Modular forms and elliptic curves over imaginary quadratic fields

Mark Lingham, MMath

Thesis submitted to The University of Nottingham
for the degree of Doctor of Philosophy

October 2005

Abstract

The aim of this thesis is to contribute to an ongoing project to understand the correspondence between cusp forms, for imaginary quadratic fields, and elliptic curves. This contribution mainly takes the form of developing explicit constructions and computing particular examples. It is hoped that as well as being of interest in themselves, they will be helpful in guiding future theoretical developments.

Cremona [7] began the programme of extending the classical techniques using modular symbols to the case of imaginary quadratic fields. He was followed by two of his students Whitley [25] and Bygott [5]. Together they have covered the cases where the class number of the field is equal to 1 or 2. This thesis extends their work to treat all fields of odd class number. It describes an algorithm, which holds for any such field, for determining the space of cusp forms, and for computing the eigenforms and eigenvalues for the action of the Hecke algebra on this space. The approach, using modular symbols, closely follows the work of the previous authors, but new techniques and theoretical simplifications are obtained which hold in the case considered.

All of the algorithms presented in this thesis have been implemented in a computer algebra package, Magma [3], and the results obtained for the fields $\mathbb{Q}(\sqrt{-23})$ and $\mathbb{Q}(\sqrt{-31})$ are included.

Acknowledgements

First, I would like to thank my supervisor Prof. J. E. Cremona for suggesting the topic of this thesis to me. His help and advice over the course of my PhD has been invaluable.

I would also like to thank my two examiners, Dr D. Delbourgo and Dr A. F. Jarvis, for taking the time to thoroughly read my thesis and suggest improvements.

Finally, I would like to thank my friends and family for all their help and encouragement. In particular I would like to give special thanks to Eleanor for her love and support.

Contents

List of Tables

List of Figures

Introduction

This thesis forms part of an ongoing project to understand the correspondence between cusp forms over imaginary quadratic number fields, and elliptic curves, both from a theoretical and a computational point of view.

There is already a sophisticated theoretical approach, using adeles, to automorphic forms over general global fields k which arose out of trying to generalise the classical case $k = \mathbb{Q}$, see [24]. Unfortunately this description is not amenable to computational investigation, but when k is an imaginary quadratic field an especially concrete description can be obtained. This description was developed initially by John Cremona in the case $h_k = 1$, see [8] and [25]. Later the theory was extended to the case $h_k = 2$, by one of his students.

The main motivation for the work in this thesis comes from the theory of elliptic curves, where an analogue of the Taniyama-Weil conjecture predicts that there is a correspondence between elliptic curves and certain modular forms defined over imaginary quadratic fields.

Over $\mathbb{Q}$ this correspondence is very well understood and many results have been proved. There exist good computational techniques for computing newforms, and given such a form for computing a matching elliptic curve, see [9]. From the work of Wiles *et al.* it is known that every elliptic curve over $\mathbb{Q}$ arises in this way, [26].

Cremona and two of his students Whitley and Bygott, have extended these computations to the case of imaginary quadratic fields $k = \mathbb{Q}(\sqrt{-d})$. The computations become more difficult as the arithmetic of k becomes more complicated. In [8] Cremona extended the classical theory to the five Euclidean fields, $d = 1, 2, 3, 7, 11$. Later Whitley, in her thesis [25], extended this work to the remaining four fields with class number one, $d = 19, 43, 67, 163$. Then Bygott [5], carried out work on class number two fields for his thesis, in particular $\mathbb{Q}(\sqrt{-5})$.

The situation is more complicated than in the classical case as the correspondence does not seem to hold in such generality. The definition of a modular form over an imaginary quadratic field is not given until chapter 2, but as motivation we state here the current conjecture about the precise relationship between modular forms and elliptic curves:

Conjecture 1. *Let k be an imaginary quadratic field. Then in general there is a one-to-one correspondence between rational newforms of weight 2, level $\mathfrak{n}$ and isogeny classes of elliptic curves defined over k with conductor $\mathfrak{n}$. There are the following exceptions to this rule:*

1. *If E has complex multiplication by an order in k, then E is associated with an Eisenstein series and not a cusp form.*
2. *If for a cusp form f there exists a quadratic character ε of $\mathrm{Gal}(\overline{k}/k)$ such that $f \otimes \varepsilon$ is the lift of a cusp form over $\mathbb{Q}$, then f corresponds to a 2-dimensional abelian variety over $\mathbb{Q}$.*

Outside of these two exceptional cases we have:

1. *For primes $\mathfrak{p}$ not dividing $\mathfrak{n}$, the Trace of Frobenius of the curve at $\mathfrak{p}$ is equal to the eigenvalue of $T_{\mathfrak{p}}$ acting on the space generated by the newform.*
2. *For primes $\mathfrak{p}$ dividing $\mathfrak{n}$: if $\mathfrak{p}^2$ divides $\mathfrak{n}$ then the Trace of Frobenius of the curve at $\mathfrak{p}$ is 0; otherwise it is minus the corresponding eigenvalue of $W_{\mathfrak{p}}$.*

Unlike in the classical case where the Eichler-Shimura construction provides a way of constructing an elliptic curve from a newform, the link between newforms and curves over number fields remains circumstantial.

This thesis attempts to describe and give examples of the correspondence for imaginary quadratic fields of odd class number. The results obtained are illustrated by calculations for the fields $\mathbb{Q}(\sqrt{-23})$ and $\mathbb{Q}(\sqrt{-31})$, which have class number 3. The non-trivial class group poses several difficulties but in the odd class number case we are able to make use of the fact that every ideal class is a square. This fact is significant because we are working with matrices in GL_2.

We will describe an algorithm for determining the space of cusp forms and for computing the eigenforms and eigenvalues for the action of the Hecke algebra on this space, for fields of odd class number. The approach using modular symbols, closely follows the work of Cremona and his earlier students, but new features arise from the increased size of the class group.

Having constructed cusp forms of weight two explicitly using the method of modular symbols, we then compare them with elliptic curves, found independently, with the corresponding conductor, to provide evidence for the conjecture.

The first two chapters of this thesis sets out the necessary background material to explain and motivate the algorithm which forms the main body of work. Chapter 1 of this thesis sets out some basic definitions and results which will be used throughout. The second chapter begins by giving an adelic description of modular forms and then derives a much simpler definition which is used in the remainder of the thesis. The chapter gives a synopsis of earlier accounts, and closely follows the exposition in [5], with some new simplifications coming from the fact that the class number is odd. In the final section of chapter 2 the link between the space of cusp forms and certain homology groups is established. All calculations carried out later in the thesis take place in these homology spaces and then make use of the link to deduce things about cusp forms.

The second part of this thesis describes the modular symbol algorithm developed for finding and describing cusp forms. The algorithm comprises several stages, which are explained in chapters 3 to 6. Chapter 3 outlines the geometrical algorithm for determining a fundamental region for the action of $\mathrm{GL}_2(\mathcal{O})$ on hyperbolic 3-space, $\mathcal{H}_3^*$. It is then shown how this can be used to form a tessellation of $\mathcal{H}_3^*$ by hyperbolic polyhedra. The following chapter then describes how, using modular symbols, this information enables us to calculate the homology group $\mathrm{H}_1(\Gamma_0(\mathfrak{n}) \setminus \mathcal{H}_3^*, \mathbb{Q})$ which is dual to the space of cusp forms of level $\mathfrak{n}$. Chapter 5 begins by defining Hecke operators in terms of their action on lattices. Certain correspondences are then used to describe their action on cusp forms. Certain other useful operators are then defined. Chapter 6 explains how these operators can be used to identify and describe the special type of cusp forms that we are interested in. All of the algorithms described in this part of the thesis have been implemented in Magma, [3].

Chapter 7 comprises the final part of the thesis and contains details of all the results obtained for the fields $\mathbb{Q}(\sqrt{-23})$ and $\mathbb{Q}(\sqrt{-31})$.

Chapter 1

Background material

This chapter describes some of the background material necessary to understand the main algorithm described later. It also serves to set up various notations that will be used throughout and contains a brief discussion of elliptic cures.

Most of the material presented here is standard and so the treatment is fairly brief. The results presented here are not for the most part new. The only new results are the result about elliptic curves over $\mathbb{Q}(\sqrt{-23})$ with everywhere good reduction, Lemma 1.2.5-1.2.7 and Lemma 1.5.1.

1.1 Quadratic number fields

Let $k = \mathbb{Q}(\sqrt{d}) \subset \mathbb{C}$ be an imaginary quadratic number field. We always suppose that $d < 0$ is a square-free integer. We write $\mathcal{O}$ for the ring of integers of an arbitrary k, and $\mathcal{O}_k$ when we want to talk about a specific field. Similarly we use h and h_k to denote class numbers.

The ring of integers $\mathcal{O}$ has the $\mathbb{Z}$-basis consisting of 1 and ω where

$$\omega = \begin{cases} \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4 \\ \sqrt{d} & \text{if } d \equiv 2,3 \pmod 4 \end{cases}$$

We will be working specifically with the fields $k = \mathbb{Q}(\sqrt{-23})$ and $k = \mathbb{Q}(\sqrt{-31})$. Later, when we want to calculate the action of Hecke operators, we will need a list of all prime ideals of small norm in these two fields. This information will also be needed when we generate a list of levels. We record in tables A.1 and A.2, in Appendix A, a list of all prime ideals with norm less than 200 in $\mathcal{O}_{\mathbb{Q}(\sqrt{-23})}$ and

$\mathcal{O}_{\mathbb{Q}(\sqrt{-31})}$.

These lists can be obtained by going through all prime ideals in $\mathbb{Z}$ in turn and determining how they behave when lifted to $\mathcal{O}_k$. This motivates the following notation for prime ideals which is used throughout this thesis; When p splits as a product of principal primes we write the generator of each prime ideal in the form $a\omega + b$, $a, b \in \mathbb{Z}$, $a > 0$. Then we set $\mathfrak{p}_p$ to be the prime of $\mathcal{O}$ above p with $\mid b \mid$ smallest, and $\overline{\mathfrak{p}}_p$ for its conjugate. As both fields have class number 3, when p splits as the product of non-principal primes, the product contains one prime ideal from each non-trivial ideal class. Fixing a choice of labels for these classes we write $\mathfrak{p}_p$ for the prime from the first class and $\overline{\mathfrak{p}}_p$ for the prime from the second.

1.2 Modules over Dedekind domains

Here we collect a few results about modules over Dedekind domains that we will need later.

Proposition 1.2.1. *Let I be an integral ideal of $\mathcal{O}$. For any non-zero element $\alpha \in I$ there exists an element $\beta \in I$ such that*

$$I = \alpha\mathcal{O} + \beta\mathcal{O}.$$

Proof. [6], Proposition 4.7.7 (1), pg 192. □

Lemma 1.2.2. *Let $\mathfrak{a}$ be fractional ideal and $\mathfrak{b}$ an integral ideal of a Dedekind domain $\mathfrak{D}$. Then there exists an integral ideal in the same ideal class as $\mathfrak{a}$ and coprime to $\mathfrak{b}$.*

Proof. [5], Lemma 1, pg 11. □

The following structure theory can be found in any textbook on module theory, for example [2].

Let T be a finitely generated torsion module over $\mathcal{O}$. Then standard structure theory tells us that there exist integral ideals $\mathfrak{a}_i$ such that

$$T \cong \frac{\mathcal{O}}{\mathfrak{a}_1} \oplus \cdots \oplus \frac{\mathcal{O}}{\mathfrak{a}_r}. \tag{1.1}$$

If further we assume that $\mathfrak{a}_i \supseteq \mathfrak{a}_{i-1}$, then this decomposition is unique up to isomorphism.

We define

$$\mathrm{ord}(T) \;=\; \prod \mathfrak{a}_i \tag{1.2}$$

for any decomposition of the form (1.1).

Let M be a non-zero finitely generated torsion-free $\mathcal{O}$-module. By standard structure theory,

$$M \;\cong\; \mathfrak{b} \oplus \mathcal{O}^{r-1}, \tag{1.3}$$

where r is the rank of M, $\mathfrak{b}$ is an ideal of $\mathcal{O}$ and the ideal class $\mathrm{cl}(\mathfrak{b})$ of $\mathfrak{b}$ is uniquely determined, whilst $\mathfrak{b}$ may be any ideal in that class. We call $\mathrm{cl}(\mathfrak{b})$ the **Steinitz class** of M, and write

$$\mathrm{cl}(M) = \mathrm{cl}(\mathfrak{b}).$$

A special case of (1.3) is that for any two ideals $\mathfrak{a}$ and $\mathfrak{b}$,

$$\mathfrak{a} \oplus \mathfrak{b} \cong \mathfrak{a}\mathfrak{b} \oplus \mathcal{O}. \tag{1.4}$$

Note that if the Steinitz class of M is principal then M is isomorphic to $\mathcal{O}^r$.

Theorem 1.2.3 (Invariant factor theorem). *Let $N \subseteq M$ be finitely generated torsion-free A-modules of the same rank r. Then there exist elements $e_1, \ldots, e_r$ of M, fractional ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$, and integral ideals $\mathfrak{b}_1 \supseteq \ldots \supseteq \mathfrak{b}_r$ such that*

$$\begin{aligned} M &= \mathfrak{a}_1 e_1 \oplus \cdots \oplus \mathfrak{a}_r e_r, \\ N &= \mathfrak{a}_1 \mathfrak{b}_1 e_1 \oplus \cdots \oplus \mathfrak{a}_r \mathfrak{b}_r e_r. \end{aligned}$$

The ideals $\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_r$ are uniquely determined by the pair M, N, and are called the invariant factors of N in M.

Proof. [11], Theorem 22.12, pg 150. □

Corollary 1.2.4. *Let $N \subseteq M$ be finitely generated torsion-free $\mathcal{O}$-modules of the same rank r. Then M/N is a finitely generated torsion module. We define the* ***index of M in N*** *to be* $\mathrm{ord}(M/N)$*. It satisfies the following property*

$$\mathrm{cl}(N) = \mathrm{cl}(M)\,\mathrm{cl}(\mathrm{ord}(M/N)).$$

Proof. Using (1.4) and Theorem 1.2.3 we have $\mathrm{cl}(M) = \mathrm{cl}(\prod \mathfrak{a}_i)$, $\mathrm{cl}(N) = \mathrm{cl}(\prod \mathfrak{a}_i\mathfrak{b}_i)$, whilst $M/N \cong \prod(\mathcal{O}/\mathfrak{b}_i)$, so $\mathrm{ord}(M/N) = \prod \mathfrak{b}_i$. □

In particular, if M is free then N is free if and only if $\mathrm{ord}(M/N)$ is a principal ideal.

Now if $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals of $\mathcal{O}$ such that $\mathfrak{ab}$ is principal then

$$\mathfrak{a} \oplus \mathfrak{b} \cong \mathfrak{ab} \oplus \mathcal{O} \cong \mathcal{O} \oplus \mathcal{O}$$

If we represent elements of $\mathfrak{a} \oplus \mathfrak{b}$ by row vectors then the isomorphism is represented by a 2×2 matrix over $\mathcal{O}$. If we in fact look at the isomorphism right to left, we get a matrix $M_{\mathfrak{a},\mathfrak{b}}$, whose first column generates $\mathfrak{a}$ and whose second column generates $\mathfrak{b}$. The index of $\mathfrak{a} \oplus \mathfrak{b}$ in $\mathcal{O} \oplus \mathcal{O}$ is simply $\mathfrak{ab}$.

Lemma 1.2.5. *Given ideals $\mathfrak{a}$,$\mathfrak{b}$ and $\mathfrak{n}$, such that $\mathfrak{ab} = \langle \mu \rangle$, there exists a matrix M, with determinant μ, which gives an isomorphism $\mathcal{O} \oplus \mathcal{O} \to \mathfrak{a} \oplus \mathfrak{b}$ and whose lower left entry lies in $\mathfrak{n}$.*

Proof. By Proposition 1.2.1 we can choose an $\mathcal{O}$-basis of x, z of $\mathfrak{a}$ with $z \in \mathfrak{n}$. Then

$$\begin{aligned}\langle \mu \rangle &= \mathfrak{ab} \\ &= \langle x, z \rangle \mathfrak{b} \\ &= x\mathfrak{b} + z\mathfrak{b}\end{aligned}$$

so we can solve $\mu = xw - zy$ with $y, w \in \mathfrak{b}$. Then we take

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

This gives the isomorphism we want. Since $x, z \in \mathfrak{a}$ and $y, w \in \mathfrak{b}$ we have $\mathcal{O}^2 \cdot M \subseteq \mathfrak{a} \oplus \mathfrak{b}$. But now suppose $(u, v) \in \mathfrak{a} \oplus \mathfrak{b}$. Then we claim that we can find $(r, s) \in \mathcal{O}^2$ such that $(r, s)M = (u, v)$. We have $(r, s) = (u, v)M^{-1}$, so $\mu r = uw - vz$, $\mu s = -uy + vx$. Now uw, vz, uy, vx all contain one element from $\mathfrak{a}$ and one from $\mathfrak{b}$, and so are divisible by μ. Hence such a pair (r, s) exists, so in fact $\mathcal{O}^2 \cdot M = \mathfrak{a} \oplus \mathfrak{b}$. □

Lemma 1.2.6. *Suppose $M = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$ satisfies $x, z \in \mathfrak{a}$ and $y, w \in \mathfrak{b}$. Then $\mathcal{O}^2 \cdot M = \mathfrak{a} \oplus \mathfrak{b}$ if and only if $\langle \det(M) \rangle = \mathfrak{ab}$.*

Proof. The proof of Lemma 1.2.5 gives $\Leftarrow$. The implication in the other direction follows from the following argument. Suppose we have a matrix M such that $\mathcal{O}^2 \cdot M = \mathfrak{a} \oplus \mathfrak{b}$. Then using the construction in the above proof we can find another matrix M' with the same property that has determinant μ. It follows that

$$\mathcal{O}^2 \cdot MM'^{-1} = \mathcal{O}^2 \cdot M'M^{-1} = \mathcal{O}^2$$

Hence MM'^{-1} and $M'M^{-1}$ have integral entries, hence integral determinants. Thus the determinants of M and M' differ by at most a unit. □

Now we want to be able to find all submodules, $\mathcal{A}$, of $\mathcal{O} \oplus \mathcal{O}$ with a given principal index $\mathfrak{m}$. We need to consider each factorisation $\mathfrak{m} = \mathfrak{ab}$, with $\mathfrak{b} \mid \mathfrak{a}$, and find all $\mathcal{A}$ such that

$$\frac{\mathcal{O} \oplus \mathcal{O}}{\mathcal{A}} \cong \frac{\mathcal{O}}{\mathfrak{a}} \oplus \frac{\mathcal{O}}{\mathfrak{b}}.$$

In general $\mathcal{A}$ will have the form

$$\mathcal{A} = \mathcal{O}^2 \cdot M_{\mathfrak{a},\mathfrak{b}} V,$$

for some $V \in \mathrm{GL}_2(\mathcal{O})$.

We want to know when two such expressions give the same submodule. If we define

$$\Gamma_0(\mathfrak{n}) \quad := \quad \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}) : c \in \mathfrak{n} \right\}, \tag{1.5}$$

for $\mathfrak{n}$ a non-zero ideal in $\mathcal{O}$,then the answer is given by the following Lemma:

Lemma 1.2.7. *Let $\mathfrak{b} \mid \mathfrak{a}$. Define $M_{\mathfrak{a},\mathfrak{b}}$ as before and let $V_1, V_2 \in \mathrm{GL}_2(\mathcal{O})$. Then*

$$\mathcal{O}^2 \cdot M_{\mathfrak{a},\mathfrak{b}} V_1 = \mathcal{O}^2 \cdot M_{\mathfrak{a},\mathfrak{b}} V_2 \Longleftrightarrow V_1 \in \Gamma_0(\mathfrak{a}\mathfrak{b}^{-1}) V_2.$$

Proof. Now

$$\begin{aligned} \mathcal{O}^2 \cdot M_{\mathfrak{a},\mathfrak{b}} V_1 = \mathcal{O}^2 \cdot M_{\mathfrak{a},\mathfrak{b}} V_2 &\iff \mathcal{O}^2 \cdot M_{\mathfrak{a},\mathfrak{b}} V_1 V_2^{-1} = \mathcal{O}^2 \cdot M_{\mathfrak{a},\mathfrak{b}} \\ &\iff (\mathfrak{a} \oplus \mathfrak{b}) \cdot V_1 V_2^{-1} = \mathfrak{a} \oplus \mathfrak{b} \end{aligned}$$

So we need to know when

$$(\mathfrak{a} \oplus \mathfrak{b}) \cdot V = \mathfrak{a} \oplus \mathfrak{b}.$$

Let $V = \left(\begin{smallmatrix} v_1 & v_2 \\ v_3 & v_4 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathcal{O})$. Then

$$\begin{aligned} (\mathfrak{a} \oplus \mathfrak{b}) \cdot V &= \left\{ \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} v_1 & v_2 \\ v_3 & v_4 \end{pmatrix} : x \in \mathfrak{a}, y \in \mathfrak{b} \right\} \\ &= \left\{ \begin{pmatrix} xv_1 + yv_3 & xv_2 + yv_4 \end{pmatrix} : x \in \mathfrak{a}, y \in \mathfrak{b} \right\} \end{aligned}$$

Then

$$\begin{aligned} (\mathfrak{a} \oplus \mathfrak{b}) \cdot V = \mathfrak{a} \oplus \mathfrak{b} &\iff xv_1 + yv_3 \in \mathfrak{a},\ xv_2 + yv_4 \in \mathfrak{b} \quad \forall\, x \in \mathfrak{a}, y \in \mathfrak{b} \\ &\iff yv_3 \in \mathfrak{a},\ xv_2 \in \mathfrak{b} \\ &\iff v_3 \in \mathfrak{a}\mathfrak{b}^{-1} \end{aligned}$$

since $\mathfrak{b} \mid \mathfrak{a} \Rightarrow \mathfrak{b} \supset \mathfrak{a}$ so $xv_2 \in \mathfrak{a} \Rightarrow xv_2 \in \mathfrak{b}$.

Therefore

$$(\mathfrak{a} \oplus \mathfrak{b}) \cdot V = \mathfrak{a} \oplus \mathfrak{b} \Longleftrightarrow V \in \Gamma_0(\mathfrak{a}\mathfrak{b}^{-1}).$$

□

So to get all possible submodules of index $\mathfrak{m}$ we take the set

$$\{\mathcal{O}^2 \cdot M_{\mathfrak{a},\mathfrak{b}} W\},$$

where $\mathfrak{a}, \mathfrak{b}$ run over all factorisations $\mathfrak{m} = \mathfrak{a}\mathfrak{b}$ with $\mathfrak{b} \mid \mathfrak{a}$, and W runs through a set of right coset representatives of $\Gamma_0(\mathfrak{a}\mathfrak{b}^{-1})$ in $\mathrm{GL}_2(\mathcal{O})$.

1.3 Elliptic curves

Most of the results stated here are well known and can be found in any standard textbook, such as [20].

As before let k be an imaginary quadratic number field with ring of integers $\mathcal{O}$. Define E, an **elliptic curve** defined over k, to be a smooth projective curve over k of genus 1 with a fixed k-rational point O. It is well known, see [20], that E can be described by an equation of the form:

$$y^2z + a_1xyz + a_3yz^2 \;=\; x^3 + a_2x^2z + a_4xz^2 + a_6z^3, \tag{1.6}$$

where $a_i \in \mathcal{O}$ and the distinguished point O is the point at infinity $(0:1:0)$.

We define:

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= a_1a_3 + 2a_4, \\ b_6 &= a_3^2 + 4a_6, \\ c_4 &= b_2^2 - 24b_4, \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6, \end{aligned}$$

and the **discriminant** of E is

$$\Delta \;=\; \frac{c_4^3 - c_6^2}{1728}. \tag{1.7}$$

The non-singularity or smoothness of E is equivalent to $\Delta \neq 0$.

The **j-invariant** of an elliptic curve is defined to be

$$j(E) \;=\; \tfrac{c_4^3}{\Delta} \;=\; 1728 + \tfrac{c_6^2}{\Delta} \in k.$$

Proposition 1.3.1. *Two elliptic curves are isomorphic over $\overline{k}$ if and only if they have the same j-invariant.*

Proof. [20] □

Now we fix a prime ideal $\mathfrak{p} \lhd \mathcal{O}$. We define $E_{\mathfrak{p}}$, the **reduction** of E, modulo $\mathfrak{p}$, to be:

$$y^2z + \overline{a_1}xyz + \overline{a_3}yz^2 \;=\; x^3 + \overline{a_2}x^2z + \overline{a_4}xz^2 + \overline{a_6}z^3, \tag{1.8}$$

where $\overline{a_i}$ is the reduction of a_i modulo $\mathfrak{p}$. $E_{\mathfrak{p}}$ is defined over $\mathcal{O}/\mathfrak{p}$. If the class number of k is greater than one there may not be a global minimal model, but we can assume that the model is minimal at $\mathfrak{p}$. Then $E_{\mathfrak{p}}$ is an elliptic curve if and only if $\overline{\Delta} \neq 0$. If $\mathrm{ord}_{\mathfrak{p}}(\Delta) \geq 0$ then $E_{\mathfrak{p}}$ is **singular** and we say that E has **bad reduction** at $\mathfrak{p}$. The reduction is said to be

$$\begin{cases} \textbf{multiplicative} & \text{if } E_{\mathfrak{p}} \text{ has a node,} \\ \textbf{additive} & \text{if } E_{\mathfrak{p}} \text{ has a cusp.} \end{cases}$$

If $E_{\mathfrak{p}}$ has multiplicative reduction then the reduction is said to be **split** if the slopes of the tangents at the node are in $\mathcal{O}/\mathfrak{p}$ and **non-split** otherwise.

The **conductor** of E, $\mathfrak{f}_E$, is the ideal of $\mathcal{O}$ defined by:

$$\mathfrak{f}_E = \prod_{\mathfrak{p} \lhd \mathcal{O}} \mathfrak{p}^{f_{\mathfrak{p}}}, \tag{1.9}$$

where

$$f_{\mathfrak{p}} = \begin{cases} 0 & \text{if } E_{\mathfrak{p}} \text{ is non-singular,} \\ 1 & \text{if } E_{\mathfrak{p}} \text{ has multiplicative reduction,} \\ 2 + \delta_{\mathfrak{p}} & \text{if } E_{\mathfrak{p}} \text{ has additive reduction.} \\ & \text{(where } \delta_{\mathfrak{p}} \geq 0 \text{ and } \delta_{\mathfrak{p}} = 0 \text{ if } \mathrm{char}(k_{\mathfrak{p}}) \neq 2, 3) \end{cases}$$

An elliptic curve, E, is an abelian group. A **k-morphism** between 2 elliptic curves E_1 and E_2, both defined over the same field k, is a map $\psi : E_1 \to E_2$, also defined over k, which preserves the group structure.

An **isogeny** between E_1 and E_2 is a morphism

$$\psi : E_1 \to E_2,$$

satisfying $\psi(O) = O$. E_1 and E_2 are said to be **isogenous** if there exists a non-constant isogeny between them. Two isogenous elliptic curves have the same conductor.

Isogeny is an equivalence relation, so each elliptic curve belongs to a unique equivalence class which we call an **isogeny class**.

For each $m \in \mathbb{Z}$ we can define an isogeny **multiplication by *m***

$$[m] : E \longrightarrow E$$

in the natural way; If $m > 0$ then

$$[m](P) = \underbrace{P + \ldots + P}_{m \text{ terms}},$$

if $m < 0$ then $[m](P) = [-m](-P)$, and $[0](P) = O$.

Elliptic curves E_1 and E_2 are said to be **m-isogenous** if there exist isogenies

$$\phi : E_1 \longrightarrow E_2$$

$$\hat{\phi} : E_2 \longrightarrow E_1$$

such that $\hat{\phi} \circ \phi = [m]$ on E_1 and $\phi \circ \hat{\phi} = [m]$ on E_2.

The map $[\quad] : \mathbb{Z} \longrightarrow \mathrm{End}_k(E)$ is usually surjective. If it is not, i.e. if $\mathrm{End}_k(E)$ is strictly larger than $\mathbb{Z}$, then we say that E has **complex multiplication**.

Proposition 1.3.2. *Let E be an elliptic curve defined over a number field k, and assume that E has complex multiplication. Then the ring $End(E)$ is an order in an imaginary quadratic field.*

Proof. [20], Theorem 6.1, pg 165. □

If $\mathrm{End}(E) = \mathcal{O}'$, for some order $\mathcal{O}'$, then we say that E has complex multiplication by $\mathcal{O}'$.

Theorem 1.3.3. *Let k be an imaginary quadratic field, $\mathcal{O}'$ an order of k and E an elliptic curve with complex multiplication by $\mathcal{O}'$. Then the field $L = k(j(E))$ is the ring class field of $\mathcal{O}'$.*

Proof. [19], Theorem 5.4, pg 123. □

Now $[L : k] = h(\mathcal{O}')$, which will be an integer multiple of $h(\mathcal{O})$. So if k is an imaginary quadratic field of class number greater than 1 then the extension L/k will have degree at least two. If E were defined over k then we would have $j(E) \in k$, and so the extension would be trivial. Therefore no elliptic curve defined over k can have complex multiplication by an order in k. So the first exceptional case in Conjecture 1 cannot happen for the fields being considered.

Definition 1.3.4. *Let E be an elliptic curve over a number field with $\mathfrak{p}$ a prime ideal in $\mathcal{O}$ with norm $N(\mathfrak{p})$. If E has good reduction at $\mathfrak{p}$, the **local L-function** of E at $\mathfrak{p}$ is*

$$L_{\mathfrak{p}}(E,T) \ := \ 1 - a_{\mathfrak{p}}T + N(\mathfrak{p})T^2,$$

*where $a_{\mathfrak{p}}$ is the **trace of Frobenius** $N(\mathfrak{p}) + 1 - \#E_{\mathfrak{p}}$, and $\#E_{\mathfrak{p}}$ is the number of points on the reduced curve. If E has bad reduction at $\mathfrak{p}$, the **local L-function** of E at $\mathfrak{p}$ is*

$$L_{\mathfrak{p}}(E,T) = \begin{cases} 1 - T & \textit{if the reduction is split multiplicative,} \\ 1 + T & \textit{if the reduction is non-split multiplicative,} \\ 1 & \textit{if the reduction is additive.} \end{cases}$$

We can now define the **global L-series** using these local L-functions.

Definition 1.3.5. *Let E be an elliptic curve over a number field. The **(global) L-series** of E is*

$$L(E,s) := \prod_{\mathfrak{p}} L_{\mathfrak{p}}(N(\mathfrak{p})^{-s})^{-1}.$$

where $s \in \mathbb{C}$ is a complex variable with $Re(s) > 3/2$. Here the product is taken over all prime ideals of $\mathcal{O}$.

Theorem 1.3.6. *Let E be an elliptic curve over a number field k. Then the L-series of E at s with $Re(s) > 3/2$ is*

$$L(E,s) = \sum_{\mathfrak{a}} a(\mathfrak{a})N(\mathfrak{a})^{-s},$$

where the sum is over all integral ideals $\mathfrak{a}$ of $\mathcal{O}$.

If $\mathfrak{a} = \mathfrak{p}_1^{m_1} \dots \mathfrak{p}_r^{m_r}$, $m_i \in \mathbb{N}$ is the factorisation of $\mathfrak{a}$ into powers of distinct prime ideals, the integer $a(\mathfrak{a})$ is defined as

$$a(\mathfrak{a}) := a(\mathfrak{p}_1^{m_1}) \cdot \ldots \cdot a(\mathfrak{p}_r^{m_r}).$$

Further let $\mathfrak{p}$ be a prime ideal. Then

- $a(\langle 1 \rangle) = 1$,
- *if E has good reduction modulo $\mathfrak{p}$:*

$$a(\mathfrak{p}) = a_{\mathfrak{p}},$$

$$a(\mathfrak{p}^k) = a(\mathfrak{p})a(\mathfrak{p}^{k-1}) - N(\mathfrak{p})a(\mathfrak{p}^{k-2}) \text{ for } k \geq 2,$$

- *if E has split multiplicative reduction modulo $\mathfrak{p}$:*

$$a(\mathfrak{p}^k) = 1 \text{ for } k \in \mathbb{N},$$

- *if E has non-split multiplicative reduction modulo $\mathfrak{p}$:*

$$a(\mathfrak{p}^k) = (-1)^k \text{ for } k \in \mathbb{N},$$

- *if E has additive reduction modulo $\mathfrak{p}$:*

$$a(\mathfrak{p}^k) = 0 \text{ for } k \in \mathbb{N}.$$

Proof. [17], Theorem 7.4, pg 200. □

The L-series of elliptic curves are *a priori* defined only for complex numbers $s \in \mathbb{C}$ with $Re(s) > 3/2$. However conjecturally the L-series can be analytically continued to the whole complex plane. The following conjecture is due to Hasse and Weil.

Conjecture 2. *Let E be an elliptic curve over a quadratic number field k with L-series $L(s)$. Further let $\mathfrak{f}_E$ be the conductor of E, D the discriminant of k. We define*

$$\Lambda(s) := (2\pi)^{-2s} N(\mathfrak{f}_E)^{s/2} |D|^s \Gamma(s)^2 L(E, s),$$

with $\Gamma(s)$ the usual gamma function. Then $\Lambda(s)$ has an analytic continuation to the whole of $\mathbb{C}$ and satisfies

$$\Lambda(s) = \varepsilon \Lambda(2 - s),$$

with $\varepsilon \in \{\pm 1\}$.

The sign ε is called the **sign of the functional equation** of E. Conjecture 3 below is part of the Birch and Swinnerton-Dyer conjecture.

Conjecture 3. *Let E be an elliptic curve over k of rank r, with L-series satisfying a functional equation. Then*

$$\varepsilon = (-1)^{r-1}$$

So the rank of E should be odd / even if ε equal $+1/-1$.

We have the following theorem due to Faltings:

Theorem 1.3.7. *Two elliptic curves E and E' are isogenous if and only if $L(E,s) = L(E',s)$.*

Proof. See [13] □

We therefore have a one-to-one correspondence between

$$\{\text{isogeny classes of elliptic curves over } k\} \leftrightarrow \{\text{certain } L\text{-series}\}$$

Once we have a list of modular forms we will want to match them up with elliptic curves with the corresponding conductor. Therefore we will want a list of elliptic curves over $\mathbb{Q}(\sqrt{-23})$ and $\mathbb{Q}(\sqrt{-31})$ with small conductor. In the past Cremona and his students have generated this list by systematically searching through curves with small coefficients. This method was also used to find the majority of curves over the two fields considered in this thesis. However we have developed a general method for finding all elliptic curves with good reduction outside a given set of primes S. It involves calculating a list of all possible j-invariants that such a curve could have. Then one takes a standard choice of curve with each j-invariant and looks at a finite number of twists. The first step relies on being able to find all S-integral points on certain elliptic curves defined over k. So at present the lists produced by our algorithm are not necessarily complete, as we do not have a algorithm which is guaranteed to find all S-integral points. All of the details of this method can be found in [10].

As a simple illustration of some of the steps in the method we apply it here to the case $S = \emptyset$ in order to prove the following proposition.

Proposition 1.3.8. *There are no elliptic curves of everywhere good reduction over* $\mathbb{Q}(\sqrt{-23})$.

Proof. We need the following elementary lemma.

Lemma 1.3.9. *Let E be an elliptic curve over k with everywhere good reduction. Then $j \in \mathcal{O}_{\mathbb{Q}(\sqrt{-23})}$ and either $j = 0$, $j = 1728$, or j satisfies the following conditions for every prime $\mathfrak{p} \in \mathcal{O}_{\mathbb{Q}(\sqrt{-23})}$:*

$$\begin{aligned} \mathrm{ord}_{\mathfrak{p}}(j) &\equiv 0 \pmod 3 \\ \mathrm{ord}_{\mathfrak{p}}(j-1728) &\equiv 0 \pmod 2 \end{aligned}$$

Proof. Choosing a minimal model at $\mathfrak{p}$, we see that $j = \frac{c_4^3}{\Delta}$ is integral at $\mathfrak{p}$ and $\mathrm{ord}_{\mathfrak{p}}(j) = 3\,\mathrm{ord}_{\mathfrak{p}}(c_4)$ is a multiple of three, since Δ is a unit at $\mathfrak{p}$. Similarly, $j - 1728 = \frac{c_6^2}{\Delta}$ implies that $\mathrm{ord}_{\mathfrak{p}}(j-1728)$ is even. □

The first condition implies that $\langle j \rangle = \mathfrak{a}^3$ for some integral ideal of $\mathcal{O}_{\mathbb{Q}(\sqrt{-23})}$. The second condition implies that $\langle j - 1728 \rangle = \mathfrak{b}^2$ for some integral ideal of $\mathcal{O}_{\mathbb{Q}(\sqrt{-23})}$.

Since $\mathbb{Q}(\sqrt{-23})$ has class number 3, $\mathfrak{b}^2$ principal implies that $\mathfrak{b}$ must be principal, say $\mathfrak{b} = \langle y \rangle$. Let $\mathfrak{c}_1, \mathfrak{c}_2, \mathfrak{c}_3$ be integral ideals representing the 3 ideal classes and write $\mathfrak{c}_i^3 = \langle u_i \rangle$. Then $\exists\, x \in k^*$ such that $\mathfrak{a}^3 = \langle u_i x^3 \rangle$ for one of the i. So we know that $j = \pm y^2 + 1728$ and $j = \pm u_i x^3$. Combining these, and changing the sign of x if necessary, we get

$$y^2 = u_i x^3 \pm 1728.$$

Multiplying through by u_i^2 we get

$$(u_i y)^2 = (u_i x)^3 \pm 1728 u_i^2.$$

Then replacing $(u_i x, u_i y)$ by (x, y) we have

$$E_i^{\pm} : y^2 = x^3 \pm 1728 u_i^2.$$

Since $u_i x^3$ is equal to j up to a unit, it must be integral. Hence $(u_i x)^3$ is integral so $u_i x$ is integral. Likewise $u_i y$ is integral. Thus if E has everywhere good reduction it must have j-invariant coming from an integral point on one of the 6 curves $E_i^{\pm}$. We can take $\mathfrak{c}_1 = \langle 1 \rangle$, $\mathfrak{c}_2 = \langle 2, \omega \rangle$ and $\mathfrak{c}_3 = \langle 2, \omega + 1 \rangle$. Then $u_1 = 1$, $u_2 = \omega - 2$ and $u_3 = w + 1$. This gives

$$E_1^{\pm} : y^2 = x^3 \pm 1728$$

$$E_2^{\pm} : y^2 = x^3 \pm 1728(\omega - 2)^2$$

$$E_3^{\pm} : y^2 = x^3 \pm 1728(\omega + 1)^2$$

We find that $E_2^{\pm}, E_3^{\pm}$ both have rank 0 and trivial torsion. So in particular they have no integral points except the point at infinity which gives $j = 0$. It can be proven using elliptic logarithms that the only $\mathcal{O}$-integral points on $E_1^{\pm}$ are the 2-torsion points $(\mp 12, 0)$ and infinity. So we know that $j \in \{-1728, 0, 1728\}$.

Now here we do not need to use the next step of our general method, because we can make use of a special result. Define the set

$$\mathcal{R} = \left\{ A \in \mathbb{Z} : \begin{array}{l} \text{if 2 divides } A \text{ then 16 divides } A \text{ or } A - 4; \\ \text{and if 3 divides } A \text{ then 27 divides } A - 12 \end{array} \right\}.$$

A result of Setzer, ([18], Theorem 2(a)) tells us that if $j = A^3$ with $A \notin \mathcal{R}$ then no elliptic curve with that j-invariant can have everywhere good reduction. Since $-12, 0, 12 \notin \mathcal{R}$, it follows that there are no elliptic curves of everywhere good reduction over $\mathbb{Q}(\sqrt{-23})$. $\square$

1.4 $\mathcal{H}_3^*$ and some hyperbolic geometry

Define the 3-dimensional upper half-space to be:

$$\begin{aligned} \mathcal{H}_3 &= \mathbb{C} \times \mathbb{R}^+ \\ &= \{(z, t) : z \in \mathbb{C}, t > 0\} \end{aligned}$$

We define the extended 3-dimensional upper half-space to be, (as a set):

$$\mathcal{H}_3^* = \mathcal{H}_3 \cup k \cup \{\infty\}, \tag{1.10}$$

where k is associated with a fixed subfield of $\mathbb{C}$.

We will be interested in the action of the group

$$\Gamma = \mathrm{GL}_2(\mathcal{O}) \tag{1.11}$$

and certain subgroups of it on $\mathcal{H}_3^*$.

The action of $\mathrm{GL}_2(\mathbb{C})$ on $\mathcal{H}_3^*$ is defined to be:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot (z,t) \quad = \quad \left(\frac{(az+b)(\bar{c}\bar{z}+\bar{d}) + a\bar{c}t^2}{|cz+d|^2+|c|^2t^2}, \frac{|ad-bc|t}{|cz+d|^2+|c|^2t^2} \right) \tag{1.12}$$

We equip $\mathcal{H}_3$ with the hyperbolic metric

$$ds^2 \quad = \quad t^{-2}(dx^2+dy^2+dt^2), \tag{1.13}$$

where $z = x+iy$.

This is compatible with the action of $\mathrm{GL}_2(\mathbb{C})$ defined above:

Lemma 1.4.1. *The metric (1.13) is invariant under the action of* $\mathrm{GL}_2(\mathbb{C})$ *defined by (1.12).*

Proof. [23], Lemma 3.3, pg 16. □

Lemma 1.4.2.

1. *The set consisting of all hemispheres in $\mathcal{H}_3$ with centre in the plane $t = 0$, together with all vertical (half) planes in $\mathcal{H}_3$, is stable under the action of* $\mathrm{GL}_2(\mathbb{C})$.

2. *The set consisting of all vertical semicircles in $\mathcal{H}_3$ with centre in the plane $t = 0$, together with all vertical (half) lines in $\mathcal{H}_3$, is stable under the action of* $\mathrm{GL}_2(\mathbb{C})$.

3. *The set considered in 2. consists exactly of all geodesics for the metric (1.13).*

Proof. [23], Lemma 3.4, pg 16. □

The points, $\{(k,0) : k \in k\}$ and the point at infinity, $(0,\infty)$, in $\mathcal{H}_3$ are called the **cusps**. We usually represent cusps, including the cusp at infinity, as $\frac{\lambda}{\mu}$, with $\lambda, \mu \in \mathcal{O}$ not both zero, (we take $\infty = 1/0$). This expression is not unique but the ideal class $\mathrm{cl}(\langle \lambda, \mu \rangle)$ is well-defined.

Definition 1.4.3. *The* ***class*** *of a cusp* $\frac{\lambda}{\mu}$*, denoted* $\mathrm{cl}(\lambda, \mu)$*, is the ideal class of the ideal* $\langle \lambda, \mu \rangle$*. A cusp is* ***principal*** *if its class is the principal class.*

Clearly any principal cusp $\frac{\lambda}{\mu}$ may be expressed in "lowest terms", i.e. with $\langle \lambda, \mu \rangle = \mathcal{O}$. In general we have

Lemma 1.4.4. *Let* $\mathfrak{a}$ *be an integral ideal. Then every cusp with class* $\mathrm{cl}(\mathfrak{a})$ *may be written in the form* $\frac{\lambda}{\mu}$ *with* $\langle \lambda, \mu \rangle = \mathfrak{a}$*.*

Proof. If the cusp $\frac{\lambda}{\mu}$ has class $\mathrm{cl}(\mathfrak{a})$ then we can write

$$\langle \beta \rangle \langle \lambda, \mu \rangle = \mathfrak{a}$$

for some $\beta \in k^\times$, and then set

$$\lambda' = \beta\lambda, \quad \mu' = \beta\mu.$$

Then we have $\frac{\lambda'}{\mu'} = \frac{\lambda}{\mu}$, where $\lambda', \mu' \in \mathcal{O}$ and $\langle \lambda', \mu' \rangle = \mathfrak{a}$. $\square$

It is clear from (1.12) that $\mathrm{GL}_2(k)$ maps cusps to cusps and in this case the formula for the action simplifies to:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \frac{\lambda}{\mu} = \frac{a\lambda + b\mu}{c\lambda + d\mu}. \tag{1.14}$$

Considering (1.14) it can be seen that the orbit of ∞ under Γ is the set of principal cusps:

$$\left\{ \frac{\lambda}{\mu} : \lambda, \mu \in \mathcal{O}, \langle \lambda, \mu \rangle = \mathcal{O} \right\}.$$

Indeed, it clearly contains this set and to see that it cannot contain a non-principal cusp just note that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \infty = \frac{a}{c}.$$

We have $ad - bc = \pm 1$, hence $1 \in \langle a, c \rangle$ so $\langle a, c \rangle = \mathcal{O}$.

Hence the action of Γ is transitive if and only if every ideal is principal. In general we have:

Lemma 1.4.5. *The orbit of a cusp, $\alpha = \frac{\lambda}{\mu}$, under Γ is the set of cusps with class* $\mathrm{cl}(\alpha)$*.*

Proof. The action of $\mathrm{GL}_2(\mathcal{O})$ preserves the class of a cusp, since if $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, then $\langle a\lambda + b\mu, c\lambda + d\mu\rangle = \langle \lambda, \mu\rangle$. To complete the proof we now show that $\mathrm{GL}_2(\mathcal{O})$ is transitive on each class. In fact we can show that the action of $\mathrm{SL}_2(\mathcal{O})$ is transitive. Suppose $\mathrm{cl}(\lambda, \mu) = \mathrm{cl}(\lambda', \mu')$, so there is $u \in k^*$ with $\langle \lambda, \mu\rangle = u\langle \lambda', \mu'\rangle$. Set $I = \langle \lambda, \mu\rangle$ and let J be an ideal in the inverse class, with $IJ = \langle \theta\rangle$. Then we can find $a_1, a_2, b_1, b_2 \in J$ with $\theta = a_1\lambda + a_2\mu$ and $\theta = b_1(u\lambda') + b_2(u\mu')$. Put

$$\sigma = \begin{pmatrix} \frac{a_1(u\lambda')+b_2\mu}{\theta} & \frac{a_2(u\lambda')-b_2\lambda}{\theta} \\ \frac{a_1(u\mu')-b_1\mu}{\theta} & \frac{a_2(u\mu')+b_1\lambda}{\theta} \end{pmatrix}.$$

From the definition of a_1, a_2, b_1, b_2 it is clear that

$$\sigma\left(\frac{\lambda}{\mu}\right) = \frac{u\lambda'}{u\mu'} = \frac{\lambda'}{\mu'}$$

and $\det\sigma = 1$. Since the numerators of the entries of σ are by choice in IJ, σ has in fact integral entries. So $\sigma \in \mathrm{SL}_2(\mathcal{O})$ and we are done. $\square$

So there are h orbits of cusps under Γ.

1.5 Congruence subgroups

The subgroups of Γ that we will be interested in are the subgroups $\Gamma_0(\mathfrak{n})$, cf (1.5).

We will need to know when 2 cusps, α_1, α_2, are equivalent under the action of $\Gamma_0(\mathfrak{n})$. Clearly for them to be equivalent modulo $\Gamma_0(\mathfrak{n})$ they must be equivalent modulo Γ, and so by Lemma 1.4.5, they must generate ideals in the same ideal class. Hence by Lemma 1.4.4 we can choose the numerators and denominators of the two cusps so that they actually generate the same ideal.

This is a new result which holds over **any** number field.

Lemma 1.5.1. *Let $\alpha_1 = \frac{p_1}{q_1}, \alpha_2 = \frac{p_2}{q_2}$ be two cusps with the same ideal class, written such that*

$$\langle p_1, q_1\rangle = \langle p_2, q_2\rangle = \mathfrak{d}.$$

Let $\delta = Norm(\mathfrak{d})$, and let $\bar{\mathfrak{d}}$ be an ideal such that $\mathfrak{d}\bar{\mathfrak{d}} = \langle\delta\rangle$. The following are equivalent

1. $\alpha_2 = M\alpha_1$ *for some* $M \in \Gamma_0(\mathfrak{n}) \cap \mathrm{SL}_2(\mathcal{O})$.

2. $q_2 s_1 - q_1 s_2 \in \frac{1}{\delta} q_1 q_2 \bar{\mathfrak{d}}^2 + \delta\mathfrak{n}$, *where* s_i *satisfies* $p_i s_i \equiv \delta \pmod{q_i}$.

Proof. Since $\mathfrak{d}\bar{\mathfrak{d}} = \langle\delta\rangle$ we can find $r_i, s_i \in \bar{\mathfrak{d}}$ such that

$$p_i s_i - q_i r_i = \delta.$$

Set

$$M_i = \begin{pmatrix} p_i & r_i \\ q_i & s_i \end{pmatrix}$$

so that

$$M_2 M_1^{-1}(\alpha_1) = \alpha_2.$$

N.B. this matrix lies in Γ.

Now suppose that

$$M_1' = \begin{pmatrix} p_1 & r_1' \\ q_1 & s_1' \end{pmatrix}$$

is another such matrix with determinant δ. Then

$$\begin{aligned} M_1^{-1} M_1' &= \tfrac{1}{\delta} \begin{pmatrix} s_1 & -r_1 \\ -q_1 & p_1 \end{pmatrix} \begin{pmatrix} p_1 & r_1' \\ q_1 & s_1' \end{pmatrix} \\ &= \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \end{aligned}$$

Where $x = \frac{1}{\delta}(s_1 r_1' - r_1 s_1') \in \frac{1}{\delta}\bar{\mathfrak{d}}^2$.

Since

$$M_1' = M_1 \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},$$

the most general matrix in Γ taking α_1 to α_2 is:

$$M_2 \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} M_1^{-1} = \begin{pmatrix} * & * \\ \frac{1}{\delta}(q_2 s_1 - q_1 s_2 - x q_1 q_2) & * \end{pmatrix}$$

where $x \in \frac{1}{\delta}\bar{\mathfrak{d}}^2$.

So there exists a matrix in $\Gamma_0(\mathfrak{n})$ taking α_1 to α_2 if and only if

$$q_2 s_1 - q_1 s_2 \in \frac{1}{\delta} q_1 q_2 \bar{\mathfrak{d}}^2 + \delta\mathfrak{n}.$$

$\square$

Now if $M(\alpha_1) = \alpha_2$ for some $M \in \Gamma_0(\mathfrak{n})$ with $\det M = -1$, then writing $M = M' \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ we have

$$\begin{aligned} M' \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \alpha_1 &= \alpha_2 \\ M'(-\alpha_1) &= \alpha_2 \end{aligned}$$

So to test for equivalence under the full group $\Gamma_0(\mathfrak{n})$ we just need to apply the test in the above Lemma to both the pair (α_1, α_2) and $(-\alpha_1, \alpha_2)$.

N.B. we have made no assumption on the class number, other than that it is finite, so this result holds for any number field. In the case $h = 1$ this gives the same condition as the classical one if we write the cusps in lowest form so that $\mathfrak{d} = \mathcal{O}$ and $\delta = 1$.

Chapter 2

Modular forms

The definition of modular forms over imaginary quadratic fields used in this thesis is based on Weil's adelic approach to modular forms over algebraic number fields as described in [24]. We do not try to motivate the definition here, just give a brief sketch of the theory. The exposition follows that in [5] closely, but is included here as it has not been published anywhere.

There are several questions that arise when searching for a theory of modular forms for $\mathrm{GL}_2(\mathcal{O})$. What should the range and domain of the functions be? How should the notion of weight be extended and what analytic properties should we require? The requirement of holomorphicity must be modified or weakened if the domain does not have a complex structure. It was soon discovered that the existence of a non-trivial class group poses serious difficulties when trying to extend the classical definition. However there is an adelic approach to automorphic forms over $\mathbb{Q}$ which can be extended in such a way that these difficulties largely disappear.

Here we present this adelic formulation, most of which holds for an arbitrary number field. However we will take k to be an imaginary quadratic field throughout as it is the only case we are interested in in this thesis and it makes the theory a lot simpler at several points. We will also only consider modular forms with unramified characters as these are the forms expected to correspond to elliptic curves and hence are the ones we are interested in. Those interested in the general results should consult [5] or [24]. At one key point we also assume that the class number is odd as this allows us to make a further simplification.

2.1 Ideles and characters

We begin by describing some necessary adelic theory. Throughout this chapter, we let k be an imaginary quadratic number field and $\mathcal{O}$ its ring of integers; we write v for a place of k, and k_v for the completion of k at v. Our restriction on k means that there is a unique infinite place, which is complex and so we shall identify $k_\infty \cong \mathbb{C}$. If v is finite, we write $\mathcal{O}_v$ for the valuation ring of integers in k_v, P_v for the unique maximal ideal of $\mathcal{O}_v$ and $\mathfrak{p}_v$ for the prime ideal $P_v \cap \mathcal{O}$ of $\mathcal{O}$ corresponding to the place v.

Recall an **adele** of k is a family $x = (x_v)$ of elements $x \in k_v$, where v runs over all places of k, and for which x_v is integral in k_v for almost all v. The adeles form a topological ring, denoted $k_{\mathbb{A}}$; addition and multiplication are defined componentwise. Thus

$$k_{\mathbb{A}} = \{(x_v) : x_v \in k_v \text{ for all } v,\ x_v \in \mathcal{O}_v \text{ for almost all } v\}.$$

The idele group $k_{\mathbb{A}}^\times$ of k is the group of units of the adele ring $k_{\mathbb{A}}$; explicitly

$$k_{\mathbb{A}}^\times = \{(x_v) \in k_{\mathbb{A}} : x_v \in k_v^\times \text{ for all } v,\ x_v \in \mathcal{O}_v^\times \text{ for almost all } v\}.$$

Given $x \in k_{\mathbb{A}}^\times$, define a fractional ideal $\mathrm{il}(x)$ of k by $\mathrm{il}(x)_v = x_v\mathcal{O}_v$ for all finite places v. Explicitly,

$$\mathrm{il}(x) \quad = \quad \prod_{v \nmid \infty} \mathfrak{p}_v^{\mathrm{ord}_v(x_v)}. \tag{2.1}$$

We write

$$I_k^\infty = k_\infty^\times \times \prod_{v \nmid \infty} \mathcal{O}_v^\times.$$

Lemma 2.1.1. *Let $r_1, \ldots, r_h \in k_{\mathbb{A}}^\times$ be chosen such that the $\mathrm{il}(r_i)$ represent the h distinct ideal classes of k. Then there is a disjoint union*

$$k_{\mathbb{A}}^\times = \bigcup_i^h r_i \cdot k^\times \cdot I_k^\infty.$$

Proof. Let $x \in k_{\mathbb{A}}^\times$. There is a unique i such that the fractional ideal $\mathrm{il}(r_i^{-1}x)$ is principal. Now write $x' = r_i^{-1}x$, so that $\mathrm{il}(x') = \langle c \rangle$ for some $c \in k^\times$. Then

$x'' = c^{-1}x'$ satisfies $x''_v \in \mathcal{O}_v^\times$ for all finite v. Hence $x'' \in I_k^\infty$. □

If J_k and P_k denote the group of fractional ideals and of principal fractional ideals, then il : $k_\mathbb{A}^\times \to J_k$ is a surjective homomorphism with kernel I_k^∞, and the composite $k_\mathbb{A}^\times \to J_k \to J_k/P_k$ is surjective with kernel $k^\times I_k^\infty$.

A **modulus** of k is a formal product $\mathfrak{m} = \prod_v \mathfrak{p}_v^{\mathfrak{n}_v}$ of prime powers, with $n_v \geq 0$ for all places v, with $n_v = 0$ for almost all v, and with $n_v \in \{0, 1\}$ for the infinite place v.

We set

$$U_v^{n_v} = \begin{cases} \mathcal{O}_v^\times & \text{if } v \nmid \infty \text{ and } n_v = 0, \\ 1 + P_v^{n_v} & \text{if } v \nmid \infty \text{ and } n_v > 0, \\ \mathbb{C}^\times = k_v^\times & \text{if } v \text{ is complex.} \end{cases}$$

For $a_v \in k_v^\times$, we set

$$a_v \equiv 1 \pmod{\mathfrak{p}_v^{n_v}} \Longleftrightarrow a_v \in U_v^{n_v}.$$

For every idele $a = (a_v)$, we set

$$a \equiv 1 \pmod{\mathfrak{m}} \Longleftrightarrow a_v \equiv 1 \pmod{\mathfrak{p}_v^{n_v}} \text{ for all } v,$$

and define

$$I_k^\mathfrak{m} = \{\alpha \in k_\mathbb{A}^\times : \alpha \equiv 1 \pmod{\mathfrak{m}}\}.$$

Let C_k denote the idele class group $k_\mathbb{A}^\times/k^\times$. The group $C_k^\mathfrak{m} = I_k^\mathfrak{m} \cdot k^\times/k^\times$ is called the **congruence subgroup** mod $\mathfrak{m}$ of C_k. The factor group $C_k/C_k^\mathfrak{m}$ is called the **ray class group** mod $\mathfrak{m}$.

In the special case $\mathfrak{m} = 1$ we have $I_k^1 = I_k^\infty$ and so by the remarks above we have $C_k/C_k^1 \cong J_k/P_k$. So the ray class group mod 1 is canonically isomorphic to the ideal class group Cl_k.

Let ψ be a character of C_k. Write ψ_v for the local component of ψ at v. We may define $f(v)$ to be the smallest non-negative integer such that ψ_v is trivial on the subgroup $U_v^{f(v)}$ of $\mathcal{O}_v$. $f(v) = 0$ for almost all v, so we can define an ideal

$$\mathfrak{f}_\psi = \prod_{v \nmid \infty} \mathfrak{p}_v^{f(v)}$$

called the **conductor** of ψ

We say that ψ has **discrete infinite components** if the image of ψ_v for each infinite place v is a discrete subgroup of the unit circle. If v is complex this means that ψ_v is trivial. Thus if ψ has discrete infinite components, then it is trivial on $I_k^{\mathfrak{m}}$, where the modulus $\mathfrak{m}$ is equal to $\mathfrak{f}_\psi$.

Definition 2.1.2. *A* ***Dirichlet character*** *is a character ψ of the idele class group having discrete infinite components. The* ***defining modulus*** *of ψ is the modulus $\mathfrak{m}$ defined above. If v is a place dividing $\mathfrak{m}$, we say that ψ is ramified at v.*

Definition 2.1.3. *Let $\mathfrak{m}$ be a modulus of k. A* ***Dirichlet character mod*** $\mathfrak{m}$ *is one whose defining modulus divides $\mathfrak{m}$.*

Let ψ be a Dirichlet character mod 1, (another way of saying this is that ψ is **unramified**). Then ψ is trivial on $I_k^1 = I_k^\infty$ and hence on C_k^1, and so may be viewed as a character, $\hat{\psi}$, of the ray class group C_k/C_k^1, or on the ideal class group Cl_k.

Hence such a character just captures the action of the class group. Note such characters are equivalent to Galois characters of the Hilbert class field k^1 of k, since it is well known that $G(k^1/k) \cong Cl_k$.

Finally, for each place v of k, write G_v for $\mathrm{GL}_2(k_v)$, so in particular $G_\infty = \mathrm{GL}_2(\mathbb{C})$. We now define $G_{\mathbb{A}}$ in the obvious way as the adelisation of $\mathrm{GL}_2(k)$:

$$G_{\mathbb{A}} = \{(x_v) : x_v \in G_v \text{ for all } v,\ x_v \in \mathrm{GL}_2(\mathcal{O}_v) \text{ for almost all } v\}.$$

Equivalently, we may regard $G_{\mathbb{A}}$ as $\mathrm{GL}_2(k_{\mathbb{A}})$

2.2 Action of $G_{\mathbb{A}}$ on lattices

If v is finite, that is, non-Archimdean, we write $\mathcal{O}_v$ for the ring of valuation integers in k_v. Recall that $\mathcal{O}_v$ will always be a principal ideal domain.

Let E be a finite-dimensional k-vector space and let L be a lattice in E, i.e. an $\mathcal{O}$-submodule such that $L \otimes_{\mathcal{O}} k = E$. For a finite place v of k write $E_v = E \otimes_k k_v$ and let L_v be the $\mathcal{O}_v$-submodule generated by L in E_v, in other words, $L_v = L \otimes_{\mathcal{O}} \mathcal{O}_v$. Then L_v is a lattice in E_v, and in fact is the closure of L in E_v.

Theorem 2.2.1. *Let M be a k-lattice in E. For each finite place v of k, let M_v be the closure of M in E_v and L_v any k_v-lattice in E_v. Then there is a k-lattice L in E whose closure in E_v is L_v for every v if and only if L_v=M_v for almost all v; when that is so, there is only one such k-lattice, and it is given by $L = \cap_v(E \cap L_v)$.*

Proof. [5], Theorem 77, pg 127. □

In our situation the dimension of E is 2 and after choosing a basis, we may identify E with k^2 and choose for M the standard lattice $\mathcal{O}^2$.

Now for $a = (a_v) \in G_{\mathbb{A}}$ and a lattice L, we define aL to be the unique lattice in k^2 satisfying $(aL)_v = a_v L_v$ for all finite places v. This works because $L_v = \mathcal{O}_v^2$ for almost all v and $a_v \in \mathrm{GL}_2(\mathcal{O}_v)$ for almost all v so that $a_v L_v = \mathcal{O}_v^2$ for almost all v. When $a \in G_k$, this definition agrees with the usual action of a matrix on a set of column vectors. So the action of $G_{\mathbb{A}}$ extends the action of G_k, and there is no confusion when we write aL with $a \in G_{\mathbb{A}}$. To see this if $a \in \mathrm{GL}_2(\mathcal{O})$ then we can embed it in $G_{\mathbb{A}}$ by taking $\bar{a} = (a_v)$ with $a_v = a$ for all v. Then $\bar{a}L$ is defined to be the unique lattice such that $(\bar{a}L)_v = a_v L_v$ for all v, which is clearly just aL.

Lemma 2.2.2. *Let L and L' be lattices in $\mathcal{O}^2$ which are isomorphic as $\mathcal{O}$-modules. Then there exists $\gamma \in \Gamma$ such that $\gamma L = L'$.*

Proof. [5], Lemma 78, pg 128. □

Consider the following open subgroup of $G_{\mathbb{A}}$:

$$\Omega_1 \quad = \quad G_\infty \times \prod_{v \nmid \infty} \mathrm{GL}_2(\mathcal{O}_v). \tag{2.2}$$

It follows from the discussion above that Ω_1 is the stabiliser of $\mathcal{O}^2$ under the action of $G_{\mathbb{A}}$, i.e.

$$\Omega_1 = \{c \in G_{\mathbb{A}} : c\mathcal{O}^2 = \mathcal{O}^2\}.$$

Proposition 2.2.3. *Let L be a lattice in $\mathcal{O}^2$ and let $a \in G_{\mathbb{A}}$. Then*

$$\mathrm{cl}(aL) = \mathrm{cl}(\mathrm{il}(\det(a)) \cdot \mathrm{cl}(L).$$

Proof. [5], Proposition 79, pg 129. □

Now more generally, for each integral ideal $\mathfrak{n}$, we consider the stabiliser of $\mathcal{O} \oplus \mathfrak{n}$:

$$\Omega_{\mathfrak{n}} = \{c \in G_{\mathbb{A}} : c(\mathcal{O} \oplus \mathfrak{n}) = \mathcal{O} \oplus \mathfrak{n}\}. \tag{2.3}$$

$G_{\mathbb{A}}$ acts transitively on lattices, so the groups $\Omega_{\mathfrak{n}}$ are all conjugate. Explicitly, if n is an idele with $\mathrm{il}(n) = \mathfrak{n}$, then

$$\Omega_{\mathfrak{n}} = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \Omega_1 \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}^{-1}. \tag{2.4}$$

The group

$$\Omega_0(\mathfrak{n}) := \Omega_1 \cap \Omega_{\mathfrak{n}}, \tag{2.5}$$

turns out to be an adelic analogue of the congruence subgroup $\Gamma_0(\mathfrak{n})$, in a manner to be explained below.

Let $\mathfrak{n}$ be an integral ideal, which we shall call the **level**. Choose an idele $n = (n_v) \in k_{\mathbb{A}}^{\times}$, with $\mathrm{il}(n) = \mathfrak{n}$ and $n_v = 1$ for $v \nmid \mathfrak{n}$. For each place v of k, define a compact open subgroup K_v of $\mathrm{GL}_2(k_v)$ by

$$K_v = \left\{ \begin{pmatrix} a & b \\ n_v c & d \end{pmatrix} : a, b, c, d \in \mathcal{O}_v,\ ad - n_v bc \in \mathcal{O}_v^{\times} \right\} \tag{2.6}$$

if v is finite, and let

$$K_\infty = U_2(\mathbb{C}).$$

Then set

$$\mathcal{K} = \prod_v K_v$$

to be the product over all places v, finite and infinite.

By (2.2) and (2.4) we have

$$\Omega_{\mathfrak{n}} = \prod_{v \nmid \infty} K'_v \times G_\infty,$$

where
$$K'_v = \left\{ \begin{pmatrix} a & n_v^{-1}b \\ n_v c & d \end{pmatrix} : a,b,c,d \in \mathcal{O}_v,\ ad-bc \in \mathcal{O}_v^\times \right\}.$$
Taking the intersection $\Omega_0(\mathfrak{n}) = \Omega_1 \cap \Omega_\mathfrak{n}$ gives
$$\Omega_0(\mathfrak{n}) = \prod_{v \nmid \infty} K_v \times G_\infty. \tag{2.7}$$

Then
$$G_k \cap \Omega_0(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,d \in \mathcal{O},\ c \in \mathfrak{n},\ ad-bc \in \mathcal{O}^\times \right\},$$
so that the group of "principal" adeles in $\Omega_0(\mathfrak{n})$ is nothing other than the usual congruence subgroup $\Gamma_0(\mathfrak{n})$ of $\mathrm{GL}_2(\mathcal{O})$.

Let Z denote the centre of $\mathrm{GL}_2(k)$; it consists of scalar matrices and can thus be identified with the multiplicative group $k^\times$. Write $Z_\mathbb{A}$ for the corresponding adelised group; $Z_\mathbb{A}$ can be identified with the idele group $k_\mathbb{A}^\times$ of k.

Weil, [24], proves the following decomposition
$$G_\mathbb{A} = G_k B_\mathbb{A} \mathcal{K} Z_\mathbb{A}, \tag{2.8}$$
where
$$B_\mathbb{A} = \left\{ \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} : x \in k_\mathbb{A}, y \in k_\mathbb{A}^\times \right\}.$$

2.3 Harmonic differential forms

Let V, W be real differentiable manifolds of dimension m. We denote the space of differential r-forms on V by $\Omega^r(V)$. An important operation on differential forms is the exterior derivative:
$$d : \Omega^r(V) \to \Omega^{r+1}(V).$$
Another important operator is the Hodge star operator:
$$* : \Omega^r(V) \to \Omega^{m-r}(V).$$

We can use these two maps to define another map $\delta : \Omega^r(V) \to \Omega^{r-1}(V)$, which lowers the degree of the form, by

$$\delta = (-1)^{m(r+1)+1} * d * .$$

Finally, we can define the "Laplacian", an operator preserving the degree of a form, by

$$\Delta = \delta d + d\delta.$$

Definition 2.3.1. *An r-form w is called harmonic if* $\Delta w = 0$.

If V is compact, there is an inner product on $\Omega^r(V)$ given by

$$(\alpha, \beta) \quad = \quad \int_V \alpha \wedge *\beta. \tag{2.9}$$

If $f : V \to W$ is a smooth map of manifolds, then it induces a map $f^* : \Omega^r(W) \to \Omega^r(V)$, which associates to a differential r-form w on W an r-form f^*w on V, called its **pullback** along f to V.

Now let G be a Lie group over $\mathbb{R}$, that is, a group with a compatible structure as a differentiable manifold. For fixed $a \in G$, we have a diffeomorphism from G to itself:

$$L_a : g \mapsto ag \qquad \text{left translation.}$$

A differential r-form w on G is called **left-invariant under** a if it is invariant under pullback along L_a, that is, $L_a^* w = w$. If w is left-invariant under all $g \in G$, we will simply call it **left-invariant**.

We now consider a particular Lie group, namely $\mathrm{GL}_2(\mathbb{C})$. There is a decomposition

$$G_\infty = B_\infty Z_\infty K_\infty$$

where

$$\begin{aligned}
G_\infty &= \mathrm{GL}_2(\mathbb{C}), \\
Z_\infty &= \left\{ \zeta \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} : \zeta \in \mathbb{C}^\times \right\}, \\
B_\infty &= \left\{ t^{-1/2} \begin{pmatrix} t & z \\ 0 & 1 \end{pmatrix} : z \in \mathbb{C}, t \in \mathbb{R}^+ \right\}, \\
K_\infty &= U_2(\mathbb{C}).
\end{aligned}$$

Since $B_\infty \cap Z_\infty K_\infty = \{I_2\}$, B_∞ provides a complete set of right coset representatives for $Z_\infty K_\infty$ in G_∞. So B_∞ may be identified with the coset space $G_\infty/Z_\infty K_\infty$. It may also be identified in the obvious manner with the space $\mathcal{H}_3$. We write $\pi : G_\infty \to \mathcal{H}_3$ for the canonical projection of G_∞ onto $\mathcal{H}_3$; the restriction of π to B_∞ is the bijection identifying B_∞ with $\mathcal{H}_3$. Thus every element of $\mathcal{H}_3$ can be written as $\pi(b)$ for suitable $b \in B_\infty$.

The space $\mathcal{H}_3$ is a differential manifold of dimension 3. The group G_∞ acts on $\mathcal{H}_3$ on the left. The map $L_g : G_\infty \to G_\infty$ induces a unique map $\tilde{L}_g : \mathcal{H}_3 \to \mathcal{H}_3$ satisfying $\tilde{L}_g \circ \pi = \pi \circ L_g$.

Now we introduce an irreducible representation ρ of K_∞; as K_∞ is compact, its representation space V is of finite dimension over $\mathbb{C}$. We assume that, on the centre of K_∞, ρ coincides with our unramified character ψ. We can extend ρ to $K_\infty Z_\infty$ by putting $\rho(\kappa\zeta) = \rho(\kappa)\psi(\zeta)$. The representation ρ will generalise the role of the "weight" in our definition of modular forms. Next we define a suitable 3-dimensional representation ρ whose associated modular forms are associated with harmonic differentials, as analogous to the classical weight 2 modular forms.

We are interested in harmonic differential 1-forms on $\mathcal{H}_3$ and their pullbacks to $\mathrm{GL}_2(\mathbb{C})$. We start by choosing a basis $\beta_1, \beta_2, \beta_3$ (over $\mathbb{C}$) for the left-invariant differential forms on $\mathcal{H}_3$. We denote the pullback to G_∞ of these differentials by $\pi^*\beta_i$. These pullbacks are right-invariant under $Z_\infty K_\infty$. Now for each i, let w_i be the left-invariant differential 1-form on G_∞ which agrees with $\pi^*\beta_i$ at the identity $e \in G_\infty$. This defines w_i uniquely, since the values at the non-identity fibres are determined by left-translation. Write w (respectively β, $\pi^*\beta$) for the column vector of the w_i (resp. β_i, $\pi^*\beta_i$). Right-translation by elements of $K_\infty Z_\infty$ in G_∞ operate on the w_i through a representation of $K_\infty Z_\infty$ which is obviously trivial on Z_∞.

We can choose the basis β as follows:

$$\beta_1 = -\frac{dz}{t}, \quad \beta_2 = \frac{dt}{t}, \quad \beta_3 = \frac{d\bar{z}}{t}. \tag{2.10}$$

Let $J(g;(z,t))$ be the Jacobian matrix of $L_g : \mathcal{H}_3 \to \mathcal{H}_3$ in terms of our chosen basis β. To see how to choose ρ we just look at the classical situation. By analogy ρ should come from the Jacobian matrix $J(g;(z,t))$.

Lemma 2.3.2. *Let* $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$. *Write* $\Delta = ad - bc$, $r = \overline{cz + d}$ *and* $s = \bar{c}t$. *Then*

$$J(g;(z,t)) = \frac{1}{|\Delta|(r\bar{r} + s\bar{s})} \begin{pmatrix} \Delta & 0 & 0 \\ 0 & |\Delta| & 0 \\ 0 & 0 & \bar{\Delta} \end{pmatrix} \begin{pmatrix} r^2 & -2rs & s^2 \\ r\bar{s} & r\bar{r} - s\bar{s} & -\bar{r}s \\ \bar{s}^2 & 2\bar{r}\bar{s} & \bar{r}^2 \end{pmatrix}$$

Proof. [5], Lemma 62, pg 98. □

We can now define ρ to be the restriction of $J(g;(0,1))$ to $g \in ZK$.

Proposition 2.3.3. *Let* w *be defined as above. Then*

1. *For* $\phi : G_\infty \to \mathbb{C}^3$, *the form* $\phi \cdot w$ *induces* $f \cdot \beta$, *where* $f : \mathcal{H}_3 \to \mathbb{C}^3$ *is given by*

$$f(z,t) \quad = \quad \phi\left(\begin{pmatrix} t & z \\ 0 & 1 \end{pmatrix}\right). \tag{2.11}$$

2. *The pullback to* G_∞ *of a differential form* $f \cdot \beta$ *on* $\mathcal{H}_3$ *is* $\phi \cdot w$, *where*

$$\phi(g) \quad = \quad f(\pi(g))\rho(\pi(g)^{-1}g). \tag{2.12}$$

3. *A differential form on* G_∞ *is the pullback of one on* $\mathcal{H}_3$ *if and only if it can be written as* $\phi \cdot w$, *where* $\phi : G_\infty \to \mathbb{C}^3$ *satisfies*

$$\phi(g\kappa\zeta) = \phi(g)\rho(\kappa\zeta).$$

Proof. [5], Lemma 60, pg 94. □

Let ϕ and f be related as in Proposition 2.3.3.

Definition 2.3.4. *The function* f *is* ***moderate*** *if there exists* $N \geq 0$ *such that, for every compact subset* S *of* $\mathbb{C}$,

$$\| f(z,t) \| = O(t^N + t^{-N}),$$

uniformly over $z \in S$, *where* $\| \ \|$ *denotes any fixed norm of* $\mathbb{C}^3$.

Remark: Roughly speaking this condition ensures that f is of moderate growth as its argument approaches the cusps.

Definition 2.3.5. *We say that ϕ is moderate if and only if f is moderate*

Definition 2.3.6. *The function ϕ is **admissible** if it is moderate and $f \cdot \beta$ is harmonic.*

Let $\rho : Z_\infty K_\infty \to \mathrm{GL}_3(\mathbb{C})$ be a representation. We refer to ρ as the weight as it generalises the concept of the weight in the classical setting. Consider the following two sets of functions:

$$\begin{aligned} S_1 &= \{f : \mathcal{H}_3 \to \mathbb{C}^3\}, \\ S_2 &= \left\{\phi : G_\infty \to \mathbb{C}^3 : \phi(\zeta g \kappa) = \phi(g)\rho(\zeta\kappa)\ \forall\, \zeta \in Z_\infty, g \in G_\infty, \kappa \in K_\infty\right\}. \end{aligned}$$

There is an obvious map $^\dagger : S_2 \to S_1$, given essentially by restriction to B_∞; explicitly,

$$\phi^\dagger(\pi(b)) = \phi(b) \qquad (b \in B_\infty). \tag{2.13}$$

In the other direction, we can define a map $^\sharp : S_1 \to S_2$ by

$$f^\sharp(\zeta b \kappa) = f(\pi(b))\rho(\zeta\kappa) \qquad (\zeta \in Z_\infty, b \in B_\infty, \kappa \in K_\infty). \tag{2.14}$$

Lemma 2.3.7. *The map $^\dagger : S_2 \to S_1$ is a bijection, with inverse $^\sharp : S_1 \to S_2$.*

Proof. [5], Lemma 68, pg 109. □

2.3.1 Action of G_∞

We can define a natural right action of G_∞ on the set $\{\phi : G_\infty \to \mathbb{C}^3\}$ by $\phi \mapsto \phi|\gamma$, where

$$(\phi|\gamma)(\delta) = \phi(\gamma\delta) \qquad \gamma, \delta \in G_\infty. \tag{2.15}$$

It is clear that this action preserves the set $\mathcal{S}_2$; thus (2.15) defines a right action of G_∞ on $\mathcal{S}_2$. Using the bijection of Lemma 2.3.7 we can transfer this action to the set $\mathcal{S}_1$. For $f \in \mathcal{S}_1$ and $\gamma \in G_\infty$, we define $f|\gamma = ((f^\sharp)|\gamma)^\dagger$. Explicitly,

$$(f|\gamma)(\pi(b)) = f(\gamma\pi(b))\rho(\pi(\gamma b)^{-1}\gamma b) \qquad b \in B_\infty.$$

Comparing this with the classical formula

$$(f|\gamma)(z) = f(\gamma \cdot z)\mu(\gamma, z) \qquad \mu(\gamma, z) = \left(\frac{d}{dz}(\gamma \cdot z)\right)^{1/2}$$

we see how ρ takes the place of the automorphy factor μ.

2.4 Automorphic forms

Let $\Phi : G_{\mathbb{A}} \to \mathbb{C}^3$ be a function, let ψ be an unramified Dirichlet character, and let $\rho : K_\infty \to \mathrm{GL}_3(\mathbb{C})$ be an irreducible representation of K_∞ which agrees with ψ on the centre of K_∞. Fix an ideal $\mathfrak{n}$ (the level) and a corresponding idele n, and define K_v, $v \nmid \infty$ as before. (The range of Φ is chosen to be the representation space of K_∞ so that everything makes sense).

Consider the following conditions on Φ:

(A) $\Phi(\gamma g) = \Phi(g)$ for all $\gamma \in G_k$ and $g \in G_{\mathbb{A}}$;

(B) $\Phi(g\zeta) = \Phi(g)\psi(\zeta)$ for all $g \in G_{\mathbb{A}}$ and $\zeta \in Z_{\mathbb{A}}$;

(C) $\Phi(g\kappa) = \Phi(g)\rho(\kappa_\infty)$ for all $g \in G_{\mathbb{A}}$ and $\kappa \in \mathcal{K}$.

By $\psi(\zeta)$ we mean $\psi(\det(\zeta))$ and when we want to consider κ as an element of $G_{\mathbb{A}}$ we just assume that it is trivial in all components not explicitly defined.

It follows from the decomposition (2.8) that any function $\Phi : G_{\mathbb{A}} \to \mathbb{C}^3$, satisfying (A)-(C), is uniquely determined by its restriction to $B_{\mathbb{A}}$. Thus given $\Phi : G_{\mathbb{A}} \to \mathbb{C}^3$, we can define $F : k_{\mathbb{A}} \times k_{\mathbb{A}}^\times \to \mathbb{C}^3$ by

$$F(x, y) = \phi\left(\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}\right). \tag{2.16}$$

Proposition 2.4.1. *Let $\Phi : G_{\mathbb{A}} \to \mathbb{C}^3$ satisfy conditions (A)-(C), and define F by (2.16). Then F has the following properties:*

1. *$F(x + \kappa, y) = F(x, y)$ for all $\kappa \in k$;*
2. *$F(\kappa x, \kappa y) = F(x, y)$ for all $\kappa \in k^\times$;*
3. *$F(x + yz, y) = F(x, y)$ for all $z \in \mathcal{O}_v$ for each finite place v;*

4. $F(x, uy) = F(x, y)$ *for all* $u \in \prod_{v \nmid \infty} \mathcal{O}_v^\times$.

Proof. [5], Lemma 98, pg 148. □

Once and for all, choose a non-trivial additive character φ of $k_{\mathbb{A}}$, trivial on k. Any other choice φ' can be written as $\varphi'(x) = \varphi(\xi x)$ with $\xi \in k^\times$. For every place v, write φ_v for the character of k_v induced by φ on k_v. For finite v, we say that φ_v is of **order** δ, if φ_v is trivial on $\pi_v^{-\delta}\mathcal{O}_v$ but not on $\pi_v^{-\delta-1}\mathcal{O}_v$; one can show that δ equals 0 for almost all v. For each finite v, let $\delta(v)$ be the order of φ_v. Let $d = (\delta_v)$ be the idele given by $d_v = \pi_v^{\delta(v)}$ for finite v and $d_w = 1$ for infinite w. The idele d is called a **differental idele** belonging to φ; it depends on the choice of the prime element π, but the ideal $\mathrm{il}(d)$ does not. We may assume φ is chosen so that $\varphi_\infty = e^{-2\pi i(x+\bar{x})}$; this determines φ uniquely, and $\mathrm{il}(d)$ is then the **different** of the number field k in the usual sense.

Proposition 2.4.2. *Let* $\Phi : G_{\mathbb{A}} \to \mathbb{C}^3$ *satisfy conditions (A)-(C). Define* F *by (2.16). Then* F *has a Fourier expansion*

$$F(x, y) = c_0(y) + \sum_{\xi \in k^\times} c(\xi d y)\varphi(\xi x),$$

with $c_0(\kappa u y) = c_0(y)$ *for all* $\kappa \in k^\times$, $u \in \prod \mathcal{O}_v^\times$, *with* $c(y)$ *depending only on* y_∞ *and* $\mathrm{il}(y)$, *and with* $c(y) = 0$ *unless the ideal* $\mathrm{il}(y)$ *is integral.*

Proof. [5], Proposition 99, pg 149. □

Definition 2.4.3. *Let* Φ *be as in Proposition 2.4.2. We say that* Φ *is* ***cuspidal*** *if and only if* $c_0(y) = 0$ *for all* $y \in k_{\mathbb{A}}^\times$.

Let $\Phi : G_{\mathbb{A}} \to \mathbb{C}^3$ be a function satisfying (A)-(C).

Definition 2.4.4. *The function* Φ *is* ***admissible*** *if the induced function* $\Phi_\infty : \mathrm{GL}_2(\mathbb{C}) \to \mathbb{C}^3$ *is admissible in the sense of Definition 2.3.6.*

Definition 2.4.5. *An* ***automorphic form*** *of weight two for* $\Gamma_0(\mathfrak{n})$ *is a function* $\Phi : G_{\mathbb{A}} \to \mathbb{C}^3$ *that satisfies conditions (A)-(C) and is admissible. A* ***cuspform*** *is a cuspidal automorphic form.*

Now in order to actually work with these automorphic forms we will need a more concrete description. This can be obtained as follows.

Proposition 2.4.6. *Let $a_1, \ldots, a_h \in G_{\mathbb{A}}$ be such that the ideals* $\mathrm{il}($*det* $a_i)$ *represent the h ideal classes of k. Then $G_{\mathbb{A}}$ decomposes as a disjoint union*

$$G_{\mathbb{A}} = \bigcup_{i=1}^{h} G_k \cdot a_i \cdot \Omega_0(\mathfrak{n}). \tag{2.17}$$

Proof. [5], Proposition 87, pg 136 □

So any function Φ on $G_k \setminus G_{\mathbb{A}}$ thus determines a collection of h functions $\Phi^{(i)} : \Omega_0(\mathfrak{n}) \to \mathbb{C}^3$, via

$$\Phi^{(i)}(x) = \Phi(a_i x).$$

At this point we make a specific choice for the a_i, (which is only possible when h is odd), to simplify things. Once and for all, let $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ be integral ideals of $\mathcal{O}$ representing the h ideal classes; as usual, we take $\mathfrak{a}_1 = \mathcal{O}$ to represent the principal class. Since h is odd we can find an ideal $\mathfrak{p}_i$ such that $\mathrm{cl}(\mathfrak{a}_i) = \mathrm{cl}(\mathfrak{p}_i^2)$. Then we adjust our choice of $\mathfrak{a}_i$ so that in fact $\mathfrak{a}_i = \mathfrak{p}_i^2$. Now let $\pi_i \in k_{\mathbb{A}}^{\times}$ be ideles with $\mathrm{il}(\pi_i) = \mathfrak{p}_i$ and set

$$a_i = \begin{pmatrix} \pi_i & 0 \\ 0 & \pi_i \end{pmatrix} \in G_{\mathbb{A}}.$$

Then $\mathrm{il}(\det(a_i)) = \mathfrak{p}_i^2 = \mathfrak{a}_i$. The point is that the a_i are then central elements, i.e. they commute with everything.

Let $z \in Z_{\mathbb{A}}$ and suppose $\mathrm{il}(\det z)$ is principal, so $\psi(z)$ is trivial. Then using Proposition 2.4.6 we can write

$$z a_i = \delta a_i w \qquad \delta \in G_k, w \in \Omega_0(\mathfrak{n}).$$

Then we have

$$\begin{aligned} \Phi^{(i)}(x) &= \Phi(a_i x) \\ &= \Phi(z a_i x)\psi(z)^{-1} \\ &= \Phi(\delta a_i w x) \\ &= \Phi^{(i)}(w x) \end{aligned}$$

So $\Phi^{(i)}$ is left-invariant under all the $w \in \Omega_0(\mathfrak{n})$ that arise in this way. The set of such w is

$$\widetilde{\Omega}_0(\mathfrak{n}) \;=\; \Omega_0(\mathfrak{n}) \cap G_k Z_{\mathbb{A}}^1,$$

where $Z_{\mathbb{A}}^1 = \{z \in Z_{\mathbb{A}} : \mathrm{il}(\det(z)) \text{ is principal}\}$.

In the case of general class number there is an analogous set for each individual ideal class.

Now suppose $\delta z \in \Omega_0(\mathfrak{n}) \subset \Omega_1$, then we must have $\delta_v z_v \in \mathrm{GL}_2(\mathcal{O}_v)$ for all $v \nmid \infty$. Hence $\mathrm{il}(\det \delta z) = \mathcal{O}$. It follows that $\delta \in \mathrm{GL}_2(\mathcal{O})$ and $z_v = 1$ for all finite v. Indeed suppose $\mathrm{il}(\det z) = \mathfrak{a}^2$ with $\mathfrak{a} = \langle a \rangle$ [1], then multiplying each component of δ by a we can force $z_v = 1$ for all $v \nmid \infty$, which means we must then have $\delta \in \mathrm{GL}_2(\mathcal{O})$. Intersecting again with $\Omega_0(\mathfrak{n})$ we obtain

$$\widetilde{\Omega}_0(\mathfrak{n}) = \hat{Z}_{\mathbb{A}} \Gamma_0(\mathfrak{n})$$

where $\hat{Z}_{\mathbb{A}}$ is the subset of $Z_{\mathbb{A}}$ whose elements equal the identity at $v \nmid \infty$ and are scalar at the infinite place.

Now the fact that the class number is odd allows us to use the non-principal elements of $Z_{\mathbb{A}}$ to determine all the functions $\Phi^{(j)}$ from one $\Phi^{(i)}$. Indeed, fix i and choose any $j \neq i$. Then for all $x \in \Omega_0(\mathfrak{n})$,

$$\begin{aligned}
\Phi^{(j)}(x) &= \Phi(a_j x) \\
&= \Phi(x)\psi(a_j) \\
&= \Phi(a_i x)\psi(a_j a_i^{-1}) \\
&= \Phi^{(i)}(x)\hat{\psi}(\mathfrak{a}_j \mathfrak{a}_I^{-1})
\end{aligned}$$

It is easy to show that $\Phi^{(j)}$ is invariant under $\widetilde{\Omega}_0(\mathfrak{n})$. It follows that the "principal" component $\Phi^{(1)}$ contains all the information, and the other components are in some sense redundant.

Conversely suppose we are given a collection of h functions $\Phi^{(i)}$ invariant under $\widetilde{\Omega}_0(\mathfrak{n})$. Then we can define Φ on $G_{\mathbb{A}}$, left-invariant under G_k, by

$$\Phi(\gamma a_i w) = \Phi^{(i)}(w).$$

[1] $\Omega_0(\mathfrak{n})$ and G_k are principal, hence z must be. The fact that $\mathfrak{a}^2$ is principal implies $\mathfrak{a}$ is principal since h is odd

Now let $a \in G_{\mathbb{A}}$ and $z \in Z_{\mathbb{A}}$ and write $a = \gamma a_i w_0$ and $za_i = \delta a_j w_1$ with $\gamma, \delta \in G_k$ and $w_0, w_1 \in \Omega_0(\mathfrak{n})$. Then it follows that $z\gamma^{-1}a = \delta a_j w_1 w_0$. The fact that z is central and Φ is left-invariant under G_k, (which comes from its definition), then implies that

$$\begin{aligned}
\Phi(za) &= \Phi(a_j w_1 w_0) \\
&= \Phi^{(j)}(w_1 w_0) \\
&= \Phi^{(i)}(w_0)\psi(\delta a_j w_1 a_i^{-1}) \\
&= \Phi^{(i)}(w_0)\hat{\psi}(\mathrm{il}(\det a_j a_i^{-1})) \\
&= \Phi(a)\psi(z)
\end{aligned}$$

So Φ transforms in the correct way under the action of the centre.

Notation: For $a \in G_{\mathbb{A}}$, we write a_∞ for the infinite component and a_0 for the finite part. Thus, we may write $a = (a_0, a_\infty)$.

From (2.7), we can see that if $a \in \Omega_0(\mathfrak{n})$, then $a_0 \in \prod_{v \nmid \infty} K_v$. So it follows that functions $\Omega_0(\mathfrak{n})$ which are right-invariant under $\prod_{v \nmid \infty} K_v$ correspond naturally to functions on $G_\infty = \mathrm{GL}_2(\mathbb{C})$. We now apply this to the functions $\Phi^{(i)}$ obtained above.

Given $\Phi^{(i)}$ as above, we can, using the above notation, define functions $\phi^{(i)} : \mathrm{GL}_2(\mathbb{C}) \to \mathbb{C}^3$ by

$$\phi^{(i)}(\delta) = \Phi^{(i)}(1, \delta_\infty).$$

The ϕ will still be left-invariant under $\Gamma_0(\mathfrak{n})$ and invariant under the projection of $\hat{Z}_{\mathbb{A}}$ onto the infinite component, which is just Z_∞.

Conversely given $\phi^{(i)} : \mathrm{GL}_2(\mathbb{C}) \to \mathbb{C}^3$, left-invariant under $\Gamma_0(\mathfrak{n})$ and invariant under Z_∞, we can define $\Phi^{(i)} : \Omega_0(\mathfrak{n}) \to \mathbb{C}^3$ by

$$\Phi^{(i)}(x) = \phi^{(i)}(x_\infty).$$

We can summarise our work so far in the following theorem, which only holds for h odd and when the a_i are chosen as above.

Theorem 2.4.7. *There is a bijection between, on the one hand, the set of functions Φ on $G_{\mathbb{A}}$ that satisfy properties (A) - (C), and, on the other hand, the set of h-tuples of functions $\phi^{(i)}$ on $\mathrm{GL}_2(\mathbb{C})$ such that for $1 \le i \le h$, $\phi^{(i)}$ is left-invariant under $\Gamma_0(\mathfrak{n})$, and invariant under Z_∞.*

Proof. Follows from [5], Theorem 96. $\square$

So we now have a h-tuple of functions

$$\phi^{(i)} : \mathrm{GL}_2(\mathbb{C}) \to \mathbb{C}^3$$

invariant under Z_∞, and left-invariant under $\Gamma_0(\mathfrak{n})$.

Then as explained in section 2.3 we can extend ρ to a function on $Z_\infty K_\infty$. Then (B) and (C) imply that

$$\phi(g\zeta\kappa) = \phi(g)\rho(\zeta\kappa) \qquad g \in G_\infty, \zeta \in Z_\infty, \kappa \in K_\infty,$$

so we can see that $\phi^{(i)} \in S_2$, which was defined earlier. Thus using Lemma 2.3.7 we are able to set up another equivalence with a h-tuple of functions

$$f^{(i)} : \mathcal{H}_3 \longrightarrow \mathbb{C}^3$$

by defining

$$f^{(i)}(z,t) = \phi^{(i)}\left(\begin{pmatrix} t & z \\ 0 & 1 \end{pmatrix}\right).$$

These functions will still have the same invariant properties as the $\phi^{(i)}$.

We now develop $f^{(i)}$ as a Fourier series, using the fact that $\phi^{(i)}$ is left-invariant under $\Gamma_0(\mathfrak{n})$. For fixed t, we may regard $f^{(i)}$ as a function of z alone, and expand it in terms of the characters of $\mathbb{C}^+$, the additive group of $\mathbb{C}$. These characters all have the form $z \mapsto \varphi(wz)$, for some $w \in \mathbb{C}$, where φ is any non-trivial character. We chose φ as before, that is

$$\varphi(z) = e^{-2\pi i Tr(z)} \qquad z \in \mathbb{C}.$$

We have for $w \in \mathcal{O}$,

$$f^{(i)}(z+w,t) = \phi^{(i)}\left(\begin{pmatrix} 1 & w \\ 0 & 1 \end{pmatrix}\begin{pmatrix} t & z \\ 0 & 1 \end{pmatrix}\right) = f^{(i)}(z,t).$$

So it follows that $f^{(i)}$ has a Fourier expansion in terms of the characters of $\mathbb{C}^+$ that are trivial on $\mathcal{O}$. The character $z \mapsto \varphi(wz)$ is trivial on $\mathcal{O}$ if and only if

$w \in W = (\sqrt{D})^{-1}\mathcal{O}$, the inverse different of k, since

$$\{w \in k : Tr(w\mathcal{O}) \subseteq \mathbb{Z}\} = W.$$

Thus the expansion of $f^{(i)}$ takes the form

$$f^{(i)}(z,t) = c_0(t) + \sum_{\xi \in W} c_\xi(t)\varphi(\xi z).$$

The condition of admissibility which requires harmonicity imposes some partial differential equations, which reduce to the Cauchy-Riemann equations in the real case; thus harmonicity generalises holomorphicity. These PDEs have a unique admissible solution up to the choice of an additive character. This solution involves the K-Bessel functions K_0 and K_1, and generalises the q-expansion that appears in the classical case. See [4], section 1.9.

Specifically we have

Proposition 2.4.8. *Let $f : \mathcal{H}_3 \to \mathbb{C}^3$ be an admissible function given by the Fourier series*

$$f(z,t) = c_0(t) + \sum_{\xi \in \mathbb{C}^\times} c_\xi(t)\varphi(\xi z).$$

Then

$$c_0(t) = (c_{0,0}, c_{0,1}t^2, c_{0,2}t)$$

for constants $c_{0,0}, c_{0,1}$ and $c_{0,2}$, and

$$c_\xi(t) = c(\xi)H(t|\xi|) \cdot \begin{pmatrix} \xi/|\xi| & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \bar{\xi}/|\xi| \end{pmatrix}$$

for each $\xi \in \mathbb{C}^\times$, where $c(\xi)$ is a constant depending on ξ and where $H(t)$ is given by

$$H(t) = \left(-\frac{i}{2}t^2 K_1(4\pi t), t^2 K_0(4\pi t), \frac{i}{2}t^2 K_1(4\pi t) \right).$$

Proof. [5], Proposition 104, pg 158. □

The following definition is only valid when h is odd.

Definition 2.4.9. *A modular form of weight 2 for $\Gamma_0(\mathfrak{n})$, is an h-tuple $F = (f^{(1)}, \ldots, f^{(h)})$ of functions $f^{(i)} : \mathcal{H}_3 \to \mathbb{C}^3$, such that each $f^{(i)}$ is admissible, and such that each $f^{(i)}$ is left-invariant under $\Gamma_0(\mathfrak{n})$ and invariant under Z_∞. Moreover, F is a cuspform if each $f^{(i)}$ is cuspidal, i.e. has zero constant term in it's Fourier expansion.*

The qualification "of weight 2", to be omitted henceforth, refers to the representation ρ of $U_2(\mathbb{C})$ which is implicit in the definition of $f^{(i)}|\gamma$.

The complex vector space of cusp forms for $\Gamma_0(\mathfrak{n})$ with character ψ will be denoted $S(\mathfrak{n}, \psi)$. In particular, the space of cuspforms with trivial character will be denoted $S(\mathfrak{n})$.

N.B. The only part of the definition which depends on the level is the invariance under $\Gamma_0(\mathfrak{n})$. So if $\mathfrak{n} \mid \mathfrak{n}'$, then a modular form for $\Gamma_0(\mathfrak{n})$ is automatically a modular form for $\Gamma_0(\mathfrak{n}')$, since $\Gamma_0(\mathfrak{n}) \supset \Gamma_0(\mathfrak{n}')$.

2.5 Homology

We now briefly discuss how we can use results of Kurcanov [15] to express $S(\mathfrak{n})$ as the dual of a homology group.

For an arbitrary subgroup Γ' of finite index in Γ, we denote by $\bar{X}_{\Gamma'}$ the topological space $\Gamma' \setminus \mathcal{H}_3^*$. We now form the disjoint union

$$\bar{X}_0(\mathfrak{n}) = \bigcup_{i=1}^{h} \bar{X}_{\Gamma_0(\mathfrak{n})}.$$

The object of central interest is the first cohomology group with coefficients in $\mathbb{C}$,

$$H^1(\bar{X}_0(\mathfrak{n}), \mathbb{C}) = \bigoplus_{i=1}^{h} H^1(\bar{X}_{\Gamma_0(\mathfrak{n})}, \mathbb{C}).$$

We put

$$\hat{S}(\mathfrak{n}) = \sum_{\psi} S(\mathfrak{n}, \psi),$$

where the sum runs over all unramified Dirichlet characters of k.

Later when we look at those forms expected to correspond to elliptic curves we will discover that we only need consider those forms with $\psi = 1$, as these are the only forms in the odd class number case that have rational coefficients.

Kurcanov's main result is that

$$\hat{S}(\mathfrak{n}) \cong H^1(\bar{X}_0(\mathfrak{n}), \mathbb{C}).$$

Now there is an exact duality

$$H_1(\bar{X}_0(\mathfrak{n}), \mathbb{C}) \times H^1(\bar{X}_0(\mathfrak{n}), \mathbb{C}) \to \mathbb{C},$$

given by integrating a differential form along a chain; this is essentially de Rham's theorem. Remarkably, as in the classical case, the duality works at the level of the rational (Hecke) structure, so that it suffices to work out

$$H_1(\bar{X}_0(\mathfrak{n}), \mathbb{Q}) \tag{2.18}$$

Let A and B be points in $\mathcal{H}_3^*$ which are equivalent under the action of Γ', so that $B = \gamma(A)$ for some $\gamma \in \Gamma'$. Any smooth path from A to B in $\mathcal{H}_3^*$ projects to a closed path in the quotient space $\bar{X}_{\Gamma'}$, and hence determines a homology class in $H^1(\bar{X}_{\Gamma'}, \mathbb{Z})$ which depends only on A and B and not on the path chosen, because $\mathcal{H}_3^*$ is simply connected. In fact the class only depends on γ. We denote this homology class by the **modular symbol** $\{A, B\}_{\Gamma'}$, or simply $\{A, B\}$ if the group Γ' is clear from the context. The symbol $\{A, B\}_{\Gamma'}$ gives a functional $S(\Gamma') \to \mathbb{C}$ via $F \mapsto \int_A^B F \cdot \beta$ (β was defined in (2.10)), since by the harmonicity the integral is independent of the path from A to B. We may thus extend the definition of the symbol $\{A, B\}$ to points $A, B \in \mathcal{H}_3^*$ not necessarily Γ'-equivalent by identifying $\{A, B\}$ with the functional $F \mapsto \int_A^B F \cdot \beta$; now, in general, we have $\{A, B\} \in H^1(\bar{X}_{\Gamma'}, \mathbb{C})$. A generalisation of the Manin-Drinfeld Theorem says that when A, B are k-rational cusps and Γ' is a congruence subgroup, then $\{A, B\} \in H^1(\bar{X}_{\Gamma'}, \mathbb{Q})$.

We can therefore calculate (2.18) using modular symbols between cusps. In fact we will only compute the homology group on one copy of $\bar{X}_{\Gamma_0(\mathfrak{n})}$ as they are all the same. This is equivalent to finding only the $f^{(1)}$ component of a cusp form. Using the fact that h is odd allows us to extract all the information that we need from this one copy of hyperbolic three space.

Chapter 3

Geometrical algorithms

As usual let k be an imaginary quadratic number field with ring of integers $\mathcal{O} = \mathbb{Z} + \omega\mathbb{Z}$ and class number h. One of the main goals of this chapter is to obtain a tessellation of $\mathcal{H}_3^*$ on which Γ acts, a tessellation by "ideal" polyhedra (i.e. hyperbolic polyhedra all of whose vertices are at cusps). Our approach closely follows the work of Cremona and his previous students, the main innovation in this thesis being the method for constructing the polyhedra around a singular point. This problem doesn't occur when $h = 1$ and in the case $h = 2$ Bygott avoided the issue by working with an enlargement of Γ. We develop the theory for general k, and give all the geometrical details for $k = \mathbb{Q}(\sqrt{-23})$ and $k = \mathbb{Q}(\sqrt{-31})$, which have $h = 3$. There are two stages.

First, we find a fundamental region $\mathcal{F}_k$ for the action of Γ on $\mathcal{H}_3^*$. This involves studying the geometry of hemispheres, and leads to certain algorithms, akin to the Euclidean algorithm, which will be important for our computations later in the thesis.

Then, we cut $\mathcal{F}_k$ into pieces and glue together various translates of these pieces to form hyperbolic tetrahedra, with vertices at the cusps, which tessellate $\mathcal{H}_3^*$.

3.1 Fundamental region

We will define here, the action of three particular matrices in $\Gamma = \mathrm{GL}_2(\mathcal{O})$ which we will use later.

$$T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} : (z, r) \longmapsto (z+1, r), \tag{3.1}$$

$$U := \begin{pmatrix} 1 & \omega \\ 0 & 1 \end{pmatrix} : (z, r) \longmapsto (z+\omega, r), \tag{3.2}$$

$$J := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} : (z, r) \longmapsto (-z, r). \tag{3.3}$$

N.B. for any imaginary quadratic field (except $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$), the group $\langle T, U, J, -I\rangle \subset \Gamma$ is equal to the stabiliser of ∞, which we denote E_∞. It can be written as:

$$E_\infty = \left\{ \pm \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in \{\pm 1\}, b \in \mathcal{O} \right\}. \tag{3.4}$$

Definition 3.1.1. *A* ***fundamental domain*** *or* ***fundamental region*** *for the action of a group G on a topological space X is a connected subset F of X such that every orbit of G meets F at most once and meets the closure of F at least once.*

Bygott ([5], pg 57), makes the following definition:

Definition 3.1.2. *The* ***pseudo-Euclidean function*** *for k is the function $\Delta : \mathbb{P}^1(k) \to \mathbb{N}$ given by:*

$$\frac{\lambda}{\mu} \longmapsto \frac{\mathrm{N}\langle \mu \rangle}{\mathrm{N}\langle \lambda, \mu \rangle}.$$

Clearly $\Delta(\alpha) = 0$ if and only if $\alpha = \infty$. Note that $\Delta(\alpha) = 1$ if and only if $\alpha \in \mathcal{O}$. If $\alpha = \frac{\lambda}{\mu}$ is a principal cusp written in lowest terms, then $\Delta(\alpha) = N(\mu) = |\mu|^2$. Thus Δ generalises the notion of "size of the denominator".

Definition 3.1.3. *For $\alpha \in k$, the hemisphere attached to α, denoted S_α, is the set*

$$S_\alpha := \left\{ (z, r) \in \mathcal{H}_3^* : |z - \alpha|^2 + r^2 = \frac{1}{\Delta(\alpha)} \right\}. \tag{3.5}$$

In hyperbolic space, this is a geodesic surface; in Euclidean space it is a hemisphere. We say that a point $(z, r) \in \mathcal{H}_3^*$ lies under S_α, or that S_α covers (z, r), if

$$|z-\alpha|^2 + r^2 < \frac{1}{\Delta(\alpha)}.$$

Definition 3.1.4. *For $\alpha \in k$, the circle attached to α, denoted C_α, is the set*

$$C_\alpha \quad := \quad \left\{(z,0) \in \mathcal{H}_3^* : |z-\alpha|^2 = \frac{1}{\Delta(\alpha)}\right\}. \tag{3.6}$$

Clearly $C_\alpha = S_\alpha \cap \mathbb{C}$ is a circle in $\mathbb{C}$, where we identify $\mathbb{C}$ with the floor of $\mathcal{H}_3^*$.

Definition 3.1.5. *A hemisphere S_α or a circle C_α is **principal** if α is a principal cusp.*

It turns out that we only need to use principal hemispheres in the construction of our tessellation. In this case there is a simpler description of S_α. If $\alpha = \frac{\lambda}{\mu}$ in lowest terms, we have:

$$S_\alpha = \left\{(z,r) \in \mathcal{H} : |\mu z - \lambda|^2 + |\mu|^2 r^2 = 1\right\}.$$

In this case the S_α are Euclidean hemispheres centre $(\frac{\lambda}{\mu}, 0)$, radius $\frac{1}{|\mu|}$.

Lemma 3.1.6. *Let $(z, r) \in \mathcal{H}_3$. Then the set of principal cusps α such that S_α covers (z, r) is finite.*

Proof. Let $\alpha = \frac{\lambda}{\mu}$ be a principal cusp such that S_α covers the point (z, r). Then we must have:

$$|\mu z - \lambda|^2 + |\mu|^2 r^2 < 1.$$

Now

$$|\mu z - \lambda|^2 \geq 0 \ \text{ so } \ |\mu|^2 r^2 < 1,$$

i.e.

$$|\mu|^2 < r^{-2}.$$

This gives an upper bound for $|\mu|$. Since $\mu \in \mathcal{O}$ the number of such μ is finite.

Now, for each such (fixed) μ, we seek λ, satisfying

$$|\mu z - \lambda|^2 < 1 - |\mu|^2 r^2.$$

Set $\delta = \mu z - \lambda$. We wish to find all δ with $|\delta|^2 < 1 - |\mu|^2 r^2$, then $\lambda = \mu z - \delta$. Thus we have upper bounds for the norms of both λ and μ, so there can only be a finite number of such α's. $\square$

Clearly the same idea shows that there are only finitely many α's such that S_α contains (z, r).

Lemma 3.1.7. *Let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathcal{O})$, let $\alpha = -d/c$ be a principal cusp, and let $(z', r') = M \cdot (z, r)$. Then*

$$\frac{r}{r'} = \begin{cases} 1 & \text{if } \alpha = \infty, \\ |cz - d|^2 + |c|^2 r^2 & \text{otherwise.} \end{cases}$$

Hence $r' > r$ if and only if (z, r) lies under the hemisphere S_α. Similarly, $r' = r$ if and only if $(z, r) \in S_\alpha$, and $r' < r$ if and only if (z, r) lies outside of S_α.

Proof. [5], Lemma 49, pg 59. $\square$

In other words, if S_α covers (z, r), then applying M raises the "height" of (z, r), (but only finitely many greater heights can be obtained, by Lemma 3.1.6). The points which cannot be raised, because they lie under no suitable principal hemisphere, are of special importance.

Lemma 3.1.8. *Let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathcal{O})$, let $\alpha = -d/c$, and let β be an arbitrary cusp. Then*

$$\Delta(M_\alpha \cdot \beta) = \begin{cases} \Delta(\beta) & \text{if } \alpha = \infty, \\ |c|^2 & \text{if } \beta = \infty, \\ \Delta(\beta)|c\beta - d|^2 & \text{otherwise.} \end{cases}$$

Consequently, $\Delta(M \cdot \beta) < \Delta(\beta)$ if and only if β lies inside C_α. Similarly, $\Delta(M \cdot \beta) = \Delta(\beta)$ if and only if $\beta \in C_\alpha$, and $\Delta(M \cdot \beta) > \Delta(\beta)$ if and only if β lies outside C_α.

Proof. [5], Lemma 50, pg 60. $\square$

In other words, if β lies inside C_α then applying M reduces the "size" of β as measured by Δ. In view of this, the points that lie inside no C_α are of special importance.

Definition 3.1.9. *A cusp β is **singular** if it lies inside no principal C_α.*

Lemma 3.1.10. *Let β be a cusp. Then β is singular if and only if $\Delta(\beta)$ is minimal for points in the Γ orbit of β.*

Proof. [5], Corollary 51, pg 61. ☐

Now we saw in section 1.4 that Γ maps cusps to cusps. We also saw that there are h orbits of cusps, Lemma 1.4.5. Any principal cusp is equivalent to ∞, so it follows that the number of singular points in the fundamental region for Γ is equal to $h-1$.

We have the following general definition of the fundamental region $\mathcal{F}_k$:

Definition 3.1.11. *Let k be an imaginary quadratic field of discriminant D, where $D \neq -4, -3$. We define*

$$
\begin{aligned}
\mathcal{B}_k &= \left\{ \begin{array}{ll} (z,r) \in \mathcal{H}_3^* : & |cz-d|^2 + |d|^2 r^2 \geq 1 \textit{ for all } c,d \in \mathcal{O} \\ & \textit{with } \langle c,d \rangle = \mathcal{O} \end{array} \right\} \\
\partial\mathcal{B}_k &= \left\{ \begin{array}{ll} (z,r) \in \mathcal{H}_3^* : & |cz-d|^2 + |d|^2 r^2 \geq 1 \textit{ for all } c,d \in \mathcal{O} \textit{ with} \\ & \langle c,d \rangle = \mathcal{O} \textit{ and } |cz-d|^2 + |d|^2 r^2 = 1 \\ & \textit{for at least one pair } c,d \end{array} \right\} \\
F_k &= \left\{ x+iy \in \mathbb{C} : -1/2 < x \leq 1/2,\ 0 \leq y \leq \sqrt{|D|}/4 \right\} \\
\mathcal{F}_k &= \{(z,r) \in \mathcal{B}_k : z \in F_k\}
\end{aligned}
$$

$\mathcal{B}_k$ is the region above all principal hemispheres, $\partial\mathcal{B}_k$ is the "floor" of this region and F_k is a fundamental region for the action of $E_\infty = \langle T, U, J \rangle$ on $\mathbb{C}$.

When $D = -4, -3$ F_k needs to be defined differently, see [12], Definition 3.1, pg 318.

Theorem 3.1.12. *The set $\mathcal{F}_k$ is a fundamental region for Γ on $\mathcal{H}_3^*$.*

Proof. Let $(z,r) \in \mathcal{H}_3$. If there is at least one principal cusp $\alpha = \frac{\lambda}{\mu}$ such that S_α covers (z,r), we may choose, from among the finitely many such cusps, one that minimises the quantity $|\mu z - \lambda|^2 + |\mu|^2 r^2$; otherwise (z,r) is already in $\mathcal{B}_k$. Put $(z', r') = M_\alpha \cdot (z,r)$. Multiplying M_α on the left by an element of E_∞ if necessary, we may assume that $z' \in F_k$. By Lemma 3.1.7, r' is maximal among the r-coordinates of points in the Γ-orbit of (z,r), so no principal hemisphere covers (z', r'). Consequently $M_\alpha \cdot (z,r) \in \mathcal{F}_k$.

Now let z be a cusp. The same argument works unless the image of z modulo E_∞ is a singular point. But then the cusp will already be equivalent to a point in $\mathcal{F}_k$.

Now let $(z,r),(z',r')$ be two points in the interior of $\mathcal{F}_k$, and suppose that $M\cdot(z,r)=(z',r')$ for some $M=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\Gamma$. Then $r\geq r'$, since $S_{-d/c}$ does not cover (z,r); by symmetry $r=r'$. Hence (z,r) lies on $S_{-d/c}$, forcing $c=0$, so (up to scalars) $M\in E_\infty$. Since $z,z'\in F_k$, we deduce that $z=z'$. □

So all that remains is to actually find an explicit description of $\mathcal{F}_k$. Swan proves that the floor of $\mathcal{F}_k$ is contained in the union of finitely many hemispheres S_α, ([23], Theorem 3.13, pg 22). He also gives an algorithm for finding all the S_α which form part of the boundary.

Define:

$$S \;=\; \{S_\alpha : S_\alpha \text{ is principal and } S_\alpha\cap\mathcal{F}_k\neq\emptyset\} \tag{3.7}$$

Swan's algorithm for determining $\mathcal{F}_k$ is as follows:

1. Start with a set of principal hemispheres $S'=\{S_{\alpha_i} : i=1,\ldots,n\}$ which cover F_k, except for finitely many isolated points.

2. Find $V:=\{p\in\mathcal{H}_3 : p\in S_{\alpha_i} \text{ for 3 or more } i\in\{1,\ldots,n\}\}$.

3. For each $v\in V$ find $S_v:=\{\text{principal hemispheres which cover } v\}$, using the method from the proof of Lemma 3.1.6.

4. If $S_v=\emptyset$ for all $v\in V$ then we are done, $S=S'$

Otherwise

5. $\forall v=(z,r)\in V$ with $S_v\neq\emptyset$ find S_β such that $(z,r')\in S_\beta$ has the largest r co-ordinate.

6. Set $S'=S'\cup\{S_\beta\}$.

7. Goto 2.

This algorithm was used by Cremona and Whitley to determine $\mathcal{F}_k$ for all k with class number 1. We have implemented it in Magma and used it to obtain $\mathcal{F}_k$ for $k=\mathbb{Q}(\sqrt{-23}),\mathbb{Q}(\sqrt{-31})$, both with class number 3.

3.2 Examples

Let $A = \{\alpha \in k : S_\alpha \in S\}$.

3.2.1 $\mathbb{Q}(\sqrt{-23})$

We find that for this field the set A contains the points:

$$
\begin{array}{lll}
C_1 = \dfrac{5\omega-2}{12} & C_8 = \dfrac{2\omega-1}{4} & C_{15} = \dfrac{5\omega-2}{8} \\
C_2 = \dfrac{5\omega-3}{12} & C_9 = \dfrac{2\omega+1}{4} & C_{16} = \dfrac{\omega-2}{3} \\
C_3 = \dfrac{7\omega-10}{12} & C_{10} = \dfrac{3\omega+2}{8} & C_{17} = \dfrac{\omega+1}{3} \\
C_4 = \dfrac{7\omega-9}{12} & C_{11} = \dfrac{3\omega+3}{8} & C_{18} = -1 \\
C_5 = \dfrac{7\omega+2}{12} & C_{12} = \dfrac{3\omega-6}{8} & C_{19} = 0 \\
C_6 = \dfrac{7\omega+3}{12} & C_{13} = \dfrac{3\omega-5}{8} & C_{20} = 1 \\
C_7 = \dfrac{2\omega-3}{4} & C_{14} = \dfrac{5\omega-3}{8} &
\end{array}
$$

N.B. these are not written in lowest terms.

Figure 3.1, below, shows the floor of $\mathcal{B}_k$ comprising of sections of hemisphere centred on points in A.

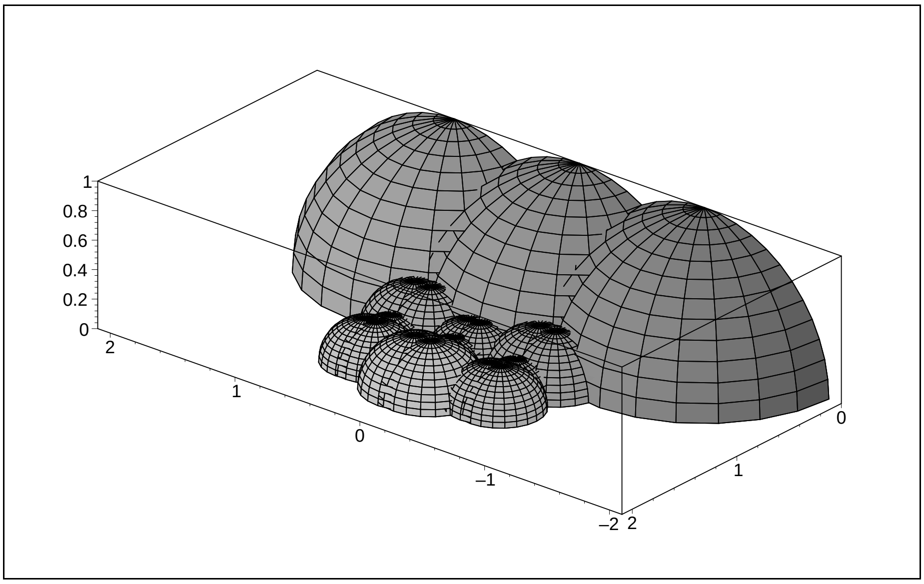


Figure 3.1: S_α for all $\alpha \in A$

Figure 3.2 shows the outline of all the hemispheres pictured in Figure 3.1 on the floor of $\mathcal{H}_3^*$.

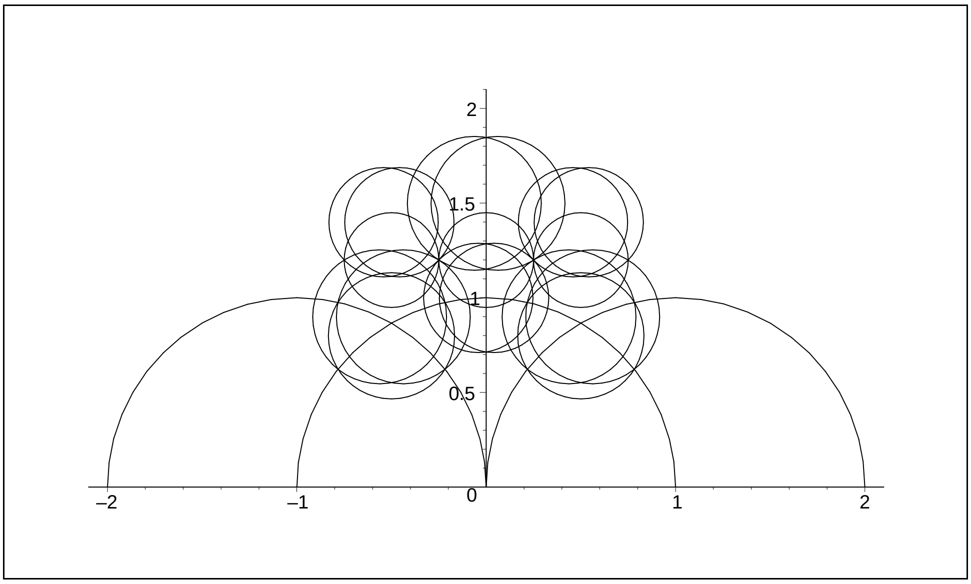


Figure 3.2: C_α for all $\alpha \in A$

Note that this diagram illustrates another symmetry, given by $z \mapsto -\bar{z}$. This is not in Γ, but would allow us to obtain all the geometry from just half of the region F_k.

Figure 3.3 below shows a projection of the fundamental region down onto the floor of F_k. Only the thick lines are "true edges" or 1-cells of $\partial\mathcal{B}_k$.

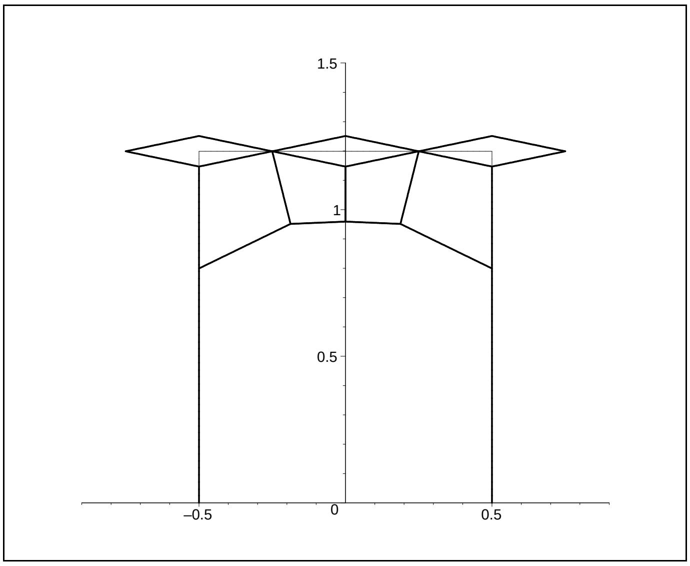


Figure 3.3: Projection of the fundamental region onto the floor

Figure 3.4 shows how the orbits of Figure 3.3 under Γ fit together to cover the floor of $\mathcal{H}_3^*$.

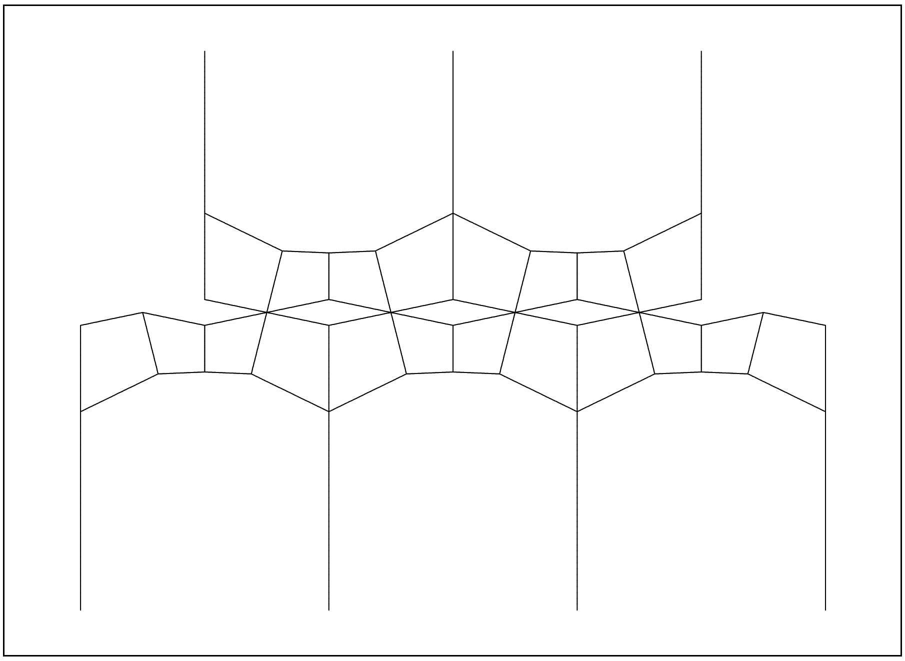


Figure 3.4: Tessellation of $\mathbb{C}$ by the fundamental region

3.2.2 $\mathbb{Q}(\sqrt{-31})$

As the size of the discriminant of k increases so does the complexity of the geometry. For this field we have 24 hemispheres, 4 more than for the first field.

$$
\begin{array}{lll}
C_1 = \dfrac{11\omega-7}{20} & C_2 = \dfrac{11\omega-4}{20} & C_3 = \dfrac{9\omega-16}{20} \\
C_4 = \dfrac{9\omega-13}{20} & C_5 = \dfrac{9\omega+4}{20} & C_6 = \dfrac{9\omega+7}{20} \\
C_7 = \dfrac{3\omega-7}{10} & C_8 = \dfrac{3\omega-6}{10} & C_9 = \dfrac{3\omega+3}{10} \\
C_{10} = \dfrac{3\omega+4}{10} & C_{11} = \dfrac{5\omega-5}{8} & C_{12} = \dfrac{5\omega}{8} \\
C_{13} = \dfrac{3\omega-3}{8} & C_{14} = \dfrac{3\omega}{8} & C_{15} = \dfrac{2\omega-3}{4} \\
C_{16} = \dfrac{2\omega-1}{4} & C_{17} = \dfrac{2\omega+1}{4} & C_{18} = \dfrac{\omega-2}{3} \\
C_{19} = \dfrac{\omega-1}{3} & C_{20} = \dfrac{\omega}{3} & C_{21} = \dfrac{\omega+1}{3} \\
C_{22} = -1 & C_{23} = 0 & C_{24} = 1
\end{array}
$$

The following figures show the same information as Figures 3.1-3.4, for $\mathbb{Q}(\sqrt{-31})$.

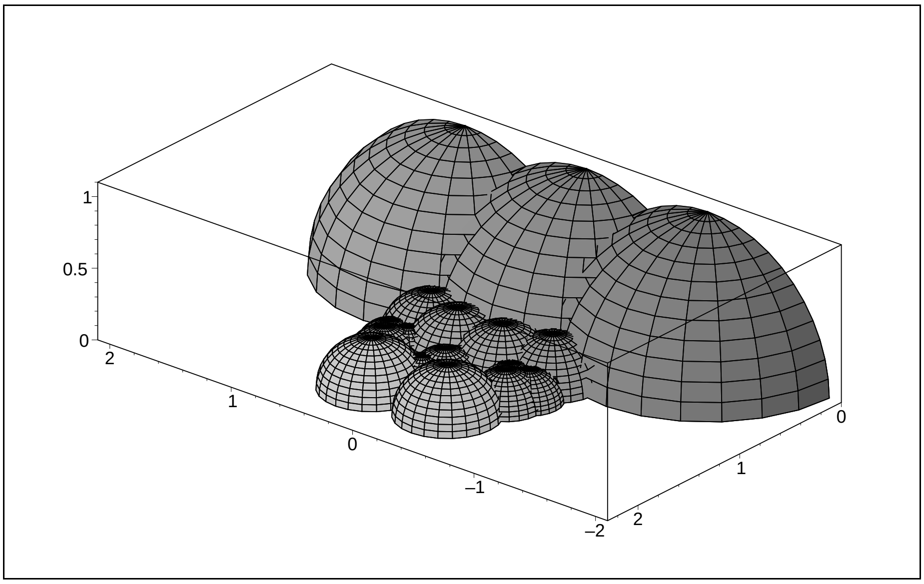


Figure 3.5: S_α for all $\alpha \in A$

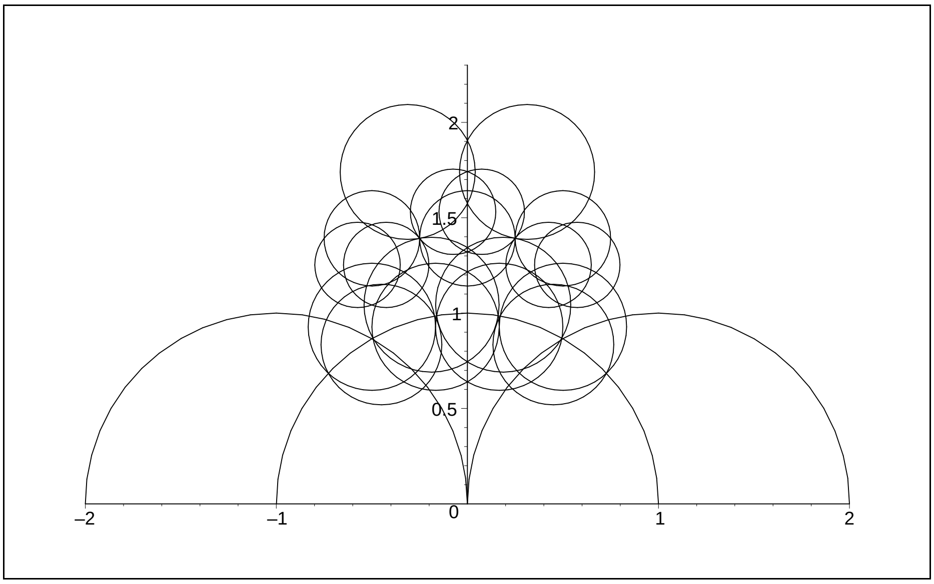


Figure 3.6: C_α for all $\alpha \in A$

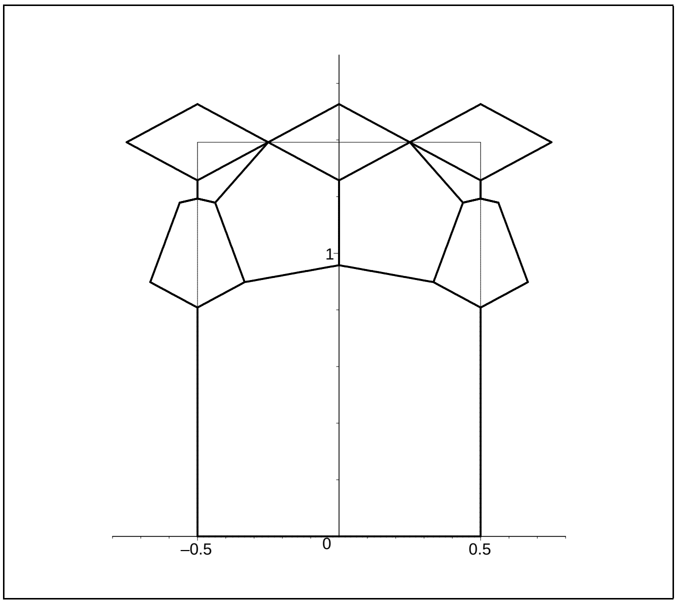


Figure 3.7: Projection of the fundamental region onto the floor

3.3 Pseudo-Euclidean algorithm

Having determined $\mathcal{F}_k$ we can give an explicit "pseudo-Euclidean" algorithm. More precisely, we need to know:

1. a fundamental region F_k for $\mathbb{C}$ with respect to E_∞;

2. a sub-algorithm that returns, given $z \in \mathbb{C}$, a matrix $M \in E_\infty$, such that $M \cdot z \in F_k$;

3. a list $s_1, \ldots, s_n$ of the singular points in F_k, together with $s_0 = \infty$;

4. the decomposition of F_k into polygonal 2-cells, $P_1, \ldots, P_m$, obtained by projecting $\partial\mathcal{B}_k$ onto $\mathbb{C}$;

5. for each $i \in \{1, \ldots, m\}$, the cusp α_i such that P_i is the projection onto $\mathbb{C}$ of the hyperbolic polygon $S_{\alpha_i} \cap \partial\mathcal{B}_k$;

6. for each $i \in \{1, \ldots, m\}$, an "inversion matrix" $M_i \in \Gamma$ such that $M_i \cdot \alpha_i = \infty$.

It is shown in [5] pg 67 that we can further choose the M_i uniquely so that $M_i \cdot \infty \in \{\alpha_1, \ldots, \alpha_m\}$.

This algorithm is used in section 4.3 to convert M-symbols to modular symbols, and forms a key part of the overall algorithm which must be determined separately for each individual field.

3.3.1 The algorithm for cusps

This algorithm maps any cusp to a singular point or ∞. More precisely, given $\beta \in \mathbb{P}^1(k)$, this algorithm returns a matrix M, expressed as a word in the elements of E_∞ and the matrices M_i, such that $M \cdot \beta = s_j$ for some $j \in \{0, ..n\}$.

1. If $\beta \in \{s_0, \ldots, s_n\}$ then stop; otherwise, apply a matrix in E_∞, found using the sub-algorithm above, to amp β into F_k.
2. If $\beta \in \{s_0, \ldots, s_n\}$ then stop; otherwise, choose i such that β lies inside C_{α_i}, apply the inversion matrix M_i, and go to 1.

This algorithm always terminates because each inversion step reduces the natural number $\Delta(\beta)$ by Lemma 3.1.8, which can only happen a finite number of times; after which β is clearly one of the singular points or ∞.

There is also a very similar algorithm for interior points. It will not be used in this thesis but has applications in other areas, such as the reduction of Hermitian forms over k, cf [22].

3.4 Tessellation of $\mathcal{H}_3^*$

We are interested in the vertices of the fundamental region, i.e. the 0-cells of the cell decomposition of $\partial\mathcal{B}_k$. They are the points above the "true vertices" (points where three or more "true edges" meet) of Figure 3.3. They are clearly the points where the height of the covering of the floor has a local minimum.

We consider the tessellation of $\mathbb{C}$ dual to the one shown in Figure 3.3, i.e. with vertices at the centres of the hemispheres making up the 2-cells of $\partial\mathcal{B}_k$, and with two vertices joined by an edge if and only if the corresponding hemispheres meet at a 1-cell or 0-cell of $\partial\mathcal{B}_k$.

3.4.1 Method

Here we outline the method which can be used when there are no singular points. This is true in the case when $h = 1$ and was also the case when Bygott looked at $h = 2$ because he introduced additional hemispheres. It is useful to describe the method here because it can still be used to find the polyhedra around the principal cusps. I will describe the new method that I used for the polyhedra around the singular points in the next section.

Let $\mathcal{F}$ be the fundamental region and let

$$V := \{\text{vertices of } \mathcal{F}\} \setminus \{\infty\}.$$

N.B. we know from Swan that V is finite.

Then, for each $v \in V$ define

$$A_v := \{\alpha \in A : v \in S_\alpha\}.$$

So A_v is the set of the centres of the hemispheres in the floor of $\mathcal{F}$ which contain v.

Definition 3.4.1. *Let $v, w \in V$. Then we define*

$$E_v := \{\gamma \in \Gamma : \gamma v = v\}, \tag{3.8}$$
$$F_{vw} := \{\gamma \in \Gamma : \gamma v = w\}. \tag{3.9}$$

We will associate a polyhedron with every $v \in V$ and denote it by P_v. We begin by partitioning the space $\mathcal{F}$ into $n = \#V$ subsets, each associated with some vertex $v \in V$. We do this using the vertical half-planes $Q_{\lambda,\mu;\sigma,\tau}$ through the points $\alpha = \frac{\lambda}{\mu}, \beta = \frac{\sigma}{\tau}$ and ∞, where $\alpha, \beta \in A$ and $S_\alpha \cap S_\beta \neq \emptyset$.

Each $v \in V$ is the point of intersection of $\{S_\alpha : \alpha \in A_v\}$. So, it is the intersection of three or more hemispheres. Thus, to each $v \in V$, there is associated a subset $\mathcal{F}^v$ of $\mathcal{F}$ which is bounded below by the union of $\{S_\alpha : \alpha \in A_v\}$ and with vertical sides which are the sections of the half-planes passing through $\alpha \in A_v$.

We now construct the polyhedron P_v by gluing together transforms of $\mathcal{F}^v$ by elements of E_v along corresponding edges.

If two vertices $v, w \in V$ are equivalent under the action of Γ, then the polyhedra P_v, P_w are also equivalent under this action. Thus we form P_v by gluing together translates of $\mathcal{F}^v$ by elements of E_v, and translates of $\mathcal{F}^w$ by elements of F_{vw} for all $w \in V$ which are equivalent to v, along common edges. Then

$$P_w = \gamma(P_v), \quad \gamma \in F_{vw}$$

Then the orbits of the P_v under Γ give a tessellation of $\mathcal{H}_3^*$ by hyperbolic polyhedra.

The following two lemmas will help us to determine E_v and F_{vw}.

Lemma 3.4.2. *Let $v \in V$ and let its stabiliser be E_v. Then*

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in E_v \Longrightarrow \frac{a}{c}, \frac{-d}{c} \in A_v.$$

Proof. Suppose γ fixes $v \in \mathcal{H}_3$. Then it follows that γ fixes some hemisphere containing v. In fact γ must fix $S_{c,-d}$, so $\frac{-d}{c} \in A_v$, by definition.

Similarly, γ^{-1} fixes $S_{c,a}$ and so $\frac{a}{c} \in A_v$, since $\gamma \in E_v \Rightarrow \gamma^{-1} \in E_v$. □

Lemma 3.4.3.

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in F_{vw} \Longrightarrow \frac{a}{c} \in A_w, \frac{-d}{c} \in A_v.$$

Proof. Use the same argument as 3.4.2. □

So $v, w \in V$ are equivalent under the action of $\Gamma \Leftrightarrow F_{vw} \neq \emptyset$.

Lemma 3.4.4. *Let $\zeta(v)$ denote the height of v. If $v, w \in V$ are equivalent then*

$$\zeta(v) = \zeta(w)$$

Proof. Let $v, w \in \mathcal{F}_k$ be Γ-equivalent. $\mathcal{F}_k$ is a subset of $\mathcal{B}_k$ and so $\zeta(\gamma(v)) \leq \zeta(v)$, for all $v \in \Gamma$. But $w = \gamma(v)$ for some $\gamma \in F_{vw}$, so $\zeta(w) \leq \zeta(v)$. Also $v = \delta(w)$ for some $\delta \in F_{wv}$, so $\zeta(v) \leq \zeta(w)$. Thus, $\zeta(v) = \zeta(w)$. □

The converse of this is not true in general.

Algorithm for finding E_v:

1. Find A_v and list all the points in the form $\frac{\lambda_i}{\mu_i}$
2. Fix $\mu \in \mathcal{O}$ such that there exists $\lambda \in \mathcal{O}$ with $\frac{\lambda}{\mu} \in A_v$.
3. Determine all $\lambda_i \in \mathcal{O}$ such that $\frac{\lambda_i}{\mu} \in A_v$.

4. Construct all matrices of the form:

$$\begin{pmatrix} \lambda_i & (\lambda_i\lambda_j \pm 1)/\mu \\ \mu & \lambda_j \end{pmatrix}$$

   with λ_i and λ_j not necessarily distinct.

5. Keep those matrices which lie in Γ and fix v.

6. Go to 2.

The algorithm for determining F_{vw} is similar. The only difference is that λ_j is chosen so that $\frac{\lambda_j}{\mu} \in A_w$.

3.4.2 Results

We have implemented the algorithm for finding a tessellation of $\mathcal{H}_3^*$ in Magma and describe the results here.

3.4.3 $\mathbb{Q}(\sqrt{-23})$

The set V contains the following points:

$$\begin{aligned}
P_1 &= \left(\frac{11\omega - 17}{23}, \sqrt{\frac{11}{184}}\right) & P_6 &= \left(\frac{\omega + 1}{3}, \frac{1}{3}\right) \\
P_2 &= \left(\frac{11\omega + 6}{23}, \sqrt{\frac{11}{184}}\right) & P_7 &= \left(\frac{73\omega - 71}{184}, \sqrt{\frac{11}{184}}\right) \\
P_3 &= \left(\frac{\omega - 1}{2}, 0\right) & P_8 &= \left(\frac{73\omega - 2}{184}, \sqrt{\frac{11}{184}}\right) \\
P_4 &= \left(\frac{\omega}{2}, 0\right) & P_9 &= \left(\frac{22\omega - 11}{46}, \sqrt{\frac{11}{184}}\right) \\
P_5 &= \left(\frac{\omega - 2}{3}, \frac{1}{3}\right) & P_{10} &= \left(\frac{2\omega - 1}{5}, \frac{\sqrt{2}}{5}\right)
\end{aligned}$$

The tables below list the stabilisers of each point and the matrices which map points to different points in the same orbit. The tables each detail a separate orbit of vertices.

	P_1	P_2	P_7	P_8	P_9
P_1	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}\omega+1&3\\-\omega+2&-\omega-1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}\omega-2&\omega+1\\\omega+1&3\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}2\omega-1&\omega+5\\4&-2\omega+3\end{smallmatrix}\right)$
P_2	$\left(\begin{smallmatrix}1&-1\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}\omega+1&-\omega+2\\-\omega+2&-3\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}\omega-2&3\\\omega+1&-\omega+2\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}2\omega-1&\omega+6\\4&-2\omega-1\end{smallmatrix}\right)$
P_7	$\left(\begin{smallmatrix}\omega+1&3\\-\omega+2&-\omega-1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}3&-\omega+2\\-\omega+2&-\omega-1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}\omega-3&\omega+2\\\omega+2&-\omega+3\end{smallmatrix}\right)$
P_8	$\left(\begin{smallmatrix}-3&\omega+1\\\omega+1&-\omega+2\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}\omega-2&3\\\omega+1&-\omega+2\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}\omega+2&-\omega+3\\-\omega+3&-\omega-2\end{smallmatrix}\right)$
P_9	$\left(\begin{smallmatrix}2\omega-3&\omega+5\\4&-2\omega+1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}2\omega+1&-\omega+6\\4&-2\omega+1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}\omega-3&\omega+2\\\omega+2&-\omega+3\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}\omega+2&-\omega+3\\-\omega+3&-\omega-2\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$

	P_5	P_6
P_5	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}-1&-1\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}\omega+1&3\\-\omega+2&-\omega-1\end{smallmatrix}\right), \left(\begin{smallmatrix}-3&\omega-2\\\omega+1&3\end{smallmatrix}\right), \left(\begin{smallmatrix}\omega-2&\omega+1\\3&-\omega+2\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right), \left(\begin{smallmatrix}\omega-2&\omega+1\\\omega+1&3\end{smallmatrix}\right), \left(\begin{smallmatrix}\omega+1&3\\3&-\omega+2\end{smallmatrix}\right), \left(\begin{smallmatrix}3&-\omega+2\\-\omega+2&-\omega-1\end{smallmatrix}\right)$
P_6	$\left(\begin{smallmatrix}1&-1\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}-1&0\\1&-1\end{smallmatrix}\right), \left(\begin{smallmatrix}-3&\omega+1\\\omega+1&-\omega+2\end{smallmatrix}\right), \left(\begin{smallmatrix}\omega-2&3\\3&-\omega-1\end{smallmatrix}\right), \left(\begin{smallmatrix}\omega+1&-\omega+2\\-\omega+2&-3\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}-1&-1\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}\omega-2&3\\\omega+1&-\omega+2\end{smallmatrix}\right), \left(\begin{smallmatrix}\omega+1&-\omega+2\\3&-\omega-1\end{smallmatrix}\right), \left(\begin{smallmatrix}3&-\omega-1\\-\omega+2&-3\end{smallmatrix}\right)$

	P_{10}
P_{10}	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}\omega-3&\omega+2\\\omega+2&-\omega+3\end{smallmatrix}\right), \left(\begin{smallmatrix}\omega+2&-\omega+3\\\omega+3&-\omega-2\end{smallmatrix}\right)$

Table 3.8: E_v and F_{vw} for $\mathbb{Q}(\sqrt{-23})$

P_3 and P_4 have infinite stabilisers because they lie on the floor. They are not in the same orbit because Γ preserves the class of cusps. So, there are five orbits of V under Γ.

It is the fact that E_{P_3} and E_{P_4} are infinite which means that the method outlined above does not work. However it turns out that it is still possible to generate the polyhedra using the stabilisers, you just have to restrict attention to certain special elements of E_v.

For example, to find the shape of the polyhedra around $\frac{\omega}{2}$ we begin by looking at $\mathcal{F}_{\omega/2}$. It naturally divides into three pieces, as shown in Figure 3.9, each with a vertex at $\frac{\omega}{2}$. It turns out that we need to look at those elements of $E_{\omega/2}$ which also fix another vertex of $\mathcal{F}_{\omega/2}$. Label the three sections A, B, C from left to right and the lines where they join a and b. Then the image of A under the stabiliser of a glues to the bottom of B. So does the image of C under b. These three pieces form a complete tetrahedron.

Figure 3.9 below shows how the fundamental region was divided up.

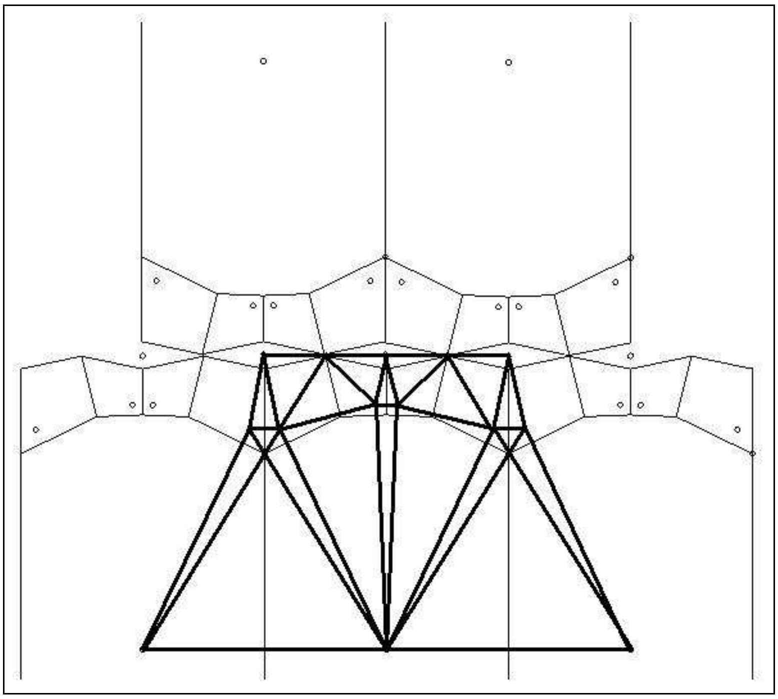


Figure 3.9: Projection of the hyperbolic tessellation onto the floor

3.4.4 $\mathbb{Q}(\sqrt{-31})$

Again we see that the geometry is more complicated, we have 4 more vertices.

$$
\begin{aligned}
P_1 &= \left(\frac{9\omega-20}{31}, \sqrt{\frac{3}{31}}\right) & P_8 &= \left(\frac{30\omega-46}{93}, \sqrt{\frac{23}{279}}\right)\\
P_2 &= \left(\frac{28\omega-45}{62}, \sqrt{\frac{11}{248}}\right) & P_9 &= \left(\frac{28\omega+17}{62}, \sqrt{\frac{11}{248}}\right)\\
P_3 &= \left(\frac{3\omega+2}{7}, \sqrt{\frac{2}{49}}\right) & P_{10} &= \left(\frac{30\omega+16}{93}, \sqrt{\frac{23}{279}}\right)\\
P_4 &= \left(\frac{105\omega-161}{248}, \sqrt{\frac{11}{248}}\right) & P_{11} &= \left(\frac{3\omega-5}{7}, \sqrt{\frac{2}{49}}\right)\\
P_5 &= \left(\frac{32\omega-16}{93}, \sqrt{\frac{23}{279}}\right) & P_{12} &= \left(\frac{9\omega+11}{31}, \sqrt{\frac{3}{31}}\right)\\
P_6 &= \left(\frac{14\omega-7}{31}, \sqrt{\frac{11}{248}}\right) & P_{13} &= \left(\frac{\omega-1}{2}, 0\right)\\
P_7 &= \left(\frac{105\omega+56}{248}, \sqrt{\frac{11}{248}}\right) & P_{14} &= \left(\frac{\omega}{2}, 0\right)
\end{aligned}
$$

This time they fall into 6 orbits. The tables below list the stabilisers of each point and the matrices which map points to different points in the same orbit. The tables each detail a separate orbit of vertices.

	P_1	P_2
P_1	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}-1&-1\\1&0\end{smallmatrix}\right),\left(\begin{smallmatrix}0&-1\\1&1\end{smallmatrix}\right),$ $\left(\begin{smallmatrix}-3&\omega-2\\\omega+1&3\end{smallmatrix}\right),\left(\begin{smallmatrix}\omega+1&3\\-\omega+2&-\omega-1\end{smallmatrix}\right),\left(\begin{smallmatrix}\omega-2&\omega+1\\3&-\omega+2\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right),$ $\left(\begin{smallmatrix}\omega+1&3\\3&-\omega+2\end{smallmatrix}\right),\left(\begin{smallmatrix}3&-\omega+2\\-\omega+2&-\omega-1\end{smallmatrix}\right),\left(\begin{smallmatrix}\omega-2&\omega+1\\\omega+1&3\end{smallmatrix}\right)$
P_2	$\left(\begin{smallmatrix}1&-1\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right),\left(\begin{smallmatrix}-1&0\\1&-1\end{smallmatrix}\right),$ $\left(\begin{smallmatrix}\omega-2&3\\3&-\omega-1\end{smallmatrix}\right),\left(\begin{smallmatrix}\omega+1&-\omega+2\\-\omega+2&-3\end{smallmatrix}\right),\left(\begin{smallmatrix}-3&\omega+1\\\omega+1&-\omega+2\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}0&-1\\1&-1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&-1\\1&0\end{smallmatrix}\right),$ $\left(\begin{smallmatrix}3&-\omega-1\\-\omega+2&-3\end{smallmatrix}\right),\left(\begin{smallmatrix}\omega+1&-\omega+2\\3&-\omega-1\end{smallmatrix}\right),\left(\begin{smallmatrix}\omega+2&3\\\omega+1&-\omega+2\end{smallmatrix}\right)$

	P_3	P_4
P_3	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}\omega-6&3\omega-1\\\omega+3&-\omega+6\end{smallmatrix}\right),$ $\left(\begin{smallmatrix}2\omega+1&8\\-\omega+4&-2\omega-1\end{smallmatrix}\right),\left(\begin{smallmatrix}\omega-2&\omega+1\\3&-\omega+2\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}2\omega-3&2\omega+5\\\omega+3&-\omega+6\end{smallmatrix}\right),$ $\left(\begin{smallmatrix}\omega+1&3\\3&-\omega+2\end{smallmatrix}\right),\left(\begin{smallmatrix}\omega+5&-2\omega+7\\-\omega+4&-2\omega-1\end{smallmatrix}\right)$
P_4	$\left(\begin{smallmatrix}1&-1\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}\omega-6&2\omega+5\\\omega+3&-2\omega+3\end{smallmatrix}\right),$ $\left(\begin{smallmatrix}\omega-2&3\\3&-\omega-1\end{smallmatrix}\right),\left(\begin{smallmatrix}2\omega+1&-2\omega+7\\-\omega+4&-\omega-5\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}\omega+1&-\omega+2\\3&-\omega-1\end{smallmatrix}\right),$ $\left(\begin{smallmatrix}2\omega-3&8\\\omega+3&-2\omega+3\end{smallmatrix}\right),\left(\begin{smallmatrix}\omega+5&-3\omega+2\\-\omega+4&-\omega-5\end{smallmatrix}\right)$

	P_5	P_6	P_7
P_5	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}-3&\omega-2\\\omega+1&3\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}\omega&3\\3&-\omega+1\end{smallmatrix}\right),\left(\begin{smallmatrix}-3&\omega-1\\\omega&3\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right),\left(\begin{smallmatrix}\omega+1&3\\3&-\omega+2\end{smallmatrix}\right)$
P_6	$\left(\begin{smallmatrix}\omega-1&3\\3&-\omega\end{smallmatrix}\right),\left(\begin{smallmatrix}-3&\omega-1\\\omega&3\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}\omega&3\\3&\omega+1\end{smallmatrix}\right),\left(\begin{smallmatrix}3&-\omega\\-\omega+1&-3\end{smallmatrix}\right)$
P_7	$\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right),\left(\begin{smallmatrix}\omega-2&3\\3&-\omega-1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}\omega-1&3\\3&-\omega\end{smallmatrix}\right),\left(\begin{smallmatrix}3&-\omega\\-\omega+1&-3\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}3&-\omega-1\\-\omega+2&-3\end{smallmatrix}\right)$

	P_8	P_9	P_{10}	P_{11}	P_{12}
P_8	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}2\omega-3&\omega+7\\4&-2\omega+1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}2\omega+1&-\omega+8\\4&-2\omega+1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}-3&\omega-1\\\omega&3\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}3&-\omega\\-\omega+1&-3\end{smallmatrix}\right)$
P_9	$\left(\begin{smallmatrix}2\omega-1&\omega+7\\4&-2\omega+3\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}2\omega+1&8\\-\omega+4&-2\omega-1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}2\omega-3&2\omega+5\\\omega+3&-\omega+6\end{smallmatrix}\right)$
P_{10}	$\left(\begin{smallmatrix}2\omega-1&-\omega+8\\4&-2\omega-1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&-1\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}2\omega+1&-2\omega+7\\-\omega+4&-\omega-5\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}2\omega-3&8\\\omega+3&-2\omega+3\end{smallmatrix}\right)$
P_{11}	$\left(\begin{smallmatrix}-3&\omega-1\\\omega&3\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}2\omega+1&8\\-\omega+4&-2\omega-1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}\omega+5&-2\omega+7\\-\omega+4&-2\omega-1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}\omega+1&3\\3&-\omega+2\end{smallmatrix}\right)$
P_{12}	$\left(\begin{smallmatrix}3&-\omega\\-\omega+1&-3\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}\omega-6&2\omega+5\\\omega+3&-2\omega+3\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}2\omega-3&8\\\omega+3&-2\omega+3\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}\omega-2&3\\3&-\omega-1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$

Table 3.10: E_v and F_{vw} for $\mathbb{Q}(\sqrt{-31})$

Having now obtained a tessellation of $\mathcal{H}_3$ by ideal polyhedra we will show in the next chapter how to use this to calculate the 1-homology group of various quotients of $\mathcal{H}_3$.

Chapter 4

Homology

The tessellation of $\mathcal{H}_3^*$ we constructed in the previous section will now be used to calculate the 1-homology groups of various quotients of $\mathcal{H}_3^*$.

Let G be a subgroup of finite index in Γ. Then when we pass to the quotient $G \setminus \mathcal{H}_3^*$ we will obtain a tessellation of the quotient space by a finite number of hyperbolic polyhedra. In order to calculate the 1-homology on these spaces we study the vertices and edges of these tessellation, and how they behave under the action of Γ. The edges of a tessellation will split up into a finite number of orbits under Γ. We can choose a representative from each class, e_i, of the form $\{\alpha, \infty\}$, where $\alpha \in A$. Now let $\mathcal{G}$ be a complete set of coset representatives for G in Γ. Let I be an indexing set for the e_i. Each edge of one of the tessellations will have the form γe_i for some $i \in I$ and some $\gamma \in \mathcal{G}$; thus the homology of $\Gamma_0(\mathfrak{n}) \setminus \mathcal{H}_3^*$ is generated by the γe_i.

There is some redundancy: the stabiliser of the (unordered) edge e_i, when non-trivial, gives rise to some "edge relations". From our polyhedra, we obtain one "face relation" for each orbit of faces. Note that a polyhedron with F faces gives rise to at most $F-1$ independent face relations.

The relations we obtain encode all the necessary geometrical information about k in the form of algebraic symbols that are readily stored on a computer; the required homology calculations reduce to algebraic manipulations and linear algebra.

Define $V(G)$ to be the $\mathbb{Q}$-vector space spanned by the formal symbols $\{(\gamma)_\alpha : \alpha \in I, \gamma \in \mathcal{G}\}$. We let Γ act on $V(G)$, on the left, via

$$\gamma : (g)_\alpha \longmapsto (\gamma g)_\alpha.$$

Then $V(G)$ is a $\mathbb{Q}\Gamma$ module.

We define relations between the symbols $(\gamma)_\alpha$ corresponding to the edge and face relations that arise from the tessellation. Let $R(G)$ be the $\mathbb{Z}\Gamma$ submodule of $V(G)$ generated by these relations.

Let $V_0(G)$ be the set of cusp modulo G and define the "boundary map"

$$\delta : V(G) \longrightarrow V_0(G)$$

to be the map induced from

$$\delta : (\gamma)_\alpha \longmapsto [\gamma(\infty)] - [\gamma(\alpha)]$$

by $\mathbb{Q}$-linearity, where $[\alpha]$ denotes the class of cusps G-equivalent to α. We let $Z(G)$ denote the kernel of this boundary map.

Finally we set

$$H(G) := Z(G)/R(G).$$

There is a natural isomorphism from $H(G)$ to $\mathrm{H}_1(G \setminus \mathcal{H}_3^*, \mathbb{Q})$ induced by the map:

$$\xi : (\gamma)_\alpha \longmapsto \{\gamma(\alpha), \gamma(\infty)\}. \tag{4.1}$$

4.1 $\mathbb{Q}(\sqrt{-23})$

4.1.1 Generators

In the case being considered, the edges of the tessellation of $\mathcal{H}_3^*$ fall into nine orbits. Taking $C_1, \ldots, C_{20}$ as defined in section 3.2.1, and letting $C_{21} = \frac{\omega-1}{2}$, $C_{22} = \frac{\omega}{2}$, these can be written as:

$$\begin{array}{rclcrcl}
(\gamma)_a &=& \gamma\{C_1, \infty\} & \quad & (\gamma)_f &=& \gamma\{C_{17}, \infty\} \\
(\gamma)_b &=& \gamma\{C_2, \infty\} & & (\gamma)_g &=& \gamma\{C_{19}, \infty\} \\
(\gamma)_c &=& \gamma\{C_8, \infty\} & & (\gamma)_h &=& \gamma\{C_{21}, \infty\} \\
(\gamma)_d &=& \gamma\{C_{10}, \infty\} & & (\gamma)_i &=& \gamma\{C_{22}, \infty\} \\
(\gamma)_e &=& \gamma\{C_{13}, \infty\} & & & &
\end{array}$$

where $\gamma \in \Gamma$.

When we pass to the quotient $G \backslash \mathcal{H}_3^*$, for a given G, these nine orbits become finite, and we have one generator of each type for each element of $\mathcal{G}$. So we have $9[\Gamma : G]$ generators.

4.1.2 Edge relations

These come from matrices in the stabiliser of an edge of the tessellation. As with the face relations, the relations listed below are just used to generate the actual relations the will be used in the calculations at each level.

$$\begin{aligned}
\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_a &= -\left(\begin{smallmatrix} \omega+2 & -\omega+3 \\ -\omega+3 & -\omega-2 \end{smallmatrix}\right)_a \\
\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_b &= -\left(\begin{smallmatrix} \omega-3 & \omega+2 \\ \omega+2 & -\omega+3 \end{smallmatrix}\right)_b \\
\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_c &= -\left(\begin{smallmatrix} 2\omega-1 & 6 \\ 4 & -2\omega+1 \end{smallmatrix}\right)_c \\
\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_d &= -\left(\begin{smallmatrix} \omega-2 & 3 \\ \omega+1 & -\omega+2 \end{smallmatrix}\right)_d \\
\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_e &= -\left(\begin{smallmatrix} \omega+1 & 3 \\ -\omega+2 & -\omega-1 \end{smallmatrix}\right)_e \\
\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_f &= -\left(\begin{smallmatrix} \omega+1 & -\omega+2 \\ 3 & -\omega-1 \end{smallmatrix}\right)_f \\
\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_g &= -\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)_g \\
&= \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)_g \\
\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_h &= \left(\begin{smallmatrix} -1 & \omega-1 \\ 0 & 1 \end{smallmatrix}\right)_h \\
\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_i &= \left(\begin{smallmatrix} -1 & \omega \\ 0 & 1 \end{smallmatrix}\right)_i
\end{aligned}$$

So for example the first relation says that $M(\infty) = C_1$ and $M(C_1) = \infty$, where $M = \left(\begin{smallmatrix} \omega+2 & -\omega+3 \\ -\omega+3 & -\omega-2 \end{smallmatrix}\right)$.

4.1.3 Face relations

The computations carried out in Section 3.4.2 show that there are five distinct Γ-orbits of polyhedra in the tessellation of $\mathcal{H}_3^*$. We need only consider the face relations coming from one polyhedron from each orbit. The figure below shows the choice of representatives that was taken.

N.B. 4.1(b) and 4.1(c), 4.1(b) and 4.1(e) share common faces, so we will get redundant relations.

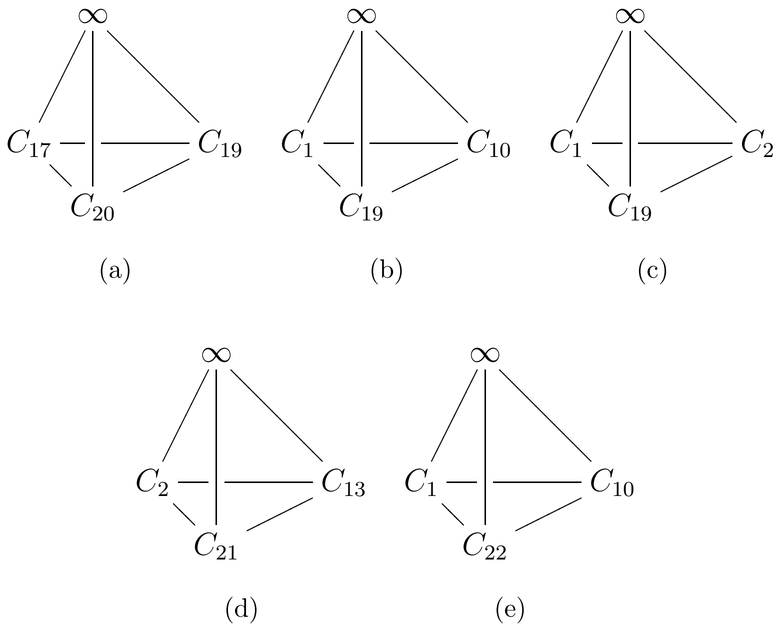


Figure 4.1: Representative polyhedra from the five orbits

The relations listed below are in a sense templates for the actual relations that will be used to calculate the 1-homology. They are given in terms of the symbols $(\gamma)_x$ with $\gamma \in \Gamma$. In order to turn them into relations for a specific subgroup G, the γs must be reduced to elements of $\mathcal{G}$. Then each of these relations will give us $[\Gamma : G]$ relations by pre-multiplying each term of the relation by an element of $\mathcal{G}$.

Below we list the face relations coming from each representative polyhedron. An R denotes the fact that the relation is redundant.

Face relations coming from Figure 4.1(a):

$$\begin{tikzcd}[arrows=-] & \infty \arrow[dl] \arrow[dr] & \\ C_{17} \arrow[rr] & & C_{19}\end{tikzcd} \qquad \left(\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right)_d + \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_g - \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_f = 0$$

$$\begin{tikzcd}[arrows=-] & \infty \arrow[dl] \arrow[dr] & \\ C_{17} \arrow[rr] & & C_{20}\end{tikzcd} \qquad \left(\begin{smallmatrix} -1 & 0 \\ -1 & -1 \end{smallmatrix}\right)_e + \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)_g - \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_f = 0$$

$$\begin{tikzcd}[arrows=-] & \infty \arrow[dl] \arrow[dr] & \\ C_{19} \arrow[rr] & & C_{20}\end{tikzcd} \qquad \left(\begin{smallmatrix} 1 & 0 \\ 1 & -1 \end{smallmatrix}\right)_g + \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)_g - \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_g = 0$$

$$\begin{tikzcd}[arrows=-] & C_{20} \arrow[dl] \arrow[dr] & \\ C_{17} \arrow[rr] & & C_{19}\end{tikzcd} \qquad \left(\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right)_d + \left(\begin{smallmatrix} 1 & 0 \\ 1 & -1 \end{smallmatrix}\right)_g - \left(\begin{smallmatrix} -1 & 0 \\ -1 & -1 \end{smallmatrix}\right)_e = 0 \text{ R}$$

Face relations coming from Figure 4.1(b):

$$\begin{tikzcd}[arrows=-] & \infty \arrow[dl] \arrow[dr] & \\ C_{1} \arrow[rr] & & C_{10}\end{tikzcd} \qquad \left(\begin{smallmatrix} -\omega+2 & -\omega-3 \\ -\omega-1 & \omega-4 \end{smallmatrix}\right)_c + \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_d - \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_a = 0$$

$$\begin{tikzcd}[arrows=-] & \infty \arrow[dl] \arrow[dr] & \\ C_{1} \arrow[rr] & & C_{19}\end{tikzcd} \qquad \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)_b + \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_g - \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_a = 0$$

$$\begin{tikzcd}[arrows=-] & \infty \arrow[dl] \arrow[dr] & \\ C_{10} \arrow[rr] & & C_{19}\end{tikzcd} \qquad \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)_e + \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_g - \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_d = 0$$

$$\begin{tikzcd}[arrows=-] & C_{19} \arrow[dl] \arrow[dr] & \\ C_{1} \arrow[rr] & & C_{10}\end{tikzcd} \qquad \left(\begin{smallmatrix} -\omega+2 & -\omega-3 \\ -\omega-1 & \omega-4 \end{smallmatrix}\right)_c + \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)_e - \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)_b = 0 \text{ R}$$

Face relations coming from Figure 4.1(c):

$$\begin{array}{ccc} & \infty & \\ \diagup & & \diagdown \\ C_1 & \text{---} & C_2 \end{array} \qquad \left(\begin{smallmatrix} -\omega+3 & \omega+2 \\ -\omega-2 & -\omega+3 \end{smallmatrix}\right)_g + \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_b - \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_a = 0$$

$$\begin{array}{ccc} & \infty & \\ \diagup & & \diagdown \\ C_1 & \text{---} & C_{19} \end{array} \qquad \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)_b + \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_g - \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_a = 0 \text{ R}$$

$$\begin{array}{ccc} & \infty & \\ \diagup & & \diagdown \\ C_2 & \text{---} & C_{19} \end{array} \qquad \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)_a + \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_g - \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_b = 0$$

$$\begin{array}{ccc} & C_{19} & \\ \diagup & & \diagdown \\ C_1 & \text{---} & C_2 \end{array} \qquad \left(\begin{smallmatrix} -\omega+3 & \omega+2 \\ -\omega-2 & -\omega+3 \end{smallmatrix}\right)_g + \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)_a - \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)_b = 0 \text{ R}$$

Face relations coming from Figure 4.1(d):

$$\begin{array}{ccc} & \infty & \\ \diagup & & \diagdown \\ C_2 & \text{---} & C_{13} \end{array} \qquad \left(\begin{smallmatrix} -\omega-1 & \omega-4 \\ \omega-2 & \omega+3 \end{smallmatrix}\right)_c + \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_e - \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_b = 0$$

$$\begin{array}{ccc} & \infty & \\ \diagup & & \diagdown \\ C_2 & \text{---} & C_{15} \end{array} \qquad -\left(\begin{smallmatrix} -\omega+3 & -2\omega-1 \\ -\omega-2 & \omega-5 \end{smallmatrix}\right)_h + \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_h - \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_b = 0$$

$$\begin{array}{ccc} & \infty & \\ \diagup & & \diagdown \\ C_{13} & \text{---} & C_{15} \end{array} \qquad -\left(\begin{smallmatrix} \omega+1 & 3 \\ -\omega+2 & -\omega-1 \end{smallmatrix}\right)_h + \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_h - \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_e = 0$$

$$\begin{array}{ccc} & C_{15} & \\ \diagup & & \diagdown \\ C_2 & \text{---} & C_{13} \end{array} \qquad \left(\begin{smallmatrix} -\omega-1 & \omega-4 \\ \omega-2 & \omega+3 \end{smallmatrix}\right)_c - \left(\begin{smallmatrix} \omega+1 & 3 \\ -\omega+2 & -\omega-1 \end{smallmatrix}\right)_h + \left(\begin{smallmatrix} -\omega+3 & -2\omega-1 \\ -\omega-2 & \omega-5 \end{smallmatrix}\right)_h = 0 \text{ R}$$

Face relations coming from Figure 4.1(e):

$$\begin{tikzcd}[column sep=small] & \infty \arrow[dl, dash] \arrow[dr, dash] & \\ C_1 \arrow[rr, dash] & & C_{10} \end{tikzcd} \qquad \begin{pmatrix} -\omega+2 & -\omega-3 \\ -\omega-1 & \omega-4 \end{pmatrix}_c + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_d - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_a = 0 \text{ R}$$

$$\begin{tikzcd}[column sep=small] & \infty \arrow[dl, dash] \arrow[dr, dash] & \\ C_1 \arrow[rr, dash] & & C_{16} \end{tikzcd} \qquad -\begin{pmatrix} \omega+2 & -\omega+3 \\ -\omega+3 & -\omega-2 \end{pmatrix}_i + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_i - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_a = 0$$

$$\begin{tikzcd}[column sep=small] & \infty \arrow[dl, dash] \arrow[dr, dash] & \\ C_{10} \arrow[rr, dash] & & C_{16} \end{tikzcd} \qquad -\begin{pmatrix} -\omega+2 & -\omega-3 \\ -\omega-1 & \omega-4 \end{pmatrix}_i + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_i - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_d = 0$$

$$\begin{tikzcd}[column sep=small] & C_{16} \arrow[dl, dash] \arrow[dr, dash] & \\ C_1 \arrow[rr, dash] & & C_{10} \end{tikzcd} \qquad \begin{pmatrix} -\omega+2 & -\omega-3 \\ -\omega-1 & \omega-4 \end{pmatrix}_c - \begin{pmatrix} -\omega+2 & -\omega-3 \\ -\omega-1 & \omega-4 \end{pmatrix}_i + \begin{pmatrix} \omega+2 & -\omega+3 \\ -\omega+3 & -\omega-2 \end{pmatrix}_i = 0 \text{ R}$$

So there are at most 13 independent face relations. There may be more redundancy coming from the orbits of the unoriented faces under Γ.

4.2 $\mathbb{Q}(\sqrt{-31})$

4.2.1 Generators

In the case being considered, the edges of the tessellation of $\mathcal{H}_3^*$ fall into 14 orbits. Taking $C_1, \ldots, C_{24}$ as defined in section 3.2.2, and letting $C_{25} = \frac{\omega-1}{2}$, $C_{26} = \frac{\omega}{2}$, these can be written as:

$$\begin{array}{rclcrcl}
(\gamma)_a & = & \gamma\{C_4, \infty\} & & (\gamma)_b & = & \gamma\{C_5, \infty\} \\
(\gamma)_c & = & \gamma\{C_8, \infty\} & & (\gamma)_d & = & \gamma\{C_9, \infty\} \\
(\gamma)_e & = & \gamma\{C_{13}, \infty\} & & (\gamma)_f & = & \gamma\{C_{14}, \infty\} \\
(\gamma)_g & = & \gamma\{C_{15}, \infty\} & & (\gamma)_h & = & \gamma\{C_{16}, \infty\} \\
(\gamma)_i & = & \gamma\{C_{18}, \infty\} & & (\gamma)_j & = & \gamma\{C_{19}, \infty\} \\
(\gamma)_k & = & \gamma\{C_{20}, \infty\} & & (\gamma)_l & = & \gamma\{C_{23}, \infty\} \\
(\gamma)_m & = & \gamma\{C_{25}, \infty\} & & (\gamma)_n & = & \gamma\{C_{26}, \infty\}
\end{array}$$

where $\gamma \in \Gamma$.

4.2.2 Edge relations

$$\begin{aligned}
\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)_a &= -\left(\begin{smallmatrix}2\omega+1&8\\-\omega+4&-2\omega-1\end{smallmatrix}\right)_a \\
\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)_b &= -\left(\begin{smallmatrix}2\omega-3&8\\\omega+3&-2\omega+3\end{smallmatrix}\right)_b \\
\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)_c &= -\left(\begin{smallmatrix}-3&\omega-2\\\omega+1&3\end{smallmatrix}\right)_c \\
\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)_d &= -\left(\begin{smallmatrix}-3&\omega+1\\\omega-2&3\end{smallmatrix}\right)_d \\
\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)_e &= -\left(\begin{smallmatrix}3&-\omega+1\\-\omega&-3\end{smallmatrix}\right)_e \\
\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)_f &= -\left(\begin{smallmatrix}-3&\omega\\\omega-1&3\end{smallmatrix}\right)_f \\
\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)_g &= -\left(\begin{smallmatrix}2\omega-3&2\omega+6\\4&-2\omega+3\end{smallmatrix}\right)_g \\
&= -\left(\begin{smallmatrix}2\omega-3&\omega+7\\4&-2\omega+1\end{smallmatrix}\right)_h \\
\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)_h &= -\left(\begin{smallmatrix}2\omega-1&8\\4&-2\omega+1\end{smallmatrix}\right)_h \\
\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)_i &= -\left(\begin{smallmatrix}\omega-2&\omega+1\\3&-\omega+2\end{smallmatrix}\right)_i \\
\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)_k &= -\left(\begin{smallmatrix}\omega&3\\3&-\omega+1\end{smallmatrix}\right)_j \\
\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)_l &= -\left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right)_l \\
&= -\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)_h \\
&= \left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)_h \\
\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)_m &= \left(\begin{smallmatrix}-1&\omega-1\\0&1\end{smallmatrix}\right)_m \\
\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)_n &= \left(\begin{smallmatrix}-1&\omega\\0&1\end{smallmatrix}\right)_n
\end{aligned}$$

4.2.3 Face relations

There are six distinct Γ-orbits of polyhedra in the tessellation of $\mathcal{H}_3^*$. We need only consider the face relations coming from one polyhedron from each orbit. The figure below shows the choice of representatives that was taken.

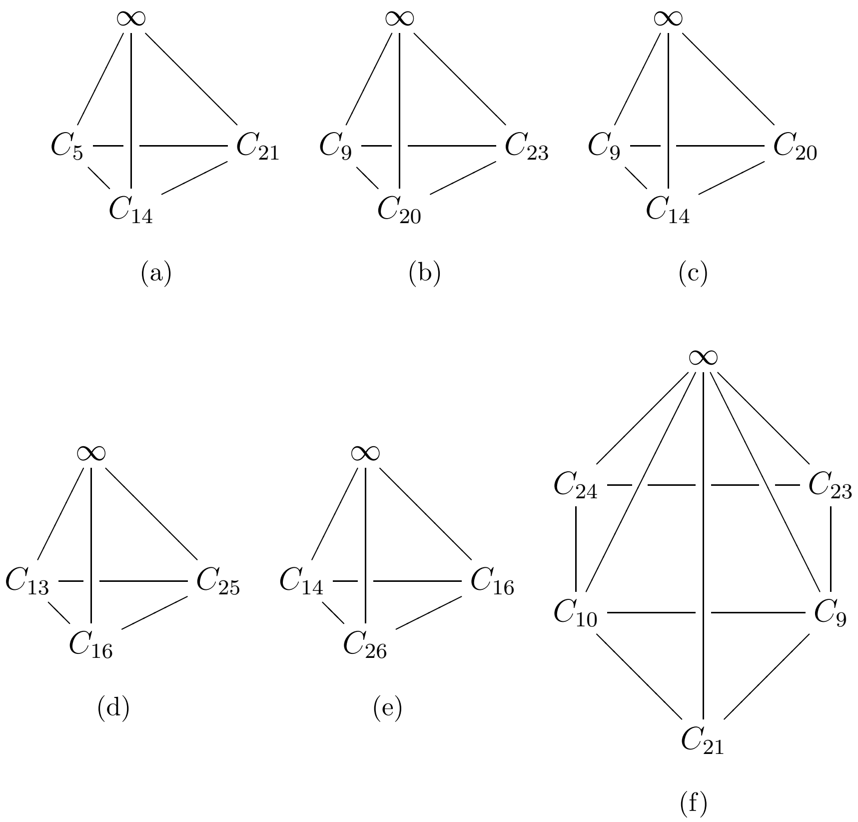
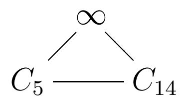
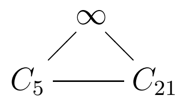


Figure 4.2: Representative polyhedra from the five orbits

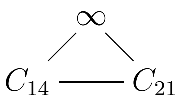
Face relations coming from Figure 4.2(a):



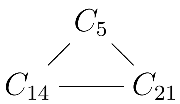
$$\begin{pmatrix} -3 & \omega \\ \omega-1 & 3 \end{pmatrix}_h + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_f - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_b = 0$$



$$\begin{pmatrix} \omega+1 & 3 \\ 3 & -\omega+2 \end{pmatrix}_a + \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}_i - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_b = 0$$



$$\begin{pmatrix} \omega+1 & 3 \\ 3 & -\omega+2 \end{pmatrix}_e + \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}_i - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_f = 0$$



$$\begin{pmatrix} \omega+1 & 3 \\ 3 & -\omega+2 \end{pmatrix}_e + \begin{pmatrix} 2\omega-3 & 2\omega+5 \\ \omega+3 & -\omega+6 \end{pmatrix}_a + \begin{pmatrix} -3 & \omega \\ \omega-1 & 3 \end{pmatrix}_h = 0 \text{ R}$$

Face relations coming from Figure 4.2(b):

$$\begin{tikzcd}[column sep=small] & \infty \arrow[dl, dash] \arrow[dr, dash] & \\ C_9 \arrow[rr, dash] & & C_{20} \end{tikzcd} \qquad \left(\begin{smallmatrix} \omega & 3 \\ 3 & -\omega+1 \end{smallmatrix}\right)_f + \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_k - \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_d = 0$$

$$\begin{tikzcd}[column sep=small] & \infty \arrow[dl, dash] \arrow[dr, dash] & \\ C_9 \arrow[rr, dash] & & C_{23} \end{tikzcd} \qquad \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)_i + \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_l - \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_d = 0$$

$$\begin{tikzcd}[column sep=small] & \infty \arrow[dl, dash] \arrow[dr, dash] & \\ C_{20} \arrow[rr, dash] & & C_{23} \end{tikzcd} \qquad \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)_e + \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_l - \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_k = 0$$

$$\begin{tikzcd}[column sep=small] & C_9 \arrow[dl, dash] \arrow[dr, dash] & \\ C_{20} \arrow[rr, dash] & & C_{23} \end{tikzcd} \qquad \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)_e - \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)_i + \left(\begin{smallmatrix} \omega & 3 \\ 3 & -\omega+1 \end{smallmatrix}\right)_f = 0 \text{ R}$$

Face relations coming from Figure 4.2(c):

$$\begin{tikzcd}[column sep=small] & \infty \arrow[dl, dash] \arrow[dr, dash] & \\ C_9 \arrow[rr, dash] & & C_{14} \end{tikzcd} \qquad \left(\begin{smallmatrix} -3 & \omega \\ \omega-1 & 3 \end{smallmatrix}\right)_j + \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_f - \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_d = 0$$

$$\begin{tikzcd}[column sep=small] & \infty \arrow[dl, dash] \arrow[dr, dash] & \\ C_9 \arrow[rr, dash] & & C_{20} \end{tikzcd} \qquad \left(\begin{smallmatrix} \omega & 3 \\ 3 & -\omega+1 \end{smallmatrix}\right)_f + \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_k - \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_d = 0 \text{ R}$$

$$\begin{tikzcd}[column sep=small] & \infty \arrow[dl, dash] \arrow[dr, dash] & \\ C_{14} \arrow[rr, dash] & & C_{20} \end{tikzcd} \qquad \left(\begin{smallmatrix} \omega & 3 \\ 3 & -\omega+1 \end{smallmatrix}\right)_l + \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_k - \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_f = 0$$

$$\begin{tikzcd}[column sep=small] & C_9 \arrow[dl, dash] \arrow[dr, dash] & \\ C_{14} \arrow[rr, dash] & & C_{20} \end{tikzcd} \qquad \left(\begin{smallmatrix} \omega & 3 \\ 3 & -\omega+1 \end{smallmatrix}\right)_l - \left(\begin{smallmatrix} \omega & 3 \\ 3 & -\omega+1 \end{smallmatrix}\right)_f + \left(\begin{smallmatrix} -3 & \omega \\ \omega-1 & 3 \end{smallmatrix}\right)_j = 0 \text{ R}$$

Face relations coming from Figure 4.2(d):

$$\begin{array}{ccc} & \infty & \\ / & & \backslash \\ C_{13} & \text{---} & C_{16} \end{array} \qquad \left(\begin{smallmatrix} 2\omega-1 & \omega+7 \\ 4 & -2\omega+3 \end{smallmatrix}\right)_a + \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_h - \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_e = 0$$

$$\begin{array}{ccc} & \infty & \\ / & & \backslash \\ C_{13} & \text{---} & C_{25} \end{array} \qquad -\left(\begin{smallmatrix} -3 & \omega-1 \\ \omega & 3 \end{smallmatrix}\right)_m + \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_m - \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_e = 0$$

$$\begin{array}{ccc} & \infty & \\ / & & \backslash \\ C_{16} & \text{---} & C_{25} \end{array} \qquad -\left(\begin{smallmatrix} 2\omega-1 & \omega+7 \\ 4 & -2\omega+3 \end{smallmatrix}\right)_m + \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_m - \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_h = 0$$

$$\begin{array}{ccc} & C_{13} & \\ / & & \backslash \\ C_{16} & \text{---} & C_{25} \end{array} \qquad -\left(\begin{smallmatrix} 2\omega-1 & \omega+7 \\ 4 & -2\omega+3 \end{smallmatrix}\right)_m + \left(\begin{smallmatrix} -3 & \omega-1 \\ \omega & 3 \end{smallmatrix}\right)_m + \left(\begin{smallmatrix} 2\omega-1 & \omega+7 \\ 4 & -2\omega+3 \end{smallmatrix}\right)_a = 0 \text{ R}$$

Face relations coming from Figure 4.2(e):

$$\begin{array}{ccc} & \infty & \\ / & & \backslash \\ C_{14} & \text{---} & C_{16} \end{array} \qquad \left(\begin{smallmatrix} -2\omega+1 & \omega-8 \\ -4 & 2\omega+1 \end{smallmatrix}\right)_b + \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_h - \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_f = 0$$

$$\begin{array}{ccc} & \infty & \\ / & & \backslash \\ C_{14} & \text{---} & C_{26} \end{array} \qquad -\left(\begin{smallmatrix} -3 & \omega \\ \omega-1 & 3 \end{smallmatrix}\right)_n + \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_n - \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_f = 0$$

$$\begin{array}{ccc} & \infty & \\ / & & \backslash \\ C_{16} & \text{---} & C_{26} \end{array} \qquad -\left(\begin{smallmatrix} -2\omega+1 & \omega-8 \\ -4 & 2\omega+1 \end{smallmatrix}\right)_n + \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_n - \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)_h = 0$$

$$\begin{array}{ccc} & C_{14} & \\ / & & \backslash \\ C_{16} & \text{---} & C_{26} \end{array} \qquad -\left(\begin{smallmatrix} -2\omega+1 & \omega-8 \\ -4 & 2\omega+1 \end{smallmatrix}\right)_n + \left(\begin{smallmatrix} -3 & \omega \\ \omega-1 & 3 \end{smallmatrix}\right)_n + \left(\begin{smallmatrix} -2\omega+1 & \omega-8 \\ -4 & 2\omega+1 \end{smallmatrix}\right)_b = 0 \text{ R}$$

Face relations coming from Figure 4.2(f):

$$\begin{tikzcd}[column sep=small] & \infty \arrow[dl, dash] \arrow[dr, dash] & \\ C_9 \arrow[rr, dash] & & C_{10} \end{tikzcd} \qquad \begin{pmatrix} \omega-2 & 3 \\ \omega+1 & -\omega+2 \end{pmatrix}_l + \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}_c - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_d = 0$$

$$\begin{tikzcd}[column sep=small] & \infty \arrow[dl, dash] \arrow[dr, dash] & \\ C_9 \arrow[rr, dash] & & C_{21} \end{tikzcd} \qquad \begin{pmatrix} \omega+1 & 3 \\ 3 & -\omega+2 \end{pmatrix}_l + \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}_i - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_d = 0$$

$$\begin{tikzcd}[column sep=small] & \infty \arrow[dl, dash] \arrow[dr, dash] & \\ C_9 \arrow[rr, dash] & & C_{23} \end{tikzcd} \qquad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}_i + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_l - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_d = 0 \text{ R}$$

$$\begin{tikzcd}[column sep=small] & \infty \arrow[dl, dash] \arrow[dr, dash] & \\ C_{10} \arrow[rr, dash] & & C_{21} \end{tikzcd} \qquad \begin{pmatrix} -\omega-1 & \omega-2 \\ -3 & \omega+1 \end{pmatrix}_l + \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}_c + \begin{pmatrix} \omega-2 & \omega+1 \\ \omega+1 & 3 \end{pmatrix}_c = 0$$

$$\begin{tikzcd}[column sep=small] & \infty \arrow[dl, dash] \arrow[dr, dash] & \\ C_{10} \arrow[rr, dash] & & C_{24} \end{tikzcd} \qquad \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix}_i + \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}_l + \begin{pmatrix} \omega-2 & \omega+1 \\ \omega+1 & 3 \end{pmatrix}_c = 0$$

$$\begin{tikzcd}[column sep=small] & \infty \arrow[dl, dash] \arrow[dr, dash] & \\ C_{23} \arrow[rr, dash] & & C_{24} \end{tikzcd} \qquad \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix}_l + \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}_l - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_l = 0$$

$$\begin{tikzcd}[column sep=small] & C_{21} \arrow[dl, dash] \arrow[dr, dash] & \\ C_9 \arrow[rr, dash] & & C_{10} \end{tikzcd} \qquad \begin{pmatrix} \omega-2 & 3 \\ \omega+1 & -\omega+2 \end{pmatrix}_l + \begin{pmatrix} -\omega-1 & \omega-2 \\ -3 & \omega+1 \end{pmatrix}_l + \begin{pmatrix} -3 & \omega+1 \\ \omega-2 & 3 \end{pmatrix}_l = 0$$

$$\begin{tikzcd}[column sep=small] C_9 \arrow[r, dash] \arrow[d, dash] & C_{10} \arrow[d, dash] \\ C_{23} \arrow[r, dash] & C_{24} \end{tikzcd} \qquad \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix}_l + \begin{pmatrix} \omega-2 & \omega+1 \\ \omega+1 & 3 \end{pmatrix}_i + \begin{pmatrix} -3 & \omega-2 \\ \omega-2 & \omega+1 \end{pmatrix}_l + \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}_i = 0 \text{ R}$$

N.B. There are more relations than there are for $\mathbb{Q}(\sqrt{-2})$. Computations on the imaginary quadratic fields considered so far suggest that the number rises as d increases.

4.3 M-Symbols

Given a level $\mathfrak{n}$ we will need a convenient way of writing down the generators and relations for $\mathrm{H}_1(\Gamma_0(\mathfrak{n}) \setminus \mathcal{H}_3^*, \mathbb{Q})$. M-Symbols provide such a method and we explain them here.

The following result is well known.

Proposition 4.3.1. *The natural map*

$$\mathrm{SL}_2(\mathcal{O}) \longrightarrow \mathrm{SL}_2(\mathcal{O}/\mathfrak{n})$$

given by reducing each matrix entry modulo $\mathfrak{n}$ is surjective.

Lemma 4.3.2. *Let $c, d \in \mathcal{O}$ satisfy $\langle c, d\rangle + \mathfrak{n} = \mathcal{O}$. Then there exists $c', d' \in \mathcal{O}$, with $c' \equiv c \pmod{\mathfrak{n}}$ and $d' \equiv d \pmod{\mathfrak{n}}$ such that $\langle c', d'\rangle = \mathcal{O}$.*

Proof. Write $\alpha\mu - \beta\lambda \equiv 1 \pmod{\mathfrak{n}}$ for some $\alpha, \beta \in \mathcal{O}$, and lift $\left(\begin{smallmatrix}\alpha & \beta \\ \mu & \lambda\end{smallmatrix}\right)$ to $\mathrm{SL}_2(\mathcal{O})$ using Proposition 4.3.1. $\square$

On the set of ordered pairs $c, d \in \mathcal{O} \times \mathcal{O}$ such that $\langle c, d\rangle + \mathfrak{n} = \mathcal{O}$, we now define the relation $\sim$, where

$$(c_1, d_1) \sim (c_2, d_2) \iff c_1 d_2 \equiv c_2 d_1 \pmod{\mathfrak{n}}.$$

This is an equivalence relation, and we can identify the equivalence classes with the elements of $\mathbb{P}^1(\mathfrak{n})$, the projective line over $\mathcal{O}/\mathfrak{n}$. The equivalence class of (c, d) will be denoted $(c : d)$, and such symbols will be called **cd-symbols of level $\mathfrak{n}$**. Notice that the components c and d of a cd-symbol $(c : d)$ are only determined modulo $\mathfrak{n}$, and that by Lemma 4.3.2 we can always choose them such that $\langle c, d\rangle = \mathcal{O}$.

There is a natural map

$$\Gamma \longrightarrow \mathbb{P}^1(\mathfrak{n}), \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto (c : d).$$

By Lemma 4.3.2 this map is surjective.

Proposition 4.3.3. *Two elements of Γ have the same image in $\mathbb{P}^1(\mathfrak{n})$ if and only if they lie in the same right coset of $\Gamma_0(\mathfrak{n})$ in Γ.*

Proof. [5], Proposition 27, pg 29. □

Thus, we may obtain a set of right coset representatives for $\Gamma_0(\mathfrak{n})$ in Γ by lifting each cd-symbol arbitrarily to an element of $\mathrm{SL}_2(\mathcal{O})$.

In practice we can find all cd-symbols of level $\mathfrak{n}$ as follows. First factorise $\mathfrak{n}$ into prime powers

$$\mathfrak{n} = \mathfrak{p}_1^{n_1} \dots \mathfrak{p}_r^{n_r}$$

For each factor we have the symbols

$(x : 1)$ where x is reduced mod $\mathfrak{p}_i^{n_i}$
$(1 : y)$ where y is reduced mod $\mathfrak{p}_i^{n_i}$ and not invertible mod $\mathfrak{p}_i^{n_i}$

The symbols from each prime power factor can then be combined using the Chinese Remainder Theorem to form cd-symbols of level $\mathfrak{n}$.

An **M-symbol** is then defined to be a pair, $((c : d), e_i)$, consisting of a cd-symbol and a directed edge of the tessellation of $G \setminus \mathcal{H}_3^*$.

Having stored $V(\Gamma_0(\mathfrak{n}))$ as a space generated by M-symbols in the computers memory, we wish to compute Hecke eigenvalues. To do this, we convert M-symbols to modular symbols, a trivial step, and act on the modular symbols with the Hecke operators. The modular symbols obtained must then be converted back into a $\mathbb{Z}$-linear combination of M-symbols.

Conversion from M-symbols to modular symbols is simply via the map ξ, cf (4.1). To convert modular symbols to M-symbols we need to make use of the pseudo-Euclidean algorithm explained in section 3.3.

Since $\{\alpha, \beta\} = \{\infty, \beta\} - \{\infty, \alpha\}$, it suffices to consider the symbol $\{\infty, \beta\}$, where $\beta \in k$. We define a sequence of cusps β_i and matrices $B_i \in \Gamma$ as follows. Put $\beta_0 = \beta$ and $B_0 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. If after $i-1$ steps, β_{i-1} is not a singular point, choose $T_i \in E_\infty$ such that $T_i \cdot \beta_{i-1}$ lies in F_k, then choose $c(i) \in \{1, \dots, m\}$ such that $T_i \cdot \beta_{i-1}$ lies inside the circle $C_{\alpha_{c(i)}}$. Let $A_i = M_{\alpha_{c(i)}} T_i$ and define $\beta_i = A_i \cdot \beta_{i-1}$ and $B_i = B_{i-1} A_i^{-1}$. Now iterate until β_N is a singular point z for some N. Then $B_N \cdot z = \beta$. We have

$$B_i \cdot (M_{c(i)} \cdot \infty) = B_{i-1} T_i^{-1} M_{c(i)}^{-1} M_{c(i)} \cdot \infty = B_{i-1} \cdot \infty.$$

It follows that if $z = \infty$

$$\begin{aligned}
\{\infty, \beta\} &= \{B_0 \cdot \infty, B_N \cdot \infty\} \\
&= \sum_{i=1}^{N} \{B_{i-1} \cdot \infty, B_i \cdot \infty\} \\
&= \sum_{i=1}^{N} B_i \{M_{c(i)} \cdot \infty, \infty\}
\end{aligned}$$

Since we took care earlier to ensure that that each $M_i \cdot \infty$ is one of the basic inversion centres $\alpha_1, \ldots, \alpha_m$, this expression has the required form (provided our choice of basic edges was chosen to include the edges $\{\alpha_i, \infty\}$).

If $z \neq \infty$ then we just have

$$\begin{aligned}
\{\infty, \beta\} &= \{B_0 \cdot \infty, B_N \cdot \infty\} + \{B_N \cdot \infty, B_N \cdot z\} \\
&= \sum_{i=1}^{N} \{B_{i-1} \cdot \infty, B_i \cdot \infty\} + B_N \{\infty, z\} \\
&= \sum_{i=1}^{N} B_i \{M_{c(i)} \cdot \infty, \infty\} + B_N \{\infty, z\}
\end{aligned}$$

This has the required form provided our choice of basic edges also includes the edges from the singular points to infinity.

So at this point we now have an algorithm for calculating $\mathrm{H}_1(\Gamma_0(\mathfrak{n}) \setminus \mathcal{H}_3^*, \mathbb{Q})$. This allows us to deduce an upper bound on the number of rational newforms at a given level. Next we shall see how to define operators on this space which enable us to find an enumerate all newforms.

Chapter 5

Operators

5.1 Hecke operators

We now consider the action of certain operators on the space of cusp forms $\hat{S}(\mathfrak{n})$ and on the homology space $V(\Gamma_0(\mathfrak{n}))$. Hecke operators play a key role in the study of modular forms over $\mathbb{Q}$ and here we need to develop a practical theory of Hecke operators for prime ideals in $\mathcal{O}$. The presence of non-principal prime ideals means that the theory cannot be carried over directly. We make use of an indirect approach to defining the action of Hecke operators, as it simplifies their definition.

5.1.1 Modular points and Hecke theory

It is well known that classical modular forms for $\mathrm{SL}_2(\mathbb{Z})$ correspond to certain functions on $\mathbb{Z}$-lattices in $\mathbb{C}$. This idea extends to forms for $\Gamma_0(N)$; such forms correspond to functions on "modular points" defined over $\mathbb{Z}$, which are $\mathbb{Z}$-lattices in $\mathbb{C}$ equipped with some extra structure. Modular points may be used to introduce Hecke operators; the theory is described in [14].

We use this approach to define Hecke operators for modular forms over k. The details of the theory can be found in Chapter 7 of [5]. A modular point for $\Gamma_0(\mathfrak{n})$ is a pair (Λ, S) where Λ is a lattice in $\mathbb{C}^2$ and $S \subset \mathbb{C}^2/\Lambda$ is a cyclic $\mathcal{O}$-module isomorphic to $\mathcal{O}/\mathfrak{n}$. Let $\mathcal{M}(\mathfrak{n})$ denote the set of modular points for $\Gamma_0(\mathfrak{n})$ and $\mathbb{Z}\mathcal{M}(\mathfrak{n})$ the free abelian group generated by $\mathcal{M}(\mathfrak{n})$.

For each integral ideal $\mathfrak{a}$ of $\mathcal{O}$, define a $\mathbb{Z}$-linear map

$$T_{\mathfrak{a}} : \mathbb{Z}\mathcal{M}(\mathfrak{n}) \to \mathbb{Z}\mathcal{M}(\mathfrak{n}),$$

by

$$T_{\mathfrak{a}}(\Lambda, S) = \sum_{\substack{[\Lambda:\Lambda']=\mathfrak{a} \\ (\Lambda',S')\in\mathcal{M}(\mathfrak{n})}} (\Lambda', S').$$

Also for each integral ideal $\mathfrak{a} \nmid \mathfrak{n}$ of $\mathcal{O}$, define an endomorphism

$$T_{\mathfrak{a},\mathfrak{a}} : \mathbb{Z}\mathcal{M}(\mathfrak{n}) \to \mathbb{Z}\mathcal{M}(\mathfrak{n}),$$

by

$$T_{\mathfrak{a},\mathfrak{a}}(\Lambda, S) = (\mathfrak{a}\Lambda, S').$$

Bygott proves in [5] that these operators take modular points to modular points, i.e. that such S' exist.

Using simple lattice arguments the following identities can be proved:

$$\begin{array}{rcll} T_{\mathfrak{a}}T_{\mathfrak{b}} & = & T_{\mathfrak{a}\mathfrak{b}} & \text{if } \mathfrak{a}+\mathfrak{b}=\mathcal{O}, \\ T_{\mathfrak{p}^r}T_{\mathfrak{p}} & = & T_{\mathfrak{p}^{r+1}} + N(\mathfrak{p})T_{\mathfrak{p}^{r-1}}T_{\mathfrak{p},\mathfrak{p}} & \mathfrak{p}\nmid\mathfrak{n}, \\ T_{\mathfrak{p}^r} & = & (T_{\mathfrak{p}})^r & \mathfrak{p}\mid\mathfrak{n}. \end{array}$$

Now let $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ be integral ideals of $\mathcal{O}$ representing the h ideal classes; as usual, we take $\mathfrak{a}_1 = \mathcal{O}$ to represent the principal class. By structure theory, see Chapter 1, every lattice $\Lambda \subset \mathbb{C}^2$ is isomorphic to $\mathfrak{a}_i \oplus \mathcal{O}$ for some i, called the **class** of Λ. Hence Λ has the form $\mathfrak{a}_i\omega_1 \oplus \mathcal{O}\omega_2$ for vectors $\omega_1, \omega_2 \in \mathbb{C}^2$ which are linearly independent over $\mathbb{C}$. We may regard the row vectors ω_1, ω_2 as the rows of a matrix

$$\omega = \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C})$$

and define

$$\Lambda_\omega^{(i)} = \mathfrak{a}_i\omega_1 \oplus \mathcal{O}\omega_2$$

The set of modular points of class i for $\Gamma_0(\mathfrak{n})$ is denoted $\mathcal{M}_i(\mathfrak{n})$. Thus there is a disjoint union

$$\mathcal{M}(\mathfrak{n}) = \bigcup_{i=1}^{h} \mathcal{M}_i(\mathfrak{n})$$

It is possible to construct maps $\theta_i : \mathrm{GL}_2(\mathbb{C}) \to \mathcal{M}_i(\mathfrak{n})$ taking a matrix to a modular point with lattice equal to $\Lambda_\omega^{(i)}$, see [5], Lemma 116, pg 181.

Recall the definition of $\mathcal{S}_2$ given in chapter 2:

$$\mathcal{S}_2 \quad = \quad \left\{\phi : G_\infty \to \mathbb{C}^3 : \phi(\zeta g \kappa) = \phi(g)\rho(\zeta\kappa) \;\forall\, \zeta \in Z_\infty, g \in G_\infty, \kappa \in K_\infty\right\},$$

where $G_\infty = \mathrm{GL}_2(\mathcal{O})$, with centre Z_∞ and subgroup $K_\infty = U_2(\mathbb{C})$, and $\rho : Z_\infty K_\infty \to \mathbb{C}^3$ is a representation.

Definition 5.1.1. *A function $F : \mathcal{M}(\mathfrak{n}) \to \mathbb{C}^3$ is of* ***weight*** *ρ if*

$$F(\zeta P \kappa) = F(P)\rho(\zeta\kappa) \quad \forall\, P \in \mathcal{M}(\mathfrak{n}), \zeta \in \mathbb{C}^\times, \kappa \in K_\infty$$

Now modular forms correspond to certain weight-ρ functions on modular points. We define

$$\mathcal{S}_3 = \left\{\phi \in \mathcal{S}_2 \mid \phi|\gamma = \phi \text{ for all } \gamma \in \widetilde{\Omega}_0(\mathfrak{n})\right\},$$

$$\mathcal{S}_4 = \left\{F : \mathcal{M}(\mathfrak{n}) \to \mathbb{C}^3 \mid F \text{ is of weight } \rho\right\}.$$

Bygott proves the following, where $\mathcal{S}_3^h$ simply denotes h copies of $\mathcal{S}_3$.

Proposition 5.1.2. *There exist inverse bijections $\sharp : \mathcal{S}_3^h \to \mathcal{S}_4$ and $\flat : \mathcal{S}_4 \to \mathcal{S}_3^h$.*

Proof. Follows from [5], Proposition 120, pg 186. □

So given a modular form Φ, we can define the action of Hecke operators on it by defining

$$\Phi \mid T_{\mathfrak{a}} = (\Phi^\sharp \mid T_{\mathfrak{a}})^\flat, \qquad \Phi \mid T_{\mathfrak{a},\mathfrak{a}} = (\Phi^\sharp \mid T_{\mathfrak{a},\mathfrak{a}})^\flat.$$

5.1.2 Practical definition

No element of $\mathrm{GL}_2(\mathcal{O})$ can ever capture the action of a Hecke operator simultaneously on all of the components of a modular form, so we need to look at the action on individual components.

We have

$$\begin{aligned} T_{\mathfrak{p}} &: \mathcal{M}_i \to \mathcal{M}_j && \text{where } j \text{ is such that } \mathrm{cl}(\mathfrak{a}_j) = \mathrm{cl}(\mathfrak{p}\mathfrak{a}_i) \\ T_{\mathfrak{p},\mathfrak{p}} &: \mathcal{M}_i \to \mathcal{M}_j && \text{where } j \text{ is such that } \mathrm{cl}(\mathfrak{a}_j) = \mathrm{cl}(\mathfrak{p}^2\mathfrak{a}_i) \end{aligned}$$

We call operators which preserve the class of modular points as **principal**. Now

$$(\Phi \mid T_{\mathfrak{a}})^{(i)} = \sum_{M} \phi^{(j)} \mid M,$$

where M runs through the finite set of matrices for which $\Lambda^{(j)}_{M\omega}$ contains $\Lambda^{(i)}_{\omega}$ with index $\mathfrak{a}$.

If $\mathfrak{p}$ is principal then $i = j$ and the situation is directly analogous to the classical case. If $\mathfrak{p}$ is non-principal though we cannot find such matrices M. However when h is odd it is still possible to determine the action of $T_{\mathfrak{p}}$ when $\mathfrak{p}$ is non-principal.

What we must do is consider a product of operators $T_{\mathfrak{q},\mathfrak{q}}T_{\mathfrak{p}}$, where $\mathfrak{p}\mathfrak{q}^2$ is principal. This product preserves the class of the component, so it's restriction to the principal component of a modular form is well defined.

We now explain how these principal operators can be realised explicitly in terms of matrices over $\mathcal{O}$, allowing us to determine their action using modular symbol calculations. For simplicity we just define their action on lattices, rather than full modular points. At the end of this section we will explain the extra condition that the group S places on $T_{\mathfrak{p}}$. We can define for $\mathfrak{p}$ principal

$$\begin{aligned} T_{\mathfrak{p},1}(\Lambda) &:= T_{\mathfrak{p}}(\Lambda) \\ &= \sum_{[\Lambda:\Lambda']=\mathfrak{p}} (\Lambda') \end{aligned}$$

and otherwise

$$\begin{aligned} T_{\mathfrak{q}\mathfrak{p},\mathfrak{q}}(\Lambda) &:= T_{\mathfrak{q},\mathfrak{q}}T_{\mathfrak{p}}(\Lambda) \\ &= \sum_{[\mathfrak{q}\Lambda:\Lambda']=\mathfrak{p}} (\Lambda') \end{aligned}$$

Using the results from chapter 1, we can write these as

$$T_{\mathfrak{p}} = \sum_{V \in \Gamma/\Gamma_0(\mathfrak{p})} M_{\mathfrak{p},1} V$$

and

$$T_{\mathfrak{qp},\mathfrak{q}} = \sum_{V\in\Gamma/\Gamma_0(\mathfrak{p})} M_{\mathfrak{qp},\mathfrak{q}}V.$$

To define the Hecke operator for a composite ideal $\mathfrak{m}$, we just take

$$T_{\mathfrak{m}} = \sum_{\substack{\mathfrak{a}|\mathfrak{b}\\ \mathfrak{ab}=\mathfrak{m}}} \sum_{V\in\Gamma/\Gamma_0(\mathfrak{ab}^{-1})} M_{\mathfrak{a},\mathfrak{b}}V.$$

Let $\mathbb{T}$ be the algebra over $\mathbb{C}$, of all Hecke operators associated to ideals in $\mathcal{O}$. It follows from the relations listed earlier that $\mathbb{T}$ is generated by $T_{\mathfrak{p}}$, with $\mathfrak{p}$ prime.

In order for the action of the Hecke matrices to be well defined on modular points and not just lattices their lower left entry must lie in the level $\mathfrak{n}$. By Lemma 1.2.5 we can choose $M_{\mathfrak{a},\mathfrak{b}}$ so that its lower left entry lies in the level. Given a cd-symbol of level coprime to $\mathfrak{n}$, we can always use the Chinese Remainder Theorem to find an equivalent symbol with $c \in \mathfrak{n}, d \notin \mathfrak{n}$. Hence we can also choose V so that its lower left entry lies in $\mathfrak{n}$. Then the lower left entry of their product will also lie in the level.

5.2 Complex conjugation

Let $\gamma \in \mathrm{GL}_2(\mathbb{C})$ and $(z,t) \in \mathcal{H}_3$, so $\gamma \cdot (z,t) = (z',t')$ as given by (1.12). Writing $\bar\gamma$ for the complex conjugate of γ, we see at once that $\bar\gamma \cdot (\bar z, t) = (\bar{z'}, t')$. It follows that the conjugation action $(z,t) \mapsto (\bar z, t)$ on $\mathcal{H}_3$ induces a homeomorphism

$$c : \Gamma_0(\mathfrak{n}) \setminus \mathcal{H}_3 \to \Gamma_0(\bar{\mathfrak{n}}) \setminus \mathcal{H}_3.$$

By functoriality, there is an induced $\mathbb{Q}$-linear isomorphism

$$c : H_1(\Gamma_0(\mathfrak{n}) \setminus \mathcal{H}_3, \mathbb{Q}) \to H_1(\Gamma_0(\bar{\mathfrak{n}}) \setminus \mathcal{H}_3, \mathbb{Q}).$$

of homology. This map is simply given in terms of modular symbols by

$$\{\alpha, \beta\} \mapsto \{\bar\alpha, \bar\beta\}.$$

The conjugation map is useful because it behaves well with respect to the Hecke operators, in the following sense. Write $T_{\mathfrak{p}}^{\mathfrak{n}}$ for the Hecke operator $T_{\mathfrak{p}}$ at level $\mathfrak{n}$, and $\overline{T_{\mathfrak{p}}^{\mathfrak{n}}}$ for its "conjugate", i.e for the formal linear combination of matrices obtained by conjugating each matrix, $M_{\mathfrak{a},\mathfrak{b}}W$, in $T_{\mathfrak{p}}^{\mathfrak{n}}$. Formally we have $\overline{T_{\mathfrak{p}}^{\mathfrak{n}}} = T_{\bar{\mathfrak{p}}}^{\bar{\mathfrak{n}}}$. Indeed it is clear that $\overline{M_{\mathfrak{a},\mathfrak{b}}}$ is equivalent to $M_{\bar{\mathfrak{a}},\bar{\mathfrak{b}}}$ modulo $\Gamma_0(\overline{\mathfrak{a}\mathfrak{b}^{-1}})$. Now since complex conjugation turns a list of residues modulo $\mathfrak{p}$ into one modulo $\bar{\mathfrak{p}}$ and turns a congruence condition modulo $\mathfrak{p}$ into one modulo $\bar{\mathfrak{p}}$, W is also transformed in the correct way.

Thus, if $v \in H_1(\Gamma_0(\mathfrak{n}) \setminus \mathcal{H}_3, \mathbb{Q})$ is an eigenvector with $T_{\mathfrak{p}}^{\mathfrak{n}}v = \lambda v$, then

$$T_{\bar{\mathfrak{p}}}^{\bar{\mathfrak{n}}}c(v) = c(T_{\mathfrak{p}}^{\mathfrak{n}}v) = \lambda c(v).$$

Thus, to every eigenspace in $H_1(\Gamma_0(\mathfrak{n}) \setminus \mathcal{H}_3, \mathbb{Q})$ there corresponds one in $H_1(\Gamma_0(\bar{\mathfrak{n}}) \setminus \mathcal{H}_3, \mathbb{Q})$ with the eigenvalues for $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ interchanged. By duality, to every modular form f at level $\mathfrak{n}$ there corresponds a form at level $\bar{\mathfrak{n}}$ with the eigenvalues for $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ interchanged; we denote this "conjugate" form by $\bar{f}$.

We now introduce another class of operators on the space of cusp forms which tell us information at the bad primes.

5.3 Atkin-Lehner and Fricke involutions

Now although it is possible to define Hecke operators for $\mathfrak{p} \mid \mathfrak{n}$, the same information can be obtained using much simpler operators known as Atkin-Lehner or W-involutions. The action of these operators is simpler to calculate because they can be expressed in terms of a single matrix.

Classically for $q^\alpha || N$ we have the Atkin-Lehner involutions

$$W_q := \begin{pmatrix} q^\alpha x & y \\ Nz & q^\alpha w \end{pmatrix}$$

where $q^\alpha xw - \frac{N}{q^\alpha}yz = 1$.

The Fricke involution at level N is given by

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

These operators satisfy various properties. They normalise $\Gamma_0(N)$, and their squares, mod scalars, lie in $\Gamma_0(N)$. This is equivalent to the fact that their action is well defined on $\Gamma_0(N)\backslash\mathcal{H}_2$ and they are involutions. They also form an abelian 2-group and commute with the Hecke operators T_p for $p \nmid N$.

We can use the fact that the class number is odd to generalise the definition of these operators to any ideal $\mathfrak{m}$ in $\mathcal{O}$ dividing $\mathfrak{n}$, such that $\mathfrak{m}$ and $\frac{\mathfrak{n}}{\mathfrak{m}}$ are coprime. If $h = 2n+1$ then take

$$W_{\mathfrak{m}} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \tag{5.1}$$

where $x \in \mathfrak{m}^{n+1}, y \in \mathfrak{m}^n, z \in \mathfrak{n}\mathfrak{m}^n, w \in \mathfrak{m}^{n+1}$ and $\langle xw - yz\rangle = \mathfrak{m}^{2n+1}$.

Lemma 5.3.1. *For any ideal $\mathfrak{m}$ dividing $\mathfrak{n}$, such that $\mathfrak{m}$ and $\frac{\mathfrak{n}}{\mathfrak{m}}$ are coprime we can find a matrix of the form (5.1).*

Proof. First we choose $z \in \mathcal{O}$ such that

$$\mathrm{ord}_{\mathfrak{p}}(z) = \begin{cases} \mathrm{ord}_{\mathfrak{p}}(\mathfrak{m}^{n+1}) & \forall\ \mathfrak{p}|\mathfrak{m} \\ \mathrm{ord}_{\mathfrak{p}}(\mathfrak{n}) & \forall\ \mathfrak{p}|\frac{\mathfrak{n}}{\mathfrak{m}} \end{cases}$$

Then we choose $x \in \mathcal{O}$ such that

$$\begin{aligned} \mathrm{ord}_{\mathfrak{p}}(x) &= 0\ \ \forall\ \mathfrak{p}|z, \mathfrak{p} \nmid \mathfrak{m} \\ &\geq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{m}^{n+1})\ \ \forall\ \mathfrak{p}|\mathfrak{m} \end{aligned}$$

Then $\langle x, z\rangle = \langle x\mu, z\rangle = \mathfrak{m}^{n+1}$ where $\mathfrak{m}^{2n+1} = \langle \mu \rangle$. Now

$$\begin{aligned} \langle \mu \rangle &= \mathfrak{m}^{n+1}\mathfrak{m}^n \\ &= \langle x\mu, z\rangle \mathfrak{m}^n \\ &= x\mu\mathfrak{m}^n + z\mathfrak{m}^n \end{aligned}$$

so we can solve $\mu = x\mu w - zy$ with $y, w \in \mathfrak{m}^n$. Then the matrix

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

satisfies all the required properties. $\square$

In particular if we take $\mathfrak{m} = \mathcal{O}$ we get an element of $\Gamma_0(\mathfrak{n})$ and if we take $\mathfrak{m} = \mathfrak{n}$ we get the analogue of the classical Fricke involution.

Lemma 5.3.2. *$W_\mathfrak{m}$ is an involution, (i.e. $W_\mathfrak{m}^2$ (modulo scalars) lies in $\Gamma_0(\mathfrak{n})$), normalises $\Gamma_0(\mathfrak{n})$ and is independent of the particular choice of x, y, z, w.*

Proof.

$$W_\mathfrak{m}^2 = \begin{pmatrix} x' & y' \\ z' & w' \end{pmatrix}$$

where

$$\begin{aligned} x' &\in \mathfrak{m}^{2n+2} + \mathfrak{n}\mathfrak{m}^{2n} \\ y' &\in \mathfrak{m}^{2n+1} \\ z' &\in \mathfrak{n}\mathfrak{m}^{2n+1} \\ w' &\in \mathfrak{m}^{2n+2} + \mathfrak{n}\mathfrak{m}^{2n} \end{aligned}$$

and has determinant generating $\mathfrak{m}^{2(2n+1)}$. Each entry is divisible by the generator, μ, of $\mathfrak{m}^{2n+1}$ and so we can factor out a scalar matrix $\left(\begin{smallmatrix} \mu & 0 \\ 0 & \mu \end{smallmatrix}\right)$. It is easy to see that the remaining factor is an element of $\Gamma_0(\mathfrak{n})$. Hence $W_\mathfrak{m}^2$ acts trivially on $\Gamma_0(\mathfrak{n})\backslash\mathcal{H}_3$. Thus $W_\mathfrak{m}$ is an involution.

The adjoint of $W_\mathfrak{m}$ satisfies the same properties as the original matrix. Hence the same argument as above shows that $W_\mathfrak{m}^{-1}W'_\mathfrak{m} \in \Gamma_0(\mathfrak{n})$. So any two choices of matrix have the same action.

To see that $W_\mathfrak{m}$ normalises $\Gamma_0(\mathfrak{n})$ we need to prove that

$$W_\mathfrak{m}\Gamma_0(\mathfrak{n}) = \Gamma_0(\mathfrak{n})W_\mathfrak{m}.$$

This is not hard to see, as multiplying $W_\mathfrak{m}$ on the left by any element in $\Gamma_0(\mathfrak{n})$ gives you another matrix with the same properties. But we know that any two matrices satisfying these properties must differ by multiplication by an element of $\Gamma_0(\mathfrak{n})$ on the right. This shows inclusion one way, inclusion in the other direction follows by a symmetric argument. □

It is not hard to check that the set of all such operators forms an abelian 2-group and that the Fricke involution can be formed as a product of Atkin-Lehner involutions, where $\mathfrak{m}$ runs over prime power divisors of $\mathfrak{n}$.

Indeed suppose $\mathfrak{m}_1 \mid \mathfrak{n}$, $\mathfrak{m}_2 \mid \mathfrak{n}$ and $\mathfrak{m}_1$ and $\mathfrak{m}_2$ are coprime. Let

$$M_{\mathfrak{m}_1} = \begin{pmatrix} x_1 & y_1 \\ z_1 & w_1 \end{pmatrix} \qquad M_{\mathfrak{m}_2} = \begin{pmatrix} x_2 & y_2 \\ z_2 & w_2 \end{pmatrix}$$

Then we have

$$M_{\mathfrak{m}_1} M_{\mathfrak{m}_2} = \begin{pmatrix} x_1x_2 + y_1z_2 & x_1y_2 + y_1w_2 \\ z_1x_2 + w_1z_2 & z_1y_2 + w_1w_2 \end{pmatrix}$$

Now

$$\begin{aligned} x_1x_2 + y_1z_2 &\in (\mathfrak{m}_1\mathfrak{m}_2)^{n+1} \\ x_1y_2 + y_1w_2 &\in (\mathfrak{m}_1\mathfrak{m}_2)^{n+1} \\ z_1x_2 + w_1z_2 &\in \mathfrak{n}(\mathfrak{m}_1\mathfrak{m}_2)^{n} \\ z_1y_2 + w_1w_2 &\in (\mathfrak{m}_1\mathfrak{m}_2)^{n+1} \end{aligned}$$

Hence

$$M_{\mathfrak{m}_1} M_{\mathfrak{m}_2} = M_{\mathfrak{m}_1\mathfrak{m}_2}.$$

In fact in general we have

$$M_{\mathfrak{m}_1} M_{\mathfrak{m}_2} = M_{\mathfrak{m}_3},$$

where $\mathfrak{m}_3 = \mathfrak{m}_1\mathfrak{m}_2 \gcd(\mathfrak{m}_1, \mathfrak{m}_2)^{-2}$.

REMARK: There is a more general way of defining these operators. We could take an ideal $\mathfrak{c}$ such that $\mathfrak{m}\mathfrak{c}^2 = \langle \mu \rangle$ is principal and $\mathfrak{c}$ is coprime to $\mathfrak{n}/\mathfrak{m}$. Then define $W_\mathfrak{m}$ to be a matrix of the form

$$\begin{pmatrix} \mathfrak{m}\mathfrak{c} & \mathfrak{c} \\ \mathfrak{n}\mathfrak{c} & \mathfrak{m}\mathfrak{c} \end{pmatrix}$$

with determinant μ. This will give equivalent operators but in practice might allow the use of matrices with smaller entries, particularly for $h > 3$, hence speeding up computation.

Chapter 6

Eigenforms and newforms

In this chapter we identify precisely which cusp forms we expect to correspond to elliptic curves. We do this first by restricting to the class of cusp forms whose L-series can be expressed as an Euler product of the same form as that of the L-series of an elliptic curve, i.e.

$$L(f,s) = \prod_{\mathfrak{p}|\mathfrak{n}} \frac{1}{1 - a_{\mathfrak{p}} N(\mathfrak{p})^{-s}} \prod_{\mathfrak{p}\nmid\mathfrak{n}} \frac{1}{1 - a_{\mathfrak{p}} N(\mathfrak{p})^{-s} + N(\mathfrak{p})^{1-s}},$$

with $a_{\mathfrak{p}} \in \mathbb{Z}$.

The Hecke operators, $T_{\mathfrak{p}}$, play a central role in identifying these cusp forms. As in the classical case we are looking for cusp forms which are simultaneous eigenforms for all the Hecke operators. To find these forms we try to decompose the space of cusp forms in such a way as to obtain a basis of such forms. Such a decomposition is initially blocked by the appearance of forms from lower levels at every multiple of their level, since as was mentioned earlier at the end of section 2.4, if $\mathfrak{n}' \mid \mathfrak{n}$ then $\hat{S}(\mathfrak{n}') \subseteq \hat{S}(\mathfrak{n})$. The way out of this problem is to look at a subspace of $\hat{S}(\mathfrak{n})$ which we call the **newspace**. We simply define the newspace $\hat{S}(\mathfrak{n})^{new}$ to be the space of all forms which do not arise from, (in a sense explained later), forms in $\hat{S}(\mathfrak{n}')$ for some $\mathfrak{n}'|\mathfrak{n}$. This space has exactly the properties we are looking for. In particular

Theorem 6.0.1. *$\hat{S}(\mathfrak{n})^{new}$ is the largest $\mathbb{T}$-invariant subspace of $\hat{S}(\mathfrak{n})$ on which $\mathbb{T}$ is semi-simple and commutative.*

Proof. Miyake, [16], pg 183. □

In other words, $\hat{S}(\mathfrak{n})^{new}$ as a module over the Hecke algebra $\mathbb{T}$, decomposes into the direct sum of simple submodules, i.e. modules which have no nontrivial submodules or equivalently $\hat{S}(\mathfrak{n})^{new}$ decomposes into subspaces which contain no smaller subspaces invariant under $\mathbb{T}$.

Miyake also shows that two normalised simultaneous eigenforms for $\mathbb{T}$ which have the same eigenvalues for almost all primes must in fact be equal.

So there exists a decomposition, (over $\mathbb{C}$),

$$\hat{S}(\mathfrak{n})^{new} = \bigoplus V_i$$

of $\hat{S}(\mathfrak{n})^{new}$ into a direct sum of (orthogonal) one-dimensional subspaces V_i, each of which is a simultaneous eigenspace for all elements of $\mathbb{T}$.

In each V_i there is exactly one form f_i with $c(1) = 1$ (said to be normalised). This follows because of the relations between coefficients, which means that if $c(1) = 0$ then $c(\mathfrak{p}) = 0$ for all $\mathfrak{p}$.

Since this form f_i is an eigenform for all the operators $T_{\mathfrak{p}}$, $L(f_i, s)$ has an Euler product, and because it is an eigenform for $W_{\mathfrak{n}}$, $\Lambda(f_i, s)$ should satisfy a functional equation of opposite sign to ε, where ε is the eigenvalue of $W_{\mathfrak{n}}$ acting on V_i. There is an adelic description of the Fricke involution which Kurcanov shows implies a functional equation. Cremona gives a simpler non-adelic proof when $h = 1$. However the Fricke involutions that I have defined do not interchange 0 and ∞ like the classical of adelic ones, so the standard derivation doesn't work here.

To see that being an eigenform for all the Hecke operators implies the existence of an Euler product, recall that

$$\begin{array}{rcll} T_{\mathfrak{a}} T_{\mathfrak{b}} & = & T_{\mathfrak{a}\mathfrak{b}} & \text{if } \gcd(\mathfrak{a}, \mathfrak{b}) = 1, \\ T_{\mathfrak{p}^r} T_{\mathfrak{p}} & = & T_{\mathfrak{p}^{r+1}} + N(\mathfrak{p}) T_{\mathfrak{p}^{r-1}} T_{\mathfrak{p},\mathfrak{p}} & \mathfrak{p} \nmid \mathfrak{n}, \\ T_{\mathfrak{p}^r} & = & T_{\mathfrak{p}}^r & \mathfrak{p} \mid \mathfrak{n}. \end{array}$$

These are proved in Chapter 7 of [5] using lattice arguments.

There is also an adelic approach to defining Hecke operators. This is described in [24], Chapter VI. Using this theory it is possible to deduce the following result:

Proposition 6.0.2. *Let f be a cusp form with Fourier coefficients $c(\mathfrak{m})$. If f is an eigenform for all $T_{\mathfrak{p}}$, $\mathfrak{p} \nmid \mathfrak{n}$, then $c(1) \neq 0$, and when we normalise f so that*

$c(1) = 1$, *we have*

$$T_{\mathfrak{m}} f = c(\mathfrak{m}) f.$$

Hence if f is a normalised eigenform for all the $T_{\mathfrak{m}}$, with trivial character, then

$$\begin{aligned} c(\mathfrak{a})c(\mathfrak{b}) &= c(\mathfrak{ab}) \quad \text{if } \gcd(\mathfrak{a}, \mathfrak{b}) = 1 && (6.1) \\ c(\mathfrak{p}^r)c(\mathfrak{p}) &= c(\mathfrak{p}^{r+1}) + N(\mathfrak{p})c(\mathfrak{p}^{r-1}) \quad r \geq 1, \mathfrak{p} \nmid \mathfrak{n} && (6.2) \\ c(\mathfrak{p}^r) &= c(\mathfrak{p})^r \quad r \geq 1, \mathfrak{p} \mid \mathfrak{n} && (6.3) \end{aligned}$$

which is precisely the condition required for $L(f, s) = \sum_{\mathfrak{a}} c(\mathfrak{a}) N(\mathfrak{a})^{-s}$ to have an Euler product of the required form. Indeed for a prime ideal $\mathfrak{p} \nmid \mathfrak{n}$, define

$$\begin{aligned} L_{\mathfrak{p}}(f, s) &= \sum_m c(\mathfrak{p}^m) N(\mathfrak{p})^{-ms} \\ &= 1 + c(\mathfrak{p})N(\mathfrak{p})^{-s} + c(\mathfrak{p}^2)(N(\mathfrak{p})^{-s})^2 + \ldots \end{aligned}$$

By inspection, the coefficient of $(N(\mathfrak{p})^{-s})^r$ in the product

$$(1 - c(\mathfrak{p})N(\mathfrak{p})^{-s} + N(\mathfrak{p})^{1-s}) L_{\mathfrak{p}}(f, s)$$

is

$$\begin{array}{cc} 1 & \text{for } r = 0 \\ 0 & \text{for } r = 1 \\ \vdots & \vdots \\ c(\mathfrak{p}^{l+1}) - c(\mathfrak{p}^l)c(\mathfrak{p}) + N(\mathfrak{p})c(\mathfrak{p}^{l-1}) & \text{for } r = l + 1 \end{array}$$

Therefore

$$L_{\mathfrak{p}}(f, s) = \frac{1}{1 - c(\mathfrak{p})N(\mathfrak{p})^{-s} + N(\mathfrak{p})^{1-s}}$$

if and only if equation (6.2) holds.

Similarly, for a prime ideal $\mathfrak{p} \mid \mathfrak{n}$

$$\begin{aligned} L_{\mathfrak{p}}(f, s) &:= \sum_m c(\mathfrak{p}^m) N(\mathfrak{p})^{-ms} \\ &= \frac{1}{1 - c(\mathfrak{p})N(\mathfrak{p})^{-s}} \end{aligned}$$

if and only if equation (6.3) holds.

If $\mathfrak{a}$ factorises as $\mathfrak{a} = \prod \mathfrak{p}_i^{n_i}$, then the coefficient of $(N(\mathfrak{p})^{-s})^r$ in $\prod L_{\mathfrak{p}}(f,s)$ is $\prod c(\mathfrak{p}_i^{n_i})$, which equals $c(\mathfrak{a})$ if (6.1) holds.

Recall that we are using Atkin-Lehner involutions instead of Hecke operators at the primes dividing the level. The link between the eigenvalues of these operators and the $a_{\mathfrak{p}}$ is more complicated, see [1]. If $f|W_{\mathfrak{q}} = \varepsilon_{\mathfrak{q}} f$ with $\varepsilon = \pm 1$ then

$$a(\mathfrak{q}, f) = \begin{cases} -\varepsilon_{\mathfrak{q}} & \text{if } \mathfrak{q}^2 \nmid N \\ 0 & \text{if } \mathfrak{q}^2 | N \end{cases}$$

Finally for $L(f,s)$ to be a candidate for being the L-function of an elliptic curve over k the Fourier coefficients of f must lie in $\mathbb{Z}$. For f to have rational coefficients its character must have order 1 or 2. In the case h odd, $h \neq 1$, this implies that the character must be trivial as the non-trivial unramified characters will have have order ≥ 3. So we are just interested in forms in $S(\mathfrak{n}, 1) = S(\mathfrak{n})$. As mentioned before, to study such forms it is enough to work with just one homology component.

So it follows that a modular form will have an L-series satisfying the various properties described in Theorem 1.3.6 if and only if it is a rational newform.

Our discussion of the L-series of a modular form has been entirely algebraic. Classically there is a rich analytic theory. Over $\mathbb{Q}$ and fields of class number 1 it is possible to obtain the L-series directly from the modular forms via a Melin transform. There is an analogous adelic theory for general fields but we have not been able to obtain a concrete description in the special case considered in this thesis. Also it has not been proven that the eigenvalues of the Hecke operators satisfy $|c(\mathfrak{p})| \leq 2\sqrt{N(\mathfrak{p})}$. So can not say that the L-series obtained above definitely converges for $\mathrm{Re}(s) > 3/2$, as expected for the L-series of an elliptic curve.

The first stage in finding the modular forms we are interested in is to restrict to the newspace. One method of doing this is to make use of certain natural "degeneracy maps". In this chapter we begin by recalling the classical theory and then show how this method can be extended to modular forms over imaginary quadratic fields.

6.1 Classical degeneracy maps

The classical concept of the newspace was first described by Atkin and Lehner in [1]. Their description was completely in terms of modular forms, but in this section we shall describe a more modern formulation in terms of homology and modular symbols, described in [21], as it is of more practical utility.

We start by describing certain natural maps between spaces of classical modular symbols of different levels. Fix a positive integer N. Let M be a positive divisor of N. For any positive divisor t of N/M, let $T = \left(\begin{smallmatrix} t & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

Proposition 6.1.1. *For each divisor t of N/M there is a well-defined linear map*

$$\alpha_t : \mathcal{M}_k(N) \longrightarrow \mathcal{M}_k(M) \qquad \alpha_t(x) = Tx = \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix} x.$$

Proof. [21], Proposition 2.15, pg 24 □

Definition 6.1.2. *(New modular symbols). The subspace $\mathcal{M}_k(N)^{new}$ of new modular symbols is the intersection of the kernels of the α_t as t runs through all positive divisors of N/M and M runs through positive divisors of N strictly less than N.*

Proposition 6.1.3. *Let f be a newform in $S_2(M)$ where $M|N$. Write $\frac{N}{M} = \prod p_i^{\beta_i}$. Then the oldclass in $S_2(N)$ coming from f has dimension $\prod(1+\beta_i)$.*

Proof. [9], Lemma 2.7.1 □

6.2 Generalised degeneracy maps

We now show how to generalise degeneracy maps to the case of imaginary quadratic number fields with odd class number. In the classical case $\alpha_t : \langle t^{-1}\rangle \oplus \mathbb{Z} \to \mathbb{Z} \oplus \mathbb{Z}$. The correct generalisation of this is to define a map $\alpha_{\mathfrak{d}} : \mathfrak{d}^{-1} \oplus \mathcal{O} \to \mathfrak{c} \oplus \mathfrak{c}$ where $\mathrm{cl}(\mathfrak{c}^2) = \mathrm{cl}(\mathfrak{d}^{-1})$.

First we need to introduce a new class of subgroups of $\mathrm{GL}_2(k)$. We define:

$$\mathrm{GL}_2^{\mathfrak{q}}(\mathcal{O}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, d \in \mathcal{O}, b \in \mathfrak{q}^{-1}, c \in \mathfrak{q}, ad - bc \in \mathcal{O}^\times \right\}$$

These matrices are important because they are the stabilisers of certain lattices. In particular let $\mathfrak{b}$ and $\mathfrak{c}$ be (fractional) ideals in $\mathcal{O}$, and let $V = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(k)$ with $\det(V) \in \mathcal{O}^\times$. Then

$$\begin{aligned}(\mathfrak{b} \oplus \mathcal{O}) \cdot V = \mathfrak{b} \oplus \mathcal{O} &\iff ax + cy \in \mathfrak{b}, \ \ bx + dy \in \mathcal{O} \ \ \forall\, x \in \mathfrak{b}, y \in \mathcal{O} \\ &\iff a, d \in \mathcal{O}, \ \ b \in \mathfrak{b}^{-1}, \ \ c \in \mathfrak{b} \\ &\iff V \in \mathrm{GL}_2^{\mathfrak{b}}(\mathcal{O})\end{aligned}$$

and

$$\begin{aligned}(\mathfrak{bc} \oplus \mathfrak{c}) \cdot V = \mathfrak{bc} \oplus \mathfrak{c} &\iff ax + cy \in \mathfrak{bc}, \ \ bx + dy \in \mathfrak{c} \ \ \forall\, x \in \mathfrak{bc}, y \in \mathfrak{c} \\ &\iff a, d \in \mathcal{O}, \ \ b \in \mathfrak{b}^{-1}, \ \ c \in \mathfrak{b} \\ &\iff V \in \mathrm{GL}_2^{\mathfrak{b}}(\mathcal{O})\end{aligned}$$

Lemma 6.2.1. *Let $\mathfrak{n}$ and $\mathfrak{m}$ be ideals of $\mathcal{O}$ with $\mathfrak{m}|\mathfrak{n}$. For each divisor $\mathfrak{d}$ of $\mathfrak{n}/\mathfrak{m}$ there exists a matrix $M_{\mathfrak{d}} \in \mathrm{GL}_2(k)$ satisfying:*

1. *$M_{\mathfrak{d}} : \mathfrak{d}^{-1} \oplus \mathcal{O} \to \mathfrak{c} \oplus \mathfrak{c}$ where $\mathrm{cl}(\mathfrak{c}^2) = \mathrm{cl}(\mathfrak{d}^{-1})$.*
2. *$M_{\mathfrak{d}} \Gamma_0(\mathfrak{n}) M_{\mathfrak{d}}^{-1} \subseteq \Gamma_0(\mathfrak{m})$.*
3. *The lower left entry of $M_{\mathfrak{d}}$ lies in $\mathfrak{n}$.*

Proof. Since h is odd we can choose an ideal $\mathfrak{c}$ with $\mathrm{cl}(\mathfrak{c}^2) = \mathrm{cl}(\mathfrak{d}^{-1})$. Let $\mathfrak{q}$ be an ideal in the same class as $\mathfrak{c}$ which is coprime to $\mathfrak{nd}$. We can do this by Lemma 1.2.2. Then we can define a matrix giving an isomorphism

$$A : \mathfrak{c} \oplus \mathfrak{c} \longrightarrow \mathfrak{d}^{-1} \oplus \mathcal{O}$$

as the product of three matrices taking

$$(\mathfrak{c} \oplus \mathfrak{c}) \longrightarrow (\mathfrak{c} \oplus \mathfrak{q}) \longrightarrow (\mathfrak{cq} \oplus \mathcal{O}) \longrightarrow (\mathfrak{d}^{-1} \oplus \mathcal{O})$$

Then for any $\gamma \in \mathrm{GL}_2(\mathcal{O})$ we have

$$A^{-1}\gamma A : \mathfrak{d}^{-1} \oplus \mathcal{O} \longrightarrow \mathfrak{d}^{-1} \oplus \mathcal{O}.$$

and so $A^{-1}\gamma A \in \mathrm{GL}_2^{\mathfrak{d}^{-1}}(\mathcal{O})$.

Now the first and third matrices in the product are diagonal matrices, and since $\mathfrak{q}$ is coprime to $\mathfrak{n}\mathfrak{d}$ we can use Bezout's theorem to find $a \in \mathfrak{q}, c \in \mathfrak{n}\mathfrak{d}$ such that $a - c = 1$. Then take the second matrix to be

$$\begin{pmatrix} a & 1 \\ c & 1 \end{pmatrix}$$

Hence A has lower left entry in $\mathfrak{n}$

Now suppose we have $\gamma \in \Gamma_0(\mathfrak{n})$. Then it is clear that $A^{-1}\gamma A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(\mathfrak{m})$, since $a, d \in \mathcal{O}$, $b \in \mathfrak{d}$ which is an integral ideal and $c \in \mathfrak{n}\mathfrak{d}^{-1} \subseteq \mathfrak{m}$. Then $M_{\mathfrak{d}} = A^{-1}$ has the required properties. □

Proposition 6.2.2. *Let* $\mathfrak{n}$ *and* $\mathfrak{m}$ *be ideals of* $\mathcal{O}$ *with* $\mathfrak{m}|\mathfrak{n}$. *For each divisor* $\mathfrak{d}$ *of* $\mathfrak{n}/\mathfrak{m}$ *the map*

$$\alpha_{\mathfrak{d}} : \Gamma_0(\mathfrak{n}) \setminus \mathcal{H}_3 \longrightarrow \Gamma_0(\mathfrak{m}) \setminus \mathcal{H}_3 \qquad \alpha_{\mathfrak{d}}(x) = M_{\mathfrak{d}}x$$

where $M_{\mathfrak{d}}$ *is as defined above, is well defined and independent of the particular matrix chosen.*

Proof. To see that the action of this map is well defined, let γ be any element of $\Gamma_0(\mathfrak{n})$. Then

$$\begin{aligned} \alpha_{\mathfrak{d}}(\gamma x) = \alpha_{\mathfrak{d}}(x) \mod \Gamma_0(\mathfrak{m}) &\iff M_{\mathfrak{d}}\gamma x = M_{\mathfrak{d}}x \mod \Gamma_0(\mathfrak{m}) \\ &\iff M_{\mathfrak{d}}\gamma x = \gamma' M_{\mathfrak{d}}x \text{ for some } \gamma' \in \Gamma_0(\mathfrak{m}) \\ &\iff M_{\mathfrak{d}}\gamma = \gamma' M_{\mathfrak{d}} \\ &\iff M_{\mathfrak{d}}\Gamma_0(\mathfrak{n})M_{\mathfrak{d}}^{-1} \in \Gamma_0(\mathfrak{m}) \end{aligned}$$

If $M_{\mathfrak{d}}^1$ and $M_{\mathfrak{d}}^2$ are two choices for $M_{\mathfrak{d}}$, then by definition

$$M_{\mathfrak{d}}^1(M_{\mathfrak{d}}^2)^{-1} : \mathfrak{c} \oplus \mathfrak{c} \to \mathfrak{c} \oplus \mathfrak{c}.$$

Hence

$$M_{\mathfrak{d}}^1(M_{\mathfrak{d}}^2)^{-1} : \mathcal{O} \oplus \mathcal{O} \to \mathcal{O} \oplus \mathcal{O}.$$

So $M_{\mathfrak{d}}^1(M_{\mathfrak{d}}^2)^{-1} \in \mathrm{GL}_2(\mathcal{O})$, but since the lower left entry of each matrix lies in $\mathfrak{n}$, the same is true of their product. Hence in fact $M_{\mathfrak{d}}^1(M_{\mathfrak{d}}^2)^{-1} \in \Gamma_0(\mathfrak{n})$, proving the second assertion. □

This map between the quotient spaces induces a map between the homology spaces.

This then induces a map by duality in the opposite direction

$$a_{\mathfrak{d}} : S_k(\mathfrak{m}) \to S_k(\mathfrak{n})$$

We can now define exactly what we mean by "arising from", we mean contained in the image of one of these maps. Thus we define the **oldspace** of cusp forms to be the sum of the images of $\alpha_{\mathfrak{d}}$ as $\mathfrak{d}$ runs through all divisors of $\mathfrak{n}/\mathfrak{m}$ and $\mathfrak{m}$ runs through all non-trivial divisors of $\mathfrak{n}$. We then define the **newspace** of cusp forms to be the orthogonal complement, with respect to the Petersson inner product[1], of the oldspace.

In practice we need only take $\mathfrak{m} = \mathfrak{n}\mathfrak{p}^{-1}$ for each prime divisor, $\mathfrak{p}$, of $\mathfrak{n}$, giving $\mathfrak{d} = \mathfrak{p}$ or $\mathcal{O}$.

The subspace of modular symbols corresponding to the newspace of modular forms is the intersection of the kernel of $\alpha_{\mathfrak{d}}$ as $\mathfrak{d}$ runs through all divisors of $\mathfrak{n}/\mathfrak{m}$ and $\mathfrak{m}$ runs through all non-trivial divisors of $\mathfrak{n}$.

[1] There is a natural analogue of the classical Petersson inner product, see [16].

Chapter 7

Results

7.1 $\mathbb{Q}(\sqrt{-23})$

Table 7.1 below details all of the rational newforms that I have found, (up to complex conjugation), listed in order of norm. They have all been found either by searching through curves with small coefficients, or via the method described at the end of section 1.3. Each row represents a newform. The first column shows the factorisation of the level and the second shows the norm of the level. The third simply assigns a name to each form and the fourth column shows the coefficients for all prime ideals of norm less than 50. The last column shows the eigenvalue of the Fricke involution. An * next to the name denotes a modular form for which I do not have a matching elliptic curve at present. To be precise given a modular form f, we say that we have found a matching elliptic curve if we have found an elliptic curve E over k such that:

1. Conductor(E) = Level$(f) = \mathfrak{n}$.
2. For primes $\mathfrak{p}$ not dividing $\mathfrak{n}$, the Trace of Frobenius of E at $\mathfrak{p}$ is equal to the eigenvalue of $T_{\mathfrak{p}}$ acting on the space generated by the newform.
3. For primes $\mathfrak{p}$ dividing $\mathfrak{n}$: if $\mathfrak{p}^2$ divides $\mathfrak{n}$ then the Trace of Frobenius of E at $\mathfrak{p}$ is 0; otherwise it is minus the corresponding eigenvalue of $W_{\mathfrak{p}}$.
4. The eigenvalue of the Fricke involution satisfies Conjecture 3.

Conditions (2) and (3) are tested at least for all primes of norm ≤ 50. Together they imply that the first few Euler factors of $\mathrm{L}(f,s)$ and $\mathrm{L}(E,s)$ agree.

Note that f_{18},f_{28} and f_{52} in Table 7.1 are equal to their own conjugates. This means that they correspond to elliptic curves which are the lift of a curve defined over $\mathbb{Q}$.

Table 7.2 lists for completeness the various newforms we have found which do not have rational coefficients. These are expected to correspond not to elliptic curves but rather possibly to higher dimensional abelian varieties. The constants $t_1, \ldots, t_5$ satisfy the following equations:

$$\begin{aligned} t_1^2 + t_1 - 1 &= 0 \\ t_2^2 - t_2 - 4 &= 0 \\ t_3^2 - 3 &= 0 \\ t_4^3 + t_4^2 - 2t_4 - 1 &= 0 \end{aligned}$$

Table 7.3 lists all the matching elliptic curves that we have been able to find. N.B. since k has class number 3, elliptic curves don't have a global minimal model, so the models given here for the curves are fairly arbitrary.

$\mathfrak{n}$	$N(\mathfrak{n})$		$\mathfrak{p}_2$	$\bar{\mathfrak{p}}_2$	$\mathfrak{p}_3$	$\bar{\mathfrak{p}}_3$	$\mathfrak{p}_{13}$	$\bar{\mathfrak{p}}_{13}$	$\mathfrak{p}_{23}$	$\mathfrak{p}_5$	$\mathfrak{p}_{29}$	$\bar{\mathfrak{p}}_{29}$	$\mathfrak{p}_{31}$	$\bar{\mathfrak{p}}_{31}$	$\mathfrak{p}_{41}$	$\bar{\mathfrak{p}}_{41}$	$\mathfrak{p}_{47}$	$\bar{\mathfrak{p}}_{47}$	$\mathfrak{p}_7$	ε
$\mathfrak{p}_2\bar{\mathfrak{p}}_3$	6	f_1	1	1	0	-1	-2	2	-4	-2	6	6	0	-4	-2	2	8	0	-6	-1
$\bar{\mathfrak{p}}_2\mathfrak{p}_{13}$	26	f_2	0	-1	-2	1	1	5	6	-1	0	-3	5	-4	12	9	9	6	-4	-1
$\mathfrak{p}_3\bar{\mathfrak{p}}_3^2$	27	f_3	-1	1	-1	-0	2	2	0	6	-2	2	8	8	6	-6	0	0	-2	-1
$\mathfrak{p}_2^2\bar{\mathfrak{p}}_2^3$	32	f_4	-0	-0	-1	-3	-1	3	-8	-2	-5	-1	-5	5	3	-5	-13	-3	-2	1
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_3^2$	36	f_5	-1	-1	+0	-2	2	-4	-6	2	0	-6	-10	8	-6	-6	0	12	-4	1
$\mathfrak{p}_2^3\bar{\mathfrak{p}}_2\bar{\mathfrak{p}}_3$	48	f_6	-0	-1	0	-1	6	2	4	-2	-10	-2	8	4	-2	-6	0	8	10	-1
$\bar{\mathfrak{p}}_2^2\mathfrak{p}_{13}$	52	f_7	1	-0	2	2	-1	6	-8	-6	10	2	2	0	-6	-6	4	-6	2	-1
$\mathfrak{p}_2\bar{\mathfrak{p}}_3^3$	54	f_8	-1	0	1	+0	-4	-4	-3	8	-3	0	-4	-4	0	3	-12	0	-4	1
$\bar{\mathfrak{p}}_2\bar{\mathfrak{p}}_3^3$	54	f_9	0	-1	-2	+0	5	-4	-3	-1	-9	6	-4	5	3	0	-9	-3	-4	1
$\bar{\mathfrak{p}}_2\mathfrak{p}_{31}$	62	f_{10}	1	1	3	0	-5	5	3	-2	-8	-8	-1	7	-5	5	0	1	-6	-1
$\mathfrak{p}_2^4\bar{\mathfrak{p}}_2^2$	64	f_{11}	-0	-0	1	-1	-5	-5	0	-2	3	3	1	-1	-9	-9	-3	3	-2	1
$\bar{\mathfrak{p}}_2^3\mathfrak{p}_3\bar{\mathfrak{p}}_3$	72	f_{12}	-1	-0	-1	-1	6	-2	0	2	-2	6	-8	-8	2	10	0	0	2	-1
$\mathfrak{p}_2^2\bar{\mathfrak{p}}_2\mathfrak{p}_3^2$	72	f_{13}	-0	1	-0	-2	-4	2	6	8	6	-6	2	8	6	0	0	0	2	-1

Table 7.1: Rational Newforms for $\mathbb{Q}(\sqrt{-23})$ - Part 1 of 4

$\mathfrak{n}$	$N(\mathfrak{n})$		$\mathfrak{p}_2$	$\bar{\mathfrak{p}}_2$	$\mathfrak{p}_3$	$\bar{\mathfrak{p}}_3$	$\mathfrak{p}_{13}$	$\bar{\mathfrak{p}}_{13}$	$\mathfrak{p}_{23}$	$\mathfrak{p}_5$	$\mathfrak{p}_{29}$	$\bar{\mathfrak{p}}_{29}$	$\mathfrak{p}_{31}$	$\bar{\mathfrak{p}}_{31}$	$\mathfrak{p}_{41}$	$\bar{\mathfrak{p}}_{41}$	$\mathfrak{p}_{47}$	$\bar{\mathfrak{p}}_{47}$	$\mathfrak{p}_7$	ε
$\bar{\mathfrak{p}}_2\bar{\mathfrak{p}}_3\mathfrak{p}_{13}$	78	$f_{14}*$	0	-1	3	-1	1	0	1	4	10	2	-5	1	-3	-11	-11	6	-9	-1
$\mathfrak{p}_2\bar{\mathfrak{p}}_3\bar{\mathfrak{p}}_{13}$	78	$f_{15}*$	-1	-2	-1	-1	3	-1	-8	3	-1	10	-6	-1	-3	0	-6	-5	8	1
	78	f_{16}	1	-2	-3	-1	-5	1	-4	1	-3	-6	6	5	7	-4	-10	3	-12	1
$\bar{\mathfrak{p}}_2\mathfrak{p}_{41}$	82	f_{17}	0	-1	1	-2	-1	2	3	-1	0	9	-4	2	-1	-6	-3	-12	-4	1
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_{23}$	92	f_{18}	-1	-1	0	0	-2	-2	1	6	2	2	0	0	6	6	0	0	2	-1
$\mathfrak{p}_2^2\bar{\mathfrak{p}}_2^3\mathfrak{p}_3$	96	f_{19}	-0	-0	1	2	4	-2	2	8	10	-6	-10	0	-2	0	-8	-8	-2	-1
$\mathfrak{p}_2^4\bar{\mathfrak{p}}_2\mathfrak{p}_3$	96	f_{20}	-0	1	1	2	4	-2	-6	-8	-6	-6	-2	8	6	0	0	0	-2	-1
$\mathfrak{p}_2^5\mathfrak{p}_3$	96	f_{21}	-0	-1	-1	0	6	-6	0	6	-6	-2	0	0	2	6	8	8	-6	-1
$\bar{\mathfrak{p}}_2^2\mathfrak{p}_3\bar{\mathfrak{p}}_3^2$	108	f_{22}	1	-0	-1	+0	-4	4	8	4	-6	0	-4	0	8	10	12	-4	12	-1
$\mathfrak{p}_2^2\bar{\mathfrak{p}}_3^3$	108	f_{23}	-0	-2	3	+0	4	-4	-1	-2	3	-6	6	8	-8	5	2	6	6	-1
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_3\bar{\mathfrak{p}}_3^2$	108	f_{24}	1	-1	-1	-0	-6	-6	0	-2	-2	2	-8	-8	6	-6	-8	8	6	1
	108	f_{25}	-1	1	1	-0	2	2	0	2	-6	6	-4	-4	-6	6	-12	12	14	-1
	108	f_{26}	1	-1	1	-0	2	2	0	-10	6	-6	8	8	6	-6	0	0	-10	-1

Table 7.1: Rational Newforms for $\mathbb{Q}(\sqrt{-23})$ - Part 2 of 4

$\mathfrak{n}$	$N(\mathfrak{n})$		$\mathfrak{p}_2$	$\bar{\mathfrak{p}}_2$	$\mathfrak{p}_3$	$\bar{\mathfrak{p}}_3$	$\mathfrak{p}_{13}$	$\bar{\mathfrak{p}}_{13}$	$\mathfrak{p}_{23}$	$\mathfrak{p}_5$	$\mathfrak{p}_{29}$	$\bar{\mathfrak{p}}_{29}$	$\mathfrak{p}_{31}$	$\bar{\mathfrak{p}}_{31}$	$\mathfrak{p}_{41}$	$\bar{\mathfrak{p}}_{41}$	$\mathfrak{p}_{47}$	$\bar{\mathfrak{p}}_{47}$	$\mathfrak{p}_7$	ε
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_{29}$	116	f_{27}	-1	-1	1	1	-7	2	0	-4	-1	3	-4	5	-6	-12	6	0	5	1
$\mathfrak{p}_{11}$	121	f_{28}	-2	-2	-1	-1	4	4	-1	-9	0	0	7	7	-8	-8	8	8	-10	-1
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\bar{\mathfrak{p}}_{31}$	124	f_{29}	1	1	-2	-3	-1	-5	-3	4	-2	6	-7	-1	3	-7	-3	-10	-8	1
$\mathfrak{p}_2^4\bar{\mathfrak{p}}_2^3$	128	f_{30}	+0	+0	-1	1	-1	-1	0	6	-9	-9	3	-3	-1	-1	-1	1	-10	1
$\mathfrak{p}_3\bar{\mathfrak{p}}_{47}$	141	f_{31}	-1	-1	1	0	2	6	4	-2	10	-2	-8	-8	2	10	8	-1	6	-1
$\mathfrak{p}_2^4\mathfrak{p}_3\bar{\mathfrak{p}}_3$	144	f_{32}	-0	-1	-1	1	-2	-2	0	-6	-2	-2	-8	8	-6	-6	0	0	2	1
	144	f_{33}	+0	-1	1	-1	6	-2	8	-6	6	-2	0	0	-6	2	8	-8	10	-1
$\mathfrak{p}_2^3\bar{\mathfrak{p}}_2\mathfrak{p}_3^2$	144	f_{34}	-0	-1	+0	2	6	-4	-2	-2	8	10	2	-8	10	6	0	-4	4	-1
$\mathfrak{p}_2^2\bar{\mathfrak{p}}_2^2\bar{\mathfrak{p}}_3^2$	144	f_{35}	-0	-0	1	-0	5	5	0	2	3	-3	-1	-1	9	-9	3	-3	2	-1
$\bar{\mathfrak{p}}_2^4\mathfrak{p}_3^2$	144	f_{36}	-1	-0	-0	0	-2	2	-4	2	-6	6	-4	0	2	2	0	-8	6	1
$\mathfrak{p}_2^3\bar{\mathfrak{p}}_2\mathfrak{p}_3\bar{\mathfrak{p}}_3$	144	f_{37}	-0	1	-1	1	-2	-2	8	2	6	-2	0	8	-6	10	-8	-8	10	-1
$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$	150	$f_{38}*$	1	0	1	-1	1	-7	-1	-1	-8	-6	-6	-3	5	4	6	-4	2	1
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_3\mathfrak{p}_{13}$	156	f_{39}	1	-1	1	-2	1	-4	-6	2	6	0	8	-4	0	6	12	6	8	-1
	156	$f_{40}*$	1	1	-1	2	1	0	6	6	-6	-8	0	-4	-4	2	-12	10	8	-1

Table 7.1: Rational Newforms for $\mathbb{Q}(\sqrt{-23})$ - Part 3 of 4

$\mathfrak{n}$	$N(\mathfrak{n})$		$\mathfrak{p}_2$	$\bar{\mathfrak{p}}_2$	$\mathfrak{p}_3$	$\bar{\mathfrak{p}}_3$	$\mathfrak{p}_{13}$	$\bar{\mathfrak{p}}_{13}$	$\mathfrak{p}_{23}$	$\mathfrak{p}_5$	$\mathfrak{p}_{29}$	$\bar{\mathfrak{p}}_{29}$	$\mathfrak{p}_{31}$	$\bar{\mathfrak{p}}_{31}$	$\mathfrak{p}_{41}$	$\bar{\mathfrak{p}}_{41}$	$\mathfrak{p}_{47}$	$\bar{\mathfrak{p}}_{47}$	$\mathfrak{p}_7$	ε
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_3\bar{\mathfrak{p}}_{13}$	156	$f_{41}*$	-1	1	-1	0	-6	1	4	-2	-10	-2	4	-8	10	6	0	-8	-6	1
$\mathfrak{p}_2\bar{\mathfrak{p}}_3^4$	162	f_{42}	-1	0	-2	+0	-1	2	-6	-4	0	-3	-4	8	6	0	3	-9	14	1
	162	f_{43}	1	-2	0	-0	1	-4	2	-8	0	3	-6	2	-2	-10	-7	-3	6	1
$\mathfrak{p}_2\mathfrak{p}_3^3\bar{\mathfrak{p}}_3$	162	f_{44}	1	-2	-0	-1	-2	-1	-1	1	-6	-9	3	-10	-8	5	5	3	6	1
$\mathfrak{p}_2\mathfrak{p}_3^2\bar{\mathfrak{p}}_3^2$	162	f_{45}	-1	-1	-0	-0	-2	2	4	-2	-6	-6	0	-4	2	-2	-8	0	-6	1
$\mathfrak{p}_2\bar{\mathfrak{p}}_3\mathfrak{p}_{29}$	174	$f_{46}*$	1	-1	-2	1	-4	0	-6	-6	-1	0	4	4	-8	2	-8	2	2	1
$\mathfrak{p}_3\mathfrak{p}_{59}$	177	f_{47}	2	2	1	2	-5	0	1	-4	2	4	4	-3	6	6	7	5	5	-1
$\mathfrak{p}_2^5\bar{\mathfrak{p}}_2\mathfrak{p}_3$	192	f_{48}	+0	1	1	-2	-4	-6	-6	4	-10	2	6	-8	6	-4	-8	0	6	1
$\mathfrak{p}_2^6\mathfrak{p}_3$	192	f_{49}	+0	1	1	0	6	6	0	-6	6	-2	0	0	-2	-6	8	8	-6	-1
$\mathfrak{p}_2^6\bar{\mathfrak{p}}_3$	192	f_{50}	+0	-1	0	-1	-2	-2	4	2	-6	6	0	4	2	-2	8	0	-6	1
$\mathfrak{p}_2^2\bar{\mathfrak{p}}_2^4\mathfrak{p}_3$	192	f_{51}	-0	-0	-1	-2	4	-2	6	-8	-6	-6	2	-8	6	0	0	0	-2	1
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_7$	196	f_{52}	-1	-1	-2	-2	-4	-4	0	-10	-6	-6	-4	-4	6	6	-12	-12	1	-1

Table 7.1: Rational Newforms for $\mathbb{Q}(\sqrt{-23})$ - Part 4 of 4

$\mathfrak{n}$	$N(\mathfrak{n})$		$\mathfrak{p}_2$	$\bar{\mathfrak{p}}_2$	$\mathfrak{p}_3$	$\bar{\mathfrak{p}}_3$	$\mathfrak{p}_{13}$	$\bar{\mathfrak{p}}_{13}$
$\mathfrak{p}_{23}$	23	g_1	t_1	t_1	$-2t_1-1$	$-2t_1-1$	3	3
$\mathfrak{p}_3\mathfrak{p}_5$	75	g_2	t_2	2	1	$-t_2$	$-t_2-2$	$-t_2+4$
$\mathfrak{p}_3^2\bar{\mathfrak{p}}_3^2$	81	g_3	$-t_3$	t_3	$+0$	$+0$	-4	-4
$\mathfrak{p}_3\mathfrak{p}_{29}$	87	g_4	t_4	$-t_4^2+1$	1	$t_4^2+t_4-2$	$-3t_4^2-2t_4+3$	$-t_4^2-2t_4-2$
$\mathfrak{p}_2^4\bar{\mathfrak{p}}_2^3$	128	g_5	-0	$+0$	t_2	$-t_2$	t_2+2	t_2+2

	$\mathfrak{p}_{23}$	$\mathfrak{p}_5$	$\mathfrak{p}_{29}$	$\bar{\mathfrak{p}}_{29}$	$\mathfrak{p}_{31}$	$\bar{\mathfrak{p}}_{31}$
g_1	1	$-4t_1-6$	-3	-3	$6t_1+3$	$6t_1+3$
g_2	$-t_2+6$	-1	$-t_2-1$	t_2-3	t_2+1	$-2t_2+1$
g_3	0	-4	$-4t_3$	$4t_3$	-4	-4
g_4	$-3t_4^2-t_4+3$	$3t_4^2+t_4-5$	1	$3t_4^2-5$	$3t_4^2+2t_4-4$	$-3t_4-4$
g_5	0	$-4t_2+2$	t_2+2	t_2+2	t_2-4	$-t_2+4$

	$\mathfrak{p}_{41}$	$\bar{\mathfrak{p}}_{41}$	$\mathfrak{p}_{47}$	$\bar{\mathfrak{p}}_{47}$	$\mathfrak{p}_7$	ε
g_1	$-4t_1-1$	$-4t_1-1$	$-2t_1-1$	$-2t_1-1$	$4t_1-6$	-1
g_2	$2t_2+5$	$-5t_2+3$	$2t_2-6$	$-4t_2$	$-t_2-7$	-1
g_3	$-4t_3$	$4t_3$	$2t_3$	$-2t_3$	-4	1
g_4	$-4t_4+1$	$t_4^2+2t_4$	$3t_4^2-4t_4-7$	$5t_4^2+t-9$	$2t_4^2+7t_4-4$	1
g_5	$-3t_2+6$	$-3t_2+6$	$5t_2-4$	$-5t_2+4$	$-4t_2+2$	1

Table 7.2: Other Newforms for $\mathbb{Q}(\sqrt{-23})$

$\mathfrak{n}$	$N(\mathfrak{n})$	a_1	a_2	a_3	a_4	a_6	Rank
$\mathfrak{p}_2\bar{\mathfrak{p}}_3$	6	ω	-1	0	$-\omega-6$	0	0
$\bar{\mathfrak{p}}_2\mathfrak{p}_{13}$	26	ω	$-\omega+1$	1	-1	0	0
$\mathfrak{p}_3\bar{\mathfrak{p}}_3^2$	27	1	$-\omega-1$	1	1	$\omega-2$	0
$\mathfrak{p}_2^2\bar{\mathfrak{p}}_2^3$	32	0	$-\omega$	0	$4\omega-1$	-5	1
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_3^2$	36	$\omega+1$	$-\omega$	$\omega+1$	$-\omega-1$	0	1
$\mathfrak{p}_2^3\bar{\mathfrak{p}}_2\bar{\mathfrak{p}}_3$	48	0	$\omega-1$	0	$5\omega+6$	0	0
$\bar{\mathfrak{p}}_2^2\bar{\mathfrak{p}}_{13}$	52	$\omega+1$	1	0	-1	0	0
$\mathfrak{p}_2\bar{\mathfrak{p}}_3^3$	54	$\omega+1$	$\omega-1$	ω	-2ω	0	1
$\bar{\mathfrak{p}}_2\bar{\mathfrak{p}}_3^3$	54	0	ω	$\omega+1$	$2\omega-6$	-4	1
$\bar{\mathfrak{p}}_2\mathfrak{p}_{31}$	62	$\omega+1$	-1	0	$-2\omega-2$	$-\omega+3$	0
$\mathfrak{p}_2^4\bar{\mathfrak{p}}_2^2$	64	0	$-\omega-1$	0	3	$-2\omega-5$	1
$\bar{\mathfrak{p}}_2^3\mathfrak{p}_3\bar{\mathfrak{p}}_3$	72	$\omega+1$	1	$\omega+1$	0	0	0
$\mathfrak{p}_2^2\bar{\mathfrak{p}}_2\mathfrak{p}_3^2$	72	ω	$\omega+1$	0	$-2\omega-4$	$\omega+3$	0

Table 7.3: Elliptic Curves over $\mathbb{Q}(\sqrt{-23})$ - Part 1 of 4

$\mathfrak{n}$	$N(\mathfrak{n})$	a_1	a_2	a_3	a_4	a_6	Rank
$\bar{\mathfrak{p}}_2\bar{\mathfrak{p}}_3\mathfrak{p}_{13}$	78						
$\mathfrak{p}_2\bar{\mathfrak{p}}_3\bar{\mathfrak{p}}_{13}$	78						
$\mathfrak{p}_2\bar{\mathfrak{p}}_3\bar{\mathfrak{p}}_{13}$	78	$\omega+1$	$\omega+1$	1	$-\omega-4$	$\omega+5$	1
$\bar{\mathfrak{p}}_2\mathfrak{p}_{41}$	82	ω	0	1	6	$-2\omega-4$	1
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_{23}$	92	1	-1	0	-10	-12	0
$\mathfrak{p}_2^2\bar{\mathfrak{p}}_2^3\mathfrak{p}_3$	96	0	$-\omega-1$	0	$5\omega-22$	$-6\omega+48$	0
$\mathfrak{p}_2^4\bar{\mathfrak{p}}_2\mathfrak{p}_3$	96	ω	$\omega-1$	0	$-\omega-1$	0	0
$\mathfrak{p}_2^5\mathfrak{p}_3$	96	ω	ω	ω	$-\omega-5$	$-2\omega-4$	0
$\bar{\mathfrak{p}}_2^2\mathfrak{p}_3\bar{\mathfrak{p}}_3^2$	108	$\omega+1$	$-\omega-1$	0	$-\omega$	$3\omega+1$	0
$\mathfrak{p}_2^2\bar{\mathfrak{p}}_3^3$	108	0	0	ω	$2\omega-3$	$\omega+3$	0
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_3\bar{\mathfrak{p}}_3^2$	108	0	0	0	$552\omega+1221$	$4888\omega-34762$	1
	108	1	$\omega-1$	0	$2\omega-3$	5	0
	108	0	0	0	$-53160\omega-43995$	$-5067640\omega+19402006$	2

Table 7.3: Elliptic Curves over $\mathbb{Q}(\sqrt{-23})$ - Part 2 of 4

$\mathfrak{n}$	$N(\mathfrak{n})$	a_1	a_2	a_3	a_4	a_6	Rank
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_{29}$	116	$\omega+1$	0	$\omega+1$	$2\omega-1$	$-6\omega-8$	1
$\mathfrak{p}_{11}$	121	0	-1	1	0	0	0
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\bar{\mathfrak{p}}_{31}$	124	1	$\omega-1$	$-\omega+1$	$\omega+3$	$7\omega-9$	1
$\mathfrak{p}_2^4\bar{\mathfrak{p}}_2^3$	128	0	$\omega+1$	0	$\omega-2$	-1	1
$\mathfrak{p}_3\bar{\mathfrak{p}}_{47}$	141	1	$\omega-1$	$\omega+1$	-4	$-\omega$	0
$\mathfrak{p}_2^4\mathfrak{p}_3\bar{\mathfrak{p}}_3$	144	$-\omega+2$	ω	$-\omega+2$	$3\omega+3$	$2\omega+4$	1
	144	ω	$\omega-1$	0	1	0	0
$\mathfrak{p}_2^3\bar{\mathfrak{p}}_2\mathfrak{p}_3^2$	144	0	0	0	$-18927\omega-14202$	$1857222\omega-1211004$	0
$\mathfrak{p}_2^3\bar{\mathfrak{p}}_2\mathfrak{p}_3^2$	144	0	ω	0	$-\omega-3$	$-2\omega+3$	0
$\bar{\mathfrak{p}}_2^4\mathfrak{p}_3^2$	144	$\omega+1$	-1	$\omega+1$	$-5\omega+3$	$2\omega+2$	1
$\mathfrak{p}_2^3\bar{\mathfrak{p}}_2\mathfrak{p}_3\bar{\mathfrak{p}}_3$	144	0	0	0	$864\omega-26811$	$-95472\omega+1553094$	0
$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$	150						
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_3\mathfrak{p}_{13}$	156	1	0	ω	-2	$-2\omega+4$	0
	156						

Table 7.3: Elliptic Curves over $\mathbb{Q}(\sqrt{-23})$ - Part 3 of 4

$\mathfrak{n}$	$N(\mathfrak{n})$	a_1	a_2	a_3	a_4	a_6	Rank
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_3\bar{\mathfrak{p}}_1 3$	156						
$\mathfrak{p}_2\bar{\mathfrak{p}}_3^4$	162	$\omega+1$	$\omega-1$	0	$-2\omega-6$	$-2\omega+6$	1
	162	$\omega+1$	-1	1	$-4\omega-2$	$\omega+5$	1
$\mathfrak{p}_2\mathfrak{p}_3^3\bar{\mathfrak{p}}_3$	162	$\omega+1$	$\omega+1$	1	-7	$-3\omega+5$	1
$\mathfrak{p}_2\mathfrak{p}_3^2\bar{\mathfrak{p}}_3^2$	162	1	-1	ω	-2ω	4	1
$\mathfrak{p}_2\bar{\mathfrak{p}}_3\mathfrak{p}_{29}$	174						
$\mathfrak{p}_3\mathfrak{p}_{59}$	177	0	$-\omega-1$	1	$\omega-2$	1	0
$\mathfrak{p}_2^5\bar{\mathfrak{p}}_2\mathfrak{p}_3$	192	ω	$-\omega+1$	0	$-4\omega-4$	0	1
$\mathfrak{p}_2^6\mathfrak{p}_3$	192	ω	0	ω	$-\omega-1$	$-\omega$	0
$\mathfrak{p}_2^6\bar{\mathfrak{p}}_3$	192	ω	-1	ω	2	$-\omega+1$	1
$\mathfrak{p}_2^2\bar{\mathfrak{p}}_2^4\mathfrak{p}_3$	192	0	$\omega-2$	0	-8	$-\omega-5$	1
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_7$	196	1	0	1	-1	0	2

Table 7.3: Elliptic Curves over $\mathbb{Q}(\sqrt{-23})$ - Part 4 of 4

7.2 $\mathbb{Q}(\sqrt{-31})$

Here we record the same information for $\mathbb{Q}(\sqrt{-31})$. The data is arranged in the same format.

$\mathfrak{n}$	$N(\mathfrak{n})$		$\mathfrak{p}_2$	$\bar{\mathfrak{p}}_2$	$\mathfrak{p}_5$	$\bar{\mathfrak{p}}_5$	$\mathfrak{p}_7$	$\bar{\mathfrak{p}}_7$	$\mathfrak{p}_3$	$\mathfrak{p}_{19}$	$\bar{\mathfrak{p}}_{19}$	$\mathfrak{p}_{31}$	$\mathfrak{p}_{41}$	$\bar{\mathfrak{p}}_{41}$	$\mathfrak{p}_{47}$	$\bar{\mathfrak{p}}_{47}$	ε
$\mathfrak{p}_2\mathfrak{p}_5$	10	f_1	1	1	-1	0	2	4	-4	-6	0	4	-2	2	6	-8	-1
$\mathfrak{p}_2\mathfrak{p}_7$	14	f_2	-1	0	0	3	1	-1	1	2	2	5	9	-6	-6	12	-1
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_5$	20	f_3	-1	-1	-1	0	-4	2	-2	2	-4	-4	0	-12	0	6	1
	20	f_4*	1	-1	-1	0	2	-4	4	2	8	-4	6	-6	6	0	-1
$\mathfrak{p}_2^3\bar{\mathfrak{p}}_2^2$	32	f_5	-0	-0	-1	3	-3	-5	-2	-7	3	0	-9	-1	0	0	1
$\mathfrak{p}_2^4\bar{\mathfrak{p}}_2$	32	f_6	-0	-1	2	2	-2	2	4	-4	4	0	-8	-8	-2	2	-1
$\mathfrak{p}_7^2$	49	f_7	-1	2	2	1	-0	1	3	0	6	-3	-5	-4	10	2	-1
$\mathfrak{p}_2\mathfrak{p}_5^2$	50	f_8	1	-1	+0	0	-2	4	4	6	0	-4	-2	2	-6	-8	-1
$\mathfrak{p}_2\bar{\mathfrak{p}}_{31}$	62	f_9*	1	1	2	4	0	-2	-2	-4	8	-1	2	2	-2	4	-1
$\mathfrak{p}_2^4\bar{\mathfrak{p}}_2^2$	64	f_{10}	-0	-0	-1	-1	1	-1	-2	5	-5	0	-5	-5	-8	8	1
$\mathfrak{p}_2\mathfrak{p}_5\mathfrak{p}_7$	70	f_{11}	1	-2	-1	-3	1	1	-1	0	-6	1	-5	-4	-6	10	1
$\mathfrak{p}_2\bar{\mathfrak{p}}_5\bar{\mathfrak{p}}_7$	70	f_{12}	-1	0	0	-1	-1	1	1	-7	2	5	9	12	-6	3	-1
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_{19}$	76	$f_{13}*$	-1	1	0	-2	-2	0	0	1	-8	8	4	-2	-4	-6	1

Table 7.4: Rational Newforms for $\mathbb{Q}(\sqrt{-31})$ - Part 1 of 4

$\mathfrak{n}$	$N(\mathfrak{n})$		$\mathfrak{p}_2$	$\bar{\mathfrak{p}}_2$	$\mathfrak{p}_5$	$\bar{\mathfrak{p}}_5$	$\mathfrak{p}_7$	$\bar{\mathfrak{p}}_7$	$\mathfrak{p}_3$	$\mathfrak{p}_{19}$	$\bar{\mathfrak{p}}_{19}$	$\mathfrak{p}_{31}$	$\mathfrak{p}_{41}$	$\bar{\mathfrak{p}}_{41}$	$\mathfrak{p}_{47}$	$\bar{\mathfrak{p}}_{47}$	ε
$\mathfrak{p}_2\bar{\mathfrak{p}}_2^3\mathfrak{p}_5$	80	$f_{14}*$	1	-0	-1	-4	-2	0	4	-6	-4	0	2	6	-6	-12	1
	80	f_{15}	1	-0	1	2	4	0	-2	0	-4	0	2	-6	-12	0	-1
$\mathfrak{p}_2\bar{\mathfrak{p}}_2^3\bar{\mathfrak{p}}_5$	80	f_{16}	-1	-0	4	-1	0	2	4	-8	-2	4	6	-6	12	-2	-1
$\mathfrak{p}_2^4\mathfrak{p}_5$	80	f_{17}	-0	-1	1	-2	0	0	2	-4	-4	-8	10	-6	8	-8	1
$\mathfrak{p}_2^4\bar{\mathfrak{p}}_5$	80	f_{18}	+0	-1	-2	1	0	-4	2	0	8	-4	-6	-6	-8	4	-1
$\mathfrak{p}_2\bar{\mathfrak{p}}_{41}$	82	f_{19}	-1	0	-3	0	-1	2	-2	5	-1	5	6	-1	6	3	1
$\mathfrak{p}_2\mathfrak{p}_7^2$	98	f_{20}	1	1	1	0	-0	-3	-4	1	0	-10	-2	2	-1	-8	1
	98	$f_{21}*$	1	-2	-2	-3	-0	-3	-1	4	6	5	7	8	2	-2	1
$\mathfrak{p}_2^2\mathfrak{p}_5\bar{\mathfrak{p}}_5$	100	f_{22}	-0	1	-1	-1	-4	-2	2	-6	6	-2	10	-10	12	-2	-1
	100	f_{23}	-0	-2	-1	1	-4	-2	5	3	-3	-8	1	5	-12	-8	1
	100	f_{24}	-0	0	1	-1	2	-4	1	-1	-7	8	-3	9	0	-12	1
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_5^2$	100	f_{25}	-1	1	+0	0	4	2	2	-2	4	4	0	-12	0	6	-1
	100	$f_{26}*$	1	1	+0	0	-2	-4	-4	-2	-8	4	6	-6	-6	0	1

Table 7.4: Rational Newforms for $\mathbb{Q}(\sqrt{-31})$ - Part 2 of 4

$\mathfrak{n}$	$N(\mathfrak{n})$		$\mathfrak{p}_2$	$\bar{\mathfrak{p}}_2$	$\mathfrak{p}_5$	$\bar{\mathfrak{p}}_5$	$\mathfrak{p}_7$	$\bar{\mathfrak{p}}_7$	$\mathfrak{p}_3$	$\mathfrak{p}_{19}$	$\bar{\mathfrak{p}}_{19}$	$\mathfrak{p}_{31}$	$\mathfrak{p}_{41}$	$\bar{\mathfrak{p}}_{41}$	$\mathfrak{p}_{47}$	$\bar{\mathfrak{p}}_{47}$	ε
$\mathfrak{p}_2^4\mathfrak{p}_7$	112	f_{27}	-0	-2	-2	1	1	1	3	0	-6	-3	-5	4	-10	-2	1
	112	$f_{28}*$	-0	2	2	-3	1	-3	-1	-4	-6	5	7	-8	-2	2	1
$\mathfrak{p}_2^4\bar{\mathfrak{p}}_7$	112	f_{29}	-0	1	1	-2	-1	-1	3	6	0	3	4	-5	2	10	-1
$\mathfrak{p}_2\bar{\mathfrak{p}}_2^3\mathfrak{p}_7$	112	$f_{30}*$	1	-0	0	-1	-1	-3	1	-6	2	-9	-7	-6	6	12	1
$\mathfrak{p}_{11}$	121	f_{31}	-2	-2	1	1	-2	-2	-5	0	0	7	-8	-8	8	8	-1
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_{31}$	124	f_{32}	1	1	-2	-2	0	0	-6	4	4	-1	-6	-6	-8	-8	1
$\mathfrak{p}_2\bar{\mathfrak{p}}_2^6$	128	f_{33}	-1	-0	-2	2	-2	2	-4	4	4	0	8	8	-2	2	-1
$\mathfrak{p}_2^3\bar{\mathfrak{p}}_2^4$	128	f_{34}	-0	+0	-2	-2	-4	4	-2	-4	4	0	6	6	-12	12	-1
$\mathfrak{p}_7\bar{\mathfrak{p}}_{19}$	133	$f_{35}*$	-1	0	-2	3	-1	3	-1	-2	-1	-1	-7	-10	6	-2	1
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_5\mathfrak{p}_7$	140	$f_{36}*$	-1	1	1	-4	-1	-2	-2	6	4	0	4	-12	-12	-2	1
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_5\bar{\mathfrak{p}}_7$	140	f_{37}	1	1	-1	0	2	1	4	2	-4	-4	-6	6	-6	12	-1
$\mathfrak{p}_2^2\mathfrak{p}_5\mathfrak{p}_7$	140	$f_{38}*$	-0	0	1	-1	-1	1	1	-6	-2	3	7	-6	0	-2	1
$\mathfrak{p}_2\bar{\mathfrak{p}}_{71}$	142	f_{39}	1	-1	-2	2	-4	-4	-2	0	-4	8	6	2	0	0	-1
$\mathfrak{p}_2^3\bar{\mathfrak{p}}_2\mathfrak{p}_3$	144	f_{40}	-0	-1	3	-3	4	0	-1	7	-1	4	-8	-12	7	9	-1

Table 7.4: Rational Newforms for $\mathbb{Q}(\sqrt{-31})$ - Part 3 of 4

$\mathfrak{n}$	$N(\mathfrak{n})$		$\mathfrak{p}_2$	$\bar{\mathfrak{p}}_2$	$\mathfrak{p}_5$	$\bar{\mathfrak{p}}_5$	$\mathfrak{p}_7$	$\bar{\mathfrak{p}}_7$	$\mathfrak{p}_3$	$\mathfrak{p}_{19}$	$\bar{\mathfrak{p}}_{19}$	$\mathfrak{p}_{31}$	$\mathfrak{p}_{41}$	$\bar{\mathfrak{p}}_{41}$	$\mathfrak{p}_{47}$	$\bar{\mathfrak{p}}_{47}$	ε
$\mathfrak{p}_2\bar{\mathfrak{p}}_2^4\mathfrak{p}_5$	160	f_{41}	-1	+0	-1	-2	-2	-2	0	0	4	8	0	8	6	6	1
	160	f_{42}	1	+0	-1	4	-2	4	0	6	-8	-4	6	2	-6	0	-1
	160	f_{43}	1	-0	1	-2	0	0	2	4	4	8	10	-6	-8	8	-1
$\mathfrak{p}_2^3\bar{\mathfrak{p}}_2^2\mathfrak{p}_5$	160	$f_{44}*$	-0	-0	-1	-2	2	0	-2	-2	-2	10	6	-6	10	0	1
$\mathfrak{p}_5^2\bar{\mathfrak{p}}_7$	175	$f_{45}*$	-1	1	-0	-2	0	1	0	2	-2	4	-2	-2	2	8	1
	175	$f_{46}*$	-1	-1	-0	2	0	1	0	-2	2	-4	-2	-2	-2	8	1
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_{47}$	188	$f_{47}*$	-1	-1	3	-3	-4	-4	-5	8	5	-4	6	3	9	-1	1
$\mathfrak{p}_2\bar{\mathfrak{p}}_5\mathfrak{p}_{19}$	190	f_{48}	-1	-1	2	-1	4	0	-2	1	-4	0	2	6	8	0	-1
$\mathfrak{p}_2\mathfrak{p}_{97}$	194	$f_{49}*$	-1	0	-3	0	-1	-4	1	-4	-4	-4	-3	-6	12	-9	-1
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_7\bar{\mathfrak{p}}_7$	196	f_{50}	-1	-1	0	0	1	1	-2	2	2	-4	6	6	-12	-12	1
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_7^2$	196	f_{51}	1	1	-2	2	-0	2	4	4	-4	0	-8	8	2	-2	-1
	196	$f_{52}*$	-1	1	3	0	+0	-1	4	-7	8	2	6	6	3	0	-1
$\mathfrak{p}_2^2\bar{\mathfrak{p}}_2\mathfrak{p}_5\bar{\mathfrak{p}}_5$	200	f_{53}	-0	-1	1	-1	-4	2	-2	2	2	-10	-6	6	12	-6	1
$\mathfrak{p}_2^3\mathfrak{p}_5\bar{\mathfrak{p}}_5$	200	f_{54}	-0	-2	1	-1	0	-2	-1	1	-1	0	1	-3	8	4	1

Table 7.4: Rational Newforms for $\mathbb{Q}(\sqrt{-31})$ - Part 4 of 4

$\mathfrak{n}$	$N(\mathfrak{n})$	a_1	a_2	a_3	a_4	a_6	Rank
$\mathfrak{p}_2\mathfrak{p}_5$	10	1	$-\omega-1$	1	$\omega-3$	1	0
$\mathfrak{p}_2\mathfrak{p}_7$	14	$\omega+1$	0	1	$-\omega-1$	0	0
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_5$	20	ω	$-\omega+1$	ω	$-\omega$	0	1
	20						
$\mathfrak{p}_2^3\bar{\mathfrak{p}}_2^2$	32	0	-1	0	$-\omega+3$	-3	1
$\mathfrak{p}_2^4\bar{\mathfrak{p}}_2$	32	0	0	0	621	$-2916\omega-10638$	0
$\mathfrak{p}_7^2$	49	$\omega+1$	1	1	$-2\omega-4$	$-\omega+2$	0
$\mathfrak{p}_2\mathfrak{p}_5^2$	50	0	0	0	$-25920\omega-10395$	$-3981312\omega+3297078$	0
$\mathfrak{p}_2\bar{\mathfrak{p}}_{31}$	62						
$\mathfrak{p}_2^4\bar{\mathfrak{p}}_2^2$	64	0	$\omega+1$	0	$\omega-2$	-1	1
$\mathfrak{p}_2\mathfrak{p}_5\mathfrak{p}_7$	70	$-\omega+1$	$-\omega+1$	1	ω	$-\omega+1$	1
$\mathfrak{p}_2\bar{\mathfrak{p}}_5\bar{\mathfrak{p}}_7$	70	$\omega+1$	0	1	0	0	0
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_{19}$	76						

Table 7.5: Elliptic Curves over $\mathbb{Q}(\sqrt{-31})$ - Part 1 of 4

$\mathfrak{n}$	$N(\mathfrak{n})$	a_1	a_2	a_3	a_4	a_6	Rank
$\mathfrak{p}_2\bar{\mathfrak{p}}_2^3\mathfrak{p}_5$	80						
	80	0	0	0	$-324\omega + 3429$	$-25812\omega - 17226$	2
$\mathfrak{p}_2\bar{\mathfrak{p}}_2^3\bar{\mathfrak{p}}_5$	80	0	0	0	1917	$-11664\omega + 5886$	0
$\mathfrak{p}_2^4\mathfrak{p}_5$	80	ω	ω	ω	$-\omega - 3$	$-2\omega + 2$	1
$\mathfrak{p}_2^4\bar{\mathfrak{p}}_5$	80	0	0	0	$1728\omega - 18603$	$-95364\omega + 495882$	0
$\mathfrak{p}_2\bar{\mathfrak{p}}_{41}$	82	$\omega + 1$	$\omega - 1$	0	$-2\omega - 3$	3	1
$\mathfrak{p}_2\mathfrak{p}_7^2$	98	1	$\omega + 1$	1	$\omega - 2$	-1	1
	98						
$\mathfrak{p}_2^2\mathfrak{p}_5\bar{\mathfrak{p}}_5$	100	0	0	0	$-675\omega - 4968$	$28782\omega + 123984$	0
	100	0	$\omega - 1$	ω	-5	$-\omega + 1$	1
	100	0	0	0	$648\omega + 216$	$972\omega - 24732$	1
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_5^2$	100	0	0	0	$-1485\omega - 29835$	$-77166\omega - 1798146$	0
	100						

Table 7.5: Elliptic Curves over $\mathbb{Q}(\sqrt{-31})$ - Part 2 of 4

$\mathfrak{n}$	$N(\mathfrak{n})$	a_1	a_2	a_3	a_4	a_6	Rank
$\mathfrak{p}_2^4\mathfrak{p}_7$	112	0	0	$-\omega+2$	$3\omega-8$	$-\omega-1$	1
	112						
$\mathfrak{p}_2^4\bar{\mathfrak{p}}_7$	112	$-\omega+2$	1	0	-4	ω	0
$\mathfrak{p}_2\bar{\mathfrak{p}}_2^3\mathfrak{p}_7$	112						
$\mathfrak{p}_{11}$	121	0	-1	1	0	0	0
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_{31}$	124	1	-1	1	-1	1	1
$\mathfrak{p}_2\bar{\mathfrak{p}}_2^6$	128	$-\omega+1$	-1	0	-1	$-2\omega+3$	0
$\mathfrak{p}_2^3\bar{\mathfrak{p}}_2^4$	128	0	$\omega+1$	0	ω	0	0
$\mathfrak{p}_7\bar{\mathfrak{p}}_{19}$	133						
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_5\mathfrak{p}_7$	140						
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_5\bar{\mathfrak{p}}_7$	140	1	1	1	$\omega-5$	$2\omega-5$	0
$\mathfrak{p}_2^2\mathfrak{p}_5\mathfrak{p}_7$	140						
$\mathfrak{p}_2\bar{\mathfrak{p}}_{71}$	142	1	1	1	$-\omega$	$-\omega+1$	0
$\mathfrak{p}_2^3\bar{\mathfrak{p}}_2\mathfrak{p}_3$	144	0	0	0	$-1971\omega-3672$	$-78354\omega-22896$	0

Table 7.5: Elliptic Curves over $\mathbb{Q}(\sqrt{-31})$ - Part 3 of 4

$\mathfrak{p}_2\bar{\mathfrak{p}}_2^4\mathfrak{p}_5$	160	$\omega+1$	1	0	ω	0	1
	160	$\omega+1$	1	$\omega+1$	$-2\omega+2$	$-\omega+3$	0
	160	0	0	0	$-1323\omega+5400$	$-347382\omega-148176$	0
$\mathfrak{p}_2^3\bar{\mathfrak{p}}_2^2\mathfrak{p}_5$	160						
$\mathfrak{p}_5^2\bar{\mathfrak{p}}_7$	175						
	175						
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_{47}$	188						
$\mathfrak{p}_2\bar{\mathfrak{p}}_5\mathfrak{p}_{19}$	190	1	ω	1	1	$2\omega+2$	0
$\mathfrak{p}_2\mathfrak{p}_{97}$	194						
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_7\bar{\mathfrak{p}}_7$	196	1	0	1	-1	0	1
$\mathfrak{p}_2\bar{\mathfrak{p}}_2\mathfrak{p}_7^2$	196	0	0	0	$17739\omega+35613$	$-715878\omega+6711606$	0
	196						
$\mathfrak{p}_2^2\bar{\mathfrak{p}}_2\mathfrak{p}_5\bar{\mathfrak{p}}_5$	200	0	0	0	$-5427\omega-19224$	$-2419794\omega+3211920$	1
$\mathfrak{p}_2^3\mathfrak{p}_5\bar{\mathfrak{p}}_5$	200	0	0	0	$108\omega+756$	$29052\omega+44388$	1

Table 7.5: Elliptic Curves over $\mathbb{Q}(\sqrt{-31})$ - Part 4 of 4

Appendix A

Tables A.1 and A.2 list all prime ideals in the ring of integers of $\mathbb{Q}(\sqrt{-23})$ and $\mathbb{Q}(\sqrt{-31})$, with norm up to 200. Where there are two ideals of a particular norm, the first prime ideal listed is $\mathfrak{p}_p$ and the second is $\bar{\mathfrak{p}}_p$.

$Norm(\mathfrak{p})$	$\mathfrak{p}$
2	$\langle 2, \omega \rangle, \langle 2, \omega + 1 \rangle$
3	$\langle 3, \omega + 2 \rangle, \langle 3, \omega \rangle$
13	$\langle 13, \omega + 8 \rangle, \langle 13, \omega + 4 \rangle$
23	$\langle 2\omega - 1 \rangle$
25	$\langle 5 \rangle$
29	$\langle 29, \omega + 10 \rangle, \langle 29, \omega + 18 \rangle$
31	$\langle 31, \omega + 7 \rangle, \langle 31, \omega + 23 \rangle$
41	$\langle 41, \omega + 25 \rangle, \langle 41, \omega + 15 \rangle$
47	$\langle 47, \omega + 33 \rangle, \langle 47, \omega + 13 \rangle$
49	$\langle 7 \rangle$
59	$\langle 2\omega + 5 \rangle, \langle 2\omega - 7 \rangle$
71	$\langle 71, \omega + 20 \rangle, \langle 71, \omega + 50 \rangle$
73	$\langle 73, \omega + 29 \rangle, \langle 73, \omega + 43 \rangle$
101	$\langle 4\omega + 1 \rangle, \langle 4\omega - 5 \rangle$
121	$\langle 11 \rangle$
127	$\langle 127, \omega + 99 \rangle, \langle 127, \omega + 27 \rangle$
131	$\langle 131, \omega + 48 \rangle, \langle 131, \omega + 82 \rangle$
139	$\langle 139, \omega + 122 \rangle, \langle 139, \omega + 16 \rangle$
151	$\langle 151, \omega + 108 \rangle, \langle 151, \omega + 42 \rangle$
163	$\langle 163, \omega + 100 \rangle, \langle 163, \omega + 62 \rangle$
167	$\langle 2\omega + 11 \rangle, \langle 2\omega - 13 \rangle$

173	$\langle 4\omega+7\rangle, \langle 4\omega-11\rangle$
179	$\langle 179, \omega+113\rangle, \langle 179, \omega+65\rangle$
193	$\langle 193, \omega+19\rangle, \langle 193, \omega+173\rangle$
197	$\langle 197, \omega+137\rangle, \langle 197, \omega+59\rangle$

Table A.1: Prime ideals of norm ≤ 200 in $\mathcal{O}_{\mathbb{Q}(\sqrt{-23})}$

$Norm(\mathfrak{p})$	$\mathfrak{p}$
2	$\langle 2, \omega\rangle, \langle 2, \omega+1\rangle$
5	$\langle 5, \omega+1\rangle, \langle 5, \omega+3\rangle$
7	$\langle 7, \omega+4\rangle, \langle 7, \omega+2\rangle$
9	$\langle 3\rangle$
19	$\langle 19, \omega+5\rangle, \langle 19, \omega+13\rangle$
31	$\langle 2\omega-1\rangle$
41	$\langle 41, \omega+12\rangle, \langle 41, \omega+28\rangle$
47	$\langle 2\omega+3\rangle, \langle 2\omega-5\rangle$
59	$\langle 59, \omega+48\rangle, \langle 59, \omega+10\rangle$
67	$\langle 2\omega+5\rangle, \langle 2\omega-7\rangle$
71	$\langle 71, \omega+26\rangle, \langle 71, \omega+44\rangle$
97	$\langle 97, \omega+77\rangle, \langle 97, \omega+19\rangle$
101	$\langle 101, \omega+63\rangle, \langle 101, \omega+37\rangle$
103	$\langle 103, \omega+62\rangle, \langle 103, \omega+40\rangle$
107	$\langle 107, \omega+20\rangle, \langle 107, \omega+86\rangle$
109	$\langle 109, \omega+94\rangle, \langle 109, \omega+14\rangle$
113	$\langle 113, \omega+79\rangle, \langle 113, \omega+33\rangle$
121	$\langle 11\rangle$
131	$\langle 2\omega+9\rangle, \langle 2\omega-11\rangle$
149	$\langle 4\omega+3\rangle, \langle 4\omega-7\rangle$
157	$\langle 157, \omega+17\rangle, \langle 157, \omega+139\rangle$
163	$\langle 163, \omega+67\rangle, \langle 163, \omega+95\rangle$
169	$\langle 13\rangle$
173	$\langle 4\omega+5\rangle, \langle 4\omega-9\rangle$

191	$\langle 191, \omega + 163\rangle, \langle 191, \omega + 27\rangle$
193	$\langle 193, \omega + 55\rangle, \langle 193, \omega + 137\rangle$

Table A.2: Prime ideals of norm ≤ 200 in $\mathcal{O}_{\mathbb{Q}(\sqrt{-31})}$

Bibliography

[1] A. O. L. Atkin and J. Lehner. Hecke operators on $\Gamma_0(m)$. *Math. Ann.*, 185:134–160, 1970.

[2] A. J. Berrick and M. E. Keating. *An introduction to rings and modules with K-theory in view*, volume 65 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2000.

[3] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[4] D. Bump. *Automorphic forms and representations*, volume 55 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1997.

[5] J. Bygott. *Modular forms over imaginary quadratic number fields*. PhD thesis, Exeter University, 1998.

[6] H. Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[7] J. Cremona. *Modular symbols*. D.Phil. thesis, Oxford University, 1981.

[8] J. E. Cremona. Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields. *Compositio Math.*, 51(3):275–324, 1984.

[9] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997.

[10] J. E. Cremona and M. P. Lingham. Finding all elliptic curves with good reduction outside a given set of primes. Preprint available at http://www.maths.nott.ac.uk/personal/jec/papers/.

[11] C. W. Curtis and I. Reiner. *Representation theory of finite groups and associative algebras.* Pure and Applied Mathematics, Vol. XI. Interscience Publishers, a division of John Wiley & Sons, New York-London, 1962.

[12] J. Elstrodt, F. Grunewald, and J. Mennicke. *Groups acting on hyperbolic space.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 1998. Harmonic analysis and number theory.

[13] G. Faltings. Die Vermutungen von Tate und Mordell. *Jahresber. Deutsch. Math.-Verein.*, 86(1):1–13, 1984.

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

[15] P. F. Kurčanov. Cohomology of discrete groups and Dirichlet series that are related to Jacquet-Langlands cusp forms. *Izv. Akad. Nauk SSSR Ser. Mat.*, 42(3):588–601, 1978.

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

[17] S. Schmitt and H. G. Zimmer. *Elliptic curves*, volume 31 of *de Gruyter Studies in Mathematics.* Walter de Gruyter & Co., Berlin, 2003. A computational approach, With an appendix by Attila Pethö.

[18] B. Setzer. Elliptic curves with good reduction everywhere over quadratic fields and having rational j-invariant. *Illinois J. Math.*, 25(2):233–245, 1981.

[19] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan.* Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1.

[20] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1986.

[21] W. Stein. *Explicit approaches to modular abelian varities.* PhD thesis, University of California at Berkeley, 2000.

[22] M. Stoll and J. E. Cremona. On the reduction theory of binary forms. *J. Reine Angew. Math.*, 565:79–99, 2003.

[23] R. G. Swan. Generators and relations for certain special linear groups. *Advances in Math.*, 6:1–77 (1971), 1971.

[24] A. Weil. *Dirichlet series and automorphic forms.* Springer-Verlag, 1971.

[25] E. Whitley. *Modular forms and elliptic curves over imaginary quadratic number fields.* PhD thesis, Exeter University, 1990.

[26] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.