UNIVERSIDAD DE BUENOS AIRES
Facultad de Ciencias Exactas y Naturales
Departamento de Matemática

Cálculo de formas de Hilbert de pesos entero y medio entero

Tesis presentada para optar al título de Doctor de la Universidad de Buenos Aires en el área Ciencias Matemáticas

Nicolás Sirolli

Director de tesis: Ariel Pacetti
Consejero de estudios: Ariel Pacetti

Buenos Aires, abril de 2013

Gracias, Ariel.

Cálculo de formas de Hilbert de pesos entero y medio entero

Introducción

En esta tesis hemos trabajado en dos temas distintos relacionados con el cálculo de formas modulares de Hilbert: el problema de calcular representantes para clases de ideales en álgebras de cuaterniones totalmente definidas, y el problema de calcular preimágenes para el mapa de Shimura en formas modulares de Hilbert. Aunque los dos temas pueden ser considerados por separado, por lo cual hemos dividido esta tesis en dos capítulos, ambos están estrechamente relacionados: el método que damos para calcular preimágenes para el mapa de Shimura depende fuertemente de la posibilidad de calcular representantes para clases de ideales.

Capítulo 1: Cálculo de representantes para clases de ideales en álgebras de cuaterniones

La teoría de álgebras de cuaterniones sobre cuerpos de números juega un rol central en varios cálculos relacionados con formas modulares. La idea de obtener formas modulares como series theta asociadas a ciertos retículos en álgebras de cuaterniones se retrotrae a Hecke (ver [Hec40]). Eichler y otros (ver [Eic73], [HS73], [Piz76b]) probaron que toda forma modular cuyo nivel no sea un cuadrado puede ser obtenida como una combinación lineal de estas series theta, usando como retículos los ideales para cierto orden en un álgebra de cuaterniones definida. Como ideales equivalentes dan la misma serie theta, para este propósito alcanza con considerar clases de ideales. Pizer dio en [Piz80] un algoritmo para calcular los órdenes de Eichler y sus clases de ideales, el cual consiste en precalcular el número de clases del orden y luego empezar a calcular ideales (de una manera bastante aleatoria) hasta que el número de clases es alcanzado.

El cálculo de formas modulares de Hilbert ha sido un tema de intensa investigación en los últimos años. Poder calcularlas es crucial para obtener evidencias numéricas para comprobar la veracidad de ciertas construcciones de la Teoría de Números que son bien conocidas sobre los números racionales pero que son todavía conjeturales sobre otros cuerpos de números, como la teoría de Eichler-Shimura. Las clases de ideales para órdenes de Eichler en álgebras de cuaterniones totalmente definidas sobre cuerpos de números totalmente reales pueden ser utilizadas para calcular formas modulares de Hilbert, como se explica en [CS01] para formas modulares de Hilbert sobre $\mathbb{Q}[\sqrt{5}]$ y en [SW05] sobre otros cuerpos cuadráticos reales, siguiendo las ideas de Pizer

Todos estos métodos requieren primero encontrar un orden apropiado en una tal álgebra, y luego calcular representantes para sus clases de ideales. El propósito de nuestro trabajo es calcular ambas cosas de una manera eficiente, y en un contexto general. Concretamente, dada un álgebra de cuaterniones totalmente definida B sobre un cuerpo totalmente real F, damos un algoritmo para calcular representantes para clases de ideales para cualquier orden de Bass en B.

Consideramos una vasta familia de órdenes, los órdenes de Bass. Además de los bien conocidos órdenes de Eichler, esta familia incluye los órdenes de nivel p^{2r+1} considerados por Pizer en [Piz76a], los órdenes utilizados en [PRV05] para calcular formas modulares de nivel p^2, y los órdenes considerados en [PT07] para calcular preimágenes para tales formas bajo la correspondencia de Shimura. El resto de los órdenes de Bass son incluidos por completitud.

Nuestro algoritmo, en contraste con los métodos *à la Pizer*, no requiere conocimientos sobre número de clases, evita el cálculo aleatorio de ideales, y evita el uso repetido de la forma norma para chequear equivalencia entre ideales, todo lo cual hace que el método sea eficiente.

Como la implementación completa (en SAGE) de nuestro algoritmo está aún bajo desarrollo, no podemos hacer una comparación sistemática a gran escala de tiempos de ejecución; de todas maneras, en [PRV00] hay un algoritmo, que puede ser considerado como un caso particular del nuestro, que calcula representantes para clases de ideales para órdenes de nivel p^2 en el álgebra sobre $\mathbb{Q}$

ramificada exactamente en p y en infinito. Este algoritmo tiene un rendimiento mucho mejor que el de MAGMA en algunos casos sencillos. Por ejemplo, al calcular representantes para clases de ideales para un orden de discriminante 103^2 en el álgebra sobre $\mathbb{Q}$ ramificada exactamente en 103 e infinito, con una computadora Intel Core™2 CPU 6600 con 2 Gb de memoria RAM, MAGMA (V2.16-6) necesita 1254,96 segundos, mientras que las rutinas en PARI/GP (V2.5.0) tardan 0,00218 segundos.

Los resultados obtenidos en este capítulo fueron enviados y aceptados para su publicación en la revista *Mathematics of Computation*, en un trabajo conjunto con mi director de tesis, Ariel Pacetti. Ver [PS13].

Capítulo 2: Preimágenes para el mapa de Shimura en formas modulares de Hilbert

El mapa de Shimura es un mapa Hecke lineal entre formas modulares de peso medio entero y formas modulares de peso entero, introducido en [Shi73] para formas modulares clásicas y generalizado en [Shi87] a formas modulares de Hilbert, así como al contexto automorfo en trabajos de Waldspurger, Flicker y otros. Calcular preimágenes para el mapa de Shimura comenzó a ser un tema de interés a partir de las fórmulas dadas por Waldspurger, Kohnen-Zagier, Gross y otros, relacionando los valores centrales de twists de la serie L asociada a una forma modular de peso entero f con los coeficientes de una forma de peso medio entero g correspondiendo a f por el mapa de Shimura (por ejemplo, ver [BSP90]). Estas fórmulas fueron utilizadas por Tunnell en [Tun83] para resolver el clásico problema de los números congruentes. Fueron generalizadas para formas modulares de Hilbert en [Shi93a] y [BM07].

El problema de calcular preimágenes para el mapa de Shimura para formas modulares clásicas ha sido considerado, por ejemplo, en [Shi75] y [Gro87]. Nuestro método para calcular preimágenes en el caso de formas modulares de Hilbert se basa en las ideas presentes en [PT07], las cuales a su vez generalizan el método de Gross. Las preimágenes son obtenidas considerando ciertas series theta ternarias asociadas a ideales en álgebras de cuaterniones. Específicamente, damos un mapa Hecke lineal del espacio generado por las clases de ideales para un orden de discriminante $\mathfrak{D}$ en un álgebra de cuaterniones totalmente definida al espacio de formas modulares de Hilbert de peso paralelo $\mathbf{3/2}$ y nivel $4\mathfrak{D}$. Poder calcular estas clases de ideales, problema considerado en el Capítulo 1 de esta tesis, es por lo tanto crucial para nuestro método.

La correspondencia entre clases de ideales en álgebras de cuaterniones y formas modulares de peso medio entero tiene su contraparte automorfa, que fue estudiada en [Wal91] sobre cuerpos de números cualesquiera, y en particular en el contexto de formas modulares de Hilbert. La ventaja de nuestro método es que, siendo más explícito, permite calcular efectivamente los coeficientes de las formas modulares de Hilbert de peso medio entero, los cuales aparecen en las fórmulas de tipo Waldspurger.

Hasta donde sabemos, [Xue11] es el único resultado existente sobre cálculos con coeficientes de formas de Hilbert de peso medio entero. En este artículo el autor también sigue el método de Gross para calcular estos coeficientes con el objetivo de probar una fórmula de tipo Waldspurger, pero con varias restricciones como trabajar con formas de nivel potencia de primo y sobre un cuerpo base con número de clases impar, y sin considerar los operadores de Hecke ni la correspondencia de Shimura.

Los resultados obtenidos en este capítulo fueron enviados para su publicación, de la cual se puede encontrar una versión preliminar en [Si12].

Computing integral and half-integral weight Hilbert modular forms

Introduction

In this thesis we have worked in two different subjects related to the computation of Hilbert modular forms: the problem of computing ideal classes representatives in totally definite quaternion algebras, and the problem of computing preimages for the Shimura map on Hilbert modular forms. Though both subjects can be considered separately, and because of that we have split this work in two chapters, they are closely related: the method we give for computing preimages for the Shimura map relies heavily on the possibility of computing ideal classes representatives.

Chapter 1: Computing ideal classes representatives in quaternion algebras

The theory of quaternion algebras over number fields plays a central role in many computations related to modular forms. The idea of obtaining modular forms as theta series attached to certain lattices in quaternion algebras goes back to Hecke (see [Hec40]). Eichler and others (see [Eic73], [HS73], [Piz76b]) proved that every modular form whose level is not a square can be obtained as a linear combination of such theta series, using as lattices the ideals for a certain order in a definite quaternion algebra. Since equivalent ideals yield the same theta series, it suffices to consider ideal classes. Pizer gave in [Piz80] an algorithm for computing the Eichler order and its ideal classes, which consists in precomputing the class number of the order and then start computing ideals (in a rather random way) until the class number is reached.

Computing Hilbert modular forms has been a subject of intense research during the last years. Their knowledge is crucial for obtaining numerical evidence for certain constructions in number theory that are well known over the rational numbers but still conjectural over other number fields, such as the Eichler-Shimura theory. Ideal classes for Eichler orders in totally definite quaternion algebras over totally real fields can be used to compute Hilbert modular forms, as explained in [CS01] for Hilbert modular forms over $\mathbb{Q}[\sqrt{5}]$ and in [SW05] over other real quadratic fields, following the ideas of Pizer.

All these methods require first to find a suitable order in such an algebra, and then compute representatives for its ideal classes. The purpose of our work is to compute both things in an efficient way, and in a rather general setting. Concretely, given a totally definite algebra B over a totally field F, we give an algorithm for computing ideal classes representatives for any Bass order in B.

We consider a broad family of orders, namely the Bass orders. Besides the well known Eichler orders, this family includes the orders considered by Pizer in [Piz76a], the orders used in [PRV05] for computing modular forms of level p^2, and the orders considered in [PT07] for computing preimages for such forms under the Shimura correspondence. The rest of the Bass orders are included for completeness.

Our algorithm, in contrast with the methods *à la Pizer*, does not require any knowledge of class numbers, avoids the random computings of ideals, and avoids the repeated usage of the norm form for checking equivalences between ideals, thus making the method efficient.

Although in [DD08] the authors, using a smart cohomological trick, manage to compute Hilbert modular forms for any level using just maximal orders (which avoids computing representatives for other orders), their approach can not be used for computing preimages for the Shimura map on Hilbert modular forms of half-integral weight, subject that we consider in Chapter 2 of this thesis.

Since the full implentation (in `SAGE`) of our algorithm is still in progress, we can not make a systematic large scale comparision of running times; however, in [PRV00] there is an algorithm, which can be considered as a special case of ours, that computes ideal classes representatives for orders of discriminant p^2 in the algebra over $\mathbb{Q}$ ramified exactly at p and at infinity. This algorithm has a much better performance than MAGMA's in some simple cases. For example, when computing ideal representatives for an order of discriminant 103^2 in the algebra over $\mathbb{Q}$ ramified exactly at 103 and at infinity, with an Intel Core™2 CPU 6600 with 2 Gb of RAM memory, MAGMA (V2.16-6) needs 1254,96 seconds, whereas the routines in PARI/GP (V2.5.0) take 0,00218 seconds.

The results obtained in this chapter were sent and accepted for their publication in the journal *Mathematics of Computation*, in a joint work with my thesis advisor, Ariel Pacetti. See [PS13].

Chapter 2: Preimages for the Shimura map on Hilbert modular forms

The Shimura map is a Hecke linear map between half-integral weight modular forms and integral weight ones, introduced in [Shi73] in the classical setting and generalized in [Shi87] to Hilbert modular forms, as well as to the automorphic setting by the work of Waldspurger, Flicker and others. Computing preimages for the Shimura map became an interesting subject after the formulas given by Waldspurger *et al.* relating the central values of twists of the L-series associated to an integral weight modular form f with the coefficients of a half-integral weight form g mapping to f by the Shimura map (for example, see [BSP90]). These formulas were used by Tunnell in [Tun83] for solving the classical congruent number problem. They were generalized to the Hilbert setting in [Shi93a] and [BM07].

The problem of computing preimages for the Shimura map in the classical setting has been considered, for example, in [Shi75] and [Gro87]. Our method for computing preimages in the Hilbert setting relies in the ideas present in [PT07], which in turn generalize the method of Gross. The preimages are obtained by considering certain ternary theta series associated to ideals in quaternion algebras. Specifically, we give a Hecke linear map from the space generated by the ideal classes of an order of discriminant $\mathfrak{D}$ in a totally definite quaternion algebra to the space of Hilbert modular forms of parallel weight $\mathbf{3}/\mathbf{2}$ and level $4\mathfrak{D}$. The problem of computing these ideal classes, considered in Chapter 1 of this thesis, is thus crucial for our method.

The correspondence between ideal classes in quaternion algebras and half-integral weight modular forms has its automorphic counterpart, and was studied in [Wal91] over any number field, and in particular in the Hilbert setting. The advantage of our method is that, being more explicit, it allows to compute effectively the coefficients of the half-integral weight Hilbert modular forms, which appear in Waldspurger's type formulas.

As far as we know, [Xue11] is the unique existing result regarding computations with coefficients of half-integral weight Hilbert modular forms. In this article the author also follows the method of Gross for computing these coefficients to prove a Waldspurger's type formula, but with several restrictions such as working with level a power of a prime and odd class number of the base field, and with no focus on Hecke operators nor the Shimura correspondence.

The results obtained in this chapter were sent for their publication; there is a preprint available at [Si12].

Contents

Chapter 1

Computing ideal classes representatives in quaternion algebras

Summary

Let F be a number field and let B be a quaternion algebra over F. When computing ideal classes representatives, locally isomorphic orders in B can be regarded as equal, since two such orders have a connecting ideal, and multiplication by this ideal gives a bijection between ideal classes representatives for both orders. Hence, it is natural to group locally isomorphic orders into *genera*. Our first main result is the following theorem.

Theorem A. *There is an algorithm that, given a Bass order R in B, computes Bass suborders of R of any given genus.*

In particular, Theorem A allows us to calculate any Bass order in any quaternion algebra, since by [Voi10] we know how to obtain maximal orders in this general setting.

The second main result concerns the computation of left ideal classes representatives for Bass orders, assuming that F is totally real and B is totally definite.

Theorem B. *There is an algorithm that, given a Bass order R in B and a set of representatives S of left R-ideal classes, computes left ideal classes representatives for Bass suborders of R of any given genus. Furthermore, the set of norms of the computed ideals is the same as the set of norms of the ideals in S.*

Hence, starting from a set of representatives for a maximal order (which can be obtained following [Piz80] or [SW05] in certain particular cases, and [KV10] in the general setting), we can compute representatives for any Bass order in B.

The algorithm is such that that the constructed ideals are contained in the given ones. This avoids, in contrast with the methods *à la Pizer* (see, e.g., [Piz80], [CS01], [SW05]), the repeated usage of norm forms for checking equivalences between ideals (see [Piz80, Proposition 1.18]). The details are explained in Remark 1.3.20. We also avoid the randomness of those methods, by obtaining the classes representatives from the sets of ideals $\Psi(I)$ (see Section 1.3).

In [Lem11] it was shown that Bass orders can be described locally in terms of certain ternary quadratic forms. The strategy for proving Theorems A and B is to reduce the situation to the case of considering *maximal* Bass suborders of R. This allows to construct both the desired suborder and its ideal classes representatives in terms of local computations related to the forms in correspondence with the orders. In this special case, we also give a method to compute the ideal classes representatives by global means.

This chapter is organized as follows. In the first section we give the basic definitions that will be used throughout this chapter, some of which will be used in Chapter 2 as well. In the second section we prove Theorem A, first recalling the local description of Bass orders. The third section is devoted to prove Theorem B. In the fourth section we present an example of our algorithm: we show how to

construct representatives of ideal classes for an Eichler order of discriminant (30) in the quaternion algebra B over $\mathbb{Q}[\sqrt{5}]$ ramified exactly at the two infinite places.

Throughout this chapter, in order to make the exposition clearer, we assume that no dyadic primes occur in the discriminants of the orders considered. This case, with the extra assumption that 2 is inert in F, is treated separately in the appendix.

1.1 Basic notions and notation

We start by recalling some basic definitions and properties of quaternion algebras that will be used in this chapter. A concise exposition of the subject can be found in [Lem11], while a more detailed exposition can be found in [Vig80], [Kap69].

Let $\mathcal{O}$ be a Dedekind domain, and let F denote its fraction field. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$. By $\mathcal{O}_\mathfrak{p}$ we denote the completion of $\mathcal{O}$ at $\mathfrak{p}$, and we denote completions of other objects in a similar way. By $v_\mathfrak{p}$ we denote the $\mathfrak{p}$-adic valuation on $F_\mathfrak{p}$. The residue field $\mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p}$ is denoted by $\mathbb{F}_\mathfrak{p}$, and by $\pi_\mathfrak{p}$ we denote an element of $\mathcal{O}$ which is a local uniformizer of $\mathfrak{p}\mathcal{O}_\mathfrak{p}$.

We will be mainly interested in the case when $\mathcal{O}$ is the ring of integers of a number field, or the completion of such a ring. In the latter case the completion subindexes become redundant, but it is convenient to treat both cases simultaneously.

A *quaternion algebra* over F is a four dimensional, central and simple F-algebra with unity. Such algebra has a natural F-linear involution $x \mapsto \bar{x}$, that induces the linear form *(reduced) trace* given by $\mathrm{Tr}(x) = x + \bar{x}$ and the quadratic form *(reduced) norm* given by $N(x) = x\bar{x}$. The bilinear form corresponding to the latter is given by $(x, y) \mapsto \mathrm{Tr}(x\bar{y})$. By the Skolem-Noether theorem, every automorphism of a quaternion algebra is interior.

For every quaternion algebra B over F there exist $a, b \in F^\times$ such that

$$B \simeq \left\langle 1, i, j, k : i^2 = a,\ j^2 = b,\ ij = -ji = k \right\rangle_F$$

We denote the quaternion algebra in the right hand side by $(a, b)_F$.

Every quaternion algebra B over F is either isomorphic to the algebra of 2×2 matrices over F, or to a unique division algebra. In the first case we say that B is *unramified*, and in the second case we say that B is *ramified*.

If F is a number field, the number of places v (archimedean and non-archimedean) such that B_v is ramified is finite and even. This follows from the fact that the algebra $(a, b)_F$ is ramified at v if and only if the Hilbert symbol $(a, b)_v$ equals -1. Conversely, if S is set of places of F of finite and even order, there exists a quaternion algebra over F ramified exactly at the places of S, unique up to isomorphism.

Let B be a quaternion algebra over F. A *lattice* Λ in B is a finitely generated $\mathcal{O}$-module $\Lambda \subseteq B$ such that the natural map $\Lambda \otimes_\mathcal{O} F \to B$ is an isomorphism. Given a lattice Λ, its *dual lattice* $\Lambda^\vee$ is defined by

$$\Lambda^\vee = \{x \in B : \mathrm{Tr}(x\Lambda) \subseteq \mathcal{O}\}$$

An *order* is a lattice R which is also a subring with unity. Its *(reduced) discriminant* (also called *level*) is the ideal $d(R) \subseteq \mathcal{O}$ whose square is the ideal generated by $\{\det(\mathrm{Tr}(x_i\bar{x}_j)) : x_1, \ldots, x_4 \in R\}$.

Given a lattice Λ, the set

$$R_l(\Lambda) = \{x \in B : x\Lambda \subseteq \Lambda\}$$

is an order called *the left order of* Λ . The right order is defined and denoted in a similar way. We define the *inverse* of Λ by

$$\Lambda^{-1} = \{x \in B : \Lambda x \Lambda \subseteq \Lambda\}.$$

We say that Λ is *invertible* if $\Lambda\Lambda^{-1} = R_l(\Lambda)$ and $\Lambda^{-1}\Lambda = R_r(\Lambda)$. An order R is called a *Gorenstein* order if every lattice Λ such that $R_l(\Lambda) = R$ is invertible, and it is called a *Bass* order if every order containing it is a Gorenstein order.

Given two lattices $\Lambda \supseteq \Lambda'$ in B, the *index* of Λ' in Λ is the ideal $[\Lambda : \Lambda'] \subseteq \mathcal{O}$ generated by $\{\det(\phi) : \phi \in \mathrm{End}_F(B),\ \phi(\Lambda) \subseteq \Lambda'\}$.

Let R be an order in B. A *left R-(invertible) ideal* is an invertible lattice I such that $R_l(I) = R$; in particular, I is an R-module. Two left R-ideals I and J are called *equivalent* if there exists $x \in B^\times$ such that $I = Jx$. The set of equivalence classes is denoted by $Cl(R)$, and its size is called the *class number* of R. A left R-ideal I is called *principal* if it is equivalent to R, i.e., if there exists $x \in B^\times$ such that $I = Rx$. A lattice I is invertible if and only if $I_\mathfrak{p}$ is a principal $R_\mathfrak{p}$-module for all $\mathfrak{p}$. In particular every left $R_\mathfrak{p}$-ideal is principal, and hence $Cl(R_\mathfrak{p})$ is trivial.

Let R, R' be orders in B. By the Skolem-Noether theorem, $R_\mathfrak{p} \simeq R'_\mathfrak{p}$ if and only if there exists $x_\mathfrak{p} \in B_\mathfrak{p}^\times$ such that $x_\mathfrak{p} R_\mathfrak{p} x_\mathfrak{p}^{-1} = R'_\mathfrak{p}$. We say that R and R' are in the same *genus* if $R_\mathfrak{p} \simeq R'_\mathfrak{p}$ for all $\mathfrak{p}$. This is equivalent to the existence of an ideal I connecting R and R', i.e., such that $R_l(I) = R$ and $R_r(I) = R'$.

Notation index

- $\mathfrak{p}, \mathfrak{q}, \ldots$: prime ideals of $\mathcal{O}$.
- $\Lambda, \Lambda', \ldots$: lattices in B.
- $R, R', \ldots$: orders in B.
- $R^{\times,1} = \{x \in R : N(x) = 1\}$.
- $I, J, \ldots$: invertible lattices in B.
- $\langle a_1, \ldots, a_n \rangle$: the quadratic form $\sum_{i=1}^n a_i x_i^2$
- $\operatorname{diag}(a_1, \ldots, a_n)$: the diagonal matrix with a_i as (i, i) coefficient.

1.2 Constructing suborders

The aim of this section is to prove Theorem A. Its proof, together with a precise description of the input of the algorithm, will be given at the end of the section, once we have developed the necessary tools.

The problem can be reduced to compute *maximal* suborders of R in any given genus. The index of a maximal suborder of a given order is known, according to [Brz83, Corollary 1.11], which we recall here.

Proposition 1.2.1. *Let R be an order in B, and let R' be a maximal suborder of R. Then, there exists $\mathfrak{p}$ such that $[R : R'] = \mathfrak{p}$ or $\mathfrak{p}^2$ and $\mathfrak{p}R \subseteq R'$.*

This proposition, together with the local to global correspondence of lattices in vector spaces over F, implies that maximal suborders of a given order R can be obtained by describing the maximal suborders of $R_\mathfrak{p}$ for every $\mathfrak{p}$.

Local Bass orders

From here on we assume that $\mathfrak{p} \nmid (2)$, and we fix $\delta \in \mathcal{O}$ such that $\left(\frac{\delta}{\mathfrak{p}}\right) = -1$.

The correspondence between isomorphism classes of Gorenstein orders in quaternion algebras over local fields and ternary quadratic forms was developed in [Brz82]. This correspondence was explored further in [Lem11], where it is refined to describe Bass orders. We summarize here the results we extract from this article.

Let $R_\mathfrak{p}$ be an order, and let $\mathcal{E} = \{f_0, f_1, f_2, f_3\}$ be a basis of $R_\mathfrak{p}^\vee$ as an $\mathcal{O}_\mathfrak{p}$-module satisfying

$$\operatorname{Tr}(f_0) = 1, \quad \operatorname{Tr}(f_1) = \operatorname{Tr}(f_2) = \operatorname{Tr}(f_3) = 0. \tag{1.2.2}$$

Denote by $M_\mathcal{E}$ the Gram matrix of the norm form in the trace zero submodule of $R_\mathfrak{p}^\vee$ corresponding to $\mathcal{E}$, i.e.

$$M_\mathcal{E} = \left(\operatorname{Tr}(f_i \bar{f}_j) \right)_{1 \le i,j \le 3}.$$

To $R_\mathfrak{p}$ we associate the ternary quadratic form $d \cdot M_\mathcal{E}$, where d is any generator of $d(R_\mathfrak{p})$.

Conversely, to an integral ternary quadratic form f over $\mathcal{O}_\mathfrak{p}$ can be associated an order $C_0(f)$ in a quaternion algebra over $F_\mathfrak{p}$: the order and the algebra are given by the even part of the Clifford algebras associated to f over $\mathcal{O}_\mathfrak{p}$ and $F_\mathfrak{p}$ respectively.

By [Lem11, Propositions 5.8 and 5.10], the maps $R_\mathfrak{p} \mapsto d \cdot M_\mathcal{E}$ and $f \mapsto C_0(f)$ give a bijection between isomorphism classes of Bass orders in quaternion algebras over $F_\mathfrak{p}$ and the set of ternary quadratic forms of Table 1.1, where we group forms into *classes* that will be treated in a unified way when convenient.

Class	Form	Parameters	Hilbert Symbol
A1	$\langle 1, -1, \pi_\mathfrak{p}^s \rangle$	$s \geq 0$	1
A2	$\langle 1, -\delta, \pi_\mathfrak{p}^s \rangle$	$s \geq 1$	$(-1)^s$
B	$\langle 1, \pi_\mathfrak{p}, \epsilon_1 \pi_\mathfrak{p} \rangle$	$\epsilon_1 \in \{1, \delta\}$	$\left(\frac{-\epsilon_1}{\mathfrak{p}}\right)$
C	$\langle 1, \epsilon_1 \pi_\mathfrak{p}, \epsilon_2 \pi_\mathfrak{p}^s \rangle$	$\epsilon_1, \epsilon_2 \in \{1, \delta\}$, $s \geq 2$	$\left(\frac{\epsilon_1}{\mathfrak{p}}\right)^s \left(\frac{-\epsilon_2}{\mathfrak{p}}\right)$

Table 1.1: Ternary quadratic forms in correspondence with local Bass orders.

In particular, every Bass order R induces a family $(f_\mathfrak{p})_\mathfrak{p}$ of ternary quadratic forms, letting $f_\mathfrak{p}$ be the form in Table 1.1 corresponding to $R_\mathfrak{p}$. This family satisfies that $f_\mathfrak{p} = \langle 1, -1, 1 \rangle$ for almost every $\mathfrak{p}$, and is independent of the genus of R.

Equation (1.2.4) below implies that, given a form $f = \langle 1, a, b \rangle$, then the quaternion algebra $C_0(f) \otimes_{\mathcal{O}_\mathfrak{p}} F_\mathfrak{p}$ is a matrix algebra if and only if $\langle a, b, ab \rangle$ is isotropic, i.e., if and only if the Hilbert symbol $(\frac{-a,-b}{\mathfrak{p}})$ equals 1. The sign for each case is shown in Table 1.1.

The graphs in Figure 1.1 show how the isomorphism classes of Bass orders in quaternion algebras over $F_\mathfrak{p}$ are distributed. Each vertex represents an isomorphism class of Bass orders, and there is an edge between two vertices if and only if there is an order $R_\mathfrak{p}$ corresponding to the top vertex, and an order $R'_\mathfrak{p}$ corresponding to the bottom vertex, such that $R'_\mathfrak{p}$ is a maximal suborder of $R_\mathfrak{p}$; if f and g are the corresponding forms from Table 1.1, we will say that g is *beneath* f. Note that these graphs reflect the assertion of Proposition 1.2.1.

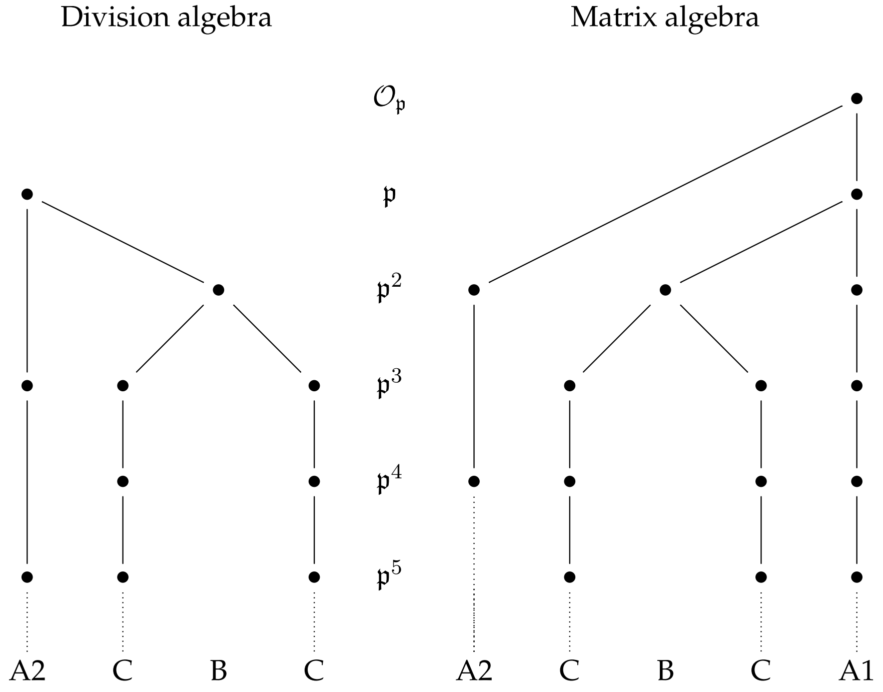

Figure 1.1: Graph of isomorphism classes of local Bass orders, ordered by inclusion.

All the orders in the left graph lie in the division quaternion algebra, while all the orders in the right graph lie in the matrix algebra. Horizontally aligned vertices have the same discriminant, which is indicated in the middle column. Vertically aligned vertices correspond to forms of the same *class*, which is indicated in the bottom row. The orders of class A1 are the so called *local Eichler orders* (see, e.g., [Brz83, Section 2]), and the orders of class A2 in the division algebra are the *orders of level* p^{2r+1} considered in [Piz76a] (see also [Brz83, Section 3]). Also in the division algebra, the orders of class B are the *orders of level* p^2 considered in [PRV05], and the vertices of class C and discriminant p^3 are represented by the orders $\mathcal{O}^+, \mathcal{O}^-$ considered in [PT07].

An order R in a quaternion algebra B is called an *Eichler* order if it is the intersection of two maximal orders. This is equivalent to $R_\mathfrak{p}$ being of class A1 for every unramified prime $\mathfrak{p}$, and $R_\mathfrak{p}$ being a maximal order for every ramified prime $\mathfrak{p}$. If we write $d(R) = \mathfrak{m}\mathfrak{n}$ with the primes dividing $\mathfrak{m}$ being exactly those ramified in B, the ideal $\mathfrak{n}$ is called the *level* of R.

Definition. *Let $R_\mathfrak{p}$ be a Bass order in correspondence with the form $f = \langle 1, a, b\rangle$, and let $\mathcal{B} = \{1, e_1, e_2, e_3\}$ be a basis of $R_\mathfrak{p}$ as an $\mathcal{O}_\mathfrak{p}$-module. We say that $\mathcal{B}$ is a* good basis *if the e_i satisfy*

$$\begin{aligned} &e_1^2 = -ab, && e_2^2 = -b, && e_3^2 = -a, \\ &e_1e_2 = -be_3, && e_2e_3 = -e_1, && e_3e_1 = -ae_2, \\ &e_2e_1 = be_3, && e_3e_2 = e_1, && e_1e_3 = ae_2. \end{aligned} \tag{1.2.3}$$

Every Bass order has a good basis (see [Lem11, Section 4], and also [GL09]), and in such basis the norm form is given by

$$N = \langle 1, ab, b, a\rangle. \tag{1.2.4}$$

Example. For $s \geq 0$, let

$$E_s = \left\{ \begin{pmatrix} a & b \\ \pi_\mathfrak{p}^s c & d \end{pmatrix} : a, b, c, d \in \mathcal{O}_\mathfrak{p} \right\}.$$

Then, the order $E_s \subseteq M_2(F_\mathfrak{p})$ is a Bass order of class A1 and discriminant $\mathfrak{p}^s$. Furthermore,

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad e_1 = \begin{pmatrix} 0 & 1 \\ \pi_\mathfrak{p}^s & 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 & 1 \\ -\pi_\mathfrak{p}^s & 0 \end{pmatrix}, \quad e_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

is a good basis for E_s. In fact, it is straightforward to see that these elements satisfy the equations (1.2.3) corresponding to $f = \langle 1, -1, \pi_\mathfrak{p}^s\rangle$.

Note that E_{s+1} is a maximal suborder of E_s.

Example. Let $K_\mathfrak{p} = F_\mathfrak{p}(\sqrt{\delta})$ be the unique unramified quadratic extension of $F_\mathfrak{p}$. For $\alpha \in K_\mathfrak{p}$, denote by $\overline{\alpha}$ its conjugated in $K_\mathfrak{p}$. Then $D_\mathfrak{p} = \left\{ \left(\begin{smallmatrix} \alpha & \beta \\ \pi_\mathfrak{p}\overline{\beta} & \overline{\alpha} \end{smallmatrix}\right) : \alpha, \beta \in K_\mathfrak{p} \right\}$ is the (unique) division quaternion algebra over $F_\mathfrak{p}$.

Let $\mathcal{O}_{K_\mathfrak{p}} = \mathcal{O}_\mathfrak{p} + \sqrt{\delta}\mathcal{O}_\mathfrak{p}$ be the ring of integers of $K_\mathfrak{p}$. For $r \geq 0$, let

$$P_{2r+1} = \left\{ \begin{pmatrix} \alpha & \pi_\mathfrak{p}^r \beta \\ \pi_\mathfrak{p}^{r+1}\overline{\beta} & \overline{\alpha} \end{pmatrix} : \alpha, \beta \in \mathcal{O}_{K_\mathfrak{p}} \right\}.$$

Then, the order $P_{2r+1} \subseteq D_\mathfrak{p}$ is a Bass order of class A2 and discriminant $\mathfrak{p}^{2r+1}$. Furthermore,

- If there exists $\mu \in \mathcal{O}_\mathfrak{p}$ such that $\mu^2 = -1$, then

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad e_1 = \begin{pmatrix} 0 & -\mu\sqrt{\delta}\pi_\mathfrak{p}^r \\ \mu\sqrt{\delta}\pi_\mathfrak{p}^{r+1} & 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 & \mu\pi_\mathfrak{p}^r \\ \mu\pi_\mathfrak{p}^{r+1} & 0 \end{pmatrix}, \quad e_3 = \begin{pmatrix} -\sqrt{\delta} & 0 \\ 0 & \sqrt{\delta} \end{pmatrix}$$

  is a good basis for P_{2r+1}.

- If such μ does not exist, we may assume that $\delta = -1$. Using Hensel's lemma, take $\beta_0, \beta_1 \in \mathcal{O}_\mathfrak{p}$ such that $\beta_0^2 + \beta_1^2 = -1$. Let $\beta = \beta_0 + \beta_1\sqrt{\delta}$. Then,

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad e_1 = \begin{pmatrix} 0 & -\beta\sqrt{\delta}\pi_\mathfrak{p}^r \\ \overline{\beta}\sqrt{\delta}\pi_\mathfrak{p}^{r+1} & 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 & \beta\pi_\mathfrak{p}^r \\ \overline{\beta}\pi_\mathfrak{p}^{r+1} & 0 \end{pmatrix}, \quad e_3 = \begin{pmatrix} -\sqrt{\delta} & 0 \\ 0 & \sqrt{\delta} \end{pmatrix}$$

  is a good basis for P_{2r+1}.

In fact, it is straightforward to see in each case that these elements satisfy the equations (1.2.3) corresponding to $f = \langle 1, -\delta, \pi_\mathfrak{p}^s \rangle$.

Note that P_{2r+3} is a maximal suborder of P_{2r+1}.

Let $R_\mathfrak{p}$ be an order in correspondence with the form $f = \langle 1, a, b \rangle$, and let $\mathcal{E} = \{f_0, f_1, f_2, f_3\}$ be a basis of $R_\mathfrak{p}^\vee$ satisfying (1.2.2). Let $e_i = 4ab \cdot f_j \bar{f}_k$, where (i, j, k) is an even permutation of $(1, 2, 3)$, and denote $\mathcal{E}^\dagger = \{1, e_1, e_2, e_3\}$. Then $\mathcal{E}^\dagger$ is a basis of $R_\mathfrak{p}$ (see [Lem11, Section 4]).

Proposition 1.2.5. *With the notation as above, if $\mathcal{E}$ is such that*

$$2ab \cdot M_\mathcal{E} = \mathrm{diag}(1, a, b), \tag{1.2.6}$$

then $\mathcal{E}^\dagger$ is a good basis of $R_\mathfrak{p}$

For a proof see [Lem11, Section 4].

Remark 1.2.7. Conversely, if $\mathcal{B}$ is a good basis of $R_\mathfrak{p}$, then $M_{\mathcal{B}^\vee}$ satisfies (1.2.6), where given a basis $\mathcal{B} = \{e_0, e_1, e_2, e_3\}$ of $R_\mathfrak{p}$, we denote by $\mathcal{B}^\vee = \{f_0, f_1, f_2, f_3\}$ the basis of $R_\mathfrak{p}^\vee$ characterized by the equations $\mathrm{Tr}(e_i \bar{f}_j) = \delta_{ij}$.

Constructing maximal suborders, the local case.

Given an order $R_\mathfrak{p}$ corresponding to a form f from Table 1.1, we construct a representative for each of the one or two isomorphism classes of maximal suborders of $R_\mathfrak{p}$ (see Figure 1.1). To do this, given a good basis $\{1, e_1, e_2, e_3\}$ of $R_\mathfrak{p}$ and a form g from Table 1.1 beneath f, we give elements $d_1, d_2, d_3 \in R_\mathfrak{p}$ satisfying the equations (1.2.3) corresponding to the form g. Then, the order $R'_\mathfrak{p} = \langle 1, d_1, d_2, d_3 \rangle_{\mathcal{O}_\mathfrak{p}}$ is a maximal suborder of $R_\mathfrak{p}$ in correspondence with the form g, for which $\{1, d_1, d_2, d_3\}$ is a good basis.

Using Hensel's Lemma, take $\alpha_0, \alpha_1, \beta_0, \beta_1, \mu, \nu \in \mathcal{O}_\mathfrak{p}$ satisfying:

- $\alpha_0^2 - \alpha_1^2 = \pi_\mathfrak{p}$.
- $\beta_0^2 + \beta_1^2 = \delta$.
- $\mu^2 = -1$, when $\left(\frac{-1}{\mathfrak{p}}\right) = 1$.
- $\nu^2 = -\delta$, when $\left(\frac{-1}{\mathfrak{p}}\right) = -1$.

Proposition 1.2.8. *The elements d_1, d_2, d_3 defined by Table 1.2 satisfy the equations* (1.2.3) *corresponding to the form g.*

Proof. In each case, it is easy to check that the d_i's satisfy the equations (1.2.3) corresponding to g, using that the e_i's satisfy the equations corresponding to f. □

Though it is not needed in our algorithms, we now show that this construction is general, in the sense that every maximal suborder of $R_\mathfrak{p}$ can be obtained by the previous procedure, if we start with a suitable good basis of $R_\mathfrak{p}$.

Lemma 1.2.9. *Let $R'_\mathfrak{p}$ be a non-maximal Bass order. The number of Bass orders which are minimal with respect to the property of containing $R'_\mathfrak{p}$ properly is two if $R'_\mathfrak{p}$ is of class A1, and one otherwise.*

Proof. This is [Brz83, Propositions 1.12 and 2.3]. □

Lemma 1.2.10. *Let $R'_\mathfrak{p}$ and $R''_\mathfrak{p}$ be isomorphic maximal suborders of $R_\mathfrak{p}$. Then, there exists $x \in B_\mathfrak{p}^\times$ normalizing $R_\mathfrak{p}$ such that $xR'_\mathfrak{p}x^{-1} = R''_\mathfrak{p}$.*

Form	Form beneath	Good basis for R'_{p}
$\langle 1,-1,\pi_{\mathrm{p}}^{s}\rangle$	$\langle 1,-1,\pi_{\mathrm{p}}^{s+1}\rangle$	$d_1=\alpha_0e_1+\alpha_1e_2$, $d_2=\alpha_1e_1+\alpha_0e_2, d_3=e_3$
$\langle 1,-1,1\rangle$	$\langle 1,-\delta,\pi_{\mathrm{p}}^{2}\rangle$	$d_1=\pi_{\mathrm{p}}(\beta_1e_1-\beta_0e_3)$, $d_2=\pi_{\mathrm{p}}e_2, d_3=\beta_0e_1+\beta_1e_3$
$\langle 1,-1,\pi_{\mathrm{p}}\rangle$	$\langle 1,\pi_{\mathrm{p}},\pi_{\mathrm{p}}\rangle$, if $\left(\frac{-1}{\mathrm{p}}\right)=1$	$d_1=\mu\pi_{\mathrm{p}}e_3, d_2=\mu e_1, d_3=e_2$
	$\langle 1,\pi_{\mathrm{p}},\delta\pi_{\mathrm{p}}\rangle$, if $\left(\frac{-1}{\mathrm{p}}\right)=-1$	$d_1=\nu\pi_{\mathrm{p}}e_3, d_2=\nu e_1, d_3=e_2$
$\langle 1,-\delta,\pi_{\mathrm{p}}^{s}\rangle$	$\langle 1,-\delta,\pi_{\mathrm{p}}^{s+2}\rangle$	$d_1=\pi_{\mathrm{p}}e_1, d_2=\pi_{\mathrm{p}}e_2, d_3=e_3$
$\langle 1,-\delta,\pi_{\mathrm{p}}\rangle$	$\langle 1,\pi_{\mathrm{p}},\delta\pi_{\mathrm{p}}\rangle$, if $\left(\frac{-1}{\mathrm{p}}\right)=1$	$d_1=\mu\pi_{\mathrm{p}}e_3, d_2=\mu e_1, d_3=e_2$
	$\langle 1,\pi_{\mathrm{p}},\pi_{\mathrm{p}}\rangle$, if $\left(\frac{-1}{\mathrm{p}}\right)=-1$	$d_1=\nu^{-1}\pi_{\mathrm{p}}e_3, d_2=\nu^{-1}e_1$, $d_3=e_2$
$\langle 1,\pi_{\mathrm{p}},\pi_{\mathrm{p}}\rangle$	$\langle 1,\pi_{\mathrm{p}},\pi_{\mathrm{p}}^{2}\rangle$	$d_1=\pi_{\mathrm{p}}e_2, d_2=e_1, d_3=e_3$
	$\langle 1,\delta\pi_{\mathrm{p}},\pi_{\mathrm{p}}^{2}\rangle$	$d_1=\pi_{\mathrm{p}}(-\beta_1e_2+\beta_0e_3)$, $d_2=e_1, d_3=\beta_0e_2+\beta_1e_3$
$\langle 1,\pi_{\mathrm{p}},\delta\pi_{\mathrm{p}}\rangle$	$\langle 1,\pi_{\mathrm{p}},\delta\pi_{\mathrm{p}}^{2}\rangle$	$d_1=\pi_{\mathrm{p}}e_2, d_2=e_1, d_3=e_3$
	$\langle 1,\delta\pi_{\mathrm{p}},\delta\pi_{\mathrm{p}}^{2}\rangle$	$d_1=\pi_{\mathrm{p}}e_3, d_2=e_1, d_3=e_2$
$\langle 1,\pi_{\mathrm{p}},\pi_{\mathrm{p}}^{s}\rangle$	$\langle 1,\pi_{\mathrm{p}},\pi_{\mathrm{p}}^{s+1}\rangle$	$d_1=\pi_{\mathrm{p}}e_2, d_2=e_1, d_3=e_3$
$\langle 1,\delta\pi_{\mathrm{p}},\pi_{\mathrm{p}}^{s}\rangle$	$\langle 1,\delta\pi_{\mathrm{p}},\delta\pi_{\mathrm{p}}^{s+1}\rangle$	$d_1=\delta\pi_{\mathrm{p}}e_2, d_2=e_1, d_3=e_3$
$\langle 1,\pi_{\mathrm{p}},\delta\pi_{\mathrm{p}}^{s}\rangle$	$\langle 1,\pi_{\mathrm{p}},\delta\pi_{\mathrm{p}}^{s+1}\rangle$	$d_1=\pi_{\mathrm{p}}e_2, d_2=e_1, d_3=e_3$.
$\langle 1,\delta\pi_{\mathrm{p}},\delta\pi_{\mathrm{p}}^{s}\rangle$	$\langle 1,\delta\pi_{\mathrm{p}},\pi_{\mathrm{p}}^{s+1}\rangle$	$d_1=\delta\pi_{\mathrm{p}}e_2, d_2=\delta^{-1}e_1$, $d_3=e_3$

Table 1.2: Construction of maximal suborders, in terms of good bases and ternary quadratic forms.

Proof. Since R'_{p} and R''_{p} are isomorphic, there exists $x\in B_{\mathrm{p}}^{\times}$ such that $xR'_{\mathrm{p}}x^{-1}=R''_{\mathrm{p}}$. If $xR_{\mathrm{p}}x^{-1}=R_{\mathrm{p}}$, we are done, and the previous lemma says that this is necessarily the case when R''_{p} is not of class A1, since we have the inclusions $R''_{\mathrm{p}}\subseteq xR_{\mathrm{p}}x^{-1}$ and $R''_{\mathrm{p}}\subseteq R_{\mathrm{p}}$.

Then, we can assume that $xR_{\mathrm{p}}x^{-1}\neq R_{\mathrm{p}}$ and that R''_{p} is of class A1 Hence R'_{p} and R_{p} are also of class A1 (see Figure 1.1). We can then assume, without loss of generality, that $R_{\mathrm{p}}=E_s$ and $R'_{\mathrm{p}}=E_{s+1}$. Consider the matrix $y=\left(\begin{smallmatrix}\pi_{\mathrm{p}}^{-1}&0\\0&1\end{smallmatrix}\right)$, and let $\tilde{R}_{\mathrm{p}}=yR_{\mathrm{p}}y^{-1}$. Then,

$$\tilde{R}_{\mathrm{p}}=\left\{\begin{pmatrix}a&\pi_{\mathrm{p}}^{-1}b\\\pi_{\mathrm{p}}^{s+1}c&d\end{pmatrix}:a,b,c,d\in\mathcal{O}_{\mathrm{p}}\right\}.$$

Since $R'_{\mathrm{p}}\subseteq\tilde{R}_{\mathrm{p}}$, we have that $R''_{\mathrm{p}}\subseteq x\tilde{R}_{\mathrm{p}}x^{-1}$. Since we already had that $R''_{\mathrm{p}}\subseteq R_{\mathrm{p}}$ and $R''_{\mathrm{p}}\subseteq xR_{\mathrm{p}}x^{-1}$, the previous lemma implies that $x\tilde{R}_{\mathrm{p}}x^{-1}=R_{\mathrm{p}}$. In particular, xy normalizes R_{p}. Then, since $R''_{\mathrm{p}}=(xy)(y^{-1}R'_{\mathrm{p}}y)(xy)^{-1}$, we can assume that

$$R''_{\mathrm{p}}=y^{-1}R'_{\mathrm{p}}y=\left\{\begin{pmatrix}a&\pi_{\mathrm{p}}b\\\pi_{\mathrm{p}}^{s}c&d\end{pmatrix}:a,b,c,d\in\mathcal{O}_{\mathrm{p}}\right\}.$$

In this case, taking $\tilde{x}=\left(\begin{smallmatrix}0&1\\\pi_{\mathrm{p}}^{-s}&0\end{smallmatrix}\right)$ we get that $\tilde{x}$ normalizes R_{p} and conjugates R'_{p} onto R''_{p}, which completes the proof. □

Proposition 1.2.11. *Let R_{p} be an order in correspondence with the form f, and R'_{p} be a maximal suborder of R_{p} in correspondence with the form g. Then, there exists a good basis $\{1,e_1,e_2,e_3\}$ of R_{p} such that the elements d_1,d_2,d_3 given by Table 1.2 in terms of f and g define a good basis for R'_{p}.*

Proof. Let $1,\tilde{e}_1,\tilde{e}_2,\tilde{e}_3$ be any good basis of R_{p}. In terms of f,g and the $\tilde{e}_i$, consider the elements $\tilde{d}_i$ defined by Table 1.2. Let R''_{p} be the suborder of R_{p} given by

$$R''_{\mathrm{p}}=\left\langle 1,\tilde{d}_1,\tilde{d}_2,\tilde{d}_3\right\rangle_{\mathcal{O}_{\mathrm{p}}}.$$

Since R'_{p} and R'''_{p} are isomorphic, by the previous lemma there exists x normalizing R_{p} such that $xR'_{\mathrm{p}}x^{-1}=R''_{\mathrm{p}}$. Then, letting $e_i=x\tilde{e}_ix^{-1}$ our goal is achieved. □

Quasi-good bases

So far, given an order $R_\mathfrak{p}$, we must obtain a good basis of it to compute its suborders. This involves diagonalizing a ternary quadratic form over $\mathcal{O}_\mathfrak{p}$, which is not desirable from the computational point of view. Nevertheless, as we will show in this subsection by introducing the notion of quasi-good bases, this can be reduced to diagonalize the corresponding form modulo $\mathfrak{p}^n$ for a certain small non-negative integer n.

Definition. *Let $\mathcal{B} = \{1, e_1, e_2, e_3\}$ be a basis of $R_\mathfrak{p}$. We say that $\mathcal{B}$ is a* quasi-good *basis if there exists a good basis $\tilde{\mathcal{B}} = \{1, \tilde{e}_1, \tilde{e}_2, \tilde{e}_3\}$ of $R_\mathfrak{p}$ satisfying*

$$\tilde{e}_i \equiv e_i \mod (\mathfrak{p}R_\mathfrak{p}) \quad (1 \leq i \leq 3).$$

Proposition 1.2.12. *Let $\mathcal{B} = \{1, e_1, e_2, e_3\}$ be a quasi-good basis of an order $R_\mathfrak{p}$ in correspondence with a form f, and let g be a form beneath f. Let d_1, d_2, d_3 be as in Table 1.2. Then,*

$$R'_\mathfrak{p} = \langle 1, d_1, d_2, d_3 \rangle_{\mathcal{O}_\mathfrak{p}}$$

is a maximal suborder of $R_\mathfrak{p}$ in correspondence with the form g.

Proof. Let $\tilde{\mathcal{B}} = \{1, \tilde{e}_1, \tilde{e}_2, \tilde{e}_3\}$ be a good basis of $R_\mathfrak{p}$ as in the definition above. In terms of these elements and the form g, define elements $\tilde{d}_1, \tilde{d}_2, \tilde{d}_3$ according to Table 1.2, and let $\Lambda_\mathfrak{p} = \left\langle 1, \tilde{d}_1, \tilde{d}_2, \tilde{d}_3 \right\rangle_{\mathcal{O}_\mathfrak{p}}$. The table shows that $\tilde{d}_i \equiv d_i \mod (\mathfrak{p}R_\mathfrak{p})$ for every $1 \leq i \leq 3$. Since $\mathfrak{p}R_\mathfrak{p} \subseteq \Lambda_\mathfrak{p}$, we have that

$$\Lambda_\mathfrak{p} = \left\langle 1, \tilde{d}_1, \tilde{d}_2, \tilde{d}_3 \right\rangle_{\mathcal{O}_\mathfrak{p}} + \mathfrak{p}R_\mathfrak{p} \supseteq R'_\mathfrak{p}.$$

Then, it suffices to see that $d(R'_\mathfrak{p}) = d(\Lambda_\mathfrak{p})$ to complete the proof.

Let $e \in \{1, 2\}$ be such that $[R_\mathfrak{p} : \Lambda_\mathfrak{p}] = \mathfrak{p}^e$. Following Table 1.2 case by case, it can be proved that $d(R'_\mathfrak{p}) = \mathfrak{p}^e d(R_\mathfrak{p})$. Since $d(\Lambda_\mathfrak{p}) = \mathfrak{p}^e d(R_\mathfrak{p})$, we are done.

□

Remark 1.2.13. Let $m = v_\mathfrak{p}(d(R'_\mathfrak{p}))$. The proof shows that, when constructing the d_i's, the elements $\alpha_0, \alpha_1, \ldots$ in Table 1.2 need to be calculated only up to precision $\pi_\mathfrak{p}^{m+1}$, since in that case the ideal $d(\Lambda_\mathfrak{p})$ remains unchanged.

It shows also that $\{1, d_1, d_2, d_3\}$ needs not to be a quasi-good basis for $R'_\mathfrak{p}$, since we only get that $\tilde{d}_i \equiv d_i \mod (\mathfrak{p}R_\mathfrak{p})$. Nevertheless, since $\mathfrak{p}^2 R_\mathfrak{p} \subseteq \mathfrak{p}R'_\mathfrak{p}$, it is a quasi-good basis if the stronger congruence $\tilde{e}_i \equiv e_i \mod (\mathfrak{p}^2 R_\mathfrak{p})$ holds.

Proposition 1.2.12 shows that obtaining quasi-good bases is enough for our purpose of computing suborders. In what follows we show how to obtain these bases.

Let $f = \langle 1, a, b \rangle$ be the form in correspondence with the order $R_\mathfrak{p}$, and let $\mathcal{E} = \{f_0, f_1, f_2, f_3\}$ be a basis of $R_\mathfrak{p}^\vee$ satisfying (1.2.2). The existence of good bases implies that there exists $C \in GL_3(\mathcal{O}_\mathfrak{p})$ such that $2ab \cdot C^t M_\mathcal{E} C = \operatorname{diag}(1, a, b)$. Hence, $2ab \cdot M_\mathcal{E} \in M_3(\mathcal{O}_\mathfrak{p})$ and $\det(M_\mathcal{E}) = 8^{-1}(ab)^{-2}u^2$ for some $u \in \mathcal{O}_\mathfrak{p}^\times$.

Proposition 1.2.14. *Let $n = 2v_\mathfrak{p}(a) + 1$. Assume that $\mathcal{E}$ satisfies the following conditions.*

(1) There exists $\tilde{b} \in \mathcal{O}_\mathfrak{p}$ such that

$$2ab \cdot M_\mathcal{E} \equiv \operatorname{diag}(1, a, \tilde{b}) \mod (M_3(\mathfrak{p}^n \mathcal{O}_\mathfrak{p})).$$

(2) $\det(M_\mathcal{E}) = 8^{-1}(ab)^{-2}$.

Then, $\mathcal{E}^\dagger$ is a quasi-good basis of $R_\mathfrak{p}$.

Remark 1.2.15. The congruence in (1) is the really relevant hypothesis. If this congruence is satisfied and $u \in \mathcal{O}_\mathfrak{p}^\times$ is such that $\det(M_\mathcal{E}) = 8^{-1}(ab)^{-2}u^2$, then the basis $\{f_0, f_1, f_2, u^{-1}f_3\}$ satisfies (1) and also (2).

The proof of Proposition 1.2.14 is based on the following lifting lemma.

Lemma 1.2.16. *Let r, m be non negative integers such that $m > 2r$, and let $A \in M_3(\mathcal{O}_\mathfrak{p})$ be a symmetric matrix. Suppose that there exists $C \in GL_3(\mathcal{O}_\mathfrak{p})$ such that*

$$C^t AC \equiv \operatorname{diag}(\alpha, \beta, \gamma) \mod (M_3(\mathfrak{p}^m \mathcal{O}_\mathfrak{p})),$$

with $v_\mathfrak{p}(\alpha) = 0$ and $v_\mathfrak{p}(\beta) = r$. Then, there exists $C' \in GL_3(\mathcal{O}_\mathfrak{p})$ satisfying $C' \equiv C \mod (M_3(\mathfrak{p}^{m-r}\mathcal{O}_\mathfrak{p}))$ such that

$$C'^t AC' \equiv \operatorname{diag}(\alpha', \beta', \gamma') \mod (M_3(\mathfrak{p}^{m+1}\mathcal{O}_\mathfrak{p})),$$

with $\alpha' \equiv \alpha \mod (\mathfrak{p}^{m-r}\mathcal{O}_\mathfrak{p})$ and $\beta' \equiv \beta \mod (\mathfrak{p}^m \mathcal{O}_\mathfrak{p})$.

Proof. Write

$$C^t AC = \operatorname{diag}(\alpha, \beta, \gamma) + \pi_\mathfrak{p}^m \begin{pmatrix} a & b & c \\ b & d & e \\ c & e & f \end{pmatrix},$$

with $a, b, \dots, f \in \mathcal{O}_\mathfrak{p}$. We claim that there exists a matrix $C_0 \in GL_3(\mathcal{O}_\mathfrak{p})$ such that

$$C_0^t AC = \begin{pmatrix} \alpha + a\pi_\mathfrak{p}^m & 0 & c'\pi_\mathfrak{p}^m \\ -b\pi_\mathfrak{p}^r & \beta + d'\pi_\mathfrak{p}^m & e'\pi_\mathfrak{p}^m \\ -c\pi_\mathfrak{p}^r & -e\pi_\mathfrak{p}^r & \gamma + f'\pi_\mathfrak{p}^m \end{pmatrix},$$

with $c', d', e', f' \in \mathcal{O}_\mathfrak{p}$. This can be shown by performing row operations on $C^t AC$, using the diagonal entries as pivots to first obtain zeroes at the $(3, 1), (2, 1), (1, 2)$ and $(3, 2)$ entries, and then obtain $-c\pi_\mathfrak{p}^r, -e\pi_\mathfrak{p}^r$ and $-b\pi_\mathfrak{p}^r$ at the $(3, 1), (3, 2)$ and $(2, 1)$ entries respectively.

Let $C' = C + \pi_\mathfrak{p}^{m-r} C_0$. Then,

$$C'^t AC' = \begin{pmatrix} \alpha' & 0 & c'\pi_\mathfrak{p}^{2m-r} \\ 0 & \beta' & e'\pi_\mathfrak{p}^{2m-r} \\ c'\pi_\mathfrak{p}^{2m-r} & e'\pi_\mathfrak{p}^{2m-r} & \gamma' \end{pmatrix} + \pi_\mathfrak{p}^{2(m-r)} C_0^t AC_0.$$

where $\alpha' = \alpha + a\pi_\mathfrak{p}^m + 2\pi_\mathfrak{p}^{m-r}(\alpha + a\pi_\mathfrak{p}^m)$ and $\beta' = \beta + d'\pi_\mathfrak{p}^m + 2\pi_\mathfrak{p}^{m-r}(\beta + d'\pi_\mathfrak{p}^m)$. Since $2(m - r) \geq m + 1$, we are done. □

Proof of Proposition 1.2.14. Let $r = v_\mathfrak{p}(a)$. By letting $m \to \infty$ in the previous lemma, we get a matrix $C = (c_{ij}) \in GL_3(\mathcal{O}_\mathfrak{p})$ satisfying $C \equiv I \mod (M_3(\mathfrak{p}^{r+1}\mathcal{O}_\mathfrak{p}))$ such that

$$2ab \cdot C^t M_\mathcal{E} C = \operatorname{diag}(\alpha, \beta, \gamma),$$

with $\alpha \equiv 1 \mod (\pi_\mathfrak{p}^{r+1})$ and $\beta \equiv a \mod (\pi_\mathfrak{p}^{2r+1})$. Using Hensel's lemma, take $x_1, x_2 \in \mathcal{O}_\mathfrak{p}^\times$ satisfying $x_i \equiv 1 \mod (\pi_\mathfrak{p}^{r+1})$ such that $\alpha = x_1^2$ and $\beta = x_2^2 a$. Taking determinants we see that $\gamma = x_3^2 b$, where $x_3 = \frac{\det(C)}{x_1 x_2}$.

Now let $\tilde{C} = C \cdot \operatorname{diag}(x_1, x_2, x_3)^{-1}$. Then $\tilde{C}$ satisfies that

$$2ab \cdot \tilde{C}^t M_\mathcal{E} \tilde{C} = \operatorname{diag}(1, a, b).$$

Let $\tilde{f}_i = \sum_{j=1}^3 \tilde{c}_{ji} f_j$, where $\tilde{C} = (\tilde{c}_{ij})$, let $\tilde{f}_0 = f_0$, and let $\tilde{\mathcal{E}} = \{\tilde{f}_0, \tilde{f}_1, \tilde{f}_2, \tilde{f}_3\}$. Then $\tilde{\mathcal{E}}^\dagger$ is a good basis of $R_\mathfrak{p}$, for (1.2.6) is verified by $M_{\tilde{\mathcal{E}}}$. The congruences satisfied by the x_i's and C imply that $\tilde{f}_i \equiv f_i \mod (\mathfrak{p}R_\mathfrak{p}^\vee)$ for $1 \leq i \leq 3$. Hence $\mathcal{E}^\dagger$ is a quasi-good basis of $R_\mathfrak{p}$, since [Brz82, Proposition 3.2] gives that $4ab \cdot R_\mathfrak{p}^\vee R_\mathfrak{p}^\vee \subseteq R_\mathfrak{p}$.

□

From local to global

Let Λ be a lattice in B, and let $\Lambda'_\mathfrak{p} \subseteq \Lambda_\mathfrak{p}$ be a sublattice of index $\mathfrak{p}^e$, where e is a non-negative integer. Let $\Lambda' \subseteq B$ be the lattice given by

$$\Lambda'_\mathfrak{q} = \begin{cases} \Lambda_\mathfrak{q} & \text{if } \mathfrak{q} \neq \mathfrak{p}, \\ \Lambda'_\mathfrak{p} & \text{if } \mathfrak{q} = \mathfrak{p}. \end{cases}$$

Given a set of generators for Λ as an $\mathcal{O}$-module and a set of generators for $\Lambda'_\mathfrak{p}$ as an $\mathcal{O}_\mathfrak{p}$-module, how can we construct a set of generators for Λ' as an $\mathcal{O}$-module?

Assume that $\Lambda = \langle v_1, v_2, \dots, v_m \rangle_\mathcal{O}$ and that $\Lambda'_\mathfrak{p} = \langle w_1, w_2, \dots, w_n \rangle_{\mathcal{O}_\mathfrak{p}}$. For each i write $w_i = \sum_j a_{ij} v_j$, with $a_{ij} \in \mathcal{O}_\mathfrak{p}$. There exist elements $b_{ij} \in \mathcal{O}$ and $c_{ij} \in \pi_\mathfrak{p}^e \mathcal{O}_\mathfrak{p}$ such that $a_{ij} = b_{ij} + c_{ij}$ (they can be constructed, for example, by looking at the $\mathfrak{p}$-adic expansion of the a_{ij}). Let $\tilde{w}_i = \sum_j b_{ij} v_j$.

Proposition 1.2.17. *With the notation as above,*

$$\Lambda' = \mathfrak{p}^e \Lambda + \langle \tilde{w}_1, \tilde{w}_2, \dots, \tilde{w}_n \rangle_\mathcal{O}.$$

Proof. It is enough to check that these two lattices coincide at all completions. Denote by Λ'' the lattice in the right hand side.

- If $\mathfrak{q} \neq \mathfrak{p}$, then $\pi_\mathfrak{p}$ is a unit in $\mathcal{O}_\mathfrak{q}$. So $\mathfrak{p}^e \Lambda_\mathfrak{q} = \Lambda_\mathfrak{q}$, which implies that $\Lambda''_\mathfrak{q} = \Lambda_\mathfrak{q} + \langle \tilde{w}_1, \tilde{w}_2, \dots, \tilde{w}_n \rangle_{\mathcal{O}_\mathfrak{q}} = \Lambda_\mathfrak{q}$.
- Since $\mathfrak{p}^e \Lambda_\mathfrak{p} \subseteq \Lambda'_\mathfrak{p}$, we have that $\Lambda''_\mathfrak{p} \subseteq \Lambda_\mathfrak{p}$; the reverse inclusion is deduced from the fact that $\tilde{w}_i \equiv w_i \mod (\mathfrak{p}^e \Lambda_\mathfrak{p})$.

□

Remark 1.2.18. Using the Hermite Normal Form algorithm (see [Coh00, Chapter I]), for every lattice in B we can compute a generating set over $\mathcal{O}$ with at most five elements. In particular, this can be done for the sum describing Λ', and we can assume that Λ is given in this way.

The algorithm

We are now ready to prove our first main result, which we recall here.

Theorem A. *There is an algorithm that, given a Bass order R in B, computes Bass suborders of R of any given genus.*

Proof. It suffices to give an algorithm which computes maximal suborders of R in any given genus. So we assume that we are given a prime $\mathfrak{p}$, the form $f_\mathfrak{p}$ corresponding to $R_\mathfrak{p}$, and a form $g_\mathfrak{p}$ beneath $f_\mathfrak{p}$. The algorithm, which we describe below, will return a Bass order $R' \subseteq R$ with $R'_\mathfrak{q} = R_\mathfrak{q}$ for all $\mathfrak{q} \neq \mathfrak{p}$, and such that $R'_\mathfrak{p}$ corresponds to $g_\mathfrak{p}$.

Algorithm 1.2.19.

Step 1. Use Proposition 1.2.14 to find a quasi-good basis for $R_\mathfrak{p}$.

Step 2. Use Proposition 1.2.12 to construct a suborder $R'_\mathfrak{p} \subseteq R_\mathfrak{p}$ corresponding to the form $g_\mathfrak{p}$.

Step 3. Use Proposition 1.2.17 to construct an order R' such that

$$R'_\mathfrak{q} = \begin{cases} R_\mathfrak{q} & \text{if } \mathfrak{q} \neq \mathfrak{p}, \\ R'_\mathfrak{p} & \text{if } \mathfrak{q} = \mathfrak{p}. \end{cases}$$

□

1.3 Computing ideal classes representatives for suborders

The aim of this section is to prove Theorem B. We start introducing some notation and definitions.

If R is an order in B, we denote by $\mathfrak{I}(R)$ the set of left R-ideals and by $Cl(R)$ the set of equivalence classes of left R-ideals. The equivalence class of an ideal I is denoted by $[I]$. The *norm* of an ideal I is defined as the fractional ideal $N(I) \subseteq F$ generated by the elements $N(x)$ as x runs over I.

Throughout this section, let $R' \subseteq R$ be orders in B.

Definition. *For $I \in \mathfrak{I}(R)$, we define*

$$\Psi_{R'}^{R}(I) = \{J \in \mathfrak{I}(R') : RJ = I\},$$

and we denote that set simply by $\Psi(I)$ when there is no possible confusion on which are the orders under consideration.

This definition was introduced in [PRV05], and later used in [PT07]. We will consider these sets for orders in B as well as for their completions. Both cases can and will be treated in an unified way.

Remark 1.3.1. Identifying ideals with ideles, the set $\Psi(I)$ is simply the preimage of I under the natural map

$$\widehat{R'}^{\times}\backslash\widehat{B}^{\times} \longrightarrow \widehat{R}^{\times}\backslash\widehat{B}^{\times},$$

where $\widehat{\ }$ denotes tensor with $\widehat{\mathbb{Z}}$ over $\mathbb{Z}$.

By $[\Psi(I)]$ we denote the set of classes of elements of $\Psi(I)$, i.e.

$$[\Psi(I)] = \{[J] : J \in \Psi(I)\}.$$

Note that if $[I_1] = [I_2]$, then $[\Psi(I_1)] = [\Psi(I_2)]$.

Proposition 1.3.2. *With the notation as above,*

$$Cl(R') = \coprod_{[I]\in Cl(R)} [\Psi(I)].$$

Proof. This is straightforward using the idelic description of $\Psi(I)$, but we give a direct proof.

Let $J \in \mathfrak{I}(R')$. Take $I = RJ$. Then it is clear that $I \in \mathfrak{I}(R)$ and $J \in \Psi(I)$. This shows that the union on the right hand side gives all of $Cl(R')$.

We now show that the union is disjoint. If there are $J_i \in \Psi_{R'}^{R}(I_i)$ for $i = 1, 2$ such that $[J_1] = [J_2]$, then $[I_1] = [I_2]$. Indeed, let $x \in B^{\times}$ be such that $J_1 = J_2 x$. Then,

$$I_1 = RJ_1 = RJ_2 x = I_2 x.$$

□

This proposition shows that the sets $\Psi(I)$ can be used to give a system of representatives for $Cl(R')$, in terms of a system of representatives for $Cl(R)$. The next proposition shows that by constructing representatives for $Cl(R')$ using these sets, we will not enlarge the norms of the R-ideals that we start with.

Proposition 1.3.3. *Let $I \in \mathfrak{I}(R)$, and let $J \in \mathfrak{I}(R')$ such that $J \subseteq I$. Then, $J \in \Psi(I)$ if and only if $N(I) = N(J)$.*

Proof. Let $\mathfrak{q}$ be a prime of $\mathcal{O}$. Since $J_{\mathfrak{q}} \subseteq I_{\mathfrak{q}}$ we can write $I_{\mathfrak{q}} = R_{\mathfrak{q}} x_{\mathfrak{q}}$ and $J_{\mathfrak{q}} = R'_{\mathfrak{q}} z_{\mathfrak{q}} x_{\mathfrak{q}}$, with $z_{\mathfrak{q}} \in R_{\mathfrak{q}}$. Then, $N(I_{\mathfrak{q}}) = N(J_{\mathfrak{q}})$ if and only if $z_{\mathfrak{q}} \in R_{\mathfrak{q}}^{\times}$, which is equivalent to the equality $R_{\mathfrak{q}} J_{\mathfrak{q}} = I_{\mathfrak{q}}$. These local facts imply the global statement. □

Given $I \in \mathfrak{I}(R)$, we have an action of the group $R_r(I)^{\times}$ on $\Psi(I)$ by right multiplication, which stabilizes the left R'-ideal classes.

Proposition 1.3.4. *Let $I \in \mathfrak{I}(R)$, and let $J \in \Psi(I)$. Then, the action of $R_r(I)^\times$ on $[J] \cap \Psi(I)$ is transitive and the stabilizer of J is $R_r(J)^\times$. In particular, $\#\big([J] \cap \Psi(I)\big) = [R_r(I)^\times : R_r(J)^\times]$.*

Proof. To prove that the action is transitive, let $J_1, J_2 \in \Psi(I)$ be such that $[J_1] = [J_2]$. If $x \in B^\times$ is such that $J_1 = J_2 x$, then $x \in R_r(I)^\times$, since $I = RJ_1 = RJ_2 x = Ix$. The other two statements are clear. □

The corollary below, which follows immediately, can be used to get information about the class numbers, as we will see in Section 1.4. It can also be used to check whether a set of non-equivalent R'-ideals is already a full set of representatives for the R'-ideal classes.

Corollary 1.3.5. *Let $I \in \mathfrak{I}(R)$. Then,*

$$\#\Psi(I) = \sum_{[J] \in [\Psi(I)]} [R_r(I)^\times : R_r(J)^\times].$$

In what follows, we describe two different methods for computing the set $\Psi(I)$ for a given $I \in \mathfrak{I}(R)$. The first one will rely on the action of the units described above, in the local setting, whereas the second one will only involve global calculations.

Local method: The action by $(R'_\mathfrak{p})^\times \backslash R_\mathfrak{p}^\times$

We first remark that the set $(R'_\mathfrak{p})^\times \backslash R_\mathfrak{p}^\times$ is not necessarily a group, since in general $(R'_\mathfrak{p})^\times$ is not a normal subgroup of $R_\mathfrak{p}^\times$.

Proposition 1.3.6. *Let $I_\mathfrak{p} \in \mathfrak{I}(R_\mathfrak{p})$, say $I_\mathfrak{p} = R_\mathfrak{p} x_\mathfrak{p}$. Then, the map*

$$\begin{aligned} (R'_\mathfrak{p})^\times \backslash R_\mathfrak{p}^\times &\longrightarrow \Psi(I_\mathfrak{p}) \\ \alpha_\mathfrak{p} &\mapsto R'_\mathfrak{p}(\alpha_\mathfrak{p} x_\mathfrak{p}) \end{aligned}$$

is bijective.

Proof. This map is the composition of the maps

$$\begin{aligned} (R'_\mathfrak{p})^\times \backslash R_\mathfrak{p}^\times &\longrightarrow \Psi(R_\mathfrak{p}), \\ \alpha_\mathfrak{p} &\mapsto R'_\mathfrak{p} \alpha_\mathfrak{p} \end{aligned} \qquad\qquad \begin{aligned} \Psi(R_\mathfrak{p}) &\longrightarrow \Psi(I_\mathfrak{p}). \\ J_\mathfrak{p} &\mapsto J_\mathfrak{p} x_\mathfrak{p} \end{aligned}$$

Both maps are bijective. This is clear for the second map. For the first one, this follows by Proposition 1.3.4, since all $R_\mathfrak{p}$-ideals are equivalent. □

Proposition 1.3.7. *Suppose that $[R : R'] = \mathfrak{p}^e$ for some $e \geq 1$. Let $I \in \mathfrak{I}(R)$. The map*

$$\begin{aligned} \Psi_{R'}^{R}(I) &\longrightarrow \Psi_{R'_\mathfrak{p}}^{R_\mathfrak{p}}(I_\mathfrak{p}) \\ J &\mapsto J_\mathfrak{p} \end{aligned}$$

is bijective. In particular, $\#\Psi_{R'}^{R}(I) = [R_\mathfrak{p}^\times : (R'_\mathfrak{p})^\times]$.

Proof. The fact that $I_\mathfrak{q} = J_\mathfrak{q}$ for all $\mathfrak{q} \neq \mathfrak{p}$ implies that the map is bijective. The equality follows from Proposition 1.3.6. □

These propositions imply immediately the following result.

Corollary 1.3.8. *Suppose that $[R : R'] = \mathfrak{p}^e$ for some $e \geq 1$. Let $I \in \mathfrak{I}(R)$, and write $I_\mathfrak{p} = R_\mathfrak{p} x_\mathfrak{p}$. If $\{\alpha_j\}$ is a system of representatives for $(R'_\mathfrak{p})^\times \backslash R_\mathfrak{p}^\times$, then $\Psi_{R'}^{R}(I) = \{J_j\}$, where $J_j \in \mathfrak{I}(R')$ is the ideal locally given by*

$$(J_j)_\mathfrak{q} = \begin{cases} I_\mathfrak{q} & \text{if } \mathfrak{q} \neq \mathfrak{p}, \\ R'_\mathfrak{p}(\alpha_j x_\mathfrak{p}) & \text{if } \mathfrak{q} = \mathfrak{p}. \end{cases}$$

Remark 1.3.9. A method to construct a local generator at $\mathfrak{p}$ of an ideal I is to consider the entry with minimum valuation at $\mathfrak{p}$ of the Gram matrix of a generating set $\{w_1, \dots, w_m\}$ for I over $\mathcal{O}$, since the norm is generated by an element with minimum valuation in such matrix. If this minimum is attached in the entry (i, j), then a local generator is $w_i + w_j$ if $i \neq j$, and w_i if $i = j$.

Proposition 1.3.10. *Assume that $\mathfrak{p}R_\mathfrak{p} \subseteq R'_\mathfrak{p}$. Then, the natural map*

$$\phi : (R'_\mathfrak{p})^\times \backslash R_\mathfrak{p}^\times \longrightarrow (\mathfrak{p}R_\mathfrak{p} \backslash R'_\mathfrak{p})^\times \backslash (\mathfrak{p}R_\mathfrak{p} \backslash R_\mathfrak{p})^\times.$$

is bijective.

Proof. Consider the ring morphism $\phi_1 : R_\mathfrak{p} \to \mathfrak{p}R_\mathfrak{p} \backslash R_\mathfrak{p}$. We claim that the induced group homomorphism $\phi_1 : R_\mathfrak{p}^\times \to (\mathfrak{p}R_\mathfrak{p} \backslash R_\mathfrak{p})^\times$ is surjective. Indeed, let $[x] \in (\mathfrak{p}R_\mathfrak{p} \backslash R_\mathfrak{p})^\times$. Then there exist $y, z \in R_\mathfrak{p}$ such that $xy = 1 + \pi_\mathfrak{p} z$. Then $N(xy) \equiv 1 \mod (\pi_\mathfrak{p})$, and hence $x \in R_\mathfrak{p}^\times$ as claimed.

Compose ϕ_1 with the map p that projects $(\mathfrak{p}R_\mathfrak{p} \backslash R_\mathfrak{p})^\times$ onto the quotient set $(\mathfrak{p}R_\mathfrak{p} \backslash R'_\mathfrak{p})^\times \backslash (\mathfrak{p}R_\mathfrak{p} \backslash R_\mathfrak{p})^\times$. Then $p \circ \phi_1$ is surjective, and passes to the quotient set $(R'_\mathfrak{p})^\times \backslash R_\mathfrak{p}^\times$ to give a surjective map $\phi : (R'_\mathfrak{p})^\times \backslash R_\mathfrak{p}^\times \to (\mathfrak{p}R_\mathfrak{p} \backslash R'_\mathfrak{p})^\times \backslash (\mathfrak{p}R_\mathfrak{p} \backslash R_\mathfrak{p})^\times$.

We claim that ϕ is injective. Indeed, let $x, y \in R_\mathfrak{p}^\times$ be such that $\phi(x) = \phi(y)$. Then, since $(R'_\mathfrak{p})^\times \to (\mathfrak{p}R_\mathfrak{p} \backslash R'_\mathfrak{p})^\times$ is also an epimorphism, we have $z \in (R'_\mathfrak{p})^\times$ and $w \in R_\mathfrak{p}$ such that $x = zy + \pi_\mathfrak{p} w$. Hence, $x = (z + \pi_\mathfrak{p} w y^{-1}) y$, which shows that $[x] = [y] \in (R'_\mathfrak{p})^\times \backslash R_\mathfrak{p}^\times$, since $\pi_\mathfrak{p} w y^{-1} \in \mathfrak{p}R_\mathfrak{p} \subseteq R'_\mathfrak{p}$ and hence $z + \pi_\mathfrak{p} w y^{-1} \in (R'_\mathfrak{p})^\times$. □

By Proposition 1.2.1, this result shows that, in order to give a system of representatives for the sets $(R'_\mathfrak{p})^\times \backslash R_\mathfrak{p}^\times$ when $R'_\mathfrak{p}$ is a maximal suborder of $R_\mathfrak{p}$, it will be enough to do the calculations modulo $\mathfrak{p}$.

Given a quasi-good basis $\mathcal{B} = \{1, e_1, e_2, e_3\}$ of $R_\mathfrak{p}$, and assuming that $R'_\mathfrak{p}$ is obtained from $R_\mathfrak{p}$ by means of Algorithm 1.2.19, we proceed to give a system of representatives for the sets $(R'_\mathfrak{p})^\times \backslash R_\mathfrak{p}^\times$, in terms of the form g corresponding with $R'_\mathfrak{p}$. The indexes $[R_\mathfrak{p}^\times : (R'_\mathfrak{p})^\times]$ are well known in the Eichler case, and are computed in [Brz90, Theorems 3.3 and 3.10] in the remaining cases, so it will suffice to give in each case the correct number of non-equivalent units.

Let q denote the order of the residue field $\mathbb{F}_\mathfrak{p}$, and let $\{a_1, a_2, \dots, a_q\} \subseteq \mathcal{O}_\mathfrak{p}$ be a set of representatives for $\mathbb{F}_\mathfrak{p}$ such that $a_1 = 1, a_2 = -1$ and $a_q = 0$. Let δ, β_0, β_1 be as in Proposition 1.2.8. Finally, let $S = \{\tilde{\gamma} \in \mathbb{F}_\mathfrak{p} \times \mathbb{F}_\mathfrak{p} : 1 - \delta\tilde{\gamma}_1^2 + \tilde{\gamma}_2^2 \neq 0\}$, and for each $\tilde{\gamma} \in S$ let $\gamma \in \mathcal{O}_\mathfrak{p} \times \mathcal{O}_\mathfrak{p}$ be any lift of $\tilde{\gamma}$.

Proposition 1.3.11. *With the previous notation and hypotheses, Table 1.3 gives a system of representatives for $(R'_\mathfrak{p})^\times \backslash R_\mathfrak{p}^\times$.*

$R_\mathfrak{p}$-class	$R'_\mathfrak{p}$-class	$[R_\mathfrak{p}^\times : (R'_\mathfrak{p})^\times]$	Representatives	Condition
A1	A1	$q+1$	$e_1, 1 + \frac{a_i}{2}(e_1 - e_2) \quad (1 \leq i \leq q)$	$d(R_\mathfrak{p}) = 1$
		q	$1 + \frac{a_i}{2}(e_1 - e_2) \quad (1 \leq i \leq q)$	$d(R_\mathfrak{p}) \neq 1$
	A2	$q(q-1)$	$e_2, 1 + \gamma_1(\beta_1 e_3 - \beta_0 e_1) + \gamma_2 e_2 \quad (\tilde{\gamma} \in S)$	
	B	$q-1$	$1, a_i + e_3 \quad (3 \leq i \leq q)$	
A2	A2	q^2	$1 + a_i e_1 + a_j e_2 \quad (1 \leq i, j \leq q)$	
	B	$q+1$	$1, a_i + e_3 \quad (1 \leq i \leq q)$	
B	C	q	$1, a_i + e_2 \quad (1 \leq i \leq q-1)$	$g \neq \langle 1, \delta\pi_\mathfrak{p}, \delta\pi_\mathfrak{p}^2 \rangle$
			$1, a_i + e_3 \quad (1 \leq i \leq q-1)$	$g = \langle 1, \delta\pi_\mathfrak{p}, \delta\pi_\mathfrak{p}^2 \rangle$
C	C	q	$1, a_i + e_2 \quad (1 \leq i \leq q-1)$	

Table 1.3: The indexes $[R_\mathfrak{p}^\times : (R'_\mathfrak{p})^\times]$, and representatives for $(R'_\mathfrak{p})^\times \backslash R_\mathfrak{p}^\times$.

Proof. According to Proposition 1.3.10 we may assume that $\mathcal{B}$ is a good basis, and it suffices to calculate a system of representatives for the set $(\mathfrak{p}R_\mathfrak{p} \backslash R'_\mathfrak{p})^\times \backslash (\mathfrak{p}R_\mathfrak{p} \backslash R_\mathfrak{p})^\times$.

First notice that $\mathfrak{p}R_\mathfrak{p} \backslash R_\mathfrak{p}$ is a $\mathbb{F}_\mathfrak{p}$-algebra that inherits naturally from $B_\mathfrak{p}$ a norm form $N : \mathfrak{p}R_\mathfrak{p} \backslash R_\mathfrak{p} \to \mathbb{F}_\mathfrak{p}$ such that $(\mathfrak{p}R_\mathfrak{p} \backslash R_\mathfrak{p})^\times = \{x \in \mathfrak{p}R_\mathfrak{p} \backslash R_\mathfrak{p} : N(x) \neq 0\}$. This allows us to easily check that all the given representatives are indeed units, and also to give the needed description of $(\mathfrak{p}R_\mathfrak{p} \backslash R'_\mathfrak{p})^\times$.

We will do the details in a single case, namely when $R_\mathfrak{p}$ has class A1 and $R'_\mathfrak{p}$ has class B. The rest of the cases can be treated similarly.

Let $x = x_0 + x_1e_1 + x_2e_2 + x_3e_3 \in \mathfrak{p}R_\mathfrak{p}\backslash R_\mathfrak{p}$. In these coordinates we have that the norm form is given by $N(x) = x_0^2 - x_3^2$ (see (1.2.4)), and that $x \in \mathfrak{p}R_\mathfrak{p}\backslash R'_\mathfrak{p}$ if and only if $x_3 = 0$. Hence, the elements of the form $a_i + e_3$ belong to $(\mathfrak{p}R_\mathfrak{p}\backslash R_\mathfrak{p})^\times$, if $i \geq 3$. They are not equivalent modulo $(\mathfrak{p}R_\mathfrak{p}\backslash R'_\mathfrak{p})^\times$, since if

$$(a_i + e_3)(x_0 + x_1e_1 + x_2e_2) = a_ix_0 + (a_ix_1 + x_2)e_1 + (a_ix_2 + x_1)e_2 + x_0e_3 = a_j + e_3,$$

then $x_0 = 1$ and hence $i = j$. And they are not equivalent to 1, since they do not belong to $\mathfrak{p}R_\mathfrak{p}\backslash R'_\mathfrak{p}$. □

Global method: The colon lattice

Let $I \in \mathfrak{I}(R)$. We introduce an alternative method to calculate $\Psi(I)$, using global tools. Consider the lattice

$$\Lambda_I = \{y \in B : yI^{-1} \subseteq R'\}.$$

It satisfies that $\Lambda_I = \Lambda_R I$. For simplicity, we will just consider $\Lambda = \Lambda_R$. It is clear that $\Lambda \subseteq R'$ and $R \subseteq R_r(\Lambda)$.

Lemma 1.3.12. *The lattice Λ satisfies the following properties:*

(1) $\mathfrak{p}R \subseteq \Lambda$, and hence $[R : \Lambda] \mid \mathfrak{p}^4$.

(2) $\Lambda \subseteq J$ for all $J \in \Psi(R)$.

Proof. The inclusion in (1) follows from the fact that $\mathfrak{p}R \subseteq R'$. The inclusion in (2) is clear if we consider the completion at primes $\mathfrak{q} \neq \mathfrak{p}$, so we will look only at the completion at $\mathfrak{p}$. Let $J \in \Psi(R)$, and write $J_\mathfrak{p} = R'_\mathfrak{p}u_\mathfrak{p}$ with $u_\mathfrak{p} \in R_\mathfrak{p}^\times$. Then,

$$\alpha_\mathfrak{p} \in \Lambda_\mathfrak{p} \Rightarrow \alpha_\mathfrak{p}R_\mathfrak{p} \subseteq R'_\mathfrak{p} \Rightarrow \alpha_\mathfrak{p}u_\mathfrak{p}^{-1} \in R'_\mathfrak{p} \Rightarrow \alpha_\mathfrak{p} \in R'_\mathfrak{p}u_\mathfrak{p} = J_\mathfrak{p}.$$

□

Since $\mathfrak{p}R_\mathfrak{p} \subseteq R'_\mathfrak{p}$, we can consider $R_\mathfrak{p}/R'_\mathfrak{p}$ as a $\mathbb{F}_\mathfrak{p}$-vector space. When $e = 2$, we can go further. Since in that case $R'_\mathfrak{p}$ has class A2, the ring $\mathcal{O}_\mathfrak{p} + \sqrt{\delta}\mathcal{O}_\mathfrak{p}$ embeds into $R'_\mathfrak{p}$, and hence into $R_\mathfrak{p}$. Then we can consider $R_\mathfrak{p}/R'_\mathfrak{p}$ as a $\mathbb{K}_\mathfrak{p}$-vector space, where $\mathbb{K}_\mathfrak{p}$ is the quadratic extension of $\mathbb{F}_\mathfrak{p}$ given by $\mathbb{K}_\mathfrak{p} = (\mathcal{O}_\mathfrak{p} + \sqrt{\delta}\mathcal{O}_\mathfrak{p})/\mathfrak{p}(\mathcal{O}_\mathfrak{p} + \sqrt{\delta}\mathcal{O}_\mathfrak{p})$.

Lemma 1.3.13.

(1) If $e = 1$, then $\dim_{\mathbb{F}_\mathfrak{p}}(R_\mathfrak{p}/R'_\mathfrak{p}) = 1$.

(2) If $e = 2$, then $\dim_{\mathbb{K}_\mathfrak{p}}(R_\mathfrak{p}/R'_\mathfrak{p}) = 1$.

Proof. It follows immediately from the fact that $|R_\mathfrak{p}/R'_\mathfrak{p}| = q^e$.

□

Proposition 1.3.14. *$[R' : \Lambda] = \mathfrak{p}^e$, and hence $[R : \Lambda] = \mathfrak{p}^{2e}$. In particular, if $e = 2$ then $\Lambda = \mathfrak{p}R$.*

Proof. It is enough to consider the completion at $\mathfrak{p}$. Then, we need to show that $|R'_\mathfrak{p}/\Lambda_\mathfrak{p}| = q^e$. Consider the morphism (of additive groups)

$$\psi : R'_\mathfrak{p} \to \mathrm{End}(R_\mathfrak{p}/R'_\mathfrak{p})$$
$$\alpha \mapsto (v \mapsto \alpha \cdot v).$$

Its kernel is $\Lambda_\mathfrak{p}$. The induced morphism $\psi : R'_\mathfrak{p}/\Lambda_\mathfrak{p} \to \mathrm{End}(R_\mathfrak{p}/R'_\mathfrak{p})$ is easily seen to be also a $\mathbb{F}_\mathfrak{p}$-vector space (respectively $\mathbb{K}_\mathfrak{p}$-vector space) morphism when $e = 1$ (respectively $e = 2$). Note that since $1 \notin \Lambda_\mathfrak{p}$, it is not the null morphism. Hence, the result follows from the previous lemma.

□

Corollary 1.3.15. *The set $\Psi(I)$ is given by*

$$\Psi(I) = \{J : RJ = I,\, R_l(J) = R',\, \Lambda_I \subseteq J \subseteq I,\, [I : J] = [J : \Lambda_I] = \mathfrak{p}^e\}.$$

Proof. When $I = R$, the result follows immediately from Lemma 1.3.12 and Proposition 1.3.14. The arguments used for the general case are entirely analogous.

□

In particular, to calculate $\Psi(I)$ (whose cardinality we already know by Proposition 1.3.7), we can limit ourselves to calculate the lattices between Λ_I and I with the indicated indexes, and then determine which of them satisfy the first two equalities. Furthermore, the equality $R_l(J) = R'$ can be replaced by the equality $N(J) = N(I)$, which sometimes is easier to verify.

Remark 1.3.16. If $e = 1$, then $[I : \Lambda_I] = \mathfrak{p}^2$, and there are $q + 1$ lattices between these two. We have seen that the number of elements of $\Psi(I)$ is $q - 1$, q or $q + 1$. Hence, almost all lattices constructed are needed. This makes this method effective.

Remark 1.3.17. In the case $e = 2$, we know that the elements in $\Psi(I)$ have a $(\mathcal{O}_\mathfrak{p} + \sqrt{\delta}\mathcal{O}_\mathfrak{p})$-module structure. If we only consider lattices between Λ_I and I which have this extra structure, there are $q^2 + 1$ such lattices. The order of $\Psi(I)$ is $q^2 - q$ if R is the maximal order and R' is of class A2, and q^2 if both orders are of class A2. Hence, except for the maximal order, this construction is effective as well.

The algorithm

We now prove our second main result, which we first recall. We assume that F is totally real and B is totally definite (i.e., B ramifies at every infinite place of F).

Theorem B. *There is an algorithm that, given a Bass order R in B and a set of representatives S of left R-ideal classes, computes left ideal classes representatives for Bass suborders of R of any given genus. Furthermore, the set of norms of the computed ideals is the same as the set of norms of the ideals in S.*

Proof. It suffices to give an algorithm that works when considering maximal suborders of R. In particular, we assume that we are given the same input as in Algorithm 1.2.19, plus the set S. The algorithm will return a set S' of representatives for left ideal classes representatives for the suborder R' obtained by Algorithm 1.2.19.

By Proposition 1.3.2, it suffices to give an algorithm which calculates, for each $I \in S$, a set of representatives S'_I for $[\Psi(I)]$, and then return $S' = \bigcup_{I \in S} S'_I$. Note that the set of norms of ideals is preserved due to Proposition 1.3.3.

The hypothesis of F being totally real and B being totally definite is used in Step *4.1*, as we explain below. The algorithm works as follows.

Algorithm 1.3.18.

Step 1. Using Proposition 1.3.11, compute a set of representatives for $(R'_\mathfrak{p})^\times \backslash R_\mathfrak{p}^\times$.

Step 2. Using Remark 1.3.9, find a local generator for $I_\mathfrak{p}$.

Step 3. Using Corollary 1.3.8 and Proposition 1.2.17, compute the set $\Psi(I)$.

Step 4. Set $T = \Psi(I)$ and set $S'_I = \emptyset$.

> *Step 4.1*. Pick $J \in T$ and compute the set $[J] \cap \Psi(I)$ by letting $R_r(J)^\times \backslash R_r(I)^\times$ act on J (see Proposition 1.3.4).
>
> *Step 4.2*. Set $S'_I = S'_I \cup \{J\}$. If $T \backslash [J] = \emptyset$, return S'_I. Else, let $T = T \backslash [J]$ and go to Step 4.1.

□

We do not have a general method for, given $J \in \Psi(I)$, computing a system of representatives for the (finite) set $R_r(J)^\times \backslash R_r(I)^\times$ needed in Step *4.1*; otherwise, the algorithm would work without the hypotheses on F and B. Under these hypotheses, the set $\mathcal{O}^\times \backslash R_r(I)^\times$ is finite and can be used as well to compute $[J] \cap \Psi(I)$.

The finiteness of the set $\mathcal{O}^\times \backslash R_r(I)^\times$, as well as a method to compute it, can be obtained considering the exact sequence

$$1 \longrightarrow \{\pm 1\} \backslash R_r(I)^{\times,1} \longrightarrow \mathcal{O}^\times \backslash R_r(I)^\times \xrightarrow{N} (\mathcal{O}^\times)^2 \backslash \mathcal{O}_+^\times, \tag{1.3.19}$$

where $\mathcal{O}_+^\times$ denotes the group of totally positive units of $\mathcal{O}$. Assuming B totally definite, the quadratic form $\mathrm{Tr}_{F/\mathbb{Q}} \circ N : B \to \mathbb{Q}$ is positive definite, and hence the group $R_r(I)^{\times,1}$ is finite and can be calculated using the Lenstra–Lenstra–Lovász lattice basis reduction algorithm. Furthermore, its possible group structures are known (see [Vig76, Théorème 5]). The group $(\mathcal{O}^\times)^2 \backslash \mathcal{O}_+^\times$ is always finite, and equals the null group in many cases, such as for fields F having narrow class number equal to 1 (see [EMP86]).

Remark 1.3.20. Since $R_r(J)^\times \subseteq R_r(I)^\times$ for every $J \in \Psi(I)$, when iterating the algorithm we need to apply the previous procedure to compute the sets $\mathcal{O}^\times \backslash R_r(I)^\times$ only for the initial set of ideals.

Remark 1.3.21. We can compute $\Psi(I)$ by the global method given in Corollary 1.3.15 instead of using Steps 1, 2 and 3, although to our knowledge there is no advantage of one method over the other.

1.4 Example: The Consani-Scholten quintic

In this section we show how we can use our method to compute ideal classes representatives for an Eichler order of discriminant (30) in the quaternion algebra ramified exactly at the two infinite places of the real quadratic field $F = \mathbb{Q}[\sqrt{5}]$.

A similar example was considered in [CS01] to give numerical evidence supporting the conjectural modularity of the Galois representation attached to the third étale cohomology vector space of a certain quintic threefold (see [CS01, Theorem 0.3] for details). In that article the algebra considered is ramified also at (2) and (3), since the Galois representation associated to the quintic has semi-stable reduction at those places. The representatives are constructed following the method of Pizer (see [Piz80]), which involves seeking for ideals and checking for equivalence between the constructed ones until the class number, which has to be precomputed or can be deduced during the computation using the mass formula, is reached. We consider instead the quaternion algebra ramified only at the two infinite places, since in that case the maximal order has class number equal to 1, which makes calculations simpler. We first make use of Theorem A to compute an Eichler order of discriminant (30) and then we make use of Theorem B to compute its left ideal classes representatives. Most of the computations were made with the aid of `SAGE` ([S$^+$11]).

Denote by $\omega = \frac{1+\sqrt{5}}{2}$ and let $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\omega$ be the ring of integers of F. Let B be the quaternion algebra $(-1,-1)_F$. It is unramified at all finite places $\mathfrak{p}$ not dividing 2, since the Hilbert symbol $(-1,-1)_\mathfrak{p}$ equals 1 for such $\mathfrak{p}$, and it is ramified at the two infinite places. Since 2 is inert in the extension $F/\mathbb{Q}$, by parity reasons B does not ramify at (2).

Warning. In order to make the notation lighter, throughout this section we sometimes omit parentheses when referring to principal ideals in $\mathcal{O}$, e.g. when referring to the order $R(2)$ defined below and its completion $R(2)_2$. But we do use parentheses when referring to residue fields, e.g. to avoid confusing $\mathbb{F}_{(2)}$ with the finite field of order 2.

Constructing the orders

Starting with a maximal order in B as input, we compute an Eichler order in B of discriminant (30). Considering the prime factorization of (30) in $\mathcal{O}$, we iterate Algorithm 1.2.19 to construct a chain of orders

$$R(1) \supseteq R(2) \supseteq R(6) \supseteq R(6\sqrt{5}) \supseteq R(30),$$

where $R(\mathfrak{N})$ denotes an order of discriminant $\mathfrak{N}$.

The maximal order we use is the order given in [Vig80, Chapter V], namely

$$R(1) = \left\langle \frac{1+\omega^{-1}i+\omega j}{2}, \frac{\omega^{-1}i+j+\omega k}{2}, \frac{\omega i+\omega^{-1}j+k}{2}, \frac{i+\omega j+\omega^{-1}k}{2} \right\rangle_{\mathcal{O}}.$$

Discriminant (2)

In this first step we use Algorithm 1.2.19 referring to the Appendix, since we take $\mathfrak{p} = (2)$.

Step 1. The order $R(1)_2$ is in correspondence with the form $f = H \perp \langle 1 \rangle$. Using the basis for $R(1)$ given above, we get that

$$\mathcal{B} = \left\{1, \tfrac{1}{2}(1+\omega^{-1}i+\omega j), \tfrac{1}{2}(\omega i+\omega^{-1}j+k), \tfrac{1}{2}(i+\omega j+\omega^{-1}k)\right\}$$

is a basis for $R(1)_2$. Its dual basis is

$$\mathcal{B}^{\vee} = \left\{f_0, \omega i-(1+\omega)k, \tfrac{1}{2}\big((1+\omega)i-j-\omega k\big), \tfrac{1}{2}\big(-(1+2\omega)i+\omega j+(1+3\omega)k\big)\right\},$$

where $f_0 = \frac{1}{2}(1-\omega i+(1+\omega)k)$. Diagonalizing $M_{\mathcal{B}^{\vee}}$ (as a ternary quadratic form), we see that letting

$$\begin{aligned} f_1 &= \tfrac{1}{5}\big((2+\omega)i-j-(1+\omega)k\big),\\ f_2 &= \tfrac{1}{2}\big((1+\omega)i-j+(6+11\omega)k\big),\\ f_3 &= \tfrac{1}{5}\big(-(47+88\omega)i+(11+26\omega)j+(43+32\omega)k\big), \end{aligned}$$

the hypotheses of Proposition 1.5.7 are satisfied by $\mathcal{E} = \{f_0, f_1, f_2, f_3\}$. Hence, letting

$$\begin{aligned} e_1 &= \tfrac{1}{2}\big(-(232+384\omega)-(79+119\omega)i-(265+212\omega)j-(2-5\omega)k\big),\\ e_2 &= \tfrac{1}{25}\big(268+444\omega+(6-31\omega)i-(17+84\omega)j-(1+\omega)k\big),\\ e_3 &= \tfrac{1}{10}\big(13+24\omega-(7+12\omega)i-(10+21\omega)j)-k\big), \end{aligned}$$

we get that $\mathcal{E}^{\dagger} = \{1, e_1, e_2, e_3\}$ is a quasi-good basis for $R(1)_2$.

Step 2. We are descending from $f = H \perp \langle 1 \rangle$ to $g = H \perp \langle 2 \rangle$. To illustrate Proposition 1.2.11, we show that we can construct a well-known order of discriminant (2). For this purpose, we conjugate the quasi-good basis found above by $x = e_1+e_2$ (which belongs to $R(1)_2^{\times}$, by Table 1.8), thus obtaining another quasi-good basis of $R(1)_2$. Proposition 1.5.5 gives then that $\left\{1, xe_1x^{-1}, 2\cdot xe_2x^{-1}, xe_3x^{-1}\right\}$ is a basis of $R(2)_2$.

Step 3. Applying Proposition 1.2.17 to this basis, we obtain that

$$R(2) = \left\langle 1, i, j, \frac{1+i+j+k}{2} \right\rangle_{\mathcal{O}}$$

is an Eichler order of discriminant (2). Note that the given basis is a basis for the classical maximal order in the quaternion algebra $(-1,-1)_{\mathbb{Q}}$.

Discriminant (6)

Diagonalizing modulo 3 the quadratic form associated to $\left\{x \in R(2)_3{}^{\vee} : \mathrm{Tr}(x) = 0\right\}$, we obtain using Proposition 1.2.14 that $\left\{1, \frac{1}{2}(i+j), \frac{k}{2}, 2(i-j)\right\}$ is a quasi-good basis for $R(2)_3$.

We use Table 1.2 to descend from $\langle 1, -1, 1 \rangle$ to $\langle 1, -1, 3 \rangle$, using $\alpha_0 = 2, \alpha_1 = -1$ as parameters, and we get that a basis for $R(6)_3$ is given by $\left\{1, i+j-\frac{k}{2}, -\frac{1}{2}(i+j)+k, 2(i-j)\right\}$. Using Proposition 1.2.17, we get that

$$R(6) = \left\langle 1, i+2k, 3k, \frac{1+i+j+k}{2} \right\rangle_{\mathcal{O}}$$

is an Eichler order of discriminant (6).

Discriminant $(6\sqrt{5})$

The basis $\mathcal{E} = \left\{\frac{1}{2}, -i, -\frac{k}{2}, -\frac{j}{4}\right\}$ of $R(6)_{\sqrt{5}}{}^{\vee}$ satisfies the hypotheses of Proposition 1.2.14, but with a stronger congruence in (1), namely mod $(\sqrt{5})^2$. This implies that the basis for $R(6\sqrt{5})_{\sqrt{5}}$ obtained below is a quasi-good basis (see Remark 1.2.13).

We apply Table 1.2 using $\alpha_0 = 2 + \frac{\omega}{3}, \alpha_1 = -2$ as parameters, thus obtaining that $\{1, -(1+\frac{\omega}{6})i + 2k, i - (2+\frac{\omega}{3})k, -2j\}$ is basis for $R(6\sqrt{5})_{\sqrt{5}}$. Then Proposition 1.2.17 gives that

$$R(6\sqrt{5}) = \left\langle 1, i+2k, 3\sqrt{5}k, \frac{1+i+j+7k}{2} \right\rangle_{\mathcal{O}}.$$

is an Eichler order of discriminant $(6\sqrt{5})$.

Discriminant (30)

To construct $R(30)$, we use the quasi-good basis obtained in the previous step and $\alpha_0 = \frac{139}{82} + \frac{61}{123}\omega, \alpha_1 = -2$ as parameters. The basis for $R(30)_{\sqrt{5}}$ obtained in this way is $\{1, -(\frac{34}{9} + \frac{31}{36}\omega)i + (\frac{303}{41} + \frac{68}{41}\omega)k, (\frac{303}{82} + \frac{34}{41}\omega)i - (\frac{68}{9} + \frac{31}{18}\omega)k, -2j\}$. Applying Proposition 1.2.17, we obtain that

$$R(30) = \left\langle 1, i+2k, 15k, \frac{1+i+j+7k}{2} \right\rangle_{\mathcal{O}}.$$

is an Eichler order of discriminant (30).

Constructing the ideals

We now proceed to compute ideal classes representatives for $R(30)$ iterating Algorithm 1.3.18, and using the quasi-good bases obtained above.

Before starting, note that Equation (1.3.19) implies that only norm one global units need to be considered when checking for equivalence of ideals in Step *4.1*, since F has narrow class number 1.

In [Vig80, Théorème 3.7] it is shown that $R(1)$ has class number equal to one. It is also shown that $R(1)^{\times,1} = E_{120}$, where E_{120} is the binary icosahedral group. Explicitly, if we let

$$E_{24} = \left\{ \pm 1, \pm i, \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2} \right\}$$

and $u = \frac{1}{4}(i + \omega j + \omega^{-1}k)(1+i+j+k)$, then

$$E_{120} = \left\{ u^m x : 0 \le m \le 4, x \in E_{24} \right\}.$$

Using this explicit description we can avoid the use of LLL for computing $R(1)^{\times,1}$. Furthermore, by Remark 1.3.20, this group contains all of the global units needed in our computations.

Discriminant (2)

The calculation of $Cl(R(2))$ can be done without using the algorithm. Since $|R(2)^{\times,1}| = 24$ and $[R(1)_2^{\times} : R(2)_2^{\times}] = 5$ (see Table 1.8), Corollary 1.3.5 implies that $\left[\Psi_{R(2)}^{R(1)}(R(1))\right] = [R(2)]$, from which we conclude that $R(2)$ has class number equal to 1 as well.

Discriminant (6)

We now compute $Cl(R(6))$, following Algorithm 1.3.18 closely. We have $S = \{R(2)\}$ as input.

Step 1. To obtain a set of representatives for $R(6)_3^\times \backslash R(2)_3^\times$, we use $\{0, 1, 2, \omega, 2\omega, \omega+1, \omega+2, 2\omega+1, 2\omega+2\}$ as a set of representatives for $\mathbb{F}_{(3)}$.

Step 2. The ideal $R(2)_3$ is trivially generated by 1, so there is no need to use Remark 1.3.9 in this case.

Steps 3 and 4. The set $\Psi^{R(2)}_{R(6)}(R(2))$ has ten ideals, which we do not list for length reasons. The action of $R(2)^{\times,1}$ on $\Psi^{R(2)}_{R(6)}(R(2))$ has two orbits, namely $[I]$ and $[J]$, where $I = R(6)$ and J is the $R(6)$-ideal corresponding to the fifth generator of $R(6)_3^\times \backslash R(2)_3^\times$, which is given by

$$J = \left\langle i + (\omega - 1)k, j - (\omega + 1)k, 3k, 1 + \frac{\omega}{2}(3 - i - j - 3k) \right\rangle_{\mathcal{O}}.$$

This result agrees with Corollary 1.3.5, since $|R_r(I)^{\times,1}| = 6$, $|R_r(J)^{\times,1}| = 4$ and $[R(2)_3^\times : R(6)_3^\times] = 10$.

Hence, the algorithm gives that $Cl(R(6)) = \{[I], [J]\}$.

Discriminant ($6\sqrt{5}$)

We compute $Cl(R(6\sqrt{5}))$ in the same way as before. We avoid writing down all the details but give enough information so the reader can verify the computations easily.

- We take $\{0, 1, 2, 3, 4\}$ as a set of representatives for $\mathbb{F}_{(\sqrt{5})}$.
- 1 is a local generator of $J_{\sqrt{5}}$, since $J_{\sqrt{5}} = R(6)_{\sqrt{5}}$.
- Denote $\Psi^{R(6)}_{R(6\sqrt{5})}(I) = \{I_1, \dots, I_6\}$ and $\Psi^{R(6)}_{R(6\sqrt{5})}(J) = \{J_1, \dots, J_6\}$, where the notation is such that the n-th ideal corresponds to the n-th representative of $R(6\sqrt{5})^\times_{\sqrt{5}} \backslash R(6)^\times_{\sqrt{5}}$, following the labeling given in Table 1.3.
- The action of $R_r(I)^{\times,1}$ on $\Psi^{R(6)}_{R(6\sqrt{5})}(I)$ gives that $\left[\Psi^{R(6)}_{R(6\sqrt{5})}(I)\right] = \{[I_1], [I_4]\}$, and the action of $R_r(J)^{\times,1}$ on $\Psi^{R(6)}_{R(6\sqrt{5})}(J)$ gives that $\left[\Psi^{R(6)}_{R(6\sqrt{5})}(J)\right] = \{[J_1], [J_2], [J_3], [J_5]\}$ (see Table 1.4 for an explicit description of these ideals).

Hence, we have that $Cl(R(6\sqrt{5})) = \{[I_1], [I_4], [J_1], [J_2], [J_3], [J_5]\}$. This agrees with Corollary 1.3.5, since we have that $|R_r(I_1)^{\times,1}| = |R_r(I_4)^{\times,1}| = |R_r(J_1)^{\times,1}| = |R_r(J_3)^{\times,1}| = 2$, and $|R_r(J_2)^{\times,1}| = |R_r(J_5)^{\times,1}| = 4$.

Ideal	Basis	Ideal above
I_1	$i + 2k, 3\sqrt{5}k, 1, \frac{1}{2}(1 + i + j + 7k)$	I
I_4	$i + 2k, 3\sqrt{5}k, j + 14k, \frac{1}{2}(1 + i + j + 19k)$	
J_1	$i + (\omega - 1)k, 3\sqrt{5}k, j - (\omega + 7)k, \frac{1}{2}(1 - i - j + (18 + \sqrt{5})k)$	J
J_2	$i + (\omega - 1)k, 3\sqrt{5}k, j - (\omega + 4)k, \frac{1}{2}(1 - i - j + (6 + \sqrt{5})k)$	
J_3	$i + (\omega - 1)k, 3\sqrt{5}k, j - (\omega + 1)k, \frac{1}{2}(1 - i + j + (6 - \sqrt{5})k)$	
J_5	$i + (\omega - 1)k, 3\sqrt{5}k, j - (\omega - 5)k, \frac{1}{2}(1 - i - j + \sqrt{5}k)$	

Table 1.4: Representatives for $Cl(R(6\sqrt{5}))$.

Discriminant (30)

Finally, we compute $Cl(R(30))$.

- The residue field is the same as before, so we take the same representatives for $\mathbb{F}_{(\sqrt{5})}$.

- The local generators at $\sqrt{5}$ for the ideals in $Cl(R(6\sqrt{5}))$ were constructed using Corollary 1.3.8. They are $1, 1-\frac{3}{4}i+\frac{3}{2}k, 1, 1-\frac{i}{4}+\frac{k}{2}, 1-\frac{i}{2}+k$ and $1-i+2k$ for I_1, I_4, J_1, J_2, J_3 and J_5 respectively.
- Since $R_r(I_1)^{\times,1} = R_r(I_4)^{\times,1} = R_r(J_1)^{\times,1} = R_r(J_3)^{\times,1} = \{\pm 1\}$, we have that between the ideals in $\Psi_{R(30)}^{R(6\sqrt{5})}(I_1), \Psi_{R(30)}^{R(6\sqrt{5})}(I_4), \Psi_{R(30)}^{R(6\sqrt{5})}(J_1)$ and $\Psi_{R(30)}^{R(6\sqrt{5})}(J_3)$ there are no equivalences.
- The action of $R_r(J_2)^{\times,1}$ on $\Psi_{R(30)}^{R(6\sqrt{5})}(J_2)$ gives that $\left[\Psi_{R(30)}^{R(6\sqrt{5})}(J_2)\right] = \{[J_{2,1}], [J_{2,2}], [J_{2,3}]\}$, and the action of $R_r(J_5)^{\times,1}$ on $\Psi_{R(30)}^{R(6\sqrt{5})}(J_5)$ gives that $\left[\Psi_{R(30)}^{R(6\sqrt{5})}(J_5)\right] = \{[J_{5,1}], [J_{5,2}], [J_{5,3}]\}$ (see Table 1.5).

In particular, $\#Cl(R(30)) = 4 \cdot 5 + 6 = 26$.

Ideal	Basis	Ideal above
$I_{1,1}$	$i+2k, 15k, 1, \frac{1}{2}(1+i+j+7k)$	I_1
$I_{1,2}$	$i+2k, 15k, j+2(1+3\omega)k, , \frac{1}{2}(1+i+j+(7-6\sqrt{5})k)$	
$I_{1,3}$	$i+2k, 15k, j-(1+3\omega)k, \frac{1}{2}(1+i+j+(-8+3\sqrt{5})k)$	
$I_{1,4}$	$i+2k, 15k, j-(4-3\omega)k, \frac{1}{2}(1+i+j+(8+3\sqrt{5})k)$	
$I_{1,5}$	$i+2k, 15k, j-(7+6\omega)k, \frac{1}{2}(1+i+j+(7+6\sqrt{5})k)$	
$I_{4,1}$	$i+2k, 15k, j+2(2-3\omega)k, \frac{1}{2}(1+i+j-(11+6\sqrt{5})k)$	I_4
$I_{4,2}$	$i+2k, 15k, j-(7+3\omega)k, \frac{1}{2}(1+i+j+(4+3\sqrt{5})k)$	
$I_{4,3}$	$i+2k, 15k, j+(5+3\omega)k, \frac{1}{2}(1+i+j+(1-6\sqrt{5})k)$	
$I_{4,4}$	$i+2k, 15k, j+2(1-3\omega)k, \frac{1}{2}(1+i+j+(19+6\sqrt{5})k)$	
$I_{4,5}$	$i+2k, 15k, j+14k, \frac{1}{2}(1+i+j+19k)$	
$J_{1,1}$	$i+(2-5\omega)k, 15k, j+5(1+\omega)k, \frac{1}{2}(1+i+j+(2-5\sqrt{5})k)$	J_1
$J_{1,2}$	$i+(2-5\omega)k, 15k, j+(2-4\omega)k, \frac{1}{2}(1+i+j+(17+4\sqrt{5})k)$	
$J_{1,3}$	$i+(2-5\omega)k, 15k, j+(2-\omega)k, \frac{1}{2}(1+i+j-(13+2\sqrt{5})k)$	
$J_{1,4}$	$i+(2-5\omega)k, 15k, j-(4+7\omega)k, \frac{1}{2}(1+i+j+(2+7\sqrt{5})k)$	
$J_{1,5}$	$i+(2-5\omega)k, 15k, j-(1+7\omega)k, \frac{1}{2}(1+i+j+(2+\sqrt{5})k)$	
$J_{2,1}$	$i+(2-5\omega)k, 15k, j+(5-7\omega)k, \frac{1}{2}(1+i+j-(4+5\sqrt{5})k)$	J_2
$J_{2,2}$	$i+(2-5\omega)k, 15k, j+(5-4\omega)k, \frac{1}{2}(1+i+j+(11+4\sqrt{5})k)$	
$J_{2,3}$	$i+(2-5\omega)k, 15k, j+2(1+\omega)k, \frac{1}{2}(1+i+j+(11-2\sqrt{5})k)$	
$J_{3,1}$	$i+(2-5\omega)k, 15k, j-(4-5\omega)k, \frac{1}{2}(1+i+j-(10+5\sqrt{5})k)$	J_3
$J_{3,2}$	$i+(2-5\omega)k, 15k, j-(7+4\omega)k, \frac{1}{2}(1-i+j+(5+4\sqrt{5})k)$	
$J_{3,3}$	$i+(2-5\omega)k, 15k, j+(5+2\omega)k, \frac{1}{2}(1+i+j+(5-2\sqrt{5})k)$	
$J_{3,4}$	$i+(2-5\omega)k, 15k, j+(2-7\omega)k, \frac{1}{2}(1+i+j+(20+7\sqrt{5})k)$	
$J_{3,5}$	$i+(2-5\omega)k, 15k, j+(1+\omega)k, \frac{1}{2}(1+i+j-(10-\sqrt{5})k)$	
$J_{5,1}$	$i+(2-5\omega)k, 15k, j+(2+5\omega)k, \frac{1}{2}(1+i+j+(8-5\sqrt{5})k)$	J_5
$J_{5,2}$	$i+(2-5\omega)k, 15k, j-(1+4\omega)k, \frac{1}{2}(1+i+j+(15+4\sqrt{5})k)$	
$J_{5,3}$	$i+(2-5\omega)k, 15k, j-2(2-\omega)k, \frac{1}{2}(1-i+j-(6-3\sqrt{5})k)$	

Table 1.5: Representatives for $Cl(R(30))$.

We end this section remarking that all the results obtained agree with Eichler's mass formula ([Vig80, Corollaire V.2.3]), which we recall here.

Proposition 1.4.1. *Let B be a totally ramified quaternion algebra, and let $R \subseteq B$ be an Eichler of discriminant $d(R) = \mathfrak{m}\mathfrak{n}$, where $\mathfrak{n}$ is the level of R. Let $I_1, \ldots, I_n \in \mathfrak{I}(R)$ be a set of representatives for the left R-ideals equivalence classes, and let $w_i = [R_r(I_i)^\times : \mathcal{O}^\times]$.*

$$\sum_{i=1}^{n} w_i = 2^{1-d} \cdot |\zeta_F(-1)| \cdot h(F) \cdot N(\mathfrak{n}) \prod_{\mathfrak{p}|\mathfrak{m}} (N(\mathfrak{p})-1) \prod_{\mathfrak{p}|\mathfrak{n}} (N(\mathfrak{p})+1),$$

where $d = [F : Q]$, $h(F)$ is the class number of F and ζ_F is the Dedekind zeta function of F.

1.5 Appendix: The case $\mathfrak{p} = (2)$

If $\mathfrak{p} \mid (2)$ we can apply the same techniques used in the previous sections, but in this case local Bass orders are described in terms of a different set of ternary quadratic forms. This set is described in [Lem11] in the case $\mathfrak{p} = (2)$, i.e. if 2 is inert in $F/\mathbb{Q}$, which is the case that we will consider in this appendix. The remaining cases are more involved, and remain to be studied.

Consider the matrices

$$H = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad J = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

Given f, g quadratic forms, let $f \perp g$ denote their orthogonal sum. According to [Lem11, Propositions 5.8 and 5.12], isomorphism classes of Bass orders in quaternion algebras over $\mathbb{F}_{(2)}$ are in one to one correspondence with the forms f of Table 1.6. As in the case $\mathfrak{p} \nmid (2)$, orders of class A1 are the so called *Eichler orders*.

Class	Form	Parameters	Condition	Algebra
A1	$H \perp \langle 2^s \rangle$	$s \geq 0$		1
A2	$J \perp \langle 2^s \rangle$	$s \geq 1$		$(-1)^s$
B	$\langle 1, 1, \delta_1 2^s \rangle$	$s \geq 0, \delta_1 \in \{1, 3\}$	$\delta_1 = 1$	-1
			$\delta_1 = 3$	1
C	$\langle 1, 6, \delta_1 2^s \rangle$	$s \geq 1, \delta_1 \in \{1, 3\}$	$\delta_1 = 1$	$(-1)^s$
			$\delta_1 = 3$	$(-1)^{s+1}$
D	$\langle 1, 5, \delta_1 2^s \rangle$	$s \geq 3, \delta_1 \in \{1, 3\}$	$\delta_1 = 1$	$(-1)^{s+1}$
			$\delta_1 = 3$	$(-1)^s$
E	$\langle 1, 2, \delta_2 2^s \rangle$	$s \geq 3, \delta_2 \in \{1, 5\}$	$\delta_2 = 1$	-1
			$\delta_2 = 5$	1
F	$\langle 1, 14, \delta_2 2^s \rangle$	$s \geq 4, \delta_2 \in \{1, 5\}$	$\delta_2 = 1$	1
			$\delta_2 = 5$	-1
G	$\langle 1, 10, \delta_2 2^s \rangle$	$s \geq 4, \delta_2 \in \{1, 5\}$	$\delta_2 = 1$	$(-1)^{s+1}$
			$\delta_2 = 5$	$(-1)^s$

Table 1.6: Ternary quadratic forms in correspondence with local Bass orders, when $\mathfrak{p} = (2)$.

In the right column of Table 1.6 we indicate with 1 or -1 whether the order $C_0(f)$ belongs to the matrix algebra or to the division algebra. As before, this depends on whether the norm form associated to $C_0(f)$ is isotropic or not. We omit the calculations.

Figure 1.2 shows how isomorphism classes of Bass orders in quaternion algebras over $\mathbb{F}_{(2)}$ are distributed.

The notion of good basis must be extended to include the non-diagonal forms of Table 1.6. As in the previous section, we omit parentheses when denoting completions at (2) to make notation lighter.

Definition. *Let R_2 be a Bass order in correspondence with the form $f = H \perp \langle 2^s \rangle$ (respectively, with $f = J \perp \langle 2^s \rangle$). A basis $\mathcal{B} = \{1, e_1, e_2, e_3\}$ of R_2 as an $\mathcal{O}_2$-module is* good *if the e_i satisfy*

$$(1.5.1) \qquad \begin{aligned} e_1^2 &= 0, & e_1e_2 &= 2^s(1 - e_3), & e_2e_1 &= 2^s e_3, \\ e_2^2 &= 0, & e_2e_3 &= 0, & e_3e_2 &= e_2, \\ e_3^2 &= e_3, & e_3e_1 &= 0, & e_1e_3 &= e_1. \end{aligned}$$

Respectively, if the e_i satisfy

$$(1.5.2) \qquad \begin{aligned} e_1^2 &= -2^s, & e_1e_2 &= 2^s(1 - e_3), & e_2e_1 &= 2^s e_3, \\ e_2^2 &= -2^s, & e_2e_3 &= -e_1, & e_3e_2 &= e_1 + e_2, \\ e_3^2 &= e_3 - 1, & e_3e_1 &= -e_2, & e_1e_3 &= e_1 + e_2. \end{aligned}$$

Note that in such bases the norm form is given by

$$(1.5.3) \qquad N(x) = \begin{cases} x_0^2 + x_0x_3 - 2^s x_1x_2, & f = H \perp \langle 2^s \rangle, \\ x_0^2 + x_0x_3 + x_3^2 - 2^s x_1x_2 + 2^s x_1^2 + 2^s x_2^2, & f = J \perp \langle 2^s \rangle. \end{cases}$$

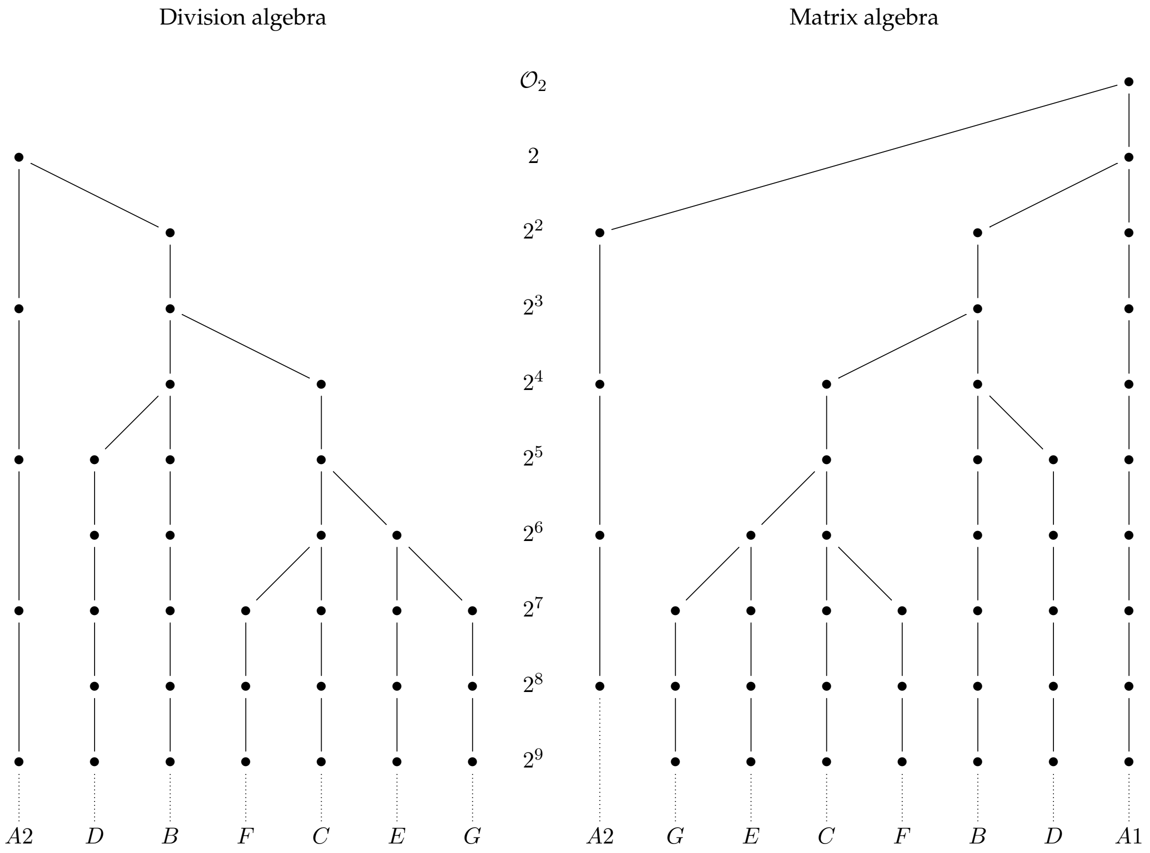

Figure 1.2: Graph of isomorphism classes of local Bass orders, ordered by inclusion, when $\mathfrak{p} = (2)$.

Remark 1.5.4. We can extend Remark 1.2.7 to non-diagonal forms as follows. Let R_2 be an order in correspondence with $f = H \perp \langle 2^s \rangle$, and let $\mathcal{B}$ be a good basis of R_2. Then,

$$-2^s \cdot M_{\mathcal{B}^\vee} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 2^{s+1} \end{pmatrix}.$$

Respectively if R_2 is in correspondence with $f = J \perp \langle 2^s \rangle$, then

$$2^s 3 \cdot M_{\mathcal{B}^\vee} = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 2^{s+1} \end{pmatrix}.$$

In order to state the analogue of Proposition 1.2.8, using Hensel's lemma take $\mu_1, \dots, \mu_6 \in \mathcal{O}_2$ satisfying:

- $\mu_1^2 = -7$
- $3\mu_3^2 = -5$
- $3\mu_5^2 = -29$
- $3\mu_2^2 = -13$
- $\mu_4^2 = -15$
- $3\mu_6^2 = -533.$

Proposition 1.5.5. *Let R_2 be an order corresponding to a form f from Table 1.6, and let $\{1, e_1, e_2, e_3\}$ be a good basis for R_2. Let g be a form beneath f, and let d_1, d_2, d_3 be as in Table 1.7.*

Then, $R_2' = \langle 1, d_1, d_2, d_3 \rangle_{\mathcal{O}_2}$ is a maximal suborder of R_2 in correspondence with the form g, of which $\{1, d_1, d_2, d_3\}$ is a good basis.

Proof. All the cases can be easily checked. Many of them follow from Propositions 1.5.10, 1.5.11 and 1.5.12 below (see the proof of Proposition 1.5.13). □

Form	Form beneath	Good basis for R_2'
$H \perp \langle 1 \rangle$	$J \perp \langle 4 \rangle$	$d_1 = 2(\mu_1 - 2e_1 - 3e_2 - 2\mu_1 e_3)$, $d_2 = 2(-\mu_1 + 3e_1 + 2e_2 + 2\mu_1 e_3)$, $d_3 = -2 - \mu_1 e_1 \mu_1 e_2 + 5e_3$
$H \perp \langle 2^s \rangle$	$H \perp \left\langle 2^{s+1} \right\rangle$	$d_1 = e_1, d_2 = 2e_2, d_3 = e_3$
$H \perp \langle 2 \rangle$	$\langle 1, 1, 3 \rangle$	$d_1 = \mu_1 - e_1 + 2e_2 - 2\mu_1 e_3$, $d_2 = -5 + 2\mu_1 e_1 + \mu_1 e_2 + 10e_3$, $d_3 = \mu_1 + 3e_1 + e_2 - 2\mu_1 e_3$
$J \perp \langle 2^s \rangle$	$J \perp \left\langle 2^{s+2} \right\rangle$	$d_1 = 2e_1, d_2 = 2e_2, d_3 = e_3$
$J \perp \langle 2 \rangle$	$\langle 1, 1, 1 \rangle$	$d_1 = \mu_2 - e_1 + 2e_2 - 2\mu_2 e_3$, $d_2 = \mu_2 - 2e_1 + e_2 - 2\mu_2 e_3$, $d_3 = -3 - \mu_2 e_1 + \mu_2 e_2 + 6e_3$
$\langle 1, 1, \delta_1 2^s \rangle$	$\left\langle 1, 1, \delta_1 2^{s+1} \right\rangle$	$d_1 = e_1 - e_2, d_2 = e_1 + e_2, d_3 = e_3$
$\langle 1, 2, \delta_2 2^s \rangle$	$\left\langle 1, 2, \delta_3 2^{s+1} \right\rangle$	$d_1 = -2e_2, d_2 = e_1, d_3 = e_3$
$\langle 1, 5, 2^s \rangle$	$\left\langle 1, 5, 3 \cdot 2^{s+1} \right\rangle$	$d_1 = e_1 - 5e_2, d_2 = e_1 + e_2, d_3 = e_3$
$\langle 1, 6, 2^s \rangle$	$\left\langle 1, 6, 3 \cdot 2^{s+1} \right\rangle$	$d_1 = -6e_2, d_2 = e_1, d_3 = e_3$
$\langle 1, 10, 2^s \rangle$	$\left\langle 1, 10, 5 \cdot 2^{s+1} \right\rangle$	$d_1 = -10e_2, d_2 = e_1, d_3 = e_3$
$\langle 1, 1, 6 \rangle$	$\langle 1, 6, 6 \rangle$	$d_1 = 6e_3, d_2 = e_2, d_3 = -e_1$
$\langle 1, 1, 2 \rangle$	$\langle 1, 6, 2 \rangle$	$d_1 = 2e_1 + 6e_3, d_2 = e_2, d_3 = 2e_3 - e_1$
$\left\langle 1, 1, 2^2 \right\rangle$	$\left\langle 1, 5, 3 \cdot 2^3 \right\rangle$	$d_1 = e_1 - 5e_2 + 4e_3, d_2 = e_1 + e_2 + 4e_3$, $d_3 = e_3 - e_1$
$\langle 1, 14, \delta_2 2^s \rangle$	$\left\langle 1, 14, \delta_2 2^{s+1} \right\rangle$	$d_1 = e_1 - 14\mu_1 e_2, d_2 = \mu_1 e_1 + e_2, d_3 = e_3$
$\langle 1, 5, 3 \cdot 2^s \rangle$	$\left\langle 1, 5, 2^{s+1} \right\rangle$	$d_1 = e_1 - 5\mu_2 e_2, d_2 = \mu_2 e_1 + e_2, d_3 = e_3$
$\langle 1, 10, 5 \cdot 2^s \rangle$	$\left\langle 1, 10, 2^{s+1} \right\rangle$	$d_1 = -2e_2, d_2 = \frac{1}{5} e_1, d_3 = e_3$
$\langle 1, 6, 3 \cdot 2^s \rangle$	$\left\langle 1, 6, 2^{s+1} \right\rangle$	$d_1 = 2e_1 - 2e_2, d_2 = \frac{1}{3} e_1 + 2e_2$, $d_2 = \frac{1}{3} e_1 + 2e_2, d_3 = e_3$
$\left\langle 1, 6, 3 \cdot 2^2 \right\rangle$	$\left\langle 1, 2, 2^3 \right\rangle$	$d_1 = 2(-\mu_3 e_2 + 2e_3), d_2 = \frac{1}{3} e_1$, $d_3 = e_2 + \mu_3 e_3$
$\left\langle 1, 2, 2^3 \right\rangle$	$\left\langle 1, 1, 2^4 \right\rangle$	$d_1 = -2e_2 + 8e_3, d_2 = e_1, d_3 = e_2 + 5e_3$
$\left\langle 1, 2, 5 \cdot 2^3 \right\rangle$	$\left\langle 1, 10, 5 \cdot 2^4 \right\rangle$	$d_1 = -2\mu_4 e_2 + 40e_3, d_2 = e_1$, $d_3 = e_2 + \mu_4 e_3$
$\left\langle 1, 6, 3 \cdot 2^3 \right\rangle$	$\left\langle 1, 14, 2^4 \right\rangle$	$d_1 = 2(-\mu_3 e_2 + 4e_3), d_2 = \frac{1}{3} e_1$, $d_3 = e_2 + \mu_3 e_3$
$\left\langle 1, 6, 2^2 \right\rangle$	$\left\langle 1, 2, 5 \cdot 2^3 \right\rangle$	$d_1 = 2(\mu_5 e_1 - 3\mu_5 e_2 - 10e_3)$, $d_2 = e_1 + 2e_2, d_3 = e_1 - 3e_2 + \mu_5 e_3$
$\left\langle 1, 6, 2^3 \right\rangle$	$\left\langle 1, 14, 5 \cdot 2^4 \right\rangle$	$d_1 = 2(\mu_5 e_1 - 3\mu_5 e_2 - 60e_3)$, $d_2 = e_1 + 2e_2, d_3 = 3e_1 - 9e_2 + \mu_5 e_3$

Table 1.7: Construction of maximal suborders, in terms of good bases and ternary quadratic forms, when $\mathfrak{p} = (2)$.

The notion of quasi-good basis remains unchanged, as well as the use of such bases for computing suborders and representatives for the quotients $(R_2')^\times \backslash R_2^\times$. We must show how to obtain quasi-good bases in this setting.

Remark 1.5.6. Proposition 1.2.14 still holds for diagonal forms, setting $n = 3v_2(a) + 2$ in order to be able to use Hensel's lemma in its proof.

Proposition 1.5.7. *Let R_2 be an order in correspondence with $f = H \perp \langle 2^s \rangle$. Let $\mathcal{E} = \{f_0, f_1, f_2, f_3\}$ be a basis of $R_2^\vee$ satisfying (1.2.2). Assume that $\mathcal{E}$ satisfies the following conditions.*

(1) There exists $\beta \in \mathcal{O}_2$ such that

$$-2^s \cdot M_{\mathcal{E}} \equiv \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & \beta \end{pmatrix} \mod (M_3(2^3 \mathcal{O}_2)).$$

(2) $\det(M_{\mathcal{E}}) = 2^{1-2s}$.

Let $e_i = -2^s \cdot f_j \bar{f}_k$, where (i,j,k) is an even permutation of $(1,2,3)$. Then, $\mathcal{E}^\dagger = \{1, e_1, e_2, e_3\}$ is a quasi-good basis of R_2.

The following lifting lemma is needed in the proof of Proposition 1.5.7, which we omit, since it is quite similar to the proof of Proposition 1.2.14.

Lemma 1.5.8. *Let m be an integer such that $m \geq 3$, and let $A \in M_3(\mathcal{O}_2)$ be a symmetric matrix. Assume that there exists $C \in GL_3(\mathcal{O}_2)$ such that*

$$C^t AC \equiv \begin{pmatrix} 0 & \alpha & 0 \\ \alpha & 0 & 0 \\ 0 & 0 & \beta \end{pmatrix} \mod (M_3(2^m \mathcal{O}_2)),$$

with $v_2(\alpha) = 0$.

Then, there exists $C' \in GL_3(\mathcal{O}_2)$ satisfying $C' \equiv C \mod (M_3(2^{m-1}\mathcal{O}_2))$ such that

$$C'^t AC' \equiv \begin{pmatrix} 0 & \alpha' & 0 \\ \alpha' & 0 & 0 \\ 0 & 0 & \beta' \end{pmatrix} \mod (M_3(2^{m+1} \mathcal{O}_2)),$$

with $\alpha' \equiv \alpha \mod (2^{m-1}\mathcal{O}_2)$.

Proof. Write

$$C^t AC = \begin{pmatrix} 0 & \alpha & 0 \\ \alpha & 0 & 0 \\ 0 & 0 & \beta \end{pmatrix} + 2^m \begin{pmatrix} a & b & c \\ b & d & e \\ c & e & f \end{pmatrix},$$

with $a, b, \ldots, f \in \mathcal{O}_2$. We claim that there exists a matrix $C_0 \in GL_3(\mathcal{O}_2)$ such that

$$C_0^t AC = \begin{pmatrix} -a & b' & c'2^m \\ d' & -d & e'2^m \\ -2c & -2e & f' \end{pmatrix},$$

with $b', c', d', e', f' \in \mathcal{O}_2$. This can be shown by performing row operations on $C^t AC$, using the $(1,2)$ and $(2,1)$ entries as pivots to first obtain zeroes at the $(1,1), (2,2), (3,1)$ and $(3,2)$ entries, and then obtain $-a, -d, -2c$ and $-2e$ at the $(1,1), (2,2), (3,1)$ and $(3,2)$ entries respectively.

Now let $C' = C + 2^{m-1}C_0$. Then,

$$C'^t AC' = \begin{pmatrix} 0 & \alpha' & c'2^{2m-1} \\ \alpha' & 0 & e'2^{2m-1} \\ c'2^{2m-1} & e'2^{2m-1} & \beta' \end{pmatrix} + 2^{2(m-1)} C_0^t AC_0.$$

where $\alpha' = \alpha + 2^{m-1}(b' + d')$. Since $2(m-1) \geq m+1$, we are done. □

For orders of class A2 we only state the corresponding analogue of Proposition 1.5.7.

Proposition 1.5.9. *Let R_2 be an order in correspondence with $f = J \perp \langle 2^s \rangle$. Let $\mathcal{E} = \{f_0, f_1, f_2, f_3\}$ be a basis of $R_2^\vee$ satisfying (1.2.2). Assume that $\mathcal{E}$ satisfies the following conditions.*

(1) There exists $\beta \in \mathcal{O}_2$ such that

$$2^s 3 \cdot M_{\mathcal{E}} \equiv \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & \beta \end{pmatrix} \mod (M_3(2^3 \mathcal{O}_2)).$$

(2) $\det(M_{\mathcal{E}}) = 2^{1-2s}3^{-2}$.

Let $e_i = 2^s 3 \cdot f_j \bar{f}_k$, where (i,j,k) is an even permutation of $(1,2,3)$. Then, $\mathcal{E}^\dagger = \{1, e_1, e_2, e_3\}$ is a quasi-good basis of R_2.

Finally, we proceed to give systems of representatives for the quotient sets $(R_2')^\times \backslash R_2^\times$ when R_2' is a maximal suborder of R_2 obtained using Algorithm 1.2.19. We start stating three general results which, though stated and used only when $\mathfrak{p} = (2)$, hold without restrictions on $\mathfrak{p}$.

Let $\mathcal{B} = \{1, e_1, e_2, e_3\}$ be a good basis for R_2. Let q be the order of the residue field $\mathbb{F}_{(2)}$, and let $a_1, a_2, \ldots, a_q \in \mathcal{O}_2$ be a set of representatives for $\mathbb{F}_{(2)}$.

Proposition 1.5.10. *Suppose that R_2 is in correspondence with the form $f = \langle 1, a, b\rangle$, and let $\lambda \in \mathcal{O}_2$. Assume that there exist $\alpha_0, \alpha_3 \in \mathcal{O}_2$ such that $\alpha_0^2 + a\alpha_3^2 = \lambda$. Let $v = \alpha_0 + \alpha_3 e_3$, and let $d_1 = ve_1, d_2 = ve_2, d_3 = e_3$.*

Then, $R_2' = \langle 1, d_1, d_2, d_3\rangle_{\mathcal{O}_2}$ is a suborder of R_2 in correspondence with the form $g = \langle 1, a, \lambda b\rangle$, of which $\{1, d_1, d_2, d_3\}$ is a good basis. Furthermore, if $v_2(\lambda) = 1$ and $v_2(b) \geq 1$, then R_2' is a maximal suborder of R_2, the index of $(R_2')^\times$ in $R_2^\times$ is q, and a set of representatives for the set $(R_2')^\times \backslash R_2^\times$ is given by $\{1 + a_i e_2 : 1 \leq i \leq q\}$.

Proof. The first assertion is easily checked. We use Proposition 1.3.10 to prove the second assertion. Since $v_2(b) \geq 1$, by (1.2.4) the norm form on $2R_2 \backslash R_2$ is given by $N(x) = x_0^2 + ax_3^2$. Hence, $|(2R_2 \backslash R_2)^\times| = c \cdot q^2$, where $c = \#\{(x_0, x_3) \in {\mathbb{F}_{(2)}}^2 : x_0^2 + ax_3^2 \neq 0\}$.

We have that

$$2R_2 \backslash R_2' = \left\{x \in 2R_2 \backslash R_2 : x_0, x_3 \in \mathbb{F}_{(2)}, (x_1, x_2) \in A \cdot {\mathbb{F}_{(2)}}^2\right\},$$

where $A = \left(\begin{smallmatrix} \alpha_0 & \alpha_3 \\ -\alpha_3 & \alpha_0 \end{smallmatrix}\right)$. Since $\alpha_0^2 + a\alpha_3^2 = \lambda$ and $v_2(\lambda) = 1$, this matrix has rank 1. Hence, $|(2R_2 \backslash R_2')^\times| = c \cdot q$, which shows that $[R_2^\times : (R_2')^\times] = q$.

To see that the given units are not equivalent, take $x \in (2R_2 \backslash R_2')^\times$. Then, it is easy to see that

$$(1 + a_i e_2)x = x_0 + (x_1 - a_i x_2 x_3)e_1 + (a_i x_0 + x_2)e_2 + x_3 e_3 = 1 + a_j e_2$$

implies that $i = j$.

□

The next two results can be proved following the same ideas as the ones used above.

Proposition 1.5.11. *Suppose that R_2 is in correspondence with the form $f = \langle 1, a, b\rangle$, and let $\mu \in \mathcal{O}_2$. Assume that there exist $\alpha_0, \alpha_2 \in \mathcal{O}_2$ such that $\alpha_0^2 + b\alpha_2^2 = \mu$. Let $v = \alpha_0 + \alpha_2 e_2$, and let $d_1 = ve_1, d_2 = e_2, d_3 = ve_3$.*

Then, $R_2' = \langle 1, d_1, d_2, d_3\rangle_{\mathcal{O}_2}$ is a suborder of R_2 in correspondence with the form $g = \langle 1, \mu a, b\rangle$, of which $\{1, d_1, d_2, d_3\}$ is a good basis. Furthermore, if $v_2(\mu) = 1$ and $v_2(b) \geq 1$, then R_2' is a maximal suborder of R_2, the index of $(R_2')^\times$ in $R_2^\times$ is q, and a set of representatives for the set $(R_2')^\times \backslash R_2^\times$ is given by $\{1 + a_i e_3 : 1 \leq i \leq q\}$.

Proposition 1.5.12. *Suppose that R_2 is in correspondence with the form $f = \langle 1, a, b\rangle$. Let $a', b' \in \mathcal{O}_2$. Assume that there exist $\alpha_1, \alpha_2, \alpha_3 \in \mathcal{O}_2$ such that $ab\alpha_1^2 = b'$, and $a\alpha_3^2 + b\alpha_2^2 = a'$. Let $d_2 = \alpha_1 e_1, d_3 = \alpha_2 e_2 + \alpha_3 e_3, d_1 = d_3 d_2$.*

Then, $R_2' = \langle 1, d_1, d_2, d_3\rangle_{\mathcal{O}_2}$ is a suborder of R_2 in correspondence with the form $g = \langle 1, a', b'\rangle$, of which $\{1, d_1, d_2, d_3\}$ is a good basis. Furthermore, if $v_2(b') = v_2(b) + 1, v_2(a) = v_2(a') = 1$ and $v_2(b) \geq 1$, then R_2' is a maximal suborder of R_2, the index of $(R_2')^\times$ in $R_2^\times$ is q, and a set of representatives for the set $(R_2')^\times \backslash R_2^\times$ is given by $\{1 + a_i e_3 : 1 \leq i \leq q\}$.

Assume that the given system of representatives for $\mathbb{F}_{(2)}$ is such that $a_1 = 1$, and that a_{q-1} and a_q are the two solutions in $\mathbb{F}_{(2)}$ of $t^2 + t + 1 = 0$, when $q = 2^s$ with even s.

Proposition 1.5.13. *Let $\mathcal{B} = \{1, e_1, e_2, e_3\}$ be a quasi-good basis of R_2, and assume that R_2' is a maximal suborder of R_2 that has been built using Algorithm 1.2.19. Then, Table 1.8 gives the index of $(R_2')^\times$ in $R_2^\times$ and a system of representatives for the quotient set.*

Proof. As in the $\mathfrak{p} \nmid (2)$ case, by Proposition 1.3.10, we may assume that $\mathcal{B}$ is a good basis for R_2, as well as we may perform all calculations modulo $2R_2$.

R_2-class	R_2'-class	$[R_2^\times : (R_2')^\times]$	Representatives	Condition
A1	A1	$q+1$	$e_1+e_2, 1+a_ie_2 \quad (1 \leq i \leq q)$	$s=0$
		q	$1+a_ie_2 \quad (1 \leq i \leq q)$	$s \geq 1$
	A2	$q(q-1)$	$(1+a_ie_2)(e_1+a_je_2) \quad (1 \leq i,j \leq q, a_j \neq 0)$	s odd
		$q(q+1)$	$(1+a_ie_2)(e_1+a_je_2) \quad (1 \leq i,j \leq q, a_j \neq 0)$, $(1+a_ie_2)(a_j+e_1) \quad (1 \leq i \leq q, q-2 \leq j \leq q)$	s even
	B	$q-1$	$1+a_ie_2 \quad (1 < i \leq q)$	
A2	A2	q^2	$1+a_ie_1+a_je_2 \quad (1 \leq i,j \leq q)$	
	B	$q-1$	$e_3, 1+a_ie_3 \quad (1 \leq i \leq q-2)$	s even
		$q+1$	$e_3, 1+a_ie_3 \quad (1 \leq i \leq q)$	s odd
B	B	q	$e_2, 1+a_ie_2 \quad (1 < i \leq q)$	$s=0$
			$1+a_ie_2 \quad (1 \leq i \leq q)$	$s \geq 1$
	C	q	$1+a_ie_3 \quad (1 \leq i \leq q)$	
	D	q	$1+a_ie_2 \quad (1 \leq i \leq q)$	
C	C	q	$1, a_i+e_2 \quad (1 \leq i \leq q)$	
	E	q	$1, a_i+e_2 \quad (1 \leq i \leq)$	$\delta_1 = 1$
			$1, a_i+e_3 \quad (1 \leq i \leq q)$	$\delta_1 = 3$
	F	q	$1, a_i+e_2 \quad (1 \leq i \leq q)$	$\delta_1 = 1$
			$1, a_i+e_3 \quad (1 \leq i \leq q)$	$\delta_1 = 3$
D	D	q	$1, a_i+e_2 \quad (1 \leq i \leq q)$	
E	E	q	$1, a_i+e_2 \quad (1 \leq i \leq q)$	
	G	q	$1, a_i+e_3 \quad (1 \leq i \leq q)$	
F	F	q	$1, a_i+e_2 \quad (1 \leq i \leq q)$	
G	G	q	$1, a_i+e_2 \quad (1 \leq i \leq q)$	

Table 1.8: The indexes $[R_2^\times : (R_2')^\times]$, and representatives for $(R_2')^\times \backslash R_2^\times$.

The cases B to B, C to C, D to D, E to E, F to F and G to G are covered by Proposition 1.5.10. The case B to C is covered by Proposition 1.5.11.

To prove the case B to D, use Proposition 1.5.11 to descend from $\langle 1, 1, 2^2 \rangle$ to $\langle 1, 5, 2^2 \rangle$, and Proposition 1.5.10 to descend from this form to $\langle 1, 5, 3 \cdot 2^3 \rangle$. A similar argument works for the other form of class B.

The cases C to E (with $\delta_1 = 3$), C to F (with $\delta_1 = 3$) and E to G are covered by Proposition 1.5.12.

Now we will prove the case from A2 to B. The remaining cases can be treated in a similar way, with no further difficulties.

By (1.5.3), the norm form on $2R_2 \backslash R_2$ is given by $N(x) = x_0^2 + x_0x_3 + x_3^2$. Hence, a standard calculation shows that

$$|(2R_2 \backslash R_2)^\times| = \begin{cases} q^4 - q^2(2q-1), & \text{if } r \text{ is even,} \\ q^4 - q^2, & \text{if } r \text{ is odd.} \end{cases}$$

Since $d_1 = 1+e_1, d_2 = 1+e_2$ and $d_3 = 1+e_1+e_2$ in $2R_2 \backslash R_2$, we have that $2R_2 \backslash R_2' = \langle 1, e_1, e_2 \rangle_{\mathbb{F}_{(2)}}$. Hence $|(2R_2 \backslash R_2)^\times| = q^3 - q^2$, and this proves the equality on $[R_2^\times : (R_2')^\times]$.

Now we need to find the right amount of non equivalent units. It is easily seen that the elements in the set $\{1 + a_ie_3 : 1 \leq i \leq q\} \cup \{e_3\}$ are not mutually equivalent modulo $(2R_2 \backslash R_2)^\times$, and they are all units, except for $1 + a_{q-1}e_3$ and $1 + a_qe_3$ when $q = 2^s$ with even s.

□

Chapter 2

Preimages for the Shimura map on Hilbert modular forms

Summary

We start this chapter by recalling some basic facts about Hilbert modular forms, including their correspondence with automorphic forms. Some good references for the theory of Hilbert modular forms are Garrett's book [Gar90] and Gebhardt's dissertation [Geb09], and of course Shimura's article [Shi78].

In the second section, given a totally definite quaternion algebra B and an Eichler order $R \subseteq B$, we define Hecke operators acting on the vector space $M(R)$ generated by left ideal classes representatives for R. We state the main properties of these operators showing that, away from the discriminant of the order, they satisfy the same relations as the Hecke operators on Hilbert modular forms. We recall a Jacquet-Langlands-type result that assures that, under certain hypotheses, for every Hilbert modular newform there is a vector in $M(R)$ having the same eigenvalues for the Hecke operators, if we choose B and R appropriately.

In the third section we introduce half-integral weight Hilbert modular forms, following [Shi87]. We state the main properties of the Hecke operators acting on them, and we recall Shimura's theorem giving a Hecke linear map from the space of Hilbert modular forms of parallel weight $3/2$ to the space of Hilbert modular forms of parallel weight 2.

In the fourth section we show how certain ternary theta series associated to the left ideal classes of a given order R can be used to produce Hilbert modular forms of parallel weight $3/2$. This construction actually gives a Hecke linear map from the space $M(R)$ to the space of Hilbert modular forms of parallel weight $3/2$ (see Theorem 2.4.11).

In the fifth section we show how the results of the previous sections can be used to construct preimages of the Shimura map, at least in the case where the level of the modular form is odd and square-free. This is stated in Theorem 2.5.3, which is our main result. We also state a Waldspurger's type formula by Baruch and Mao, which relates the Fourier coefficients of the preimages and central values of twisted L-functions.

In the final section we consider the space of Hilbert modular cusp forms over $F = \mathbb{Q}[\sqrt{5}]$, with level $(6+\sqrt{5})$ and parallel weight 2. This space is 1-dimensional, and it is spanned by a newform that corresponds to an elliptic E curve over F. We apply our method to this cusp form to construct a parallel weight $3/2$ modular form in Shimura correspondence with it, and compare its zero coefficients with the ranks of imaginary quadratic twists of E.

We remark that though for simplicity we consider the Shimura correspondence in parallel weights $3/2$ and 2, our techniques can be used for general weights, adding spherical polynomials to the ternary theta series. This is work in progress.

2.1 Hilbert modular forms

Let F be a totally real number field of degree d over $\mathbb{Q}$, with different ideal $\mathfrak{d}$. We let $\mathbf{a}$ denote the set of all embeddings $\tau : F \hookrightarrow \mathbb{R}$, and for $\xi \in F$ and $\tau \in \mathbf{a}$, we denote $\tau(\xi) = \xi_\tau$. We let

$$F^+ = \{\xi \in F^\times : \xi_\tau > 0 \quad \forall \tau \in \mathbf{a}\},$$

the subgroup of *totally positive* elements of $F^\times$.

We denote by $F_\mathbb{A}$ the ring of adeles of F, and by $F_\mathbb{A}^\times$ the group of ideles of F. We let $F_\mathbf{a}$ and $F_\mathbf{f}$ denote respectively the archimedean and the non-archimedean parts of $F_\mathbb{A}$.

Let G denote the group scheme SL_2 and $\tilde{G}$ the group scheme GL_2, both over F. Also, let

$$\tilde{G}^+(F) = \{\gamma \in \tilde{G}(F) : \det \gamma \in F^+\}.$$

Let $\mathcal{H}$ denote the Poincaré upper-half plane. Then $\mathrm{GL}_2^+(\mathbb{R})^\mathbf{a}$ acts on $\mathcal{H}^\mathbf{a}$ component-wise, and $\tilde{G}^+(F)$ also acts on $\mathcal{H}^\mathbf{a}$ via the natural embedding $\tilde{G}^+(F) \hookrightarrow \mathrm{GL}_2^+(\mathbb{R})^\mathbf{a}$. If $\gamma \in \mathrm{GL}_2^+(\mathbb{R})^\mathbf{a}$, with $\gamma_\tau = \left(\begin{smallmatrix} a_\tau & b_\tau \\ c_\tau & d_\tau \end{smallmatrix}\right)$, we let $j(\gamma, z)$ denote the automorphy factor

$$j(\gamma, z) = \prod_{\tau \in \mathbf{a}} (c_\tau z_\tau + d_\tau).$$

Again, this also makes sense for $\gamma \in \tilde{G}^+(F)$. Given a function $g : \mathcal{H}^\mathbf{a} \to \mathbb{C}$ and $\gamma \in \tilde{G}^+(F)$, we denote by $g|\gamma$ the function given by $(g|\gamma)(z) = N_{F/\mathbb{Q}}(\det \gamma) j(\gamma, z)^{-2} g(\gamma z)$.

Let $\tilde{\Gamma} \subseteq \tilde{G}^+(F)$ be a congruence subgroup (we will consider only certain congruence subgroups defined below, see [Shi78, page 639] for a general definition). The space of Hilbert modular forms of weight $\mathbf{2}$ (also called parallel weight 2) with respect to $\tilde{\Gamma}$, which we denote by $M_\mathbf{2}(\tilde{\Gamma})$, is the space of holomorphic functions $g : \mathcal{H}^\mathbf{a} \to \mathbb{C}$ such that

- $g|\gamma = g \quad \forall\, \gamma \in \tilde{\Gamma}$.
- If $d = 1$, $g(z)$ is holomorphic at the cusps.

The holomorphicity condition at the cusps is automatic for totally real fields other than $\mathbb{Q}$. This is the so called Koecher principle. See [Gar90, Section 1.4] for a proof.

Let $\mathcal{O}_F$ be the ring of integers of F. We denote $\mathcal{O}_F$ by $\mathcal{O}$ when there is no chance of confussion. Given fractional ideals $\mathfrak{r}, \mathfrak{n}$, we will be mainly interested in the groups

$$\begin{aligned}
&\tilde{\Gamma}[\mathfrak{r}, \mathfrak{n}] = \left\{\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \tilde{G}^+(F) : a, d \in \mathcal{O}, b \in \mathfrak{r}^{-1}, c \in \mathfrak{r}\mathfrak{n}, \det \gamma \in \mathcal{O}^\times\right\}, \\
&\Gamma[\mathfrak{r}, \mathfrak{n}] = G(F) \cap \tilde{\Gamma}[\mathfrak{r}, \mathfrak{n}].
\end{aligned}$$

Let $e_F : F \times \mathcal{H}^\mathbf{a} \to \mathbb{C}$ be the exponential function given by

$$e_F(\xi, z) = \exp\left(2\pi i \sum_{\tau \in \mathbf{a}} \xi_\tau z_\tau\right).$$

For a fractional ideal $\mathfrak{a}$, let $\mathfrak{a}^+ = \mathfrak{a} \cap F^+$, and denote by $\mathfrak{a}^\vee$ its dual with respect to the trace form. If $g \in M_\mathbf{2}(\tilde{\Gamma}[\mathfrak{r}, \mathfrak{n}])$, since $g(z + \xi) = g(z)$ for every $\xi \in \mathfrak{r}^{-1}$ (where we denote $z + \xi = (z_\tau + \xi_\tau)_\tau \in \mathcal{H}^\mathbf{a}$), the form g has a Fourier series expansion

$$g(z) = \sum_{\xi \in ((\mathfrak{r}^{-1})^\vee)^+ \cup \{0\}} c(\xi, g) e_F(\xi, z).$$

We say that g is *cuspidal* if $c(0, g|\gamma) = 0$ for all $\gamma \in \tilde{G}^+(F)$. The subspace of such g is denoted by $S_\mathbf{2}(\tilde{\Gamma}[\mathfrak{r}, \mathfrak{n}])$.

For a fractional ideal $\mathfrak{a}$, denote by $[\mathfrak{a}]$ its class in the narrow class group $Cl^+(F)$. Take $\mathfrak{b}_1, \ldots, \mathfrak{b}_r \subseteq \mathcal{O}$ representatives for $Cl^+(F)$, which we fix from now on. Let $\mathfrak{c}$ be an integral ideal. The spaces of *Hilbert modular forms* and *Hilbert modular cusp forms* of level $\mathfrak{c}$ are defined respectively by

$$M_\mathbf{2}(\mathfrak{c}) = \bigoplus_{l=1}^{r} M_\mathbf{2}(\tilde{\Gamma}[\mathfrak{b}_l, \mathfrak{c}]), \quad S_\mathbf{2}(\mathfrak{c}) = \bigoplus_{l=1}^{r} S_\mathbf{2}(\tilde{\Gamma}[\mathfrak{b}_l, \mathfrak{c}]).$$

Since for any $\xi \in F^+$ the group $\tilde{\Gamma}[\mathfrak{b}_l, \mathfrak{c}]$ is conjugate over $\tilde{G}^+(F)$ to the group $\tilde{\Gamma}[\xi\mathfrak{b}_l, \mathfrak{n}]$, the spaces $M_{\mathbf{2}}(\mathfrak{c})$ and $S_{\mathbf{2}}(\mathfrak{c})$, in certain sense, do not depend on the representatives $\mathfrak{b}_l$ chosen.

We now consider Hilbert modular forms from the automorphic point of view. Let $t_l \in F_{\mathbf{f}}^\times$ be such that the fractional ideal corresponding to t_l is $\mathfrak{b}_l$. Let $\hat{\mathcal{O}}^\times = \prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^\times$, where the subscript $\mathfrak{p}$ as usual denotes the completion at $\mathfrak{p}$, and let $F_{\mathbf{a}}^+ \subseteq F_{\mathbf{a}}^\times$ denote the connected component of the identity. Right from the definition of $Cl^+(F)$ we get the decomposition

$$F_{\mathbb{A}}^\times = \bigsqcup_{l=1}^{r} F^\times t_l \; (F_{\mathbf{a}}^+ \times \hat{\mathcal{O}}^\times). \tag{2.1.1}$$

Strong approximation for G asserts that $G(F)\,\mathrm{SL}_2(\mathbb{R})^{\mathbf{a}}$ is dense in $G(F_{\mathbb{A}})$ (see [Pra77]). This implies that if K is an open, compact subgroup of $\tilde{G}(F_{\mathbf{f}})$, then the natural map

$$\tilde{G}(F)\backslash\tilde{G}(F_{\mathbb{A}})/(\mathrm{GL}_2^+(\mathbb{R})^{\mathbf{a}} \times K) \longrightarrow F^\times\backslash F_{\mathbb{A}}^\times/(F_{\mathbf{a}}^+ \times \det(K))$$

is a bijection. This fact together with decomposition (2.1.1) gives the following theorem.

Theorem 2.1.2. *Let K be an open, compact subgroup of $\tilde{G}(F_{\mathbf{f}})$. If $\det(K) = \hat{\mathcal{O}}^\times$, then*

$$\tilde{G}(F_{\mathbb{A}}) = \bigsqcup_{l=1}^{r} \tilde{G}(F) \left(\begin{smallmatrix} 1 & 0 \\ 0 & t_l \end{smallmatrix}\right) (\mathrm{GL}_2^+(\mathbb{R})^{\mathbf{a}} \times K).$$

Let $K_0(\mathfrak{c}) \subseteq \tilde{G}(F_{\mathbf{f}})$ denote the open, compact subgroup given by

$$K_0(\mathfrak{c}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \prod_{\mathfrak{p}} \mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}}) : c_{\mathfrak{p}} \in \mathfrak{c}_{\mathfrak{p}} \,\forall\, \mathfrak{p} \right\}.$$

It certainly satisfies that $\det(K_0(\mathfrak{c})) = \hat{\mathcal{O}}^\times$.

Definition. *A map $\phi : \tilde{G}(F_{\mathbb{A}}) \to \mathbb{C}$ is a* Hilbert automorphic form *of weight* **2** *for $K_0(\mathfrak{c})$ if it satisfies*

(H.1) $\phi(\gamma x) = \phi(x)$ for all $\gamma \in \tilde{G}(F)$.

(H.2) Consider the diagonal embedding $F_{\mathbf{a}}^+ \hookrightarrow \mathrm{GL}_2^+(\mathbb{R})^{\mathbf{a}}$. Then, $\phi(tx) = \phi(x)$ for all $t \in F_{\mathbf{a}}^+$.

(H.3) For $\theta \in \mathbb{R}^{\mathbf{a}}$, let $r(\theta) = \begin{pmatrix} \cos(\theta_\tau) & -\sin(\theta_\tau) \\ \sin(\theta_\tau) & \cos(\theta_\tau) \end{pmatrix}_\tau \in \mathrm{SO}_2(\mathbb{R})^{\mathbf{a}}$. Then,

$$\phi(xr(\theta)k) = e^{-2i\sum_{\tau\in\mathbf{a}}\theta_\tau}\phi(x), \quad \forall\, r(\theta) \in \mathrm{SO}_2(\mathbb{R})^{\mathbf{a}}, k \in K_0(\mathfrak{c}).$$

(H.4) ϕ is "slowly increasing".

(H.5) As a function of $\mathrm{GL}_2(\mathbb{R})^{\mathbf{a}}$, ϕ is smooth.

(H.6) ϕ is an eigenfunction of the Casimir operator Δ_τ, with eigenvalue 0, for all $\tau \in \mathbf{a}$.

We say that ϕ is cuspidal *if it also satisfies*

(H.7) $\int_{F_{\mathbb{A}}/F} \phi\left(\left(\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right) x\right)\, dy = 0$ for almost every $y \in \tilde{G}(F_{\mathbb{A}})$.

Implicit in (H.2) and (H.3) lays the fact that we only consider forms with trivial character, which are enough for our purposes. For a precise statement of (H.4) and (H.6), we refer to [Gel75] (Chapter 2 and section C of Chapter 3); see also [Geb09, Chapter 2]. We remark that if ϕ is cuspidal, then $|\phi| \in L^2(F_{\mathbb{A}}^\times \tilde{G}(F)\backslash\tilde{G}(F_{\mathbb{A}}))$.

Denote $\mathbf{i} = (i, \ldots, i) \in \mathcal{H}^{\mathbf{a}}$. Then $\mathrm{GL}_2^+(\mathbb{R})^{\mathbf{a}}$ acts transitively on $\mathcal{H}^{\mathbf{a}}$, with the stabilizer of $\mathbf{i}$ being $\mathrm{SO}_2(\mathbb{R})^{\mathbf{a}}$. Using this it is not hard to prove part of the following result (we refer to [Gel75, Proposition 3.1] or [Geb09, Theorem 2.3.7]).

Theorem 2.1.3. *Let ϕ be a Hilbert automorphic form of weight $\mathbf{2}$ for $K_0(\mathfrak{c})$. For $l = 1, \ldots, r$ let $g_l : \mathcal{H}^{\mathbf{a}} \to \mathbb{C}$ be given by*

$$g_l(z) = j(x_{\mathbf{a}}, \mathbf{i})^2 \phi\left(\left(\begin{smallmatrix} 1 & 0 \\ 0 & t_l \end{smallmatrix}\right) x_{\mathbf{a}}\right),$$

where $x_{\mathbf{a}} \in \mathrm{GL}_2^+(\mathbb{R})^{\mathbf{a}}$ is any element satisfying $x_{\mathbf{a}}\mathbf{i} = z$. Then $g_l \in M_{\mathbf{2}}(\tilde{\Gamma}[\mathfrak{b}_l, \mathfrak{c}])$. Furthermore, g_l is a cusp form if ϕ is a cusp form.

Conversely, given $g_l \in M_{\mathbf{2}}(\tilde{\Gamma}[\mathfrak{b}_l, \mathfrak{c}])$ for $l = 1, \ldots, r$, using Theorem 2.1.2 define $\phi : \tilde{G}(F_{\mathbb{A}}) \to \mathbb{C}$ by

$$\phi\left(\gamma \left(\begin{smallmatrix} 1 & 0 \\ 0 & t_l \end{smallmatrix}\right) x_{\mathbf{a}} k_0\right) = j(x_{\mathbf{a}}, \mathbf{i})^{-2} g_l(x_{\mathbf{a}}\mathbf{i}), \text{ for } \gamma \in \tilde{G}(F), x_{\mathbf{a}} \in \mathrm{GL}_2^+(\mathbb{R})^{\mathbf{a}}, k_0 \in K_0(\mathfrak{c}).$$

Then ϕ is an automorphic Hilbert modular form of weight $\mathbf{2}$ for $K_0(\mathfrak{c})$. Furthermore, ϕ is a cusp form if every g_l is a cusp form.

This theorem says there is a bijection between $M_{\mathbf{2}}(\mathfrak{c})$ and the space of automorphic Hilbert modular forms for $K_0(\mathfrak{c})$. This isomorphism depends on the particular choice of representatives $\mathfrak{b}_l$, but the space of automorphic Hilbert modular forms for $K_0(\mathfrak{c})$ does not. In particular, if $r = 1$ we have a bijection between Hilbert modular forms for $\tilde{\Gamma}[\mathcal{O}, \mathfrak{c}]$ and automorphic Hilbert modular forms for $K_0(\mathfrak{c})$, as in the rational case.

To every $g \in M_{\mathbf{2}}(\mathfrak{c})$ we can associate a "q-expansion" indexed by integral ideals. Letting $\left(\begin{smallmatrix} \epsilon & 0 \\ 0 & 1 \end{smallmatrix}\right)$ act on g_l, with $\epsilon \in \mathcal{O}_+^\times = \mathcal{O}^\times \cap F^+$, it is easy to see that $c(\xi, g_l)$ depends only on $\xi\mathcal{O}$. Then given a non-zero integral ideal $\mathfrak{m}$, we let

$$c(\mathfrak{m}, g) = c(\xi, g_l), \quad \text{with } \xi \in \mathfrak{b}_l^+ \text{ such that } \mathfrak{m} = \xi\mathfrak{b}_l^{-1},$$

and this is well defined. These Fourier coefficients can be obtained in terms of the automorphic form corresponding to g, and do not depend on the representatives $\mathfrak{b}_l$ chosen. In terms of these Fourier coefficients we define the *L-series* associated to g, which is given by

$$L(g, s) = \sum_{\mathfrak{m} \subseteq \mathcal{O}} c(\mathfrak{m}, g) N(\mathfrak{m})^{-s}.$$

The action of the Hecke operators $T_{\mathfrak{p}}$ on $M_{\mathbf{2}}(\mathfrak{c})$ is naturally defined in the adelic setting, for which we refer to [Shi78]. This action is such that if $g_l \in M_{\mathbf{2}}(\tilde{\Gamma}[\mathfrak{b}_l, \mathfrak{c}])$, then $T_{\mathfrak{p}}(g_l) \in M_{\mathbf{2}}(\tilde{\Gamma}[\mathfrak{b}_{l'}, \mathfrak{c}])$, where l' is such that $[\mathfrak{p}\mathfrak{b}_l] = [\mathfrak{b}_{l'}]$. Note in particular that the Hecke operators do not preserve the spaces $M_{\mathbf{2}}(\tilde{\Gamma}[\mathfrak{b}_l, \mathfrak{c}])$, which explains why we need to consider r-tuples as above. We give the description of the action of the Hecke operators on Fourier coefficients (see [Shi78, (2.20)]).

Proposition 2.1.4. *Let $g \in M_{\mathbf{2}}(\mathfrak{c})$, and let $\mathfrak{p}$ be a prime not dividing $\mathfrak{c}$. Then, for every integral ideal $\mathfrak{m}$*

$$c(\mathfrak{m}, T_{\mathfrak{p}}g) = N(\mathfrak{p})c(\mathfrak{p}\mathfrak{m}, g) + c(\mathfrak{m}\mathfrak{p}^{-1}, g),$$

where we set $c(\mathfrak{m}\mathfrak{p}^{-1}, g) = 0$ if $\mathfrak{p} \nmid \mathfrak{m}$.

We denote by $\mathbb{T}$ the algebra generated by all of the Hecke operators, and by $\mathbb{T}_0$ the algebra generated by the Hecke operators $T_{\mathfrak{p}}$ with $\mathfrak{p} \nmid \mathfrak{c}$. The operators in $\mathbb{T}_0$ are self-adjoint with respect to the Petersson inner product on $S_{\mathbf{2}}(\mathfrak{c})$, which in the automorphic setting is given by the inner product of $L^2(F_{\mathbb{A}}^\times \tilde{G}(F) \backslash \tilde{G}(F_{\mathbb{A}}))$. See [Shi78, Proposition 2.4].

The *old* subspace of $S_{\mathbf{2}}(\mathfrak{c})$, which we define in the adelic setting, is the space generated by the functions $x \mapsto \phi(x \left(\begin{smallmatrix} t^{-1} & 0 \\ 0 & 1 \end{smallmatrix}\right))$, with ϕ an automorphic cusp form of level $\mathfrak{b}$ with $\mathfrak{b} \mid \mathfrak{c}, \mathfrak{b} \neq \mathfrak{c}$, and $t \in F_{\mathbb{A}}^\times$ such that the ideal corresponding to t divides $\mathfrak{b}^{-1}\mathfrak{c}$. This space is stable under the action of $\mathbb{T}_0$, and hence the same property holds for its orthogonal complement, which we denote by $S_{\mathbf{2}}^{new}(\mathfrak{c})$. The forms in $S_{\mathbf{2}}^{new}(\mathfrak{c})$ which are eigenfunctions for all the operators in $\mathbb{T}_0$ are called *newforms*.

The following is the multiplicity one theorem for (Hilbert) automorphic forms, due to Miyake (see [Miy71]).

Theorem 2.1.5. *Let g be a newform in $S_{\mathbf{2}}^{new}(\mathfrak{c})$. If $h \in S_{\mathbf{2}}(\mathfrak{c})$ is an eigenfunction for all the operators in $\mathbb{T}_0$, with the same eigenvalues as g, then h is a multiple of g.*

The space $M_{\mathbf{2}}(\mathfrak{c})$ comes also equipped with *Atkin-Lehner* involutions $W_{\mathfrak{p}}$, defined for $\mathfrak{p} \mid \mathfrak{c}$. These involutions commute, and they commute with the action of $\mathbb{T}_0$ as well. By Theorem 2.1.5, given a newform g in $S_{\mathbf{2}}^{new}(\mathfrak{c})$, for each $\mathfrak{p} \mid \mathfrak{c}$ we have that $W_{\mathfrak{p}}g = w_{\mathfrak{p}}g$ with $w_{\mathfrak{p}} \in \{1, -1\}$. Furthermore, the sign of the functional equation of the L-series associated to g equals $(-1)^d \prod_{\mathfrak{p} \mid \mathfrak{c}} w_{\mathfrak{p}}$. See [Shi78, (2.48)].

2.2 Quaternionic modular forms

We refer to Section 1.1 for the definitions and basic results concerning the arithmetic of quaternion algebras.

Let B a totally definite quaternion algebra over F, i.e. B is such that $B_\tau = B \otimes_F F_\tau$ is a ramified quaternion algebra over F_τ for every $\tau \in \mathbf{a}$. Let $\mathfrak{D}$ be an integral ideal of F. We fix an Eichler order $R \subseteq B$ of discriminant $\mathfrak{D}$, and we recall that by $\mathfrak{I}(R)$ we denote the set of invertible (i.e., locally principal) left R-ideals.

Two ideals $I, J \in \mathfrak{I}(R)$ are equivalent if there exists $x \in B^\times$ such that $I = Jx$. We denote by $[I]$ the equivalence class of I under this relation. We fix $I_1, \ldots, I_n \in \mathfrak{I}(R)$ representing the left ideals equivalence classes.

The space of *quaternionic modular forms* for R is the vector space over $\mathbb{C}$ spanned by the ideal classes $[I_1], \ldots, [I_n]$, and is denoted by $M(R)$. On $M(R)$ we consider the inner product defined by

$$\langle [I_i], [I_j] \rangle = \#\{x \in \mathcal{O}^\times \backslash B^\times : I_i x = I_j\} = \begin{cases} 0, & i \neq j, \\ [R_r(I_i)^\times : \mathcal{O}^\times], & i = j. \end{cases}$$

Here $[R_r(I_i)^\times : \mathcal{O}^\times]$ denotes the index of $\mathcal{O}^\times$ in $R_r(I_i)^\times$, which is finite due to (1.3.19).

We let $e_0 = \sum_{i=1}^n \frac{1}{\langle [I_i],[I_i] \rangle}[I_i] \in M(R)$, and we denote by $S(R)$ the orthogonal complement of $\mathbb{C}e_0$ in $M(R)$. Then $S(R) = \{v \in M(R) : \deg v = 0\}$, where $\deg : M(R) \to \mathbb{C}$ is the linear map defined by $\deg([I_i]) = 1$. We call $S(R)$ the space of *quaternionic cusp forms*.

Let $\mathfrak{m}$ be a non-zero integral ideal. For $I \in \mathfrak{I}(R)$ denote

$$t_\mathfrak{m}(I) = \{J \in \mathfrak{I}(R) : J \subseteq I, [I : J] = \mathfrak{m}^2\},$$

where $[I : J]$ denotes the index of J in I. We let $T_\mathfrak{m}$ be the $\mathfrak{m}$-th Hecke operator acting on $M(R)$, defined by

$$T_\mathfrak{m}([I]) = \sum_{J \in t_\mathfrak{m}(I)} [J].$$

These definitions of quaternionic modular forms and Hecke operators agree with the definitions given in [DV10].

There is an action of the group of fractional ideals on $\mathfrak{I}(R)$. Given a fractional ideal $\mathfrak{n}$ and $I \in \mathfrak{I}(R)$, we define $\mathfrak{n}I \in \mathfrak{I}(R)$ as the R-ideal locally given by $(\mathfrak{n}I)_\mathfrak{p} = R_\mathfrak{p}(x_\mathfrak{p}\xi_\mathfrak{p})$, if $\mathfrak{n}$ and I are locally given by $\mathfrak{n}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}\xi_\mathfrak{p}$, and $I_\mathfrak{p} = R_\mathfrak{p}x_\mathfrak{p}$, respectively. This induces an action of $Cl(F)$ on $M(R)$, which commutes with the action of the Hecke operators.

Lemma 2.2.1. *Let $\pi_\mathfrak{p}$ denote a local uniformizer at $\mathfrak{p}$. Let $x_\mathfrak{p} \in M_2(\mathcal{O}_\mathfrak{p})$ with $\pi_\mathfrak{p} \mid \det(x_\mathfrak{p})$. Then,*

$$\begin{aligned} &\# \operatorname{SL}_2(\mathcal{O}_\mathfrak{p}) \backslash \{y_\mathfrak{p} \in M_2(\mathcal{O}_\mathfrak{p}) : \det(y_\mathfrak{p}) = \pi_\mathfrak{p}, x_\mathfrak{p} y_\mathfrak{p}^{-1} \in M_2(\mathcal{O}_\mathfrak{p})\} \\ &\qquad = \begin{cases} 1, & x_\mathfrak{p} \notin \pi_\mathfrak{p} M_2(\mathcal{O}_\mathfrak{p}), \\ N(\mathfrak{p}) + 1, & x_\mathfrak{p} \in \pi_\mathfrak{p} M_2(\mathcal{O}_\mathfrak{p}). \end{cases} \end{aligned}$$

Proof. Let $q = N(\mathfrak{p})$, and let $\alpha_1, \ldots, \alpha_q \in \mathcal{O}$ be representatives for the residual classes modulo $\mathfrak{p}$. Then

$$\begin{pmatrix} \pi_\mathfrak{p} & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & \alpha_1 \\ 0 & \pi_\mathfrak{p} \end{pmatrix}, \ldots, \begin{pmatrix} 1 & \alpha_q \\ 0 & \pi_\mathfrak{p} \end{pmatrix}$$

is a system of representatives for the action of $\operatorname{SL}_2(\mathcal{O}_\mathfrak{p})$ on $\{y_\mathfrak{p} \in M_2(\mathcal{O}_\mathfrak{p}) : \det(y_\mathfrak{p}) = \pi_\mathfrak{p}\}$ by left multiplication. The result follows from the fact that, given $x_\mathfrak{p} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathcal{O}_\mathfrak{p})$,

$$x_\mathfrak{p} \begin{pmatrix} \pi_\mathfrak{p} & 0 \\ 0 & 1 \end{pmatrix}^{-1} \in M_2(\mathcal{O}_\mathfrak{p}) \iff \pi_\mathfrak{p} \mid a, \pi_\mathfrak{p} \mid c,$$

$$x_\mathfrak{p} \begin{pmatrix} 1 & \alpha \\ 0 & \pi_\mathfrak{p} \end{pmatrix}^{-1} \in M_2(\mathcal{O}_\mathfrak{p}) \iff \pi_\mathfrak{p} \mid b - \alpha a, \pi_\mathfrak{p} \mid d - \alpha c.$$

□

The Hecke operators on $M(R)$ satisfy the following equalities, which are also satisfied by the Hecke operators on Hilbert modular forms (see [Shi78, (2.12)]).

Proposition 2.2.2. *Let $\mathfrak{m}, \mathfrak{n}$ be integral ideals, and let $\mathfrak{p}$ be a prime ideal such that $\mathfrak{p} \nmid \mathfrak{D}$. The Hecke operators on $M(R)$ satisfy:*

(1) $T_{\mathfrak{m}} T_{\mathfrak{n}} = T_{\mathfrak{m}\mathfrak{n}}$, if $(\mathfrak{m} : \mathfrak{n}) = 1$.

(2) $T_{\mathfrak{p}^{k+2}} = T_{\mathfrak{p}^{k+1}} T_{\mathfrak{p}} - N(\mathfrak{p})\mathfrak{p} T_{\mathfrak{p}^k}$, for every $k \geq 0$.

(3) $T_{\mathfrak{m}} T_{\mathfrak{p}} = T_{\mathfrak{m}\mathfrak{p}} + N(\mathfrak{p})\mathfrak{p} T_{\mathfrak{m}/\mathfrak{p}}$, if $\mathfrak{p} \mid \mathfrak{m}$.

Proof. We follow the same ideas as in [PT07, Proposition 1.3], where the result is proved in the case $F = \mathbb{Q}$.

(1) Let $I \in \mathfrak{I}(R)$. If $J \in t_{\mathfrak{m}}(L)$ with $L \in t_{\mathfrak{n}}(I)$, then $J \in t_{\mathfrak{m}\mathfrak{n}}(I)$. Moreover, since $(\mathfrak{m} : \mathfrak{n}) = 1$, for every $J \in t_{\mathfrak{m}\mathfrak{n}}(I)$ there exists a unique $L \in t_{\mathfrak{n}}(I)$ such that $J \in t_{\mathfrak{m}}(L)$, namely the ideal given by $L_{\mathfrak{p}} = I_{\mathfrak{p}}$ for $\mathfrak{p} \nmid \mathfrak{n}$ and $L_{\mathfrak{p}} = J_{\mathfrak{p}}$ for $\mathfrak{p} \mid \mathfrak{n}$. Hence

$$T_{\mathfrak{m}\mathfrak{n}}([I]) = \sum_{L \in t_{\mathfrak{n}}(I)} \sum_{J \in t_{\mathfrak{m}}(L)} [J] = T_{\mathfrak{m}}(T_{\mathfrak{n}}([I])),$$

which proves that $T_{\mathfrak{m}\mathfrak{n}} = T_{\mathfrak{m}} T_{\mathfrak{n}}$.

(2) Let $J \in \mathfrak{I}(R)$. Given $I \in t_{\mathfrak{p}^{k+2}}(J)$, write $I_{\mathfrak{p}} = J_{\mathfrak{p}} x_{\mathfrak{p}}$, with $x_{\mathfrak{p}} \in R_r(J_{\mathfrak{p}})$. Then we have a bijection

$$R_r(J_{\mathfrak{p}})^{\times} \backslash \{y_{\mathfrak{p}} \in R_r(J_{\mathfrak{p}}) : v_{\mathfrak{p}}(N(y_{\mathfrak{p}})) = 1, x_{\mathfrak{p}} y_{\mathfrak{p}}^{-1} \in R_r(J_{\mathfrak{p}})\} \to \{K \in t_{\mathfrak{p}}(J) : I \in t_{\mathfrak{p}^{k+1}}(K)\},$$

assigning to each $y_{\mathfrak{p}}$ the ideal K given locally by $K_{\mathfrak{q}} = J_{\mathfrak{q}}$ for $\mathfrak{q} \neq \mathfrak{p}$ and $K_{\mathfrak{p}} = J_{\mathfrak{p}} y_{\mathfrak{p}}$. Since $\mathfrak{p} \nmid \mathfrak{D}$ we can identify $R_r(J_{\mathfrak{p}})$ with $M_2(\mathcal{O}_{\mathfrak{p}})$. By the previous lemma, these sets have one element if $x_{\mathfrak{p}} \notin \pi_{\mathfrak{p}} M_2(\mathcal{O}_{\mathfrak{p}})$, and $q + 1$ elements otherwise. Hence, we have a non-disjoint union

$$t_{\mathfrak{p}^{k+2}}(J) = \bigcup_{K \in t_{\mathfrak{p}}(J)} t_{\mathfrak{p}^{k+1}}(K).$$

If $I \in t_{\mathfrak{p}^{k+2}}(J)$ is such that $x_{\mathfrak{p}} = \pi_{\mathfrak{p}} z_{\mathfrak{p}}$ with $z_{\mathfrak{p}} \in M_2(\mathcal{O}_{\mathfrak{p}})$, then letting $I' = \mathfrak{p}^{-1} I$ we have that $I' \in t_{\mathfrak{p}^k}(J)$. Conversely, for each $I' \in t_{\mathfrak{p}^k}(J)$ we have that $I = \mathfrak{p} I' \in t_{\mathfrak{p}^{k+2}}(J)$. Using this, the equality follows easily.

(3) This follows from (1) and (2).

□

The Hecke operators are normal with respect to $\langle\, , \rangle$, but not necessarily self-adjoint if $Cl(F)$ is non trivial, as we see in Proposition 2.2.4 below.

Lemma 2.2.3. *Let $I, J \in \mathfrak{I}(R)$. Then, $I \in t_{\mathfrak{m}}(J)$ if and only if $\mathfrak{m} J \in t_{\mathfrak{m}}(I)$.*

Proof. Both statements are equivalent, so we will prove the "only if" statement. Let $I \in t_{\mathfrak{m}}(J)$. We prove that $\mathfrak{m} J \in t_{\mathfrak{m}}(I)$ by showing that this assertion holds in every completion.

Let $\mathfrak{p}$ be a prime ideal. Take $x_{\mathfrak{p}}$ in $R_r(I_{\mathfrak{p}})$ such that $I_{\mathfrak{p}} = J_{\mathfrak{p}} x_{\mathfrak{p}}$. Then, $\mathfrak{m}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}} N(x_{\mathfrak{p}})$. Since $\overline{x_{\mathfrak{p}}} \in R_r(I_{\mathfrak{p}})$, we have that $\mathfrak{m}_{\mathfrak{p}} J_{\mathfrak{p}} \subseteq J_{\mathfrak{p}} x_{\mathfrak{p}} \overline{x_{\mathfrak{p}}} \subseteq I_{\mathfrak{p}}$. Furthermore, $[I_{\mathfrak{p}} : \mathfrak{m}_{\mathfrak{p}} J_{\mathfrak{p}}] = [J_{\mathfrak{p}} : J_{\mathfrak{p}} \overline{x_{\mathfrak{p}}}] = \mathfrak{m}_{\mathfrak{p}}^2$.

□

Proposition 2.2.4. *The adjoint of $T_{\mathfrak{m}}$ with respect to $\langle\, , \rangle$ is $\mathfrak{m}^{-1} T_{\mathfrak{m}}$.*

Proof. Let $I, J \in \mathfrak{I}(R)$. Then

$$\begin{aligned}\langle [I], T_{\mathfrak{m}}([J])\rangle &= \sum_{L \in t_{\mathfrak{m}}(J)} \#\{x \in \mathcal{O}^\times \backslash B^\times : Ix = L\} = \#\{x \in \mathcal{O}^\times \backslash B^\times : Ix \in t_{\mathfrak{m}}(J)\} \\ &= \#\{x \in \mathcal{O}^\times \backslash B^\times : \mathfrak{m}J \in t_{\mathfrak{m}}(Ix)\} = \#\{x \in \mathcal{O}^\times \backslash B^\times : \mathfrak{m}Jx^{-1} \in t_{\mathfrak{m}}(I)\} \\ &= \langle T_{\mathfrak{m}}([I]), \mathfrak{m}[J]\rangle,\end{aligned}$$

where the third equality follows by the previous lemma. This proves the assertion. □

Proposition 2.2.5. *The spaces $\mathbb{C}e_0$ and $S(R)$ are preserved by the action of the Hecke operators and by the action of $Cl(F)$.*

Proof. The action of $Cl(F)$ preserves both spaces, since this action permutes the classes $[I_1], \dots, [I_n]$.

Consider the action of the Hecke operators on $S(R)$. By Proposition 2.2.2, it suffices to prove that $T_{\mathfrak{p}}(S(R)) \subseteq S(R)$ for every prime ideal $\mathfrak{p}$. Let $\mathfrak{p}$ be a prime ideal. Given $I \in \mathfrak{I}(R)$, the set $t_{\mathfrak{p}}(I)$ is in bijection with the set

$$R_{\mathfrak{p}}^\times \backslash \{x_{\mathfrak{p}} \in R_{\mathfrak{p}} : \mathcal{O}_{\mathfrak{p}} N(x_{\mathfrak{p}}) = \mathfrak{p}\mathcal{O}_{\mathfrak{p}}\},$$

and hence $\# t_{\mathfrak{p}}(I) = c$ does not depend on I. Let $v = \sum_{i=1}^n \lambda_i [I_i] \in M(R)$. Then

$$\deg(T_{\mathfrak{p}}(v)) = \sum_{i=1}^n \lambda_i \Big(\sum_{J \in t_{\mathfrak{p}}(I_i)} 1 \Big) = c \cdot \deg(v),$$

which proves that $T_{\mathfrak{p}}(v)$ is cuspidal if (and only if) v is cuspidal.

Finally, these facts together with Proposition 2.2.4 imply that e_0 is a Hecke eigenvector. □

Since the Hecke operators are commuting, normal operators, $S(R)$ has a basis of simultaneous eigenvectors for the whole Hecke algebra. However, since the operators $T_{\mathfrak{p}}$ with $\mathfrak{p} \mid \mathfrak{D}$ do not satisfy the same relations as the Hecke operators on Hilbert modular forms, we will be interested only in the algebra of operators $\mathbb{T}_0$ generated by the operators $T_{\mathfrak{p}}$ with $\mathfrak{p} \nmid \mathfrak{D}$.

The following result is a generalization of the solution to the basis problem studied by Eichler, vastly generalized by Jacquet-Langlands. See for example [Hid81, Proposition 2.12].

Theorem 2.2.6. *Let B be a quaternion algebra, and let R be an Eichler order in B of discriminant $\mathfrak{c}$. Then there is an injective map of $\mathbb{T}_0$-modules $S(R) \hookrightarrow S_2(\mathfrak{c})$, whose image contains all the newforms.*

Remark 2.2.7. Let $\mathfrak{c}$ be an integral ideal. Since every quaternion algebra is ramified at an even number of places, there exist a totally definite quaternion algebra B and an Eichler order R as in the theorem above in the following cases:

- d is even.
- d is odd and there exists a prime $\mathfrak{p}$ such that $\mathfrak{p} || \mathfrak{c}$.

In the first case we can take B to be the quaternion algebra ramified only at the archimedean places (as in the example given in Section 1.4), whereas in the second case we can take B to be the quaternion algebra ramified at the archimedean places and at $\mathfrak{p}$. Of course, other choices might be possible, as in the example given in [CS01].

In particular, such B and R exist if $\mathfrak{c}$ is square-free.

Remark 2.2.8. The conclusion from Theorem 2.2.6 that we need for our purposes is that, under certain hypotheses, given a newform $g \in S_2(\mathfrak{c})$ there exists a quaternion algebra B and an Eichler order $R \subseteq B$ such that there exists a $\mathbb{T}_0$-eigenvector $v \in S(R)$ with the same eigenvalues as g. A more precise version of Theorem 2.2.6 claims that such v exists if and only if there exists an order R of discriminant $\mathfrak{c}$ in a quaternion algebra B which is not ramified at those primes $\mathfrak{p}$ for which the automorphic representation associated to g belongs to the principal series at $\mathfrak{p}$. If the parity of the number of places at which the automorphic representation associated to g belongs to the principal series allows so, such an order can be found within the family of Bass orders considered in Chapter 1. An example in which the parity condition implies that such an order does not exist can be obtained by taking g to be the cusp form corresponding to the elliptic curve 139A, since the corresponding automorphic representation belongs to the principal series at $p = 13$.

2.3 Hilbert modular forms of half-integral weight

Classical modular forms of half-integral weight were introduced in [Shi73], which is mandatory reading as an introduction to the subject. In the Hilbert setting, they were also introduced by Shimura, in [Shi87]. We follow this article closely, though omitting and avoiding many technical details which are not relevant for our purposes.

As in the rational case, half-integral weight Hilbert modular forms are defined in terms of the theta function given by

$$\theta(z) = \sum_{\xi \in \mathcal{O}} e_F(\xi^2, z/2), \quad z \in \mathcal{H}^{\mathbf{a}}.$$

By means of this theta function we introduce the factor of automorphy J, which is given by

$$J(\gamma, z) = \left(\frac{\theta(\gamma z)}{\theta(z)}\right) j(\gamma, z) \quad \gamma \in G(F), z \in \mathcal{H}^{\mathbf{a}}.$$

This agrees with the factor of automorphy introduced (in a more technical way) by Shimura, after [Shi87, Lemma 4.3].

Let $\mathfrak{b} \subseteq \mathcal{O}$ be an ideal divisible by 4. Let ψ be a Hecke character of F with conductor dividing $\mathfrak{b}$, and denote by ψ^* the character on ideals prime to $\mathfrak{b}$ induced by ψ. For an integral ideal $\mathfrak{m}$ we denote $\psi_{\mathfrak{m}} = \prod_{\mathfrak{p}|\mathfrak{m}} \psi_{\mathfrak{p}}$. We also denote $\psi_{\mathbf{a}} = \prod_{\tau \in \mathbf{a}} \psi_\tau$.

For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G(F)$ and $f : \mathcal{H}^{\mathbf{a}} \to \mathbb{C}$, we let $(f|\gamma)(z) = \psi_{\mathfrak{b}}(a)^{-1} J(\gamma, z)^{-1} f(\gamma z)$. A *Hilbert modular form* of weight $\mathbf{3/2} = (3/2, \ldots, 3/2)$ (also called of parallel weight $3/2$), level $\mathfrak{b}$ and character ψ, is an holomorphic function f on $\mathcal{H}^{\mathbf{a}}$ satisfying

$$f|\gamma = f \quad \forall \gamma \in \Gamma[2^{-1}\mathfrak{d}, \mathfrak{b}].$$

The space of such f is denoted by $M_{\mathbf{3/2}}(\mathfrak{b}, \psi)$. It is trivial unless $\psi_{\mathbf{a}}(-1) = (-1)^d$.

This definition is slightly different from the definition used in the rational case, where the automorphy factor given by $\left(\frac{\theta(\gamma z)}{\theta(z)}\right)^3$ was used. However both definitions are equivalent. If $F = \mathbb{Q}$ and $f \in M_{\mathbf{3/2}}(N\mathbb{Z}, \psi)$, where ψ is the Hecke character induced by the Dirichlet character $\tilde{\psi}$, then $\tilde{f}(z) = f(2z)$ is a classical modular form of weight $3/2$, level N and character $\tilde{\psi} \cdot \left(\frac{-1}{*}\right)$.

In [Shi87] there are defined Hecke operators for square-free ideals $\mathfrak{m}$. Due to normalization issues, here we denote by $T_{\mathfrak{m}}$ the $\mathfrak{m}$-th Hecke operator of [Shi87] multiplied by $N(\mathfrak{m})$. These operators satisfy that $T_{\mathfrak{m}\mathfrak{n}} = T_{\mathfrak{m}} T_{\mathfrak{n}}$ for relatively prime ideals $\mathfrak{m}, \mathfrak{n}$. We warn the reader that, regardless of our normalization, the notation for the Hilbert setting is not consistent with that of [Shi73]: if $\mathfrak{p} = p\mathbb{Z}$ with p a rational prime, then our operator $T_{\mathfrak{p}}$ agrees with the operator T_{p^2} from [Shi73].

The automorphic counterpart of half-integral weight Hilbert modular forms is more involved than in the integral weight case, since the former correspond to functions on the metaplectic covering of $G(F_{\mathbb{A}})$. Note that working with unimodular matrices is enough, as opposed to the integral weight case. This is due to the fact that instead of using the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & \pi_{\mathfrak{p}}^2 \end{smallmatrix}\right)$ for defining the action of $T_{\mathfrak{p}}$ in the metaplectic covering of $G(F_{\mathbb{A}})$, the unimodular matrix $\left(\begin{smallmatrix} 1/\pi_{\mathfrak{p}} & 0 \\ 0 & \pi_{\mathfrak{p}} \end{smallmatrix}\right)$ can be used, since these matrices are conjugate.

In particular, using strong approximation over $G(F_{\mathbb{A}})$ we get that an automorphic form of half-integral weight corresponds to a single function on $\mathcal{H}^{\mathbf{a}}$, instead of the r-tuple of functions that we need to consider in the integral weight case.

Given $f \in M_{\mathbf{3/2}}(\mathfrak{b}, \psi)$, there is a Fourier series attached to each ideal class in F. More precisely, for every $\xi \in F$ and every fractional ideal $\mathfrak{m}$ there is a complex number $\lambda(\xi, \mathfrak{m}, f)$, such that

$$f(z) = \sum_{\xi \in F} \lambda(\xi, \mathcal{O}, f) e_F(\xi, z/2) \qquad \text{(the } q\text{-expansion at } \mathcal{O}\text{)},$$

and such that

$$\lambda(\xi b^2, \mathfrak{m}, f) = N_{F/\mathbb{Q}}(b)\psi_{\mathbf{a}}(b)\lambda(\xi, b\mathfrak{m}, f) \quad \forall\, b \in F^\times, \tag{2.3.1}$$

$$\lambda(\xi, \mathfrak{m}, f) = 0, \quad \text{unless } \xi \in (\mathfrak{m}^{-2})^+ \cup \{0\}. \tag{2.3.2}$$

See [Shi87, Proposition 3.1]. We say that f is a *cusp form* if $\lambda(0, \mathfrak{m}, f|\gamma) = 0$ for every fractional ideal $\mathfrak{m}$, for every $\gamma \in G(F)$. The space of such f is denoted by $S_{\mathbf{3/2}}(\mathfrak{b}, \psi)$.

Note that (2.3.1) shows that there are actually $|Cl(F)|$ Fourier series attached to f. The description of the Fourier coefficients $\lambda(\xi, \mathfrak{m}, f)$ for non-principal $\mathfrak{m}$ is done in the automorphic setting, which we do not treat, but we can compute them explicitly in the case of forms given by theta series, which we will consider below.

Definition. *The* Kohnen plus space $M^+_{\mathbf{3/2}}(\mathfrak{b}, \psi)$ *is the subspace of those* $f \in M_{\mathbf{3/2}}(\mathfrak{b}, \psi)$ *satisfying that* $\lambda(\xi, \mathcal{O}, f) = 0$ *for every* $\xi \in \mathcal{O}^+$ *such that* $-\xi$ *is not a square modulo* $4\mathcal{O}$. *We denote* $S^+_{\mathbf{3/2}}(\mathfrak{b}, \psi) = M^+_{\mathbf{3/2}}(\mathfrak{b}, \psi) \cap S_{\mathbf{3/2}}(\mathfrak{b}, \psi)$.

This definition extends naturally the classical Kohnen plus space to the Hilbert setting. We will see below in Remarks 2.5.2 and 2.5.5 that it has similar properties as those obtained in [Koh82] for classical modular forms.

The action of the Hecke operators, which as in the classical setting is defined in terms of double coclasses, can be described in terms of Fourier coefficients. See [Shi87, Proposition 5.4] (and recall our normalization).

Proposition 2.3.3. *Let* $f \in M_{\mathbf{3/2}}(\mathfrak{b}, \psi)$, *and let* $\mathfrak{p}$ *be a prime ideal such that* $\mathfrak{p} \nmid \mathfrak{b}$. *Let* $\mathfrak{m}$ *be a fractional ideal, and take* $c_\mathfrak{p} \in F_\mathfrak{p}$ *such that* $\mathcal{O}_\mathfrak{p} c_\mathfrak{p} = \mathfrak{m}_\mathfrak{p}$. *Then,*

$$\lambda(\xi, \mathfrak{m}, T_\mathfrak{p}(f)) = N(\mathfrak{p})\lambda(\xi, \mathfrak{p}\mathfrak{m}, f) + \psi^*(\mathfrak{p})\big(\tfrac{\xi c_\mathfrak{p}^2}{\mathfrak{p}}\big)\lambda(\xi, \mathfrak{m}, f) + \psi^*(\mathfrak{p}^2)\lambda(\xi, \mathfrak{p}^{-1}\mathfrak{m}, f),$$

where $\big(\tfrac{*}{\mathfrak{p}}\big)$ *denotes the quadratic residue symbol modulo* $\mathfrak{p}$.

For $\mathfrak{n} \subseteq \mathcal{O}$, we introduce a formal symbol $M(\mathfrak{n})$ such that $M(\mathfrak{n}\mathfrak{m}) = M(\mathfrak{n})M(\mathfrak{m})$ for all $\mathfrak{n}, \mathfrak{m} \subseteq \mathcal{O}$. Then we can consider the ring of formal series in these symbols, indexed by integral ideals. These turn into Dirichlet series when we specialize $M(\mathfrak{n})$ to $N(\mathfrak{n})^{-s}$, with s a complex variable. The following result, which is essentially [Shi87, Theorems 6.1 and 6.2], is the generalization of the Shimura correspondence for Hilbert modular forms. We assume for simplicity that ψ is a quadratic character, since this will be the case in our setting.

Theorem 2.3.4. *For each* $\xi \in \mathcal{O}^+$ *there is a linear map* $\mathrm{Shim}_\xi : M_{\mathbf{3/2}}(\mathfrak{b}, \psi) \to M_{\mathbf{2}}(\mathfrak{b}/2)$, *characterized by the following property. Write* $\xi\mathcal{O} = \mathfrak{q}^2\mathfrak{r}$ *with* $\mathfrak{q}, \mathfrak{r} \subseteq \mathcal{O}$ *and* $\mathfrak{r}$ *square-free, and let* ϵ_ξ *be the Hecke character corresponding to* $F(\sqrt{\xi})/F$. *Let* $f \in M_{\mathbf{3/2}}(\mathfrak{b}, \psi)$. *Then (formally),*

$$\sum_{\mathfrak{m} \subseteq \mathcal{O}} c(\mathfrak{m}, \mathrm{Shim}_\xi(f))M(\mathfrak{m}) = \left(\sum_{\mathfrak{m} \subseteq \mathcal{O}} \lambda(\xi, \mathfrak{q}^{-1}\mathfrak{m}, f)M(\mathfrak{m})\right)\left(\sum_{\mathfrak{m} \subseteq \mathcal{O}} (\psi^*\epsilon_\xi^*)(\mathfrak{m})N(\mathfrak{m})^{-1}M(\mathfrak{m})\right). \tag{2.3.5}$$

This map is such that if f *is a* $\mathbb{T}$*-eigenform, then* $\mathrm{Shim}_\xi(f) \neq 0$ *if and only if* $\lambda(\xi, \mathfrak{q}^{-1}, f) \neq 0$. *In that case,* $\mathrm{Shim}_\xi(f)$ *is a* $\mathbb{T}$*-eigenform, with the same system of eigenvalues as* f.

Actually, (2.3.5) is used to define the function $\mathrm{Shim}_\xi(f)$ in terms of a q-expansion, and the proof of the theorem consists in using the criterion of Weil (see [Wei80, Theorem 7]) to see that $\mathrm{Shim}_\xi(f)$ is a Hilbert modular form with level and weight as above.

Though Theorem 2.3.4 claims that the Shimura map is $\mathbb{T}$-linear when acting in eigenforms, this does not imply the Hecke linearity in all of $M_{\mathbf{3/2}}(\mathfrak{b}, \psi)$, since this space does not necessarily have a basis of $\mathbb{T}$-eigenforms. Nevertheless, by looking at the Fourier coefficients we get the following result.

Proposition 2.3.6. *The Shimura map* $\mathrm{Shim}_\xi : M_{\mathbf{3/2}}(\mathfrak{b}, \psi) \to M_{\mathbf{2}}(\mathfrak{b}/2)$ *is* $\mathbb{T}_0$*-linear.*

Proof. Let $f \in M_{\mathbf{3/2}}(\mathfrak{b}, \psi)$, and let $\mathfrak{p}$ be a prime ideal with $\mathfrak{p} \nmid \mathfrak{b}$. We must prove that $c(\mathfrak{m}, \mathrm{Shim}_\xi(T_\mathfrak{p} f))$ $= c(\mathfrak{m}, T_\mathfrak{p}(\mathrm{Shim}_\xi\, f))$ for every integral ideal $\mathfrak{m}$.

Using Proposition 2.1.4 and (2.3.5), we have that

$$\begin{aligned} c(\mathfrak{m}, \mathrm{Shim}_\xi(T_\mathfrak{p} f)) = N(\mathfrak{p}) \sum_{\mathfrak{n} | \mathfrak{p}\mathfrak{m}} \lambda(\tau, \mathfrak{q}^{-1}\mathfrak{n}, f)(\psi\epsilon_\tau)^*(\mathfrak{n}^{-1}\mathfrak{p}\mathfrak{m}) N(\mathfrak{n}^{-1}\mathfrak{p}\mathfrak{m})^{-1} \\ + \sum_{\mathfrak{n} | \mathfrak{p}^{-1}\mathfrak{m}} \lambda(\tau, \mathfrak{q}^{-1}\mathfrak{n}, f)(\psi\epsilon_\tau)^*((\mathfrak{n}\mathfrak{p})^{-1}\mathfrak{m}) N((\mathfrak{n}\mathfrak{p})^{-1}\mathfrak{m})^{-1}. \end{aligned}$$

On the other hand, using Proposition 2.3.3 and (2.3.5) we have that

$$\begin{aligned} c(\mathfrak{m}, T_\mathfrak{p}(\mathrm{Shim}_\xi\, f)) = \sum_{\mathfrak{n} | \mathfrak{m}} \Big(N(\mathfrak{p})\lambda(\xi, \mathfrak{q}^{-1}\mathfrak{n}\mathfrak{p}, f) + \psi^*(\mathfrak{p})\big(\tfrac{\xi c_\mathfrak{p}^2}{\mathfrak{p}}\big)\lambda(\xi, \mathfrak{q}^{-1}\mathfrak{n}, f) \\ + \lambda(\xi, (\mathfrak{p}\mathfrak{q})^{-1}\mathfrak{n}, f)\Big)(\psi\epsilon_\xi)^*(\mathfrak{n}^{-1}\mathfrak{m}) N(\mathfrak{n}^{-1}\mathfrak{m})^{-1}, \end{aligned}$$

where $c_\mathfrak{p} \in F_\mathfrak{p}$ is such that $\mathcal{O}_\mathfrak{p} c_\mathfrak{p} = \mathfrak{q}^{-1}\mathfrak{m}_\mathfrak{p}$. Notice that $\epsilon_\xi^*(\mathfrak{p}) = \big(\tfrac{\xi c_\mathfrak{p}^2}{\mathfrak{p}}\big)$.

Since $\mathfrak{r}$ is square-free, (2.3.2) implies that $\lambda(\xi, (\mathfrak{p}\mathfrak{q})^{-1}\mathfrak{n}, f) = 0$ unless $\mathfrak{p} \mid \mathfrak{n}$. Using this, it is tedious but not hard to see that the equations above imply that both Fourier coefficients agree.

□

2.4 Ternary theta series

Theta series of totally definite ternary quadratic forms can be used to construct Hilbert modular forms of weight $\mathbf{3/2}$, as we show in Proposition 2.4.4 below. Since the number of variables of these quadratic forms is not even, they are not considered in the classical literature. Transformation formulas in this (and much more) generality are studied in [Shi87, Section 11] and in [Shi93b]. We start this section by recalling some results from [Shi87] that we need to prove Proposition 2.4.4. We first need to introduce some notation.

Given a fractional ideal $\mathfrak{n}$, we denote

$$\Gamma_\mathbb{A}[\mathfrak{n}] = \Big\{ \big(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\big) \in G(F_\mathbb{A}) : a_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}, b_\mathfrak{p} \in (2\mathfrak{d}^{-1})_\mathfrak{p}, c_\mathfrak{p} \in (2\mathfrak{n}\mathfrak{d})_\mathfrak{p}, d_\mathfrak{p} \in \mathcal{O}_\mathfrak{p} \quad \forall\, \mathfrak{p} \Big\},$$

which agrees with the group $D[2\mathfrak{d}^{-1} : 2\mathfrak{n}\mathfrak{d}] \cdot G_\mathbf{a}$ from [Shi87]. We denote by P the subscheme of G consisting of the upper triangular matrices. Given a 2×2 matrix β, we use the notation $\beta = \big(\begin{smallmatrix} a_\beta & b_\beta \\ c_\beta & d_\beta \end{smallmatrix}\big)$ to refer to the coefficients of β. For $\beta \in G(F)$, we denote by $\mathfrak{a}_\beta$ the fractional ideal given locally by $(\mathfrak{a}_\beta)_\mathfrak{p} = (c_\beta)\mathfrak{d}_\mathfrak{p}^{-1} + d_\beta \mathcal{O}_\mathfrak{p}$.

Let $S \in M_3(F)$ be a totally negative definite matrix. Consider the natural embedding of F^3 in $F_\mathbf{f}^3$. Given $\eta \in \mathcal{S}(F_\mathbf{f}^3)$ (here we denote by $\mathcal{S}$ the Schwartz-Bruhat space of locally constant functions), we consider the theta series attached to S given by

$$g(z; \eta) = \sum_{\xi \in F^3} \eta(\xi) e_F(\xi S \xi^t, \tfrac{z}{2}).$$

Here we set $u = 0$ in the theta series $g(z, u; \eta)$ introduced in [Shi87].

Denote by ψ the Hecke character corresponding to the quadratic extension $F(\sqrt{\det S})/F$, and let $\mathfrak{f}$ denote its conductor.

In [Shi87, Proposition 2.4] there is defined an action of $G(F)$ on $\mathcal{S}(F_{\mathbf{f}}^3)$, which is denoted by $(\beta, \eta) \mapsto {}^{\beta}\eta$. In terms of this action we have the following transformation formula for $g(z; \eta)$.

Proposition 2.4.1. *For every $\beta \in G(F) \cap P(F_{\mathbb{A}})\Gamma_{\mathbb{A}}[\mathcal{O}]$,*

$$g(\beta z; {}^{\beta}\eta) = \overline{J(\beta, z)}g(z; \eta).$$

Proof. This is [Shi87, Proposition 11.4]. Note that since S is totally negative definite, the automorphy factor J_S involved in that result is given by

$$J_S(\beta, z) = h(\beta, z) \cdot |j(\beta, z)|^3 j(\beta, z)^{-3}.$$

It satisfies that $\overline{J_S} = J$, since by [Shi87, (2.19b)] we have that $j^2 = h^4$. □

The following two results show how $G(F)$ acts on $\mathcal{S}(F_{\mathbf{f}}^3)$ in certain cases.

Proposition 2.4.2. *Given $\eta \in \mathcal{S}(F_{\mathbf{f}}^3)$, let M be an $\mathcal{O}$-lattice in F^3 such that $\eta(x + u) = \eta(x)$ for every $u \in M$. Furthermore, let $\mathfrak{r}, \mathfrak{n}, \mathfrak{z}$ be fractional ideals of F satisfying:*

(1) $xSx^t \in \mathfrak{r}$ for every $x \in F^3$ such that $\eta(x) \neq 0$.

(2) $xSx^t \in \mathfrak{n}$ for every $x \in F^3$ such that $\mathrm{Tr}(xSy^t) \in \mathfrak{d}^{-1}$ for every $y \in M$.

(3) $\eta(xa) = \eta(x)$ for every $a \in \hat{\mathcal{O}}^{\times}$ such that $a_{\mathfrak{p}} - 1 \in \mathfrak{z}_{\mathfrak{p}}$ for every $\mathfrak{p}$.

Let $\mathfrak{a} = \mathfrak{r}^{-1} \cap \mathcal{O}$ and $\mathfrak{b} = 4\mathfrak{D} \cap \mathfrak{z} \cap 4\mathfrak{a} \cap 4\mathfrak{d}^{-1}\mathfrak{a}\mathfrak{n}^{-1}$. Then

$${}^{\beta}\eta(x) = \psi_{\mathfrak{f}}(d_\beta)\eta(x(a_\beta)_{\mathfrak{z}}) \qquad \forall\, \beta \in \Gamma[2^{-1}\mathfrak{d}\mathfrak{a}^{-1}, \mathfrak{b}],$$

where $(a_\beta)_{\mathfrak{z}}$ denotes the projection of a_β to $\prod_{\mathfrak{p}|\mathfrak{z}} F_{\mathfrak{p}}^{\times}$.

Proof. This is [Shi87, Proposition 11.7]. □

Proposition 2.4.3. *Given $\eta \in \mathcal{S}(F_{\mathbf{f}}^3)$, there is an open subgroup U of $\Gamma_{\mathbb{A}}[\mathfrak{f}]$ such that if $\beta \in G(F) \cap \left(\begin{smallmatrix} t & 0 \\ 0 & t^{-1} \end{smallmatrix}\right) U$ with $t \in F_{\mathbf{f}}^{\times}$, then*

$${}^{\beta}\eta(x) = \psi_{\mathbf{a}}(d_\beta)\psi^*(d_\beta\mathfrak{a}_\beta^{-1})N(\mathfrak{a}_\beta)^{3/2}\eta(xt) \qquad \forall\, x \in F_{\mathbf{f}}^3.$$

Proof. This is [Shi87, Proposition 11.5]. □

We now apply these results to our setting. Let B be a totally definite quaternion algebra over F. For $x \in B$ denote $\Delta(x) = \mathrm{Tr}(x)^2 - 4N(x)$, the *discriminant* of x. Let $V = B/F$, and for $x \in B$ denote by $[x]$ its class in V. Then Δ determines an integral, totally negative definite quadratic form on V. For $I \in \mathfrak{I}(R)$, we consider $R_r(I)/\mathcal{O}$ as a lattice in V, which we denote by L_I.

From here on, let ψ be the Hecke character corresponding to the quadratic extension $F(\sqrt{-1})/F$. This quadratic character has conductor $\mathfrak{f}$ dividing $4\mathcal{O}$, and the corresponding ideal character satisfies $\psi^*(\mathfrak{p}) = \left(\frac{-1}{\mathfrak{p}}\right)$ for $\mathfrak{p} \nmid 2$. By local class field theory, ψ satisfies the equality $\psi_{\mathbf{a}}(-1) = (-1)^d$. Hence, the space $M_{\mathbf{3/2}}(4\mathfrak{D}, \psi)$ is not trivially zero.

Proposition 2.4.4. *Given $I \in \mathfrak{I}(R)$, let*

$$\vartheta_I(z) = \sum_{[x] \in L_I} e_F\big(-\Delta(x), \tfrac{z}{2}\big).$$

Then $\vartheta_I \in M_{\mathbf{3/2}}^{+}(4\mathfrak{D}, \psi)$. Furthermore, the Fourier coefficients of ϑ_I are given by

$$\lambda(\xi, \mathfrak{a}, \vartheta_I) = N(\mathfrak{a})^{-1} \cdot \#\{[x] \in \mathfrak{a}^{-1}L_I : -\Delta(x) = \xi\}.$$

Proof. Let $\{v_1, v_2, v_3\}$ be a basis of V, and let $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3$ be fractional ideals such that $L_I = \oplus_{i=1}^3 \mathfrak{a}_i v_i$. Through this basis we identify V with F^3. Let S be the matrix of the quadratic form Δ with respect to this basis. If $B = (a,b)_F$, then the determinant of Δ with respect to the basis $\{[i],[j],[k]\}$ equals $-(8ab)^2$ (recall the notation from Section 1.1). This shows that $\det(S) = -1 \in F^\times/(F^\times)^2$.

Let $\eta \in \mathcal{S}(F_{\mathbf{f}}^3)$ be the characteristic function of $M = \mathfrak{a}_1 \oplus \mathfrak{a}_2 \oplus \mathfrak{a}_3$. Then the theta series $g(z;\eta)$ defined by S and η satisfies that

$$g(z;\eta) = \sum_{\xi \in F^3} \eta(\xi) e_F(\Delta(\xi), \tfrac{\bar{z}}{2}) = \overline{\vartheta_I(z)}. \tag{2.4.5}$$

The function η satisfies the hypotheses of Proposition 2.4.2, taking $\mathfrak{r} = \mathfrak{z} = \mathcal{O}$, and $\mathfrak{n} = \mathfrak{d}^{-2}\mathfrak{D}^{-1}$. The first two assertions are clear. To prove the last equality, take $[x] \in V$ such that $[x]S[y]^t \in \mathfrak{d}^{-1}$ for every $[y] \in L_I$. Assume, without loss of generality, that $\operatorname{Tr}(x) = 0$. Then, a simple calculation shows that $2\operatorname{Tr}(x\bar{y}) \in \mathfrak{d}^{-1}$ for every $y \in R_r(I)$. Hence, by [Geb09, Lemma 1.2.5], we have that $\Delta([x]) = -N(2x) \in \mathfrak{d}^{-2}\mathfrak{D}^{-1}$.

Then Propositions 2.4.1 and 2.4.2 together with (2.4.5) give that

$$\vartheta_I(\beta z) = \psi_{\mathfrak{f}}^{-1}(d_\beta) J(\beta, z) \vartheta_I(z) \quad \forall\, \beta \in \Gamma[2^{-1}\mathfrak{d}, 4\mathfrak{D}].$$

Since ψ is quadratic and its conductor $\mathfrak{f}$ divides $4\mathfrak{D}$, we have that $\psi_{\mathfrak{f}}^{-1}(d_\beta) = \psi_{4\mathfrak{D}}(a_\beta)$ for all $\beta \in \Gamma[2^{-1}\mathfrak{d}, 4\mathfrak{D}]$. This proves that $\vartheta_I \in M_{\mathbf{3/2}}(4\mathfrak{D}, \psi)$. To see that it belong to the Kohnen plus space, note that

$$\lambda(\xi, \mathcal{O}, \vartheta_I) = \#\{[x] \in L_I : -\Delta(x) = \xi\}$$

equals 0 if $-\xi$ is not a square modulo $4\mathcal{O}$.

We now consider the Fourier coefficients of ϑ_I. Given a fractional ideal $\mathfrak{a}$, take $t \in F_{\mathbf{f}}^\times$ such that $t\mathcal{O} = \mathfrak{a}$. Let $\beta \in G(F)$ be as in Proposition 2.4.3. Since $\beta = \left(\begin{smallmatrix} t & 0 \\ 0 & t^{-1} \end{smallmatrix}\right) q$ with $q \in \Gamma_{\mathbb{A}}[\mathfrak{f}]$, we have that $\mathfrak{a}_\beta = t^{-1}\mathcal{O} = \mathfrak{a}^{-1}$. Then by [Shi87, (3.14c)] we have that

$$\psi_{\mathbf{a}}(d_\beta)\psi^*(d_\beta \mathfrak{a}) J(\beta, \beta^{-1}z)\vartheta_I(\beta^{-1}z) = N(\mathfrak{a})^{-1/2} \sum_{\xi \in F} \lambda(\xi, \mathfrak{a}, \vartheta_I) e_F(\xi, z/2). \tag{2.4.6}$$

On the other hand, by Propositions 2.4.1 and 2.4.3, we have that

$$J(\beta, \beta^{-1}z)\vartheta_I(\beta^{-1}z) = \overline{g(z;{}^{\beta}\eta)} = \psi_{\mathbf{a}}(d_\beta)\psi^*(d_\beta\mathfrak{a}) N(\mathfrak{a})^{-3/2} \sum_{\xi \in F^3} \eta(\xi t) e_F(\Delta(\xi), \tfrac{z}{2}). \tag{2.4.7}$$

Since the map $\xi \mapsto \eta(\xi t)$ equals 1 if $\xi \in \mathfrak{a}^{-1}L_I$ and 0 otherwise, comparing (2.4.6) and (2.4.7) yields the desired equality.

□

We now prove that this construction is $\mathbb{T}_0$-linear. For this, we start with the following auxiliary result.

Lemma 2.4.8. *Let $\mathfrak{p}$ be a prime ideal such that $\mathfrak{p} \nmid 4\mathfrak{D}$. Let $[x] \in \mathfrak{p}^{-1}L_I$. Then,*

$$\#\{J \in t_{\mathfrak{p}}(I) : [x] \in L_J\} = \begin{cases} 1 + N(\mathfrak{p}), & [x] \in \mathfrak{p}L_I, \\ 1 + \left(\frac{\Delta(x)}{\mathfrak{p}}\right), & [x] \in L_I \setminus \mathfrak{p}L_I, \\ 0 \text{ or } 1, & [x] \in \mathfrak{p}^{-1}L_I \setminus L_I. \end{cases}$$

Proof. Note that given $J \in t_{\mathfrak{p}}(I)$, we have that $[x] \in L_J$ if and only if $[x] \in (L_J)_{\mathfrak{p}}$, since $(L_I)_{\mathfrak{q}} = (L_J)_{\mathfrak{q}}$ for every $\mathfrak{q} \neq \mathfrak{p}$. Since $\mathfrak{p} \nmid 4\mathfrak{D}$ we can identify $R_r(I)_{\mathfrak{p}}$ with $M_2(\mathcal{O}_{\mathfrak{p}})$. Then, the set $\{J \in t_{\mathfrak{p}}(I) : [x] \in L_J\}$ is in bijection with the set

$$\mathfrak{X} = \mathrm{SL}_2(\mathcal{O}_{\mathfrak{p}}) \backslash \{y_{\mathfrak{p}} \in M_2(\mathcal{O}_{\mathfrak{p}}) : \det y_{\mathfrak{p}} = \pi_{\mathfrak{p}},\ y_{\mathfrak{p}} x_{\mathfrak{p}} y_{\mathfrak{p}}^{-1} \in F_{\mathfrak{p}} + M_2(\mathcal{O}_{\mathfrak{p}})\},$$

letting to each such $y_\mathfrak{p}$ correspond the ideal $J \in \mathfrak{I}(R)$ given locally by

$$J_\mathfrak{q} = \begin{cases} I_\mathfrak{q}, & \mathfrak{q} \neq \mathfrak{p}, \\ I_\mathfrak{p} y_\mathfrak{p}, & \mathfrak{q} = \mathfrak{p}. \end{cases}$$

To compute the set $\mathfrak{X}$, we use the same system of representatives for the action of $\mathrm{SL}_2(\mathcal{O}_\mathfrak{p})$ in $\{y_\mathfrak{p} \in M_2(\mathcal{O}_\mathfrak{p}) : \det y_\mathfrak{p} = \pi_\mathfrak{p}\}$ as in Lemma 2.2.1. We start by considering the first two cases. Assume then that $x \in R_r(I)$. Write $x_\mathfrak{p} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathcal{O}_\mathfrak{p})$. Then, we have that

$$\begin{pmatrix} \pi_\mathfrak{p} & 0 \\ 0 & 1 \end{pmatrix} x_\mathfrak{p} \begin{pmatrix} \pi_\mathfrak{p} & 0 \\ 0 & 1 \end{pmatrix}^{-1} \in F_\mathfrak{p} + M_2(\mathcal{O}_\mathfrak{p}) \iff \pi_\mathfrak{p} \mid c,$$
$$\begin{pmatrix} 1 & \alpha \\ 0 & \pi_\mathfrak{p} \end{pmatrix} x_\mathfrak{p} \begin{pmatrix} 1 & \alpha \\ 0 & \pi_\mathfrak{p} \end{pmatrix}^{-1} \in F_\mathfrak{p} + M_2(\mathcal{O}_\mathfrak{p}) \iff \pi_\mathfrak{p} \mid -c\alpha^2 + (d-a)\alpha + b.$$

If $x_\mathfrak{p} \in \mathcal{O}_\mathfrak{p} + \mathfrak{p}M_2(\mathcal{O}_\mathfrak{p})$, we see that $\mathfrak{X}$ has $1 + N(\mathfrak{p})$ elements. If $x_\mathfrak{p} \notin \mathcal{O}_\mathfrak{p} + \mathfrak{p}M_2(\mathcal{O}_\mathfrak{p})$, let $P = -cX^2 + (d-a)X + b \in k_\mathfrak{p}[X]$. Then $P \neq 0$, and its discriminant equals $(d-a)^2 + 4bc = \Delta(x_\mathfrak{p})$. Hence $\mathfrak{X}$ has $1 + \left(\frac{\Delta(x_\mathfrak{p})}{\mathfrak{p}}\right)$ elements.

Now consider the case when $[x] \in \mathfrak{p}^{-1}L_I \setminus L_I$. Assume then that $\pi_\mathfrak{p} x_\mathfrak{p} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathcal{O}_\mathfrak{p})$, and that $x_\mathfrak{p} \notin F_\mathfrak{p} + M_2(\mathcal{O}_\mathfrak{p})$. Then, we have that

$$\text{(2.4.9)} \qquad \begin{pmatrix} \pi_\mathfrak{p} & 0 \\ 0 & 1 \end{pmatrix} x_\mathfrak{p} \begin{pmatrix} \pi_\mathfrak{p} & 0 \\ 0 & 1 \end{pmatrix}^{-1} \in F_\mathfrak{p} + M_2(\mathcal{O}_\mathfrak{p}) \iff \begin{cases} \pi_\mathfrak{p}^2 \mid c, \\ \pi_\mathfrak{p} \mid d-a, \end{cases}$$

$$\text{(2.4.10)} \qquad \begin{pmatrix} 1 & \alpha \\ 0 & \pi_\mathfrak{p} \end{pmatrix} x_\mathfrak{p} \begin{pmatrix} 1 & \alpha \\ 0 & \pi_\mathfrak{p} \end{pmatrix}^{-1} \in F_\mathfrak{p} + M_2(\mathcal{O}_\mathfrak{p}) \iff \begin{cases} \pi_\mathfrak{p}^2 \mid -c\alpha^2 + (d-a)\alpha + b, \\ \pi_\mathfrak{p} \mid (d-a) - 2c\alpha. \end{cases}$$

Suppose that (2.4.9) holds, and that there exists α such that (2.4.10) holds. Then $\pi_\mathfrak{p} \mid c, d-a, b$, thus contradicting the fact that $x_\mathfrak{p} \notin F_\mathfrak{p} + M_2(\mathcal{O}_\mathfrak{p})$. Finally, assume that there exist distinct α_1, α_2 such that (2.4.10) holds. Then, substracting equations we see that $\pi_\mathfrak{p} \mid 2c$. If $\pi_\mathfrak{p} \mid c$ we have that $\pi_\mathfrak{p} \mid d-a, b$, which again is not possible. If $\pi_\mathfrak{p} \mid 2$, we have that $\pi_\mathfrak{p} \mid d-a$, and hence the polynomial P defined above has null discriminant. This is a contradiction, since P has α_1, α_2 as roots. Thus, we have proved that $\mathfrak{X}$ has at most one element, which completes the proof. □

For $\xi \in F^+ \cup \{0\}$, a fractional ideal $\mathfrak{a}$ and $I \in \mathfrak{I}(R)$, denote

$$a(\xi, \mathfrak{a}, [I]) = \#\{[x] \in \mathfrak{a}^{-1}L_I : -\Delta(x) = \xi\}.$$

Let $e_\xi \in M(R)$ be given by

$$e_\xi = \sum_{[J] \in Cl(R)} \tfrac{a(\xi, \mathcal{O}, [J])}{\langle [J],[J] \rangle} \cdot [J].$$

This agrees with our previous definition of e_0.

Theorem 2.4.11. *Given $v \in M(R)$, let*

$$\text{(2.4.12)} \qquad \theta(v)(z) = \sum_{\xi \in \mathcal{O}^+ \cup \{0\}} \langle e_\xi, v \rangle e_F\left(\xi, \tfrac{z}{2}\right) = \deg(v) + \sum_{\xi \in \mathcal{O}^+} \langle e_\xi, v \rangle e_F\left(\xi, \tfrac{z}{2}\right).$$

Then, $\theta(v) \in M^+_{\mathbf{3/2}}(4\mathfrak{D}, \psi)$, and $\theta(v)$ is cuspidal if and only if v is cuspidal. Furthermore, the map θ is $\mathbb{T}_0$-linear.

Proof. First assume that $v = [I]$, with $I \in \mathfrak{I}(R)$. Then $\theta([I]) = \vartheta_I$, which implies the first claim. To prove the Hecke linearity, let $\mathfrak{p}$ be a prime ideal not dividing $4\mathfrak{D}$. Let $f = \theta(T_\mathfrak{p}([I]))$. Since

$$f = \sum_{\xi \in \mathcal{O}^+ \cup \{0\}} \Big(\sum_{J \in t_\mathfrak{p}(I)} \langle e_\xi, [J] \rangle \Big) e_F\left(\xi, \tfrac{z}{2}\right),$$

we have that

$$\lambda(\xi, \mathcal{O}, f) = \#\{(J, [x]) \in \mathfrak{I}(R) \times V : J \in t_{\mathfrak{p}}(I),\ [x] \in L_J,\ -\Delta(x) = \xi\}.$$

To compute the size of this set, we use Lemma 2.4.8, considering the following three possibilities for those $[x] \in V$ for which there exists $J \in t_{\mathfrak{p}}(I)$ such that $[x] \in L_J$, $-\Delta(x) = \xi$. Note that since $\mathfrak{p}I \subseteq J \subseteq I$ for $J \in t_{\mathfrak{p}}(I)$, then every such $[x]$ belongs to $\mathfrak{p}^{-1}L_I$.

- $[x] \in \mathfrak{p}L_I$. There are $a(\xi, \mathfrak{p}^{-1}, [I])$ such $[x]$, and for each one there are $1 + N(\mathfrak{p})$ ideals J as above.
- $[x] \in L_I \setminus \mathfrak{p}L_I$. There are $a(\xi, \mathcal{O}, [I]) - a(\xi, \mathfrak{p}^{-1}, [I])$ such $[x]$, and for each one there are $1 + \left(\frac{\Delta(x)}{\mathfrak{p}}\right)$ ideals J as above. Note that $a(\xi, \mathfrak{p}^{-1}, [I])\left(\frac{\Delta(x)}{\mathfrak{p}}\right) = 0$, since if there exists $[y] \in \mathfrak{p}L_I$ such that $\Delta([y]) = \xi$, then $\mathfrak{p} \mid \xi$.
- $[x] \in \mathfrak{p}^{-1}L_I \setminus L_I$. There are $a(\xi, \mathfrak{p}, [I]) - a(\xi, \mathcal{O}, [I])$ such $[x]$, and for each one there is just one ideal J as above.

Adding up, using Propositions 2.3.3 and 2.4.4 we see that

$$\begin{aligned}\lambda(\xi, \mathcal{O}, f) &= a(\xi, \mathfrak{p}^{-1}, [I])\big(1 + N(\mathfrak{p})\big) + \\ &\quad + \big(a(\xi, \mathcal{O}, [I]) - a(\xi, \mathfrak{p}^{-1}, [I])\big)\Big(1 + \big(\tfrac{\Delta(x)}{\mathfrak{p}}\big)\Big) + a(\xi, \mathfrak{p}, [I]) - a(\xi, \mathcal{O}, [I]) \\ &= N(\mathfrak{p})a(\xi, \mathfrak{p}^{-1}, [I]) + a(\xi, \mathcal{O}, [I])\big(\tfrac{\Delta(x)}{\mathfrak{p}}\big) + a(\xi, \mathfrak{p}, [I]) \\ &= \lambda(\xi, \mathfrak{p}^{-1}, \vartheta_I) + \big(\tfrac{\xi}{\mathfrak{p}}\big)\psi^*(\mathfrak{p})\lambda(\xi, \mathcal{O}, \vartheta_I) + N(\mathfrak{p})\lambda(\xi, \mathfrak{p}, \vartheta_I) \\ &= \lambda(\xi, \mathcal{O}, T_{\mathfrak{p}}(\vartheta_I)),\end{aligned}$$

which proves that $T_{\mathfrak{p}}(\theta([I])) = \theta(T_{\mathfrak{p}}([I]))$.

Finally, let $v \in S(R)$. Then (2.4.12) shows that $\theta(v)$ is cuspidal at infinity. Since for $I, J \in \mathfrak{I}(R)$ the lattices L_I and L_J are locally conjugated, we have that $\theta(v)$ is a linear combination of theta series corresponding to quadratic forms in the same genus. Hence, $\theta(v)$ is cuspidal. This is a classical result by Siegel, generalized to the totally real field setting in [Wal94]. □

2.5 Computing preimages

The main application of what we explained in the previous sections is to construct preimages of the Shimura map. This is, given $\xi \in \mathcal{O}^+$, and given a newform g of weight $\mathbf{2}$, to construct a form f of weight $\mathbf{3/2}$ such that $\mathrm{Shim}_\xi(f) = g$.

Let $\mathfrak{c}$ be an integral ideal, and suppose that B is a totally definite quaternion algebra having an Eichler order R of discriminant $\mathfrak{c}$ (see Remark 2.2.7).

Proposition 2.5.1. *Let $v \in S(R)$. Then, $\mathrm{Shim}_\xi(\theta(v))$ is a cusp form.*

Proof. We can assume that v is a $\mathbb{T}_0$-eigenvector. Denote $g = \mathrm{Shim}_\xi(\theta(v))$. Then if for $\mathfrak{p} \nmid \mathfrak{c}$ we let $\omega_{\mathfrak{p}}$ denote the $\mathfrak{p}$-th eigenvalue of v, since the maps θ and Shim_ξ are $\mathbb{T}_0$-linear, we have that $T_{\mathfrak{p}}g = \omega_{\mathfrak{p}}g$.

By the theory of Hilbert Eisenstein series, for which we refer to and borrow the notation from [Wil86] and [AL13], it suffices to prove that g is orthogonal to every Eisenstein series $E = E_{\psi_1,\psi_2}$.

Let $\mathfrak{p} \nmid \mathfrak{c}$. We have that $T_{\mathfrak{p}}E = c(\mathfrak{p}, E)E$ (see [AL13, Proposition 3,3]). Then, the self-adjointness of the Petersson inner product implies that

$$\omega_{\mathfrak{p}}\langle g, E\rangle = c(\mathfrak{p}, E)\langle g, E\rangle.$$

This implies that $\langle g, E\rangle = 0$, since by [Sha90] we have that $|\omega_{\mathfrak{p}}| \leq 2N(\mathfrak{p})^{7/10}$, whereas by the definition of E (see [AL13, Proposition 3.1]) we have that $|c(\mathfrak{p}, E)| \geq N(\mathfrak{p}) - 1$.

We finish by remarking that though in [AL13] the authors consider weights $\mathbf{k} \geq \mathbf{3}$, the results we used are still valid in weight $\mathbf{2}$ when $F \neq \mathbb{Q}$. The case $F = \mathbb{Q}$ follows by the same arguments, taking special care with the definition of the Eisenstein series of weight 2 (see [Wil86]). □

We have then the following diagram of $\mathbb{T}_0$-linear maps:

$$\begin{tikzcd}
S(R) \arrow[rr, hook, "\text{J-L}"] \arrow[dr, "\theta"] & & S_{\mathbf{2}}(\mathfrak{c})\ . \arrow[dl, dotted] \\
& S^{+}_{\mathbf{3/2}}(4\mathfrak{c}, \psi) \arrow[ur, bend right, "\mathrm{Shim}_\xi"'] &
\end{tikzcd}$$

The commutativity of this diagram is considered in Theorem 2.5.3 below.

Remark 2.5.2. According to Theorem 2.3.4, the map Shim_ξ in principle divides the level by 2, and hence for $v \in S(R)$, the form $\mathrm{Shim}_\xi(\theta(v))$ would have level $2\mathfrak{c}$ instead of the level $\mathfrak{c}$ claimed in the diagram. In the classical setting, when $\mathfrak{c}$ is odd and square-free, (a small part of) the theory of Kohnen asserts that when applied to forms in the Kohnen plus space, the Shimura map divides the level by 4. In the setting of Hilbert modular forms, the theory of the Kohnen plus space is currently under development by Hiraga and Ikeda. The case when $\mathfrak{c} = \mathcal{O}$ has been achieved in [HI13], and the general (odd, square-free) case is expected to be developed soon.

We summarize this discussion in the next theorem, which is the main result of this chapter.

Theorem 2.5.3. *Let $g \in S^{new}_{\mathbf{2}}(\mathfrak{c})$ be a newform, and let $v_g \in S(R)$ be a $\mathbb{T}_0$-eigenvector with the same eigenvalues as g. Let $\tilde{g} = \mathrm{Shim}_\xi(\theta(v_g))$. If $\tilde{g}$ has level $\mathfrak{c}$, then $\tilde{g}$ is a multiple of g.*

Proof. First, note that such v_g exists (and is unique) due to Theorem 2.2.6. Since the operators θ and Shim_ξ are $\mathbb{T}_0$-linear, then the cusp form $\tilde{g}$ has the same eigenvalues as g, and then by Theorem 2.1.5 $\tilde{g}$ is a multiple of g. □

Remark 2.5.4. It could happen that $\tilde{g}$ is the zero cusp form. Nevertheless, for odd and square-free $\mathfrak{c}$, the theory of the Kohnen space under development by Hiraga and Ikeda asserts that:

- A linear combination of the maps Shim_ξ is an isomorphism between the new subspace of $S^{+}_{\mathbf{3/2}}(4\mathfrak{c}, \psi)$ and $S^{new}_{\mathbf{2}}(\mathfrak{c})$ (which in particular implies that there exists ξ such that $\mathrm{Shim}_\xi(\theta(v_g)) \neq 0$).
- If $\theta(v_g)$ is not zero, then $\theta(v_g)$ is a newform mapping to a non-zero multiple of g under this isomorphism, by a strong multiplicity one result in $S^{+}_{\mathbf{3/2}}(4\mathfrak{c}, \psi)$.

Remark 2.5.5. We expect $\tilde{g}$ to have level $\mathfrak{c}$. Since we know that in the worst case it has level $2\mathfrak{c}$, then it must be a linear combination of $g(z)$ and $g(2z)$. In any given example, this combination can be found in terms of Fourier coefficients, and we can verify that $\tilde{g}$ has actually level $\mathfrak{c}$ by seeing that the coefficient corresponding to $g(2z)$ is null.

The main issue is then to know whether there exists a quaternion algebra B and an Eichler order R such that $\theta(v_g) \neq 0$. We assume from now on that $\mathfrak{c}$ is odd and square-free.

The following conjecture is just a naive generalization to the Hilbert setting of the result due to Böcherer and Schulze-Pillot for classical modular forms of odd and square-free level (see [BSP90, page 378]).

Conjecture 2.5.6. *The form $\theta(v_g)$ is non zero if and only if $L(g, 1) \neq 0$ and the quaternion algebra B ramifies exactly at the archimedean primes and at all primes $\mathfrak{p}$ dividing $\mathfrak{c}$ where the Atkin-Lehner involution $W_\mathfrak{p}$ acts on g with eigenvalue $w_\mathfrak{p} = -1$.*

Note that if $L(g, 1) \neq 0$, the functional equation safisied by $L(g, s)$ implies that $(-1)^d \prod_{\mathfrak{p} | \mathfrak{c}} w_\mathfrak{p} = 1$. Then an algebra B as in the conjecture exists, and it is unique up to isomorphism.

Definition. *Let $\xi \in \mathcal{O}_F^+$, and let $K = F(\sqrt{-\xi})$. We say that $-\xi$ is a* fundamental discriminant *if $\mathcal{O}_K$ has relative discriminant $\xi\mathcal{O}_F$ over $\mathcal{O}_F$, and there exists $\zeta \in \mathcal{O}_F$ such that*

$$\mathcal{O}_K = \mathcal{O}_F + \frac{\zeta + \sqrt{-\xi}}{2}\mathcal{O}_F.$$

The following result from [Xue11] is useful for finding fundamental discriminants.

Proposition 2.5.7. *Suppose that the relative discriminant of K over F is $\xi\mathcal{O}_F$. If every prime of F dividing 2 splits over K, then $-\xi$ is a fundamental discriminant.*

The relation between Fourier coefficients and central values of twisted L-series is given by the following theorem, which was proved for classical forms in [BSP90, page 378] and in a more general setting for Hilbert modular forms in [BM07, Theorem 4.3], generalizing Waldspurger's results over $\mathbb{Q}$.

Theorem 2.5.8. *Let $g \in S_{\mathbf{2}}^{new}(\mathfrak{c}, \psi^2)$ be a newform such that $f = \theta(v_g) \in S^+_{\mathbf{3/2}}(4\mathfrak{c}, \psi)$ is non-zero. Let $\xi \in \mathcal{O}^+$ be such that $-\xi$ is a fundamental discriminant. Let ϵ_ξ be the Hecke character corresponding to $F(\sqrt{-\xi})/F$. Then*

$$|\lambda(\xi, \mathcal{O}, f)|^2 = \kappa L(g, \epsilon_\xi, 1) \prod_{\mathfrak{p}|\mathfrak{c}} (c(\mathfrak{p}, g) - \epsilon_\xi(\mathfrak{p})), \tag{2.5.9}$$

where κ is a non-zero constant, and $L(g, \epsilon_\xi, s)$ is the twist of the L-series of g by ϵ_ξ.

In particular, under the above assumptions, this conjecture states that $L(g, \epsilon_\xi, 1) = 0$ if and only if $\lambda(\xi, \mathcal{O}, f) = 0$, if ξ is such that the product over $\mathfrak{p} \mid \mathfrak{c}$ in the right hand side of (2.5.9) is non-zero. This sort of results are important for obtaining (under the Birch and Swinnerton-Dyer conjecture) information about the rank of twists of elliptic curves, as in the congruent number problem. We give an example of this in the next section.

2.6 An example

We let $F = \mathbb{Q}(\sqrt{5})$, which has trivial narrow class group. Denote $\omega = \frac{1+\sqrt{5}}{2}$. We let E be the elliptic curve over F given by

$$E: \quad y^2 + xy + \omega y = x^3 - (1+\omega)x^2.$$

This curve has prime conductor, equal to $\mathfrak{c} = (5 + 2\omega)$, and satisfies that $L(E, 1) \neq 0$. The space $M_{\mathbf{2}}(\mathfrak{c})$ has dimension 2, and it is generated by an Eisenstein series and a newform g which corresponds to E. Its first eigenvalues are given in [Dem05]; we only state that $c(\mathfrak{c}, g) = -1$. According to Conjecture 2.5.6, we choose B to be the unramified totally definite algebra over F, i.e. the algebra $B = (-1, -1)_F$ considered in Section 1.4. If R is an Eichler order of discriminant $\mathfrak{c}$ in B, then Theorem 2.2.6 asserts that there exists $v \in S(R)$ which is an eigenvector for $\mathbb{T}_0$ with the same eigenvalues as g.

Using the algorithm introduced in Chapter 1, with the aid of SAGE ([S+11]), we obtain the desired order, which is given by

$$R = \left\langle \frac{1 - (\omega+1)j - (\omega+10)k}{2}, \frac{i - \omega j + -(\omega+21)k}{2}, j - 5k, (5\omega - 3)k \right\rangle_{\mathcal{O}}.$$

This order has class number equal to 2, and hence there is no need to compute the Hecke operators in this example, since $S(R)$ is 1-dimensional. A set of representatives for the set of R-ideal classes is given by R and the ideal I given by

$$I = \left\langle \frac{1 - (\omega+1)j - (\omega+38)k}{2}, \frac{i - \omega j + -(\omega+49)k}{2}, j + 3k, (5\omega - 3)k \right\rangle_{\mathcal{O}}.$$

We have that $v = [R] - [I]$ is an eigenvector for the whole Hecke algebra, since $\deg(v) = 0$.

Let $f = \theta(v)$. We consider L_R and L_I as lattices of dimension 6 over $\mathbb{Z}$, and use LLL on the integral, positive definite quadratic form $\mathrm{Tr}_{F/\mathbb{Q}} \circ (-\Delta)$ to compute the Fourier coefficients $\lambda(\xi, \mathcal{O}, f)$, with $\mathrm{Tr}_{F/\mathbb{Q}}(\xi) \leq 100$ and $-\xi$ a fundamental discriminant. We find that there are non-zero coefficients, thus verifying Conjecture 2.5.6. The zero coefficients split into two families, which we consider below.

- **The trivial zeros** are the ones such that $\lambda(\xi, \mathcal{O}, \theta([R])) = \lambda(\xi, \mathcal{O}, \theta([I])) = 0$. For this zeros Theorem 2.5.8 is easy to verify. The local-global principle for quadratic forms implies that the non existence of points $x \in L_R \cup L_I$ with $-\Delta(x) = \xi$ is equivallent to the equality $\epsilon_\xi(\mathfrak{c}) = -1$, so in this case both sides of (2.5.9) vanish trivially.

- **The non-trivial zeros** are the ones such that $\lambda(\xi, \mathcal{O}, \theta([R])) = \lambda(\xi, \mathcal{O}, \theta([I])) \neq 0$. For these zeros, we have that $\epsilon_\xi(\mathfrak{c}) = 1$, and hence by (2.5.9) that $L(g, \epsilon_\xi, 1) = 0$. The non-trivial zeros with $\mathrm{Tr}_{F/\mathbb{Q}}(\xi) \leq 100$ are

  $$35 + 8w, 39 + 15w, 47 - 9w, 51 - 5w, 62 - 27w.$$

  For these ξ, the Birch and Swinnerton-Dyer conjecture predicts that the rank of the quadratic twist of E by $-\xi$ should be positive (and even, because the sign of the functional equation equals 1). We verified using 2-descent that all these curves have rank equal to 2.

Epilogue

We consider the classical diophantine problem of deciding whether a positive, square-free integer n is the area of a right triangle with rational sides. This problem was partially solved by Tunnell in [Tun83]. The full solution must wait for the Birch and Swinnerton-Dyer conjecture to be proved.

Let $F = \mathbb{Q}$. Let E be the elliptic curve over $\mathbb{Q}$ given by

$$E: \quad y^2 = x^3 - x.$$

This curve, which is the curve 32A2 in Cremona's notation, is up to isogeny the unique elliptic curve of conductor 32, and has complex multiplication by $\mathbb{Z}[i]$. This is the curve related to the congruent number problem: a positive integer n is a congruent number if and only if the twisted curve

$$E \otimes n: \quad y^2 = x^3 - n^2 x$$

has positive rank. See [Kob93] for a comprehensive introduction to this problem.

The space $S(\Gamma_0(32))$ is one dimensional, and hence it is spanned by the normalized newform g corresponding to E. Its q-expansion is

$$g = q - 2q^5 - 3q^9 + 6q^{13} + 2q^{17} - q^{25} - 10q^{29} - 2q^{37} + 10q^{41} + 6q^{45} - 7q^{49} + 14q^{53} - 10q^{61} + O(q^{64}).$$

Since the automorphic representation corresponding to g is supercuspidal at 2, by Remark 2.2.8 if B is a quaternion algebra over $\mathbb{Q}$ and $R \subseteq B$ is an order of discriminant 32, then there exists a $\mathbb{T}_0$-eigenvector $v \in S(R)$ with the same eigenvalues as g.

We consider the Hamilton quaternion algebra $B = (-1,-1)_{\mathbb{Q}}$, which is ramified exactly at 2 and at infinity. Using the algorithms developed in Chapter 1 (from where we borrow some notation), we construct a Bass order of discriminant 32 in B and compute its ideal classes representatives. For this purpose, we consider a chain of orders

$$R(2) \supseteq R(16) \supseteq R(32)$$

with discriminants $2, 16$ and 32 respectively, which belong to the class A2 at $p = 2$.

We start with the well known maximal order given by

$$R(2) = \left\langle 1, i, j, \frac{1+i+j+k}{2} \right\rangle_{\mathbb{Z}}.$$

This order has class number equal to one (see [Piz80, Theorem 1.12]). We have that $R(2)^{\times,1} = E_{24}$, where E_{24} is the binary tetrahedral group given by

$$E_{24} = \left\{ \pm 1, \pm i, \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2} \right\}.$$

Calculations with this order are rather easy, since we do not need to use quasi-good bases: by simple inspection we find that $\{1, j-k, i-j, \frac{1+i+j+k}{2}\}$ is a good basis for $R(2)_2$.

The order $R(16)$ obtained is given by

$$R(16) = \left\langle i+j+k, -2j+2k, 2k, \frac{1+i+j+k}{2} \right\rangle_{\mathbb{Z}}.$$

Since $|R(6)^{\times,1}| = 6$, by Corollary 1.3.5 we see that $R(16)$ has class number equal to one as well.

The order $R(32)$ obtained is given by

$$R(32) = \left\langle i+j+k, -4j+4k, 4k, \frac{1+i+j+k}{2} \right\rangle_{\mathbb{Z}},$$

and its ideal classes representatives are given by $Cl(R(32)) = \{[R(32)], [I]\}$, where

$$I = \left\langle i-j-9k, 4j+20k, 4k, \frac{1-3i+5j+3k}{2} \right\rangle_{\mathbb{Z}}.$$

In particular $S(R(32))$ is one dimensional, and it is generated by $v = [R(32)] - [I]$. Hence, v is a $\mathbb{T}_0$-eigenvector with the same eigenvalues as g. Though we do not consider them in this thesis, we mention that the quaternary theta series associated to v, which is given by

$$\Theta(z) = \sum_{x \in R(32)} e^{2\pi i N(x) z} - \sum_{x \in I} e^{2\pi i N(x) z},$$

satisfies that $\Theta = -6g$.

Letting $f = \theta(v)$, we get that

$$f = 2(q^3 - q^{11} - q^{19} - 2q^{35} + 3q^{43} + 2q^{51} + q^{59} - q^{67} - q^{75} + q^{83} - 2q^{91} + q^{99} + O(q^{100})).$$

Then, by Theorem 2.5.3 f maps to (a multiple of) g by the Shimura map. Note that f lies in the Kohnen plus space, while the forms used in the main theorem of [Tun83] do not.

Since the level of f is even (and not square-free), we can not apply Theorem 2.5.8 to relate the coefficients of f with the central values of the twists of $L(E, s)$. So we need to go back to the original work of Waldspurger (see [Wal91]), from where we extract the following result.

Theorem. *Let ψ denote the quadratic character $\left(\frac{-1}{*}\right)$. Let $f \in S_{3/2}(128, \psi)$ mapping to g by the Shimura map. Then for square-free $n_1, n_2 \in \mathbb{N}$ such that $n_1/n_2 \in (\mathbb{Q}_2^\times)^2$,*

$$a_{n_1}^2 L(E \otimes n_2, 1)\psi(n_1/n_2)(n_2/n_1)^{1/2} = a_{n_2}^2 L(E \otimes n_1, 1).$$

Then using that $L(E \otimes 3, 1) \neq 0$, by the theorem of Coates-Wiles we get that $3, 11, 18, 35, 43, 51, \ldots$ are not congruent numbers.

By repeating this procedure using an order of discriminant 32 which belongs to the class B at $p = 2$, we obtain that the form $\tilde{f} \in S_{3/2}(128, \psi)$ whose q-expansion is

$$\tilde{f} = 2(q + q^9 - 4q^{17} - 3q^{25} + 4q^{33} + q^{49} + 4q^{57} + 4q^{73} - 3q^{81} - 4q^{89} - 4q^{97} + O(q^{100}))$$

also maps to g by the Shimura map (thus showing the lack of multiplicity one in the Kohnen plus space with level 128). Then using that $L(E, 1) \neq 0$, by the theorem of Coates-Wiles we get that $17, 33, 57, 73, 89, 97, \ldots$ are not congruent numbers, while if the Birch and Swinnerton-Dyer conjecture holds, then 41 and 65 are congruent numbers.

Bibliography

[AL13] Timothy W. Atwill and Benjamin Linowitz. Newform theory for Hilbert Eisenstein series. *Ramanujan J.*, 30(2):257–278, 2013.

[BM07] Ehud Moshe Baruch and Zhengyu Mao. Central value of automorphic L-functions. *Geom. Funct. Anal.*, 17(2):333–384, 2007.

[Brz82] Juliusz Brzeziński. A characterization of Gorenstein orders in quaternion algebras. *Math. Scand.*, 50(1):19–24, 1982.

[Brz83] Juliusz Brzeziński. On orders in quaternion algebras. *Comm. Algebra*, 11(5):501–522, 1983.

[Brz90] Juliusz Brzeziński. On automorphisms of quaternion orders. *J. Reine Angew. Math.*, 403:166–186, 1990.

[BSP90] Siegfried Böcherer and Rainer Schulze-Pillot. On a theorem of Waldspurger and on Eisenstein series of Klingen type. *Math. Ann.*, 288(3):361–388, 1990.

[Coh00] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[CS01] Caterina Consani and Jasper Scholten. Arithmetic on a quintic threefold. *Internat. J. Math.*, 12(8):943–972, 2001.

[DD08] Lassina Dembélé and Steve Donnelly. Computing Hilbert modular forms over fields with nontrivial class group. In *Algorithmic number theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 371–386. Springer, Berlin, 2008.

[Dem05] Lassina Dembélé. Explicit computations of Hilbert modular forms on $\mathbb{Q}(\sqrt{5})$. *Experiment. Math.*, 14(4):457–466, 2005.

[DV10] Lassina Dembele and John Voight. Explicit methods for Hilbert modular forms. 2010. http://arxiv.org/abs/1010.5727

[Eic73] M. Eichler. The basis problem for modular forms and the traces of the Hecke operators. In *Modular functions of one variable, I (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 75–151. Lecture Notes in Math., Vol. 320. Springer, Berlin, 1973.

[EMP86] H. M. Edgar, R. A. Mollin, and B. L. Peterson. Class groups, totally positive units, and squares. *Proc. Amer. Math. Soc.*, 98(1):33–37, 1986.

[Gar90] Paul B. Garrett. *Holomorphic Hilbert modular forms*. The Wadsworth & Brooks/Cole Mathematics Series. Wadsworth & Brooks/Cole Advanced Books & Software, Pacific Grove, CA, 1990.

[Geb09] Ute Gebhardt. Explicit construction of spaces of Hilbert modular cusp forms using quaternionic theta series. 2009. Thesis (Ph.D.)–Universitat des Saarlandes.

[Gel75] Stephen S. Gelbart. *Automorphic forms on adèle groups*. Princeton University Press, Princeton, N.J., 1975. Annals of Mathematics Studies, No. 83.

[GL09] Benedict H. Gross and Mark W. Lucianovic. On cubic rings and quaternion rings. *J. Number Theory*, 129(6):1468–1478, 2009.

[Gro87] Benedict H. Gross. Heights and the special values of L-series. In *Number theory (Montreal, Que., 1985)*, volume 7 of *CMS Conf. Proc.*, pages 115–187. Amer. Math. Soc., Providence, RI, 1987.

[Hec40] E. Hecke. Analytische Arithmetik der positiven quadratischen Formen. *Danske Vid. Selsk. Math.-Fys. Medd.*, 17(12):134, 1940.

[HI13] Kaoru Hiraga and Tamotsu Ikeda. On the Kohnen plus space for Hilbert modular forms of half-integral weight I. 2013. Preprint.

[Hid81] Haruzo Hida. On abelian varieties with complex multiplication as factors of the Jacobians of Shimura curves. *Amer. J. Math.*, 103(4):727–776, 1981.

[HS73] Hiroaki Hijikata and Hiroshi Saito. On the representability of modular forms by theta series. In *Number theory, algebraic geometry and commutative algebra, in honor of Yasuo Akizuki*, pages 13–21. Kinokuniya, Tokyo, 1973.

[Kap69] Irving Kaplansky. Submodules of quaternion algebras. *Proc. London Math. Soc. (3)*, 19:219–232, 1969.

[Kob93] Neal Koblitz. *Introduction to elliptic curves and modular forms*, volume 97 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1993.

[Koh82] Winfried Kohnen. Newforms of half-integral weight. *J. Reine Angew. Math.*, 333:32–72, 1982.

[KV10] Markus Kirschmer and John Voight. Algorithmic enumeration of ideal classes for quaternion orders. *SIAM J. Comput.*, 39(5):1714–1747, 2010.

[Lem11] Stefan Lemurell. Quaternion orders and ternary quadratic forms. 2011. http://arxiv.org/abs/1103.4922

[Miy71] Toshitsune Miyake. On automorphic forms on GL_2 and Hecke operators. *Ann. of Math. (2)*, 94:174–189, 1971.

[Piz76a] Arnold Pizer. On the arithmetic of quaternion algebras. II. *J. Math. Soc. Japan*, 28(4):676–688, 1976.

[Piz76b] Arnold Pizer. The representability of modular forms by theta series. *J. Math. Soc. Japan*, 28(4):689–698, 1976.

[Piz80] Arnold Pizer. An algorithm for computing modular forms on $\Gamma_0(N)$. *J. Algebra*, 64(2):340–390, 1980.

[Pra77] Gopal Prasad. Strong approximation for semi-simple groups over function fields. *Ann. of Math. (2)*, 105(3):553–572, 1977.

[PRV00] Ariel Pacetti and Fernando Rodríguez Villegas. Computational number theory, 2000. http://www.ma.utexas.edu/users/villegas/cnt/cnt.html

[PRV05] Ariel Pacetti and Fernando Rodríguez Villegas. Computing weight 2 modular forms of level p^2. *Math. Comp.*, 74(251):1545–1557 (electronic), 2005. With an appendix by B. Gross.

[PS13] Ariel Pacetti and Nicolás Sirolli. Computing ideal classes representatives in quaternion algebras. 2013. Available at http://arxiv.org/abs/1007.2821. To appear in *Mathematics of Computation*.

[PT07] Ariel Pacetti and Gonzalo Tornaría. Shimura correspondence for level p^2 and the central values of L-series. *J. Number Theory*, 124(2):396–414, 2007.

[S$^+$11] W. A. Stein et al. *Sage Mathematics Software (Version 4.7)*. The Sage Development Team, 2011. http://www.sagemath.org.

[Sha90] F. Shahidi. Best estimates for Fourier coefficients of Maass forms. In *Automorphic forms and analytic number theory (Montreal, PQ, 1989)*, pages 135–141. Univ. Montréal, Montreal, QC, 1990.

[Shi73] Goro Shimura. On modular forms of half integral weight. *Ann. of Math. (2)*, 97:440–481, 1973.

[Shi75] Takuro Shintani. On construction of holomorphic cusp forms of half integral weight. *Nagoya Math. J.*, 58:83–126, 1975.

[Shi78] Goro Shimura. The special values of the zeta functions associated with Hilbert modular forms. *Duke Math. J.*, 45(3):637–679, 1978.

[Shi87] Goro Shimura. On Hilbert modular forms of half-integral weight. *Duke Math. J.*, 55(4):765–838, 1987.

[Shi93a] Goro Shimura. On the Fourier coefficients of Hilbert modular forms of half-integral weight. *Duke Math. J.*, 71(2):501–557, 1993.

[Shi93b] Goro Shimura. On the transformation formulas of theta series. *Amer. J. Math.*, 115(5):1011–1052, 1993.

[Si12] Nicolás Sirolli. Preimages for the Shimura map on Hilbert modular forms. 2012. Available at http://arxiv.org/abs/1208.4011. Submitted.

[SW05] Jude Socrates and David Whitehouse. Unramified Hilbert modular forms, with examples relating to elliptic curves. *Pacific J. Math.*, 219(2):333–364, 2005.

[Tun83] J. B. Tunnell. A classical Diophantine problem and modular forms of weight $3/2$. *Invent. Math.*, 72(2):323–334, 1983.

[Vig76] Marie-France Vignéras. Simplification pour les ordres des corps de quaternions totalement définis. *J. Reine Angew. Math.*, 286/287:257–277, 1976.

[Vig80] Marie-France Vignéras. *Arithmétique des algèbres de quaternions*, volume 800 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

[Voi10] John Voight. Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms. 2010. http://arxiv.org/abs/1004.0994

[Wal91] Jean-Loup Waldspurger. Correspondances de Shimura et quaternions. *Forum Math.*, 3(3):219–307, 1991.

[Wal94] Lynne H. Walling. A remark on differences of theta series. *J. Number Theory*, 48(2):243–251, 1994.

[Wei80] André Weil. *Dirichlet Series and Automorphic Forms*, volume 189 of *Lecture Notes in Mathematics*. Springer, Berlin, 1971.

[Wil86] Andrew Wiles. On p-adic representations for totally real fields. *Ann. of Math. (2)*, 123(3):407–456, 1986.

[Xue11] Hui Xue. Central values of L-functions and half-integral weight forms. *Proc. Amer. Math. Soc.*, 139(1):21–30, 2011.

Index