UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Centre de Formació Interdisciplinària Superior

McGill
UNIVERSITY

Bachelor's Thesis

Hilbert Modular Forms and the Theory of Complex Multiplication

Jordi Guillem Rodríguez Manso

McGill Advisor:
Prof. Henri Darmon

UPC tutor:
Víctor Rotger Cerdà

May 2022

In partial fullfilment of the requirements for the
Bachelor's degree in Mathematics
Bachelor's degree in Data Science and Engineering

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Escola Tècnica Superior d'Enginyeria
de Telecomunicació de Barcelona

telecos
BCN

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat d'Informàtica de Barcelona

FIB

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat de Matemàtiques i Estadística

Acknowledgements

The completion of this thesis would not have been possible without the support and assistance of several people.

First, I would like to thank Fundació Privada Cellex and CFIS for their funding that allowed me to complete this thesis abroad. I would have never had such an opportunity without them.

I would like to thank my supervisors, Professor Henri Darmon, from McGill University, for introducing me to the beautiful world of modular forms and complex multiplication and guiding me in the development of this thesis and Victor Rotger, from UPC, for willing to help at any time.

I would also like to express my gratitude to some of Professor Darmon's PhD students for sharing their knowledge with me and answering my questions and solving my doubts, with a especial mention to Marti Roset, who has spent an inestimable amount of time helping me.

I would also like to acknowledge my room mate, university colleague and friend Jordi Vilà for the time we shared this year and the many stimulating discussions we had about our projects.

Finally, I would also like to thank my family and friends for their unconditional support. You are always there to listen to me and advice me in the tough times and keep me motivated every day. I would like to make an special mention to the wonderful people I have met in Montreal this year.

Abstract

In this thesis we present the main properties of Hilbert modular surfaces and their associated modular forms. The most remarkable one is that they can be viewed as modular varieties associated to the orthogonal group of a quadratic space of type $(2,2)$. This property provides a source of modular forms, which we will study, with a special focus on the so-called Borcherds lift and the Doi-Naganuma lift. Once the foundations of Hilbert modular surfaces and modular forms are established, we introduce the theory of Complex Multiplication, starting with some basic facts for elliptic curves that will serve as an introduction to the Theory of Complex Multiplication for Hilbert modular surfaces. We will show how to obtain the so-called CM points on the Hilbert Modular surface and how to evaluate Borcherds lifts on them. We will also see that those values are nice algebraic numbers in some concrete fields and that when we evaluate our modular function on a full CM cycle we get rational numbers with several prime factors. We provide several examples of those numerical computations on SageMath to support the theoretical results.

Resum

En aquesta tesi presentem les propietats principals de les superfícies modulars de Hilbert i les formes modulars associades. La més remarcable és que poden ser vistes com a varietats modulars associades al grup ortogonal d'un espai quadràtic de tipus $(2,2)$. Aquesta propietat dona una font de formes modulars, que estudiarem, posant un especial èmfasi al Borcherds lift i el Doi-Naganuma lift. Una vegada els fonaments per les superfícies modulars de Hilbert hagin estat establerts, introduirem la teoria de la Multiplicació Complexa, començant per alguns fets bàsics en el cas de corbes el·líptiques que servirà com a introducció per al cas de Multiplicació Complexa per a superfícies modulars de Hilbert. Mostrarem com obtenir els anomenats punts CM a la superfície modular de Hilbert i com avaluar el Borcherds lift en aquests punts. També veurem que aquests valors són nombres algebraics que pertanyen a cossos concrets i que quan avaluem una funció modular en tot un cicle CM obtenim nombres racionals amb múltiples factors primers. Donem diversos exemples de càlculs numèrics fets amb SageMath per confirmar els resultats teòrics.

Resumen

En esta tesis presentamos las propiedades principales de las superficies modulares de Hilbert y las formas modulares asociadas. La más remarcable es que pueden ser vistas como variedades modulares asociadas al grupo ortogonal de un espacio cuadrático de tipo $(2,2)$. Esta propiedad nos da una fuente de formas modulares, que estudiaremos, poniendo especial énfasis en el Borcherds lift y el Doi-Naganuma lift. Una vez hayamos establecido los fundamentos de las superficies modulares de Hilbert, introduciremos la teoría de la Multiplicación Compleja, empezando por algunos hechos básicos en el caso de curvas elípticas que nos servirá como introducción para el caso de Multiplicación Compleja para superficies modulares de Hilbert. Mostraremos cómo obtener los llamados puntos CM en la superficie modular de Hilbert y cómo evaluar el Borcherds lift en esos puntos. También veremos que esos valores son números algebraicos pertenecientes a unos cuerpos concretos y que cuando evaluamos una función modular en todo el ciclo CM obtenemos números racionales con muchos factores primos. Damos varios ejemplos de los cálculos numéricos realizados con SageMath para respaldar los resultados teóricos.

Keywords

modular forms, complex multiplication, real quadratic fields, orthogonal groups, ideal class group, algebraic number theory

Paraules clau

formes modulars, multiplicació complexa, cossos quadràtics reals, grups ortogonals, grup de classes d'ideals, teoria algebraica de nombres

Palabras clave

formas modulares, multiplicación compleja, cuerpos cuadráticos reales, grupos ortogonales, grupo de clases de ideales, teoría algebraica de números

MSC2020: 11G15, 11F41

Contents

Chapter 0

Introduction

The Kronecker-Weber theorem states that every abelian extension of $\mathbb{Q}$ is contained in some cyclotomic field (a field of the form $\mathbb{Q}(e^{2\pi in})$ for some integer n). At the beginning of the 20th century Hilbert published his famous list of 23 unsolved problems that guided the research of many mathematicians during the 20th century. The 12th of these problems asks for a generalization of the Kronecker-Weber theorem for number fields other than $\mathbb{Q}$. More explicitly, it asks to find and analogue of the exponential function $z \mapsto e^{2\pi iz}$ such that when we adjoint its values to a number field K, we obtain an abelian extension of K.

The Theory of Complex Multiplication of elliptic curves gives a complete answer for this problem when K is an imaginary quadratic extension of $\mathbb{Q}$ (i.e. $K = \mathbb{Q}(\sqrt{d})$ for some rational $d < 0$). This theory shows that values of the j-invariant (a modular function whose Fourier expansion is $j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + \ldots$ for $q = e^{2\pi i\tau}$) at the CM points together with some values of the Weber function generate all abelian extensions of K. Furthermore, it shows that $K(j(\tau))$ is the Hilbert Class field of K, the maximal unramified abelian extension of K. Shimura and Taniyama developed the theory of complex multiplication for higher dimensional abelian varieties and they managed to give a partial answer for the cases where K is a CM field (a degree 2 imaginary extension of a totally real field). Although many things change from the case of elliptic curves (for instance we can't generate all class fields just using Complex Multiplication, we have to consider principally polarized abelian varities, a new field called the reflex field appears...) there is one thing that is really similar. When we evaluate the j-function on a certain set of points and multiply the results we get nice integers with many prime factors. A similar thing happens with Hilbert modular functions when we evaluate them on all the points of a certain set which is known as a CM cycle, with the difference that this time the results are rationals and not necessarily integers. In this thesis we won't focus on the part of generating class fields using the theory of Complex Multiplication. We will rather work on the problem of obtaining all points on a CM cycle to evaluate Hilbert Modular functions at them and get those nice rational numbers (and also evaluating Hilbert modular functions at single CM points to get certain algebraic numbers, although this time they will not generate the Hilbert Class field like in the elliptic curves case).

In the first chapter we study some basic properties of Hilbert Modular forms and Hilbert modular surfaces. Hilbert modular forms are a generalization of elliptic modular forms. They were first developed by Hilbert and his student Blumenthal in the beginning of the 20th century. After their initial work it took several years to continue their study because both algebraic geometry and the theory of complex functions needed more study. Those modular forms are similar in many ways to classical elliptic modular forms (they transform similarly, they also have a Fourier expansion) but the fact that they are functions in several variables adds an extra complexity. Unlike in the case of elliptic modular forms, the space of Hilbert modular forms is much more complex and so it is more difficult to determine its dimension. It is also much harder to find a fundamental domain for the action of the Hilbert modular group.

A really nice property about Hilbert Modular surfaces is that they can be viewed as modular varieties for orthogonal groups of certain quadratic spaces. For this reason in the second chapter we study quadratic spaces, the Clifford algebra and several realizations of the hermitian symmetric domain associated to the orthogonal group of a quadratic space. This tools will allow us to see why Hilbert Modular Surfaces can also be seen as modular varieties of orthogonal groups and how we can use this to lift Hilbert Modular forms from modular forms for orthogonal groups.

In the third chapter we describe two lifts that provide a source of modular forms: the Doi-Naganuma lift and the Borcherds Lift. We will see that sometimes they give the same modular forms, and at the end of this chapter we use this to show how one can evaluate Borcherds lifts at points of $\mathbb{H}^2$ in those particular cases (the code used can be found in the appendix). Evaluating the Borcherds lift will be particularly important in the last chapter.

In the last chapter we will start by stating the main facts of Complex Multiplication for elliptic curves. The most stunning one is the fact that the modular function j that we mentioned before gives algebraic integers when evaluated at CM points. This will serve as an introduction for Complex Multiplication for Abelian varieties. We will see that for higher dimension abelian varieties we need to introduce the notion of the reflex field and the reflex type (this doesn't happen for elliptic curves as the reflex field coincides with the base field and there is just one canonical way to embed an order in an imaginary quadratic field into the ring of endomorphisms). Hilbert modular surfaces parametrize isomorphism classes of abelian varieties with Real Multiplication (that is abelian varieties such that we can embed an order in a totally real field into its endomorphism ring) which is a particular case of abelian varieties with Complex Multiplication. We will see how to enumerate all the isomorphism classes of abelian surfaces with Complex Multiplication and how to relate those classes with points on the Hilbert Modular Surfaces. We also present a certain Galois action on those classes that will allows to describe the the nature of the values of Hilbert Modular functions on those points. Abelian surfaces (with CM) have Complex Multiplication by orders in quartic CM fields, so we will study the possibilities for a quartic CM field and make explicit the notion of reflex field in each case. With the help of the method explained in chapter 3 to evaluate Borcherds lifts and an algorithm to get the CM points in the Hilbert Modular surface, we will get analogous results to those obtained for the j-invariant. The value of the Borcherds lift at one CM point is a nice algebraic number belonging to a concrete extension of the reflex field, while the product of all the values at a cycle is a rational number with multiple prime factors. We provide several examples of those computations for each possible case of quartic CM field.

Chapter 1

Hilbert Modular forms

In this first chapter we define the Hilbert modular group, Hilbert modular surfaces and Hilbert modular forms and explain the most significant features of them. Although they are similar to classical elliptic modular forms, the fact that they are functions in several variables, adds an extra complexity which changes some things. For instance we'll see that the space of Hilbert modular is finite dimensional, but unlike the classical case it is hard to determine a basis for the graded ring of modular forms. Similarly it is difficult to determine a precise fundamental domain and not very useful, but it is useful to know the existence of one to be able to proof some results that involve integrating on a fundamental domain or proving that a certain function is bounded. We will also discuss several properties about this forms such as the Fourier expansions, growth conditions of the coefficients or the number of cusps of Hilbert modular surfaces. In the end will see the first examples of Hilbert modular forms, the Eisenstein series, and the restriction to the diagonal trick, which allows us to get an elliptic modular by restricting the domain of our Hilbert modular form. Since we know the structure of the space of elliptic modular forms (dimension and generators), this will give a lot of information on the structure of our Hilbert modular form. This fact will be exploited in the third chapter when we construct some Borcherds lift from the Doi-Naganuma lift.

Although there is a more general definition for Hilbert modular forms on n variables, we restrict to Hilbert modular forms on $\mathbb{H}^2$ (2 variables) for real quadratic extensions of $\mathbb{Q}$, where $\mathbb{H} = \{\alpha \in \mathbb{C} \mid \operatorname{Im}(\alpha) > 0\}$ is the complex upper half plane. The reason for this is that in the last chapter (about Complex Multiplication) we will restrict to the cases of abelian surfaces and quartic CM fields (to be defined later) so we don't need a more general setting now. We start by summarizing the main properties of real quadratic fields, one of the central objects of study on this thesis.

1.1 Real quadratic fields

Let $D > 1$ be a squarefree integer and consider the field $F = \mathbb{Q}(\sqrt{D}) \subset \mathbb{R}$. We denote by $\mathcal{O}_F$ the ring of algebraic integers of F (those elements of F that are roots of some monic polynomial with integer coefficients). Recall that:

$$\mathcal{O}_F = \begin{cases} \mathbb{Z} + \frac{1+\sqrt{D}}{2}\mathbb{Z}, & \text{if } D \equiv 1 \pmod 4 \\ \mathbb{Z} + \sqrt{D}\mathbb{Z}, & \text{if } D \equiv 2, 3 \pmod 4 \end{cases} \tag{1.1}$$

and for the discriminant $\Delta_F = \mathrm{disc}(F)$ we have:

$$\Delta_F = \begin{cases} D & \text{if } D \equiv 1 \pmod 4 \\ 4D & \text{if } D \equiv 2, 3 \pmod 4 \end{cases} \tag{1.2}$$

Remark 1.1. In many references instead of using D and Δ_F, they use d and D for the square of the element that we adjoint to $\mathbb{Q}$ and the discriminant, respectively. However, here we use this different notation to leave d as a variable for the future. We make this remark to avoid any possible confusion.

We don't consider the case where D is a multiple of 4 as it contradicts the assumption that it is squarefree. We denote by $\mathcal{O}_F^*$ the group of units of $\mathcal{O}_F$ (the elements that have its inverse in $\mathcal{O}_F$). By the Dirichlet unit theorem there is a unique unit $\varepsilon_0 > 1$ (which is called the fundamental unit of F) such that $\mathcal{O}_F^* = \{\pm 1\} \times \{\varepsilon_0^n \mid n \in \mathbb{Z}\}$. The two embeddings of F are real, and they are the identity and conjugation, which we will denote by $x \mapsto x'$ and maps the element $r + s\sqrt{D} \mapsto r - s\sqrt{D}$ for $r, s \in \mathbb{Q}$. The norm of an element $x \in F$ is $\mathrm{N}(x) = xx'$ and the trace in F of an element x is $\mathrm{tr}(x) = x + x'$.

An integral ideal of $\mathcal{O}_F$ is a $\mathcal{O}_F$-submodule of $\mathcal{O}_F$, while a fractional ideal is an $\mathcal{O}_F$-submodule of F. Fractional ideals form a group with the operation of ideal multiplication, and the neutral element is $\mathcal{O}_F$ since $\mathcal{O}_F\mathfrak{a} = \mathfrak{a}$ for any ideal $\mathfrak{a}$. The inverse of a fractional ideal is

$$\mathfrak{a}^{-1} = \{x \in F, x\mathfrak{a} \subset \mathcal{O}_F\}$$

Although it is not that easy for ideals of other types of field, in the case where F is a quadratic extension of $\mathbb{Q}$, we have an explicit formula for $\mathfrak{a}^{-1}$ which is given by $\mathfrak{a}^{-1} = \frac{1}{N(\mathfrak{a})}\mathfrak{a}'$ where $\mathfrak{a}'$ is the conjugate ideal of $\mathfrak{a}$ (its elements are the conjugates of the elements in $\mathfrak{a}$) and $N(\mathfrak{a})$ is the ideal norm which is given by $N(\mathfrak{a}) = [\mathcal{O}_F : \mathfrak{a}]$ for an integral ideal, and for a fractional ideal $\mathfrak{b}$, if we write it as $\mathfrak{b} = r\mathfrak{a}$ for some integral ideal $\mathfrak{a}$, $N(\mathfrak{b}) = N(r)N(\mathfrak{a})$ where $N(r)$ is the norm of the element r in the quadratic extension F.

An important ideal that will frequently appear is the different ideal of F. For a general number field K, the different ideal $\mathfrak{d}_K$ is defined to be the ideal I^{-1} where $I = \{x \in K \mid \mathrm{tr}_{K/\mathbb{Q}}(x\mathcal{O}_K) \subset \mathbb{Z}\}$. In the case of a real quadratic field $F = \mathbb{Q}(\sqrt{D})$, we have:

$$\mathfrak{d}_F = \begin{cases} (\sqrt{D}) & \text{if } D \equiv 1 \pmod 4 \\ (2\sqrt{D}) & \text{if } D \equiv 2, 3 \pmod 4 \end{cases}$$

If we consider the set of all ideals of F, it is possible to define an equivalence relation on it. Two fractional ideals $\mathfrak{a}, \mathfrak{b}$ are in the same equivalence class if there exists an $r \in F$ such that $\mathfrak{a} = r\mathfrak{b}$. The group of equivalence classes is denoted by $\mathrm{Cl}(F)$

and is called the ideal class group. It is a finite abelian group and its order is called the class number. This group will take an important role in the last chapter. When $|\mathrm{Cl}(F)| = 1$, $\mathcal{O}_F$ is a principal ideal domain and all integral ideals can be generated by a single element. That's not usually the case for most F, but the following property is true (in fact it holds for any Dedekind domain).

Property 1.2. If $\mathfrak{a} \subset F$ is a fractional ideal, then there exist $\alpha, \beta \in F$ such that $\mathfrak{a} = \alpha\mathcal{O}_F + \beta\mathcal{O}_F$.

This property together with the fact that the ideal class group is finite, will be useful to prove that the number of cusps of a Hilbert modular surface is finite.

1.2 The Hilbert modular group

Let $\mathrm{SL}_2(F) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mid a, b, c, d \in F, ad - bc = 1\}$ be the special linear group of 2×2 matrices with coefficients in F. We can embed this group into $\mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{R})$ by using the two real embeddings of F. This group acts on $\mathbb{H} \times \mathbb{H}$ via the action

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \left(\frac{az_1 + b}{cz_1 + d}, \frac{a'z_2 + b'}{c'z_2 + d'}\right) \tag{1.3}$$

where $z = (z_1, z_2) \in \mathbb{H}^2$. Note that this action is well defined since $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} z = (z_1, z_2) = z$ and it can be checked that for $g, h \in \mathrm{SL}_2(F)$, $h(gz) = (hg)z$.

Definition 1.3. If $\mathfrak{a}$ is a fractional ideal of F, we write

$$\Gamma(\mathcal{O}_F \oplus \mathfrak{a}) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(F) \mid a, d \in \mathcal{O}_F, b \in \mathfrak{a}^{-1}, c \in \mathfrak{a}\right\}$$

for the Hilbert modular group corresponding to ideal $\mathfrak{a}$. When $\mathfrak{a} = \mathcal{O}_F$, we write

$$\Gamma_F = \Gamma(\mathcal{O}_F \oplus \mathcal{O}_F) = \mathrm{SL}_2(\mathcal{O}_F)$$

Note that the last equality comes from the fact that $\mathcal{O}_F$ is the neutral element of the ideal class group and hence, $\mathcal{O}_F^{-1} = \mathcal{O}_F$. The group Γ_F is called the full Hilbert modular group. Also note that we can define an action on $\mathbb{H}^2$ for any subgroup of $\mathrm{SL}_2(\mathbb{R})$ (for instance for Γ_F) by restricting the action defined in (1.3) to that subgroup.

Definition 1.4. Let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_F$. Let

$$\Gamma(\mathfrak{a}) = \left\{\gamma \in \Gamma_F \mid \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{\mathfrak{a}}\right\}$$

This subgroup of Γ_F is called the principal congruence subgroup of level $\mathfrak{a}$. A subgroup $\Gamma \subset \mathrm{SL}_2(F)$ such that Γ contains $\Gamma(\mathfrak{a})$ with finite index is called a congruence subgroup.

It is easy to verify that both $\mathit{\Gamma}(\mathcal{O}_F \oplus \mathfrak{a})$ and $\mathit{\Gamma}(\mathfrak{a})$ are groups by computing the product of two elements of them and by noting that for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$

$$\gamma^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Example 1.5. Although here we are dealing with real quadratic spaces, if we let $F = \mathbb{Q}$ and $\mathfrak{a} = (N)$ for some integer N, we obtain the classical congruence subgroups $\mathit{\Gamma}(N)$ that appear in the theory of classical elliptic modular forms.

Proposition 1.6. *Let $\mathit{\Gamma}_1$ and $\mathit{\Gamma}_2$ be congruence subgroups. Then*

(i) $\mathit{\Gamma}_1 \cap \mathit{\Gamma}_2$ is also a congruence subgroup and $\mathit{\Gamma}_1$ is commensurable to $\mathit{\Gamma}_2$ ($\mathit{\Gamma}_1 \cap \mathit{\Gamma}_2$ has finite index in both $\mathit{\Gamma}_1$ and $\mathit{\Gamma}_2$).

(ii) $\mathit{\Gamma}_F = \mathrm{SL}_2(\mathcal{O}_F)$ is a congruence subgroup.

Proof. By definition, there exists $\mathfrak{a}$ non-zero ideal of $\mathcal{O}_F$ such that, $\mathit{\Gamma}(\mathfrak{a}) \subset \mathit{\Gamma}_1$ and the quotient is finite. Similarly, there exists $\mathfrak{b}$ such that $\mathit{\Gamma}(\mathfrak{b}) \subset \mathit{\Gamma}_2$ and the quotient is finite. Let $g_1, g_2, \ldots, g_n$ be representatives of $\mathit{\Gamma}_1/\mathit{\Gamma}(\mathfrak{a})$ and $h_1, h_2, \ldots, h_m$ be representatives of $\mathit{\Gamma}_2/\mathit{\Gamma}(\mathfrak{b})$. Then

$$\mathit{\Gamma}_1 \cap \mathit{\Gamma}_2 = \left(\bigcup_{1 \le i \le n} g_i \mathit{\Gamma}(\mathfrak{a}) \right) \bigcap \left(\bigcup_{1 \le j \le m} h_j \mathit{\Gamma}(\mathfrak{b}) \right) = \bigcup_{1 \le i \le n, 1 \le j \le m} (g_i \mathit{\Gamma}(\mathfrak{a}) \cap h_j \mathit{\Gamma}(\mathfrak{b}))$$

Note that when $\mathfrak{a}$ and $\mathfrak{b}$ are coprime, we can apply the Chinese Remainder Theorem and we can express each term of the form $g_i \mathit{\Gamma}(\mathfrak{a}) \cap h_j \mathit{\Gamma}(\mathfrak{b})$ as $r_{i,j} \mathit{\Gamma}(\mathfrak{a} \cap \mathfrak{b})$ for some $r_{i,j}$. However, if $\mathfrak{a}$ and $\mathfrak{b}$ are not coprime, the intersection may be empty or not depending on g_i and h_j. In any case, we can write

$$\bigcup_{1 \le i \le n, 1 \le j \le m} (g_i \mathit{\Gamma}(\mathfrak{a}) \cap h_j \mathit{\Gamma}(\mathfrak{b})) = \bigcup_{1 \le k \le l} r_k \mathit{\Gamma}(\mathfrak{a} \cap \mathfrak{b})$$

for some $l \le nm$ (if $\mathfrak{a}, \mathfrak{b}$ are coprime, $l = nm$ as every pair of congruences has solution). Clearly one of the g_i and one of the h_j is the identity because $\mathit{\Gamma}(\mathfrak{a})$ and $\mathit{\Gamma}(\mathfrak{b})$ are contained in $\mathit{\Gamma}_1$ and $\mathit{\Gamma}_2$, respectively, which implies that the corresponding r_k is also the identity, so we have that $\mathit{\Gamma}(\mathfrak{a} \cap \mathfrak{b}) \subset \mathit{\Gamma}_1 \cap \mathit{\Gamma}_2$. It is clearly contained with finite index $l \le nm$. And since the index of $\mathit{\Gamma}(\mathfrak{a} \cap \mathfrak{b})$ in $\mathit{\Gamma}(\mathfrak{a})$ is finite, and the index of $\mathit{\Gamma}(\mathfrak{a})$ in $\mathit{\Gamma}_1$ is finite, the index of $\mathit{\Gamma}(\mathfrak{a} \cap \mathfrak{b})$ in $\mathit{\Gamma}_1$ is also finite, which implies that $\mathit{\Gamma}_1 \cap \mathit{\Gamma}_2$ has finite index in $\mathit{\Gamma}_1$ (and analogously for $\mathit{\Gamma}_2$).

That $\mathit{\Gamma}_F = \mathrm{SL}_2(\mathcal{O}_F)$ is a congruence subgroup is a direct consequence of the fact that $\mathit{\Gamma}_F = \mathit{\Gamma}(\mathcal{O}_F)$ so $\mathit{\Gamma}_F$ contains $\mathit{\Gamma}(\mathcal{O}_F)$ with index 1. □

1.3 Hilbert modular surfaces and cusps

Let $\mathit{\Gamma} \subset \mathrm{SL}_2(F)$ be a subgroup commensurable with $\mathit{\Gamma}_F$ (recall that this means that $\mathit{\Gamma}_F \cap \mathit{\Gamma}$ has finite index in $\mathit{\Gamma}$ and $\mathit{\Gamma}_F$). For a point $p \in \mathbb{H}^2$, the stabilizer of p, $\mathit{\Gamma}_p = \{\gamma \in \mathit{\Gamma} \mid \gamma p = p\}$ is a finite subgroup of $\mathit{\Gamma}$. If $|\mathit{\Gamma}_p/\{\pm 1\}| > 1$ (there is a non trivial element which fixes the point), we say that p is an elliptic fixed point.

Definition 1.7. For a Hilbert modular group $\mathit{\Gamma}$, the quotient

$$Y(\mathit{\Gamma}) = \mathit{\Gamma}\backslash\mathbb{H}^2$$

is called a Hilbert modular surface.

The Hilbert modular surface is a normal complex surface whose singularities are the elliptic fixed points. There is a finite number of them. In general, the Hilbert modular surface $Y(\mathit{\Gamma})$ is not compact (it has some points at infinity) but it can be compactified by adding a finite number of points which are called the cusps of $\mathit{\Gamma}$ which we will describe now.
We can let $\mathrm{SL}_2(F)$ act on the projective space

$$\mathbb{P}^1(F) = \left\{ \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in F^2 \setminus \{0\} \right\} / F^*$$

by matrix multiplication on the left. Throughout the following lines we will use $\left(\begin{smallmatrix} \alpha \\ \beta \end{smallmatrix}\right)$ and $(\alpha : \beta)$ indistinctly to refer to the elements of $\mathbb{P}^1(F)$. Notice that since $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\infty = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right)$, the action of $\mathrm{SL}_2(F)$ is transitive. However, that's not necessarily the case for other subgroups of $\mathrm{SL}_2(F)$. For a subgroup $\mathit{\Gamma} \subset \mathrm{SL}_2(F)$, the orbits under the action of $\mathit{\Gamma}$ on $\mathbb{P}^1(F)$ are called the cusps (or cusp points) of $\mathit{\Gamma}$. Let $(\alpha : \beta) \in \mathbb{P}^1(F)$. Note that we can assume that α, β are integral since we can multiply both by a common denominator and nothing changes. Now to $(\alpha : \beta) \in \mathbb{P}^1(F)$ we can associate the ideal $\alpha\mathcal{O}_F + \beta\mathcal{O}_F$.

Proposition 1.8. *The map*

$$\begin{aligned} \varphi \colon \mathit{\Gamma}_F\backslash\mathbb{P}^1(F) &\longrightarrow \mathrm{Cl}(F) \\ (\alpha : \beta) &\longmapsto \alpha\mathcal{O}_F + \beta\mathcal{O}_F, \end{aligned}$$

is bijective.

Proof. First we have to show that φ is well-defined (that the image of an $\mathit{\Gamma}$-class does not depend on the representative that we choose). Clearly we have $\varphi(\alpha\colon \beta) = \varphi(t\alpha\colon t\beta)$ since $\mathfrak{a} = \alpha\mathcal{O}_F + \beta\mathcal{O}_F$ and $\mathfrak{b} = t\alpha\mathcal{O}_F + t\beta\mathcal{O}_F = t\mathfrak{a}$ are in the same ideal class. Now for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathit{\Gamma}_F$ let $\left(\begin{smallmatrix} \alpha_1 \\ \beta_1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} \alpha_2 \\ \beta_2 \end{smallmatrix}\right)$. We have to show that $\varphi(\alpha_1\colon \beta_1) = \varphi(\alpha_2\colon \beta_2)$. But this follows from

$$\varphi(\alpha_1\colon \beta_1) = \alpha_1\mathcal{O}_F + \beta_1\mathcal{O}_F = (a\alpha_2 + b\beta_2)\mathcal{O}_F + (c\alpha_2 + d\beta_2)\mathcal{O}_F \subset \varphi(\alpha_2\colon \beta_2)$$

since the elements of $(a\alpha_2 + b\beta_2)\mathcal{O}_F + (c\alpha_2 + d\beta_2)\mathcal{O}_F$ are of the form $\alpha_2(ar_1 + cr_2) + \beta_2(br_1 + dr_2)$ for $r_1, r_2 \in \mathcal{O}_F$, so $ar_1 + cr_2, br_1 + dr_2 \in \mathcal{O}_F$.

Now, since the inverse of $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is $\gamma^{-1} = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$, we have that

$$\varphi(\alpha_2\colon \beta_2) = \alpha_2\mathcal{O}_F + \beta_2\mathcal{O}_F = (d\alpha_1 - b\beta_1)\mathcal{O}_F + (-c\alpha_1 + a\beta_1)\mathcal{O}_F \subset \varphi(\alpha_1\colon \beta_1)$$

Therefore $\varphi(\alpha_1\colon \beta_1) = \varphi(\alpha_2\colon \beta_2)$ and the map is well defined.

The surjectivity of φ comes from a well-known fact that holds in any Dedekind ring, although we just need it for $\mathcal{O}_F$. For any fractional ideal $\mathfrak{a} \subset F$, there exist $\alpha, \beta \in F$ such that $\mathfrak{a} = \alpha\mathcal{O}_F + \beta\mathcal{O}_F$ (Property 1.2).

Finally, to prove the injectivity, assume that $\mathfrak{a} = \varphi(\alpha_1 \colon \beta_1) = \varphi(\alpha_2 \colon \beta_2)$. Then $1 \in \mathcal{O}_F = \mathfrak{a}\mathfrak{a}^{-1} = (\alpha_1\mathcal{O}_F + \beta_1\mathcal{O}_F)\mathfrak{a}^{-1} = \alpha_1\mathfrak{a}^{-1} + \beta_1\mathfrak{a}^{-1}$, so there exist $\gamma_1, \delta_1 \in \mathfrak{a}^{-1}$ such that $\alpha_1\delta_1 - \beta_1\gamma_1 = 1$. Then for

$$M := \begin{pmatrix} \alpha_1 & \gamma_1 \\ \beta_1 & \delta_1 \end{pmatrix} \in \mathrm{SL}_2(F)$$

we have $M\infty = M\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} \alpha_1 \\ \beta_1 \end{smallmatrix}\right)$. Analogously we find that there exist $\gamma_2, \delta_2 \in \mathfrak{a}^{-1}$ such that for

$$N := \begin{pmatrix} \alpha_2 & \gamma_2 \\ \beta_2 & \delta_2 \end{pmatrix} \in \mathrm{SL}_2(F)$$

we have $N\infty = N\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} \alpha_2 \\ \beta_2 \end{smallmatrix}\right)$. So we have $\left(\begin{smallmatrix} \alpha_2 \\ \beta_2 \end{smallmatrix}\right) = NM^{-1}\left(\begin{smallmatrix} \alpha_1 \\ \beta_1 \end{smallmatrix}\right)$ and

$$NM^{-1} = \begin{pmatrix} \alpha_2 & \gamma_2 \\ \beta_2 & \delta_2 \end{pmatrix} \begin{pmatrix} \delta_1 & -\gamma_1 \\ -\beta_1 & \alpha_1 \end{pmatrix} = \begin{pmatrix} \alpha_2\delta_1 - \gamma_2\beta_1 & -\alpha_2\gamma_1 + \gamma_2\alpha_1 \\ \beta_2\delta_1 - \delta_2\beta_1 & -\beta_2\gamma_1 + \delta_2\alpha_1 \end{pmatrix} \in \mathit{\Gamma}_F,$$

which proves the injectivity and finishes the proof of the proposition. □

A direct corollary of this proposition is

Corollary 1.9. *The number of cusps of $\mathit{\Gamma}$ is equal to $h(F)$, the class number of F (number of classes in the class group).*

In particular, the number of cusp points is finite and by adding them to the Hilbert modular surface, we can make it into a compact space. We can embed $\mathbb{P}^1(F)$ into $\mathbb{P}^1(\mathbb{R}) \times \mathbb{P}^1(\mathbb{R})$ using the two real embeddings of F, and now $\mathbb{P}^1(\mathbb{R})$ can be seen as the set of rational boundary points on $\mathbb{H}^2$.

If we denote by $(\mathbb{H}^2)^* = \mathbb{H}^2 \cup \mathbb{P}^1(F)$, we can give the set $(\mathbb{H}^2)^*$ a topology that will make $\mathit{\Gamma}\backslash(\mathbb{H}^2)^*$ a compact Hausdorff space with the quotient topology (Baily-Borel compactification). This topology is the unique that has the following properties:

(i) The induced topology on $\mathbb{H}^2$ agrees with the usual topology.

(ii) $\mathbb{H}^2$ is an open set in $(\mathbb{H}^2)^*$

(iii) The sets $U_C \cup \{\infty\}$, where $U_C = \{(z_1, z_2) \in \mathbb{H}^2 \mid \Im(z_1)\Im(z_2) > C\}$ for $C > 0$ are a base of open neighborhoods of the cusp at ∞.

(iv) If $\kappa \in \mathbb{P}^1(F)$ and $\rho \in \mathrm{SL}_2(F)$ is such that $\rho\infty = \kappa$, then the sets $\rho(U_C \cup \infty)$ are a base of open neighborhoods of the cusp κ.

Lemma 1.10. *The stabilizer of the cusp infinity $\mathit{\Gamma}(\mathcal{O}_F \oplus \mathfrak{a})_\infty$ consists on the elements of $\mathit{\Gamma}(\mathcal{O}_F \oplus \mathfrak{a})$ of the form $\left(\begin{smallmatrix} \varepsilon & \mu \\ 0 & \varepsilon^{-1} \end{smallmatrix}\right)$ where $\varepsilon \in \mathcal{O}_F^*$ and $\mu \in \mathfrak{a}^{-1}$.*

Proof. If for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ we have $\gamma\infty = \infty$, we need $c = 0$. Since the determinant has to be 1, $a, d \in \mathcal{O}_F^*$ are each other's inverse. Finally b can be any element in $\mathfrak{a}^{-1}$. □

Remark 1.11. The base of open neighborhoods of (iv) does not depend on the choice of ρ, because the stabilizer Γ_∞ of ∞ acts trivially on U_C. If $\gamma = \left(\begin{smallmatrix} \varepsilon & \mu \\ 0 & \varepsilon^{-1} \end{smallmatrix}\right) \in \Gamma_\infty$, then

$$\gamma z = (\varepsilon^2 z_1 + \epsilon\mu, (\varepsilon')^2 z_2 + \varepsilon'\mu')$$

so the product of the imaginary parts remains the same since $(\varepsilon\varepsilon')^2 = 1$.

1.4 Siegel domains

Many times it is important to prove the existence of a "nice" fundamental set $S \subset \mathbb{H}^2$ so that $\Gamma S = \mathbb{H}^2$. For instance to be able to prove the convergence of certain integrals it is nice to know that we are integrating over a "small" set. In general it's not practical to try to describe a fundamental domain (a set S satisfying $\Gamma S = \mathbb{H}^2$ and that $\gamma S \cap S$ has measure 0 for all non-trivial γ). When we are working with elliptical modular forms for the group $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$, we have a nice description of a fundamental set:

$$S = \left\{ z \in \mathbb{H} \mid |z| \geq 1 \text{ and } |\mathrm{Re(z)}| \leq \frac{1}{2} \right\}$$

And although a similar result is possible in more general settings, it is unnecessary as in most cases we just need to make sense of integrals in the quotient $\Gamma\backslash\mathbb{H}^2$ or to prove that an $\mathrm{SL}_2(\mathcal{O}_F)$-invariant function is bounded in $\mathbb{H}^2$. In subsequent sections we will make use of those fundamental sets precisely for those reasons.

Definition 1.12. A subset $S \subset \mathbb{H}^2$ is said to be a fundamental set for Γ if $\Gamma S = \mathbb{H}^2$, that is

$$\mathbb{H}^2 = \bigcup_{\gamma \in \Gamma} \Gamma(S)$$

.

Definition 1.13. A fundamental set S for a group Γ is a fundamental domain if it satisfies:

(i) S is measurable

(ii) For all non-trivial $\gamma \in \Gamma$, we have that $\gamma S \cap S$ has measure zero.

It is possible to prove that every measurable fundamental set contains a fundamental domain. We now proceed by giving nice examples of sets that will help us build a fundamental set, which are known as Siegel domains.

Definition 1.14. Fix a positive real number r. We define the Siegel domain for r as:

$$S_r = \{(z_1, z_2) \in \mathbb{H}^2 \mid |\mathrm{Re}(z_1)|, |\mathrm{Re}(z_2)| < r, \mathrm{Im}(z_1), \mathrm{Im}(z_2) > \frac{1}{r}\}$$

Now, thanks to the next Theorem (its proof is a bit extense and can be found in [Gar90], chapter 1.6, page 20) we can use Siegel domains to build a fundamental set for Γ.

Theorem 1.15. *Let $p_1, \dots, p_l \in \mathbb{P}^1(F)$ be a set of representatives for the cusps Γ, and let $\gamma_1, \dots, \gamma_l \in \mathrm{SL}_2(F)$ such that $\gamma_j \infty = p_j$. There is a $r > 0$ such that*

$$S = \bigcup_{j=1}^{l} \gamma_j S_r$$

is a measurable fundamental set for Γ.

We will use this result when we prove that the space of modular forms of a fixed weight is finite dimensional.

1.5 Hilbert modular forms

Now that we have introduced the basic elements that we need to define Hilbert modular forms, such as the Hilbert modular group and surface or the cusps, we can proceed with the definition of holomorphic Hilbert modular forms. In this section we also show the existence of Fourier expansion of a certain form and several lemmas that show that for a holomorphic Hilbert modular form of a certain weight to exist, the weight can't be negative. One stunning fact that we will see in this section is that unlike what happens with elliptic modular forms, a holomorphic modular is automatically holomorphic at the cusps (by the Koecher principle).

Definition 1.16. For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(F)$, $k = (k_1, k_2) \in \mathbb{Z}^2$ and $z = (z_1, z_2) \in \mathbb{H}^2$, let

$$\mu(\gamma, z)^k = (cz_1 + d)^{k_1}(c'z_2 + d')^{k_2}$$

which is called the automorphy factor (in the following lines we will see why).

Definition 1.17. Let Γ be a congruence subgroup of Γ_F. An holomorphic function $f : \mathbb{H}^2 \to \mathbb{C}$ is called an holomorphic Hilbert modular form of weight $(k_1, k_2) := k$ for the group Γ if

$$f(\gamma z) = \mu(\gamma, z)^k f(z) \tag{1.4}$$

for all $\gamma \in \Gamma$ and $z \in \mathbb{H}^2$. When $k_1 = k_2$, f is simply called a holomorphic Hilbert modular form of weight k_1 (and it is said to have parallel weight).

We can also have non-holomorphic Hilbert modular forms. For instance, meromorphic functions that satisfy condition (1.4) are called meromorphic Hilbert modular forms and are also Hilbert modular forms. But since we will just dealwith holomorphic Hilbert modular forms we will sometimes refer to them as Hilbert modular forms for brevity. Note, that some of the results that we will present in the next pages are not true or slightly different for non-holomorphic modular forms, and that's why we have to make the distinction.

Definition 1.18. For $f : \mathbb{H}^2 \to \mathbb{C}$ the Petersson slash operator is defined by

$$(f \mid_{k_1,k_2} \gamma)(z) = \mu(\gamma, z)^{-1} f(\gamma z)$$

When $k_1 = k_2 =: k$ we just write $(f \mid_k \gamma)(z)$ instead of $(f \mid_{k_1,k_2} \gamma)(z)$.

Using the Petersson slash operator, we can rewrite condition (1.4) as

$$(f \mid_{k_1,k_2} \gamma)(z) = f(z) \qquad \forall \gamma \in \mathit{\Gamma}, z \in \mathbb{H}^2$$

Similarly to what happens with elliptic modular forms, we can also define modular forms for the group $\mathit{\Gamma}$ with a group character χ. Those kinds of modular forms will appear in the next chapters when we talk about the theta lifting, so we are also going to introduce their definition now, but we will continue talking about Hilbert Modular forms without character after that.

Definition 1.19. Let $\mathit{\Gamma}$ be a congruence subgroup of $\mathit{\Gamma}_F$ and $\chi : \mathit{\Gamma} \to \mathbb{C}^*$ a group character that only takes finitely many different values. An holomorphic function $f : \mathbb{H}^2 \to \mathbb{C}$ is called a Hilbert modular form of weight (k_1, k_2) for the group $\mathit{\Gamma}$ and character χ if

$$(f \mid_{k_1,k_2} \gamma)(z) = \chi(\gamma) f(z)$$

for all $\gamma \in \mathit{\Gamma}$ and $z \in \mathbb{H}^2$.

Notation 1.20. we denote by $M_k(\mathit{\Gamma}, \chi)$ the space of Hilbert modular forms of weight $k \in \mathbb{Z}^2$, for the group $\mathit{\Gamma}$ and character χ and simply $M_k(\mathit{\Gamma})$ when we are not considering any character (which can also be seen as the case where the character is trivial). When we are considering the full space of Hilbert modular forms of any weight, we remove the subindex and write $M(\mathit{\Gamma}, \chi)$ or $M(\mathit{\Gamma})$.

Note that if we have two Hilbert modular forms $f \in M_k(\mathit{\Gamma})$ and $g \in M_{k'}(\mathit{\Gamma})$, then $fg \in M_{k+k'}(\mathit{\Gamma})$. Therefore

$$M(\mathit{\Gamma}) = \bigoplus_{k \in Z^2} M_k(\mathit{\Gamma})$$

has the structure of a graded ring with the grading that we just described.

1.5.1 Fourier expansion of holomorphic Hilbert modular forms

In a similar way to what happens in the classic case, Hilbert modular forms also have a Fourier expansion. The main difference is that in this case it is not indexed by integers, but by the elements of a dual lattice. We will also prove some conditions on the coefficients of the Fourier expansion.

Proposition 1.21. *Let $\mathit{\Gamma}$ be a congruence subgroup, and let $\mathit{\Lambda} = \{\lambda \in F \mid \{\left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right) \in \mathit{\Gamma}\}$. Then any $f \in M_k(\mathit{\Gamma})$ has a Fourier expansion of the following form:*

$$f(z) = \sum_{\nu \in \mathit{\Lambda}^\vee} a_\nu e(\operatorname{tr}(\nu z))$$

where $e(x) = e^{2\pi i x}$, $tr(\nu z) = \nu z_1 + \nu' z_2$ *and*

$$\Lambda^\vee = \{\lambda \in F \mid \mathrm{tr}(\lambda \Lambda) \subset \mathbb{Z}\}$$

is the dual lattice of Λ *with respect to the trace form on* F*. The Fourier series is absolutely and uniformly convergent on compact sets of* $\mathbb{H}^2$*.*

Proof. Note that since Γ is a congruence subgroup, it contains $\Gamma(\mathfrak{a})$ for some ideal $\mathfrak{a}$ of $\mathcal{O}_F$, and therefore, $\mathfrak{a} \subset \Lambda$. Writing $z = x + yi$ with $x = (x_1, x_2) \in \mathbb{R}^2$ and $y = (y_1, y_2) \in \mathbb{R}^2$, $f(x+yi)$ is as smooth as we could desire as a function of x and periodic by the rank 2 (over $\mathbb{Z}$) lattice Λ, so it has a Fourier expansion (as a function of x)

$$f(x+yi) = \sum_{\nu \in \Lambda^\vee} a_\nu(y) e(\mathrm{tr}(\nu x))$$

which is absolutely and uniformly convergent for x in compact subsets of $\mathbb{R}^2$. The only exponentials that appear are those that make $\mathrm{tr}(\nu x)$ and integer, so that's why we are summing over $\Lambda^\vee$. Since f is holomorphic, it must satisfy the Cauchy-Riemann equations $i\frac{\partial f}{\partial x_1} = \frac{\partial f}{\partial y_1}$ and $i\frac{\partial f}{\partial x_2} = \frac{\partial f}{\partial y_2}$. So we have must have

$$i \sum_{\nu \in \Lambda^\vee} a_\nu(y)(2\pi i \nu) e(\mathrm{tr}(\nu x)) = \sum_{\nu \in \Lambda^\vee} \frac{\partial a_\nu(y)}{\partial y_1} e(\mathrm{tr}(\nu x))$$

$$i \sum_{\nu \in \Lambda^\vee} a_\nu(y)(2\pi i \nu') e(\mathrm{tr}(\nu x)) = \sum_{\nu \in \Lambda^\vee} \frac{\partial a_\nu(y)}{\partial y_2} e(\mathrm{tr}(\nu x))$$

By uniqueness of the Fourier expansion we must have

$$-a_\nu(y)(2\pi\nu) = \frac{\partial a_\nu(y)}{\partial y_1}$$

$$-a_\nu(y)(2\pi\nu') = \frac{\partial a_\nu(y)}{\partial y_2}$$

for each $\nu \in \Lambda^\vee$ And this is a system of differential equations whose solution is given by

$$a_\nu(y) = a_\nu e^{-2\pi tr(\nu y)}$$

for a constant a_ν. To see that the expansion is absolutely and uniformly convergent, we observe that as y_1 or y_2 increase, $e^{-2\pi tr(\nu y)}$ doesn't increase. As we have already established the absolute and uniform convergence in x, the proposition is proven. □

There is an explicit formula for the Fourier coefficients given by

$$a_\nu = \frac{1}{\mathrm{vol}(\mathbb{R}^2/\Lambda)} \int_{\mathbb{R}^2/\Lambda} f(z) e(-\mathrm{tr}(\nu z)) dx_1 dx_2$$

where $\mathbb{R}^2/\Lambda$ is the quotient of $\mathbb{R}^2$ with the lattice described in the statement of Proposition 1.21.

One important property of holomorphic Hilbert modular forms is that they are automatically holomorphic at the cusps, as opposed to what happened in the one-dimensional case where an holomorphic modular function could not be holomorphic at the cusps. This surprising property is given by the Koecher principle. Our next goal will be to prove it, but before we will need an auxiliary lemma.

Lemma 1.22. *Let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_F$. Then there exists a unit $u \in \mathcal{O}_F^*$ such that $u \equiv 1 \pmod{\mathfrak{a}}$ (meaning that $u - 1 \in \mathfrak{a}$) and $u \neq \pm 1$.*

Proof. If $\mathfrak{a} = \mathcal{O}_F$ the statement if clear as for all the units u, $u - 1 \in \mathcal{O}_F$. Assume that $\mathfrak{a} \neq \mathcal{O}_F$ and select a unit $\varepsilon \in \mathcal{O}_F^*, \varepsilon \neq \pm 1$ (for instance the fundamental unit) and consider the sequence $\varepsilon, \varepsilon^2, \varepsilon^3, \dots \pmod{\mathfrak{a}}$. Since the index of $\mathfrak{a}$ in $\mathcal{O}_F$ is finite, there are finitely many values that $\varepsilon, \varepsilon^2, \varepsilon^3, \dots \pmod{\mathfrak{a}}$ can take. Therefore, there exist $n, m \in \mathbb{Z}, n > m$ such that $\varepsilon^n \equiv \varepsilon^m \pmod{\mathfrak{a}} \iff \varepsilon^m(\varepsilon^{n-m} - 1) \equiv 0 \pmod{\mathfrak{a}}$, which implies that $u := \varepsilon^{n-m} \equiv 1 \pmod{\mathfrak{a}}$ because otherwise we would have $\varepsilon^m \in \mathfrak{p}$ for some prime ideal dividing $\mathfrak{a}$ and this would imply that $1 \in \mathfrak{p} \implies \mathfrak{p} = \mathcal{O}_F$ (since $1 = \varepsilon^m \varepsilon^{-m}$ and $\varepsilon^{-m} \in \mathcal{O}_F$). Note that $u \neq \pm 1$ and, therefore, it satisfies the desired conditions. □

Theorem 1.23 (Koecher principle)**.** *Let $f \colon \mathbb{H}^2 \to \mathbb{C}$ be an holomorphic function satisfying $f\,|_{k_1,k_2}\,\gamma = f \quad \forall \gamma \in \Gamma$, a congruence subgroup of Γ_F. Then in the Fourier expansion of*

$$f(z) = \sum_{\nu \in \Lambda^\vee} a_\nu e(\mathrm{tr}(\nu z))$$

(where Λ is the lattice defined in Proposition 1.21) we have that $a_\nu = 0$ unless $\nu = 0$ or ν is totally positive (i. e. we have $\nu, \nu' > 0$)

Proof. Since Γ is a congruence subgroup, it contains $\Gamma(\mathfrak{a})$ for some non-zero ideal $\mathfrak{a}$. Using the previous Lemma, we know that there exists $u \in \mathcal{O}_F^*$ such that $u \equiv 1 \pmod{\mathfrak{a}}$, so the transformation law for $\left(\begin{smallmatrix} u & 0 \\ 0 & u^{-1} \end{smallmatrix}\right)$ (which belongs to Γ by the construction of u) implies that

$$u^{k_1} u'^{k_2} \sum_{\nu \in \Lambda^\vee} a_\nu e(\mathrm{tr}(\nu u^2 z)) = \sum_{\nu \in \Lambda^\vee} a_\nu e(\mathrm{tr}(\nu z))$$

Using the uniqueness of the Fourier expansion, we deduce that for each exponential, the coefficients must be equal giving

$$u^{k_1} u'^{k_2} a_{u^{-2}\nu} = a_\nu \tag{1.5}$$

Assume that for $\nu \in \Lambda^\vee$ we have $a_\nu \neq 0$ and $\nu < 0$ or $\nu' < 0$. Without loss of generality, assume the first case. Now there exists a unit $\varepsilon \in \Lambda$ such that $\varepsilon > 1$ and $0 < \varepsilon' < 1$ (either u^2 or $\frac{1}{u^2}$ work since both are greater than 0 and not equal to 1). Then as $n \to \infty$, $\mathrm{tr}(\varepsilon^{2n}\nu) = \varepsilon^{2n}\nu + (\varepsilon')^{2n}\nu'$ tends to $-\infty$ as the second term in the sum tends to 0 and $\varepsilon^{2n} \to \infty, \nu < 0$. Let's consider the following series which is a subseries of the Fourier expansion at $z = (i, i)$ (so it must converge absolutely):

$$\sum_{n\geq 1} e(i\mathrm{tr}(\nu\varepsilon^{2n}))a_{\nu\varepsilon^{2n}}$$

But by the identity from (1.5),

$$\sum_{n\geq 1} |a_{\nu\varepsilon^{2n}} e(i\mathrm{tr}(\nu\varepsilon^{2n}))| = |a_\nu| \sum_{n\geq 1} \varepsilon^{k_1 n}\varepsilon'^{k_2 n} e^{-2\pi tr(\nu\varepsilon^{2n})} \to \infty.$$

since all terms in the sum are positive and the exponential goes to ∞ faster than $\varepsilon^{k_1 n}\varepsilon'^{k_2 n}$ goes to 0. This contradicts the convergence, and therefore, no such ν exists. □

Corollary 1.24. *A holomorphic Hilbert modular form for the group Γ has a Fourier expansion at the cusp ∞ of the form*

$$f(z) = a_0 + \sum_{\substack{\nu\in\Lambda^\vee \\ \nu\gg 0}} a_\nu e(\mathrm{tr}(\nu z)) \tag{1.6}$$

The constant term a_0 is the value of f at ∞ (we can write $f(\infty) = a_0$). If $\kappa \in \mathbb{P}^1(F)$ is a cusp of Γ, we take $\rho \in \mathrm{SL}_2(F)$ such that $\rho\infty = \kappa$ and $f(\kappa) = (f\mid_{k_1,k_2} \rho)(\infty)$ is the value of f at the cusp κ. Note that this value depends on the choice of γ unless $(k_1, k_2) = (0, 0)$ (by a non-zero factor).

Definition 1.25. A holomorphic Hilbert modular form is called a cusp form if it vanishes at all the cusps of Γ.

Proposition 1.26. *Let f be an holomorphic Hilbert modular form of weight (k_1, k_2) for the group congruence group Γ. If $k_1 \neq k_2$, f is a cusp form.*

Proof. It is a consequence of the relation between the coefficients of the Fourier expansion that we saw in the proof of Koecher's principle. From (1.5), we had:

$$u^{k_1}u'^{k_2}a_{u^{-2}\nu} = a_\nu$$

for some unit $u \neq \pm 1$, so for $\nu = 0$, we get that

$$(u^{k_1}u'^{k_2} - 1)a_0 = 0$$

proving that the f is a cusp form if $k_1 \neq k_2$ since $u^{k_1}u'^{k_2} = 1 \iff u^{k_1}u'^{k_1}u'^{k_2-k_1} = 1 \iff N(u)^{k_1}u'^{k_2-k_1} = 1 \implies u'^{k_2-k_1} = \pm 1 \implies u' = \pm 1 \implies u = \pm 1$ which is not the case. □

To finish this section we will prove that not for every pair of integers (k_1, k_2) there exists an holomorphic Hilbert modular of weight (k_1, k_2). Actually we will see that such forms only exist when $k_1, k_2 > 0$ or $k_1 = k_2 = 0$. But before directly proving it we will need some additional lemmas.

Lemma 1.27. *Let f be a modular form of weight (k_1, k_2) for the congruence subgroup Γ. Then $h(z) = |f(z)y_1^{k_1/2}y_2^{k_2/2}|$ is Γ-invariant (where $z = (x_1 + iy_1, x_2 + iy_2)$).*

Proof. Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathit{\Gamma}$. We want to see that $h(\gamma z) = h(z)$ for all $z \in \mathbb{H}^2$. Let $\Im(z)$ be the imaginary part of z. Note that if we consider the action of $\mathrm{SL}_2(F)$ on $\mathbb{H}$ defined by

$$\gamma z = \begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}$$

we have that

$$\Im(\gamma z) = \Im(\frac{az+b}{cz+d}) = \Im(\frac{(az+b)(c\overline{z}+d)}{(cz+d)(c\overline{z}+d)}) = \Im(\frac{(az+b)(c\overline{z}+d)}{|cz+d|^2}) =$$

$$= \Im(\frac{ac|z|^2 + adz + bc\overline{z} + bd}{|cz+d|^2}) = \frac{1}{|cz+d|^2}\Im(ac|z|^2 + adz + bc\overline{z} + bd) =$$

$$= \frac{1}{|cz+d|^2}\Im(adz + bc\overline{z}) = \frac{1}{|cz+d|^2}\Im(adz - bcz) = \frac{\Im(z)}{|cz+d|^2}$$

But then

$$h(\gamma z) = \left|f(\gamma z)\Im(\gamma z_1)^{k_1/2}\Im(\gamma' z_2)^{k_2/2}\right| = \left|f(z)(cz_1+d)^{k_1}(c'z_2+d')^{k_2}\Im(\gamma z_1)^{k_1/2}\Im(\gamma' z_2)^{k_2/2}\right| =$$

$$= \left|f(z)\Im(z_1)^{k_1/2}\Im(z_2)^{k_2/2}\right| = |f(z)y_1^{k_1/2}y_2^{k_2/2}| = h(z)$$

where γ' denotes the matrix resulting of conjugating in F the entries of γ. □

Lemma 1.28. *Let f be an holomorphic modular form of weight (k_1, k_2) for $\mathit{\Gamma}$ and let $h(z) = |f(z)y_1^{k_1/2}y_2^{k_2/2}|$. Then*

1. *If f has parallel weight $k := k_1 = k_2$, then h attains a maximum in $\mathbb{H}^2$.*
2. *If f is a cusp form h vanishes at the cusps and attains a maximum in $\mathbb{H}^2$.*

Proof. By the previous proposition, we know that h is $\mathit{\Gamma}$-invariant. Therefore, to prove that it attains a maximum in $\mathbb{H}^2$, we only need to prove that it attains a maximum in a fundamental set. By Theorem 1.15, it is enough to show that for any $\gamma \in \mathrm{SL}_2(F)$ and any $t > 0$, $h(\gamma z)$ attains a maximum on the Siegel domain S_t. From equation (1.6) we know that the Fourier expansion of f at the cusp $\gamma\infty$ tells us that

$$h(\gamma z) = (y_1 y_2)^k a_0 + (y_1 y_2)^k \sum_{\substack{\nu \in \Lambda^\vee \\ \nu \gg 0}} a_\nu e(\mathrm{tr}(\nu z))$$

where $\Lambda \subset F$ is the rank 2 lattice over $\mathbb{Z}$ defined in Proposition 1.21. Since k is negative,

$$\lim_{y_1 y_2 \to \infty} (y_1 y_2)^{k/2} = 0$$

so

$$\lim_{y_1 y_2 \to \infty} h(\gamma z) = 0$$

since the sum converges uniformly and absolutely. Therefore $h(\gamma z)$ is bounded on S_t and hence it attains a maximum on S_t, completing the first part of the lemma.

The second part is proven similarly and the fact that h vanishes at the cusps is direct from the fact that f also vanishes at the cusps. □

Proposition 1.29. *Let f be an holomorphic modular form of weight (k_1, k_2) for the congruence subgroup Γ. Then f is identically 0 unless $k_1, k_2 > 0$ or $k_1 = k_2 = 0$. If $k_1 = k_2 = 0$, then f is constant.*

Proof. We will start by proving that there are no non-zero holomorphic modular forms of weight (k_1, k_2) when one of them is 0 and the other isn't. Without loss of generality assume that $k_1 = 0$ and $k_2 \neq 0$. Then, since $k_1 \neq k_2$, Proposition 1.26 says that f is a cusp form and by Lemma 1.28, $h(z) = y_2^{h_2/2} f(z)$ is such that $|h|$ achieves a maximum in $\mathbb{H}^2$. As a function of the first variable z_1, h must be constant due to the maximum modulus principle. Recall that this principle says that if $z_0 \in U \subset \mathbb{C}$, for a connected open subset U, and g is an holomorphic function such that $|g(z_0)| \geq |g(z)|$ for all z in a neighborhood of z_0, then g is constant in U. So

$$h(z_1, z_2) = h(\gamma(z_1, z_2)) = h(\gamma z_1, \gamma' z_2) = h(z_1, \gamma' z_2)$$

for all $\gamma \in \Gamma$. Since $\{\gamma' z_2 \mid \gamma \in \Gamma\}$ is dense in $\mathbb{H}$ ($\mathcal{O}_F$ is dense in $\mathbb{R}$ and the same happens for any ideal of F, so it is not hard to see it also for Γ), h must be constant also in z_2 and therefore in all $\mathbb{H}^2$. But it vanishes at the cusps, so it must vanish in all $\mathbb{H}^2$ and $f = 0$.

For the case where $k_1 = k_2 = 0$, if f is a cusp form, by Proposition 1.28, $|f|$ attains a maximum in $\mathbb{H}^2$ and by the maximum modulus principle, it is constant in each variable, so it is constant. Since it vanishes at the cusps, $f = 0$. If it is not a cusp form, consider

$$g(z) = \prod_{\kappa \in \Gamma \backslash \mathbb{P}^1(F)} (f(z) - f(\kappa))$$

which vanishes at all the cusps. With a similar reasoning we find out that $g = 0$, so f takes only the values that takes at the cusps and by continuity, this values must be the same. Hence f is constant.

Lastly, assume that one of k_1, k_2 is negative. Then if $k_1 \neq k_2$ by Proposition 1.26, f is a cusp form. And if $k_1 = k_2$ f has parallel negative weight. In any case, by Proposition 1.28, $h(z) = |f(z) y_1^{k_1/2} y_2^{k_2/2}|$ attains a maximum, so it is bounded by a constant $C > 0$ on $\mathbb{H}^2$. Then the coefficients of the Fourier expansion at the cusp ∞ satisfy

$$|a_\nu| \leq \frac{1}{\mathrm{vol}(\mathbb{R}^2/\Lambda)} \int_{\mathbb{R}^2/\Lambda} |f(z) e(-\mathrm{tr}(\nu z))| dx_1 dx_2 \leq \frac{C}{\mathrm{vol}(\mathbb{R}^2/\Lambda)} \int_{\mathbb{R}^2/\Lambda} |y_1^{-k_1/2} y_2^{-k_2/2}| dx_1 dx_2$$

Letting $y_1 \to 0$, we see that a_ν vanishes for all $\nu \in \Lambda^\vee$, so $f = 0$ as we wanted to prove. □

To finish with this section we give a result from Hecke that gives a bound on the growth of the coefficients of Hilbert modular forms.

Proposition 1.30. *Let $f \in M_k(\Gamma)$ for some congruence group Γ and a_ν be its Fourier coefficients.*

(i) Then $a_\nu = O(N(\nu)^k)$ when $N(\nu) \to \infty$ ($|a_\nu| \leq C N(\nu)^k$ for some constant C for sufficiently large $N(\nu)$)

(ii) If f is a cusp form the estimate is stronger: $a_\nu = O(N(\nu)^{k/2}$.

Proof. For a general congruence group, the first part is hard. For the full Hilbert modular group we can use the fact that every modular form can be written as the sum of a cusp form and Eisenstein series (to be presented in the next section) which is established in Theorem 1.32 and compute bounds for each Eisenstein series (we know their Fourier coefficients) and use the bound of the second part of this proposition for the cusp form.

The bound for cusp forms can be easily proven with the results we just presented. Using the expression for the Fourier coefficients of the expansion at ∞ and Proposition 1.28 which tells us that $|f(z)(y_1y_2)^{k/2}|$ is bounded on $\mathbb{H}^2$, we have

$$|a_\nu| \leq \frac{1}{\operatorname{vol}(\mathbb{R}^2/\Lambda)} \int_{\mathbb{R}^2/\Lambda} |f(z)e(-\operatorname{tr}(\nu z))|\, dx_1dx_2 \leq C \int_{\mathbb{R}^2/\Lambda} (y_1y_2)^{-k/2} e^{-2\pi(\nu y_1 + \nu' y_2)} dx_1dx_2$$

for $y_1, y_2 \in \mathbb{R}$ and for some constant $C > 0$. If $y_1 = 1/\nu$, $y_2 = 1/\nu'$, we get that

$$|a_\nu| \leq C\operatorname{vol}(\mathbb{R}^2/\Lambda)N(\nu)^{k/2}$$

proving the proposition. □

1.6 Eisenstein series

In this section we show the first examples of Hilbert modular forms. We will restrict to the simpler case where $\mathit{\Gamma} = \mathit{\Gamma}_F = \mathrm{SL}_2(\mathcal{O}_F)$ for the real quadratic field F. We will write $N(x)$ for the norm of $x \in F$ and $N(\mathfrak{a})$ for the norm of a fractional ideal $\mathfrak{a} \subset F$ indistinguishably.

Recall the definition for the norm of an ideal that wegave when we introduced real quadratic fields. For $z = (z_1, z_2) \in \mathbb{H}^2$, recall that $N(\alpha z + \beta) = (\alpha z_1 + \beta)(\alpha' z_2 + \beta')$. The group of units of $\mathcal{O}_F$ acts on $\mathfrak{b} \times \mathfrak{b}$ for a fractional ideal $\mathfrak{b}$ by $(\alpha, \beta) \mapsto (\varepsilon\alpha, \varepsilon\beta)$ for $\varepsilon \in \mathcal{O}_F^*$. Since $N(\varepsilon(\alpha z + \beta)) = N(\varepsilon)N(\alpha z + \beta)$ and $N(\varepsilon)^k = 1$, for $k \in \mathbb{Z}$ even, $N(\alpha z + \beta)^k$ is well defined for $(\alpha, \beta) \in \mathcal{O}_F^* \backslash \mathfrak{b} \times \mathfrak{b}$ and even k.

Definition 1.31. Let $k > 2$ be an even integer. We define the Eisenstein series of weight k for an ideal $\mathfrak{b} \in \mathrm{Cl}(F)$ by

$$E_{k,\mathfrak{b}}(z) = N(\mathfrak{b})^k \sum_{\substack{(\alpha,\beta) \in \mathcal{O}_F^* \backslash \mathfrak{b} \times \mathfrak{b} \\ (\alpha,\beta) \neq (0,0)}} N(\alpha z + \beta)^{-k}$$

The Eisenstein series $E_{k,\mathfrak{b}}$ converges uniformly absolutely in every Siegel domain and does not depend on the representative $\mathfrak{b}$ of the ideal class that we choose. If $\mathfrak{a} = r\mathfrak{b}$ is another representative, then:

$$E_{k,\mathfrak{b}}(z) = N(\mathfrak{b})^k \sum_{\substack{(\alpha,\beta) \in \mathcal{O}_F^* \backslash \mathfrak{b} \times \mathfrak{b} \\ (\alpha,\beta) \neq (0,0)}} N(\alpha z + \beta)^{-k} = N(r\mathfrak{a})^k \sum_{\substack{(\alpha,\beta) \in \mathcal{O}_F^* \backslash r\mathfrak{a} \times r\mathfrak{a} \\ (\alpha,\beta) \neq (0,0)}} N(\alpha z + \beta)^{-k} =$$

$$= N(\mathfrak{a})^k N(r)^k \sum_{\substack{(\alpha,\beta)\in\mathcal{O}_F^*\backslash\mathfrak{a}\times\mathfrak{a}\\(\alpha,\beta)\neq(0,0)}} N(r\alpha z+r\beta)^{-k} = N(\mathfrak{a})^k N(r)^k \sum_{\substack{(\alpha,\beta)\in\mathcal{O}_F^*\backslash\mathfrak{a}\times\mathfrak{a}\\(\alpha,\beta)\neq(0,0)}} N(r)^k N(\alpha z+\beta)^{-k} =$$

$$= E_{k,\mathfrak{a}}(z)$$

For this reason we may simply write $E_{k,B}$ for $B \in \mathrm{Cl}(F)$ to denote the Eisenstein series for $\mathfrak{b} \in B$. For a proof of the uniform and absoulte convergence see [Gar90], section 1.5.

Theorem 1.32. *Let $k > 2$ be an even integer. Then $E_{k,B} \in M_k(\Gamma_F)$ and the set of Eisenstein series for $B \in \mathrm{Cl}(F)$ are linearly independent. As a corollary, the space of modular forms of weight k for Γ_F may be written as*

$$M_k(\Gamma_F) = S_k(\Gamma_F) \oplus \bigoplus_{B\in Cl(F)} \mathbb{C}E_{k,B}$$

Proof. To check that $E_{k,B} \in M_k(\Gamma_F)$ we just need to check that for any $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_F$

$$E_{k,B}(\gamma z) = N(\mathfrak{b})^k \sum_{\substack{(\alpha,\beta)\in\mathcal{O}_F^*\backslash\mathfrak{b}\times\mathfrak{b}\\(\alpha,\beta)\neq(0,0)}} (\alpha\frac{az_1+b}{cz_1+d}+\beta)^{-k}(\alpha'\frac{a'z_2+b'}{c'z_2+d'}+\beta')^{-k} =$$

$$= N(\mathfrak{b})^k N(cz+d)^k \sum_{\substack{(\alpha,\beta)\in\mathcal{O}_F^*\backslash\mathfrak{b}\times\mathfrak{b}\\(\alpha,\beta)\neq(0,0)}} (\alpha(az_1+b)+\beta(cz_1+d))^{-k}(\alpha'(a'z_2+b')+\beta'(c'z_2+d'))^{-k} =$$

$$= N(\mathfrak{b})^k N(cz+d)^k \sum_{\substack{(\alpha,\beta)\in\mathcal{O}_F^*\backslash\mathfrak{b}\times\mathfrak{b}\\(\alpha,\beta)\neq(0,0)}} N((\alpha a+\beta c)z+\alpha b+\beta d)^{-k} =$$

$$= N(\mathfrak{b})^k N(cz+d)^k \sum_{\substack{(\alpha,\beta)\in\mathcal{O}_F^*\backslash\mathfrak{b}\times\mathfrak{b}\\(\alpha,\beta)\neq(0,0)}} N(\alpha z+\beta)^{-k} =$$

$$= \mu(\gamma, z)^k E_{k,B}$$

where the second to last equality because for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_F$ the action $(\alpha, \beta) \mapsto (a\alpha + c\beta, b\alpha + d\beta)$ is a bijection of $\{(\alpha, \beta) \in \mathcal{O}_F^*\backslash\mathfrak{b} \times \mathfrak{b} \mid (\alpha, \beta) \neq (0, 0)\}$ to itself. The other part of the theorem is proven in [Gar90] in page 17. □

We can define Eisenstein series for odd values of $k > 2$, although the series will be identically zero if there exists a unit of negative norm. Note that $E_{k,B}$ is a symmetric Hilbert modular form in the sense that $E_{k,B}(z_1, z_2) = E_{k,B}(z_2, z_1)$ for all $(z_1, z_2) \in \mathbb{H}^2$. For any pair $(\alpha, \beta) \in \mathcal{O}_F^*\backslash\mathfrak{b} \times \mathfrak{b}$ if both (α, β) and (α', β') belong to the same equivalence class under the action of $\mathcal{O}_F^*$ then $N(\alpha z + \beta) = (\alpha z_1 + \beta)(\alpha' z_2 + \beta') = N(\alpha z' + \beta)$ where $z' = (z_2, z_1)$. And if they are not in the same equivalence class, then for each pair (α, β) over which we are summing, we have a different pair (α', β') such that $N(\alpha z + \beta) = N(\alpha' z' + \beta')$ and thus $E_{k,B}$ is symmetric.

In a similar way to how it is done in the classical case, we can compute the Fourier expansion of the Eisenstein series which has the following form:

Theorem 1.33. *Let $k > 2$ be an even integer. The Eisenstein series $E_{k,B}$ has a Fourier expansion*

$$E_{k,B} = \zeta_{B^{-1}}(k) + \frac{(2\pi i)^{2k}}{(k-1)!^2} D^{\frac{1}{2}-k} \sum_{\substack{\nu \in \mathfrak{d}_F^{-1} \\ \nu \gg 0}} \sigma_{k-1,\mathfrak{d}_F B}(\mathfrak{d}_F \nu) e^{2\pi i tr(\nu z)} \tag{1.7}$$

where $\mathfrak{d}_F$ is the different ideal of F and $\sigma_{m,\mathfrak{a}}(\mathfrak{c})$ is the divisor sum

$$\sigma_{m,B}(\mathfrak{c}) = \sum_{\substack{\mathfrak{b} \in B \\ \mathfrak{b} | \mathfrak{c}}} N(\mathfrak{b})^s$$

1.7 Finite dimensionality of the space of cuspforms and modular forms

The goal of this section is to show that $M_k(\Gamma)$ has finite dimension. We will do it with the help of the previously defined fundamental sets. To compute integrals on fundamental domains, we will use a measure that is invariant on $\mathbb{H}^2$ under the action of $\mathrm{SL}_2(\mathbb{R})^2$, which is induced by the Haar measure on $\mathbb{H}$ under the action of $\mathrm{SL}_2(\mathbb{R})$ and is given by the differential form

$$d\mu = \frac{dx_1 dy_1}{y_1^2} \frac{dx_2 dy_2}{y_2^2}$$

Definition 1.34. Let $f, g \in M_k(\Gamma)$. The Petersson scalar product is defined by

$$\langle f, g \rangle = \int_{\mathcal{F}} f(z)\overline{g(z)}(y_1 y_2)^k d\mu$$

where $\mathcal{F}$ is any fundamental domain for Γ.

Proposition 1.35. *When at least one of f and g are cusp forms, the Petersson scalar product converges absolutely and does not depend on the choice of the fundamental domain.*

Proof. A similar argument to that of Proposition 1.28 shows that $f(z)\overline{g(z)}(y_1y_2)^k$ is invariant under Γ and bounded on $\mathbb{H}^2$. Hence, that the integral does not depend on the choice of $\mathcal{F}$ follows from the absolute convergence using the theorem on dominated convergence for the Lebesgue integral. To prove the absolute convergence, it is enough to show that

$$\int_{\mathcal{F}} d\mu < \infty$$

However, since we saw that S (from Theorem 1.15) is a fundamental set that consists of a finite union of images of S_r by elements of $\mathrm{SL}_2(F)$ for some r, it is enough to prove that

$$\int_{\mathcal{S}_r} d\mu < \infty$$

But this follows from

$$\int_{\mathcal{S}_r} d\mu = \int_{\mathcal{S}_r} \frac{dx_1 dy_1}{y_1^2}\frac{dx_2 dy_2}{y_2^2} = \int_{\frac{1}{t}}^{\infty}\int_{-t}^{t}\int_{\frac{1}{t}}^{\infty}\int_{-t}^{t}\frac{dx_1 dy_1}{y_1^2}\frac{dx_2 dy_2}{y_2^2} =$$

$$= (\int_{-t}^{t} dx_1)(\int_{\frac{1}{t}}^{\infty}\frac{dy_1}{y_1^2})(\int_{-t}^{t} dx_2)(\int_{\frac{1}{t}}^{\infty}\frac{dy_2}{y_2^2})) < \infty$$

Where the last inequality is true since $\int_{\frac{1}{t}}^{\infty}\frac{dy}{y^2}$ converges and so does $\int_{-t}^{t} dx$. Actually their exact values can be computed and are t and $2t$ respectively. □

Now that we have a well-defined scalar product we can use it to define the associated norm on $S_k(\mathit{\Gamma})$:

$$||f||_2 := \sqrt{\langle f, f\rangle}$$

We can also define the maximum norm by

$$||f||_\infty := \max_{z\in\mathcal{F}}(|f(z)|(y_1y_2)^{\frac{k}{2}})$$

Those two norms are related by the following lemma which is proven in [Fre90], in page 68.

Lemma 1.36. *There is a constant A such that*

$$||f||_\infty \leq A \cdot ||f||_2$$

for all $f \in S_k(\mathit{\Gamma})$.

Using this lemma we are ready to prove the following

Theorem 1.37. *The vector space $M_k(\mathit{\Gamma})$ is finite dimensional.*

Proof. It is enough to show that $S_k(\mathit{\Gamma})$ is finite dimensional. To see why, assume that $\dim S_k(\mathit{\Gamma}) < \infty$ and $\dim M_k(\mathit{\Gamma}) = \infty$. That means that for every $N > 0$ we can pick N modular forms from $M_k(\mathit{\Gamma})$ that are linearly independent and independent with $S_k(\mathit{\Gamma})$. But the number of cusps is finite, so we can choose a finite subset of modular forms whose linear combination vanishes at all cusps, giving a cuspform and contradicting the hypothesis.

Let's proof then that $\dim S_k(\mathit{\Gamma}) < \infty$. Let $f_1, f_2, \ldots, f_m$ be an orthonormal set of cuspforms with respect to the Petersson scalar product. Let

$$f = \sum_{j=1}^{m} \lambda_j f_j$$

be an arbitrary linear combination of them ($\lambda_j \in \mathbb{C}$). By the previous lemma, there exists A such that $||f||_\infty \leq A \cdot ||f||_2$, so for all $z \in \mathbb{H}^2$ we have

$$\left|\sum_{j=1}^{m} \lambda_j (y_1y_2)^{k/2} f_j(z)\right| \leq A\left(\sum_{j=1}^{m}|\lambda_j|^2\right)^{\frac{1}{2}}$$

When $\lambda_j = \overline{f_j(z)}$, we have that

$$\left|\sum_{j=1}^{m} |f_j(z)|^2 (y_1 y_2)^{k/2}\right| \leq A \left(\sum_{j=1}^{m} |f_j(z)|^2\right)^{\frac{1}{2}}$$

Now by squaring and dividing by the sum on the right hand side, we get

$$\sum_{j=1}^{m} |f_j(z)|^2 (y_1 y_2)^{k} \leq A^2$$

Finally, by integrating over $\mathcal{F}$ and using that $f_1, f_2, \ldots, f_m$ is an orthonormal set and hence, $\langle f_j, f_j \rangle = 1$ we obtain

$$\sum_{i=1}^{m} \langle f_i, f_i \rangle = m \leq A^2 \mathrm{vol}(\mathit{\Gamma} \backslash \mathbb{H}^2)$$

which is finite. This concludes the proof of the Theorem. □

1.8 Restriction to the Diagonal

We finish this chapter by mentioning a useful trick for Hilbert modular forms. If we take a modular form of parallel weight k, $f \in M_k(\mathit{\Gamma}_F)$ and consider its restriction to the diagonal $g(\tau) = f(\tau, \tau)$, then since $\mathrm{SL}_2(\mathbb{Z})$ can be embedded in $\mathit{\Gamma}_F = \mathrm{SL}_2(\mathcal{O}_F)$ and for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \subset \mathit{\Gamma}_F$ we have that $\gamma = \gamma'$, g transforms in the following way:

$$g(\gamma\tau) = f(\gamma\tau, \gamma\tau) = f(\gamma\tau, \gamma'\tau) = f(\gamma(\tau, \tau)) = (c\tau + d)^{2k} f(\tau, \tau) = (c\tau + d)^{2k} g(\tau)$$

which means that g is an elliptical modular form of weight $2k$. This fact is really useful as we know the dimension of the space of elliptic modular forms of weight $2k$ and which elements generate them. Therefore, it is not really hard to find what is the modular form g (by looking at the first few coefficients, for instance) which tells us information about the Hilbert modular form f. We will use this trick in the third chapter to prove that certain modular forms that we lift with the Doi-Naganuma lift are equal to some concrete Borcherds lift. The details will be explained there once we introduce the two lifts.

But we can also use this trick right now to get some nice identities. For $k = 2, 4$, we have that the dimension of the space of elliptic modular forms of weight $2k$ is 1 and the space is generated by the elliptic Eisenstein series, so the restriction to the diagonal of $E_{k,B}$ (the Hilbert modular Eisentein series) coincides with a multiple of the classical Eisenstein series. Therefore we can deduce some interesting identities, like the values of the Dedekind zeta function of F, by comparing the coefficients of the Fourier expansion given by equation 1.7 with the Fourier expansion for elliptic modular forms. For instance we can we get the following:

Proposition 1.38. *The values of the Dedekind zeta function of the real quadratic field F at the arguments $-1, -3$ are given by*

$$\zeta_F(-1) = \frac{1}{60} \sum_{\substack{x \in \mathbb{Z} \\ x^2 < \Delta_F \\ x^2 \equiv \Delta_F \pmod 4}} \sigma_1\left(\frac{\Delta_F - x^2}{4}\right)$$

$$\zeta_F(-3) = \frac{1}{120} \sum_{\substack{x \in \mathbb{Z} \\ x^2 < \Delta_F \\ x^2 \equiv \Delta_F \pmod 4}} \sigma_3\left(\frac{\Delta_F - x^2}{4}\right)$$

where Δ_F is the discriminant of F and $\sigma_m(n)$ is the sum of the m-th powers of the divisors of n.

Chapter 2

Orthogonal groups

An interesting property of Hilbert modular surfaces is that they can also be seen as modular varieties associated to the orthogonal group of a certain quadratic space. This property is useful to study some features of Hilbert modular surfaces such as certain divisors (the so-called Hirzebruch-Zagier divisors) which are necessary when studying the Borcherds lift. In this chapter we start by introducing the basic notions of quadratic spaces and the Clifford algebra. We also discuss some realizations of an hermitian symmetric domain corresponding to the orthogonal group of a quadratic space of type $(2, n)$. Afterwards, we will use those notions to prove the desired results for our case of Hilbert modular surfaces and introduce the theta lifting. Although the introduction to quadratic spaces and Clifford algebras could be much shorter and skip some results and examples, they are included for clarity and to make the explanation easier to follow. However, that doesn't mean that all the definitions are as general as they could possibly be.

2.1 Quadratic forms

Let R be a commutative ring with unity 1 and R^* the group of invertible elements, and assume that 2 is an invertible element. Let M be a finitely generated R-module and $B : M \times M \to R$ be a symmetric bilinear form (it is linear in both arguments). We define a quadratic form to be an application $Q : M \to R$ such that $Q(x) = B(x, x)$ for some bilinear form B. We will usually refer to $B(x, y)$ as (x, y) for brevity. Note that we can recover the bilinear form from the quadratic form by $(x, y) = \frac{1}{2}(Q(x + y) - Q(x) - Q(y))$. The pair (M, Q) is called a quadratic module over R. When R is a field, we call it a quadratic space.

We say that x and y are orthogonal if $(x, y) = 0$. For a set $S \subset M$, the orthogonal complement is defined to be

$$S^{\perp} = \{x \in M \mid (x, y) = 0 \ \forall \ y \in S\}$$

The quadratic module is non-degenerate when $M^{\perp} = 0$. For a non-zero $x \in M$, if $Q(x) = 0$, it is called isotropic, and anisotropic otherwise.

Given two quadratic modules $(M_1, Q_1), (M_2, Q_2)$ an R-linear map $\sigma : M_1 \to M_2$ is an isometry if it is injective and $Q_2(\sigma(x)) = Q_1(x)$ for all $x \in M$. When σ is surjective, we say that M_1 and M_2 are isometric. The orthogonal group of M consists on the isometries from M to itself,

$$O_M = \{\sigma \in \mathrm{Aut}(M) \mid \sigma \text{ is an isometry}\}$$

The special orthogonal group SO_M is the subset of elements of O_M with determinant 1. It is clear that both have a group structure.

Example 2.1. One of the most common type of isometries are reflections. Given an element $x \in M$ such that $Q(x) \in R^*$, the reflection in the hyperplane $x^\perp$ is defined by

$$\tau_x = y - \frac{2(y,x)x}{Q(x)} \, y \in M.$$

Note that it is precisely the reflection by hyperplane $x^\perp$ because $\tau_x(x) = x - \frac{2(x,x)x}{Q(x)} = x - 2x = -x$, if $y \in x^\perp$, $(x, y) = 0 \implies \tau_x(y) = y$ and $\tau_x^2 = \mathrm{id}$. The last part is true as for any $y \in M$

$$\tau_x(\tau_x(y)) = \tau_x(y - \frac{2(x,y)x}{Q(x)}) = y - \frac{2(x,y)x}{Q(x)} - \frac{2(x, y - \frac{2(x,y)x}{Q(x)})}{Q(x)} x =$$

$$= y - \frac{2(x,y)x}{Q(x)} - \frac{2(x,y)x}{Q(x)} + \frac{4(x,y)(x, \frac{x}{Q(x)})}{Q(x)} x = y - \frac{2(x,y)x}{Q(x)} - \frac{2(x,y)x}{Q(x)} + \frac{4(x,y)}{Q(x)} x = y$$

A nice property of reflections is given by the next theorem.

Theorem 2.2. *Let M be a non-degenerate quadratic space over a field k of characteristic $\neq 2$. Then the orthogonal group O_M is generated by reflections and SO_M is the subgroup of O_M whose elements can be written as the composition of an even number of reflections.*

Let p, q be non-negative integers. The quadratic space over $\mathbb{R}$, $\mathbb{R}^{p+q}$ with the quadratic form

$$x_1^2 + \ldots + x_p^2 - x_{p+1}^2 - \ldots - x_{p+q}^2$$

is denoted by $\mathbb{R}^{p,q}$. If (V, Q) is a finite dimensional quadratic space over $\mathbb{R}$, then there exist p, q such that V is isometric to $\mathbb{R}^{p,q}$. In this case we say that V is of type (p, q). Its orthogonal group is denoted by $O_V = O(p, q)$.

2.2 The Clifford algebra

Let (V, Q) be a finitely generated quadratic module over a commutative ring R. For an R-algebra A the center of A is

$$Z(A) = \{x \in A \mid xy = yx \ \forall \ y \in A\}$$

(the set of elements that commute with any element in A).

Consider the tensor algebra

$$T_V = R \oplus V \oplus (V \otimes_R V) \oplus (V \otimes_R V \otimes_R V) \oplus \dots$$

and let I_V be the two-sided ideal generated by $Q(v) - v \otimes v$ for all $v \in V$. Then the Clifford algebra of V is defined by

$$C_V = T_V / I_V$$

For brevity we denote an element $v_1 \otimes v_2 \otimes \dots \otimes v_m$ $(v_j \in V)$ by $v_1 v_2 \dots v_m$. Note that in the Clifford algebra of V we have by definition that for $u, v \in V \subset C_V$:

$$Q(v) - v^2 = 0 \iff Q(v) = v^2$$

$$uv + vu = (u+v)(u+v) - uu - vv = Q(u+v) - Q(u) - Q(v) = 2B(u,v)$$

In particular, when u and v are orthogonal, $uv = -vu$. Assume that V is free and that $v_1, \dots, v_n$ is a basis of V. Then those vectors generate C_V as an R-algebra and the elements

$$v_{i_1} v_{i_2} \dots v_{i_m} \qquad (1 \leq i_1 < \dots < i_m \leq n)$$

are a basis of C_V, so C_V is a free module of rank 2^n.

Now we give some examples of the Clifford algebras $C_{p,q}$ associated to the real quadratic space $\mathbb{R}^{p,q}$.

Example 2.3. When $p = 0, q = 1$, $\mathbb{R}^{0,1}$ is a one dimensional space and has as quadratic form associated $Q(x) = -x_1^2$. There exists an element v such that $Q(v) = -1$ and all the other elements in V are multiples of v. Therefore, in the Clifford algebra we only have elements of the form $a + bv$ where $a, b \in \mathbb{R}$ and v is such that $v^2 = -1$. Therefore, $C^{1,0} \cong \mathbb{C}$.

Example 2.4. When $p = 1, q = 1$, $\mathbb{R}^{1,1}$ is a two dimensional space and has as quadratic form associated $Q(x) = x_1^2 - x_2^2$. There exist two elements $v_1 = (1,0), v_2 = (0,1)$ such that $Q(v_1) = 1, Q(v_2) = -1$ and $B(v_1, v_2) = 0$. All other elements in V are a linear combination of v_1, v_2. Therefore, in the Clifford algebra we have elements of the form $a + bv_1 + cv_2 + dv_1v_2$ where $a, b, c, d \in \mathbb{R}$ (that's true because we can always express elements in V as linear combinations of v_1 and v_2 and reduce all terms that contain a v_1^2 or v_2^2 using the relation $Q(v) = v^2$). Identifying

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad v_1 \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad v_2 \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad v_1v_2 \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

we have that those for matrices span $M_2(\mathbb{R})$ and

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = - \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

since $v_1^2 = 1$, $v_2^2 = -1$ and $v_1v_2 = -v_2v_1$ the identification is well defined. And since those 4 matrices span $M_2(\mathbb{R})$, we have $C^{1,1} \cong M_2(\mathbb{R})$.

Similarly it can be shown that $C^{0,2} \cong \mathbb{H}$ (the Hamilton quaternion algebra).

We define the even Clifford algebra of V to be the R-subalgebra generated by products of an even number of vectors in our basis. It is denoted by C_V^0. Note that the definition makes sense as the relation $Q(v) = v^2$ involves an even number of vectors and it is a subalgebra since the product of two elements that are product of an even number of vectors, is also an element consisting of an even number of vectors. If we denote by C_V^1 the R-submodule generated by the elements that are products of an odd number of vectors of the basis (which is not a subalgebra as the product of two elements in C_V^1 lies on C_V^0), then we have the following decomposition:

$$C_V = C_V^0 \oplus C_V^1$$

We can give another characterization of C_V^0 and C_V^1. Consider the isometry σ of V defined by $\sigma(v) = -v$ (multiplication by -1). Then it induces an algebra automorphism that agrees with σ on $V \subset C_V$ called the canonical automorphism $J : C_V \to C_V$ such that

$$C_V^0 = \{x \in C_V \mid J(x) = x\} \qquad C_V^1 = \{x \in C_V \mid J(x) = -x\}$$

There is also another automorphism called the canonical involution and is defined by ${}^t : C_V \to C_V$ such that $(v_1 v_2 \dots v_m)^t = v_m v_{m-1} \dots v_2 v_1$ where $v_1, v_2 \dots v_m \in V$. In $R \oplus V$ it is the identity. Using this automorphism we can define the Clifford norm

$$N : C_V \to C_V, N(x) = x^t x$$

When $x \in V$, it coincides with $Q(x)$ so it is an extension of the quadratic form. In general it is not multiplicative.

Now we will compute the center of Clifford algebra and of the even Clifford algebra, but we will need the following lemma.

Lemma 2.5. *Let $A, B \subset \{1, 2, \dots, n\}$ and let $v_A = \prod_{j \in A} v_j$ where the product over the elements is taken in increasing order of the indices (analogously with v_B). Then $v_A v_B = (-1)^{|A||B| - |A \cap B|} v_B v_A$.*

Proof. Recall that we have $v_i v_j = -v_j v_i$ if $i \neq j$ and obviously $v_i v_j = v_j v_i$ if $i = j$. Let $A = \{i_1, i_2, \dots, i_r\}$ and $B = \{j_1, j_2, \dots, j_s\}$. Then we start swapping the elements with indices in A with all the elements with indices in B, starting with i_r, and finishing with i_1. Each time we do a swap there is a change of sign unless we are swapping two elements with the same index. Therefore we have $|A||B| - |A \cap B|$ sign changes as there are $|A||B|$ swaps, $|A \cap B|$ of which don't affect the sign. □

Write $\delta = v_1 v_2 \dots v_n$, then we have:

Theorem 2.6. *The center of C_V is*

$$Z(C_V) = \begin{cases} k \textit{ for even } n \\ k + k\delta \textit{ for odd } n \end{cases}$$

The center of C_V^0 is

$$Z(C_V^0) = \begin{cases} k + k\delta \textit{ for even } n \\ k \textit{ for odd } n \end{cases}$$

Proof. Let's find first the center of C_V. Clearly $k \subset Z(C_V)$. Now let v_A be an element different from δ and 1. Then there exists $i \in A$ and $j \notin A$, so consider $B = \{i, j\}$ for those indices. Then, $|A \cap B| = 1$ and hence $|A||B| - |A \cap B|$ is odd. So we have $v_A v_B = -v_B v_A$ (by the previous lemma) and therefore $v_A \notin Z(C_V)$. When n is odd, for any A we have that for $B = \{1, 2, \ldots, n\}$, $|A \cap B| = |A|$, so $|A||B| - |A \cap B| = |A||B| - |A| = |A|(|B| - 1)$ which is even. Therefore, $v_A v_B = v_B v_A$ for any A, and $k\delta \subset Z(C_V)$. Note that if we have a linear combination $\sum \lambda_A v_A \in Z(C_V)$, every term in the sum must also be in the center, so we are done with the first part.

For $Z(C_V^0)$, note that $k \subset Z(C_V^0)$ trivially. If n is even, for any A, we have that for $B = \{1, 2, \ldots, n\}$ $v_A v_B = v_B v_A$ since $|A||B| - |A \cap B| = |A||B| - |A| = |A|(|B| - 1)$ is even ($|A|$ must be even if $v_A \in C_V^0$) Obviously, $\delta \notin Z(C_V^0)$ for odd n because $\delta \notin C_V^0$. We can use the same reasoning as before to see that $Z(C_V^0) \subset k + k\delta$ (no other element is in the center). Let v_A be defined as before for some non-empty A such that $|A|$ is even and $v_A \neq \delta, v_A \neq 1$, and let $B = \{i, j\}$ for $i \in A$, $j \notin A$. Then, $v_A v_B = -v_B v_A$ because $|A||B| - |A \cap B| = |A||B| - 1$ is odd.

□

Example 2.7. Assume that $n = 4$ and that v_1, v_2, v_3, v_4 is an orthogonal basis of V and put $q_j = Q(v_j) \in k^*$ for $j = 1, 2, 3, 4$. Then by the previous theorem, the center of the even Clifford algebra is $k + k\delta$ and

$$C_V^0 = Z + Zv_1v_2 + Zv_2v_3 + Zv_1v_3.$$

Since $(v_1v_2)^2 = -q_1q_2$, $(v_2v_3)^2 = -q_2q_3$ $(v_1v_3)^2 = -1$ and $(v_1v_2)(v_2v_3) = q_2(v_1v_3) = -(v_2v_3)(v_1v_2)$, C_V^0 is isomorphic to the quaternion algebra $(-q_1q_2, -q_2q_3)$ over $\mathbb{Z}$. The conjugation in the quaternion algebra is identified with the canonical involution and the norm with the Clifford norm.

2.2.1 The Spin group

The setting is the same as before, R is a commutative ring with unity 1 and (V, Q) is a finitely generated quadratic module over R. The Clifford group CG_V of V is defined to be

$$\mathrm{CG}_V = \{x \in C_V \mid x \text{ is invertible and } xVJ(x)^{-1} = V\}$$

Note that it is a group since $1 \in \mathrm{CG}_V$, for $x, y \in \mathrm{CG}_V$ we have $xyV = xVJ(y) = VJ(x)J(y) = VJ(xy)$ so $xy \in \mathrm{CG}_V$ and $x \in \mathrm{CG}_V \iff xVJ(x)^{-1} = V \iff V = x^{-1}VJ(x) = x^{-1}VJ(x^{-1})^{-1} \iff x^{-1} \in \mathrm{CG}_V$. For every $x \in \mathrm{CG}_V$ we can define the application $\alpha_x(v) = xvJ(x)^{-1}$. By the definition of CG_V, it is an automorphism of V. We have a linear representation from CG_V to $\mathrm{Aut}(V)$ called the vector representation that maps $x \mapsto \alpha_x$. Note that the involution $x \mapsto x^t$ takes CG_V to itself, since $xV = VJ(x) \iff (xV)^t = (VJ(x))^t \iff Vx^t = J(x^t)V \iff J(Vx^t) = J(J(x^t)V) \iff -VJ(x^t) = -x^tV \iff x^tVJ(x^t)^{-1} = V$. Therefore, for an $x \in \mathrm{CG}_V$, we have $N(x) \in \mathrm{CG}_V$.

Proposition 2.8. *The kernel of the vector representation $\alpha : \mathrm{CG}_V \to \mathrm{Aut}_k(V)$ is equal to k^*. The Clifford induces an homomorphism $\mathrm{CG}_V \to k^*$*

Proof. Clearly for $x \in k^*$, α_x is the identity, so $k^* \subset \ker(\alpha)$. Now let's show that if $x \in \ker(\alpha)$, $x \in k^*$. Write $x = x_0 + x_1$ where $x_0 \in C_V^0$ and $x_1 \in C_V^1$. We have that $xv = J(x)v$ for all $v \in V$. Therefore for all $v \in V$ we have

$$\begin{aligned} x_0 v &= v x_0 \\ x_1 v &= -v x_1 \end{aligned}$$

Since V generates the algebra C_V and x_0 commutes with every element in V, it commutes with every element of C_V and therefore is an invertible element of $Z(C_V)$ and C_V^0. Applying Theorem 2.6, we find that $x_0 \in k^*$. Now all we need is to prove that $x_1 = 0$. Going back to the notation that we introduced before, if $x_1 = \sum_{A \in I} \lambda_A v_A$ satisfies $x_1 v = -v x_1$, it must be true for all the terms in the sum. Now pick one v_A of the sum and let $v = v_i$ for some $i \in A$. The number of swaps to move $v = v_i$ from the back of $v_A v_i$ to the front $(v_i v_A)$, is odd, but in one of them the sign doesn't change as we are swapping v_i with itself. Therefore, there is an even number of sign changes, giving $v_A v_i = v_i v_A$ and contradicting $x_1 v = -v x_1$ unless no such A exists and $x_1 = 0$.

For the second part of the proposition, let $v \in V$ and $x \in \mathrm{CG}_V$. Then $w = \alpha_x(v) = xvJ(x)^{-1} \in V$, which means that $w = -J(w) = -J(w)^t$. Therefore, since the inverse and the two involutions commute, $xvJ(x)^{-1} = -J(xvJ(x)^{-1})^t = -(J(x)J(v)x^{-1})^t = -(x^t)^{-1}(-v^t)J(x)^t = (x^t)^{-1}vJ(x^t)$. From $xvJ(x)^{-1} = (x^t)^{-1}vJ(x^t)$ we get $x^t xv = vJ(x^t)J(x) \iff N(x)v = vJ(N(x))$, so $N(x) \in ker(\alpha) = k^*$. Now it is direct that for $x, y \in \mathrm{CG}_V$, $N(xy) = (xy)^t xy = y^t x^t xy = y^t N(x) y = N(x) y^t y = N(x)N(y)$, so the norm is multiplicative for the Clifford group. □

Proposition 2.9. *Let $x \in \mathrm{CG}_V$. The automorphism $\alpha_x \in \mathrm{Aut}_R(V)$ is an isometry.*

Proof. Let $v \in V$, and $w = \alpha_x(v) = xvJ(x)^{-1}$. Since $x \in \mathrm{CG}_V$, $w \in V$, and the Clifford norm coincides with the quadratic form, so

$$Q(w) = N(w) = (xvJ(x)^{-1})^t(xvJ(x)^{-1}) = J(x^{-1})^t v^t x^t xvJ(x^{-1}) = J(x^{-1})^t v^t N(x) vJ(x^{-1}) =$$
$$= N(x)J(x^{-1})^t N(v) J(x^{-1}) = N(x)N(J(x^{-1}))N(v) = Q(v)$$

where we used that $N(x), N(v) \in k$, so it commutes with the elements of the Clifford algebra, that $N(y) = N(J(y))$ and the multiplicativity of the norm that we saw in the previous lemma. To see $N(y) = N(J(y))$, just recall that in the previous proposition we saw that $N(x)v = vJ(N(x)) \iff N(x)vJ(N(x))^{-1} = v$. □

Using the last two propositions we see that vector representation defines an homomorphism $\alpha : \mathrm{CG}_V \mapsto O_V$. Furthermore, for $x \in \mathrm{CG}_V \cap V$, $\alpha_x = \tau_x$, the reflection in the hyperplane $x^\perp$.

Definition 2.10. For a quadratic space V we define the general spin group by

$$\mathrm{GSpin}_V = \mathrm{CG}_V \cap C_V^0$$

and the Spin group by

$$\mathrm{Spin}_V = \{x \in \mathrm{GSpin}_V \mid N(x) = 1\}$$

Under the hypothesis of Theorem 2.2 the vector representation $\alpha : \mathrm{CG}_V \mapsto O_V$ is surjective. Its kernel is k^* by Lemma 2.8, CG_V and GSpin_V are central extensions of O_V and SO_V, respectively

$$1 \longrightarrow k^* \longrightarrow \mathrm{CG}_V \xrightarrow{\alpha} O_V \longrightarrow 1$$

$$1 \longrightarrow k^* \longrightarrow \mathrm{GSpin}_V \xrightarrow{\alpha} SO_V \longrightarrow 1$$

According to Lemma 2.8, the Clifford norm defines an homomorphism $\mathrm{CG}_V \to k^*$, which induces a homomorphism

$$\theta : O_V \to k^*/(k^*)^2$$

called the spinor norm. It is defined by taking a section of the vector representation α from O_V to CG_V and then taking the Clifford norm on CG_V. Since the kernel of α is k^* (Lemma 2.8) the section is defined up to a scalar in k^*, and the norm up to an element of (k^*), so it is well-defined. For a reflection τ_x, $\theta(\tau_x) = x$ (recall that $\tau_x = \alpha_x$ and $N(x) = Q(x)$ for $x \in V$. So we have another exact sequence

$$1 \longrightarrow \{\pm 1\} \longrightarrow \mathrm{Spin}_V \xrightarrow{\alpha} \mathrm{SO}_V \xrightarrow{\theta} k^*/(k^*)^2$$

Proposition 2.11. *Assume that* $\dim(V) \leq 4$. *Then*

$$\mathrm{GSpin}_V = \{x \in C_V^0 \mid N(x) \in k^*\} \tag{2.1}$$

$$\mathrm{Spin}_V = \{x \in C_V^0 \mid N(x) = 1\} \tag{2.2}$$

Proof. By definition it is clear that the second equality follows from the first one. It is also clear that $\mathrm{GSpin}_V \subset \{x \in C_V^0 \mid N(x) \in k^*\}$ since for $x \in \mathrm{GSpin}_V$ we have that $x \in \mathrm{CG}_V \cap C_V^0$, so $N(x) \in k^*$ and $x \in C_V^0$. Now let's see the converse. Assume that $x \in C_V^0$ and $N(x) \in k^*$, we need to show that $x \in \mathrm{CG}_V$. $\frac{1}{N(x)}x^t$ is the inverse of x, so x is invertible, so we just need to show that $xVJ(x)^{-1} \in V$, but since $x \in C_V^0$, $J(x) = x$. Let $v \in V$ and $w = xvx^{-1} \in C_V^1$ (the product of an element in C_V^0 and one in C_V^1 is in C_V^1). The fact that $\dim(V) \leq 4$ implies that if $x \in C_V^1$, we have $x \in V \iff x^t = x$. This is true because for an element in $y \in V \oplus V \oplus V$ we have $y^t = -y$. That's true because if v_1, v_2, v_3, v_4 are an orthogonal basis and i, j, k are pairwise different, $(v_i v_j v_k)^t = v_k v_j v_i = v_i v_k v_j = -v_i v_j v_k$. Therefore, to show $w \in V$, we just to show $w = w^t \iff xvx^{-1} = (x^t)^{-1} v x^t \iff N(x)v = vN(x)$ which is true since $N(x) \in k^*$. □

2.2.2 Quadratic space of dimension 4

Now we focus on the cases where (V, Q) is a rational quadratic space of dimension 4 over the field k. We put $q_i = Q(v_i) \in k^*$ where v_1, v_2, v_3, v_4 is an orthogonal basis of V. By what we previously saw, Spin_V is the group of elements of norm 1 in the quaternion algebra $(-q_1 q_2, -q_2 q_3)$ over $Z(C_V^0) = k + k\delta$. Our goal is to describe the vector representation of Spin_V (that is SO_V) just in terms of C_V^0. This can be done by identifying V with an isometric copy $\tilde{V}$ inside C_V^0. The vector representation on V translates to a new vector representation in $\tilde{V}$ that we'll call the twisted vector representation.

Lemma 2.12. *Let $v_0 \in V$ with $q_0 = Q(v_0) \neq 0$ and σ is the adjoint automorphism associated to v_0, $x^\sigma = v_0 x v_0^{-1}$ for $x \in C_V^0$. Then*

1. *$\delta^\sigma = -\delta$*
2. *The fixed algebra of σ in C_V^0 is a quaternion algebra B_0 over k such that $C_V^0 = B_0 \otimes_k Z$.*

Proof. Up to multiplication by an element in k^*, δ does not depend on the chosen basis, so rechoosing our basis, we can assume that $v_0 = v_4$ (by picking v_0 as an element of the basis and extending it to an orthogonal basis. Then $\delta^\sigma = v_0 \delta v_0^{-1} = v_0 v_1 v_2 v_3 v_0 v_0^{-1} = v_0 v_1 v_2 v_3 = -v_1 v_2 v_3 v_0 = -\delta$. For (ii), consider the basis of C_V^0

$$1, i = v_1 v_2, j = v_2 v_3, k = ij = q_2 v_1 v_3, \delta, \delta i, \delta j, \delta k$$

Then, $1^\sigma = 1$, $i^\sigma = v_0 v_1 v_2 v_0^{-1} = v_0 v_0^{-1} v_1 v_2 = i$ and similarly for j and k, proving that B_0 is spanned by $1, i, j, k$ and so it is the quaternion algebra $(-q_1 q_2, -q_2 q_3)$. It is also clear that $B = B_0 + \delta B_0 = B_0 \otimes_k Z$. □

Therefore, on the center $Z(C_V^0) = k + k\delta$, the automorphism σ agrees with the conjugation in Z/k. Let

$$\widetilde{V} = \{x \in C_V^0 \mid x^t = x^\sigma\}$$

This is a quadratic space over k with the quadratic form

$$\widetilde{Q}(x) = q_0 \cdot x^\sigma x = q_0 \cdot N(x)$$

There is an action of the group Spin_V on $\widetilde{V}$. If $x \in \widetilde{V}$ and $g \in \mathrm{Spin}_V$, the action is defined by

$$x \mapsto \widetilde{\alpha}_g(x) := g x g^{-\sigma}$$

The action is well defined since

$$(gxg^{-\sigma})^t = (g^{-\sigma})^t x^t g^t = N(g)^{-1} g^\sigma x^\sigma g^t = g^\sigma x^\sigma g^{-1} = (gxg^{-\sigma})^\sigma$$

and the quadratic form is preserved by this action since

$$\widetilde{Q}(gxg^{-\sigma}) = (gxg^{-\sigma})^t (gxg^{-\sigma}) = (gxg^{-\sigma})^\sigma (gxg^{-\sigma}) = (g^\sigma x^\sigma g^{-1})(gxg^{-\sigma}) = g^\sigma (x^t x) g^{-\sigma} = \widetilde{Q}(x)$$

Lemma 2.13. *The assignment $x \mapsto x \cdot v_0$ defines an isometry of quadratic spaces*

$$(\widetilde{V}, \widetilde{Q}) \to (V, Q)$$

which is compatible with the actions of Spin_V.

Proof. Using the basis of Lemma 2.12 for C_V^0, $\widetilde{V}$ is spanned by $1, \delta i, \delta j, \delta k$, which means that the map $x \mapsto x \cdot v_0$ is a linear isomorphism between $\widetilde{V}$ and V. Now, if we pick $x \in \widetilde{V}$,

$$Q(x \cdot v_0) = (x \cdot v_0)^2 = x v_0 \cdot x v_0 = x x^\sigma v_0^2 = q_0 N(x) = \widetilde{Q}(x)$$

and the map is an isometry. Note that

$$\widetilde{\alpha}_g(x) \cdot v_0 = g x g^{-\sigma} v_0 = g x v_0 g^{-1} v_0^{-1} v_0 = g(x v_0) g^{-1}$$

so the isometry is compatible with the action of Spin_V on each of V and $\widetilde{V}$. □

2.3 Rational Quadratic spaces of type (2,n)

Let V be a non-degenerate quadratic space over $\mathbb{Q}$ and Q the quadratic form associated to it. As a quadratic space over $\mathbb{R}$ ($V(\mathbb{R}) = V \otimes_{\mathbb{Q}} \mathbb{R}$) it is isometric to $\mathbb{R}^{p,q}$ for some pair of integers (p, q) called the type of V. The orthogonal group $\mathrm{O}_V(\mathbb{R})$ contains a maximal compact subgroup K such that $\mathrm{O}_V(\mathbb{R})/K$ is a symmetric space. When $p = 2$ or $q = 2$ it has a complex structure (it is hermitian). From now on, let's assume that V has type $(2, n)$ (we make this assumption but everything would work the same for the case $(n, 2)$ if we replace Q by $-Q$) and study dome realizations of this hermitian symmetric domain.

2.3.1 Grassmannian model

Here we consider the two dimensional subspaces of $V(\mathbb{R})$ on which the quadratic form is positive definite.

$$\mathrm{Gr}(V) = \{v \subset V(\mathbb{R}) \mid \dim v = 2, \quad Q(x) > 0 \ \forall x \in v\}$$

$\mathrm{O}_V(\mathbb{R})$ acts transitively on $\mathrm{Gr}(V)$ as for any $v_1, v_2 \in \mathrm{Gr}(V)$, by Witt's theorem, we can extend the isometry between v_1 and v_2 to an isometry between $V(\mathbb{R})$ and $V(\mathbb{R})$. Now, fix $v_0 \in \mathrm{Gr}(V)$ and consider the stabilizer K_{v_0} of v_0 in $\mathrm{O}_V(\mathbb{R})$. It preserves v_0, so it also preserves the orthogonal complement, which means that choosing a basis, $K_{v_0} \cong \mathrm{O}(2) \times \mathrm{O}(n)$. It can be seen that it is a maximal compact subgroup of $\mathrm{O}_V(\mathbb{R})$. It is compact for being the product of the two compact groups $\mathrm{O}(2)$, $\mathrm{O}(n)$ (groups of the type $\mathrm{O}(m)$ are bounded because if $M \in \mathrm{O}(m)$ is written in a orthogonal basis, we have that the norm of the columns is equal, up to sign, to the value of the quadratic form on a element of the base and hence bounded). The maximality of K_{v_0} is not hard to prove, and $\mathrm{Gr}(V) \cong \mathrm{O}_V(\mathbb{R})/K_{v_0}$ is a realization of the hermitian symmetric space. However, with this description we don't see the complex structure of $\mathrm{O}_V(\mathbb{R})/K_{v_0}$.

2.3.2 Projective model

Consider the projective space

$$P(V(\mathbb{C})) = V(\mathbb{C})\backslash\{0\})/\mathbb{C}^*$$

The zero quadric

$$\mathcal{N} = \{[Z] \in P(V(\mathbb{C})) \mid (Z, Z) = 0\}$$

is a closed algebraic subvariety of dimension n ($P(V(\mathbb{C}))$ has dimension $n + 1$, since $V(\mathbb{C})$ has dimension $n + 2$ and there is one restriction).

The subset of $\mathcal{N}$ defined by

$$\mathcal{K} = \{[Z] \in P(V(\mathbb{C})) \mid (Z, Z) = 0, (Z, \overline{Z}) > 0\}$$

consists of two connected components. Notice that it is well defined, as the definition doesn't depend on the representative of $P(V(\mathbb{C}))$ that we choose. If we write $Z = X + iY$ for $X, Y \in \mathbb{R}$, then the above conditions can be written as

$$[Z] \in \mathcal{N} \iff (X + iY, X + iY) = (X, X) + 2i(X, Y) - (Y, Y) = 0 \iff$$

$$\iff (X,Y)=0 \text{ and } (X,X)=(Y,Y)$$

$$[Z]\in\mathcal{K} \iff [Z]\in\mathcal{N} \text{ and } (X+iY,X-iY)=(X,X)+(Y,Y)+2i(X,Y)>0 \iff$$

$$\iff (X,Y)=0 \text{ and } (X,X)=(Y,Y)>0$$

The action of $\mathrm{O}_V(\mathbb{R})$ on $\mathcal{K}$ is transitive as we can always choose and element that maps $X_1\mapsto X_2$ and $Y_1\mapsto Y_2$ by using Witt's extension Theorem, and it will map $[Z_1]=[X_1+iY_1]$ to $[Z_2]=[X_2+iY_2]$. Consider the subgroup of $\mathrm{O}_V(\mathbb{R})$ of elements whose spinor norm equals the determinant and denoted by $\mathrm{O}_V^+(\mathbb{R})$. Those elements preserve the orientation of positive definite planes, so $\mathrm{O}_V^+(\mathbb{R})$ preserves the 2 components of $\mathcal{K}$ and $\mathrm{O}_V\backslash\mathrm{O}_V^+(\mathbb{R})$ interchanges them. Fix one of the two components and call it $\mathcal{K}^+$ and as we just did for a $Z\in V(\mathbb{C})$ consider the decomposition into its real and imaginary part so that $Z=X+iY$ where $X,Y\in V(\mathbb{R})$. Using this decomposition we can find an isomorphism between $\mathcal{K}^+$ and $\mathrm{Gr}(V)$ in the following way.

Lemma 2.14. *The assignment $[Z]\mapsto v(Z):=\mathbb{R}X+\mathbb{R}Y$ defines a real analytic isomorphism $\mathcal{K}^+\mapsto\mathrm{Gr}(V)$.*

Proof. The assignment is well defined, since if we have two representatives $Z_1,Z_2\in[Z]$, it means that $Z_1=X_1+iY_1$ and $Z_2=X_2+iY_2=(X_1+iY_1)(a+bi)=(aX_1-bY_1)+i(bX_1+aY_1)$. But then $v(Z_2)=\mathbb{R}(aX_1-bY_1)+\mathbb{R}(bX_1+aY_1)=\mathbb{R}X+\mathbb{R}Y=v(Z_1)$ (it's just a change of basis for the plane). Before we deduced that $[Z]\in\mathcal{K}$ implies (X,Y) and $(X,X)=(Y,Y)>0$. Therefore, $v(Z)=\mathbb{R}X+\mathbb{R}Y\in\mathrm{Gr}(V)$ since it is a positive definite two dimensional space. Conversely, given $v\in\mathrm{Gr}(V)$, either $[X+iY]$ or $[Y-iX]$ are in $\mathcal{K}$, so we can choose a suitably oriented orthogonal basis X,Y and it gives a unique $[Z]=[X+iY]\in\mathcal{K}^+$. □

Now we can see the complex structure, but it is not the direct analogue of the upper half plane, the standard model for the hermitian symmetric space for $\mathrm{SL}_2(\mathbb{R})$.

2.3.3 Tube domain model

Pick an isotropic vector e_1 (i.e. $(e_1,e_1)=0$) and $e_2\in V$ with $(e_1,e_2)=1$. Let $W=V\cap e_1^\perp\cap e_2^\perp$. Then W has type $(1,n-1)$ and $V=W\oplus\mathbb{Q}e_1\oplus\mathbb{Q}e_2$. For a $Z\in V(\mathbb{C})$ we can write it as $Z=z+ae_2+be_1$ with $z\in W(\mathbb{C})$ and $a,b\in\mathbb{C}$ and we will denote it by $Z=(z,a,b)$. Consider the domain

$$\mathcal{H}=\{z\in W(\mathbb{C})\mid Q(\Im(z))>0\}$$

Lemma 2.15. *The assignment*

$$z\mapsto\psi(z):=[(z,1,\frac{-Q(z)-Q(e_2)}{2}]$$

defines an holomorphic map $\psi:\mathcal{H}\to\mathcal{K}$.

Proof. If $z \in \mathcal{H}$, then $\psi(z) = [z + e_2 - \frac{(Q(z)+Q(e_2))}{2} e_1]$ satisfies $(\psi(z), \psi(z)) = (z, z) + (e_2, e_2) - (Q(z) + Q(e_2))(e_2, e_1) = Q(z) + Q(e_2) - (Q(z) + Q(e_2)) = 0$ (recall that $(z, e_2) = (z, e_1) = 0$) and $(\psi(z), \overline{\psi(z)}) = (z, \overline{z}) + (e_2, e_2) - (Q(z) + Q(e_2))(e_1, e_2) - (\overline{(Q(z) + Q(e_2))}(e_1, e_2) = (z, \overline{z}) + Q(e_2) - \frac{1}{2}(Q(z) + \overline{Q(z)} + Q(e_2) + \overline{Q(e_2)}) = (z, \overline{z}) + Q(e_2) - \frac{1}{2}(Q(z) + Q(\overline{z}) + Q(e_2) + Q(e_2)) = (z, \overline{z}) - \frac{1}{2}((z, z) + (\overline{z}, \overline{z}))) = -\frac{1}{2}(z - \overline{z}, z - \overline{z}) = -\frac{1}{2}Q(i\Im(z)) = \frac{1}{2}Q(\Im(z)) > 0$, so $\psi(z) \in \mathcal{H}$.

Conversely, if $[Z] \in \mathcal{K}$ and we write $Z = X + iY$, since X, Y generate a two dimensional positive definite space, we must have $(Z, e_1) \neq 0$ (otherwise e_1 would belong to a negative definite subspace, contradicting the fact that is isotropic). Therefore, there exist a representative of $[Z]$ of the form $(z, 1, b)$. From $Q(Z) = 0$, we get $(z+e_2+be_1, z+e_2+be_1) = 0 \iff (z, z)+(e_2, e_2)+2b(e_2, e_1) = 0 \iff Q(z)+Q(e_2)+2b = 0 \iff b = -\frac{Q(z)+Q(e_2)}{2}$. And therefore, $[Z]$ is of the form $(z, 1, -\frac{Q(z)+Q(e_2)}{2})$, to see that $z \in \mathcal{H}$, we can use $(z + e_2 + -\frac{Q(z)+Q(e_2)}{2} e_1, \overline{z + e_2 + -\frac{Q(z)+Q(e_2)}{2} e_1}) > 0 \iff (z, \overline{z}) + (e_2, e_2) - \frac{1}{2}(Q(z) + Q(e_2) + Q(\overline{Z} + Q(e_2)) > 0 \iff (z, \overline{z}) - \frac{1}{2}((z, z) + (\overline{z}, \overline{z})) > 0 \iff -\frac{1}{2}(z - \overline{z}, z - \overline{z}) > 0 \iff -Q(z - \overline{z}) > 0 \iff -Q(2i\Im(z)) > 0 \iff Q(\Im(z)) > 0$.

The holomorphicity follows from the fact that it is defined by polynomial equations. □

If we view the domain $\mathcal{H} \subset W(\mathbb{C})$ as the positive norm vectors of $W(\mathbb{R})$, it has two connected components corresponding to the two cones in the Lorentzian space $W(\mathbb{R})$. We can identify the one to which $\mathcal{K}^+$ is mapped when applying ψ as $\mathcal{H}^+$. When $n = 1$, then $\mathcal{H}$ consists of those elements $z \in \mathbb{C}$ such that $\Im(z)^2 > 0$ (those with $\Im(z) \neq 0$), so $\mathcal{H}$ can be identified with $\mathbb{C} - \mathbb{R}$ and $\mathcal{H}^+$ with the upper half plane $\mathbb{H}$. We will see that for $n = 2$, we can identify $\mathcal{H}^+$ with $\mathbb{H}^2$.

2.3.4 Lattices

We still consider a non-degenerate quadratic space (V, Q) over $\mathbb{Q}$ of type $(2, n)$.

Definition 2.16. A lattice in V is a Z-module $L \subset V$ such that $V = L \otimes_{\mathbb{Z}} \mathbb{Q}$.

A lattice is integral if the bilinear form associated to Q is integral on L ($(x, y) \in \mathbb{Z}$ for $x, y \in L$). Furthermore, it is even if the bilinear form takes even values on L. The dual lattice $L^\vee$ is defined to be

$$L^\vee = \{x \in V \mid (x, y) \in \mathbb{Z} \text{ for all } y \in L\}$$

A lattice is integral if and only if $L \subset L^\vee$ and in this case the quotient is a finite abelian group. Assume now that L is an even lattice. Then $\mathrm{O}_L \subset \mathrm{O}_V(\mathbb{R}) \cong \mathrm{O}(2, n)$ is a discrete subgroup. Let $\mathit{\Gamma} \subset \mathrm{O}_L \cap \mathrm{O}_V^+(\mathbb{R})$ be a subgroup of finite index. Then $\mathit{\Gamma}$ acts properly discontinuously on $\mathrm{Gr}(V), \mathcal{K}^+$ and $\mathcal{H}^+$. We consider the quotient $Y(\mathit{\Gamma}) = \mathit{\Gamma} \backslash \mathcal{H}^+$ similarly to the case of Hilbert modular surfaces and it is a normal complex space which is compact if and only if V is anisotropic. If it is not compact, it can be compactified by adding some boundary points.

2.4 The Hilbert Modular Group as an Orthogonal group

Here we discuss the isomorphism that relates the Hilbert modular group to an orthogonal group of type $(2,2)$, which is one the main points of the chapter.

Let $D \in \mathbb{Q}^* \setminus \mathbb{Q}^2$ and let $F = \mathbb{Q}(\sqrt{D})$. Consider the four dimensional $\mathbb{Q}$-space $V = \mathbb{Q} \oplus \mathbb{Q} \oplus F$ (F is a two dimensional $\mathbb{Q}$-space) with the quadratic form $Q(a,b,\nu) = \nu\nu' - ab$ where ν' is the conjugate of ν. Note that by writing $\nu = x + y\sqrt{D}$ and $a = z + t, b = z - t$, we get $Q(a,b,\nu) = x^2 - Dy^2 - z^2 + t^2$, so (V,Q) is a rational quadratic space of type $(2,2)$ if $D > 0$ and of type $(3,1)$ if $D < 0$. The bilinear form associated to Q is $B(x_1,x_2) = \frac{1}{2}(\nu_1\nu_2' + \nu_1'\nu_2 - b_1a_2 - a_1b_2)$ where $x_j = (a_j, b_j, \nu_j)$. Consider the orthogonal basis of (V,Q)

$$v_1 = (1,1,0) \qquad v_2 = (1,-1,0)$$

$$v_3 = (0,0,1) \qquad v_4 = (0,0,\sqrt{D})$$

Then we have $Q(v_1) = -1, Q(v_2) = Q(v_3) = 1, Q(v_4) = -D$. therefore $\delta = v_1v_2v_3v_4$ and $\delta^2 = v_1v_2v_3v_4v_1v_2v_3v_4 = v_1v_2v_3v_4v_4v_3v_2v_1 = Q(v_1)Q(v_2)Q(v_3)Q(v_4) = D$. From Theorem 2.6 we know that the center of the even Clifford algebra of V is $Z(C_V^0) = \mathbb{Q} + \mathbb{Q}\delta \cong F$ and Example 2.7 tells us that

$$C_V^0 = Z + Zv_1v_2 + Zv_2v_3 + Zv_1v_3$$

is isomorphic to the $(1,-1)$ quaternion algebra over F, also known as the split quaternion algebra $M_2(F)$ over F. The isomorphism is given by the following assignements:

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad v_1v_2 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad v_2v_3 \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad v_1v_3 \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

so the element $\dfrac{a+d}{2} + \dfrac{a-d}{2}v_1v_2 + \dfrac{b-c}{2}v_2v_3 + \dfrac{b+c}{2}v_1v_3$ in C_V^0 is assigned to $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(F)$. The isomorphism between $Z = \mathbb{Q} + \mathbb{Q}\delta$ and F is realized by $x + y\delta \mapsto x + y\sqrt{D}$.

The operation of canonical involution on C_V^0 corresponds to the conjugation

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^* = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

in $M_2(F)$ since $(\frac{a+d}{2} + \frac{a-d}{2}v_1v_2 + \frac{b-c}{2}v_2v_3 + \frac{b+c}{2}v_1v_3)^t = \frac{a+d}{2} + \frac{d-a}{2}v_1v_2 + \frac{c-b}{2}v_2v_3 + \frac{-b-c}{2}v_1v_3$ which corresponds to

$$\begin{pmatrix} \dfrac{a+d+d-a}{2} & \dfrac{c-b-b-c}{2} \\ \dfrac{b-c-b-c}{2} & \dfrac{a-d+a+d}{2} \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

The Clifford norm on C_V^0 corresponds to the determinant in $M_2(F)$ since

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^* \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix}$$

This means that by Proposition 2.11 Spin_V can be identified with the matrices in $M_2(F)$ of determinant 1, that is with $\mathrm{SL}_2(F)$. So we have $\mathrm{Spin}_V \cong \mathrm{SL}_2(F)$. Then $\mathit{\Gamma}_F = \mathrm{SL}_2(\mathcal{O}_F)$ and other commensurable groups can be viewed as arithmetic subgroups of Spin_V. In fact, in the case of $\mathrm{SL}_2(\mathcal{O}_F)$, it turns out that $\mathit{\Gamma}_F = \mathrm{Spin}_L$ where L is the lattice $\mathbb{Z} \oplus \mathbb{Z} \oplus \mathcal{O}_F \subset V$.

The next step is to describe the vector representation (how Spin_V acts on V) using Lemmas 2.12 and 2.13. Let σ be the automorphism of C_V^0 associated to the basis vector v_1, that is $x^\sigma = v_1 x v_1^{-1}$ for $x \in C_V^0$. Then $\delta^\sigma = -\delta$, and on F we have that σ agrees with conjugation in $F/\mathbb{Q}$. On $M_2(F)$ the action of σ is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix}^\sigma = \begin{pmatrix} d' & -c' \\ -b' & a \end{pmatrix}$$

Consider now

$$\widetilde{V} = \{X \in M_2(F) \mid X^* = X^\sigma\} = \{X \in M_2(F) \mid X^t = X'\} = \left\{ \begin{pmatrix} a & \nu' \\ \nu & b \end{pmatrix} \mid a, b \in \mathbb{Q}, \nu \in F \right\}$$

with the quadratic form

$$\widetilde{Q}(X) = -X^\sigma \cdot X = -\begin{pmatrix} b & -\nu' \\ -\nu & a \end{pmatrix} \begin{pmatrix} a & \nu' \\ \nu & b \end{pmatrix} = -\begin{pmatrix} ab - \nu\nu' & 0 \\ 0 & ab - \nu\nu' \end{pmatrix} = -\det(X)$$

The bilinear form associated is

$$\widetilde{B}(X_1, X_2) = -\mathrm{tr}(X_1 X_2^*)$$

and the Spin group acts isometrically on $\widetilde{V}$ via

$$X \mapsto g \cdot X := gXg^{-\sigma} = gX(g')^t \tag{2.3}$$

In this case, the isometry of Lemma 2.13 is given by

$$\begin{pmatrix} a & \nu' \\ \nu & b \end{pmatrix} \mapsto (a, b, \nu)$$

since (writing $\nu = x + y\delta$)

$$\left(\frac{a+b}{2} + \frac{a-b}{2} v_1 v_2 + \frac{\nu' - \nu}{2} v_2 v_3 + \frac{\nu + \nu'}{2} v_1 v_3\right) \cdot v_1 = \frac{a+b}{2} v_1 + \frac{a-b}{2} v_2 + \frac{\nu' - \nu}{2} v_2 v_3 v_1 + \frac{\nu + \nu'}{2} v_3 =$$

$$= \frac{a+b}{2} v_1 + \frac{a-b}{2} v_2 - y\delta v_2 v_3 v_1 + \frac{\nu + \nu'}{2} v_3 = \frac{a+b}{2} v_1 + \frac{a-b}{2} v_2 + y v_4 + \frac{\nu + \nu'}{2} v_3 =$$

$$= \left(\frac{a+b}{2}, \frac{a+b}{2}, 0\right) + \left(\frac{a-b}{2}, \frac{b-a}{2}, 0\right) + (0, 0, y\sqrt{D}) + \left(0, 0, \frac{\nu + \nu'}{2}\right) = (a, b, \nu)$$

Let's now describe the symmetric space corresponding to $\mathrm{O}_{\widetilde{V}}$. $\widetilde{V}(\mathbb{C}) = M_2(\mathbb{C})$ and the subset of the zero quadric $\mathcal{K}$ defined in subsection 2.3.2 is

$$\mathcal{K} = \{[Z] \in P(M_2(\mathbb{C})) \mid \det(Z) = 0, -\mathrm{tr}(Z\overline{Z}^*) > 0\}$$

The vectors $e_1 = (\begin{smallmatrix}-1 & 0\\ 0 & 0\end{smallmatrix})$ and $e_2 = (\begin{smallmatrix}0 & 0\\ 0 & 1\end{smallmatrix})$ are isotropic (determinant 0), $(e_1, e_2) = 1$ and put $W = \widetilde{V} \cap e_1^{\perp} \cap e_2^{\perp}$ for the orthogonal complement (like we did with the tube domain model).

Note that if $X = (\begin{smallmatrix}x_1 & x_2\\ x_3 & x_4\end{smallmatrix}) \in W$, then $\widetilde{B}(X, \lambda e_1 + \mu e_2) = -\mathrm{tr}((\begin{smallmatrix}x_1 & x_2\\ x_3 & x_4\end{smallmatrix})(\begin{smallmatrix}\mu & 0\\ 0 & -\lambda\end{smallmatrix})) = -\mathrm{tr}((\begin{smallmatrix}\mu x_1 & -\lambda x_2\\ \mu x_3 & -\lambda x_4\end{smallmatrix})) = -\mu x_1 + \lambda x_4 = 0$ for all $\mu, \lambda \in \mathbb{C}$, so $x_1 = x_4 = 0$ and

$$W(\mathbb{C}) = \left\{\begin{pmatrix}0 & x_2\\ x_3 & 0\end{pmatrix} \mid x_2, x_3 \in \mathbb{C}\right\}$$

And for the tube domain, $H \cong \{(z_1, z_2) \in \mathbb{C}^2 \mid \Im(z_1)\Im(z_2) > 0\}$. For $z = (z_1, z_2) \in \mathbb{C}^2 \cong W(\mathbb{C})$ we put

$$M(z) = \begin{pmatrix}z_1z_2 & z_1\\ z_2 & 1\end{pmatrix} \in M_2(\mathbb{C})$$

Then $[M(z)] \in \mathcal{N}$ because $M(z)$ has determinant 0 and

$$[M(z)] \in \mathcal{K} \iff -\mathrm{tr}\left(\begin{pmatrix}z_1z_2 & z_1\\ z_2 & 1\end{pmatrix}\begin{pmatrix}\overline{z_1z_2} & \overline{z_1}\\ \overline{z_2} & 1\end{pmatrix}^*\right) = -\mathrm{tr}\left(\begin{pmatrix}z_1z_2 & z_1\\ z_2 & 1\end{pmatrix}\begin{pmatrix}1 & -\overline{z_1}\\ -\overline{z_2} & \overline{z_1z_2}\end{pmatrix}\right) > 0 \iff$$

$$\iff -(z_1z_2 - z_1\overline{z_2} - \overline{z_1}z_2 + \overline{z_1z_2}) > 0 \iff -(z_1 - \overline{z_1})(z_2 - \overline{z_2}) > 0 \iff -i\Im(z_1)i\Im(z_2) > 0 \iff$$
$$\iff \Im(z_1)\Im(z_2) > 0$$

Therefore the biholomorphic map $z \mapsto [M(z)]$ that we defined that takes $\mathbb{C}^2$ to the zero quadric $\mathcal{N}$, when it is restricted to the tube H it maps to $\mathcal{K}$. So the two components of H, $\{(z_1, z_2) \in \mathbb{C}^2 \mid \Im(z_1), \Im(z_2) > 0\} \cup \{(z_1, z_2) \in \mathbb{C}^2 \mid \Im(z_1), \Im(z_2) < 0\}$ can be identified with $\mathcal{K}$. We may identify the first of the two connected subsets with $\mathcal{K}^+$, which gives a biholomorphic map

$$\mathbb{H}^2 \to \mathcal{K}^+, \qquad z \mapsto [M(z)]$$

If we consider the action of $\mathrm{SL}_2(F)$, $X \mapsto g \cdot X$ on $\mathcal{K}^+$ (the one given in equation 2.3) and the usual action of $\mathrm{SL}_2(F)$ described in the first chapter, they commute with the biholomorphic map $z \mapsto [M(z)]$ by

$$\gamma \cdot M(z) = N(cz + d)M(\gamma z)$$

for $\gamma \in (\begin{smallmatrix}a & b\\ c & d\end{smallmatrix})$. This can be checked by computing both sides of the equation. For $\gamma \cdot M(z)$ we have:

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}z_1z_2 & z_1\\ z_2 & 1\end{pmatrix}\begin{pmatrix}a' & b'\\ c' & d'\end{pmatrix} = \begin{pmatrix}(az_1z_2 + bz_2)a' + (az_1 + b)b' & (az_1z_2 + bz_2)c' + (az_1 + b)d'\\ (cz_1z_2 + dz_2)a' + (cz_1 + d)b' & (cz_1z_2 + dz_2)c' + (cz_1 + d)d'\end{pmatrix}$$

And for $N(cz + d)M(\gamma z)$ we have:

$$N(cz{+}d)\begin{pmatrix} \dfrac{az_1+b}{cz_1+d}\dfrac{a'z_2+b'}{c'z_2+d'} & \dfrac{az_1+b}{cz_1+d} \\ \dfrac{a'z_2+b'}{c'z_2+d'} & 1 \end{pmatrix} = \begin{pmatrix} (az_1+b)(a'z_2+b') & (az_1+b)(c'z_2+d') \\ (a'z_2+b')(cz_1+d) & (cz_1+d)(c'z_2+d') \end{pmatrix}$$

Since both expressions are the same it is true that the action commutes with the map by $\gamma \cdot M(z) = N(cz+d)M(\gamma z)$ and that implies that modular forms of weight k like in definition 2.17 (we will see in the next section) can be identified with modular forms of parallel weight k from definition 1.19.

2.5 Modular forms for O(2,n)

Let V be a non-degenerate quadratic space over $\mathbb{Q}$ of type $(2,2)$, let L be an even lattice and $\mathit{\Gamma} \subset O_L \cap O_V^+(\mathbb{R})$. We denote by

$$\widetilde{K}^+ = \{Z \in V(\mathbb{C})\backslash\{0\} \mid [Z] \in K^+\}$$

the cone over $\mathcal{K}^+$.

Definition 2.17. Let $k \in \mathbb{Z}$, and let χ be a character for the group $\mathit{\Gamma}$. We say that a meromorphic function $F\colon \widetilde{\mathcal{K}}^+ \to \mathbb{C}$ is a meromorphic modular form of weight k and character χ for the group $\mathit{\Gamma}$ if it satisfies the following conditions:

(i) $F(\alpha Z) = \alpha^{-k}F(Z) \quad \forall \alpha \in \mathbb{C}\backslash\{0\}, Z \in \widetilde{K}^+$

(ii) $F(\gamma \cdot Z) = \chi(\gamma)F(Z) \quad \forall \gamma \in \mathit{\Gamma}$ (where the action is the one from equation (2.3))

(iii) F is meromorphic at the boundary

When F is holomorphic on $\widetilde{K}^+$ and at the boundary, we call it an holomorphic modular form.

Now we can see how to identify modular forms for $O(2,n)$ with modular forms in the sense of definition 1.19. If $F : \mathcal{K}^+ \to \mathbb{C}$ is a modular form of weight k, group $\mathit{\Gamma}$ and character χ, then $f(z) = F(M(z))$ is a Hilbert modular form of parallel weight k for the group $\mathit{\Gamma}$ and character χ since

$$f(\gamma z) = F(M(\gamma z)) = N(cz+d)^k F(N(cz+d)M(\gamma z)) = N(cz+d)^k F(\gamma \cdot M(z)) =$$

$$= N(cz+d)^k \chi(\gamma) F(M(z)) = N(cz+d)^k \chi(\gamma) f(z)$$

2.6 Heegner divisors and Hirzebruch-Zagier divisors

Modular varieties for orthogonal groups come with a family of divisors called the Heegner divisors. In view of the relation between Hilbert modular surfaces and modular varieties associated to certain orthogonal groups, those divisors lead to the Hirzebruch-Zagier divisors a family of algebraic divisors on a Hilbert modular surface.

Definition 2.18. Let m be a positive integer. The Hirzebruch-Zagier divisor T_m of discriminant m for the lattice $L = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathcal{O}_F \subset V$ is defined by

$$T_m = \sum_{\substack{(a,b,\lambda)\in L^\vee/\{\pm 1\} \\ ab-\lambda\lambda'=m/\Delta_F}} \{(z_1, z_2) \in \mathbb{H}^2 \mid az_1z_2 + \lambda z_1 + \lambda' z_2 + b = 0\}$$

These family of divisors will be important when we talk about the Borcherds lift, as those functions will have support on them. They are invariant under the action of $\mathrm{SL}_2(\mathcal{O}_F)$.

2.7 Theta lifting

Although there are several ways to get modular forms for orthogonal groups, here we show the theta lifting which allows us to lift automorphic forms on $\mathrm{SL}_2(\mathbb{R})$ to automorphic forms on $\mathrm{O}(2, n)$ by integrating the former against a kernel function, the so-called theta function.

Let V, L, Γ be defined as in section 2.3.4 and assume that $\dim(V) = n+2$ is even. We define the level of a lattice L the minimum integer N such that $NQ(\lambda)$ is an integer for all $\lambda \in L^\vee$. Consider the discriminant of L modified by a sign $\Delta = (-1)^{\frac{n+2}{2}} \det(S)$. Since $n + 2$ is even, it can be proven that $\mathrm{disc}(L) = \det(S) \not\equiv 2 \pmod 4$, so $\Delta \equiv 0 \pmod 4$ if $\mathrm{disc}(L)$ is even. Furthermore, with the sign modification, when $\det(S)$ is odd, $\Delta \equiv 1 \pmod 4$, so we can define a quadratic Dirichlet character $\chi_\Delta(n) = \left(\frac{\Delta}{n}\right)$ (the Kronecker symbol). This character is completely multiplicative and satisfies $\chi_\Delta(0) = 0$, $\chi_\Delta(1) = 1$, $\chi_\Delta(-1) = \mathrm{sign}(D)$, $\chi_\Delta(p)$ coincides with the Legendre symbol $\left(\frac{\Delta}{p}\right)$ when p is an odd prime and $\chi_\Delta(2) = 0$ if Δ is even, $\chi_\Delta(2) = 1$ if $\Delta \equiv 1 (\mathrm{mod}\ 8)$ and $\chi_\Delta(2) = -1$ if $\Delta \equiv 5 \pmod 8$.

For a fixed element $v \in \mathrm{Gr}(V)$ we can decompose each $\lambda \in V(\mathbb{R})$ as $\lambda = \lambda_v + \lambda_{v^\perp}$ where λ_v and $\lambda_{v^\perp}$ are the projections of λ on v and $v^\perp$ respectively. Since Q on $v^\perp$ is negative definite, and positive definite on v we can define a positive definite quadratic form $Q_v(\lambda) = Q(\lambda_v) - Q(\lambda_{v^\perp})$ associated to v. Recall that thanks to the isomorphism between $\mathcal{K}^+$ and $\mathrm{Gr}(V)$, we can associate to element $Z \in \widetilde{\mathcal{K}}^+$ a positive definite plane $v(Z) \in \mathrm{Gr}(V)$.

Definition 2.19. Let $r \in \mathbb{N} \cup \{0\}$. The Siegel theta function of weight r for the lattice L is defined to be

$$\Theta_r(\tau, Z) = y^{\frac{n}{2}} \sum_{\lambda \in L^\vee} \frac{(\lambda, Z)^r}{(Z, \overline{Z})^r} e(Q(\lambda_{v(Z)})N\tau + Q(\lambda_{v(Z)^\perp})N\overline{\tau})$$

where $\tau = x + iy \in \mathbb{H}$, $Z \in \widetilde{\mathcal{K}}^+$ and $e(t) = e^{2\pi it}$.

Note that we can also write

$$\Theta_r(\tau, Z) = y^{\frac{n}{2}} \sum_{\lambda \in L^\vee} \frac{(\lambda, Z)^r}{(Z, \overline{Z})^r} e(Q(\lambda)Nx + Q_{v(Z)}(\lambda)Niy).$$

Since $e(-2\pi Q_{v(Z)}(\lambda)Ny)$ decays rapidly, the series converges normally on $\mathbb{H} \times \widetilde{\mathcal{K}}^+$. It is non-holomorphic in both variables τ and Z. Using the Poisson summation formula and Weil representation one can show the following:

Proposition 2.20. *As a function of τ, $\Theta_r(\tau, Z)$ is a modular form of weight $r+1-\frac{n}{2}$ character χ_Δ for the group $\mathit{\Gamma}_0(N)$. That is*

$$\Theta_r(\gamma\tau, Z) = \chi_\Delta(d)(c\tau + d)^{r+1-\frac{n}{2}}\Theta_r(\tau, Z)$$

for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathit{\Gamma}_0(N)$, where

$$\mathit{\Gamma}_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \ (mod\ N) \right\}$$

Proposition 2.21. *As a function of Z, $\overline{\Theta_r(\tau, Z)}$ is a modular form of weight r for $\mathit{\Gamma}$.*

We can use $\Theta_r(\tau, Z)$ to lift modular forms for $\mathit{\Gamma}_0(N)$ to modular forms on the orthogonal group. More precisely if f is a cusp form of weight $k = r + \frac{2-n}{2}$ for $\mathit{\Gamma}_0(N)$ with character χ_Δ, the theta lift $\mathit{\Phi}(Z, f)$ of f defined by

$$\mathit{\Phi}(Z, f) = \int_{\mathcal{F}} f(\tau)\overline{\Theta_r(\tau, Z)}y^{k-2}dxdy.$$

where $\mathcal{F}$ is any fundamental domain for $\mathit{\Gamma}_0(N)$.

Theorem 2.22. *The theta lift $\mathit{\Phi}(Z, f)$ of f is an holomorphic modular form of weight $r = k - 1 + \frac{n}{2}$ for the orthogonal group $\mathit{\Gamma}$.*

Proof. The transformation law is direct from the fact that $\overline{\Theta_r(\tau, Z)}$ transforms as a modular form of weight r for the group $\mathit{\Gamma}$. For the proof of holomorphicity, see [Oda77] □

Chapter 3

Additive and multiplicative lifts

In this chapter we present two different lifts that will provide a source of Hilbert modular forms, the Doi-Naganuma lift and the Borcherds lift. We also discuss local Borcherds products an introduction for the Borcherds lift. Finally we will see how in some cases the two lifts can give the same modular forms, and use this property to evaluate the Borcherds lift on points of $\mathbb{H}^2$ by using the explicit expression of the Doi-Naganuma lift. That coincidence is very convenient as it is usually easier and better for numerical purposes to evaluate additive formulas than products.

3.1 The Doi-Naganuma lift

In this section we present the Doi-Naganuma lift for the full Hilbert Modular group Γ_F. The proofs of the main theorems of this section are long and can be found in the literature, so we will just to present the results to show a different way of obtaining modular forms and their properties and because we are more interested in doing numerical computations with them rather than in the theoretical details. We will apply those results in the end of the chapter to show how to evaluate some concrete Hilbert modular forms.

Let $F \subset \mathbb{R}$ be the real quadratic field of discriminant Δ_F. To make things simpler we will focus on the cases where $F = \mathbb{Q}(\sqrt{p})$ for some primer number p and the discriminant $\Delta_F = p$ (so $p \equiv 1 \pmod 4$). Let (V, Q) be the rational quadratic space of type $(2,2)$ corresponding to F as in section 2.4 and let $L = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathcal{O}_F$. The Siegel theta function $\Theta_k(\tau, z)$ of weight k is a modular function in both τ (for the group $\Gamma_0(p)$ and character $\chi_p(n) = \left(\frac{p}{n}\right)$, the Kronecker symbol) and z (for the group Γ_F).

The Doi-Naganuma lift is a small modification of the lifting that we have already seen that makes explicit computations of modular forms much more convenient.

Definition 3.1. We denote by $M_k(p, \chi_p)$ the space of holomorphic modular forms of weight k for the group $\Gamma_0(p)$ and character χ_p (this character is the one that we have already described in the previous chapter, but when $p = 4k+1$, it also corresponds to the Jacobi symbol $\chi_p(n) = \left(\frac{n}{p}\right)$). The modular forms in $M_k(p, \chi_p)$ satisfy

$$f(\gamma z) = \chi_p(d)(cz+d)^k f(z)$$

for $z \in \mathbb{H}$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(p)$ (recall that $\Gamma_0(p) = \{\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mid \gamma \in \mathrm{SL}_2(\mathbb{Z})$ and $c \equiv 0 \pmod{p}\}$.

If we apply the transformation law for $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in \Gamma_0(p)$ we get that $f(z) = \chi_p(-1)(-1)^k f(z)$, but since we are assuming $p \equiv 1 \pmod 4$, $\chi_p(-1) = 1$ (it is a quadratic residue). Therefore, for odd k we get $f(z) = -f(z)$, so when k is odd this space contains only the trivial modular form $f = 0$. Therefore, from now on, we will assume that k is even. A modular form $f \in M_k(p, \chi_p)$ has a Fourier expansion of the form:

$$f(\tau) = \sum_{n \geq 0} c(n) q^n$$

where $q = e^{2\pi i \tau}$. We define two subspaces of $M_k(p, \chi_p)$ that are called the plus and minus subspaces are defined by

$$M_k^+(p, \chi_p) = \{f \in M_k(p, \chi_p) \mid \chi_p(n) = -1 \implies c(n) = 0\}$$

$$M_k^-(p, \chi_p) = \{f \in M_k(p, \chi_p) \mid \chi_p(n) = 1 \implies c(n) = 0\}$$

Basically, the plus space is the space of modular forms that only have non-zero coefficients $c(n)$ for those n such that $\chi_p(n) \neq -1$ (and similarly for the minus space). We denote by $S_k^+(p, \chi_p)$ and $S_k^-(p, \chi_p)$ the subspaces of cusp forms of the plus and minus space.

At first sight it is not obvious that there exist modular forms in the plus or minus subspaces. We selected some subset of the non-negative integers and we considered the modular forms (of a certain weight and for a certain group and character) that have null coefficients at those positions. Certainly, not for every subset of the non-negative integers it is possible to do that, but it is not hard to see that such modular forms exist, and we will give an example based on the Eisenstein series of $M_k(p, \chi_p)$. We have two different Eisenstein series for $M_k(p, \chi_p)$ whose Fourier expansions are given by

$$G_k(\tau) = \frac{L(1-k, \chi_p)}{2} + \sum_{n=1}^{\infty} \sum_{d|n} d^{k-1} \chi_p(d) q^n$$

$$H_k(\tau) = \sum_{n=1}^{\infty} \sum_{d|n} d^{k-1} \chi_p(\frac{n}{d}) q^n$$

Usually $G_k(\tau)$ is normalized so that the independent term is equal to 1, but we have normalized it that way so that when we add or substract them we get the following:

$$G_k(\tau) \pm H_k(\tau) = \frac{L(1-k, \chi_p)}{2} + \sum_{n=1}^{\infty} \sum_{d|n} d^{k-1} (\chi_p(d) \pm \chi_p(\frac{n}{d})) q^n$$

Note that if $\chi_p(n) = 1$, then for any divisor d of n, we have that $1 = \chi_p(n) = \chi_p(d)\chi_p(\frac{n}{d})$, so $\chi_p(d) = \chi_p(\frac{n}{d})$ as the character only takes values 1 and -1, which means that whenever $\chi_p(n) = 1$, $\chi_p(d) - \chi_p(\frac{n}{d}) = 0$ and the n-th coefficient of

$E_k^- := G_k(\tau) - H_k(\tau)$ vanishes, so $E_k^- \in M_k^-(p, \chi_p)$. Similarly, $E_k^+ := G_k(\tau) + H_k(\tau) \in M_k^+(p, \chi_p)$.

Those two modular functions are particularly interesting due to the next result by Hecke.

Proposition 3.2. *The spaces $M_k^{\pm}(p, \chi_p)$ can be decomposed as*

$$M_k^{\pm}(p, \chi_p) = \mathbb{C}E_k^{\pm} \oplus S_k^{\pm}(p, \chi_p)$$

So given $f \in S_k^+(p, \chi_p)$ (respectively in the minus space of cuspforms) we can substract a multiple of E_k^+ and it will always give a cuspform (in the plus/minus space). Furthermore, also due to Hecke, we have that

Proposition 3.3. *The spaces $M_k(p, \chi_p)$ can be decomposed as*

$$M_k(p, \chi_p) = M_k^+(p, \chi_p) \oplus M_k^-(p, \chi_p)$$

which implies that given $f \in M_k(p, \chi_p)$ we can write it as a sum of a modular form in the plus space and one in the minus space.

Now that we are familiarized with the plus and minus spaces we can proceed to define the modified theta lift, but we will need some preliminary definitions. Given a modular form $f = \sum_{n \geq 0} c(n)q^n$, we define

$$\widetilde{c}(n) = \begin{cases} c(n) & \text{if } p \nmid n \\ 2c(n) & \text{if } p \mid n \end{cases} \tag{3.1}$$

Modular forms in the plus space are similar in many ways to elliptic modular forms for $\mathrm{SL}_2(\mathbb{Z})$. In [BB01] (Theorem 5) states that $M_k^{\pm}(p, \chi_p)$ is isomorphic to a space of vector-valued modular forms of weight k. By interpreting modular forms in the plus (minus) space as vector valued modular forms it is possible to prove the next result.

Proposition 3.4. *Let $f = \sum_{n \in Z} c(n)q^n \in M_{k_1}^{\pm}(p, \chi_p)$ and $g = \sum_{n \in \mathbb{Z}} a(n)q^n \in M_{k_2}^{\pm}(p, \chi_p)$ (either both belong to the plus space or both belong to minus space). The bilinear pairing defined by*

$$\langle f, g \rangle = \sum_{n \in \mathbb{Z}} \sum_{m \in \mathbb{Z}} \widetilde{c}(m)a(pn - m)q^n$$

is a modular form of weight $k_1 + k_2$ for $SL_2(\mathbb{Z})$.

Observation 3.5. In the classical case of elliptic modular forms in one variable for $\mathrm{SL}_2(\mathbb{Z})$ we have a formula for the dimension of the space of modular forms of weight $2k$, and for weight $4, 6, 8, 10$ we know that the dimension is 1, so the space of is spanned by the Eisenstein series of weight $2k$ (usually denoted by E_{2k}). Therefore, by the previous proposition we know that for instance, when $k = 2$ or $k = 4$, $\langle E_k^+, E_k^+ \rangle = \lambda E_{2k}$ for some $\lambda \in \mathbb{C}$ that can be determined by looking at the first term of the series of each side. From here, we can deduce some nice identities for divisor sums involving some Dirichlet characters.

Note that we don't require for f to be holomorphic in Proposition 3.4 as the result is true also for non-holomorphic modular forms. For instance, we can use it with the complex conjugate of the Siegel theta function of the lattice that we described at the beginning of this section, which satisfies the plus space condition. To see why it satisfies the plus space condition, recall that in our current setting, $L = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathcal{O}_F$ and the dual lattice is $L^\vee = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathfrak{d}_F^{-1}$. So the level N of L is p and for $(a, b, \lambda) \in L^\vee$, $-pQ(a, b, \lambda) = p(ab - \lambda\lambda') \equiv -p\lambda\lambda' \pmod p$ which is a square modulo p because if $\lambda = \frac{1}{\sqrt{p}}(x + y\frac{1+\sqrt{p}}{2}) \in \mathfrak{d}_F$ for $x, y \in \mathbb{Z}$, then

$$-p\lambda\lambda' = -p\frac{1}{\sqrt{p}}(x+y\frac{1+\sqrt{p}}{2})\frac{1}{\sqrt{p}}(-x+y\frac{-1+\sqrt{p}}{2}) = -(x+y\frac{1+\sqrt{p}}{2})(-x+y\frac{-1+\sqrt{p}}{2}) =$$

$$= x^2 + xy + y^2\frac{1-p}{4} = (x + \frac{y}{2})^2 - \frac{p}{4}y^2 \equiv (x + \frac{y}{2})^2 \pmod p$$

as 4 is coprime to p. Therefore the imaginary part of the exponentials that do not belong to the variable τ, are of the form $2\pi im$ where m is a square modulo p, so there are no non-zero coefficients whose character is -1 and $\overline{\Theta_k(\tau, Z)}$ belongs to the plus space.

Definition 3.6. The modified theta lifting for $f \in M_k^+(p, \chi_p)$ is defined by the integral

$$\Phi(z, f) = \int_{SL_2(\mathbb{Z})\backslash\mathbb{H}} \langle f(\tau), \overline{\Theta_k(\tau, z)} \rangle v^{k-2} du dv$$

When f is a cusp form the integral converges absolutely. Otherwise it has to be regularized as it is done in [Bor98]. The main theorem for the theta lift (whose proof can be found in [Bor98], Theorem 14.3) is the following:

Theorem 3.7. *Let $f = \sum_{n\in\mathbb{Z}} c(n)q^n \in M_k^+(p, \chi_p)$. The modified theta lift $\Phi(z, f)$ satisfies*

(i) $\Phi(z, f)$ is a Hilbert modular form of weight k for the group Γ_F.

(ii) It has the Fourier expansion

$$\Phi(z, f) = -\frac{B_k}{2k}\widetilde{c}(0) + \sum_{\substack{\nu\in\mathfrak{d}_F^{-1} \\ \nu\gg 0}} \sum_{d|\nu} d^{k-1}\widetilde{c}\left(\frac{p\nu\nu'}{d^2}\right) q_1^\nu q_2^{\nu'}$$

where $z = (z_1, z_2)$,$q_j = e^{2\pi i z_j}$ and B_k is the k-th Bernoulli number

(iii) If f is a cusp form, $\Phi(z, f)$ is also a cusp form.

By extending the definition of $\Phi(z, f)$ so that it is identically zero for $f \in M_k^-(p, \chi_p)$ we get the Doi-Naganuma lift

$$DN : M_k(p, \chi_p) \to M_k(\Gamma)$$

Summarizing, given a modular form $f \in M_k^+(p, \chi_p)$ for even $k > 0$, we can get a modular form for the Hilbert modular group (without having to compute the bilinear pairing and the integral) by using the formula from Theorem 3.7 (ii) where the coefficients $\widetilde{c}(n)$ are the modified coefficients of f as we described before. This makes computations really convenient. We will use this result in the end of the chapter.

3.2 Borcherds lift

In this section, we describe the Borcherds lift for Hilbert modular surfaces. It lifts some weakly holomorphic modular forms of weight 0 to meromorphic Hilbert modular forms that have zeros and poles on the Hirzebruch-Zagier divisors and have an absolutely convergent product expansion on some subset of $\mathbb{H}^2$. We start by studying local Borcherds products at the cusps of Hilbert modular surfaces and we restrict ourselves to this case although the results can be made more generally for $\mathrm{O}(2,n)$. As always, F is a real quadratic field of discriminant Δ (as there is no confusion, we won't add the subscript) and $\mathit{\Gamma}_F$ is the Hilbert modular group. This study of the local Borcherds products will allow us to introduce some concepts that will appear when we present the Borcherds lift, like the Weyl chambers or the Weyl vector and will show how we can obtain a function that is invariant under the stabilizer of the cusp infinity as an infinite convergent product.

3.2.1 Local Borcherds products

Definition 3.8. For a positive integer m, the local Hirzebruch-Zagier divisor at ∞ of discriminant m is defined by

$$T_m^\infty = \sum_{\substack{\lambda \in \mathfrak{d}_F^{-1}/\{\pm 1\} \\ -\lambda\lambda' = m/\Delta \\ b \in \mathbb{Z}}} \{(z_1, z_2) \in \mathbb{H}^2 \mid \lambda z_1 + \lambda' z_2 + b = 0\} \subset \mathbb{H}^2$$

Note that it goes through the cusp ∞. This divisor can be decomposed into a sum of smaller divisors in the following way:

$$T_m^\infty = \sum_{\substack{\lambda \in \mathfrak{d}_F^{-1}/\mathcal{O}_F^{*,2} \\ -\lambda\lambda' = m/\Delta \\ \lambda > 0}} T_\lambda^\infty$$

where

$$T_\lambda^\infty = \sum_{\substack{u \in \mathcal{O}_F^{*,2} \\ b \in \mathbb{Z}}} \{(z_1, z_2) \in \mathbb{H}^2 \mid \lambda u z_1 + \lambda' u' z_2 + b = 0\}$$

Note that this divisor T_λ^∞ is invariant under the action of the stabilizer of ∞, and so T_m^∞ is also invariant under the action of this group ($\mathit{\Gamma}_{F,\infty}$). To check we just need to note that the image of (z_1, z_2) by an element of the stabilizer of infinity which is of the form $(\varepsilon^2 z_1 + \varepsilon\mu, (\varepsilon')^2 z_2 + \varepsilon'\mu')$ satisfies

$$\lambda u \varepsilon^2 z_1 + \lambda' u' (\varepsilon')^2 z_2 + \lambda u \varepsilon \mu + \lambda' u' \varepsilon' \mu' + b = 0$$

for some $u \in \mathcal{O}_F^{*,2}$ and $b \in \mathbb{Z}$. But $\lambda u \varepsilon \mu + \lambda' u' \varepsilon' \mu' + b \in \mathbb{Z}$ and $u\varepsilon^2 \in \mathcal{O}_F^{*,2}$, so that's true because $(z_1, z_2) \in T_\lambda^\infty$.

Now we proceed to define an holomorphic function on $\mathbb{H}^2/\Gamma_{F,\infty}$ whose divisor is T_λ^∞. We start by defining the Weyl chambers, but to do that we will need some additional notation. Let

$$S(m) = \bigcup_{\substack{\lambda\in\mathfrak{d}_F^{-1} \\ -\lambda\lambda'=m/\Delta}} \{(y_1, y_2) \in (\mathbb{R}^+)^2 \mid \lambda y_1 + \lambda' y_2 = 0\}$$

Each term in the union defines an hyperplane of $(\mathbb{R}^+)^2$, so $S(m)$ is a union of hyperplanes. The complement of $S(m)$, $(\mathbb{R}^+)^2 \setminus S(m)$ is not connected, as each of the hyperplanes that form $S(m)$ is a semistraight going through the origin. Each connected component of the complement is a Weyl chamber of index m. An element $\lambda \in \mathfrak{d}_F^{-1}$ such that $-\lambda\lambda' = \frac{m}{\Delta}$ is called positive with respect to a subset W of a Weyl chamber if $\mathrm{tr}(\lambda w) > 0$ for all $w \in W$. Note that this is equivalent to asking just that $\mathrm{tr}(\lambda w_0) > 0$ for an $w_0 \in W$ as the sign of $\mathrm{tr}(\lambda w)$ doesn't change inside a Weyl chamber because it is continuous and only vanishes at the hyperplanes that define $S(m)$. To denote that λ is positive with respect to W, we put $(\lambda, W) > 0$. When λ is positive but $u\lambda$ is not for any $u \in \mathcal{O}_F^{*,2}$ with $u < 1$, we say that λ is reduced. Note that λ being reduced is equivalent to

$$(\varepsilon_0^{-2}\lambda, W) < 0 \text{ and } (\lambda, W) > 0$$

for the fundamental unit ε_0. It implies that $\lambda > 0$.

Denote by $R(m, W)$ the set of all $\lambda \in \mathfrak{d}_F^{-1}$ with $-\lambda\lambda' = \frac{m}{\Delta}$ which are reduced with respect to W. It is a finite set and satisfies

$$\{\lambda \in \mathfrak{d}_F^{-1} \mid -\lambda\lambda' = \frac{m}{\Delta}\} = \{\pm\lambda u \mid \lambda \in R(m, W), u \in \mathcal{O}_F^{*,2}\}$$

Let W be a subset of a Weyl chamber of index m and $\lambda \in \mathfrak{d}_F^{-1}$ with $-\lambda\lambda' = m/\Delta$ and define an holomorphic function $\psi_\lambda^\infty : \mathbb{H}^2 \to \mathbb{C}$ ‘

$$\psi_\lambda^\infty(z) = \prod_{u\in\mathcal{O}_F^{*,2}} (1 - e(\sigma_u \mathrm{tr}(u\lambda z))$$

where $e(x) = e^{2\pi i x}$ and

$$\sigma_u = \begin{cases} 1, & \text{if } (u\lambda, W) > 0 \\ -1, & \text{if } (u\lambda, W) < 0 \end{cases}$$

The sign is added so that the obtained product is convergent. Note that by definition we have $\mathrm{div}(\psi_\lambda^\infty) = T_\lambda^\infty$. Furthermore, this function is invariant under the subgroup of translations $\{\left(\begin{smallmatrix} 1 & \mu \\ 0 & 1 \end{smallmatrix}\right)\} \subset \Gamma_{F,\infty}$, but not under the full group $\Gamma_{F,\infty}$. However, we can modify our function so that it is invariant under the action of the full group. Consider the automorphy factor

$$J(\gamma, z) = \frac{\psi_\lambda^\infty(\gamma z)}{\psi_\lambda^\infty(z)}$$

Since $\mathit{\Gamma}_{F,\infty}$ is generated by translations and $\left(\begin{smallmatrix}\varepsilon_0 & 0\\ 0 & \varepsilon_0^{-1}\end{smallmatrix}\right)$, where ε_0 is the fundamental unit, we only need to consider what happens with the automorphy factor for that generator of the diagonal subgroup of $\mathit{\Gamma}_{F,\infty}$. We have that

$$\frac{\psi_\lambda^\infty(\varepsilon_0^2 z)}{\psi_\lambda^\infty(z)} = \prod_{u\in\mathcal{O}_F^{*,2}} \frac{1-e(\sigma_{u/\varepsilon_0^2}\mathrm{tr}(u\lambda z))}{1-e(\sigma_u\mathrm{tr}(u\lambda z))} \tag{3.2}$$

since

$$\psi_\lambda^\infty(\varepsilon_0^2 z) = \prod_{u\in\mathcal{O}_F^{*,2}}(1-e(\sigma_u\mathrm{tr}(u\varepsilon_0^2\lambda z))) = \prod_{\widetilde{u}\in\mathcal{O}_F^{*,2}}(1-e(\sigma_{\widetilde{u}/\varepsilon_0^2}\mathrm{tr}(\widetilde{u}\lambda z)))$$

by doing the change of variables $\widetilde{u} = u\varepsilon_0^2$. Note that $\sigma_u = \sigma_{u/\varepsilon_0^2}$ for all except one $u\in\mathcal{O}_F^{*,2}$, so all the factors in the product of (3.2) are equal to 1 except one of them. Assuming that λ is reduced, we have

$$\frac{\psi_\lambda^\infty(\varepsilon_0^2 z)}{\psi_\lambda^\infty(z)} = \frac{1-e(-\mathrm{tr}(\lambda z))}{1-e(\mathrm{tr}(\lambda z))} = \frac{(1-e(-\mathrm{tr}(\lambda z)))e(1/2-\mathrm{tr}(\lambda z))}{(1-e(\mathrm{tr}(\lambda z)))e(1/2-\mathrm{tr}(\lambda z))} =$$

$$= \frac{(1-e(-\mathrm{tr}(\lambda z)))e(1/2-\mathrm{tr}(\lambda z))}{e(1/2-\mathrm{tr}(\lambda z))-e(1/2)} = \frac{(1-e(-\mathrm{tr}(\lambda z)))e(1/2-\mathrm{tr}(\lambda z))}{-e(-\mathrm{tr}(\lambda z))+1} = e(1/2-\mathrm{tr}(\lambda z))$$

Consider the invertible holomorphic function on $\mathbb{H}^2$

$$I_\lambda(z) = e\left(\mathrm{tr}\left(\frac{\lambda}{\varepsilon_0^2-1}z\right)\right)$$

which satisfies

$$\frac{I_\lambda(\varepsilon_0^2 z)}{I_\lambda(z)} = e\left(\mathrm{tr}\left(\frac{\lambda\varepsilon_0^2}{\varepsilon_0^2-1}z\right)-\mathrm{tr}\left(\frac{\lambda}{\varepsilon_0^2-1}z\right)\right) = e(\mathrm{tr}(\lambda z))$$

and $I_\lambda(z+\mu) = I_\lambda(z)$ for all $\mu\in(\epsilon_0^2-1)\mathcal{O}_F$. So up to torsion, the automorphy factor $J(\gamma, z)$ becomes trivial once we multiply our original function by $I_\lambda(z)$. That is

$$\Psi_\lambda^\infty(z) = I_\lambda(z)\psi_\lambda^\infty(z) = e\left(\mathrm{tr}\left(\frac{\lambda}{\epsilon_0^2-1}z\right)\right)\prod_{u\in\mathcal{O}_F^{*,2}}(1-e(\sigma_u\mathrm{tr}(u\lambda z))$$

is an holomorphic function that satisfies that a power of it is invariant under the action of $\mathit{\Gamma}_{F,\infty}$ and whose divisor is T_λ^∞. It is clear that

$$\frac{\Psi_\lambda^\infty(\varepsilon_0^2 z)}{\Psi_\lambda^\infty(z)} = e(1/2) = -1$$

so any even power of Ψ_λ^∞ is invariant under the diagonal subgroup of $\mathit{\Gamma}_{F,\infty}$. And for the translations, we have that

$$\frac{\Psi_\lambda^\infty(z+\mu)}{\Psi_\lambda^\infty(z)} = e\left(\operatorname{tr}\left(\frac{\lambda}{\varepsilon_0^2-1}\mu\right)\right)$$

but $(\varepsilon_0^2-1)(1-\varepsilon_0^{-2}) = (\varepsilon_0-\varepsilon_0^{-1})^2 \in \mathbb{Z}$, so we can cancel the denominator by raising Ψ_λ^∞ to an integer and raising Ψ_λ^∞ to 2 times this integer will make it invariant under the whole group $\Gamma_{F,\infty}$.

Although each of I_λ and ψ_λ^∞ depend on the choice of the Weyl chamber, their product doesn't. Now we can do an analogous reasoning to get a similar product whose divisor is T_m^∞ instead.

Definition 3.9. Let W be a Weyl chamber of $S(m)$. The Weyl vector of index m for the camber W is defined to be

$$\rho_{m,W} = \sum_{\lambda\in R(m,W)} \frac{\lambda}{\varepsilon_0^2-1}$$

The local Borcherds product for the divisor T_m^∞ is

$$\Psi_m^\infty = \prod_{\substack{\lambda\in\mathfrak{d}_F^{-1}/\mathcal{O}_F^{*,2}\\ -\lambda\lambda=m/\Delta\\ \lambda>0}} \Psi_\lambda^\infty(z) = e(\operatorname{tr}(\rho_{m,W}z)) \prod_{\substack{\lambda\in\mathfrak{d}_F^{-1}\\ -\lambda\lambda=m/\Delta\\ (\lambda,W)>0}} (1-e(\operatorname{tr}(\lambda z)))$$

Proposition 3.10. *The divisor of Ψ_m^∞ is equal to T_m^∞. There is a power of Ψ_m^∞ which is invariant under the action of $\Gamma_{F,\infty}$.*

Proof. It is clear by construction and the decomposition of T_m^∞ as a sum of T_λ^∞ that the divisor of Ψ_m^∞ is equal to T_m^∞. It is also clear that $\Psi_m^{\infty,2}$ is invariant under the diagonal subgroup of $\Gamma_{F,\infty}$. And a similar reasoning to the previous one shows that the term $e(\operatorname{tr}(\rho_{m,W}\mu))$ gets cancelled when raised to an appropiate integer. □

Example 3.11. Here we compute more explicitly Ψ_1^∞ for $D=\Delta=5$ as an example. It will be useful for the computations in the next section. Namely we compute the Weyl vector. Let $\varepsilon_0 = \frac{1+\sqrt{5}}{2}$ be a positive fundamental unit. Then $(\varepsilon_0^{-1},\varepsilon_0) \in (\mathbb{R}^+)^2$ and $(\varepsilon_0^{-1},\varepsilon_0) \notin S(1)$ because $\lambda\varepsilon_0^{-1}+\lambda'\varepsilon_0 = 0$ has no solution for $\lambda \in \mathfrak{d}_F^{-1}$ such that $-\lambda\lambda' = 1/D$ since $\lambda\varepsilon_0^{-1}+\lambda'\varepsilon_0 = 0 \implies \lambda^2+\varepsilon_0^2/D = 0$ which is a contradiction. Thus $(\varepsilon_0^{-1},\varepsilon_0)$ lies in a Weyl chamber W of index 1 and the set of reduced λ with respect to W such that $\lambda \in \mathfrak{d}_F^{-1}$ and $-\lambda\lambda' = 1/D$ satisfy $(\lambda,W)>0 \iff \varepsilon_0^{-1}\lambda+\lambda'\varepsilon_0 > 0$ and $(\varepsilon_0^{-2}\lambda,W) < 0 \iff \varepsilon_0^{-3}\lambda+\lambda'\varepsilon_0^3 < 0$. Rearranging the equations, multiplying by $\lambda>0$ and using $\lambda\lambda' = -1/D$, we get that

$$\frac{\varepsilon_0^6}{D} > \lambda^2 > \frac{\varepsilon_0^2}{D}$$

Since $\lambda\lambda' = -1/D$ and $\lambda \in \mathfrak{d}_F^{-1}$, $\sqrt{D}\lambda \in \mathcal{O}_F$ and has norm 1 (by multiplicativity of the norm). So $\sqrt{D}\lambda = \pm\varepsilon_0^k$ for some $k\in\mathbb{Z}$. Since we must have

$$\frac{\varepsilon_0^6}{D} > \lambda^2 = \frac{\varepsilon_0^{2k}}{D} > \frac{\varepsilon_0^2}{D}$$

and ε_0^{2k} is increasing in k, $k = 2$ is the only solution. Then

$$R(1, W) = \{\varepsilon_0/\sqrt{D}\}$$

and the Weyl vector is equal to

$$\rho_{1,W} = \frac{\varepsilon_0^2}{\sqrt{D}(\varepsilon_0^2 - 1)} = \frac{\varepsilon_0}{\sqrt{D}(\varepsilon_0 - \varepsilon_0^{-1})} = \frac{\varepsilon_0}{\sqrt{D}\mathrm{tr}(\varepsilon_0)}$$

Analogous computations can be done for $D \neq 5$ without changing almost anything. The main difference is that $R(1, W)$ contains also another element if the fundamental unit has norm 1 and not -1.

3.2.2 Borcherds lift

When $k = 0$, the space $M_k(p, \chi_p)$ is trivial, so the Doi-Naganuma map only gives the trivial modular form that is identically zero. We may ask if there is something we can do in this case to lift Hilbert modular forms. Assuming that there exists an $f = \sum_{n\in\mathbb{Z}} c(n)q^n \in M_0^+(p, \chi_p)$ and writing its formal expansion from Theorem 3.7

$$\Phi(z, f) = -\frac{B_0}{2k}\widetilde{c}(0) + \sum_{\substack{\nu\in\mathfrak{d}_F^{-1} \\ \nu\gg 0}} \sum_{d|\nu} \frac{1}{d}\widetilde{c}\left(\frac{p\nu\nu'}{d^2}\right) q_1^{\nu} q_2^{\nu'}$$

which can be reordered to

$$\Phi(z, f) = -\frac{B_k}{2k}\widetilde{c}(0) + \sum_{\substack{\nu\in\mathfrak{d}_F^{-1} \\ \nu\gg 0}} \log(1 - q_1^{\nu} q_2^{\nu'})^{\widetilde{c}(p\nu\nu')}$$

Borcherds, among others, tried to discard the assumption that f is holomorphic and replace it by something weaker. He considered f to be weakly holomorphic which gives meromorphic modular forms with a product expansion like the above. This works for the more general case $\mathrm{O}(2, n)$ and lifts weakly holomorphic modular forms of weight $1 - n/2$ to meromorphic modular forms on $\mathrm{O}(2, n)$ with zeros and poles supported by Heegner divisors. But here we focus on $n = 2$, the case for Hilbert modular surfaces, for which we can lift weakly holomorphic modular forms of weight 0 to Hilbert Modular forms with zeros and poles supported on Hirzebruch-Zagier divisors. For the sake of simplicity, let's assume that the real quadratic field associated to our Hilbert modular surface has prime discriminant, so $D = \Delta_F = p$.

A meromorphic modular form is called weakly holomorphic if it is holomorphic outside the cusps. We denote by $W_k(p, \chi_p)$ the space of weakly holomorphic modular forms of weight k and character χ_p for the group $\Gamma_0(p)$. As before, by $W_k^+(p, \chi_p)$ we refer to the subspace of $W_k(p, \chi_p)$ for which the modular forms satisfy the plus space condition (the n-th coefficient vanishes when $\chi_p(n) = -1$). Modular forms in $W_k(p, \chi_p)$ have a Fourier expansion of the form $f = \sum_{n\geq N} c(n)q^n$ for some $N \in \mathbb{Z}$ and the growth of their coefficients is bounded by $O(e^{C\sqrt{n}})$ for some positive constant

$C > 0$. Any $f = \sum_{n \geq N} c(n)q^n \in W_k^+(p, \chi_p)$ for $k \leq 0$ is determined by its principal part $\sum_{n<0} c(n)q^n$ because the difference of two modular forms of $W_k^+(p, \chi_p)$ with the same principal part is holomorphic at the cusp ∞ and can also be proven to be holomorphic at the cusp 0. Those are the only two cusps for $\Gamma_0(p)$, so it is holomorphic at the cusps. But the only holomorphic modular form of weight $k \leq 0$ with character is the one that is identically zero.

For a $f = \sum_{n \geq N} c(n)q^n \in W_k^+(p, \chi_p)$ we can define concepts similar to the ones that appeared when we presented local Borcherds products. The Weyl chambers corresponding to f are the connected components of

$$(\mathbb{R}^+)^2 \setminus \bigcup_{\substack{m>0 \\ c(-m) \neq 0}} S(m)$$

For a Weyl chamber W, its corresponding Weyl vector is defined by

$$\rho_{f,W} = \sum_{m>0} \widetilde{c}(-m)\rho_{m,W} \in F$$

where the $\rho_{m,W}$ are the Weyl vectors defined in Definition 3.9 and the coefficients $\widetilde{c}(-m)$ are given by equation (3.1). Now we have all we need to state Borcherds' Theorem for the Borcherds lift in our case for Hilbert modular forms.

Theorem 3.12. *Let $f = \sum_{n \geq N} c(n)q^n$ be a weakly holomorphic modular form in $W_0^+(p, \chi_p)$ such that $\widetilde{c}(n) \in \mathbb{Z}$ for all $n < 0$. Then, theres exists a meromorphic Hilbert modular form (with some unitary character of finite order) $\Psi(z, f)$ for Γ_F such that:*

(i) The weight of Ψ is equal to $c(0)$, the constant term of f.

(ii) The divisor of Ψ is determined by the principal part of f at the cusp ∞ and it is explicitly given by

$$\operatorname{div}(\Psi) = \sum_{n<0} \widetilde{c}(n)T_{-n}$$

where T_m denotes the Hirzebruch-Zagier divisor (defined in Definition 2.18).

(iii) Let W be a Weyl chamber associated to f and let $N = \min\{n \mid c(n) \neq 0\}$. Then Ψ has the following Borcherds product expansion

$$\Psi(z, f) = q_1^{\rho} q_2^{\rho'} \prod_{\substack{\nu \in \mathfrak{d}_F^{-1} \\ (\nu, W) > 0}} \left(1 - q_1^{\nu} q_2^{\nu'}\right)^{\widetilde{c}(p\nu\nu')}$$

where ρ if the Weyl vector corresponding to f and chamber W and $q_j = e^{2\pi i z_j}$. The product converges normally for all z such that $y_1 y_2 > \frac{|N|}{p}$ outside the set of poles.

The function $\Psi(z, f)$ is not exactly a Hilbert modular as we are used to because it is a Hilbert modular form with a unitary character of finite order. That means that to the usual transformation law we have to add a character. However, this character has finite order, so after raising it to some power n we get a Hilbert modular form in the sense that we are used to. Furthermore, it turns out that we can choose this n so that all Fourier coefficients are in $\mathbb{Z}$ when the Borcherds product is holomorphic.

Note that we are not specifying the choice of the Weyl chamber, but it is not hard to see that the Borcherds lift does not depend on it (it may depend up to a multiplicative constant) because if we have two lifts for two different chambers with the same divisor and weight (from the Theorem), their quotient is holomorphic and of weight 0 so it must be a constant.

Note that the divisor of the Borcherds lift $\Psi(z, f)$ is determined by the principal part of f, so to describe which are the possible linear combinations of Hirzebruch-Zagier divisors that occur as divisors of Borcherds lifts, it is enough to understand the principapl part of the modular forms in $W_0^+(p, \chi_p)$. It is easy to obtain necessary conditions for the principal part. Let $f = \sum_{n \geq N} c(n) q^n \in W_0^+(p, \chi_p)$ and $g \in M_{2-k}^+$ with Fourier coefficients $b(n)$. Then the bilinear pairing from Proposition 3.4 $\langle f, g \rangle$ is a weakly holomorphic modular of weight 2 for $\mathrm{SL}_2(\mathbb{Z})$ which implies that the constant term in its Fourier expansion is 0. Therefore

$$\sum_{n<0} \widetilde{c}(n) b(-n) = 0$$

Applying this for the Eisenstein series $E_{2-k}^+(\tau)$ (it appeared in the discussion of the Doi-Naganuma lift) we get a formula for the constant term of f. If $B_{2-k}^+(n)$ is the n-th coefficient of $E_{2-k}^+(\tau)$ after normalizing it so that the constant term is 1, we have

$$c(0) = -\frac{1}{2} \sum_{n<0} \widetilde{c}(n) B_{2-k}^+(-n)$$

for any $f = \sum_{n \geq N} c(n) q^n \in W_0^+(p, \chi_p)$.

It turns out that the necessary condition is also sufficent as proven in [BB01] (Theorem 6).

Theorem 3.13. *There exists an $f \in W_0^+(p, \chi_p)$ with principal part $= \sum_{n<0} c(n) q^n$, if and only if $c(n) = 0$ if $\chi_p(n) = -1$ (so it satisfies the plus space condition) and*

$$\sum_{n<0} \widetilde{c}(n) b(-n) = 0$$

for every cusp form $g = \sum_{m>0} b(m) q^m \in S_{2-k}^+(p, \chi_p)$.

3.2.3 Explicit computation of the Borcherds lifts

To finish this chapter, we can use all the previous results to compute some Borcherds lifts. We will focus on the case $p = 5$. By a result from Hecke, the dimension of $S_2^+(p, \chi_p)$ is equal to $\lfloor \frac{p-5}{24} \rfloor$, so $S_2^+(5, \chi_5)$ is trivial so we don't have any additional restrictions for the Fourier coefficients of modular forms in $W_0^+(5,\chi_5)$. For any $m \in \mathbb{Z}^+$ with $\chi_5(m) \neq -1$ there exists a unique $f_m = \sum_{n\geq -m} c_m(n)q^n \in W_0^+(5,\chi_5)$ whose Fourier expansion starts with

$$f_m = \begin{cases} q^{-m} + c_m(0) + O(q) & \text{if } p \nmid m \\ \frac{1}{2}q^{-m} + c_m(0) + O(q) & \text{if } p \mid m \end{cases}$$

and those f_m form a basis of $W_0^+(5,\chi_5)$. The Borcherds lift Ψ_m of f_m is a Hilbert modular form of weight $c_m(0) = -B_2^+/(m)$ for the group $\mathit{\Gamma}_F$ and has divisor T_m. The first few f_m are computed in [BB01]. Here we show the first coefficients of three of them (f_1, f_6, f_{10}).

$$\begin{aligned} f_1 &= q^{-1} + 5 + 11q - 54q^4 + \dots \\ f_6 &= q^{-6} + 10 + 264q - 136476q^4 + \dots \\ f_{10} &= \frac{1}{2}q^{-10} + 10 + 3400q + 3471300q^4 + \dots \end{aligned}$$

By looking at the constant terms we see that Ψ_1 has weight 5 and Ψ_6 and Ψ_{10} both have weight 10. Observing the coefficients of

$$E_2^+(\tau) = 1 - 10q - 30q^4 - 30q^5 - 20q^6 - 70q^9 - 20q^{10} - 120q^{11} - \dots$$

we see that the other Ψ_m for low values of m have higher weights and indeed the only three Borcherds lift of weight 10 are Ψ_1^2, Ψ_6 and Ψ_{10}. Let's compute their Borcherds product expansions explicitly.

When there are no elements $\lambda \in \mathfrak{d}_F^{-1}$ such that $-\lambda\lambda' = m/\Delta$, $S(m)$ is empty and there is only one Weyl chamber $((\mathbb{R}^+)^2)$ and the Weyl vector is 0. Note that $S(m)$ is empty when it does not exist an element λ in $\mathfrak{d}_F^{-1}$ such that $N(\lambda) = -m/\Delta = m/N(\sqrt{\Delta})$ but the norm is multiplicative, so $N(\sqrt{\Delta}\lambda) = m$ and now $\sqrt{\Delta}\lambda \in \mathcal{O}_F$. So $S(m)$ is empty when there is no element of norm m in $\mathcal{O}_F$. That's precisely what happens for $m = 6$ and $m = 10$ as proven in the next Lemma.

Lemma 3.14. *There are no solutions to* $N(x + y\frac{1+\sqrt{5}}{2}) = (x + \frac{y}{2})^2 - 5(\frac{y}{2})^2 = m$ *for* $m = 6$ *and* $m = 10$.

Proof. Multiplying by 4 to each side we can rewrite the equation as $(2x+y)^2 - 5y^2 = 4m$. For $m = 6$, taking the equation modulo 3, we must have $(2x + y)^2 \equiv 2y^2($ mod 3). But squares modulo 3 are either congruent to 0 or to 1, so we must have that both $2x + y$ and y are multiples of 3. But then $(2x + y)^2 - 5y^2$ is a multiple of 9 while 24 is not, which is a contradiction. For $m = 10$, we have $x^2 + xy - y^2 = 10$ by developing the squares and dividing by 4. Since the RHS is even, so must be the LHS. The only possibility for this to happen is that both x and y are even. But then the LHS is a multiple of 4 while the RHS is not. □

By the previous lemma, we have that

$$\Psi_6 = \prod_{\substack{\nu\in\mathfrak{d}_F^{-1} \\ (\nu,W)>0}} \left(1 - q_1^{\nu} q_2^{\nu'}\right)^{\widetilde{c}_6(5\nu\nu')} = \prod_{\substack{\nu\in\mathfrak{d}_F^{-1} \\ \nu\gg 0}} \left(1 - q_1^{\nu} q_2^{\nu'}\right)^{\widetilde{c}_6(5\nu\nu')}$$

$$\Psi_{10} = \prod_{\substack{\nu \in \mathfrak{d}_F^{-1} \\ (\nu, W) > 0}} \left(1 - q_1^{\nu} q_2^{\nu'}\right)^{\widetilde{c}_{10}(5\nu\nu')} = \prod_{\substack{\nu \in \mathfrak{d}_F^{-1} \\ \nu \gg 0}} \left(1 - q_1^{\nu} q_2^{\nu'}\right)^{\widetilde{c}_{10}(5\nu\nu')}$$

For $m = 1$, like in example 3.11, let W be the unique Weyl chamber of index 1 that contains $(\varepsilon_0^{-1}, \varepsilon_0^{-1})$. The corresponding Weyl vector is $\rho_1 = \frac{\varepsilon_0}{\sqrt{5}tr(\varepsilon_0)}$and the Borcherds lift has the form

$$\Psi_1 = q_1^{\rho_1} q_2^{\rho_1'} \prod_{\substack{\nu \in \mathfrak{d}_F^{-1} \\ \varepsilon_0\nu' - \varepsilon_0'\nu > 0}} \left(1 - q_1^{\nu} q_2^{\nu'}\right)^{\widetilde{c}_1(5\nu\nu')}$$

Note that for Ψ_6 and Ψ_{10} we have that $(\nu, W) > 0 \iff \nu \gg 0$ because we must have $\mathrm{tr}(\nu w_0) > 0$ both for $w_0 = (1, \varepsilon)$ and for $w_0 = (\varepsilon, 1)$ for arbitrary small ε, so $\nu, \nu' > 0$. And clearly if $\nu \gg 0$, $\mathrm{tr}(\nu w_0) > 0$ for any $w_0 \in (\mathbb{R}^+)^2$.

The divisors of $\Psi_1, \Psi_6, \Psi_{10}$ are the Hirzebruch-Zagier divisors T_1, T_6, T_{10} as the modular forms we lifted only have one non-zero coefficient $\widetilde{c}(n)$ for $n < 0$.

3.3 Evaluating Borcherds products numerically

If we want to evaluate numerically the values of Hilbert modular functions, it is usually not practical to use the expression of Theorem 3.12 because the infinite product only converges on a certain domain and even when it converges, there are other methods that converge faster. Also, in some cases where we are doing the product over a subset of $\mathfrak{d}_F$ that does not have a nice form, it is difficult to index the terms. The good news is that in some cases it is possible to obtain Borcherds lift from the Doi-Naganuma lift. In particular, it is possible to obtain $\Psi_1^2, \Psi_6, \Psi_{10}$ from the Doi-Naganuma lift, following the approach by Bruinier and Yang ([BY06]), and as we will see when we use this approach in the last chapter, we will have a fast convergence. Recall that the Doi-Naganuma lift takes modular forms on the space $M_k^+(p, \chi_p)$ to Hilbert modular forms and for an $f = \sum_{n \in \mathbb{Z}} c(n) q^n \in M_k^+(p, \chi_p)$, the Doi-Naganuma lift $\Phi(f)(z)$ satisfies

$$\Phi(f)(z) = -\frac{B_k}{2k}\widetilde{c}(0) + \sum_{\substack{\nu \in \mathfrak{d}_F^{-1} \\ \nu \gg 0}} \sum_{d | \nu} d^{k-1} \widetilde{c}\left(\frac{p\nu\nu'}{d^2}\right) q_1^{\nu} q_2^{\nu'}$$

where $z = (z_1, z_2)$,$q_j = e^{2\pi i z_j}$ and B_k is the k-th Bernoulli number. From the previous formula we see that $\Phi(f)(z_1, z_2) = \Phi(f)(z_2, z_1)$ because we sum over ν if only if we sum over ν', so the lift is symmetrical. The dimension of $M_{10}^+(5, \chi_5)$ is 3, so $S_{10}^+(5, \chi_5)$ has dimension 2. Let h_1, h_2 be a basis of it. Since the DN lift takes cusp forms to cusp forms, $\Phi(h_1), \Phi(h_2) \in S_{10}(\Gamma_F)$. If we consider $\Phi(h_j)(z, z)$ for $\mathrm{SL}_2(\mathbb{Z}) \subset \Gamma_F$ using the restriction to the diagonal trick of chapter 1, we get a classical elliptic modular form of weight 20 for $\mathrm{SL}_2(\mathbb{Z})$. Since the space of cusp forms of weight 20 has dimension 1, there is a linear combination $\lambda_1 h_1 + \lambda_2 h_2$ whose image by the lift H vanishes on the restriction of the diagonal. But it is possible to prove that the Hirzebruch-Zagier divisor T_1 is the orbit of $\{(\tau, \tau) \mid \tau \in \mathbb{H}^2\}$ under the action of $\mathrm{SL}_2(\mathcal{O}_F)$, which means that H vanishes in all the divisor T_1. Then H/Ψ_1 is an holomorphic Hilbert modular form of weight 5 for the group $\mathit{\Gamma}_F$. Gundlach build an antisymmetric modular form of weight 5, $\mathit{\Theta}$ as the product of theta functions and proved it to be a multiple of Ψ_1, so Ψ_1 is antisymmetric $(\Psi_1(z_1, z_2) = -\Psi_1(z_2, z_1))$ since $\mathit{\Theta}$ is. Since H is symmetric, H/Ψ_1 is also antisymmetric, so it vanishes again on the diagonal and therefore on T_1. That means that H/Ψ_1^2 is an holomorphic modular form of weight 0, and therefore it is constant (we saw this on chapter 1 in Proposition 1.29). Then Ψ_1^2 is a multiple of H and therefore on the image of $S_{10}^+(5, \chi_5)$ of the Doi-Naganuma lift. The exact modular form that maps to Ψ_1^2 can be determined by looking at which linear combination of the first coefficients of the images of h_1, h_2 give the first coefficients of Ψ_1^2.

Now, since $\mathit{\Gamma}_F$ only has one cusp (the class number of F is 1, so that follows from Corollary 1.9), the difference of Ψ_6 and a certain multiple of the image of $E_{10}^+(\tau)$ by the Doi-Naganuma lift will be in $S_{10}(\mathit{\Gamma}_F)$ (call it $\Psi_6 - H'$). Like before, a certain linear combination of h_1, h_2 has a Doi-Naganuma lift H'' such that $\Psi_6 - H' - H''$ is in $S_{10}(\mathit{\Gamma}_F)$ and vanishes on the diagonal and hence on T_1, so using the same argument as before, we get that it is a multiple of Ψ_1^2, which is a Doi-Naganuma lift. Then Ψ_6 is a Doi-Naganuma lift (for being the sum of two such lifts) and the same reasoning works for Ψ_{10}. The exact modular forms that lift Ψ_6 and Ψ_{10} can be found by looking at the first few coefficients of the Borcherds products expansion and looking at which modular forms when lifted give the same coefficients. The exact approach would be to lift all the elements of a basis of $M_{10}^+(5, \chi_5)$ and find a linear combination that gives the desired Borcherds product. The same linear combination with the basis elements will have the desired image by the Doi-Naganuma lift (by the linearity of the lift). This part can be a bit tedious, but can be done. However, we did not need it because in [BY06], Bruninier and Yang already give us the three modular forms g_1, g_6, g_{10} such that $DN(g_1) = \Psi_1^2$, $DN(g_6) = \Psi_6$, $DN(g_{10}) = \Psi_{10}$. Their Fourier expansions start with:

$$g_1 = q^4 - q^5 - q^6 - 18q^9 + 19q^{10} + \dots$$
$$g_6 = -132 - 264q + 306360q^4 - 271512q^5 - 236400q^6 + 1613256q^9 + \dots$$
$$g_{10} = -132 - 3400q + 4047800q^4 - 3834200q^5 - 5106800q^6 - 55443800q^9 + \dots$$

Therefore we can use SageMath to get a basis of $M_{10}^+(5, \chi_5)$ and find (using basic linear algebra) the only linear combination coincides for the first few coefficients. Once we have it must also coincide for the rest of the coefficients because it is the only modular form in $M_{10}^+(5, \chi_5)$ satisfying those constraints.

For evaluating the Borcherds products Ψ_1^2, Ψ_6 and Ψ_{10} at points of $\mathbb{H}^2$, since we have a summation formula for the Doi-Naganuma lift we can try to evaluate the first few terms in the sum hoping that it will converge with a lot of precision. We have to select the order in which to pick the values of the set $\{\nu \in \mathfrak{d}_F^{-1} \mid \nu \gg 0\}$ so that the convergence is as fast as possible. For a fixed ν, the inner sum is easy and finite as we only need to sum for those $d \in \mathbb{Z}$ such that $\nu/d \in \mathfrak{d}_F^{-1}$ and writting $\nu = x/\sqrt{5}$ for $x \in \mathcal{O}_F$, it is the same as summing over the $d \in \mathbb{Z}$ such that $x/d \in \mathcal{O}_F$. And writing $x = x_1 + x_2(\frac{1+\sqrt{5}}{2})$ it is equivalent to d dividing both x_1 and x_2.

To decide the order in which we perform the summation, we will write every $\nu = x/\sqrt{5}$ for $x \in \mathcal{O}_F$ and we will write $x = x_1 + x_2(\frac{1+\sqrt{5}}{2})$. For a given x_2 there are only finitely many x_1 that make $\nu \gg 0$. To see why this is true, note that

$$\nu = \frac{x_1}{\sqrt{5}} + \frac{x_2(1+\sqrt{5})}{2\sqrt{5}}$$

$$\nu' = -\frac{x_1}{\sqrt{5}} + \frac{x_2(-1+\sqrt{5})}{2\sqrt{5}}$$

so if $\nu, \nu' > 0$ isolating x_1 in both conditions and putting it together we need

$$x_2\frac{-1+\sqrt{5}}{2} > x_1 > -x_2\frac{1+\sqrt{5}}{2}$$

So we will start summing from $x_2 = 1$ up to some limit that we call the number of iterations which will usually be around 80 (even with 50 or even 30 we usually have a result with a relative error of less than 10^{-40}). And for each x_2 we will sum over all the possible values of x_1.

Note that the exponents of $q_1^{\nu}q_2^{\nu'}$ are of the form $2\pi i(\nu z_1 + \nu z_2)$ so for the convergence we are interested in its imaginary part $\nu\Im(z_1) + \nu'\Im(z_2)$. But

$$\nu\Im(z_1) + \nu'\Im(z_2) \geq (\nu + \nu')\min(\Im(z_1), \Im(z_2)) = x_2 \min(\Im(z_1), \Im(z_2))$$

So as x_2 grows $q_1^{\nu}q_2^{\nu'}$ decreases exponentially (it decreases because $e^{2\pi i i} = e^{-2\pi}$), while the coefficients of the modular form grow slower and $\sum_{d|\nu} d^{k-1}$ just grows like a polynomial. Note also that from this reasoning we can deduce that the greater the imaginary parts are, the faster the convergence should theoretically be.

In the last chapter we will use this approach to evaluate the Borcherds lifts at CM points. Although we may not get all Borcherds lifts in this way for any real quadratic field, the technique also works for fields other than $F = \mathbb{Q}(\sqrt{5})$. For instance, in a similar way one can obtain the 3 Borcherds products of weight 6 for $\mathbb{Q}(\sqrt{13})$, $\Psi_1^6, \Psi_{14}, \Psi_{26}$ as the images of the Doi-Naganuma lift of three modular forms in $M_6^+(13, \chi_{13})$ and evaluate in the same way. Actually the implementation that we give in the appendix works for $\mathbb{Q}(\sqrt{p})$ for any $p \equiv 1 \pmod 4$, and so it works for $p = 13$. We will also evaluate a few modular functions on $\mathbb{Q}(\sqrt{13})$ to show it.

Chapter 4

Complex Multiplication

For every elliptic curve, its endomorphisms ring contains $\mathbb{Z}$, but in some cases it is even bigger. The origin of the theory of Complex Multiplication comes from studying elliptic curves whose endomorphism ring is strictly larger than $\mathbb{Z}$. Those elliptic curves are said to have Complex Multiplication, and the aim of this study was to find a way to explicitly construct the class fields for some number fields, generalizing the Kronecker-Weber Theorem to number fields other than $\mathbb{Q}$. This problem is the well-known Hilbert's 12th problem, and a complete solution for imaginary quadratic is given by elliptic curves with Complex Multiplication.

Generalizing the theory for abelian varieties helps in constructing some class fields for other number fields (the so-called CM fields) and although it is some progress to solve Hilbert's 12th problem, we are still far from solving it completely.

In the following lines we summarize the main results of the theory of complex multiplication for elliptic curves, so that it serves as an introduction for the theory of Complex Multiplication for abelian varieties (a more general case) and for Hilbert modular surfaces (the case we are interested in). The results we will state can be found along with their proofs and a more extense discussion of the theory of complex multiplication for elliptic curves in [Cox89] and [Sil94].

4.1 Complex Multiplication for elliptic curves

4.1.1 The Weierstrass $\wp$-function and the j-invariant

Let E be an elliptic curve over $\mathbb{C}$. The equation of an elliptic curve can be transformed by doing an appropriate change of variables to be of the form $y^2 = 4x^3 + ax + b$ (this is true for any elliptic curve over a field of characteristic different from 2 and 3). Every elliptic curve of that form is isomorphic to a complex torus $\mathbb{C}/L$ where L is a lattice in $\mathbb{C}$. The isomorphism can be realized in the following way:

Recall that a lattice L is an additive subgroup of $\mathbb{C}$ which is generated by two non-zero complex numbers ω_1, ω_2 that are linearly independent over $\mathbb{R}$ (i.e. $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$), so $L = \{a\omega_1 + b\omega_2 \mid a, b \in \mathbb{Z}\}$ and we denote this lattice by $L = [\omega_1, \omega_2]$.

Definition 4.1. An elliptic function f for a lattice L is a function defined on $\mathbb{C}$

except maybe for isolated singularities, that satisfies:

1. $f(z)$ is meromorphic on $\mathbb{C}$.
2. $f(z+\omega) = f(z)$ for all $\omega \in L$.

The most important elliptic function (we will see why now) is the Weierstrass $\wp$-function, which is defined for a lattice L and a complex number z by:

$$\wp_L(z) = \frac{1}{z^2} + \sum_{\omega \in L-\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

The sum that defines it converges absolutely on any compact subset of $\mathbb{C}$ that doesn't contain a point in L. The importance of this function comes from the fact that it parametrizes elliptic curves using the following theorem:

Theorem 4.2. *Let $\wp_L(z)$ be the Weierstrass $\wp$-function for the lattice L. Then*

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(L)\wp(z) - g_3(L)$$

where $g_2(L)$ and $g_3(L)$ are constants defined by

$$g_2(L) = 60 \sum_{\omega \in L-\{0\}} \frac{1}{\omega^4} \qquad g_3(L) = 140 \sum_{\omega \in L-\{0\}} \frac{1}{\omega^6}$$

Now given a lattice L, we can consider the map $\phi : \mathbb{C}/L \to \mathbb{C}^2$ given by $z \mapsto (\wp_L(z), \wp_L'(z))$, so we see that $\mathbb{C}/L \cong E$ where E is the elliptic curve with equation $y^2 = 4x^3 - g_2(L)x - g_3(L)$. Conversely, given an elliptic curve E with equation $y^2 = 4x^3 + ax + b$, there exists a lattice L such that $g_2(L) = -a$, $g_3(L) = -b$ (see for instance [Cox89] Corollary 11.7), which means that every elliptic curve is isomorphic to a complex torus $\mathbb{C}/L$ for some lattice L. But note that any lattice $L = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ is isomorphic to a lattice of the form $L = \mathbb{Z} + \omega\mathbb{Z}$ where $\omega \in \mathbb{H}$ by choosing $\omega = \frac{\omega_1}{\omega_2}$ or $\omega = \frac{\omega_2}{\omega_1}$ (whichever makes $\omega \in \mathbb{H}$), since $\mathbb{Z} + \omega Z = \omega_1^{-1}L$ or $\mathbb{Z} + \omega Z = \omega_2^{-1}L$. Therefore, we can identify any elliptic curve with a $\tau \in \mathbb{H}$.
Now, given a lattice L we can define the j-invariant of the lattice to be

$$j(L) = 1728 \frac{g_2(L)^3}{g_2(L)^3 - 27g_3(L)^2}$$

where g_2, g_3 are defined as above. We can extend this definition to define the j-invariant of an elliptic curve E by

$$j(E) = j(\mathbb{C}/L) = j(L)$$

Using the definition of g_2, g_3 and of j for a lattice, it is easy to prove that if $L' = \lambda L$ is homothetic to L, they have the same j-invariant (see [Cox89] Theorem 10.9), so the j-invariant of an elliptic curve is well defined.

Furthermore, we can define it on the upper half plane $\mathbb{H}$ by letting $j(\tau) = j([1,\tau])$ for $\tau \in \mathbb{H}$. It turns out that j is an holomorphic function on $\mathbb{H}$ that is $\mathrm{SL}_2(\mathbb{Z})$-invariant, so it is a modular function for $\mathrm{SL}_2(\mathbb{Z})$. Its Fourier expansion is given by $j(\tau) = \frac{1}{q} + 744 + 196884q + \dots$ where $q = e^{2\pi i\tau}$.

4.1.2 The ring of endomorphisms of an elliptic curve

The endomorphisms ring $\mathrm{End}(E)$ of an elliptic curve $E = \mathbb{C}/L$ can be identified with $\{\alpha \in \mathbb{C} \mid \alpha L \subset L\}$ using the isomorphism between E and $\mathbb{C}/L$. Clearly $\mathbb{Z} \subset \mathrm{End}(E)$, but there are cases in which the set $\mathrm{End}(E)$ is even bigger. In this case we say that E has complex multiplication. The name comes from the fact that in this case $\{\alpha \in \mathbb{C} \mid \alpha L \subset L\}$ is an order $\mathcal{O}$ in an imaginary quadratic extension of $\mathbb{Q}$.

Orders in imaginary quadratic fields gives rise to lattices in a natural way. For an order $\mathcal{O}$ in a imaginary quadratic field K, and a proper fractional $\mathcal{O}$-ideal $\mathfrak{a}$, we can write $\mathfrak{a} = [\alpha, \beta]$ for some $\alpha, \beta \in K$ that are linearly independent over $\mathbb{R}$. Since we can see K as a subset of $\mathbb{C}$, $\mathfrak{a} = [\alpha, \beta]$ is a lattice in $\mathbb{C}$, so we can define the j-invariant of a proper fractional ideal $j(\mathfrak{a})$.

If an elliptic curve has complex multiplication by an order $\mathcal{O}$, then $E \cong \mathbb{C}/\mathfrak{a}$ for some fractional ideal $\mathfrak{a}$ of $\mathcal{O}$. The converse is also true, and two elliptic curves $\mathbb{C}/\mathfrak{a}$ and $\mathbb{C}/\mathfrak{b}$ are isomorphic if and only if $\mathfrak{a}$ and $\mathfrak{b}$ are in the same ideal class, which means that the number of isomorphism classes of elliptic curves with complex multiplcation by $\mathcal{O}$ is the class number of $\mathcal{O}$. By adjoining the values of the j-invariant at the ideals of an order to K we get the ring class field of $\mathcal{O}$. More explicitly, if $\mathfrak{a}$ is a proper fractional ideal of $\mathcal{O}$, $K(j(\mathfrak{a}))$ is the ring class field of $\mathcal{O}$.

In particular, if we focus to the case where the order is the ring of integers $\mathcal{O}_K$, $K(j(\mathfrak{a}))$ is the Hilbert class field of K (the maximal unramified abelian extension of K). Furthermore, if $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ are the representatives of the ideal class group of K, we have that $[\mathbb{Q}(j(\mathfrak{a}_i)) : \mathbb{Q}] = [K(j(\mathfrak{a}_i)) : K] = h$ for any $i \in \{1, 2, \ldots, h\}$ and that $j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_h)$ are conjugate algebraic integers. The minimal polynomial of $j(\mathfrak{a}_i)$ over $\mathbb{Q}$ is the one with roots $j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_h)$, so the independent term of this polynomial

$$\prod_{i=1}^{h} j(\mathfrak{a}_i) \in \mathbb{Z}$$

As a particular case, when K has class number 1, $j(\mathcal{O}_K)$ is an integer.

Since $\mathbb{H}$ parametrizes classes of elliptic curves and we saw that the j-invariant is a modular function $j : \mathbb{H} \to \mathbb{C}$ whose value $j(\tau)$ coincides with the value $j([1, \tau])$, we can rewrite all the previous discussion for points in $\mathbb{H}$. A point $\tau \in \mathbb{H}$ is called a CM point of type $\mathcal{O}_K$ if the elliptic curve $E_\tau = \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$ has complex multiplication $\mathcal{O}_K$. Then, in view of what we just said, the values of the j-function on CM points (known as singular moduli) are algebraic integers that generate the Hilbert class field of K. And if we consider $\mathcal{CM}(K)$, all the CM points of type $\mathcal{O}_K$, the Galois group $\mathrm{Gal}(H/K)$ acts transitively on them, and

$$j(\mathcal{CM}(K)) = \prod_{\tau \in \mathcal{CM}(K)} j(\tau) \in \mathbb{Z}$$

4.2 Differences in the theory of Complex Multiplication for higher dimension abelian varieties

There are some changes that need to be made to generalize the theory of Complex Multiplication and some concepts that we have to introduce. Since the endomorphism rings now will have higher dimension we won't be embedding orders in imaginary quadratic fields into them. We will embed imaginary quadratic extensions of totally real field, which are known as CM fields. In the case of elliptic curves there is only one canonical way to embed it because there are only two embeddings which are complex conjugate to each other. In the general case for a variety of dimension n, we have $2n$ embeddings. We will choose n of them such that no two are complex conjugate (this will be called a CM type) and depending on the choice we will get different results (not always).

In the case of elliptic curves the j-invariant was really important as it described helped building the Hilbert class field, but its importance also relies on the fact that it is the moduli space of elliptic curves (its value determines the isomorphism class of elliptic curves). For higher dimensional abelian varieties it is hard to generalize this because they have too many automorphisms and we can't find a moduli space in a similar way. However, there's a way to solve this problem and it is by considering abelian varieties with a polarization (in the case of elliptic curves polarizations are unique, so we can forget about them).

Since the points on the moduli space parametrize isomorphism classes of abelian varieties with CM, to understand the shape of the values of modular functions at those points, we will need to understand how abelian varieties transform under automorphisms of $\mathbb{C}$. We will require automorphisms σ of $\mathbb{C}$ on an abelian variety ($A \mapsto \sigma(A)$) to preserve the CM type. But this means that σ won't necessarily fix the field K. It fixes a field generate by all symmetric expresions on the values of the CM type and it is called the reflex field of K. We won't construct class fields for K but for the reflex field.

In terms of the results obtained, for the general case the theory of complex multiplication does not generate all abelian extensions of the CM field. In some cases this can be fixed by using a combination of complex multiplication and class field theory, like Shimura did, but were are not gonna get into the details of that because our main goal is not constructing all the class fields.

Now, we begin by defining one of the main objects of study in this chapter, the CM fields (along with their CM types) and their reflex fields.

4.3 CM-fields

Definition 4.3. A CM-field K is a totally imaginary extension (i.e. it cannot be embedded into the real numbers) of a totally real number field K_0 (all of its embeddings into $\mathbb{C}$ are real). Equivalently, a CM-field is a field $K = K_0(\sqrt{\alpha})$ where K_0 is a totally real number field and $\alpha \in K_0$ is a totally negative element (i.e. the image of α for all embeddings of K_0 into $\mathbb{C}$ is a negative real).

Example 4.4. For the n-th root of unity $\xi = e^{2\pi i/n}$ $(n > 2)$, $\mathbb{Q}(\xi)$ is a totally imaginary quadratic extension of the totally real field $\mathbb{Q}(\xi + \xi^{-1})$, and therefore it is a CM-field.

Now, we proceed to prove a characterization of CM-fields that will be very useful to prove that certain number fields that will appear later are CM-fields.

Proposition 4.5. *A number field K is a CM-field if only if the next two conditions are both satisfied*

(i) Complex conjugation induces a non-trivial automorphism of K

(ii) Every embedding of K into $\mathbb{C}$ commutes with complex conjugation

Proof. Assume that $K = K_0(\sqrt{\alpha})$ is a CM-field which, by definition, is an imaginary quadratic extension of the totally real field K_0 and write an element z of K as $x+y\sqrt{\alpha}$ where $x, y \in K_0 \subset \mathbb{R}$ and $\alpha < 0$ is also a real number. Then, clearly $\overline{z} = x - y\sqrt{\alpha} \in K$ (where $\overline{\cdot}$ denotes complex conjugation) and the first condition is satisfied. Let's see the second condition. Pick an embedding σ of K into $\mathbb{C}$. Then $\sigma(x), \sigma(y)$ are both real numbers as they belong to K_0. And $\sigma(\sqrt{\alpha})$ satisfies $\sigma(\sqrt{\alpha})^2 = \sigma(\alpha)$ which is a negative real number (recall that α is totally negative real number by the definition of CM field), so $\sigma(\sqrt{\alpha})$ is the square root of a negative real. Then we have

$$\overline{\sigma(z)} = \overline{\sigma(x) + \sigma(\sqrt{\alpha})\sigma(y)} = \sigma(x) - \sigma(\sqrt{\alpha})\sigma(y) = \sigma(\overline{z})$$

so conjugation commutes with any embedding and the second condition is proved.

Assume now that the two conditions are satisfied and let K_0 be the field that is fixed by complex conjugation. Note that it is properly contained in K as we know by the first condition that complex conjugation is a non-trivial automorphism, which means that not all elements of K are fixed by it. Since complex conjugation is an automorphism of order 2, we have that $[K : K_0] = 2$ and therefore, $K = K_0(\sqrt{\alpha})$ for $\alpha \in K_0$. So we only need to see that α is totally negative and that K_0 is totally real. For an embedding σ from K_0 to $\mathbb{C}$ and any $x \in K_0$, by the second condition, we have

$$\overline{\sigma(x)} = \sigma(\overline{x}) = \sigma(x)$$

where the last equality comes from the fact that K_0 is fixed by complex conjugation and therefore $x = \overline{x}$. But from $\overline{\sigma(x)} = \sigma(x)$ we deduce that $\sigma(x) \in \mathbb{R}$. Since that's true for any $x \in K_0$ and any embedding, K_0 is totally real. Finally, if we extend σ to an embedding of K into $\mathbb{C}$, we have that $\sigma(\sqrt{\alpha})^2 = \sigma(\alpha)$. If for some σ, $\sigma(\alpha)$ was non-negative, $\sigma(\sqrt{\alpha})$ would be real, and therefore

$$\sigma(\sqrt{\alpha}) = \overline{\sigma(\sqrt{\alpha})} = \sigma(\overline{\sqrt{\alpha}})$$

meaning that $\sqrt{\alpha}$ is real since an embedding is injective. But this is a contradiction, since the first condition says that conjugation induces a non-trivial automorphism on K. Therefore, $\sigma(\alpha) < 0$ for all σ and α is totally negative. This finishes the proof of the proposition. □

As a consequence of this proposition, it is easy to see that the following two results are true.

Lemma 4.6. *The composite of CM-fields is a CM-field.*

Proof. Any embedding on the composite of two fields F_1, F_2 induces an embedding in those two fields, so complex conjugation induces a non-trivial embedding on the composite (it is not trivial on F_1, F_2) and every embedding commutes with complex multiplication because it induces an embedding on F_1 and another on F_2 that commute with complex conjugation. □

Lemma 4.7. *The Galois closure of a CM-field is a CM-field.*

Proof. Let K be a CM-field and L its Galois closure. L clearly satisfies condition one in Proposition 4.5 because by restricting it to K it is non-trivial, and so it must be true for L. Let's check the second condition. Write $K = \mathbb{Q}(\alpha_1)$ and $L = \mathbb{Q}(\alpha_1, \dots, \alpha_r)$ where $\alpha_1, \dots, \alpha_r$ are the roots of the minimal polynomial of α_1. For every j, there is an embedding ϕ_j that sends α_1 to α_j. Take any $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ we want to see that it commutes with complex conjugation, so it is enough to see that for every α_j, $\overline{\sigma(\alpha_j)} = \sigma(\overline{\alpha_j})$. But

$$\overline{\sigma(\alpha_j)} = \overline{\sigma(\phi_j(\alpha_1))} = \sigma(\phi_j(\overline{\alpha_1})) = \sigma(\overline{\phi_j(\alpha_1)}) = \sigma(\overline{\alpha_j})$$

because both ϕ_j and $\sigma \circ \phi_j$ are embeddings from K to $\mathbb{C}$, so they commute with complex conjugation. This proves the second condition and the lemma. □

4.3.1 CM-types

Definition 4.8. For a CM-field K a CM-type $\Phi = \{\phi_1, \phi_2, \dots, \phi_n\}$ on K is a set of complex embeddings such that no two of them are complex conjugates of each other and for any embedding ϕ, either ϕ or $\overline{\phi} \in \Phi$. Equivalently, $\Phi = \{\phi_1, \phi_2, \dots, \phi_n\}$ and $\overline{\Phi} = \{\overline{\phi_1}, \overline{\phi_2}, \dots, \overline{\phi_n}\}$ are a partition of the embeddings of K into $\mathbb{C}$.

We say that (K, Φ) is a CM-type to make clear with respect to which CM field but sometimes we also refer to Φ as the CM type.

Definition 4.9. For a CM-type (K, Φ) and for every $x \in K$, we define the determinant and the trace to be:

$$\det(\Phi(x)) = \prod_{j=1}^{n} \phi_j(x)$$

$$\mathrm{tr}(\Phi(x)) = \sum_{j=1}^{n} \phi_j(x)$$

Definition 4.10. Two CM types Φ_1, Φ_2 of K are called equivalent if there is an automorphism K such that $\Phi_2 = \Phi_1 \circ \sigma$.

Definition 4.11. We say that a CM type (K, Φ) is primitive if it is not induced by a CM type on a proper CM subfield $\widetilde{K} \subset K$. That is, we can't define the CM type (K, Φ) by picking a CM type $(\widetilde{K}, \widetilde{\Phi})$ and choosing the set of embeddings from K into $\mathbb{C}$ such that when restricted to $\widetilde{K}$ lie in $\widetilde{\Phi}$.

We will give some examples of primitive and non-primitive CM types when we talk about quartic CM fields (and actually characterize all of them).

4.3.2 Reflex field

Let (K, Φ) be a CM-type. In the following lines we are going to describe how we can associate to it another pair of CM field and CM-type, called the reflex of (K, Φ). To start, we define the field of the associated pair, the reflex field. There are two equivalent definitions and we will see both. The first one gives an explicit formula and the second an interpretation using Galois Theory.

Definition 4.12. The reflex field K^r for a CM-type (K, Φ) is defined to be the field generated by adjoining $\mathrm{tr}(\Phi(x))$ to $\mathbb{Q}$ for all $x \in K$. Explicitly:

$$K^r = \mathbb{Q}\left(\{\mathrm{tr}(\Phi(x))\}_{x\in K}\right) = \mathbb{Q}\left(\left\{\sum_{j=1}^{n} \phi_j(x)\right\}_{x\in K}\right)$$

Proposition 4.13. *The reflex field K^r is a CM-field.*

Proof. First of all note that K^r is a finite extension of $\mathbb{Q}$. That's true because if $L/\mathbb{Q}$ is the Galois closure of K, then $K^r \subset L$ (since we have that $\phi(x) \in L$ for any $x \in K$ and any embedding $\phi : K \hookrightarrow \mathbb{C}$) and the Galois closure is always a finite extension. Now let's use Proposition 4.5 to prove that K^r is a CM field. We just need to check that both conditions are satisfied. To prove the first one, just note that since K is a CM-field, conjugation commutes with every embedding, so for any $x \in K$, $\overline{\mathrm{tr}(\Phi(x))} = \mathrm{tr}(\Phi(\overline{x})) \in K^r$ (since $\overline{x} \in K$), and therefore complex conjugation induces an automorphism on K^r. It is non-trivial because if it wasn't, we would have $\overline{\mathrm{tr}(\Phi(x))} = \mathrm{tr}(\Phi(x))$ for all $x \in K$, so we would have

$$\mathrm{tr}(\Phi(\overline{x})) = \mathrm{tr}(\Phi(x)) \iff \sum_{i=1}^{n} \phi_i(\overline{x}) = \sum_{i=1}^{n} \phi_i(x) \iff \sum_{i=1}^{n}((\phi_i \circ h) - \phi_i)(x) = 0$$

where h denotes complex conjugation. However, this means that $\sum_{i=1}^{n}((\phi_i \circ h) - \phi_i) = 0$ but by the Dirichlet theorem of independence of characters (see [Mil21] Theorem 5.14), we must have that $\Phi \circ h = \Phi$ which is a contradiction since Φ is a CM-type.

To see the second condition for K^r, take any $\sigma \in \mathrm{Aut}(\mathbb{C})$, and note that applying the second condition for K, we have:

$$\overline{\sigma(\mathrm{tr}(\Phi(x)))} = \sum_{i=1}^{n} \overline{(\sigma \circ \phi_i)(x)} = \sum_{i=1}^{n} (\sigma \circ \phi_i)(\overline{x}) = \sum_{i=1}^{n} \sigma(\overline{\phi_i(x)}) = \sigma(\overline{\mathrm{tr}(\Phi(x))})$$

since $(\sigma \circ \phi_i)$ is an embedding from K into $\mathbb{C}$ and hence it commutes with complex conjugation, and the same applies to ϕ_i. Therefore K^r satisfies the second condition and is a CM-field. □

Next, we will use Galois theory to give an equivalent definition for the reflex field K^r that will be helpful to define the reflex type of (K, Φ). Let L be the Galois closure of $K/\mathbb{Q}$ and G its Galois group. In the proof of the previous proposition, we saw that $K^r \subset L$. Let H and H' denote the subgroups of G that fix K and K^r (fundamental theorem of Galois theory). We get the following diagrams of extensions and of the groups that fix them:

$$\begin{tikzcd}
 & L \arrow[dl, dash] \arrow[dr, dash] & \\
K \arrow[dr, dash] & & K^r \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \{1\} \arrow[dl, dash] \arrow[dr, dash] & \\
H \arrow[dr, dash] & & H' \arrow[dl, dash] \\
 & G &
\end{tikzcd}$$

For every element σ of G, we have that $\sigma|_K \in \Phi \cup \overline{\Phi}$ since that's the set of embeddings of K into $\mathbb{C}$. And those are all the possible embeddings of K, because every embedding of K can be extended to an element $\sigma \in G$. Denote by $\widetilde{\phi_i}$ the extension of $\phi_i \in \Phi$ to an embedding of L, which is an automorphism since L is a Galois extension.

Now if we pick two automorphisms, $\sigma, \sigma' \in G$ that agree on K, then $\sigma^{-1}\sigma'$ fixes K, so $\sigma^{-1}\sigma' \in H \implies \sigma' H = \sigma H$, which means that if we descompose G into right cosets σH, two elements are in the same coset if when restricted to K they give the same embedding. Therefore since all the elements $\{\widetilde{\phi_1}, \widetilde{\phi_2}, \ldots, \widetilde{\phi_n}, \widetilde{\overline{\phi_1}}, \ldots \widetilde{\overline{\phi_n}}\}$ are different when restricted to K (they are extensions of different embeddings), we can write G in the following way:

$$G = \bigcup_{i=1}^{n} \widetilde{\phi_i} H \cup \bigcup_{i=1}^{n} \overline{\widetilde{\phi_i}} H = S \cup \overline{S}$$

where $S = \bigcup_{i=1}^{n} \widetilde{\phi_i} H$, and all unions are disjoint, so $S \cap \overline{S} = \emptyset$.

With the following proposition, we are going to characterize H', and therefore K^r as it is the field fixed by H'.

Proposition 4.14. *Let H, H' and G be the groups defined above (fixing K, K^r and $\mathbb{Q}$, respectively) and let $S = \bigcup_{i=1}^{n} \widetilde{\phi_i} H$ where the $\widetilde{\phi_i}$ are extensions of the embeddings of K to automorphisms of L. Then*

$$H' = \{g \in G \mid gS = S\}$$

Proof. If $g \in G$ and $Sg = S$, we want to see that $g \in H'$, or equivalently, that g fixes K^r. But clearly g fixes $\mathbb{Q}$, so it is enough to see that g fixes $\operatorname{tr}(\Phi(x))$ for all $x \in K$. But from $gS = S$, we deduce that that g just permutes the cosets of S, and since restricted to K all elements in a coset give the same embedding, we have that

$$\operatorname{tr}(\Phi(x)) = \sum_{i=1}^{n} \widetilde{\phi}_i(x) = \sum_{i=1}^{n} (g \circ \widetilde{\phi}_i)(x) = g \circ \operatorname{tr}(\Phi(x))$$

because recall that $\widetilde{\phi}_i(x) = \phi_i(x)$ for $x \in K$.

Conversely, if $g \in H'$, it means that for any $x \in K$

$$\sum_{i=1}^{n} \widetilde{\phi}_i(x) = \sum_{i=1}^{n} (g \circ \widetilde{\phi}_i)(x)$$

and now we can apply Dirichlet's independence of characters theorem for embeddings to get that $gS = S$. □

With this proposition, we can characterize the reflex field of a CM-type (K, Φ) as the fixed field for the automorphisms $\sigma \in \operatorname{Aut}(L/\mathbb{Q})$ such that $\sigma \circ \Phi = \Phi$ (where the composition is done elementwise). So we can view it as the field that is generated by adjoining any symmetric polynomial expression in $(\phi_1(x), \dots, \phi_n(x))$. To be clear, if f is a symmetric polynomial in n variables, then for any $\sigma \in H'$ and any $x \in K$, we have that $\sigma(f(\phi_1(x), \dots, \phi_n(x))) = f(\phi_1(x), \dots, \phi_n(x))$ because σ permutes the ϕ_i. And clearly, we don't need to adjoin anything else as

$$K^r = \mathbb{Q}\left(\{\operatorname{tr}(\Phi(x))\}_{x \in K}\right)$$

and $\operatorname{tr}(\Phi(x))$ is a symmetric polynomial expression of the type we mentioned before.

Now we can proceed to define the reflex type. Proposition 4.14 implies that $H' = \{g \in G \mid S^{-1}g = S^{-1}\}$ where $S^{-1} = \{\sigma^{-1} \mid \sigma \in S\}$. The elements of S^{-1} are elements of G, so if we consider their restriction on K^r and remove duplicates, we get $\psi_1, \psi_2, \dots, \psi_m$, distinct embeddings of K^r into $\mathbb{C}$. Call $\widetilde{\psi}_i$ one of the elements of S^{-1} (if there is only one there is no choice) such that when restricted to K^r gives ψ_i. Then by these observations

$$S^{-1} \subset \bigcup_{i=1}^{m} \widetilde{\psi}_i H' \subset S^{-1}H' = S^{-1} \implies S^{-1} = \bigcup_{i=1}^{m} \widetilde{\psi}_i H'$$

Recall that from Lemma 4.7, the Galois closure of a CM-field is also a CM-field, so complex conjugation commutes with all elements, which tells us that $\sigma \in S \implies \sigma^{-1} \in S^{-1}$ and if $\sigma \in \overline{S}$, then $\sigma^{-1} \in \overline{S}^{-1} = \overline{S^{-1}}$ (due to the commutation of conjugation with any element of G), so

$$G = S^{-1} \cup \overline{S^{-1}} \text{ and } S^{-1} \cap \overline{S^{-1}} = \emptyset$$

so $\psi_1, \dots, \psi_m, \overline{\psi_1}, \dots, \overline{\psi_m}$ are all the embeddings of K^r into $\mathbb{C}$ so $\{\psi_1, \dots, \psi_m\}$ is a CM-type Φ^r on K^r. Then $[K^r : \mathbb{Q}] = [G : H'] = 2m$ is the degree of the reflex field over $\mathbb{Q}$.

Definition 4.15. The type (K^r, Φ^r) defined above is called the reflex type of (K, Φ).

Note that we found an explicit way to build Φ^r by finding the inverses of the elements of Φ as elements of the Galois group of the Galois closure, and then restricting them to K^r.

Example 4.16. Suppose that (K, Φ) is a CM-type and $K/\mathbb{Q}$ is Galois. Then $L = K$ in all the previous discussion and $H = \{1\}$, so $S = \Phi = \{\phi_1, \ldots, \phi_n\}$ and $S^{-1} = \{\phi_1^{-1}, \ldots, \phi_n^{-1}\}$. We know that $K^r \subset K$, so $\Phi^r \subset S^{-1}$ but we can't say much more if we don't know anything else about Φ. However, in some concrete cases we can say something else. For instance, if $K = \mathbb{Q}(\alpha)$ is a quadratic imaginary extension of $\mathbb{Q}$, then we know that $K = K^r$ and $\Phi = \Phi^r$. More generally, if K is Galois and Φ is primitive, $(K^r, \Phi^r) = (K, \Phi^{-1})$.

4.3.3 Type norm map

We proceed to define the type norm map for a CM type Φ of a CM field K.

Definition 4.17. Let K be a CM field and Φ a CM type of K. The type norm map $N_\Phi : K \to K^r$ is defined by

$$x \mapsto \prod_{\phi \in \Phi} \phi(x)$$

Lemma 4.18. *The type norm map is well defined, i.e. its image lies on K^r, the reflex field of K.*

Proof. Let L be the Galois closure of K. In the prove of the equivalent definition of the reflex field, we saw that $K^r \subset L$. To prove that the image of the type norm lies on K^r, we only need to see that it is fixed by the elements $\sigma \in \mathrm{Gal}(L/K^r)$, which are the elements in the group H' that appeared in the discussion of the definition of the reflex field using Galois theory. But that is just Proposition 4.14. □

Lemma 4.19. *Let Φ be a CM type on a CM field K with Galois closure L, and denote by I_K the group of ideals of K. The type norm map induces homomorphisms $N_\Phi : I_K \to I_{K^r}$ and $N_\Phi : \mathrm{Cl}(K) \to \mathrm{Cl}(K^r)$ (on the class group) mapping*

$$\mathfrak{a} \mapsto \mathfrak{a}' \text{ where } \mathfrak{a}'\mathcal{O}_L = \prod_{\phi \in \Phi} \phi(\mathfrak{a})\mathcal{O}_L$$

Note that we have to include the ring of integers of the Galois closure so that the ideals and their image are both ideals of the same field. For the proof of this lemma, see [Shi98], proposition 29 in section 8.3.

As it is shown by [Str10] in Lemma 7.2, the reflex field of the reflex field of K is a subfield of K and in the particular case that Φ is primitive, they are exactly equal (the reflex type of the reflex type also coincides in this case). Therefore we can also define a dual type norm map $N_{\Phi^r} : K^r \to K$, which is well defined (and it can also be extended to an homomorphism of ideals and classes of ideals).

It is not hard to see that

$$\begin{aligned} N_\Phi(x)\overline{N_\Phi(x)} &= N_{K/\mathbb{Q}}(x) \text{ for all } x \in K^* \\ N_\Phi(\mathfrak{a})\overline{N_\Phi(\mathfrak{a})} &= N_{K/\mathbb{Q}}(\mathfrak{a}) \text{ for all } \mathfrak{a} \in I_K \end{aligned} \tag{4.1}$$

since the left hand side is the product of the images by all the embeddings of K. We will use this fact later to see that a certain map is well defined.

Now we proceed to study quartic CM fields. We will motivate why later but they will be a central object in the chapter.

4.4 Quartic CM fields

The first step is to characterize all the possibilities for quartic CM fields. The totally real subfield associated to a CM field of degree 4 must be a degree 2 real field, and therefore, it must be a real quadratic field of the form $F = \mathbb{Q}(\sqrt{d})$ for $d > 0$ (we used D in the first chapter to avoid the confusion with matrix entries, but for the rest of the chapter we will use d). Now the CM field K must be equal to $F(\sqrt{\alpha})$ for $\alpha \in F$, a totally negative element which can be written as $\alpha = r+s\sqrt{d}$ for $r, s \in \mathbb{Q}$. It turns out that depending on α there are 3 types of CM extensions (biquadratic, cyclic Galois and non-Galois), as we will see now. First we distinguish whether $K = F(\sqrt{r + s\sqrt{d}})$ is Galois or not.

If K is Galois there are two possibilities for the Galois group of K as there are only two groups of order 4. It can be $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Case 1: $\mathrm{Gal}(K/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

There exists an element $\rho \in \mathrm{Gal}(K/\mathbb{Q})$ that corresponds to complex conjugation, and another element of order 2 that we will call σ. The Galois group is $\mathrm{Gal}(F/\mathbb{Q}) = \{1, \sigma, \rho, \sigma\rho\}$ and contains three subgroups of order 2: $G_1 = \{1, \rho\}$, $G_2 = \{1, \sigma\}$, $G_3 = \{1, \rho\sigma\}$. The group G_1 consists of the elements of K that are fixed by complex conjugation, so it is $\mathbb{Q}(\sqrt{d})$. Since the field fixed by G_2 has degree two, it is of the form $\mathbb{Q}(\sqrt{a})$ for some $a \in \mathbb{Q}$ such that $a < 0$. If it was positive it would also be fixed by G_1. Now $\mathbb{Q}(\sqrt{d}, \sqrt{a})$ contains both $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{a})$ but clearly it is not equal to any of them since $\mathbb{Q}(\sqrt{d})$ is totally real and $\mathbb{Q}(\sqrt{d}, \sqrt{a})$ is not and $\sqrt{d} \notin \mathbb{Q}(\sqrt{a})$ because that would mean $\sqrt{d} = x + y\sqrt{a} \implies d = x^2 + y^2a + 2xy\sqrt{a}$ which is impossible unless $xy = 0$. And $y = 0 \implies \sqrt{d} \in \mathbb{Q}$, $x = 0 \implies \sqrt{d} = y\sqrt{a}$ which is not real. So we have that $K = \mathbb{Q}(\sqrt{d}, \sqrt{a})$, and the third subfield of order two must be $\mathbb{Q}(\sqrt{ad})$. The diagram of the corresponding subextensions is given on the left. On the right we can see the group that fixes each field according to Galois theory.

$$\begin{tikzcd}
& K=\mathbb{Q}(\sqrt{d},\sqrt{a}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
F=\mathbb{Q}(\sqrt{d}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{a}) \arrow[d, dash] & \mathbb{Q}(\sqrt{da}) \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}
& \{1\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\{1,\rho\} \arrow[dr, dash] & \{1,\rho\sigma\} \arrow[d, dash] & \{1,\sigma\} \arrow[dl, dash] \\
& \{1,\rho,\sigma,\sigma\rho\} &
\end{tikzcd}$$

Case 2: $\mathrm{Gal}(K/\mathbb{Q}) = \mathbb{Z}/4\mathbb{Z}$.

The group is cyclic so it is generated by one element σ, and $\mathrm{Gal}(K/\mathbb{Q}) = \{1, \sigma, \sigma^2 = \rho, \sigma^3\}$ (ρ, complex conjugation, must be σ^2 because it is the only embedding of order 2). If $K = F(\sqrt{\alpha})$ where $\alpha = r + s\sqrt{d}$, the minimal polynomial of $\sqrt{\alpha}$ over $\mathbb{Q}$ is a degree 4 polynomial and the Galois group permutes the roots of this polynomial. It is not hard to find this polynomial because $x = \sqrt{r + s\sqrt{d}} \implies x^2 - r = s\sqrt{d} \implies (x^2 - r)^2 = s^2 d \implies x^4 - 2rx^2 + r^2 - s^2 d = 0$. It is a monic polynomial with coefficients in $\mathbb{Q}$ of degree 4, and hence it must be the minimum polynomial of α. The roots of this polynomial are given by

$$x^2 = \frac{2r \pm \sqrt{4r^2 - 4(r^2 - s^2 d)}}{2} \iff x = \pm\sqrt{r \pm s\sqrt{d}}$$

So σ must send $\sqrt{\alpha} = \sqrt{r + s\sqrt{d}}$ to one of the other roots. Since α is totally negative, it can't send it to $-\sqrt{r + s\sqrt{d}}$ because that corresponds to complex conjugation ($\sigma^2 = \rho$). It turns out that we can define σ to be the embedding that sends $\sqrt{\alpha}$ to any of the other two options. Let $\sigma(\sqrt{\alpha}) = \sigma(\sqrt{r + s\sqrt{d}}) = \sqrt{r - s\sqrt{d}} = \sqrt{\alpha'}$, which means that both $\sqrt{\alpha}$ and $\sqrt{\alpha'}$ belong to K. Then $\sigma(\sigma(\sqrt{\alpha})) = -\alpha$ (since σ^2 is complex conjugation and α is pure imaginary. So $\sigma(\sqrt{\alpha'}) = -\alpha$.

Case 3: $K/\mathbb{Q}$ is not Galois.

In a similar way to the previous case, we get that the roots of the minimal polynomial of $\sqrt{\alpha} = \sqrt{r + s\sqrt{d}}$ are $\pm\sqrt{r \pm s\sqrt{d}}$. The difference now is that $\sqrt{r - s\sqrt{d}} \notin K$ (as this would mean that all the roots belong to K and K would be Galois). Therefore, $F(\sqrt{\alpha}) \neq F(\sqrt{\alpha'})$. Note that $\alpha\alpha' = r^2 - s^2 d > 0$ since α is totally negative and $\sqrt{r^2 - s^2 d} \notin F$ because then $\sqrt{r - s\sqrt{d}} = \frac{\sqrt{r^2 - s^2 d}}{\sqrt{r + s\sqrt{d}}} \in F(\sqrt{r + s\sqrt{d}}) = K$ contradicting our assumption. Therefore, $\mathbb{Q}(\sqrt{\alpha\alpha'})$ is a quadratic extension different from $F = \mathbb{Q}(\sqrt{d}))$. Let $L = \mathbb{Q}(\sqrt{\alpha}, \sqrt{\alpha'})$. Then L is normal because so is $\mathbb{Q}$ and adjoining normal elements gives a normal extension ($\sqrt{\alpha}$, $\sqrt{\alpha'}$ are normal because their minimal polynomial is the one that we have previously seen and decomposes in linear factors over L because their roots are $\sqrt{\alpha}, \sqrt{\alpha'}, -\sqrt{\alpha}, -\sqrt{\alpha'}$). But since $L = K(\sqrt{r^2 - s^2 d})$

because $\sqrt{r-s\sqrt{d}} = \frac{\sqrt{r^2-s^2d}}{\sqrt{r+s\sqrt{d}}}$ and $\sqrt{r+s\sqrt{d}}$ already belong to K, we have that $[L:K]=2$ and therefore, $[L:\mathbb{Q}]=[L:K][K:\mathbb{Q}]=8$. The Galois group of L permutes the 4 elements $\{\pm\sqrt{\alpha}, \pm\sqrt{\alpha'}\}$, but not every permutation is valid. It consists of eight automorphisms that map $(\sqrt{\alpha}, \sqrt{\alpha'})$ to $(\pm\sqrt{\alpha}, \pm\sqrt{\alpha'})$, $(\pm\sqrt{\alpha}, \mp\sqrt{\alpha'})$, $(\pm\sqrt{\alpha'}, \pm\sqrt{\alpha})$ and $(\pm\sqrt{\alpha'}, \mp\sqrt{\alpha})$. $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to D_4 the dihedral group of symmetries of a square. The isomorphism can be realized by letting σ and τ be the automorphisms that map $(\sqrt{\alpha}, \sqrt{\alpha'})$ to $(\sqrt{\alpha'}, -\sqrt{\alpha})$ and $(\sqrt{\alpha'}, \sqrt{\alpha})$, respectively. Then $\mathrm{Gal}(L/\mathbb{Q})$ is generated by σ and τ and they satisfy $\sigma^4=\tau^2=1$, $\sigma^2=\rho$ (complex conjugation) and $\tau\sigma=\sigma^3\tau$. The subgroup $\{1,\tau\sigma\}$ has order 2 and hence fixes a subfield of L of degree 4, since $(\tau\sigma)(\sqrt{\alpha})=\sqrt{\alpha}$, $K=F(\sqrt{\alpha})$ is the subfield fixed by $\{1,\sigma\tau\}$.

Note that in the first two cases, $\sqrt{\alpha'}\in K$, so $L=F(\sqrt{\alpha},\sqrt{\alpha'})$ is the Galois closure of K in all three cases. Then the previous discussion can be summarized in the following way:

Let $F=\mathbb{Q}(\sqrt{d})$ be a real quadratic field. Let K be a CM extension of F, i.e. $K=F(\sqrt{\alpha})$ where $\alpha\in F$ is a totally negative element. Then $L=F(\sqrt{\alpha},\sqrt{\alpha'})$ is the Galois closure of K and there are three possibilities for the Galois group of L.

$$\mathrm{Gal}(L/\mathbb{Q}) = \begin{cases} \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}, & \text{if } K/\mathbb{Q} \text{ is biquadratic} \\ \mathbb{Z}/4\mathbb{Z}, & \text{if } K/\mathbb{Q} \text{ is cyclic} \\ D_4, & \text{if } K/\mathbb{Q} \text{ is not Galois} \end{cases}$$

It would be nice if we were able to identify in which of the three cases are we just by looking at $\alpha=r+s\sqrt{d}$ and it turns out that it is possible by the following lemma

Lemma 4.20. *Let $\widetilde{F}=\mathbb{Q}(\sqrt{\alpha\alpha'})$ where α' is the conjugate of α in F.*

(i) $K/\mathbb{Q}$ is biquadratic if an only if $\widetilde{F}=\mathbb{Q}$

(ii) $K/\mathbb{Q}$ is cyclic if an only if $\widetilde{F}=F$

(iii) $K/\mathbb{Q}$ is non-Galois if an only if $\widetilde{F}\neq F$ is a real quadratic field.

Proof. We have seen that the three possibilities enumerated in this lemma are all the possibilities for K. Therefore, we just need to proof the direct implications and we will automatically have that the converse are true.

If $K/\mathbb{Q}$ is biquadratic, $\alpha=r\in\mathbb{Q}$ $(s=0)$, so $\sqrt{\alpha\alpha'}=\alpha$ and $\widetilde{F}=\mathbb{Q}$.

If $K/\mathbb{Q}$ is cyclic, we have that $\widetilde{F}=\mathbb{Q}(\sqrt{r^2-s^2d})=\mathbb{Q}(\sqrt{\alpha\alpha'})$ is a real quadratic field and is a subfield of $K=\mathbb{Q}(\sqrt{\alpha})=\mathbb{Q}(\sqrt{\alpha},\sqrt{\alpha'})$, but since the Galois group is cyclic of order 4, there is only one subgroup of order 2, so there is only one subfield of degree 2, which is fixed by $\{1,\sigma^2=\rho\}$. Therefore $\widetilde{F}=\mathbb{Q}(\sqrt{d})$ It can't happen that $\widetilde{F}=\mathbb{Q}$ because this would mean that $\sqrt{\alpha\alpha'}\in\mathbb{Q}$ and then $\sigma(\sqrt{\alpha\alpha'})=\sqrt{\alpha\alpha'}$. But we saw in the second case of the discussion that σ is such that $\sigma(\sqrt{\alpha})=\sqrt{\alpha'}$ and $\sigma(\sqrt{\alpha'})=-\sqrt{\alpha}$, so $\sigma(\sqrt{\alpha\alpha'})=-\sqrt{\alpha\alpha'}$ and $\sqrt{\alpha\alpha'}\notin\mathbb{Q}$.

If $K/\mathbb{Q}$ is not Galois, then $\widetilde{F} = \mathbb{Q}(\sqrt{\alpha\alpha'})$ is a real quadratic field because $\alpha\alpha' > 0$ since α is totally negative. It can't be $\mathbb{Q}$ because then $\sqrt{\alpha\alpha'} \in \mathbb{Q} \implies \sqrt{\alpha'} \in \mathbb{Q}(\alpha)$ which is not the case in view of the previous discussion. We must see also that $\widetilde{F} \neq \mathbb{Q}(\sqrt{d})$ so we must see that $\sqrt{\alpha\alpha'} \notin \mathbb{Q}(\sqrt{d})$. Assume that this is the case for the sake of contradiction, then $\sqrt{\alpha\alpha'} \in \mathbb{Q}(\sqrt{d}) \subset K$, but $\sqrt{\alpha} \in K \implies \sqrt{\alpha'} \in K$ which contradicts that we are in the non-Galois case. Hence $\widetilde{F}$ is a real quadratic field different from $F = \mathbb{Q}(\sqrt{d})$. □

Thus, we have seen that there are 3 different types of quartic CM fields. The next step would be to study the possibilities for the CM types of those fields.

4.4.1 Possibilities for the CM type of a quartic CM field

Let K be a quartic CM field. Since its degree over $\mathbb{Q}$ is 4, there are 4 complex embeddings into $\mathbb{C}$ which come in conjugate pairs. Therefore we can let the set of embeddings be $\{\phi_1, \phi_2, \overline{\phi_1}, \overline{\phi_2}\}$. There are four possible CM types $\Phi_1 = \{\phi_1, \phi_2\}$, $\Phi_2 = \{\overline{\phi_1}, \phi_2\}$, $\overline{\Phi_2} = \{\phi_1, \overline{\phi_2}\}$ and $\overline{\Phi_1} = \{\overline{\phi_1}, \overline{\phi_2}\}$. We denote the first two by Φ_1 and Φ_2 and by an abuse of notation, the others are their conjugates (conjugate of each element). Note that Φ_1 and $\overline{\Phi_1}$ are equivalent (Definition 4.10) and the same happens for the other two.

Case 1: If $K = \mathbb{Q}(\sqrt{d}, \sqrt{a})$ for $d > 0$ and $a < 0$ is biquadratic, the embeddings are determined by the images of $\sqrt{d}$ and $\sqrt{a}$. We can let ϕ_1 be the identity on K and ϕ_2 be such that $\phi_2(\sqrt{d}) = -\sqrt{d}$ and $\phi_2(\sqrt{a}) = \sqrt{a}$ and this together with the four possible pairs of non-conjugate embeddings determines all CM types.

Note that $\mathbb{Q}(\sqrt{a}) \subset K$ is also a CM field with two CM types: $\{\phi_1|_{\mathbb{Q}(\sqrt{a})}\}$ and $\{\overline{\phi_1}|_{\mathbb{Q}(\sqrt{a})}\}$. $\Phi_1 = \{\phi_1, \phi_2\}$ is induced by the first one and $\overline{\Phi_1} = \{\overline{\phi_1}, \overline{\phi_2}\}$ by the second one.

By looking at $\mathbb{Q}(\sqrt{ad}) \subset K$ we find that the other two CM types are induced by the 2 CM types on $\mathbb{Q}(\sqrt{ad})$. Therefore there are two equivalence classes of CM-types and none of them is primitive.

Case 2: If $K = \mathbb{Q}(\sqrt{\alpha})$ is cyclic Galois for $\alpha \in \mathbb{Q}(\sqrt{d})$ a totally negative element, the embeddings are determined by the image of $\sqrt{\alpha}$. There is one embedding σ such that $\sigma(\sqrt{\alpha}) = \sqrt{\alpha'}$. The four possible CM types are all equivalent since $\Phi_1 = \{1, \sigma\}$, $\Phi_2 = \{\sigma^2, \sigma\} = \Phi_1 \circ \sigma$, $\overline{\Phi_1} = \{\sigma^2, \sigma^3\} = \Phi_1 \circ \sigma^2$ and $\overline{\Phi_2} = \{1 = \sigma^4, \sigma^3\} = \Phi_1 \circ \sigma^3$. All of them are primitive since K has no proper imaginary quadratic subfield and therefore the CM types can't be induced by CM types on proper CM subfields (if it had an imaginary quadratic subfield it would be fixed by a subgroup of order 2, but the only such group is $\{1, \sigma^2\}$ which fixes the real quadratic subfield).

Case 3: If $K = \mathbb{Q}(\sqrt{\alpha})$ is non-Galois for $\alpha \in \mathbb{Q}(\sqrt{d})$ a totally negative element, the embeddings are also determined by the image of $\sqrt{\alpha}$ and by letting ϕ_1 be the identity on K and ϕ_2 be such that $\phi_2(\sqrt{\alpha}) = \sqrt{\alpha'}$, we get the four possible CM types $\Phi_1, \Phi_2, \overline{\Phi_1}, \overline{\Phi_2}$. The difference with the previous case is that ϕ_2 is not an automorphism because K is not Galois, so the equivalence classes of CM types go in pairs again and Φ_1, Φ_2 are not equivalent. They are all primitive because as before, K does not contain a proper CM subfield (it would be an imaginary quadratic extension). It doesn't contain one because it would be a fixed field by a subgroup or order 4 of the Galois group of L, the Galois closure of K. There are 3 such groups but only one contains a subgroup that fixes K, therefore only this one can fix a subfield of K. However the fixed field by this group is the real quadratic subfield $\mathbb{Q}(\sqrt{d})$.

In view of the above discussion we see that a CM type (K, Φ) for a quartic CM field is primitive if and only if K is not biquadratic. This will be an important distinction to make in the following sections.

4.4.2 Possibilities for reflex field of a quartic CM field

The last step on our study of quartic CM fields is to find their reflex field K^r which will be useful when we compute the values of modular functions at CM points.

Case 1: If $K = \mathbb{Q}(\sqrt{d}, \sqrt{a})$ for $d > 0$ and $a < 0$ is biquadratic, the elements of K can be written as $\lambda_1 + \lambda_2\sqrt{d} + \lambda_3\sqrt{a} + \lambda_4\sqrt{ad}$ for $\lambda_i \in \mathbb{Q}$. Recall that the reflex field K^r is generated over $\mathbb{Q}$ by the elements $\mathrm{tr}(\Phi(x))$ for $x \in K$. If $\Phi = \{\phi_1, \phi_2\}$ (as defined before), the reflex field is generated by elements of the form $2\lambda_1 + 2\lambda_3\sqrt{a}$ over $\mathbb{Q}$, so $K^r = \mathbb{Q}(\sqrt{a})$. If $\Phi = \{\overline{\phi_1}, \phi_2\}$, the reflex field is generated by elements of the form $2\lambda_1 + 2\lambda_4\sqrt{ad}$ over $\mathbb{Q}$, so $K^r = \mathbb{Q}(\sqrt{da})$. Similarly $\{\phi_1, \overline{\phi_2}\}$ and $\{\overline{\phi_1}, \overline{\phi_2}\}$ have $\mathbb{Q}(\sqrt{ad})$ and $\mathbb{Q}(\sqrt{a})$ as their reflex fields, respectively. Note that if two CM types are equivalent, then they have the same reflex field because of the definition of the reflex field as $\mathbb{Q}\left(\{\mathrm{tr}(\Phi(x))\}_{x\in K}\right)$.

Case 2: If $K = \mathbb{Q}(\sqrt{\alpha})$ is cyclic Galois for $\alpha \in \mathbb{Q}(\sqrt{d})$ totally negative, the elements of K can be written as $\lambda_1+\lambda_2\sqrt{\alpha}+\lambda_3\sqrt{\alpha}^2+\lambda_4\sqrt{\alpha}^3$ for $\lambda_i \in \mathbb{Q}$. If $\Phi = \{1, \sigma\}$ where σ is such that $\sigma(\sqrt{\alpha}) = \sqrt{\alpha'}$, the reflex field is generated by elements of the form $2\lambda_1 + \lambda_2(\sqrt{\alpha} + \sqrt{\alpha'}) + \lambda_3(\alpha + \alpha') + \lambda_4(\sqrt{\alpha}^3 + \sqrt{\alpha'}^3)$ over $\mathbb{Q}$. Since $2\lambda_1$ and $2\lambda_3(\alpha + \alpha') \in \mathbb{Q}$, the reflex field K^r is generated by $\sqrt{\alpha} + \sqrt{\alpha'}$ and $\sqrt{\alpha}^3 + \sqrt{\alpha'}^3 = (\sqrt{\alpha} + \sqrt{\alpha'})(\alpha + \alpha' - \sqrt{\alpha\alpha'})$, so it is also the field generated over $\mathbb{Q}$ by $\sqrt{\alpha} + \sqrt{\alpha'}$ and $\sqrt{\alpha\alpha'}$. By Lemma 4.20, $\mathbb{Q}(\sqrt{\alpha\alpha'}) = \mathbb{Q}(\sqrt{d})$, so K^r is generated by $\sqrt{\alpha} + \sqrt{\alpha'}$ over $\mathbb{Q}(\sqrt{d})$. But then, since $\alpha - \alpha' \in \mathbb{Q}(\sqrt{d})$ and $\sqrt{\alpha} - \sqrt{\alpha'} = \frac{\alpha-\alpha'}{\sqrt{\alpha}+\sqrt{\alpha'}}$, we have that the reflex is generated by $\sqrt{\alpha} + \sqrt{\alpha'}$, $\sqrt{\alpha} - \sqrt{\alpha'}$ and $\sqrt{d}$ over $\mathbb{Q}$, so it is generated by $\sqrt{\alpha}, \sqrt{\alpha'}$ and $\sqrt{d}$. Therefore $K^r = \mathbb{Q}(\sqrt{\alpha}) = K$ as $\sqrt{\alpha'}$ and $\sqrt{d}$ already belong to K.

The other CM types are equivalent of the form $\Phi\sigma$, $\Phi\sigma^2$, $\Phi\sigma^3$ and since σ is an automorphism of K, $\{x \mid x \in K\} = \{\sigma(x) \mid x \in K\}$, so the reflex of all of them is the same. The totally real subfield of K^r is $F^r = \mathbb{Q}(\sqrt{d})$.

Case 3: Lastly, if $K = \mathbb{Q}(\sqrt{\alpha})$ is non-Galois for $\alpha \in \mathbb{Q}(\sqrt{d})$ totally negative, and we consider the CM type $\Phi = \{1, \sigma\}$ where $\sigma(\sqrt{\alpha}) = \sqrt{\alpha'}$, like in the previous case, we get that the reflex field is generated by $(\sqrt{\alpha}+\sqrt{\alpha'})$ and $(\sqrt{\alpha}^3+\sqrt{\alpha'}^3)$ or equivalently, by $(\sqrt{\alpha}+\sqrt{\alpha'})$ and $(\sqrt{\alpha\alpha'})$. Now since $(\sqrt{\alpha}+\sqrt{\alpha'})^2 = 2(\sqrt{\alpha\alpha'})+\alpha+\alpha'$, we see that $(\sqrt{\alpha\alpha'}) \in \mathbb{Q}(\sqrt{\alpha} + \sqrt{\alpha'})$ so the reflex field $K^r = \mathbb{Q}(\sqrt{\alpha} + \sqrt{\alpha'})$. And for $\Phi = \{1, \overline{\sigma}\}$, the reflex field is generated by $\sqrt{\alpha} - \sqrt{\alpha'}$, $\alpha + \alpha'$ and $\sqrt{\alpha}^3 - \sqrt{\alpha'}^3$. The second is rational, and dividing the third by the first generator, we see that $\alpha + \sqrt{\alpha\alpha'} + \alpha'$ and $\sqrt{\alpha} - \sqrt{\alpha'}$ generate the reflex field K^r. But $(\sqrt{\alpha} - \sqrt{\alpha'})^2 = \alpha + \alpha' - 2\sqrt{\alpha\alpha'}$ so $\sqrt{\alpha\alpha'}$ adds nothing more and K^r is just $\mathbb{Q}(\sqrt{\alpha} - \sqrt{\alpha'})$. For the conjugate CM types the reflex is the same that for the original CM type. Note that in both cases K^r is a quartic CM field as $x^4 - 2x^2(\alpha + \alpha') + \alpha^2 + (\alpha')^2 + \alpha\alpha'$is the minimal polynomial over $\mathbb{Q}$ of the element that geneartes K^r. The totally real subfield of K^r is $F^r = \mathbb{Q}(\sqrt{\alpha\alpha'})$.

4.5 Abelian varieties with Complex Multiplication

The importance of CM fields comes from the fact that we can embed them into the endomorphism ring of abelian varieties with complex multiplication in a similar way to what happened with elliptic curves and imaginary quadratic fields. For that reason we need to introduce the basics of abelian varieties. We want get too much into the geometric details, just a basic notion for completeness.

Definition 4.21. An abelian variety over a field k is a projective variety with a commutative group law.

When $k = \mathbb{C}$, the abelian variety is isomorphic to a complex torus. More concretely, if A is an n-dimensional abelian variety over $\mathbb{C}$, it is isomorphic to $\mathbb{C}^n/L$ where $L \subset \mathbb{C}^n$ is a lattice of rank $2n$. Note that when $n = 1$ we are in the case of elliptic curves and as we have already discussed, they are isomorphic to a complex torus $\mathbb{C}/L$ where L is a lattice in $\mathbb{C}$. For elliptic curves, the converse is also true. Any complex torus is isomorphic to an elliptic curve. However, this converse is not always true for dimension $n > 1$.

Definition 4.22. Let A and B be abelian varities. An homomorphism $\lambda : A \to B$ is a rational map between A and B that also preserves the group structure (it is a group homomorphism). When A and B are of the same dimension, we say that λ is an isogeny. If $A = B$, it is called an endomorphism.

We denote by $\mathrm{Hom}(A, B)$ and $\mathrm{End}(A)$ the ring of homomorphisms of A to B and the ring of endomorphism of A, respectively. When there is an isogeny from A to B there is also one from B to A, and we say that A and B are isogenous. This defined an equivalence relation of isogenic varieties. Given an isogeny between A and B it induces an homomorphism between the complex torus to which A and B are isomorphic, which is an homomorphism between $\mathbb{C}^n/L_1$ and $\mathbb{C}^n/L_2$. This last homomorphism at the same time induces a linear map $\lambda : \mathbb{C}^n \to \mathbb{C}^n$ such that $\lambda(L_1) \subset L_2$. All those induced correspondences can be summarized by the following isomorphism:

$$\mathrm{Hom}(A, B) \cong \{M \in M_n(\mathbb{C}) \mid ML_1 \subset L_2\}$$

where $M_n(\mathbb{C})$ is the set of $n \times n$ matrices with coefficients in $\mathbb{C}$.

Recall that we said that when $n > 1$, the complex torus $\mathbb{C}^n/L$ does not always define a projective variety, but this fact is true if there exists a Riemann form on $\mathbb{C}^n/L$.

Definition 4.23. A bilinear form $E(x, y)$ with values in $\mathbb{R}$ is a Riemann form on $\mathbb{C}^n/L$ if it satisfies

(i) $E(x,y) \in \mathbb{Z}$ for all $x, y \in L$

(ii) $E(x,y) = -E(y,x)$

(iii) $(x,y) \mapsto E(ix,y)$ is a positive symmetric form (not necessarily strictly positive, it can be degenerate)

If a torus has a Riemann form, we say that is polarized and in this case it is true that the complex torus is isomorphic to an abelian variety. There are other ways to define a polarization for a generic abelian variety when we don't have the isomorphism with a complex torus, but we are not going to get into this geometric details.

Now that we have the basic facts that we will need about abelian varieties and their endomorphism rings, we can start with the definitions related to Complex Multiplication. The endomorphism ring of an abelian variety A always has dimension lower or equal to $2\dim(A)$. In the cases where equality holds, the abelian variety has Complex Multiplication. The precise definition is the following one.

Definition 4.24. Let K be a CM field of degree $2n$. An abelian variety A of dimension n has CM by K if there is an embedding $\iota : K \to \mathrm{End}(A) \otimes \mathbb{Q}$. We sometimes just refer to the abelian variety A but we can also say that the pair (A, ι) has complex multiplication by K when we want to make explicit the embedding ι from K into $\mathrm{End}(A) \otimes \mathbb{Q}$. We say that (A, ι) has CM by $\mathcal{O}_K$ if the same holds with $\iota^{-1}(\mathrm{End}(A)) = \mathcal{O}_K$.

Note that we don't need i to determine if an abelian variety has CM, as all the information is needed is included in A, but when we have a pair (A, ι), ι contains the information of how we embed K into $\mathrm{End}(A) \otimes \mathbb{Q}$. Once this is clear, it makes sense to define abelian varieties (A, ι) with CM of type (K, Φ) for a certain CM-type.

Definition 4.25. We say that (A, ι) has type (K, Φ) if it has CM by K and the representation of $\mathrm{End}(A) \otimes \mathbb{Q}$ is equivalent to the direct sum $\phi_1 \oplus \phi_2 \oplus \ldots \oplus \phi_n$ of the n embeddings in the CM type, that is when we view $\mathrm{End}(A)$ as a matrix in $M_n(\mathbb{C})$, it can be diagonalized and the components in the diagonal are the images by the Φ.

Let our abelian variety be defined over k and denote by $\overline{k}$ its algebraic closure. For an element $\sigma \in \mathrm{Gal}(\overline{k}/\mathbb{Q})$ we define

$$\begin{aligned} \sigma\iota : K &\to \mathrm{End}(\tau A) \otimes \mathbb{Q} \\ x &\mapsto \sigma(\iota(x)) \end{aligned}$$

And we write $\sigma(A, \iota)$ for the variety $(\sigma A, \sigma\iota)$. From the definition we get the following Lemma ([Str10], Lemma 4.2 in chapter 1).

Lemma 4.26. *If $\sigma \in \mathrm{Gal}(\overline{k}/\mathbb{Q})$ and (A, ι) has type Φ, $\sigma(A, \iota)$ has type $\sigma\Phi$.*

Definition 4.27. An abelian variety A is called simple if it is not isogenous to a product of lower-dimensional abelian varieties.

Theorem 3.5 in chapter 1 of [Lan83] states that a CM type is primitive if and only if the abelian varieties whose endomorphism algebra is K is simple. In the quartic CM field case, the variety is not simple if and only if K is biquadratic. In this case, since we must have $2\dim(A) = 4 = \dim(K)$ for an abelian variety A to have complex multiplication by K, we must have that A is a product of two elliptic curves. As we pointed out before, this will be an important distinction to make in the following sections.

4.6 Moduli space of abelian surfaces with CM

Recall that $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ parametrizes isomorphism classes of elliptic curves. This fact allowed us to evaluate the modular function j at the points corresponding to those elliptic curves and get the nice algebraic numbers that we already discussed. Similarly, we need a result that relates classes of abelian varieties with CM with points in a modular surface. If we consider the Hilbert modular surface $Y(\mathit{\Gamma}_F) = \mathrm{SL}_2(\mathcal{O}_F)\backslash\mathbb{H}^2$, a result by Goren ([Gor02]) states that it parametrizes classes of triples (A, ι, m) where

(i) A is an abelian surface over $\mathbb{C}$

(ii) $\iota : \mathcal{O}_F \to \mathrm{End}(A)$ is a real multiplication by $\mathcal{O}_F$

(iii) $m : (P_A, P_A^+) \to (\mathfrak{d}_F^{-1}, \mathfrak{d}_F^{-1,+})$ is an $\mathcal{O}_F$-linear isomorphism between the polarization module $P_A = \mathrm{Hom}_{\mathcal{O}_F}^{\mathrm{sym}}(A, A^\vee)$ of A and $\mathfrak{d}_F^{-1}$, taking the positive elements to the positive elements.

An abelian variety A of dimension n has real multiplication when we can embed a totally real field F of degree n into $\mathrm{End}(A) \otimes \mathbb{Q}$. So if an abelian variety has complex multiplication by a CM field, it has real multiplication by its totally real subfield which menas that principally polarized abelian varieties with complex multiplication by $\mathcal{O}_K$ are a special case of principally polarized abelian varieties with real multiplication by $\mathcal{O}_F$, so we can identify principally polarized abelian surfaces with complex multiplication with a subset of $Y(\mathit{\Gamma}_F)$. We don't focus too much on the details about the third part of the statement. We just need to know that we work with principally polarized abelian surfaces and we can think of it in terms of the Riemann form of Definition 4.23.

Now that we saw this result we can see why we focused on quartic CM fields: because the Hilbert modular surface parametrizes abelian surfaces (with some extra conditions) and those have complex multiplication by a quartic CM field. Therefore from now, we will just focus on principally polarized abelian surfaces with CM and quartic CM fields and abandon any more general notion of those concepts. Furthermore, for simplicity we will assume that the totally real subfield of our quartic CM field has narrow class number 1 although many things still work in more general cases. We do this assumption as the numerical computations that we will perform will be for those cases and proving some results is much easier.

4.7 CM points

We now introduce the definition of CM points for quartic CM field of narrow class number 1. There are two equivalent definitions, one given by the previous result and another related to ideals of K.

Definition 4.28. Let $\Phi = (\phi_1, \phi_2)$ be a CM type of K. We call a point $z = (A, \iota, m) \in Y(\mathit{\Gamma}_F)$ a CM point of type (K, Φ) if one of the following two equivalent conditions is satisfied:

(i) There exists $\tau \in K$ such that $\Phi(\tau) = (\phi_1(\tau), \phi_2(\tau)) = z$ as a point in $\mathbb{H}^2$ and $\mathcal{O}_F + \tau\mathcal{O}_F$ is a fractional ideal of K.

(ii) (A, ι) is an abelian variety of type (K, Φ) with CM by $\iota' : \mathcal{O}_K \hookrightarrow \mathrm{End}(A)$ such that $\iota = \iota'|_{\mathcal{O}_F}$.

Sometimes we will make an abuse by calling both $z \in \mathbb{H}^2$ and $\tau \in K$ CM points, but it will be clear to what of the two objects we are refering when we do this.

Definition 4.29. A CM cycle of type (K, Φ) is the 0-cycle in $Y(\mathit{\Gamma}_F)$ of CM points of type (K, Φ). It is denoted by $\mathcal{CM}(K, \Phi, \mathcal{O}_F)$.

In the next section we will see how to relate the two equivalent definitions. More precisely, we will see how to relate CM points (thought as principally polarized abelian surfaces with complex multiplication) with ideals of K and from here we will see how we can represent those principally polarized abelian surfaces by points of $Y(\mathit{\Gamma}_F) = \mathrm{SL}_2(\mathcal{O}_F)\backslash\mathbb{H}^2$ (how to explicitly obtain the coordinates).

4.8 Abelian surfaces with CM by $\mathcal{O}_K$

For this section we mainly follow [Str10].

Let $\Phi = (\phi_1, \phi_2)$ be a primitive CM-type for a quartic CM field K. Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_K$. Then, since $[K : \mathbb{Q}] = 4$, the ideal $\mathfrak{a}$ has dimension 4 over $\mathbb{Z}$ and so does $\Phi(\mathfrak{a}) = (\phi_1(\mathfrak{a}), \phi_2(\mathfrak{a}))$ since it is completely determined by $\mathfrak{a}$. Since the 4 elements that generate $\mathfrak{a}$ over $\mathbb{Z}$ are linearly independent, we can consider the lattice $\Phi(\mathfrak{a})$ and the quotient $\mathbb{C}^2/\Phi(\mathfrak{a})$ which is a complex torus and an abelian surface. Let $\mathcal{D}_K^{-1}$ be the inverse of the different ideal of K. That is

$$\mathcal{D}_K^{-1} = \{x \in K \mid \mathrm{tr}_{K/\mathbb{Q}}(x\mathcal{O}_K) \subset \mathbb{Z}\}$$

Assume that the ideal $(\mathfrak{a}\bar{\mathfrak{a}}\mathcal{D}_K)^{-1}$ is principal and generated by an element $\xi \in K$, such that $\Phi(\xi) \in (i\mathbb{R}^+)^2$ (the positive imaginary axis). Consider the map $E_{\Phi,\xi} : \mathbb{C}^2 \times \mathbb{C}^2 \to \mathbb{R}$ defined by

$$E_{\Phi,\xi}(z, w) = \phi_1(\xi)(\overline{z_1}w_1 - z_1\overline{w_1}) + \phi_2(\xi)(\overline{z_2}w_2 - z_2\overline{w_2})$$

It clearly satisfies $E_{\Phi,\xi}(z, w) = -E_{\Phi,\xi}(w, z)$ and

$$(z, w) \mapsto E_{\Phi,\xi}(iz, w) = -i\phi_1(\xi)(\overline{z_1}w_1 + z_1\overline{w_1}) - i\phi_2(\xi)(\overline{z_2}w_2 + z_2\overline{w_2})$$

is symmetric and satisfies

$$(z, z) \mapsto E_{\Phi,\xi}(iz, z) = -2i\phi_1(\xi)(z_1\overline{z_1}) - 2i\phi_2(\xi)(z_2\overline{z_2}) > 0$$

because $z_j\overline{z_j}$ is just the norm of a complex number and $\Phi(\xi) \in (i\mathbb{R}^+)^2$. Furthermore, the restriction of $E_{\Phi,\xi}$ to $\Phi(K) \times \Phi(K)$ gives a map $E_{\Phi,\xi} : \Phi(K) \times \Phi(K) \to \mathbb{Q}$ defined by

$$E_{\Phi,\xi}(\Phi(\alpha), \Phi(\beta)) = \phi_1(\xi)\phi_1(\overline{\alpha}\beta - \alpha\overline{\beta}) + \phi_2(\xi)\phi_2(\overline{\alpha}\beta - \alpha\overline{\beta}) = \mathrm{tr}_{K/\mathbb{Q}}(\xi\overline{\alpha}\beta)$$

for α, β in K, and it is integer valued on $\Phi(\mathfrak{a}) \times \Phi(\mathfrak{a})$ because since ξ generates $(\mathfrak{a}\overline{\mathfrak{a}}\mathcal{D}_K)^{-1}$, any element of the form $\xi\overline{\alpha}\beta$ for $\alpha, \beta \in \mathfrak{a}$ is in $\mathcal{D}_K^{-1}$ and by the definition, its trace is integral. Therefore, $E_{\Phi,\xi}$ defines a Riemann form on $\mathbb{C}^2/\Phi(\mathfrak{a})$ (and therefore a principal polarization).

The principally polarized abelian surface $A(\Phi, \mathfrak{a}, \xi) := (\mathbb{C}^2/\Phi(\mathfrak{a}), E_{\Phi,\xi})$ has complex multiplication by $\mathcal{O}_K$ and conversely, any abelian surface with complex multiplication by $\mathcal{O}_K$ is isomorphic to $A(\Phi, \mathfrak{a}, \xi)$ for some triple $(\Phi, \mathfrak{a}, \xi)$ (see [Str10] Theorem 5.2 in chapter 1). Two principally polarized abelian surfaces of the same type $A(\Phi, \mathfrak{a}_1, \xi_1)$ and $A(\Phi, \mathfrak{a}_2, \xi_2)$ are isomorphic if there exists $\lambda \in K^*$ such that $\mathfrak{a}_2 = \lambda\mathfrak{a}_1$ and $\xi_2 = (\lambda\overline{\lambda})^{-1}\xi_1$. This result is true even if Φ is not primitive but the converse is only true when Φ is primitive, so in the biquadratic case we may have isomorphic principally polarized abelian surfaces with CM by $\mathcal{O}_K$, $A(\Phi, \mathfrak{a}_1, \xi_1)$ and $A(\Phi, \mathfrak{a}_2, \xi)$ such that a λ satisfying the previous relation doesn't exist (that's also Theorem 5.2 in [Str10]).

Two principally polarized abelian surfaces of different types $A(\Phi_1, \mathfrak{a}_1, \xi_1)$ and $A(\Phi_2, \mathfrak{a}_2, \xi)$ are isomorphic if there exists $\sigma \in \mathrm{Aut}(K)$ such that $\Phi_1 \circ \sigma = \Phi_2$ and $A(\Phi_1, \sigma(\mathfrak{a}_2), \sigma(\xi_2))$ is isomorphic to $A(\Phi_1, \mathfrak{a}_1, \xi_1)$. We say that two pairs $(\Phi_1, \mathfrak{a}_1, \xi_1)$ and $(\Phi_2, \mathfrak{a}_2, \xi_2)$ are equivalent when they give rise to isomorphic principally polarized abelian surfaces.

Now it is starting to be clear how we can relate classes of principally polarized abelian surfaces with classes of ideals of K, because every polarized abelian surface is isomorphic to $A(\Phi, \mathfrak{a}, \xi)$ for some $\mathfrak{a}$. However, it could be the case that for two principally polarized abelian varieties $A(\Phi, \mathfrak{a}_1, \xi_1)$ and $A(\Phi, \mathfrak{a}_2, \xi_2)$ such that $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are in the same ideal class no $\lambda \in K^*$ relating the two existed, and they would not be isomorphic. We can always choose $\lambda \in K^*$ so that $\mathfrak{a}_2 = \lambda\mathfrak{a}_1$ but maybe the choice does not give $\xi_2 = (\lambda\overline{\lambda})^{-1}\xi_1$, so we need some result that assures us that this is always the case, and therefore an ideal class will be associated to just one isomorphism class of principally polarized abelian varieties with CM by $\mathcal{O}_K$. We will prove this when the narrow class number of F, the totally real subfield of K is 1 and from now on we will always assume this.

Proposition 4.30. *Assume that K is a quartic CM field with totally real subfield F of class number 1 and that Φ is a CM type of K. Then the principally polarized abelian varieties $A(\Phi, \mathfrak{a}_1, \xi_1)$ and $A(\Phi, \mathfrak{a}_2, \xi_2)$ are isomorphic if $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are in the same ideal class (the result is still true is the CM type is not primitive).*

Proof. Choosing a proper λ, we can get an $A(\Phi, \mathfrak{a}_1, \xi')$ isomorphic to $A(\Phi, \mathfrak{a}_2, \xi_2)$. But then from the fact that ξ_1 and ξ' generate the same ideal we know that they are related by a unit $u \in \mathcal{O}_K^*$ ($\xi_1 = u\xi'$). Since $\Phi(\xi_1) \in (i\mathbb{R}^+)^2$ and $\Phi(\xi') \in (i\mathbb{R}^+)^2$, this unit has to be real, and hence from $\mathcal{O}_F^*$. But now, this unit has to be totally positive because since restricting Φ to F gives the two possible embeddings of F, we wouldn't have $\Phi(\xi_1) \in (i\mathbb{R}^+)^2$ and $\Phi(u\xi') \in (i\mathbb{R}^+)^2$ if this wasn't the case. But then if $\xi_1 = u\xi'$ for a totally positive unit, u must be a square of a unit (the narrow class number 1 assumption assures that the fundamental unit has norm -1) and there exists $\lambda \in \mathcal{O}_F^* \subset K$ such that $\mathfrak{a}_1 = \lambda \mathfrak{a}_1$ and $\xi_1 = (\lambda\overline{\lambda})^{-1}\xi' = \lambda^{-2}\xi'$, so they are isomorphic. And so are $A(\Phi, \mathfrak{a}_1, \xi_1)$ and $A(\Phi, \mathfrak{a}_2, \xi_2)$. □

Note also that it is not necessarily the case that to each ideal class we can associate an isomorphism class of abelian varieties, because for this to happen we need the additional condition that $(\mathfrak{a}\overline{\mathfrak{a}}\mathcal{D}_K)^{-1}$ is principal. Actually, if F does not have class number 1, there are some classes of ideals such that $(\mathfrak{a}\overline{\mathfrak{a}}\mathcal{D}_K)^{-1}$ is not principal. The total number of pairs (Φ, A) such that Φ is a CM type and and A an isomorphism class of principally polarized abelian varieties with CM by $\mathcal{O}_K$ and type Φ is

$$\frac{h_K}{h_F}|\mathcal{O}_F^*/N_{K/F}(\mathcal{O}_K^*)|$$

where h_k, h_F are the class numbers of K and F, respectively. That's Proposition 5.3 in Chapter 1 in [Str10]. But in the case where F has narrow class number 1 (in particular has class number 1) $(\mathfrak{a}\overline{\mathfrak{a}}\mathcal{D}_K)^{-1}$ is always principal and we have a bijection between classes of ideals of K and isomorphism classes of principally polarized abelian varieties with CM by $\mathcal{O}_K$ of a fixed type. That it is always principal comes from two facts that $\mathcal{D}_K$ is principal by a straightforward application of Theorem 4 in [Wam99] because F has class number 1. And that looking at prime ideals $\mathfrak{p}$ dividing $\mathfrak{a}$ and considering whether $(\mathfrak{p} \cap F)\mathcal{O}_K$ splits, ramifies or it is inert, we can see that in all cases $\mathfrak{p}\overline{\mathfrak{p}}$ is principal.

Therefore, this section gives sense to the definition of CM point that we gave before. The only thing that's left is to see that there exists a $\tau \in K$ such that $\Phi(\tau) \in \mathbb{H}^2$ and $\mathcal{O}_F + \tau\mathcal{O}_F$ is an ideal in the same class of $\mathfrak{a}$.

A similar result (but not the same) is true for any totally real field F, but recall that we were focusing on the case were F has narrow class number 1.

Lemma 4.31. *Given a class of pairs* $[\mathfrak{a}, \xi]$ *representing an abelian variety with CM by* (K, Φ)*, there is a decomposition*

$$\mathfrak{a} = \alpha\mathcal{O}_F + \beta\mathcal{O}_F$$

such that $\tau = \frac{\alpha}{\beta} \in K^*$ *satisfies* $\Phi(\tau) \in \mathbb{H}^2$ *and* $z = \Phi(\tau)$ *represents the class* $[\mathfrak{a}, \xi]$ *in* $Y(\mathit{\Gamma}_F)$.

Proof. Since $\mathfrak{a}$ is a projective module of rank 2 over the Dedekind domain $\mathcal{O}_F$, there exist $\alpha, \beta \in K^*$ such that

$$\mathfrak{a} = \alpha\mathcal{O}_F + \beta\mathcal{O}_F$$

Note that $(\mathfrak{a}/\beta, (\beta\overline{\beta})\xi) \in [\mathfrak{a}, \xi]$ so the ideal

$$\frac{\mathfrak{a}}{\beta} = \frac{\alpha}{\beta}\mathcal{O}_F + \mathcal{O}_F$$

gives rise to an abelian surface in the same isomorphism class. Now consider $y = \alpha/\beta \in K^*$ and the four elements in K^* in the set $\{\pm y, \pm y\varepsilon_0\}$ where ε_0 is the fundamental unit of F (which has norm -1 because of the narrow class number 1 assumption). Then for any $\tau \in \{\pm y, \pm y\varepsilon_0\}$, $\tau\mathcal{O}_F + \mathcal{O}_F$ is the same ideal $\mathfrak{a}/\beta$ and one of the elements satisfies the condition that $\Phi(\tau) \in \mathbb{H}^2$. That's true because since the two embeddings are not complex conjugate, when restricted to F they give the two real embeddings. Therefore $\phi_1(\varepsilon_0)\phi_2(\varepsilon_0) = -1$, which means that $\phi_1(\varepsilon_0)$ and $\phi_2(\varepsilon_0)$ have different signs. Now if $\Im(\phi_1(y)), \Im(\phi_2(y))$ have the same sign, we do nothing. Otherwise we consider $y\varepsilon_0$, and the embeddings give the same sign for the imaginary part. If it is positive, we found the desired τ. Otherwise we multiply it by -1. In any case we proved that the τ from the statement exists. Since the abelian variety $A(\Phi, \mathfrak{a}, \xi)$ is isomorphic to $A(\Phi, \mathfrak{a}/\beta, \beta\overline{\beta}\xi)$, $z = \Phi(\tau)$ represents the class $[\mathfrak{a}, \xi]$ in $Y(\Gamma_F)$. □

From the fact that the Hilbert modular surface parametrizes abelian varieties with real multiplication (of which complex multiplication is a particular case) and the way we found to represent them with coordinates in $\mathbb{H}^2$, we gave sense to the definition of CM point of type (K, Φ) for a CM field K of degree 4. Moreover, since the Hilbert modular surface is the quotient of $\mathbb{H}^2$ by the action of $\mathrm{SL}_2(\mathcal{O}_F)$, we expect that two fractional ideals of $\mathcal{O}_K$ of the form $\tau_1\mathcal{O}_F + \mathcal{O}_F$ and $\tau_2\mathcal{O}_F + \mathcal{O}_F$ are in the same ideal class if and only if $\Phi(\tau_1)$ and $\Phi(\tau_2)$ are equivalent under the action of $\mathrm{SL}_2(\mathcal{O}_F)$. We can check that with straightforward computations:

When we restrict the two embeddings of the same type to F we get the two totally real embeddings of F. Without loss of generality assume that $\phi_1|_F = \mathrm{id}$, so that $\phi_2|_F$ is the conjugation in F. Then we have $(\phi_1(\tau_1), \phi_2(\tau_1)) = \left(\dfrac{x\phi_1(\tau_2) + y}{z\phi_1(\tau_2) + t}, \dfrac{x'\phi_2(\tau_2) + y'}{z'\phi_2(\tau_2) + t'}\right) = \left(\phi_1\left(\dfrac{x\tau_2 + y}{z\tau_2 + t}\right), \phi_2\left(\dfrac{x\tau_2 + y}{z\tau_2 + t}\right)\right)$ for $\begin{pmatrix} x & y \\ z & t \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}_F)$, so $\Phi(\tau_1)$ and $\Phi(\tau_2)$ are equivalent under the action of $\mathrm{SL}_2(\mathcal{O}_F)$ if and only if τ_1 and τ_2 are equivalent under the action of $\mathrm{SL}_2(\mathcal{O}_F)$. But if $\tau_1 = \frac{x\tau_2+y}{z\tau_2+t}$, then the ideals $\mathfrak{a}_1 = \tau_1\mathcal{O}_F + \mathcal{O}_F = \frac{x\tau_2+y}{z\tau_2+t}\mathcal{O}_F + \mathcal{O}_F$ and $\mathfrak{a}_2 = \tau_2\mathcal{O}_F + \mathcal{O}_F$ are in the same equivalence class. More concretely with have that $(\tau_2 z + t)\mathfrak{a}_1 = \mathfrak{a}_2$ as fractional $\mathcal{O}_K$-ideals. The inclusion $(\tau_2 z + t)\mathfrak{a}_1 \subset \mathfrak{a}_2$ is clear because for every $a, b \in \mathcal{O}_F$, $(x\tau_2 + y)a + (z\tau_2 + t)b = \tau_2(xa + zb) + ya + tb \in \tau_2\mathcal{O}_F + \mathcal{O}_F$. For the other inclusion, we just need to see that for every $a, b \in \mathcal{O}_F$, there exist $r, s \in \mathcal{O}_F$ such that $(x\tau_2 + y)r + (z\tau_2 + t)s = \tau_2 a + b$. But this is equivalent to having a solution of

$$\begin{pmatrix} x & z \\ y & t \end{pmatrix}\begin{pmatrix} r \\ s \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$$

for every pair $a, b \in \mathcal{O}_F$. And that's true because $\left(\begin{smallmatrix} x & z \\ y & t \end{smallmatrix}\right)$ is invertible for being the transpose of an element in $\mathrm{SL}_2(\mathcal{O}_F)$ (and hence an element of $\mathrm{SL}_2(\mathcal{O}_F)$).

Conversely, if $\tau_1\mathcal{O}_F + \mathcal{O}_F$ and $\tau_2\mathcal{O}_F + \mathcal{O}_F$ are in the same ideal class, we have that $\tau_1\mathcal{O}_F + \mathcal{O}_F = \lambda(\tau_2\mathcal{O}_F + \mathcal{O}_F)$ for some $\lambda \in K^*$. That means that $x\tau_1 + y = \lambda\tau_2 \in$

has a solution for $x, y \in \mathcal{O}_F$ and the same for $z\tau_1 + t = \lambda$. Dividing the first by the second one, we get that there exist $x, y, z, t \in \mathcal{O}_F$ such that: $\tau_2 = \frac{x\tau_1+y}{z\tau_1+t}$. Analogously, we get that there exist $a, b, c, d \in \mathcal{O}_F$ such that $\tau_1 = \frac{a\tau_2+b}{c\tau_2+d}$. Therefore,

$$\begin{pmatrix} x & y \\ z & t \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}$$

and the matrices are each other's inverse and have coefficients in $\mathcal{O}_F$, so they are in $\mathrm{GL}_2(\mathcal{O}_F)$.

Note that we know that the two matrices above have totally positive determinant because, from the fact that $\Phi(\tau_1), \Phi(\tau_2) \in \mathbb{H}^2$, we know that $\phi_j(\tau_1)$ and $\phi_j(\tau_2)$ have the same sign for the imaginary part for $\phi_j \in \Phi$. But we have

$$\Im(\phi_j(\tau_1)) = \Im(\frac{a\phi_j(\tau_2)+b}{c\phi_j(\tau_2)+d}) = \Im(\frac{(a\phi_j(\tau_2)+b)(c\overline{\phi_j(\tau_2)}+d)}{(c\phi_j(\tau_2)+d)(c\overline{\phi_j(\tau_2)}+d)}) =$$
$$= \Im(\frac{(a\phi_j(\tau_2)+b)(c\overline{\phi_j(\tau_2)}+d)}{|c\phi_j(\tau_2)+d|^2}) = \Im(\frac{ac|\phi_j(\tau_2)|^2 + ad\phi_j(\tau_2) + bc\overline{\phi_j(\tau_2)} + bd}{|c\phi_j(\tau_2)+d|^2}) =$$
$$= \frac{\Im(ac|\phi_j(\tau_2)|^2 + ad\phi_j(\tau_2) + bc\overline{\phi_j(\tau_2)} + bd)}{|c\phi_j(\tau_2)+d|^2} = \frac{\Im(ad\phi_j(\tau_2) + bc\overline{\phi_j(\tau_2)})}{|c\phi_j(\tau_2)+d|^2} =$$
$$= \frac{1}{|c\phi_j(\tau_2)+d|^2}\Im(ad\phi_j(\tau_2) - bc\phi_j(\tau_2)) = \frac{(ad-bc)\Im(\phi_j(\tau_2))}{|c\phi_j(\tau_2)+d|^2}$$

which means that $\phi_1(\tau_1)$ and $\phi_1(\tau_2)$ have the same sign if and only if the determinant is positive. But now, doing the same for ϕ_2 and the conjugate matrix in F, we get that $a'd' - b'c'$ is also positive, so the determinant is totally positive, and invertible, and therefore it is a square of the fundamental unit (call it ε_0^{2k}). That means that

$$\begin{pmatrix} a/\varepsilon_0^k & b/\varepsilon_0^k \\ c/\varepsilon_0^k & d/\varepsilon_0^k \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}_F)$$

and gives the same action that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, so τ_1 and τ_2 are $\mathrm{SL}_2(\mathcal{O}_F)$-equivalent.

So far we have seen that each ideal class of K determines a unique CM point in $\mathrm{SL}_2(\mathcal{O}_F)\backslash\mathbb{H}^2$, so the number of CM points in a cycle is equal to the class number of K, and if we consider them as points in $\tau \in K$, then each τ of the CM cycle generates gives an ideal $\mathcal{O}_F + \tau\mathcal{O}_F$ in a different class of the ideal class group.

The interest on CM cycles comes from a result of Shimura (which is usually known as the first Main Theorem of Complex Multiplication and that we will see shortly) that tells us the fact that the field of moduli for $\mathcal{CM}(K, \Phi, \mathcal{O}_F)$ is the reflex field K^r, so evaluating certain modular functions at CM cycles gives values K^r. Furthermore, this result also tells us that evaluating modular functions at a unique CM point gives values in an algebraic extension of K^r. When we evaluate a modular function at all the possible CM cycles (for a fixed K we consider the cycle for each possible CM type) and multiply the results, those numbers are rational numbers. Sometimes, we even get integers with nice factorizations (integers with lots of divisors).

Remark 4.32. When we say certain modular functions it is because not any modular function works. For instance if f is a modular function whose values at certain points are algebraic, then πf is also a modular function and now its values at the same points are obviously not algebraic. Therefore, those modular forms have to be of a especial form. We want them to be a rational function on $\mathrm{SL}_2(\mathcal{O}_F)\backslash\mathbb{H}^2$. We will not get into the details of what this means because it would be really tedious, but the remark is necessary. For our purposes, we just need to know that the functions we will use (quotients of Borcherds lifts) satisfy those assumptions, and their values at CM points will be algebraic.

4.8.1 First Main Theorem of Complex Multiplication

Here we state the first Main Theorem of Complex Multiplication in the words of Shimura (it can be found [Shi98], page 112, Main Theorem 1).

Theorem 4.33. *Let (K, Φ) be a primitive CM type and (K^r, Φ^r) be its reflex. Let H be the group of all the ideals $\mathfrak{a}$ of K such that there exists an element $\mu \in K^r$ such that $N_\Phi(\mathfrak{a}) = (\mu)$ and $N(\mathfrak{a}) = \mu\overline{\mu}$ where $N(\mathfrak{a})$ is the ideal norm. Let (A, i) be an abelian variety with CM by $\mathcal{O}_K$ and $\mathcal{C}$ a polarization of A. Let k_0 be the field of moduli of $(A, \mathcal{C})$. Then H is an ideal group of K and the composite of the fields k_0 and K^r is the unramified class field over K^r corresponding to the ideal group I/H where I denotes the set of all the ideals of K.*

We don't get into the details of what is the field of moduli that appears in the statement, because we are not really interested in that part of the Theorem. We just need to know that there exits some number field k_0, and not exactly how it is defined (it is the fixed field by the group of automorphisms that when applied to an abelian variety give another that is isomorphic).

The proof of this Theorem contains the explicit Galois action which we will discuss in the next section. But we wanted to state the theorem before to do the following remark.

Remark 4.34. One of the hypothesis of the Theorem is that the CM type is primitive. However, a year later, in [Shi62], Proposition 1, Shimura proved that this condition is not necessary. Therefore, it is still true that for a biquadratic CM field we get values on the reflex field when we evaluate modular functions on the CM cycle. Since the original prove was not meant for this case, in the following discussion of the Galois action we will still consider the CM type to be primitive, but the main result it is still valid as we will check when we compute the values of modular functions at the end of the chapter.

4.8.2 The Shimura class group and the CM-action

Now we can discuss the CM action on the proof of the first Main Theorem of Complex Multiplication.

Let K be a primitive quartic CM-field (all its CM-types are primitive) and let Φ be a CM-type of K. Also let A be a principally polarized abelian surface with complex multiplication by $\mathcal{O}_K$ of CM-type Φ. Denote by F the real quadratic subfield of K.

We define a group $\mathcal{C}(K)$ called the Shimura class group as

$$\{(\mathfrak{a}, \alpha) \mid \mathfrak{a} \text{ is a fractional } \mathcal{O}_K\text{-ideal with } \mathfrak{a}\overline{\mathfrak{a}} = (\alpha) \text{ and } \alpha \in F \text{ is totally positive}\}/\sim$$

where the equivalence relation is the following: Two pairs $(\mathfrak{a}, \alpha)$ and $(\mathfrak{b}, \beta)$ are equivalent if and only if there exists an element $u \in K^*$ such that $\mathfrak{b} = u\mathfrak{a}$ and $\beta = u\overline{u}\alpha$. The multiplication in the group is defined component wise, i.e. $(\mathfrak{a}, \alpha) \cdot (\mathfrak{b}, \beta) = (\mathfrak{a}\mathfrak{b}, \alpha\beta)$, so the class of $(\mathcal{O}_K, 1)$ is the neutral element of $\mathcal{C}(K)$.

We can define a natural action of $\mathcal{C}(K)$ on $\mathcal{CM}(K, \Phi, \mathcal{O}_F)$, the set of isomorphism classes of principally polarized abelian surfaces that have CM by $\mathcal{O}_K$ of a fixed CM-type Φ in the following way:

$$(\mathfrak{b}, \beta) \cdot A(\Phi, \mathfrak{a}, \xi) = A(\Phi, \mathfrak{b}^{-1}\mathfrak{a}, \beta\xi)$$

Note that since ξ is a generator of $(\mathfrak{a}\overline{\mathfrak{a}}\mathcal{D}_K)^{-1}$, $\beta\xi$ is a generator of $\beta(\mathfrak{a}\overline{\mathfrak{a}}\mathcal{D}_K)^{-1} = (\mathfrak{b}^{-1}\mathfrak{a}\overline{\mathfrak{b}^{-1}\mathfrak{a}}\mathcal{D}_K)^{-1}$ and from the fact that β is totally positive, we have $\Phi(\beta\xi) \in (i\mathbb{R}^+)^2$ so the action is well defined (it is also compatible with the equivalence relations we defined). For every pair of principally polarized abelian surfaces $A(\Phi, \mathfrak{a}_1, \xi_1)$ and $A(\Phi, \mathfrak{a}_2, \xi_2)$ there exists a unique class in the Shimura class group that sends one to the other, so the action is regular ([Shi98], section 14.6) The class is explicitly given by $(\mathfrak{a}_2^{-1}\mathfrak{a}_1, \widetilde{\alpha})$ where $\widetilde{\alpha}$ is the totally positive generator of $\mathfrak{a}_2^{-1}\mathfrak{a}_1\overline{\mathfrak{a}_2^{-1}\mathfrak{a}_1}$.

Consider the natural map induced by the type norm map $m : \mathrm{Cl}(K^r) \to \mathcal{C}(K)$ defined by

$$\mathfrak{b} \mapsto (N_{\Phi^r}(\mathfrak{b}), N(\mathfrak{b}))$$

This map is well defined by equation (4.1) below the definition of the type norm map.

By Class Field Theory, if we let H_{K^r} be the Hilbert Class Field of K^r, we have the following isomorphism:

$$\mathrm{Gal}(H_{K^r}/K^r) \cong \mathrm{Cl}(K^r)$$

which induces a map $m : \mathrm{Gal}(H_{K^r}/K^r) \to \mathcal{C}(K)$. This map doesn't need to be injective, but has a kernel H. By [Shi98] this kernel H consists of the elements that fix the field of moduli k_0 of any abelian variety of type (K, Φ) and the quotient of $\mathrm{Gal}(H_{K^r}/K^r)$ with H gives an injective homomorphism between $\mathrm{Gal}(k_0K^r/K^r)$ and $\mathcal{C}(K)$. With this injective map and the action of $\mathcal{C}(K)$ on $\mathcal{CM}(K, \Phi, \mathcal{O}_F)$, we have described the Galois action of $\mathrm{Gal}(k_0K^r/K^r)$ on $\mathcal{CM}(K, \Phi, \mathcal{O}_F)$. There exist examples where the kernel H described above is not trivial, which means that the composite of K^r and k_0 doesn't generate the whole Hilbert Class field.

Thanks to the action of the Shimura class group we know that $\mathcal{CM}(K, \Phi, \mathcal{O}_F)$ is defined over K^r, so the values of Hilbert modular functions (that are rational over the Hilbert modular surface) on CM points of $\mathcal{CM}(K, \Phi, \mathcal{O}_F)$ lie on K^r (thanks to Remark 4.34 that is also true in the biquadratic case). However, we can say even more.

Lemma 4.35. *Let Φ be a primitive CM type of a CM field K and let $\sigma \in \mathrm{Aut}(K)$. Then*

$$\mathcal{CM}(K, \Phi, \mathcal{O}_F) = \mathcal{CM}(K, \Phi \circ \sigma, \mathcal{O}_F)$$

In particular, since complex conjugation define an automorphism,

$$\mathcal{CM}(K, \Phi, \mathcal{O}_F) = \mathcal{CM}(K, \overline{\Phi}, \mathcal{O}_F)$$

Proof. Let $[\mathfrak{a}, \xi] \in \mathcal{CM}(K, \Phi, \mathcal{O}_F)$, then by Lemma 4.31 we have that

$$\mathfrak{a} = \alpha\mathcal{O}_F + \beta\mathcal{O}_F$$

with $z = \Phi(\alpha/\beta) \in \mathbb{H}^2$ and z represents the class $[\mathfrak{a}, \xi]$ in $Y(\mathit{\Gamma}_F)$. We have that

$$\sigma^{-1}(\mathfrak{a}) = \sigma^{-1}(\alpha)\mathcal{O}_F + \sigma^{-1}(\beta)\mathcal{O}_F$$

and $(\Phi \circ \sigma)(\sigma^{-1}(\alpha)/\sigma^{-1}(\beta)) = \Phi(\alpha/\beta) = z$. We have $\sigma(\mathcal{D}_K^{-1}) = \mathcal{D}_K^{-1}$ because any automorphism fixes the ring of integers and the trace of an element is the trace of the image of the same element by any automorphism (the automorphism permutes the embeddings). Since ξ generates $(\mathfrak{a}\overline{\mathfrak{a}}\mathcal{D}_K)^{-1}$, $\sigma^{-1}(\xi)u$ generates $(\sigma^{-1}(\mathfrak{a})\overline{\sigma^{-1}(\mathfrak{a})}\mathcal{D}_K)^{-1}$ where u is any unit of K^*. And u can be chosen so that $\Phi(\sigma^{-1}(\xi)u) \in (\mathbb{R}^+)^2$ (in an analogous way to what we did in Lemma 4.31).

Therefore $[\mathfrak{a}, \xi]$ for the type Φ and $[\sigma^{-1}(\mathfrak{a}), \sigma^{-1}(\xi)u]$ for the type $\Phi \circ \sigma$ give the same point $z \in Y(\mathit{\Gamma}_F)$. Since the map $\mathfrak{a} \mapsto \sigma^{-1}(\mathfrak{a})$ is an automorphism on the ideal class group, we have

$$\mathcal{CM}(K, \Phi, \mathcal{O}_F) = \mathcal{CM}(K, \Phi \circ \sigma, \mathcal{O}_F)$$

□

As we said before, for a fixed CM type Φ, $\mathcal{CM}(K, \Phi, \mathcal{O}_F)$ is defined over K^r (even in the non-primitive case). Assume that Φ is primitive and let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$. Then $\mathcal{CM}(K, \Phi, \mathcal{O}_F)$ is fixed by $\mathrm{Gal}(\overline{\mathbb{Q}}/K^r)$. Proposition 5.5 in chapter 3 of [Lan83] states that $\overline{A(\Phi, \mathfrak{a}, \xi)} = A(\Phi, \overline{\mathfrak{a}}, \xi)$, so complex conjugation on $\mathcal{CM}(K, \Phi, \mathcal{O}_F)$ just permutes the elements, which means that $\mathcal{CM}(K, \Phi, \mathcal{O}_F)$ is fixed by $\mathrm{Gal}(\overline{\mathbb{Q}}/F^r)$ and the cycle is defined over F^r the totally real subfield corresponding to K^r.

But we can say even more. In the non-Galois case we have two equivalence classes of CM types (let's call Φ_1 and Φ_2 its representatives). We know that $\mathcal{CM}(K, \Phi_1, \mathcal{O}_F)$ and $\mathcal{CM}(K, \Phi_2, \mathcal{O}_F)$ are both defined over F^r. If we pick $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that σ is not trivial on F^r, then the CM type $\sigma \circ \Phi_1$ is equivalent to Φ_2 and by Lemma 4.26 we have that $\sigma\mathcal{CM}(K, \Phi_1, \mathcal{O}_F) = \mathcal{CM}(K, \sigma \circ \Phi_1, \mathcal{O}_F) = \mathcal{CM}(K, \Phi_2, \mathcal{O}_F)$. So they are Galois conjugate to each other.

In the Galois case we have that all the CM types are equivalent and by Lemma 4.35, for an automorphism $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we have that $\sigma\mathcal{CM}(K, \Phi, \mathcal{O}_F) = \mathcal{CM}(K, \sigma \circ \Phi, \mathcal{O}_F) = \mathcal{CM}(K, \Phi, \mathcal{O}_F)$ which means that $\mathcal{CM}(K, \Phi, \mathcal{O}_F)$ is defined over $\mathbb{Q}$. The last equality is true because $\sigma \circ \Phi$ is also a CM type (we don't need to specify which one) and therefore it is equivalent to Φ. Note that in the usual definition of equivalence, σ acts on the right, so we must check that $\sigma \circ \Phi$ is a CM type. But that is true as long as $\sigma \circ \phi_1 \neq \rho \circ \sigma \circ \phi_2$ where ρ denotes complex conjugation. But since ρ commutes with any automorphism of K because K is a CM field (Proposition 4.5), we have that

$$\sigma \circ \phi_1 \neq \rho \circ \sigma \circ \phi_2 \iff \sigma \circ \phi_1 \neq \sigma \circ \rho \circ \phi_2 \iff \phi_1 \neq \rho \circ \phi_2$$

which is true because Φ is a CM type.

Summarizing we have the following. There are 3 possibilities for quartic CM fields K:

- If K is Galois, the 4 CM types are equivalent and the 4 CM cycles $\mathcal{CM}(K, \Phi, \mathcal{O}_F)$ are the same and defined over $\mathbb{Q}$
- If K is non-Galois, there are two classes of equivalent CM types (let's call one representative of each Φ_1 and Φ_2). The two CM cycles $\mathcal{CM}(K, \Phi_1, \mathcal{O}_F)$ and $\mathcal{CM}(K, \Phi_2, \mathcal{O}_F)$ are defined over F^r and are Galois conjugate to each other, which means that $\mathcal{CM}(K, \Phi_1, \mathcal{O}_F) + \mathcal{CM}(K, \Phi_2, \mathcal{O}_F)$ is defined over $\mathbb{Q}$.
- If K is biquadratic there are two classes of equivalent CM types. The CM cycles $\mathcal{CM}(K, \Phi_1, \mathcal{O}_F)$ and $\mathcal{CM}(K, \Phi_2, \mathcal{O}_F)$ are defined over K^r (which is an imaginary quadratic field that depends on the CM type Φ).

Now, that we have all the theory that we need we can start with the computational part. We will first see the algorithm to enumerate all the CM points of a given type for a quartic CM field and then we will evaluate modular functions on them using the algorithm in the end of Chapter 3. We will also comment the results obtained and relate them to the theory.

4.9 Algorithm to enumerate all CM points of a given type for a quartic CM field

In this section we describe the algorithm in [Cas14] which is a modification of the one given by [Str10] to compute all CM points in the cycle $\mathcal{CM}(K, \Phi, \mathcal{O}_F)$.

A quartic abelian CM field $K = F(\sqrt{\alpha})$ ($\alpha \in \mathcal{O}_F$) is given where $F = \mathbb{Q}(\sqrt{d})$ for $d > 0$ is a totally real quadratic field of narrow class number equal to 1 and $\alpha \in \mathcal{O}_F$ is totally negative.

The algorithm outputs representatives for $\mathcal{CM}(K, \Phi, \mathcal{O}_F)$. As we have seen so far, it is enough for our algorithm to output a list $z_1, z_2, \dots, z_h$ (where h is the class number of K) such that the h ideals $z_j\mathcal{O}_F + \mathcal{O}_F$ are representatives of the h distinct equivalence classes in the ideal class group of K and $\Phi(z_j) \in \mathbb{H}^2$. The steps are of the algorithm are:

1. Compute representatives for the ideal class group of K.
2. Compute an integral base for $\mathcal{O}_K$ and write each element on the base as $x_i + \sqrt{\alpha} y_i$ where $x_i, y_i \in F$.

3. Compute all elements $a \in \mathcal{O}_F$ up to multiplication by $(\mathcal{O}_F^*)^2$ such that

$$|N_{F/\mathbb{Q}}(a)| \leq p\sqrt{|N_{F/\mathbb{Q}}(\alpha)|\frac{6}{\pi^2}}$$

4. Compute a set of representatives S_a of $\mathcal{O}_F/(a)$

5. For every pair (a, b) and every pair (x_i, y_i) computed in step 2, check if $y_i a, x_i + y_i b, x_i - y_i b, y_i \frac{\alpha - b^2}{a} \in \mathcal{O}_F$. Remove those pairs that don't satisfy at least one of the conditions.

6. For every pair (a, b) that is left, let

$$z = \frac{\sqrt{\alpha} - b}{a}$$

be the candidate to be a CM point. Check if $\Phi(z) \in \mathbb{H}^2$ for our CM type and if we don't have yet any CM point for the ideal class of $\mathcal{O}_F + z\mathcal{O}_F$. If so, add z to the list of CM points and continue for the other ideal classes until we have one point for each class.

The logic behind the algorithm is the following. If $\alpha \in \mathcal{O}_F$, then there exists a monic polynomial $p(x)$ of degree 2 that has α as one of its roots. Then $p(x^2)$ is a monic polynomial of degree 4 with $\sqrt{\alpha}$ as one of its roots, which means that $\sqrt{\alpha} \in \mathcal{O}_K$. For every ideal class of $\mathcal{O}_K$ there is one representative that can be written as $z\mathcal{O}_F + \mathcal{O}_F$ for $z \in K$ such that $\Phi(z) \in \mathbb{H}^2$ (that's just Lemma 4.31). If for some such z, $z\mathcal{O}_F + \mathcal{O}_F$ is an $\mathcal{O}_K$-ideal, then since $1 \in \mathcal{O}_F$ and $(z\mathcal{O}_F + \mathcal{O}_F)\mathcal{O}_K = z\mathcal{O}_F + \mathcal{O}_F$, we have that $\mathcal{O}_K \subset z\mathcal{O}_F + \mathcal{O}_F$ which means that $\sqrt{\alpha} \in z\mathcal{O}_F + \mathcal{O}_F$. Therefore, $\sqrt{\alpha} = za + b$ for $a, b \in \mathcal{O}_F$ and z can be chosen of the form

$$z = \frac{\sqrt{\alpha} - b}{a}$$

for $a, b \in \mathcal{O}_F$. But note that z and $z + c$ for $c \in \mathcal{O}_F$ are equivalent under the action of $\mathrm{SL}_2(\mathcal{O}_F)$ so they give the same CM point class, and therefore b can be chosen in the set of representatives of $\mathcal{O}_F/(a)$. Furthermore, transforming z by $\left(\begin{smallmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathcal{O}_F)$ where $\varepsilon \in \mathcal{O}_F^*$ we see that a can be chosen in a fundamental domain for multiplication by $(\mathcal{O}_F^*)^2$. Streng proves that there exists an a in a certain fundamental domain and elements in this domain satisfiy the inequality of step 3 (Lemma 6.5 in Chapter 2 of [Str10]). There are infinitely many values of a that satisfy the inequality, but finitely many if we pick all the a's in a fundamental domain for multiplication by $(\mathcal{O}_F^*)^2$.

Step 6 is clear as we just need to choose one z such that $\Phi(z) \in \mathbb{H}^2$ for each ideal class of K (that's why we compute representatives in step 1). The only step that is not so clear is 5 and it is in the algorithm for the following reason. For a given $z \in K$ there is no guarantee that $z\mathcal{O}_F + \mathcal{O}_F$ is an $\mathcal{O}_K$-ideal. The sum of two elements is clearly inside it but it is not clear that $(z\mathcal{O}_F + \mathcal{O}_F)\mathcal{O}_K = z\mathcal{O}_F + \mathcal{O}_F$ holds. Clearly, the inclusion $(z\mathcal{O}_F + \mathcal{O}_F)\mathcal{O}_K \supset z\mathcal{O}_F + \mathcal{O}_F$ is true, but the other does not need to be true. Note that in step 2 we compute an integral basis of $\mathcal{O}_K$, so it is enough to check that $(z\mathcal{O}_F + \mathcal{O}_F)(x_i + y_i\sqrt{\alpha}) \subset z\mathcal{O}_F + \mathcal{O}_F$ for the elements of the integral basis of $\mathcal{O}_K$. Actually it is a necessary condition that $z(x_i + y_i\sqrt{\alpha}) = zr + s$ for $r, s \in \mathcal{O}_F$ and $(x_i + y_i\sqrt{\alpha}) = zr + s$ for different $r, s \in \mathcal{O}_F$ both hold. But this condition is also sufficient because then every $\mathcal{O}_F$-linear combination will satisfy it. By writting $z = \frac{\sqrt{\alpha}-b}{a}$ from $(x_i + y_i\sqrt{\alpha}) = zr + s$ we get

$$x_i + y_i\sqrt{\alpha} = \frac{\sqrt{\alpha} - b}{a}r + s \iff ax_i + ay_i\sqrt{\alpha} = \sqrt{\alpha}r - br + as$$

And the parts with $\sqrt{\alpha}$ multiplying must coincide so we deduce the value of r and substituting it we get the value of s: $ay_i = r$ and $x_i + by_i = s$. Since r and s where any values in $\mathcal{O}_F$, we just get as necessary conditions $ay_i, x_i + y_ib \in \mathcal{O}_F$. Doing the same with the other necessary condition we get

$$\frac{\sqrt{\alpha} - b}{a}(x_i + y_i\sqrt{\alpha}) = \frac{\sqrt{\alpha} - b}{a}r + s \iff (\sqrt{\alpha} - b)(x_i + y_i\sqrt{\alpha}) = \sqrt{\alpha}r - br + sa \iff$$

$$\iff \sqrt{\alpha}x_i + y_i\alpha - bx_i - by_i\sqrt{\alpha} = \sqrt{\alpha}r - br + sa$$

from where we get $x_i - by_i = r$ and substituting the value of r we get that $y_i(\alpha - b^2)a^{-1} = s$, giving the 2 other conditions in step 5.

Regarding the implementation, most of the steps can be done straightforward using SageMath methods. The trickiest part is step 3. To compute all elements a with a bounded norm, up to multiplication by a positive unit, we compute all ideals (a) (which have the same norm as a) and if a is an element that generates this ideal, return $\pm a, \pm a\varepsilon$ where ε is a unit of negative norm. Finding all ideals of a bounded norm is easy if we find all prime ideals up to a certain norm and then create all possible products. To find all prime ideals, we just observe that a prime ideal $\mathfrak{p}$ has norm a power of a prime, and it must divide the ideal generated by some prime p, because since $\mathcal{O}_F/\mathfrak{p}$ is a finite field, it has characteristic p for some prime p, so $p + \mathfrak{p} = 0 + \mathfrak{p}$ in $\mathcal{O}_F/\mathfrak{p}$ and $(p) \subset \mathfrak{p}$. Therefore we consider all primes p below our bound, and factor the ideal generated by p using SageMath methods. Once we have all prime ideals that satisfy the bound, we brute force all the possible products that still satisfy the bound. The implementation of the algorithm can be found in the appendix.

In the following table we show some examples of CM cycles found using this implementation of the algorithm. We include cases for the 3 possibilities of CM field K (biquadratic, cyclic and non-Galois). For space reasons we include examples with low class number but everything works the same for higher class number fields. Note that the CM points depend on the CM type, so we must specify it. We will consider only two different CM-types, $\Phi_1 = (\phi_1, \phi_2), \Phi_2 = (\phi_1, \overline{\phi_2})$ where ϕ_1 is the identity and ϕ_2 is the other embedding that maps $\sqrt{\alpha}$ to $\sqrt{\alpha}$, because the other CM types are equivalent.

(K, Φ)	h_K	CM points
$\left(\mathbb{Q}\left(\sqrt{5}, \sqrt{-3}\right), \Phi_1\right)$	1	$\frac{1}{2}(\sqrt{-3} - \sqrt{5})$
$\left(\mathbb{Q}\left(\sqrt{5}, \sqrt{-3}\right), \Phi_2\right)$	1	$\frac{1}{4}(\sqrt{-15} + \sqrt{-3} - \sqrt{5} - 5)$
$\left(\mathbb{Q}\left(\sqrt{5}, \sqrt{-11}\right), \Phi_1\right)$	2	$\frac{1}{2}(\sqrt{-11} - \sqrt{5})$ $\frac{1}{4}(\sqrt{-11} - \sqrt{5})$
$\left(\mathbb{Q}\left(\sqrt{5}, \sqrt{-11}\right), \Phi_2\right)$	2	$\frac{1}{4}(\sqrt{-55} + \sqrt{-11} - \sqrt{5} - 5)$ $\frac{\sqrt{-55}}{10} - \frac{\sqrt{5}}{5} - \frac{3}{2}$
$\left(\mathbb{Q}\left(\sqrt{-5+\sqrt{5}}\right), \Phi_1\right)$	2	$\sqrt{-5+\sqrt{5}}$ $\frac{1}{2}\sqrt{-5+\sqrt{5}}$
$\left(\mathbb{Q}\left(\sqrt{-5+\sqrt{5}}\right), \Phi_2\right)$	2	$\frac{1}{2}(\sqrt{5}+1)\sqrt{-5+\sqrt{5}}$ $\frac{1}{4}(\sqrt{5}+1)\sqrt{-5+\sqrt{5}}$
$\left(\mathbb{Q}\left(\sqrt{-11+4\sqrt{5}}\right), \Phi_1\right)$	1	$\frac{1}{2}(\sqrt{-11+4\sqrt{5}} - \sqrt{5})$
$\left(\mathbb{Q}\left(\sqrt{-11+4\sqrt{5}}\right), \Phi_2\right)$	1	$\frac{1}{4}((\sqrt{5}+1)\sqrt{-11+4\sqrt{5}} - \sqrt{5} - 5)$
$\left(\mathbb{Q}\left(\sqrt{-65+18\sqrt{13}}\right), \Phi_1\right)$	1	$\frac{1}{6}((\sqrt{13}+4)\sqrt{-65+18\sqrt{13}} - 4\sqrt{13} - 13)$
$\left(\mathbb{Q}\left(\sqrt{-65+18\sqrt{13}}\right), \Phi_2\right)$	1	$\frac{1}{4}((\sqrt{13}+3)\sqrt{-65+18\sqrt{13}} - 3\sqrt{13} - 13)$

Table 4.1: CM points for quartic CM fields

4.10 Evaluating Hilbert modular functions at CM points

From the previous chapter we know how to evaluate certain Borcherds products at CM points. We saw that sometimes the Borcherds lift can be obtained as the Doi-Naganuma lift which makes computations much easier. Now, if we divide two Borcherds products of the same weight (Ψ_6/Ψ_1^2, for instance) we get a Hilbert modular function, and using the theory we have seen, we know that its value at CM points are algebraic numbers. Furthermore, the product of all the values of a cycle (the value of the function on the cycle) are algebraic numbers of very small degree (at most 2 since they lie on F^r, the totally real subfield of the reflex for the non-biquadratic case) and in some cases rational numbers. Our goal is to check those results given by the theory of Complex Multiplication numerically. Note that even if our result is known to be a rational and we have 100 decimal digits of precision, since $\mathbb{Q}$ is dense in $\mathbb{R}$ and the precision of the computer is finite, we can find infinitely many rational as close as we wish to the value we obtain. In some cases, if we know that the denominator of our rational number is bounded (we will see some proven results related to this), we may be able to get a unique value. However, this will not be the case every time, so to know the exact values we will rely on some heuristics. For instance, when a number is less than 10^{-50} away from an integer, it's "safe" to assume it to be an integer. Similar things will happen when we know that a value belongs to an algebraic extension. There are infinitely many numbers in that extension as close as we wish to our approximation, but makes sense to assume that the minimal polynomial will not have really large coefficients and that SageMath method algdep will help us determining the exact value of the modular function. This function of SageMath accepts a complex number z, and two integers n and m and tries to find a polynomial of degree at most n such that a number that coincides with z up to an error of 10^{-m} is a root of it. In the case where we try to find a degree 1 polynomial, this can be done by using continuous fractions, but for higher degrees, the internal implementation of algdep is harder.

To discuss the numerical values obtained, we split the CM points depending on whether K is biquadratic, cyclic or non-Galois and discuss some of the results. We also add a table at the end of the case with some more values that we don't discuss. Thanks to Lemma 4.20 we can easily identify in which case we are just by looking at $\alpha \in F$, the square of the element we adjoint to F to get $K = F(\sqrt{\alpha})$. We have 4 embeddings from K into $\mathbb{C}$ and we will denote them by $\{\phi_1, \phi_2, \overline{\phi_1}, \overline{\phi_2}\}$. ϕ_1 will always be the identity and ϕ_2 will be the embedding such that $\Im(\phi_2(\sqrt{\alpha})) > 0$. The four CM types will be denoted by $\Phi_1 = (\phi_1, \phi_2)$, $\Phi_2 = (\phi_1, \overline{\phi_2})$, $\overline{\Phi_2} = (\overline{\phi_1}, \phi_2)$ and $\overline{\Phi_2} = (\overline{\phi_1}, \overline{\phi_2})$.

K is cyclic

According to Lemma 4.20, for K to be cyclic Galois that $\alpha = x + y\sqrt{D}$ satisfies that $\sqrt{x^2 - Dy^2} = k\sqrt{D}$ for some $k \in \mathbb{Q}$, so $x^2 - Dy^2 = Dk^2$. Let's start with some examples for $D = 5$. Note that $(x, y, k) = (5/2, 1/2, 1)$ gives a solution, so $K = F(\sqrt{(-5+\sqrt{5})/2})$ is Galois cyclic and note that $(-5+\sqrt{5})/2 \in \mathcal{O}_F$. The class number of K is one, so there is only one point. We have 4 possible CM types but they are all equivalent, so we should we get the same result for all of them. That's exactly what happens if we try numerically. The results of evaluating Ψ_6/Ψ_1^2 and Ψ_{10}/Ψ_1^2 doing 80 iterations of the outer sum for evaluating the Doi-Naganuma are (after approximating) $248832 = 2^{10} \cdot 3^5$ and $3200000 = 2^{10} \cdot 5^5$. The actual values where complex numbers whose imaginary part was in the order of 10^{-300} and the real part was off by less than 10^{-100}. In this case, the result is not only a rational but also an integer. Furthermore, it satisfies the formula given by Bruinier and Yang in [BY06].

In this article Bruinier and Yang tried to find a formula for the values of Hilbert modular functions similar to those obtained by Gross and Zagier for the different of the values of the j-invariant on two points. The problem is so difficult that they just found the answer for concrete cases. They focused on the non-biquadratic case. They assumed that $F = \mathbb{Q}(\sqrt{p})$ for a prime number p such that $p \equiv 1 \pmod 4$ and that the discriminant of $K = F(\sqrt{\alpha})$ is p^2q where $q \equiv 1 \pmod 4$ is also prime. The nice thing about the formula is that it gives as a direct corollary that the values of the modular functions have prime factors that are bounded by some constant. Although we don't have a similar formula for other cases, it is reasonable to expect that other cases will also give results with small prime factors and as we will see that is exactly what happens (also for the non-Galois and the biquadratic case).

We can now check a case where the class number of K is greater than 1. Let $K = F\left(\sqrt{(-15+3\sqrt{5})/2}\right)$, which has class number 4. If we compute Ψ_6/Ψ_1^2 at the 4 CM points and compute the polynomial they satisfy, we get a polynomial with non-integer coefficients. However, they must be rational and by using algdep SageMath method on them, we see that they are close to rational numbers with denominator 961. Actually by multiplying the coefficients by 961, we see that they turn out to be off to an integer by less than 10^{-100}. The polynomial is that the CM values satisfy is

$$P(x) = 961x^4 - 10444049220446208x^3 + 4001489959533907437158 4x^2$$

$$-3191277558026282505516299059 2x + 545948319606643177763568923285913 6$$

Its roots can be computed exactly and turn out to be $5433946808832 \pm 2430134784000\sqrt{5}$ and $1726935552/961 \pm 435456000/961\sqrt{5}$ so they all belong to F^r. In particular, they belong to any extension of the reflex of K, $K^r = \mathbb{Q}(\sqrt{\alpha} + \sqrt{\alpha'})$. Note that all those numbers have norms which have lots of factors, and in particular, the product of the CM values (independent term of the polynomial divided by 961) factors as $2^{36} \cdot 3^{16} \cdot 31^{-2} \cdot 41^2 \cdot 691 \cdot 1051 \cdot 1171 \cdot 1291$.

Finally for $F = \mathbb{Q}(\sqrt{13})$ we can also use the same technique to get the Borcherds products $\Psi_1^6, \Psi_{14}, \Psi_{26}$ and the values obtained for the Galois extension of class number 1, $\mathbb{Q}\left(\sqrt{-65+18\sqrt{13}}\right)$ are $2^6 \cdot 7$ and $2^6 \cdot 13^2$ for Ψ_{14}/Ψ_1^6 and Ψ_{26}/Ψ_1^6, respectively.

In the following table we summarize the products of the CM values on the cycle $\mathcal{CM}(K, \Phi, \mathcal{O}_F)$ for $\Phi = (\phi_1, \phi_2)$ of the commented cases and some other cyclic Galois examples that we add.

K	h_K	$\frac{\Psi_6}{\Psi_1^2}(\mathcal{CM}(K,\Phi,\mathcal{O}_F))$	$\frac{\Psi_{10}}{\Psi_1^2}(\mathcal{CM}(K,\Phi,\mathcal{O}_F))$
$\mathbb{Q}\left(\sqrt{\frac{-5+\sqrt{5}}{2}}\right)$	1	$2^{10}\cdot 3^5$	$2^{10}\cdot 5^5$
$\mathbb{Q}\left(\sqrt{\frac{-15+3\sqrt{5}}{2}}\right)$	4	$2^{36}\cdot 3^{16}\cdot 31^{-2}\cdot 41^2\cdot$ $691\cdot 1051\cdot 1171\cdot 1291$	$-2^{36}\cdot 5^{20}\cdot 359\cdot 599\cdot 719$
$\mathbb{Q}\left(\sqrt{-5+\sqrt{5}}\right)$	2	$2^{20}\cdot 3^{10}\cdot 331\cdot 571$	$-2^{18}\cdot 5^{10}\cdot 199\cdot 239$
$\mathbb{Q}\left(\sqrt{-65+26\sqrt{5}}\right)$	2	$2^{20}\cdot 3^{10}\cdot 31^{-2}\cdot 41^{-2}\cdot 79^2\cdot$ $241\cdot 541\cdot 1021\cdot 1201$	$2^{20}\cdot 5^{10}\cdot 13^2\cdot 41^{-2}\cdot$ $269\cdot 809\cdot 829$

K	h_K	$\frac{\Psi_{14}}{\Psi_1^6}(\mathcal{CM}(K,\Phi,\mathcal{O}_F))$	$\frac{\Psi_{26}}{\Psi_1^6}(\mathcal{CM}(K,\Phi,\mathcal{O}_F))$
$\mathbb{Q}\left(\sqrt{-65+18\sqrt{13}}\right)$	2	$2^6\cdot 7$	$2^6\cdot 13^2$

Table 4.2: CM values for Galois quartic CM fields

K is non-Galois

In this case we have two pairs of equivalent CM types, and evaluating the modular function on just one cycle doesn't assure us that we will get a rational value, like before. If we let $\Phi_1 = (\phi_1, \phi_2)$ (with the choice that we said at the beginning of the section) and $\Phi_2 = (\phi_1, \overline{\phi_2})$, then the product of the CM values for all the points in $\mathcal{CM}(K,\Phi_1,\mathcal{O}_F) + \mathcal{CM}(K,\Phi_2,\mathcal{O}_F)$ is rational, and the product of the values for one of the products belongs to the totally real subfield of the reflex field $F^r = \mathbb{Q}(\sqrt{\alpha\alpha'})$ if we let $K = F(\sqrt{\alpha})$.

Let $\alpha = -4+\sqrt{5}$. Note that $\sqrt{\alpha\alpha'} = \sqrt{11}$, so by Lemma 4.20 we are in the non Galois case. The class number of $K = F(\sqrt{\alpha})$ is 2, so we have two CM points for each CM type. Let's consider the modular function Ψ_{10}/Ψ_1^2. The value $\Psi_{10}/\Psi_1^2(\mathcal{CM}(K,\Phi_1,\mathcal{O}_F))$ doesn't have to be rational and by using algdep it does not seem to be the case. However if we try to look for a degree 2 polynomial that vanishes at our CM value, we get the following polynomial:

$$x^2 - 11077177225773056x + 25353855120179200000000000000000$$

whose roots are $5538588612886528 \pm 695577503858688\sqrt{11}$. The one with the positive sign coincides with the numerical value with an error of less than 10^{-130}. Therefore $\Psi_{10}/\Psi_1^2(\mathcal{CM}(K,\Phi_1,\mathcal{O}_F)) \in \mathbb{Q}(\sqrt{11})$, which is the totally real subfield of $K^r = \mathbb{Q}(\sqrt{\alpha}+\sqrt{\alpha'})$ the reflex field of K.

As we could expect, for the other CM type we get $\Psi_{10}/\Psi_1^2(\mathcal{CM}(K,\Phi_2,\mathcal{O}_F)) = 5538588612886528 - 695577503858688\sqrt{11}$ and therefore the product of the two CM values is the integer 25353855120179200000000000000000. For Ψ_6/Ψ_1^2 we have that $\Psi_6/\Psi_1^2(\mathcal{CM}(K,\Phi_1,\mathcal{O}_F)) = 471547166588928+55168371523584\sqrt{11}$, $\Psi_6/\Psi_1^2(\mathcal{CM}(K,\Phi_2,\mathcal{O}_F)) = 471547166588928 - 55168371523584\sqrt{11}$ and its product is the integer that can be found on the next table. For space reasons, we denote $\mathcal{CM}(K,\Phi,\mathcal{O}_F)$ by $\mathcal{CM}(K,\Phi)$ omitting the $\mathcal{O}_F$.

K	h_K	$\frac{\Psi_6}{\Psi_1^2}(\mathcal{CM}(K,\Phi_1)+\mathcal{CM}(K,\Phi_2))$	$\frac{\Psi_{10}}{\Psi_1^2}(\mathcal{CM}(K,\Phi_1)+\mathcal{CM}(K,\Phi_2))$
$\mathbb{Q}\left(\sqrt{-4+\sqrt{5}}\right)$	2	$2^{36}\cdot 3^{20}\cdot 43\cdot 211\cdot 283\cdot 307$	$2^{36}\cdot 5^{17}\cdot 127\cdot 151^2\cdot 167$
$\mathbb{Q}\left(\sqrt{-26+11\sqrt{5}}\right)$	4	$2^{72}\cdot 3^{40}\cdot 23^{-2}\cdot 29^2\cdot 37^2\cdot$ $47^{-2}\cdot 67^3\cdot 163\cdot 229^2$ $277^2\cdot 859\cdot 1483\cdot 1987\cdot 2011$	$2^{72}\cdot 5^{35}\cdot 23^3\cdot 29^2\cdot 47^{-1}\cdot$ $73^2\cdot 227\cdot 607\cdot 911^2\cdot 967\cdot 1087$
$\mathbb{Q}\left(\sqrt{-21+2\sqrt{5}}\right)$	1	$2^{20}\cdot 3^{10}\cdot 31^2\cdot 37\cdot 229$	$2^{20}\cdot 5^{12}\cdot 17\cdot 113$
$\mathbb{Q}\left(\sqrt{-31+8\sqrt{5}}\right)$	5	$2^{66}\cdot 3^{50}\cdot 13^{-2}\cdot 37^2\cdot 131^2\cdot 137^2$ $\cdot 151^2\cdot 173^2\cdot 229\cdot 613\cdot 997\cdot 1153$	$2^{66}\cdot 5^{44}\cdot 59^2\cdot 71^2\cdot 157\cdot$ $241^2\cdot 317\cdot 541^2\cdot 577\cdot 641$

Table 4.3: CM values for non-Galois quartic CM fields

K is biquadratic

In this case the CM types are not primitive but we still know that the values fall on a quadratic field, that depends on the CM type. If $K=\mathbb{Q}(\sqrt{d},\sqrt{\alpha})$ with $d>0$ and $\alpha<0$ integers, then we may have $K^r=\mathbb{Q}(\sqrt{\alpha})$ or $K^r=\mathbb{Q}(\sqrt{\alpha d})$ depending on the CM type.

In the biquadratic case we also have two pairs of equivalent CM types (conjugate pairs are always equivalent). As before, we will let $\Phi_1=(\phi_1,\phi_2)$ and $\Phi_2=(\phi_1,\overline{\phi_2})$ represent those equivalent pairs where ϕ_1 is the identity and ϕ_2 is the embedding that satisfies $\phi_2(\sqrt{\alpha})=\sqrt{\alpha}$ other than the identity.

For the case $\mathbb{Q}\left(\sqrt{5},\sqrt{-11}\right)$ which has class number 2 and the CM type Φ_2, we get that the polynomial whose roots are the values of $\frac{\Psi_{10}}{\Psi_1^2}$ on $\mathcal{CM}(K,\Phi_2,\mathcal{O}_F)$ is

$$x^2+\frac{986328125}{11}x+275421142578125$$

and therefore the exact values are $-49316406/11\pm 409765625\sqrt{5}/22$ which lie on $F=\mathbb{Q}(\sqrt{5})$. For $\frac{\Psi_6}{\Psi_1^2}$ the polynomial whose roots are the CM values on the cycle is

$$x^2-117654039x+28827586046349$$

whose exact roots also lie in $\mathbb{Q}(\sqrt{5})$ and are $117654039/2\pm -52396875\sqrt{5}/2$.

A last interesting case is $\mathbb{Q}\left(\sqrt{5},\sqrt{-23}\right)$ which has class number 3. All the CM values for $\frac{\Psi_6}{\Psi_1^2}$ are rational and two of them are equal. They are 504476024832 and 2615721984/3887 (twice). For $\frac{\Psi_{10}}{\Psi_1^2}$ two of the values are 0 and the other is the rational number 11552000000000/23.

One of the differences that we observe in the biquadratic case is that for Φ_1 in several cases Ψ_1^2 vanishes while the other Borcherds lift don't. Moreover in some cases we get that if K has class number 2, for instance, for one point in the cycle Ψ_1^2 vanishes while for the others doesn't and for the other point we get a nice integer. An example of this would be $\mathbb{Q}(\sqrt{5}, \sqrt{-11})$ where one point gives $2^{14} \cdot 13$ as its CM value for Ψ_6/Ψ_1^2 and the other vanishes at Ψ_1^2 but not at Ψ_6. The fact that Ψ_1^2 vanishes on a CM point means that it belongs to the Hirzebruch-Zagier divisor T_1. We only present the table for Φ_2 as for Φ_1 we have plenty of zeros. From the results on that table we observe that Ψ_6 does not seem to vanish, so the CM points don't belong to T_6, but in some cases Ψ_{10} vanishes, which suggests that depending on α, there is a CM point in T_{10} or not.

K	h_K	$\frac{\Psi_6}{\Psi_1^2}(\mathcal{CM}(K, \Phi_2))$	$\frac{\Psi_{10}}{\Psi_1^2}(\mathcal{CM}(K, \Phi_2))$
$\mathbb{Q}\left(\sqrt{5}, \sqrt{-1}\right)$	1	$2^9 \cdot 19^2$	0
$\mathbb{Q}\left(\sqrt{5}, \sqrt{-2}\right)$	1	$2^8 \cdot 3^6 \cdot 43$	0
$\mathbb{Q}\left(\sqrt{5}, \sqrt{-3}\right)$	1	$3^4 \cdot 13^3$	5^9
$\mathbb{Q}\left(\sqrt{5}, \sqrt{-7}\right)$	1	$2^{16} \cdot 37$	0
$\mathbb{Q}\left(\sqrt{5}, \sqrt{-11}\right)$	2	$3^{12} \cdot 23^2 \cdot 41^2 \cdot 61$	$5^{17} \cdot 19^2$
$\mathbb{Q}\left(\sqrt{5}, \sqrt{-19}\right)$	4	$17^2 \cdot 19^2 \cdot 23^2 \cdot 29^2 \cdot 47^2 \cdot$ $59^2 \cdot 79^2 \cdot 89^2 \cdot 109$	$5^{34} \cdot 17^2 \cdot 29 \cdot 31^2$
$\mathbb{Q}\left(\sqrt{5}, \sqrt{-23}\right)$	3	$2^{42} \cdot 3^{22} \cdot 13^{-3} \cdot 19^2 \cdot 23^{-2} \cdot 73^2$	0
$\mathbb{Q}\left(\sqrt{5}, \sqrt{-43}\right)$	7	$13^9 \cdot 17^4 \cdot 19^2 \cdot 23^2 \cdot 29^4 \cdot 43^2 \cdot$ $53^2 \cdot 71^2 \cdot 89^2 \cdot 103^2 \cdot 173^2 \cdot 193^2$	$5^{66} \cdot 13^4 \cdot 17^5 \cdot 19^{-2} \cdot 23^2 \cdot 61$

Table 4.4: CM values for biquadratic CM fields

Appendix

Implementation of the algorithm to enumerate the CM points

The following implementation in SageMath returns the images of the CM points by the CM type in a list for a quartic CM field whose totally real subfield has narrow class number 1. Note that the CM points are not unique (they are up to the action of $\mathrm{SL}_2(\mathcal{O}_F)$) so the same algorithm may get different outcomes on different machines or different versions of SageMath.

```
p = 5
var('X')
F.<sqrt_p> = NumberField(X^2-p, embedding = 1)
q = F(-17+2*sqrt_p)
K.<sqrt_q> = F.extension(X^2-q)

embdsKtoK = Hom(K, K).list()
embdsKtoC = K.complex_embeddings(prec=1000)

for emb in embdsKtoK:
    if emb(sqrt_p) == sqrt_p:
        if emb(sqrt_q) == sqrt_q:
            id_emb = emb
        else:
            conj_emb = emb

for emb in embdsKtoC:
    if emb(sqrt_p).real() > 0:
        if emb(sqrt_q).imag() > 0:
            phi1 = emb
            evaluate = emb
        else:
            phi1conj = emb
    else:
        if emb(sqrt_q).imag() > 0:
            phi2 = emb
        else:
            phi2conj = emb


# Compute a set of representatives of the ideal class group of K.
C = K.class_group().list()
```

```
representatives_ideal_class = [x.ideal() for x in C]

# Compute an integral basis of OK.
OF = F.ring_of_integers()
OK = K.ring_of_integers()
basisOK = OK.basis()

# Write each element in the integral basis of OK in the form x + y*sqrt_q
x = [(conj_emb(bb)+bb)/2 for bb in basisOK]
y = [(-conj_emb(bb)+bb)/(2*sqrt_q) for bb in basisOK]

def generate(prime_ideals, bound, pos, I, nrm_id):
    if pos >= len(prime_ideals):
        return [I]
    id_p = prime_ideals[pos]
    nrm_p = id_p.absolute_norm()
    expon = 0
    ans = []
    while nrm_id*(nrm_p^expon) <= bound:
        ans += generate(prime_ideals, bound, pos+1, I*(id_p^expon), nrm_id*(nrm_p^expon))
        expon += 1
    return ans


# Generate prime ideals of bounded norm
upper_bound = sqrt(abs(q.absolute_norm()))*p*6/(pi^2)
prime = 2
prime_ideals = []
while prime < upper_bound:
    I = F.ideal(prime)
    decomp = I.factor()
    for fact in decomp:
        if fact[0].absolute_norm() <= upper_bound:
            prime_ideals.append(fact[0])
    prime = next_prime(prime)

# Generate all ideals of bounded norm as a product of prime ideals
ideals_bound = generate(prime_ideals, upper_bound, 0, F.ideal(1), 1)


def representatives(gens, order_gens, pos, val):
    if pos >= len(gens):
        return [val.lift()]
    ans = []
    for i in range(order_gens[pos]):
        ans += representatives(gens, order_gens, pos+1, val+i*gens[pos])
    return ans

# Generate all candidate pairs (a,b)
candidate_pairs = []
fund_unit = F.unit_group().gens()[1]
```

```
for I in ideals_bound:
    a = I.gens_reduced()[0]
    R = QuotientRing(OF, I, 'w')
    gens = list(R.gens())
    order_gens = []
    for g in gens:
        o = 1
        while o*g != 0: o += 1
        order_gens.append(o)
    reps = list(Set(representatives(gens, order_gens, 0, 0)))
    for b in reps:
        candidate_pairs.append((a, b))
        candidate_pairs.append((-a, b))
        candidate_pairs.append((a*fund_unit, b))
        candidate_pairs.append((-a*fund_unit, b))


def is_integralofF(x):
    minpolyQ = x.absolute_minpoly()
    if minpolyQ.degree() > 2: return False
    coeffs = minpolyQ.coefficients()
    for coef in coeffs:
        if not coef.is_integral():
            return False
    return (minpolyQ.leading_coefficient() == 1)

# Filter the pairs that don't give a z such that z*O_F+O_F is an O_K ideal
filtered_cand = []
for cand in candidate_pairs:
    a, b = cand
    valid = True
    for i in range(len(x)):
        if (not is_integralofF(y[i]*a) or (not is_integralofF(x[i]+y[i]*b)) or (not is_integralofF(x[i]-y[i]*b)) or (not is_integralofF(y[i]*(q-b*b)/a))):
            valid = False
            break

    if valid:
        filtered_cand.append(cand)

# Keep a CM point for each ideal class
cm_pts_found = [0]*len(representatives_ideal_class)

for cand in filtered_cand:
    z = (sqrt_q-cand[1])/cand[0]
    if (phi1(z).imag() > 0.0 and phi2(z).imag() > 0.0):
        for idx in range(len(representatives_ideal_class)):
            if K.ideal(1,z).ideal_class_log() == representatives_ideal_class[idx].ideal_class_log():
                cm_pts_found[idx] = z


```

```
print(len(cm_pts_found)," CM points:", cm_pts_found)
cm_pts_H2 = [(phi1(cm_pt), phi2(cm_pt)) for cm_pt in cm_pts_found]
print("Image by the CM type:", cm_pts_H2)
```

Implementation of the algorithm to evaluate the Borcherds lift

The following implementation in SageMath uses the Doi-Naganuma lift to evaluate certain Borcherds lifts. The first part computes the modular forms that we will lift. As it is right now, it will compute the lift for $p = 5$ but it can be changed for instance for $p = 13$. However, it is assumed that $p \equiv 1 \pmod 4$.

The current code will be very slow because of the 3 lines that compute the coefficients of the three modular forms in the plus space g_1, g_6, g_{10}. It is recommended to precompute the coefficients and save them on a text file so that every time that a computation must be done this part can be executed instantly.

```
# Get the 3 modular forms of the plus space whose image
# by the Doi-Naganuma lift gives the Borcherds lifts
chi = DirichletGroup(p)[2]
weight = 10
m = ModularForms(chi, weight)
m1, m2, m3, m4, m5, m6 = m.gens()
g1 = m4
g6 = (-108972864*m1+124723618560*m4+6600*m6)/412751-132*m5
g10 = (-1403360000*m1+1669006720000*m4+6600*m6)/412751-132*m5
g1_coeffs = g1[0:10000]
g6_coeffs = g6[0:10000]
g10_coeffs = g10[0:10000]

ITERS = 80

# Computes the Doi-Naganuma lift
def DNlift(p, weight, z1, z2, LIM, g):
    sq = sqrt(p)
    S = -bernoulli(weight)*g[0]/(weight)
    for x2 in range(1, LIM):
        LOW = ceil(-x2*(1+sq)/2)
        HI = floor(x2*(sq-1)/2)
        for x1 in range(LOW, HI+1):
            innersum = 0
            lim_d = min(abs(x1), x2)
            if lim_d == 0: lim_d = x2
            for d in range(1, lim_d+1):
                if x1%d == 0 and x2%d == 0:
                    mult = 1
                    if ((x2*x2*((p-1)/4)-x1*(x1+x2))//(d*d))%p == 0: mult = 2
                    innersum += d^(weight-1)*g[(x2*x2*((p-1)/4)-x1*(x1+x2))//(d*d)]*mult
            S += innersum*exp(numerical_approx(2*pi*sqrt(-1)*(z1*(x1/sq+x2*(1/2+1/(2*sq)))+z2*(-x1/sq+x2*(1/2-1/(2*sq)))), digits=1000))
    return S

VALUE = 1
VALUES = []
for (z1,z2) in cm_pts_H2:
    S1 = DNlift(p, weight, z1, z2, ITERS, g1_coeffs)
    S2 = DNlift(p, weight, z1, z2, ITERS, g6_coeffs)
    res = numerical_approx(S2/S1, digits=1000)
    VALUE *= res
    VALUES.append(res)
print(VALUE)
print(VALUES)
```

Bibliography

[BB01] Jan Hendrik Bruinier and Michael Bundschuh. *On Borcherds Products Associated with Lattices of Prime Discriminant.* 2001.

[Bil12] Margaret Bilu. “Complex multiplication of abelian varieties”. In: 2012.

[Bor98] Richard E. Borcherds. “Automorphic forms with singularities on Grassmannians”. In: *Inventiones Mathematicae* 132.3 (1998), pp. 491–562.

[Bru08] Bruinier. *The 1-2-3 of Modular Forms.* Springer-Verlag Berlin Heidelberg, 2008.

[BY05] Jan Hendrik Bruinier and Tonghai Yang. *Twisted Borcherds products on Hilbert Modular Surfaces and their CM values.* 2005.

[BY06] Jan Hendrik Bruinier and Tonghai Yang. *CM-values of Hilbert modular functions.* 2006.

[Cas14] Robert Cass. *The Chowla-Selberg formula for quartic abelian CM fields.* 2014.

[Cox89] David A. Cox. *Primes of the form x^2+ny^2.* John Wiley & Sons, Inc, 1989.

[ET13] Andreas Enge and Emmanuel Thomé. “Computing class polynomials for abelian surfaces”. In: (2013).

[Fre90] Eberhard Freitag. *Hilbert modular forms.* Springer-Verlag Berlin Heidelberg, 1990.

[Gar90] Paul B. Garrett. *Holomorphic Hilbert Modular Forms.* Brooks/Cole publishing company, 1990.

[Gee88] Gerard van der Geer. *Hilbert Modular Surfaces.* Springer-Verlag Berlin Heidelberg, 1988.

[Gor02] Eyal Z. Goren. *Lectures on Hilbert Modular Varieties and Modular Forms.* American Mathematical Society, 1002.

[KR99] S. Kudla and M. Rapoport. *Arithmetic Hirzebruch Zagier cycles.* 1999.

[Lan83] Serge Lang. *Complex Multiplication.* Springer-Verlag New York Inc, 1983.

[Mil20] James S. Milne. *Complex Multiplication (v0.10).* 2020.

[Mil21] James S. Milne. *Fields and Galois Theory (v5.00).* 2021.

[Oda77] Takayuki Oda. “On Modular Forms Associated with Indefinite Quadratic Forms of Signature $(2, n-2)$.” In: *Mathematische Annalen* 231 (1977), pp. 97–144.

[RL11] David Gruenewald Reinier Bröker and Kristin Lauter. *Explicit CM-theory for level* 2*-structures on abelian surfaces.* 2011.

[Shi62] Goro Shimura. “On the class-fields obtained by complex multiplication of abelian varieties”. In: (1962).

[Shi98] Goro Shimura. *Abelian varieties with Complex Multiplication and modular functions.* Princeton University Press, 1998.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves.* Springer-Verlag New York, Inc, 1994.

[Str10] Marco Streng. “Complex multiplication of abelian surfaces”. 2010.

[Wam99] Paul Van Wamelen. *Examples of genus two CM curves defined over the rationals.* 1999.