = \mathcal{L}_1$ for some $\sigma \in \mathrm{SU}(A, \Phi)$. Then $\sigma x_2\Lambda = x_1\Lambda$, so $\sigma x_2 = x_1\mu$ for some $\mu \in \Lambda^*$. This gives $\mathrm{nr}(\mu) = 1$, and furthermore

$$\beta_2 = \Phi(x_2, x_2) = \Phi(\sigma x_2, \sigma x_2) = \Phi(x_1\mu, x_1\mu) = \overline{\mu}^*\beta_1\mu.$$

Assume now that $\beta_2 = \overline{\mu}^*\beta_1\mu$, where $\mu \in \Lambda^1$. If we put $\sigma = x_1\mu x_2^{-1}$, then $\sigma\mathcal{L}_2 = \mathcal{L}_1$ and $\mathrm{nr}(\sigma) = 1$. Furthermore,

$$\Phi(\sigma x_2, \sigma x_2) = \Phi(x_1\mu, x_1\mu) = \overline{\mu}^*\beta_1\mu = \beta_2 = \Phi(x_2, x_2),$$

so $\sigma \in \mathrm{SU}(A, \Phi)$. □

We write $\beta_1 \sim_{\Lambda^1} \beta_2$ if there exists $\mu \in \Lambda^1$ such that $\beta_2 = \overline{\mu}^*\beta_1\mu$. Let analogously $\beta_1 \sim_{\Lambda_p^1} \beta_2$ denote the corresponding property in the local case. Then we get the following corollary to theorem 8.3:

Corollary 8.7. *If $\beta_1, \beta_2 \in L$, then $\beta_1 \sim_{\Lambda^1} \beta_2$ if and only if $\beta_1 \sim_{\Lambda_p^1} \beta_2$ for every prime p.*

Now we are prepared to compute f_N. Let $L(N)$ denote the set

$$L(N) = \{\beta \in L \mid \beta \text{ primitive and } q(\beta) = N\}.$$

Two elements $\beta_1, \beta_2 \in L(N)$ are equivalent if there exists $\mu \in \Lambda^1$ such that $\beta_2 = \pm\overline{\mu}^* \beta_1 \mu$, i.e. if $\beta_2 \sim_{\Lambda^1} \pm\beta_1$. We have that f_N is the number of classes in $L(N)$ under this equivalence relation.

Take an element $\beta \in L(N)$. Recall that the group Γ_β is a group extension of Λ^1_β of degree 1 or 2. We have in fact that $[\Gamma_\beta : \Lambda^1_\beta] = 2$ if and only if $-\beta \sim_{\Lambda^1} \beta$. Hence, we get the following result from corollary 8.7, lemma 5.13 and proposition 5.15 (and the observation that if $(-1, D)_p = 1$, then $p \mid d$):

Proposition 8.8. $[\Gamma_\beta : \Lambda^1_\beta] = 2$ *if and only if the following conditions hold for every prime* p *such that* $p \mid D$:

i) *if* $(-1, D)_p = 1$, *then* $p \mid q(\beta)$,

ii) *if* $(-1, D)_p = -1$, *then* $v_p(d) \leq v_p(q(\beta)) < 2v_p(D)$.

Since $[\Gamma_\beta : \Lambda^1_\beta]$ only depends on $q(\beta)$, proposition 8.8 defines implicitly a function κ on the set of all integers, which are primitively represented by (L, q), such that

$$[\Gamma_\beta : \Lambda^1_\beta] = \kappa(N),$$

for all $\beta \in L(N)$.

We now want to determine which positive integers N that are primitively represented by q, i.e. when $L(N)$ is non-empty. By theorem 3.8, N is primitively represented by q if and only if N is primitively represented by q_p for every prime p. Using the local description of q given in proposition 7.14 and the fact that q represents the integer $B = d_0(\Lambda_\tau)/d_0(\Lambda)$ by corollary 7.17, we get: q represents N if and only if $p^2 \nmid N$ for every prime $p \mid d(\Lambda)$ and $\chi_{D,p}(NB) \neq -1$ for every prime $p \mid D$.

Assume now that N is such that if p is a prime with $p \mid d(\Lambda)$, then $p^2 \nmid N$. Then we get, by proposition 5.15, that the number of Λ^1-orbits of $L(N)$ is

$$\prod_{p \mid D} (\chi_{D,p}(NB) + 1) a_{D,p}(N).$$

If $\kappa(N) = 2$, then $-\beta \sim_{\Lambda^1} \beta$ for all $\beta \in L(N)$. If $\kappa(N) = 1$, then $-\beta \not\sim_{\Lambda^1} \beta$ for all $\beta \in L(N)$. We have therefore proved:

Theorem 8.9. *If there exists a prime* p *such that* $p \mid d(\Lambda)$ *and* $p^2 \mid N$, *then* $f_N = 0$. *Otherwise*

$$f_N = \frac{\kappa(N)}{2} \prod_{p \mid D} (\chi_{D,p}(NB) + 1) a_{D,p}(N),$$

where $B = d_0(\Lambda_\tau)/d_0(\Lambda)$.

9 The intersection points of the curves

In this chapter, we will examine how the curves F_β intersect each other. To each intersection point $z \in \mathcal{H}\times\mathcal{H}$ of two curves C_{β_1} and C_{β_2}, we associate an oriented binary form q_z. For a given oriented positive definite binary form φ, we introduce, in the same way as it is done in [22] for the case of Hilbert modular surfaces, a rational number $s(\varphi)$ which mainly depends on how many points in X that satisfy $q_z \cong \varphi$.

We determine which forms φ that can occur. It turns out that there exists a point $z \in \mathcal{H}\times\mathcal{H}$ such that $q_z \cong \varphi$ if and only if φ_p is primitively representable by q_p for every prime p (proposition 9.14). We also describe the classes of forms that correspond to elliptic points. The main result is a formula for $s(\varphi)$ given in theorem 9.16.

Observe that in this chapter, all results are proved under the assumption that neither 2 nor 3 is ramified in k.

9.1 Special points

For the rest of this chapter, we will for simplicity make the following assumption: We assume that neither 2 nor 3 is ramified in k, i.e. we assume that $d \equiv 1$ or $d \equiv 5 \pmod{12}$. In particular, the only orders of elliptic points that can occur are 2, 3 and 5.

We want to investigate the intersection points of the curves F_β on X. First, we make the following observation.

Lemma 9.1. *Let β_i be elements of L with $q(\beta_i) > 0$, for $i = 1, 2$. The two curves C_{β_1} and C_{β_2} intersect each other if and only if β_1 and β_2 generate a positive definite sublattice of (L, q).*

Proof. The claim is obvious if $C_{\beta_1} = C_{\beta_2}$, so we can assume that β_1 and β_2 are linearly independent. A straightforward calculation shows that the binary form

$$(x, y) \mapsto \mathrm{nr}(x\beta_1 + y\beta_2) \quad x, y \in \mathbb{Z}$$

is positive definite if and only if

$$\mathrm{tr}(\beta_1^{-1}\beta_2)^2 < 4\,\mathrm{nr}(\beta_1^{-1}\beta_2),$$

i.e. if and only if $\beta_1^{-1}\beta_2$ is an elliptic element. But the existence of an intersection point between C_{β_1} and C_{β_2} is clearly equivalent to the existence of a fixed point of the mapping $\beta_1^{-1}\beta_2 : \mathcal{H} \to \mathcal{H}$, so the claim follows. □

If z is the intersection point of two different curves C_{β_1} and C_{β_2}, then either z maps to a singular point on X, or to a transversal intersection point

between the curves F_{β_1} and F_{β_2}. If it happens that $F_{\beta_1} = F_{\beta_2}$, then this curve has a node at this point.

Let $z = (z_1, z_2)$ be a point in $\mathcal{H}\times\mathcal{H}$ and define

$$L_z = \{\beta \in L \mid q(\beta) > 0 \text{ and } \beta z_1 = z_2\} \cup \{0\}.$$

We also let $W_z = \mathbb{Q}L_z$ be the corresponding subspace of W, so $L_z = L \cap W_z$. If L_z is non-trivial, then it is a positive definite sublattice of L, and hence L_z is a $\mathbb{Z}$-lattice of rank 1 or 2.

Definition 9.2. The point z is called *special* if the lattice L_z has rank 2.

We want to show that it is possible to make consistent choices of orientations on all the lattices L_z, where z is a special point. Consider therefore the set

$$\mathcal{L} = \{(z, \beta) \in (\mathcal{H}\times\mathcal{H}) \times M_2(\mathbb{R}) \mid \det(\beta) > 0 \text{ and } \beta z_1 = z_2\} \cup \mathcal{H}\times\mathcal{H} \times \{0\}.$$

$\mathcal{L}$ is a 2-dimensional real vector bundle on $\mathcal{H}\times\mathcal{H}$. It is possible to extend the action of $\mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{R})$ on $\mathcal{H}\times\mathcal{H}$ to an action on $\mathcal{L}$ by

$$\gamma(z, \beta) = (\gamma z, \gamma_2 \beta \gamma_1^{-1}),$$

if $\gamma = (\gamma_1, \gamma_2) \in \mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{R})$. Hence, a choice of orientation on a specific fiber $\mathcal{L}_z$ extends naturally to an orientation on the vector bundle $\mathcal{L}$, and the orientation is preserved under the action of $\mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{R})$. In particular, it is preserved under the action of Λ^1. From now on, we fix such a choice of orientation.

If z is a special point, then the lattice L_z is naturally embedded via ϱ_0 in the fiber $\mathcal{L}_z$ of $\mathcal{L}$. Hence, we can choose a $\mathbb{Z}$-basis e_1, e_2 of L_z, which is positive as an $\mathbb{R}$-basis of $\mathcal{L}_z$ and define an oriented binary form (L_z, q_z) by

$$q_z = q|_{L_z},$$

and declaring that e_1, e_2 is a positive $\mathbb{Z}$-basis of L_z. If $z' = \lambda z$, where $\lambda \in \Lambda^1$, then we have $q_{z'} \cong q_z$. Hence, to any Λ^1-orbit of special points in $\mathcal{H}\times\mathcal{H}$, we have associated an isomorphism class of positive definite oriented binary forms.

If the point ζ in X is the image of $z \in \mathcal{H}\times\mathcal{H}$, then we say that ζ is *special* if z is special in the previous sense and we denote the isomorphism class of q_z by q_ζ. The goal of this chapter is to compute, for a given oriented positive definite binary form φ, the number of points in the set

$$X(\varphi) = \{\zeta \in X \mid q_\zeta \cong \varphi\},$$

Following Hirzebruch and Zagier (see [22]), we make the following definition:

Definition 9.3. Let φ be an oriented binary form. Then we put

$$s(\varphi) = \sum_{\zeta \in X(\varphi)} \frac{w_\varphi}{v_\zeta}, \tag{9.1}$$

where w_φ is the number of elements in the group of oriented automorphisms of φ, and v_ζ is the order of the isotropy group in Λ^1 of a point $z \in \mathcal{H} \times \mathcal{H}$ representing ζ (so w_φ and v_ζ both take values in the set $\{2, 4, 6\}$).

Let now M be any optimally embedded sublattice of L of rank 2 such that $q|_M$ is positive definite. Take two generators β_1, β_2 of M. The curves C_{β_1} and C_{β_2} intersect, by lemma 9.1, in some point z, and we have $M = L_z$. The lattice L_z is oriented, and hence we can associate to M an isomorphism class of oriented binary forms.

Definition 9.4. For M as above, we define

$$M^\perp = \{x \in L^\# \mid \mathrm{tr}(x^* M) = (0)\},$$

We let $q_M^\#$ denote the restriction of $q^\#$ to $M^\perp$.

We have that $M^\perp$ is an optimally embedded sublattice of $L^\#$ of rank 2. Note that $q_M^\#$ is a binary integral quadratic form, but that we do not consider it as an oriented binary form.

If φ is a positive definite oriented binary form, then a necessary condition for the existence of a point $z \in \mathcal{H} \times \mathcal{H}$ such that $\varphi \cong q_z$ is that (L_p, q_p) represents φ_p primitively for every prime p. We will see later, in proposition 9.14, that this condition is in fact sufficient.

Lemma 9.5. *Let p be a prime and φ_p a non-degenerate binary quadratic form over $\mathbb{Z}_p$. Then (L_p, q_p) represents φ_p primitively if and only if the following conditions are satisfied:*

i) if p is unramified in k, then $p \nmid m(\varphi_p)$,

ii) if $p \mid d(\Lambda)$, then φ_p is anisotropic, and it is either a modular form with $p^2 \nmid m(\varphi_p)$ or a non-modular form with $d(\varphi_p) = (p)$ if $p \neq 2$ and $d(\varphi_p) = (8)$ if $p = 2$,

iii) if $p \mid D$, then $p \mid d(\varphi_p)$ and $p^2 \nmid m(\varphi_p)$. Furhermore, if $m(\varphi_p) = 1$, then φ_p represents $B = d_0(\Lambda_\mathbb{Z})/d_0(\Lambda)$, and if $m(\varphi_p) = p$, then φ_p represents $-BD$.

Proof. Recall the local description of (L_p, q_p) given in proposition 7.14. We will show that the conditions given are necessary for φ_p to be primitively representable by (L_p, q_p). That they are sufficient is straightforward to check in each case, by using the local classification of binary forms over $\mathbb{Z}_p$ (see e.g. [7], chapter 8). In particular, it is clear that if p is split in k and $p \nmid d(\Lambda)$, then every non-degenerate binary form over $\mathbb{Z}_p$ is primitively represented by (L_p, q_p).

i) Assume that p is unramified in k. Assume that $p \mid m(\varphi_p)$. Then there exists a basis of L_p such that the matrix of q_p is of the form $Q = \left(\begin{smallmatrix} pA & C \\ C^t & E \end{smallmatrix}\right)$, where A, C and E are 2×2 matrices, and A (and E) has even entries on the diagonal if $p = 2$. If $p \neq 2$, then we immediately get $\det(Q) \equiv (\det(C))^2 \pmod{p}$, which would contradict proposition 7.14. If $p = 2$, then a calculation gives that $\det(Q)$ is a square modulo 8, so we get a contradiction in this case too.

ii) Assume now that $p \mid d(\Lambda)$, so we have that $(L_p, q_p) \cong (\Omega_p, \mathrm{nr})$. It is clear that φ_p must be anisotropic, since q_p is anisotropic. Furthermore, recall that if $x \in \Omega_p$ and $p^2 \mid \mathrm{nr}(x)$, then $x \in p\Omega_p$. Hence $p^2 \nmid q(x)$ for every primitive element $x \in L$. In particular, we get $p^2 \nmid m(\varphi_p)$. Assume now that φ_p is non-modular. Then there exists an orthogonal basis e_1, e_2 of M, and since $p^2 \nmid q(e_1), q(e_2)$, we get that $d(\varphi_p)$ is as claimed.

iii) Assume now that $p \mid D$. We have that q_p is isometric to the form $B(x^2 - dy^2 + Dzw)$. Now, if we reduce this form modulo p, the form we get has rank 1. Hence, every binary form φ_p represented by q_p has rank at most 1, when reduced modulo p. This shows that $p \mid d(\varphi_p)$.

Assume now that $p^2 \mid m(\varphi_p)$. Then we get that the matrix of q_p, in some basis, is of the block form $Q = \left(\begin{smallmatrix} p^2A & C \\ C^t & E \end{smallmatrix}\right)$. Since the rank of the matrix Q reduced modulo p is 1, we must have that C is of the form pC_0. But this implies that $p^4 \mid \det(Q)$, which is a contradiction. Hence we have $p^2 \nmid m(\varphi_p)$.

If $p \nmid m(\varphi_p)$, then it is clear that φ_p represents B. Assume that $p \mid m(\varphi_p)$. If φ_p is modular, then it is clear that φ_p represents $-BD$, so assume that $p^3 \mid d(\varphi_p)$. Let $\alpha \in \mathbb{Z}_p$ be an element represented by φ_p such that $v_p(\alpha) = 1$. In a suitable basis, the matrix of q_p is now

$$Q = \begin{pmatrix} 2\alpha & 0 & pb & pc \\ 0 & 2p^2a & pe & pf \\ pb & pe & 2B & 0 \\ pc & pf & 0 & 2pg \end{pmatrix},$$

where $a, b, c, e, f, g \in \mathbb{Z}_p$. We get $\det(Q) \equiv -4p^2f^2B\alpha \pmod{p^4}$. Hence $\left(\frac{-4p^2f^2B\alpha/p^3}{p}\right) = \left(\frac{B^4D^3/p^3}{p}\right)$, so $\left(\frac{\alpha/p}{p}\right) = \left(\frac{-BD/p}{p}\right)$. This shows that φ_p represents $-BD$. □

Lemma 9.6. *With M as above, we have that the binary form $q_M^\#$ is negative definite, it has discriminant*

$$d(q_M^\#) = d(q_M)/D$$

and content

$$m(q_M^\#) = m(q_M)/t,$$

where t is the product of all primes p dividing D such that q_M is modular at p.

Proof. It is clear that $q_M^\#$ is negative definite. Let p be a prime, and let $\varphi = (q_M)_p$ and $\varphi^\perp = (q_M^\#)_p$.

If $p \nmid d(\Lambda)D$, then (L_p, q_p) is unimodular, and the claim follows directly from lemma 3.9.

If $p \mid d(\Lambda)$, then $(L_p, q_p) \cong (\Omega_p, \mathrm{nr})$. Let A be the matrix of an anisotropic unimodular binary quadratic form over $\mathbb{Z}_p$. The matrix of q_p is then given by $\left(\begin{smallmatrix} A & 0 \\ 0 & pA \end{smallmatrix}\right)$ in a suitable $\mathbb{Z}_p$-basis e_1, e_2, e_3, e_4 of L. A $\mathbb{Z}_p$-basis of $L_p^\#$ is then given by pe_1, pe_2, e_3, e_4, and $q_p^\# = \frac{1}{p}\,\mathrm{nr}$. By the symmetry of the roles played by (L_p, q_p) and $(L_p^\#, q_p^\#)$, and part ii) of lemma 9.5, it is sufficient to prove the claim when φ is modular. Assume first that φ is unimodular. If this is the case, then it is easy to see that M must be the column space of a 4×2 matrix $\left(\begin{smallmatrix} I \\ B \end{smallmatrix}\right)$. Then $M^\perp$ is given by the column space of $\left(\begin{smallmatrix} A^{-1}B^tA \\ -I \end{smallmatrix}\right)$. Hence we get that $\varphi^\perp$ is unimodular. The same type of calculation shows that if φ is p-modular, then so is also $\varphi^\perp$.

If $p \mid D$, then we use explicit calculations to verify the claim. Let $e_1, \ldots, e_4$ be a basis for L_p such that the matrix of q_p (up to a constant factor in $\mathbb{Z}_p^*$) in this basis is

$$Q = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & -2d & 0 & 0 \\ 0 & 0 & 0 & 4d \\ 0 & 0 & 4d & 0 \end{pmatrix}$$

(recall that $p \neq 2$). We have the dual basis $\frac{1}{2}e_1$, $\frac{-1}{2d}e_2$, $\frac{1}{4d}e_4$, $\frac{1}{4d}e_3$ of $L_p^\#$. The matrix $Q^\#$ of the dual form, in this basis, is

$$Q^\# = \begin{pmatrix} 2d & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Now we identify sublattices M of L_p with column spaces of matrices U. The orthogonal complement $M^\perp \subset L_p^\#$ of a sublattice M is identified with the column space if some matrix $U^\perp$. The matrices of φ and $\varphi^\perp$ are then given by U^tQU and $(U^\perp)^tQ^\#U^\perp$ respectively. It is easy to see that it is sufficient to verify the claim when U is one of the matrices $U_1, \ldots, U_4$ given in table 1, where $a, b, c, e \in \mathbb{Z}_p$. We can verify that we have $d(\varphi_i) = 4dd(\varphi_i^\perp)$

$U_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ a & b \\ c & e \end{pmatrix}$	$U_1^\perp = \begin{pmatrix} -a & -c \\ -b & -e \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\varphi_1=[1+4dac, 4d(bc+ae), d(4be-1)]$ $\varphi_1^\perp=[da^2-b^2, 2dac-2be+1, dc^2-e^2]$ $m(\varphi_1)=(1), \quad m(\varphi_1^\perp)=(1)$
$U_2 = \begin{pmatrix} 1 & 0 \\ a & pb \\ 0 & 1 \\ c & e \end{pmatrix}$	$U_2^\perp = \begin{pmatrix} -a & -c \\ 1 & 0 \\ -pb & -e \\ 0 & 1 \end{pmatrix}$	$\varphi_2=[1-da^2, 2d(2c-pab), 4de-p^2db^2]$ $\varphi_2^\perp=[da^2-1, 2dac-pb, dc^2-e]$ $m(\varphi_2)=(1), \quad m(\varphi_2^\perp)=(1)$
$U_3 = \begin{pmatrix} pa & pb \\ 1 & 0 \\ 0 & 1 \\ c & e \end{pmatrix}$	$U_3^\perp = \begin{pmatrix} 1 & 0 \\ -pa & -c \\ -pb & -e \\ 0 & 1 \end{pmatrix}$	$\varphi_3=[p^2a^2-d, 2p^2ab+4dc, p^2b^2+4de]$ $\varphi_3^\perp=[d-p^2a^2, -2pac-pb, -c^2-e]$ $m(\varphi_3)=(p), \quad m(\varphi_3^\perp)=(p, e+c^2)$
$U_4 = \begin{pmatrix} pa & pb \\ pc & pe \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$	$U_4^\perp = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ -pa & -pc \\ -pb & -pe \end{pmatrix}$	$\varphi_4=[p^2(a^2-dc^2), -2p^2dce+2p^2ab+4d, p^2(b^2-de^2)]$ $\varphi_4^\perp=[d+p^2ab, p^2(bc+ae), p^2ce-1]$ $m(\varphi_4)=(p), \quad m(\varphi_4^\perp)=(1)$

Table 1: Explicit computations of $\varphi^\perp$ in the case $p \mid D$

for $i = 1, 2, 3, 4$. Furthermore, the claim about $m(\varphi^\perp)$ follows by inspection and the following two additional remarks: $p^3 \mid d(\varphi_3)$ if and only if $p \mid e + c^2$, and $p^3 \nmid d(\varphi_4)$. □

9.2 The binary form of an elliptic point

We will prove that an elliptic point of order 2 or 3 is a special point and we will determine which equivalence classes of binary forms that can appear for such points. It turns out that there are two families of binary forms that can occur, and we say that an elliptic point is of type I or type II according to the type of its associated form. We start with a technical lemma on complex quadratic fields in A.

Let $k_1 \subset A$ be a complex quadratic field over $\mathbb{Q}$. Let $k_1 = \mathbb{Q}(\gamma_1)$ where $\gamma_1^2 \in \mathbb{Q}$ with $\gamma_1^2 < 0$. Let K be the totally complex biquadratic field

$$K = k(\gamma_1) \subseteq A.$$

K contains exactly 3 non-trivial subfields, namely k, k_1 and $k_2 = \mathbb{Q}(\gamma_2)$, where $\gamma_2 = \sqrt{d}\gamma_1$.

Lemma 9.7. *There exists an orthogonal decomposition $W = W_1 \perp W_2$ such that $\dim_{\mathbb{Q}} W_i = 2$, $W_i^* W_i = k_i$ and $W_i k_i = W_i$, for $i = 1, 2$.*

Proof. We will treat the two cases $\tau(K) = K$ and $\tau(K) \neq K$ separately. We consider first the case $\tau(K) = K$.

In this case, we have that K is closed under the two commuting involutions τ and $x \mapsto x^*$. Observe now that we must have $\tau(\gamma_1) = \gamma_1$ or $\tau(\gamma_1) = \gamma_1^*$, since the minimal equation of $\tau(\gamma_1)$ is the same as the minimal equation of γ_1. In the former case, we have that $\tau(\gamma_2) = \gamma_2^*$, so exchanging k_1 and k_2 if necessary, we may without loss of generality assume that

$$\tau(\gamma_1) = \gamma_1^*.$$

Define

$$W_1 = K \cap W.$$

Now in fact $W_1 = k_1$, so W_1 clearly has the properties required by the lemma. Let now

$$W_2 = W_1^{\perp} = \{w \in W \mid \mathrm{tr}(w^* K) = (0)\}.$$

Since $\mathrm{nr}|_{W_1}$ is definite, we get that $W_1 \cap W_2 = (0)$, and hence $W = W_1 \perp W_2$. Take now $a, b \in W_2$ and $x \in K$. We get $a^* b x = -a^* x b = x a^* b$, so all elements of $W_2^* W_2$ commute with all elements in K. Hence we get $W_2^* W_2 \subset K$, since K is a maximal commutative subalgebra of A. Furthermore, we have that $W_2^* W_2$ is a complex field, since $\mathrm{nr}|_{W_2}$ is definite, so we must have that $W_2^* W_2 = k_2$.

It remains to show that $W_2 \gamma_2 = W_2$. Take $a \in W_2$, so we have $\mathrm{tr}(a) = \mathrm{tr}(a\gamma_1) = 0$. Then

$$\tau(a\gamma_2)^* = -\sqrt{d}\gamma_1 a = \sqrt{d} a^* \gamma_1^* = \sqrt{d} a \gamma_1 = a\gamma_2,$$

so $a\gamma_2 \in W$. Furthermore, $\mathrm{tr}((a\gamma_2)^* K) = \mathrm{tr}(a^* \gamma_2^* K) = \mathrm{tr}(a^* K) = (0)$, so we get that in fact $a\gamma_2 \in W_2$. We are done in the case $\tau(K) = K$.

Now we consider the case $\tau(K) \neq K$, which clearly implies that $\tau(K) \cap K = k$. Let i be 1 or 2. We have $A = K + \tau(\gamma_i)^* K$, since $\tau(\gamma_i)^* \notin K$, and we conclude that

$$1,\ \gamma_i,\ \tau(\gamma_i)^*,\ \tau(\gamma_i)^* \gamma_i$$

is a k-basis of A. We define the $\mathbb{Q}$-vector space

$$W_i = \{w \in W \mid w\gamma_i^* = \tau(\gamma_i) w\}.$$

It is clear that $W_1 \cap W_2 = (0)$. Furthermore, it is straightforward to check that

$$\gamma_i + \tau(\gamma_i)^*,\ \tau(\gamma_i)^* \gamma_i + \gamma_i^2 \in W_i. \tag{9.2}$$

It is clear that elements in (9.2) are linearly independent over $\mathbb{Q}$, since they are linearly independent over k. Hence $W = W_1 \oplus W_2$ and $\dim_{\mathbb{Q}} W_i = 2$. It is easy to check that $W_i\gamma_i = W_i$.

Now we want to show that $W_i^* W_i = k_i$. Let $a, b \in W_i$. Using $a\gamma_i^* = \tau(\gamma_i)a$, $b\gamma_i^* = \tau(\gamma_i)b$ and $\mathrm{nr}(\gamma_i) \in \mathbb{Q}$, we get

$$\gamma_i a^* b = a^* \tau(\gamma_i)^* b = a^* b \gamma_i,$$

so a^*b commutes with γ_i. Hence $a^*b \in K$, since K is a maximal commutative subalgebra of A. We conclude that $W_i^* W_i$ is a subfield of K. Since we have $W_i\gamma_i = W_i$, the only possibility is that $W_i^* W_i = k_i$. Finally, using (9.2), it follows immediately that $W = W_1 \perp W_2$. □

Let z be an elliptic point of order $n = 2$ or $n = 3$. There exists an element $\rho \in \Lambda_z^1$ with $\rho^2 + 1 = 0$ if $n = 2$, or with $\rho^2 + \rho + 1 = 0$ if $n = 3$. Consider now the field

$$K = k(\rho) \subseteq A,$$

which is a totally complex field of degree 4 over $\mathbb{Q}$. We also consider the rings

$$S_1 = \mathbb{Z}[\rho]$$

and

$$S_2 = \begin{cases} \mathbb{Z}[\sqrt{d}\rho] & \text{if } n = 2, \\ \mathbb{Z}[\sqrt{d}\rho + (\sqrt{d}+1)/2] & \text{if } n = 3. \end{cases}$$

By our assumption on k, we have that both S_1 and S_2 are maximal quadratic orders. We also have $S_1, S_2 \subset \Lambda$ and $d(S_2) = Dd(S_1)$.

Proposition 9.8. *If $z \in \mathcal{H}\times\mathcal{H}$ is an elliptic point of order 2 or 3, then z is a special point. Furthermore, we have that either $L_z S_1 = L_z$ or $L_z S_2 = L_z$.*

If $z \in \mathcal{H}\times\mathcal{H}$ is an elliptic point of order 5, then $L_z = \{0\}$, i.e. there exist no $\beta \in L$ such that $z \in C_\beta$.

Proof. Let first z be an elliptic point of order 2 or 3. By lemma 9.7, there exists an orthogonal decomposition

$$W = W_1 \perp W_2 \tag{9.3}$$

such that $W_1 S_1 = W_1$ and $W_2 S_2 = W_2$. We have that both $q|_{W_1}$ and $q|_{W_2}$ are definite quadratic forms. Let i be such that $q|_{W_i}$ is positive definite.

We have that $W_1\rho = W_1$, and therefore we get

$$\tau(\rho)W_1\rho^* = \tau(\rho)W_1 = \tau(\rho)\tau(W_1)^* = \tau(W_1\rho^*)^* = \tau(W_1)^* = W_1.$$

Since the map $w \mapsto \tau(\rho)w\rho^*$ is an isometry of (W, q), we conclude that it must respect the orthogonal decomposition (9.3). Hence we have

$$\tau(\rho)W_j\rho^* = W_j,$$

for $j = 1, 2$.

Let now M be the lattice $M = L \cap W_i$. By lemma 9.1, we have that $M = L_{z'}$ for some point $z' \in \mathcal{H}\times\mathcal{H}$. Since $\tau(\rho)M\rho^* = M$, ρ must preserve the intersection point z' of the curves C_β for $\beta \in M$, i.e. $\rho z' = z'$. Hence $z' = z$, so z is a special point and

$$L_z = L \cap W_i.$$

It remains to show that $L_z S_i = L_z$. Take $\beta \in L_z$ and $\lambda \in S_i$. We have $W_i S_i = W_i$, so we know that $\beta\lambda \in W_i$. We also get $\overline{\Lambda}\beta\lambda\Lambda \subseteq \overline{\Lambda}\beta\Lambda \subseteq \Lambda$, so $\beta\lambda \in L$. We are done.

Let now z be an elliptic point of order 5 and choose $\rho \in \Lambda_z^1$ with $\rho^5 = 1$, $\rho \neq 1$. Assume that we have $z \in C_\beta$ for some $\beta \in L$. First we want to show that we must have $\rho \notin \Gamma_\beta$. Assume to the contrary that $\rho \in \Gamma_\beta$. Since we have $[\Gamma_\beta : \Lambda_\beta^1] = 1$ or 2, we would get that $\rho \in \Lambda_\beta^1$. But this is impossible, a unit root of order 5 can not exist in a quaternion order over $\mathbb{Z}$. Hence we must have $\tau(\rho)\beta\rho^* \neq \pm\beta$ for every element $\beta \in L_z \setminus \{0\}$. But then the binary form q_z represents every non-zero value at least 10 times, which is absurd. □

Corollary 9.9. *Let q_z be the quadratic form of an elliptic point z of order $n = 2$ or $n = 3$. There are two cases:*

i) $q_z \cong mD\varphi$, *where* $\varphi = [1, 0, 1]$ *if* $n = 2$ *or* $\varphi = [1, -1, 1]$ *if* $n = 3$, *and where m is a positive integer with $m \mid d(\Lambda)$. If $n = 2$, then we have $\Lambda_z^1 \cap \Lambda_\beta^1 = \{\pm 1\}$ and $\Lambda_z^1 \subseteq \Gamma_\beta$ for all $\beta \in L_z \setminus \{0\}$, and if $n = 3$, then we have $\Lambda_z^1 \cap \Gamma_\beta = \{\pm 1\}$ for all $\beta \in L_z \setminus \{0\}$.*

ii) $q_z \cong m\varphi$, *where* $d_0(\varphi) = -4D$ *if* $n = 2$ *or* $d_0(\varphi) = -3D$ *if* $n = 3$, *and m is a positive integer with $m \mid d(\Lambda)$. We have $\Lambda_z^1 \subseteq \Lambda_\beta^1$ for all $\beta \in L_z \setminus \{0\}$.*

Proof. We use the notations of the proof of proposition 9.8.

Consider first the case $L_z S_1 = L_z$, which implies that $L_z = L \cap W_1$. We want to show that i) holds. We have that $W_2 S_2 = W_2$, so $S_2 \subseteq W_2^* W_2 = C_0(W_2, q^\perp|_{W_2})$. Furthermore, since we have that $W_2 \subseteq W_\beta$ for all non-zero $\beta \in L_z$, we get $S_2 \subseteq A_\beta$, and therefore

$$S_2 \subseteq \Lambda_\beta,$$

for every $\beta \in L_z \setminus \{0\}$.

Take now an element $\beta \in L_z \setminus \{0\}$. Since we have $S_2 \subseteq \Lambda_\beta$, we necessarily get $S_1 \cap \Lambda_\beta = \mathbb{Z}$. Hence $\Lambda_z^1 \cap \Lambda_\beta^1 = \{\pm 1\}$, and from this follows, that $\rho \in \Gamma_\beta$ if and only if $\tau(\rho)\beta = -\beta\rho$. Since $\beta\rho \in W$, we get $\beta\rho = \tau(\beta\rho)^* = \tau(\rho^*)\beta$. Hence, we see that $\rho \in \Gamma_\beta$ if and only if $\rho^* = -\rho$. This gives $\rho \in \Gamma_\beta$ if $n = 2$, and $\rho \notin \Gamma_\beta$ if $n = 3$.

Since L_z is an S_1-module, and since we know that $D \mid d(q_z)$, we get that $q_z \cong mD\varphi$, where $m \in \mathbb{Z}$ and $d_0(\varphi) = d(S_1)$. We must show that $m \mid d(\Lambda)$. By lemma 9.6, we have $d_0(q_z^\perp) = m^2 Dd(S_1)$, so we get

$$m^2 Dd(S_1)\mathbb{Z} = d(q_z^\perp) = d(S_2 \cap \Theta) = d(S_2)[S_2 : S_2 \cap \Theta]^2.$$

We know by lemma 7.11 that $[S_2 : S_2 \cap \Theta] \mid d(\Lambda)$, and hence $m \mid d(\Lambda)$.

Consider now the case $L_z S_2 = L_z$. The argument is similar in this case. We want to show that ii) holds. We have $W_1\rho = W_1$, so $\rho \in C_0(W_1, q^\perp|_{W_1})$. Furthermore, since $W_1 \subseteq W_\beta$ for all non-zero $\beta \in L_z$, we get $\rho \in A_\beta$, and hence

$$S_1 \subseteq \Lambda_\beta,$$

for every $\beta \in L_z \setminus \{0\}$. In particular, we have $\Lambda_z^1 \subseteq \Lambda_\beta^1$.

Now, since L_z is an S_2-module, we get $q_z \cong m\varphi$, where φ is a primitive form with $d_0(\varphi) = d(S_2) = Dd(S_1)$. By lemma 9.6, we get $d_0(q_z^\perp) = m^2 d(S_1)$, so

$$m^2 d(S_1)\mathbb{Z} = d(q_z^\perp) = d(S_1 \cap \Theta) = d(S_1)[S_1 : S_1 \cap \Theta]^2.$$

As in the previous case, this implies $m \mid d(\Lambda)$. □

We say that an elliptic point which satisfies condition i) (respectively ii)) in corollary 9.9, is an *elliptic point of type* I (respectively II).

9.3 The number of special points

We want to determine which oriented binary forms φ that are equivalent to q_z for some point z, and furthermore compute the value $s(\varphi)$. This computation is somewhat long and technical, but much of the complication arises since we want to handle also non-primitive forms. It is especially the factor m_3 (see below) that complicates things. The reader who so wishes, can only consider the case $m_3 = 1$, which is all we need in the applications in chapter 12.

Let us now fix a positive definite oriented binary form φ such that $\varphi \cong q_z$ for some point $z \in \mathcal{H} \times \mathcal{H}$. Let $\Delta = d_0(\varphi)$ and $m(\varphi) = (m)$, where $m > 0$. We write $m = m_1 m_2 m_3$, where m_1 contains those prime factors which divide

D, m_2 those prime factors which divide $d(\Lambda)$ and m_3 contains all other prime factors. By lemma 9.5, we have that $m_1 \mid D$, that $m_2 \mid d(\Lambda)$ and that every prime dividing m_3 is split in k.

Recall now the classical result saying that any primitive binary form represents infinitely many primes. Hence we can choose a prime r not dividing $Dd(\Lambda)\Delta$, such that $N = mr$ is represented by φ. The curve F_N is now non-empty, and by theorem 8.9, we have

$$f_N = 2^{b-1}[\Gamma_\beta : \Lambda_\beta^1] = 2^{b-1}\kappa(N), \tag{9.4}$$

where β is any primitive element in L with $q(\beta) = N$ and b is the number of primes which divide D but which do not divide m_1. Assume that

$$F_N = F_{\beta_1} \cup \cdots \cup F_{\beta_{f_N}}.$$

Since φ represents N, we have that if $\zeta \in X$ with $q_\zeta \cong \varphi$, then $\zeta \in F_N$. Hence, for every $z \in \mathcal{H}\times\mathcal{H}$ with $q_z \cong \varphi$, we have that ζ is equivalent under Λ^1 to some point z' on some curve C_{β_i}. Our first goal is to compute the number of $\Lambda_{\beta_i}^1$-orbits of points $z \in C_{\beta_i}$ with $q_z \simeq \varphi$.

Let us now fix one element β among β_i. The order Λ_β is an Eichler order of discriminant $Nd_0(\Lambda)/m_2 = m_1 m_3 d_0(\Lambda) r$. Define

$$\Psi_{\varphi,\beta} = \{z \in C_\beta \mid q_z \simeq \varphi\}.$$

We want to calculate the number of Λ_β^1-orbits of $\Psi_{\varphi,\beta}$.

For every $z \in \Psi_{\varphi,\beta}$, consider the lattice $L_z^\# = (L_z)^\perp$ with the quadratic form $q_z^\# = q^\#|_{L_z^\#}$. We define S_z^0 to be the image of $C_0(L_z^\#, q_z^\#)$ in Λ, so S_z^0 is a quadratic order. Let

$$S_z = (\mathbb{Q}S_z^0) \cap \Lambda.$$

Lemma 9.10. *S_z is an optimally embedded complex quadratic order in Λ_β with discriminant $\frac{\Delta}{m_2^2 D}$.*

Proof. We have $d(S_z^0) = \Delta/D$ by lemma 9.6, and S_z^0 is optimally embedded in $\Lambda_\beta \cap \Theta$ by lemma 3.4. Note also that we have $S_z^0 = S_z \cap \Theta$, so if $p \nmid d(\Lambda)$, then $(S_z)_p = (S_z^0)_p$. If $p \mid d(\Lambda)$, then $(S_z)_p$ is a optimally embedded order in $(\Lambda_\beta)_p \cong \Omega_p$, which implies that $(S_z)_p$ is a maximal order in its quotient field. But the only case where $(S_z^0)_p$ is not a maximal order in its quotient field is if $p \mid m_2$. The claim follows. □

Since all the quadratic orders S_z, for $z \in \Psi_{\varphi,\beta}$, are isomorphic, we let S_φ denote an element in this isomorphism class. Note that $|S_\varphi^*| \neq 2$ if and only if the corresponding special points are elliptic points of type II.

To be able to handle the case $m_3 \neq 1$, we first need a local result. Recall the correspondence between optimally embedded quadratic orders and optimally embedded sublattices given in lemma 3.4.

Lemma 9.11. *Let p be a prime, k a positive integer and $\Delta = p^{2k}\Delta_1$, where Δ_1 is the discriminant of a non-degenerate integral binary form over $\mathbb{Z}_p$. Let Λ_1 be an Eichler order over $\mathbb{Z}_p$ with $d(\Lambda_1) = (p^k)$ and identify Λ_1 with $C_0(M,g)$ for some ternary quadratic $\mathbb{Z}_p$-lattice (M,g). If S is a quadratic order over $\mathbb{Z}_p$ which is optimally embedded in Λ_1, then we denote the binary form $g|_{M_S}$ by g_S. Let Λ_0 and Λ_0' be the two unique maximal orders such that $\Lambda_1 = \Lambda_0 \cap \Lambda_0'$. Let S be a quadratic order over $\mathbb{Z}_p$.*

i) Let S be an optimally embedded quadratic order in Λ_1, and assume that $d(S) = \Delta$ and $p^k \mid m(g_S)$. Then S is optimally embedded in exactly one of Λ_0 and Λ_0'.

ii) For any optimally embedded $S \subseteq \Lambda_0$ with $d(S) = \Delta$, there exist $\lambda \in \Lambda_0^*$ such that $S' = \lambda S \lambda^{-1} \subseteq \Lambda_1$, and $p^k \mid m(g_{S'})$.

iii) Let S and S' be optimally embedded in Λ_0, and assume that $S, S' \subseteq \Lambda_1$, $d(S) = d(S') = \Delta$ and that $p^k \mid m(g_S),\ m(g_{S'})$. If $S' = \lambda S \lambda^{-1}$, where $\lambda \in \Lambda_0^*$, then $\lambda \in \Lambda_1^*$.

Proof. Let $\Lambda_1 = \left(\begin{smallmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p^k\mathbb{Z}_p & \mathbb{Z}_p \end{smallmatrix}\right)$. Using the canonical construction of section 2.4, we choose M as the lattice

$$M = \{\alpha = \begin{pmatrix} x & p^{-k}y \\ z & -x \end{pmatrix} \mid x, y, z \in \mathbb{Z}_p\},$$

with quadratic form $g(\alpha) = -p^k \det(\alpha) = p^k x^2 + yz$ for $\alpha \in M$. The maximal orders Λ_0 and Λ_0' are given by $\left(\begin{smallmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ \mathbb{Z}_p & \mathbb{Z}_p \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} \mathbb{Z}_p & p^{-k}\mathbb{Z}_p \\ p^k\mathbb{Z}_p & \mathbb{Z}_p \end{smallmatrix}\right)$ respectively. We also introduce the order $\Lambda_2 = \left(\begin{smallmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p^{2k}\mathbb{Z}_p & \mathbb{Z}_p \end{smallmatrix}\right)$.

i) Let $S = \mathbb{Z}_p[\omega]$, where $\omega = \left(\begin{smallmatrix} a & b \\ p^k c & d \end{smallmatrix}\right)$ and $(\mathrm{tr}(\omega))^2 - 4\det(\omega) = (a-d)^2 + 4p^k bc = \Delta$. Since S is optimally embedded in Λ_1, and we have $p \mid \Delta$, we get that $(b,c) = (1)$. Assume first that b is a unit. Computing $M_S = \{\alpha \in M \mid \mathrm{tr}(\alpha S) = (0)\}$, we get

$$M_S = \mathbb{Z}_p \begin{pmatrix} b & 0 \\ d-a & -b \end{pmatrix} + \mathbb{Z}_p \begin{pmatrix} 0 & -p^{-k}b \\ c & 0 \end{pmatrix}.$$

Thus $p^k \mid m(g_S)$ if and only if $p^k \mid c$ and $p^k \mid a-d$. Hence, S is optimally embedded in Λ_0 but not in Λ_0'. Similarly, if we assume instead that c is

a unit, we get that S is primitively embedded in Λ_0' but not in Λ_0. This proves i).

From the calculation in the proof of i), we also get the following fact: If S is optimally embedded in Λ_0 with $d(S) = \Delta$ and $S \subseteq \Lambda_1$, then $p^k \mid m(g_S)$ if and only if $S \subseteq \Lambda_2$.

ii) Let $S = \mathbb{Z}_p[\omega]$, where $\omega = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $(a-d)^2 + 4bc = \Delta$. By optimality, we must have $(b, c) = (1)$, and we assume that $b \in \mathbb{Z}_p^*$. The case $c \in \mathbb{Z}_p^*$ is analogous. By the above remark, we need to find an element $\lambda \in \Lambda_0^*$ such that $\lambda\omega\lambda^{-1} \in \Lambda_2$. Let $\lambda = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$. By a calculation, we get that $\lambda\omega\lambda^{-1} \in \Lambda_2$ if and only if

$$4p^{2k} \mid \Delta w^2 - (2bz - (a-d)w)^2.$$

Hence, if $p = 2$ and $\Delta_1 \equiv 1 \pmod 4$, then we may choose $\lambda = \left(\begin{smallmatrix} 1 & 0 \\ \frac{a-d+2^k}{2b} & 1 \end{smallmatrix}\right)$, and otherwise we may choose $\lambda = \left(\begin{smallmatrix} 1 & 0 \\ \frac{a-d}{2b} & 1 \end{smallmatrix}\right)$.

iii) Let $S = \mathbb{Z}_p[w]$. By the hypothesis on S, we have that $\omega = \left(\begin{smallmatrix} a & b \\ p^{2k}c & d \end{smallmatrix}\right)$, with $(a-d)^2 + p^{2k}bc = \Delta$ and $b \in \mathbb{Z}_p^*$. If $\lambda = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in \Lambda_0$ with $\det(\lambda) \in \mathbb{Z}_p^*$, then by a direct calculation, we get that $\lambda\omega\lambda^{-1} \in \Lambda_2$ if and only if $p^k \mid z$. This shows the claim. □

Lemma 9.12. *The number of equivalence classes of points $z \in \Psi_{\varphi,\beta}$, under the action of Λ_β^1, is*

$$2^a e(S_\varphi, \Lambda_0),$$

where Λ_0 is any order containing Λ_β such that $d(\Lambda_\beta) = m_3 d(\Lambda_0)$ and a is the number of different primes dividing m_3.

Proof. Take a point $z \in \Psi_{\varphi,\beta}$. The successive construction of the quadratic order $S_z \subseteq \Lambda_\beta$ outlined above goes as follows

$$z \mapsto L_z \mapsto L_z^\# \mapsto C_0(L_z^\#, q_z^\#) \mapsto S_z.$$

If $\lambda \in \Lambda_\beta^1$, then one can verify that the corresponding chain for λz is

$$\lambda z \mapsto \overline{\lambda} L_z \lambda^* \mapsto \overline{\lambda} L_z^\# \lambda^* \mapsto \lambda C_0(L_z^\#, q_z^\#)\lambda^{-1} \mapsto \lambda S_z \lambda^{-1}.$$

Hence, to every class of points in $\Psi_{\varphi,\beta}$, we may associate a Λ_β^1-conjugacy class of quadratic orders $S \subseteq \Lambda_\beta$.

We want to examine this construction in the opposite direction. Take therefore a quadratic order $S \subseteq \Lambda_\beta$, which is isomorphic to S_φ and optimally embedded in Λ_β. We consider the order $S^0 = S \cap \Theta$, which is optimally embedded in the image of $C_0(L_\beta^\#, q_\beta^\#)$. There is a sublattice $M_S \subseteq \Lambda_\beta^\#$ such

that S^0 is the natural image of $C_0(M_S, q_\beta^{\#}|_{M_S})$. Let L_S be the orthogonal complement of M_S inside L, i.e. $L_S = \{x \in L \mid tr(x^* M_S) = (0)\}$. Note that we have $\beta \in L_S$. Furthermore, the lattice L_S is positive definite with respect to q, end hence $L_S = L_{z_S}$ for some point $z_S \in C_\beta$. We denote the oriented binary form q_{z_S} of this point by φ_S. Note though that we do not necessarily have $z \in \Psi_{\varphi,\beta}$, i.e. that $\varphi_S \simeq \varphi$. It is clear, using lemma 9.6, that we must have $d_0(\varphi_S) = \Delta$, but we may have $m(\varphi_S) \neq (m)$.

Claim. *We have $v_p(m(\varphi_S)) = v_p(m)$ for every prime p with $p \nmid m_3$.*

We have that φ_S represents $N = mr$, so $m(\varphi_S) \mid mr$. Now, since $r \nmid \Delta$, we can not have $r \mid m(\varphi_S)$, and hence $m(\varphi_S) \mid m$. To prove the claim, we need to show that $m_1 m_2 \mid m(\varphi_S)$.

Assume that $p \mid m_1$ and assume to the contrary that $p \nmid m(\varphi_S)$. Then φ_S is a primitive form with $p^2 \mid d(\varphi_S)$. Such a form can not represent an element $\alpha \in \mathbb{Z}_p$ with $v_p(\alpha) = 1$. But φ_S represents N and we get a contradiction. Hence $p \mid m(\varphi_S)$.

Assume now that $p \mid m_2$. Since φ_p is modular, we have that $(S_\varphi)_p \cong (S)_p$ is unramified and hence we must have that $(\varphi_S)_p$ is modular anisotropic. But φ_S represents N and $v_p(N) = 1$, so we must have $p \mid m(\varphi_S)$. This proves the claim.

If now S is such that $m(\varphi_S) = (m)$, then by lemma 3.3, we have $\varphi_S \simeq \varphi$. Hence the Λ_β^1-classes of points $z \in \Psi_{\varphi,\beta}$ correspond one-to-one to Λ_β^1-classes of optimally embedded orders $S \subset \Lambda_\beta$ with $S \cong S_\varphi$ which satisfy the additional requirement that $m_3 \mid m(\varphi_S)$.

Let $\mathcal{A}$ be the set of orders $\Lambda_0 \subseteq A_\beta$ which have the following properties:

i) $\Lambda_0 \supseteq \Lambda_\beta$,

ii) $d(\Lambda_0) = d(\Lambda_\beta)/m_3$,

iii) there exists an order $\Lambda_0' \supseteq \Lambda_\beta$ such that $d(\Lambda_0') = d(\Lambda_0)$ and $\Lambda_\beta = \Lambda_0 \cap \Lambda_0'$.

By lemma 2.27, we have that $\mathcal{A}$ contains 2^a orders. By lemma 9.11, we get that if $z \in \Psi_{\varphi,\beta}$, then S_z is optimally embedded in a unique order $\Lambda_0 \in \mathcal{A}$. Furthermore, we get from this lemma that the number of Λ_β^1-classes of orders S_z which are optimally embedded in Λ_0 equals the number of Λ_0^1-conjugacy classes of optimally embedded orders $S \in \Lambda_0$ with $S \cong S_\varphi$. By lemma 3.7, this number is $e(S_\varphi, \Lambda_0)$. Furthermore, by proposition 3.5, the number $e(S_\varphi, \Lambda_0)$ does not depend on the particular choice of Λ_0. We are done. □

Lemma 9.13. *If $\varphi \ncong \overline{\varphi}$, then exactly half of the $\Lambda^1_{\beta_i}$-orbits of points $z \in C_{\beta_i}$ with $q_z \simeq \varphi$ consist of points with $q_z \cong \varphi$.*

Proof. Let the map $T = T_\beta : \mathcal{H}\times\mathcal{H} \to \mathcal{H}\times\mathcal{H}$ be as in lemma 7.26, so $T(z_1, z_2) = (s\beta^* z_2, \overline{s}\beta z_1)$, where $s \in \Lambda_\beta$. Fix a special point $z = (z_0, \beta z_0) \in C_\beta$ with $q_z \cong \varphi$. We want to show that $q_{z'} \cong \overline{\varphi}$, where $z' = T(z) \in C_\beta$. First we show that

$$S_{z'} \cong S_z.$$

Take an element $\lambda \in \Lambda_\beta$ such that $\lambda z = z$, i.e. $\lambda \in S_z$. We have $\lambda z_0 = z_0$ and $\beta\lambda = \overline{\lambda}\beta$. We get that $z' = (s\beta^*\beta z_0, \overline{s}\beta z_0) = (sz_0, \beta s z_0)$, so $(s\lambda s^{-1})(z') = z'$. We also have $s\lambda s^{-1} \in \Lambda_\beta$, since s belongs to the normaliser of Λ_β. This shows that $S_{z'} = sS_z s^{-1}$. In particular, we get that $d(q_{z'}) = d(q_z)$. We also need to show that $m(q_{z'}) = m(q_z)$. If we can prove that this holds, then we claim that we are done. We get namely, by lemma 3.3, that $q_z \simeq q_{z'}$ since both q_z and $q_{z'}$ represent N primitively. But the map T reverses the orientation of the vector bundle $\mathcal{L}$, so we must have $q_z \cong \overline{q}_{z'}$.

As in the proof of lemma 9.12, we get that $v_p(m(q_z)) = v_p(m(q_z))$ for every prime p which is not split in k, and for the split primes p such that $p \mid d(\Lambda)$. We now want to show that this holds also if p is a split prime with $p \nmid d(\Lambda)$. We will need to use a different approach to settle this case.

If $\alpha \in L$ with $q(\alpha) > 0$, then we get $T(C_\alpha) = C_{\overline{s}\beta\alpha^*\beta s^*}$. We define therefore a map $f : W \to W$, by

$$f(x) = \mathrm{nr}(s\beta)^{-1}\overline{s}\beta x^*\beta s^*.$$

We have $q(f(x)) = q(x)$ for all $x \in W$. We also have $T(C_\alpha) = C_{f(\alpha)}$ for all $\alpha \in L$ with $q(\alpha) > 0$, so $f(W_z) = W_{z'}$. The problem is that in general we have $f(L) \neq L$. We want to show that if p is split in k with $p \nmid d(\Lambda)$, then we have $f(L_p) = L_p$. As a consequence of this, we will get that $f(L_z) = L_{z'}$, and hence

$$(q_z)_p \simeq (q_{z'})_p.$$

As usual, we identify Λ_p with $M_2(\mathbb{Z}_p)\times M_2(\mathbb{Z}_p)$ and let ι be the involution given by $\iota(x, y) = (y, x)$. Let $\gamma \in W_\iota$ be the element given by lemma 7.5, so we have $\overline{x} = \gamma^{-1}\iota(x)\gamma$ for all $x \in A_p$ and $L_p = \gamma^* L_\iota$. Furthermore, we let β_0 be as in the proof of lemma 4.12 if applied to the involution $x \mapsto \beta^{-1}\overline{x}\beta$, so $\beta_0^{-1}\iota(x)\beta_0 = \beta^{-1}\overline{x}\beta$, $\iota(\beta_0)^* = \beta_0$ and β_0 is primitive in Λ_p. We get $\gamma\beta = u\beta_0$ for some $u \in k_p^*$, so we have

$$\begin{aligned} f(L_p) &= \mathrm{nr}(s\beta)^{-1}\overline{s}\beta L_p^*\beta s^* = \mathrm{nr}(s\beta)^{-1}\beta s L_\iota \gamma\beta s^* = \\ &= \mathrm{nr}(s\beta_0)^{-1}\gamma^*\beta_0 s L_\iota \beta_0 s^* = \gamma^* L_\iota = L_p. \end{aligned}$$

Here, the next to last equality follows from the fact that $\mathrm{nr}(s)^{-1}\beta_0 s \in \Lambda_p^*$ and $\mathrm{nr}(\beta_0)^{-1}\beta_0 s^* \in \Lambda_p^*$, which follows immediately from the explicit description of β_0 and s in the proof of lemma 4.12. We are done. □

Proposition 9.14. *If φ is a positive definite oriented binary form, then there exists a point $z \in \mathcal{H}\times\mathcal{H}$ such that $\varphi \cong q_z$ if and only if q_p represents φ_p primitively for every prime p.*

Proof. Assume that φ is a positive definite oriented binary form such that q_p represents φ_p primitively for every prime p, i.e. φ satisfies the conditions of lemma 9.5. Let Δ, $m = m_1m_2m_3$ and $N = mr$ be as above. Since q_p represents φ_p primitively for every prime, and φ represents N primitively, we get that q_p represents N primitively for every prime p. Hence, by theorem 3.8, we get that q represents N primitively, say by $\beta \in L$.

Consider now the imaginary quadratic order which has discriminant $\Delta/(m_2^2D)$. We denote this order by S_φ. Let p be a prime. Since q_p represents φ_p, we can follow the opposite construction given in the proof of lemma 9.12, but this time locally at p, and get that $(S_\varphi)_p$ is primitively embeddable in $(\Lambda_\beta)_p$. But Λ_β is an Eichler order, and hence we get by proposition 3.5 that there exists a primitive embedding $f : S_\varphi \to \Lambda_\beta$.

Consider the image $S = f(S_\varphi)$. We choose an over-order Λ_0 of Λ_β as in the proof of lemma 9.12. Using a suitable conjugate $\lambda S\lambda^{-1} \subseteq \Lambda_\beta$, where $\lambda \in \Lambda_0^1$, we can now follow the opposite construction, and arrive at some point $z \in C_\beta$ which satisfies $q_z \simeq \varphi$. If it should happen that $q_z \not\cong \varphi$, then by lemma 9.13 there is some other point $z' \in C_\beta$ such that $q_{z'} \cong \varphi$. □

Definition 9.15. If φ is a binary form over $\mathbb{Z}$ and p a prime, then we let

$$\alpha_p(\varphi) = \begin{cases} 1 & \text{if } \varphi_p \text{ is modular,} \\ 2 & \text{otherwise.} \end{cases}$$

We also introduce the modified class number h' (compare e.g. [22]), which counts forms φ with multiplicity $2/w_\varphi$. Hence $h'(-3) = 1/3$, $h'(-4) = 1/2$ and $h'(N) = h(N)$ otherwise.

Theorem 9.16. *A positive definite oriented binary form φ is represented by q if and only if φ_p satisfies the conditions of lemma 9.5 for every prime p. For such a form, we have*

$$s(\varphi) = 2^{a-1}h'\left(\frac{\Delta}{m_2^2D}\right)\prod_{p|D}\alpha_p(\varphi)\prod_{p|d(\Lambda)}\frac{2}{\alpha_p(\varphi)}, \tag{9.5}$$

where a is the number of different primes dividing m_3.

Proof. We claim that, with N, β and Λ_0 as above, we have

$$s(\varphi) = \frac{f_N 2^a e(S_\varphi, \Lambda_0)}{\kappa(N)|S_\varphi^*|}. \tag{9.6}$$

Let C denote the disjoint union of the curves $C_{\beta_i}/\Lambda^1_{\beta_i}$, for $i = 1, \ldots, f_N$. Let Ψ_φ consist of those points of C which map to points $\zeta \in X$ with $q_\zeta \simeq \varphi$. By lemma 9.12, we have that $\#(\Psi_\varphi) = f_N 2^a e(S_\varphi, \Lambda_0)$.

Assume first that $w_\varphi = 2$ and that the points are not elliptic. Assume that $\kappa(N) = 1$. If $\varphi \ncong \overline{\varphi}$, then by lemma 3.3, we get that through every point $\zeta \in X$ with $q_\zeta \cong \varphi$ there passes exactly one branch of F_N. Hence, we get $s(\varphi) = \#(X(\varphi)) = \#(\Psi_\varphi)/2$, by lemma 9.13. If $\varphi \cong \overline{\varphi}$, then two branches of F_N pass through each point of $X(\varphi)$, and hence we get $s(\varphi) = \#(X(\varphi)) = \#(\Psi_\varphi)/2$ in this case too.

If $\kappa(N) = 2$, then the groups $\Gamma_{\beta_i}/\Lambda^1_{\beta_i}$ act on $\Psi_{\varphi,\beta_i}/\Lambda^1_{\beta_i}$ without fixed points, since the points are not elliptic, and hence we get $s(\varphi) = \#(\Psi_\varphi)/4$, which is in agreement with (9.6).

Consider now the case that $w_\varphi > 2$ and that the points are not elliptic. We have $w_\varphi/2$ branches of F_N passing through each point of $X(\varphi)$. But we want to count every point with multiplicity w_φ, and hence (9.6) holds in this case too by the same reasoning as above.

Assume now that the points are elliptic of type II. The above argument applies in this case too. We have for instance, by corollary 9.9, that the groups $\Gamma_{\beta_i}/\Lambda^1_{\beta_i}$ act on $\Psi_{\varphi,\beta_i}/\Lambda^1_{\beta_i}$ without fixed points if $\kappa(N) = 2$. Furthermore, the points are to be counted with multiplicity $2/|S_\varphi^*|$, so we get that (9.6) holds.

Assume finally that the points are elliptic of type I. These points are to be counted with multiplicity 1. Consider first elliptic points of order 2. In this case we have, by corollary 9.9, that $\kappa(N) = 2$, $|S_\varphi^*| = 2$ and that $\Gamma_{\beta_i}/\Lambda^1_{\beta_i}$ acts trivially on $\Psi_{\varphi,\beta_i}/\Lambda^1_{\beta_i}$. Furthermore, there are 4 branches of F_N through each point of $X(\varphi)$. Hence $s(\varphi) = \#(X(\varphi)) = \#(\Psi_\varphi)/4$, which agrees with formula (9.6). Consider now elliptic points of order 3. In this case, we have $|S_\varphi^*| = 2$ and that $\Gamma_{\beta_i}/\Lambda^1_{\beta_i}$ acts without fixed points on $\Psi_{\varphi,\beta_i}/\Lambda^1_{\beta_i}$ if $\kappa(N) = 2$. We have 2 branches of F_N through each point of $X(\varphi)$, so $s(\varphi) = \#(X(\varphi)) = \#(\Psi_\varphi)/(2\kappa(N))$. Hence (9.6) holds in this case too.

We need to check that (9.6) simplifies to (9.5). By (9.4) and propositions 3.5 and 3.6, we get that

$$s(\varphi) = 2^{a-1}\frac{2h(S_\varphi)}{|S_\varphi^*|}\frac{e_r(S_\varphi, \Lambda_0)}{2}\Big(2^b \prod_{p|D} e_p(S_\varphi, \Lambda_0)\Big) \prod_{p|d(\Lambda)} e_p(S_\varphi, \Lambda_0).$$

Now we only need to use proposition 3.6, and our assumption that $e_p(S_\varphi, \Lambda_0)$ is non-zero for every prime p, to get the result. □

10 Curves

In this chapter, we treat the case of groups constructed from indefinite rational quaternion algebra acting on $\mathcal{H}$.

Let A be such an algebra, and Λ a $\mathbb{Z}$-order in A. In section 10.1, we recall some well known facts about the action of Λ^1 on $\mathcal{H}$.

Many authors, see e.g. [8], study congruence subgroups of Λ^1 and determine the genus of the corresponding quotient curves. In section 10.2, we will instead consider extensions of the group $\Lambda^1/\{\pm 1\}$, coming from the normaliser of Λ. The motivation for doing this, is that such extensions arise naturally when we study the modular curves F_β.

In section 10.3, we consider the example where Λ is a maximal order with discriminant 39. The reason that we choose this particular example is that it appears in chapter 12, and there we need to know the genus of the quotients given by some of the extended groups.

10.1 General theory

We will now recall some general facts about the situation when groups of units in a quaternion order over $\mathbb{Z}$ act on $\mathcal{H}$. These facts are generally known, see for example [46] and the references therein for proofs and further details.

Let ω be the arithmetical hyperbolic measure on $\mathcal{H}$,

$$\omega = -\frac{1}{2\pi}\frac{dx \wedge dy}{y^2},$$

where $z = x + iy$. Let A be an indefinite rational quaternion algebra, and let $\varrho : A \to M_2(\mathbb{R})$ be an embedding. Let $\Lambda \subseteq A$ be a $\mathbb{Z}$-order, and let Λ^1 act on $\mathcal{H}$ via the map ϱ. Let $\mathcal{F} \subseteq \mathcal{H}$ be a fundamental domain of this action. Let e_r denote the number of equivalence classes of elliptic points of order r. We have that $e_r = 0$ if $r \geq 4$. Let e_∞ denote the number of cusps, i.e. the number of equivalence classes of parabolic elements. Let C denote the compactification of the quotient $\mathcal{H}/\Lambda^1$, and let g be the geometric genus of C.

The genus g of the curve C can be computed from the fundamental equation

$$2 - 2g = \int_{\mathcal{F}} \omega + \frac{1}{2}e_2 + \frac{2}{3}e_3 + e_\infty. \tag{10.1}$$

The numbers which occur on the right hand side of (10.1) can be computed for a general order Λ, but it will be sufficient for our purposes to consider the case of Eichler orders.

Assume that Λ is an Eichler order, and that $d(\Lambda) = N_0 d(A)$. Then the hyperbolic volume is given by

$$\int_{\mathcal{F}} \omega = -\frac{1}{6} d_0(\Lambda) \prod_{p|d(A)} \frac{p-1}{p} \prod_{p|N_0} \frac{p+1}{p}. \tag{10.2}$$

The numbers of elliptic points are given by

$$e_2 = \begin{cases} \prod_{p|d(A)} \left(1 - \left(\frac{-4}{p}\right)\right) \prod_{p|N_0} \left(1 + \left(\frac{-4}{p}\right)\right) & \text{if } 4 \nmid N_0 \\ 0 & \text{if } 4 \mid N_0, \end{cases} \tag{10.3}$$

and

$$e_3 = \begin{cases} \prod_{p|d(A)} \left(1 - \left(\frac{-3}{p}\right)\right) \prod_{p|N_0} \left(1 + \left(\frac{-3}{p}\right)\right) & \text{if } 9 \nmid N_0 \\ 0 & \text{if } 9 \mid N_0. \end{cases} \tag{10.4}$$

If we furthermore assume that A is a skew field, then we have of course no cusps, so $e_\infty = 0$.

10.2 Actions of extended groups

We use the notations of section 10.1. Let Γ denote the image of Λ^1 in $\mathrm{Aut}(\mathcal{H})$, so $\Gamma \cong \Lambda^1/\{\pm 1\}$. However, this subgroup of $\mathrm{Aut}(\mathcal{H})$ is not in general a maximal discrete subgroup. Hence, it will sometimes be of interest to study extensions of Γ. In this section, we will study group extensions which are constructed using elements $\gamma \in \Lambda$ such that $\mathrm{nr}(\gamma) \mid d(A)$ and $\mathrm{nr}(\gamma) > 0$. It is of course possible to use other elements of A^+ which normalise Λ, to generate extensions of Γ. But for simplicity, we will only consider this restricted class of extensions.

Recall that the norm $\mathrm{nr} : \Lambda \to \mathbb{Z}$ is surjective, by lemma 2.28. Hence, for any positive divisor n of $d(A)$, there exists an element $\gamma \in \Lambda$ with $\mathrm{nr}(\gamma) = n$. Such an element acts on $\mathcal{H}$ via the Moebius map given by the matrix $\varrho(\gamma) \in \mathrm{GL}_2^+(\mathbb{R})$. We have the following elementary result:

Lemma 10.1. *Let Λ be an Eichler order over $\mathbb{Z}$ and n a positive divisor of $d(A)$. We have*

i) if $\gamma \in \Lambda$ and $\mathrm{nr}(\gamma) = n$, then $\gamma\Lambda\gamma^{-1} = \Lambda$,

ii) if $\gamma \in \Lambda$ and $\mathrm{nr}(\gamma) = n$, then there exists $\lambda \in \Lambda^1$ such that $\gamma^2 = n\lambda$,

iii) if $\gamma_1, \gamma_2 \in \Lambda$ and $\mathrm{nr}(\gamma_1) = \mathrm{nr}(\gamma_2) = n$, then there exists $\lambda \in \Lambda^1$ such that $\gamma_2 = \lambda\gamma_1$.

Proof. i) This follows directly from proposition 2.11.

ii) The claim follows if we show that $\gamma^2 n^{-1} \in \Lambda_p$ for all primes p. This is clear if $p \nmid d(A)$, since in that case n is a unit in $\mathbb{Z}_p$. Take a prime p with $p \mid d(A)$. In this case, the claim follows since $\mathrm{nr}(\gamma^2 n^{-1}) = 1$ and $\Lambda_p = \{x \in A_p \mid \mathrm{nr}(x) \in \mathbb{Z}_p\}$ (proposition 2.11).

iii) Analogously with the proof of ii), we get that $\gamma_2 \gamma_1^{-1} \in \Lambda_p$ for all primes p, and the claim follows. □

Let n and γ be as in the lemma. By assertions i) and ii), it is clear that γ generates an extension in which Γ has index at most 2. By iii), it is clear that two elements with the same norm n induce the same group extension. Furthermore, it is clear that this extension is trivial if and only if $n = 1$.

Hence, for every positive divisor n of $d(A)$, we can choose an element $\gamma \in \Lambda$ with $\mathrm{nr}(\gamma) = n$ and consider the map $\varrho(\gamma) : \mathcal{H} \to \mathcal{H}$. This induces a well defined map

$$\iota_n : C \to C.$$

If $n \neq 1$, then ι_n is an involution on C, and we have that ι_1 is the identity map. Hence, we have a 2-group

$$G = \{\iota_n \mid n \in \mathbb{Z}_+ \text{ and } n \mid d(A)\}$$

acting on C. The number of elements of G is 2^t, where t is the number of prime divisors of $d(A)$.

We now want to study the set of fixed points of any non-trivial involution in G. Since G is a 2-group, it is clear that if ι_n and $\iota_{n'}$ are two different non-trivial elements in G, then the sets of points fixed by ι_n and $\iota_{n'}$ respectively are disjoint.

To compute the number of fixed points, we first make some elementary observations about traces of elements.

Lemma 10.2. *Let p be a prime and consider Ω_p, the maximal order in the skew field $\mathbb{H}_p$ over $\mathbb{Q}_p$. If $\gamma \in \Omega_p$ with $p \mid \mathrm{nr}(\gamma)$, then $p \mid \mathrm{tr}(\gamma)$.*

Proof. Recall that the norm and trace of an element $\gamma \in \Omega_p$, in the coordinates of section 2.5, are given by

$$\begin{aligned} \mathrm{nr}(\gamma) &= a_0^2 - a_0 a_1 + \epsilon a_1^2 - p(a_2^2 - a_2 a_3 + \epsilon a_3^2) \\ \mathrm{tr}(\gamma) &= 2a_0 + a_1, \end{aligned}$$

where $\epsilon \in \mathbb{Z}_p$ and $1 - 4\epsilon \in \mathbb{Z}_p^* \setminus (\mathbb{Z}_p^*)^2$. If $p \mid \mathrm{nr}(\gamma)$, then $p \mid (a_0^2 - a_0 a_1 + \epsilon a_1^2)$. Hence $p \mid a_0$ and $p \mid a_1$, so $p \mid \mathrm{tr}(\gamma)$. □

As a direct consequence, we get:

Corollary 10.3. *If $\gamma \in \Lambda$ is an element with $\mathrm{nr}(\gamma) = n$ and $n \mid d(A)$, then $n \mid \mathrm{tr}(\gamma)$.*

If $\lambda \in \Lambda \setminus \mathbb{Z}$, then we let $S(\lambda)$ denote the quadratic order over $\mathbb{Z}$ given by

$$S(\lambda) = \mathbb{Q}(\lambda) \cap \Lambda.$$

By construction, we have that $S(\lambda)$ is an optimally embedded order in Λ containing λ. If $\Delta \neq 0$ is an integer with $\Delta \equiv 0 \pmod 4$ or $\Delta \equiv 1 \pmod 4$, then we let S_Δ be a quadratic order over $\mathbb{Z}$ with discriminant Δ.

Now we are ready to determine the number of fixed points of an involution ι_n, where $n > 1$ and $n \mid d(A)$. Take an element $\gamma \in \Lambda$ with $\mathrm{nr}(\gamma) = n$ and a point $z \in \mathcal{H}$. The point z maps to a fixed point of ι_n in C, if and only if there exists a $\lambda \in \Lambda^1$ such that $\gamma z = \lambda z$. This gives that $\gamma_1 := \lambda^{-1}\gamma$ is an elliptic element. By corollary 10.3, we have $\mathrm{tr}(\gamma_1) = kn$ for some integer k, and hence we get

$$\mathrm{tr}(\gamma_1)^2 - 4\,\mathrm{nr}(\gamma_1) = k^2n^2 - 4n < 0.$$

This inequality implies that $k = 0$ or $k = \pm 1$, and the latter case can only happen if $n = 2$ or $n = 3$.

Consider first the case $k = \pm 1$. Replacing γ_1 with $-\gamma_1$ if necessary, we can assume that $\mathrm{tr}(\gamma_1) > 0$. Consider first the case $\mathrm{nr}(\gamma_1) = 2$ and $\mathrm{tr}(\gamma_1) = 2$. Then we get that $\gamma_1 - 1 \in \Lambda^1$ and $(\gamma_1 - 1)^2 = -1$, and hence z is in fact an elliptic point with respect to the group Λ^1. Similarly, if $\mathrm{nr}(\gamma_1) = 3$ and $\mathrm{tr}(\gamma_1) = 3$, then $\gamma_1 - 2 \in \Lambda^1$ and $(\gamma_1 - 2)^3 = 1$, so z is an elliptic point of order 3. Conversely, it is clear that if $n = 2$ or $n = 3$, then every elliptic point of C of order n is a fixed point of ι_n.

Now we want to study those fixed points of an involution ι_n which are not elliptic points of C. If $\gamma_1 \in \Lambda$ with $\mathrm{nr}(\gamma_1) = n$ and $\mathrm{tr}(\gamma_1) = 0$, then the order $S(\gamma)$ contains a copy of the order $\mathbb{Z}[\sqrt{-n}]$. Conversely, if S is a quadratic order optimally embedded in Λ and which contains a copy of $\mathbb{Z}[\sqrt{-n}]$, then S determines a fixed point of ι_n.

Take now elements $\gamma, \gamma' \in \Lambda$ with $\mathrm{nr}(\gamma) = \mathrm{nr}(\gamma') = n$ and $\mathrm{tr}(\gamma) = \mathrm{tr}(\gamma') = 0$, and let $z, z' \in \mathcal{H}$ be the fixed points of γ and γ' respectively. These points map to the same point in C if and only if $z' = \lambda z$ for some $\lambda \in \Lambda^1$. But then γ and $\lambda^{-1}\gamma'\lambda$ both have z as fixed point and hence they generate the same subfield of A. We get that the quadratic orders $S(\gamma)$ and $S(\gamma')$ satisfy $S(\gamma') = \lambda S(\gamma)\lambda^{-1}$.

Hence, we have that the fixed points of ι_n correspond to Λ^1-conjugacy classes of optimally embedded orders S in Λ which contain $\mathbb{Z}[\sqrt{-n}]$. By lemma 3.7, the number of such classes is $e(S, \Lambda)$. Furthermore, n is square

free, and hence the only possible isomorphism classes for S are orders of discriminant $-n$ or $-4n$. We have proved

Proposition 10.4. *Let Λ be an Eichler order over $\mathbb{Z}$ and $n > 1$ an integer with $n \mid d(A)$. Then the number of fixed points of ι_n is given by*

i) $e_2 + e(S_{-8}, \Lambda)$ *if* $n = 2$,

ii) $e_3 + e(S_{-12}, \Lambda)$ *if* $n = 3$,

iii) $e(S_{-n}, \Lambda) + e(S_{-4n}, \Lambda)$ *if* $n \equiv 3 \pmod 4$,

iv) $e(S_{-4n}, \Lambda)$ *otherwise.*

The embedding numbers can be calculated using the results cited in section 3.5.

10.3 An example

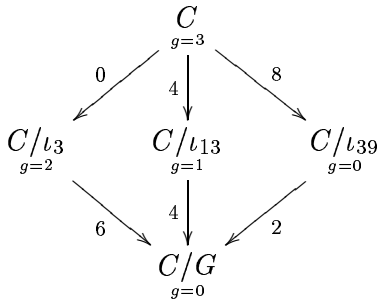
As an example illustrating the group of involutions studied in section 10.2, we consider the case where Λ is a maximal order with discriminant 39. By the formulas of section 10.1, we get $\int_{\mathcal{F}} \omega = -4$ and $e_2 = e_3 = 0$. Hence the genus g of C is 3. We have that the group G of involutions acting on C is

$$G = \{\iota_1, \iota_3, \iota_{13}, \iota_{39}\}$$

in this case. By proposition 10.4, we get:

Involution	Number of fixed points
ι_3	$e_3 + e(S_{-12}, \Lambda) = 0$
ι_{13}	$e(S_{-52}, \Lambda) = 4$
ι_{39}	$e(S_{-39}, \Lambda) + e(S_{-156}, \Lambda) = 4 + 4 = 8$

Given the number of fixed points of an involution ι, it is easy to calculate the genus of the curve C/ι using Hurwitz' formula. Doing this, we get the following diagram consisting of all possible quotients of C by subgroups of G:



In this diagram, a number at an arrow indicates the number of ramification points of the corresponding map. We have also indicated the genus g of each of the curves.

One conclusion we can draw from this investigation is that the curve C is hyperelliptic, since C/ι_{39} is a rational curve. Since the genus of C is 3, an equivalent way to express this is to say that C is not a plane curve.

11 Surfaces

First we will recall some general facts about numerical invariants of projective surfaces in general, and about Shimura surfaces in particular. We also recall the notion of local Chern divisors associated to quotient singularities, which are needed to compute self-intersections of the modular curves.

In section 11.3, we study extensions of the subgroup. It turns out that for the case we will study in chapter 12, there is a canonical discrete extension $\widehat{\Gamma}$ of Γ such that $\widehat{\Gamma}/\Gamma$ is isomorphic to the dihedral group D_4.

In section 11.4, we study the resolution of singularities generated by finite subgroups of $\mathrm{Aut}(\mathcal{H}\times\mathcal{H})$. Such quotient singularities are of course well investigated, the reason that we treat this subject at such great lengths is that we will need rather detailed information about how the proper transforms of the curves F_β meet the exceptional divisors of the singularities. In section 11.5, we show a way to get that information which is practical in concrete examples.

11.1 Numerical invariants

We first recall some well known general definitions and facts about non-singular projective surfaces, see for example [1] for more details.

Let Z be a non-singular surface. We let $e(Z)$ denote the topological Euler characteristic of Z, and K_Z the canonical divisor of Z. The geometric genus of Z is defined by $p_g(Z) = h^2(\mathcal{O}_Z)$, and the so called irregularity of Z is $q(Z) = h^1(\mathcal{O}_Z)$. The arithmetic genus of Z is

$$\chi(Z) = 1 - q(Z) + p_g(Z). \tag{11.1}$$

(Note that in many books $\chi(Z)-1$ is called the arithmetic genus.) p_g, q and χ are birational invariants. The arithmetic genus can be computed using Noethers formula:

$$\chi(Z) = \frac{K_Z^2 + e(Z)}{12}. \tag{11.2}$$

The following result will be useful to compute χ for the various surfaces in chapter 12 (see [1], p. 183):

Lemma 11.1. *Let Z be a non-singular surface with an involution $\iota : Z \to Z$. Assume that the set of fixed points of ι is the union of a finite set of rational curves B_i, $i = 1, \ldots, n$. Then we have*

$$\chi(Z/\iota) = \frac{1}{2}\chi(Z) + \sum_{i=1}^{n}(B_i^2 + 2).$$

To prove that surfaces are rational, the following corollary of Castelnuovo's criterion for rationality of a surface (see [21], corollary 1, p. 255) is useful:

Proposition 11.2. *Let Z be a non-singular surface with $q = 0$. If Z contains a non-singular rational curve D with $D^2 \geq 0$, then Z is rational.*

We now summarise some well known results about the numerical invariants of Shimura surfaces. For a more detailed discussion, we refer to [21] and [47].

Let A and Λ be as in chapter 6. Let Γ' be a discrete subgroup of $\mathrm{Aut}(\mathcal{H}) \times \mathrm{Aut}(\mathcal{H})$, which contains the image Γ of Λ^1. Let $\mathcal{F}$ be a fundamental domain for the group action, let X be the quotient surface $X = \mathcal{H} \times \mathcal{H}/\Gamma'$ and let Y be the minimal desingularisation of X.

Let ω be the Gauss-Bonnet form on $\mathcal{H} \times \mathcal{H}$:

$$\omega = \frac{1}{(2\pi)^2} \frac{dx_1 \wedge dy_1}{y_1^2} \wedge \frac{dx_2 \wedge dy_2}{y_2^2},$$

where $z_k = x_k + iy_k$, $k = 1, 2$ are the standard coordinates on the two factors of $\mathcal{H} \times \mathcal{H}$. The Euler characteristic $e(X)$ is given by

$$e(X) = \int_{\mathcal{F}} \omega + \sum_{r>1} e_r \frac{r-1}{r}, \tag{11.3}$$

where e_r is the number of classes of elliptic points of order r (see [21], p. 197).

Assume now that $\Gamma' = \Gamma$. The formula for the volume of the fundamental domain $\mathcal{F}$ can be found for example in [47], p. 193. In our case, when Λ is a maximal order and the quaternion algebra A admits an involution of type 2, the formula may be written as

$$\int_{\mathcal{F}} \omega = 2\zeta_k(-1) \prod_{p | d_0(\Lambda)} (p-1)^2. \tag{11.4}$$

Here ζ_k is the zeta-function of the field k. The value $\zeta_k(-1)$ can be easily computed using a formula of Siegel (see e.g. [21], p. 192).

By Satz 8 in [15], we have that the irregularity q of the surface Y vanishes:

$$q(Y) = 0 \tag{11.5}$$

In our case, we also have, since A is a skew field, that

$$\chi(X) = \frac{1}{4}e(X) \tag{11.6}$$

(see [47], p. 206–207).

11.2 Quotient singularities

Let $p > 1$ be an integer, ρ a primitive p-th root of unity, and q_1 and q_2 two integers which are relatively prime to p. We define an action of the cyclic group C_p of order p on $\mathbb{C}^2$, generated by the mapping

$$(z_1, z_2) \mapsto (\rho^{q_1} z_1, \rho^{q_2} z_2).$$

The origin of $\mathbb{C}^2$ maps to a singular point of $\mathbb{C}/C_p$, which we denote by P. A singular point of a complex space, which are locally isomorphic to P, is said to be a *quotient singularity* of type $(p; q_1, q_2)$.

Let z be a quotient singularity on X. Let D_j be the components of the minimal resolution of the singularity. The Chern divisor of the singularity is defined to be

$$c_1^{(z)} = \sum_j a_j D_j,$$

where the rational numbers a_j satisfy

$$\sum_j a_j (D_i D_j) = 2 + D_i^2,$$

for all i. If the singularity is of type $(2; 1, 1)$, then the exceptional divisor is a single (-2)-curve, and if the singularity is of type $(3; 1, 2)$, then the exceptional divisor consist of two transversal (-2)-curves. Hence $c_1^{(z)} = 0$ in these cases. If the singularity is of type $(3; 1, 1)$, then $c_1^{(z)} = \frac{1}{3}D_1$, where D_1 is the (-3)-curve which is the resolution.

The following result is needed to compute the self-intersections of the modular curves. For a proof, see [21], section 4.3.

Proposition 11.3. *Assume that X has s quotient singularities, and let $c_1^{(\nu)}$, for $\nu = 1, \ldots, s$, be the corresponding Chern divisors on Y. Consider a modular curve F_β on Y. We have:*

$$c_1[F_\beta] = 2 \int_{C_\beta/\Gamma_\beta} \omega + \sum_{\nu=1}^{s} c_1^{(\nu)} F_\beta, \tag{11.7}$$

where ω is the Gauss-Bonnet form on C_β (and $c_1[F_\beta] = -K_Y F_\beta$).

11.3 Extensions of the group Γ

We will now construct discrete subgroups of $\mathrm{Aut}(\mathcal{H}\times\mathcal{H})$ which extend the group Γ. Recall that we have a natural sequence

$$(1) \to \mathrm{Aut}(\mathcal{H}) \times \mathrm{Aut}(\mathcal{H}) \to \mathrm{Aut}(\mathcal{H}\times\mathcal{H}) \to S_2 \to (1).$$

We will construct a tower of discrete subgroups of $\mathrm{Aut}(\mathcal{H}\times\mathcal{H})$

$$\Gamma \subseteq \Gamma_1 \subseteq \Gamma_2 \subseteq \Gamma_3 \subset \widehat{\Gamma}, \tag{11.8}$$

where $\Gamma_3 \subset \mathrm{Aut}(\mathcal{H}) \times \mathrm{Aut}(\mathcal{H})$ and $\widehat{\Gamma} \not\subset \mathrm{Aut}(\mathcal{H}) \times \mathrm{Aut}(\mathcal{H})$.

First we need some preparatory results. The following can be found, for example, in [42], lemma 1.3.

Proposition 11.4. *If k is a totally real number field with ring of integers R and Λ is a maximal order in a totally indefinite quaternion algebra over k, then the norm map $\mathrm{nr} : \Lambda \to R$ is surjective.*

This result is originally by Eichler. So is the following, which is a version of his norm theorem (see [35], theorem 34.9):

Proposition 11.5. *If J is a two-sided Λ ideal, then J is principal if and only if the R-ideal $\mathrm{nr}(J)$ is principal.*

Let $\mathrm{Cl}^+(k)$ be the class group of k in the narrow sense (i.e. two ideals $\mathfrak{i}_1$ and $\mathfrak{i}_2$ are equivalent if $\mathfrak{i}_1 = x\mathfrak{i}_2$ for some $x \in k$ with $\mathrm{nr}(x) > 0$). For a proof of the following result, see [16], theorem 39.

Proposition 11.6. *Let k be a real quadratic field with discriminant D, and let t be the number of different primes dividing D. Then*

$$\#(\mathrm{Cl}^+(k)/\,\mathrm{Cl}^+(k)^2) = 2^{t-1}.$$

Furthermore, the subgroup of 2-torsion elements of $\mathrm{Cl}^+(k)$ is the subgroup generated by ideals $\mathfrak{g}$ with $\mathfrak{g} \mid D$.

Let now t be the number of primes dividing D and let a be the number of prime ideals in R dividing $d(\Lambda)$. Let $\mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_a$ be a prime factorisation of the ideal $d(\Lambda) \subseteq R$, where we assume that we have ordered the factors so that $\mathfrak{p}_{2j} = \overline{\mathfrak{p}}_{2j-1}$ for $j = 1, 2, \ldots, a/2$. Let ϵ_0 be a fundamental unit of R. If $\mathrm{nr}\,\epsilon_0 = 1$, then we assume that ϵ_0 is chosen to be totally positive.

Let A^+ be the set of all elements in A with totally positive norm. If $\lambda \in A^+$, then λ acts on $\mathcal{H}\times\mathcal{H}$ by

$$\lambda(z_1, z_2) = (\varrho_0(\lambda)z_1, \varrho_0(\overline{\lambda})z_2),$$

so we can extend the definition of the map ϱ and get a map

$$\varrho : A^+ \to \mathrm{Aut}(\mathcal{H}\times\mathcal{H})$$

such that $\ker \varrho = k^*$ and $\Gamma = \varrho(\Lambda^1)$. As we will see, it is never the case that the group Γ is a maximal discrete subgroup of $\mathrm{Aut}(\mathcal{H}\times\mathcal{H})$.

The most obvious way to extend the group Γ is to use more units in Λ, if that is possible. Let R^+ denote the group

$$R^+ = \{x \in R^* \mid x >> 0\}.$$

We have that $R^+ \supseteq (R^*)^2$. The index $[R^+ : (R^*)^2]$ equals 2 or 1, depending on whether the fundamental unit ϵ_0 of R is totally positive or not. Let

$$\Lambda^{(1)} = \{\lambda \in \Lambda \mid \mathrm{nr}\,\lambda \in R^+\},$$

and define

$$\Gamma_1 = \varrho(\Lambda^{(1)}).$$

We have that $\Lambda^{(1)} \supseteq R^*\Lambda^1$. If $\lambda \in \Lambda^{(1)}$, then $\varrho(\lambda)$ is an element of Γ if and only if $\lambda \in R^*\Lambda^1$. Assume that $\epsilon_0 \in R^+$. By proposition 11.4, there exists an element $\lambda \in \Lambda$ such that $\mathrm{nr}\,\lambda = \epsilon_0$ and therefore $\Gamma_1 = \Gamma \cup \varrho(\lambda)\Gamma$ is an extension of Γ of degree 2. We have that λ acts as an involution on the surface $\mathcal{H}\times\mathcal{H}/\Gamma$.

We can go one step further and use elements in A^+ normalising Λ. We define

$$N^+(\Lambda) = \{n \in A^+ \mid n\Lambda n^{-1} = \Lambda\}$$

and

$$\Gamma_3 = \varrho(N^+(\Lambda)).$$

Proposition 11.7. *Γ_3 is a finite extension of Γ which contains Γ as a normal subgroup. Furthermore, the quotient group Γ_3/Γ is a 2-group with at most 2^{t+a-1} elements.*

Proof. It is clear that Γ is a normal subgroup of Γ_3. Take $n \in N^+(\Lambda)$. We can, without loss of generality, assume that $n \in \Lambda$. Define

$$J = \Lambda n (= n\Lambda),$$

which is a two-sided Λ-ideal. By corollary 2.13, we have that J can be uniquely written in the form

$$J = \mathfrak{i} J_0, \tag{11.9}$$

where $\mathfrak{i}$ is an ideal in R and J_0 is a two-sided ideal in Λ such that $\mathrm{nr}(J_0)$ divides $d(\Lambda)$. Such an ideal J_0 must necessarily satisfy $J_0^2 = \mathrm{nr}(J_0)\Lambda$.

We want to show that Γ_3/Γ is a 2-group. Taking the norm of both sides of equation (11.9), we get $\mathfrak{i}^2 \mathrm{nr}(J_0) = \mathrm{nr}(n)R$. Hence we get $n^2\Lambda = \mathfrak{i}^2 J_0^2 = \mathfrak{i}^2 \mathrm{nr}(J_0)\Lambda = \mathrm{nr}(n)\Lambda$. If we put $\epsilon = (\mathrm{nr}(n))^{-1} n^2$, then we have $\epsilon \in \Lambda^1$ and $\varrho(n^2) = \varrho(\epsilon) \in \Gamma$. This shows that Γ_3/Γ is a 2-group.

For each prime factor $\mathfrak{p}$ of $d(\Lambda)$, we define a map

$$\vartheta_{\mathfrak{p}} : k^* \to \mathbb{Z}/2\mathbb{Z},$$

by $\vartheta_{\mathfrak{p}}(x) = v_{\mathfrak{p}}(x) + 2\mathbb{Z}$. Here $v_{\mathfrak{p}}$ denotes the valuation corresponding to the prime ideal $\mathfrak{p}$. We may extend the definition of $\vartheta_{\mathfrak{p}}$ to all non-zero R-ideals. Let now

$$\vartheta : N^+(\Lambda) \to (\mathbb{Z}/2\mathbb{Z})^{\oplus a}$$

be defined through

$$\vartheta(n) = \left(\vartheta_{\mathfrak{p}_j}(\mathrm{nr}(J_0(n)))\right)_{j=1}^{a}$$

Here $J_0(n)$ denotes the unique two-sided Λ-ideal given by equation (11.9), i.e. we have $n\Lambda = \mathfrak{i}(n) J_0(n)$, $J_0(n) \subseteq \Lambda$ and $\mathrm{nr}(J_0(n)) \mid d(\Lambda)$. It is clear that the map ϑ factors through Γ_3, and we get a group homomorphism

$$\vartheta : \Gamma_3 \to (\mathbb{Z}/2\mathbb{Z})^{\oplus a}.$$

Let now

$$\Gamma_2 = \ker(\vartheta).$$

We have $\Gamma \subseteq \Gamma_2$ and $[\Gamma_3 : \Gamma_2] \leq 2^a$. We want to estimate $[\Gamma_2 : \Gamma]$. To each element $\varrho(n) \in \Gamma_2$, we can, by equation (11.9), associate an ideal class $[\mathfrak{i}] \in \mathrm{Cl}(k)$, where the ideal $\mathfrak{i}$ satisfies

$$n\Lambda = \mathfrak{i}\Lambda. \tag{11.10}$$

We get a group homomorphism

$$\psi : \Gamma_2 \to \mathrm{Cl}(k).$$

It is clear that the kernel of ψ is Γ_1.

Taking the norm of both sides of equation (11.10), we get that $\mathfrak{i}^2 = \mathrm{nr}(n)R$. Hence the ideal class of $\mathfrak{i}^2$ is trivial in the group $\mathrm{Cl}^+(k)$. Consider now the (well defined) map

$$f : \mathrm{Cl}(k) \to \mathrm{Cl}^+(k),$$

given by $[\mathfrak{i}] \mapsto [\mathfrak{i}^2]$, and the natural map

$$g : \mathrm{Cl}^+(k) \to \mathrm{Cl}(k).$$

We have seen that $\psi(\Gamma_2) \subseteq \ker f$, and hence we get

$$[\Gamma_2 : \Gamma] = [\Gamma_2 : \Gamma_1][\Gamma_1 : \Gamma] \leq \#\ker(f)\#\ker(g) = \#\ker(f \circ g),$$

where the last equality holds since g is surjective. Now, the kernel of $f \circ g$ consists of the 2-torsion elements of $\mathrm{Cl}^+(k)$, so we get

$$[\Gamma_2 : \Gamma] \leq \#(\mathrm{Cl}^+(k)/\,\mathrm{Cl}^+(k)^2) = 2^{t-1},$$

by proposition 11.6. The claim follows. □

We know, by proposition 11.6, that the set of all ideal classes $[\mathfrak{g}]$, where $\mathfrak{g}$ is a square free ideal in R such that $\mathfrak{g} \mid D$, generates the subset of 2-torsion elements in $\mathrm{Cl}^+(k)$. Hence we can reformulate the construction of Γ_2 as follows. If $\mathfrak{g}$ is a square free ideal in R such that $\mathfrak{g} \mid D$, then we define the set

$$\Lambda^{\mathfrak{g}} = \{\lambda \in \mathfrak{g}\Lambda \mid \lambda \in A^+ \text{ and } \mathrm{nr}(\lambda)R = \mathfrak{g}^2\}.$$

We claim that $\Lambda^{\mathfrak{g}}$ is non-empty. Namely, note that the ideal $\mathfrak{g}^2$ is generated by some positive integer k. By proposition 11.5, there is an element $\lambda_1 \in \mathfrak{g}\Lambda$ such that $\mathrm{nr}(\lambda_1) = \epsilon k$, with $\epsilon \in R^*$. By proposition 11.4, there is $\lambda_2 \in \Lambda$ such that $\mathrm{nr}(\lambda_2) = \epsilon^{-1}$, and hence $\lambda_1\lambda_2 \in \Lambda^{\mathfrak{g}}$. From the proof of the proposition, we now see that

$$\Gamma_2 = \bigcup_{\substack{\mathfrak{g} \mid D \\ \mathfrak{g} \text{ square free}}} \varrho(\Lambda^{\mathfrak{g}}).$$

Now we want to construct the group $\widehat{\Gamma}$ in (11.8), which also contains elements shifting the factors of $\mathcal{H}\times\mathcal{H}$. Let T be a choice of a map $T : \mathcal{H}\times\mathcal{H} \to \mathcal{H}\times\mathcal{H}$, as given by lemma 7.26. We have that T is of the form $T(z_1, z_2) = (\omega z_2, \overline{\omega} z_1)$, where $\omega \in A$ with $\omega\overline{\Lambda} = \Lambda\omega$, $\omega\overline{\omega} \in \mathbb{Z}\Lambda^1$ and $\mathrm{nr}(\omega) >> 0$. If $\lambda \in \Lambda^1$, then we get

$$T\varrho(\lambda)T = \varrho(\omega\overline{\lambda}\overline{\omega}) = \varrho(\omega\overline{\lambda}\omega^{-1})\varrho(\omega\overline{\omega}) \in \Gamma. \tag{11.11}$$

Hence we have $T\Gamma T = \Gamma$, so $\Gamma \cup T\Gamma$ is a group extension of Γ. We conclude that T acts as an involution on $\mathcal{H}\times\mathcal{H}/\Gamma$. The group $\Gamma \cup T\Gamma$ does depend on the particular choice of T though.

Take an element $n \in N^+(\Lambda)$. As in (11.11), we get that $T\varrho(n)T = \varrho(\omega\overline{n}\omega^{-1})\varrho(\omega\overline{\omega})$. Since we have $\omega\overline{n}\omega^{-1} \in N^+(\Lambda)$, we get $T\Gamma_3 T = \Gamma_3$. Hence we can also conclude that the set

$$\widehat{\Gamma} = \Gamma_3 \cup T\Gamma_3$$

is a group. In particular, we have that T acts as an involution on $\mathcal{H}\times\mathcal{H}/\Gamma_3$. We also note that $\widehat{\Gamma}$ is well defined extension of Γ_3, i.e. it does not depend on the choice of ω. Consider namely two different choices of elements ω_1 and ω_2, corresponding to maps T_1 and T_2 respectively. Then we get $\omega_2\omega_1^{-1} \in N^+(\Lambda)$, and hence $T_2 = \varrho(\omega_2\omega_1^{-1})T_1$, where $\varrho(\omega_2\omega_1^{-1}) \in \Gamma_3$. From now on, we fix the choice of T.

Consider the group

$$G = \widehat{\Gamma}/\Gamma,$$

which we can identify with a group of automorphisms of X. We have natural subgroups $G_2 \subseteq G_3 \subset G$, where $G_2 = \Gamma_2/\Gamma$ and $G_3 = \Gamma_3/\Gamma$. The 2-group G_3 consists of involutions on X. We want to determine the group structure of G. We have an exact sequence

$$1 \to G_3 \to G \to S_2 \to 1. \tag{11.12}$$

This sequence splits, by sending the generator of S_2 to $T \in G$. The group structure of $\widehat{\Gamma}/\Gamma$ is determined by the action of T on G_3 given by conjugation with T. We have an exact sequence

$$(1) \to G_2 \to G_3 \xrightarrow{\vartheta} (\mathbb{Z}/2\mathbb{Z})^{\oplus a}.$$

Lemma 11.8. *Conjugation by T acts trivially on G_2. The induced action on $G_3/G_2 \cong \Gamma_3/\Gamma_2$ is the restriction to the image of ϑ of the map linear map $(\mathbb{Z}/2\mathbb{Z})^{\oplus a} \to (\mathbb{Z}/2\mathbb{Z})^{\oplus a}$, which is given by the matrix*

$$M = \begin{pmatrix} 0 & 1 & & & \\ 1 & 0 & & & \\ & & 0 & 1 & \\ & & 1 & 0 & \\ & & & & \ddots \end{pmatrix}.$$

Proof. Let $\mathfrak{g}$ be a square free ideal in R with $\mathfrak{g} \mid D$. Let $\lambda \in \Lambda^{\mathfrak{g}}$. We have that $\mathrm{nr}(\lambda)R = \mathfrak{g}^2$, $\lambda\Lambda = \mathfrak{g}\Lambda$ and $\mathrm{nr}(\lambda) >> 0$. Since the ideal $\mathfrak{g}^2$ is generated by a rational integer, we get $\mathrm{nr}(\lambda) = \epsilon x$, where $\epsilon \in R^*$ with $\mathrm{nr}_{k/\mathbb{Q}}(\epsilon) = 1$ and $x \in \mathbb{Z}$. Now we have $T\varrho(\lambda)T^{-1} = \varrho(\omega\overline{\lambda}\omega^{-1})$. Therefore,

$$\omega\overline{\lambda}\omega^{-1}\Lambda = \omega\overline{\lambda\Lambda}\omega^{-1} = \omega\overline{\mathfrak{g}\Lambda}\omega^{-1} = \mathfrak{g}\Lambda = \lambda\Lambda,$$

so $\omega\overline{\lambda}\omega^{-1} = \lambda\nu$ for some $\nu \in \Lambda^*$. We get $\mathrm{nr}(\nu) = \mathrm{nr}(\overline{\lambda})/\mathrm{nr}(\lambda) = \overline{\epsilon}/\epsilon = \epsilon^{-2} \in (R^*)^2$, so $\varrho(\nu) \in \Gamma$. Hence $T\varrho(\lambda)T^{-1} = \varrho(\lambda)\varrho(\nu) \in \varrho(\lambda)\Gamma$, so we have shown that conjugation by T acts trivially on G_2.

Assume now that $n \in N^+(\Lambda)\cap\Lambda$. If we write $n\Lambda = \mathfrak{i}J_0$ as in (11.9), then we get $\omega\overline{n}\omega^{-1}\Lambda = \overline{\mathfrak{i}}(\omega\overline{J}_0\omega^{-1})$. We have that $\omega\overline{J}_0\omega^{-1} \subseteq \Lambda$ is a two-sided Λ-ideal with $\mathrm{nr}(\omega\overline{J}_0\omega^{-1}) = \overline{\mathrm{nr}(J_0)}$. Hence we see that $\vartheta(\omega\overline{n}\omega^{-1}) = M\vartheta(n)$ under our assumption on the ordering of the ideals $\mathfrak{p}_i$. This proves the lemma. □

Remark. When $a = 0$, i.e. when Γ is a Hilbert modular group, then Γ_3 is the well known Hurwitz-Maass extension of Γ. It can be shown that $[\Gamma_3 : \Gamma] = 2^{t-1}$, and that Γ_3 is the unique maximal discrete subgroup of $\mathrm{Aut}(\mathcal{H}) \times \mathrm{Aut}(\mathcal{H})$ containing Γ. See for example [17], p. 11, for further details.

Proposition 11.9. *Assume that $D = p$ is a prime, $h(k) = 1$ and $d_0(\Lambda) = q$, where q is a rational prime. Then $G \cong D_4$, the dihedral group.*

Proof. In this case, we have that $t = 1$ and $a = 2$, so we get $\Gamma_2 = \Gamma$ and $[\Gamma_3 : \Gamma] \leq 4$.

We have that the prime q is split in k. Since $h(k) = 1$, we can therefore write a prime factorisation $q = uv$, with $u, v \in R$. Since $p \equiv 1 \pmod 4$, we have that R contains a unit with norm -1. Hence we can assume that both u and v are totally positive. Since $\mathrm{nr} : \Lambda \to R$ is surjective, by proposition 11.4, we can choose elements $\lambda_u, \lambda_v \in \Lambda$, with $\mathrm{nr}(\lambda_u) = u$ and $\mathrm{nr}(\lambda_v) = v$. Hence, we have that $[\Gamma_3 : \Gamma] = 4$, so the map ϑ is surjective in this case.

If we use the additive notation, then the sequence (11.12) is

$$0 \to \mathbb{Z}/2 \times \mathbb{Z}/2 \to \widehat{\Gamma}/\Gamma \to \mathbb{Z}/2 \to 0,$$

where the action of T by conjugation on $\Gamma_3/\Gamma \cong \mathbb{Z}/2 \times \mathbb{Z}/2$ is given by the linear map with matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. This gives immediately that $\widehat{\Gamma}/\Gamma$ is isomorphic to the dihedral group D_4. □

Finally, we remark that one open question remains. We do not know whether $\widehat{\Gamma}$ is a maximal discrete subgroup of $\mathrm{Aut}(\mathcal{H}\times\mathcal{H})$ in the case that A is a skew field.

11.4 Finite subgroups of $\mathrm{Aut}(\mathcal{H}\times\mathcal{H})$

Let Γ be a discrete subgroup of $\mathrm{Aut}(\mathcal{H}\times\mathcal{H})$ and $z = (z_1, z_2)$ a point in $\mathcal{H}\times\mathcal{H}$. Let Γ_z be the finite subgroup of Γ consisting of all $\gamma \in \Gamma$ such that $\gamma z = z$. Let $\Gamma_{z,0}$ denote the group

$$\Gamma_{z,0} = \Gamma_z \cap (\mathrm{Aut}(\mathcal{H})\times\mathrm{Aut}(\mathcal{H})).$$

We make the assumption that both the projections of $\Gamma_{z,0}$ into the two factors $\mathrm{Aut}(\mathcal{H})$ are injective. This implies, in particular, that $\Gamma_{z,0}$ is a cyclic group. Let n denote the order of Γ_z, and let n_0 denote the order of $\Gamma_{z,0}$.

Consider the quotient surface $\mathcal{H}\times\mathcal{H}/\Gamma_z$. We are interested in the singularity of this surface, and its resolution. Furthermore, we will also examine curves of the form

$$C_\beta = \{(u, \beta u) \mid u \in \mathcal{H}\} \subseteq \mathcal{H}\times\mathcal{H}, \tag{11.13}$$

where $\beta \in \mathrm{SL}_2(\mathbb{R})$. If C_β is such a curve which happens to contain the point z, consider the proper transform of the image of C_β in $\mathcal{H}\times\mathcal{H}/\Gamma_z$ in the resolution of $\mathcal{H}\times\mathcal{H}/\Gamma_z$. We want to find out how this curve intersects the exceptional divisors of the resolved singularity.

Let Δ denote the unit disc $\Delta = \{\zeta \in \mathbb{C} \mid \ |\zeta| < 1\}$, and let Δ^2 denote the pluridisc $\Delta \times \Delta$. Consider the map $\eta : \mathcal{H}\times\mathcal{H} \to \Delta^2$ given by

$$\eta(\zeta_1, \zeta_2) = \left(\frac{\zeta_1 - z_1}{\zeta_1 - \overline{z}_1}, \frac{\zeta_2 - z_2}{\zeta_2 - \overline{z}_2}\right). \tag{11.14}$$

Let $\gamma \in \Gamma_{z,0}$ be given by $(\gamma_1, \gamma_2) \in \mathrm{SL}_2(\mathbb{R})^2$, where $\gamma_j = \left(\begin{smallmatrix} a_j & b_j \\ c_j & d_j \end{smallmatrix}\right)$ for $j = 1, 2$, and let $s_j = \mathrm{tr}(\gamma_j)$ and $n_j = \det(\gamma_j)$. Then we get

$$(\eta \circ \gamma \circ \eta^{-1})(\zeta_1, \zeta_2) = (r_1\zeta_1, r_2\zeta_2),$$

where

$$r_j = \left(\frac{s_j^2}{2n_j} - 1\right) - i\,\mathrm{sign}(s_j c_j)\sqrt{1 - \left(\frac{s_j^2}{2n_j} - 1\right)^2}.$$

The factors r_1 and r_2 will be called the factors of rotation of the group element γ. They are of course roots of unity and they have the same order by the assumption we have on $\Gamma_{z,0}$. It is clear that η transforms Γ_z to a subgroup G of $\mathrm{GL}_2(\mathbb{C})$. Let G_0 denote the subgroup of G corresponding to $\Gamma_{z,0}$. Hence, we have

$$G_0 = \left\langle \begin{pmatrix} \rho & 0 \\ 0 & \rho^k \end{pmatrix} \right\rangle,$$

where $\rho = e^{2\pi i/n_0}$ and k is an integer with $(k, n_0) = 1$. Assume that $G \neq G_0$, and choose an element $g \in G \setminus G_0$. After replacing the variable ζ_2 with a suitable multiple if necessary, we may assume that g is given by a matrix of the form $\left(\begin{smallmatrix} 0 & \sigma \\ 1 & 0 \end{smallmatrix}\right)$, where $\sigma \in \mathbb{C}$. Since we have $g^2 \in G_0$, we get $\sigma = \rho^m$ for some integer m. We will use the notation

$$G(n_0, k, m) = \left\langle \begin{pmatrix} \rho & 0 \\ 0 & \rho^k \end{pmatrix}, \begin{pmatrix} 0 & \rho^m \\ 1 & 0 \end{pmatrix} \right\rangle.$$

Let now C_β be a curve as in (11.13), where $\beta = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$. If $z \in C_\beta$, then a calculation gives that $\eta(C_\beta)$ is the line

$$\{(u, Mu) \mid u \in \Delta\} \subseteq \Delta^2, \tag{11.15}$$

where the factor $M \in \mathbb{C}$, which satisfies $|M| = 1$, is given by

$$M = -\frac{c\overline{z}_1 + d}{cz_1 + d}.$$

The action of G on Δ^2 can of course be extended to an action on $\mathbb{C}^2$. Note that this action is equivalent to the induced action of Γ_z on the tangent space T_z of the point $z \in \mathcal{H}\times\mathcal{H}$.

Let H be a normal subgroup of G. We let ζ_1 and ζ_2 be coordinates on $\mathbb{C}^2$. Let $a, b \in \mathbb{C}$, with $(a, b) \neq (0, 0)$. The line $a\zeta_1 + b\zeta_2 = 0$ in $\mathbb{C}^2$ maps to a curve in $\mathbb{C}^2/H$. If Y is a resolution of $\mathbb{C}^2/H$, then we let $l_{a\zeta_1+b\zeta_2=0}$ denote the proper transform of this curve in Y. We will let l denote a generic member of this family of curves.

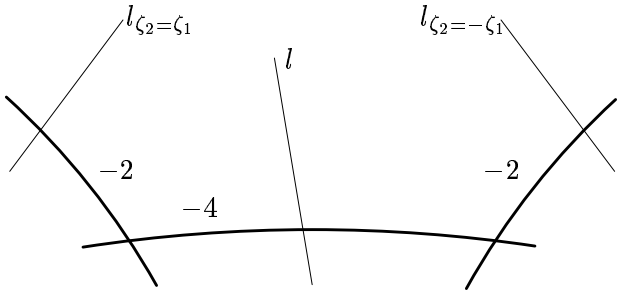
In the example in chapter 12, the cases described in the following lemma will occur.

Lemma 11.10. *Assume that* $\Gamma_z \neq \Gamma_{z,0}$. *If* $\Gamma_z \cong \mathbb{Z}/12$, *then the action of* Γ_z *on* T_z *is equivalent to* $G(6, 1, 1)$ *and if* $\Gamma_z \cong D_6$, *then it is equivalent to* $G(6, -1, 0)$. *If* $\Gamma_z \cong \mathbb{Z}/4$, *then the action is equivalent to* $G(2, 1, 1)$ *and if* $\Gamma_z \cong \mathbb{Z}/2 \times \mathbb{Z}/2$, *then it is equivalent to* $G(2, 1, 0)$.

Proof. k is only significant modulo n_0, so if $n_0 = 2$ then we may choose $k = 1$ and if $n_0 = 6$ then we may choose $k = \pm 1$. Consider first the case $k = 1$. By conjugation with matrices of the form $\gamma = \left(\begin{smallmatrix} \rho & 0 \\ 0 & \rho^a \end{smallmatrix}\right)$, where $a \in \mathbb{Z}$, we see that $G(n_0, 1, m)$ and $G(n_0, 1, m + 2a)$ are equivalent. (Note that the set of lines in $\mathbb{C}^2$ given in (11.15) is preserved under action of γ, since $|\rho| = 1$.) Hence, we only need to consider the cases $m = 0$ and $m = 1$. In particular, we are done in the case $|\Gamma_z| = 4$. If $k = -1$, then we only need to consider the cases $\rho^m = \pm 1$. Hence, in the case $|\Gamma_z| = 12$, we have four cases and the claim now follows by inspection of these. □

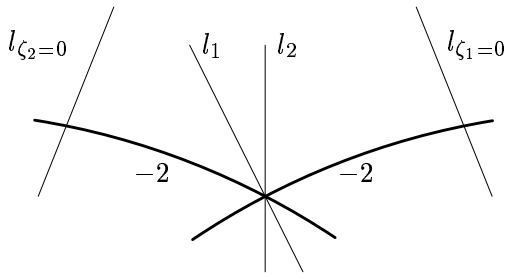
Now we will examine the four cases of lemma 11.10. For certain normal subgroups H of these groups G, we will describe the minimal resolution of the singularity $\mathbb{C}^2/H$ and how the exceptional divisors intersect the curves l. In each case, we will successively introduce notations as follows: If we consider normal subgroups $H_1 \subseteq H_2 \subseteq \ldots$, then we let Y_i denote the canonical resolution surface $\mathcal{H}\times\mathcal{H}/H_i$, and E_i the corresponding exceptional divisor, for $i = 1, 2, \ldots$

Consider first the case $G = G(6,1,1)$, so G is generated by $\left(\begin{smallmatrix} 0 & \rho \\ 1 & 0 \end{smallmatrix}\right)$, where $\rho = e^{2\pi i/6}$. We have $G \cong \mathbb{Z}/12$ and $G_0 = G^2$. The singularity of $\mathbb{C}^2/G$ is of type $(12;1,7)$ in the notation of section 11.2. We will consider the actions induced by the successive subgroups $G_0^2 \lhd G_0 \lhd G$. If we blow up $0 \in \mathbb{C}^2$, then G_0^2 acts trivially on the exceptional divisor. Taking the quotient with G_0^2 yields a (-3)-curve E_1 as exceptional divisor on the surface Y_1. Every curve l intersects E_1 transversally. Consider the involution ι_1 on Y_1 induced by G_0. It has E_1 as fixed point set. Hence the quotient Y_1/ι_1 is smooth and we get a (-6)-curve E_2 as exceptional divisor. Every divisor l is transversal to E_2. Finally G induces an involution ι_2 on Y_2. It has two fixed points, the intersection points of E_2 with the curves $l_{\zeta_2=\zeta_1}$ and $l_{\zeta_2=\zeta_1}$ respectively. Blowing up these points and taking the quotient, we arrive at the following configuration:



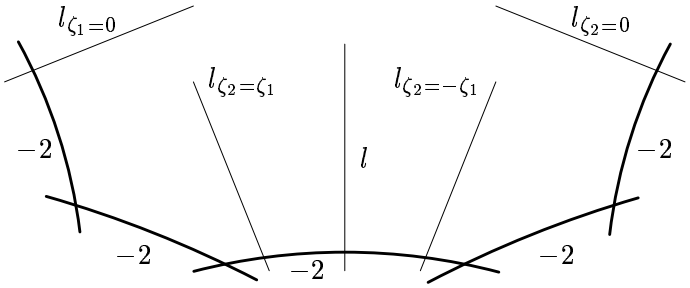
So, with two exceptions, all proper transforms of images of lines in $\mathbb{C}^2$ intersect the (-4)-component transversally.

Consider now the case $G = G(6,-1,0)$, so $G = \left\langle \left(\begin{smallmatrix} \rho & 0 \\ 0 & \rho^{-1} \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \right\rangle$, where $\rho = e^{2\pi i/6}$, and we have $G \cong D_6$. We first consider the action of G_0^2. Blowing up $0 \in \mathbb{C}^2$, we get two isolated fixed points. Blowing up these, we get the two (-1)-curves fixed by the group action. Taking the quotient, the (-3)-curve maps to a (-1)-curve, which we blow down. We get the configuration

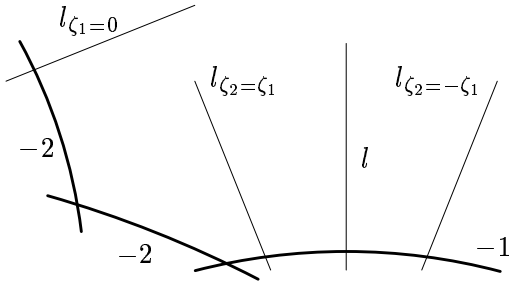


where l_1 and l_2 illustrate two generic curves l. They intersect transversally. The induced action of G_0 now has three fixed points, the intersection point of the two (-2)-curves and the intersection points of these curves with $l_{\zeta_1=0}$

and $l_{\zeta_2=0}$ respectively. When we blow up these and take the quotient, we get



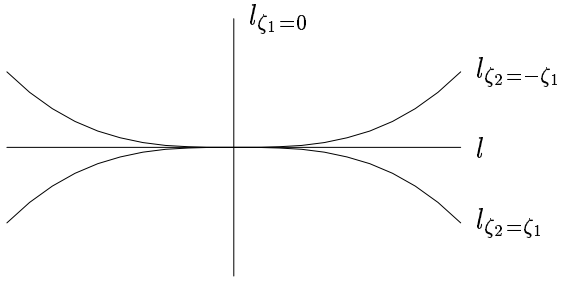
The involution induced by G on this surface has got the divisors $l_{\zeta_2=\zeta_1}$ and $l_{\zeta_2=-\zeta_1}$ as fixed point set so the quotient has the configuration



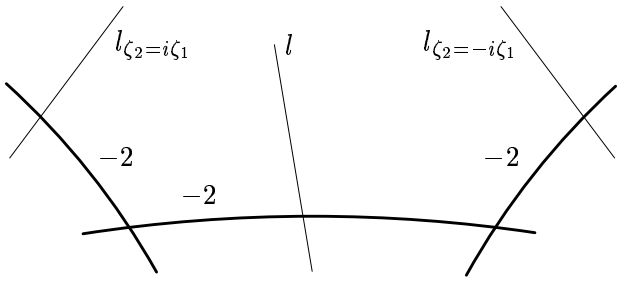
The configuration of the (-1)-curve and the two (-2)-curves can now be blown down. Hence, we have shown that $\mathbb{C}^2/G$ is non-singular. This can also be seen directly, since one can verify that

$$\mathbb{C}[\zeta_1,\zeta_2]^G = \mathbb{C}[\zeta_1^6+\zeta_2^6,\zeta_1\zeta_2]$$

and so $\mathbb{C}^2/G$ is simply isomorphic to the affine plane. Define an isomorphism $\mathbb{C}[u,v]\cong\mathbb{C}[\zeta_1,\zeta_2]^G$ by $u\mapsto\zeta_1^6+\zeta_2^6$ and $v\mapsto\zeta_1\zeta_2$. Then the lines $\zeta_1=0$ and $\zeta_2=0$ map to the line $v=0$, and the line $\zeta_2=a\zeta_1$ for $a\neq 0$ maps to the curve $a^3u=(1+a^6)v^3$. Hence two general lines in $\mathbb{C}^2$ are either mapped to the same curve, or to two smooth curves in $\mathbb{C}^2/G$ having intersection multiplicity 3. The only exceptions are the two lines that are invariant under the subgroup G_0. They are mapped to one curve, which meets the other curves in the family transversally.



Consider now the case $G = G(2,1,1)$. The group G is generated by $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $G \cong \mathbb{Z}/4$. The singularity of $\mathbb{C}^2/G$ is of type $(4;1,3)$. The action of G_0 gives, as above, an exceptional curve E_1 with self-intersection -2 intersecting all curves l transversally. The induced action of G on Y_1 has two fixed points. Blowing up these and then taking the quotient, we get the configuration



Hence the proper transforms of the images of the two lines in $\mathbb{C}^2$ invariant under the group action meet the outer (-2)-curves transversally, the proper transforms of the image of any other line intersect the middle (-2)-curve transversally.

Consider finally the case $G = G(2,1,0) = \left\langle \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \right\rangle$, which is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$. The action of G_0 is as in the previous case. The induced action of G has $l_{\zeta_2=\zeta_1}$ and $l_{\zeta_2=-\zeta_1}$ as fixed point locus. Taking the quotient, we hence get a (-1)-curve which we blow down. $\mathbb{C}^2/G$ is smooth and the images of two lines in $\mathbb{C}^2$ either coincide or intersect transversally.

11.5 The action on $\mathbb{P}(W_z)$

Let again Γ be as in chapter 6, and let $\widetilde{\Gamma} \supseteq \Gamma$ be a discrete subgroup of $\mathrm{Aut}(\mathcal{H}\times\mathcal{H})$ as in section 11.3. Let $z = (z_1, z_2) \in \mathcal{H}\times\mathcal{H}$ be a special point which is also elliptic with respect to $\widetilde{\Gamma}$. We want to show how an action of $\widetilde{\Gamma}_z$ on $\mathbb{P}(W_z)$ can be used to determine how the curves F_β meet the exceptional divisor of the minimal resolution of the quotient singularity.

Now $\widetilde{\Gamma}_z$ acts naturally on the tangent space T_z of the point z in $\mathcal{H}\times\mathcal{H}$, and this action determines the structure of the corresponding singularity of the quotient surface $\mathcal{H}\times\mathcal{H}/\widetilde{\Gamma}$. Consider the induced action on the projective line $\mathbb{P}_{\mathbb{C}}(T_z)$:

$$\widetilde{\Gamma}_z \times \mathbb{P}_{\mathbb{C}}(T_z) \to \mathbb{P}_{\mathbb{C}}(T_z).$$

As we saw in section 11.4, how a curve F_β meets the exceptional divisor can in many cases be determined by finding out for which elements in $\widetilde{\Gamma}_z$ the tangent vector of F_β determines a fixed point in $\mathbb{P}_{\mathbb{C}}(T_z)$.

If $g \in \widetilde{\Gamma}_z$ and $\beta \in W_z \setminus \{0\}$, then we have that $gC_\beta = C_{\beta'}$ for some $\beta' \in W_z \setminus \{0\}$. More precisely, β' can be chosen as $\overline{\gamma}\beta\gamma^*$ if g is of the form $g(\zeta_1, \zeta_2) = (\gamma\zeta_1, \overline{\gamma}\zeta_2)$ for some $\gamma \in A^+$, and as $\overline{\gamma}\beta^*\gamma^*$ if g is of the form $g(\zeta_1, \zeta_2) = (\gamma\zeta_2, \overline{\gamma}\zeta_1)$ for some $\gamma \in A^+$. Since β' is well defined up to a non-zero rational factor, this gives a well defined action of $\widetilde{\Gamma}_z$ on the projective space $\mathbb{P}_{\mathbb{Q}}(W_z)$:

$$\widetilde{\Gamma}_z \times \mathbb{P}_{\mathbb{Q}}(W_z) \to \mathbb{P}_{\mathbb{Q}}(W_z). \tag{11.16}$$

We want to clarify the relationship between the two actions obtained. Consider therefore the group

$$\mathcal{G}_z = \{g \in \mathrm{Aut}(\mathcal{H}\times\mathcal{H}) \mid gz = z\},$$

and the 2-dimensional real vector space

$$\mathcal{W}_z = \{\beta \in M_2(\mathbb{R}) \mid \det(\beta) > 0 \text{ and } \beta z_1 = z_2\} \cup \{0\}.$$

For each non-zero element $\beta \in \mathcal{W}_z$, we consider the curve $C_\beta = \{(\zeta, \beta\zeta) \mid \zeta \in \mathcal{H}\} \ni z$. By letting $\mathcal{G}_z$ act on these curves, we get analogously a natural action of $\mathcal{G}_z$ on $\mathbb{P}_{\mathbb{R}}(\mathcal{W}_z)$ by $g[\beta] = [g_1\beta g_2^*]$, if g is of the form $g(\zeta_1, \zeta_2) = (g_1\zeta_1, g_2\zeta_2)$, and by $g[\beta] = [g_1\beta^* g_2^*]$, if g is of the form $g(\zeta_1, \zeta_2) = (g_1\zeta_2, g_2\zeta_1)$ for some $g_i \in \mathrm{SL}_2(\mathbb{R})$, $i = 1, 2$.

We have a map $W_z \to \mathcal{W}_z$ given by the representation ϱ_0. By the following lemma, we see that the image of the $\mathbb{Q}$-vector space W_z is dense in $\mathcal{W}_z$.

Lemma 11.11. *The map $W \otimes_{\mathbb{Q}} \mathbb{R} \to M_2(\mathbb{R})$, given by $w \otimes x \mapsto x\varrho_0(w)$, is an isomorphism.*

Proof. Recall that we have the isomorphism

$$\begin{aligned} f : A \otimes_{\mathbb{Q}} \mathbb{R} &\cong M_2(\mathbb{R}) \times M_2(\mathbb{R}) \\ a \otimes x &\mapsto (x\varrho_0(a), x\varrho_0(\overline{a})). \end{aligned}$$

We have $W = \{w \in A \mid \overline{w} = w^*\}$, and hence the image of $W \otimes_{\mathbb{Q}} \mathbb{R}$ under f is the diagonal $\{(X, X^*) \mid X \in M_2(\mathbb{R})\}$. This set projects surjectively onto the first factor of $M_2(\mathbb{R}) \times M_2(\mathbb{R})$. We are done. □

We have hence natural inclusions

$$\mathbb{P}_{\mathbb{Q}}(W_z) \hookrightarrow \mathbb{P}_{\mathbb{R}}(\mathcal{W}_z) \hookrightarrow \mathbb{P}_{\mathbb{C}}(T_z). \tag{11.17}$$

The first inclusion in (11.17) is given by ϱ_0, the second inclusion is given as follows: To each non-zero element $\beta \in \mathcal{W}_z$, we associate the line in T_z

generated by a tangent vector of the curve C_β at the point z. It is clear that the maps in (11.17) commute with the actions of $\widetilde{\Gamma}_z$.

We conclude that all the information we need to determine the intersection of the curves F_β with the exceptional divisors is available in the action (11.16).

12 An example

We will now consider the example where $k = \mathbb{Q}(\sqrt{13})$ and $d_0(\Lambda) = 3$. This is one of the cases with the smallest hyperbolic volume of the fundamental domain. Since $h(k) = 1$ in this case, there is only one maximal order in A up to isomorphism (by proposition 11.5 and lemma III.5.6 in [46]).

We will see in section 12.4, that we have a natural tower of discrete groups acting on $\mathcal{H}\times\mathcal{H}$

$$\Gamma \subset \Gamma_{\mathrm{I}} \subset \Gamma_{\mathrm{II}} \subset \Gamma_{\mathrm{III}}. \tag{12.1}$$

Each group extension in (12.1) is of index 2 and we have $\Gamma_{\mathrm{III}} = \widehat{\Gamma}$ in the notation of section 11.3. We will consider the 4 quotient surfaces X, $X_{\mathrm{I}} = \mathcal{H}\times\mathcal{H}/\Gamma_{\mathrm{I}}$, $X_{\mathrm{II}} = \mathcal{H}\times\mathcal{H}/\Gamma_{\mathrm{II}}$ and $X_{\mathrm{III}} = \mathcal{H}\times\mathcal{H}/\Gamma_{\mathrm{III}}$. We let Y, Y_{I}, Y_{II} and Y_{III} respectively denote the canonical minimal resolution of the corresponding quotient surface. The main result is:

Theorem 12.1. *Y is a minimal surface of general type, Y_I is a $K3$-surface blown up 4 times, Y_{II} is a special Enriques surface blown up 2 times and Y_{III} is a rational surface with Euler number $e = 12$.*

12.1 The order Λ and the lattice L

Consider the ternary form

$$f = x_1^2 + x_1x_2 + x_2^2 - 2x_3^2$$

over $\mathbb{Z}$. Using the notation of section 2.3, we write the even Clifford algebra of f as $\Lambda_{\mathbb{Z}} = \mathbb{Z} + E_1\mathbb{Z} + E_2\mathbb{Z} + E_3\mathbb{Z}$. The order $\Lambda_{\mathbb{Z}}$ is a maximal and has discriminant 6.

Denote by f_k the form f considered over k. Let $A = C_0(f_k)$. We have a natural embedding of $\Lambda_{\mathbb{Z}}$ in A. Since 2 is unramified and 3 is split in k, we get that the R-order $R\Lambda_{\mathbb{Z}}$ in A is contained in exactly two maximal orders. We choose Λ to be one of them, namely

$$\Lambda = R + RE_2 + RE_3 + R\frac{E_1 - rE_2}{2},$$

where $r = (1+\sqrt{13})/2$ (so $\Lambda \cap \overline{\Lambda} = R\Lambda_{\mathbb{Z}}$). Since Λ contains a unit with norm -1 (for example $1+E_2$), we only need to consider one action of Λ^1 (cf. section 6.3).

Since 2 is not ramified in k, we get that the lattice L is given by

$$L = \{\beta \in A \mid \overline{\beta}^* = \beta \text{ and } \overline{\Lambda}\beta \subseteq \Lambda\}. \tag{12.2}$$

We have the following $\mathbb{Z}$-basis $\beta_0, \ldots, \beta_3$ for L:

$$2,\ r - \sqrt{13}E_3,\ \sqrt{13}E_1,\ \sqrt{13}E_2. \tag{12.3}$$

The form q on L is given by $q(\beta) = 1/2\,\mathrm{nr}(\beta)$, and we get

$$q(t_0\beta_0 + \cdots + t_3\beta_3) = 2{t_0}^2 + t_0t_1 + 5{t_1}^2 - 13({t_2}^2 - t_2t_3 + {t_3}^2) \tag{12.4}$$

In a suitable basis, the dual form $q^{\#}$ is given by

$$q^{\#} = 2{s_0}^2 + s_0s_1 + 5{s_1}^2 - ({s_2}^2 - s_2s_3 + {s_3}^2)$$

The discriminants of q and $q^{\#}$ are $3^2 13^3$ and $3^2 13$ respectively.

We now summarise some facts about the curves F_N. By theorem 8.9, the number of components of F_N is

$$f_N = \begin{cases} 0 & \text{if } \left(\frac{N}{13}\right) = 1 \text{ or } 9 \mid N, \\ 2 & \text{if } 13^2 \mid N \text{ and } 9 \nmid N, \\ 1 & \text{otherwise.} \end{cases} \tag{12.5}$$

If β is a primitive element of L, then we have, by theorem 7.16, that $d_0(\Lambda_\beta)$ is the least common multiple of $q(\beta)$ and 3. Furthermore, by proposition 7.22, we have that the discriminant of the algebra A_β is given by

$$d_0(A_\beta) = 3d_{13}d_u,$$

where

$$d_{13} = \begin{cases} 13 & \text{if } \left(\frac{N_{13}}{13}\right) = 1, \text{ where } N_{13} = q(\beta)13^{-v_{13}(q(\beta))}, \\ 1 & \text{otherwise,} \end{cases}$$

and d_u is the product of those primes p which are unramified in k and such that $v_p(q(\beta))$ is odd. Finally, by proposition 8.8, we have

$$\kappa(N) = \begin{cases} 2 & \text{if } 13 \mid N, \\ 1 & \text{otherwise.} \end{cases}$$

Elliptic element	Order	Binary form	Discriminant	Branches
$\epsilon_1,\ \epsilon_2$	2	$[13,0,13]$	$-4\cdot 13^2$	$F_{13},\ F_{13}$
$\epsilon_3,\ \epsilon_4$	2	$[39,0,39]$	$-4\cdot 13^2\cdot 3^2$	$F_{39},\ F_{39}$
$\epsilon_5,\ \epsilon_6$	2	$[2,2,7]$	$-4\cdot 13$	F_2
$\epsilon_7,\ \epsilon_8$	2	$[6,6,21]$	$-4\cdot 13\cdot 3^2$	F_6
$\rho_1,\ \rho_2$	3	$[13,-13,13]$	$-3\cdot 13^2$	$F_{13},\ F_{39}$
ρ_3	3	$[2,1,5]$	$-3\cdot 13$	$F_2,\ F_6,\ F_5,\ F_{15}$
ρ_4	3	$[2,-1,5]$	$-3\cdot 13$	$F_2,\ F_6,\ F_5,\ F_{15}$

Table 2: Elliptic points

12.2 Elliptic points

There is a formula in [38] which gives the number of equivalence classes of elliptic points in $\mathcal{H}\times\mathcal{H}$ with respect to the group Γ. We will not use it though, but instead we will use corollary 9.9 and theorem 9.16. The point is that in this way, we will also get information about which binary forms that are associated to each of the elliptic points.

First we determine the elliptic points of order 2. The elliptic points of type I have binary forms $\varphi = [13,0,13]$ or $\varphi = [39,0,39]$, and we have $s(\varphi) = \alpha_{13}(\varphi)h'(-52)/\alpha_3(\varphi) = 2$. Since $w_\varphi = v_\zeta = 4$ in equation (9.1), we get 2 equivalence classes of points for each of these forms. Hence we have 4 points of type I. The elliptic points of type II has binary form $[2,-2,7]$ or $[6,-6,21]$. We get $s(\varphi) = 1$ for each of these forms, and since $w_\varphi = 2$ and $v_\zeta = 4$, we get a total of 4 points of type II.

The elliptic points of order 3 can be determined in the same way. We get 2 points of type I, with form $[13,-13,13]$, and 2 points of type II, one with form $[2,1,5]$ and one with form $[2,-1,5]$.

Table 2 shows, for each elliptic element, the binary form associated with the corresponding singular point. The last column in this table has one entry for each branch of the curves F_N, where $N \in \{2,6,5,15,13,39\}$, which passes through the quotient singularity on X. Observe that for the elliptic elements ρ_1 and ρ_2, the corresponding binary forms represent the values 13 and 39 six times each. But, as we will see in section 12.5, the corresponding three branches of curves in $\mathcal{H}\times\mathcal{H}$ are identified under the action of Γ, so we get just one branch of F_{13} and F_{39} respectively through each of the corresponding singularities. (We will see that these two singularities are of type $(3;1,2)$, so the isotropy groups of the corresponding points $z \in \mathcal{H}\times\mathcal{H}$ act non-trivially on the branches through the points.)

	39	13	15	5	6	2
2	$[2,0,39]$	–	$[2,\pm1,5]$	$[2,\pm1,5]$	$[2,\pm1,5]$	–
6	–	$[6,0,13]$	$[2,\pm1,5]$	$[2,\pm1,5]$	–	
5	$[5,0,39]$	$[5,-3,5]$	$[5,\pm2,8]$	$[5,-3,5]$		
	$[5,-5,11]$		$[2,\pm1,5]$			
15	$[15,-9,15]$	$[15,0,13]$	$[15,-9,15]$			
		$[7,-1,7]$				
13	$[13,0,39]$	$[13,-13,13]$				
	$[13,-13,13]$	$[13,0,13]$				
39	$[13,-13,13]$					
	$[39,0,39]$					

Table 3: Intersections

12.3 Modular curves

We need to study sufficiently many curves on Y to be able to draw conclusions about the surfaces that we consider. It turns out that the curves F_2, F_6, F_5, F_{15}, F_{13} and F_{39} will be interesting in this case. We know, by (12.5), that each one of these curves is irreducible.

Take $\beta \in L$. If $q(\beta) = 2$ or 6, then $\Gamma_\beta = \Lambda_\beta^1$, where Λ_β is a maximal order with discriminant $d_0(\Lambda_\beta) = 6$. By the results referred to in section 10.1, we get that C_β/Γ_β is a rational curve.

If $q(\beta) = 5$ or 15, then $\Gamma_\beta = \Lambda_\beta^1$, where Λ_β is a maximal order with discriminant $d_0(\Lambda_\beta) = 15$. We get that C_β/Γ_β is an elliptic curve.

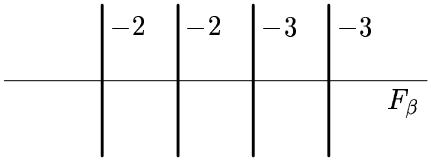
If $q(\beta) = 13$ or 39, then Λ_β is a maximal order with discriminant $d_0(\Lambda_\beta) = 39$ and $[\Gamma_\beta : \Lambda_\beta^1] = 2$. We know from (7.6), that the involution acting on C_β/Λ_β^1 is the involution induced by an element $n \in \Lambda_\beta$ with $\mathrm{nr}(n) = 13$. Hence, we have the situation described in the example in section 10.3, and we get that C_β/Γ_β is an elliptic curve.

Now we want to determine the intersection points of the curves F_N, including the case when a curve F_N is intersecting itself, i.e. it has a node. So, for all pairs $N_1, N_2 \in \{2,6,5,15,13,39\}$, we select from the finite list of definite binary forms which represent N_1 and N_2 (with non-trivially different representations if $N_1 = N_2$), those that are primitively representable by (L,q). Since we only need to check that a form satisfies the condition of lemma 9.5 for every prime p, this is straightforward to do. The result is shown in table 3. In table 4, we give the values of $s(\varphi)$ for the binary forms occurring in table 3 which do not correspond to elliptic points.

Binary form	Branches	Discriminant	$s(\varphi)$
$[2,0,39]$	$F_2,\ F_{39}$	$-8\cdot 3\cdot 13$	$h(-24)=2$
$[6,0,13]$	$F_6,\ F_{13}$	$-8\cdot 3\cdot 13$	$h(-24)=2$
$[5,-3,5]$	$F_5,\ F_5,\ F_{13}$	$-7\cdot 13$	$2h(-7)=2$
$[15,-9,15]$	$F_{15},\ F_{15},\ F_{39}$	$-3^2\cdot 7\cdot 13$	$2h(-7)=2$
$[5,2,8]$	$F_5,\ F_{15}$	$-4\cdot 3\cdot 13$	$h(-12)=1$
$[5,-2,8]$	$F_5,\ F_{15}$	$-4\cdot 3\cdot 13$	$h(-12)=1$
$[5,0,39]$	$F_5,\ F_{39}$	$-4\cdot 3\cdot 5\cdot 13$	$h(-60)=2$
$[15,0,13]$	$F_{15},\ F_{13}$	$-4\cdot 3\cdot 5\cdot 13$	$h(-60)=2$
$[5,-5,11]$	$F_5,\ F_{39}$	$-3\cdot 5\cdot 13$	$h(-15)=2$
$[7,-1,7]$	$F_{15},\ F_{13}$	$-3\cdot 5\cdot 13$	$h(-15)=2$
$[13,0,39]$	$F_{13},\ F_{39}$	$-4\cdot 3\cdot 13^2$	$h(-156)/2=2$

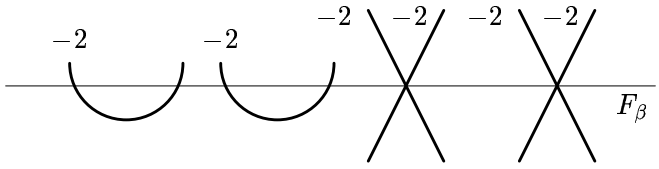
Table 4: Special points

We determine the self-intersections of the curves. Take an element $\beta\in L$. If $q(\beta)=2$ or 6, then we have the following situation on Y:



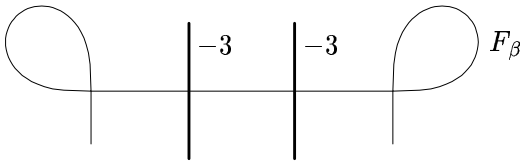
Since $\int_{C_\beta/\Gamma_\beta}\omega=-\frac{1}{3}$, we get by (11.7) that $c_1[F_\beta]=0$. Hence we get $F_\beta^2=-2$, since $g(F_\beta)=0$.

Assume now that $q(\beta)=13$ or 39. On Y we have:



Since $\int_{C_\beta/\Gamma_\beta}\omega=\frac{1}{2}\int_{C_\beta/\Lambda_\beta^1}\omega=-2$, we get $c_1[F_\beta]=-4$. Since $g(F_\beta)=1$, we get $F_\beta^2=-4$.

Assume finally that $q(\beta)=5$ or 15. We have the following configuration on Y:



Since $\int_{C_\beta/\Gamma_\beta}\omega = -\frac{4}{3}$, we get $c_1[F_\beta] = -2$. Blow up Y in the two points which are nodes of F_β. Let Z denote the resulting surface, let D_1 and D_2 be the two exceptional curves and p the map $p : Z \to Y$. We have $K_Z = p^*K_Y + D_1 + D_2$, and the proper transform $\widetilde{F}_\beta$ of F_β is $\widetilde{F}_\beta = p^*F_\beta - 2C_1 - 2C_2$. Hence $K_Z\widetilde{F}_\beta = K_YF_\beta - 2C_1^2 - 2D_2^2 = 6$. Since $\widetilde{F}_\beta$ is an elliptic curve, we get $\widetilde{F}_\beta^2 = -6$. From this follows directly that $F_\beta^2 = 2$.

12.4 The extended groups

In the present case, we have, by proposition 11.9, that Γ_3/Γ is a 2-group with 4 elements. It is given as follows. Let $v = 4 + \sqrt{13}$, so $3 = v\overline{v}$. There exists $\lambda_x \in \Lambda$ such that $\mathrm{nr}(\lambda_x) = x$ for $x = v$, $\overline{v}$ and 3, and we let $\gamma_x = \varrho(\lambda_x) : \mathcal{H}\times\mathcal{H} \to \mathcal{H}\times\mathcal{H}$. This gives three well defined involutions on X, which we denote ι_3, ι_v and $\iota_{\overline{v}}$.

Lemma 12.2. *If $\beta \in L$, then $13 \mid q(\beta)$ if and only if $\beta \in \sqrt{13}\Lambda$. Furthermore, if $q(\beta) = 13$, then we have*

$$\frac{1}{26}\beta L^*\beta = L. \tag{12.6}$$

Proof. The first statement is trivial to check using (12.3) and (12.4). Equation (12.6) can be checked by hand when β is, for example, $\sqrt{13}(r - E_1 - E_3)$. Let $\beta' \in L$ be another element with $q(\beta') = 13$. We have $\beta' = \pm\overline{\lambda}\beta\lambda^*$ for some $\lambda \in \Lambda^1$, since F_{13} only has one component. Hence, we get that $\frac{1}{26}\beta' L^*\beta' = L$. □

If $\omega \in A$ with $\mathrm{nr}(\omega) >> 0$, then we define a map $\Omega(\omega) : \mathcal{H}\times\mathcal{H} \to \mathcal{H}\times\mathcal{H}$, by

$$\Omega(\omega)(z_1, z_2) = (\omega z_2, \overline{\omega} z_1). \tag{12.7}$$

Let us now fix an element $\beta_{13} \in L$ with $q(\beta_{13}) = 13$, and define a map $T_{\mathcal{H}\times\mathcal{H}} : \mathcal{H}\times\mathcal{H} \to \mathcal{H}\times\mathcal{H}$, by

$$T_{\mathcal{H}\times\mathcal{H}} = \Omega(\beta_{13}^*).$$

From lemma 12.2, it follows that $\frac{1}{26}\beta_{13}(L^\#)^*\beta_{13} = L^\#$, which implies that $\beta_{13}^{-1}\overline{\Lambda}\beta_{13} = \Lambda$. Hence we get $T_{\mathcal{H}\times\mathcal{H}} \in \widehat{\Gamma}$, so $\widehat{\Gamma} = \Gamma_3 \cup T_{\mathcal{H}\times\mathcal{H}}\Gamma_3$. We also

have that $T^2_{\mathcal{H}\times\mathcal{H}}$ is the identity, and that $T_{\mathcal{H}\times\mathcal{H}}\Gamma T_{\mathcal{H}\times\mathcal{H}} = \Gamma$. Hence $T_{\mathcal{H}\times\mathcal{H}}$ determines an involution on X, which we denote T. We have

$$T\iota_x = \iota_{\overline{x}}T,$$

for $x \in \{1, v, \overline{v}, 3\}$.

For easier notation, we now define $\Gamma_{\mathrm{I}} = \Gamma \cup \gamma_3\Gamma$, $\Gamma_{\mathrm{II}} = \Gamma_{\mathrm{I}} \cup \gamma_v\Gamma_{\mathrm{I}}$ and $\Gamma_{\mathrm{III}} = \widehat{\Gamma}$. Thus we have a sequence of group extensions as claimed in (12.1). We let $G_{\mathrm{I}} = \{\iota_1, \iota_3\}$, $G_{\mathrm{II}} = \{\iota_1, \iota_v, \iota_{\overline{v}}, \iota_3\}$ and

$$G_{\mathrm{III}} = \{\iota_1, \iota_v, \iota_{\overline{v}}, \iota_3, T, T\iota_v, T\iota_{\overline{v}}, T\iota_3\}$$

denote the corresponding groups acting on X, so $G_{\mathrm{III}} \cong D_4$. We have that G_{I} is the center of G_{III}, so the filtration (12.1) is in some sense canonical.

Lemma 12.3. *If $\omega \in A^+$, then $\Omega(\omega) \in \Gamma_{III}$ if and only if $\omega\beta_{13} \in N(\Lambda)$.*

Proof. Follows immediately from the construction of Γ_{III}. □

The induced action of the elements of the group G_{III} on the set of curves F_N, is described by the following lemma:

Lemma 12.4. *For every positive integer N represented by q, we have that*

$$\iota_3(F_N) = F_N. \tag{12.8a}$$

and

$$T(F_N) = F_N. \tag{12.8b}$$

If $3 \nmid N$, then

$$\iota_x(F_N) = F_{3N} \text{ and } \iota_x(F_{3N}) = F_N, \tag{12.8c}$$

for $x = v$ and $x = \overline{v}$.

Proof. We show (12.8c) first. Let $x = v$ or $\overline{v}$, and take $\lambda_x \in \Lambda$ with $\mathrm{nr}(\lambda_x) = x$. Take a positive integer N such that $3 \nmid N$, and assume that $\beta \in L$ is a primitive element with $q(\beta) = N$. We have $\lambda_x C_\beta = C_{\beta'}$, where $\beta' = \overline{\lambda}_x\beta\lambda_x^*$. It is clear that $\beta' \in L_p$ primitively for every prime $p \neq 3$. Recall now that by proposition 7.14, we have that if $w \in W_3$, then $w \in L_3$ if and only if $q(w) \in \mathbb{Z}_3$. Since we have that $q(\beta') = 3q(\beta)$, (12.8c) follows.

As an immediate consequence of (12.8c), we get that $\iota_3(F_N) = F_N$ for all N, since $\iota_3 = \iota_v\iota_{\overline{v}}$.

Finally, we prove (12.8b). If $\beta \in L$, we get that $T_{\mathcal{H}\times\mathcal{H}}(C_\beta) = C_{\beta'}$, where $\beta' = \beta_{13}\beta^*\beta_{13}$. By lemma 12.2, we can define a function $g : L \to L$ by $g(\beta) = \frac{1}{26}\beta_{13}\beta^*\beta_{13}$. We have that g is an isometry of (L, q), and that $T_{\mathcal{H}\times\mathcal{H}}(C_\beta) = C_{g(\beta)}$ for every $\beta \in L$, so we are done. □

12.5 Points with non-trivial isotropy group

In this section, we want to find the points on $\mathcal{H}\times\mathcal{H}$ which have a non-trivial isotropy group in Γ_{III} and describe how the exceptional divisors of the corresponding singularities meet the modular curves.

We start by searching for the fixed points on X of the elements of G_{III}. First, we examine whether the involution ι_v has any fixed points. The point $z=(z_1,z_2)\in\mathcal{H}\times\mathcal{H}$ maps to a fixed point of ι_v on X if and only if there exists an element $\lambda\in\Lambda^1$ such that

$$(\lambda_v z_1, \overline{\lambda}_v z_2) = (\lambda z_1, \overline{\lambda} z_2).$$

Hence, we want to find $\lambda\in\Lambda^1$ such that $\mu=\lambda^*\lambda_v$ is elliptic, i.e.

$$tr(\mu)^2 - 4\,\mathrm{nr}(\mu) << 0. \tag{12.9}$$

Now we have $\mathrm{nr}(\mu)=v$, and it is straightforward to check that $tr(\mu)^2 << 4v$ if and only if $\mathrm{tr}(\mu)=0$. Hence, we get

$$\mu^2 = -v.$$

Consider now the field $K=k(\mu)$. We get that $\mu^2\equiv -(v+\overline{v}) = -8\equiv 1 \pmod{(\overline{v})}$. Hence K is split at the prime spot $(\overline{v})$, and therefore $K_{(\overline{v})}$ can not be embedded in the skew field $A_{(\overline{v})}$. This shows that no such element μ exists, and we conclude that the involution ι_v on X does not have any fixed points. The same conclusion holds for $\iota_{\overline{v}}$ too, by the same argument.

Now we want to determine the fixed points of ι_3. By the same reasoning as above, we want to find $\mu\in\Lambda$ with $\mathrm{nr}(\mu)=3$ and

$$\mathrm{tr}(\mu)^2 << 12.$$

From this, we get the possibilities $\mathrm{tr}(\mu)=0$ or $\mathrm{tr}(\mu)=\frac{\pm 1\pm\sqrt{13}}{2}$. In the latter cases, we again get a contradiction if we try to embed $k(\mu)$ into A. Hence, we get the only possibility

$$\mu^2 = -3.$$

Consider the quadratic order $S_1=\mathbb{Q}(\mu)\cap\Lambda$. Since $\mu\in S_1$, we have two cases, either $d(S_1)=-3$ or $d(S_1)=-12$. In the first case, we have $(\mu+1)/2\in\Lambda$, and hence z is an elliptic point of order 3 with respect to Γ. These are known from section 12.2. It remains to examine the case $d(S_1)=-12$, i.e. $S_1=\mathbb{Z}[\mu]$. We now proceed as in section 9.2. Let $S_2=\mathbb{Z}[\sqrt{13}\mu]$. By the same argument as in the proof of proposition 9.8, we get that $L_z S_i = L_z$ for $i=1$ or $i=2$. In the first case, we get $q_z\cong 13\varphi$, where $d_0(\varphi)=-12$, i.e. $q_z\cong[13,0,39]$. There are $s([13,0,39])=h(-156)/2=2$ such points. In the

second case, we get that q_z is a primitive form with discriminant -156, so we get $q_z \cong [5, \pm 2, 8]$. There is 1 point on X corresponding to each of these two forms.

We now search for fixed points of T on X. Let $w = \beta_{13}^*$ and take a point $z \in \mathcal{H} \times \mathcal{H}$. We have $T_{\mathcal{H}\times\mathcal{H}}(z) = \lambda z$ if and only if $wz_2 = \lambda z_1$ and $\overline{w}z_1 = \overline{\lambda} z_2$, which is equivalent to

$$\begin{cases} z_2 = w^*\lambda z_1 \\ z_1 = w\overline{\lambda}w^*\lambda z_1. \end{cases} \tag{12.10}$$

If (12.10) is satisfied, then we have two cases. Either we have $w\overline{\lambda}w^*\lambda \in k$, or $w\overline{\lambda}w^*\lambda$ is elliptic.

Assume first that $w\overline{\lambda}w^*\lambda \in k$. This is equivalent to the condition

$$w^*\lambda = x\overline{(w^*\lambda)}^*,$$

for some $x \in k$. Since $\mathrm{nr}(\lambda), \mathrm{nr}(w) \in \mathbb{Q}$, we get $x^2 = 1$. Consider first the case $x = 1$. This means that $w^*\lambda \in W$. Since $w^* \in L$, we get $\overline{\Lambda}w^*\lambda \in \Lambda\lambda = \Lambda$, so $w^*\lambda \in L$. Conversely, every point of $C_{w^*\lambda}$ is a fixed point of $\lambda^* T_{\mathcal{H}\times\mathcal{H}}$. Hence we get that F_{13} is point-wise fixed by T on X. Consider now the case $x = -1$. We want to show that this case is not possible. We would have $\frac{1}{\sqrt{13}}w^*\lambda \in W$ and, as above, $\frac{1}{\sqrt{13}}w^*\lambda \in L_p$ for every rational prime $p \neq 13$. Since furthermore $w \in \sqrt{13}\Lambda$, we would get $\overline{\Lambda}_{13}\frac{1}{\sqrt{13}}w^*\lambda = \Lambda_{13}\frac{1}{\sqrt{13}}w^*\lambda \subseteq \Lambda\lambda = \Lambda$, so $\frac{1}{\sqrt{13}}w^*\lambda \in L_{13}$ too. Hence $\frac{1}{\sqrt{13}}w^*\lambda \in L$, but this contradicts the fact that (L, q) does not represent 1.

We now consider the case that $w\overline{\lambda}w^*\lambda$ is elliptic. Let $\mu = w\overline{\lambda}w^{-1}\lambda$. Since $w\overline{\lambda}w^{-1} \in \Lambda$, we have $\mu \in \Lambda^1$. We get $\mu(z_1, z_2) = (z_1, z_2)$, and hence z is an elliptic point with respect to Γ.

In exactly the same way, we get that the fixed points of $\iota_3 T$ are given by F_{39}, and possibly additional isolated points which are elliptic with respect to Γ.

Consider now the maps $\iota_v T$ and $\iota_{\overline{v}} T$. Since $(\iota_v T)^2 = (\iota_{\overline{v}} T)^2 = \iota_3$, we have that the fixed points of these two maps form a subset of the fixed points of ι_3.

Now that we have located all points with non-trivial isotropy group in Γ_{III}, we want to describe them in more detail. Take $z = (z_1, z_2) \in \mathcal{H}\times\mathcal{H}$. If $\gamma \in \Gamma_{\mathrm{III},z}$ is non-trivial, but $\Gamma_{\mathrm{II},z}$ is trivial, then we know from the above that $z \in C_\beta$ for some $\beta \in L$ with $q(\beta) = 13$ or $q(\beta) = 39$, and that $\gamma z' = z'$ for every $z' \in C_\beta$. Hence we only need to study points z such that $\Gamma_{\mathrm{II},z}$ is non-trivial. We first note that, since ι_v and $\iota_{\overline{v}}$ lack fixed points on X, we have $\Gamma_{\mathrm{II},z} = \Gamma_{\mathrm{I},z}$ for every point $z \in \mathcal{H}\times\mathcal{H}$. Furthermore, we have:

Lemma 12.5. *If $|\Gamma_z| = 2$, then $|\Gamma_{II,z}| = 2$. If $|\Gamma_z| = 3$, then $|\Gamma_{II,z}| = 6$.*

Proof. Assume first that $|\Gamma_z| = 2$. We have $\Gamma_z = \langle \varrho(\epsilon) \rangle$ for some $\epsilon \in \Lambda$ with $\epsilon^2 = -1$. Consider the ring $S = R[\epsilon]$. We have that S is a maximal order in the biquadratic field $K = k(\epsilon)$, so $S = \Lambda \cap K$. To prove that $|\Gamma_{\mathrm{II},z}| = 2$, it is now sufficient to check that S does not contain any element x with $\mathrm{nr}_{K/k}(x) = 3$. Let $x = \alpha_1 + \alpha_2\epsilon$, where $\alpha_1, \alpha_2 \in R$. If $\mathrm{nr}_{K/k}(x) = 3$, then $\alpha_1^2 + \alpha_2^2 = 3$. In particular, we get $\alpha_1^2, \alpha_2^2 << 3$, which implies that $\alpha_1, \alpha_2 = 0, \pm 1$. Hence the equation $\mathrm{nr}_{K/k}(x) = 3$ does not have any solution x in S.

Assume now that $|\Gamma_z| = 3$, so we have $\Gamma_z = \langle \varrho(\rho) \rangle$ for some $\rho \in \Lambda^1$ with $\rho^2 + \rho + 1 = 0$. We get $\varrho(\rho - 1) \in \Gamma_{\mathrm{II},z}$ and $\varrho(\rho - 1)^2 = \varrho(\rho)$, since $(\rho - 1)^2 = -3\rho$. □

We now claim that the isotropy groups of all points with non-trivial isotropy group $\Gamma_{\mathrm{II},z}$ are as given in table 5. We already know which binary

	Γ_z	$\Gamma_{\mathrm{I},z}$	$\Gamma_{\mathrm{II},z}$	$\Gamma_{\mathrm{III},z}$
$[2,-2,7]$	$\mathbb{Z}/2$	$\mathbb{Z}/2$	$\mathbb{Z}/2$	$\mathbb{Z}/4$
$[2,-2,7]$	$\mathbb{Z}/2$			
$[6,-6,21]$	$\mathbb{Z}/2$	$\mathbb{Z}/2$		
$[6,-6,21]$	$\mathbb{Z}/2$			
$[13,0,13]$	$\mathbb{Z}/2$	$\mathbb{Z}/2$	$\mathbb{Z}/2$	$\mathbb{Z}/2 \times \mathbb{Z}/2$
$[13,0,13]$	$\mathbb{Z}/2$			
$[39,0,39]$	$\mathbb{Z}/2$	$\mathbb{Z}/2$		
$[39,0,39]$	$\mathbb{Z}/2$			
$[2,1,5]$	$\mathbb{Z}/3$	$\mathbb{Z}/6$	$\mathbb{Z}/6$	$\mathbb{Z}/12$
$[2,-1,5]$	$\mathbb{Z}/3$	$\mathbb{Z}/6$		
$[13,-13,13]$	$\mathbb{Z}/3$	$\mathbb{Z}/6$	$\mathbb{Z}/6$	D_6
$[13,-13,13]$	$\mathbb{Z}/3$	$\mathbb{Z}/6$		
$[13,0,39]$	(1)	$\mathbb{Z}/2$	$\mathbb{Z}/2$	$\mathbb{Z}/2 \times \mathbb{Z}/2$
$[13,0,39]$	(1)	$\mathbb{Z}/2$		
$[5,2,8]$	(1)	$\mathbb{Z}/2$	$\mathbb{Z}/2$	$\mathbb{Z}/4$
$[5,-2,8]$	(1)	$\mathbb{Z}/2$		

Table 5: Overview of points z with non-trivial isotropy group $\Gamma_{\mathrm{II},z}$

forms that can occur for such points z. All we have to do is to make some explicit calculations to verify the claim. When we do that, we will also investigate how the modular curves meet the exceptional divisors of the resolutions of the quotient singularities. We have 6 cases to consider:

Case 1: points with form $[2,-2,7]$ or $[6,-6,21]$. We have 2 equivalence

classes of points on $\mathcal{H}\times\mathcal{H}$ associated with each of these two forms. Consider the element

$$\epsilon = 1 + E_1 - 2E_3 \in \Lambda^1,$$

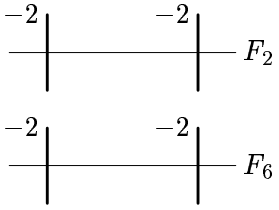
which satisfies $\epsilon^2 = -1$. Let z be the point such that $\epsilon z = z$. Since $\overline{\epsilon} = \epsilon$, we get $1 \in W_z$. Since also $\sqrt{13}\epsilon \in W_z$, it follows immediately

$$L_z = 2\mathbb{Z} + (\sqrt{13}\epsilon - 1)\mathbb{Z},$$

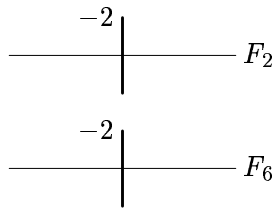
so we get that the corresponding quadratic form q_z is $[2, -2, 7]$. Consider now the element $g = \Omega(\epsilon - 1)$. We have $(\epsilon - 1)\beta_{13} \in 2\sqrt{13}\Lambda^1$, so $g \in \Gamma_{\mathrm{III}}$ by lemma 12.3. Furthermore, we have $g^2 = \varrho(\epsilon)$, since $(\epsilon - 1)\overline{(\epsilon - 1)} = -2\epsilon$. This shows that $\Gamma_{\mathrm{III},z}$ is a cyclic group of order 4 generated by g. Hence the action of $\Gamma_{\mathrm{III},z}$ is equivalent to $G(2,1,1)$, by lemma 11.10, and the singularity is of type $(4;1,3)$. The action of g on $\mathbb{P}(W_z)$ (see section 11.5) is induced by the linear map $W_z \to W_z$ given by

$$l \mapsto \overline{(\epsilon - 1)}l^*(\epsilon - 1)^*.$$

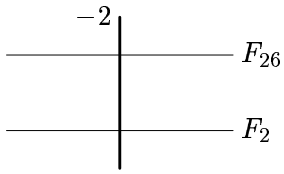
2 and $2\sqrt{13}\epsilon$ are two eigenvectors of this map. Therefore, the special curves meeting the exceptional divisor of the singularity are F_2 and F_{26}. We now summarise the situation. We have 4 equivalence classes, with respect to Γ, of points with form $[2, -2, 7]$ or $[6, -6, 21]$, and these are identified by Γ_{II}. Hence, on X we have 4 singularities of type $(2;1,1)$ corresponding to these forms, so on Y we have the following situation:



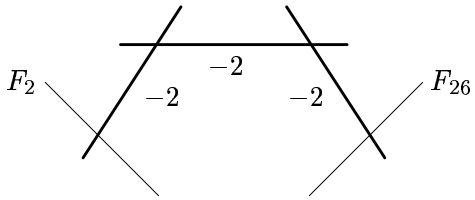
The involution ι_3 identifies the two points associated with $[2, -2, 7]$ and the two points associated with $[6, -6, 21]$ respectively, so on Y_{I} we have



The involution on Y_{I} identifies F_2 and F_6, so on Y_{II} the situation is



where we have also drawn the curve F_{26}. The involution on Y_{II} has now two isolated fixed points on this configuration, the intersection points of the (-2)-curve with F_2 and F_{26} respectively. Blowing up these and taking the quotient, we get



All other curves F_N meeting this exceptional divisor intersect the middle component of the three (-2)-curves.

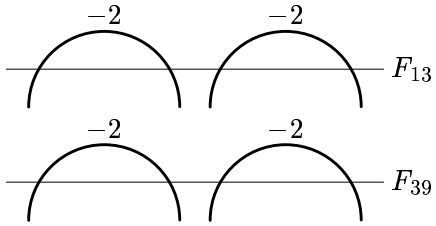
Case 2: points with form $[13,0,13]$ or $[39,0,39]$. There are two Γ-classes of points on $\mathcal{H}\times\mathcal{H}$ for each of these forms. Consider the element

$$\epsilon = -\frac{1+\sqrt{13}}{2} + \frac{3}{2}E_1 + \frac{9+\sqrt{13}}{4}E_2 + (1+\sqrt{13})E_3,$$

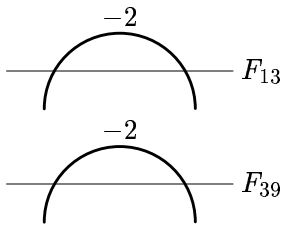
which satisfies $\epsilon^2 = -1$. It can be verified that $\beta_{13}\epsilon = -\overline{\epsilon}\beta_{13}$, i.e. $\epsilon \in \Gamma_{\beta_{13}}$, which implies that

$$L_z = \beta_{13}\mathbb{Z} + \beta_{13}\epsilon\mathbb{Z}.$$

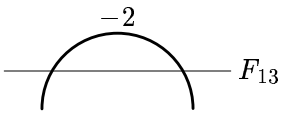
In particular, $q_z = [13,0,13]$. Furthermore, it is clear that $T_{\mathcal{H}\times\mathcal{H}} \in \Gamma_{\mathrm{III},z}$, so $\Gamma_{\mathrm{III},z} \cong \mathbb{Z}/2 \times \mathbb{Z}/2$. On Y, we have:



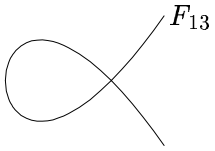
on Y_{I}:



and on Y_{II}:



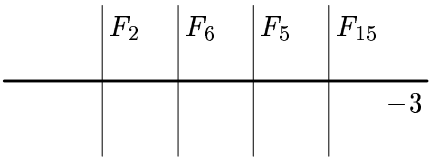
The involution T on Y_{II} fixes the points on F_{13}, so the (-2)-curve maps to a (-1)-curve on the quotient. If we blow down this curve, we get that F_{13} has a node on Y_{III}:



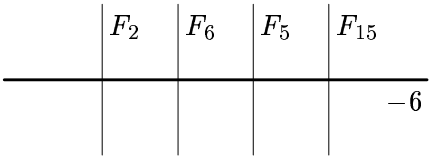
Case 3: points with form $[2,1,5]$ or $[2,-1,5]$. There is one Γ-class of points on $\mathcal{H}\times\mathcal{H}$ corresponding to each of these forms. If we let $\rho = -E_3$, then $\rho^2+\rho+1=0$. We have that $1 \in W_z$, since $\overline{\rho}=\rho$, and we also clearly have that $\sqrt{13}E_3 \in W_z$. We conclude that

$$L_z = \beta_1\mathbb{Z} + \beta_2\mathbb{Z},$$

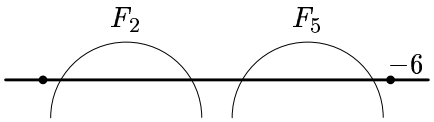
so $q_z \cong [2,\pm 1,5]$. By lemma 12.5, $\Gamma_{\mathrm{II},z}$ is a cyclic group of order 6 generated by $\varrho(\rho-1)$. Let now $\omega = 1+\frac{3-\sqrt{13}}{2}E_3$. We get that $\omega\beta_{13} = 2\sqrt{13}\lambda_0$, where $\lambda_0 \in \Lambda$ with $\mathrm{nr}(\lambda_0)=\overline{v}$, so $\Omega(\omega)\in\Gamma_{\mathrm{III}}$ by lemma 12.3. Furthermore, since $\omega\overline{\omega} = 2(1-\rho)$, we get that $\Gamma_{\mathrm{III},z}$ is a cyclic group of order 12 generated by $g=\Omega(\omega)$. Therefore the group action is equivalent to $G(6,1,1)$, and the quotient singularity is of type $(12;1,7)$. If we compute the action of g on $\mathbb{P}(W_z)$, we get that it can be given by a matrix $m = \left(\begin{smallmatrix}1 & -2\\ -1 & -1\end{smallmatrix}\right)$. This matrix lacks rational eigenvectors in W_z, so the action on $\mathbb{P}(W_z)$ is fixed point free. On Y, we have two configurations



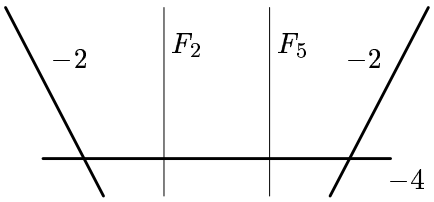
The involution ι_3 fixes the (-3)-curves, so on Y_{I}, we have two configurations



Now the involution on Y_{I} identifies F_2 with F_6 and F_5 with F_{15} respectively. On Y_{II}, we have one configuration



The involution T has two fixed points on the (-6)-curve. None of these points belong to any curve F_N. Blowing up these points, and then taking the quotient, we arrive at the following picture on Y_{III}:



Case 4: points with form $[13,-13,13]$. There are two Γ-classes of points on $\mathcal{H}\times\mathcal{H}$ having this form. Let

$$\rho = -3-\sqrt{13}+\frac{7+2\sqrt{13}}{2}E_1+\frac{13+5\sqrt{13}}{4}E_2+(5+2\sqrt{13})E_3,$$

which satisfies $\rho^2+\rho+1=0$. It can be verified that

$$\overline{\rho}\beta_{13}\rho = \beta_{13}, \tag{12.11}$$

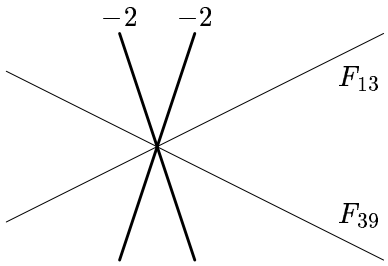
and therefore we get

$$L_z = \beta_{13}\mathbb{Z}+\beta_{13}\rho\mathbb{Z}.$$

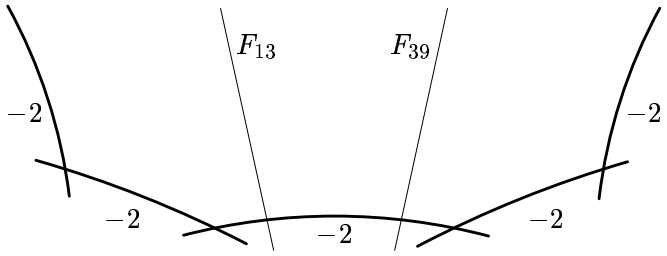
In particular, $q_z \cong [13,-13,13]$. Furthermore, $g=\varrho(1-\rho)\in\Gamma_{\mathrm{I}}$, so $\Gamma_{\mathrm{II},z}$ is a cyclic of order 6 generated by g. We also have $T_{\mathcal{H}\times\mathcal{H}}\in\Gamma_{\mathrm{III},z}$. By (12.11), we get $Tg=g^5T$. Hence we get that $\Gamma_{\mathrm{III},z}$ is isomorphic to the dihedral group D_6. The group action of $G_{\mathrm{III},z}$ is equivalent to $G(6,-1,0)$. The action of g^2 on $W_z=\beta_{13}\mathbb{Q}(\rho)$ is

$$\beta_{13}x \mapsto \overline{\rho}(\beta_{13}x)\rho^* = (\beta_{13}x)\rho,$$

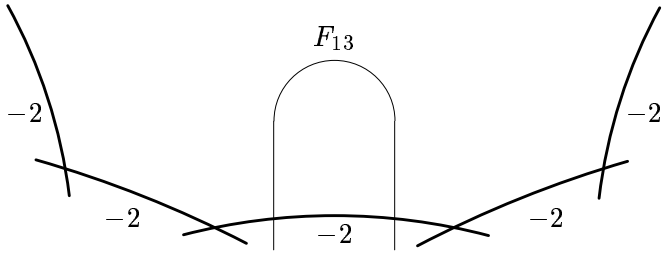
where $x\in\mathbb{Q}(\rho)$, by (12.11). This map clearly lacks eigenvectors. The action of T on the other hand, is given by $\beta_{13}x\mapsto\beta_{13}x^*$, so the eigenvectors are given by β_{13} and $\beta_{13}(2\rho-1)$. On Y, we have two configurations



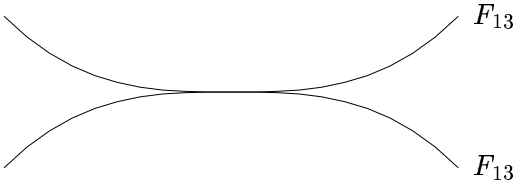
Blowing up the three fixed points of i_3 on each of these two configurations and taking the quotient, we get two copies of



on Y_{I}. On Y_{II}, we have one configuration like this



Finally, taking the quotient by the induced involution on Y_{II}, and blowing down the resulting exceptional curves, we get two branches of F_{13} meeting with order 3 on Y_{III}:



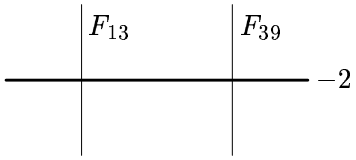
Case 5: points with form $[13, 0, 39]$. There are two Γ-classes of points on $\mathcal{H}\times\mathcal{H}$ for this form. If we let

$$\lambda = \sqrt{13} - 2 + \frac{1-\sqrt{13}}{4}E_1 + \frac{2\sqrt{13}-5}{2}E_2 + (4-2\sqrt{13})E_3,$$

then we have $\lambda \in \Lambda$, $\lambda^2 = -3$ and $\beta_{13}\lambda = -\overline{\lambda}\beta_{13}$, so

$$L_z = \beta_{13}\mathbb{Z} + \beta_{13}\lambda\mathbb{Z}.$$

$\Gamma_{\mathrm{II},z}$ has order 2, and is generated by $g = \varrho(\lambda)$. We clearly have $T_{\mathcal{H}\times\mathcal{H}} \in \Gamma_{\mathrm{III},z}$, so $\Gamma_{\mathrm{III},z} \cong \mathbb{Z}/2\times\mathbb{Z}/2$. On Y the we have just the two branches of F_{13} and F_{39} intersecting transversally at each of the two points. On Y_{I}, we have two configurations



On Y_{II} and on Y_{III}, the pictures are exactly the same as for the forms $[13, 0, 13]$ and $[39, 0, 39]$.

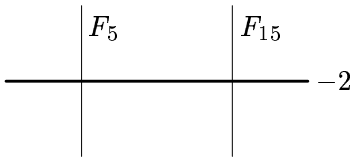
Case 6: points with form $[5, \pm 2, 8]$. There is one Γ-class of points on $\mathcal{H} \times \mathcal{H}$ for each of these two forms. Consider the element

$$\lambda = 2 - \sqrt{13} + \frac{11 - 3\sqrt{13}}{2} E_1 + (\sqrt{13} - 5) E_2 + (10 - 3\sqrt{13}) E_3.$$

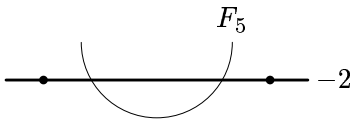
We have $\lambda \in \Lambda$ and $\mathrm{nr}(\lambda) = \overline{v}$. Let $\omega = \lambda \beta_{13}^*$, and $g = \Omega(\omega)$. Furthermore $\omega\overline{\omega} = 26\gamma$, where $\gamma \in \Lambda$ with $\gamma^2 = -3$. This implies that $\Gamma_{\mathrm{III},z}$ is cyclic of order 4 generated by g, and the singularity is of type $(4; 1, 3)$. It can be verified that $\gamma \in \Lambda_{\beta_2}$ and, in fact, we get

$$L_z = \beta_2 \mathbb{Z} + \beta_2 \frac{1 + \sqrt{13}\gamma}{5} \mathbb{Z}.$$

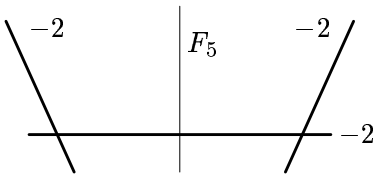
It can also be verified that the action of g on W_z can be given by the matrix $\left(\begin{smallmatrix} -1 & 2 \\ 1 & 1 \end{smallmatrix}\right)$. This matrix has no rational eigenvectors. On Y, we have just the two branches of F_5 and F_{15} intersecting transversally at each of the two points. On Y_{I} we have two configurations



On Y_{II}, we have one configuration

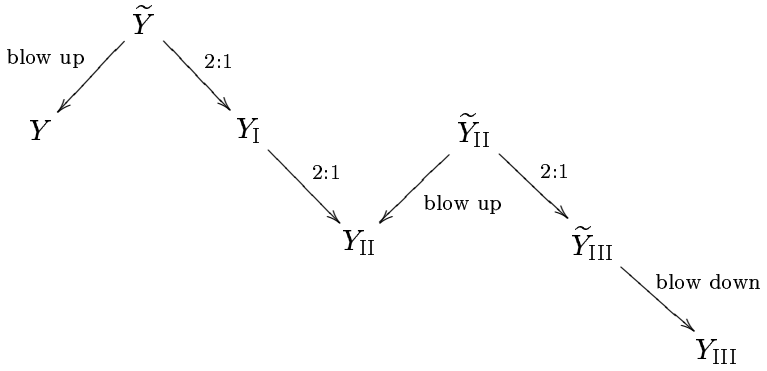


Finally, on Y_{III}, we have one configuration



12.6 Surfaces

We now have all the information necessary to present the configurations of curves on the different surfaces, we are studying. We start with the surface Y and proceed by a sequence of blow ups and quotient constructions. We will use the convention that whenever we have two surfaces Z and $\widetilde{Z}$, then $\widetilde{Z}$ is isomorphic to the surface Z blown up in a finite set of points. For easier navigation among the surfaces, we first summarise in a diagram the sequence of surfaces that we will construct:



(12.12)

We have drawn the configuration of curves on Y in figure 1. Here all curves drawn with thick lines are exceptional curves coming from the canonical resolution of the singularities of X. If the self-intersection number of such a curve is not explicitly given in the figure, then it is -2. Furthermore, the rational curves F_2 and F_6 have self-intersection -2 and the elliptic curves F_{13} and F_{39} have self-intersection -4. The nodal elliptic curves F_5 and F_{15} have self-intersection 2.

The involution ι_3 has 8 fixed points on X. On the surface Y, the fixed point locus of the lifted involution consists of the two (-3)-curves coming from the $(3;1,1)$ singularities and the 10 isolated points $x_1,\ldots,x_{10}$, which are indicated in figure 1. Blowing up these 10 points on Y to the surface $\widetilde{Y}$, and thereafter taking the quotient, we get a surface which, in fact, is the minimal desingularisation Y_{I} of X_{I}. We indicate the configuration of curves in figure 2. We have that $F_2^2 = F_6^2 = -1$, that F_{13} and F_{39} are non-singular rational curves with $F_{13}^2 = F_{39}^2 = -4$, and that F_5 and F_{15} are nodal rational curves with $F_5^2 = F_{15}^2 = 0$.

We let ι_{I} denote the involution on Y_{I} induced by the group Γ_{II}. It is fixed point free. If N is not divisible by 3, then ι_{I} maps F_N to F_{3N} and vice versa. We denote their common images in Y_{II} by F_N. We have of course that the self-intersection of F_2, F_{13} and F_5 respectively, are the same as for the corresponding curves on Y_{I}. The configuration on Y_{II} is drawn in figure 3.

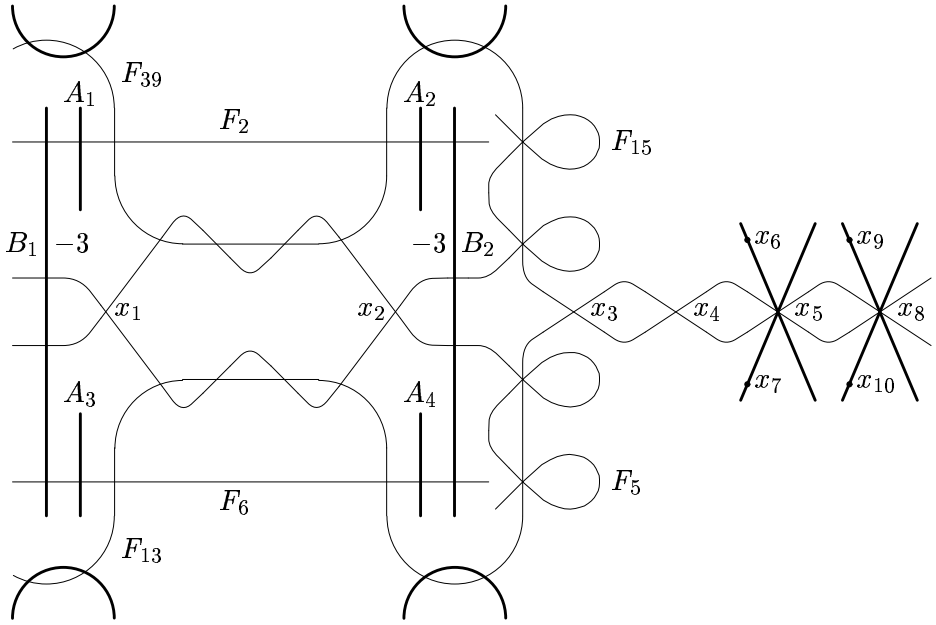


Figure 1: Y

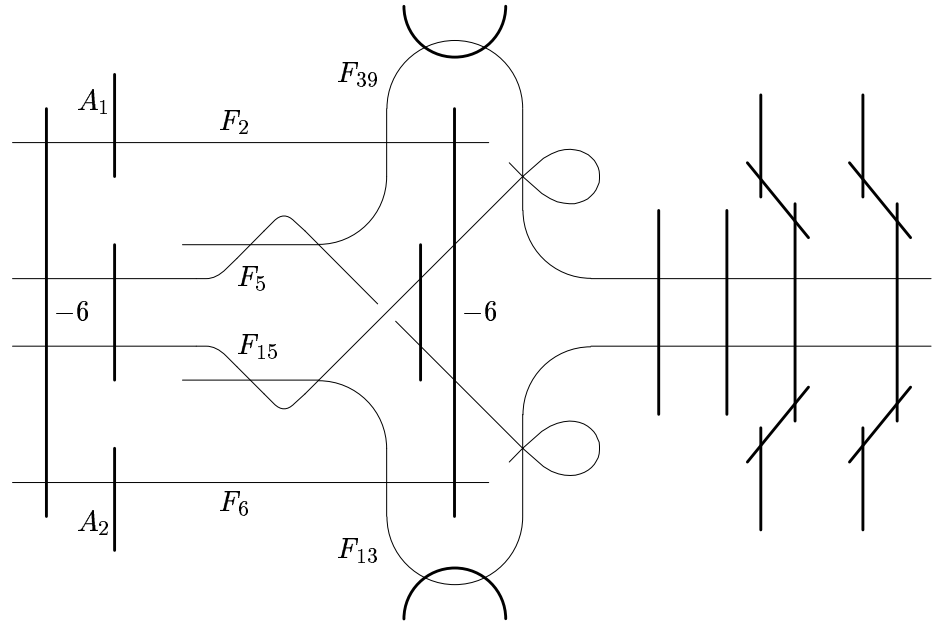


Figure 2: Y_{I}

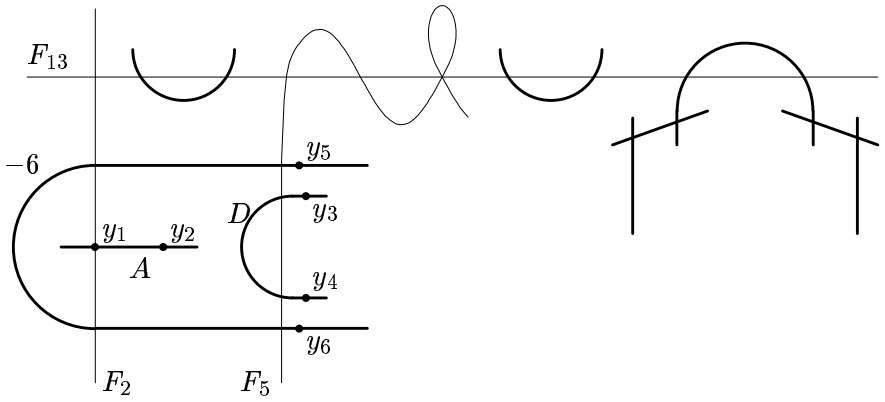


Figure 3: Y_{II}

The involution on Y_{II} induced by Γ_{III} has the curve F_{13} and the 6 isolated points $y_1, \ldots, y_6$ as fixed point locus. We blow up these points and then we take the quotient. The surface we get is Y_{III} blown up 5 times, see figure 4. On this surface, we have that F_2, F_{13} and F_5 are non-singular rational curves and we have $F_2^2 = -1$, $F_{13}^2 = -8$ and $F_5^2 = 0$.

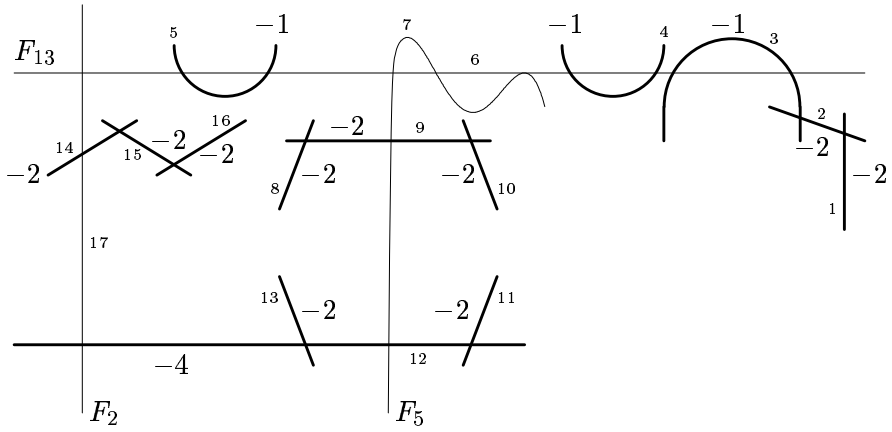


Figure 4: $\widetilde{Y}_{\mathrm{III}}$

We blow down the exceptional curve configurations which meet F_{13} and we get the surface Y_{III}. See figure 5, but disregard for now the curves C_{18} and C_{19}.

We determine the numerical invariants. Since $\zeta_k(-1) = \frac{1}{6}$, we get that $\int_X \omega = \frac{4}{3}$ by equation (11.4). Furthermore $e_2 = 8$ and $e_3 = 4$, so by (11.3), we get $e(X) = 8$. It is now straightforward, using lemma 11.1 and the additivity property of the Euler characteristic, to compute the numerical

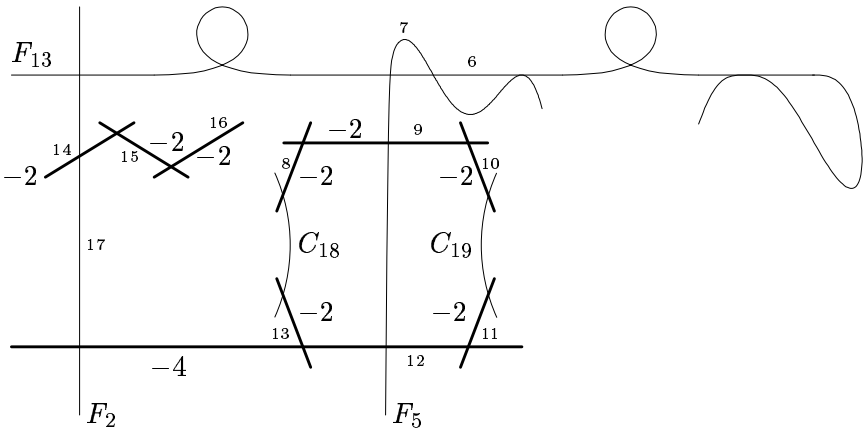


Figure 5: Y_{III}

	Y	Y_{I}	Y_{II}	Y_{III}
e	22	28	14	12
χ	2	2	1	1
K^2	2	-4	-2	0
q	0	0	0	0
p_g	1	1	0	0

Table 6: Numerical invariants of the surfaces

invariants of all surfaces. We summarise the result in table 6.

Proposition 12.6. *Y_{III} is a rational surface.*

Proof. If we blow down the configuration consisting of F_2, C_{14}, C_{15} and C_{16}, then the image of C_{12} is a non-singular rational curve with $C_{12}^2 = 0$. Hence, by proposition 11.2, we get that Y_{III} is a rational surface. □

Now we want to compute the canonical divisors of the surfaces. We consider first $\widetilde{Y}_{\mathrm{III}}$. This is a rational surface, so linear and numerical equivalence of divisors coincide. Furthermore the Euler number of $\widetilde{Y}_{\mathrm{III}}$ is 17, and hence the rank of the unimodular lattice $\mathrm{Pic}(\widetilde{Y}_{\mathrm{III}})$ is 15. Consider now the sublattice of $\mathrm{Pic}(\widetilde{Y}_{\mathrm{III}})$ generated by the 17 curves C_i, where we have indicated the

numbering in figure 4. The intersection matrix (C_iC_j) is given by

$$\begin{pmatrix}
-2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & -1 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & -1 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 2 & 2 & 2 & -8 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & -4 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -2 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -2 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -2 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & -1
\end{pmatrix} \tag{12.13}$$

The rank of this matrix is 15, and hence the curves C_i generate a sublattice of $\mathrm{Pic}(\widetilde{Y}_{\mathrm{III}})$ of full rank. We can compute the relations among the curves, and doing that we see that we can, for example, eliminate C_{13} and C_{16}. Computing the determinant of the resulting intersection matrix, we get the value 4. We conclude that index of the sublattice in $\mathrm{Pic}(\widetilde{Y}_{\mathrm{III}})$ generated by the curves C_i is 2.

We now know that the canonical divisor of $\widetilde{Y}_{\mathrm{III}}$ is a linear combination of the curves C_i (with rational coefficients). Since all curves C_i are rational, we have, by the adjunction formula, that

$$(K + C_i)C_i = -2$$

for $i = 1, \ldots, 17$. Solving this system of linear equations, we get for instance the following representation of $2K$ on $\widetilde{Y}_{\mathrm{III}}$:

$$2K = 4F_2 - F_{13} + 3C_{14} + 2C_{15} + C_{16}. \tag{12.14}$$

Using (12.14), we can trace $2K$ backwards and get the following relation on Y_{II}:

$$2K = 4F_2 + 2A. \tag{12.15}$$

Let now Z denote the surface we get if we blow down first F_2 and then A on Y_{II}. By (12.15), we have that $2K = 0$ on Z. Furthermore, $e(Z) = 12$ and $q(Z) = 0$. This shows that Z is an Enriques surface (see [1], chapter VI). We have shown:

Proposition 12.7. *Y_{II} is an Enriques surface blown up 2 times.*

Since the map $Y_{\mathrm{I}} \to Y_{\mathrm{II}}$ is unramified, we immediately get the following corollary:

Proposition 12.8. *Y_I is a $K3$-surface blown up 4 times with $K = 2F_2 + A_1 + 2F_6 + A_2$.*

The presentation of K in proposition 12.8, now implies that the canonical divisor on Y is given by

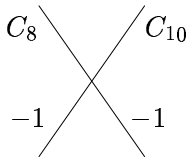
$$K = 2F_2 + 2F_6 + \sum A_i + \sum B_i.$$

We conclude that Y is a minimal surface (since if E an exceptional divisor on Y, then $KE = -1$, which is impossible since K is effective and does not contain any exceptional component). Furthermore, since K is effective and $K^2 > 0$, we have that Y is of general type (see [1]).

Proposition 12.9. *Y is a minimal surface of general type.*

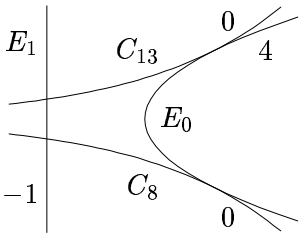
Lemma 12.10. *On Y_{III} there exist two rational (-1)-curves C_{18} and C_{19}, which meet the curves C_8, C_{10}, C_{11} and C_{13} as indicated in figure 5 (where we have possibly swapped the numbers of the curves C_8 and C_{10}). We also have $C_{18}F_{13} = C_{19}F_{13} = 2$ (which is not indicated in the figure), but neither C_{18} nor C_{19} intersect any of the other curves in the figure.*

Proof. We will construct C_{18}, the construction of C_{19} is analogous. Blow up the intersection point of F_5 and C_{12}. Let E_0 denote the exceptional curve. Blow down, in the following order, the curves F_2, C_{14}, C_{15}, C_{16}, C_{12}, C_{11}, F_5, and C_9. We now have a rational surface with Euler characteristic $e = 5$ and which contains the following configuration:



It is clear that if we blow down one of these two curves, we get the surface $\mathbb{P}^1 \times \mathbb{P}^1$, and if we blow down the other curve, we get $\mathbb{P}^2$ blown up in one point. We can suppose, after possibly swapping the numbers of these two curves, that we get the latter situation of we blow down C_{10}.

It is now straightforward to check (using (12.13)) that the curves E_0, C_8 and C_{13} are configured as in the following picture:



(12.16)

This gives that the unique exceptional curve on the surface, which we denote by E_1, must necessarily be situated as indicated in (12.16). Furthermore, we get by (12.13) that $F_{13}E_0 = 20$ and $F_{13}C_{13} = 8$. Since $E_0 = 2(C_{13} + E_1)$, this gives that $F_{13}E_1 = 2$.

Let now C_{18} be the proper transform of E_1 in Y_{III}. Since C_{18} is disjoint with the locus of the curves being blown down, it is clear that C_{18} is a (-1)-curve and $F_{13}C_{18} = 2$. We are done. □

We can now blow down Y_{III} in the following way: F_2, C_{14}, C_{15}, C_{16} and C_{18}, C_8 and C_{19}, C_{10}. The surface we get is isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$, and the image of F_{13} is a divisor of bi-degree $(4,4)$. We get that Y_{II} is birational to the double cover over $\mathbb{P}^1 \times \mathbb{P}^1$ ramified in F_{13}, C_{13} and C_{11}, i.e. a divisor of bi-degree $(4,6)$. The two projections of $\mathbb{P}^1 \times \mathbb{P}^1$ on its two factors induce two pencils of curves on Y_{II}: one elliptic fibration and a pencil of genus 2 curves.

It would of course be interesting to further study this elliptic fibration. In particular, it would be interesting to determine the type of the two double fibers. But to do so requires more detailed knowledge about how the curves C_{18} and C_{19} meet F_{13} on Y_{III}. We know that the intersection numbers $C_{18}F_{13}$ and $C_{19}F_{13}$ equal 2, and we know the singularities of F_{13}, but this leaves us with 4 possible ways in which C_{18} may meet F_{13}, and similarly for C_{19}. Unfortunately we have not been able to settle this question.

There is however one more thing that we can say about Y_{II}. Recall that an Enriques surface is called special if it has an elliptic pencil with a 2-section which is a (-2)-curve (see [1], p. 275). The curve F_5 on Y_{II} is a fiber of the elliptic fibration, so we get that the (-2)-curve D on Y_{II} is a 2-section. Hence we get

Proposition 12.11. *Y_{II} is a special Enriques surface.*

This completes the proof of theorem 12.1.

List of symbols

References

[1] W. Barth, C. Peters, A. Van de Ven, *Compact Complex Surfaces,* Springer-Verlag, 1984

[2] Z.I. Borevich, I.R. Shafarevich, *Number theory,* Academic Press, 1968

[3] J. Brzezinski, *On orders in quaternion algebras,* Communications in algebra, 11(5), 501–522 (1983)

[4] J. Brzezinski, *A characterisation of Gorenstein orders in quaternion algebras,* Math. Scand. 50, 19–24 (1982)

[5] J. Brzezinski, *On automorphisms of quaternion orders,* J. Reine Angew. Math. 403, 166–186 (1990)

[6] J. Brzezinski, *On embedding numbers into quaternion orders,* Comment. Math. Helvetici 66, 302–318 (1991)

[7] J. W. S. Cassels, *Rational Quadratic Forms,* Academic Press, 1978

[8] D. A. Cox, W. R. Parry, *Genera of congruence subgroups in $\mathbb{Q}$-quaternion algebras,* J. Reine Angew. Math. 351, 66–112 (1984)

[9] C. W. Curtis, I. Reiner, *Methods of representation theory, vol. I,* Wiley, 1981

[10] C. W. Curtis, I. Reiner, *Methods of representation theory, vol. II,* Wiley, 1987

[11] P. Deligne, *Travaux de Shimura,* Séminaire Bourbaki, 1970/71, exp 389, Lecture Notes in Math. 244, p. 275–288 Springer-Verlag, 1971

[12] M. Eichler, *Untersuchungen in der Zahlentheorie der rationalen Quaternionenalgebren,* J. Reine Angew. Math. 174, 129–159 (1936)

[13] M. Eichler, *Zur Zahlentheorie der Quaternionen-Algebren,* J. Reine Angew. Math. 195, 127–151 (1955)

[14] H. Franke, *Kurven in Hilbertsche Modulflächen und Humbertsche Flächen im Siegel-Raum,* Bonner Mathematishe Schriften, 1978

[15] E. Freitag, *Über die Struktur der Funktionenkörper zu hyperabelschen Gruppen. I,* J. Reine Angew. Math. 247, 13–117 (1971)

[16] A. Fröhlich, M. J. Taylor, *Algebraic number theory,* Cambridge University Press, 1991

[17] G. van der Geer, *Hilbert Modular Surfaces,* Springer-Verlag, 1988

[18] G. van der Geer, D. Zagier, *The Hilbert Modular Group for the Field* $\mathbb{Q}(\sqrt{13})$*,* Inventiones math. 42, 93–133 (1977)

[19] W. F. Hammond, *The two actions of Hilbert's modular group,* Amer. J. Math. 99, 389–392 (1977)

[20] W. Hausmann, *Kurven auf Hilbertsche Modulflächen,* Bonner Mathematishe Schriften, 1980

[21] F. Hirzebruch, *Hilbert modular surfaces,* L'Ens. Math. 19, 183–281 (1973)

[22] F. Hirzebruch, D. Zagier, *Intersection Numbers of Curves on Hilbert Modular Surfaces and Modular Forms of Nebentypus,* Inventiones math. 23, 1–29 (1974)

[23] F. Hirzebruch, D. Zagier, *Classification of Hilbert modular surfaces,* Complex analysis and algebraic geometry, p. 43–77. Iwanami Shoten, Tokyo, 1977

[24] F. Hirzebruch, *The Hilbert modular group, resolution of the singularities at the cusps and related problems,* Séminaire Bourbaki, 1970/71, exp 396, Lecture Notes in Math. 244, p. 275–288 Springer-Verlag, 1971

[25] R. Jacobowitz, *Hermitian Forms over Local Fields,* Amer. J. Math. 84, p. 441–465 (1962)

[26] I. Kersten, *Brauergruppen von Körpern,* Friedr. Vieweg & Sohn, 1990

[27] M. Kneser, *Composition of Binary Quadratic Forms,* Journal of Number Theory 15, p. 406–413 (1982)

[28] M.-A. Knus, *Quadratic and hermitian forms over rings,* Springer-Verlag, 1991

[29] K. Kodaira, *On Kähler varieties of restricted type,* Annals of Mathematics, vol. 60 p. 28–48 (1954)

[30] T. Miyake, *Modular Forms,* Springer-Verlag, 1989

[31] O. T. O'Meara, *Introduction to Quadratic Forms,* Springer-Verlag, 1973

[32] M. Peters, *Ternäre und quaternäre quadratische Formen und Quaternionenalgebren,* Acta Arithmetica 15, p. 329–365 (1969)

[33] A. Prestel, *Die elliptischen Fixpunkte der Hilbertschen Modulgruppen,* Math. Ann. 177 (1968)

[34] P. Ponomarev, *Arithmetic of quaternary quadratic forms,* Acta Arithmetica 29, p. 1–48 (1976)

[35] I. Reiner, *Maximal Orders,* Academic Press, 1975

[36] K. W. Roggenkamp, V. Huber-Dyson, *Lattices over Orders I,* Springer-Verlag, 1970

[37] I. Shavel, *A class of algebraic surfaces of general type constructed from quaternion algebras,* Pacific Journal of Mathematics, vol. 76, No. 1, p. 221–245 (1975)

[38] V. Schneider, *Die elliptischen Fixpunkte zu Modulgruppen in Quaternionenschiefkörpern,* Math. Ann. 217 (1975)

[39] W. Scharlau, *Quadratic and Hermitian Forms,* Springer-Verlag, 1985

[40] J.-P. Serre, *A Course in Arithmetic,* Springer-Verlag, 1973

[41] G. Shimura, *Arithmetic of Unitary Groups,* Annals of Mathematics, vol. 79 p. 369–409 (1964)

[42] G. Shimura, *On Dirichlet Series and Abelian Varieties Attached to Automorphic Forms,* Annals of Mathematics, vol. 76 p. 237–294 (1962)

[43] G. Shimura, *Euler Products and Eisenstein Series,* American Mathematical Society, 1997

[44] G. Shimura, *Introduction to the arithmetic theory of automorphic functions,* Iwanami Shoten, Publishers and Princeton University Press, 1971

[45] K. Takeuchi, *Algebraic surfaces derived from unit groups of quaternion algebras,* in *Number theory (Banff, AB, 1988),* p. 529–552, de Gruyter, Berlin, 1990

[46] M.-F. Vignéras, *Arithmétique des Algèbres de Quaternions,* Springer-Verlag, 1980

[47] M.-F. Vignéras, *Invariants numériques des groupes de Hilbert,* Math. Ann. 224, 189–215 (1976)

[48] D. B. Zagier, *Zetafunktionen und quadratische Körper,* Springer-Verlag, 1981