THE QUATERNIONIC BRIDGE BETWEEN ELLIPTIC CURVES AND HILBERT MODULAR FORMS

Thesis by

Jude Thaddeus U. Socrates

In Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

1993

(Submitted May 17, 1993)

ACKNOWLEDGMENTS

It is with great pleasure that I thank the following persons and institutions for providing me with assistance in one form or another while this thesis was being completed.

To my advisor, Prof. Dinakar Ramakrishnan, for patiently explaining to me the concepts that I needed to know, for helping me choose an interesting problem and for the many hours of stimulating discussions that we had.

To Professors Greg Anderson, Richard Taylor and Jacques Tillouine, for providing useful suggestions to solve my problem.

To Professors Hiroaki Hijikata, Arnold Pizer, Thomas Shemanske and R.G.E. Pinch, for corresponding with me and explaining aspects of their work to me.

To Drs. Michael Aschbacher, Yongchang Zhu and Robert Valenza, for being on my final examination committee and for giving me constructive remarks on my thesis.

To the Alfred P. Sloan Foundation, for awarding me with a Doctoral Dissertation Fellowship during the last year of my stay at Caltech.

To the Campus Computing Organization at Caltech and the *CRAY* User Support Group at the Jet Propulsion Laboratory, for providing me with assistance in using their computing facilities.

To the staff of the Millikan library, especially at the Inter-Library Loan division, for helping me obtain materials that I needed.

To the staff of the Mathematics department for the constant support that they provided.

To my fellow graduate students at Caltech, especially those in the Number Theory group, for the interesting conversations and friendship.

To my family, for giving me their love and encouragement. To my friends, for standing by me.

To Sam Overton, for being my best friend.

To all these people, I extend my deepest gratitude.

Jude Thaddeus U. Socrates
Pasadena, California
May, 1993

ABSTRACT

The main result of this thesis is a matching between an elliptic curve E over $F = \mathbf{Q}(\sqrt{509})$ which has good reduction everywhere, and a normalized holomorphic Hilbert modular eigenform $\mathbf{f}$ for F of weight 2 and full level. The curve E is not F-isogenous to its Galois conjugate E^σ and does not possess potential complex multiplication. The eigenform $\mathbf{f}$ has rational eigenvalues, does not come from the base change of an elliptic modular form, and does not satisfy $\mathbf{f} = \mathbf{f} \otimes \epsilon$ for any quadratic character ϵ of F associated to a degree 2 imaginary extension of F. We show that $a_\wp(E) = a_\wp(\mathbf{f})$ for a large set Σ of σ invariant primes in F. This provides the first known non-trivial example of the conjectural Langlands correspondence (see Section 1.1) in the everywhere unramified case.

The method we use exploits the isomorphism between the spaces of holomorphic Hilbert modular cusp forms and quaternionic cusp forms. The construction of $\mathbf{f}$ involves explicity constructing a maximal order $\mathcal{O}$ in the quaternion algebra $\mathbf{B}/F$ which is ramified precisely at the infinite primes. We determine the type number T_1 of $\mathbf{B}$ as well as the class number H_1 for $\mathcal{O}$, which equals T_1 in our case of interest. We found that for $\mathbf{Q}(\sqrt{509})$, $T_1 = H_1 = 24$. One sees that the space of weight 2 full level cusp forms for F has dimension 23.

The main tools are Θ-series attached to ideals and Brandt matrices $B(\xi)$ for an order in $\mathbf{B}$ for quadratic fields $\mathbf{Q}(\sqrt{m})$ with class number 1 and whose fundamental unit u has norm -1. ($\mathbf{Q}(\sqrt{509})$ is such a field.) The Θ-series gives a way to obtain representatives of left $\mathcal{O}$-ideal classes and hence representatives of maximal orders of different type. The Hecke action on quaternionic cusp forms is given by the modified Brandt matrices $B'(\xi)$, hence a set of simultaneous eigenvectors for these matrices corresponds to the normalized eigenforms for F.

Applying these algorithms to $\mathbf{Q}(\sqrt{509})$, we prove that there are exactly three normalized eigenforms which have rational eigenvalues for all the Hecke operators. We show that for one of these eigenforms $\mathbf{f}$, $a_\wp(\mathbf{f}) \neq a_\wp(\mathbf{f}^\sigma)$ for certain primes $\wp$, proving that $\mathbf{f}$ does not come from base change. We also note that there is another elliptic curve $E'/\mathbf{Q}(\sqrt{509})$ which is isogenous to its Galois conjugate and hence not isogenous to either E or E^σ. We show that $a_\wp(E') = a_\wp(\mathbf{f}')$ $\forall \wp \in \Sigma$, where $\mathbf{f}'$ is the third normalized eigenform that we found above. This is compatible with the expectation that all three non-isogenous elliptic curves correspond to normalized eigenforms with rational eigenvalues.

Contents

Chapter 1

Introduction

1.1 Langlands' Conjecture

Let $m > 1$ be a squarefree integer and $F = \mathbf{Q}(\sqrt{m})$. Let

$$S_2 = \left\{ \begin{array}{c} \text{Normalized holomorphic Hilbert modular eigenforms} \\ \mathbf{f}, \text{ of weight 2 and full level, with coefficients in } \mathbf{Q} \end{array} \right\}$$

and let

$$\mathcal{E} = \left\{ \begin{array}{c} \text{Elliptic curves } E/F, \text{ up to } F\text{-isogeny,} \\ \text{with good reduction everywhere} \end{array} \right\}$$

Conjecture 1.1 (Langlands) *There is a bijection:*

$$S_2 \longleftrightarrow \mathcal{E}$$

which preserves L-series, that is, if $\mathbf{f}$ *corresponds to* E, *then* $L(\mathbf{f}, s) = L(E, s)$. *We say that such an elliptic curve is modular.*

The reader who is not familiar with the terms above can refer to the appendices where these terms are defined. For an exposition of this conjecture, one can see [Ram1], Section 6, and the references cited therein.

The L-series of an elliptic curve uniquely determines it up to isogeny. In fact, a theorem of Faltings states that two elliptic curves E_1 and E_2 are isogenous if and only if the local factors $L_\wp(E_1, s)$ and $L_\wp(E_2, s)$ are equal outside a finite set of primes Σ (see Corollary 2 in [Fal]). In fact, by the Cebotarev Density Theorem, it suffices to take Σ to be any set of Dirichlet density 0. Analogously, by the Strong Multiplicity One Theorem, two normalized eigenforms $\mathbf{f}_1$ and $\mathbf{f}_2$ are equal if and only if the Fourier coefficients $a_\wp(\mathbf{f}_1)$ and $a_\wp(\mathbf{f}_2)$ are equal outside a finite set of primes Σ. By [Ram2], it even suffices to take Σ to be any set of Dirichlet density less than $1/8$.

Langlands' conjecture is far from being proven, although there are some fragmentary results. Given $\mathbf{f} \in S_2$, it is known how to obtain a corresponding $E \in \mathcal{E}$ when one of the following conditions is satisfied:

1. $\mathbf{f}$ is the "base change" of an elliptic modular form ([La]). In this case, the corresponding E is F-isogenous to its Galois conjugate E^σ.

2. $\mathbf{f} = \mathbf{f} \otimes \epsilon$, where ϵ is a quadratic character of F corresponding to a totally imaginary quadratic extension K of F. In this case, the corresponding E has potential complex multiplication (CM).

Given $E \in \mathcal{E}$ which has potential CM, it is also known how to obtain the corresponding $\mathbf{f} \in S_2$. When neither condition above is fulfilled, no examples are known of this correspondence. However, when one considers the natural extension of Conjecture 1.1 to the case of elliptic curves E and weight 2 eigenforms $\mathbf{f}$ of non-trivial conductor, one knows how to associate E to $\mathbf{f}$ when $\mathbf{f}$ is sufficiently ramified at some prime $\wp$, i.e., the local representation of $GL_2(F_\wp)$ defined by $\mathbf{f}$ is supercuspidal or special (see [Ca]).

We should note that for small m, methods of algebraic geometry can be used to determine the dimension of the space of cusp forms, and construct a basis for these (see [HvG]). However, it is difficult to explicitly construct a basis consisting of

simultaneous eigenvectors for the Hecke operators using these methods, nor is it easy to compute their eigenvalues. As we shall see, it will be necessary to choose a large m in order to provide a non-trivial example of Langlands' conjectural correspondence.

Our method (see below) exploits the correspondence between unramified eigenforms of weight 2 and suitable forms on a totally definite quaternion algebra, thereby reducing the problem to calculations on certain finite sets.

1.2 An Approach Using Quaterion Algebras

Quaternion algebras were used in the following manner in order to study the set S_2: Denote by $\mathcal{R}$ the ring of integers of F, $\wp$ a prime ideal of $\mathcal{R}$ and $F_\wp$ the localization of F with respect to $\wp$. Let $\mathbf{B}/F$ be the unique (up to isomorphism) quaternion algebra which is ramified only at the infinite primes of F. This means that the localized algebra $\mathbf{B}_\wp = \mathbf{B} \otimes_F F_\wp$ is isomorphic to the matrix algebra $M_2(F_\wp)$ for all the finite primes $\wp$, and over the infinite places $\infty_i, i = 1, 2$ of F, $\mathbf{B}_{\infty_i}$ is the unique division quaternion algebra over $\mathbf{R}$.

Let $\mathbf{G} = \mathbf{B}^\times$. We construct the double coset space:

$$X = M_{\mathbf{G}} \setminus \mathbf{G}(\mathbf{A}_F^f) \,/\, \mathbf{G}(F),$$

where $\mathbf{A}_F$ is the ring of adeles of F, $\mathbf{A}_F^f$ the subring of finite adeles, and $M_{\mathbf{G}} = \prod_{\wp<\infty} GL_2(\mathcal{R}_\wp)$ is the maximal compact subgroup of

$$\mathbf{G}(\mathbf{A}_F^f) = \{\, (\alpha_\wp)_{\wp<\infty} | \alpha_\wp \in GL_2(F_\wp)\ \forall\ \wp \text{ and } \alpha_\wp \in GL_2(\mathcal{R}_\wp) \text{ for almost all } \wp \,\}.$$

X can be canonically identified with a natural set existing in the global algebra $\mathbf{B}$. First we give some definitions: An *ideal* I of $\mathbf{B}$ is an $\mathcal{R}$-module in $\mathbf{B}$ for which $I \otimes_{\mathcal{R}} F \cong \mathbf{B}$. An element $\mathbf{b} \in \mathbf{B}$ is *integral* or is said to be an integer, if $\mathcal{R}[\mathbf{b}]$ is an $\mathcal{R}$-lattice in $\mathbf{B}$. An *order* in $\mathbf{B}$ is a ring $\mathcal{O}$ consisting of integers and containing $\mathcal{R}$

such that $F\mathcal{O} = \mathbf{B}$. A *left ideal* for an order $\mathcal{O}$ is an ideal I for which $\mathcal{O}I \subset I$. Two ideals I_1 and I_2 are said to be *right equivalent* if $I_1 = I_2\mathbf{b}$ for some $\mathbf{b} \in \mathbf{B}^\times$. Similarly, two orders $\mathcal{O}_1$ and $\mathcal{O}_2$ are *of the same type* if $\mathcal{O}_1 = \mathbf{b}\mathcal{O}_2\mathbf{b}^{-1}$ for some $\mathbf{b} \in \mathbf{B}^\times$. The number of right equivalence classes of left $\mathcal{O}$-ideals is called the *class number* H_1 *of* $\mathcal{O}$ and the number of type classes of maximal orders of $\mathbf{B}$ is called the *type number* T_1 *of* $\mathbf{B}$. Both of these numbers are actually finite (for any order $\mathcal{O}$).

Fact: The set X is canonically identified with the right equivalence classes of left $\mathcal{O}$-ideals where $\mathcal{O}$ is any maximal order of $\mathbf{B}$. Denote by

$$S = \{\mathbf{f} : X \to \mathbf{C}\}/\{\text{ constant functions on } X\ \}.$$

For convenience, we shall refer to the elements of S as *quaternionic cusp forms*, though this term is not usually restricted to this special infinity type and ramification. For details, one can look at the appendices and the references cited there.

S is also a Hecke module. The action of the Hecke operator $\mathbf{T}_\wp$ on S, where $\wp < \infty$ is given by the following: Let $\pi_\wp$ be a uniformizer for $\mathcal{R}_\wp$, and $g_\wp \in \mathbf{G}(\mathbf{A}_F^f)$ such that the $\wp$-th component of $g_\wp$ is $\begin{bmatrix} \pi_\wp & 0 \\ 0 & 1 \end{bmatrix}$, and 1 otherwise. Since $GL_2(\mathcal{R}_\wp)$ is open and compact in $GL_2(\mathcal{F}_\wp)$, we can decompose as a finite disjoint union:

$$\left(\prod_{\wp<\infty} GL_2(\mathcal{R}_\wp)\right) g_\wp \left(\prod_{\wp<\infty} GL_2(\mathcal{R}_\wp)\right) = \coprod_{i=1}^{n} \left(\prod_{\wp<\infty} GL_2(\mathcal{R}_\wp)\right) g_i.$$

Denote by $R_\wp$ a complete set of inequivalent representatives of $\mathcal{R}_\wp/\pi_\wp$. A classical result states that we can choose the set $\{g_i\}$ to be

$$\left\{ \begin{bmatrix} \pi_\wp & \alpha \\ 0 & 1 \end{bmatrix} \;\middle|\; \alpha \in R_\wp \right\} \bigcup \left\{ \begin{bmatrix} 1 & 0 \\ 0 & \pi_\wp \end{bmatrix} \right\}.$$

Define, for $\mathbf{f} \in S$, $h \in \mathbf{G}(\mathbf{A}_\mathcal{F}^f)$:

$$\left(\mathbf{T}_\wp(\mathbf{f})\right)(h) = \sum_{i=1}^{n} \mathbf{f}(g_i h).$$

One sees that this descends to a well-defined action on S.

Let $\mathcal{S}$ be the **C**-vector space of holomorphic Hilbert modular cusp forms **f** of weight 2 and full level. $\mathcal{S}$ is a multiplicity free direct sum of simultaneous 1-dimensional Hecke eigenspaces. A similar decomposition holds for S. By Jacquet, Langlands and Shimizu (see [GJ], Theorem 8.3), there is a Hecke-equivariant correspondence:

$$\mathcal{S} \longleftrightarrow S$$

Thus, we have reduced the problem to computations involving the elements of the finite set X!

The exact manner in which $\mathcal{S}$ corresponds to S will be exploited in this thesis in order to construct *Brandt matrices* $B(\xi)$ and modified Brandt matrices $B'(\xi)$, which are families of rational matrices indexed by $\xi \in \mathcal{R}_{>>0}$, the totally positive elements of $\mathcal{R}$. (see Chapter 8). These are objects that were first defined over **Q** and later used in order to construct cusp forms for congruence subgroups of $SL_2(\mathbf{Z})$.

Note that the construction of quaternionic cusp forms can be generalized to a number field $\mathcal{F}$ of *even* degree n over **Q**, and **B** the quaternion algebra over $\mathcal{F}$ which is the division algebra only at the infinite primes.

1.3 Results

Let $F = \mathbf{Q}(\sqrt{509})$. The main result of this thesis is a matching

$$E \longleftrightarrow \mathbf{f}.$$

E is an elliptic curve over F which has good reduction everywhere, is not F-isogenous to its Galois conjugate and does not possess potential CM (see Chapter 2). $\mathbf{f}$ is a weight 2, full level holomorphic eigenform with rational eigenvalues, does not come from the base change of an elliptic modular form, and does not satisfy $\mathbf{f} = \mathbf{f} \otimes \epsilon$ for any quadratic character ϵ of F associated to a degree 2 imaginary extension of F (see Chapter 3). (These properties are analogous to those of the elliptic curve E.) We prove that

$$a_{\wp}(E) = a_{\wp}(\mathbf{f})$$

for a large set Σ of σ-invariant primes in F. This lends evidence to Conjecture 1.1. This also gives the first known non-trivial correspondence in the everywhere unramified case. In the future, we plan to prove that the Euler factors of the L-series for these two objects are equal for *all* primes of F.

By the results of [T], [Ca], and also of [BR], one knows that there exists an irreducible, continuous representation:

$$\sigma_\ell : \mathrm{Gal}(\overline{\mathbf{Q}}/F) \longrightarrow GL_2(\mathbf{Q}_\ell)$$

such that $\mathrm{tr}(\sigma_\ell(\mathbf{f})(\mathrm{Frob}_\wp)) = a_\wp(\mathbf{f})$ for all $\wp$. For the equality of L-series, we need to show that the traces of Frobenii on $\sigma_\ell(\mathbf{f})$ coincide with those on $\sigma_\ell(E)$, the Galois representation on $T_\ell(E) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$, where $T_\ell(E)$ is the Tate module of E. The existing method of Faltings and Serre do not apply directly. See Section 10.5 for further details.

Our **construction of f** involves explicity studying the object S of the previous section. The key steps are as follows:

We first find relations for the quaternion algebra $\mathbf{B}$ over $\mathbf{Q}(\sqrt{509})$ which is ramified only at the infinite primes. We also construct a basis for a maximal order in $\mathbf{B}$ which is actually valid for any $F = \mathbf{Q}(\sqrt{m})$ for which $m \equiv 5 \bmod 8$, such as $m = 509$ (see Chapter 4).

We find an effectively computable formula for the type number T_1 of $\mathbf{B}$ as well as the class number H_1 for the maximal order $\mathcal{O}$, which equals T_1 in our case of interest (see Chapter 5). This general formula is applicable also for other real quadratic fields when certain conditions are met. We find that for $\mathbf{Q}(\sqrt{509})$, $T_1 = H_1 = 24$. Thus one sees that the space of weight 2 cusp forms for F of full level is of dimension 23.

We extend the definition of Θ-series attached to ideals in an algebra $\mathbf{B}$ defined over a quadratic fields F with $h(F) = 1$ and whose fundamental unit u has norm -1, such as $\mathbf{Q}(\sqrt{509})$ (see Chapter 6). We develop algorithms to explicitly construct this object, which first require us to find a complete set of representatives of right equivalence classes of left $\mathcal{O}$-ideals. (see Chapter 7). The Θ-series give us a way to obtain such representatives. Once these are found, the right orders of these ideals are automatically representatives of maximal orders belonging to different type classes.

For fields satisfying the properties in the previous paragraph, we also define Brandt matrices $B(\xi)$ and modified Brandt matrices $B'(\xi)$ for an order in $\mathbf{B}$ (see Chapter 8). We show that the Hecke action on S is given by the $B'(\xi)$, hence a set of simultaneous eigenvectors for these matrices corresponds to the normalized eigenforms in S_2. In other words, an eigenvector $\mathbf{v}$ corresponds to an eigenform $\mathbf{f}$ such that the eigenvalue of $\mathbf{v}$ with respect to $B'(\pi)$ equals the eigenvalue of $\mathbf{f}$ with respect to the $\wp$-th Hecke operator, where $\wp = (\pi)$ and $\pi \in \mathcal{R}_{>>0}$. This completes the algorithm to find $\mathbf{f}$.

In Chapter 9, we apply these algorithms to $F = \mathbf{Q}(\sqrt{509})$ in order to construct quaternionic cusp forms for F. We show that there are exactly three one-dimensional simultaneous eigenspaces $< \mathbf{v}_1 >, < \mathbf{v}_2 >$ and $< \mathbf{v}_3 >$ which have rational eigenvalues

for the modified Brandt matrices $B'(\xi)$ for all $\xi \in F_{>>0}$. In fact, the generators $\mathbf{v}_i$, $i = 1 \ldots 3$, can be chosen to have integer entries. We also compute the corresponding eigenvalues of these spaces for a large set Σ of primes in F.

In Chapter 10, we complete the proofs of our main result. We show that the eigenform $\mathbf{f}$ corresponding to $\mathbf{v}_1$ satisfies $a_\wp(\mathbf{f}) \neq a_\wp(\mathbf{f}^\sigma)$ for certain primes $\wp$, where σ is the nontrivial automorphism of F. This proves that $\mathbf{f}$ is not the base change of an elliptic modular form. In this regard, we note that there is another elliptic curve $E'/\mathbf{Q}(\sqrt{509})$ which has good reduction everywhere, is isogenous to its Galois conjugate and hence not isogenous to either E or E^σ. We found that $a_\wp(E') = a_\wp(\mathbf{f}')$ for the same set of primes Σ, where the eigenform $\mathbf{f}'$ corresponds to $\mathbf{v}_3$. It is observed that $a_\wp(\mathbf{f}') = a_\wp(\mathbf{f}'^\sigma)$. This is indeed as expected.

Notation. We shall denote by m a positive squarefree integer, $F = \mathbf{Q}(\sqrt{m})$, and $\mathcal{R}$ the ring of integers of F. If $m \equiv 1 \bmod 4$, we let $\theta = \frac{1+\sqrt{m}}{2}$, so $\mathcal{R} = \mathbf{Z}[\theta]$. For any number field $\mathcal{F}$, we denote by $h(\mathcal{F})$ the order of its ideal class group $\mathrm{Cl}(\mathcal{F})$, and $h^+(\mathcal{F})$ the order of the narrow class group $\mathrm{Cl}^+(\mathcal{F})$ (i.e., the group of fractional ideals modulo the subgroup of principal ideals with a totally positive generator). We shall fix an algebraic closure $\overline{\mathbf{Q}}$ which will contain all the number fields that we will consider. Results which begin with a letter refer to a statement in the Appendix (i.e., Proposition D.4 is found in Appendix D).

Chapter 2

The Interesting Elliptic Curve

In this chapter, we show that there is at least one totally real quadratic field where we can find an elliptic curve which does not fall in either of the two categories in Section 1.1. The following elliptic curve is in a table found in R.G.E. Pinch's thesis ([Pin]), among other curves which have good reduction everywhere over certain quadratic fields. We show below that E is not F-isogenous to its Galois conjugate. This is also noted (without proof) in [Cr], where one also finds a Weierstrass equation for an elliptic curve E' which *is* F-isogenous to its Galois conjugate. We shall see this equation for E' in the last chapter.

Theorem 2.1 *Let $F = \mathbf{Q}(\sqrt{509})$ and $\theta = \frac{1+\sqrt{509}}{2}$. There exists an elliptic curve E defined over F such that:*

1. *E has good reduction everywhere,*
2. *E is not isogenous over F to its Galois conjugate, and*
3. *E does not possess potential complex multiplication.*

A minimal Weierstrass equation for E is given by:

$$E : y^2 - xy - \theta y = x^3 + (2 + 2\theta)x^2 + (162 + 3\theta)x + 71 + 34\theta$$

Proof. We shall use the notation in Appendix B.2. Using the relation $\theta^2 = \theta + 127$, the associated values for E are:

$$
\begin{aligned}
b_2 &= a_1^2 + 4a_2 \\
&= (-1)^2 + 4(2 + 2\theta) \\
&= 9 + 8\theta \\
b_4 &= 2a_4 + a_1a_3 \\
&= 2(162 + 3\theta) + (-1)(-\theta) \\
&= 324 + 7\theta \\
b_6 &= a_3^2 + 4a_6 \\
&= (-\theta)^2 + 4(71 + 34\theta) \\
&= \theta + 127 + 284 + 136\theta \\
&= 411 + 137\theta \\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\
&= (-1)^2(71 + 34\theta) + 4(2 + 2\theta)(71 + 34\theta) - (-1)(-\theta)(162 + 3\theta) + \\
&\quad (2 + 2\theta)(-\theta)^2 - (162 + 3\theta)^2 \\
&= (71 + 34\theta) + 4(142 + 210\theta + 68(\theta + 127)) - (162\theta + 3(\theta + 127)) + \\
&\quad (2 + 2\theta)(\theta + 127) - (26244 + 972\theta + 9(\theta + 127)) \\
&= (71 + 34\theta) + 4(8778 + 278\theta) - (381 + 165\theta) + \\
&\quad (2\theta + 254 + 254\theta + 2\theta^2) - (27387 + 981\theta) \\
&= 7669 + 256\theta + 2(\theta + 127) \\
&= 7923 + 258\theta \\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\
&= -(9 + 8\theta)^2(7923 + 258\theta) - 8(324 + 7\theta)^3 - 27(411 + 137\theta)^2 \\
&\quad +9(9 + 8\theta)(324 + 7\theta)(411 + 137\theta) \\
&= -(81 + 144\theta + 64\theta^2)(7923 + 258\theta) \\
&\quad -8(104976 + 4536\theta + 49\theta^2)(324 + 7\theta)
\end{aligned}
$$

$$
\begin{aligned}
& -27(168921 + 112614\theta + 18769\theta^2) \\
& +9(2916 + 63\theta + 2592\theta + 56\theta^2)(411 + 137\theta) \\
= \; & -(8209 + 208\theta)(7923 + 258\theta) - 8(104976 + 4536\theta + 49\theta + 6223)(324 + 7\theta) \\
& -27(168921 + 112614\theta + 18769\theta + 2383663) \\
& +9(2916 + 2655\theta + 56\theta + 7112)(411 + 137\theta) \\
= \; & -(65039907 + 1647984\theta + 2117922\theta + 53664\theta^2) \\
& -8(111199 + 4585\theta)(324 + 7\theta) - 27(2552584 + 131383\theta) \\
& +9(10028 + 2711\theta)(411 + 137\theta) \\
= \; & -(65039907 + 3765906\theta + 53664\theta + 6815328) \\
& -8(36028476 + 1485540\theta + 778393\theta + 32095\theta^2) \\
& -27(2552584 + 131383\theta) + 9(412150813738836\theta + 1114221\theta + 371407\theta^2) \\
= \; & -(71855235 + 3819570\theta) - 8(36028476 + 2263933\theta + 32095\theta + 4076065) \\
& -27(2552584 + 131383\theta) + 9(4121508 + 2488057\theta + 371407\theta + 47168689) \\
= \; & -(71855235 + 3819570\theta) - 8(40104541 + 2296028\theta) \\
& -27(2552584 + 131383\theta) + 9(51290197 + 2859464\theta) \\
= \; & 442 + 41\theta
\end{aligned}
$$

Here, $\Delta = u$, the fundamental unit of F, with $N(u) = -1$. Thus, the equation given for E is indeed minimal, and since the discriminant is a unit in $\mathcal{R}$, E has good reduction everywhere.

Next we show that E is not isogenous to E^σ. Suppose not. Then the local factors of the L-series of E and E^σ will be the same for all the primes (see Section B.9). However, we will presently show that for either of the prime ideals $\wp \mid (5)$, the reductions $\tilde{E}$ and $\tilde{E}^\sigma$ do not have the same number of points in the residue field $\mathcal{R}/\wp \cong \mathbf{Z}/5$. This contradicts the equality of the local factors. Note that $509 \equiv 4 = 2^2 \bmod 5$, so we choose $\wp = (5, 2 + \sqrt{509}) = (5, 1 + 2\theta)$. Now, by Proposition E.5, $\theta \equiv \frac{5-1}{2}(2-1) = 2 \bmod \wp$, so we have:

$$\begin{array}{rcccccl} a_1 & = & -1 & & & \equiv & 4 \mod \wp \\ a_3 & = & -\theta & \equiv & -2 & \equiv & 3 \\ a_2 & = & 2+2\theta & \equiv & 2+2\cdot 2 & \equiv & 1 \\ a_4 & = & 162+3\theta & \equiv & 2+3\cdot 2 & \equiv & 3 \\ a_6 & = & 71+34\theta & \equiv & 1+4\cdot 2 & \equiv & 4 \end{array}$$

hence the reduced curve is:

$$\tilde{E}/(\mathbf{Z}/5) : y^2 + 4xy + 3y = x^3 + x^2 + 3x + 4$$

To find the number of affine points on the reduced curve, we simply let $x = x_\circ = 0 \ldots 4$ to obtain polynomials $f(y) = y^2 + by + c = 0$. We compute the discriminant $\mathrm{disc}(f) \equiv b^2 + c \bmod 5$. The number of affine points with x-coordinate $x_\circ$ is <u>two</u> if $\mathrm{disc}(f)$ is 1 or 4 (the squares of $(\mathbf{Z}/5)^\times$), <u>one</u> if $\mathrm{disc}(f)$ is 0, and <u>zero</u> if $\mathrm{disc}(f)$ is 2 or 3. We tabulate these values below:

$x_\circ$	$f(y)$	$\mathrm{disc}(f)$	# points $(x_\circ, y)$
0	y^2+3y+1	0	1
1	y^2+2y+1	0	1
2	y^2+y+3	4	2
3	y^2+1	4	2
4	y^2+4y+4	0	1

Hence there are 7 finite points in $\tilde{E}/(\mathbf{Z}/5)$.

Similarly, for $\tilde{E}^\sigma/(\mathbf{Z}/5)$ we obtain the following coefficients:

$$\begin{array}{lllll} a_1^\sigma = -1 & & & \equiv 4 & \bmod \wp \\ a_3^\sigma = -1+\theta & \equiv 4+2 & & \equiv 1 & \\ a_2^\sigma = 4-2\theta & \equiv 4-2\cdot 2 & & \equiv 0 & \\ a_4^\sigma = 165-3\theta & \equiv 2\cdot 2 & & \equiv 4 & \\ a_6^\sigma = 105-34\theta & \equiv 1\cdot 2 & & \equiv 2 & \end{array}$$

hence the reduced curve is:

$$\tilde{E}^\sigma/(\mathbf{Z}/5) : y^2 + 4xy + y = x^3 + 4x + 2$$

Applying the same procedure above to find the number of affine points on this curve, we get:

$x_\circ$	$f(y)$	disc(f)	# points $(x_\circ, y)$
0	y^2+y+3	4	2
1	y^2+3	3	0
2	y^2+4y+2	3	0
3	y^2+3y+4	3	0
4	y^2+2y+3	2	0

Hence there are only 2 finite points in $\tilde{E}^\sigma/(\mathbf{Z}/5)$, and we conclude that E is not isogenous to E^σ.

Though it is not needed in the proof of Theorem 2.1, we can use the same method above in order to compute the number of points in the reduced curve for various primes of F. We include both inert primes and split primes. As expected, the number of points on the reduced curves is the same for both E and E^σ at *inert* primes, since σ gives a bijection of these points. For split primes $\wp \mid (p)$, we counted points on the reduced curves only for one of the primes $\wp$, and included the squareroot of m modulo p in the indicated column. The entries in the column for E and E^σ exchange values for $\wp^\sigma$. Using a computer to do the calculations, we obtain the following table:

Table 2.1. Cardinality of Reduced Curves for E and E^σ

p	$\sqrt{m} \bmod p^*$	$\#E_\wp(k_\wp)$	$\#E^\sigma_\wp(k_\wp)$
3		13	13
5	2	2	7
7		55	55
11	5	8	13
13		168	168
17	4	20	15
19		373	373
23	7	22	27
29	4	29	19
31		979	979
37	18	40	30
41		1699	1699
43	6	47	42
47		2165	2165
53		2828	2828
59		3503	3503
61		3724	3724
67	24	59	74
71	15	64	59
73	12	69	69
79		6273	6273
83	29	74	69
89	8	83	93
97	11	110	90
101	2	111	106
103	32	89	94
107	9	95	110
109	20	115	115
113	31	107	102
127	1	145	120
131		17079	17079
137	57	125	135
139		19563	19563
149		22343	22343

* this column is blank if p is inert in F

To finish the proof of Theorem 2.1, it remains to show that E does not possess potential CM. We first remark that the $h^+(F) = 1$. Our conclusion about E is now a consequence of the following:

Proposition 2.2 *Let $\mathcal{F}$ a totally real number field which satisfies $h^+(\mathcal{F}) = 1$. Let $E/\mathcal{F}$ be an elliptic curve which has good reduction everywhere. Then E does not possess any potential complex multiplication.*

Proof. Suppose $E(\mathbf{C})$ has CM defined over the field $\mathbf{Q}(\sqrt{n})$, where $n < 0$. Consider the field $K = \mathcal{F}(\sqrt{n})$. Then E and its complex multiplications are defined over K. Consider the ℓ-adic representation defined by the Tate module of E/K:

$$\sigma_\ell = \sigma_\ell(E/K) : H \longrightarrow GL_2(\mathbf{Q}_\ell)$$

where $H = \mathrm{Gal}(\overline{\mathbf{Q}}/K)$. We construct another representation:

$$\begin{array}{rccc} \sigma_\ell^{[\rho]} & : & H & \longrightarrow & GL_2(\mathbf{Q}_\ell) \\ & & \tau & \longrightarrow & \sigma_\ell(\rho\tau\rho^{-1}) \end{array}$$

where $\mathrm{Aut}(K/\mathcal{F}) = \{1, \rho\}$. Now, since E is actually defined over $\mathcal{F}$, σ_ℓ extends to a representation

$$\tilde{\sigma}_\ell : G \longrightarrow GL_2(\mathbf{Q}_\ell)$$

where $G = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathcal{F})$. However, we note that

$$\tilde{\sigma}_\ell(\rho\tau\rho^{-1}) = \tilde{\sigma}_\ell(\rho)\tilde{\sigma}_\ell(\tau)\tilde{\sigma}_\ell(\rho)^{-1} = \tilde{\sigma}_\ell(\rho)\sigma_\ell(\tau)\tilde{\sigma}_\ell(\rho)^{-1}$$

hence $\sigma_\ell^{[\rho]} \cong \sigma_\ell$.

Since E has CM over K, the representation σ_ℓ is *abelian* (see [Si], p. 109), so $\sigma_\ell = \chi_\ell \oplus \chi'_\ell$ for some Galois characters χ_ℓ, χ'_ℓ of H. It can easily be seen from such a decomposition that, in the obvious notation, $\sigma_\ell^{[\rho]} = \chi_\ell^{[\rho]} \oplus \chi_\ell'^{[\rho]}$ as well. Now, χ_ℓ corresponds to a weight 1 grossencharacter ψ of K, and $\chi_\ell = \chi_\ell^{[\rho]}$ if and only if $\psi(z) = \psi(\overline{z})$ for all $z \in K_\infty^* = \mathbf{C}^*$. But $\psi(z) = z^{-1}$ and $\psi(\overline{z}) = \overline{z}^{-1}$, hence

$\psi(z) \neq \psi(\overline{z})$, so $\chi_\ell \neq \chi_\ell^{[\rho]}$. Thus $\chi'_\ell = \chi_\ell^{[\rho]}$, and so $\sigma_\ell = \chi_\ell \oplus \chi_\ell^{[\rho]}$, hence $\tilde{\sigma}_\ell = \mathrm{Ind}_H^G(\chi_\ell)$. Since the degree of χ_ℓ is 1, we get the formula for the conductor of $\tilde{\sigma}_\ell$:

$$\mathrm{cond}(\tilde{\sigma}_\ell) = N_{\mathcal{F}}^K(\mathrm{cond}(\chi_\ell)) \mid \mathrm{disc}(K/\mathcal{F}) \mid$$

(see [Mar]). Recall, though, that E has good reduction everywhere, so every $\tilde{\sigma}_\ell$ is unramified at all the finite primes. Since $\tilde{\sigma}_\ell$ is ramified at all the primes which divide $\mathrm{cond}(\tilde{\sigma}_\ell)$, we see that $\mathrm{disc}(K/\mathcal{F})$ must be the unit ideal. Thus K is a finite abelian extension of $\mathcal{F}$ where every finite prime of $\mathcal{F}$ is unramified, so K has to be contained in the Hilbert$^+$ Class Field H^+ of $\mathcal{F}$. But H^+ has degree $h^+(\mathcal{F}) = 1$ over $\mathcal{F}$, so $\mathcal{F}$ is its own Hilbert$^+$ Class Field. This is impossible, since $n < 0$. ■

Chapter 3

The Interesting Eigenform

In this chapter, we state the existence of a holomorphic Hilbert modular cusp form $\mathbf{f}$ over F of weight 2 and full level which has properties that are analogous to those of the elliptic curve E that we found in the previous chapter. We shall show in a later chapter that the eigenvalues $a_\wp(\mathbf{f})$ are equal to the coefficients $a_\wp(E)$ for that elliptic curve, for a large set Σ of finite primes $\wp$. This lends evidence to the expectation that $\mathbf{f}$ is modular, and corresponds to E under Langlands' correspondence.

Theorem 3.1 *Let $F = \mathbf{Q}(\sqrt{509})$. There is a holomorphic Hilbert modular cusp form $\mathbf{f}$ over F of weight 2 and full level such that:*

1. *$\mathbf{f}$ is an eigenvector for all the Hecke operators $T_\wp$, and all of its eigenvalues are rational,*
2. *$\mathbf{f}$ does not come from the base change of an elliptic modular form, and*
3. *$\mathbf{f} \neq \mathbf{f} \otimes \epsilon$ for any quadratic character ϵ of F corresponding to some quadratic imaginary extension K of F.*

Parts (1) and (2) of this Theorem will be proved in Section 10.3. Part (3) is a consequence of the following:

Proposition 3.2 *Let* $\mathbf{f}$ *be a holomorphic newform of weight 2 and level* $\mathcal{N}$ *for* F*, a totally real quadratic field. Suppose* $h^+(F) = 1$*. Then* $\mathbf{f} \neq \mathbf{f} \otimes \epsilon$ *for any quadratic character* ϵ *of* F *corresponding to some quadratic imaginary extension* K *of* F*.*

Proof. Suppose that for some quadratic imaginary extension K of F we have $\mathbf{f} = \mathbf{f} \otimes \epsilon$. The holomorphic eigenform $\mathbf{f}$ corresponds to a vector $\tilde{\mathbf{f}}$ and a cuspidal representation (π, V_π) of $GL_2(\mathbf{A}_F)$ which is trivial at the infinite primes such that the representation space V_π of $\pi \cong \otimes'_v \pi_v$ is:

$$V_\pi = < \pi(g)\tilde{\mathbf{f}} \mid g \in GL_2(\mathbf{A}_F) >$$

where $< \cdot >$ means "span of." The condition $\mathbf{f} = \mathbf{f} \otimes \epsilon$ means that $\pi \cong \pi \otimes (\epsilon \circ \det)$. By a theorem of Labesse and Langlands ([LL]), we have an equality of L-series:

$$L(\pi, s) = L(\chi, s)$$

for some grossencharacter χ of the quadratic extension K. (Note that these two L-series are defined over different fields. This equality means that for any place v of F, the v-th Euler factor $L(\pi_v, s)$ equals $\prod_{\omega|v} L(\chi_\omega, s)$.) Moreover, it is known that the conductor of π (cf. [Cas] and [Ge], pp. 73 and 89) in this case is given by:

$$\mathrm{cond}(\pi) = \prod_v \mathrm{cond}(\pi_v) = N_F^K(\mathrm{cond}(\chi)) \mid \mathrm{disc}(K/F) \mid$$

Recall that since $\mathbf{f}$ is of full level, π must be unramified at all the finite primes of F. Thus, $\mathrm{cond}(\pi)$ must be the unit ideal, hence, as in Theorem 2.1, we must have K contained in the Hilbert$^+$ Class Field of F, which is impossible since $h^+(F) = 1$ and F is totally real. ∎

Chapter 4

The Algebra B and A Maximal Order $\mathcal{O}$

From this chapter to Chapter 8, we shall be concerned with developing the theoretical background necessary in order to construct the eigenform $\mathbf{f}$ by using the function space S defined in Chapter 1. This will enable us to perform the necessary calculations for the field $\mathbf{Q}(\sqrt{509})$.

In this chapter, we obtain defining relations for $\mathbf{B}$, the positive definite quaternion algebra which is unramified at all finite primes, over fields $\mathbf{Q}(\sqrt{m})$ with $m \not\equiv 1 \bmod 8$, regardless of class number. We also find that in this same algebra, we can find a basis for a maximal order $\mathcal{O}$ which is expressible in terms of θ and the generators i, j, and $k = ij$, when $m \equiv 5 \bmod 8$. This includes $\mathbf{Q}(\sqrt{509})$.

By the Local-Global Correspondence in Appendix D, the set of left ideal classes of $\mathcal{O}$ is in bijection with the set consisting of the $\mathcal{O}\tilde{x}_i$, where $\tilde{x}_i \in X$ and X is the finite set described in Chapter 1. Here, $\mathcal{O}\tilde{x}_i$ means that ideal J of $\mathbf{B}$ such that $J_\wp = \mathcal{O}_\wp x_{i,\wp}$, where $\tilde{x}_i = (x_{i,\wp})_{\wp<\infty}$. The ideal J exists precisely because of the Local-Global Correspondence. Thus, in principle, one can find a complete set of representatives of left $\mathcal{O}$-ideal classes given a basis for $\mathcal{O}$.

4.1 The Algebra

Theorem 4.1 *Let $m \not\equiv 1 \bmod 8$ be a positive squarefree integer, $F = \mathbf{Q}(\sqrt{m})$. Then*

$$\mathbf{B} = (-1, -1)$$

is the unique quaternion algebra defined over F with $\mathrm{Ram}(\mathbf{B}) = \{\infty_1, \infty_2\}$.

Proof. Recall that the notation $\mathbf{B} = (a, b)$ means that $\mathbf{B}$ has basis $\{1, i, j, ij\}$ over F, where $i^2 = a$, $j^2 = b$ and $ij = -ji$. It is clear that $\mathbf{B} = (-1, -1)$ is positive definite. We shall show that over every finite prime, $\mathbf{B}$ is locally the matrix algebra. Let $\mathbf{B}'$ be the quaternion algebra over $\mathbf{Q}$ given by $\mathbf{B}' = (-1, -1)$. Then $\mathbf{B} = \mathbf{B}' \otimes_{\mathbf{Q}} F$. The isomorphism type of $\mathbf{B}'_p = \mathbf{B}' \otimes_{\mathbf{Q}} \mathbf{Q}_p$ is determined by the Hilbert symbol $(-1, -1)$ in the respective $\mathbf{Q}_p$ (see Appendix D.4). But a simple calculation [Se1, Chapter III.1.2] shows that $(-1, -1) = 1$ if $p \neq 2$ and $(-1, -1) = -1$ for $p = 2$. Since $(-1, -1)$ is clearly positive definite, we see that $\mathrm{Ram}(\mathbf{B}') = \{\infty, 2\}$. Hence for any prime $\wp$ of F which does not divide 2,

$$\mathbf{B}_\wp = \mathbf{B} \otimes_F F_\wp = \mathbf{B}'_p \otimes_{\mathbf{Q}_p} F_\wp = M_2(\mathbf{Q}_p) \otimes_{\mathbf{Q}_p} F_\wp = M_2(F_\wp).$$

Now, if $m \equiv 2$ or $3 \bmod 4$, 2 is ramified in F, and if $m \equiv 5 \bmod 8$, 2 is inert in F. So if $m \not\equiv 1 \bmod 8$, there is only one prime $\wp$ lying over 2. Since $\mathrm{Ram}(\mathbf{B})$ has even cardinality and already contains the two infinite primes, we see that $\mathbf{B}$ is also unramified over the prime dividing 2. ∎

4.2 The Maximal Order

When $m \equiv 5 \bmod 8$, the algebra **B** contains a canonical maximal order:

Theorem 4.2 *Let $m \equiv 5 \bmod 8$, F, $\mathcal{R}$ and θ as usual,* $\mathbf{B} = (-1,-1)$. *Let*

$$\mathcal{O} = \mathcal{R}\left[\frac{1+i+j+k}{2}, \frac{i+\theta j+(1+\theta)k}{2}, j, k\right].$$

Then $\mathcal{O}$ is a maximal order of **B** *(regardless of m!).*

Proof. In the following computations, we let

$$\delta_1 = \frac{1+i+j+k}{2}, \quad \delta_2 = \frac{i+\theta j+(1+\theta)k}{2}.$$

First we prove that $\mathcal{O}$ is an order. Obviously $\mathcal{O}$ is a full lattice in **B**. Next, we show that Hurwitz's quaternions

$$\mathcal{H} = \mathbf{Z}[\,\delta_1,\, i,\, j,\, k\,]$$

is a ring with $\mathbf{Z} \subset \mathcal{H} \subset \mathcal{O}$. Easily, $1 = 2\delta_1 - i - j - k \in \mathcal{H}$, so $\mathbf{Z} \subset \mathcal{H}$. To show that $\mathcal{H} \subset \mathcal{O}$, we only have to prove that $i \in \mathcal{O}$:

$$\begin{aligned} i &= i + (\theta-\theta)j + (1+\theta-(1+\theta))k \\ &= 2\left(\frac{i+\theta j+(1+\theta)k}{2}\right) - \theta j - (1+\theta)k \\ &= 2\delta_2 - \theta j - (1+\theta)k \in \mathcal{O} \end{aligned}$$

We show that $\mathcal{H}$ is closed under multiplication. Since $-1, i, j$ and k are in $\mathcal{H}$, we just have to show that products involving δ_1 are in $\mathcal{H}$:

$$
\begin{aligned}
\delta_1^2 &= (1+i+j+k)(1+i+j+k)/4 \\
&= ((1+i+j+k)+(i+i^2+ji+ki)+ \\
&\quad (j+ij+j^2+kj)+(k+ik+jk+k^2))/4 \\
&= ((1+i+j+k)+(i-1-k+j)+(j+k-1-i)+(k-j+i-1))/4 \\
&= (-2+2i+2j+2k)/4 = (-1+i+j+k)/2 \\
&= -1+\frac{1+i+j+k}{2} \\
&= -1+\delta_1 \in \mathcal{H} \\
\delta_1 i &= \left(\frac{1+i+j+k}{2}\right) i \\
&= (i+i^2+ji+ki)/2 = (i-1-k+j)/2 = (-1+i+j-k)/2 \\
&= \frac{-1-i-j-k}{2}+i+j \\
&= -\delta_1+i+j \in \mathcal{H} \\
i\delta_1 &= i\left(\frac{1+i+j+k}{2}\right) \\
&= (i+i^2+ij+ik)/2 = (i-1+k-j)/2 = (-1+i-j+k)/2 \\
&= \frac{-1-i-j-k}{2}+i+k \\
&= -\delta_1+i+k \in \mathcal{H} \\
\delta_1 j &= \left(\frac{1+i+j+k}{2}\right) j \\
&= (j+ij+j^2+kj)/2 = (j+k-1-i)/2 = (-1-i+j+k)/2 \\
&= \frac{-1-i-j-k}{2}+j+k \\
&= -\delta_1+j+k \in \mathcal{H} \\
j\delta_1 &= j\left(\frac{1+i+j+k}{2}\right) \\
&= (j+ji+j^2+jk)/2 = (j-k-1+i)/2 = (-1+i+j-k)/2 \\
&= \frac{-1-i-j-k}{2}+i+j \\
&= -\delta_1+i+j \in \mathcal{H} \\
\delta_1 k &= \left(\frac{1+i+j+k}{2}\right) k \\
&= (k+ik+jk+k^2)/2 = (k-j+i-1)/2 = (-1+i-j+k)/2
\end{aligned}
$$

$$
\begin{aligned}
&= \frac{-1-i-j-k}{2} + i + k \\
&= -\delta_1 + i + k \in \mathcal{H} \\
k\delta_1 &= k\left(\frac{1+i+j+k}{2}\right) \\
&= (k + ki + kj + k^2)/2 = (k + j - i - 1)/2 = (-1 - i + j + k)/2 \\
&= (-1 - i + (-1+2)j + (-1+2)k)2 \\
&= -\left(\frac{1+i+j+k}{2}\right) + j + k \\
&= -\delta_1 + j + k
\end{aligned}
$$

Next we show that $\mathcal{O}$ is a ring, i.e., the product of δ_2 and any basis element is expressible as an $\mathcal{R}$-linear combination of basis elements. The computations are more confusing than that for $\mathcal{H}$, so we show all the intermediate steps. The factor on the right of the first product is always expanded first. The product is then brought to the form $t_1 + t_2 i + t_3 j + t_4 k$. We often put all these under a common denominator of either 1 or 2. We then bring it to a quaternion which is in $\mathcal{H}$ or of the form $s_1\delta_1 + s_2\delta_2 + s_3 j + s_4 k$. To do the second, we must solve :

$$
\begin{aligned}
t_1 &= s_1/2 \\
t_2 &= s_1/2 + s_2/2 \\
t_3 &= s_1/2 + s_2\theta/2 + s_3 \\
t_4 &= s_1/2 + s_2(1+\theta)/2 + s_4
\end{aligned}
$$

We have tried to show this in a natural manner by expanding the t_i's in terms of the s_i's. One notes that for some products, it is imperative that $m \equiv 5 \bmod 8$ in order for the final expression to have coefficients in $\mathcal{R}$. The actual derivations now follow:

$$
\begin{aligned}
\delta_2^2 &= -\mathbf{nr}(\delta_2) \\
&= -(1 + \theta^2 + (1+\theta)^2)/4 \\
&= -(1 + \theta^2 + 1 + 2\theta + \theta^2)/4 \\
&= -(1 + \theta + \theta^2)/2
\end{aligned}
$$

$$
\begin{aligned}
&= -\frac{1+\theta+\theta+\frac{m-1}{4}}{2} \\
&= -\theta-\left(\frac{m+3}{8}\right) \\
\delta_1\delta_2 &= (1+i+j+k)(i+\theta j+(1+\theta)k)/4 \\
&= ((i+i^2+ji+ki)+\theta(j+ij+j^2+kj)+(1+\theta)(k+ik+jk+k^2))/4 \\
&= ((i-1-k+j)+\theta(j+k-1-i)+(1+\theta)(k-j+i-1))/4 \\
&= ((-1-\theta-1-\theta)+(1-\theta+1+\theta)i+ \\
&\quad (1+\theta-1-\theta)j+(-1+\theta+1+\theta)k)/4 \\
&= (-2(1+\theta)+2i+2\theta k))/4 \\
&= (-(1+\theta)+i+\theta k))/2 \\
&= (-(1+\theta)+(-(1+\theta)+(2+\theta))i+ \\
&\quad (-(1+\theta)+(2+\theta)\theta+((1+\theta)-(2+\theta)\theta))j+ \\
&\quad (-(1+\theta)+(2+\theta)(1+\theta)+(1+2\theta-(2+\theta)(1+\theta))k)/2 \\
&= -(1+\theta)\left(\frac{1+i+j+k}{2}\right)+(2+\theta)\left(\frac{i+\theta j+(1+\theta)k}{2}\right)+ \\
&\quad \left(\frac{1+\theta-2\theta-\theta-\frac{m-1}{4}}{2}\right)j+\left(\frac{1+2\theta-2-\theta-2\theta-\theta-\frac{m-1}{4}}{2}\right)k \\
&= -(1+\theta)\delta_1+(2+\theta)\delta_2-\left(\frac{m-5}{8}+\theta\right)j-\left(\frac{m+3}{8}+\theta\right)k \\
\delta_2\delta_1 &= \frac{(i+\theta j+(1+\theta)k)(1+i+j+k)}{4} \\
&= (i+\theta j+(1+\theta)k+(i^2+\theta ji+(1+\theta)ki)+(ij+\theta j^2+(1+\theta)kj) \\
&\quad +(ik+\theta jk+(1+\theta)k^2)/4 \\
&= (i+\theta j+(1+\theta)k+(-1-\theta k+(1+\theta)j)+(k-\theta-(1+\theta)i)+ \\
&\quad (-j+\theta i-(1+\theta))/4 \\
&= ((-2-2\theta)+2\theta j+2k)/4 \\
&= (-(1+\theta)+\theta j+k)/2 \\
&= (-(1+\theta)+(-(1+\theta)+(1+\theta))i+ \\
&\quad (-(1+\theta)+(1+\theta)\theta-(-1-2\theta+(1+\theta)\theta)j+
\end{aligned}
$$

$$
\begin{aligned}
& (-(1+\theta)+(1+\theta)(1+\theta)-((-2-\theta)+(1+\theta)(1+\theta)))k)/2 \\
= \; & -(1+\theta)\left(\frac{1+i+j+k}{2}\right)+(1+\theta)\left(\frac{i+\theta j+(1+\theta)k}{2}\right)- \\
& \left(\frac{-1+\frac{m-1}{4}}{2}\right)j-\left(\frac{-1+2\theta+\frac{m-1}{4}}{2}\right)k \\
= \; & -(1+\theta)\delta_1+(1+\theta)\delta_2-\left(\frac{m-5}{8}\right)j-\left(\frac{m-5}{8}+\theta\right)k \\
\delta_2 j \; = \; & \left(\frac{i+\theta j+(1+\theta)k}{2}\right)j \\
= \; & (ij+\theta j^2+(1+\theta)kj)/2=(k-\theta-(1+\theta)i)/2=(-\theta+(-1-\theta)i+k)/2 \\
= \; & (-\theta+(-\theta-1)i+(-\theta-\theta+2\theta)j+(-\theta-(1+\theta)+2+2\theta)k)/2 \\
= \; & -\theta\left(\frac{1+i+j+k}{2}\right)-\left(\frac{i+\theta j+(1+\theta)k}{2}\right)+\theta j+(1+\theta)k \\
= \; & -\theta\delta_1-\delta_2+\theta j+(1+\theta)k \\
j\delta_2 \; = \; & j\left(\frac{i+\theta j+(1+\theta)k}{2}\right) \\
= \; & (ji+\theta j^2+(1+\theta)jk)/2=(-k-\theta+(1+\theta)i)/2=(-\theta+(1+\theta)i-k)/2 \\
= \; & (-\theta+(-\theta+1+2\theta)i+(-\theta+(1+2\theta)\theta-(-\theta+(1+2\theta)\theta))j+ \\
& (-\theta+(1+2\theta)((1+\theta)-(-\theta+(1+2\theta)(1+\theta)-1)k)/2 \\
= \; & -\theta\left(\frac{1+i+j+k}{2}\right)+(1+2\theta)\left(\frac{i+\theta j+(1+\theta)k}{2}\right)+\left(\frac{-\theta+\theta+2\theta^2}{2}\right)j \\
& -\left(\frac{-\theta+1+3\theta+2\theta^2-1}{2}\right)k \\
= \; & -\theta\delta_1+(1+2\theta)\delta_2+\theta^2 j-(\theta+\theta^2)k \\
\delta_2 k \; = \; & \left(\frac{i+\theta j+(1+\theta)k}{2}\right)k \\
= \; & (ik+\theta jk+(1+\theta)k^2)/2=(-j+\theta i-(1+\theta))/2=(-(1+\theta)+\theta i-j)/2 \\
= \; & (-(1+\theta)+(-(1+\theta)+1+2\theta)i+ \\
& (-(1+\theta)+(1+2\theta)\theta-(-\theta+(1+2\theta)\theta))j+ \\
& (-(1+\theta)+(1+2\theta)(1+\theta)+((1+\theta)-(1+2\theta)(1+\theta)))k/2 \\
= \; & -(1+\theta)\left(\frac{1+i+j+k}{2}\right)+(1+2\theta)\left(\frac{i+\theta j+(1+\theta)k}{2}\right)+\theta^2 j-(\theta+\theta^2)k \\
= \; & -(1+\theta)\delta_1+(1+2\theta)\delta_2+\left(\frac{m-1}{4}+\theta\right)j-\left(\frac{m-1}{4}+2\theta\right)k
\end{aligned}
$$

$$
\begin{aligned}
k\delta_2 &= k\left(\frac{i+\theta j+(1+\theta)k}{2}\right)\\
&= (ki+\theta kj+(1+\theta)k^2)/2 = (j-\theta i-(1+\theta))/2 = (-(1+\theta)-\theta i+j)/2\\
&= (-(1+\theta)+(-(1+\theta)+1)i+(-(1+\theta)+\theta+2)j+\\
&\quad (-(1+\theta)+(1+\theta)-(-(1+\theta)+(1+\theta))k)/2\\
&= -(1+\theta)\left(\frac{1+i+j+k}{2}\right)+\left(\frac{i+\theta j+(1+\theta)k}{2}\right)+j\\
&= -(1+\theta)\delta_1+\delta_2+j
\end{aligned}
$$

Next, we show that every element of $\mathcal{O}$ is integral. Let

$$
\begin{aligned}
\alpha &= r_1\delta_1+r_2\delta_2+r_3 j+r_4 k\in\mathcal{O}, \text{ that is, all } r_i\in\mathcal{R}. \text{ Then:}\\
\mathbf{tr}(\alpha) &= r_1\mathbf{tr}(\delta_1)\\
&= r_1\in\mathcal{R}\\
\mathbf{nr}(\alpha) &= \mathbf{nr}\left(\frac{r_1}{2}+\frac{r_1+r_2}{2}i+\frac{r_1+\theta r_2+2r_3}{2}j+\frac{r_1+(1+\theta)r_2+2r_4}{2}k\right)\\
&= \frac{r_1^2}{4}+\frac{r_1^2+2r_1r_2+r_2^2}{4}+\frac{r_1^2+\theta^2r_2^2+4r_3^2+2\theta r_1r_2+4r_1r_3+4\theta r_2r_3}{4}+\\
&\quad \frac{r_1^2+(1+\theta)^2r_2^2+4r_4^2}{4}+\frac{2(1+\theta)r_1r_2+4r_1r_4+4(1+\theta)r_2r_4}{4}\\
&= \frac{4r_1^2+(1+\theta^2+(1+\theta)^2)r_2^2+4r_3^2+4r_4^2}{4}+\\
&\quad \frac{(2+2\theta+2(1+\theta))r_1r_2+4r_1r_3+4r_1r_4+4\theta r_2r_3+4(1+\theta)r_2r_4}{4}\\
&= r_1^2+\left(\frac{1+\theta^2+1+2\theta+\theta^2}{4}\right)r_2^2+r_3^2+r_4^2+\\
&\quad (1+\theta)r_1r_2+r_1r_3+r_1r_4+\theta r_2r_3+(1+\theta)r_2r_4\\
&= r_1^2+\left(\frac{1+\theta+\theta^2}{2}\right)r_2^2+r_3^2+r_4^2+\\
&\quad (1+\theta)r_1r_2+r_1r_3+r_1r_4+\theta r_2r_3+(1+\theta)r_2r_4\in\mathcal{R}, \text{ since}
\end{aligned}
$$

$$
\frac{1+\theta+\theta^2}{2}=\frac{1+\theta+\frac{m-1}{4}+\theta}{2}=\frac{m+3}{8}+\theta, \text{ and } m\equiv 5 \bmod 8.
$$

Finally we show that $\mathcal{O}$ is maximal. From the products we have computed above, we can easily compute the trace of the product of two basis elements. Thus:

$$\begin{aligned}
\mathrm{disc}(\mathcal{O}) &= \mathcal{R}\begin{vmatrix} -1 & -(1+\theta) & -1 & -1 \\ -(1+\theta) & -2\theta-\left(\frac{m+3}{4}\right) & -\theta & -(1+\theta) \\ -1 & -\theta & -2 & 0 \\ -1 & -(1+\theta) & 0 & -2 \end{vmatrix} \\
&= \mathcal{R}\begin{vmatrix} -1 & -(1+\theta) & -1 & -1 \\ -(1+\theta) & -2\theta-\left(\frac{m+3}{4}\right) & -\theta & -(1+\theta) \\ -1 & -\theta & -2 & 0 \\ 0 & 0 & 1 & -1 \end{vmatrix} \\
&= \mathcal{R}\begin{vmatrix} -1 & -(1+\theta) & -2 & -1 \\ -(1+\theta) & -2\theta-\left(\frac{m+3}{4}\right) & -(1+2\theta) & -(1+\theta) \\ -1 & -\theta & -2 & 0 \\ 0 & 0 & 0 & -1 \end{vmatrix} \\
&= \mathcal{R}\begin{vmatrix} 1 & 1+\theta & 2 \\ 1+\theta & 2\theta+\left(\frac{m+3}{4}\right) & 1+2\theta \\ 1 & \theta & 2 \end{vmatrix} \\
&= \mathcal{R}\begin{vmatrix} 1 & 1+\theta & 0 \\ 1+\theta & 2\theta+\left(\frac{m+3}{4}\right) & -1 \\ 1 & \theta & 0 \end{vmatrix} \\
&= \mathcal{R}\begin{vmatrix} 1 & 1+\theta \\ 1 & \theta \end{vmatrix} \\
&= \mathcal{R}
\end{aligned}$$

so $\mathcal{O}$ is indeed a maximal order (see Section D.5). ■

4.3 Discovering the Order

The order $\mathcal{O}$ was discovered using the following reasoning: It is well known that $\mathcal{H}$ is a maximal order in $\mathbf{B}' = (-1,-1)$ over $\mathbf{Q}$, and $\text{disc}(\mathcal{H}) = 4\mathbf{Z}$. Now, $\mathcal{H} \otimes_{\mathbf{Z}} \mathcal{R}$ is still an order in $\mathbf{B} = \mathbf{B}' \otimes_{\mathbf{Q}} F$, but it is no longer maximal, since its discriminant is $4\mathcal{R}$. Suppose we assume that $h(\mathbf{Q}(\sqrt{m})) = 1$. Then $\mathcal{H}$ is contained in a maximal order $\mathcal{O}$ which has a basis, say $\mathcal{O} = \mathcal{R}[e_1, \ldots, e_4]$. Then the transition matrix A, where

$$[\delta_1 \; i \; j \; k]^T = A[e_1 \; e_2 \; e_3 \; e_4]^T$$

must have determinant 2. Hence, modulo an element of $GL_4(\mathcal{R})$, A must be one of the following matrices in Hermite normal form (see [N] for the definition):

$$\begin{bmatrix} 2 & x & y & z \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & x & y \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & x \\ 0 & 0 & 0 & 1 \end{bmatrix}, \text{ or } \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}.$$

Here, $x, y, z \in \{0, 1, \theta, 1+\theta\}$, a set of representatives for $\mathcal{R}/(2)$. The inverses of the matrices above are the same as the matrices themselves, except the non-trivial row is $[\frac{1}{2} \; -\frac{x}{2} \; -\frac{y}{2} \; -\frac{z}{2}]$, etc. The entries of A should ensure that the e_i are integers in $\mathbf{B}$, i.e., their norms and traces are in $\mathcal{R}$. This eliminates the first and last choices, since $\frac{1}{2}\delta_1 + \ldots$ has trace $1/2$, and $\frac{1}{2}k$ has norm $1/4$. The norm of e_3 for the third choice is $\frac{1+x^2}{4}$, and this is never in $\mathcal{R}$ for any of the choices for x above. This leaves only the second choice, with $\{x, y\} = \{\theta, 1+\theta\}$ as possible solutions that would make e_2 an integer when $m \equiv 5 \bmod 8$. Theorem 4.2 shows that the choices for x and y that we made makes this order always maximal, and in fact the initial assumption that $\mathbf{Q}(\sqrt{m})$ has class group order 1 is unnecessary.

Chapter 5

Computing T and H

5.1 A Formula for T and H

As the next step in finding a complete set of representatives of left $\mathcal{O}$-ideal equivalence classes in the quaternion algebra $\mathbf{B} = (-1,-1)$ over $\mathbf{Q}(\sqrt{509})$, we shall derive a formula for the type number $T = T_1$ and class number $H = H_1$, which we shall show to be equal to T in our case of interest. In our terminology, H is simply the cardinality of the set X defined in Chapter 1. It turns out that aside from being able to compute T and H over this field, we can do it for other values of m, when m and $F = \mathbf{Q}(\sqrt{m})$ satisfy certain conditions.

The most important tool will be the main theorem in ([Pi1]). In it, Selberg's Trace Formula is used to construct an algorithm that determines the type number $T_{q_1q_2}$ for an arbitrary algebra $\mathbf{B}$ over a number field when the product q_1q_2 is *square-free*, i.e., the non-maximal localizations are of prime level (see Appendix D.6 for the definition of these terms). Using this, it is possible to get a simple formula for the type numbers when $\mathbf{B}$ is defined over $\mathbf{Q}$. Unfortunately, the algorithm does not give such an effectively computable formula for all quadratic fields, but we discovered that under special conditions, such a formula can be derived from this theorem.

Theorem 5.1 (Pizer) *Let $\mathcal{F}$ be a totally real number field of degree n over $\mathbf{Q}$, $\mathcal{S}$ the ring of integers of $\mathcal{F}$. Let $\mathbf{B}$ be a positive definite quaternion algebra over $\mathcal{F}$. Let q_1 be the product of the finite primes of $\mathcal{F}$ which ramify in $\mathbf{B}$ and let q_2 be a finite product of distinct finite primes of $\mathcal{F}$ such that $(q_1, q_2) = 1$. Then the type number $T_{q_1 q_2}$ of Eichler orders of level $q_1 q_2$ in $\mathbf{B}$ is*

$$T_{q_1 q_2} = \frac{1}{2^e h(\mathcal{F})} \left(M + \frac{1}{2} \sum_{\mathcal{S}_a \in C} E_{q_1 q_2}(\mathcal{S}_a) \frac{h(\mathcal{S}_a)}{w(\mathcal{S}_a)} \right), \text{ where} \tag{5.1}$$

- *e is the number of primes dividing $q_1 q_2$.*
- *M is Eichler's Mass and is given by*

$$M = \frac{2h(\mathcal{F})\zeta_{\mathcal{F}}(2)\mathrm{disc}(\mathcal{F})^{3/2}}{(2\pi)^{2n}} \prod_{\wp | q_1} (N(\wp) - 1) \prod_{\wp | q_2} (N(\wp) + 1),$$

  where $\zeta_{\mathcal{F}}$ is the zeta function of $\mathcal{F}$.

- *$h(\mathcal{S}_a)$ is the ideal class number of locally principal $\mathcal{S}_a$-fractional ideals (see* Note (1) *below).*
- *$w(\mathcal{S}_a)$ is the index of the group of units of $\mathcal{S}$ in the group of units of $\mathcal{S}_a$.*
- $E_{q_1 q_2}(\mathcal{S}_a) = \prod_{\wp | q_1} \left(1 - \left\{ \frac{\mathcal{S}_a}{\wp} \right\}\right) \prod_{\wp | q_2} \left(1 + \left\{ \frac{\mathcal{S}_a}{\wp} \right\}\right)$ *(see* Note (2) *below)*
- *C is the collection of all orders defined by the following procedure:*

  1. *let $e_1, \ldots, e_s$ be a complete set of representatives of $\mathcal{U} \bmod \mathcal{U}^2$, where $\mathcal{U}$ are the units of $\mathcal{S}$;*
  2. *let $d_1, \ldots, d_k$ be a complete set of integral ideal representatives of $E \cdot \mathrm{Fr}(\mathcal{F})^2 \bmod (\mathrm{Pr}(\mathcal{F}))$ where E is the subgroup of $\mathrm{Fr}(\mathcal{F})$ (the divisor group of $\mathcal{F}$) generated by all the $\wp$ which divide $q_1 q_2$, and $\mathrm{Pr}(\mathcal{F})$ is the subgroup of principal divisors of $\mathrm{Fr}(\mathcal{F})$.*
  3. *let $n_1, \ldots, n_t$ be a set of all elements of $\mathcal{S}$ such that*

(a) $(n_j) = d_{j'}$ *for some* j', $1 \leq j' \leq k$

(b) $(n_i) \neq (n_j)$ *for* $i \neq j$

4. *consider the collection of all polynomials over* $\mathcal{S}$ *of the form*

$$f_{\mu,\varrho,\tau}(x) = x^2 - \tau x + n_\mu e_\varrho,\ 1 \leq \varrho \leq s,\ 1 \leq \mu \leq t,\ \textit{where}$$

(a) $f_{\mu,\varrho,\tau}(x)$ *is irreducible over* $\mathcal{F}$.

(b) $\mathcal{F}[x]/f_{\mu,\varrho,\tau}(x)$ *cannot be embedded in any* $\mathcal{F}_{\infty_i}, i = 1, \ldots, n$ *(the real completions of* $\mathcal{F}$*);*

(c) *for all* $\wp < \infty$, $\wp^{s_\wp} \mid \tau$, *where* $s_\wp = \left\lfloor \frac{v_\wp(n_\mu)}{2} \right\rfloor$, *where* $\lfloor \cdot \rfloor$ *is the floor or truncate function.*

(d) *if* $v_\wp(n_\mu)$ *is odd, then* $\wp^{s_\wp+1} \mid \tau$

5. *let* a *be a root of some* $f_{\mu,\varrho,\tau}(x)$ *given above and for each* $f_{\mu,\varrho,\tau}(x)$ *choose only one root. Then* $C = \{\mathcal{S}_a \mid \mathcal{S}_a$ *is an order of* $\mathcal{F}(a)\}$ *such that*

(a) $\mathcal{S}[a] \subset \mathcal{S}_a$

(b) *if* $\wp < \infty$, *then* $a\pi_\wp^{-s_\wp} \in \mathcal{S}_{a,\wp}$, *where* $s_\wp = \left\lfloor \frac{v_\wp(N(a))}{2} \right\rfloor$

Notes:

1. It will turn out that the $\mathcal{S}_a$ are the ring of integers of the respective $\mathcal{F}(a)$, so the term "ideal class number of locally principal $\mathcal{S}_a$-fractional ideals" simply means "the class group order of $\mathcal{F}(a)$" in this case, since all fractional ideals are locally principal.

2. The symbol $\left\{\frac{\mathcal{S}_a}{\wp}\right\}$ is explicitly defined in [Pi1], but since we shall see that for the case we are interested in we have $q_1 = q_2 = 1$, i.e., these products are empty, we will not define this symbol.

It is fortunate that Theorem 5.1, though stated in a complicated manner, can be used to derive an effectively computable formula for the type number under special conditions, which are satisfied by $\mathbf{Q}(\sqrt{509})$:

Theorem 5.2 *Let $m \equiv 1 \bmod 4$ be a positive squarefree integer, $F = \mathbf{Q}(\sqrt{m})$, $\mathcal{R}$ the ring of integer of F, $\mathcal{U}$ the units of $\mathcal{R}$, u the fundamental unit of $\mathcal{U}$. Assume that*

(P1) $h(F) = 1$, *and*
(P2) $N(u) = -1$.

Let $\mathbf{B}$ *be the totally definite quaternion algebra which is unramified at all the finite primes of F. Then the type number T of* $\mathbf{B}$ *is 1 if $m = 5$, and if $m > 5$, it is given by:*

$$T = \frac{1}{48m}\sum_{u=1}^{m}\chi(u)u^2 \; + \; \frac{1}{8}h(\mathbf{Q}(\sqrt{-m})) \; + \; \frac{1}{6}h(\mathbf{Q}(\sqrt{-3m}))$$

where χ is the character mod m appearing in Proposition E.9.

Remark. Properties (P1) and (P2) of F imply that every ideal of $\mathcal{R}$ is generated by a *totally positive* element. We will also see in later chapters that this fact will enable us to construct objects that will be useful in finding representatives of ideal and type classes, as well as realize the action of the Hecke operators.

Proof of Theorem. Assume that $m \equiv 1 \bmod 4$ is a positive squarefree integer and that $F = \mathbf{Q}(\sqrt{m})$ and u have the properties above. Proposition E.12 in the Appendix shows that 3 does not divide m. This property will be used to study the biquadratic field $\mathbf{Q}(\sqrt{m}, \sqrt{-3})$, and to apply Proposition E.4 of the Appendix. We proceed to determine the quantities in Theorem 5.1.

We have $h(\mathbf{Q}(\sqrt{m})) = 1$. Since $\mathbf{B}$ is unramified for all finite primes, $q_1 = 1$, and for maximal orders, $q_2 = 1$. Thus $e = 1$. The two products in the definition of Eichler's Mass M are thus both empty. Since $m \equiv 1 \bmod 4$, $\mathrm{disc}(F) = m$, so

$$M = \frac{2\zeta_F(2)m^{3/2}}{(2\pi)^4} = \frac{m^{3/2}}{8\pi^4}\zeta_F(2)$$

We shall further simplify M by explicitly finding $\zeta_F(2)$. Our method will be that of [L], which uses generalized Bernoulli numbers. Define the nth Bernoulli number, B_n, by

$$\frac{te^t}{e^t-1} = \sum_{n\geq 0} B_n \frac{t^n}{n!}.$$

For a character χ mod f, define $B_{n,\chi}$ by

$$\sum_{u=1}^{f} \chi(u) \frac{te^{ut}}{e^{ft}-1} = \sum_{n\geq 0} B_{n,\chi} \frac{t^n}{n!}$$

One sees easily that when $\chi \equiv 1$, then $B_{n,\chi} = B_n$. For $F = \mathbf{Q}(\sqrt{m}), m > 0$, define:

$$B_{n,F} = \prod_{\chi} B_{n,\chi},$$

where the product runs through the characters mod $d = |\mathrm{disc}(F)| = m$ which correspond to characters of $\mathrm{Gal}(F/\mathbf{Q})$. Hence this product involves only the trivial character and the character χ mod d discussed in Proposition E.9 of the Appendix (used in the calculation of the class group order). Thus

$$B_{n,F} = B_n B_{n,\chi}$$

In [L], it is shown that

$$\zeta_F(n) = \frac{(2\pi)^{2n}\sqrt{d}B_{n,F}}{4d^n(n!)^2}$$

if n is a positive *even* integer. Thus we have, for $n = 2$ (knowing that $B_2 = 1/6$):

$$M = \frac{1}{48} B_{2,\chi}.$$

To explicitly find $B_{2,\chi}$, we have to individually find the coefficient of $t^2/2$ in the Taylor series expansion of

$$\frac{te^{ut}}{e^{mt}-1}$$

for $u = 1 \ldots m$. One can differentiate this expression twice and let t approach 0, but the answer is more obvious if we write the above expression as a quotient of two

power series then perform the differentiations and set $t = 0$. Using either method, we get:

$$B_{2,\chi} = \sum_{u=1}^{m} \chi(u) \left(\frac{6u^2 - 6mu + m^2}{6m} \right).$$

However, we know that

$$\sum_{u=1}^{m} \chi(u) = 0 = \sum_{u=1}^{m} \chi(u)u.$$

The first equality follows because χ is a non-trivial character, and the second because χ is an *even* character, so

$$\sum_{u=1}^{m} \chi(u)u = \sum_{u=1}^{m} \chi(m-u)(m-u) = \sum_{u=1}^{m} \chi(u)(m-u) = -\sum_{u=1}^{m} \chi(u)u$$

and the conclusion follows. Thus we are left with:

$$B_{2,\chi} = \frac{1}{m} \sum_{u=1}^{m} \chi(u)u^2, \text{ so}$$

$$M = \frac{1}{48m} \sum_{u=1}^{m} \chi(u)u^2.$$

Now we proceed with the rest of the algorithm. The product defining $E_1(\mathcal{S}_a) = E_{q_1 q_2}(\mathcal{S}_a)$ is also empty regardless of $\mathcal{S}_a$, so $E_1(\mathcal{S}_a) = 1$. Equation 5.1 then becomes:

$$T = T_1 = M + \frac{1}{2} \sum_{\mathcal{S}_a \in C} \frac{h(\mathcal{S}_a)}{w(\mathcal{S}_a)}$$

We now follow the algorithm to find the collection C:

1. Since $\mathcal{U} = \langle -1 \rangle \langle u \rangle$ and $\mathcal{U}^2 = \langle u^2 \rangle$, we get $s = 4$, and a set of representatives for $\mathcal{U} \mod \mathcal{U}^2$ is given by

   $$\{ 1, -1, u, -u \}$$

   We note that when $m = 5$, the fundamental unit is $u = \theta = \frac{1+\sqrt{5}}{2}$, and $\theta^2 = 1 + \theta$.

2. Since $q_1 q_2 = 1$ and $\mathrm{Fr}(\mathcal{F}) = \mathrm{Pr}(\mathcal{F})$, we have $k = 1, E = (1)$, and

   $$\{d\} = \{d_1\} = \{1\}$$

   is a complete set of representatives of $E \cdot \mathrm{Fr}(\mathcal{F})^2 \mod (\mathrm{Pr}(\mathcal{F}))$

3. From (2), we can take $t = 1$ and

$$n = n_1 = 1$$

4. We shall call the polynomials obtained in this step *contributing polynomials*, and denote this set by Ψ. Since $\mu = 1 = t$ and $n = n_1 = 1$, we shall abbreviate:

$$f_{\varrho,\tau}(x) = x^2 - \tau x + e_\varrho$$

Since $v_\wp(n) = 0$ for any $v_\wp$, we have $s_\wp = 0$ for every $\wp < \infty$, so condition (4.c) is always satisfied by any τ. Condition (4.d) is vacuous. Now we look at condition (4.b). Since F is totally real, this condition requires that the discriminant of $f_{\varrho,\tau}$,

$$\Delta(f_{\varrho,\tau}) = \tau^2 - 4e_\varrho,$$

be totally negative. But for any τ, $\Delta(f_{-1,\tau})$ and $\Delta(f_{-u,\tau})$ are always positive, since $u > 0$. Hence we need only consider $f_{1,\tau}$ and $f_{u,\tau}$. But $N_{\mathbf{Q}}^F(u) = u(u^\sigma) = -1$ tells us that $u^\sigma < 0$, so for any τ, $(\tau^\sigma)^2 - 4u^\sigma > 0$. So only $e_\varrho = 1$ remains. We further abbreviate:

$$f_\tau(x) = x^2 - \tau x + 1$$

Our problem is therefore to find all $\tau \in \mathcal{R}$, say $\tau = a + b\theta$, $a, b \in \mathbf{Z}$ such that:

$$\tau^2 - 4 < 0 \text{ and } (\tau^\sigma)^2 - 4 < 0, \text{ or equivalently}$$

$$-2 < \tau, \tau^\sigma < 2, \text{ or}$$

$$-2 < a + b\theta, (a + b) - b\theta < 2 \text{ or}$$

$$-2 < a + b\theta, -a - b + b\theta < 2$$

Adding these two inequalities, we see that necessarily:

$$-4 < (2\theta - 1)b < 4 \text{ or}$$

$$-4 < \sqrt{m}b < 4$$

Hence if $m > 16$, then $b = 0$ is the only possible value. In this case, $\tau = a = 0, \pm 1$. Note that these three values yield a contributing f_τ.

So now assume that $m < 16$, i.e., $m = 5, 13$. In both cases, $1 < 4/\sqrt{m} < 2$, so $b = 0, \pm 1$ are the only possible values. We check which yield contributing f_τ's:

$b = 0$: As before, $\tau = a = 0, \pm 1$.

$b = 1$: We must have

$$\begin{aligned} & -2 < a + \tfrac{1+\sqrt{m}}{2} < 2 \text{ and } -2 < a + \tfrac{1-\sqrt{m}}{2} < 2 \\ \Rightarrow \quad & \tfrac{-5-\sqrt{m}}{2} < a < \tfrac{3-\sqrt{m}}{2} \text{ and } \tfrac{-5+\sqrt{m}}{2} < a < \tfrac{3+\sqrt{m}}{2} \\ \Rightarrow \quad & \tfrac{-5+\sqrt{m}}{2} < a < \tfrac{3-\sqrt{m}}{2} \end{aligned}$$

If $m = 5$, only $a = 0$ or -1 lies in this range, and $\tau = \theta, -1 + \theta = -\theta^\sigma$ both yield contributing f_τ. If $m = 13$, there are no integers in the range above, so $b = 1$ is not possible in this case.

$b = -1$: A similar analysis yields $\frac{-3+\sqrt{m}}{2} < a < \frac{5-\sqrt{m}}{2}$. If $m = 5$, only $a = 0$ or 1 lies in this range, and $\tau = -\theta, 1 - \theta = \theta^\sigma$ both yield contributing f_τ. If $m = 13$, there are again no integers in the range above, so $b = -1$ is not possible in this case.

Clearly, condition (4.a), irreducibility, is satisfied by all the f_τ mentioned above, since the roots are imaginary. We summarize step 4 in the following:

Lemma 5.3 *Assume the hypotheses in Theorem 5.2 above.*

(a) If $m > 5$, the only contributing polynomials in Ψ are f_τ, where $\tau = 0, \pm 1$.

(b) If $m = 5$, the only contributing polynomials in Ψ are f_τ, where $\tau = 0, \pm 1, \pm\theta, \pm\theta^\sigma$.

The roots of these polynomials and the fields that they generate over $\mathbf{Q}(\sqrt{m})$ are shown below.

Table 5.1 Fields Generated by Roots of Contributing Polynomials f_τ

τ	Roots ** a_τ, a'_τ Of $f_\tau = x^2 - \tau x + 1$	$F(a_\tau)$
0	ζ_4, ζ_4^3	$\mathbf{Q}(\sqrt{m}, \zeta_4)$
1	ζ_6, ζ_6^5	$\mathbf{Q}(\sqrt{m}, \zeta_6)$
-1	ζ_6^2, ζ_6^3	$\mathbf{Q}(\sqrt{m}, \zeta_6)$
θ	$\frac{\theta+\alpha}{2}, \frac{\theta-\alpha}{2}$	$\mathbf{Q}(\zeta_5)$
$-\theta$	$\frac{-\theta+\alpha}{2}, \frac{-\theta-\alpha}{2}$	$\mathbf{Q}(\zeta_5)$
θ^σ	$\frac{\theta^\sigma+\beta}{2}, \frac{\theta^\sigma-\beta}{2}$	$\mathbf{Q}(\zeta_5)$
$-\theta^\sigma$	$\frac{-\theta^\sigma+\beta}{2}, \frac{-\theta^\sigma-\beta}{2}$	$\mathbf{Q}(\zeta_5)$

** $\alpha = \sqrt{-3+\theta}$, $\beta = \sqrt{-2-\theta}$, $\theta = \frac{1+\sqrt{5}}{2}$, $\sigma : \sqrt{5} \longrightarrow -\sqrt{5}$

The only non-obvious part is proving the last four rows for $F = \mathbf{Q}(\sqrt{5})$, but it is easy to see that $F(\alpha) = F(\beta)$, since $\alpha\beta = \sqrt{5} \in F$.

We note that the irreducible polynomial of α over F is $x^2 - (-3+\theta)$, while that of β is $x^2 - (-2-\theta)$, and the irreducible polynomial of *both* α and β is the product of these: $x^4 + 5x^2 + 5$. We shall show that $F(\alpha)$ is contained in $\mathbf{Q}(\zeta_5)$. From the fifth cyclotomic polynomial and Euler's identity, we get

$$\cos(2\pi/5) = \frac{-1+\sqrt{5}}{2}, \quad \sin(2\pi/5) = \sqrt{\frac{5+\sqrt{5}}{8}}, \text{ hence}$$

$$\theta = \frac{1+\sqrt{5}}{2} = -\zeta_5^2 - \zeta_5^3,$$

and so $F = \mathbf{Q}(\sqrt{5}) \subset \mathbf{Q}(\zeta_5)$. Also, the ring of integers $\mathcal{S}$ of $\mathbf{Q}(\zeta_5)$ is $\mathbf{Z}[\zeta_5]$. Next, one sees that $\gamma = \pm(\zeta_5^2 - \zeta_5^3) \in \mathcal{S}$ satisfies $\gamma^2 = -3 + \theta$, so $\alpha \in \mathbf{Q}(\zeta_5)$. ■

Similarly, we find that $\pm(1 + 2\zeta_5 + \zeta_5^2 + \zeta_5^3)$ are the square roots of $-2 - \theta$. Of course, it is easy to *derive* γ as a square root of $-3 + \theta$ in $\mathbf{Q}(\zeta_5)$. Since α is an algebraic integer, we must find $a \ldots d \in \mathbf{Z}$ such that $\gamma = a + b\zeta_5 + c\zeta_5^2 + d\zeta_5^3$. Since the real part of γ must be 0, we determine that $b = 2a$, $d = 2a - c$. Equating γ^2 with $-3 + \theta = -3 - \zeta_5^2 - \zeta_5^3$, we get:

$$4a^2 - 6ac + c^2 = 1 \text{ and } 3a^2 - 2ac + 2c^2 = 2$$

from which $a^2 + c^2 = 1$. Since $a, c \in \mathbf{Z}$, we get $a = 0, c = \pm 1$, and γ is determined as above.

Alternatively, one can also directly compute the ring of integers of $F(\alpha)$ and its discriminant, and use some facts about cyclotomic and abelian extensions to conclude that this field is contained in $\mathbf{Q}(\zeta_5)$.

5. We proceed to the last step of the algorithm: finding the orders $\mathcal{S}_a$. Condition (5.a) says that $\mathcal{R}[a_\tau]$ must be contained in $\mathcal{S}_a$. However, we find that $\mathcal{R}[a_\tau]$ is the maximal order of $F(a_\tau)$:

Lemma 5.4 *Let m be as in Theorem 5.2, $\mathcal{R}$ the ring of integers of $\mathbf{Q}(\sqrt{m})$. Then:*

(a) The ring of integers of $\mathbf{Q}(\sqrt{m}, \zeta_4)$ is $\mathcal{R}[\zeta_4]$.

(b) The ring of integers of $\mathbf{Q}(\sqrt{m}, \zeta_6)$ is $\mathcal{R}[\zeta_6]$.

(c) For $m = 5$, the ring of integers of $\mathbf{Q}(\zeta_5)$ is

$$\mathcal{R}\left[\frac{\pm\theta + \alpha}{2}\right] = \mathcal{R}\left[\frac{\pm\theta^\sigma + \beta}{2}\right].$$

Proof. Parts (a) and (b) are covered by Corollary E.2 of the Appendix. Let $\mathcal{S}$ be the ring of integers of $\mathbf{Q}(\zeta_5)$. Note that ζ_{10}^k generates $\mathcal{S}$ over

$\mathbf{Z}$, if $k \not\equiv 0 \bmod 5$. To show (c), we have:

$$\frac{\theta+\alpha}{2} = \frac{-\zeta_5^2 - \zeta_5^3 + \zeta_5^2 - \zeta_5^3}{2} = -\zeta_5^3 = \zeta_{10}, \text{ hence } \mathcal{S} = \mathcal{R}\left[\frac{\theta+\alpha}{2}\right].$$

Similarly, we get

$$\begin{aligned}
\frac{-\theta+\alpha}{2} &= \frac{\zeta_5^2 + \zeta_5^3 + \zeta_5^2 - \zeta_5^3}{2} \\
&= \zeta_5^2 = \zeta_{10}^4, \\
\frac{-\theta^\sigma+\beta}{2} &= \frac{-1 - \zeta_5^2 - \zeta_5^3 + 1 + 2\zeta_5 + \zeta_5^2 + \zeta_5^3}{2} \\
&= \zeta_5 = \zeta_{10}^2, \\
\frac{\theta^\sigma+\beta}{2} &= \frac{1 + \zeta_5^2 + \zeta_5^3 + 1 + 2\zeta_5 + \zeta_5^2 + \zeta_5^3}{2} \\
&= 1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 = -\zeta_5^4 = \zeta_{10}^3
\end{aligned}$$

so all these generate $\mathcal{S}$ over $\mathcal{R}$ (in fact over $\mathbf{Z}$). Hence the only possibility for $\mathcal{S}_{a_\tau}$ is the ring of integers of the respective $F(a_\tau)$. ■

Lemma 5.5 *The set of orders C consists of the rings of integers $\mathcal{S}$ of the extensions $F(a_\tau)$ where a_τ is a chosen root of a contributing polynomial f_τ as determined by Lemma 5.3.*

Proof. Only condition (5.b) needs to be verified. Our computations show that all of the roots a_τ of f_τ are roots of unity, so $N_F^{F(a_\tau)}(a_\tau) = 1$, so $s_\wp = 0$ for every $\wp$. Hence $a_\tau \in \mathcal{S}_{a_\tau,\wp}$ is always satisfied. ■

Hence, equation 5.1 becomes:

$$T = M + \frac{1}{2}\sum_{\mathcal{S}_{a_\tau} \in C} \frac{h(\mathcal{S}_{a_\tau})}{w(\mathcal{S}_{a_\tau})}$$

We first study the contributions in this sum from the biquadratic fields (1) $\mathbf{Q}(\sqrt{m}, \sqrt{-1})$ and (2) $\mathbf{Q}(\sqrt{m}, \sqrt{-3})$, which will be valid for both $m = 5$ and $m > 5$. We will apply Proposition E.9 of the Appendix to simplify the class numbers of the biquadratic extensions above:

1. Let $m_1 = -1, m_2 = -m, m_0 = m, K = \mathbf{Q}(\sqrt{-1}, \sqrt{-m})$. Hence $h_0 = 1$, by hypothesis. It is well known that the class group order of $\mathbf{Q}(\sqrt{-1})$ is 1, and the only roots of unity are powers of $\sqrt{-1}$, i.e., $h_1 = 1, w_1 = 4$. Also, the only roots of unity in $\mathbf{Q}(\sqrt{-m}), m \neq 1, 3$, are ± 1, i.e., $w_2 = 2$. By Proposition E.3, $w = 4$ and $u_0 = u$. So we obtain $h = \frac{1}{2}h(\sqrt{-m})$.

2. Let $m_1 = -3, m_2 = -3m, m_0 = 9m, K = \mathbf{Q}(\sqrt{-3}, \sqrt{-3m})$. Similarly, it is know that the class group order of $\mathbf{Q}(\sqrt{-3})$ is 1, and the only roots of unity are powers of ζ_6, i.e., $h_1 = 1, w_1 = 6$. By Proposition E.4, $w = 6$ and $u_0 = u$. Again $w_2 = 2$ and we obtain $h = \frac{1}{2}h(\sqrt{-3m})$.

Next, from Propositions E.3 and E.4, $[\mathcal{S}^\times : \mathcal{U}] = 2$ and 3, respectively, for $\mathbf{Q}(\sqrt{m}, \sqrt{-1})$ and $\mathbf{Q}(\sqrt{m}, \sqrt{-3})$.

We can now finish proving Theorem 5.2 for $m > 5$. The field $\mathbf{Q}(\sqrt{m}, \sqrt{-3})$ contributes twice in the sum (for $\tau = 1, -1$), so equation 5.1 becomes:

$$\begin{aligned} T &= M + \frac{1}{2}\left(\frac{h(\mathbf{Q}(\sqrt{m}, \sqrt{-1}))}{2} + 2\frac{h(\mathbf{Q}(\sqrt{m}, \sqrt{-3}))}{3}\right) \\ &= M + \frac{1}{4}h(\mathbf{Q}(\sqrt{m}, \sqrt{-1})) + \frac{1}{3}h(\mathbf{Q}(\sqrt{m}, \sqrt{-3})) \\ &= M + \frac{1}{8}h(\mathbf{Q}(\sqrt{-m})) + \frac{1}{6}h(\mathbf{Q}(\sqrt{-3m})) \end{aligned}$$

For $m = 5$, the field $\mathbf{Q}(\zeta_5)$ contributes 4 times in the sum, corresponding to $\tau = \theta, -\theta, \theta^\sigma, -\theta^\sigma$. Let $\mathcal{S}$ be the integers of $\mathbf{Q}(\zeta_5)$. It is well known that $\mathcal{S}^\times = \langle\zeta_{10}\rangle\langle\theta\rangle$, hence $[\mathcal{S}^\times : \mathcal{U}] = 5$. Keeping the simplifications we made for $m > 5$, we get:

$$T = M + \frac{1}{8}h(\mathbf{Q}(\sqrt{-5})) + \frac{1}{6}h(\mathbf{Q}(\sqrt{-15})) + \frac{2}{5}h(\mathbf{Q}(\zeta_5))$$

Eichler's Mass number M for $m = 5$ is $(1 - 4 - 9 + 16)/240 = 1/60$.

The appendices of [BS] show that $h(\mathbf{Q}(\sqrt{-5})) = h(\mathbf{Q}(\sqrt{-15})) = 2$. The discriminant of $\mathbf{Q}(\zeta_5)$ is 125, so the Minkowski bound for $\mathbf{Q}(\zeta_5)$ is

$$\frac{4!}{4^4}\left(\frac{4}{\pi}\right)^2\sqrt{125} < 2$$

hence every ideal class has an ideal of norm 1. Thus $\mathbf{Q}(\zeta_5)$ has class group order 1. Equation 5.1 becomes

$$T = \frac{1}{60} + \frac{1}{4} + \frac{1}{3} + \frac{2}{5} = 1$$

which finishes the proof for $m = 5$. ■

Following the proof of Theorem 5.1 in [Pi1], we see that

$$T_{q_1 q_2} = \frac{1}{2^e h(\mathcal{F})} \left(H_{q_1 q_2} + \frac{1}{2} \sum_{\mathcal{S}_a \in C_2} E_{q_1 q_2}(\mathcal{S}_a) \frac{h(\mathcal{S}_a)}{w(\mathcal{S}_a)} \right), \text{ where} \tag{5.2}$$

$C_2 = C - C_1$, and $C_1 = \{ \mathcal{S}_a \in C \mid (N(a)) = (1) \}$. That is, a is a root of $f_{\mu,\varrho,\tau}(x)$ with $(n_\mu) = (1)$. From this, we have:

Proposition 5.6 *Let m be a positive squarefree integer, $F = \mathbf{Q}(\sqrt{m})$, with $h(F) = 1$, and $\mathbf{B}$ the unique quaternion algebra with $Ram(\mathbf{B}) = \{\infty_1, \infty_2\}$. Then $H = T$, i.e., the number of left-ideal classes of a maximal order equals the type number of maximal orders. Consequently, if $I_1, \ldots, I_H$ is a complete set of representatives of distinct left $\mathcal{O}$-ideal classes for a fixed maximal order $\mathcal{O}$, then the corresponding right orders $\mathcal{O}_r(I_1), \ldots, \mathcal{O}_r(I_H)$ form a complete set of distinct representatives of maximal orders of different types.*

Proof. (The notion of a right order can be found in Appendix D.5.) We have $h(F) = 1$, $q_1 = q_2 = 1$, $2^e = 1$ and $n_\mu = n_1 = 1$ in the algorithm to find C. Thus $C_2 = \emptyset$. Substitute these in (5.2) to get the result. ■

5.2 Langlands' Conjecture for $m = 5$

Our computations above show that $H = T = 1$ for $F = \mathbf{Q}(\sqrt{5})$, hence the function space S has only the zero function. Hence S_2 has no eigenforms. In [Pin], we also see that there are no elliptic curves over F which have good reduction everywhere. Hence $\mathcal{E} = \emptyset$. Thus:

Theorem 5.7 *Langlands' Conjecture 1.1 is true for* $\mathbf{Q}(\sqrt{5})$.

5.3 T for Various F

It is surprising that there are 40 values of m in the range $16 < m < 510$ that satisfy the hypotheses of Theorem 5.2. The ideal class group orders may be computed using the formulas in Proposition E.9 of the Appendix. These m and associated class group orders, Eichler's Mass, and type numbers are tabulated below. We note that with the exception of $m = 5$ above, the character sum in the formula for M is divisible by m. We also observe that all the values of m are *prime*. The condition $N(u) = -1$ tells us that m is a squarefree product of primes $\equiv 1 \bmod 4$. The additional condition $h(F) = 1$ seems to imply that m is actually prime. We therefore ask the question: If $m \equiv 1 \bmod 4$ such that $\mathbf{Q}(\sqrt{m})$ has class number 1 and $\mathcal{R}$ has a unit of norm -1, is m a prime?

Table 5.2 Type Number for $\mathbf{B}/\mathbf{Q}(\sqrt{m})$ for Certain m

m	$h(\mathbf{Q}(\sqrt{-m}))$	$h(\mathbf{Q}(\sqrt{-3m}))$	M	T
13	2	4	$\frac{1}{12}$	1
17	4	2	$\frac{1}{6}$	1
29	6	6	$\frac{1}{4}$	2
37	2	8	$\frac{5}{12}$	2
41	8	2	$\frac{2}{3}$	2
53	6	10	$\frac{7}{12}$	3
61	6	8	$\frac{11}{12}$	3
73	4	4	$\frac{11}{6}$	3
89	12	2	$\frac{13}{6}$	5
97	4	4	$\frac{17}{6}$	4
101	14	10	$\frac{19}{12}$	5
109	6	12	$\frac{9}{4}$	5
113	8	6	3	5
137	8	6	4	6
149	14	14	$\frac{35}{12}$	7
157	6	16	$\frac{43}{12}$	7
173	14	18	$\frac{13}{4}$	8
181	10	12	$\frac{19}{4}$	8
193	4	8	$\frac{49}{6}$	10
197	10	22	$\frac{49}{12}$	9

Table 5.2 (continued) Type Number for $\mathbf{B}/\mathbf{Q}(\sqrt{m})$ for Certain m

m	$h(\mathbf{Q}(\sqrt{-m}))$	$h(\mathbf{Q}(\sqrt{-3m}))$	M	T
233	12	10	$\frac{53}{6}$	12
241	12	4	$\frac{71}{6}$	14
269	22	14	$\frac{83}{12}$	12
277	6	28	$\frac{103}{12}$	14
281	20	6	$\frac{25}{2}$	16
293	18	22	$\frac{85}{12}$	13
313	8	8	$\frac{50}{3}$	19
317	10	26	$\frac{101}{12}$	14
337	8	12	19	22
349	14	16	$\frac{151}{12}$	17
353	16	6	16	19
373	10	32	$\frac{161}{12}$	20
389	22	22	$\frac{151}{12}$	19
397	6	24	$\frac{57}{4}$	19
409	16	4	$\frac{79}{3}$	29
421	10	20	$\frac{209}{12}$	22
433	12	8	$\frac{163}{6}$	30
449	20	6	$\frac{51}{2}$	29
457	8	12	30	33
461	30	18	$\frac{61}{4}$	22
509	30	14	$\frac{215}{12}$	24

Chapter 6

Θ-Series of an Ideal

The notion and construction of a Θ-series for an ideal in a quaternion algebra is discussed in several papers, including [Pi4], [Pi5], [Pi6] and [Gr]. In these papers, $\mathbf{B}'$ is a positive definite quaternion algebra over $\mathbf{Q}$, and L is a $\mathbf{Z}$-ideal of $\mathbf{B}'$. The Θ-series of L catalogues in a certain sense the number of elements α of L that have a fixed norm, for all possible $\mathbf{nr}(\alpha)$. It is also useful in determining if two left ideals represent different ideal classes. Our objective in this chapter is to find conditions wherein we can extend the definition of a Θ-series to quaternion algebras over a quadratic field, prove analogous properties for them as those found in the papers above, and to find ways to explicitly and effectively (i.e., in reasonable computational time) find the first few terms of this (infinite) series. We shall often refer to $L/\mathbf{Z}$, a lattice in an algebra $\mathbf{B}'/\mathbf{Q}$, in order to compare our construction to those in the mentioned papers.

We assume henceforth that $F = \mathbf{Q}(\sqrt{m})$, $m > 0$, with (P1) $h(F) = 1$ and (P2) the fundamental unit u has norm -1. These properties assure us that every fractional ideal can be generated by a *totally positive* element, and every totally positive unit is a power of u^2. As usual, $\mathcal{R} = \mathbf{Z}[\theta]$ is the ring of integers of F, with $\theta = \frac{1+\sqrt{m}}{2}$.

6.1 Θ-Series of an $\mathcal{R}$-Ideal

We assume that $\mathbf{B}$ is a positive definite quaternion algebra over F. Thus the norm of any $\beta \in \mathbf{B}$ is totally positive, and every $\mathcal{R}$-ideal J of $\mathbf{B}$ has a basis of 4 elements. Denote by $\mathbf{nr}(J)_+$ a totally positive generator of $\mathbf{nr}(J)$. For any $\beta \in J$, define:

$$\mathcal{N}_J(\beta) = \mathbf{nr}(\beta)/\mathbf{nr}(J)_+$$

Thus the image of $\mathcal{N}_J$ is in $\mathcal{R}_{>>0}$, the totally positive elements of $\mathcal{R}$. We can think of $\mathcal{N}_J$ as a "scaled" norm. For $L/\mathbf{Z}$, $\mathbf{nr}(L)_+$ is simply a positive generator of $\mathbf{nr}(L)$.

Now define the Θ-*series* of J:

$$\begin{aligned} \Theta_J(\tau) &= \sum_{\beta \in J} \exp(\tau \mathcal{N}_J(\beta)) \\ &= \sum_{\xi \in \mathcal{R}_{>>0}} c_{\xi,J} \exp(\tau\xi), \text{ where} \\ c_{\xi,J} &= \#\{\, \beta \in J \mid \mathcal{N}_J(\beta) = \xi \,\}. \end{aligned}$$

We will call $c_{\xi,J}$ the *representation number* for ξ in J. Because $\mathcal{R}_{>>0}$ is dense in $\mathbf{R}_{>0}$, it is not at all clear that $c_{\xi,J}$ is always finite (for $L/\mathbf{Z}$, we will see that this is clear). We will prove later that $c_{\xi,J}$ is finite for every ξ and J, so the Θ-series is well defined. Ignoring this for now, we have:

Proposition 6.1 *The definition of $c_{\xi,J}$ for any $\mathcal{R}$-ideal J is independent of the choice of $\mathbf{nr}(J)_+$.*

Proof. Any two choices for $\mathbf{nr}(J)_+$ differ by a totally positive unit u^{2n}, for some $n \in \mathbf{Z}$. Since $\mathbf{nr}(u^n) = u^{2n}$, multiplication by $u^n \in \mathcal{R}$ gives a bijection between the set of $\beta \in J$ of norm ξ and those $\beta' \in J$ of norm $u^{2n}\xi$. ∎

Now we see that the Θ-series can be used to determine if two ideals or orders are in different classes.

Proposition 6.2 *If J is an ideal and $J' = \gamma_1 J \gamma_2$, with both $\gamma_i \in \mathbf{B}^\times$, then $c_{\xi,J} = c_{\xi,J'}$ for all $\xi \in \mathcal{R}$. Thus $\Theta_J(\tau) = \Theta_{J'}(\tau)$.*

Proof. Suppose $J' = \gamma_1 J \gamma_2$ as above. Then we can choose $\mathbf{nr}(J')_+$ to be $\mathbf{nr}(\gamma_1)(\mathbf{nr}(J)_+)\mathbf{nr}(\gamma_2)$, since the $\mathbf{nr}(\gamma_i)$ are totally positive. Every $\beta' \in J'$ is of the form $\beta' = \gamma_1 \beta \gamma_2$ for some $\beta \in J$. Thus

$$\begin{aligned} \mathbf{nr}(\beta') &= \mathbf{nr}(\gamma_1)\mathbf{nr}(\beta)\mathbf{nr}(\gamma_2), \text{ so} \\ \mathcal{N}_{J'}(\beta') &= \mathbf{nr}(\beta')/\mathbf{nr}(J')_+ \\ &= \mathbf{nr}(\gamma_1)\mathbf{nr}(\beta)\mathbf{nr}(\gamma_2)/(\mathbf{nr}(\gamma_1)\mathbf{nr}(J)_+\mathbf{nr}(\gamma_2)) \\ &= \mathcal{N}_J(\beta), \end{aligned}$$

so $\Theta_J(\tau) = \Theta_{J'}(\tau)$ as well. ■

This tells us that if two left (resp. right) $\mathcal{O}$-ideals have different Θ-series, then they are not in the same left (resp. right) ideal class (use $\gamma_1 = 1$, resp. $\gamma_2 = 1$). Two orders with different Θ-series are not of the same type (use $\gamma_1 = \gamma_2^{-1}$). It is still possible, though, for two ideals having the same Θ-series to be in different ideal classes.

6.2 Preliminaries on Quadratic Forms

As we shall see, to effectively compute the representation numbers for J, we will need to know something about quadratic forms. Assume that $\mathcal{F}$ is an arbitrary field with characteristic different from 2. We shall use multi-index notation: $X = [x_1 \dots x_n]$. We will write a *quadratic form* $f(X)$ in n-variables using a symmetric sum:

$$f(X) = \sum_{i,j=1}^{n} a_{i,j} x_i x_j$$

with the $a_{i,j} \in \mathcal{F}$, not all $a_{i,j} = 0$ and $a_{i,j} = a_{j,i}$. The *determinant* of f is the determinant of the matrix $A = [a_{i,j}]$. Two forms $f(X)$ and $f'(X')$ with coefficients

in $\mathcal{F}$ are *$\mathcal{F}$-congruent* if under a substitution of variables $(X')^T = CX^T$ into f', we obtain the form f, and the matrix C is in $GL_n(\mathcal{F})$. Every f with coefficients in $\mathbf{R}$ is uniquely $\mathbf{R}$-congruent to a form $x_1^2 + \ldots + x_i^2 - x_{i+1}^2 - \ldots - x_n^2$. We call f *positive definite* if $i = n$.

If the form f has non-zero determinant and $f(X) = 0$ for some $X \neq 0$, we call f a *zero form*. We say that f *represents* α *in* $\mathcal{F}$ if there is an $X = [a_1 \ldots a_n] \in \mathcal{F}^n$ with $f(X) = \alpha$. For instance, the Hilbert symbol $(a, b)_{\mathcal{F}}$ in $\mathcal{F}$ is 1 if and only if $ax^2 + by^2$ represents 1. Clearly, congruent forms represent the same elements of $\mathcal{F}$.

We shall be mostly interested in forms over $\mathbf{Q}$, with X assuming values only in $\mathbf{Z}^n$. If f and f' have coefficients in $\mathbf{Q}$, we say the f is *equivalent* to f', symbolically $f \sim f'$, if there is a change of variables taking f to f' with matrix C, as above, in $SL_n(\mathbf{Z})$. If $f \sim f'$, C gives a bijection between the set of $X \in \mathbf{Z}^n$ such that $f(X) = \alpha$, and the set of $X' \in \mathbf{Z}^n$ such that $f'(X') = \alpha$, for any $\alpha \in \mathbf{Q}$.

6.3 Computing Θ_J

Suppose that we are given an ideal J in terms of a basis over $\mathcal{R}$. We show that we can find an *effective* algorithm to find the $c_{\xi,J}$. As a byproduct, we find that these numbers are finite. First we explore the nature of $\mathcal{N}_J$:

Proposition 6.3 *Choose a basis $[\beta_1, \ldots, \beta_4]$ for J, and write $\beta \in J$ as*

$$\beta = \sum_{r=1}^{4} (x_r + x_{r+4}\theta)\beta_r$$

where $X = [x_1 \ldots x_8] \in \mathbf{Z}^8$. If we write $\mathcal{N}_J(\beta)$ as:

$$\mathcal{N}_J(\beta) = \Psi_1(X) + \Psi_2(X)\theta,$$

then Ψ_1 and Ψ_2 are quadratic forms with coefficients in $\mathbf{Q}$ and values in $\mathbf{Z}$. Furthermore, Ψ_1 is positive definite. These properties hold regardless of the chosen basis.

Proof. We have remarked that $\mathcal{N}_J$ has values in $\mathcal{R}_{>>0}$, so the $\Psi_{\mathtt{i}}$ are integer valued. Represent β in the form above. It is easy to see that the coefficients of $1, i, j$ and k in β are $\mathcal{R}$-linear combinations of the $x_{\mathtt{i}}$, so the $\Psi_{\mathtt{i}}$ are indeed quadratic forms with rational coefficients. Also, by Proposition E.5 of the Appendix, a necessary condition for $a + b\theta$, $a, b \in \mathbf{Z}$, to be in $\mathcal{R}_{>>0}$ is that $a > 0$. Thus $\Psi_1(X \setminus \{0\}) \subset \mathbf{Z}_{>0}$. This is possible only if Ψ_1 is positive definite. ■

Corollary 6.4 *For any $\xi \in \mathcal{R}_{>>0}$ and ideal J of $\mathbf{B}$, the representation number $c_{\xi,J}$ is finite.*

Proof. Let $\xi = a + b\theta \in \mathcal{R}$. In the notation above, the set

$$\{ X \in \mathbf{Z}^8 \mid \Psi_1(X) \leq a \}$$

is finite, since Ψ_1 is positive definite and integer valued. Thus, $c_{\xi,J}$ is also finite. ■

In the analogous construction for $L/\mathbf{Z}$, $\mathcal{N}_L(\beta) = \Psi(X)$ is itself a positive definite integer valued quadratic form, hence we see immediately that $c_{n,L}$ is finite for any $n \in \mathbf{Z}_{>0}$.

The properties above let us explicitly compute $c_{\xi,J}$ for $\xi = a + b\theta$ and $a \leq M \in \mathbf{R}$. Choose a basis for J and write $\Psi_1(X) = \sum a_{i,j}x_ix_j$, with $a_{i,j} = a_{j,i}$. Since Ψ_1 is positive definite, $a_{i,i} > 0$ for every i. Thus we can write

$$\Psi_1(X) = \frac{1}{a_{1,1}}(a_{1,1}x_1 + \cdots + a_{1,n}x_n)^2 + \Psi_1^{(2)},$$

where $\Psi_1^{(2)}$ is again a positive definite form in $x_2, \ldots, x_n$. Proceeding in this manner, we write (changing notation)

$$\begin{aligned}\Psi_1(X) \;=\; & \frac{1}{b_{1,1}}(b_{1,1}x_1 + \cdots\cdots\cdots\cdots + b_{1,n}x_n)^2 \\ & + \frac{1}{b_{2,2}}(b_{2,2}x_2 + \cdots + b_{2,n}x_n)^2 \\ & + \cdots + \frac{1}{b_{n,n}}(b_{n,n}x_n)^2\end{aligned}$$

with all the $b_{i,i} > 0$. Thus if we require $\Psi_1(X) \leq M$, then necessarily

$$| x_n | \leq \sqrt{\frac{M}{b_{n,n}}}.$$

Since $f(X) = f(-X)$ for any quadratic form, we need to let x_n run through only $0 \ldots \lfloor \sqrt{M/b_{n,n}} \rfloor$, and account separately for $x_n = 0$ and $x_n > 0$. For every fixed x_n in this range, we find that

$$\left| x_{n-1} + \frac{b_{n-1,n}}{b_{n-1,n-1}} x_n \right| \leq \sqrt{\frac{M - b_{n,n} x_n^2}{b_{n-1,n-1}}}.$$

Thus x_{n-1} must be constrained to a certain range as well, depending on the chosen $x_{n,n}$. Proceeding in this way, we see that this method of "completing the square" gives us a way to find all X such that $\Psi_1(X) \leq M$, and for such X, we automatically find $\Psi_2(X)$ as well. Thus:

Proposition 6.5 *There is a finite algorithm to find the representation numbers of any ideal of* **B**.

6.4 Rubens vs. El Greco

Unfortunately, the efficiency of this algorithm depends on the choice of basis for J. Consider the following quadratic form:

$$f(x, y) = 101x^2 - 198xy + 101y^2.$$

Suppose we want to find all $x, y \in \mathbf{Z}$ such that $f(x, y) \leq 100$. Whether we choose x or y to begin the process above, we have $a_{1,1} = 101$. We get:

$$\frac{1}{101}(101x - 99y)^2 + \frac{101}{400}(\frac{400}{101}y)^2 = 100$$

Thus we let y range through $0 \ldots 5 = \lfloor \sqrt{100 \times 101/400} \rfloor$ and do our accounting. Notice, though, from the graph on the next page, that every slice $y = n$ contains at

most one lattice point! On the other hand, a simple change of variables:

$$\begin{aligned} x &\leftarrow x \\ y &\leftarrow x + y \end{aligned}$$

which is in $SL_2(\mathbf{Z})$ tells us that

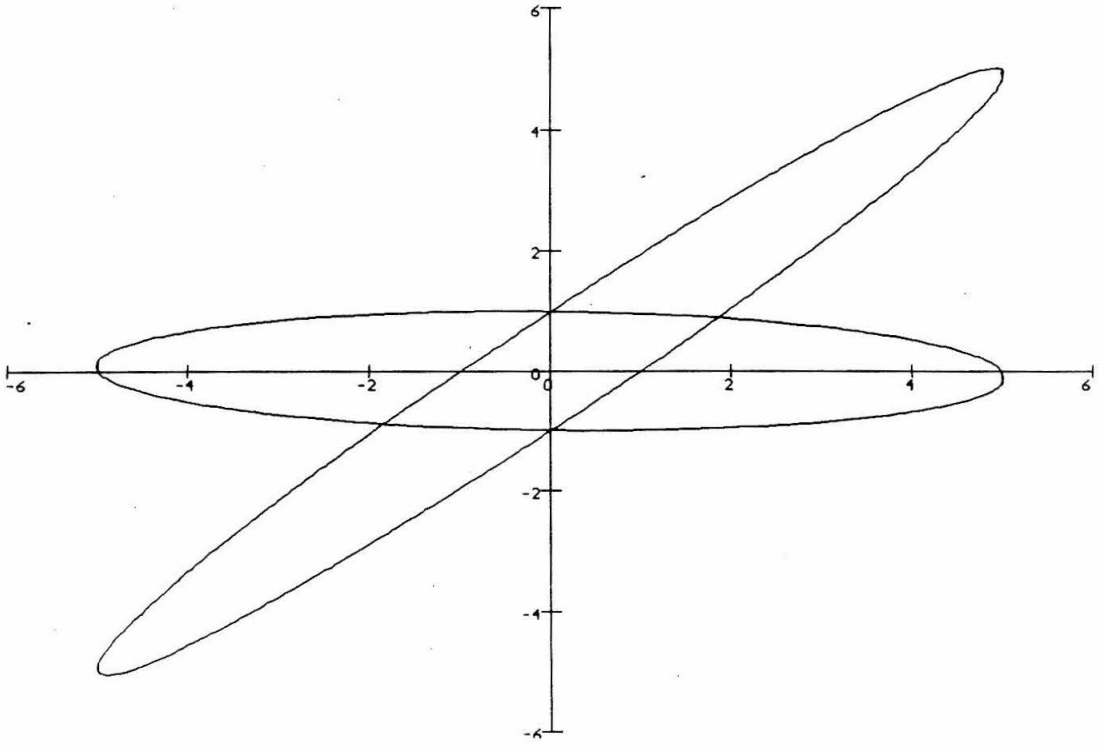
$$f \sim f^{(1)} = 4x^2 + 4xy + 101y^2.$$

Applying the same process above, choosing $a_{1,1} = 4$, we get

$$\frac{1}{4}(4x + 2y)^2 + \frac{1}{100}(100y)^2 = 100,$$

so y only ranges through 0 and 1! So in fact, the slice $y = 0$ contains almost all the lattice points!

Figure 6.1 Graphs of $101x^2 - 198xy + 101y^2 = 100$
and $4x^2 + 4xy + 101y^2 = 100$



This is a truly great improvement if we can make such a change of variables in $SL_8(\mathbf{Z})$. Among the $SL_8(\mathbf{Z})$ orbits of Ψ_1, which form will make the process above most efficient? It turns out that this optimal form is:

6.5 The Hermite Normal Form

The form equivalent to Ψ_1 that we need can be obtained from a construction due to Hermite. Before we derive it, we need the following well known result which can be found in [N]:

Proposition 6.6 *Let R be a unique factorization domain, and $M_n(R)$ the set of $n \times n$ matrices over R. If $a_1 \dots a_n \in R$ and $i \in \{1 \dots n\}$, then there is a matrix $A \in M_n(R)$ with column i equal to $[a_1 \dots a_n]$ and determinant $\gcd(a_1 \dots a_n)$.*

Sketch of Proof/Algorithm. Since we will need to do this explicitly in a future setting, we shall sketch its construction for $i = 1$ (for simplicity) and use induction on n: The proposition is trivial for $n = 1$. Now, suppose A_{n-1} is a matrix in $M_{n-1}(R)$ with $[a_1 \dots a_{n-1}]^T$ in the first column and determinant $d_{n-1} = \gcd(a_1, \dots, a_{n-1})$. Let $d_n = \gcd(a_1, \dots a_n) = \gcd(d_{n-1}, a_n)$. Let $x, y \in R$ such that $d_{n-1}x + a_n y = d_n$. Let:

$$A_n = \begin{bmatrix} & & & \frac{a_1}{d_{n-1}}y \\ & & & \frac{a_2}{d_{n-1}}y \\ & A_{n-1} & & \vdots \\ & & & \frac{a_{n-1}}{d_{n-1}}y \\ a_n & 0 \quad \dots \quad 0 & & x \end{bmatrix},$$

with the obvious adjustments when $n = 2$. Clearly A_n has entries in R, and its first column is $a_1 \dots a_n$. It is proven in [N] that $\det(A_n) = d_n$. ■

In the statement of the proposition, we can of course say "row" instead of "column."

Theorem 6.7 (Hermite) *If f is a form in n variables with* **Q** *coefficients and non-zero determinant d and if f is not a zero form, then $f \sim f^{(1)} = \sum a_{i,j}x_ix_j$ with the following properties:*

1. $0 < \mid a_{1,1} \mid \leq (4/3)^{(n-1)/2} \sqrt[n]{\mid d \mid}$,

2. $\mid a_{1,1} \mid \geq 2 \mid a_{1,j} \mid$, *if* $j > 1$,

3. $a_{1,1}f^{(1)} - (a_{1,1}x_1 + \ldots + a_{1,n}x_n)^2 = f^{(2)}$

where $f^{(2)}$ is a form in $n-1$ variables satisfying the same conditions imposed on $f^{(1)}$ with n replaced by $n-1$. The determinant of $f^{(2)}$ is $da_{1,1}^{n-2}$.

For a form f with rational coefficients, we shall call such an $f^{(1)}$ as in Theorem 6.7 to be a *Hermite normal form* (an HNF) for f. This is not necessarily unique. If f can be its own HNF, we say f is in HNF.

Proof/Algorithm. The classical proof of Theorem 6.7 appearing in [Jo] gives us a method to find an HNF for f which is easily implementable on a computer. We shall mention the details which will be required in the algorithm. A form in 1 variable is clearly in HNF already, so we assume that we can find an HNF for a form in $k-1$ variables and from this construct an HNF for a form in k variables. That is, we assume that for every form f in $k-1$ variables, there is a change of variables in $SL_{k-1}(\mathbf{Z})$ which produces an HNF for f.

Let $a_{1,1} \in \mathbf{Q}^\times$ be represented by f, and $X = [c_1 \ldots c_k]$ a solution to $f(X) = a_{1,1}$. Furthermore, we can assume that $\gcd(c_1 \ldots c_k) = 1$. By Proposition 6.6 we can find $C \in SL_k(\mathbf{Z})$ with first column $[c_1 \ldots c_k]$. The transformation $(X')^T = CX^T$ yields a form $f^{(i)}(X') = \sum a_{i,j}x'_ix'_j$.

Suppose that we transform $f^{(i)}$ once more using

$$\begin{array}{rcl} x'_1 &=& y_1 + c_{1,2}y_2 + \ldots + c_{1,k}y_k \\ x'_2 &=& c_{2,2}y_2 + \ldots + c_{2,k}y_k \\ & \cdots\cdots\cdots\cdots\cdots\cdots & \\ x'_k &=& c_{k,2}y_2 + \ldots + c_{k,k}y_k \end{array} \tag{6.1}$$

with $c_{i,j} \in \mathbf{Z}$. We obtain a form $f^{(ii)} = \sum a'_{i,j}y_iy_j$ with $a'_{1,1} = a_{1,1}$. Now let

$$f^{(2)}(y_2 \ldots, y_k) = a_{1,1}f^{(ii)} - (a_{1,1}y_1 + a'_{1,2}y_2 + \ldots + a'_{1,k}y_k)^2 \tag{6.2}$$

By induction, we can find an HNF for the form $f^{(2)}$, and since $f^{(2)}$ is independent of the $c_{1,j}$, we might as well assume that the transformation (6.1) yields an $f^{(2)}$ as in (6.2) which is in HNF. Thus condition (3) is satisfied by $f^{(ii)}$.

Now, the only terms in $f^{(ii)}$ involving y_1 will arise from the summand

$$a_{1,1}x'^2_1 + 2a_{1,2}x'_1x'_2 + \cdots + 2a_{1,k}x'_1x'_k$$

of $f^{(i)}$. Under (6.1), this becomes

$$a_{1,1}y_1^2 + 2\left(a_{1,1}c_{1,2} + \sum_{j=2}^{k} a_{1,j}c_{j,2}\right)y_1y_2 + \ldots + 2\left(a_{1,1}c_{1,k} + \sum_{j=2}^{k} a_{1,j}c_{j,k}\right)y_1y_k,$$

i.e., $a'_{1,r} = a_{1,1}c_{1,r} + \sum_{j=2}^{k} a_{1,j}c_{j,r}$. Thus we can choose every $c_{1,r}$ independently to be an integer such that

$$-\frac{1}{2} \leq \operatorname{sgn}(a_{1,1})c_{1,r} + \frac{1}{|a_{1,1}|}\sum_{j=2}^{k} a_{1,j}c_{j,r} \leq \frac{1}{2}$$

Thus condition (2) can be satisfied.

A sufficient condition for (1) to be satisfied would be that $\mid a'_{1,1} \mid$ is minimal among the $\mid a'_{r,r} \mid$ (see [Jo]). If this is not satisfied, exchange x_1 and x_r to minimize $\mid a'_{1,1} \mid$. Conditions (2) and (3) may no longer be satisfied, but if not, iterate once more from the first step of the algorithm with this new $a_{1,1}$. This process must stop because there are only a finite number of rational numbers in $(0, N)$ represented by f when $X \in \mathbf{Z}^n$, for any $N > 0$. ■

This algorithm is even more explicit when f is positive definite (hence the resulting $f^{(k)}$ are, as well). In this case, the $a_{1,1}$ in the final $f^{(1)}$ is necessarily the *minimum* positive value that f can attain! Initially, we can choose $a_{1,1}$ in the algorithm above to be the value of the smallest $a_{i,i}$ (just to make the process more efficient). Hence, in fact, $C = I$, and the first step is unecessary, yielding $f^{(1)} = f$. Thus the algorithm can be implemented inductively as follows: Begin with $f^{(1)} = \sum_{i,j=1}^{n} a_{i,j}x_ix_j$.

1. Construct $f^{(2)} = a_{1,1}f^{(1)} - (a_{1,1}x_1 + \cdots + a_{1,n}x_n)^2$.
2. Put $f^{(2)}$ in HNF (inductive step).
3. Determine $a_{1,2}, \ldots, a_{1,n}$ to satisfy Axiom (2).
4. If $a_{1,1}$ is minimal among the $a_{i,i}$, then STOP, otherwise swap x_1 and x_r to minimize $a_{1,1}$, and return to Step 1.

Even if a chosen programming language does not support recursion, we see that if n is known beforehand, this algorithm is still easily implemented via nested loops. Also, when Ψ_1 undergoes a change of variable, we must do the same with Ψ_2. Since a change of variables in $SL_8(\mathbf{Z})$ corresponds to a change of $\mathcal{R}$-basis for J, we can even reconstruct this basis for J that gives us a Ψ_1 in HNF. In our implementation, though, we will not be interested in doing this.

In some sense, the HNF of an arbitrary positive definite quadratic form f with $\mathbf{Q}$-coefficients is that form $f^{(1)} \sim f$ which makes $f^{(1)}(X) = M$ "as narrow as possible" in all dimensions except possibly one, in contrast to $f(X) = M$ which may be "long and stretched." We see that $a_{1,1}$ is as small as possible, forcing the determinant of $f^{(2)}$ to be as large as possible. Proceeding thus, we see that $b_{n,n}$ is as large as possible, so x_n is constrained to the smallest possible interval, if we set $f(X) = M$. Going back, we see that for this $b_{n,n}$, $b_{n-1,n-1}$ is as large as possible, so x_{n-1}, for any fixed x_n, is constrained to the smallest possible interval. This was starkly seen in Figure 6.1.

Chapter 7

Finding Type and Ideal Class Representatives

In this chapter, we assemble our constructions into a heuristic algorithm or strategy to find representatives for ideal classes of the maximal order

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

in $\mathbf{B} = (-1,-1)$, the objects we obtained in Chapter 4. Since $H_1 = T_1$, a byproduct of this process is also a set of representatives of type classes of maximal orders in $\mathbf{B}$. Our method is reminiscent of the bare-hands method to compute the ideal class group of a number field. Although the algorithm will be used for these specific objects, it is easy to see that it is also implementable for an arbitrary $\mathbf{B} = (a,b)/F$ and order $\mathcal{O}$, so long as F has properties (P1) and (P2), one has an explicit basis for $\mathcal{O}$, and one knows the class number of $\mathcal{O}$.

We reiterate the assumptions made so far: $m \equiv 5 \bmod 8, F = \mathbf{Q}(\sqrt{m})$, $\mathcal{R}$ is the ring of integers of F, and F possesses properties (P1) $h(F) = 1$ and (P2) $N(u) = -1$ as in Theorem 5.2. The assumptions guarantee that any ideal of $\mathcal{R}$ can be generated by a totally positive element, and every ideal of $\mathbf{B}$ has a basis over $\mathcal{R}$.

7.1 Ideals of the form $J = \mathcal{O}I$

Since our goal is to find ideal classes for a fixed maximal order, we would like to be able first to find left ideals of an arbitrary order $\mathcal{O}$. Fortunately, it is easy to manufacture such ideals in industrial quantities when they are of a particular form. Let $\alpha \in \mathbf{B}\backslash F$. Then $K = F(\alpha)$ is a quadratic field extension of F contained in $\mathbf{B}$, and the non-trivial field automorphism σ' of K fixing F can be thought of to be the conjugation in $\mathbf{B}$, i.e., $\alpha^{(\sigma')} = \overline{\alpha}$, so $N_F^K = \mathbf{nr}|_K$. Let I be an ideal of $\mathcal{S}$, the ring of integers of K. Then $J = \mathcal{O}I$ is a left ideal of $\mathcal{O}$, since $\mathcal{O}(\mathcal{O}I) = \mathcal{O}I$. Also, $\mathbf{nr}(J) = \mathbf{nr}(I)$, since $1 \in \mathcal{O}$. Clearly, if $I' = I\gamma$ for some $\gamma \in K$, then $J' = J\gamma$, so J and J' are in the same left $\mathcal{O}$-ideal class.

Proposition 7.1 *Suppose we choose $\alpha \in \mathcal{O}$, $\alpha \notin \mathcal{R}$ so that $\mathcal{S} = \mathcal{R}[\alpha]$. Then $J = \mathcal{O}I$ is an integral ideal for any ideal I of $\mathcal{S}$, i.e., $J \subset \mathcal{O}$. If I^{-1} is the inverse of I in* $\mathrm{Fr}(K)$, *then $J^{-1} = I^{-1}\mathcal{O}$ and $\mathcal{O}_r(J) = I^{-1}\mathcal{O}I$.*

Proof. Since $\mathcal{O}$ is a ring and $I \subset \mathcal{S} = \mathcal{R}[\alpha] \subset \mathcal{O}$, we have $J \subset \mathcal{O}$. By Proposition D.3,

$$J^{-1} = \overline{J}/\mathbf{nr}(J) = (\overline{\mathcal{O}I})/\mathbf{nr}(I) = \overline{I}\,\overline{\mathcal{O}}/\mathbf{nr}(I) = I^{-1}\mathcal{O},$$

recalling that conjugation is an anti-automorphism, and $\overline{\mathcal{O}} = \mathcal{O}$, since $\mathbf{tr}(\mathcal{O}) \subset \mathcal{R} \subset \mathcal{O}$. We also have:

$$J(I^{-1}\mathcal{O}I) = \mathcal{O}(II^{-1})\mathcal{O}I = \mathcal{O}\mathcal{S}\mathcal{O}I = J,$$

so $I^{-1}\mathcal{O}I \subseteq \mathcal{O}_r(J)$. But $I^{-1}\mathcal{O}I$ has the same level as $\mathcal{O}$ and $\mathcal{O}_r(J)$ by the local-global correspondence, so we have $I^{-1}\mathcal{O}I = \mathcal{O}_r(J)$. ∎

We will now see that it suffices to consider ideals of the form $\mathcal{O}I$ as in the construction above, in order to find representatives of left $\mathcal{O}$-ideal classes.

Theorem 7.2 *Every left $\mathcal{O}$-ideal class of a maximal order $\mathcal{O}$ contains an ideal of the form $\mathcal{O}I$ where I is an ideal in a field extension $K = F(\mathbf{b})$ contained in $\mathbf{B}$.*

Proof. The left $\mathcal{O}$-ideal classes are in bijection with

$$X = M_{\mathbf{G}} \setminus \mathbf{G}(\mathbf{A}_{\mathcal{F}}^f) \,/\, \mathbf{G}(F),$$

as stated in Chapter 1. Since this is a finite set, there is a finite set of primes S such that

$$\mathbf{G}(\mathbf{A}_{\mathcal{F}}^f) = M_{\mathbf{G}}\ \mathbf{B}_S^{\times}\ \mathbf{G}(F), \text{ where}$$

$$\mathbf{B}_S = \prod_{\wp \in S} \mathbf{B}_\wp \subset \mathbf{G}(\mathbf{A}_{\mathcal{F}}^f)$$

Now,

$$i_S(\mathbf{B}) := \{(\mathbf{b}, \ldots, \mathbf{b}) \in \mathbf{B}_S \mid \mathbf{b} \in \mathbf{B}\}$$

is dense in $\mathbf{B}_S$, hence $i_S(\mathbf{B}^{\times})$ is dense in $\mathbf{B}_S^{\times}$. Since $M_{\mathbf{G}}$ is open in $\mathbf{G}(\mathbf{A}_{\mathcal{F}}^f)$, we have, by Strong Approximation (see [Vi])

$$\mathbf{G}(\mathbf{A}_{\mathcal{F}}^f) = M_{\mathbf{G}}\ i_S(\mathbf{B}^{\times})\ \mathbf{G}(F).$$

Thus, every $\beta \in \mathbf{G}(\mathbf{A}_{\mathcal{F}}^f)$ is of the form $\beta = \mu\ i_S(\mathbf{b})\ \mathbf{b}_\circ$ for some $\mu \in M_{\mathbf{G}}$, $\mathbf{b}, \mathbf{b}_\circ \in \mathbf{B}^{\times}$. Thus, under the Local-Global correspondence, the left $\mathcal{O}$-ideal $\mathcal{O}\beta$ is in the same class as $\mathcal{O}i_S(\mathbf{b})$, where $i_S(\mathbf{b})$ can be viewed as a fractional ideal in $F(\mathbf{b})$. ∎

7.2 The Algorithm

We now outline the algorithm for finding representatives for left $\mathcal{O}$-ideal classes:

1. Determine the class number H.
2. Initialize the list of representatives of left $\mathcal{O}$-ideal classes to $L = \{\mathcal{O}\}$.
3. Find an element $\alpha \in \mathcal{O}$, $\alpha \notin \mathcal{R}$, such that the ring of integers $\mathcal{S}$ of the quartic field $K = F[\alpha]$ is exactly $\mathcal{R}[\alpha]$.
4. Determine $h = h(K)$ and $S = \{I_1 \ldots I_h\}$, ideal representatives for the class group of K,

   OR,

   Generate a large (but finite) list $S = \{I_i\}$ of prime ideals of K.
5. Now, for $I_i \in S$, do:
   (a) Find a basis for $J_i = \mathcal{O}I_i$.
   (b) Determine if J_i is in the same class as any of the ideals in L obtained so far. If not, add J_i to L, and keep a note of α and I_i.
6. Stop if H representatives have been found, otherwise resume from Step 3.

The following sections will now explain in further detail the steps above, and give suggestions in order to make the search more efficient.

7.3 Choosing α

Although Theorem 7.2 says that *some* extensions $F(\alpha)$ will yield class representatives, we will content ourselves with first looking through *biquadratic* extensions of F in $\mathbf{B}$. This is solely for practical (computational) reasons. It is easy to verify for such an extension if $\mathcal{R}[\alpha] = \mathcal{S}$, the integers of $K = F(\alpha)$. It would also be easier to find generators for ideals (prime or otherwise) of $\mathcal{R}[\alpha]$ by using methods similar to those in Appendix A.

The main tool to find α's so that $\mathcal{R}[\alpha] = \mathcal{S}$ will be a modification of the algorithm to find representation numbers. The main idea goes as follows: Let n be a squarefree integer relatively prime to m. We know that since $m \equiv 1 \bmod 4$, the ring of integers of $\mathbf{Q}(\sqrt{m}, \sqrt{n})$ is $\mathcal{R}[\phi]$, where ϕ is in Corollary E.2. Thus we wish to find some values for n such that $\alpha \in \mathcal{O}$ satisfies the quadratic polynomial that ϕ does. This requires two variations on the same theme. If $n \equiv 2, 3 \bmod 4$, then α should satisfy $x^2 - n = 0$. Thus α is of the form $r_2\delta_3 + r_4 j + r_3 k$, since its trace has to be 0. We thus modify the procedure to find the representation numbers of $\mathcal{O}$ to find all α of the form above with norm less than some M. After this, of course, we have to eliminate those α whose norm is not squarefree or congruent to 1 mod 4. Similarly, if $n \equiv 1 \bmod 4$, α must satisfy $x^2 - x - \frac{n-1}{4} = 0$. (Since $\mathcal{O}$ is a ring with 1, we could also have chosen $x^2 + x - \frac{n-1}{4}$.) Thus α is of the form $-\delta_1 + r_2\delta_3 + r_4 j + r_3 k$, since its trace has to be -1.

By Proposition E.9, $h(\mathbf{Q}(\sqrt{m}), \mathbf{Q}(\sqrt{n}))$ is a multiple of $h(\mathbf{Q}(\sqrt{n}))$ so if the latter number is large, so is the former. The algorithm is expected to be more efficient if there are many classes in $\mathcal{S}$ to choose from, say at least H classes. Thus we are more interested in the α for which $h(\mathbf{Q}(\sqrt{n}))$ is large.

7.4 Choosing $S = \{I_i\}$

Since the object is to investigate ideals of the form $\mathcal{O}I$, we are not really interested in finding the ideal class group of $K = F(\alpha)$. Methods are available to determine the ideal class group of arbitrary number fields (see, for instance, [PZ]), but the effort to write a computer program to implement these is not worthwhile. If the ideal class group is of small order (or *prime* order), then it would be possible to do it by hand. In particular, if it is prime, any non-principal ideal will generate the class group, so it suffices to find one such non-principal ideal.

In the general case, we may be content with just finding a large collection of *split* prime ideals $\mathcal{Q}$ in K (since every $\wp$ is principal, so is any inert prime in K). By class field theory, every ideal class has an infinite number of prime ideals, so if we have a large enough set of primes, we probably represent all the ideal classes.

7.5 Finding a Basis for an Ideal

We continue to assume that $\alpha \in \mathcal{O}\backslash\mathcal{R}$, $K = F(\alpha)$, such that $\mathcal{R}[\alpha] = \mathcal{S}$, the integers of K. The main problem with ideals of the form $J = \mathcal{O}I$, I an ideal of $\mathcal{S}$, is to find a basis of 4 elements for J. We know that if I is a *prime* ideal of $\mathcal{S}$, it is easy to find two generators for I, knowing the minimal polynomial for α. By induction, [PZ] (p. 400) show how to represent any ideal I in terms of two generators, so we assume that it is easy enough to express I in the form (c_1, c_2), $c_s \in F(\alpha) \subset \mathcal{O}$. In practice, we will often choose I to be prime. Thus if $\mathcal{O} = \mathcal{R}[\beta_1, \ldots \beta_4]$, then J is *generated* over $\mathcal{R}$ by the 8 elements $\{\beta_r c_s\}$.

Now we show how to construct a basis of 4 elements from this set. We shall follow the treatment in [Pi5].

Let $t = 4(s-1)+r$. Write $\beta_r c_s$ as $a_{1,t} + a_{2,t}i + a_{3,t}j + a_{4,t}k$, with $a_{u,t} \in F$. Let A be a greatest common $\mathbf{Z}$-denominator of all the $a_{u,t}$, i.e., all $b_{u,t} = a_{u,t}A \in \mathcal{R}$. We construct the rank-4 matrix $M = [b_{u,t}]_{u=1,4;t=1\ldots8}$, where each column represents a generator of J.

Before we proceed, we would like to point out that it is easy to find $G = \gcd(a,b) \in \mathcal{R}$ for $a, b \in \mathcal{R}$, by looking at $g = \gcd(N_{\mathbf{Q}}^F(a), N_{\mathbf{Q}}^F(b)) \in \mathbf{Z}$, One simply looks at the prime factors p of g and then determine which $\mathcal{R}$-primes $\pi|p$ divide both a and b and accounting for multiplicities. In practice, we construct beforehand a list of primes $\{\pi\}$ where $|N_{\mathbf{Q}}^F(\pi)|$ is less than some large number.

Going back to our task, any matrix obtained by multiplying M on the right with a matrix $C \in SL_8(\mathcal{R})$ (and then dividing by A) will again yield a set of generators for J, that is, by regarding each column as a quaternion in the same way that M was constructed. Thus, our goal is to find C such that MC has four columns of zeroes. It turns out that we can even find C so that MC is in lower triangular form. Naturally, we do this in stages: Let $b_1 = \gcd(b_{1,1}, \ldots, b_{1,8})$. Since $\mathcal{R}$ is a PID, we can express b_1 as

$$b_1 = \eta_1 b_{1,1} + \cdots + \eta_8 b_{1,8} \tag{7.1}$$

with $\eta_t \in \mathcal{R}$ and $\gcd(\eta_1, \ldots, \eta_8) = 1$. By Proposition 6.6, we can find $C \in SL_8(\mathcal{R})$ with first column $[\eta_1 \ldots \eta_8]^T$. Thus $M^{(1)} = MC = [b'_{u,t}]$ has $b'_{1,1} = b_1$ and every $b'_{1,t}$ is divisible by b_1. Let $C = [c_{i,j}] \in SL_8(\mathcal{R})$ with $c_{1,t} = -b_{1,t}/b_1$, 1's on the diagonal, and zeroes everywhere else. Thus we can again multiply $M^{(1)}$ on the right by C to obtain $M^{(2)}$, a matrix with all zeroes on the first row except for column 1, which has b_1. We can do the analogous process to $M^{(3)}$, the matrix obtained by deleting the first row and column of $M^{(2)}$. Proceeding thus, we obtain a lower triangular matrix. Finally, dividing all entries by A, we have $J = \mathcal{R}[\delta_1, \ldots, \delta_4]$, where:

$$\begin{aligned}
\delta_1 &= b_{1,1} + b_{2,1}i + b_{3,1}j + b_{4,1}k \\
\delta_2 &= b_{2,2}i + b_{3,2}j + b_{4,2}k \\
\delta_3 &= b_{3,3}j + b_{4,3}k \\
\delta_4 &= b_{4,4}k
\end{aligned}$$

This algorithm can be generalized to work on ideals in other forms. If $I = \wp_1\wp_2$, for example, we can find a basis for $J = \mathcal{O}I$ by applying the above process to find a basis for $J_1 = \mathcal{O}\wp_1$, then apply it once again to $J_2 = J_1\wp_2$. Similarly, it is possible to construct a basis for the order $I^{-1}\mathcal{O}I$ using this method.

7.6 Finding Solutions To $ax + by = \gcd(a, b)$

The only part of the above algorithm which needs to be made explicit is the process of expressing b_1 as a $\mathcal{R}$-linear combination of the $b_{1,t}$. Since this is done by induction, we illustrate the method for finding $x, y \in \mathcal{R}$ such that $ax + by = 1$, where $a, b \in \mathcal{R}$, $\gcd(a, b) = 1$. Now, if $\gcd(N_{\mathbf{Q}}^F(a), N_{\mathbf{Q}}^F(b)) = 1$, then it is easy to use the Euclidean algorithm to find $x', y' \in \mathbf{Z}$ such that $x'N_{\mathbf{Q}}^F(a) + y'N_{\mathbf{Q}}^F(b) = 1$, in which case we have $(x'a^\sigma)a + (y'b^\sigma)b = 1$, and we are done.

Unfortunately, if we do not have $\gcd(N_{\mathbf{Q}}^F(a), N_{\mathbf{Q}}^F(b)) = 1$, we do not know of any efficient method to find such x, y, except for a straightforward bounded search: Let $x = x_1 + x_2\theta$, $y = y_1 + y_2\theta$, be a solution. Clearly we can restrict x_1, x_2 to be within $0, \ldots, |N_{\mathbf{Q}}^F(b)|$, otherwise we can subtract an appropriate multiple of $N_{\mathbf{Q}}^F(b)$ from x and lump this amount into y. Thus if $|N_{\mathbf{Q}}^F(b)|$ is not too big, we can quickly find a solution by letting x_1 and x_2 go through this range and determining if $y = (1 - ax)/b$ is in $\mathcal{R}$. In any case, this method terminates.

Programming Note: In the inductive process of finding the η_i as in (7.1), one can note enough information in order to construct a matrix as in Proposition 6.6 with first column $[\eta_1 \ldots \eta_k]^T$ and determinant 1. The main ingredient in (6.6) is an expression for $\gcd(\eta_1, \ldots, \eta_i)$ as a $\mathcal{R}$-linear combination of the η_j for every $i \in 1 \ldots k$. To illustrate, suppose we had $a, b, c \in \mathcal{R}$. Let $ax + by = \gcd(a, b)$ and $\gcd(a, b)t + cz = \gcd(a, b, c)$, so $(ax + by)t + cz = a(xt) + b(yt) + cz = \gcd(a, b, c)$. We see that $\gcd(xt, yt) = t$ and $\frac{a}{\gcd(a,b)}xt + \frac{b}{\gcd(a,b)}yt = t$. Similarly, we find an expression for 1 as a linear combination of xt, yt and z. We leave it to the reader to generalize

this to k variables.

7.7 How to Tell Them Apart

We would like to know how to determine if two left $\mathcal{O}$-ideals belong to different ideal classes, which is Step 5b of the algorithm. In the previous chapter, we saw that the Θ-series gives a necessary test for two ideals to be in the same class. Now we give a necessary and *sufficient* condition for two ideals to be in the same class:

Proposition 7.3 *Let I and J be left $\mathcal{O}$-ideals for an Eichler order $\mathcal{O}$. Then I and J belong to the same ideal class if and only if there is an $\alpha \in M := \overline{J}I$ such that $\mathbf{nr}(\alpha) = \mathbf{nr}(I)\mathbf{nr}(J)$, i.e., with $\mathcal{N}_M(\alpha) = 1$.*

This is proven in [Pi5], with the computations valid for any quaternion algebra over a number field. A consequence of the proof is that $I = J\beta$ with $\beta = \alpha/\mathbf{nr}(J)$.

To use this proposition, we will need to construct a basis for $M = \overline{J}I$ and then its Θ-series. Alternatively, we can compute the normalized norm form $\mathcal{N}_M = \Psi_1(X) + \Psi_2(X)\theta$, where Ψ_1 is in Hermite Normal Form, and see to it that the $a_{1,1}$ coefficient of Ψ_1 is not 1. Since this is time consuming, it is often worthwhile to first check if I and J have the same initial terms in their Θ-series, and if this is so, to try again with another ideal.

This concludes the algorithm to find representatives for left $\mathcal{O}$-ideal classes. We will see in a later chapter how this heuristic was actually implemented for the fields that we are interested in. Since we know in the case that we are interested in that $T = H$, we can also find representatives for type classes of maximal orders.

Chapter 8

Brandt Matrices and Eigenforms

Brandt matrices were classically constructed from a complete set of representatives of left $\mathcal{O}$-ideal classes of an Eichler order $\mathcal{O}$ of $\mathbf{B}'$, a definite quaternion algebra over $\mathbf{Q}$ with $\mathrm{Ram}(\mathbf{B}') = \{\infty, p\}$. For such a $\mathbf{B}'$, [Pi5] and [Pi6] show that terms appearing in a so-called Brandt matrix series are actually modular forms (for $\mathbf{Q}$) of a given weight and level p.

Our goals for this chapter are as follows:

1. Extend the definition of Brandt matrices $B(\xi)$ (respectively, modified Brandt matrices $B'(\xi)$) attached to an Eichler order $\mathcal{O}$ of a quaternion algebra over certain quadratic fields F, where $\xi = 0$ or $\xi \in \mathcal{R}_{>>0}$. These are matrices in $\mathrm{Mat}(H \times H, \mathbf{Q})$ (respectively, $\mathrm{Mat}((H-1)\times(H-1), \mathbf{Q})$) where $H = H_1$, the class number of $\mathcal{O}$.

2. Describe an (equivalent) adelic construction for Brandt matrices.

3. Make explicit the adelic definition of Hecke operators on automorphic functions over quaternion algebras in order to define cusp forms.

4. Show that this construction exactly corresponds to the adelic construction of the modified Brandt matrices, and thus

5. Conclude that a basis of eigenvectors for all the modified Brandt matrices corresponds to the set of (normalized) weight 2 eigenforms of full level: such an eigenvector $\mathbf{v}$ corresponds to an eigenform $\mathbf{f}$ such that the eigenvalue of $\mathbf{v}$ with respect to $B'(\pi)$ is the eigenvalue of $\mathbf{f}$ with respect to the $\wp$-th Hecke operator (where $\wp = (\pi)$ and $\pi \in \mathcal{R}_{>>0}$), for every prime $\wp < \infty$.

We shall continue assuming that $F = \mathbf{Q}(\sqrt{m})$ has properties (P1) $h(F) = 1$ and (P2) $N(u) = -1$ as in Theorem 5.2.

8.1 Definition of Brandt Matrices

There is a general notion of Brandt matrices found in [Pi5], in fact including a character, but we shall be content with defining it only in the sense that will be useful to us. In the notation there, our construction will just be for $B_0(\xi, N)$, which will correspond to cusp forms of weight 2.

Let $\mathcal{O}$ be an Eichler order of level $N = q_1 q_2$, $H = H_N$, and $\{I_1, \ldots, I_H\}$ a complete (ordered) set of representatives of distinct left $\mathcal{O}$-ideal classes. As mentioned in Proposition D.4, $\{I_k^{-1} I_1, \ldots, I_k^{-1} I_H\}$ represent the left $\mathcal{O}_r(I_k)$-ideal classes, for every $k \in \{1, \ldots, H\}$. In the notation of Section 6.1, let

$$e_j = e(I_j) = c_{1,\mathcal{O}_r(I_j)} \tag{8.1}$$

which is simply the number of elements of **nr** 1 in the order $\mathcal{O}_r(I_j)$. Note that every unit of $\mathcal{O}_r(I_j)$ is such an element multiplied by an element of $\mathcal{U} = \mathcal{R}^\times$. Define:

$$b_{i,j}(0) = 1/e_j.$$

Now, for $\xi \in \mathcal{R}_{>>0}$, let

$$b_{i,j}(\xi) = \frac{1}{e_j} c_{\xi, I_j^{-1} I_i}$$

which is $1/e_j$ times the number of elements in the left $\mathcal{O}_r(I_j)$-ideal $I_j^{-1}I_i$ of norm $\xi\mathbf{nr}(I_i)/\mathbf{nr}(I_j)$. Now define the *$\xi$-th Brandt matrix for $\mathcal{O}$*, $B(\xi) = B(\xi, \mathcal{O})$:

$$B(\xi, \mathcal{O}) = (b_{i,j}(\xi))_{i,j=1\ldots H}.$$

Proposition 8.1 *The construction of $B(\xi, \mathcal{O})$ depends only on the ordering of the ideal classes. Thus $B(\xi, \mathcal{O})$ is well defined up to conjugation by a permutation matrix.*

Proof. A calculation similar to the proof of Proposition 6.2 shows that $c_{\xi, I_j^{-1}I_i}$ depends only on the left ideal classes of I_i and I_j. Also, $\mathcal{O}_r(I_j\alpha) = \alpha^{-1}\mathcal{O}_r(I_j)\alpha$ where $\alpha \in \mathbf{B}^\times$, so $e(I_j) = e(I_j\alpha)$ (use $\mathbf{nr}(\alpha^{-1}\beta\alpha) = \mathbf{nr}(\beta)$). Hence $b_{i,j}(\xi)$ depends only on the ordering $I_1 \ldots I_H$. ∎

Proposition 8.2 *If $\mathcal{O}$ and $\mathcal{O}'$ are Eichler orders of level N, then there is a permutation matrix M such that $B(\xi, \mathcal{O}) = M^{-1}B(\xi, \mathcal{O}')M$ for all $\xi \in \mathcal{R}_{>>0}$ or $\xi = 0$.*

Proof. Let $\mathcal{O}$ and $\mathcal{O}'$ be two orders of level N. Then there is an $\alpha \in \mathbf{G}(A_F^f)$ such that $\mathcal{O}' = \alpha\mathcal{O}\alpha^{-1}$. If $I_1 \ldots I_H$ are a complete set of representatives of distinct left $\mathcal{O}$-ideal classes, then $\alpha I_1 \ldots \alpha I_H$ is a complete set of representatives of distinct left $\mathcal{O}'$-ideal classes, and the corresponding right orders are still $\mathcal{O}_r(I_j)$. Thus $e(I_j) = e(\alpha I_j)$, and $c_{\xi,(\alpha I_j)^{-1}(\alpha I_i)} = c_{\xi,(I_j^{-1}\alpha^{-1})(\alpha I_i)} = c_{\xi, I_j^{-1}I_i}$. Thus, again only the ordering of the I_j matters, and we obtain the desired conclusion. ∎

In view of this, we shall denote by $B(\xi) = B(\xi, N) = B(\xi, \mathcal{O})$ "the" ξ-th Brandt matrix of level N, for some Eichler order $\mathcal{O}$ of level N.

The following properties of the Brandt matrices are stated in [Pi5] and proven there for quaternion algebras over $\mathbf{Q}$. The proofs carry over to our new definitions for $F = \mathbf{Q}(\sqrt{m})$ with F satisfying (P1) and (P2).

Theorem 8.3 *1.* $e_j b_{i,j}(\xi) = e_i b_{j,i}(\xi)$

2. $\sum_{j=1}^{H} b_{i,j}(\xi)$ *is independent of* i. *Denote this value by* $b(\xi)$. *Then* $b(\xi)$ *is the number of integral left* $\mathcal{O}_i$ *ideals of norm* ξ, *where* $\mathcal{O}_i = \mathcal{O}_r(I_i)$. *Thus this number depends only on the level of* $\mathcal{O}_i$ *and not on the particular order.*

3. The Brandt matrices generate a commutative semisimple ring.

8.2 Modified Brandt Matrices

Define the $H \times H$ matrix A by:

$$A = \begin{bmatrix} 1 & e_1/e_2 & e_1/e_3 & \dots & \dots & e_1/e_H \\ 1 & -1 & 0 & 0 & \dots & 0 \\ 1 & 0 & -1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}$$

Proposition 8.4 *With* A *as above and* $\xi \in \mathcal{R}_{>>0}$ *or* $\xi = 0$,

$$AB(\xi, N)A^{-1} = \begin{bmatrix} b(\xi) & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & B'(\xi, N) & \\ 0 & & & \end{bmatrix}$$

Again, this is proven in [Pi5] with the proof carrying over in our case. The submatrix $B'(\xi) = B'(\xi, N)$ will be referred to as the *ξ-th modified Brandt matrix of level N.*

8.3 The Adelic Construction

Shimizu [Sh] constructs a representation of the Hecke Algebra acting on the space of automorphic forms, and [HPS] show that this can be used to provide another construction of Brandt matrices. We follow the discussion in [HPS], and simplify it for the case that we are interested in.

Let $\mathbf{B} = (-1,-1)$ over $F = \mathbf{Q}(\sqrt{m})$ as before, with all our assumptions on F, $\mathcal{O}$ a maximal order in $\mathbf{B}$, and $\mathbf{B}(\mathbf{A}_F)$ the adelization of $\mathbf{B}$ with respect to $\mathcal{O}$:

$$\mathbf{B}(\mathbf{A}_F) = \{\tilde{a} = (a_\wp) \in \prod_\wp \mathbf{B}_\wp \mid a_\wp \in \mathcal{O}_\wp \text{ for almost all } \wp\},$$

where the product includes the infinite primes. Every left $\mathcal{O}$-ideal is of the form $\mathcal{O}\tilde{a}$, where we interpret this product to mean that (global) lattice which is locally $\mathcal{O}_\wp a_\wp$ for all the finite $\wp$. Let

$$\mathcal{U} = \mathcal{U}(\mathcal{O}) = \{\tilde{u} = (u_\wp) \in \mathbf{B}(\mathbf{A}_F) \mid u_\wp \in \mathcal{O}_\wp^\times \text{ for all } \wp < \infty\}.$$

Since $\tilde{\alpha}\mathcal{U}\tilde{\alpha}^{-1}$ is commensurable with $\mathcal{U}$ for all $\tilde{\alpha} \in \mathbf{B}(\mathbf{A}_F)$, we can define the usual Hecke ring $R(\mathcal{U}, \mathbf{B}(\mathbf{A}_F))$ (see [Shi]). Put

$$\mathcal{U}(\mathbf{A}_F) = \{\tilde{u} = (u_\wp) \in \mathbf{I}_F) \mid u_\wp \in \mathcal{R}_\wp^\times \text{ for all } \wp < \infty\}.$$

Denote also by $\mathbf{nr}$ the usual extension of $\mathbf{nr}$ to $\mathbf{B}(\mathbf{A}_F)$. For $\xi \in \mathcal{R}_{>>0}$, denote by $\mathbf{T}(\xi)$ the element of $R(\mathcal{U}, \mathbf{B}(\mathbf{A}_F))$ which is the sum of all double cosets $\mathcal{U}\tilde{a}\mathcal{U}$ such that $a_\wp \in \mathcal{O}_\wp$ for all $\wp < \infty$ and $\mathbf{nr}(\tilde{a}) \in \xi\mathcal{U}(\mathbf{A}_F)$.

Denote by $\mathcal{M} = \mathcal{M}_2(\mathcal{O})$ the complex vector space of all continuous $\mathbf{C}$-valued functions $f(\tilde{a})$ on $\mathbf{B}(\mathbf{A}_F)$, satisfying

$$f(u\tilde{a}\mathbf{b}) = f(\tilde{a})$$

for all $u \in \mathcal{U}, \tilde{a} \in \mathbf{B}(\mathbf{A}_F)$, and $\mathbf{b} \in \mathbf{B}^\times$. We define a representation of $R(\mathcal{U}, \mathbf{B}(\mathbf{A}_F))$ on $\mathcal{M}$ as follows: For $\mathcal{U}y\mathcal{U} \in R(\mathcal{U}, \mathbf{B}(\mathbf{A}_F))$, let $\mathcal{U}y\mathcal{U} = \cup_i \mathcal{U}y_i$ its decomposition into

disjoint right cosets. Now, let:

$$\rho(\mathcal{U}y\mathcal{U})f(\tilde{a}) = \sum_i f(y_i\tilde{a})$$

and extend ρ to all of $R(\mathcal{U}, \mathbf{B}(\mathbf{A}_F))$ by linearity.

It is shown in [HPS] that the structure of $\mathcal{M}_2(\mathcal{O})$ as a Hecke module is independent of the chosen maximal order.

If H is the class number of $\mathcal{O}$, we have:

$$\mathbf{B}(\mathbf{A}_F) = \bigcup_{\lambda=1}^{H} \mathcal{U}\tilde{x}_\lambda \mathbf{B}^\times.$$

Note that the $I_\lambda = \mathcal{O}\tilde{x}_\lambda$ give a complete set of representatives of left $\mathcal{O}$-ideal classes. The elements of $\mathcal{M}$ are determined by their values at the x_λ. For $f \in \mathcal{M}$, let $f_\lambda = f(\tilde{x}_\lambda)$. The map

$$f \longrightarrow (f_1, \ldots, f_H) \tag{8.2}$$

gives an isomorphism of $\mathcal{M}$ into $\mathbf{C}^H = \mathbf{C}_1 \oplus \ldots \oplus \mathbf{C}_H$, where each $\mathbf{C}_i$ is just a copy of $\mathbf{C}$. We can use the isomorphism 8.2 to give a matrix representation for ρ. For $\xi \in R(\mathcal{U}, \mathbf{B}(\mathbf{A}_F))$, let

$$B(\xi) = [\rho_{i,j}(\xi)]_{i,j=1\ldots H}$$

where $\rho_{i,j}$ is the map from $\mathbf{C}_j$ to $\mathbf{C}_i$ which is the composition of the injection of $\mathbf{C}_j$ into $\mathbf{C}^H$, the inverse of 8.2, $\rho(\xi)$, 8.2, and the projection of $\mathbf{C}^H$ into $\mathbf{C}_i$.

Proposition 8.5 *The definition of $B(\xi)$ yields the same matrix as that in 8.1, assuming that we use the same maximal order $\mathcal{O}$ and set of left $\mathcal{O}$-ideal representatives I_λ.*

This is proven in [HPS].

8.4 Relationship with Cuspforms

We shall now make explicit the isomorphism as Hecke modules between the spaces of Hilbert modular cusp forms and $\mathbf{C}$-valued functions on the finite set X modulo constant functions, which was alluded to in Chapter 1. We will follow the construction of Hida ([Hi]), which is also discussed in [T]. As before, we shall be interested only in the weight 2, full level case.

In Hida's terminology, we let $\mathcal{O}$ be the maximal order which is locally $M_2(\mathcal{S}_\wp)$ for all finite $\wp$. Let

$$U = M_{\mathbf{G}} = \prod_{\wp<\infty} GL_2(\mathcal{S}_\wp),$$

an open subgroup and the finite part of the adelization of $\mathcal{O}$, as in Chapter 1. Denote by $S(U)$ the space of $\mathbf{C}$-valued functions on X. Note that $S(U)$ is just $\mathcal{M}_2(\mathcal{O})$ in the adelic construction of Brandt matrices. The Hecke action on $S(U)$ is that given in Chapter 1. Let $\mathrm{inv}(U)$ be the subspace of $S(U)$ which are functions of the form $f \circ \mathbf{nr}$, where $\mathbf{nr}$ is the (surjective) reduced norm map

$$\mathbf{nr} : \mathbf{G}(\mathbf{A}_F^f) \to \mathbf{I}_F^f$$

and f is a $\mathbf{C}$-valued function on $\mathbf{I}_F^f$ (the finite ideles of F). However, this map, when restricted to the image of $\mathbf{B}^\times$, surjects into the totally positive elements of F (this is the Theorem of Norms in [Vi], p. 80). Since $\mathrm{inv}(U)$ is already a subspace of $S(U)$, we can view $\mathrm{inv}(U)$ as functions of the form

$$\mathbf{G}(\mathbf{A}_F^f) \xrightarrow{\mathbf{nr}} \mathbf{I}_F^f \longrightarrow \mathcal{U}(\mathcal{R}_\wp) \setminus \mathbf{I}_F^f \,/\, F_{>>0} \xrightarrow{\cong} \mathrm{Cl}^+(F) \to \mathbf{C}$$

where $\mathrm{Cl}^+(F)$ is the ray class group of F. It is well known (see [Ma], p. 178) that the order $h^+(F)$ of this group is $2h(F)$ if the fundamental unit u of F is totally positive and $h(F)$ otherwise. Thus, in our case, where we have assumed (P1) and (P2), we see that $h^+(F) = 1$, so $\mathrm{inv}(U)$ is nothing more than the space of constant functions on X.

The Hecke operators certainly fix inv(U). Thus, in order to examine the Hecke action on the space of cusp forms, we must decompose $S(U)$ into an orthogonal sum of inv(U) and a space $S_2(U)$ which is preserved by the Hecke algebra.

Let us describe the Hecke action on inv(U). Let $\mathbf{T}_\wp$ be the $\wp$-th Hecke operator, and f the function which is 1 on all elements of X. In Chapter 1, we saw the decomposition of

$$\left(\prod_{\wp<\infty} GL_2(\mathcal{S}_\wp)\right) g_\wp \left(\prod_{\wp<\infty} GL_2(\mathcal{S}_\wp)\right)$$

into disjoint right cosets. Note, though, that in this decomposition, we also obtain exactly the elements in $\mathbf{B}(\mathbf{A}_F)$ which yield, upon multiplying to the right of $\mathcal{O}$, the set of integral left $\mathcal{O}$-ideals of norm π, where π is a uniformizer for $\wp$. Thus, $\mathbf{T}_\wp(f)$ is the function with constant value equal to the number of such left ideals.

We have seen in Proposition 8.4 that the normalizing matrix A transforms the Brandt matrices into two blocks consisting of a 1×1 cell containing $b(\xi)$ and the modified Brandt matrix $B'(\xi)$. Since we noted that $b(\pi)$ is precisely the number of integral left $\mathcal{O}$-ideals of norm π, where π is a totally positive uniformizer for $\wp$, a prime ideal of F, we see that $B'(\pi)$ precisely gives the action of the Hecke operators on the cusp forms! We summarize this as:

Proposition 8.6 *Let $\{\mathbf{v}_i\}$ be a basis for $\mathbf{C}^{H-1}$ consisting of eigenvectors for all the modified Brandt matrices. Then each $\mathbf{v}_i$ corresponds to a (normalized) holomorphic Hilbert modular eigenform $\mathbf{f}_i$ of weight 2 and full level whose eigenvalue with respect to the $\wp$-th Hecke operator is precisely the eigenvalue of $\mathbf{v}_i$ with respect to $B(\pi)$, where π is a totally positive generator for $\wp$.*

Since we are interested in cusp forms which have rational eigenvalues, we will be looking for eigenvectors for the $B'(\xi)$ which actually have coefficients in $\mathbf{Z}$. In particular, we shall be factoring the characteristic polynomials of these matrices over $\mathbf{Q}$ to find rational roots.

Chapter 9

Calculations

We shall now show that the algorithm that we constructed is effective for the cases that we are interested in. The routines in this algorithm were implemented in the *Maple V* programming environment and were ran on IBM-PC 386 and 486 machines, the *SUN* machines at Caltech and the *CRAY* Supercomputer at the Jet Propulsion Laboratory.

9.1 An Appetizer

We begin with an easy example, where $F = \mathbf{Q}(\sqrt{37})$. For this field, the fundamental unit is $5 + 2\theta$ and the class and type numbers are both 2 . Thus there is an ideal class distinct from that of $\mathcal{O}$. Consider the field extension $K = F[\delta_1]$, where

$$\delta_1 = \frac{1 + i + j + k}{2}$$

is the element in the basis for $\mathcal{O}$ given in Section 4.2. Over F, 3 is a split prime, and

$$-3 = (3 + \theta)(4 - \theta),$$

hence $(3+\theta)u$ is a totally positive generator for one of the prime over 3. Recall that δ_1 is a 6th root of unity, satisfying

$$x^2 - x + 1 = 0.$$

But modulo 3, $x^2 - x + 1 \equiv (x-2)^2$, so the K ideal

$$\wp = (3+\theta, \delta_1 - 2)$$

is the ramified prime dividing $3+\theta$. Let $J = \mathcal{O}\wp$. We computed the first few terms of Θ_J and found that the smallest totally positive integer $a+b\theta$ represented in this series is 2. Hence J and $\mathcal{O}$ are in distinct ideal classes.

By looking at the Θ-series for $\mathcal{O}$, one sees that for this field, $\mathcal{O}$ has 24 elements of **nr** 1. In fact, these elements are precisely the units of $\mathcal{H} \subset \mathcal{O}$ (as in Chapter 4):

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

The right order $\mathcal{O}'$ of J has 6 elements of norm 1. Hence the normalizing matrix A is

$$A = \begin{bmatrix} 1 & 4 \\ 1 & -1 \end{bmatrix}$$

This example has the property that the modified Brandt matrices $B'(\xi)$ are already 1×1 matrices! Thus the lone entry of $B'(\pi)$, when π is totally positive uniformizer for $\wp$, is already the *$\wp$-th eigenvalue* of the unique eigenform in S_2. We assemble below these eigenvalues for $\xi = 1 \ldots 10 + 2\theta$ (in the lexicographic ordering in Proposition E.5) and the primes $\wp = a + b\theta$ of F for $11 \leq a \leq 30$. For the reader's convenience, we have put the entries for ξ and ξ^σ in two consecutive rows without an intervening line, when ξ is prime.

Table 9.1 Hecke Eigenvalues for the Brandt Matrices for $\mathbf{B}/\mathbf{Q}(\sqrt{37})$

$\xi = a + b\theta$	$\xi \mid p \in \mathbf{Z}^{**}$	Eigenvalue
1		1
2	2	0
3	3	−1
4		−1
$4 + \theta$	11	−3
$5 - \theta$		−3
5	5	−3
$5 + \theta$		−3
$6 - \theta$		−3
6		0
$6 + \theta$		3
$6 + 2\theta$		0
$7 - \theta$		3
7		9
$7 + \theta$	47	3
$7 + 2\theta$		5
$8 - 2\theta$		0
$8 - \theta$	47	3
8		0
$8 + \theta$		−6
$8 + 2\theta$		0
$8 + 3\theta$	7	3
$9 - 2\theta$		5
$9 - \theta$		−6
9		4
$9 + \theta$		1
$9 + 2\theta$		−6
$9 + 3\theta$		2
$10 - 2\theta$		0
$10 - \theta$		1
10		0
$10 + \theta$	101	−3
$10 + 2\theta$		0

** - this column is blank if ξ is not a prime in F

Table 9.1 (continued, for ξ a prime)

Hecke Eigenvalues for the Brandt Matrices for $\mathbf{B}/\mathbf{Q}(\sqrt{37})$

$\xi = a + b\theta$	$\xi \mid p \in \mathbf{Z}$	Eigenvalue
$11 - 3\theta$	7	3
$11 - \theta$	101	−3
$11 + 2\theta$	107	−12
$13 - 2\theta$	107	−12
$11 + 3\theta$	73	9
$14 - 3\theta$	73	9
13	13	−10
$13 + \theta$	173	−21
$14 - \theta$	173	−21
$13 + 3\theta$	127	−7
$16 - 3\theta$	127	−7
$14 + 3\theta$	157	3
$17 - 3\theta$	157	3
$14 + 5\theta$	41	−3
$19 - 5\theta$	41	−3
$16 + \theta$	263	9
$17 - \theta$	263	9
$16 + 3\theta$	223	19
$19 - 3\theta$	223	19
17	17	30
$17 + 5\theta$	149	15
$22 - 5\theta$	149	15
$17 + 6\theta$	67	−12
$23 - 6\theta$	67	−12
19	19	2
$19 + 3\theta$	337	13
$22 - 3\theta$	337	13
$19 + 4\theta$	293	−6
$23 - 4\theta$	293	−6

Table 9.1 (continued, for ξ a prime)

Hecke Eigenvalues for the Brandt Matrices for $\mathbf{B}/\mathbf{Q}(\sqrt{37})$

$\xi = a + b\theta$	$\xi \mid p \in \mathbf{Z}$	Eigenvalue
$19 + 6\theta$	151	-8
$25 - 6\theta$	151	-8
$19 + 7\theta$	53	9
$26 - 7\theta$	53	9
$20 + 3\theta$	379	15
$23 - 3\theta$	379	15
$22 + 7\theta$	197	3
$29 - 7\theta$	197	3
23	23	30
$23 + 5\theta$	419	15
$28 - 5\theta$	419	15
$23 + 8\theta$	137	18
$23 + 9\theta$	7	3
$25 + \theta$	641	-33
$26 - \theta$	641	-33
$25 + 3\theta$	619	-35
$28 - 3\theta$	619	-35
$25 + 7\theta$	359	-15
$26 + 3\theta$	673	-21
$29 - 3\theta$	673	-21
$26 + 9\theta$	181	-3
$28 + 3\theta$	787	23
$28 + 9\theta$	307	-7
$28 + 11\theta$	3	-1
29	29	42
$29 + 2\theta$	863	24
$29 + 5\theta$	761	-33
$29 + 6\theta$	691	12
$29 + 9\theta$	373	-21
$29 + 11\theta$	71	-3

The table of [Pin] also has an elliptic curve E over $\mathbf{Q}(\sqrt{37})$ which has good reduction everywhere. For this curve, [Pin] shows that E is isogenous to E^σ. A minimal Weierstrass equation for E is given by:

$$E/\mathbf{Q}(\sqrt{37}) : y^2 + y = x^3 + 2x^2 - (19 + 8\theta)x + (28 + 11\theta)$$

We computed $a_\wp = 1 + N(\wp) - \#E_\wp$ for the $\wp = (\xi)$ in the table above, and these values matched exactly with the eigenvalues of $B'(\xi)$.

Since the dimension of S_2 is 1, there is a single normalized cusp form $\mathbf{f}$. Thus $\mathbf{f} = \mathbf{f} \otimes \epsilon$, hence $\mathbf{f}$ is the base change of an elliptic modular form of weight 2. This is consistent with E being isogenous to E^σ.

9.2 The Main Course

We now tackle the field that we are interested in, $F = \mathbf{Q}(\sqrt{509})$. The fundamental unit of F is $u = 442 + 41\theta$ where $\theta = \frac{1+\sqrt{509}}{2}$, and the class number H is 24.

In the algorithm of Chapter 7, we first find suitable α. The α which eventually led us to distinct ideal classes were i and:

$$\begin{aligned}
\alpha_1 &= \frac{1}{2} + 5i + \frac{1+\theta}{2}j + (1 - \frac{1}{2}\theta)k \\
&= \delta_1 + 9\delta_2 - 4\theta j - (4 + 5\theta)k \\
\mathbf{nr}(\alpha_1) &= 90 \\
k &= -359 \\
h(\mathbf{Q}(\sqrt{-359})) &= 19
\end{aligned}$$

$$\begin{aligned}
\alpha_2 &= \frac{1}{2} + (4 - \frac{1}{2}\theta)i + 2j + \frac{7+\theta}{2}k \\
&= \delta_1 + (7 - \theta)\delta_2 + (65 - 3\theta)j + (63 - 2\theta)k \\
\mathbf{nr}(\alpha_2) &= 96
\end{aligned}$$

$$\begin{aligned} k &= -383 \\ h(\mathbf{Q}(\sqrt{-383})) &= 17 \end{aligned}$$

From Appendix A, we know that $\mathcal{R}[\sqrt{k}]$ has index 2 in the ring of integers of K, for either value of k above. Thus it suffices to consider $\alpha_i' = 2\alpha_i - 1$, $i = 1, 2$, which satisfy $x^2 - k = 0$, in order to generate prime ideals of K which do not divide 2, by Theorem 27 of [Ma]. We prefer α' since it has integer coefficients, and $x^2 - k$ can easily be factored over residue fields $\mathcal{R}/\wp$. Since $h(F) = 1$, we will be interested only in prime ideals of F which split in K, as inert primes are principal. If $x^2 - k$ splits into two distinct factors $(x - \beta_1)(x - \beta_2)$ modulo $\wp = (a + b\theta)$, then

$$\wp = (a + b\theta, \alpha_i' - \beta_1)(a + b\theta, \alpha_i' - \beta_2)$$

and it suffices to consider only one of the ideals I on the right, as they belong to the same K-ideal class. We have $\mathbf{nr}(\mathcal{O}I) = a + b\theta$.

Since the class number of $\mathcal{O}$ is rather large, we first used the Θ-series of $\mathcal{O}I$ for various prime ideals I in extensions $K = F(\alpha)$ above. We chose to let a be between 0 and 30, i.e., we looked at the Θ-series from 1 to $30 + 2\theta$. If the Θ-series of this $\mathcal{O}I$ is distinct from those already encoutered, then we know that this new left ideal is in a different class. Using this method, we discovered that it was even sufficient to consider the Θ-series up to $16 + \theta$ to distinguish 23 of the 24 ideal classes. The following ideals I yielded these classes. The reason for the numbering chosen will be clear in Table 9.3, which shows the Θ-series of $J_i = \mathcal{O}I_i$.

Table 9.2 Prime Ideals $I_i = (a_i + b_i\theta, \gamma_i)$, where $J_i = \mathcal{O}I_i$ have distinct Θ-Series

I_i	K	$a_i + b_i\theta$	γ_i	$I_i \mid p \in \mathbf{Z}$
I_1	F	1		
I_2	$F(\alpha_1)$	61	$-23 + 46\theta - 10i - (1+\theta)j + (-2+\theta)k$	61
I_3	$F(\alpha_1)$	$45 + 4\theta$	$81 - 10i - (1+\theta)j + (-2+\theta)k$	173
I_4	$F(\alpha_1)$	149	$45 - 10i - (1+\theta)j + (-2+\theta)k$	149
I_5	$F(\alpha_1)$	$53 + 5\theta$	$34 - 10i - (1+\theta)j + (-2+\theta)k$	101
I_6	$F(\alpha_1)$	79	$6 - 10i - (1+\theta)j + (-2+\theta)k$	79
I_7	$F(\alpha_1)$	53	$-22 + 44\theta - 10i - (1+\theta)j + (-2+\theta)k$	53
I_8	$F(\alpha_2)$	$23 + 2\theta$	$32 + (-8+\theta)i - 4j - (7+\theta)k$	67
I_9	$F(\alpha_1)$	$9 + \theta$	$14 - 10i - (1+\theta)j + (-2+\theta)k$	37
I_{10}	$F(\alpha_1)$	$10 + \theta$	$7 - 10i - (1+\theta)j + (-2+\theta)k$	17
I_{11}	$F(\alpha_1)$	$184 + 17\theta$	$22 - 10i - (1+\theta)j + (-2+\theta)k$	281
I_{12}	$F(\alpha_1)$	$107 + 10\theta$	$33 - 10i - (1+\theta)j + (-2+\theta)k$	181
I_{13}	$F(\alpha_2)$	47	$-18 + 36\theta + (-8+\theta)i - 4j - (7+\theta)k$	47
I_{14}	$F(\alpha_1)$	31	$-1 + 2\theta - 10i - (1+\theta)j + (-2+\theta)k$	31
I_{15}	$F(\alpha_1)$	$32 + 3\theta$	$3 - 10i - (1+\theta)j + (-2+\theta)k$	23
I_{16}	$F(\alpha_1)$	131	$54 - 10i - (1+\theta)j + (-2+\theta)k$	131
I_{17}	$F(\alpha_1)$	59	$-14 + 28\theta - 10i - (1+\theta)j + (-2+\theta)k$	59
I_{18}	$F(\alpha_2)$	61	$-26 + 52\theta + (-8+\theta)i - 4j - (7+\theta)k$	61
I_{19}	$F(i)$	$31 + 3\theta$	$34 + i$	89
I_{20}	$F(\alpha_1)$	$75 + 7\theta$	$15 - 10i - (1+\theta)j + (-2+\theta)k$	73
I_{21}	$F(\alpha_1)$	13	$-3 + 6\theta - 10i - (1+\theta)j + (-2+\theta)k$	13
I_{22}	$F(\alpha_1)$	157	$-6 + 12\theta - 10i - (1+\theta)j + (-2+\theta)k$	157
I_{23}	$F(i)$	$11 + \theta$	$2 + i$	5

The initial coefficients of the Θ-series of the ideals J_i are tabulated below. We remark that since $\mathcal{O}$ has 24 elements of **nr** 1, every coefficient in these Θ-series is a multiple of 24. Although we computed these coefficients up to $30 + 2\theta$, we observed that it was sufficient to consider the series up to 12 in order to uniquely determine a series, except in seven cases. J_4 and J_5 were indistinguishable up to 16. J_6 became distinguished from J_7 and J_8 at 13, and the latter two were distinguishable at 14. Also, J_{13} and J_{14} were distinguishable at 13. As before, we use the lexicographic ordering for ξ in Proposition E.5. Rows between double lines have the same initial coefficients in their Θ-series, for the range indicated.

Table 9.3 Beginning Coefficients c_{ξ,J_i} of the Θ-Series of J_1 to J_{23}

Ideal:	$\xi = a + b\theta$													
	1	2	3	4	5	6	7	8	9	10	11	$11+\theta$	$12-\theta$	12
J_1	24	24	96	24	144	96	192	24	312	144	288	0	0	96
J_2	0	24	0	24	0	96	0	24	0	144	0	0	0	96
J_3	0	0	24	0	0	24	0	0	96	0	0	0	0	24
J_4	0	0	0	24	0	0	0	24	0	0	0	0	0	96
J_5	0	0	0	24	0	0	0	24	0	0	0	0	0	96
J_6	0	0	0	0	24	0	0	0	0	24	0	0	0	0
J_7	0	0	0	0	24	0	0	0	0	24	0	0	0	0
J_8	0	0	0	0	24	0	0	0	0	24	0	0	0	0
J_9	0	0	0	0	0	24	0	0	0	0	24	0	0	24
J_{10}	0	0	0	0	0	24	0	0	0	0	0	0	0	48
J_{11}	0	0	0	0	0	0	24	0	0	24	0	0	0	24
J_{12}	0	0	0	0	0	0	24	0	0	24	0	0	0	0
J_{13}	0	0	0	0	0	0	24	0	0	0	48	0	0	0
J_{14}	0	0	0	0	0	0	24	0	0	0	48	0	0	0
J_{15}	0	0	0	0	0	0	0	24	24	0	0	0	0	48
J_{16}	0	0	0	0	0	0	0	24	0	24	24	0	0	24
J_{17}	0	0	0	0	0	0	0	24	0	24	48	0	0	0
J_{18}	0	0	0	0	0	0	0	24	0	24	0	0	0	0
J_{19}	0	0	0	0	0	0	0	48	0	0	0	0	0	0
J_{20}	0	0	0	0	0	0	0	0	24	48	48	0	0	0
J_{21}	0	0	0	0	0	0	0	0	48	24	0	0	0	24
J_{22}	0	0	0	0	0	0	0	0	48	0	48	0	0	0
J_{23}	0	0	0	0	0	0	0	0	0	48	48	24	24	48

Table 9.3 continued, for ideals with the same coefficients in the Θ-series above:

Ideal:	$\xi = a + b\theta$									
	$12+\theta$	$13-\theta$	13	$13+\theta$	$14-\theta$	14	$14+\theta$	$15-\theta$	15	$15+\theta$
J_4	0	0	0	0	0	0	0	0	0	0
J_5	0	0	0	0	0	0	0	0	0	0
J_6	0	0	24	0	0	0	0	0	96	0
J_7	0	0	0	0	0	24	0	0	144	24
J_8	0	0	0	0	0	48	0	0	96	0
J_{13}	0	0	48	0	0	24	48	48	0	0
J_{14}	0	0	24	24	24	48	0	0	24	24

Table 9.3 continued, for J_4 and J_5.

Ideal:	$\xi = a + b\theta$								
	$16-\theta$	16	$16+\theta$	$17-\theta$	17	$17+\theta$	$18-\theta$	18	$18+\theta$
J_4	0	24	0	0	48	0	0	24	24
J_5	0	48	0	0	0	0	0	0	0

After a lengthy search which did not yield another ideal with a distinct Θ-series, we switched to using the necessary and sufficient conditions of Proposition 7.3. Let I be an ideal in $\mathcal{S}$ for some $F[\alpha]$ above. The Θ-series of $\mathcal{O}I$ is identical to that of exactly one of the left ideals above, say J_s. We constructed a basis for $I' = I^{-1}J_s$, and computed $\mathcal{N}_{I'}(\alpha) = \Psi_1(X) + \Psi_2(X)\theta$, with Ψ_1 in Hermite normal form. Proposition 7.3 then says that $\mathcal{O}I$ is actually in a *different* class as J_s if and only if $a_{1,1}$, the leading term of Ψ_1, is greater than 1. (This is because $1 + b\theta$ is totally positive if and only if $b = 0$). Using this condition, we quickly determined that

$$J_{24} = \mathcal{O}I_{24} \text{ with } I_{24} = (46 + 5\theta, 334 - 10i - (1+\theta)j + (-2+\theta)k)$$

is the 24th left ideal class, with first few terms of Θ-series identical to that of J_{16}. Here, I_{24} is a prime ideal in $F[\alpha_1]$ dividing 829.

It is also interesting to note that if the corresponding right orders of the left ideals above are $\mathcal{O}_1 \ldots \mathcal{O}_{24}$, then it turns out that these orders all have *distinct* Θ-series, as shown below. Furthermore, if $\mathcal{O}_i$ has basis $\{\gamma_1, \ldots, \gamma_4\}$ it is easy to see that $\mathcal{O}_i^\sigma$, the order with basis $\{\gamma_1^\sigma, \ldots, \gamma_4^\sigma\}$ (where σ acts on coefficients), is once again a maximal order of $\mathbf{B}$. Clearly, σ permutes the order classes. Based on the Θ-series of $\mathcal{O}_i^\sigma$, we observed that σ actually fixes *all* the order classes, *except two*, and it is no surprise that these are $\mathcal{O}_{16}$ and $\mathcal{O}_{24}$.

Table 9.4 Θ-Series for Right Orders

Order:	$\xi = a + b\theta$												
	1	2	3	4	5	6	7	8	9	10	11	$11+\theta$	$12-\theta$
$\mathcal{O}_1$	24	24	96	24	144	96	192	24	312	144	288	0	0
$\mathcal{O}_2$	6	0	24	24	36	0	48	24	78	0	72	0	0
$\mathcal{O}_3$	4	4	0	4	24	0	32	12	48	48	72	0	0
$\mathcal{O}_4$	2	0	6	6	14	8	18	8	24	12	38	0	0
$\mathcal{O}_5$	6	0	6	12	36	0	48	36	6	0	90	0	0
$\mathcal{O}_6$	2	0	4	8	16	8	18	8	12	16	30	0	0
$\mathcal{O}_7$	2	0	8	4	16	2	12	22	32	20	32	0	0
$\mathcal{O}_8$	4	4	0	4	16	16	16	36	28	40	56	4	4
$\mathcal{O}_9$	2	0	4	10	16	4	10	12	22	26	36	0	0
$\mathcal{O}_{10}$	2	2	4	4	14	8	14	18	26	34	32	0	0
$\mathcal{O}_{11}$	2	4	4	8	10	16	14	22	30	34	34	0	0
$\mathcal{O}_{12}$	2	6	8	14	12	24	16	30	26	38	34	0	0
$\mathcal{O}_{13}$	4	4	0	12	24	8	16	36	20	64	48	0	0
$\mathcal{O}_{14}$	2	2	8	2	12	10	22	10	32	28	62	2	2
$\mathcal{O}_{15}$	2	0	4	8	18	8	10	10	16	24	30	0	0
$\mathcal{O}_{16}$	2	0	0	2	2	10	4	20	28	32	20	2	0
$\mathcal{O}_{17}$	2	4	0	8	12	2	20	24	22	46	50	0	0
$\mathcal{O}_{18}$	2	0	2	12	16	6	20	6	10	8	34	0	0
$\mathcal{O}_{19}$	12	36	12	84	72	36	96	180	12	216	144	0	0
$\mathcal{O}_{20}$	4	12	16	28	24	48	4	60	52	72	48	0	0
$\mathcal{O}_{21}$	2	4	0	6	10	8	24	14	26	36	38	0	0
$\mathcal{O}_{22}$	4	4	0	12	24	8	16	36	12	80	40	0	0
$\mathcal{O}_{23}$	4	4	16	4	44	16	32	4	52	44	48	0	0
$\mathcal{O}_{24}$	2	0	0	2	2	10	4	20	28	32	20	0	2

Now that we have concrete representatives of left ideal classes, we were able to explicitly construct the first few Brandt matrices $B(\xi)$ and the modified Brandt matrices $B'(\xi)$, where we chose ξ to range up to $63 + 5\theta$. This involved computing these coefficients for the Θ-series of the 300 ideals $J_r^{-1}J_s, r \geq s$, due to the symmetry properties in Theorem 8.3. We also computed the characteristic polynomials of the $B'(\xi)$ and factored them over the rationals. We found that the polynomial of $B'(19+\theta)$ had three distinct rational roots and an irreducible factor of degree 20. Hence, although $\mathbf{C}^{23}$ has a basis of eigenvectors for all the $B'(\xi)$, only three eigenvectors have eigenvalues which are all rational. The (transpose of the) three eigenvectors $\mathbf{v}_i$ corresponding to these eigenvalues are:

[0, 0, 0, 0, 1, 0, −2, −1, 1, 1, 0, −2, 0, 0, −3, 1, 0, 0, 0, −1, 2, 0, 2]

[0, 0, 0, 0, −1, 0, 2, 1, −1, 1, 0, 2, 0, 0, −2, −1, 0, 0, 0, 1, −2, 0, 3]

[45, 45, 25, 60, 23, 40, 34, 27, 18, 28, 30, 19, 35, 20, 31, 28, 20, 15, 25, 37, 51, 40, 31]

The corresponding eigenvalues are shown in Table 9.5, below:

Table 9.5 Eigenvalues for Simultaneous Rational Eigenvectors for $B'(\xi)$

$\xi = a + b\theta$	$\xi \mid p \in \mathbf{Z}^{**}$	$\mathbf{v}_1$	$\mathbf{v}_2$	$\mathbf{v}_3$
1		1	1	1
2		−1	−1	−1
3	3	−4	−4	1
4		−3	−3	−3
5		6	−6	4
6		4	4	−1
7	7	−6	−6	9
8		7	7	7
9		7	7	−8
10		6	6	−4
11		6	−6	4
$11 + \theta$	5	3	−2	−2
$12 - \theta$	5	−2	3	−2
12		12	12	−3
$12 + \theta$	29	0	10	−5
$13 - \theta$	29	10	0	−5
13	13	1	1	26
$13 + \theta$		4	9	4
$14 - \theta$		9	4	4
14		6	6	−9
$14 + \theta$	83	14	9	14
$15 - \theta$	83	9	14	14
15		24	24	4
$15 + \theta$	113	11	6	11
$16 - \theta$	113	6	11	11
16		5	5	5
$16 + \theta$		30	0	10
$17 - \theta$		0	30	10
17		−6	−6	49
$17 + \theta$	179	0	25	10
$18 - \theta$	179	25	0	10
18		−7	−7	8
$18 + \theta$		8	3	8
$19 - \theta$		3	8	8
19	19	−12	−12	38
$19 + \theta$		3	8	−12

** - this column is blank if ξ is not a prime in F.

Table 9.5 (continued for ξ a Prime)

Eigenvalues for Simultaneous Rational Eigenvectors

$\xi = a + b\theta$	$\xi \mid p \in \mathbf{Z}$	$\mathbf{v}_1$	$\mathbf{v}_2$	$\mathbf{v}_3$
$20 + \theta$	293	16	26	−9
$21 - \theta$	293	26	16	−9
$22 + \theta$	379	−20	20	−10
$23 - \theta$	379	20	−20	−10
$23 + 2\theta$	67	−7	8	−2
$25 - 2\theta$	67	8	−7	−2
$25 + \theta$	523	36	11	36
$26 - \theta$	523	11	36	36
$25 + 2\theta$	167	22	−8	12
$27 - 2\theta$	167	−8	22	12
$29 + \theta$	743	44	−36	14
$30 - \theta$	743	−36	44	14
31	31	−18	−18	57
$32 + \theta$	929	40	10	30
$33 - \theta$	929	10	40	30
$33 + 2\theta$	647	18	43	−2
$35 - 2\theta$	647	43	18	−2
$34 + \theta$	1063	4	−1	34
$35 - \theta$	1063	−1	4	34
$35 + 2\theta$	787	27	32	−48
$37 - 2\theta$	787	32	27	−48
$37 + \theta$	1279	−20	25	−40
$38 - \theta$	1279	25	−20	−40
$39 + \theta$	1433	−71	29	54
$40 - \theta$	1433	29	−71	54
$39 + 2\theta$	1091	60	0	0
$41 - 2\theta$	1091	0	60	0
$40 + 3\theta$	577	−27	33	3
$43 - 3\theta$	577	33	−27	3
41	41	−18	−18	82
$41 + 3\theta$	661	−20	−10	−25
$44 - 3\theta$	661	−10	−20	−25
$43 + 2\theta$	1427	63	−52	−62
$45 - 2\theta$	1427	−52	63	−62
$45 + 2\theta$	1607	42	57	−48
$47 - 2\theta$	1607	57	42	−48

Table 9.5 (continued for ξ a Prime)

Eigenvalues for Simultaneous Rational Eigenvectors

$\xi = a + b\theta$	$\xi \mid p \in \mathbf{Z}$	$\mathbf{v}_1$	$\mathbf{v}_2$	$\mathbf{v}_3$
$45 + 4\theta$	173	9	-1	-11
$49 - 4\theta$	173	-1	9	-11
47	47	44	44	89
$47 + \theta$	2129	30	-75	15
$48 - \theta$	2129	-75	30	15
$50 + \theta$	2423	-24	-69	-24
$51 - \theta$	2423	-69	-24	-24
$51 + 4\theta$	773	-24	-4	-29
$55 - 4\theta$	773	-4	-24	-29
53	53	-19	-19	26
$54 + \theta$	2843	-6	-61	-46
$55 - \theta$	2843	-61	-6	-46
$54 + 5\theta$	11	-2	3	-2
$59 - 5\theta$	11	3	-2	-2
$55 + \theta$	2953	81	-99	6
$56 - \theta$	2953	-99	81	6
$55 + 4\theta$	1213	-46	34	-41
$59 - 4\theta$	1213	34	-46	-41
$56 + 3\theta$	2161	-35	-55	-85
$59 - 3\theta$	2161	-55	-35	-85
$56 + 5\theta$	241	2	-8	2
$61 - 5\theta$	241	-8	2	2
$57 + 5\theta$	359	-6	9	-36
$62 - 5\theta$	359	9	-6	-36
$58 + 5\theta$	479	-24	-4	-4
$63 - 5\theta$	479	-4	-24	-4
59	59	-22	-22	38
$59 + \theta$	3413	-106	-11	-51
$60 - \theta$	3413	-11	-106	-51
$60 + \theta$	3533	6	-84	66
$61 - \theta$	3533	-84	6	66
61	61	-3	-3	122
$62 + \theta$	3779	30	0	90
$63 - \theta$	3779	0	30	90

Chapter 10

The Main Result

10.1 Introduction

We are now in a position to complete the proof of our main result. Let $F = \mathbf{Q}(\sqrt{509})$, $\mathcal{R}$ the ring of integers of F and $\theta = \frac{1+\sqrt{509}}{2}$. We recall that the curve E/F described in Chapter 2 has good reduction everywhere, is not isogenous to its Galois conjugate E^σ, and does not possess potential complex multiplication. We shall presently complete the proof of Theorem 3.1, that is, show that there is a holomorphic Hilbert modular eigenform $\mathbf{f}$ of weight 2 and full level over F, with rational eigenvalues, such that $\mathbf{f}$ does not come from base change of a cusp form over $\mathbf{Q}$. Recall that we have already shown that $\mathbf{f} \neq \mathbf{f} \otimes \epsilon$ for any quadratic character ϵ of F corresponding to a degree 2 imaginary extension of F. We shall also show that the Euler factors in the L-series of E and $\mathbf{f}$ are equal for all primes in Σ, where:

$$\Sigma = \{\pi = a + b\theta \in \mathcal{R}_{>>0} \mid \pi \text{ is a prime of } F \text{ and } 1 < a < 64\}.$$

10.2 The Eigenform

Recall that we have found that there are exactly three simultaneous eigenspaces $< \mathbf{v}_i >, i = 1 \ldots 3$, for all the Brandt matrices $B'(\xi)$ of $\mathcal{O}$, such that the $\mathbf{v}_i$ can be chosen to have entries in $\mathbf{Z}$. By Proposition 8.6, $\mathbf{v}_1$ corresponds to a holomorphic Hilbert modular eigenform $\mathbf{f}$ of weight 2 and full level, whose eigenvalue with respect to the $\wp$-th Hecke operator is the eigenvalue of $\mathbf{v}_1$ with respect to $B'(\pi)$, where $\wp = (\pi)$ and $\pi \in \mathcal{R}_{>>0}$.

10.3 Proof of Theorem 3.1

Now we conclude the proof of Theorem 3.1. Let $\mathbf{f}$ be as above. Since the entries of $\mathbf{v}_1$ are integral and all the $B'(\pi)$ have rational entries, the eigenvalues of $\mathbf{v}_1$ with respect to all the $B'(\pi)$ are rational. Hence the eigenvalues of $\mathbf{f}$ with respect to all the Hecke operators $\mathbf{T}_\wp$ are also rational, for all primes $\wp$.

Next, if $\mathbf{f}$ came from the base change of a cusp form over $\mathbf{Q}$, then

$$a_\wp(\mathbf{f}) = a_{\wp^\sigma}(\mathbf{f})$$

for all primes $\wp$. Thus to show that $\mathbf{f}$ does not come from base change, it suffices to show that there is a prime $\wp$ which does not satisfy the above equality. For a prime $\pi \in \mathcal{R}_{>>0}$, denote by $a_\pi(\mathbf{v}_1)$ the eigenvalue of $\mathbf{v}_1$ with respect to $B'(\pi)$. We observe that

$$a_\pi(\mathbf{v}_1) = 3 \neq -2 = a_{\pi^\sigma}(\mathbf{v}_1),$$

where $\pi = 11 + \theta$, and $\pi^\sigma = 12 - \theta$. Since

$$a_\wp(\mathbf{f}) = a_\pi(\mathbf{v}_1) \qquad \text{and} \qquad a_{\wp^\sigma}(\mathbf{f}) = a_{\pi^\sigma}(\mathbf{v}_1),$$

we get our desired contradiction. This concludes the proof of Theorem 3.1.

10.4 The Comparison Theorem

We now compare the curve E and the cusp form $\mathbf{f}$ corresponding to $\mathbf{v}_1$:

Theorem 10.1 *For the elliptic curve E and the Hilbert modular eigenform $\mathbf{f}$ corresponding to the eigenvector $\mathbf{v}_1$, we have*

$$a_{\wp}(E) = a_{\wp}(\mathbf{f})$$

for all primes $\wp = (\pi)$ and $\pi \in \Sigma$.

The proof of this theorem is by direct computation. For the primes π as described in the theorem which are *split*, we determine n such that $(\pi) = (p, n + \sqrt{m})$, where $p = N(\pi)$, and reduce E using Proposition E.7. We then compute

$$a_{\wp}(E) = 1 + p - \#\tilde{E}_{\wp}(\mathbf{Z}/p)$$

as in Chapter 2. A similar procedure is done for the primes $\pi^{\sigma} = (p, -n + \sqrt{m})$. For inert primes $\wp = (p)$, the coefficients are simply reduced mod p and similar computations done to count points on the reduced curves. In all cases, $a_{\wp}(E) = a_{\wp}(\mathbf{f})$.

10.5 Concluding Remarks

The elliptic curve

$$E'/\mathbf{Q}(\sqrt{509}) \quad : \quad y^2 + (1+\theta)xy + (1+\theta)y$$
$$= \quad x^3 + (-4051846 + 343985\theta)x + 4312534180 - 366073300\theta$$

found in Cremona's paper [Cr] has $a_\wp(E')$ equal to the eigenvalue of $\mathbf{v}_3$ with respect to $B'(\pi)$, with $\pi \in \Sigma$.

This accounts for all three known elliptic curves over F with good reduction everywhere and the only three normalized eigenvectors for the modified Brandt matrices which have rational eigenvalues.

Finally, we note that to any holomorphic Hilbert modular eigenform $\mathbf{f}$ of weight 2, we can attach, as in [T] and [BR], a 2-dimensional ℓ-adic Galois representation (where ℓ is a prime in the field $\mathbf{Q}(\{a_\wp(\mathbf{f})\}) = \mathbf{Q}$):

$$\sigma_\ell(\mathbf{f}) : \mathrm{Gal}(\overline{\mathbf{Q}}/F) \longrightarrow GL_2(\mathbf{Q}_\ell)$$

It is known that $L(\sigma_\ell(\mathbf{f}), s) = L(\mathbf{f}, s)$. Our Theorem above shows that the local Euler factors $L_\pi(\sigma_\ell(\mathbf{f}), s)$ and $L_\pi(\sigma_\ell(E), s)$ are equal for a large number of primes $\wp = (\pi)$ of F.

A method of Faltings and Serre, as described in [Li], gives a way to determine if two diadic representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/K)$ are isomorphic. However, this method is not applicable in our case, since it requires the traces of Frobenius $a_\wp$ to be *even*. As we can see from the tables, some of the traces are odd. In the future, we plan to try to extend this method and remove this restriction.

To conclude, we make the following:

Conjecture 10.2 *The Euler factors of $L(E, s)$ and $L(\mathbf{f}, s)$ are equal at all primes.*

Appendix A

Number Fields and Quadratic Fields

The main sources of this Appendix are [Ma], [CF] and [BS].

A *number field* $\mathcal{F} = \mathbf{Q}[\alpha]$ is a finite-dimensional field extension of $\mathbf{Q}$, for some root α of an irreducible polynomial of $\mathbf{Q}[x]$ in some fixed algebraic closure $\overline{\mathbf{Q}}$. We shall denote by $N = N_{\mathbf{Q}}^{\mathcal{F}}$ and $Tr = Tr_{\mathbf{Q}}^{\mathcal{F}}$ the (absolute) norm and trace functions from $\mathcal{F}$ to $\mathbf{Q}$.

A.1 Ring of Integers

For any $\mathcal{F}$, its *ring of integers*, $\mathcal{S}$, is defined to be the set of elements of $\mathcal{F}$ which satisfy a monic polynomial with integer coefficients. We shall refer to the elements of $\mathcal{S}$ as *algebraic integers* or simply integers when the context is clear; we may also call $\mathcal{S}$ a *number ring*. It is well know that this set in fact constitutes a ring, and it is also a Dedekind domain with fraction field $\mathcal{F}$. Its units are those elements of norm ± 1. The traces and norms of algebraic integers are rational integers.

Henceforth, $\mathcal{F}$ will denote an arbitrary number field, and $\mathcal{S}$ its ring of integers,

unless otherwise specified.

Let $\mathcal{F}$ have degree n over $\mathbf{Q}$. A *module* in $\mathcal{F}$ is a set M which consists of all $\mathbf{Z}$-linear combinations of a finite set of *generators* $\mu_1, \ldots \mu_k$. A set of generators is a *basis* for M if it is linearly independent over $\mathbf{Z}$. Every module M has a basis, and any basis for M has the same cardinality. A *full module* is one which has a basis of n elements. An *order* of $\mathcal{F}$ is a full module which contains 1 and is a ring. The ring of integers of $\mathcal{F}$ is the *maximal* order of $\mathcal{F}$, that is, every order of $\mathcal{F}$ is contained in $\mathcal{S}$. For this reason, some texts use the notation $\mathcal{O}_{\mathcal{F}}$ to denote $\mathcal{S}$, but in this thesis, the symbol $\mathcal{O}$ will denote an order in a different object.

Let $\{\alpha_1, \ldots, \alpha_n\}$ be an ordered basis for $\mathcal{S}$. Any other basis for $\mathcal{S}$ is related to this basis via a transformation in $SL_n(\mathbf{Z})$. Therefore the value

$$\mathrm{disc}(\mathcal{F}) = \mathrm{disc}(\mathcal{S}) = \det(Tr(\alpha_i \alpha_j)_{i,j=1\ldots n})$$

is independent of the basis, and we shall call this the *discriminant* of $\mathcal{F}$ or $\mathcal{S}$.

We shall be particularly interested in quadratic fields $F = \mathbf{Q}(\sqrt{m})$, where m denotes a squarefree integer. We denote by σ the (unique non-trivial) automorphism of F which sends $\sqrt{m}$ to $-\sqrt{m}$. We shall use α^σ to denote the image of α under σ. As usual, the square root of $x > 0$ will be taken to be positive, and that of $x < 0$ will be $\sqrt{-x}i$.

It is known that for quadratic fields $\mathbf{Q}(\sqrt{m})$, its ring of integers $\mathcal{R}$ and discriminant are given by :

$$\begin{aligned} \mathcal{R} &= \begin{cases} \mathbf{Z} + \mathbf{Z}\sqrt{m} & \text{if } m \equiv 2,3 \mod 4 \\ \mathbf{Z} + \mathbf{Z}\theta, \quad \theta = \frac{1+\sqrt{m}}{2} & \text{if } m \equiv 1 \mod 4 \end{cases} \\ \mathrm{disc}(\mathcal{R}) &= \begin{cases} 4m & \text{if } m \equiv 2,3 \mod 4 \\ m & \text{if } m \equiv 1 \mod 4 \end{cases} \end{aligned}$$

From now on, whenever we assume that $m \equiv 1 \mod 4$, we will let $\theta = \frac{1+\sqrt{m}}{2}$.

In this case

$$\text{if } \alpha = a + b\theta,\ a, b \in \mathbf{Q},\ \text{we have}$$
$$\alpha^\sigma = (a+b) - b\theta,\ N(\alpha) = a^2 + ab - b^2\left(\frac{m-1}{4}\right),\ Tr(\alpha) = 2a + b$$

A.2 Ideal Class Group

For any $\mathcal{F}$, the set of ideals of $\mathcal{S}$ form a free monoid under multiplication. The ideals of $\mathcal{S}$ shall be called *integral ideals.* Two integral ideals I and J are *equivalent*, symbolically $I \sim J$, if there exist principal integral ideals (α) and (β), i.e., $\alpha, \beta \in \mathcal{S}$, such that $(\alpha)I = (\beta)J$. This is an equivalence relation, hence it is possible to define a multiplication of equivalence classes of ideals. It is well-known but not obvious that there are only a finite number of equivalence classes of ideals under this relation, and that these classes from a finite group, $\mathrm{Cl}(\mathcal{F})$, called the *ideal class group of* $\mathcal{F}$. Its cardinality, which we denote by $h(\mathcal{F})$ or $h(\mathcal{S})$, will be called the *class group order.* Most authors say *ideal class number*, but this term will be used differently in this thesis. The principal ideals, $\mathrm{Cl}(\mathcal{F})^*$, clearly form the identity class. The inverse of the class of I is the class of any ideal J such that IJ is a principal integral ideal. Hence $\mathcal{S}$ is a principal ideal domain (PID) if and only if $h(\mathcal{F}) = 1$. It is also known that $\mathcal{S}$ is a PID if and only if $\mathcal{S}$ is a unique factorization doman (UFD). Every ideal can be generated over $\mathcal{S}$ by two elements, and in fact one of them can be chosen to be a rational integer, or any fixed non-zero element of the ideal.

We call J a *fractional ideal* of $\mathcal{F}$ if J is a set of the form αI, this time for some $\alpha \in \mathcal{F}^\times$ and I a nonzero integral ideal. This generalizes the concept of an integral ideal. Define J^{-1}, the inverse of J, by:

$$J^{-1} = \{\ \alpha \in \mathcal{F} \mid\ \alpha J \subset \mathcal{S}\ \}.$$

Then $JJ^{-1} = \mathcal{S}$, and the fractional ideals $\mathrm{Fr}(\mathcal{F})$ of $\mathcal{F}$ form a group under multiplication, with $\mathcal{S}$ as the identity. We also see that $\mathrm{Cl}(\mathcal{F})$ is isomorphic to the the quotient $\mathrm{Fr}(\mathcal{F})/\mathrm{Pr}(\mathcal{F})$, where $\mathrm{Pr}(\mathcal{F})$ is the subgroup of principal fractional ideals.

If $I \subset J$ are ideals, then $I^{-1} \supset J^{-1}$. The fractional ideal

$$\mathcal{S}^* = \{ \alpha \in \mathcal{F} \mid Tr(\alpha\mathcal{S}) \subset \mathbf{Z} \}$$

contains $\mathcal{S}$, so $\mathrm{diff}(\mathcal{S}) = (\mathcal{S}^*)^{-1}$ is an integral ideal, called the *absolute different* of $\mathcal{F}$.

Since $\mathcal{S}$ is a Dedekind domain, every ideal I of $\mathcal{S}$ is uniquely expressible as a product of prime ideals of $\mathcal{S}$. Hence, every fractional ideal J can be expressed as a finite product:

$$J = \wp_1^{n_1} \wp_2^{n_2} \dots \wp_k^{n_k}$$

where the $\wp_i$ are distinct prime ideals and $n_i \in \mathbf{Z}$. When J is an integral ideal, the n_i are non-negative.

Every integral prime ideal $\wp$ appears in a factorization of the principal ideal $(p) = p\mathcal{S}$ for some *unique* rational prime p. We say that $\wp$ *divides* p, or equivalently $\wp \supseteq (p)$. We say that a rational prime p is *inert* if (p) is a prime ideal of $\mathcal{S}$. The exact power of $\wp$ in the factorization of (p), denoted $e := e(\wp \mid p)$, is called the *ramification index* of $\wp$ over p. If $e > 1$ for some $\wp$ dividing p, we say that p is *ramified.* The primes p which are ramified are precisely those which divide $\mathrm{disc}(\mathcal{F})$. The residue field $\mathcal{S}/\wp$ is a finite field extension of $\mathbf{Z}/p$. The dimension of $\mathcal{S}/\wp$ over $\mathbf{Z}/p$, denoted $f := f(\wp \mid p)$, is called the *inertial degree* of $\wp$ over p. Define the *norm* of $\wp$ by $N(\wp) = q = p^f$, and extend this definition multiplicatively to any integral ideal.

If $[\mathcal{F} : \mathbf{Q}] = n$, $\wp_1 \dots \wp_r$ the primes dividing $p \in \mathbf{Z}$, $e_1 \dots e_r$ and $f_1 \dots f_r$ the corresponding ramification indices and inertial degrees, then

$$\sum_{i=1}^{r} e_i f_i = n. \tag{A.1}$$

The above formula implies that a prime ideal $\wp$ of the ring of integers of a quadratic field F is one of three kinds:

1. $\wp = (p)$ (*inert* primes) ;

2. $\wp\wp^\sigma = (p)$ (*split* primes) ;

3. $\wp^2 = (p)$ (*ramified* primes) ;

A.3 Valuations, Metrics and Completions

We now consider discrete valuations and metrics on an arbitrary field $\mathcal{F}$. A map $v : \mathcal{F} \to \mathbf{Z} \cup \infty$ is called a discrete valuation of $\mathcal{F}$ if:

1. v maps $\mathcal{F}^\times$ onto $\mathbf{Z}$.

2. $v(0) = \infty$.

3. $v(x + y) \geq \min(v(x), v(y))$ with strict inequality if $v(x) \neq v(y)$.

A map $|\ |: \mathcal{F} \to \mathbf{R}$ is called a metric of $\mathcal{F}$ if for all $x, y \in \mathcal{F}$:

1. $|\ x\ | \geq 0$ and $|\ x\ | = 0 \iff x = 0$.

2. $|\ xy\ | = |\ x\ |\ |\ y\ |$.

3. There is a constant $C \in \mathbf{R}$ such that $|\ 1 + x\ | \leq C$ if $|\ x\ | \leq 1$.

We shall say that two metrics $|\ |_1, |\ |_2$ on $\mathcal{F}$ are *equivalent* if they define the same topology on $\mathcal{F}$. This is so if and only if there is a $c > 0$ such that for all $x \in \mathcal{F}$, $|\ x\ |_1 = |\ x\ |_2^c$. Every valuation is equivalent to one where we can take $C = 2$ in Axiom 3. This gives us the usual triangle inequality: $|\ x + y\ | \leq |\ x\ | + |\ y\ |$. A metric is *discrete* if there is a $\delta > 0$ such that $1 - \delta < |\ x\ | < 1 + \delta$ implies that $|\ x\ | = 1$. A metric is *non-archimedean* if one can take $C = 1$ in Axiom 3; this is so if $|\ x + y\ | \leq \max(|\ x\ |, |\ y\ |)$.

Now we focus on a number field $\mathcal{F}$. For a prime ideal $\wp$ of $\mathcal{S}$, one can consider the *$\wp$-adic valuation* $v_\wp$ on $\mathcal{F}$. Assume that $N(\wp) = q = p^f$. If $\alpha \in \mathcal{F}^\times$, we let

$$v_\wp(\alpha) = \text{ exact power of } \wp \text{ in the factorization of } (\alpha).$$

Define $v_\wp(0) = \infty$. This makes $v_\wp$ a discrete valuation. We can also define a $\wp$-adic metric on $\mathcal{F}$:

$$| \alpha |_\wp = q^{-v_\wp(\alpha)}$$

This defines a discrete non-archimedean metric.

It is known that every field on which a metric is defined can be embedded in its *completion*, which is a (unique) minimal field that is complete with respect to this metric. Denote by $\mathcal{F}_\wp$ the $\wp$-adic completion of $\mathcal{F}$ with respect to the given $\wp$-adic metric. The *ring of integers* of $\mathcal{F}_\wp$, denoted by $\mathcal{S}_\wp$, is defined by

$$\mathcal{S}_\wp = \{ \alpha \in \mathcal{F}_\wp \mid \ | \alpha |_\wp \leq 1 \},$$

a set which is in fact a discrete valuation ring, with fraction field $\mathcal{F}_\wp$. We shall denote also by $\wp$ the maximal ideal of $\mathcal{S}_\wp$, which consists of those $\alpha \in \mathcal{S}_\wp$ with absolute value strictly less than 1.

$\mathcal{F}_\wp$ is a finite extension of $\mathbf{Q}_p$, the p-adic completion of $\mathbf{Q}$ under the usual p-adic metric. We shall only be interested in *local fields* which are completions of a number field, so we shall henceforth symbolize a (non-archimidean) local field by $\mathcal{F}_\wp$.

We shall denote by $\pi_\wp$ a uniformizer for $\mathcal{S}_\wp$, that is, $\wp = (\pi_\wp)$. The units of $\mathcal{S}_\wp$ are those elements with absolute value exactly 1. The residue field $k_\wp = \mathcal{S}_\wp/(\pi_\wp)$ is an extension of $\mathbf{Z}/p$ of degree f. The canonical map $\mathcal{S}_\wp \to k_\wp$ will be denoted by $\tilde{}$, i.e., $r \to \tilde{r}$.

We can also consider field embeddings $\infty_i \ : \ \mathcal{F} \to \mathbf{C}, \ i = 1, \ldots, n = [\mathcal{F} : \mathbf{Q}]$. Each ∞_i defines an archimedean metric:

$$| \alpha |_{\infty_i} = | \infty_i(\alpha) |$$

where the $|\ |$ on the right side above is defined by:

$$\text{for } x, y \in \mathbf{R},\ |\ x\ | = \max(x, -x),\ |\ x + iy\ | = \sqrt{x^2 + y^2}$$

The completion of $\mathcal{F}$ that such a metric defines is isomorphic to either $\mathbf{R}$ or $\mathbf{C}$. We say that ∞_i is a *real embedding* if the completion it defines is $\mathbf{R}$, and non-real otherwise. Non-real embeddings come in complex conjugate pairs ∞_i and $\overline{\infty_i} = c \circ \infty_i$, where c is complex conjugation. Thus if r is the number of real embeddings of $\mathcal{F}$ and s is half the number of non-real embeddings, then $n = r + 2s$. A number field $\mathcal{F}$ is said to be *totally real* if every embedding ∞_i of $\mathcal{F}$ yields $\mathbf{R}$ as its completion. We can also speak of *totally positive* elements of $\mathcal{F}$ or $\mathcal{S}$, which are those α such that $\infty_i(\alpha) > 0$ for every embedding $\infty_i : \mathcal{F} \to \mathbf{R}$. We denote these sets by $\mathcal{F}_{>>0}$ and $\mathcal{S}_{>>0}$. Similarly we can speak of totally negative elements of $\mathcal{F}$ or $\mathcal{S}$.

We denote by $M_{\mathcal{F}}$ the set of inequivalent metrics on $\mathcal{F}$. The non-archimedean metrics will be denoted by $M_{\mathcal{F}}^f$ and the archimedean ones by $M_{\mathcal{F}}^\infty$. It is known that these two classes are in 1-1 correspondence with the distinct primes in $\mathcal{S}$ and the distinct embeddings of $\mathcal{F}$ in $\mathbf{C}$, respectively, the correspondence constructed as above. Hence we shall also refer to them as the *finite primes*, symbolically $\wp < \infty$, and *infinite primes*, respectively. As usual, the phrase "for almost all $\wp$" means "for all but finitely many $\wp$."

We denote by $\mathbf{A}_{\mathcal{F}}$ the *ring of adeles of* $\mathcal{F}$. This consists of all vectors $(\alpha_\wp)_{\wp \in M_{\mathcal{F}}}$ where $\alpha_\wp \in \mathcal{F}_\wp$ and $\alpha_\wp \in \mathcal{S}_\wp$ for almost all $\wp$. Addition and multiplication is defined componentwise. We have $\mathbf{A}_{\mathcal{F}} = \mathbf{A}_{\mathcal{F}}^\infty \times \mathbf{A}_{\mathcal{F}}^f$, where $\mathbf{A}_{\mathcal{F}}^\infty$ are those adeles with 1 at the finite primes, and $\mathbf{A}_{\mathcal{F}}^f$ those with 1 at the infinite primes. The units of $\mathbf{A}_{\mathcal{F}}$, denoted by $\mathbf{I}_{\mathcal{F}}$, is called the *idele group of* $\mathcal{F}$. $\mathcal{F}$ and $\mathcal{F}^\times$ are embedded diagonally in $\mathbf{A}_{\mathcal{F}}$ and $\mathbf{I}_{\mathcal{F}}$, respectively. These are called the *principal* adeles and ideles, respectively.

Dirichlet's Unit Theorem states that for any number field $\mathcal{F}$, the units, $\mathcal{U}$, of the ring of integers $\mathcal{S}$ is a finitely generated abelian group. The torsion part of $\mathcal{U}$ is

the cyclic group of roots of unity in $\mathcal{F}$. The torsion-free part of $\mathcal{U}$ is generated by $r+s-1$ elements of $\mathcal{U}$.

The focus of this thesis is totally real quadratic fields. Henceforth, unless otherwise specified, m will always be a *positive* squarefree rational integer, $F = \mathbf{Q}(\sqrt{m})$ and $\mathcal{R}$ the ring of integers of F, $\mathcal{U}$ its units. From the above, the torsion free part of $\mathcal{U}$ is generated by a single element $u > 1$, which will be called the *fundamental unit* of $\mathcal{R}$. In other words, every unit is of the form $\pm u^k$ for some $k \in \mathbf{Z}$. We shall see in Appendix E that u can be effectively computed, and analytic formulas are available to effectively compute $h(F)$, based only on m and u.

A.4 Extensions

Let $\mathcal{F}'/\mathcal{F}$ be a finite extension of number fields. We can define objects for this extension analogous to some of those we saw above. To begin, $\mathcal{S}'$ and $\wp'$ will denote the corresponding integers and primes in $\mathcal{F}'$. The relative discriminant, $\mathrm{disc}_{\mathcal{F}}^{\mathcal{F}'}$ will be defined using the relative trace and a basis for $\mathcal{S}'$ over $\mathcal{S}$, which is unique up to a square in $\mathcal{U}$. Every $\wp'$ appears in the factorization of the ideal in $\mathcal{S}'$ generated by a unique $\wp$. We can define relative quantities $e(\wp' \mid \wp), f(\wp' \mid \wp)$. The norm $N(\wp') = \wp^f$ is now an integral ideal in $\mathcal{S}$. The sum in (A.1) will now equal the degree of $\mathcal{F}'$ over $\mathcal{F}$. The relative different $\mathrm{diff}(\mathcal{S}'/\mathcal{S})$ is the integral ideal which is the inverse of the dual fractional ideal

$$(\mathcal{S}')^* = \{\, \alpha \in \mathcal{F}' \mid \quad Tr_{\mathcal{F}}^{\mathcal{F}'}(\alpha \mathcal{S}') \subset \mathcal{S} \,\}$$

More importantly, when $\mathcal{F}'/\mathcal{F}$ is *Galois*, we can define certain subgroups of $G = \mathrm{Gal}(\mathcal{F}'/\mathcal{F})$. Let $\wp' \mid \wp$. Define the *decomposition group* of $\wp'$ over $\wp$ by

$$D_{\wp'} = D(\wp' \mid \wp) = \{\, \sigma \in G \mid \ (\wp')^\sigma = \wp' \,\}.$$

Define the *inertia group* of $\wp'$ over $\wp$ by

$$I_{\wp'} = I(\wp' \mid \wp) = \{\, \sigma \in G \mid \ \alpha^\sigma \equiv \alpha \mod \wp' \quad \forall\, \alpha \in \mathcal{S}' \,\}.$$

These are subgroups of G with $I_{\wp'} \subset D_{\wp'}$. Furthermore, the primes over $\wp$ are permuted by the elements of G, and the quantities e and f are independent of the prime over $\wp$.

Appendix B

Elliptic Curves

The main source of this Appendix is [Si].

B.1 Varieties and Morphisms

Let $\mathcal{F}$ be a perfect field. Denote affine n-space over $\mathcal{F}$ by $\mathbf{A}^n[\mathcal{F}]$ or just $\mathbf{A}^n$, defined to be the set of n-tuples over $\overline{\mathcal{F}}$. The set of $\mathcal{F}$-rational points of $\mathbf{A}^n$ are those with coordinates in $\mathcal{F}$. They are precesely those points all of whose coordinates are fixed under the coordinatewise action of all $\sigma \in \mathrm{Gal}(\overline{\mathcal{F}}/\mathcal{F})$.

A subset Y of $\mathbf{A}^n$ is an affine *algebraic set* if it is the set of common zeroes of a set of polynomials $T \subset \overline{\mathcal{F}}[X]$, $X = (x_1 \ldots x_n)$; we write $Y = V(T)$. For any subset Y of $\mathbf{A}^n$, define

$$I(Y) = \{\ f \in A \mid\ f(P) = 0\ \forall\ P \in Y\ \},$$

the ideal of Y. Define $\overline{\mathcal{F}}[Y] = \overline{\mathcal{F}}[X]/I(Y)$, the *affine coordinate ring* of Y. We say that Y is *defined over* $\mathcal{F}$, denoted $Y/\mathcal{F}$, if $I(Y)$ can be generated by polynomials in $\mathcal{F}[X]$. If so, let $I(Y/\mathcal{F}) = I(Y) \cap \mathcal{F}[X]$, and $\mathcal{F}[Y] = \mathcal{F}[X]/I(Y/\mathcal{F})$. Y is a *variety* if $I(Y)$ is a prime ideal in $\overline{\mathcal{F}}[X]$. For a variety $V/\mathcal{F}$, the quotient field of the integral domain $\mathcal{F}[V]$ is denoted $\mathcal{F}(V)$, and called the *function field* of V. The *dimension* of

V is the transcendence degree of $\overline{\mathcal{F}}(V)$ over $\overline{\mathcal{F}}$.

If $f_1 \ldots f_m$ generate $I(V)$, then V is *smooth* at $P \in V$ if the $m \times n$ matrix

$$(\partial f_i/\partial x_j(P))_{1 \le i \le m, 1 \le j \le n}$$

has rank $n - \dim(V)$. V is smooth if it is smooth at every point P. Let

$$M_P = \{ f \in \overline{\mathcal{F}}[V] : f(P) = 0 \}.$$

The *local ring of* V *at* P, $\overline{\mathcal{F}}[V]_P$, is the localization of $\overline{\mathcal{F}}[V]$ at M_P. The elements of $\overline{\mathcal{F}}[V]_P$ are said to be *regular* or *defined* at P.

If f is an irreducible polynomial in $\overline{\mathcal{F}}[X]$, we define the *affine curve* of f in $\mathbf{A}^n$ to be $Y = V(f) = V(\{f\})$. It is a variety with dimension $n - 1$.

Projective n-space over $\mathcal{F}$ will be denoted by $\mathbf{P}^n$. It is the set of equivalence classes of non-zero points $(x_0 \ldots x_n)$ in $\mathbf{A}^{n+1}$ under $(x_0 \ldots x_n) \sim (\lambda x_0 \ldots \lambda x_n)$ for some $\lambda \in \overline{\mathcal{F}}^{\times}$. An ideal I of $\overline{\mathcal{F}}[X] = \overline{\mathcal{F}}[x_0 \ldots x_n]$ is *homogeneous* if it is generated by homogeneous polynomials. A *projective algebraic set* V is of the form:

$$V = V(I) = \{ P \in \mathbf{P}^n \mid f(P) = 0 \ \forall \text{ homogeneous } f \in I \}$$

for a homogeneous ideal I. For such a set, its *homogeneous ideal* $I(V)$ is the ideal in $\overline{\mathcal{F}}[X]$ generated by

$$\{ f \in \overline{\mathcal{F}}[X] \mid f \text{ is homogeneous and } f(P) = 0 \ \forall P \in V \}$$

An algebraic set V is *defined over* $\mathcal{F}$, denoted $V/\mathcal{F}$, if $I(V)$ can be generated by homogeneous polynomials of $\mathcal{F}[X]$. V is a projective *variety* if $I(V)$ is a prime ideal of $\overline{\mathcal{F}}[X]$.

If $V/\mathcal{F}$ is a projective variety and we choose $\mathbf{A}^n \subset \mathbf{P}^n$, then $V \cap \mathbf{A}^n$ is an affine variety. We define the coordinate ring, function field and dimension of V to be those of $V \cap \mathbf{A}^n$ when this set is non-empty. For a point $P \in V$, choose $\mathbf{A}^n$ with

$P \in \mathbf{A}^n \subset \mathbf{P}^n$. We say that V is smoooth at P if $V \cap \mathbf{A}^n$ is smooth at P. Similarly, the local ring of V at P is that of $V \cap \mathbf{A}^n$ at P.

Let $V_1, V_2 \subset \mathbf{P}^n$ be varieties. A *rational map* from V_1 to V_2 is of the form

$$\begin{aligned} \phi &: V_1 \to V_2 \\ \phi &= [f_0, \ldots, f_n], \end{aligned}$$

where $f_0, \ldots f_n$ are such that $\forall\, P \in V_1$ where all f_i are *defined*,

$$\phi(P) = [f_0(P), \ldots, f_n(P)] \in V_2$$

Note that it is not necessary for ϕ to be defined at all the points of V_1. We say that ϕ is defined over $\mathcal{F}$ if there is a $g \in \overline{\mathcal{F}}(V_1)$ such that $gf_i \in \mathcal{F}(V_1)\ \forall\, i$.

A rational map ϕ, as above, is *regular* or *defined* at $P \in V_1$ if there is a $g \in \overline{\mathcal{F}}(V_1)$ such that:

1. $gf_i \in \overline{\mathcal{F}}[V_1]_P\ \forall\, i$, and
2. for some i, $(gf_i)(P) \neq 0$.

A *morphism* is a rational map which is regular at every P. Two varieties V_1 and V_2 are *isomorphic* if there are morphisms $\phi : V_1 \to V_2$ and $\psi : V_2 \to V_1$ such that $\psi \circ \phi = \mathrm{id}_{V_1}$ and $\phi \circ \psi = \mathrm{id}_{V_2}$.

B.2 Weierstrass Equations

Let $\mathcal{F}$ be a field with algebraic closure $\overline{\mathcal{F}}$. An *elliptic curve* E over $\mathcal{F}$ is a pair (E, O), where E is a curve of genus 1 and $O \in E(\mathcal{F})$. The notion of the genus of a curve can be found in [Si], but we will not need it here. For brevity, we shall sometimes say *curve* to mean an elliptic curve. We refer to O as the *basepoint, origin* or *identity* of the curve. Note that for any extension $\mathcal{F}'/\mathcal{F}$, E is again a curve over $\mathcal{F}'$. Every curve is given by a *Weierstrass equation*:

Theorem B.1 *Let E be an elliptic curve defined over $\mathcal{F}$.*

1. *There exist functions $x, y \in \mathcal{F}(E)$ such that the map*

$$\begin{aligned} \phi &: E \to \mathbf{P}^2 \\ \phi &= [x, y, 1] \end{aligned}$$

gives an isomorphism of $E/\mathcal{F}$ onto a curve given by a Weierstrass equation

$$C : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \qquad \text{(B.1)}$$

with coefficients $a_1, \ldots a_6 \in \mathcal{F}$; and such that $\phi(O) = [0, 1, 0]$. We refer to x and y as the Weierstrass coordinate functions of E.

2. *Any two Weierstrass equations for E as in (B.1) are related by a linear change of variables of the form*

$$X = u^2X' + r \qquad Y = u^3Y' + su^2X' + t \qquad \text{(B.2)}$$

with $u, r, s, t \in \mathcal{F}, u \neq 0$.

3. *Conversely, every smooth cubic curve C given by a Weierstrass equation as in (B.1) is an elliptic curve defined over $\mathcal{F}$ with basepoint $O = [0, 1, 0]$.*

Note that $[0,1,0]$ is the only point on the infinite line, and we may regard the rest of E as lying in the affine plane $z = 1$. We define some other quantities for E:

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \end{aligned}$$

The quantity Δ is called the *discriminant* of E. We say that E is non-singular if and only if $\Delta \neq 0$. Under a change of coordinates of the form (B.2), we get $u^{12}\Delta' = \Delta$.

B.3 Galois Conjugate

Suppose that $\mathcal{F}'/\mathcal{F}$ is a Galois extension with Galois group G and E is defined over $\mathcal{F}'$ with a given Weierstrass equation. Then for $\sigma \in G$, we can define the *σ-conjugate* of E as the curve:

$$E^\sigma : Y^2 + a_1^\sigma XY + a_3^\sigma Y = X^3 + a_2^\sigma X^2 + a_4^\sigma X + a_6^\sigma$$

This is a curve with discriminant Δ^σ, so it is nonsingular whenever E is.

B.4 Minimal Equations; Reduction Mod $\wp$

Let $\mathcal{F}_\wp$ be a finite extension of $\mathbf{Q}_p$, and let $\mathcal{S}_\wp$ be its ring of integers, $\pi_\wp$ a uniformizer, $v_\wp$ its normalized valuation. A Weierstrass equation for a curve $E/\mathcal{F}_\wp$ is said to be *minimal* if $v_\wp(\Delta)$ is minimal subject to $a_1 \ldots a_6 \in \mathcal{S}_\wp$. A minimal equation always exists, and is unique up to a change of coordinates of the form (B.2), this time with $r, s, t \in \mathcal{S}$, $u \in \mathcal{S}^\times$. If $a_i \in \mathcal{S}$ and $v_\wp(\Delta) < 12$, then the equation is minimal.

Given a minimal equation for E, one can reduce the coefficients modulo $\pi_\wp$ to obtain an equation over the finite residue field $k_\wp$:

$$\tilde{E}/k_\wp \ : y^2 + \tilde{a_1}xy + \tilde{a_3}y = x^3 + \tilde{a_2}x^2 + \tilde{a_4}x + \tilde{a_6}$$

The curve $\tilde{E}/k_\wp$ will be called the *reduction of E modulo $\pi_\wp$*, or simply the *reduced curve at $\pi_\wp$*. It may or may not be singular. We emphasize that reduction is defined only for a minimal equation. We say that $E/\mathcal{F}_\wp$ has *good* or *stable reduction* over $\mathcal{F}_\wp$ if the reduced curve $\tilde{E}/k_\wp$ is non-singular. This definition is independent of the choice of minimal equation.

Now let $\mathcal{F}$ be a number field with ring of integers $\mathcal{S}$. For a curve $E/\mathcal{F}$ given by a Weierstrass equation (B.1), we can identify $a_1 \ldots a_6$ as elements of $\mathcal{F}_\wp$ for all $v_\wp \in M_\mathcal{F}^f$, so we obtain a minimal Weierstrass equation for E at every $\mathcal{F}_\wp$ given by:

$$\tilde{E}_\wp/\mathcal{F}_\wp : y_\wp^2 + a_{1,\wp}x_\wp y_\wp + a_{3,\wp}y_\wp = x_\wp^3 + a_{2,\wp}x_\wp^2 + a_{4,\wp}x_\wp + a_{6,\wp}$$

with discriminant $\Delta_\wp$. The *minimal discriminant* of $E/\mathcal{F}$, $\mathcal{D}_{E/\mathcal{F}}$, is the ideal of $\mathcal{S}$ given by

$$\mathcal{D}_{E/\mathcal{F}} = \prod_{v_\wp \in M_\mathcal{F}^f} \wp^{v_\wp(\Delta_\wp)}.$$

It is clear that $v_\wp(\Delta_\wp) = 0$ for almost all $\wp$. A *global minimal Weierstrass equation* for $E/\mathcal{F}$ is a Weierstrass equation where $a_1 \ldots a_6 \in \mathcal{S}$ and $\Delta = \mathcal{D}_{E/\mathcal{F}}$. Such an equation is already minimal for all $v_\wp \in M_\mathcal{F}^f$. It exists only under certain conditions which we shall now describe.

Suppose we have *any* equation for E given by $a_1 \ldots a_6$ with discriminant Δ. For every $v_\wp \in M_\mathcal{F}^f$ let

$$x = u_\wp^2 x_\wp + r_\wp \qquad y = u_\wp^3 y_\wp + s_\wp u_\wp^2 y_\wp + t_\wp$$

be a change of coordinates giving the minimal equation for $\wp$. Again, the discriminants are related by $\Delta = u_\wp^{12}\Delta_\wp$, so we can define a fractional ideal a_Δ, given by:

$$a_\Delta = \prod_{v_\wp \in M_\mathcal{F}^f} \wp^{-v_\wp(u_\wp)}.$$

Hence $\mathcal{D}_{E/\mathcal{F}} = (\Delta)a_\Delta^{12}$. The ideal class of a_Δ in $\mathcal{F}$ is independent of the Weierstrass equation chosen for E, and we call the class $\overline{a_\Delta}$ the *Weierstrass class of E/F.*

Proposition B.2 *A global minimal Weierstrass equation for $E/\mathcal{F}$ exists if and only if $\overline{a_\Delta} = (1)$, i.e., a_Δ is principal.*

In particular, if $h(\mathcal{F}) = 1$, a global minimal Weierstrass equation for any curve E always exists. We shall be interested in finding the minimal equation of curves over quadratic fields with class number 1 which have *good reduction everywhere*, that is, for all $\wp < \infty$. These are precisely the curves having $\Delta \in \mathcal{U}$.

B.5 Group Law

It is possible to define an addition law on the points of E which will make E an abelian group with identity O as follows: Let $P, Q \in E$. Let L be the line in $\mathbf{P}^2$ joining P and Q (or the tangent line to E at P if $P = Q$). By Bezout's Theorem, L intersects E at exactly 3 points, counting multiplicities, since E has degree 3. Let R be the third point of intersection of L with E. Let L' be the line joining R and O. Then $P + Q$ is the third point of intersection of L' with E.

Note that under this addition law, R is the inverse of $P+Q$, i.e., $(P+Q)+R = O$. When the coefficients $a_1 \ldots a_6$ and some affine coordinates of P and Q are given, explicit formulas for $P + Q$ can be obtained.

B.6 Isogenies; Endomorphism Ring

Let (E_1, O_1) and (E_2, O_2) be curves. An *isogeny* between E_1 and E_2 is a morphism

$$\phi : E_1 \to E_2$$

satisfying $\phi(O_1) = (O_2)$. We say that E_1 and E_2 are *$\mathcal{F}$-isogenous* if there is a nontrivial isogeny $\phi : E_1 \to E_2$, i.e., with $\phi(E_1) \neq O_2$, and ϕ is defined over $\mathcal{F}$. It is possible for two curves not to be $\mathcal{F}$-isogenous, but $\mathcal{F}'$-isogenous for some extension $\mathcal{F}'/\mathcal{F}$. If E and E' are $\mathcal{F}$-isogenous, then the number of points on the reduced curves $E/\wp$ and $E'/\wp$ are the same for all primes $\wp < \infty$ of $\mathcal{F}$.

Given a nontrivial isogeny $\phi : E_1 \to E_2$, there is a notion of a unique nontrivial *dual isogeny* $\hat{\phi} : E_2 \to E_1$, with certain properties. Any non-constant rational map between curves is surjective, so the composition of non-constant isogenies is a non-constant isogeny. Hence, *being "isogenous" is an equivalence relation.*

Under the addition law, addition and negation define morphisms of the curve. Hence, we can can also define, for two elliptic curves E_1 and E_2 :

$$\mathrm{Hom}(E_1, E_2) = \{ \text{ isogenies } \phi : E_1 \to E_2 \ \}$$

which will be an abelian group under pointwise addition.

If $E_1 = E_2$ then isogenies can also be composed. Thus for a curve E we can define

$$\mathrm{End}(E) = \mathrm{Hom}(E, E)$$

which is a ring with addition as given above and multiplication given by composition.

B.7 Complex Multiplication

The addition law allows us to define or any integer n, *multiplication by n*:

$$[n] : E \to E$$

defined as follows: If $n > 0$, then

$$[n](P) = P + P + \ldots + P \ (n \text{ times})$$

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

Multiplication by n is an isogeny and is obviously a group homomorphism. Also, $[n]E \neq O$ if $n \neq 0$. Thus we can think of $\mathbf{Z}$ as contained in $\mathrm{End}(E)$. There are only three possibilities for the structure of $\mathrm{End}(E)$:

1. $\mathrm{End}(E) \cong \mathbf{Z}$.
2. $\mathrm{End}(E)$ is an order in a quadratic imaginary extension of $\mathbf{Q}$.
3. $\mathrm{End}(E)$ is an order in a quaternion algebra over $\mathbf{Q}$. However, this can happen only if $\mathrm{char}(\mathcal{F}) \neq 0$.

For different reasons, we shall be interested in orders of a quaternion algebra, so these terms will be defined in Section D. The curves which fall in the second and third categories are said to posses *complex multiplication*, abbreviated as CM-curves. We are interested in curves which fall in the *first* category; we shall call them non-CM curves. We also say that $E/\mathcal{F}$ has *potential complex multiplication* if over some extension of $\mathcal{F}'/\mathcal{F}$, $E/\mathcal{F}'$ has complex multiplication.

B.8 The Tate Module; Representation Theory

The kernel of $[n]$ will be denoted by $E[n]$. As an abstract group it is isomorphic to $\mathbf{Z}/n \times \mathbf{Z}/n$. However, it is also acted on by the absolute Galois group of $\mathcal{F}$, $G = \mathrm{Gal}(\overline{\mathcal{F}}/\mathcal{F})$, since if $[n](P) = O$ and $\sigma \in G$, then $[n](P^\sigma) = ([n](P))^\sigma = O$.

We now specialize to multiplication by ℓ^n, where ℓ is a rational prime. We define the *ℓ-adic Tate module of E* to be the group

$$T_\ell(E) = \varprojlim_n E[\ell^n],$$

with the inverse limit being taken with respect to the maps $[\ell]$:

$$E[\ell^{n+1}] \xrightarrow{[\ell]} E[\ell^n].$$

By our remark above, we see that $T_\ell(E)$ is isomorphic to $\mathbf{Z}_\ell \times \mathbf{Z}_\ell$ as an abstract group. However, since the action of G on each $E[\ell^n]$ commutes with $[\ell]$ in the inverse limit above, G also acts on $T_\ell(E)$, and this action is in fact continuous in the pro-finite topology. We thus obtain a *continuous ℓ-adic representation of G on E*:

$$\rho_\ell : G \to \mathrm{Aut}(T_\ell(E))$$

Observe that if we fix a $\mathbf{Z}_\ell$ basis for $T_\ell(E)$, we get a 2-dimensional representation for G over a field of characteristic 0:

$$\rho_\ell : G \to GL_2(\mathbf{Z}_\ell) \to GL_2(\mathbf{Q}_\ell)$$

We shall now define the usual L-series associated to a representation of a Galois group. Let $\mathcal{F}'/\mathcal{F}$ be a normal extension of number fields with Galois group G. Let $\rho : G \to GL(V)$ be a representation into a vector space over a field of characteristic 0 with character χ. For a prime $\wp$ of $\mathcal{F}$, let $\wp' \mid \wp$ be a prime in $\mathcal{F}'$. Let $D_{\wp'}$ and $I_{\wp'}$ be the decomposition group and inertia group of $\wp'$, respectively. Then $D_{\wp'}/I_{\wp'} \cong G_{\wp'}$, the Galois group of the residue extension $k_{\wp'}/k_\wp$. Thus we can define a *Frobenius substitution* $\mathrm{Frob}_{\wp'}$ for $D_{\wp'}/I_{\wp'}$, which corresponds under the isomorphism to a generator of $G_{\wp'}$. Let

$$V^{I_{\wp'}} = \{\, x \in V \mid x^\sigma = x \;\forall\, \sigma \in I_{\wp'} \,\}.$$

We can now define

$$L(\rho, s) = L(\chi, s) = \prod_{\wp < \infty} \det\left(1 - N(\wp)^{-s}\rho(\mathrm{Frob}_{\wp'})\right)\Big|^{-1}_{V^{I_{\wp'}}}.$$

The determinant of the expression above is independent of the choices of $\wp'$ over $\wp$, and depends only on the isomorphism class of ρ. The product converges for all $Re(s) > 1$.

B.9 The L-Series of E

Let $E/\mathcal{F}$ be an elliptic curve defined over a number field. To simplify the definition of the *L-series* of E, we shall assume for the rest of this section that E *has good reduction everywhere.* Let $k_\wp$ be the residue field at $\wp$, $q_\wp = \#k_\wp$, the norm of $\wp$, and $\tilde{E}_\wp/k_\wp$ the reduced curve. The L-series of $E/\mathcal{F}$ is defined by the Euler product

$$L_{E/\mathcal{F}}(s) = \prod_{\upsilon_\wp \in M_\mathcal{F}^f} L_\wp(q_\wp^{-s})^{-1}, \text{ where}$$

$$L_\wp(T) = 1 - a_\wp T + q_\wp T^2 \in \mathbf{Z}[T] \text{ and } a_\wp = q_\wp + 1 - \#\tilde{E}_\wp(k_\wp)$$

This product converges and defines an analytic function for all $s \in \mathbf{C}$, $\mathrm{Re}(s) > \frac{3}{2}$. Section B.6 tells us that *the L-series of two isogenous curves are equal.* We warn that "equality of L-series" means corresponding $\wp$-factors are equal, not just equality of the entire product. For example, for any $E/\mathbf{Q}(\sqrt{m})$, we see that if $\wp$ is inert or ramified, then $\#E_\wp(k_\wp) = E_\wp^\sigma(k_\wp)$, but for $\wp$ with $\wp\wp^\sigma = (p)$, $\#E_\wp(k_\wp) = \#E_{\wp^\sigma}^\sigma(k_{\wp^\sigma})$, so the L-series for E and E^σ are equal taken as a whole product. We shall see later that it is not always true that $\#E_\wp(k_\wp) = \#E_\wp^\sigma(k_\wp)$ (look at the subscripts!).

Let us fix a rational prime ℓ. It is known that for any prime $\wp \not| \ell$, the $\wp$-Euler factor of the representation $\rho_\ell : G = \mathrm{Gal}(\overline{\mathcal{F}}/\mathcal{F}) \to \mathrm{Aut}(T_\ell(E))$ obtained from the ℓ-adic Tate module is equal to the that of the L-series for E! This fact is independent of the ℓ chosen.

Appendix C

Hilbert Modular Forms

The main source of this Appendix is [Ga].

C.1 The Hilbert Modular Group

Let $GL_2^+(\mathbf{R})$ be the set of elements of $GL_2(\mathbf{R})$ with positive determinant. The former group acts on $\mathcal{H}$, the upper half of the complex plane, via linear fractional transformations:

$$\text{if } g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2^+(\mathbf{R}), \quad z \in \mathcal{H}, \quad \text{then } gz = \frac{az+b}{cz+d}$$

Let $\mathcal{F}$ be a totally real number field of degree n over $\mathbf{Q}$, with ring of integers $\mathcal{S}$ and real embeddings $\sigma_1 \ldots \sigma_n$, in some fixed ordering. Taken together, the σ_i give us an embedding of $GL_2(\mathcal{F})$ into $GL_2(\mathbf{R})^n$, and the image of $GL_2(\mathcal{S})$ is a discrete subgroup. Let $GL_2^+(\mathcal{F})$ and $GL_2^+(\mathcal{S})$ denote the elements of $GL_2(\mathcal{F})$ and $GL_2(\mathcal{S})$, respectively, with totally positive determinant. Componentwise, $GL_2^+(\mathbf{R})^n$ acts on $\mathcal{H}^n$, so under the embedding of $GL_2^+(\mathcal{S})$ above, this group also acts on $\mathcal{H}^n$. The group $GL_2^+(\mathcal{S})$ is called the *full Hilbert modular group of* $\mathcal{F}$.

Let $\mathbf{n}$ be a non-zero ideal of $\mathcal{S}$. Define the *principal congruence subgroup of level*

$\mathbf{n}$ by:

$$\Gamma(\mathbf{n}) = \{ \gamma \in GL_2^+(\mathcal{S}) \mid \gamma \equiv I_2 \bmod \mathbf{n} \}.$$

where I_2 is the 2×2 identity matrix. Denote by $Z(\mathcal{S})$ the center of $GL_2^+(\mathcal{S})$. A subgroup Γ of $GL_2^+(\mathcal{F})$ such that $\Gamma(\mathbf{n}) \subset Z(\mathcal{S})\Gamma$ with finite index, for some $\mathbf{n}$, is called a *congruence subgroup of* $GL_2^+(\mathcal{F})$.

C.2 Hilbert Modular Forms

For $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2^+(\mathbf{R})$, $z \in \mathcal{H}$, we define the automorphy factor:

$$\mu(g, z) = \det g^{-1/2}(cz + d).$$

Using standard multi-index notation, we extend this definition to $g = (g_1 \dots g_n) \in GL_2^+(\mathbf{R})^n$, $z = (z_1 \dots z_n) \in \mathcal{H}^n$, and $k = (k_1 \dots k_n) \in \mathbf{Z}^n$, via:

$$\mu(g, z)^k = \prod_{j=1,\dots,n} \mu(g_j, z_j)^{k_j}.$$

For a function $f : \mathcal{H}^n \to \mathbf{C}$, let

$$(f \mid_k g)(z) = f(gz)\mu(g, z)^{-k},$$

where g, z, and k are n-tuples as in the previous paragraph.

Let Γ be a congruence subgroup, $k \in \mathbf{Z}^n$. The space of *weak holomorphic Hilbert modular forms of weight* k *for* Γ is:

$$\mathrm{Wfm}_k(\Gamma) = \{ f : \mathcal{H}^n \to \mathbf{C} \mid f \text{ is holomorphic, and } f \mid_k \gamma = f \ \ \forall \gamma \in \Gamma \}.$$

We shall say that f has weight k and *full level* if $f \in \mathrm{Wfm}_k(SL_2(\mathcal{S}))$.

Proposition C.1 *Let* Γ *be a congruence subgroup, and* $\Lambda = \{u \in \mathcal{F} \left| \begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix} \in \Gamma \}$. *Then any* $f \in \mathrm{Wfm}_k(\Gamma)$ *has a Fourier expansion:*

$$f(z) = \sum_{\xi \in \Lambda^*} c_\xi \exp(2\pi i Tr(\xi z)),$$

where Tr is the **C***-linear extension to* $\mathbf{C}^m \to \mathbf{C}$ *of the Galois trace* $\mathcal{F} \to \mathbf{Q}$*, and* Λ^* *is the dual* **Z***-module:*

$$\Lambda^* = \{\, u \in \mathcal{F} \mid Tr(u\Lambda) \subset \mathcal{S} \,\}$$

The Fourier series is absolutely convergent, and uniformly convergent on compacta.

We say that $f \in \mathrm{Wfm}_k(\Gamma)$ is a *holomorphic Hilbert modular form of weight k for* Γ if $\forall\, g \in GL_2^+(\mathcal{F})$, the Fourier expansion

$$(f \mid_k g)(z) = \sum_{\xi \in \Lambda^*} c_\xi(g) \exp(2\pi i Tr(\xi z)),$$

has $c_\xi(g) = 0$ unless $\xi = 0$ or ξ is totally positive. We shall often simply say "modular form" to mean Hilbert modular form. The $\mathbf{C}$-vector space $\mathrm{Mfm}_k(\Gamma)$, of Hilbert modular forms is finite dimensional.

We define the set of holomorphic Hilbert modular *cuspforms* of weight k for Γ, denoted $\mathrm{Cfm}_k(\Gamma)$, to consist of those $f \in \mathrm{Mfm}_k(\Gamma)$ such that $\forall\, g \in GL_2^+(\mathcal{F})$, the Fourier expansion of $(f \mid_k g)(z)$ above has $c_\xi(g) = 0$ unless ξ is totally positive.

C.3 Hecke Operators

There is a general definition of Hecke operators acting on modular forms of arbitrary level in the adelic language, but fortunately, a simple characterization is possible if we define it only for $\Gamma = SL_2(\mathcal{S})$ and assume that $\mathcal{S}$ is a PID and the totally positive units are squares of units. As a consequence, every $\mathcal{S}$-ideal has a totally positive generator. These conditions will be fulfilled by the quadratic fields that we will be considering.

Let $\mathbf{n} = (\eta)$ be an ideal of $\mathcal{S}$, where η is totally positive. Let

$$\Delta(\mathbf{n}) = \left\{ \delta = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathcal{F}) \;\middle|\; \begin{array}{l} a, b, c, d \in \mathcal{S}, \text{ and } \eta^{-1} \det(\delta) \\ \text{is a totally positive unit} \end{array} \right\}$$

Define $\mathbf{T_n}$, *the* $\mathbf{n}$*-th Hecke operator* on $\mathrm{Mfm}_k(\Gamma)$, by

$$(\mathbf{T_n}(f))(z) = \sum_{\delta \in \Gamma Z(\mathcal{S}) \backslash \Delta(\mathbf{n})} (f \mid_k \delta)(z).$$

where $Z(\mathcal{S})$ is defined in Section C.1. The Hecke operators map cusp forms to cusp forms, and

$$(\mathbf{T_n}(f))(z) = \sum_{\xi \in \mathcal{S}^*} c'_\xi \exp(2\pi i Tr(\xi z)), \text{ where}$$
$$c'_\xi = \eta^{(1-k/2)} \sum_d d^{k-1} c_{\xi\eta/d^2},$$

where d runs through the divisors of η (modulo $\mathcal{U}$), such that $\xi/d \in \mathcal{S}^*$.

The ring $\mathbf{H}$ generated by the Hecke operators form a commutative set of operators acting of $\mathrm{Cfm}_k(\Gamma)$. If $\mathbf{m} + \mathbf{n} = \mathcal{S}$, then $\mathbf{T_{mn}} = \mathbf{T_m T_n}$. For a prime ideal $\wp$, $\mathbf{T}_\wp \mathbf{T}_{\wp^n} = \mathbf{T}_{\wp^{n+1}} + N(\wp)\mathbf{T}_{\wp^{n-1}}$. As a consequence of the commutativity of Hecke operators, there exists a basis of $\mathrm{Cfm}_k(\Gamma)$ consisting of *eigenforms* of every $\mathbf{T_n}$. Suppose we further assume that f is *normalized*, i.e., $c_1 = 1$. Let $\mathbf{T_n}(f) = a_\mathbf{n} f$, say. Then the field $\mathbf{Q}(\{a_\mathbf{n}\})$ generated by the eigenvalues of f for all the Hecke operators is a number field, denoted by $\mathcal{F}_f$.

C.4 L-series of an Eigenform

As with elliptic curves, we can attach an L-series to an eigenform f via:

$$L(f,s) = \prod_{\wp < \infty} \left(1 - a_\wp N(\wp)^{-s} + N(\wp)^{1-2s}\right)^{-1}$$

where $a_\wp$ is the eigenvalue of f with respect to $T_\wp$.

C.5 Galois Representations

We shall follow the treatment of Taylor's Ph.D. thesis [T] to state the existence of a representation of the absolute Galois group of $\mathcal{F}$ attached to f.

Theorem C.2 *Let* $[\mathcal{F} : \mathbf{Q}]$ *be even,* f *a Hilbert modular cuspform of weight* k*, level* $\mathbf{n}$*,* $\mathcal{S}_{\mathcal{F}_f}$ *the ring of integers of* $\mathcal{F}_f$*,* $\wp$ *a prime ideal of* $\mathcal{F}_f$ *dividing* $p \in \mathbf{Z}$*. Then there exists a representation*

$$\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathcal{F}) \to GL_2(\mathcal{S}_{\mathcal{F}_f,\wp})$$

which is unramified outside $\mathbf{n}p$ *such that if* q *is a prime of* $\mathcal{F}$*,* $q \not| \mathbf{n}p$*, then* $\mathrm{tr}\rho(\mathrm{Frob}_q) = a_q$*, and* $\det\rho(\mathrm{Frob}_q) = S_q(f)N(q)$*.*

Appendix D

Quaternion Algebras

The main source for this Appendix is [Vi].

D.1 Definitions

Let $\mathcal{F}$ be a field of any characterstic. A *quaternion algebra* $\mathbf{B}/\mathcal{F} = (D, \delta)$ is a central simple 4-dimensional algebra over $\mathcal{F}$, where D is a 2-dimensional separable algebra over $\mathcal{F}$, and $\delta \in \mathcal{F}^\times$, such that $\mathbf{B} = D + D\mathbf{v}$ (a direct sum), where $\mathbf{v} \in \mathbf{B}$ satisfies $\mathbf{v}^2 = \delta$ and $\mathbf{v}d = \overline{d}\mathbf{v}$ for every $d \in D$, where $d \to \overline{d}$ is the unique non-trivial $\mathcal{F}$-automorphism of D.

We can define an involutive anti-automorphism of $\mathbf{B}$, which we shall call the *conjugation*, via

$$\overline{d_1 + d_2\mathbf{v}} = \overline{d_1} - \overline{d_2}\mathbf{v}.$$

This extends the definition of $\overline{d}$ to $\mathbf{B}$. For $\mathbf{b} \in \mathbf{B}$, we can therefore define the *reduced trace*, $\mathbf{tr}(\mathbf{b})$, and *reduced norm*, $\mathbf{nr}(\mathbf{b})$, via

$$\mathbf{tr}(\mathbf{b}) = \mathbf{b} + \overline{\mathbf{b}}, \quad \mathbf{nr}(\mathbf{b}) = \mathbf{b}\overline{\mathbf{b}}$$

which are $\mathcal{F}$-valued functions. We shall often simply say *trace* and *norm*. The set

$\mathbf{B}^\times$ of invertible elements of $\mathbf{B}$ are precisely those elements with non-zero norm. If $\mathbf{b} \notin \mathcal{F}$, then its minimal polynomial over $\mathcal{F}$ is

$$(x - \mathbf{b})(x - \overline{\mathbf{b}}) = x^2 - \mathbf{tr}(\mathbf{b})x + \mathbf{nr}(\mathbf{b}).$$

When the characteristic of $\mathcal{F}$ is not 2, the above definition of a quaternion algebra is equivalent to the more familiar classical one: (D, δ) is equivalent to a pair (a, b), where $a, b \in \mathcal{F}^\times$ and there exist elements $i, j \in \mathbf{B}$ such that $\{1, i, j, k\}$ is a basis for $\mathbf{B}$ over $\mathcal{F}$ where $k = ij$, and

$$i^2 = a, \quad j^2 = b, \quad ij = -ji.$$

If $\mathbf{b} = x + yi + zj + tk \in \mathbf{B}$, the functions we have defined above may be recast as the more familiar:

$$\overline{\mathbf{b}} = x - yi - zj - tk, \quad \mathbf{tr}(\mathbf{b}) = 2x, \quad \mathbf{nr}(\mathbf{b}) = x^2 - ay^2 - bz^2 + abt^2.$$

D.2 $M_2(\mathcal{F})$

The matrix algebra $M_2(\mathcal{F})$ is always a quaternion algebra for any $\mathcal{F}$. In fact, when $\mathcal{F}$ is *separably closed*, every quaternion algebra is isomorphic to $M_2(\mathcal{F})$. In the definition, we can let:

$$D = \left\{ \begin{bmatrix} x & y \\ -y & x \end{bmatrix} \;\middle|\; x, y \in \mathcal{F} \right\}, \; \mathbf{v} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

D is clearly a quadratic field extension of $\mathcal{F}$, and $\delta = \mathbf{v}^2 = I$, the identity matrix. Here,

$$\text{if } \mathbf{b} = \begin{bmatrix} x & y \\ z & t \end{bmatrix} \in M_2(\mathcal{F}), \text{ then } \overline{\mathbf{b}} = \begin{bmatrix} t & -y \\ -z & x \end{bmatrix},$$
$$\mathbf{tr}(\mathbf{b}) = x + t, \quad \mathbf{nr}(\mathbf{b}) = \det(\mathbf{b}) = xt - yz$$

Note that in the classical definition, it is possible to let

$$i = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad j = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad k = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

D.3 Tensor Products

For extensions $\mathcal{F}'/\mathcal{F}$, the product $\mathcal{F}' \otimes_{\mathcal{F}} \mathbf{B}$ is a quaternion algebra over $\mathcal{F}'$, and

$$\mathcal{F}' \otimes_{\mathcal{F}} (D, \delta) = (\mathcal{F}' \otimes_{\mathcal{F}} D, \delta)$$

In particular, if $\mathbf{B}$ is defined over a number field $\mathcal{F}$, we can form the *localizations* of $\mathbf{B}$ over the completions $\mathcal{F}_\wp$, defined by $\mathbf{B}_\wp = \mathbf{B} \otimes_{\mathcal{F}} \mathcal{F}_\wp$. If $\mathrm{char}(\mathcal{F}) \neq 2$ and $\mathbf{B} = (a, b)$, $a, b \in \mathcal{F} \subset \mathcal{F}_\wp$, then $\mathbf{B}_\wp$ has basis $\{1, i, j, k\}$ over $\mathcal{F}_\wp$.

D.4 Isomorphism Types

We may classify quaternion algebras over $\mathbf{C}$, $\mathbf{R}$, or finite extensions $\mathcal{F}_\wp$ of $\mathbf{Q}_p$ up to isomorphism. As usual, $M_2(\mathcal{F})$ is always a quaternion algebra over $\mathcal{F}$. For $\mathbf{C}$, which is separably closed, this is the only quaternion algebra. For $\mathbf{R}$, the division algebra $\mathbf{H} = (-1, -1)$ is the only other possibility. For $\mathcal{F}_\wp$, the division algebra $(D_{nr}, \pi_\wp)$ is the only other possibility, where D_{nr} is the unique two dimensional unramified extension of $\mathcal{F}_\wp$ and $\pi_\wp$ is a uniformizer for $\mathcal{F}_\wp$.

For a number field $\mathcal{F}$, the classification goes as follows: Denote by $S = \{\infty_1, \ldots, \infty_r\}$ the set of *real* embeddings in $M_{\mathcal{F}}^{\infty}$.

Theorem D.1 *Every quaternion algebra* $\mathbf{B}$ *over* $\mathcal{F}$ *is determined up to isomorphism by a finite set* $\mathrm{Ram}(\mathbf{B}) \subset S \cup M_{\mathcal{F}}^{f}$ *of* <u>*even*</u> *cardinality, such that:*

$$\mathbf{B}_\wp \cong \begin{cases} \text{the division algebra} & \text{if } \wp \in \mathrm{Ram}(\mathbf{B}) \\ \text{the matrix algebra} & \text{if } \wp \notin \mathrm{Ram}(\mathbf{B}) \end{cases}$$

$\mathrm{Ram}(\mathbf{B})$ *is called the* ramification set *of* $\mathbf{B}$*, and we say that* $\mathbf{B}$ *is* ramified *at the primes in* $\mathrm{Ram}(\mathbf{B})$ *(respectively,* $\mathbf{B}$ *is* split *or* unramified *at the primes not in* $\mathrm{Ram}(\mathbf{B})$*). Furthermore, every subset of even cardinality of* $S \cup M_{\mathcal{F}}^{f}$ *occurs as the ramification set of some quaternion algebra* $\mathbf{B}$.

For $\mathbf{B} = (a, b)$, the isomorphism type of $\mathbf{B}_\wp$ over $\mathcal{F}_\wp$ is determined by the *Hilbert symbol* $(a, b)_{\mathcal{F}_\wp}$ in the respective field:

$$(a,b)_{\mathcal{F}_\wp} = \begin{cases} 1 & \text{if } ax^2 + by^2 - z^2 \text{ has a nontrivial solution in } \mathbf{A}^3(\mathcal{F}_\wp) \\ -1 & \text{otherwise} \end{cases}$$

$B_\wp$ is the matrix algebra if and only if $(a, b)_{\mathcal{F}_\wp} = 1$ in $\mathcal{F}_\wp$.

We call a quaternion algebra $\mathbf{B}$ defined over a number field $\mathcal{F}$ *positive definite* if over every *real* embedding ∞_i, the localization of $\mathbf{B}$ over the completion of $\mathcal{F}$ with respect to ∞_i is a division algebra. The above tells us that when F is a totally real quadratic field, there is a unique quaternion algebra, up to isomorphism, which is positive definite and is a matrix algebra for every finite completion of F.

D.5 Ideals and Orders

We now define some more objects when the center of $\mathbf{B}$ is the fraction field of a *Dedekind domain.* As stated before, this is the case when the center $\mathcal{F}$ is a number field or a finite extension of $\mathbf{Q}_p$. Hence, to be consistent with our notation, we shall use $\mathcal{S}$ to denote the Dedekind domain and $\mathcal{F}$ its quotient field, keeping in mind that we can put a subscript of "$\wp$" on both.

Let $\mathbf{V}$ be a vector space over $\mathcal{F}$ (for example, $\mathbf{V} = \mathbf{B}$). An *$\mathcal{S}$-lattice* of $\mathbf{V}$ is a finitely generated $\mathcal{S}$-module contained in $\mathbf{V}$. A *complete $\mathcal{S}$-lattice* of $\mathbf{V}$ is an $\mathcal{S}$-lattice $\mathcal{L}$ of $\mathbf{V}$ such that $\mathcal{F} \otimes_{\mathcal{S}} \mathcal{L} \cong \mathbf{V}$. An *ideal* of $\mathbf{B}$ is a complete $\mathcal{S}$-lattice of $\mathbf{B}$.

We say that $\mathbf{b} \in \mathbf{B}$ is an *integer*, or is *integral* (in $\mathcal{S}$) if $\mathcal{S}[\mathbf{b}]$ is an $\mathcal{S}$-lattice of $\mathbf{B}$. This is so if and only if both $\mathbf{tr}(\mathbf{b})$ and $\mathbf{nr}(\mathbf{b})$ are in $\mathcal{S}$. We must warn that unlike number fields, the integers of $\mathbf{B}$ *do not* always form a ring; they are in general not closed under addition nor multiplication. This fact motivates an object which is of great interest in this thesis:

An *order* $\mathcal{O}$ of $\mathbf{B}$ is:

- an ideal which is a ring (or equivalently)
- a ring $\mathcal{O}$ consisting of integers and containing $\mathcal{S}$, such that $\mathcal{F}\mathcal{O} = \mathbf{B}$.

We shall mostly be interested in quaternion algebras over number fields with class group order 1. In this case, every lattice is given by a basis of 4 elements. Let $\mathcal{O}$ be an order given by a basis $\{u_1 \ldots u_4\}$. We define an integral ideal called the *discriminant* $\mathrm{disc}(\mathcal{O})$ as:

$$\mathrm{disc}(\mathcal{O}) = \mathcal{S}(\det(\mathbf{tr}(u_i u_j))_{i,j=1..4})$$

Some texts take the square root of the ideal on the right, which can be shown to be a square ideal.

A *maximal order* is an order which is not strictly contained in any order. Maximal orders always exist, and every order is contained in a maximal order. If the finite primes in $\mathrm{Ram}(\mathbf{B})$ are $\wp_1 \ldots \wp_r$, then an order $\mathcal{O}$ is maximal if and only if $\mathrm{disc}(\mathcal{O}) = (\wp_1..\wp_r)^2$. Unlike the case in number fields where the maximal order is the ring of integers, maximal orders in a quaternion algebra are far from unique.

For any ideal J of $\mathbf{B}$, we have the following canonical orders:

$$\begin{aligned} \mathcal{O}_\ell(J) &= \{\, \mathbf{b} \in \mathbf{B} \mid \mathbf{b}J \subset J \,\} \\ \mathcal{O}_r(J) &= \{\, \mathbf{b} \in \mathbf{B} \mid J\mathbf{b} \subset J \,\} \end{aligned}$$

which are respectively called the *left order* and *right order* of J, respectively. These are, in fact, orders. In general, if J is an ideal and $\mathcal{O}$ is any order, we say that J is a *left $\mathcal{O}$-ideal*, respectively J is a *right $\mathcal{O}$-ideal*, if $\mathcal{O}J \subset J$, respectively $J\mathcal{O} \subset J$. Hence, for example, J is a left $\mathcal{O}_\ell(J)$-ideal.

We call J an *integral ideal* if $J \subset \mathcal{O}_\ell(J)$ (or equivalently, $J \subset \mathcal{O}_r(J)$). We call $\mathcal{O}$ an *Eichler order* if it is the intersection of two maximal orders. Hence maximal orders are likewise Eichler orders.

D.6 Local Orders

Let us characterize some orders concretely when the center of $\mathbf{B}$ is $\mathcal{F}_\wp$, a finite extension of $\mathbf{Q}_p$. When $\mathbf{B} = M_2(\mathcal{F}_\wp)$, the maximal orders are all of the form $\mathbf{b}^{-1}M_2(\mathcal{S}_\wp)\mathbf{b}$, where $\mathbf{b} \in \mathbf{B}^\times$, i.e., all maximal orders are conjugate. Similarly, every Eichler order is conjugate to

$$\mathcal{O}_n = \begin{pmatrix} \mathcal{S}_\wp & \mathcal{S}_\wp \\ \wp^n & \mathcal{S}_\wp \end{pmatrix}$$

for a unique non-negative integer n. In this case, we say that the order has *level* $\wp^n$

When $\mathbf{B}$ is the (unique) division algebra over $\mathcal{F}_\wp$, then

$$\mathcal{O} = \{\ \alpha \in \mathbf{B}\ \mid \mathbf{nr}(\alpha) \in \mathcal{S}_\wp\ \}$$

is the unique maximal order of $\mathbf{B}$. Hence this is also the unique Eichler order.

D.7 The Local-Global Correspondence

It is not surprising that there is a relationship between these objects in the algebra $\mathbf{B}$ defined over a number field and those in the localizations $\mathbf{B}_\wp$ for *finite* primes $\wp$. For $\mathcal{L}$ an ideal in $\mathbf{B}$, define its *localization* $\mathcal{L}_\wp = \mathcal{L} \otimes_{\mathcal{S}} \mathcal{S}_\wp$. We shall denote by $\mathbf{B}(\mathbf{A}_\mathcal{F})$ the adelization of $\mathbf{B}$:

$$\mathbf{B}(\mathbf{A}_\mathcal{F}) = \{\ (\alpha_\wp)_{\wp \in M_\mathcal{F}} | \alpha_\wp \in \mathbf{B}_\wp\ \forall\ \wp \in M_\mathcal{F} \text{ and } \alpha_\wp \in \mathcal{O}_\wp \text{ for almost all } \wp\ \}$$

where $\mathcal{O}$ is any (fixed) order of $\mathbf{B}$.

We say that a property of an ideal is *local* if any ideal $\mathcal{L}$ has that property if and only if $\mathcal{L}_\wp$ has that property for every $\wp < \infty$. The following properties are local:

1. being an integral ideal.

2. being an order.

3. being an Eichler order.

4. being a maximal order.

The proofs of these facts make use of the following

Proposition D.2 *Let X be a fixed ideal of* $\mathbf{B}$. *There is a bijection between the set of ideals Y of* $\mathbf{B}$, *and the following set of tuples of lattices indexed by $M_{\mathcal{F}}^f$:*

$$\{ (Y_\wp)_{\wp<\infty} \mid Y_\wp \text{ is a lattice of } \mathbf{B}_\wp \text{ such that } Y_\wp = X_\wp \text{ for almost all } \wp \}$$

This bijection is given by the following functions:

$$Y \to (Y_\wp)_{\wp<\infty}, \quad (Y_\wp)_{\wp<\infty} \to Y = \{ \alpha \in \mathbf{B} \mid \alpha \in Y_\wp \, \forall \, \wp < \infty \}$$

Let q_1 be the product of the *finite* primes in $\mathrm{Ram}(\mathbf{B})$, and $q_2 = \wp_1^{n_1} \cdots \wp_r^{n_r}$ an arbitrary product of primes not in $\mathrm{Ram}(\mathbf{B})$, with every $n_i > 0$. We say that an Eichler order $\mathcal{O}$ in $\mathbf{B}$, has *level* $q_1 q_2$ if locally, $\mathcal{O}_\wp$ is the unique Eichler order for $\wp \mid q_1$, an Eichler order of level $\wp_i^{n_i}$ if $\wp = \wp_i \mid q_2$, and $M_2(\mathcal{S}_\wp)$ if $\wp \not| q_1 q_2, \wp < \infty$.

If J is a left $\mathcal{O}$-ideal, where $\mathcal{O}$ is an Eichler order, then the right order $\mathcal{O}_r(J)$ is an Eichler order of the same level as $\mathcal{O}$.

For any ideal I, we define its *inverse, conjugate,* and *norm*, respectively, as:

$$\begin{aligned} I^{-1} &= \{ \mathbf{b} \in \mathbf{B} \mid IbI \subset I \} \\ \overline{I} &= \{ \overline{\alpha} \mid \alpha \in I \} \\ \mathbf{nr}(I) &= \{ \mathbf{nr}(\alpha) \mid \alpha \in I \} \end{aligned}$$

Proposition D.3 *Let I be an ideal, $\mathcal{O}_\ell(I) = \mathcal{O}_\ell$, and $\mathcal{O}_r(I) = \mathcal{O}_r$.*

1. *$\overline{I}$ is a left $\mathcal{O}_r$-ideal with $\mathcal{O}_r(\overline{I}) = \mathcal{O}_\ell$, and $\mathbf{nr}(\overline{I}) = \mathbf{nr}(I)$.*
2. *I^{-1} is a left $\mathcal{O}_r$-ideal with $\mathcal{O}_r(I^{-1}) = \mathcal{O}_\ell$, and $\mathbf{nr}(I^{-1}) = \mathbf{nr}(I)^{-1}$.*
3. *$I\overline{I} = \mathcal{O}_\ell \mathbf{nr}(I)$ and $\overline{I}I = \mathcal{O}_r \mathbf{nr}(I)$.*
4. *$I^{-1} = \overline{I}/\mathbf{nr}(I)$. then $\mathbf{nr}(IJ) = \mathbf{nr}(I)\mathbf{nr}(J)$.*
5. *The set consisting of all left and right ideals of all orders of a fixed level form a* Brandt grouppoid. *As a consequence, if J is an ideal with $\mathcal{O}_r(I) = \mathcal{O}_\ell(J)$, then*

$$IJ = \left\{ \sum_{r=1}^{t} i_r j_r \mid i_r \in I,\ j_r \in J,\ t \in \mathbf{Z}_{\geq 0} \right\}$$

is an ideal with $\mathcal{O}_\ell(IJ) = \mathcal{O}_\ell(I)$, $\mathcal{O}_r(IJ) = \mathcal{O}_r$, and $\mathbf{nr}(IJ) = \mathbf{nr}(I)\mathbf{nr}(J)$.

For proof, one can see [Pi7] and [R], or use the local-global correspondence in some items above.

D.8 Order and Ideal Classes

Two orders $\mathcal{O}_1$ and $\mathcal{O}_2$ are said to be of the same *type* if there is a $\mathbf{b} \in \mathbf{B}^\times$ such that $\mathcal{O}_1 = \mathbf{b}^{-1}\mathcal{O}_2\mathbf{b}$, i.e., they are conjugate. Keeping the notation above, the number of type classes of Eichler orders of level q_1q_2 will be denoted $T_{q_1q_2}$. This number is finite. The *type number* T_{q_1} of the algebra $\mathbf{B}$ is the number of equivalence classes of *maximal* orders of the same type. For $\mathbf{B}$ defined over a local field, all orders of a given level are conjugate, i.e., the type number is 1.

Two ideals J_1 and J_2 are *right equivalent* if and only if there is a $\mathbf{b} \in \mathbf{B}^\times$ such that $J_1 = J_2\mathbf{b}$. The right-equivalence classes of left $\mathcal{O}$-ideals of an order $\mathcal{O}$ are called the *left ideal classes of* $\mathcal{O}$. (It is important to use *right* equivalence on *left* $\mathcal{O}$-ideals to make this definition work!) Similarly, one can define left equivalence of right $\mathcal{O}$-ideal classes.

Both sets of left and right ideal classes of an order $\mathcal{O}$ are finite, and are of the same cardinality, called the *(ideal) class number* of $\mathcal{O}$. Also, the class number of any two Eichler orders of the same level q_1q_2 are the same, denoted $H_{q_1q_2}$. Furthermore, $T_{q_1q_2} \leq H_{q_1q_2}$. For $\mathbf{B}$ defined over a local field, all left ideals of a given order $\mathcal{O}$ are right equivalent to $\mathcal{O}$, i.e., the class number of $\mathcal{O}$ is 1.

Proposition D.4 *Let $\mathcal{O}$ be an Eichler order of level q_1q_2, and $\{I_1, \ldots, I_H\}$, $H = H_{q_1q_2}$ be a complete set of representatives of distinct left $\mathcal{O}$-ideal classes. Then the corresponding right orders $\mathcal{O}_r(I_1), \ldots \mathcal{O}_r(I_H)$ represent, with possible redundancy, all the type classes of Eichler orders of level q_1q_2. Fix $k \in \{1, \ldots, H\}$. Then $\{I_k^{-1}I_1, \ldots, I_k^{-1}I_H\}$ represent the left $\mathcal{O}_r(I_k)$-ideal classes.*

We shall see that $T_{q_1} = H_{q_1}$ in the algebra $\mathbf{B}/\mathbf{Q}(\sqrt{509})$, and we will be able to find a basis for representatives of type classes as well as left ideal classes of all maximal orders of $\mathbf{B}$.

Appendix E

Calculations on Fields

In this Appendix we study the ring of integers and their units for various kinds of number fields, particularly certain quadratic and biquadratic extension of $\mathbf{Q}$. We shall require the following proposition, which is an easy exercise in [Ma]:

Proposition E.1 *The Ring of Integers of a Biquadratic Field. Let* $K = \mathbf{Q}(\sqrt{m}, \sqrt{n})$, $m \neq 1 \neq n$ *distinct squarefree integers. Let* $k = mn/\gcd(m,n)^2$, $\mathcal{S}$ *the integers of* K.

1. *Suppose* $m \equiv 3, n \equiv k \equiv 2 \bmod 4$. *Then an integral basis for* $\mathcal{S}$ *is*
$$\left\{ 1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2} \right\}$$
and $\operatorname{disc}(\mathcal{S}) = 64mnk$.

2. *Suppose* $m \equiv 1, n \equiv k \equiv 2$ *or* $3 \bmod 4$. *Then an integral basis for* $\mathcal{S}$ *is*
$$\left\{ 1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2} \right\}$$
and $\operatorname{disc}(\mathcal{S}) = 16mnk$.

3. *Suppose* $m \equiv n \equiv k \equiv 1 \bmod 4$. *Then an integral basis for* $\mathcal{S}$ *is*
$$\left\{ 1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1+\sqrt{k}}{2}\right) \right\}$$
and $\operatorname{disc}(\mathcal{S}) = mnk$.

Corollary E.2 *Let m and n be squarefree integers, $m \equiv 1 \bmod 4, \gcd(m,n) = 1$. Let $F = \mathbf{Q}(\sqrt{m})$, $\theta = \frac{1+\sqrt{m}}{2}$, $K = \mathbf{Q}(\sqrt{m}, \sqrt{n})$, $\mathcal{R}$ the integers of F, $\mathcal{S}$ the integers of K. Then $\mathcal{S} = \mathcal{R}[\phi]$, where*

$$\phi = \begin{cases} \sqrt{n} & \text{if } n \equiv 2,3 \mod 4 \\ \frac{1+\sqrt{n}}{2} & \text{if } n \equiv 1 \mod 4 \end{cases}$$

Proof. Let $k = mn$. Note that k has the same residue as n modulo 4.

1. If $n \equiv 2,3 \bmod 4$, then by Proposition E.1 (2),

$$\mathcal{S} = \mathbf{Z}\left[1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{mn}}{2}\right] = \mathbf{Z}[\,1,\ \theta,\ \sqrt{n},\ \theta\sqrt{n}\,].$$

2. If $n \equiv 1 \bmod 4$, then by Proposition E.1 (3),

$$\mathcal{S} = \mathbf{Z}\left[1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1+\sqrt{mn}}{2}\right)\right]$$

and the last basis element is:

$$\begin{aligned} & \frac{1+m\sqrt{n}+\sqrt{m}+\sqrt{mn}}{4} \\ = \ & \frac{1-m}{4} + \frac{m+m\sqrt{n}+\sqrt{m}+\sqrt{mn}}{4} \\ = \ & \frac{1-m}{4} + \frac{m+m\sqrt{n}-1-\sqrt{n}+1+\sqrt{m}+\sqrt{n}+\sqrt{mn}}{4} \\ = \ & \frac{1-m}{4} + \frac{m-1}{2}\phi + \theta\phi, \text{ hence} \end{aligned}$$

$$\mathcal{S} = \mathbf{Z}[\,1,\ \theta,\ \phi,\ \theta\phi\,]$$

because $\frac{1-m}{4}$ and $\frac{m-1}{2}$ are both in $\mathbf{Z}$. ∎

In the following, we let $\zeta_n = e^{2\pi i/n}$, and $\overline{z}$ denote complex conjugation, viewed as the non-trivial automorphism of a complex quadratic field. We shall use the above proposition to study the fields $\mathbf{Q}(\sqrt{m}, \sqrt{-1}) = \mathbf{Q}(\sqrt{m}, \zeta_4)$ and $\mathbf{Q}(\sqrt{m}, \sqrt{-3}) = \mathbf{Q}(\sqrt{m}, \zeta_6)$, when $m \equiv 1 \mod 4$. As usual, let $F = \mathbf{Q}(\sqrt{m})$, $\theta = \frac{1+\sqrt{m}}{2}$, σ the non-trivial automorphism of F, $\mathcal{R}$ the integers of F and $\mathcal{U}$ its unit group with fundamental unit u.

Proposition E.3 *Let $m \equiv 1 \bmod 4$ be a positive squarefree integer, $K = \mathbf{Q}(\sqrt{m}, \zeta_4)$, $\mathcal{S}$ the ring of integers of K, R, u and θ as before.*

1. *An integral basis for $\mathcal{S}$ is*

$$\{\, 1,\ \theta,\ \zeta_4,\ \theta\zeta_4 \,\}$$

2. $\operatorname{disc}(K/\mathbf{Q}) = 16m^2$.

3. $\mathcal{S}^\times = \langle \zeta_4 \rangle \langle u \rangle$.

Proof. (1) follows directly from Corollary E.2 above, with $n = -1, \phi = \sqrt{-1} = \zeta_4$, and (2) from Proposition E.1 (2). For (3), let $a, b, c, d \in \mathbf{Z}, \alpha = a + b\theta + c\zeta_4 + d\theta\zeta_4 \in \mathcal{S}$. Then $\alpha \in \mathcal{S}^\times$ if and only if $N_{\mathbf{Q}}^K(\alpha) = \pm 1$. But

$$\begin{aligned}
N_{\mathbf{Q}}^K(\alpha) &= (a + b\theta + c\zeta_4 + d\theta\zeta_4)(a + b\theta + c\overline{\zeta_4} + d\theta\overline{\zeta_4}) \times \\
&\quad (a + b\theta^\sigma + c\zeta_4 + d\theta^\sigma\zeta_4)(a + b\theta^\sigma + c\overline{\zeta_4} + d\theta^\sigma\overline{\zeta_4}) \\
&= [(a + b\theta)^2 + (c + d\theta)^2][(a + b\theta^\sigma)^2 + (c + d\theta^\sigma)^2] \\
&= [(a + b\theta)(a + b\theta^\sigma)]^2 + [(a + b\theta^\sigma)(c + d\theta)]^2 + \\
&\quad [(a + b\theta)(c + d\theta^\sigma)]^2 + [(c + d\theta)(c + d\theta^\sigma)]^2 \\
&= N_{\mathbf{Q}}^F(\omega_1)^2 + (\omega_1^\sigma\omega_2)^2 + (\omega_1\omega_2^\sigma)^2 + N_{\mathbf{Q}}^F(\omega_2)^2 \qquad \text{(E.1)}
\end{aligned}$$

where $\omega_1 = a + b\theta, \omega_2 = c + d\theta$ are both in $\mathcal{R}$. But $\mathbf{Q}(\sqrt{m})$ is a real field, so the form on (E.1) is positive definite. Hence α is a unit if and only if $N_{\mathbf{Q}}^K(\alpha) = 1$. But the first and last terms in (E.1) are non-negative integers which cannot simultaneously be 0 (otherwise $\alpha = 0$), hence we must have either

$$(\omega_1 = 0 \text{ and } N_{\mathbf{Q}}^F(\omega_2) = \pm 1) \text{ or } (\omega_2 = 0 \text{ and } N_{\mathbf{Q}}^F(\omega_1) = \pm 1)$$

But $N_{\mathbf{Q}}^F(\omega_j) = \pm 1$ if and only if $\omega_j \in \mathcal{U}$. Hence the above conditions are equivalent to

$$\alpha = \pm\zeta_4 u^n \text{ or } \pm u^n, n \in \mathbf{Z}$$

which proves (3). ∎

Proposition E.4 *Let $m \equiv 1 \bmod 4$ be a positive squarefree integer, and suppose 3 does not divide m. Let $K = \mathbf{Q}(\sqrt{m}, \zeta_6)$, $\mathcal{S}$ the ring of integers of K, F, $\mathcal{R}$, u and θ as usual. Then:*

1. *An integral basis of $\mathcal{S}$ is*

$$\{\, 1,\ \theta,\ \zeta_6,\ \theta\zeta_6 \,\}$$

2. $\operatorname{disc}(K/\mathbf{Q}) = 9m^2$.

3. *$\mathcal{S}^\times = \langle\zeta_6\rangle\langle u\rangle$, where u is the fundamental unit of $\mathcal{R}$.*

Proof. Again, (1) and (2) follow from Corollary E.2, with $n = -3, \phi = \frac{1+\sqrt{-3}}{2} = \zeta_6$, and Proposition E.1 (3). Now for (3). Let $a, b, c, d \in \mathbf{Z}, \alpha = a + b\theta + c\zeta_6 + d\theta\zeta_6 \in \mathcal{S}$. Then $\alpha \in \mathcal{S}^\times$ if and only if $N_{\mathbf{Q}}^K = \pm 1$. Now,

$$\begin{aligned}
N_{\mathbf{Q}}^K(\alpha) &= (a + b\theta + c\zeta_6 + d\theta\zeta_6)(a + b\theta + c\overline{\zeta_6} + d\theta\overline{\zeta_6}) \times \\
&\quad (a + b\theta^\sigma + c\zeta_6 + d\theta^\sigma\zeta_6)(a + b\theta^\sigma + c\overline{\zeta_6} + d\theta^\sigma\overline{\zeta_6}) \\
&= \left[\left(\frac{2a+c}{2} + \left(\frac{2b+d}{2}\right)\theta\right)^2 + 3\left(\frac{c+d\theta}{2}\right)^2\right] \times \\
&\quad \left[\left(\frac{2a+c}{2} + \left(\frac{2b+d}{2}\right)\theta^\sigma\right)^2 + 3\left(\frac{c+d\theta^\sigma}{2}\right)^2\right], \text{ hence} \\
16N_{\mathbf{Q}}^K(\alpha) &= [(2a+c+(2b+d)\theta)^2 + 3(c+d\theta)^2] \times \\
&\quad [(2a+c+(2b+d)\theta^\sigma)^2 + 3(c+d\theta^\sigma)^2] \\
&= [(2a+c+(2b+d)\theta)(2a+c+(2b+d)\theta^\sigma)]^2 + \\
&\quad 3[((c+d\theta)(2a+c+(2b+d)\theta))^2 + \\
&\quad\ ((c+d\theta^\sigma)(2a+c+(2b+d)\theta^\sigma))^2] + \\
&\quad 9[(c+d\theta)(c+d\theta^\sigma)]^2 \\
&= N_{\mathbf{Q}}^F(\omega_1)^2 + 3((\omega_1\omega_2^\sigma)^2 + (\omega_1^\sigma\omega_2)^2) + 9N_{\mathbf{Q}}^F(\omega_2)^2 \qquad \text{(E.2)} \\
&\quad \text{where we have}
\end{aligned}$$

$$\begin{aligned}\omega_1 &= 2a + c + (2b + d)\theta \in \mathcal{R},\\ \omega_2 &= c + d\theta \in \mathcal{R}, \text{ hence,}\\ \alpha &= \frac{\omega_1 - \omega_2}{2} + \omega_2\zeta_6\end{aligned}$$

The form on E.2 is positive definite, so $\alpha \in \mathcal{S}^\times$ if and only if $N_{\mathbf{Q}}^K = 1$, if and only if

$$16 = N_{\mathbf{Q}}^F(\omega_1)^2 + 3((\omega_1\omega_2^\sigma)^2 + (\omega_1^\sigma\omega_2)^2) + 9N_{\mathbf{Q}}^F(\omega_2)^2.$$

We now analyze the possibilities for the terms on the right. The middle term is thrice the trace of the totally positive algebraic integer $(\omega_1\omega_2^\sigma)^2$, so it is a positive rational integer. Likewise, $N_{\mathbf{Q}}^F(\omega_j)$ is an algebraic integer for $j = 1, 2$. Hence the only possibilities for $N_{\mathbf{Q}}^F(\omega_2)$ are 0 and ± 1.

If $N_{\mathbf{Q}}^F(\omega_2) = 0$, then $\omega_2 = 0$, so $c = 0 = d$ and $\alpha = a + b\theta \in F$. So in this case, α is a unit if and only if $\alpha \in \mathcal{U}$.

If $N_{\mathbf{Q}}^F(\omega_2) = \pm 1$, then the only possibilities for $N_{\mathbf{Q}}^F(\omega_1)$ are $0, \pm 1$ and ± 2. We cannot have $N_{\mathbf{Q}}^F(\omega_1) = 0$, otherwise we get $16 = 9$. We cannot have $N_{\mathbf{Q}}^F(\omega_1) = \pm 2$ either, for otherwise we would get:

$$\begin{aligned}\pm 2 &= N_{\mathbf{Q}}^F(\omega_1)\\ &= (2a + c)^2 + (2a + c)(2a + d) - (2b + d)^2\left(\frac{m-1}{4}\right)\\ &\equiv c^2 + cd - d^2\left(\frac{m-1}{4}\right) \bmod 2\\ &= N_{\mathbf{Q}}^F(\omega_2)\\ &= \pm 1\end{aligned}$$

So the only possibility is $N_{\mathbf{Q}}^F(\omega_1) = \pm 1$. Since we are also assuming that $N_{\mathbf{Q}}^F(\omega_2) = \pm 1$, we find that $\omega_1, \omega_2 \in \mathcal{U}$, say $\omega_1 = \pm u^r, \omega_2 = \pm u^s$. Recall that $\pm 1 = N(u) = u(u^\sigma)$, so $u^\sigma = \pm u^{-1}$. We obtain:

$$\begin{aligned}16 &= 1 + 3((\omega_1\omega_2^\sigma)^2 + (\omega_1^\sigma\omega_2)^2) + 9 \Leftrightarrow\\ 2 &= (\omega_1\omega_2^\sigma)^2 + (\omega_1^\sigma\omega_2)^2 \Leftrightarrow\end{aligned}$$

$$\begin{aligned} 2 &= u^{2(r-s)} + u^{-2(r-s)} \Leftrightarrow \\ 0 &= u^{4(r-s)} - 2u^{2(r-s)} + 1 \Leftrightarrow \\ u^{2(r-s)} &= 1 \Leftrightarrow \\ r - s &= 0 \Leftrightarrow \\ r &= s \end{aligned}$$

Thus, in this case, α is a unit if and only if

$$\begin{aligned} \alpha &= \frac{\omega_1 - \omega_2}{2} + \omega_2\zeta_6 \\ &= \frac{\omega_1 + \omega_2\sqrt{-3}}{2} \\ &= \frac{\pm u^r \pm u^r\sqrt{-3}}{2} \\ &= u^r\left(\frac{\pm 1 \pm \sqrt{-3}}{2}\right) \\ &= u^r\zeta_6^k, k \in \{1,2,4,5\} \end{aligned}$$

Putting the two cases together give (3). ■

We remark that if $m \equiv 1 \bmod 8$, then it may still be possible to find an $\omega \in \mathcal{R}$ such that $N_{\mathbf{Q}}^F(\omega) = \pm 2$, since 2 is a split prime. If $m \equiv 5 \bmod 8$, then this would be impossible since 2 is inert in F. Now we describe $\mathcal{R}_{>>0}$, the totally positive elements of $\mathcal{R}$.

Proposition E.5 *Let $m \equiv 1 \bmod 4$ be a positive squarefree integer, $F = \mathbf{Q}(\sqrt{m})$, θ, $\mathcal{R}$ and $\mathcal{R}_{>>0}$ as before. Then:*

$$\mathcal{R}_{>>0} = \left\{ \alpha = a + b\theta \,\middle|\, a, b \in \mathbf{Z},\ a > 0 \text{ and } -\frac{a}{\theta} < b < \frac{a}{\theta - 1} \right\}$$

Proof. Note that $\theta - 1 > 0$. Suppose $\alpha = a + b\theta \in \mathcal{R}$ with $a, b \in \mathbf{Z}$. Then α is totally positive if and only if $\alpha > 0$ and $\alpha^\sigma = a + b - b\theta > 0$. Since $\theta^\sigma < 0$, we cannot have $a = 0$. Suppose $a < 0$. Then $\alpha > 0$ implies that $b\theta > -a > 0$, so $b > 0$. But $\alpha^\sigma > 0$

implies that $b(\theta - 1) < a < 0$, hence $b < 0$, a contradiction. Hence $a > 0$. The lower bound for b follows from $\alpha > 0$ and the upper bound from $\alpha^\sigma > 0$. ■

This trivial property of the totally positive elements of $\mathcal{R}$ allows us to order them lexicographically, first by a then by b. This will be extremely useful when considering a totally positive definite integral quadratic form on $\mathbf{Z}^n$ (i.e., with values in $\mathcal{R}_{>>0}$) which arises from the norm form of an integral ideal in a positive definite quaternion algebra over F. Now we look at a description of exactly how the primes of $\mathbf{Z}$ split in $\mathbf{Q}(\sqrt{m})$ when $m \equiv 1 \bmod 4$. The following is found in [Ma].

Proposition E.6 *Let $m \equiv 1 \bmod 4$, $\mathcal{R}$ the integers of $\mathbf{Q}(\sqrt{m})$. Suppose that p is an odd prime. Then*

$$2\mathcal{R} = \begin{cases} \left(2, \frac{1+\sqrt{m}}{2}\right)\left(2, \frac{1-\sqrt{m}}{2}\right) & \text{if } m \equiv 1 \bmod 8 \\ \text{prime} & \text{if } m \equiv 5 \bmod 8 \end{cases}$$

$$p\mathcal{R} = \begin{cases} (p, n+\sqrt{m})\,(p, n-\sqrt{m}) & \text{if } m \equiv n^2 \bmod p \\ \text{prime} & \text{if } m \text{ is not a square mod } p \end{cases}$$

Next we show how to concretely give a ring homomorphism $\mathcal{R} \to \mathbf{Z}/p$ that induces a field isomorphism $\mathcal{R}/\wp \to \mathbf{Z}/p$ when $\wp$ is split.

Proposition E.7 *Let $m \equiv 1 \bmod 4$, $F = \mathbf{Q}(\sqrt{m})$, R, the ring of integers of F, and $\wp$ a split prime of $\mathcal{R}$. Suppose $\wp = (p, n + \sqrt{m})$, where $p \in \mathbf{Z}$ is an odd prime and $m \equiv n^2 \bmod p$. Then $\mathcal{R}/\wp$ is a finite field of p elements, $\{0 \ldots p-1\}$ is a set of representatives for $\mathcal{R}$ mod $\wp$, and the map*

$$\begin{array}{rccll} \phi & : & \mathcal{R} & \longrightarrow & \mathbf{Z}/p \\ & & a & \longrightarrow & a \bmod p \qquad \text{if } a \in \mathbf{Z} \\ & & \theta & \longrightarrow & \left(\frac{p-1}{2}\right)(n-1) \bmod p \end{array}$$

defines a ring homomorphism which induces the isomorphism $\mathcal{R}/\wp \cong \mathbf{Z}/p$.

Proof. To prove that $\{0 \ldots p-1\}$ is a system of distinct representatives for $\mathcal{R}$ mod $\wp$, we must show that if $a \in \wp$ and $a \in \mathbf{Z}$, then p divides a in $\mathbf{Z}$. But we see that

$p \mid N_{\mathbf{Q}}^{F}(a) = a^2 \in p\mathbf{Z}$. Next we show that $\theta \equiv \frac{p-1}{2}(n-1)(\in \mathbf{Z})(\text{mod } \wp)$. We have $\alpha \in \wp \Leftrightarrow 2\alpha \in \wp$, since we can find $r, s \in \mathbf{Z}$, such that $rp + 2s = 1$. But

$$2\left(\theta - \frac{(p-1)(n-1)}{2}\right) = \sqrt{m} - pn + n + p = p(1-n) + (n + \sqrt{m}) \in \wp.$$

To show that ϕ is a homomorphism, we need check only that $\phi(\theta^2) = \phi(\theta)^2$. But

$$\phi(\theta^2) = \phi(\theta + \frac{m-1}{4}) \equiv \frac{2(p-1)(n-1) + m - 1}{4} \equiv \frac{2(p-1)n - 1 + n^2 - 1}{4} \bmod p$$

$$\text{and } \phi(\theta)^2 = \frac{(p-1)^2(n-1)^2}{4} \bmod p$$

and the numerators are seen to be equivalent mod p. Also,

$$\phi(n + \sqrt{m}) = \phi(n - 1 + 2\theta) \equiv p(n-1) \equiv 0 \bmod p,$$

so $\wp \subset \ker(\phi)$. Since the map is surjective onto a field, we must have $\wp = \ker(\phi)$. ■

Now we find an effective, albeit sometimes slow algorithm to compute the fundamental unit:

Proposition E.8 *Let $0 < m \equiv 1 \bmod 4$ be a squarefree integer. Let b be the smallest positive integer such that $mb^2 \pm 4 = a^2$ for some integer a. Then $u = \frac{a+b\sqrt{m}}{2} = \frac{a-b}{2} + b\theta$ is the fundamental unit of $\mathbf{Q}(\sqrt{m})$.*

Proof. Clearly, $N(u) = \pm 1$. Note that since m is odd, a and b are of the same parity, so $u \in \mathcal{R}$, hence u is a unit. The minimality of b, hence also of a, assures us that u is the smallest unit in $\mathcal{R}$ which is greater than 1. ■

We shall now give a formula for the order of the class group of a quadratic field, which can be found in [Ma]. Let $F = \mathbf{Q}(\sqrt{m})$, m squarefree, $d = \mid \text{disc}(\mathbf{Q}(\sqrt{m})) \mid$, u the fundamental unit of F if $m > 0$. We define χ, the unique nontrivial multiplicative character mod d, which corresponds to a character of $\text{Gal}(F/\mathbf{Q})$ as follows. If $p \mid d$, then $\chi(p) = 0$. If $2 > p$ does not divide d, then

$$\chi(p) = \begin{cases} 1 & \text{if } d \text{ is a square mod } p \\ -1 & \text{otherwise} \end{cases}$$

Finally, if d is odd, then

$$\chi(2) = \begin{cases} 1 & \text{if } d \equiv 1 \bmod 8 \\ -1 & \text{if } d \equiv 5 \bmod 8 \end{cases}$$

Proposition E.9 *Let everything be as above. Then*

$$h(\mathbf{Q}(\sqrt{m})) = \begin{cases} \dfrac{1}{\log(u)} \left| \displaystyle\sum_{k \in (\mathbf{Z}/d)^\times, k<d/2} \chi(k) \log\left(\sin\left(\frac{k\pi}{d}\right)\right) \right| & \text{if } m > 0 \\ \dfrac{1}{2-\chi(2)} \left| \displaystyle\sum_{k \in (\mathbf{Z}/d)^\times, k<d/2} \chi(k) \right| & \text{if } m < 0, m \neq -1, -3 \\ 1 & \text{if } m = -1, -3 \end{cases}$$

The following is a tool often used to explicitly construct the ideal class group of a number field. Let $[\mathcal{F} : \mathbf{Q}] = n$ and s half the number of non-real embeddings of $\mathcal{F}$.

Proposition E.10 (Minkowski) *Every ideal class of $\mathcal{S}$ contains an ideal I with*

$$N(I) \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(\mathcal{S})|}.$$

We will refer to the quantity on the right as the *Minkowski bound of $\mathcal{F}$*. The proposition states that if the Minkowski bound of $\mathcal{F}$ is less than 2, then $h(\mathcal{F}) = 1$.

We shall now recall Hasse's formula ([Ha]) for the class number of imaginary biquadratic extensions:

Proposition E.11 (Hasse) *Let m_1, m_2 be negative squarefree integers, $m_0 = m_1 m_2$, $F_i = \mathbf{Q}(\sqrt{m_i}), w_i$ the number of roots of unity in F_i, h_i the class group order of $F_i, i = 0, 1, 2$. Let $K = \mathbf{Q}(\sqrt{m_1}, \sqrt{m_2}), h$ the class group order of K, w the number of roots of unity in K, u the fundamental unit in K. Let u_0 be the fundamental unit of F_0. Then:*

$$h = \frac{w}{w_1 w_2} h_0 h_1 h_2 \frac{\log(u_0)}{\log(|u|)}$$

We end this Appendix with an observation about the prime factors of m when certain properties are known.

Proposition E.12 *Let $m \equiv 1 \bmod 4$ be a positive squarefree integer. If the fundamental unit u of the integers of $\mathbf{Q}(\sqrt{m})$ has norm -1, then m does not have a prime factor congruent to 3 mod 4. In particular, 3 does not divide m.*

Proof. Suppose that $N(u) = -1$ and that $p_1 \mid m$, $p_1 \equiv 3 \bmod 4$ a prime. Since $m \equiv 1 \bmod 4$ also, we find that there is a $p_2 \equiv 3 \bmod 4$ which also divides m. Thus $m = 4p_1p_2k + p_1p_2$ for some $k \in \mathbf{Z}$. Thus if $u = a + b\theta$, with $a, b \in \mathbf{Z}$, then

$$\begin{aligned} -1 &= N(u) \\ &= N(a + b\theta) \\ &= a^2 + ab - \left(\frac{m-1}{4}\right) b^2 \\ &\equiv a^2 + ab - \frac{p_1p_2 - 1}{4} b^2 \bmod p_1 \end{aligned}$$

But if $p_1p_2 = 4j + 1$, then $j \equiv -4^{-1} \bmod p_1$. So if we let $2t \equiv 1 \bmod p_1$, we get

$$\begin{aligned} -1 &\equiv a^2 + ab + t^2b^2 \bmod p_1 \\ &\equiv a^2 + 2a(tb) + (tb)^2 \\ &\equiv (a + tb)^2 \end{aligned}$$

But -1 is a square mod p if and only if $p \equiv 1 \mod 4$. ∎

Bibliography

[BR] D. Blasius and J. Rogawski, *Motives for Hilbert Modular Forms,* to appear.

[BS] Z.I. Borevich and I.R. Shafarevich, *Number Theory.* Academic Press, New York (1966).

[Ca] Henri Carayol, *Sur Les Représentations ℓ-adiques Associées Aux Formes Modulaires de Hilbert.* Annales Scientifiques de L'École Normale Supérieure, 4^e série, Tome 19 (1986), pp. 409-468.

[Cas] W. Casselman, *On Some Results of Atkin and Lehner.* Math Annalen, Vol. 201 (1973) pp. 301-314.

[CF] Cassels and Frohlich (editors), *Algebraic Number Theory.* Academic Press, San Diego (1967).

[Cr] J.E. Cremona, *Modular Symbols for $\Gamma_1(N)$ and Elliptic Curves with Everywhere Good Reduction.* Mathematical Proceedings of the Cambridge Philosophical Society (1992), Vol. 111 (March, 1992), pp. 199-218.

[Fal] Gerd Faltings, *Finiteness Theorems for Abelian Varieties over Number Fields.* Appearing in *Arithmetic Geometry.* Gary Cornell and Joseph H. Silverman (editors), Springer-Verlag, New York (1986).

[Ga] Paul Garrett, *Holomorphic Hilbert Modular Forms.* Brooks/Cole Publishing Company (1990).

[Ge] Stephen Gelbart, *Automorphic Forms on Adele Groups.* Annals of Mathematics Studies, Vol. 83, Princeton University Press (1975).

[GJ] Stephen Gelbart and Hervé Jacquet. *Forms on GL(2) from the Analytic Point of View.* Proceedings of Symposia in Pure Mathematics. Vol. 33 (1979), part 1, pp. 213-251.

[Gr] Benedict H. Gross, *Heights and Special Values of L-series.* Canadian Mathematical Society Conference Proceedings, Vol. 7 (1987).

[Ha] Helmut Hasse, *Über die Klassenzahl abelscher Zahlkörper.* Berlin (1952).

[Hi] Haruzo Hida, *On p-adic Hecke Algebras for GL_2 Over Totally Real Fields.* Annals of Mathematics, Vol. 128 (1988), pp. 295-384.

[HPS] Hiroaki Hijikata, Arnold K. Pizer and Thomas R. Shemanske, *The Basis Problem for Modular Forms on* $\Gamma_0(N)$. The American Mathematical Society (Memoirs, Volume 82, Number 418), Providence, Rhode Island (November, 1989).

[HvG] F. Hirzebruch and G. van der Geer, *Lectures on Hilbert Modular Surfaces.* Les Presses de L'Université de Montréal (1981).

[Jo] Burton W. Jones, *The Arithmetic Theory of Quadratic Forms.* The Mathematical Association of America, John Wiley and Sons, Maryland (1950).

[LL] J.P. Labesse and R.P. Langlands, *L-indistinguishability for* SL(2). Canadian Journal of Mathematics, Vol. XXXI, 4 (1979), pp. 726-785.

[La] R. P. Langlands, *Base Change for* GL(2). Annals of Math Studies, Vol. 96, Princeton University Press (1980).

[L] Von Heinrich-Wolfgang Leopoldt, *Ein Verallgemeinerung der Bernoullischen Zahlen.* Hamburger Abh., 22 (1958), pp. 131-140.

[Li] Ron Livné, *Cubic Exponential Sums and Galois Representation.* Contemporary Mathematics, Vol. 67 (1987).

[Ma] Daniel A. Marcus, *Number Fields.* Springer-Verlag, New York (1977).

[Mar] J. Martinet, *Character Theory and Artin L-functions.* Algebraic Number Fields, Academic Press (1977).

[N] Morris Newman, *Integral Matrices.* (Preprint) Mimeographed Course Notes.

[Pin] R.G.E. Pinch, *Elliptic Curves over Number Fields.* D.Phil. Thesis, Oxford University (1982).

[Pi1] Arnold K. Pizer, *Type Numbers of Eichler Orders.* J. Reine Angew. Math., 264 (1973), pp. 76-102.

[Pi2] Arnold K. Pizer, *On The Arithmetic of Quaternion Algebras.* Acta Arithmetica, Vol. 31 (1976), pp. 61-89.

[Pi3] Arnold K. Pizer, *On The Arithmetic of Quaternion Algebras II.* J. Math. Soc. Japan, Vol. 28, No. 4 (1976), pp. 676-688.

[Pi4] Arnold K. Pizer, *The Representability of Modular Forms by Theta Series.* J. Math. Soc. Japan, Vol. 28, No. 4 (1976), pp. 689-698.

[Pi5] Arnold K. Pizer, *An Algorithm for Computing Modular Forms on* $\Gamma_0(N)$. Journal of Algebra, Vol. 64 (1980), pp. 340-390.

[Pi6] Arnold K. Pizer, *Theta Series and Modular Forms of Level* p^2M. Compositio Mathematica, Vol. 40, Fasc. 2 (1980), pp. 177-241.

[Pi7] Arnold K. Pizer, *The Action of the Canonical Involution on Modular Forms of Weight 2 on* $\Gamma_o(M)$. Math. Ann., 226 (1977), pp. 99-116.

[PZ] M. Pohst and H. Zassenhaus, *Algorithmic Algebraic Number Theory.* Cambridge University Press, Cambridge (1989).

[Ram1] Dinakar Ramakrishnan, *Arithmetic of Hilbert-Blumenthal Surfaces.* Canadian Mathematical Society Conference Proceedings, Vol. 7 (1987).

[Ram2] Dinakar Ramakrishnan, *A Refinement of the Strong Multiplicity One Theorem for* GL_2. Inventiones Mathematicae, to appear.

[R] Irving Reiner. *Maximal Orders.* Academic Press, London (1975).

[Se1] Jean-Pierre Serre, *A Course in Arithmetic.* Springer-Verlag, New York (1973).

[Sh] Hideo Shimizu, *On Zeta Functions of Quaternion Algebras.* Annals of Mathematics, Vol. 81 (1965), pp. 166-193.

[Shi] Goro Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions.* Princeton University Press (1971).

[Si] Jonathan H. Silverman, *The Arithmetic of Elliptic Curves.* Springer-Verlag, New York (1986).

[T] Richard Taylor, *On Galois Representations Associated to Hilbert Modular Forms.* Inventiones Mathematicae, 98, 265-280 (1989).

[Vi] Marie-France Vignéras, *Arithmétique des Algèbres de Quaternions.* Springer-Verlag, Berlin (1980).