The Dissertation Committee for Ariel Martin Pacetti
certifies that this is the approved version of the following dissertation:

A formula for the central value of certain Hecke L-functions

Committee:

Fernando Rodriguez-Villegas, Supervisor

Benedict Gross

John Tate

Jeffrey Vaaler

Felipe Voloch

A formula for the central value of certain Hecke L-functions

by

Ariel Martin Pacetti, Licenciado

Dissertation

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

Doctor of Philosophy

The University of Texas at Austin

August 2003

I would like to dedicate this work to my parents for all the support they gave me during all this years

Acknowledgments

I would like to thank my advisor, Fernando Rodriguez Villegas for suggesting me this interesting problem and being always willing to answer any kind of question I may have. I would like to thank him and his family for making my adaption to this new culture easier.

I also would like to thank Benedict Gross, John Tate, Jeffrey Vaaler and Felipe Voloch for accepting to be part of my committee as well as for all the things I learned from them.

Ariel Martin Pacetti

The University of Texas at Austin
August 2003

A formula for the central value of certain Hecke L-functions

Publication No. _____

Ariel Martin Pacetti, Ph.D.
The University of Texas at Austin, 2003

Supervisor: Fernando Rodriguez-Villegas

Let $N \equiv 1 \bmod 4$ be the negative of a prime, $K = \mathbb{Q}(\sqrt{N})$ and $\mathcal{O}_K$ its ring of integers. Let $\mathcal{D}$ be a prime ideal in $\mathcal{O}_K$ of prime norm congruent to 3 modulo 4. Under these assumptions, there exists Hecke characters $\psi_{\mathcal{D}}$ of K with conductor $\mathcal{D}$ and infinite type $(1,0)$. Their L-series $L(\psi_{\mathcal{D}}, s)$ are associated to a CM elliptic curve $A(N, \mathcal{D})$ defined over the Hilbert class field of K. We will prove a Waldspurger-type formula for $L(\psi_{\mathcal{D}}, s)$ of the form $L(\psi_{\mathcal{D}}, 1) = \Omega \sum_I r(\mathcal{D}, I) m_{[\mathcal{D}]}(I)$ where the sum is over class ideal representatives I of a maximal order in the quaternion algebra ramified at $|N|$ and infinity. An application of this formula for the case $N = -7$ will allow us to prove the non-vanishing of a family of L-series of level $7|D|$ over K.

Contents

Introduction

Given an imaginary quadratic field K the theory of complex multiplication done by Shimura gives a relation between elliptic curves with CM given by an order of K and L-functions associated to Hecke characters ψ on K. The simplest case is when $K = \mathbb{Q}(\sqrt{N})$ with $N \equiv 1 \bmod 4$ the negative of a prime and ψ is a character of conductor $\sqrt{N}$. In this case the L-function corresponds to a CM elliptic curve $A(N)$ studied by Gross in [Gr], defined over H, the Hilbert class field of K. A formula for the central value of $L(\psi, 1)$ was given by Villegas in [Vi].

In this thesis we will study the central value of the L-series corresponding to the CM elliptic curves $A(N, \mathcal{D})$, twists of $A(N)$ by ideals $\sqrt{N}\mathcal{D}$ where $\mathcal{D}$ is a prime ideal of K prime to $\sqrt{N}$ and with prime norm congruent to 3 modulo 4. The ideal $\mathcal{D}$ has associated h Hecke characters $\psi_{\mathcal{D}}$ of K of conductor $\mathcal{D}$, where h is the class number of K. The relation between the L-series of $A(N, \mathcal{D})$ and $L(\psi_{\mathcal{D}}, s)$ is given explicitly by :

$$L(A(N, \mathcal{D})/H, s) = \prod_{\psi_{\mathcal{D}}} L(\psi_{\mathcal{D}}, s) L(\overline{\psi_{\mathcal{D}}}, s)$$

where H is the Hilbert class field of K and the product is over the h Hecke characters associated to $\mathcal{D}$ (see [Gr] formula (8.4.4) and Theorem 18.1.7). If we define $\mathfrak{B}$ be the Weil restriction of scalars of $A(N, \mathcal{D})$ to K, then $\mathfrak{B}$ is a CM abelian variety, and $L(A(N, \mathcal{D})/H, s) = L(\mathfrak{B}/K, s)$.

Let B be the quaternion algebra ramified at $|N|$ and infinity. To the ideal

$\mathcal{D}$ we will associate a maximal order $O_{[\mathcal{D}]}$ in B depending only on the class of $\mathcal{D}$. If $\{I\}$ are representatives for left $O_{[\mathcal{D}]}$-ideals, we will prove the formula $L(\psi_{\mathcal{D}}, 1) = \Omega \sum r(\mathcal{D}, I) m_I([\mathcal{D}])$ where the sum is over the ideals $\{I\}$, Ω is a period, $r(\mathcal{D}, I)$ is a rational integer and the numbers $m_I([\mathcal{D}])$ are algebraic integers.

In the last chapter we study in detail the case when the class number of K is one. In this case the elliptic curve $A(N)$ is defined over $\mathbb{Q}$ and the numbers m_I turn out to be rational integers. In the case $N = -7$ using the fact that the quaternion algebra has class number 1 for maximal ideals, we will be able to prove that the CM elliptic curves $A(N, \mathcal{D})$ defined over K have a non-vanishing L-series for all primes $\mathcal{D}$.

We finish this work with a remarkable relation between the numbers m_I and the coordinates of the eigenvector of the modular form associated to $A(N)$ represented in the Brandt matrices of level N^2.

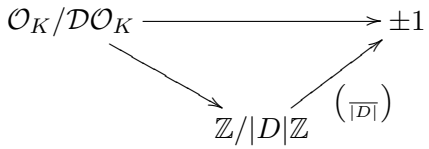
Chapter 1

L-series

1.1 L-series definition

Given a number field K, we will denote $\mathcal{O}_K$ for its ring of integers, $Cl(\mathcal{O}_K)$ the class group and h the class number.

Let N be a negative prime integer congruent to 1 mod 4, and $K := Q(\sqrt{N})$. Let D be a negative prime integer congruent to 1 mod 4 such that the ideal generated by D splits completely in K, i.e. $(D) = (\mathcal{D})(\bar{\mathcal{D}})$. The ideal $\mathcal{D}$ induces a quadratic character from $\mathcal{O}_K/\mathcal{D}$ to $\{\pm 1\}$ by extending the Kronecker symbol $\left(\frac{}{|D|}\right)$ so as to make the following diagram commute:



We will denote $\varepsilon_{\mathcal{D}}$ this character. It induces a Hecke character $\psi_{\mathcal{D}}$ on principal ideals by $\psi_{\mathcal{D}}(\langle\alpha\rangle) = \varepsilon_{\mathcal{D}}(\alpha)\alpha$.

Proposition 1.1.1. *The character ψ_D on principal ideals is well defined.*

Proof. Since 1 and -1 are the only units in K, we must check that $\varepsilon_{\mathcal{D}}(\alpha)\alpha =$

$-\varepsilon_{\mathcal{D}}(-\alpha)\alpha$. This follows from the fact that $\varepsilon_{\mathcal{D}}$ is multiplicative and $|D| \equiv 3 \bmod 4$, hence $\varepsilon_{\mathcal{D}}(-1) = -1$ $\square$

The character actually depends of the choice of $\mathcal{D}$ (i.e. we have one character associated to $\mathcal{D}$ and another one associated to $\bar{\mathcal{D}}$). Abusing notation we will denote just by ψ the character associated to $\mathcal{D}$.

The character ψ defined on principal ideals extends to h Hecke characters on $I(\mathcal{O}_K)$ the set ideals of $\mathcal{O}_K$. We fix an extension once and for all and we call it ψ. Then $\psi : I(\mathcal{O}_K) \longrightarrow T_\psi$, where T_ψ is a non-Galois degree h field extension of K.

Definition. *The L-series associated to ψ is*

$$L(\psi, s) := \sum_{\mathcal{A}} \frac{\psi(\mathcal{A})}{N\mathcal{A}^s} \tag{1.1}$$

where the sum is over all ideals $\mathcal{A}$ of $\mathcal{O}_K$.

By Hecke's work we know that $L(\psi, s)$ extends to an analytic function in the upper half plane, and satisfies the functional equation:

$$\left(\frac{2\pi}{\sqrt{ND}}\right)^{-s} \Gamma(s) L(\psi, s) = w_\psi \left(\frac{2\pi}{\sqrt{ND}}\right)^{s-2} \Gamma(2-s) L(\bar{\psi}, 2-s) \tag{1.2}$$

where w_ψ is the root number. The character ψ is associated to a CM elliptic curve $A(N, \mathcal{D})$ and defines a weight 2 modular, by $f_\psi(z) = \sum_{\mathcal{A}} \psi(\mathcal{A}) e^{2\pi i z N\mathcal{A}}$ for z in the upper half plane. The modular form f_ψ has level ND, and actually the root number is given by:

$$w_\psi = f_\psi(\frac{i}{\sqrt{ND}}) / \overline{f_\psi(\frac{i}{\sqrt{ND}})} \tag{1.3}$$

1.2 Choosing characters in a consistent way

Given an ideal $\mathcal{D}$ we choose an extension of the Hecke character ψ defined in principal ideals to the class group. in this way we get a field T_ψ depending on the extension chosen. Note that if we choose another prime ideal $\mathcal{D}'$ and extend the character

associated to $\mathcal{D}'$ in an arbitrary way, the image of both characters will lie in different fields. There is a natural way of defining a Hecke character $\psi_{\mathcal{D}'}$ associated to $\mathcal{D}'$ such that $\psi_{\mathcal{D}'}(Cl(\mathcal{O}_K)) \subset T_\psi$. Since the class group has order h we know that any ideal raised to the h-power is principal, hence we define:

$$\psi_{\mathcal{D}'}(\mathcal{A}) = \psi_{\mathcal{D}}(\mathcal{A})\frac{\varepsilon_{\mathcal{D}'}(\mathcal{A}^h)}{\varepsilon_{\mathcal{D}}(\mathcal{A}^h)} \tag{1.4}$$

Proposition 1.2.1. *the character $\psi_{\mathcal{D}'}$ defined above is a Hecke character associated to $\mathcal{D}'$ taking values in T_ψ.*

Proof. If $\mathcal{A}$ is principal, say $\mathcal{A} = \langle\alpha\rangle$, then $\psi_{\mathcal{D}'}(\alpha) = \varepsilon_{\mathcal{D}}(\alpha)\alpha\frac{\varepsilon_{\mathcal{D}'}(\alpha)^h}{\varepsilon_{\mathcal{D}}(\alpha)^h}$. Since h is odd, and ε takes the values ± 1, we get that $\psi_{\mathfrak{p}}(\alpha) = \varepsilon_{\mathfrak{p}}(\alpha)\alpha$.

Note that the character $\psi_{\mathcal{D}'}$ is well defined for all ideal $\mathcal{A}$ prime to $\mathcal{D}'\mathcal{D}$, so we need to find a way to extend it to $\mathcal{D}$; then since the character is multiplicative it will extend to any ideal $\mathcal{A}$ prime to $\mathcal{D}'$.
Let $\mathfrak{q}$ be a prime ideal in the same class equivalence as $\mathcal{D}$ and prime to $\mathcal{D}\mathcal{D}'$ (there exists such an ideal by Tchebotarev density theorem), say $\mathfrak{q}\beta = \mathcal{D}$. Then $\psi_{\mathcal{D}'}(\mathcal{D}) = \psi_{\mathcal{D}'}(\mathfrak{q}\beta) = \psi_{\mathcal{D}'}(\mathfrak{q})\psi_{\mathcal{D}'}(\beta) = \psi_{\mathcal{D}'}(\mathfrak{q})\varepsilon_{\mathcal{D}'}(\beta)\beta$. Hence $\psi_{\mathcal{D}'}$ is defined in all ideals prime to $\mathcal{D}'$, and takes values in T_ψ. □

Given a prime ideal $\mathfrak{p}$, we will denote $\psi_{\mathfrak{p}}$ the Hecke character associated to $\mathfrak{p}$ chosen in this consistent way.

Proposition 1.2.2. *The root number in the functional equation satisfy $w_\psi = -\left(\frac{2}{|N|}\right) i\frac{\alpha}{|\alpha|}$, where $\alpha = \pm\psi_{\mathcal{N}}(\mathcal{D})$ and the sign is chosen such that $K(\sqrt{\alpha\sqrt{N}})$ is the quadratic extension of K associated to the character ψ, i.e. it is $+1$ if 2 is unramified in $K(\sqrt{\alpha\sqrt{N}})$ and -1 if not.*

Proof. See [Bu-Gr] proposition 10.6, page 20 □

1.3 Computing the L-series value at 1

Given $\mathcal{A}$ an ideal of K , we will denote $[\mathcal{A}]$ its class in the class group. We can decompose the L-series as

$$L(\psi, s) = \sum_{[\mathcal{A}]} \sum_{\mathcal{B}\sim\mathcal{A}} \frac{\psi(\mathcal{B})}{N\mathcal{B}^s} \tag{1.5}$$

Proposition 1.3.1. *All integral ideals equivalent to $\mathcal{A}$ are of the form $c\mathcal{A}$ for some $c \in \mathcal{A}^{-1}$.*

Proof. If $\mathcal{B} \sim \mathcal{A}$ there are elements a and b in $\mathcal{O}_K$ such that $a\mathcal{A} = b\mathcal{B}$. Hence $\frac{a}{b}\mathcal{A} = \mathcal{B} \subset \mathcal{O}_K$; in particular $\frac{a}{b} \in \mathcal{A}^{-1} = \frac{\bar{\mathcal{A}}}{N\mathcal{A}}$. On the other hand if $c \in \mathcal{A}^{-1}$, $c = \frac{b}{N\mathcal{A}}$ for some $b \in \bar{\mathcal{A}}$. Then $ca = \frac{ba}{N\mathcal{A}} \in \mathcal{O}_K$ for all $a \in \mathcal{A}$. □

Two elements c and c' of $\mathcal{A}^{-1}$ define the same integral ideal equivalent to $\mathcal{A}$ if and only if they differ by a unit of $\mathcal{O}_K$. The only units in $\mathcal{O}_K$ are 1 and -1, then:

$$\sum_{\mathcal{B}\sim\mathcal{A}} \frac{\psi(\mathcal{B})}{N\mathcal{B}^s} = \frac{1}{2}\sum_{c\in\bar{\mathcal{A}}} \frac{\psi\left(\frac{c}{N\mathcal{A}}\mathcal{A}\right)}{N\left(\frac{c}{N\mathcal{A}}\mathcal{A}\right)^s} = \frac{1}{2}\sum_{c\in\bar{\mathcal{A}}} \frac{\psi(c)\psi(\mathcal{A})}{\psi(N\mathcal{A})}\frac{N\mathcal{A}^s}{Nc^s} = \frac{1}{2}N\mathcal{A}^s\frac{\psi(\mathcal{A})}{\psi(N\mathcal{A})}\sum_{c\in\bar{\mathcal{A}}}\frac{\psi(c)}{Nc^s}$$

Since ψ is multiplicative $\psi(\mathcal{A})\psi(\bar{\mathcal{A}}) = \psi(N\mathcal{A})$, then $\frac{\psi(\mathcal{A})}{\psi(N\mathcal{A})} = \frac{1}{\psi(\bar{\mathcal{A}})}$. Using the fact that $N\mathcal{A} = N\bar{\mathcal{A}}$ it follows that $\sum_{\mathcal{B}\sim\mathcal{A}} \frac{\psi(\mathcal{B})}{N\mathcal{B}^s} = \frac{1}{2}\frac{N\bar{\mathcal{A}}^s}{\psi(\mathcal{A})}\sum_{c\in\bar{\mathcal{A}}}\frac{\psi(c)}{Nc^s}$ and we can write the L-series as:

$$L(s,\psi) = \frac{1}{2}\sum_{[\mathcal{A}]\in Cl(\mathcal{O}_K)} \frac{N\mathcal{A}^s}{\psi(\mathcal{A})}\sum_{c\in\mathcal{A}}\frac{c\varepsilon_{\mathcal{D}}(c)}{Nc^s} \tag{1.6}$$

Without loss of generality, we may assume that $\mathcal{A} = a\mathbb{Z} + \frac{b+\sqrt{N}}{2}\mathbb{Z}$ and $\mathcal{D} = |D|\mathbb{Z} + \frac{b+\sqrt{N}}{2}\mathbb{Z}$, hence $\mathcal{A}\mathcal{D} = a|D|\mathbb{Z} + \frac{b+\sqrt{N}}{2}\mathbb{Z}$ (see [Vi] §2.3 page 552). If $c \in \mathcal{A}$ then $c = ma + n\frac{b+\sqrt{N}}{2}$, and $\varepsilon_{\mathcal{D}}(c) = \varepsilon_{\mathcal{D}}(ma + n\frac{b+\sqrt{N}}{2})$. Since $n\frac{b+\sqrt{N}}{2} \in \mathcal{D}$, $\varepsilon_{\mathcal{D}}(c) = \varepsilon_{\mathcal{D}}(a)\varepsilon_{\mathcal{D}}(m) = \varepsilon_{\mathcal{D}}(N\mathcal{A})\varepsilon_{\mathcal{D}}(m)$. We will denote $z_{\mathcal{A}}$ the point $\frac{b+\sqrt{N}}{2a}$ (respectively $z_{\mathcal{D}}$ the point $\frac{b+\sqrt{N}}{2|D|}$ and $z_{\mathcal{A}\mathcal{D}}$ the point $\frac{b+\sqrt{N}}{2a|D|}$). Also we denote by $\sum'$ the sum removing the zero element (or zero vector depending on the context). We have:

$$L(s,\psi) = \frac{1}{2}\sum_{[\mathcal{A}]\in Cl(\mathcal{O}_K)} \frac{N\mathcal{A}^{1-s}\varepsilon_{\mathcal{D}}(N\mathcal{A})}{\psi(\mathcal{A})}\sum_{m,n\in\mathbb{Z}}{}' \frac{\varepsilon_{\mathcal{D}}(m)(m + z_{\mathcal{A}\mathcal{D}}|D|n)}{N(m + z_{\mathcal{A}\mathcal{D}}|D|n)^s} \tag{1.7}$$

We would like to cancel the term in the numerator with one of the terms in the denominator, but we need to end up with a point in the upper half plane. If we rearrange the sum changing m by $-m$ and using that $\varepsilon_{\mathcal{D}}(-1) = -1$ the term in the inner sum can be written as $\frac{\varepsilon_{\mathcal{D}}(m)}{(m+(-\bar{z}_{\mathcal{AD}})|D|n)|m+(-\bar{z}_{\mathcal{AD}})|D|n|^{2s-2}}$. This sum is related to Eisenstein series that we define below:

Definition. *Let p be a prime integer and $\varepsilon(m) := \left(\frac{m}{p}\right)$. We define the Eisenstein series associated to ε by $E_1(z,s) = \sum'_{m,n\in\mathbb{Z}} \frac{\varepsilon(m)}{(m+zpn)|m+zpn|^{2s}}$.*

By (1.7) we get the relation:

$$L(s,\psi) = \frac{1}{2} \sum_{[\mathcal{A}]\in Cl(\mathcal{O}_K)} \frac{N\mathcal{A}^{1-s}\varepsilon_{\mathcal{D}}(N\mathcal{A})}{\psi(\mathcal{A})} E_1(-\bar{z}_{\mathcal{AD}}, s-1) \tag{1.8}$$

$E_1(z,s)$ turns out to be a modular form of weight 1 with a character. We need to compute its value at $s = 0$ for a point z in the upper half plane. The problem is that this series converge only for $\Re(s) > \frac{3}{2}$, but it can be analytically continued to the whole plane and satisfy a functional equation. We will compute its value at $s = 0$ using Hecke's trick. Since ε is a character of conductor p, we break the sum over m as:

$$E_1(z,s) = \sum_{m\in\mathbb{Z}}{}' \frac{\varepsilon(m)}{m} + 2\sum_{n=1}^{\infty} \sum_{r \bmod p} \varepsilon(r) \sum_{m\in\mathbb{Z}} \frac{1}{(zpn+r+mp)|zpn+r+mp|^{2s}} \tag{1.9}$$

and dividing the last sum by p^{2s+1} we get:

$$E_1(z,s) = 2L(s,\varepsilon) + 2\sum_{n=1}^{\infty} \sum_{r \bmod p} \frac{\varepsilon(r)}{p^{2s+1}} \sum_{m\in\mathbb{Z}} \frac{1}{(\frac{zpn+r}{p}+m)\left|\frac{zpn+r}{p}+m\right|^{2s}} \tag{1.10}$$

For z in the upper half plane we define:

$$H(z,s) = \sum_{m\in\mathbb{Z}} \frac{1}{(z+m)|z+m|^{2s}}$$

Lemma 1.3.1. *Let $z = x + iy$ be a point in the upper half plane, then:*

$$\sum_{m=-\infty}^{\infty} (z+m)^{-(s+1)}(\bar{z}+x)^{-s} = \sum_{n=-\infty}^{\infty} \tau_n(y, s+1, s)e^{2\pi inx}$$

where $\tau_n(y, s+1, s)$ is given by:

$$\tau_n(y, s+1, s)\frac{i\Gamma(s+1)\Gamma(s)}{(2\pi)^{2s+1}} = \begin{cases} n^{2s}e^{-2\pi ny}\sigma(4\pi ny, s+1, s) & (n > 0) \\ |n|^{2s}e^{-2\pi|n|y}\sigma(4\pi|n|y, s, s+1) & (n < 0) \\ \Gamma(2s)(4\pi y)^{-2s} & n = 0 \end{cases}$$

and $\sigma(y, \alpha, \beta) = \int_0^\infty (t+1)^{\alpha-1}t^{\beta-1}e^{-yt}dt$

Proof. This is Lemma 1 page 84 [Sh] □

The right side of lemma 1.3.1 equality converges for any $s > 0$, so we can compute the limit when s tends to 0 of $\tau_n(y, s+1, s)$ in the different cases:

- **Case $n = 0$:** $\lim_{s\to 0} \frac{(2\pi)^{2s+1}}{i\Gamma(s+1)} \frac{\Gamma(2s)}{\Gamma(s)}(4\pi y)^{-2s} = -i\pi$
- **Case $n < 0$:** $\lim_{s\to 0} \frac{(2\pi)^{2s+1}}{i\Gamma(s+1)\Gamma(s)}|n|^{2s}e^{2\pi|n|y} \int_0^\infty (t+1)^{s-1}t^s e^{-4\pi|n|yt}dt = 0$
- **Case $n > 0$:** $\lim_{s\to 0} \frac{(2\pi)^{2s+1}n^{2s}}{i\Gamma(s+1)}e^{-2\pi ny}\frac{1}{\Gamma(s)} \int_0^\infty (t+1)^s t^{s-1}e^{-4\pi nyt}dt.$

We just need to compute $\lim_{s\to 0} \frac{1}{\Gamma(s)} \int_0^1 (t+1)^s t^{s-1}e^{-4\pi nyt}dt$. Doing integration by parts:

$$\int_0^1 (t+1)^s t^{s-1}e^{-4\pi nyt}dt = \frac{2^s e^{-4\pi ny}}{s} - \int_0^1 t^s(t+1)^{s-1}e^{-4\pi nyt}dt -$$

$$-\frac{1}{s}\int_0^1 t^s(t+1)^s e^{-4\Pi nyt}(-4\pi nyt)dt$$

The function $\Gamma(z)$ has a simple pole at $z = 0$ with residue 1. Dividing the integral by $\Gamma(s)$ and taking the limit when s tends to zero we get:

$$\lim_{s\to 0} \tau_n(y, s+1, s) = -2\pi i e^{-2\pi ny} \tag{1.11}$$

We just prove:

Lemma 1.3.2. $\lim_{s\to 0} H(s, z) = -\pi i - 2\pi i \sum_{n=1}^\infty q^n$

Equation (1.10) can be written as

$$E_1(z,s) = 2L(s,\varepsilon) + 2\sum_{n=1}^{\infty}\sum_{r \bmod p}\frac{\varepsilon(r)}{p^{2s+1}}H(\frac{zpn+r}{p},s)$$

Which by lemma 1.3.1 is the same as:

$$E_1(z,s) = 2L(s,\varepsilon) + 2\sum_{n=1}^{\infty}\sum_{r \bmod p}\frac{\varepsilon(r)}{p^{2s+1}}\sum_{k\in\mathbb{Z}}\tau_k(yn,s+1,s)e^{2\pi ik(\frac{xpn+r}{p})}$$

Let $G(\varepsilon) := \sum_{r \bmod p}\varepsilon(r)\xi_p^r$ be the Gauss sum associated to the quadratic character ε. Let $\xi_p = e^{\frac{2\pi i}{p}}$. If we take the limit as s tends to zero and use lemma (1.3.2) in the inner sum we get:

$$\sum_{r \bmod p}\frac{\varepsilon(r)}{p}(-\pi i - 2\pi i\sum_{k=1}^{\infty}q^{nk}\xi_p^{rk}) = -\frac{2\pi i}{p}G(\varepsilon)\sum_{k=1}^{\infty}\varepsilon(k)q^{nk}$$

If p is congruent to 3 modulo 4 it is a well known result that $G(\varepsilon) = i\sqrt{p}$ then:

$$\lim_{s\to 0}E_1(z,s) = 2L(1,\varepsilon) + \frac{4\pi}{\sqrt{p}}\sum_{n=1}^{\infty}\left(\sum_{d|n}\varepsilon(d)\right)q^n \tag{1.12}$$

Knowing the value of $E_1(z,0)$, and using equation (1.8) we get the value of $L(1,\psi)$. We will write this number in terms of theta functions so as to relate the value for different ideals $\mathcal{D}$.

Let $L = \mathbb{Q}(\sqrt{D})$, and $\mathcal{A}$ be any ideal of L. For z in the upper half plane, we define $\Theta_{\mathcal{A}}(z) = \sum_{\lambda\in\mathcal{A}}e^{2\pi iz\frac{N\lambda}{N\mathcal{A}}} = 1 + \sum_{n=1}^{\infty}r_{\mathcal{A}}(n)q^n$ where $r_{\mathcal{A}}(n)$ is the number of elements $\lambda \in \mathcal{A}$ of norm $nN\mathcal{A}$.

Lemma 1.3.3. *Let w be the number of roots of unity in L, and z a point in the upper half plane. Then $\frac{w\sqrt{p}}{4\pi}E_1(z,0) = \sum_{\mathcal{A}\in Cl(O_L)}\Theta_{\mathcal{A}}(z)$*

Proof. We need to check that the q-expansion on both sides is the same. The constant term first on the right side is h, the class number of $\mathbb{Q}(\sqrt{-p})$. On the left side we have $\frac{L(1,\varepsilon)w\sqrt{p}}{2\pi}$ which by the class number formula is h. Since the constant

term is the same, we can apply the Mellin transform on both sides. Dividing by w we need to prove the equality:

$$\sum_{n=1}^{\infty} \frac{\sum_{d|n} \varepsilon(d)}{n^s} = \frac{1}{w} \sum_{\mathcal{A} \in Cl(O_L)} \sum_{n=1}^{\infty} \frac{r_{\mathcal{A}}(n)}{n^s} \tag{1.13}$$

Given a number field L the zeta function associated to it is:

$$\zeta_L(s) = \sum_{\mathcal{A}} \frac{1}{N\mathcal{A}^s}$$

where the sum is over all integral ideals of L. It follows easily from the definition that $\zeta_L(s) = \frac{1}{w} \sum_{\mathcal{A} \in Cl(\mathcal{O}_L)} \sum_{n=1}^{\infty} \frac{r_{\mathcal{A}}(n)}{n^s}$ which is the right hand side of (1.13).

It is a classical result that $\zeta_L(s) = \zeta(s) L(s, \varepsilon)$ (see for example [Wa] Theorem 4.3, page 33). If we look at the Mellin transform of this product, we get $\left(\sum_{n=1}^{\infty} \frac{1}{n^s}\right) \left(\sum_{m=1}^{\infty} \frac{\varepsilon(m)}{m^s}\right)$ which is the right hand side of (1.13) $\square$

Note that $-\bar{z}_{\mathcal{A}\mathcal{D}} = z_{\bar{\mathcal{A}}\bar{D}}$, hence by equation (1.8) and lemma 1.3.3 we get:

$$L(1, \psi) = \frac{2\pi}{w\sqrt{|D|}} \sum_{[\mathcal{A}] \in Cl(\mathcal{O}_K)} \frac{\varepsilon_{\mathcal{D}}(N\mathcal{A})}{\psi(\mathcal{A})} \sum_{[\mathcal{B}] \in Cl(\mathcal{O}_L)} \Theta_{\mathcal{B}}(z_{\bar{\mathcal{A}}\bar{\mathcal{D}}})$$

By the consistent way we chose the Hecke characters (see equation (1.4)) $\psi_{\bar{\mathcal{D}}}(\mathcal{A}) = \psi_{\mathcal{D}}(\mathcal{A}) \varepsilon_{\bar{\mathcal{D}}}(\mathcal{A}^h) \varepsilon_{\mathcal{D}}(\mathcal{A}^h) = \psi_{\mathcal{D}}(\mathcal{A}) \left(\frac{N\mathcal{A}}{|D|}\right)^h$. Since h is odd it follows that $\frac{\varepsilon_{\mathcal{D}}(N\mathcal{A})}{\psi_{\mathcal{D}}(\mathcal{A})} = \frac{1}{\psi_{\bar{\mathcal{D}}}(\mathcal{A})}$.

Theorem 1.3.1. *The value at $s = 1$ of $L(s, \psi)$ is given by:*

$$L(1, \psi) = \frac{2\pi}{w\sqrt{|D|}} \sum_{[\mathcal{A}] \in Cl(\mathcal{O}_K)} \sum_{[\mathcal{B}] \in Cl(\mathcal{O}_L)} \frac{\Theta_{\mathcal{B}}(z_{\mathcal{A}\bar{\mathcal{D}}})}{\psi_{\bar{\mathcal{D}}}(\bar{\mathcal{A}})}$$

Chapter 2

Theta functions in several variables

2.1 Definitions and applications

The main reference for theta functions in several variables is David Mumford's book ([Mu]). The theory of theta functions in several variables is the natural generalization of the classical theory of theta functions in one variable.

We define the **Siegel upper-half-space** $\mathfrak{h}_g$ to be the set of symmetric gxg complex matrices Ω whose imaginary part is positive definite. Note that if $g = 1$ this is just the usual upper half plane.

The generalized Theta functions are functions from $\mathbb{C}^g \mathrm{x} \mathfrak{h}_g \mapsto \mathbb{C}$, defined by: $\theta(\vec{z}, \Omega) = \sum_{\vec{n} \in \mathbb{Z}^g} \exp(\pi i \vec{n}^t \Omega \vec{n} + 2\pi i \vec{n}^t . \vec{z})$

Proposition 2.1.1. *$\theta(\vec{z}, \Omega)$ converges absolutely and uniformly in $\vec{z}$ and in Ω in each set $\max_i |Imz_i| < \frac{c_1}{2\pi}$ and $Im\Omega \geq c_2 I_g$*

Proof. See ([Mu] proposition 1.1, page 118) □

In the classical case we have an action of $Sl_2(\mathbb{R})$ on $\mathbb{C}\mathrm{x}\mathfrak{h}$. We define the

simplectic group $Sp_{2g}(\mathbb{R})$ to be the set of $2g$x$2g$ real matrices M such that $M^tAM = A$ where A is the matrix $\begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}$. Note that if $g = 1$, $Sp2(\mathbb{R}) = Sl_2(\mathbb{R})$.

Given an element $\alpha = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in Sp_{2g}(\mathbb{R})$, we define its action at a point $(\vec{z}, \Omega)$ in C^gx$\mathfrak{h}_g$ by $\alpha.(\vec{z}, \Omega) = \left(1/(C\Omega + D)^t.\vec{z}, (A\Omega + B)(C\Omega + D)^{-1}\right)$

Most of the traditional results for $Sl_2(\mathbb{R})$ acting in $\mathfrak{h}$ are true for $Sp_{2g}(\mathbb{R})$ acting in $\mathfrak{h}_g$. We state some of them in the next proposition.

Proposition 2.1.2. *The following statements are true:*

1. $Sp_{2g}(\mathbb{R})$ *acts transitively on* $\mathfrak{h}_g$*, and the stabilizer of* iI_g *is isomorphic to* $U_g(\mathbb{C})$*. Thus* $\mathfrak{h}_g \simeq Sp_{2g}(\mathbb{R})/U_g(\mathbb{C})$*.*

2. $Sp_{2g}(\mathbb{Z}) \subset Sp_{2g}(\mathbb{R})$ *is discrete and acts discontinuously on* $\mathfrak{h}_g$*.*

3. *The orbit space* $\mathfrak{h}_g/Sp_{2g}(\mathbb{Z})$ *is called the* **Siegel modular variety**. *It is a Hausdorff topological space.*

Proof. See ([Mu] pages 177-182) □

Lemma 2.1.1. *Given a vector* $\vec{m} \in \mathbb{Z}^g$ *and* $\vec{z} \in \mathbb{C}^g$*, we have:*

1. $\theta(\vec{z} + \vec{m}, \Omega) = \theta(\vec{z}, \Omega)$*.*

2. $\theta(\vec{z} + \Omega\vec{m}, \Omega) = \exp(-\pi i\vec{m}^t\Omega\vec{m} - 2\pi i\vec{m}^t\vec{z})\,\theta(\vec{z}, \Omega)$

Proof. The first statement follows directly from the definition of the Theta function. Since Ω is symmetric, $e^{\pi i(\vec{n}+\vec{m})^t\Omega(\vec{n}+\vec{m})} = e^{\pi i\vec{n}^t\Omega\vec{n}}e^{2\pi i\vec{n}^t\Omega\vec{m}}e^{\pi i\vec{m}^t\Omega\vec{m}}$. Then rearranging the sum we get the other statement. □

The Theta functions does not satisfy a functional equation for the whole group $Sp_{2g}(\mathbb{Z})$ but for a finite index subgroup $\Gamma_{1,2}$ (following Igusa notation), which

is defined to be: $\alpha = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in Sp_{2g}(\mathbb{R})$ such that A^tC and B^tD have even diagonal.

Proposition 2.1.3. $\Gamma_{1,2}$ *is generated by the elements* $\begin{pmatrix} A & 0 \\ 0 & 1/A^t \end{pmatrix}$, $\begin{pmatrix} I_g & B \\ 0 & I_g \end{pmatrix}$, $\begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}$ *with* $A \in Gl_g(\mathbb{Z})$ *and* B *any symmetric integral matrix with even diagonal.*

Proof. See ([Mu] proposition A4, page 208. $\square$.

Proposition 2.1.4. (Functional Equation) *Given* $\alpha = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_{1,2}$,

$$\theta(\alpha.(\vec{z},\Omega))) = \xi_\alpha det(C\Omega + D)^{1/2} e^{i\pi \vec{z}^t (C\Omega+D)^{-1} C\vec{z}} \theta(\vec{z},\Omega) \tag{2.1}$$

where ξ_α *is an eighth-root of unit.*

Proof. A complete proof is given in ([Mu], §5, page 189). We are interested in the special case when $\vec{z} = 0$, so we will sketch the proof to get some extra information on the root of unity.

The first step in Mumford's proof is to show that if α_1 and α_2 satisfy 2.1 then so does their product, hence we skip this step here. Using proposition 2.1.3 we will check the functional equation in each of the generators.

First case: if $\alpha = \begin{pmatrix} A & 0 \\ 0 & 1/A^t \end{pmatrix}$ with $A \in Gl_g(\mathbb{Z})$. Then $det(A) = \pm 1$, and the functional equation reads $\theta(A\vec{z}, A\Omega A^t) = \xi_\alpha \sqrt{det(A^{-1})}\theta(\vec{z},\Omega)$.

By definition $\theta(A\vec{z}, A\Omega A^t) = \sum_{n\in\mathbb{Z}^g} e^{i\pi n^t A\Omega A^t n + 2\pi i n^t A\vec{z}}$. Since $A \in Gl_g(\mathbb{Z})$ it preserves $\mathbb{Z}^g$, hence via a change of variables $\theta(A\vec{z}, A\Omega A^t) = \theta(\vec{z},\Omega)$ and $\xi_\alpha = \frac{1}{\sqrt{det(A^{-1})}}$.

Second case: if $\alpha = \begin{pmatrix} I_g & B \\ 0 & I_g \end{pmatrix}$ with B symmetric and even diagonal, the functional equation reads $\theta(\vec{z}, \Omega + B) = \xi_\alpha \theta(\vec{z}, \Omega)$. By definition $\theta(\vec{z}, \Omega + B) = \sum_{n \in \mathbb{Z}^g} e^{i\pi n^t(\Omega+B)n + 2\pi i n^t \vec{z}}$. The conditions on B assure $n^t B n$ to be an even integer if $n \in \mathbb{Z}^g$, then $\xi_\alpha = 1$.

Third case: $\alpha = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}$. This case is similar to the functional equation for the classical theta function and so is the proof. The functional equation reads $\theta(\Omega^{-1}\vec{z}, -\Omega^{-1}) = \xi_\alpha \sqrt{det(\Omega)} e^{i\pi \vec{z}^t \Omega^{-1} \vec{z}} \theta(\vec{z}, \Omega)$. We need a general version of the Poisson Summation formula.

Poisson Summation formula: let $\mathcal{S}(\mathbb{R}^g)$ denote the Schwartz space, i.e. the vector space of functions $f : \mathbb{R}^g \mapsto \mathbb{C}$ which are bounded, smooth (i.e. all partial derivatives exist and are continuous), and rapidly decreasing (i.e. $|x|^N f(x)$ tends to zero if $|x|$ tends to infinity for any N). For $f \in \mathcal{S}(\mathbb{R}^g)$ we define the Fourier transform $\hat{f} : \mathbb{R}^g \mapsto \mathbb{C}$ by

$$\hat{f}(y) = \int_{\mathbb{R}^g} e^{-2\pi i x.y} f(x) dx$$

where dx denotes $dx_1 \dots dx_g$.This integral converges for all $y \in \mathbb{R}^g$, and $\hat{f} \in \mathcal{S}(\mathbb{R}^g)$.

Lemma 2.1.2. *if $f \in \mathcal{S}(\mathbb{R}^g)$ then $\sum_{m \in \mathbb{Z}^g} f(m) = \sum_{m \in \mathbb{Z}^g} \hat{f}(m)$.*

Proof. See ([La] [XIII §1], page 249).□

The third case of the functional equation goes as follow: apply Poisson Summation Formula to $f(x) = e^{i\pi x^t \Omega x + 2\pi i x^t \vec{z}}$. Then $\sum_{n \in \mathbb{Z}^g} f(n) = \theta(\vec{z}, \Omega)$. Its Fourier transform $\hat{f}(y)$ is given by:

Lemma 2.1.3. *Let $\Omega \in \mathfrak{h}_g$ and $\vec{z} \in \mathbb{C}^g$ then*

$$\int_{\mathbb{R}^g} \exp(i\pi x^t \Omega x + 2\pi i x^t z) dx = \left(det(\frac{\Omega}{i}) \right)^{-1/2} \exp(-i\pi z^t \Omega^{-1} z)$$

.

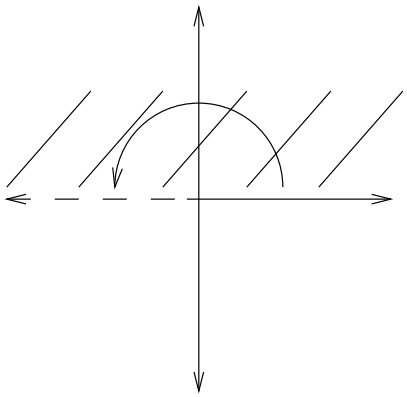


Figure 1

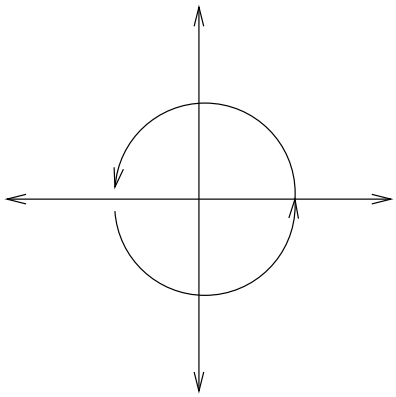


Figure 2

Proof. Since both sides are holomorphic in Ω and z, it is enough to consider the case when they are both pure imaginary (say $\Omega = iA^tA$ and $z = iy$). Then the formula follows from a change of variables (see [Mu] Lemma 5.8 page 195 for details).□

We will use Lemma 2.1.3 in the particular case of $g = 2$, $z = \vec{0}$ and $\Omega = Q\tau$, where Q is positive definite and τ is a point in the upper half plane. Then $det(\frac{\Omega}{i}) = (-i)^2\tau^2 det(Q)$. If we remove from $\mathbb{C}$ the real negative line $\mathbb{R}^-$ (see figure 1), then we can define the square root in a unique way there. Since $\tau \in \mathfrak{h}$, and Q is positive definite , $(-i)^2\tau^2 det(Q)$ is a non-negative real number, so we can consider this square root (picture 2 represents the values of $-\tau^2 det(Q)$).

Both terms of the functional equation are analytic, and by Mumford's proof they coincide in the case τ pure imaginary hence we get the formula:

$$\theta(\vec{0}, -(Q\tau)^{-1}) = \sqrt{det(Q)}\,(-i)\tau\theta(\vec{0}, Q\tau) \tag{2.2}$$

Following the previous chapter notation, given N a negative prime congruent to 1 modulo 4, and D a negative prime congruent to 1 modulo 4 such that D splits in $K := \mathbb{Q}(\sqrt{N})$, we denote $L := \mathbb{Q}(\sqrt{D})$.

The goal of this chapter is to write the identity of theorem 1.3.1 in terms of theta functions in two variables. Then we will find relations between these theta functions for different primes D using the functional equation proved above.

L is an imaginary quadratic field, so given an ideal $\mathcal{B}$ of $Cl(\mathcal{O}_L)$ we can associate to it a quadratic form of discriminant D via the group isomorphism between $Cl(\mathcal{O}_L)$ and $\{$quadratic forms of discriminant $D\}$.

More specifically, given a quadratic form of discriminant D, say $[a,b,c]$ where $b^2-4ac=D$, we associate the ideal $\langle a, \frac{b+\sqrt{D}}{2}\rangle$; and conversely given any primitive ideal (i.e. not divisible by any rational integer greater than 1) $\mathcal{A}$, we can chose a pair of generators of the form $\mathcal{A}=\langle a, \frac{b+\sqrt{N}}{2}\rangle$, and associate to it the quadratic form $[a,b,c]$ where $c=(b^2-D)/(4a)$. We will denote $Q_{\mathcal{B}}$ the matrix $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$ associated to the quadratic form $[a,b,c]$.

Given an ideal $\mathcal{B}$ in $Cl(\mathcal{O}_L)$, and a point $z\in\mathfrak{h}$, $\Theta_{\mathcal{B}}(z)=\sum_{\alpha\in\mathcal{B}} e^{2\pi i z N(\alpha)/N(\mathcal{B})}$ by definition. Let $\mathcal{B}=\langle a, \frac{b+\sqrt{N}}{2}\rangle$ with $a=N(\mathcal{B})$. If $\alpha\in\mathcal{B}$ then it can be written uniquely as $\alpha=ma+n\left(\frac{b+\sqrt{N}}{2}\right)$. Hence $N(\alpha)=a(am^2+mnb+n^2\frac{b^2-N}{4a})$ and

$$\Theta_{\mathcal{B}}(z)=\sum_{(m,n)\in\mathbb{Z}^2}\exp\left[2\pi i z(m,n)\begin{pmatrix} a & b/2 \\ b/2 & c\end{pmatrix}\begin{pmatrix} m \\ n\end{pmatrix}\right] \tag{2.3}$$

Since $z\in\mathfrak{h}$ and $Q_{\mathcal{B}}$ is symmetric, $zQ_{\mathcal{B}}\in\mathfrak{h}_2$. Hence $\Theta_{\mathcal{B}}(z)=\theta(\vec{0},zQ_{\mathcal{B}})$. So we can rewrite the main formula of theorem 1.3.1 as:

$$L(1,\psi)=\frac{2\pi}{w\sqrt{|D|}}\sum_{[\mathcal{A}]\in Cl(\mathcal{O}_K)}\sum_{[\mathcal{B}]\in Cl(\mathcal{O}_L)}\frac{\theta(\vec{0},z_{\mathcal{A}\bar{\mathcal{D}}}Q_{\mathcal{B}})}{\psi_{\bar{\mathcal{D}}}(\bar{\mathcal{A}})} \tag{2.4}$$

Although it looks like the definition of $\theta(\vec{0},z_{\mathcal{A}\mathcal{D}}Q_{\mathcal{B}})$ depends on the generators of $\mathcal{A}$ and $\mathcal{D}$ chosen, this is not the case. Note that a and $|D|$ are uniquely determined, and the number b is defined modulo $2a|D|$; hence the number $z_{\mathcal{A}\mathcal{D}}$ is defined modulo $\mathbb{Z}$. Since $Q_{\mathcal{B}}$ is symmetric and even diagonal, the second case of the functional equation says that $\theta(\vec{0},\Omega+kQ_{\mathcal{B}})=\theta(\vec{0},\Omega)$ for any $k\in\mathbb{Z}$.

Chapter 3

Normalization of the Theta function

In (2.4) we have written the value of the L-series at the point $s = 1$ in term of theta functions in two variables evaluated at the points $z_{\mathcal{A}\bar{\mathcal{D}}}Q_{\mathcal{B}}$. To compare this value for different ideals $\mathcal{D}$ we will normalize the theta function and write its value as a linear combination of certain numbers $n_{[\mathcal{A}],[\mathcal{B}],\bar{\mathcal{D}}}$ times an eta function (or a theta function in some cases).

For $z \in \mathfrak{h}$, we recall the definitions:

$$\eta(z) = e^{2\pi iz/24}\prod_{n=1}^{\infty}(1 - e^{2\pi inz})$$

$$\theta_{10}(z) = \sum_{k\ odd} e^{(\pi ik^2/4)z}$$

Where θ_{10} is one of the classical Jacobi theta functions. Following the ideas of [Ha-Vi] we want to define this two functions on ideals. Let us assume that $N \neq -3$ to avoid some technicalities coming from the fact that the Hilbert class field has extra roots of unity in this case. Given an ideal $\mathcal{A}$ of K prime to (6), say $\mathcal{A} = \langle a, \frac{b+\sqrt{N}}{2}\rangle$, define $\eta(\mathcal{A}) := e_{48}(a(3-b))\eta(\frac{b+\sqrt{N}}{2a})$ where $e_n(a) = \exp(2\pi ia/n)$, and $\theta_{10}(\mathcal{A}) = e_{16}(a(1-b))\theta_{10}(\frac{b+\sqrt{N}}{2a})$.

It is easy to check that this functions are well defined (i.e. do not depend on the generators for $\mathcal{A}$ chosen). The η case is done in [Ha-Vi] definition 8 page 502 (note that their definition of eta corresponds to $\eta(\bar{\mathcal{A}})$ with our definition) and the θ_{10} follows from the equation $\theta_{10}(z+1) = \theta_{10}(z)e_8(1)$.

Without loss of generality any time we write a basis for an ideal we will assume that b congruent to 3 modulo 48 while working with eta functions and that $b \equiv 1 \bmod 8$ while working with θ_{10} to avoid keep track of roots of unity.

Given a point $z_{\bar{\mathcal{A}}\bar{\mathcal{D}}}$, we define the normalizer:

$$\Upsilon(z_{\mathcal{A}\mathcal{D}}) := \begin{cases} \theta_{10}(\mathcal{D})\theta_{10}(\mathcal{O}_K)\psi_{\mathcal{D}}(\bar{\mathcal{A}}) & \text{if } N \equiv 1 \bmod 8 \\ \eta(\mathcal{D})\eta(\mathcal{O}_K)\psi_{\mathcal{D}}(\bar{\mathcal{A}}) & \text{for any } N \end{cases}$$

Then the main formula (2.4) can be written as:

$$L(1,\psi) = \frac{2\pi}{w\sqrt{|D|}} \left(\sum_{[\mathcal{A}]\in Cl(\mathcal{O}_K)} \sum_{[\mathcal{B}]\in Cl(\mathcal{O}_L)} \frac{\theta(\vec{0}, z_{\mathcal{A}\bar{\mathcal{D}}}Q_{\mathcal{B}})}{\Upsilon(z_{\mathcal{A}\bar{\mathcal{D}}})} \right) \eta(\bar{\mathcal{D}})\eta(\mathcal{O}_K) \tag{3.1}$$

Also an analogous formula for the case $N \equiv 1 \bmod 8$ replacing η by θ_{10}. We are interested in studying the number:

$$n_{\mathcal{A},\mathcal{B},\bar{\mathcal{D}}} = \theta(\vec{0}, z_{\mathcal{A}\bar{\mathcal{D}}}Q_{\mathcal{B}})/\Upsilon(z_{\mathcal{A}\bar{\mathcal{D}}})$$

The normalizer Υ is chosen so as to make this quotient an algebraic integer. The character $\psi_{\bar{D}}(\bar{\mathcal{A}})$ makes this quotient depend only on the class of $\mathcal{A}$ but not on $\mathcal{A}$ itself. To probe this results we will need to use the theory of complex multiplication, hence we give a summary of the main results.

3.1 Complex Multiplication

This theory was developed by Goro Shimura, but we will use basic notions and results which can be found in [St] pages 211-218.

Let $\mathcal{F}_M$ be the field of all modular functions of level M whose q-expansion at every cusp have coefficients in $\mathbb{Q}(\zeta_M)$, and $K = \mathbb{Q}(\sqrt{d})$, with $d < 0$ a discriminant. Let $K(M)$ denote the ray class field of K mod M, and for a prime ideal $\mathfrak{p}$ in K relative prime to M (say of norm p), $\sigma(\mathfrak{p})$ denotes the Frobenius automorphism of $K(M)/K$ corresponding to $\mathfrak{p}$.

$\mathcal{F}_M$ turns out to be a normal extension of $\mathcal{F}_1 = \mathbb{Q}(j(z))$ (the j-invariant) and the Galois group $\mathrm{Gal}(\mathcal{F}_M/\mathcal{F}_1)$ is isomorphic to $Gl_2(\mathbb{Z}/M\mathbb{Z})/\pm I$, i.e. given $f(z)$ a function on $\mathcal{F}_M$ and an integral matrix A of determinant relatively prime to M, we have an action of A on $f(z)$. This action is characterized by the two rules:

- if $A \in Sl_2(\mathbb{Z})$, then $(f \circ A)(z) = f(Az)$
- if $A = \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$ then $(f \circ A)(z) = (f \circ \sigma_d)(z)$; where σ_d is the automorphism of $\mathbb{Q}(\zeta_M)/\mathbb{Q}$ defined by $\sigma_d(\zeta_M) = \zeta_M^d$, and σ_d acts on f by acting on its q-expansion at infinity.

Theorem 3.1.1. *let $f(z)$ be in $\mathcal{F}_M$ and suppose that $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ in K where p is a rational prime such that $(p, dM) = 1$. Suppose that $\mathcal{A} = [\mu, \nu]$ is a fractional ideal of K with $\vartheta = \mu/\nu$ in $\mathfrak{h}$ and let $B\binom{\mu}{\nu}$ be a basis for $\bar{\mathfrak{p}}\mathcal{A}$. Then $f(\vartheta)$ is in $K(M)$ and $f(\vartheta) \circ \sigma(\mathfrak{p}) = [f \circ (pB^{-1})](B\vartheta)$.*

If in addition f is analytic in the interior of $\mathfrak{h}$ and has algebraic integer coefficients in its q-expansion at every cusp, then $f(\vartheta)$ is an algebraic integer.

Proof. This is Theorem 3 of [St] page 213. □

Proposition 3.1.1. *Following the previous notation, $\theta(\vec{0}, \frac{z}{a|D|}Q_{\mathcal{B}})/\eta(\frac{z}{|D|})\eta(z)$ is in $\mathcal{F}_{24aD^2}$ (respectively $\theta(\vec{0}, \frac{z}{a|D|}Q_{\mathcal{B}})/\theta_{10}(\frac{z}{|D|})\theta_{10}(z)$ is in F_{24aD^2}).*

For the proof we need an auxiliary lemma, hence first we will state and prove it.

Lemma 3.1.1. *if $f(z)$ is a modular form of weight k and level N and D is a positive integer then $f(\frac{z}{D})$ is a modular form of weight k and level at most ND.*

Proof. Given a modular form $f(z)$, a positive integer k and a matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $Gl_2^+(\mathbb{Q})$ (the two by two invertible matrices with positive determinant), we define $f(z)|[\gamma]_k := f(\gamma z)(cz+d)^{-k}(det\,\gamma)^{k/2}$.

Let $g(z) := f(\frac{z}{D})$ and k be the weight of $f(z)$. Up to a constant, $g = f|[\gamma]_k$ where $\gamma = \begin{bmatrix} 1 & 0 \\ 0 & D \end{bmatrix}$. If $\alpha \in \gamma^{-1}\Gamma(N)\gamma \cap Sl_2(\mathbb{Z})$ then $g|[\alpha] = f|[\gamma\gamma^{-1}\Gamma(N)\gamma]_k = f|[\gamma]_k = g$ hence $g(z)$ is a modular form of the same weight as $f(z)$ invariant under $\gamma^{-1}\Gamma(N)\gamma \cap Sl_2(\mathbb{Z})$. It is easy to check that $\Gamma(ND) \subset \gamma^{-1}\Gamma(N)\gamma \cap Sl_2(\mathbb{Z})$. $\square$

Proof of proposition 3.1.1. Let $\mathcal{B}$ be the ideal $\mathcal{B} := \mathbb{Z}a + \mathbb{Z}\frac{b+\sqrt{d}}{2}$. Then the quadratic form associated to $\mathcal{B}$ is $[a,b,c]$ with $b^2 - 4ac = D$ and the matrix of the bilinear form is $\begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$. The theta series $\theta_{\mathcal{B}}$ is the theta series associated to this quadratic form hence it has level $|D|$, weight 1 and a character $\epsilon(d) = \left(\frac{D}{d}\right)$ (see [Ogg] Theorem 20, page VI-25). Using the previous lemma, we have that $\theta_{\mathcal{B}}(\frac{z}{a|D|})$ is a modular form of weight 1 and level aD^2.

The eta function is a modular form of weight 1/2 and level 24 (respectively the Jacobi theta function θ_{10} has weight 1/2 and level 8), then $\eta(\frac{z}{|D|})$ has weight 1/2 and level $24|D|$ (respectively $\theta_{10}(\frac{z}{|D|})$ has weight 1/2 and level $8|D|$), so their product has weight 1 and level $24|D|$ (respectively weight 1 and level $8|D|$). Then the quotient has weight 0 and level at most $24aD^2$ in both cases. We do not need a sharp estimate of the q-expansion, hence the real level is not important.

From the q-expansion of the functions $\theta_{\mathcal{B}}$, θ_{10} and η it is clear that the q-expansion of $\theta(\vec{0}, \frac{z}{a|D|}Q_{\mathcal{B}})/\eta(\frac{z}{|D|})\eta(z)$ at infinity is in $\mathbb{Q}(\xi_{24aD^2})$ (and so is the q-expansion of $\theta(\vec{0}, \frac{z}{a|D|}Q_{\mathcal{B}})/\theta_{10}(\frac{z}{|D|})\theta_{10}(z)$), hence we just need to check this condition at the other cusps. For that purpose we will study the q-expansion of each form

separately.

Since the theta function $\theta_{\mathcal{B}}$ is a modular form for $\Gamma_0(|D|)$, there are just two inequivalent cusps which may be taken to be 0 and ∞. One transformation that send infinity to zero is given by the matrix $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ sending z to $-1/z$.

In the second case of the functional equation (2.2) we proved:

$$\theta\left(\vec{0}, Q_{\mathcal{B}}^{-1}(-1/z)\right) = det(Q_{\mathcal{B}})^{1/2}(-i)z\theta(\vec{0}, Q_{\mathcal{B}}z) = \sqrt{|D|}(-i)z\theta(0, Q_{\mathcal{B}}z) \tag{3.2}$$

Since $Q_{\mathcal{B}}^{-1} = \text{Adj}\,(Q_{\mathcal{B}})/|D|$, if we replace z by $z/|D|$ in the previous equation we get

$$\theta\left(\vec{0}, \text{Adj}\,(Q_{\mathcal{B}})(-1/z)\right) = (-i)z/\sqrt{|D|}\,\theta(\vec{0}, Q_{\mathcal{B}}z/|D|) \tag{3.3}$$

Replacing $Q_{\mathcal{B}}$ by its adjoint matrix, we see that the q-expansion at 0 includes a 4-th root of unity and the square root of $|D|$ (the z factor actually cancels out a factor coming from the eta function). Since $\sqrt{D} \in \mathbb{Q}(\xi_D)$, the q-expansion of $\theta(0, Q_{\mathcal{B}})$ has coefficients in $\mathbb{Q}(\xi_{8D})$ at all cusps. Replacing z by $z/a|D|$ we add at most (aD^2)-th roots of unity to the q-expansions, hence the q-expansion of $\theta(0, \frac{z}{a|D|}Q_{\mathcal{B}})$ has coefficients in $\mathbb{Q}(\xi_{24aD^2})$ at all cusps.

Lemma 3.1.2. *Let* $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in Sl_2(\mathbb{Z})$ *with* γ *even,* δ *positive (and odd), and* $\tau \in \mathfrak{h}$. *Then*

$$\eta\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = \left(\frac{\gamma}{\delta}\right) e_{24}(\kappa)\sqrt{\gamma\tau+\delta}\,\eta(\tau) \tag{3.4}$$

and

$$\theta_{10}\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = \left(\frac{\gamma}{\delta}\right) e_8(\rho)\sqrt{\gamma\tau+\delta}\,\theta_{10}(\tau) \tag{3.5}$$

where $\kappa = 3(\delta-1) + \delta(\beta-\gamma) - (\delta^2-1)\gamma\alpha$ *and* $\rho = \delta - 1 + \delta\beta$.

Proof. This is Theorem 4.3 in [Vi] page 560 □

Then if we consider any matrix in $\Gamma_0(2)$, the modular forms η and θ_{10} change by a 24-th root of unity, hence their q-expansion at the cusps equivalent module $\Gamma_0(2)$ have coefficients in $\mathbb{Q}(\xi_{24})$ and the q-expansion of $\eta(\frac{z}{|D|})$ and $\theta_{10}(\frac{z}{|D|})$ have coefficients in $\mathbb{Q}(\xi_{24aD^2})$. But modulo $\Gamma_0(2)$ there are just two not equivalent cusps which may be taken to be zero and infinity also, so we will study their q-expansion at zero.

The eta function satisfies the functional equation $\eta(-1/z) = \sqrt{z/i}\,\eta(z)$. Hence its q-expansion at zero has coefficients in $\mathbb{Q}(\xi_8)$ and $\eta(\frac{z}{|D|})$ certainly has a q-expansion with coefficients in $\mathbb{Q}(\xi_{24aD^2})$ at zero.

The Jacobi theta function satisfies the functional equation $\theta_{10}(-1/z) = \sqrt{-iz}\,\theta_{01}(z)$, where $\theta_{01}(z) = \sum_{k\in\mathbb{Z}} e^{\pi i n^2 z + \pi i n}$. This function also has a q-expansion at infinity with rational coefficients, hence the q-expansion of θ_{10} at any cusp has coefficients in $\mathbb{Q}(\xi_{24})$ and in particular $\theta_{10}(\frac{z}{|D|})$ has a q-expansion with coefficients in $\mathbb{Q}(\xi_{24aD^2})$ at all cusps. $\square$

3.2 Field of definition

Theorem 3.2.1. *The number $\theta(\vec{0}, z_{\mathcal{A}\bar{\mathcal{D}}}Q_{\mathcal{B}})/\eta(z_{\bar{\mathcal{D}}})\eta(\mathcal{O}_K)$ is in H, the Hilbert class field of K. If $N \equiv 1 \bmod 8$ then so is $\theta(\vec{0}, z_{\mathcal{A}\bar{\mathcal{D}}}Q_{\mathcal{B}})/\theta_{10}(z_{\bar{\mathcal{D}}})\theta_{10}(\mathcal{O}_K)$.*

Proof. Since the eta function does not vanish in the upper half plane, by Theorem 3.1.1 $\theta(\vec{0}, z_{a|D|}Q_{\mathcal{B}})/\eta(z_{|D|})\eta(z)$ is an algebraic integer in F some field extension of K containing H for any z in the upper half plane. We will make the eta case, and make some comments of how to prove the other case.

Since $\mathcal{A}$ and $\bar{\mathcal{D}}$ are prime to each other (we can assume also that $N\mathcal{A}$ is prime to $|D|$) we can choose basis such that $\mathcal{A} = \langle \frac{b+\sqrt{N}}{2}, a\rangle$,$\bar{\mathcal{D}} = \langle \frac{b+\sqrt{N}}{2}, |D|\rangle$ and $\mathcal{O}_K = \langle \frac{b+\sqrt{N}}{2}, 1\rangle$. We will denote z_0 the point $\frac{b+\sqrt{N}}{2}$.

Let $g(z) := \theta(\vec{0}, \frac{z}{a|D|}Q_{\mathcal{B}})/\eta(\frac{z}{|D|})\eta(z)$. Given an element σ of $\mathrm{Gal}(F/K)$ by complex multiplication theory there exists a prime ideal $\mathfrak{p}$ in K such that $\sigma =$

$\sigma_{\mathfrak{p}}$, where $\sigma_{\mathfrak{p}}$ is the element in $\mathrm{Gal}(F/K)$ corresponding to $\mathfrak{p}$ via the Artin map. Using Tchebotarev density theorem we may assume without loss of generality that $\mathfrak{p}$ is principal and prime to $\mathcal{A}$,$\bar{\mathcal{D}}$ and (6). By theorem 3.1.1, $g(z_0) \circ \sigma(\mathfrak{p}) = [g \circ (pB^{-1})](Bz_0)$, where B is the matrix that sends $\mathcal{O}_K$ to $\mathfrak{p}$.

Since $\mathfrak{p}$, $\mathcal{A}$ and $\bar{\mathcal{D}}$ are prime to each other, we can also choose b such that $\bar{\mathfrak{p}} = \langle \frac{b+\sqrt{N}}{2}, p \rangle$. Then $\bar{\mathfrak{p}}\mathcal{A}\bar{\mathcal{D}} = \langle \frac{b+\sqrt{N}}{2}, pa|D| \rangle$, and with this basis B is given by $\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$. Now $Bz_0 = \frac{z_0}{p}$ and $pB^{-1} = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} = S^{-1}BS$.

Let $g^\star(z) = g \circ S(z) = g(-1/z) = \theta(\vec{0}, -1/(a|D|z)Q_{\mathcal{B}})/\eta(\frac{-1}{|D|z})\eta(\frac{-1}{z})$. If in (3.3) we replace z by $za|D|$ and $Q_{\mathcal{B}}$ by $\mathrm{Adj}\,(Q_{\mathcal{B}})$, we get the equation:

$$\theta(\vec{0}, Q_{\mathcal{B}}(-1/a|D|z)) = (-i)\sqrt{|D|}az\theta(\vec{0}, \mathrm{Adj}\,(Q_{\mathcal{B}})az) \tag{3.6}$$

The eta function satisfies the functional equation $\eta(-1/z) = \sqrt{z/i}\,\eta(z)$. Replacing z by $|D|z$ and multiplying both equations:

$$\eta(-1/z)\eta(-1/(|D|z)) = \sqrt{|D|}\frac{z}{i}\eta(z)\eta(|D|z)$$

Note that since $|D|$ is positive, the branch of square root is the same for both equations so it cancels. Hence:

$$g(-1/z) = a\frac{\theta(\vec{0}, \mathrm{Adj}\,(Q_{\mathcal{B}})az)}{\eta(z)\eta(|D|z)}$$

The q-expansion of this quotient has rational coefficients hence it is fixed by the action of σ_p, i.e. $\sigma_p \circ g^\star = g^\star$. Then $[g \circ (pB^{-1})] = g$ and $(g(z_0))^{\sigma_p} = g(z_0/p)$.

The case of $N \equiv 1 \bmod 8$ follows analogously from the functional equation $\theta_{10}(-1/z) = \sqrt{z/i}\theta_{01}(z)$.

Proposition 3.2.1. *with the notation as above,* $g(z_0/p) = g(z_0)$.

Proof. The proposition follows easily from the next three lemmas. □
This proposition completes the proof of theorem 3.2.1. □

Lemma 3.2.1. *Let $\mathfrak{p} = \langle \mu \rangle$ be a principal ideal prime to $\mathcal{A}$ and $\bar{\mathcal{D}}$. Then the theta function $\Theta_{\mathcal{B}}$ satisfies the formula:*

$$\Theta_{\mathcal{B}}\left(\frac{b+\sqrt{N}}{2ap|D|}\right) = \bar{\mu}\varepsilon_{\bar{\mathcal{D}}}(\mu)\left(\frac{p}{|D|}\right)\Theta_{\mathcal{B}}\left(\frac{b+\sqrt{N}}{2a|D|}\right)$$

Note: since $\varepsilon_{\bar{\mathcal{D}}}(\mu)\varepsilon_{\bar{\mathcal{D}}}(\bar{\mu}) = \left(\frac{p}{|D|}\right)$, the formula may be written as $\Theta_{\mathcal{B}}(\frac{b+\sqrt{N}}{2ap|D|}) = \psi_{\bar{\mathcal{D}}}(\bar{\mu})\Theta_{\mathcal{B}}(\frac{b+\sqrt{N}}{2a|D|})$

Proof. $\Theta_{\mathcal{B}}$ is a modular form of weight 1 for $\Gamma_0(|D|)$ with a quadratic character. We chose b such that $\mathcal{A}\bar{\mathcal{D}} = \langle \frac{b+\sqrt{N}}{2}, a|D| \rangle$ and $\mathfrak{p} = \langle \frac{b+\sqrt{N}}{2}, p \rangle$ then $\mathfrak{p}\mathcal{A}\bar{\mathcal{D}} = \langle \frac{b+\sqrt{N}}{2}, pa|D| \rangle = \langle \mu\frac{b+\sqrt{N}}{2}, \mu a|D| \rangle$. Hence there exists a matrix $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ in $Sl_2(\mathbb{Z})$ such that $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} \frac{b+\sqrt{N}}{2} \\ ap|D| \end{pmatrix} = \begin{pmatrix} \mu\frac{b+\sqrt{N}}{2} \\ \mu a|D| \end{pmatrix}$.

If $\mu = \frac{m+n\sqrt{N}}{2}$, an easy computation shows that $\delta = \frac{m-nb}{2p}$ and $\gamma = n|D|a$. In particular M is in $\Gamma_0(|D|)$ and by modularity of $\Theta_{\mathcal{B}}$ we have:

$$\Theta_{\mathcal{B}}\left(\frac{b+\sqrt{N}}{2a|D|}\right) = \Theta_{\mathcal{B}}\left(M.\frac{b+\sqrt{N}}{2ap|D|}\right) = \left(\gamma\frac{b+\sqrt{N}}{2ap|D|} + \delta\right)\chi(\delta)\Theta_{\mathcal{B}}\left(\frac{b+\sqrt{N}}{2ap|D|}\right)$$

And the formula:

$$\Theta_{\mathcal{B}}\left(\frac{b+\sqrt{N}}{2a|D|}\right) = \frac{\mu}{p}\chi(\delta)\Theta_{\mathcal{B}}\left(\frac{b+\sqrt{N}}{2ap|D|}\right) \tag{3.7}$$

where $\chi(d) = \left(\frac{D}{q}\right)$ for any prime q which is sufficiently large and satisfies $q \equiv d \bmod |D|$. ([Ogg] Theorem 20, Chapter VI, page 25). Let q be a prime congruent to 1 modulo 4 and congruent to δ modulo $|D|$. Then $\chi(\delta) = \left(\frac{D}{q}\right) = \left(\frac{|D|}{q}\right) = \left(\frac{q}{|D|}\right) = \left(\frac{\frac{m-nb}{2p}}{|D|}\right) = \left(\frac{\frac{m-nb}{2}}{|D|}\right)\left(\frac{p}{|D|}\right)$. Then the proof follows from the definition of $\varepsilon_{\bar{\mathcal{D}}}$ and the fact that $\frac{\mu}{p} = (\bar{\mu})^{-1}$. $\square$

Lemma 3.2.2. *With the same assumptions as in the previous lemma, the eta function satisfies the equation $\eta(\frac{b+\sqrt{N}}{2p|D|})\eta(\frac{b+\sqrt{N}}{2p}) = \bar{\mu}\varepsilon_{\bar{\mathcal{D}}}(\mu)\left(\frac{p}{|D|}\right)\eta(\frac{b+\sqrt{N}}{2|D|})\eta(\frac{b+\sqrt{N}}{2})$.*

In term of ideals:

$$\eta(\mathfrak{p}\bar{\mathcal{D}})\eta(\mathfrak{p}) = \bar{\mu}\varepsilon_{\bar{\mathcal{D}}}(\mu)\left(\frac{p}{|D|}\right)\eta(\bar{\mathcal{D}})\eta(\mathcal{O}_K) \tag{3.8}$$

Proof. Since we choose $|N| \equiv 3 \bmod 4$, and $|N| \neq 3$, the number of units in H is 2 (see [Ha-Vi] tables 3 and 4 of page 507). Given $\mu \in \mathcal{O}_K$, define:

$$\kappa(\mu) = \chi_4(N\mu)\frac{1}{\bar{\mu}}\frac{\eta^2(u)}{\eta^2(\mathcal{O}_K)}$$

Since the number of units in H is 2, κ is a quadratic character (see [Ha-Vi], Lemma 14).We can write the left hand side of (3.8) as:

$$\eta(\mathfrak{p}\bar{\mathcal{D}})\eta(\mathfrak{p}) = \left(\frac{\eta(\mathfrak{p}\bar{\mathcal{D}})}{\eta(\bar{\mathcal{D}})}\frac{\eta(\mathcal{O}_K)}{\eta(\mathfrak{p})}\right)\frac{\eta^2(\mathfrak{p})}{\eta^2(\mathcal{O}_K)}\eta(\mathcal{O}_K)\eta(\bar{\mathcal{D}}) \tag{3.9}$$

If μ is a generator of $\mathfrak{p}$, $\frac{\eta^2(\mathfrak{p})}{\eta^2(\mathcal{O}_K)} = \kappa(\mu)\bar{\mu}\chi_4(p)$. By proposition 10 of [Ha-Vi] $\left(\frac{\eta(\mathfrak{p})}{\eta(\mathcal{O}_K)}\right)^{\sigma_{\mathcal{D}}} = \left(\frac{p}{|D|}\right)\frac{\eta(\mathfrak{p}\bar{\mathcal{D}})}{\eta(\bar{\mathcal{D}})}$. Then we get:

$$\left(\frac{\eta(\mathfrak{p}\bar{\mathcal{D}})}{\eta(\bar{\mathcal{D}})}\frac{\eta(\mathcal{O}_K)}{\eta(\mathfrak{p})}\right) = \left(\frac{p}{|D|}\right)\left(\frac{\eta(\mathfrak{p})}{\eta(\mathcal{O}_K)}\right)^{\sigma_{\mathcal{D}}-1} = \left(\frac{p}{|D|}\right)\left(\sqrt{\kappa(\mu)\bar{\mu}\chi_4(p)}\right)^{\sigma_{\mathcal{D}}-1}$$

By lemma 12 of [Ha-Vi], $\kappa(-1) = -1$. Since the right term of (3.8) remains unchanged replacing μ by $-\mu$, without loss of generality we can choose μ such that $\kappa(\mu) = \chi_4(p)$. Replacing each term on the right hand side of (3.9) we get:

$$\eta(\mathfrak{p}\bar{\mathcal{D}})\eta(\mathfrak{p}) = \left(\frac{p}{|D|}\right)\varepsilon_{\mathcal{D}}(\bar{\mu})\,\bar{\mu}\,\eta(\mathcal{O}_K)\eta(\bar{\mathcal{D}}) \tag{3.10}$$

Since $\varepsilon_{\mathcal{D}}(\bar{\mu}) = \varepsilon_{\bar{\mathcal{D}}}(\mu)$ we get the result. □

Lemma 3.2.3. *If $N \equiv 1 \bmod 8$ the Jacobi theta function θ_{10} satisfies the equation:*

$$\theta_{10}\left(\frac{b+\sqrt{N}}{2p|D|}\right)\theta_{10}\left(\frac{b+\sqrt{N}}{2p}\right) = \bar{\mu}\varepsilon_{\bar{\mathcal{D}}}(\mu)\left(\frac{p}{|D|}\right)\theta_{10}\left(\frac{b+\sqrt{N}}{2|D|}\right)\theta_{10}\left(\frac{b+\sqrt{N}}{2}\right)$$

Proof. Let $\mu = \frac{m+n\sqrt{N}}{2}$ be a generator of $\mathfrak{p}$. Then $m^2 + n^2|N| = 4p$. Looking this equation modulo 8 we get $m^2 + 7n^2 \equiv 4 \bmod 8$. The only squares modulo 8 are $0, 1$ and 4, hence both m and n are even numbers. Also $4|m$ or $4|n$, but not both.

The ideal $\mathfrak{p} = \langle \frac{b+\sqrt{N}}{2}, p \rangle = \langle \mu \frac{b+\sqrt{N}}{2}, 1 \rangle$. The matrix $M = \begin{pmatrix} \frac{m+nb}{2} & aDnc \\ n & \frac{m-nb}{2} \end{pmatrix}$ is the change of basis matrix (where c is such that $b^2 - 4aDpc = N$). If we chose b such that $\frac{m-nb}{2p} > 0$, since n is even we can apply Lemma 3.1.2 and get:

$$\theta_{10}\left(\frac{b+\sqrt{N}}{2}\right) = \left(\frac{n}{\frac{m-nb}{2p}}\right) e_8(\rho_1)\sqrt{\frac{\mu}{p}}\,\theta_{10}\left(\frac{b+\sqrt{N}}{2p}\right) \tag{3.11}$$

where $\rho_1 = \frac{m-nb}{2p} - 1 + aDnc\frac{m-nb}{2p}$. Since $4 \mid n$ or $4 \mid m$ and just one of them, $\frac{m-nb}{2p}$ is odd and ρ_1 is even. Replacing μ by $-\mu$ has the effect of changing ρ_1 by $\rho_1 + 2(\frac{m-nb}{2p})$, hence changing μ by $-\mu$ if necessary we can assume that $\rho_1 \equiv 0 \bmod 4$.

Looking at the ideal $\bar{\mathcal{D}}\mathfrak{p} = \langle \frac{b+\sqrt{N}}{2}, |D|p \rangle = \langle \mu \frac{b+\sqrt{N}}{2}, \mu|D| \rangle$ we see that the change of basis matrix is given by $\tilde{M} = \begin{pmatrix} \frac{m+nb}{2} & -anc \\ |D|n & \frac{m-nb}{2} \end{pmatrix}$. Hence applying Lemma 3.1.2 again we get:

$$\theta_{10}\left(\frac{b+\sqrt{N}}{2|D|}\right) = \left(\frac{n|D|}{\frac{m-nb}{2p}}\right) e_8(\rho_2)\sqrt{\frac{\mu}{p}}\,\theta_{10}\left(\frac{b+\sqrt{N}}{2p|D|}\right) \tag{3.12}$$

where $\rho_2 = \frac{m-nb}{2p} - 1 - anc\frac{m-nb}{2p}$. Since $2|n$ and $2 \nmid D$, $aDnc \equiv -anc \bmod 4$. Then $\rho_1 \equiv \rho_2 \bmod 4$ and by the way we chose μ, $\rho_1 + \rho_2 \equiv 0 \bmod 8$.

Multiplying equation (3.11) and equation (3.12) we get:

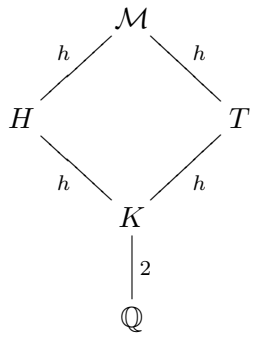
$$\theta_{10}\left(\frac{b+\sqrt{N}}{2}\right)\theta_{10}\left(\frac{b+\sqrt{N}}{2|D|}\right) = \left(\frac{|D|}{\frac{m-nb}{2p}}\right)\frac{\mu}{p}\,\theta_{10}\left(\frac{b+\sqrt{N}}{2p}\right)\theta_{10}\left(\frac{b+\sqrt{N}}{2p|D|}\right)$$

Since we are assuming $N \equiv b \equiv 1 \bmod 8$ and $b^2 - 4aDpc = N$, c must be even. Also $\rho_1 \equiv \frac{m-nb}{2} - 1 \equiv 0 \bmod 4$, then $\frac{m-nb}{2} \equiv 1 \bmod 4$. By the reciprocity law, $\left(\frac{|D|}{\frac{m-nb}{2p}}\right) = \left(\frac{\frac{m-nb}{2}}{|D|}\right)\left(\frac{p}{|D|}\right) = \varepsilon_{\bar{\mathcal{D}}}(\mu)\left(\frac{p}{|D|}\right)$ □

Note: While defining the normalization we ask an extra condition for the Jacobi theta function. The problem is that if $N \equiv 5 \bmod 8$ then the matrix M constructed

while proving the last lemma is usually not in $\Gamma_0(2)$ hence we cannot compare the value of $\theta_{10}(\mathfrak{p})$ and $\theta_{10}(\mathcal{O}_K)$ and here is where the restriction on N appears.

Theorem 3.2.2. *The number $n_{\mathcal{A},\mathcal{B},\bar{\mathcal{D}}}$ is in the field $\mathcal{M} = HT$. It corresponds to the fields diagram:*



Proof. By theorem 3.2.1 the number $\theta(\vec{0}, z_{\mathcal{A}\bar{\mathcal{D}}}Q_{\mathcal{B}})/\eta(z_{\bar{\mathcal{D}}})\eta(\mathcal{O}_K)$ is in H and T contains the image of $\psi_{\bar{\mathcal{D}}}(Cl\mathcal{O}_K)$ hence $n_{\mathcal{A},\mathcal{B},\bar{\mathcal{D}}}$ is in $\mathcal{M}$. □

Proposition 3.2.2. *The quotient $\theta_{Q_{\mathcal{B}}}(z_{\mathcal{A}\bar{\mathcal{D}}})/\psi_{\bar{\mathcal{D}}}(\bar{\mathcal{A}})$ depends only on the class of $\mathcal{B}$ and the class of $\mathcal{A}$.*

Proof. Independence of $\mathcal{B}$ is clear since $\Theta_{\mathcal{B}}$ depends only in the class of $\mathcal{B}$.
To prove independence of $\mathcal{A}$, let $\alpha \in \mathcal{O}_K$ be an element with prime norm q such that $q \nmid 6a|D|$. By definition $\Theta_{\mathcal{B}}(z_{\alpha\mathcal{A}\mathcal{D}}) = \Theta_{\mathcal{B}}(\frac{b+\sqrt{N}}{2aq|D|})$. Then by lemma 3.2.1:

$$\Theta_{\mathcal{B}}\left(\frac{b+\sqrt{N}}{2an|D|}\right) = \psi_{\bar{\mathcal{D}}}(\bar{\alpha})\Theta_{\mathcal{B}}\left(\frac{b+\sqrt{N}}{2a|D|}\right)$$

Since $\psi_{\bar{\mathcal{D}}}(\bar{\alpha}\bar{\mathcal{A}}) = \psi_{\bar{\mathcal{D}}}(\bar{\alpha})\psi_{\bar{\mathcal{D}}}(\bar{\mathcal{A}})$ we get the result. □

Since the number $n_{\mathcal{A},\mathcal{B},\bar{\mathcal{D}}}$ depends only on the equivalent classes of $\mathcal{A}$ and $\mathcal{B}$ we will denote it by $n_{[\mathcal{A}],[\mathcal{B}],\bar{\mathcal{D}}}$.

Proposition 3.2.3. *The number $n_{[\mathcal{A}],[\mathcal{B}],\bar{\mathcal{D}}}$ is an algebraic integer.*

Proof. We already proved that $\theta_{Q_{\mathcal{B}}}(z_{\mathcal{A}\bar{\mathcal{D}}})/\eta(z_{\bar{\mathcal{D}}})/\eta(z_{\mathcal{O}_K})$ is an algebraic integer (see theorem 3.2.1). The number $\psi_{\bar{\mathcal{D}}}(\bar{\mathcal{A}})$ has norm $N\mathcal{A}$. Since the quotient depends on the class of the ideal $\mathcal{A}$ but not $\mathcal{A}$ itself, using Tchebotarev density theorem we can choose two prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ in the same class of $\mathcal{A}$ of prime norms p_1 and p_2. Looking at $\mathfrak{p}_1$ we see that the minimal polynomial of $n_{[\mathfrak{p}_1],[\mathcal{B}],\bar{\mathcal{D}}}$ has rational coefficients with only 1 or p_1 in the denominator. Considering $\mathfrak{p}_2$ we see that the minimal polynomial of $n_{[\mathfrak{p}_2],[\mathcal{B}],\bar{\mathcal{D}}}$ only has 1 or p_2 in the denominator. Since $n_{[\mathfrak{p}_1],[\mathcal{B}],\bar{\mathcal{D}}} = n_{[\mathfrak{p}_1],[\mathcal{B}],\bar{\mathcal{D}}}$ its minimal polynomial must have integer coefficients.□

Proposition 3.2.4. $n_{[\mathcal{A}],[\bar{\mathcal{B}}],\bar{\mathcal{D}}} = n_{[\mathcal{A}],[\mathcal{B}],\bar{\mathcal{D}}}$

Proof. It is easy to check that the theta function $\Theta_{\mathcal{B}}$ associated to $\mathcal{B}$ is the same as the theta function $\Theta_{\mathrm{Adj}\,B}$ associated to the adjoint matrix of $\mathcal{B}$. Clearly the point $z_{\mathcal{A}\bar{\mathcal{D}}}$ and the number $\psi_{\bar{\mathcal{D}}}(\mathcal{A})$ are independent of $\mathcal{B}$. □

Lemma 3.2.4. *The character $\psi_{\bar{\mathcal{D}}}$ satisfy:* $\overline{\psi_{\mathcal{D}}(\bar{\mathcal{A}})} = \psi_{\bar{\mathcal{D}}}(\mathcal{A})$

Proof. Clearly $\overline{\psi_{\mathcal{D}}(\bar{\mathcal{A}})}\psi_{\mathcal{D}}(\bar{\mathcal{A}}) = N\mathcal{A}$. Also $N\mathcal{A} = \psi_{\mathcal{D}}(\bar{\mathcal{A}})\psi_{\mathcal{D}}(\mathcal{A})\varepsilon_{\mathcal{D}}(N\mathcal{A})$ hence $\overline{\psi_{\mathcal{D}}(\bar{\mathcal{A}})} = \left(\frac{N\mathcal{A}}{|D|}\right)\psi_{\mathcal{D}}(A)$. By the coherent way we chose the characters,

$$\psi_{\text{-}D}(\mathcal{A}) = \psi_{\mathcal{D}}(\mathcal{A})\varepsilon_{\bar{\mathcal{D}}}(\mathcal{A}^h)\varepsilon_{\mathcal{D}}(\mathcal{A}^h) = \psi_{\mathcal{D}}(\mathcal{A})\left(\frac{(N\mathcal{A})^h}{|D|}\right)$$

Since $|N|$ is prime, the class number h is odd. □

Proposition 3.2.5. $\overline{n_{[\mathcal{A}],[\mathcal{B}],\bar{\mathcal{D}}}} = n_{[\bar{\mathcal{A}}],[\mathcal{B}],\mathcal{D}}$

Proof. It is clear from their definition that $\overline{\Theta_{\mathcal{B}}(z_{\mathcal{A}\bar{\mathcal{D}}})} = \Theta_{\mathcal{B}}(-\overline{z_{\mathcal{A}\bar{\mathcal{D}}}})$ and $\overline{\eta(z_{\mathcal{A}\bar{\mathcal{D}}})} = \eta(-\overline{z_{\mathcal{A}\bar{\mathcal{D}}}})$ (respectively $\overline{\theta_{10}(z_{\mathcal{A}\bar{\mathcal{D}}})} = \theta_{10}(-\overline{z_{\mathcal{A}\bar{\mathcal{D}}}})$). Since $-\overline{z_{\mathcal{A}\bar{\mathcal{D}}}} = z_{\bar{\mathcal{A}}\mathcal{D}}$ and $\overline{\psi_{\mathcal{D}}(\bar{\mathcal{A}})} = \psi_{\bar{\mathcal{D}}}(\mathcal{A})$ by lemma 3.2.4 the result follows. □.

Proposition 3.2.6. *If the ideal $\mathcal{D}$ is principal in $\mathcal{O}_K$,* $\overline{n_{[\mathcal{A}],[\mathcal{B}],\bar{\mathcal{D}}}} = n_{[\bar{\mathcal{A}}],[\mathcal{B}],\bar{\mathcal{D}}}$

Proof. Replacing in equation (3.3) z by $a|D|z/c$ we get:

$$\Theta_{\mathcal{B}}(-c/a|D|z) = (-i)\frac{a}{c}z\sqrt{|D|}\Theta_{\mathrm{Adj}\,(\mathcal{B})}(az/c) \tag{3.13}$$

Also $|z_{\mathcal{A}\bar{\mathcal{D}}}|^2 = c/(a|D|)$, then $-\overline{z_{\mathcal{A}\bar{\mathcal{D}}}} = -\frac{c}{a|D|z_{\mathcal{A}\bar{\mathcal{D}}}}$. Evaluating equation 3.13 at $z_{\mathcal{A}\bar{\mathcal{D}}}$ we get:

$$\Theta_{\mathcal{B}}(-\overline{z_{\mathcal{A}\bar{\mathcal{D}}}}) = (-i)\frac{a}{c} z_{\mathcal{A}\bar{\mathcal{D}}} \sqrt{|D|} \Theta_{\mathrm{Adj}\,(\mathcal{B})}(\frac{a}{c} z_{\mathcal{A}\bar{\mathcal{D}}})$$

Since $\Theta_Q = \Theta_{\mathrm{Adj}\,Q}$ we can replace $\mathrm{Adj}\,(\mathcal{B})$ by B in the last equation.

If $\mathcal{A} = \langle a, \frac{b+\sqrt{N}}{2} \rangle$, there is a natural ideal associated to it defined by $\mathcal{C} := \langle c, \frac{b+\sqrt{N}}{2} \rangle$, where $b^2 - N = 4ac|D|$. Then it is clear that $\frac{a}{c} z_{\mathcal{A}\bar{\mathcal{D}}} = z_{\mathcal{C}\bar{\mathcal{D}}}$ and we get the functional equation:

$$\Theta_{\mathcal{B}}(-\overline{z_{\mathcal{A}\bar{\mathcal{D}}}}) = (-i) z_{\mathcal{C}\bar{\mathcal{D}}} \sqrt{|D|} \Theta_{\mathcal{B}}(z_{\mathcal{C}\bar{\mathcal{D}}}) \tag{3.14}$$

Also $\mathcal{A}\mathcal{C}\bar{\mathcal{D}} = \langle \frac{b+\sqrt{N}}{2} \rangle$. Then if $\bar{\mathcal{D}}$ is principal (which is the same as $\mathcal{D}$ being principal), $[\mathcal{C}] = [\bar{\mathcal{A}}]$.

The denominator part is not that straightforward hence we will break the proof into several steps and lemmas to make it easier. We will just consider the case of the eta function since the Jacobi theta function case follows from similar computations.

First we need to study the term $\eta(z_{\mathcal{O}_K})$. We chose $z_{\mathcal{O}_K} = \frac{b+\sqrt{N}}{2}$, then $\overline{\eta(z_{\mathcal{O}_K})} = \eta(-\overline{z_{\mathcal{O}_K}}) = \eta(-b + z_{\mathcal{O}_K})$. Since $b \equiv 3 \bmod 24$ and the eta function satisfies the transformation $\eta(z+1) = e_{24}\,\eta(z)$,

$$\overline{\eta(z_{\mathcal{O}_K})} = \eta(z_{\mathcal{O}_K}) e_8(-1) \tag{3.15}$$

The other eta term is $\overline{\eta(z_{\bar{\mathcal{D}}})} = \eta(-\overline{z_{\bar{\mathcal{D}}}}) = \eta(\frac{-b+\sqrt{N}}{2|D|})$. This number is the one corresponding to the ideal $\mathcal{D}$, but $-b \not\equiv 3 \bmod 24$. Note that $\frac{-b+\sqrt{N}}{2|D|} + |D|b = \frac{(2D^2-1)b+\sqrt{N}}{2|D|}$, and since $b \equiv 3 \bmod 24$ it follows that $(2D^2-1)b \equiv 3 \bmod 24$ hence:

$$\eta(-\overline{z_{\bar{\mathcal{D}}}}) = \eta(z_{\mathcal{D}}) e_8(-|D|) \tag{3.16}$$

Lemma 3.2.5. *let $\mathcal{A}$ be a principal ideal of norm a. For a positive integer n let $\sqrt{n^*} = \sqrt{n} e_8(n-1)$, then $\frac{\eta(\mathcal{A})\eta(\bar{\mathcal{A}})}{\sqrt{a^*}\,\eta(\mathcal{O}_K)^2} = 1$.*

Proof. Since we are assuming $N \neq -3$ the number of units in the Hilbert class field is 2. Then this is just Lemma 23 part (i) and (ii) of [Ha-Vi], where $\tilde{w} = w/2 = 1$ and $\mathcal{A}$ is principal. $\square$

Since $|D| \equiv 3 \bmod 4$, $\sqrt{|D|^*} = \sqrt{|D|} e_8(|D|-1)$. Then lemma 3.2.5 on the principal ideal $\mathcal{D}$ says:

$$\frac{\eta(D)\eta(\bar{\mathcal{D}})}{\eta(\mathcal{O}_K)^2} = e_8(|D|-1)\sqrt{|D|}$$

And it follows that:

$$\eta(\mathcal{D}) = \frac{\eta(\mathcal{D})\eta(\bar{\mathcal{D}})}{\eta(\mathcal{O}_K)^2}\frac{\eta(\mathcal{O}_K)^2}{\eta(\bar{\mathcal{D}})^2}\eta(\bar{\mathcal{D}}) = e_8(|D|-1)\sqrt{|D|}\,\frac{\eta(\mathcal{O}_K)^2}{\eta(\bar{\mathcal{D}})^2}\eta(\bar{\mathcal{D}})$$

Since $e_8(-1)\, e_8(-|D|)\, e_8(|D|-1) = e_8(-2) = -i$, we get:

$$\overline{\eta(\mathcal{O}_K)}\,\overline{\eta(\bar{\mathcal{D}})} = (-i)\sqrt{|D|}\eta(\mathcal{O}_K)\eta(\bar{\mathcal{D}})\frac{\eta(\mathcal{O}_K)^2}{\eta(\bar{\mathcal{D}})^2} \tag{3.17}$$

Let ν be a generator of $\bar{\mathcal{D}}$. Then $\kappa(\nu) = \chi_4(|D|)\frac{1}{\bar{\nu}}\frac{\eta^2(\nu)}{\eta^2(\mathcal{O}_K)}$. Since $\chi_4(|D|) = -1$ we can rewrite equation (3.17) as:

$$\overline{\eta(\mathcal{O}_K)}\,\overline{\eta(\bar{\mathcal{D}})} = (-i)\sqrt{|D|}\eta(\mathcal{O}_K)\eta(\bar{\mathcal{D}})/\bar{\nu} * (-\kappa(\nu))$$

Although $\kappa(\nu)$ should be in the denominator, it makes no difference since it is ± 1.

Finally we need to study the character term $\overline{\psi_{\bar{\mathcal{D}}}(\bar{\mathcal{A}})}$. Since $\overline{\psi_{\bar{\mathcal{D}}}(\bar{\mathcal{A}})}\psi_{\bar{\mathcal{D}}}(\bar{\mathcal{A}}) = N\mathcal{A}$, and $N\mathcal{A} = \psi_{\bar{\mathcal{D}}}(\bar{\mathcal{A}})\psi_{\bar{\mathcal{D}}}(\mathcal{A})\varepsilon_{\bar{\mathcal{D}}}(N\mathcal{A})$ we conclude that

$$\overline{\psi_{\bar{\mathcal{D}}}(\bar{\mathcal{A}})} = \left(\frac{N\mathcal{A}}{|D|}\right)\psi_{\bar{\mathcal{D}}}(A)$$

Clearly $\mathcal{A}\mathcal{C}\bar{\mathcal{D}} = \langle\frac{b+\sqrt{N}}{2}\rangle$, then $\mathcal{A} = \bar{\mathcal{C}}\left(\frac{b+\sqrt{N}}{2c|D|}\right)\bar{\nu}$. Since $N\mathcal{A}$ is prime to $|D|$, $\bar{\mathcal{C}}$ is prime to $\bar{\mathcal{D}}$ and also $\left(\frac{b+\sqrt{N}}{2c|D|}\right)\bar{\nu}$ is prime to $|D|$, then we can split the character as:

$$\psi_{\bar{\mathcal{D}}}(\mathcal{A}) = \psi_{\bar{\mathcal{D}}}(\bar{\mathcal{C}})z_{\mathcal{C}\bar{\mathcal{D}}}\bar{\nu}\varepsilon_{\bar{\mathcal{D}}}\left(\frac{b+\sqrt{N}}{2c|D|}\bar{\nu}\right)$$

If we denote $\xi := \varepsilon_{\bar{\mathcal{D}}}\left(N\mathcal{A}\left(\frac{b+\sqrt{N}}{2c|D|}\right)\bar{\nu}\right) = \varepsilon_{\bar{\mathcal{D}}}\left(\left(\frac{b+\sqrt{N}}{2c|D|}\right)\bar{\nu}\right)\left(\frac{N\mathcal{A}}{|D|}\right)$, we get:

$$\overline{\eta(\mathcal{O}_K)}\,\overline{\eta(\bar{\mathcal{D}})}\,\overline{\psi_{\bar{\mathcal{D}}}(\bar{\mathcal{A}})} = (-i)z_{\mathcal{C}\bar{\mathcal{D}}}\sqrt{|D|}\,\eta(\mathcal{O}_K)\eta(\bar{\mathcal{D}})\psi_{\bar{\mathcal{D}}}(\bar{\mathcal{C}})(-\kappa(\nu))\xi \tag{3.18}$$

From equations (3.14) and (3.18) we are led to prove that $(-\kappa(\nu))\xi = 1$, which will be done in the next two lemmas. □

Lemma 3.2.6. *If $\nu = \frac{m+n\sqrt{N}}{2}$ and $a = N\mathcal{A}$, then $\xi := \varepsilon_{\bar{\mathcal{D}}}\left(\frac{b+\sqrt{N}}{2c|D|}\bar{\nu}a\right) = \left(\frac{n}{|D|}\right)$*

Proof. Clearly $\left(\frac{b+\sqrt{N}}{2c|D|}\right)\bar{\nu} = \left(\frac{b+\sqrt{N}}{2c|D|}\right)\left(\frac{m-n\sqrt{N}}{2}\right) = \frac{(bm-nN)+(-bn+m)\sqrt{N}}{4c|D|}$. Since $\bar{\mathcal{D}} = \langle|D|, \frac{b+\sqrt{N}}{2}\rangle$, $\frac{\sqrt{N}}{2} \equiv \frac{-b}{2} \bmod \bar{\mathcal{D}}$. Then $\left(\frac{b+\sqrt{N}}{2c|D|}\right)\bar{\nu} \equiv \frac{n(b^2-N)}{4c|D|} \equiv an \bmod \bar{\mathcal{D}}$ and $\varepsilon_{\bar{\mathcal{D}}}(\frac{b+\sqrt{N}}{2c|D|}\bar{\nu}) = \left(\frac{an}{|D|}\right)$ as stated.□

Lemma 3.2.7. *If $\nu = \frac{m+n\sqrt{N}}{2}$ then $-\kappa(\nu) = \left(\frac{n}{|D|}\right)$*

Proof. We know that $\kappa(\nu)$ is ± 1, then we can restrict our attention on a transformation formula concerning the 4-th roots of unity of the eta function. We have:

Lemma 3.2.8. *Let $M := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a matrix in $Sl_2(\mathbb{Z})$ and $p_4(M)$ the polynomial $(b^2 - a + 2)c + (a^2 - b + 2)d + ad$. Then:*

$$\eta^2(Mz) = (cz + d)\,\xi_3\,\xi_4\,\eta^2(z)$$

where ξ_3 is a third root of unity and ξ_4 a fourth root of unity given by the formula $\xi_4 := e^{-2\pi i p_4(M)/4}$

Proof. See page 498 of [Ha-Vi].

The ideal $\bar{\mathcal{D}}$ satisfies $\bar{\mathcal{D}} = \langle\frac{b+\sqrt{N}}{2}, |D|\rangle = \left(\frac{m+n\sqrt{N}}{2}\right)\langle\frac{b+\sqrt{N}}{2}, 1\rangle$, so there is a matrix M in $Sl_2(\mathbb{Z})$ making the change of basis given by $M := \begin{pmatrix} \frac{m+nb}{2} & -anc \\ n & \frac{m-nb}{2|D|} \end{pmatrix}$. Since $nz_{\bar{\mathcal{D}}} + \frac{m-nb}{2|D|} = \frac{\nu}{|D|}$, using lemma 3.2.8 we get:

$$-\kappa(\nu) = \frac{\nu}{|D|}\frac{\eta^2(z_{\bar{\mathcal{D}}})}{\eta^2(z_{\mathcal{O}_K})} = e^{-2\pi i p_4(M)/4} \tag{3.19}$$

Let $k = \frac{m-nb}{2|D|}$, then $p_4(M) = (a^2n^2c^2 - |D|k - nb + 2)n + ((|D|k + nb)^2 + anc + 2)k + |D|k^2 + nbk$. Since $2 \nmid a|D|$ reducing $p_4(M)$ modulo 4 we get:

$$p_4(M) \equiv (n^2c^2 + k - 3n + 2)n + ((3n - k)^2 + anc + 2)k + 3k^2 + 3nk \bmod 4$$

or equivalently:

$$p_4(M) \equiv n^3c^2 - 3n^2 + 2n + n^2k + 2nk^2 + k^3 + anck + 2k + 3k^2 \bmod 4 \qquad (3.20)$$

We want to know between ν and $-\nu$ which one makes $p_4(M) \equiv 0 \bmod 4$. Since we know already that $-\kappa(\nu)\nu$ satisfies this, the strategy will be to prove that the good generator written as $\frac{r+s\sqrt{N}}{2}$ satisfies $\left(\frac{s}{|D|}\right) = +1$. This implies that if we start with ν, then $\left(\frac{n}{|D|}\right)\nu$ is the correct generator, and $-\kappa(\nu) = \left(\frac{n}{|D|}\right)$.

Since ν is a generator of $\bar{\mathcal{D}}$ it satisfies:

$$\left(\frac{m}{2}\right)^2 + \left(\frac{n}{2}\right)^2 |N| = |D| \qquad (3.21)$$

Observations:

1. Since ν is an integer, if $2|n$ then $2|m$. If $4|n$ looking equation (3.21) modulo 4 we would have that $|D| \equiv 0, 1 \bmod 4$ which is not the case, hence $4 \nmid n$. Also reducing (3.21) modulo 4 we see that 4 divides m, since $|D| \equiv |N| \equiv 3 \bmod 4$. Then $k := \frac{m-nb}{2|D|}$ is odd.

2. Since $b^2 - 4ac|D| = N$ and $2 \nmid aD$ looking modulo 8: $1 + |N| \equiv 4c \bmod 8$

To prove the equality we will need to consider different cases.

Case 2|n: Since k is odd by the observation equation (3.20) reads:

$$p_4(M) \equiv k^3 + 2ck + 2k + 3k^2 \equiv k + 2c + 1 \bmod 4$$

We can write $\left(\frac{n}{|D|}\right)$ as $\left(\frac{2}{|D|}\right)\left(\frac{n/2}{|D|}\right)$. Equation (3.21) says that $\left(\frac{|D|}{n/1}\right) = 1$, then since $n/2$ is odd, we can use the quadratic reciprocity law to get:

$$\left(\frac{n}{|D|}\right) = \left(\frac{2}{|D|}\right)(-1)^{\frac{n-2}{4}}$$

Which gives the two cases:

$$\left(\frac{n}{|D|}\right) = +1 \text{ if } \begin{cases} n \equiv 6 \bmod 8 & \text{when } |D| \equiv 3 \bmod 8 \\ n \equiv 2 \bmod 8 & \text{when } |D| \equiv 7 \bmod 8 \end{cases}$$

Let n be chosen such that $\left(\frac{n}{|D|}\right) = +1$. To prove with this choice of n, $p_4(M) \equiv 0 \bmod 4$, we consider the sub-cases:

- If $|N| \equiv 3 \bmod 8$, c is odd by the second observation and

  $$p_4(M) \equiv k + 3 \bmod 4$$

  The possibilities for $|D|$ are:

  * $|D| \equiv 3 \bmod 8$, in which case $8|m$ by looking at (3.21) modulo 8. Then $|D|k \equiv -3\frac{n}{2} \bmod 4$. Since $n \equiv 6 \bmod 8$, $k \equiv 1 \bmod 4$ and $p_4(M) \equiv 0 \bmod 4$.

  * $|D| \equiv 7 \bmod 8$, in which case $4|m$ and $8 \nmid m$ by looking at (3.21) modulo 8. Then $\frac{m}{2} \equiv 2 \bmod 4$ and $|D|k \equiv 2 - 3\frac{n}{2} \bmod 4$. Since $n \equiv 2 \bmod 8$, $|D|k \equiv 3 \bmod 4$. Then $k \equiv 1 \bmod 4$ and $p_4(M) \equiv 0 \bmod 4$.

- If $|N| \equiv 7 \bmod 8$, c is even by the second observation and

  $$p_4(M) \equiv k + 1 \bmod 4$$

  The possibilities for $|D|$ are:

  * $|D| \equiv 3 \bmod 8$, in which case $4|m$ and $8 \nmid m$ by looking at (3.21) modulo 8. Then $\frac{m}{2} \equiv 2 \bmod 4$ and $|D|k \equiv 2 - 3\frac{n}{2} \bmod 4$. Since $n \equiv 6 \bmod 8$, $|D|k \equiv 1 \bmod 4$. Then $k \equiv 3 \bmod 4$ and $p_4(M) \equiv 0 \bmod 4$.

  * $|D| \equiv 7 \bmod 8$, in which case $8|m$ by looking at (3.21) modulo 8. Then $|D|k \equiv -3\frac{n}{2} \bmod 4$. Since $n \equiv 2 \bmod 8$, $k \equiv 3 \bmod 4$ and $p_4(M) \equiv 0 \bmod 4$.

Case 2 $\nmid$ n: Since $2 \nmid m$, if we look at (3.21) modulo 8 we see that $|N|$ cannot be congruent to 7 modulo 8 (or $|D|$ would be even) hence c is odd by the second observation.

By the quadratic reciprocity law $\left(\frac{n}{|D|}\right) = (-1)^{\frac{n-1}{2}}$, so if we pick $n \equiv 1 \bmod 4$ the quadratic symbol is $+1$. Then:

$$p_4(M) \equiv k(k^2 + k + 3 + ac) \bmod 4$$

- If $2|k$, since ac is odd it is clear that $p_4(M) \equiv 0 \bmod 4$.
- If $2 \nmid k$ we need to show that $k + ac \equiv 0 \bmod 4$. Since k is odd, $2 \equiv 2k|D| \equiv m - 3 \bmod 4$ i.e. $m \equiv 1 \bmod 4$. Also since $b \equiv 3 \bmod 48$ and $4|D| \equiv 12 \bmod 16$ we get the equation:

  $$9 + |N| \equiv 12ac \bmod 16 \tag{3.22}$$

  Then reducing (3.21) modulo 16 gives:

  $$m^2 + n^2|N| \equiv 4|D| \equiv 12 \bmod 16 \tag{3.23}$$

  So we consider the two different cases for $|N|$:

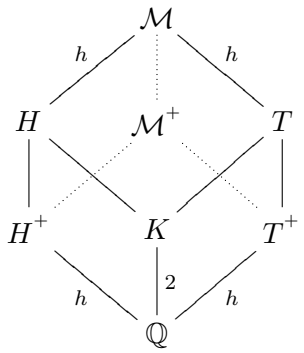
  * If $|N| \equiv 3 \bmod 16$, by (3.22) $ac \equiv 1 \bmod 4$.

  The integers m and n are congruent to 1 modulo 4 and they satisfy equation (3.23). Since 1 and 9 are the only odd squares modulo 16 then $m^2 \not\equiv n^2 \bmod 16$. Hence $m \equiv n + 4 \bmod 8$ and $2|D|k = m - bn \equiv n + 4 - 3n \equiv 4 - 2n \bmod 8$. Since $n \equiv 1 \bmod 4$, $k \equiv 3 \bmod 4$ and $k + ac \equiv 0 \bmod 4$.

  * If $|N| \equiv 11 \bmod 16$, by (3.22) $ac \equiv 3 \bmod 4$.

  Since m and n are congruent to 1 modulo 4 and they satisfy (3.23) it must be the case that $m \equiv n \bmod 8$. Then $2k|D| \equiv -2n \bmod 8$. Since $n \equiv 1 \bmod 4$, $k \equiv 1 \bmod 1$ and $k + ac \equiv 0 \bmod 4$. □

Proposition 3.2.6 implies that if $\mathcal{A}$ and $\mathcal{D}$ are both principal then the number $n_{[\mathcal{A}],[\mathcal{B}],\bar{\mathcal{D}}}$ lives in a subfield of $\mathcal{M}$ which we note $\mathcal{M}^+$ (following [Bu-Gr] notation, see page 13) and corresponds to the field diagram



The next step will be to relate the numbers $n_{[\mathcal{A}],[\mathcal{B}],\bar{\mathcal{D}}}$ for different ideals $\mathcal{D}$.

Lemma 3.2.9. *Let $\mathcal{D}$ and $\mathcal{D}'$ be two prime ideals of $\mathbb{Q}(\sqrt{N})$ with norm $|D|$ and $|D'|$ respectively, and let $\mu \in \mathbb{Q}(\sqrt{N})$ be such that $\mu\mathcal{D} = \mathcal{D}'$. Then $\frac{\eta^2(\mathcal{A}\mathcal{D}')}{\eta^2(\mathcal{A}\mathcal{D})} = \bar{\mu}\kappa(\mu)\chi_4(N\mu)$.*

Proof. Note that although κ is defined on integer elements, since it is a character on $(\mathcal{O}_K/12\mathcal{O}_K)^\times$, we can extend it multiplicatively to all elements in $\mathbb{Q}(\sqrt{N})$ with both numerator and denominator prime to 12. By definition $\kappa(\mu) = \frac{1}{\bar{\mu}}\chi_4(N\mu)\frac{\eta^2(\mu)}{\eta^2(\mathcal{O}_K)}$ then we are led to prove:

$$\frac{\eta^2(\mathcal{A}\mathcal{D}')}{\eta^2(\mathcal{A}\mathcal{D})}\frac{\eta^2(\mathcal{O}_K)}{\eta^2(\mu)} = 1 \tag{3.24}$$

By Proposition 10 of [Ha-Vi] we can write the left hand side of (3.24) as $\left(\frac{\eta^2(\mathcal{A}\mathcal{D})}{\eta^2(\mathcal{O}_K)}\right)^{\sigma_{(\bar{\mathcal{D}}'\bar{\mathcal{D}}^{-1})}-1}$.
Since $\frac{\eta^2(\mathcal{A}\mathcal{D})}{\eta^2(\mathcal{O}_K)}$ is in H (by theorem 20 of [Ha-Vi]) then $\sigma_{\mathcal{A}}$ represents the classical Artin map from $Cl(\mathcal{O}_K)$ to $\mathrm{Gal}(H/K)$, and since $\bar{\mathcal{D}}'\bar{\mathcal{D}}^{-1}$ is principal, $\sigma_{\bar{\mathcal{D}}'\bar{\mathcal{D}}^{-1}}$ is the identity. □

Lemma 3.2.10. *Let $\mathcal{D}$ and $\mathcal{D}'$ be two prime ideals of $\mathbb{Q}(\sqrt{N})$ such that $\mathcal{D} \sim \mathcal{D}'$. Then $\frac{\eta(\mathcal{A}\mathcal{D}')\eta(\mathcal{D})}{\eta(\mathcal{A}\mathcal{D})\eta(\mathcal{D}')} = \varepsilon_{\mathcal{D}}(\bar{\mathcal{A}}^h)\varepsilon_{\mathcal{D}'}(\bar{\mathcal{A}}^h)$*

Proof. By proposition 10 of [Ha-Vi] we have:

$$\frac{\eta(\mathcal{A}\mathcal{D}')\eta(\mathcal{D})}{\eta(\mathcal{D}')\eta(\mathcal{A}\mathcal{D})} = \left(\frac{\eta(\mathcal{A})}{\eta(\mathcal{O}_K)}\right)^{\sigma_{\bar{\mathcal{D}}'}}\left(\frac{\eta(\mathcal{A})}{\eta(\mathcal{O}_K)}\right)^{-\sigma_{\bar{\mathcal{D}}}}\left(\frac{a}{|D|}\right)\left(\frac{a}{|D'|}\right) \tag{3.25}$$

Since the Artin-Frobenius map is an homomorphism:

$$\left(\frac{\eta(\mathcal{A})}{\eta(\mathcal{O}_K)}\right)^{\sigma_{\bar{\mathcal{D}}'}-\sigma_{\bar{\mathcal{D}}}} = \left(\left(\frac{\eta(\mathcal{A})}{\eta(\mathcal{O}_K)}\right)^{\sigma_{(\bar{\mathcal{D}}'(\bar{\mathcal{D}})^{-1})^{-1}}}\right)^{\sigma_{\bar{\mathcal{D}}}}$$

But $\left(\frac{\eta(\mathcal{A})}{\eta(\mathcal{O}_K)}\right)^{\sigma_{(\bar{\mathcal{D}}'(\bar{\mathcal{D}})^{-1})^{-1}}} = \pm 1$ (see the proof of lemma 3.2.9), then $\sigma_{\bar{\mathcal{D}}}$ acts trivially on it.

Let $\mu \in \mathbb{Q}(\sqrt{N})$ be such that $\bar{\mathcal{D}}'\bar{\mathcal{D}}^{-1} = \frac{\bar{\mu}}{|D|}$ then using theorem 19 of [Ha-Vi] we get:

$$\left(\frac{\eta(\mathcal{A})}{\eta(\mathcal{O}_K)}\right)^{\sigma_{(\bar{\mathcal{D}}'(\bar{\mathcal{D}})^{-1})^{-1}}} = \kappa\left(\frac{\mu}{|D|}\right)^{\frac{a-1}{2}}\left(\frac{\bar{\mu}|D|}{\bar{\mathcal{A}}}\right) \tag{3.26}$$

Since $|D|$ is prime to 12, and κ is a multiplicative quadratic character, $\kappa(\frac{\mu}{|D|}) = \kappa(\mu)\kappa(|D|)$. The character κ defined on $(\mathcal{O}_K/12\mathcal{O}_K)^\times$ factors as a product of two characters, κ_3 from $(\mathcal{O}_K/3\mathcal{O}_K)^\times$ to the group of third roots of unity and κ_4 from $(\mathcal{O}_K/4\mathcal{O}_K)^\times$ to the group of fourth roots of unity (see lemma 14 of [Ha-Vi]). In our case $\kappa_3 = 1$ and the character is completely determined from the congruence modulo 4. Then $\kappa(|D|) = \kappa(-1) = -1$. Using the quadratic reciprocity law,

$$\left(\frac{\eta(\mathcal{A})}{\eta(\mathcal{O}_K)}\right)^{\sigma_{(\bar{\mathcal{D}}'(\bar{\mathcal{D}})^{-1})^{-1}}} = \kappa(\mu)^{\frac{a-1}{2}}\left(\frac{\bar{\mu}}{\bar{\mathcal{A}}}\right)\left(\frac{a}{|D|}\right) \tag{3.27}$$

Also since $\kappa(\mu)\kappa(\bar{\mu}) = \kappa(|D||D'|) = 1$, $\kappa(\mu) = \kappa(\bar{\mu})$ and we can rewrite equation (3.25) as:

$$\frac{\eta(\mathcal{A}\mathcal{D}')\eta(\mathcal{D})}{\eta(\mathcal{A}\mathcal{D})\eta(\mathcal{D}')} = \kappa(\bar{\mu})^{\frac{a-1}{2}}\left(\frac{\mu}{\mathcal{A}}\right)\left(\frac{a}{|D'|}\right)$$

Since $\bar{\mathcal{D}}\mathcal{D}' = \mu$ and ε is a multiplicative quadratic character:

$$\varepsilon_{\mathcal{D}}(\bar{\mathcal{A}}^h)\varepsilon_{\mathcal{D}'}(\bar{\mathcal{A}}^h) = \varepsilon_{\mathcal{D}}(\bar{\mathcal{A}}^h)\varepsilon_{\bar{\mathcal{D}}}(\bar{\mathcal{A}}^h)\varepsilon_{\bar{\mathcal{D}}\mathcal{D}'}(\bar{\mathcal{A}}^h) = \left(\frac{a}{|D|}\right)\left(\frac{\bar{\mathcal{A}}^h}{\mu}\right) \tag{3.28}$$

The last equality comes from the fact that since N is a prime number, h is odd. Using the reciprocity law in $\mathbb{Q}(\sqrt{N})$ (see for example theorem 21 of [Ha-Vi]):

$$\left(\frac{\bar{\mathcal{A}}^h}{\mu}\right) = \left(\frac{\mu}{\bar{\mathcal{A}}^h}\right)\kappa(\bar{\mu})^{\frac{a-1}{2}} = \left(\frac{\mu}{\bar{\mathcal{A}}}\right)\kappa(\bar{\mu})^{\frac{a-1}{2}} = \kappa(\bar{\mu})^{\frac{a-1}{2}}\left(\frac{\mu}{\mathcal{A}}\right)\left(\frac{|D||D'|}{a}\right) \tag{3.29}$$

Then the lemma follows from $\left(\frac{|D||D'|}{a}\right) = \left(\frac{a}{|D|}\right)\left(\frac{a}{|D'|}\right)$. $\square$

Theorem 3.2.3. *Let $z_{\mathcal{A}\mathcal{D}}Q_{\mathcal{B}}$ and $z_{\mathcal{A}\mathcal{D}'}Q_{\mathcal{B}'}$ be two points in $\mathfrak{h}_2$ such that they are equivalent modulo $Sp_4(\mathbb{Z})$ and $\mathcal{D} \sim \mathcal{D}'$ in $\mathbb{Q}(\sqrt{N})$. Then $n_{[\mathcal{A}],[\mathcal{B}],\bar{D}} = \pm n_{[\mathcal{A}],[\mathcal{B}']\bar{D}'}$*

Proof. By proposition 3.2.5 and proposition 3.2.6 we may restrict to the case $\mathcal{D}' \neq \bar{\mathcal{D}}$ (i.e. $\mathcal{D}$ not principal). For simplicity we will denote $\Omega_{\mathcal{D}} := z_{\mathcal{A}\mathcal{D}}Q_{\mathcal{B}}$ and $\Omega_{\mathcal{D}'} := z_{\mathcal{A}\mathcal{D}'}Q_{\mathcal{B}'}$. Since $\Omega_{\mathcal{D}}$ is equivalent to $\Omega_{\mathcal{D}'}$ there exists a matrix $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ in $Sp_4(\mathbb{Z})$ such that $\gamma \star (\Omega_{\mathcal{D}}) = \Omega_{\mathcal{D}'}$. Thinking as the action on lattices (where it acts by multiplication on the left by $1/\gamma^t$) we have that $\gamma \star \begin{pmatrix} I_2 \\ -\Omega_{\mathcal{D}} \end{pmatrix} = \begin{pmatrix} D & -C \\ -B & A \end{pmatrix} \begin{pmatrix} I_2 \\ -\Omega_{\mathcal{D}} \end{pmatrix} = \begin{pmatrix} C\Omega_{\mathcal{D}}+D \\ -(A\Omega_{\mathcal{D}}+B) \end{pmatrix} = \begin{pmatrix} I_2 \\ -\Omega_{\mathcal{D}'} \end{pmatrix} (C\Omega_{\mathcal{D}} + D)^{-1}$

By the coherent way we chose characters, $\frac{\psi_{\mathcal{D}}(\mathcal{A})}{\psi_{\mathcal{D}'}(\mathcal{A})} = \varepsilon_{\mathcal{D}}(\mathcal{A}^h)\varepsilon_{\mathcal{D}'}(\mathcal{A}^h)$ hence:

$$\frac{n_{[\mathcal{A}],[\mathcal{B}],\bar{D}}}{n_{[\mathcal{A}],[\mathcal{B}']\bar{D}'}} = \frac{\theta(\Omega_{\mathcal{D}})}{\theta(\Omega_{\mathcal{D}'})}\frac{\eta(\mathcal{D}')}{\eta(\mathcal{D})}\varepsilon_{\mathcal{D}}(\bar{\mathcal{A}}^h)\varepsilon_{\mathcal{D}'}(\bar{\mathcal{A}}^h) = \frac{\theta(\Omega_{\mathcal{D}})}{\theta(\Omega_{\mathcal{D}'})}\frac{\eta(\mathcal{A}\mathcal{D}')}{\eta(\mathcal{A}\mathcal{D})}$$

Where the last equality follows from lemma 3.2.10. We claim that:

$$\frac{\theta^2(\Omega_{\mathcal{D}})}{\theta^2(\Omega_{\mathcal{D}'})} = \mathrm{Det}(C\Omega + D)^{-1} = \frac{\eta^2(\mathcal{A}\mathcal{D})}{\eta^2(\mathcal{A}\mathcal{D}')} \tag{3.30}$$

The first equality follows at once from the functional equation (see proposition 2.1).

Since $|D|$ is prime and $\mathrm{Det}(Q) = |D|$ there exists matrices $U, V \in Sl_2(\mathbb{Z})$ such that $UQV = \begin{pmatrix} 1 & 0 \\ 0 & |D| \end{pmatrix}$ (respectively U' and V' for Q'). Then:

$$\begin{pmatrix} V^{-1} & 0 \\ 0 & U \end{pmatrix} \begin{pmatrix} I_2 \\ -\Omega_{\mathcal{D}} \end{pmatrix} V = \begin{pmatrix} I_2 \\ -UQVz_{\mathcal{A}\mathcal{D}} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ -z_{\mathcal{A}\mathcal{D}} & 0 \\ 0 & -z_{\mathcal{A}} \end{pmatrix}$$

Similarly:

$$\begin{pmatrix} V'^{-1} & 0 \\ 0 & U' \end{pmatrix} \begin{pmatrix} I_2 \\ -\Omega_{\mathcal{D}'} \end{pmatrix} V' = \begin{pmatrix} I_2 \\ -U'Q'V'z_{\mathcal{A}\mathcal{D}'} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ -z_{\mathcal{A}\mathcal{D}'} & 0 \\ 0 & -z_{\mathcal{A}} \end{pmatrix}$$

Since $\mathcal{D}' \neq \bar{\mathcal{D}}$, we may choose basis $\mathcal{D} = \langle |D|, \frac{b+\sqrt{N}}{2} \rangle$, $\mathcal{D}' = \langle |D'|, \frac{b+\sqrt{N}}{2} \rangle$ and $\mathcal{A} = \langle a, \frac{b+\sqrt{N}}{2} \rangle$. If μ is such that $\mu\mathcal{D} = \mathcal{D}'$ then $\mathcal{A}\mathcal{D}' = \langle a|D'|, \frac{b+\sqrt{N}}{2} \rangle = \langle \mu a|D|, \mu(\frac{b+\sqrt{N}}{2}) \rangle = \mu\mathcal{A}\mathcal{D}$ hence there exists a matrix $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ in $Sl_2(\mathbb{Z})$ such that:

$$M \begin{pmatrix} \mu(\frac{b+\sqrt{N}}{2}) \\ \mu a|D| \end{pmatrix} = \begin{pmatrix} \frac{b+\sqrt{N}}{2} \\ a|D'| \end{pmatrix}$$

Defining $N := \begin{pmatrix} \delta & 0 & -\gamma & 0 \\ 0 & 1 & 0 & 0 \\ -\beta & 0 & \alpha & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ it follows that:

$$N \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ -z_{\mathcal{A}\mathcal{D}} & 0 \\ 0 & -z_{\mathcal{A}} \end{pmatrix} \begin{pmatrix} \frac{\mu|D|}{|D'|} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ -z_{\mathcal{A}\mathcal{D}'} & 0 \\ 0 & -z_{\mathcal{A}} \end{pmatrix}$$

Combining these results we get that:

$$\begin{pmatrix} V'^{-1} & 0 \\ 0 & U' \end{pmatrix} N \begin{pmatrix} V^{-1} & 0 \\ 0 & U \end{pmatrix} \begin{pmatrix} I_2 \\ -\Omega_{\mathcal{D}} \end{pmatrix} \begin{pmatrix} \frac{\mu|D|}{|D'|} & 0 \\ 0 & 1 \end{pmatrix} VV'^{-1} = \begin{pmatrix} I_2 \\ -\Omega_{\mathcal{D}'} \end{pmatrix}$$

and

$$\begin{pmatrix} I_2 \\ -\Omega_{\mathcal{D}'} \end{pmatrix} = \begin{pmatrix} D & -C \\ -B & A \end{pmatrix} \begin{pmatrix} I_2 \\ -\Omega_{\mathcal{D}} \end{pmatrix} (C\Omega_{\mathcal{D}} + D)^{-1}$$

But both lattices have the same volume then $|\operatorname{Det}(C\Omega_{\mathcal{D}} + D)|^{-1} = \frac{|\mu||D|}{|D'|}$.

By lemma 3.2.9 $\frac{\eta^2(\mathcal{AD})}{\eta^2(\mathcal{AD}')} = \frac{1}{\bar{\mu}}\kappa(\mu) = \frac{\mu|D|}{|D'|}\kappa(\mu)$. Now $\operatorname{Det}(C\Omega_D + D)^{-1}$ and $\kappa(\mu)\frac{\mu|D|}{|D'|}$ have the same absolute value and both lie in $\mathbb{Q}(\sqrt{N})$ hence they differ by ± 1. Then

$$\left(\frac{\theta(\Omega_{\mathcal{D}})}{\theta(\Omega_{\mathcal{D}'})}\frac{\eta(\mathcal{AD}')}{\eta(\mathcal{AD})}\right)^2 = \operatorname{Det}(C\Omega_{\mathcal{D}} + D)^{-1}\bar{\mu}\kappa(\mu) = \pm 1$$

Or taking square roots:

$$\sqrt{\pm 1} = \frac{\theta(\Omega_{\mathcal{D}})}{\theta(\Omega_{\mathcal{D}'})}\frac{\eta(\mathcal{AD}')}{\eta(\mathcal{AD})} \tag{3.31}$$

By theorem 3.2.2 we know that $\frac{\theta(\Omega_{\mathcal{D}})}{\eta(\mathcal{D})\eta(\mathcal{O}_K)}$ and $\frac{\theta(\Omega'_{\mathcal{D}})}{\eta(\mathcal{D}')\eta(\mathcal{O}_K)}$ are in H. Since $\sqrt{-1} \notin H$ the theorem follows. □

It is not clear how to determine the sign a priori, and we are not able to give any answer in this direction.

Chapter 4

Quaternion algebras

The problem of determining whether two points in $\mathfrak{h}_2$ are equivalent or not is complicated in general. For our case we will get this equivalence via ideals in quaternion algebras. We start with the basic definitions and some elementary facts about quaternion algebras. A good reference for these results is Pizer's paper ([Pi]).

4.1 Definitions

Let F denote either the field $\mathbb{Q}$ of rational numbers, the field $\mathbb{Q}_p$ of p-adic numbers, or the field $\mathbb{R}$. A quaternion algebra B over F is a central simple algebra of dimension 4. Any such B has a basis $1, i, j, k$ over F, and multiplication in B is defined by the relations:

- $i^2 = a$
- $j^2 = b$
- $ij = -ji = k$

where a and b are nonzero elements of F. Conversely, given any $a, b \in F^\times$ (i.e. invertible elements of F) the previous relations define a quaternion algebra

over F. We denote this quaternion algebra (a, b) if $F = \mathbb{Q}$, $(a, b)_p$ if $F = \mathbb{Q}_p$ and $(a, b)_\infty$ if $F = \mathbb{R}$. Classical examples of quaternion algebras are Hamilton's quaternion algebra, which is given by $(-1, -1)$ and $M_2(\mathbb{Q})$ the two by two matrices with rational coefficients.

Let B be a quaternion algebra over F and $\alpha = x+yi+zj+wk$ be an element of B. We define conjugation on B by $\bar{\alpha} = x - yi - zj - wk$. It is easy to check it is an involution and an anti-automorphism, i.e. $\overline{\alpha\beta} = \bar{\beta}\bar{\alpha}$.

Although we define conjugation in terms of a basis chosen, it is a canonical anti-automorphism, i.e. it depends only on B and not on the particular choice of a and b used to define it.

The reduced norm on B is defined by $N(\alpha) = \alpha\bar{\alpha} = x^2 - ay^2 - bz^2 + abw^2$, and the reduced trace $Tr(\alpha) = \alpha + \bar{\alpha} = 2x$.

Given a quaternion algebra B over $\mathbb{Q}$, we denote $B_p := B \otimes_{\mathbb{Q}} \mathbb{Q}_p$ the corresponding algebra over $\mathbb{Q}_p$. To avoid separate statements, abusing notation we will denote $p = \infty$ the real case, and when we talk about primes, we will include the case $p = \infty$ unless explicitly stated. Over $\mathbb{Q}_p$ there are up to isomorphism only two quaternion algebras depending on whether the quadratic form norm represents zero or not. The corresponding quaternion algebras are $M(2, \mathbb{Q}_p)$ (the two by two matrices with coefficients in $\mathbb{Q}_p$) and a division algebra respectively. B is said to ramify at the prime p if B_p is a division algebra, and it splits at p if B_p is isomorphic to the matrix algebra $M(2, \mathbb{Q}_p)$. If B ramifies at infinity, we said that B is a definite quaternion algebra (and this is so if $a < 0$ and $b < 0$).

The way to determine if a prime is split or ramified is to consider the reduced norm, which is a quadratic form in four variables, and check weather it represents zero or not, and this question may be answer in terms of the Hilbert symbol.

Given a field F and $a, b \in F^\times$ the Hilbert symbol (a, b) is defined by:

$$(a,b) = \begin{cases} 1 & \text{if } z^2 - ax^2 - by^2 = 0 \text{ has a non-trivial solution in } F^3 \\ -1 & \text{otherwise} \end{cases}$$

The importance of the Hilbert symbol is that a prime p is ramified if and only if $(a,b)_p = -1$, where with $(a,b)_p$ we mean the Hilbert symbol over $\mathbb{Q}_p$ (see [Se], Corollary of theorem 7 page 38). The convenience of this characterization of ramified primes is that the Hilbert symbol is in practice easy to compute, and it satisfies the product formula.

Theorem 4.1.1. (Hilbert) *If $a, b \in \mathbb{Q}^\star$, then $(a,b)_p = 1$ for almost all primes p and $\prod_p (a,b)_p = 1$, where the product is over all primes including infinity.*

This is a classical result and there is a proof in [Se] page 23. For quaternion algebras this implies that the number of ramified primes is finite and even. Furthermore the even number of ramified primes determines B uniquely up to isomorphisms, and given any set consisting of an even number of primes , there exists a quaternion algebra over $\mathbb{Q}$ ramified exactly at those primes.

There is a nice exposition due to Martin Eichler where he proves by hand that the possible ramified primes are the ones that divide a or b in [Ei] Theorem 4, page 7.

From now on, let B be a quaternion algebra over $\mathbb{Q}$. A lattice on B is a free $\mathbb{Z}$-module of rank 4, and an order on B is a lattice which is also a subring containing the identity. An order is said to be maximal if it is not properly contained in any other order of B. If p is a ramified prime then there is a unique maximal order, given by $\mathcal{O}_p := \{x \in B_p | N(x) \in \mathbb{Z}_p\}$ (see [Ei] Theorem 4, page 21); if p is split, then all maximal orders are conjugate to each other by an element of $B^\times$ (see [Ei] Theorem 5, page 3). Given a lattice L on B we will note $L_p := L \otimes_{\mathbb{Z}} Z_p$ the corresponding lattice of B_p.

An important tool on proving things on quaternion algebras are the 'local-global' properties; for example an order $\mathcal{O}$ of B is maximal if and only if $\mathcal{O}_p$ is

maximal for all finite primes p (see [Ei] Theorem 3, page 19; furthermore Eichler proves that any order $\mathcal{O} = \mathbb{Q} \cap_p \mathcal{O}_p$).

Proposition 4.1.1. *Let B be the quaternion algebra over $\mathbb{Q}$ ramified precisely at $p_1, \ldots, p_n$ and ∞. Then an order $\mathcal{O}$ of B is maximal if and only if disc($\mathcal{O}$)= $(p_1 \ldots p_n)^2$, where the discriminant is taken with respect to the reduced norm of B.*

Proof. See [Pi] Proposition 1.1, page 344 □

Given a lattice L on B, it has a left (respectively right) order associated to it, defined by $O_l(L) := \{\alpha \in B | \alpha L \subset L\}$ (respectively $O_r(L) := \{\alpha \in B | L\alpha \subset L\}$).

Given a lattice L, we can define an inverse $L^{-1} := \{\alpha \in B | L\alpha L \subset L\}$ and it turns out that $O_l(L^{-1}) = O_r(L)$, $O_r(L^{-1}) = O_l(L)$, and $LL^{-1} = O_l(L)$. The norm of a lattice $N(L)$ is defined to be the unique positive rational number such that the quotients $N(\alpha)/N(L)$ is integer for all $\alpha \in L$. We say that a lattice L is an ideal if it is locally principal, i.e. if for all primes q, $L_q = O_l(L)_q \alpha_q$ for some $\alpha_q \in B_q^\times$.

Proposition 4.1.2. *Let B be the quaternion algebra over $\mathbb{Q}$ as in Proposition 4.1.1, and let L be an ideal in B. Then $O_l(L)$ is a maximal order if and only if disc(L)= $(p_1 \ldots p_n)^2 N(L)^4$*

Proof. By definition disc(L) is the determinant of the bilinear associated to L on any basis. Since L is locally principal at all primes, given a finite prime q, $L_q = O_l(L)_q \alpha_q$. Clearly $\mathrm{disc}(L_q) = N(\alpha_q)^4 \,\mathrm{disc}(O_q)$ and the statement follows from proposition 4.1.1 and the fact that the norm of L is the product over all primes q of $q^{v_q(N\alpha_q)}$ where $v_q(n)$ is the q-valuation. □

The general theory of ideals turns out to be complicated in the general case, so we will restrict our attention to the two cases we will need (see [Pi] for the theory of ideals with square free level, and [Vig] or [Ei] for the general theory of locally principal ideals).

From now on B will denote a quaternion algebra over $\mathbb{Q}$ ramified at a prime p and at infinity. Given any order R we will call a left R-ideal to a lattice L such that its left order is R.

Maximal order

We will review the theory for ideals I such that its left order is maximal. We fix a maximal order once and for all and denote it O. It is easy to see that if I is a left O-ideal, then its right order is also maximal.

Proposition 4.1.3. *Let I be a lattice such that $O_l(I) = O$. Then I is an ideal (i.e. I is locally principal).*

Proof. see [Vig] page 86. □

By scaling the ideal I, we may always assume that the ideal is contained in its left order (and hence in its right order as well), in which case the norm of the ideal is an integer.

Proposition 4.1.4. *If I is a left O-ideal then $I^{-1} = \bar{I}/N(I)$ where bar denotes conjugation.*

Proof. This is just an easy local computation and is true for some more general orders, see [Pi] proposition 1.17. □

Given two left O-ideals I and J we define them to be equivalent if there exists $\beta \in B^\times$ such that $I = J\beta$. This defines an equivalence relation on left O-ideals, and the class number $h(O)$ is defined to be the number of distinct classes of such ideals. Furthermore I and J belongs to the same class if and only if there exists an element $\alpha \in \bar{J}I$ with $N\alpha = N(I)N(J)$.

The type number for maximal orders is defined to be the number of distinct isomorphism classes of maximal orders in B.

Proposition 4.1.5. *Let $I_1, \dots I_h$ be a complete set of representatives of all distinct left O-ideal classes. Let O_j be the right order of I_j for $j = 1, \dots, h$. Then*

$I_j^{-1}I_1, \ldots, I_j^{-1}I_h$ is a complete set of representatives of all the distinct left O_j-ideals classes. Furthermore the $\{O_j\}$ represent all the isomorphisms classes of maximal orders, and each one appears once or twice.

Proof. See Proposition 1.21, page 348 of [Pi] □

Note that this implies that the class number is finite, independent of the maximal ideal chosen and that the type number is smaller or equal than the class number.

Orders of level p^2

An order is said to have order p^2 if it has index p in a maximal order. We fix an order of level p^2 once and for all and denote it $\tilde{O}$.

Proposition 4.1.6. *Any maximal order contains a unique order of index p.*

Proof. see Lemma 1.4 [Pi2]. □

Then there are as many orders of level p^2 as maximal ones. An ideal I is called of level p^2 if its left order has level p^2. The equivalence relation between left $\tilde{O}$-ideals, the class number, and the type number are defined in an analogous way to the maximal case. There is an analogous of Proposition 4.1.5 coming from the fact that left $\tilde{O}$-ideals are in close relation with left O-ideals (see [Pa-Vi] for details).

To a lattice L, we can associate the quadratic form $Q_L : L \to \mathbb{Z}$ defined by $Q_L(x) = N(x)/N(L)$ (and the bilinear form which we will denote Q_L also by $Q_L(x, y) = Tr(x\bar{y})/N(L)$). We define the Theta function associated to L as the Theta function associated to Q_L, i.e. :

$$\Theta_L(z) := \sum_{\vec{x} \in L} \exp\left(2\pi i z N(\vec{x})/N(L)\right) \tag{4.1}$$

If L is a left O-ideal (respectively a left $\tilde{O}$-ideal) , the Theta function Θ_L turns out to be a modular form of weight 2 and level p (respectively of level p^2) with trivial

character (see [Ogg] Chapter VI for the theory of theta series and [Pi] Proposition 2.11 to compute the level of the quadratic forms).

Let $\{I_1, I_2, \ldots, I_h\}$ be a set of representatives of left O-ideals classes (respectively left $\tilde{O}$-ideals), $R_j := O_r(I_j)$ for $j = 1, \ldots, h$ be the right order of I_j and $e_j := |R_j^\times|$ for $j = 1, \ldots, h$ the number of units in R_j. For a non negative integer n define:

$$b_{ij}(n) := \frac{1}{e_j}|\{\alpha \in I_j^{-1} I_i : N(\alpha) = nN(I_i)/N(I_j)\}|$$

Note that $I_j^{-1} I_i$ is a left R_j-ideal, hence the number $b_{ij}(n)$ is the coefficient of the term with q^n in the q-expansion of the Theta series (4.1) associated to the ideal $I_j^{-1} I_i$ divided by the constant $1/e_j$.

For each non negative integer n we define an $h \times h$ matrix, called the Brandt matrix by $B(n) := (b_{ij}(n))$.Actually we should write $B(n; p)$ (respectively $B(n; p^2)$) since the definition depends of the level we are considering, but we will drop the level from the notation if it is clear which case we are considering.

Note that the definition of the Brandt matrices depends on choosing ideals representatives. Let $\mathcal{J} = \{J_1, \ldots, J_h\}$ be another set of left O-ideals representatives (respectively left $\tilde{O}$-ideals), and $B(n, \mathcal{J})$ the Brandt matrix associated to $\mathcal{J}$. Then there exist an $h \times h$ permutation matrix P such that $B(n, \mathcal{J}) = PB(n)P^{-1}$. Furthermore the Brandt matrix is independent of the maximal order O chosen (respectively the order $\tilde{O}$ of level p^2). For a proof of this facts, see [Pi2] Proposition 4.2 and Proposition 4.3.

From the Brandt matrices we form a Theta series

$$\Theta(z) = \sum_n B(n) \exp(2\pi i z n) \tag{4.2}$$

i.e. $\Theta(z)$ is a matrix such that the (i-th,j-th) coordinate is $\theta_{ij}(z) := 1/e_j \, \Theta_{I_j^{-1} I_i}(z)$ which is a modular form of weight 2 and level p (respectively p^2).

Proposition 4.1.7. *The Brandt matrices have the following properties:*

- $B(n)^t = \begin{pmatrix} \frac{e_1}{N(I_1)} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \frac{e_h}{N(I_h)} \end{pmatrix}^{-1} B(n) \begin{pmatrix} \frac{e_1}{N(I_1)} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \frac{e_h}{N(I_h)} \end{pmatrix}$

- $B(n_1)B(n_2) = B(n_1 n_2)$ *for* $(n_1, n_2) = 1$

- $B(q^\nu)B(q^\mu) = \sum_{k=0}^{min(\mu,\nu)} q^k B(q^{\nu+\mu-2k})$ *for* $q \neq p$

- $B(p^\nu)B(p^\mu) = B(p^{\nu+\mu})$

And they generate a semi-simple commutative ring.

Proof. See Theorem 2, page 32 of [Ei2].□

Proposition 4.1.8. *The action of the Hecke operators* $T_2(n)$ *with* $(n, p) = 1$ *on the* $\theta_{ij}(z)$ *is given by the Brandt matrices* $B(n)$*, i.e.,* $T_2(n)(\theta_{ij}(z))$ *is the* $(i\text{-}th, j\text{-}th)$ *entry of the matrix* $\sum_m B(n)B(m)\exp(2\pi imz)$*.*

Proof. See Proposition 2.23 of [Pi].

We will use the Brandt matrices to relate its eigenvector corresponding to the CM elliptic curve of level N^2 with the numbers $n_{[\mathcal{A}],[\mathcal{B}],\bar{\mathcal{D}}}$ in the case when the class number of $\mathbb{Q}(\sqrt{N})$ is 1. We will consider just this case since it is the only case when such elliptic curve is defined over $\mathbb{Q}$.

4.2 Some results on quaternion algebras

Given an order R and a left R-ideal I, we say that I is bilateral (or ambigue) if $O_r(I) = R$.

Proposition 4.2.1. *Given* O *a maximal order, there exists only one bilateral ideal* $\mathcal{P}$ *with the property* $\mathcal{P}^2 = |N|$*. Also all bilateral ideals form an abelian group, and each such ideal has the form* $\mathcal{P}^i m$ *where* i *is* 0 *or* 1*, and* m *is a rational number.*

Proof: see [Ei2] proposition 1, page 92. □

Lemma 4.2.1. *Let O be a maximal order, $\{I_1, \ldots, I_h\}$ a set of left O-ideals representatives, and $\{R_1, \ldots, R_h\}$ be the right orders of $\{I_1, \ldots, I_h\}$ respectively. Then for a given $i = 1, \ldots, h$ the maximal order R_i appears twice on the list if and only if there is no embedding of $\mathbb{Z}[\sqrt{N}]$ into R_i.*

Proof. Let $\mathcal{P}$ be the bilateral O-ideal of norm $|N|$. For a given left O-ideal I_j, the ideal $\mathcal{P}I_j$ is another left O-ideal. Note that if $\mathcal{P}_j$ is the ideal of norm $|N|$ in R_j, then $I_j^{-1}\mathcal{P}I_j = \mathcal{P}_j$ by the uniqueness of such a bilateral ideal. Then the ideals I_j and $\mathcal{P}I_j$ are equivalent if and only if there exists $\beta \in R_j^{\times}$ such that $I_j\beta = \mathcal{P}I_j$. Multiplying on the left by I_j^{-1} we see that $R_j\beta = i_j^{-1}\mathcal{P}I_j = \mathcal{P}_j$ hence $\mathcal{P}_j$ is principal, and the element β has norm $|N|$.

To see that this is the only way in which a maximal order R appears twice in the list of right orders, suppose that I and J are two nonequivalent left O-ideals with same right order R. Then $I^{-1}J$ is a non-principal bilateral ideal for R. Let $\mathcal{P}_R$ be the ideal of norm $|N|$ in R, then by proposition 4.2.1, $\mathcal{P}_R$ is non-principal and J is equivalent to $\mathcal{P}I$. □

In (4.1) we saw how to associate a quadratic form to any lattice L. If L is a lattice in B, we can define a bilinear form associated to the lattice L_p over $\mathbb{Z}_p$ by $Q_{L_p}(x, y) = Tr(x\bar{y})/N(L)$ where x and y are elements in L_p and $N(L)$ is the reduced norm of L. Note that a change of basis of L_p corresponds to equivalence of quadratic forms over $\mathbb{Z}_p$.

Note that if we multiply a lattice L_p on the right by an element of $B_p^{\times}$ the quadratic form does not change. Also the quadratic form of $\overline{L_p}$ (the conjugate lattice) is the same as the one of L_p. Given two lattices L_p and J_p we define them to be in the "same class" if there are elements α and β in $B_p^{\times}$ such that $J_p = \alpha L_p \alpha^{-1}\beta$ or $J_p = \alpha\overline{L_p}\alpha^{-1}\beta$.

We define two quadratic forms to be "equivalent" if they are equivalent in the

traditional sense plus considering equivalent two forms that differ by a non-square element. For example, if r is a non-square modulo p we consider "equivalent" the forms with diagonals $(1, p, p, p^2)$ and (r, rp, rp, rp^2) although they are not equivalent over $\mathbb{Z}_p$.

Lemma 4.2.2. *Let L and J be two lattices in B. Then L_p and J_p have "equivalent" quadratic forms over $\mathbb{Z}_p$ if and only if they are in the "same class".*

Proof. If L_p and J_p have equivalent quadratic forms over $\mathbb{Z}_p$, then there is a matrix $M \in Sl_4(\mathbb{Z}_p)$ such that

$$M^t Q_{L_p} M = Q_{J_p} \tag{4.3}$$

If $x \in L_p$ then $Q_{L_p}(x) = \frac{N(x)}{N(L)}$ i.e. M is such that $\frac{N(Mx)}{N(L)} = \frac{N(x)}{N(J)}$. Let $\psi : B_p \to B_p$ be the linear transformation defined by the matrix M, and $\beta = \psi(1)$. Clearly $N(\beta) = \frac{N(L)}{N(J)}$. Define $\Psi(v) = \psi(v)\beta^{-1}$, then it is clear that Ψ is an isomorphism, $\Psi(1) = 1$ and Ψ is an isommetry, i.e. $N(\Psi(x)) = N(x)$ hence by lemma 6.1.2 there exists $\alpha \in B_p^\star$ such that $\Psi(v) = \alpha v \alpha^{-1}$ (or $\Psi(v) = \alpha \bar{v} \alpha^{-1}$). Therefore $J_p = \psi(L_p) = \alpha L_p \alpha^{-1} \beta$ (respectively $J_p = \alpha \overline{L_p} \alpha^{-1} \beta$).

If the two quadratic forms differ by a non-square r modulo p , say $Q_{L_p} = rQ_{J_p}$, since $N : B_p \to \mathbb{Z}_p$ is surjective, there is an element $u \in B_p$ such that $N(u) = r$. Let $(U)_q$ be the idéle defined by $U_q := \begin{cases} 1 & \text{if } q \neq p \\ u & \text{if } q = p \end{cases}$

Then the full rank lattice $I := L(U)_q$ has the same norm as L. Also I_p is in the same equivalence class as L_p and $Q_{I_p} = rQ_{L_p}$. Since I and J have "equivalent" quadratic forms ,I_p and J_p are in the same "equivalence class" hence L_p and J_p are in the same "equivalence class".

The other implication is trivial.□

Chapter 5

Constructing a non-ideal lattice

In the next chapter we will associate a lattice to a Siegel point, and prove that this lattice is actually an ideal for a maximal order. While trying to prove this we had to understand the idea of locally principal ideals and ways of checking this condition. At the same time an interesting question arise: how can we construct a lattice not locally principal for its left order? In this chapter we will construct one such a lattice, using the classification of quadratic forms. Also we will study some particular orders. We do not know at this time if this results are well known or not.

5.1 Classification of quadratic forms over $\mathbb{Z}_p$

Definition. *Let f be a quadratic form over a local field $\mathbb{Q}_p$. We say that f is integral if $f(x) = \sum_{i,j=1}^{n} f_{ij}x_ix_j$ with $f_{ij} = f_{ji} \in \mathbb{Z}_p$.*

Given an integral form, we say that it is primitive if $\max_{i,j} |f_{ij}| = 1$. In the case $p = 2$ we say that f is properly primitive if it is primitive and $\max_i |f_{ii}| = 1$. If f is primitive but not properly primitive, we say that f is improperly primitive.

Given an integral quadratic form f in n variables over $\mathbb{Z}_p$, we define its discriminant, $D(f)$ as the determinant of the bilinear form matrix in any basis of

$\mathbb{Z}_p^n$. Also we define the *reduced discriminant* as the square root of the discriminant. Given a lattice L in a quaternion algebra B we define its discriminant $D(L)$ as the determinant of the quadratic form Q_L.

Proposition 5.1.1. *Let $p \neq 2$ be a prime, and suppose that f and g are integral forms in n-variables over $\mathbb{Q}_p$ such that $D(f) = D(g)$ is a unit. Then f and g are $\mathbb{Z}_p$-equivalent.*

Proof. This is the Corollary of Theorem 3.1 of [Cas], page 116. □

Proposition 5.1.2. *For the prime $p = 2$, let f and g be two improperly primitive integral forms over $\mathbb{Z}_2$ and suppose that $D(f) = D(g)$ is a unit. Then f and g are $\mathbb{Z}_2$-equivalent.*

Proof. This is the Corollary of Lemma 4.1 of [Cas] page 119. □

We will state the classification theorem of quadratic forms in $\mathbb{Q}_p$ over $\mathbb{Z}_p$ and we will use it later to construct a not locally principal ideal.

Proposition 5.1.3. *Let $p \neq 2$ and let r be some fixed quadratic non-residue of p, that is $|r| = 1$ and $r \notin (\mathbb{Q}_p^\star)^2$. For $\epsilon = 0$ or 1 and for $m = 1, 2, \ldots$ let $h(y) = h(\epsilon, m, y)$ be the form*

$$h(\epsilon, m, y) = \begin{cases} y_1^2 + \cdots + y_{m-1}^2 + y_m^2 & \text{if } \epsilon = 0 \\ y_1 + \cdots + y_{m-1}^2 + r y_m^2 & \text{if } \epsilon = 1 \end{cases} \tag{5.1}$$

Then every non-singular $f(x) \in \mathbb{Q}_p(x)$ is $\mathbb{Z}_p$-equivalent to a form

$$g(x) = \sum_{j=1}^{J} p^{e(j)} h(\epsilon_j, m_j, y^{(j)})$$

for some J, some $e(j)$ with $e(1) < e(2) < \ldots < e(J)$ and some ϵ_j, m_j with $m_1 + \cdots + m_J = n$ and $x = (y^{(1)}, \ldots, y^{(J)})$.

Proof. This is Theorem 3.1 page 115 of [Cas]. □

5.2 Orders in quaternion algebras

Given a quaternion algebra B ramified at p and infinity, we are going to study orders of index p^r in a maximal one.

Given u a non-square of $\mathbb{Z}_p$, let $L := \mathbb{Q}_p(\sqrt{u})$. Then we can represent the quaternion algebra B_p as the subalgebra of the 2×2 matrix algebra over L given by:

$$B_p := \left\{ \begin{pmatrix} \alpha & \beta \\ p\beta^\sigma & \alpha^\sigma \end{pmatrix} \mid \alpha, \beta \in L \right\}$$

We denote by $[\alpha, \beta]$ the previous matrix. Let R_p be the ring of integers of L (i.e. $R_p := \mathbb{Z}_p + \mathbb{Z}_p\sqrt{u}$) and define $\mathfrak{D}_{2r+1} = \{[\alpha, p^r\beta] \in B_p | \, \alpha, \beta \in R_p\}$.

Definition. *An order O' of B_p is said to have level p^{2r+1} for $r = 0, 1, \ldots$ if O'_p is isomorphic over $\mathbb{Z}_p$ to $\mathfrak{D}_{2r+1}$*

Proposition 5.2.1. *An order O' in B has level p^{2r+1} for some r if and only if O' contains a subring isomorphic to R_p.*

Proof. See [Pi3] Proposition 2. □

Lemma 5.2.1. *Let O' be an order of discriminant p^{2k+2} in the quaternion algebra ramified at p and infinity. If $k \geq 2$ then there exists an order $\tilde{O}$ such that $O' \subset \tilde{O}$ with index p or p^2.*

Proof. We know that there exists a maximal order O such that $O' \subset O$ with index p^k. Using the Smith normal form, we can find basis of O and O' such that $O = \langle 1, v_1, v_2, v_3 \rangle$ and $O' = \langle 1, p^{r_1}v_1, p^{r_2}v_2, p^{r_3}v_3 \rangle$ where $r_1 + r_2 + r_3 = k$. Without loss of generality assume that $r_1 \geq r_2 \geq r_3$. We consider two different cases:

• If $r_1 > r_2 \geq r_3$ or $r_3 \geq 1$ then writing down the conditions for O to be an order it follows that the lattice $\tilde{O} = \langle 1, p^{r_1-1}v_1, p^{r_2}v_2, p^{r_3}v_3 \rangle$ is an order and clearly contains O' with index p.

• If $r_1 = r_2$ and $r_3 = 0$ then $O' = \langle 1, p^k v_1, p^k v_2, v_3 \rangle$. Let $\tilde{O} = \langle 1, p^{k-1} v_1, p^{k-1} v_2, v_3 \rangle$. It is easy to check that this is an order and O' has index p^2 in it. □

Note: this inclusion is sharp in the sense that in the algebra ramified at 7 and infinity, the order $O' = \langle 1, i, -\frac{7}{2} + \frac{7}{2}j, -\frac{7}{2}i + \frac{7}{2}k \rangle$ has index p^2 in the maximal one (it is the order used in [Pi] of level p^3) but it is not contained in $\langle 1, \frac{1}{2} + \frac{1}{2}j, \frac{7}{2}i + \frac{7}{2}k, k \rangle$ which is the unique order of index p in the maximal one.

Lemma 5.2.2. *Let O' be an order of index p^2 in $\mathfrak{D}_{2r+1}$ for some r then O' is isomorphic to one of the followings:*

1. $O' = \langle [1,0], [\sqrt{u}, \alpha], [0, p^{r+1}], [0, p^{r+1}\sqrt{u}] \rangle$ *such that* $\alpha \notin p^{r+1} R_p$.
2. $O' = \langle [1,0], [p\sqrt{u}, 0], [0, p^r], [0, p^{r+1}\sqrt{u}] \rangle$
3. $O' = \langle [1,0], [p\sqrt{u}, \alpha], [0, p^r], [0, p^{r+1}\sqrt{u}] \rangle$ *such that* $\alpha \notin p^r \mathbb{Z}_p + p^{r+1} \mathbb{Z}_p \sqrt{u}$
4. $O' = \langle [1,0], [p^2\sqrt{u}, 0], [0, p^r], [0, p^r\sqrt{u}] \rangle$
5. $\mathfrak{D}_{2r+3}$

Proof. We embed R_p into B_p as $[R_p, 0]$. Let $T := R_p \cap O'_p$. We know that T is an order of index at most p^2 in R_p. It $T = R_p$ then by proposition 5.2.1 O' has level p^{2r+1}. If T has index p in R_p, then $T = \mathbb{Z}_p + p\mathbb{Z}_p\sqrt{u}$. Let $V := \{\beta \in R_p \,|\, [\alpha, \beta] \in O' \text{ for some } \alpha\}$. Clearly V is a T-module. Here we distinguish two cases:

• If $O' = T \oplus V$, since O' has index p^2 in $\mathfrak{D}_{2r+1}$ then V has index p in $p^r R_p$ and is a T-module hence $V = p^r T$ and we get case (2).

• If O' is not a direct sum there exists an element $[v_0\sqrt{u}, \alpha]$ in O' such that $p \nmid v_0$. Multiplying by v_0^{-1} we get that $[\sqrt{u}, \alpha] \in O'$ and we can find a basis for O' of the kind $O' = \langle [1,0], [\sqrt{u}, \alpha], [0, \beta], [0, \gamma] \rangle$. In this case $V = \langle \beta, \gamma \rangle$ is a T-module and has index p^2 in $p^r R_p$ hence $V = p^{r+1} R_p$ and we get case (1).

If T has index p^2 in R_p then $T = \mathbb{Z}_p + p^2\mathbb{Z}_p\sqrt{u}$. If we can write $O' = T \oplus V$ then we get case (4). The case $O' = \langle [1,0], [\sqrt{u}, \alpha], [0, p^r], [0, p^{r+2}\sqrt{u}] \rangle$ cannot happen since $\mathbb{Z}_p + p^2\mathbb{Z}_p\sqrt{u}$ is not an R_p-module. Then the only possibility is that if $[\alpha, \beta] \in O'$ then $\alpha \equiv u_0 p\sqrt{u} \bmod T$ (as additive groups) and we get case (3). $\square$

Proposition 5.2.2. *Let O' be an order of discriminant p^{2s} in the quaternion algebra ramified at p and infinity. Then O' has no index p orders over it if and only if O' has level p^{2r+1}.*

Proof. By lemma 5.2.1 it is clear that such an order has reduced discriminant p^{2r+1} for some $r \in \mathbb{Z}_{\geq 0}$. It is also clear that there are no orders between an order of level p^{2r+1} and an order of level p^{2r-1}, so we just need to check that if an order has no index p orders over it then it is isomorphic to $\mathfrak{D}_{2r+1}$. By lemma 5.2.1 it is enough to prove that an order $O' = \langle 1, p^r v_1, p^r v_2, v_3 \rangle$ with no index p orders over it is isomorphic to $\mathfrak{D}_{2r+1}$. We do this by induction on r. If $r = 0$ it is obvious since O' is maximal. So let O' have discriminant p^{2r+3} with no index p orders over it and let $\tilde{O}$ be the index p^2 order over it as on lemma 5.2.1. To check the "inductive hypothesis", assume that there is an order containing $\tilde{O}$ with index p, then we can write basis such that $O' = \langle 1, p^{r+1}v_1, p^{r+1}v_2, v_3 \rangle \subset \tilde{O} = \langle 1, p^r v_1, p^r v_2, v_3 \rangle \subset \langle 1, p^{r-1}v_1, p^r v_2, v_3 \rangle$. But then clearly $\langle 1, p^r v_1, p^{r+1}v_2, v_3 \rangle$ is an order containing O' with index p.

Then by inductive hypothesis $\tilde{O}$ is isomorphic to $\mathfrak{D}_{2r+1}$. Then by lemma 5.2.2 we have five possibilities for the order O'. On the first four cases:

1. $\langle [1,0], [\sqrt{u}, \alpha], [0, p^{r+1}], [0, p^{r+1}\sqrt{u}] \rangle \subset \langle [1,0], [\sqrt{u}, \alpha], [0, p^r], [0, p^{r+1}\sqrt{u}] \rangle$.
2. $\langle [1,0], [p\sqrt{u}, 0], [0, p^r], [0, p^{r+1}\sqrt{u}] \rangle \subset \langle [1,0], [p\sqrt{u}, 0], [0, p^r], [0, p^r\sqrt{u}] \rangle$.
3. $\langle [1,0], [p\sqrt{u}, \alpha], [0, p^r], [0, p^{r+1}\sqrt{u}] \rangle \subset \langle [1,0], [p\sqrt{u}, \alpha], [0, p^r], [0, p^r\sqrt{u}] \rangle$.
4. $\langle [1,0], [p^2\sqrt{u}, 0], [0, p^r], [0, p^r\sqrt{u}] \rangle \subset \langle [1,0], [p\sqrt{u}, 0], [0, p^r], [0, p^r\sqrt{u}] \rangle$

each inclusion with index p (it is easy to check that the lattices are actually orders) hence O' is isomorphic to $\mathfrak{D}_{2r+3}$. $\square$

5.3 Locally Principal Ideals

Lemma 5.3.1. *If $u \in \mathfrak{D}_{2r+1}$ is such that $p^{2r+2} \mid N(u)$ then $p \mid u$.*

Proof. If $u = \begin{pmatrix} \alpha & p^r\beta \\ p^{r+1}\beta^\sigma & \alpha^\sigma \end{pmatrix}$ then $N(u) = N(\alpha) + p^{2r+1}N(\beta)$. It is clear that if $\alpha \in R_p$ is such that $p \mid N(\alpha)$ then $p \mid \alpha$, i.e. $\alpha = p\tilde{\alpha}$ for some $\tilde{\alpha} \in R_p$. By a recursive argument, since p^{2r+1} divides $N(\alpha)$, p^{r+1} divides α and p^{2r+2} divides $N(\alpha)$. Dividing by p^{2r+1} and looking modulo p we get that p also divides $N(\beta)$ hence β and u. $\square$

Lemma 5.3.2. *Let I be a full rank lattice such that its left order is $\mathfrak{D}_{2r+1}$ for some $r \geq 1$. Then $N(I) = N(\mathfrak{D}_{2r-1}I)$.*

Proof. We have to check that the q-valuation of both norms is the same for all primes q. For all primes $q \neq p$ the result follows from the fact that $(\mathfrak{D}_{2r-1})_q = (\mathfrak{D}_{2r+1})_q$. Without loss of generality we may assume that $I \subset \mathfrak{D}_{2r+1}$ and that the p-valuation of I is less or equal than $2r+1$ (otherwise by lemma 5.3.1 $I = p^s\tilde{I}$ with $\tilde{I} \subset \mathfrak{D}_{2r+1}$ and norm less or equal than $2r+1$). Let s be the p-valuation of $N(I)$. If $u \in \mathfrak{D}_{2r+1}$ has norm divisible by p^s then $u = \begin{pmatrix} p^{\lceil \frac{s}{2} \rceil}\alpha & p^r\beta \\ p^{r+1}\beta^\sigma & p^{\lceil \frac{s}{2} \rceil}\alpha^\sigma \end{pmatrix}$. If $v \in \mathfrak{D}_{2r-1}$ then $v = \begin{pmatrix} \gamma & p^{r-1}\delta \\ p^r\delta^\sigma & \gamma^\sigma \end{pmatrix}$ and $vu = [p^{\lceil \frac{s}{2} \rceil}(\alpha + p^{r+1-\lceil \frac{s}{2} \rceil}\beta^\sigma), p^{r-1}(p\alpha\beta + p^{\lceil \frac{s}{2} \rceil}\delta\alpha^\sigma)]$. Since $r \geq 1$, $N(uv)$ has p-valuation at least s. $\square$

Proposition 5.3.1. *Let I be a full rank lattice such that its left order is $\mathfrak{D}_{2r+1}$ for some r , then I is locally principal.*

Proof. Since $(\mathfrak{D}_{2r+1})_q$ is maximal for all $q \neq p$, it is enough to consider the ramified prime p. We go by induction on r.

If $r = 0$, $\mathfrak{D}_1$ is maximal, and this is a well known result (see [Vig] page 86).

Let I be a full rank lattice such that its left order is $\mathfrak{D}_{2r+3}$. For $v \in \mathbb{Z}_p$ we denote $\nu_p(v)$ its p-valuation. Let $L := \mathfrak{D}_{2r+1}I$. Since its left order contains $\mathfrak{D}_{2r+1}$, by proposition 5.2.1 $O_l(L) = \mathfrak{D}_{2t+1}$ for some $t \leq r$. Then by inductive hypothesis $\mathfrak{D}_{2r+1}I$ is locally principal. Let $\delta_p \in (\mathfrak{D}_{2r+1}I)_p$ such that $(\mathfrak{D}_{2r+1}I)_p = (\mathfrak{D}_{2t+1})_p\delta_p$.

Since $\mathbb{Q}_p$ is non-archimedian there exists $u_p \in I_p$ such that $\nu_p(N(I_p)) = \nu_p(N(u_p))$. Then by lemma 5.3.2, I and $\mathfrak{D}_{2t+1}I$ have the same norms which implies that $\nu_p(N(u_p)) = \nu_p(N(\delta_p))$. Since $(\mathfrak{D}_{2t+1})_p u_p \subset (\mathfrak{D}_{2t+1})_p\delta_p$ with same norm, they are equal. Then we have a chain of ideals $(\mathfrak{D}_{2r+3})_p u_p \subset (\mathfrak{D}_{2r+1})_p u_p \subset \ldots \subset (\mathfrak{D}_{2t+1})_p u_p$.

Since $(\mathfrak{D}_{2r+3})_p u_p \subset I_p \subset (\mathfrak{D}_{2t+1})_p u_p$, there exists $r \leq s \leq t$ such that $(\mathfrak{D}_{2s+3})_p u_p \subset I_p \subset (\mathfrak{D}_{2s+1})_p u_p$. If both containments are strict then $I_p u_p^{-1}$ would be a lattice between $(\mathfrak{D}_{2s+3})_p$ and $(\mathfrak{D}_{2s+1})_p$. The $p+1$ such lattices are:

- $\langle [1,0], [\sqrt{u},0], [0,p^s], [0,p^{s+1}\sqrt{u}]\rangle$
- $\langle [1,0], [\sqrt{u},0], [0,tp^s + p^s\sqrt{u}], [0,p^{s+1}]\rangle$ for $t = 0,1,\ldots,p-1$.

Clearly none of them has an embedding of R_p on its left order and since the left order of I_p is $\mathfrak{D}_{2r+3}$ we must have $I_p = (\mathfrak{D}_{2r+3})_p u_p$. □

Proposition 5.3.2. *Let I be a lattice in a quaternion algebra ramified at infinity. Then I is locally principal if and only if $D(I) = D(O_l(I))$.*

Proof. Let $R = O_l(I)$. If I is locally principal then for any prime q, $I_q = R_q\alpha_q$ and $\mathrm{Bil}(I_q) = N(\alpha_q)\,\mathrm{Bil}(R_q)$. Dividing by $N(I)$ we see that $\nu_q(N(\alpha_1)/N(I)) = 0$ hence $\nu_q(\mathrm{Det}(\mathrm{Bil}(I_q)/N(I))) = \nu_q(\mathrm{Bil}(R_q))$.

Assume that $D(I) = D(O)$, and let q be any prime. There exists an element $\alpha_q \in I_q$ such that $N(I_q) = N(\alpha_q)$. Clearly $R_q\alpha_q \subset I_q$ say with index q^r. Then it is easy to check that $\det(\mathrm{Bil}(I_q)) = \det(\mathrm{Bil}(R_q\alpha_q))q^{2r}$ (via the Smith normal form

for example). Since $N(I_q) = N(\alpha_q) = N(R_q\alpha_q)$, dividing by $N(I_q)$ we get that $D(I_q) = D(R_q)q^{2r}$ hence $r = 0$. $\square$

Note that this proposition gives a computational way to check if a lattice is locally principal.

We start by studying the quadratic forms with discriminant p^2 (with $p \equiv 3 \bmod 4$). By proposition 5.1.3 we have four different choices:

- $f_1(x) = x_1^2 + x_2^2 + x_3^2 + p^2x_4^2$
- $f_2(x) = x_1^2 + x_2^2 + rx_3^2 + rp^2x_4^2$
- $f_3(x) = x_1^2 + x_2^2 + px_3^2 + px_4^2$
- $f_4(x) = x_1^2 + rx_2^2 + px_3^2 + rpx_4^2$

Note that all quadratic forms coming from lattices are the restriction of the quadratic form norm in B, hence they have to be equivalent over $\mathbb{Q}_p$. A complete set of invariants for a quadratic form f over $\mathbb{Q}_p$ are $n(f)$, $d(f)$ and $c(f)$. Here $n(f)$ is the number of variables, $d(f)$ is the discriminant modulo squares and $c(f) := \prod_{i<j}(a_i, a_j)$ where $f(x) = a_1x_1^2 + \cdots + a_nx_n^2$ (see [Cas] Theorem 1.1 page 55).

The four quadratic forms f_i have the same discriminant (modulo squares) and same number of variables. The c invariants are:

- $c(f_1) = (1,1)^3(1,p^2)^3 = 1$.
- $c(f_2) = (1,1)(1,r)^2(1,rp^2)^2(r,rp^2) = (r,rp^2) = (r,r) = 1$.
- $c(f_3) = (1,1)(1,p)^4(p,p) = -1$.
- $c(f_4) = (1,r)(1,p)(1,rp)(r,p)(r,rp)(p,rp) = 1$.

We compute the quadratic symbols using the table:

$b\backslash a$	1	r	p	pr
1	1	1	1	1
r	1	1	-1	-1
p	1	-1	-1	1
pr	1	-1	1	-1

(5.2)

Where the numbers in the i-th column and j-th row correspond to the Hilbert symbol (i, j). See [Cas] page 43 for details of how to compute it.

Since the maximal order corresponds to $f_3(x)$ we have:

Proposition 5.3.3. *All ideals with discriminant p^2 are locally principal*

Note that in this case equivalence modulo $\mathbb{Z}_p$ is the same as equivalence modulo $\mathbb{Q}_p$ for quadratic forms coming from lattices in B.

Then we should study the lattices with discriminant p^4 to find a not locally principal ideal. In this case we have thirteen non-equivalent quadratic forms over $\mathbb{Z}_p$:

- $f_1(x) = x_1^2 + px_2^2 + px_3^2 + p^2x_4^2$
- $f_2(x) = rx_1^2 + px_2^2 + rpx_3^2 + p^2x_4^2$
- $f_3(x) = rx_1^2 + px_2^2 + px_3^2 + rp^2x_4^2$
- $f_4(x) = x_1^2 + px_2^2 + rpx_3^2 + rp^2x_4^2$
- $f_5(x) = x_1^2 + x_2^2 + p^2x_3^2 + p^2x_4^2$
- $f_6(x) = x_1^2 + rx_2^2 + p^2x_3^2 + rp^2x_4^2$
- $f_7(x) = px_1^2 + px_2^2 + px_3^2 + px_4^2$
- $f_8(x) = x_1^2 + x_2^2 + px_3^2 + p^3x_4^2$

- $f_9(x) = x_1^2 + x_2^2 + rpx_3^2 + rp^3x_4^2$
- $f_{10}(x) = x_1^2 + rx_2^2 + rpx_3^2 + p^3x_4^2$
- $f_{11}(x) = x_1^2 + rx_2^2 + px_3^2 + rp^3x_4^2$
- $f_{12}(x) = x_1^2 + x_2^2 + x_3^2 + p^4x_4^2$
- $f_{13}(x) = x_1^2 + x_2^2 + rx_3^2 + rp^4x_4^2$

The unique order of level p^2 under the maximal one corresponds to the first quadratic form. Computing the equivalent classes over $\mathbb{Q}_p$ (using table 5.2) we get just two equivalence classes:

- $c(f_1) = c(f_3) = c(f_8) = c(f_9) = -1$
- $c(f_2) = c(f_4) = c(f_5) = c(f_6) = c(f_7) = c(f_{10}) = c(f_{11}) = c(f_{12}) = c(f_{13}) = 1$

Note that the forms $f_1 = (1, p, p, p^2)$ and $f_3 = (r, p, p, rp^2) = (r, rp, rp, rp^2)$ differ by a non-square, hence they correspond to lattices in the same "equivalence class". The same is true with the forms $f_8 = (1, 1, p, p^3)$ and $f_9 = (1, 1, rp, rp^3)$ hence there are just two "equivalent classes" of lattices of discriminant p^4, the ones corresponding to the form f_1 and the ones corresponding to the form f_8.

Claim: lattices corresponding to f_8 are not locally principal.

Let O'_p be the unique order of discriminant p^4 in B_p (which has index p in the maximal order). If I is a full rank lattice corresponding to the quadratic form f_8 and locally principal, by Lemma 4.2.2 and proposition 5.3.2, I_p is "equivalent" to O'_p. Then the quadratic forms f_8 and f_1 would be "equivalent" over $\mathbb{Z}_p$, which is not the case.

Then we have two different lattices, the *principal ones* corresponding to the quadratic form f_1 and the *not principal ones* corresponding to the quadratic form f_8.

5.3.1 A not locally principal lattice

Let $p = 3$ and consider the quaternion algebra ramified at 3 and infinity given by $B = (-1, -3)$.

By a small search we find that the lattice:

$$I = \langle 1, i, \frac{1}{2} - \frac{3j}{2}, \frac{i}{2} - \frac{k}{2} \rangle$$

has norm 1 and discriminant 3^4. Its diagonalized quadratic form over $\mathbb{Z}_3$ is the vector $(2, 2, 2 * 3, 2 * 3^3)$ which is "equivalent" to f_8 in the previous notation (they differ by a non-square). Then I is not locally principal.

Its left order is given by:

$$O_l(I) = \langle 1, \frac{-1}{2} + \frac{3j}{2}, \frac{3i}{2} + \frac{3k}{2}, 3i \rangle$$

Since $D(O_l(I)) = 3^8$ we can double check by proposition 5.3.2 that I is not locally principal.

Chapter 6

Siegel Space and applications

In chapter 3 we defined the Siegel space with the main purpose of defining generalized Theta functions over it and write the value of $L(\psi, s)$ at $s = 1$ in terms of such Theta functions. In this chapter we will give different interpretations of the Siegel space and construct Siegel points associated to ideals in the quaternion algebra $B = (-1, N)$.

Definition. *A complex torus is a complex variety isomorphic to $\mathbb{C}^g/L$, where L is a full rank lattice on $\mathbb{C}^g$.*

A complex torus is a *projective variety* if it can be embedded into some projective space as an algebraic subvariety. In the case of genus 1, a complex torus is just an elliptic curves, and it is easy to see that all elliptic curves are algebraic varieties (an embedding into $\mathbb{P}^2$ can actually be written using Riemann-Roch). This fact is not true in higher genus, so we will recall criteria for a complex torus to be an algebraic variety.

Let Ω be a point in $\mathfrak{h}_g$. To Ω we associate the lattice $L_\Omega \subset \mathbb{C}^g$ by $L_\Omega := \mathbb{Z}^g + \Omega\mathbb{Z}^g$. As we saw in Lemma 2.1.1 the Theta function $\theta(\vec{z}, \Omega)$ is "quasi-periodic" for translation by L_Ω, i.e. periodic up to a single multiplication factor.

Fix $\Omega \in \mathfrak{h}_g$. An entire function $f(\vec{z})$ onto $\mathbb{C}^g$ is L_Ω-quasi periodic of weight l if:

- $f(\vec{z}+\vec{m}) = f(\vec{z})$,
- $f(\vec{z}+\Omega\vec{m}) = \exp(-\pi i l m^t \Omega m - 2\pi i l z^t m) f(\vec{z})$

for all $\vec{m} \in \mathbb{Z}^g$. Let R_l^Ω denote the vector space of such functions.

If $\{f_0, \ldots, f_n\}$ is a basis of R_l^Ω such that for every $\vec{a} \in \mathbb{C}^g$ there is an i_0 with $f_{i_0}(\vec{a}) \neq 0$, we can define an holomorphic map $\Psi : \mathbb{C}^g/L_\Omega \to \mathbb{P}^n$ by $\vec{z} \mapsto (f_0(\vec{z}), \ldots, f_n(\vec{z}))$. Then the problem of embedding a complex torus is equivalent to find enough functions in R_l^Ω for some l.

Following [Mu] we define a slight generalization of the theta functions, the so called theta functions with rational characteristic, by the formula:

$$\theta \begin{bmatrix} \vec{a} \\ \vec{b} \end{bmatrix} (\vec{z}, \Omega) = \exp(\pi i \vec{a}^t \Omega \vec{a} + 2\pi i \vec{a}^t (\vec{z} + \vec{b})) \theta(\vec{z} + \Omega\vec{a} + \vec{b}, \Omega)$$

where $\vec{a}, \vec{b} \in \mathbb{Q}^g$.

To the point Ω we can associate the "complex structure":

Define $\alpha_\Omega : \mathbb{R}^g \times \mathbb{R}^g \to \mathbb{C}^g$ by $(\vec{x}, \vec{y}) \mapsto \Omega\vec{x} + \vec{y}$. This gives an identification of $\mathbb{R}^g \times \mathbb{R}^g$ with $\mathbb{C}^g$.

Let A be the real skew-symmetric form of determinant 1 on $\mathbb{R}^{2g} \times \mathbb{R}^{2g}$ defined by the matrix $A := \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}$, and define the bi-multiplicative map $e : \mathbb{R}^{2g} \times \mathbb{R}^{2g} \to \mathbb{C}^\star$ by $e(\vec{x}, \vec{y}) := \exp(2\pi i A(\vec{x}, \vec{y}))$.

Let $L^\perp$ be the dual lattice of L with respect to e, i.e. $L^\perp := \{x \in \mathbb{Q}^{2g} : e(x, a) = 1 \, \forall a \in L\}$.

Let $L \subset \mathbb{Z}^{2g}$ be a sublattice with index s. By duality, $\mathbb{Z}^{2g} \subset L^\perp$ with index s also. Consider $\{(a_i, b_i)\} \in L^\perp$ for $i = 1, \ldots, s$ be coset representatives of $L^\perp/\mathbb{Z}^{2g}$, and define the map $\phi_L : \mathbb{C}^g/\alpha_\Omega(L) \to \mathbb{P}^{s-1}$ by $z \mapsto (\ldots, \theta \begin{bmatrix} a_i \\ b_i \end{bmatrix} (z, \Omega), \ldots)$.

Theorem 6.0.1. *(Lefschetz): Let $L \subset \mathbb{Z}^{2g}$ be a lattice of index s, and assume that $L \subset rL^\perp$ for some $r \in \mathbb{N}$. Then:*

1. *if $r \geq 2$ then ϕ_L is well defined on all of $\mathbb{C}^g/\alpha_\Omega(L)$.*

2. *if $r \geq 3$, then ϕ_L is an embedding and the image is an algebraic subvariety of $\mathbb{P}^{s-1}$, i.e. the complex torus $\mathbb{C}^g/\alpha_\Omega(L)$ is embedded as an algebraic subvariety of $\mathbb{P}^{s-1}$.*

3. *every complex torus that can be embedded in a projective space is isomorphic to $\mathbb{C}^g/\alpha_\Omega(L)$ for some $\Omega \in \mathfrak{h}_g$ and some L.*

Proof. See Theorem 1.3 page 128 of [Mu]. □

Lemma 6.0.3. *Let $A : \mathbb{R}^{2g} \times \mathbb{R}^{2g} \to \mathbb{R}$ be the skew-symmetric form given by the matrix $A := \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}$. Then the following data on $\mathbb{R}^{2g}$ are equivalent:*

1. *a complex structure $U : \mathbb{R}^{2g} \to \mathbb{R}^{2g}$ (i.e. a linear map with $U^2 = -I$) such that there exists a positive definite Hermitian H for this complex structure, and $A = \Im H$ (the imaginary part).*

2. *a homomorphism $i : \mathbb{Z}^{2g} \to V$, where V is a complex space, plus a positive definite Hermitian form H on V such that $\Im H(ix, iy) = A(x, y)$.*

3. *a g-dimensional complex subspace $P \subset \mathbb{C}^{2g}$ such that if we note $A_\mathbb{C}$ the complex linear extension of A, we have:*

   - *$A_\mathbb{C}(x, y) = 0$ for all $x, y \in P$*
   - *$iA_\mathbb{C}(x, \bar{x}) < 0$ for all $x \in P - \{0\}$.*

4. *a complex matrix Ω in $\mathfrak{h}_g$*

Note: we can rewrite condition (1) as:

- $A(Ux, Uy) = A(x, y)$ for all $x, y \in R^{2g}$ ($\mathbb{C}$-linearity)
- $A(Ux, x) > 0$ for all $x \in \mathbb{R}^{2g} - \{0\}$ (positive definite)

Proof. This statement is Lemma 4.1 of [Mu]. We will need the relations between the matrices A, U, H and Ω. For this purpose we will sketch the equivalence between the first and last conditions.

If U is a complex structure, the bilinear form $H(x,y) := A(Ux,y) + iA(x,y)$ is a positive definite Hermitian form with imaginary part A.

(3. $\Rightarrow$ 1.) Given $\Omega \in \mathfrak{h}_g$ we have $\Omega = \Re + i\Im$, where $\Re = \Re(\Omega)$ and $\Im = \Im(\Omega)$. Consider the matrix:

$$U := \begin{pmatrix} \Im^{-1}\Re & \Im^{-1} \\ -\Re\Im^{-1}\Re - \Im & -\Re\Im^{-1} \end{pmatrix}$$

It is easy to check that $U^2 = -I_{2g}$ and $U^t A U = A$. Since $\Im^{-1}$ is real, symmetric and positive definite, there exists a real matrix C such that $\Im^{-1} = C^t C$. From this it follows easily that $A(Ux,y)$ is positive definite. Then from Ω we know how to construct the matrices U and H.

(1. $\Rightarrow$ 3.) A complex structure U as in (1) is a linear map $U : \mathbb{R}^{2g} \to \mathbb{R}^{2g}$ such that $U^2 = -I_{2g}$. This induces an isomorphism between $\mathbb{R}^{2g}$ and $\mathbb{C}^g$ in the following way: we can extend U by $\mathbb{C}$-linearity to get an isomorphism $U_{\mathbb{C}} : \mathbb{C}^{2g} \to \mathbb{C}^{2g}$. Since $U_{\mathbb{C}}^2 = -I_{2g}$ the eigenvalues of $U_{\mathbb{C}}$ are $\pm i$, and since $U_{\mathbb{C}}$ is defined over the reals, it is easy to check that both eigenvalues appear with the same multiplicity. Let $\{v_1, \ldots, v_g\} \subset \mathbb{C}^{2g}$ be the eigenvectors with eigenvalue $-i$. Clearly:

$$U_{\mathbb{C}} v_j = (-i)v_j \text{ iff } U(\Re(v_j)) = \Im(v_j) \text{ and } U(\Im(v_j)) = -\Re(v_j)$$

Since $\mathbb{C}^{2g} = \langle v_1, \ldots, v_g \rangle \oplus \langle \bar{v_1}, \ldots, \bar{v_g} \rangle$ it is clear that $\{\Re(v_j), \Im(v_j)\}_{j=1}^g$ is a basis for $\mathbb{R}^{2g}$. Then if we define the isomorphism $I_U : \mathbb{R}^{2g} \to \mathbb{C}^g$ by $I_U(\Re v_j) = e_j$ and $I_U(\Im(v_j)) = ie_j$, it satisfies $I_U(U(x)) = iI_U(x)$.

Given the isomorphism $I_U : \mathbb{R}^{2g} \to \mathbb{C}^g$, we extend it by $\mathbb{C}$-linearity to get a $\mathbb{C}$-linear map $I_U : \mathbb{C}^{2g} \to \mathbb{C}^g$, and define P be the kernel of it. P is a subspace or $\mathbb{C}^{2g}$ of rank g, which can be written as $P = \{ix - Ux | x \in \mathbb{R}^{2g}\}$. Then P is

isomorphic to $\mathbb{C}^g$ via Π_1, the projection on the first g- coordinates. Let Π_2 denote the projection on the last g-coordinates, i.e. $\Pi_2(\vec{x}) = (x_{g+1}, \ldots, x_{2g})$. We define Ω as a linear function from $\mathbb{C}^g$ to $\mathbb{C}^g$ by $\Omega(\vec{x}) = -\Pi_2(\Pi_1^{-1}(\vec{x}))$, or in other words, Ω is such that $P = \{(\vec{x}, -(\Omega(\vec{x}))^t) | \vec{x} \in \mathbb{C}^g\}$. $\square$

Note that by definition $Sp_{2g}(\mathbb{Z})$ are the matrices S such that $S^t A S = A$. This corresponds to make a change of basis in the ambient space keeping the Hermitian form matrix unchanged. We should think the Siegel space not just as the space of positive definite Hermitian forms H but as pairs (V, H) such that the matrix of the imaginary part of H on the basis V is reduced.

Thinking the action of $Sp_{2g}(\mathbb{Z})$ on the Siegel space as a change of basis, it is clear how to define this action on the Hermitian form H and on U, which in matrix notation can be written as $S \star H = S^t H S$ and $S \star U = S^{-1} U S$.

We would like to generalize the definition of the Siegel space so as to become independent of basis. For that purpose, note that given a non-degenerate skew symmetric matrix A, there exists a basis W (which we will call a skew symmetric reduced basis) such that $(A)_W = \begin{pmatrix} O & I_g \\ -I_g & 0 \end{pmatrix}$, where by $(A)_W$ we mean the matrix of A on the basis W.

Definition. *Let V be a real vector space of even dimension $2n$. We call a triple (P, J, U) a Siegel point if:*

- *P is a positive definite real symmetric $2n \times 2n$ form (that will correspond to the real part of H).*
- *J is a real $2n \times 2n$ non-degenerate skew symmetric matrix (that will correspond to the imaginary part of H).*
- *$U \in \mathbb{R}^{2n \times 2n}$ is such that $U^2 = -I_{2g}$. (complex structure)*

With the relation:

$$-JU = U^t J = P \tag{6.1}$$

Via the matrix U we can put a complex structure on the vector space V. Let H be the bilinear form $H(x,y) := P(x,y) + iJ(x,y)$. The condition (6.1) implies that $H(ix,y) = iH(x,y)$. Since J is skew symmetric and P symmetric, it follows that $H(x,y) = \overline{H(y,x)}$. Then H defined in this way is a positive definite Hermitian form, and satisfies the condition of Lemma 6.0.3 hence gives a point in the Siegel space.

We will call a *quasi-morphism* of B to a map $\Phi : B \to B$ such that it is $\mathbb{R}$-linear (in the sense that $\Phi(x+y) = \Phi(x) + \Phi(y)$ and $\Phi(\lambda x) = \lambda\Phi(x)$ if $\lambda \in \mathbb{R}$, but not necessarily $\Phi(1) = 1$). Given γ a quasi-isomorphism of the vector space V, we define an action of γ on a Siegel point (P, J, U) as (P', J', U') where $P' = \gamma^t P \gamma$, $J' = \gamma^t J \gamma$ and $U' = \gamma^{-1} U \gamma$. If we choose a skew symmetric reduced base of V, i.e. a base where J is of the form $\begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$, and we restrict γ to an automorphism that preserves the matrix J, then $\gamma \in Sp_{2n}(\mathbb{Z})$ and the action of γ on the Siegel point Ω associated to (P, J, U) is the usual action of $Sp_{2n}(\mathbb{Z})$ on the Siegel space $\mathfrak{h}_n$.

6.1 Siegel Points from Quaternion algebras

Let N be a negative prime congruent to 1 modulo 4, and $B = (-1, N)$ the quaternion algebra ramified at N and infinity. Let O be a maximal order in B such that there exists an embedding (not necessarily optimal) of $\mathbb{Z} + \mathbb{Z}\sqrt{N}$ into O. Let $u \in O$ be the image of $\sqrt{N}$, i.e. $u^2 = N$ and $Tr(u) = 0$. To a left O-ideal I we associate a Siegel point (P, J, U) as follows:

- We take V the real vector space $V := B \otimes_{\mathbb{Q}} \mathbb{R}$.
- Define U acting on V as left multiplication by $\frac{u}{\sqrt{|N|}}$.
- We think of I as a full rank lattice in V.
- For $x, y \in I$ define $P(x,y) := \frac{1}{\sqrt{|N|}} Tr(x\bar{y})/N(I)$.
- For $x, y \in I$ define $J(x,y) := Tr(u^{-1}x\bar{y})/N(I)$.

Proposition 6.1.1. *The triple (P, J, U) defined as before is a Siegel point.*

Proof. We start checking the properties of the matrices P, J and U:

• Clearly P is real. Since $Tr(x\bar{y})$ is real, $Tr(x\bar{y}) = Tr(y\bar{x})$ which implies that $P(x, y)$ is symmetric. At last, $P(x, x) = \frac{1}{\sqrt{|N|}} N(x)/N(I)$ then P is positive definite.

• Clearly J is real. Since u is pure imaginary, u^{-1} is also. Then $J(x, x) = Tr(u^{-1}N(x))/N(I) = 0$.

Clearly $J(x, y)$ is non-degenerate, since for any non-zero $x \in V$, $J(x, u^{-1}x) \neq 0$. So we are led to prove that $J(x, y) = -J(y, x)$. We have the trace identity:

$$Tr(xy) = Tr(yx) \tag{6.2}$$

By definition, $N(I)J(y, x) = Tr(u^{-1}y\bar{x}) = Tr(x\bar{y}\bar{u}^{-1})$. Since u is pure imaginary, $\bar{u} = -u$. Then $Tr(x\bar{y}\bar{u}^{-1}) = -Tr(x\bar{y}u^{-1}) = -Tr(u^{-1}x\bar{y})$ by (6.2) and $J(y, x) = -J(x, y)$.

• Let $x \in V$, then $U^2(x) = U(\frac{u}{\sqrt{|N|}}x) = \frac{u^2}{|N|}x = -x$.

As for the relation, it is clear that $J(\frac{u}{\sqrt{|N|}}x, y) = P(x, y)$. Using (6.2) and that $\bar{u} = -u$, it is also clear that $J(x, \frac{u}{\sqrt{|N|}}y) = -P(x, y)$. □

Definition. *Given a lattice I in B we define its dual by $I^{\#} := \{b \in B : Tr(bI) \subset \mathbb{Z}\}$. Given an order R we define its different by $R^{\iota} := NR^{\#}$.*

Proposition 6.1.2. *If O is a maximal order, O^{ι} is a bilateral ideal for O of index N^2, and $\frac{1}{N}O \subset O^{\iota} \subset O$.*

Proof. See [Vig] Lemma 4.7, page 24.

Proposition 6.1.3. *If $x, y \in I$ then $J(x, y) \in \mathbb{Z}$. Also the matrix of J on the basis given by I has determinant* 1.

Proof. Since we are considering the reduced norm, if V is the matrix associated to multiplication (on the left or on the right) by v, then $N(v) = \sqrt{\det(V)}$. Let

$W(x,y) := Tr(x\bar{y})$ be the bilinear form of B. If we denote W the matrix of $W(x,y)$ on the basis given by I, $J = \frac{1}{N(I)}(U^{-1})^t W$. Then $\det(J) = N(I)^{-4}N(u)^{-2}\det(W)$. By definition $\det(W) = disc(I)$, which is an ideal for a maximal order, then by Proposition 4.1.2 $disc(I) = N^2N(I)^4$ and $\det(J) = 1$.

Since the trace is linear, $J(x,y) = Tr(u^{-1}x\frac{\bar{y}}{N(I)})$. By proposition 4.1.4, $I^{-1} = \bar{I}/N(I)$ and $II^{-1} = O$, hence $J(x,y) \in \mathbb{Z}$ for all $x, y \in I$ if and only if $Tr(u^{-1}v) \in \mathbb{Z}$ for all $v \in O$. By proposition 6.1.2 this is the same as $u^{-1} \in O^{\#}$. But $u^{-1} = -\frac{u}{N}$, and since $u \in O$ it follows that $\frac{u}{N} \in \frac{1}{N}O \subset O^{\#}$. $\square$

This gives a method for assigning to every left O-ideal a Siegel point. Note that choosing a skew symmetric reduced basis of I we get a Siegel point in the classical sense. We fixed a maximal order O with an embedding of $\mathbb{Z}[\sqrt{N}]$.

Proposition 6.1.4. *Let $u \in O$ with $N(u) = |N|$ and $Tr(u) = 0$, and denote by U the complex multiplication associated to u. If I, I' are two equivalent left O-ideals, then the Siegel points $(P,J,U)_I$ and $(P,J,U)_{I'}$ are equivalent.*

Proof. Since $I \sim I'$ there exists $\alpha \in B^{\times}$ such that $I = I'\alpha$. Let W denote the quasi-isomorphism of B given by $W(v) = v\alpha$. We claim that W is the quasi-isomorphism that makes the two Siegel points equivalent.
Clearly $W(I') = I$, then we need to check that $W^*P = P'$, $W^*J = J'$ and $W^*U = U$.

- If $x, y \in I$ by definition $W^*P(x,y) := P(W(x), W(y)) = P(x\alpha, y\alpha) = \frac{Tr(x\alpha\bar{\alpha}\bar{y})}{N(I)} = \frac{N\alpha}{N(I)}Tr(x\bar{y}) = P'(x,y)$.
- The equality $W^*J = J'$ follows from a similar argument.
- By definition U is given by multiplying on the left by $u/\sqrt{|N|}$ while W is given by multiplying on the right by α then clearly this maps commute with each other and $W^*U := W^{-1} \circ U \circ W = U$. $\square$

Lemma 6.1.1. *Let U be the complex multiplication associated to u and $\alpha \in B$ be such that $\alpha O\alpha^{-1} = O$. Let $I' := \alpha I\alpha^{-1}$ and $u' := \alpha u\alpha^{-1}$. Then $(P,J,U) \sim (P',J',U')$.*

Proof. Let $W : B \to B$ be the quasi-isomorphism defined by $W(x) = \alpha x \alpha^{-1}$. By hypothesis $W(R) = R$, $W(I) = I'$ and it is easily seen that $W^*P = P'$ and $W^*J = J'$.

As for the complex multiplication, if $x \in B$ then $W^{-1} \circ U \circ W(x) = W^{-1} \circ U(\alpha x \alpha^{-1}) = W^{-1}(u\alpha x \alpha^{-1})/\sqrt{|N|} = \alpha^{-1} u \alpha x/\sqrt{|N|} = U'(x)$. $\square$

This lemma suggest that while looking at equivalence classes of Siegel points we should consider not just elements u in O corresponding to $\sqrt{N}$ (i.e. $u^2 = N$ and $Tr(u) = 0$) but modulo conjugation by the normalizer of O. It is clear that $\mathcal{N}(O) = \{h \in B \,|\, Oh \text{ is bilateral}\}$. By proposition 4.2.1 and the fact that $u \in O$ with $N(u) = |N|$, we know that all bilateral ideals are principal, generated by $u^s m$ where $s = 0, 1$ and m is a rational number. In term of elements, the generator is well defined up to units in O then :

$$\mathcal{N}(O) = \{\zeta u^s m \,|\, s = 0 \text{ or } 1\,, m \in \mathbb{Q} \text{ and } \zeta \in O \text{ is a unit}\} \tag{6.3}$$

Corollary. *If I and I' are left O-ideals with the same right order then the Siegel points $(P, J, U)_I$ and $(P, J, U)_{I'}$ are equivalent.*

Proof. If I and I' are equivalent this follows from proposition 6.1.4. If I and I' are not equivalent, we know by proposition 4.2.1 that $O_r(I)$ has no embedding of $\mathbb{Z}[\sqrt{N}]$. Let u be the element in O giving the complex multiplication. Then uI has the same left and right order as I but they are not equivalent, hence $uI \sim I' \sim uIu^{-1}$. By proposition 6.1.1 the Siegel points $(P, J, U)_I$ and $(P, J, U')_{uI}$ are equivalent. Note that U' is given by $u^{-1}uu = u$. $\square$

This means that we should index the Siegel points not by the class number of ideals, but by the type number of maximal orders.

We still have equivalent Siegel points coming from conjugation by units of O and this are all the possibilities for $\mathcal{N}(O)$. For counting equivalent classes of Siegel points, fixed a maximal order O we have to count the number of embeddings of $\mathbb{Z}[\sqrt{N}]$ into O modulo conjugation by units of O.

Given a maximal ideal O, let $V := \{I_1, \ldots, I_h\}$ be a set of left O-ideal representatives and $T := \{R_1, \ldots, R_t\}$ the distinct right orders of the ideals in V, where we assume that $O_r(I_j) = R_j$. We index the Siegel points by pairs (ϕ, R_i) where ϕ is an embedding from $\mathbb{Z}[\sqrt{N}]$ to some R_j and R_i is an order in T. By this we mean the Siegel point obtained with the complex multiplication given by $\phi(\sqrt{N})$, and an ideal I with left order R_j and right order R_i.

If d is a negative discriminant we denote by $h(d)$ the class number of binary quadratic forms of discriminant d. Let $u(d) = 1$ unless $d = -3, -4$ when $u(d) = 3, 2$ respectively (half the number of units in the ring of integers of discriminant d). For $D > 0$ we define the Hurwitz's class number $H(D)$ by:

$$H(D) := \sum_{df^2 = -D} \frac{h(d)}{u(d)} \tag{6.4}$$

Given $D > 0$ let $L = \mathbb{Q}[\sqrt{-D}]$ and $\mathcal{O}$ its ring of integers. Define $H_N(D)$ be the modified invariant by:

$$H_N(D) = \begin{cases} 0 & \text{if } N \text{ splits in } \mathcal{O} \\ H(D) & \text{if } N \text{ is inert in } \mathcal{O} \\ \frac{1}{2}H(D) & \text{if } N \text{ is ramified in } \mathcal{O} \text{ but does not divide} \\ & \text{the conductor of } \mathcal{O} \\ H_N(D/N^2) & \text{if } N \text{ divides the conductor of } \mathcal{O} \end{cases} \tag{6.5}$$

Then the number of embeddings of $\mathcal{O}$ into R_i $(i = 1, \ldots, n)$ modulo conjugation by $R_i^\times/\{\pm 1\}$ is $H_N(D)$ (see [Gr2] the proof of Proposition 1.9, page 122).
In the case N a negative prime and $D = -4N$, we get :

$$H_N(4N) = \begin{cases} \frac{1}{2}h(4N) & \text{if } N \equiv 1 \bmod 4 \\ h(N) & \text{if } N \equiv 7 \bmod 8 \\ 2h(N) & \text{if } N \equiv 3 \bmod 8 \text{ and } N \geq 11 \end{cases} \tag{6.6}$$

Note that in the case $D = 4N$ an order R_i on T appears twice as a right order if and only if it has no embedding of $\mathcal{O}_{4N}$. In this case it does not contribute to the

sum, and hence the number of embeddings of $\mathbb{Z}[\sqrt{N}]$ into the t orders in T is also $H_N(4N)$. With this we proved:

Proposition 6.1.5. *The number of non-equivalent Siegel points constructed is at most $H_N(4N)t$.*

Proposition 6.1.6. *Let B be a quaternion algebra over a commutative field K, and let $B_0 := \{\beta \in B \,|\, Tr(\beta) = 0\}$. If $\psi : B_0 \to B_0$ is an isommetry of K-vector spaces then there exists an element $\beta \in B^\star$ such that $\sigma(x) = \beta x \beta^{-1}$ or $\sigma(x) = -\beta x \beta^{-1} = \beta \bar{x} \beta^{-1}$.*

Proof. See [Vig] Theorem 3.3, page 12 □

Lemma 6.1.2. *Let $\psi : B \to B$ be an isomorphism of $\mathbb{Q}$-vector spaces (respectively $\sigma : B_q \to B_q$ an isomorphism of $\mathbb{Q}_q$-vector spaces) such that $\sigma(1) = 1$ and σ is an isommetry. Then there exists an $\alpha \in B^\star$ (respectively $\alpha \in B_q^\star$) such that $\sigma(x) = \alpha x \alpha^{-1}$ or $\sigma(x) = \alpha \bar{x} \alpha^{-1}$.*

Proof. Since $\sigma(1) = 1$ and σ is a morphism, $\sigma(\mathbb{Q}) = \mathbb{Q}$. Denoting B_0 the trace zero elements, $\sigma(B_0) = B_0$ and $\sigma|_{B_0} : B_0 \to B_0$ is an isommetry. By proposition 6.1.6 we get two different cases:

1. $\sigma_{B_0}(x) = \alpha \bar{x} \alpha^{-1}$ for some $\alpha \in B^\star$. Then σ is the antiautomorphism given by $\sigma(x) = \alpha \bar{x} \alpha^{-1}$.

2. $\sigma_{B_0}(x) = \alpha x \alpha^{-1}$ for some $\alpha \in B^\star$. Then σ is an automorphism given by $\sigma(x) = \alpha x \alpha^{-1}$. □

Theorem 6.1.1. *The $H_N(4N)t$ Siegel points $\{(\phi, R_i)\}$ constructed above are non-equivalent.*

Proof. The proof breaks in two steps. First we will prove that for a fixed embedding of $\mathbb{Z}[\sqrt{N}]$ into R (say u is the image of $\sqrt{N}$), the t left R-ideals give non-equivalent

points (P, J, U) where U is multiplication by $u/\sqrt{|N|}$. Then we will prove that different embeddings give non-equivalent Siegel points.

Let I_1, I_2 two left R-ideals. Abusing notation we will denote P_i the symmetric form P_{I_i} and the same with J. Suppose there exists $W : V \to V$ a quasi-isomorphism making the Siegel points (P_1, J_1, U) and (P_2, J_2, U) equivalent. Let $\beta = W(1)$, σ be the map: $\sigma(v) = W(v)\beta^{-1}$ and V_0 the trace zero elements space. We claim that σ is an isommetry.

By hypothesis $W^*P_1 = P_2$ then evaluating at $(1, 1)$ we have

$$(W^*P_1)(1,1) = P_2(1,1) = \frac{2}{N(I_2)}$$

By definition, $(W^*P_1)(1,1) = \frac{Tr(W(1),\overline{W(1)})}{N(I_1)} = 2\frac{N(\beta)}{N(I_1)}$ hence

$$N(\beta) = \frac{N(I_1)}{N(I_2)} \tag{6.7}$$

Then $\|x\| = P(x,x)N(I)/2 = W^*(P'(x,x))N(I)/2 = \frac{\|W(x)\|}{N(I')}N(I) = \frac{\|W(x)\|}{\|\beta\|} = \|\sigma(x)\|$, i.e. σ is an isommetry. Since σ is an isommetry and $\sigma(1) = 1$, by lemma 6.1.2 we have two different cases:

1. $\sigma(x) = \alpha\bar{x}\alpha^{-1}$ for some $\alpha \in B^\times$, i.e. σ is an antiautomorphism and $W(x) = \alpha\bar{x}\alpha^{-1}\beta^{-1}$.

2. $\sigma(x) = \alpha x\alpha^{-1}$ for some $\alpha \in B^\times$ and $W(x) = \alpha x\alpha^{-1}\beta^{-1}$.

We know that W preserves the complex multiplication, i.e. $W^{-1} \circ U \circ W(x) = U(x)$. If we are in the first case, $W^{-1}(x) = \alpha^{-1}\bar{\beta}\bar{x}\alpha$. Then $W^*U(x) = W^{-1}(u\alpha\bar{x}\alpha^{-1}\beta^{-1}) = \alpha^{-1}\bar{\beta}\bar{\beta}^{-1}\bar{\alpha}^{-1}x\bar{\alpha}\bar{u}\alpha = x\alpha^{-1}\bar{u}\alpha$. It must be the case that $ux = x\alpha^{-1}\bar{u}\alpha$ for all $x \in B$ (which is the same as saying that $ux\alpha^{-1} = x\alpha^{-1}\bar{u}$) which would imply that $u \in \mathbb{Q}$ and is not the case. Then we are in the second case.

Since $W(I_1) = I_2$, $I_2 = \alpha I_1\alpha^{-1}\beta^{-1}$. In particular $\alpha R\alpha^{-1} = R$, i.e. $\alpha \in \mathcal{N}(R)$. Then I_1 and I_2 have the same right order and represent the same class between the t left R-ideals we started with.

Assume that there is a left R-ideal I and a left R'-ideal I' such that R and R' are non-conjugate maximal orders and the Siegel points (P, J, U) and (P', J', U') are equivalent. Then there exist a quasi-isomorphism $W : V \to V$ that sends one point to the other. Arguing as before we get the same two possible cases for W. In the first case, since $W^*U = U'$ we would get that $u'x\alpha^{-1} = x\alpha^{-1}\bar{u}$ for all $x \in V$. Taking $x = \alpha$ we would get that $u' = \bar{u}$ and it commutes with all elements of V, then it is rational which is not the case.
Then $W(x) = \alpha x \alpha^{-1}\beta^{-1}$ and $I' = \alpha I \alpha^{-1}\beta$. In particular the orders R and R' are conjugate which is a contradiction. □

6.2 Ideals associated to Siegel points

We want to find relations between the numbers $n_{[\mathcal{A}],[\mathcal{B}],\bar{\mathcal{D}}}$. For this purpose to each point $z_{\mathcal{A}\bar{\mathcal{D}}}Q_{\mathcal{B}}$ on the Siegel space $\mathfrak{h}_2$ we will assign a left O-ideal I in B (for some maximal order O) and an embedding of $\mathbb{Z}[\sqrt{N}]$ into O such that the Siegel point (P, J, U) is $z_{\mathcal{A}\bar{\mathcal{D}}}Q_{\mathcal{B}}$ in the right basis. This implies that there are at most $H_N(4N)t$ different values (up to a sign) for $n_{[\mathcal{A}],[\mathcal{B}],\bar{\mathcal{D}}}$.

Proposition 6.2.1. *Given a negative prime number N congruent to 1 modulo 4, let B be the quaternion algebra ramified at $|N|$ and ∞. Let D be a negative prime number such that $|D|$ splits in $\mathbb{Q}(\sqrt{N})$. Then there exists u and v in B such that:*

- $Tr(u\bar{v}) = 0$, $Tr(u) = 0$ *and* $Tr(v) = 0$
- $N(u) = |N|$
- $N(v) = |D|$
- *u and v are in a maximal order R of B*

Proof. Since $|N| \equiv 3 \bmod 4$, we can assume $B = (-1, N)$. Choosing $u = j$ it is clear that $Tr(u) = 0$ and $N(u) = |N|$, hence we are looking for v in B such that

$Tr(uv) = 0$ and $Tr(v) = 0$ and $N(v) = |D|$. This conditions forces v to have the form $v = xi+yk$ and we are looking for an integer solution of the quadratic equation:

$$x^2 + |N|y^2 - |D|z^2 = 0 \tag{6.8}$$

We can assume that the solution is primitive (i.e. $gcd(x, y, z) = 1$). If (x, y, z) is a solution, clearly $gcd(z, N) = 1 = gcd(x, N)$ and $gcd(x, D) = 1 = gcd(y, D)$.
To prove the existence of such a solution we use the Hasse-Minkowski principle. Clearly (6.8) has a non-zero solution over $\mathbb{R}$, so we need to prove the existence of local non-zero solutions for all primes. We consider the different cases:

- For a prime $p \neq N$ and $p \neq D$ the quadratic form clearly has a local solution (see [Se] corollary 2, page 6).

- For the prime $|N|$ by Hensel's Lemma it is enough to look for solutions of (6.8) modulo $|N|$:

  $$x^2 - |D|z^2 \equiv 0 \bmod |N| \text{ iff } \left(xz^{-1}\right)^2 \equiv |D| \bmod |N|$$

  This equation has solution if and only if $\left(\frac{|D|}{|N|}\right) = 1$. By quadratic reciprocity law and the fact that $|N| \equiv 3 \bmod 4$ this last condition is equivalent to ask that $|D|$ splits in $\mathbb{Q}(\sqrt{N})$ which is the case.

- For the prime $|D|$, looking at (6.8) modulo $|D|$:

  $$x^2 + |N|y^2 \equiv 0 \bmod |D| \text{ iff } N \equiv \left(xy^{-1}\right)^2 \bmod |D| \text{ iff } \left(\frac{N}{|D|}\right) = 1$$

  Which is the case since $|D|$ splits in $\mathbb{Q}(\sqrt{N})$.

Given u and v as before, consider the rank 4 lattice $R = \langle 1, u, v, uv\rangle$. It is easy to see that R is actually an order, hence contained in a maximal one. $\square$
Remark: if we define $R = \langle 1, \frac{1+j}{2}, v, \left(\frac{1+j}{2}\right) v\rangle$ it is easy to see that this is also an order. The advantage of this order is that it contains an embedding of the ring of integers of $\mathbb{Q}(\sqrt{N})$, but is not maximal.

Let $z_{\mathcal{A}\bar{\mathcal{D}}}Q_{\mathcal{B}} = (\frac{b_1+\sqrt{N}}{2a_1|D|}) \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$, $u = j$ and v as in proposition 6.2.1. Let $w_3 = \frac{-b+v}{2}$, $w_4 = a$ and define

$$I_z := \left\langle \left(\frac{b_1 - j}{2a_1|D|}\right)(2aw_3 + bw_4), \left(\frac{b_1 - j}{2a_1|D|}\right)(bw_3 + 2cw_4), w_3, w_4 \right\rangle \tag{6.9}$$

This definition makes sense for any pair of generators if the ideal $\mathcal{B}$. With the choice we made it is the same as:

$$I_z := \left\langle \left(\frac{b_1 - j}{2a_1|D|}\right)av, \left(\frac{b_1 - j}{2a_1|D|}\right)\left(\frac{|D| + bv}{2}\right), \frac{v-b}{2}, a \right\rangle \tag{6.10}$$

Proposition 6.2.2. *The element $\frac{1+j}{2}$ is in the left order of I_z.*

Proof. This is an easy but tedious computation, so we will write the product of $\frac{1+j}{2}$ with each element of the basis as a linear combination of the basis of I_z.

- $\left(\frac{1+j}{2}\right)a = ba_1\left(\frac{b_1-j}{2a_1|D|}\right)av - 2aa_1\left(\frac{b_1-j}{2a_1|D|}\right)\left(\frac{|D|+bv}{2}\right) + \left(\frac{b_1+1}{2}\right)a$. In the basis of I_z it is given by the coordinates $[ba_1, -2aa_1, 0, \frac{b_1+1}{2}]$ which clearly are integers.
- $\left(\frac{1+j}{2}\right)\left(\frac{v-b}{2}\right) = (-2a_1c)\left(\frac{b_1-j}{2a_1|D|}\right)av + ba_1\left(\frac{b_1-j}{2a_1|D|}\right)\left(\frac{|D|+bv}{2}\right) + \left(\frac{b_1+1}{2}\right)\left(\frac{v-b}{2}\right)$. This follows from the fact that $b^2 - 4ac = D$. In the basis of I_z it is given by the coordinates $[-2ca_1, ba_1, \frac{b_1+1}{2}, 0]$ which are integers. For the first two elements we will use that $\left(\frac{1+j}{2}\right)\left(\frac{b_1-j}{2a_1|D|}\right) = \left(\frac{(b_1-N)-(1-b_1)j}{4a_1|D|}\right)$. Then:
- $\left(\frac{1+j}{2}\right)\left(\frac{b_1-j}{2a_1|D|}\right)av = \left(\frac{1-b_1}{2}\right)\left(\frac{b_1-j}{2a_1|D|}\right)av + 2ac_1\left(\frac{v-b}{2}\right) + bc_1a$. This follows from the fact that $b_1^2 - 4a_1c_1|D| = N$. In the basis of I_z it is given by the coordinates $[\frac{1-b_1}{2}, 0, 2ac_1, bc_1]$ which are clearly integers.
- $\left(\frac{1+j}{2}\right)\left(\frac{b_1-j}{2a_1|D|}\right)\left(\frac{|D|+bv}{2}\right) = \left(\frac{1-b_1}{2}\right)\left(\frac{b_1-j}{2a_1|D|}\right)\left(\frac{|D|+bv}{2}\right) + bc_1\left(\frac{v-b}{2}\right) + 2cc_1a$. This follows from $b_1^2 - 4a_1c_1|D| = N$ and $b^2 - 4ac = D$. In the basis of I_z it is given by the coordinates $[0, \frac{1-b_1}{2}, bc_1, 2cc_1]$ which clearly are integers. □

Proposition 6.2.3. *The element a_1v is in the left order of I_z.*

Proof. Since $\mathcal{B}$ is an ideal, it is clear that $v\langle w_3, w_4\rangle \subset \langle w_3, w_4\rangle$. By the way we

choose v, it satisfies $vj = -jv$, then

$$(a_1 v)\left(\frac{b_1 - j}{2a_1|D|}\right) = \left(\frac{b_1 - j}{2a_1|D|}\right)(-a_1 v) + \frac{b_1}{|D|}v \tag{6.11}$$

For the part corresponding to the first two elements of I_z note that they can be written as $\left(\frac{b_1-j}{2a_1|D|}\right)v(a)$ and $\left(\frac{b_1-j}{2a_1|D|}\right)v\left(\frac{v-b}{2}\right)$. Since $\mathcal{B}$ is an ideal, $v\mathcal{B} \subset \mathcal{B}$ and the assertion follows from equation (6.11). $\square$

Corollary. *The order $R = \langle 1, \frac{1+j}{2}, a_1 v, \frac{1+j}{2}a_1 v\rangle$ is contained in the left order of I_z and has discriminant $(a_1^2 ND)^2$ or index $a_1^2|D|$ in a maximal order.*

Proof. It is clear that R is in the left order of I_z by the previous two propositions. It is also clear that it is an order. To compute its discriminant, note that the bilinear matrix associated to it is:

$$\begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & \frac{1-N}{2} & 0 & 0 \\ 0 & 0 & 2a_1^2|D| & a_1^2|D| \\ 0 & 0 & a_1^2|D| & a_1^2|D|\frac{1-N}{2} \end{pmatrix}$$

Then note that the index in a maximal order (which has discriminant N^2) is the square root of the discriminant. $\square$

Theorem 6.2.1. *Let U be the complex multiplication associated to $\frac{-j}{\sqrt{|N|}}$. Then the Siegel point (P, J, U) associated to the ideal I_z in the given basis is $z_{\mathcal{A}\bar{\mathcal{D}}}Q_{\mathcal{B}}$.*

Proof. By proposition 6.2.2 the element $-j$ is in the left order of I_z. On proving that the Siegel points are the same we need to prove that the given basis of I_z is simplectic, i.e. that the matrix $J(x, y)$ in the given basis is a multiple of the matrix $\begin{pmatrix} 0 & I_2 \\ -I_2 & 0 \end{pmatrix}$, and check that the matrix U associated to the point $z_{\mathcal{A}\bar{\mathcal{D}}}Q_{\mathcal{B}}$ is the same as the complex multiplication matrix on I_z.

By definition $J(x, y)$ is skewsymmetric so we have less conditions to check. For simplicity we denote $\{v_1, v_2, v_3, v_4\}$ the given basis of I_z, and note that $u^{-1} = \frac{j}{|N|}$.

Clearly $J(x,y)$ has zero in the diagonal, since $J(\frac{j}{|N|}v_i, v_i) = Tr(\frac{j}{|N|}N(v_i)) = 0$ for $i = 1, \ldots, 4$. The other entries of $J(x,y)$ on the basis I_z are given by:

• **(3,4)** $J(\frac{j}{|N|}v_3, v_4) = \frac{1}{|N|}Tr(jw_3\bar{w}_4) = 0$ since $Tr(j) = 0$ and $Tr(jv) = 0$.

• **(1,2)** $J(\frac{j}{|N|}v_1, v_2) = \frac{1}{|N|}N(\frac{b_1-j}{2a_1|D|})Tr(j(2aw_3 + bw_4)(b\bar{w}_3 + 2c\bar{w}_4))$.

Since we will prove that this number is zero, we restrict to the trace part which by the distributive law is: $Tr(j(2abN(w_3) + 4acw_3\bar{w}_4 + b^2w_4\bar{w}_3 + 2bdN(w_4)))$.

Clearly that the first and last terms are zero. The middle terms are also zero because of the previous case.

• **(1,3)** $J(\frac{j}{|N|}v_1, v_3) = \frac{1}{|N|}Tr((\frac{jb_1+|N|}{2a_1|D|})(2aw_3 + bw_4)\bar{w}_3)$.

The part corresponding to the term with jb_1 in the distributive is zero by the previous computation, so we just consider the other part to get:

$$J(\frac{j}{|N|}v_1, v_3) = \frac{1}{|N|}Tr(\frac{|N|}{2a_1|D|}(2aN(w_3)+bw_4\bar{w}_3)) = \frac{1}{2a_1|D|}(4aN(w_3)+bTr(w_4\bar{w}_3))$$

Note that:

$$N(w_3) = \frac{b^2 + |D|}{4} = ac \tag{6.12}$$

Then the $(1,3)$-th entry is $\frac{1}{2a_1|D|}(4a^2c - ab^2) = \frac{a}{2a_1}$

• **(1,4)** $J(\frac{j}{|N|}v_1, v_4) = \frac{1}{|N|}Tr((\frac{b_1j+|N|}{2a_1|D|})(2aw_3 + bw_4)\bar{w}_4)$.

As before, the part corresponding to b_1j in the distributive is zero, so we are left with: $\frac{1}{a_1|D|}(aTr(w_3\bar{w}_4) + bN(w_4))$.

By definition, $w_4 = a$ and $Tr(w_3) = -b$ then $aTr(w_3\bar{w}_4)+bN(w_4) = -ba^2+ba^2 = 0$.

• **(2,3)** $J(\frac{j}{|N|}v_2, v_3) = \frac{1}{|N|}Tr((\frac{b_1j+|N|}{2a_1|D|})(bw_3 + 2cw_4)\bar{w}_3)$.

In the distributive the terms with b_1j are zero, while the other terms are:

$\frac{1}{a_1|D|}(bN(w_3) + cTr(w_4\bar{w}_3)) = \frac{1}{a_1|D|}(bN(w_3) + cTr(w_4\bar{w}_3)) = \frac{1}{a_1|D|}(bac - cab) = 0$ using (6.12).

• **(2,4)** $J(\frac{j}{|N|}v_2, v_4) = \frac{1}{|N|}Tr((\frac{b_1j+|N|}{2a_1|D|})(bw_3 + 2cw_4)\bar{w}_4)$.

In the distributive the terms with b_1j are zero, while the other terms are:

$\frac{1}{2a_1|D|}Tr(bw_3\bar{w}_4 + 2cN(w_4)) = \frac{1}{2a_1|D|}(bTr(w_3\bar{w}_4) + 4cN(w_4)) = \frac{-ab^2+4a^2c}{2a_1|D|} = \frac{a}{2a_1}$.

We have to divide this matrix by the norm of I_z and end up with a skew-symmetric matrix of determinant one. This implies that $N(I_z) = \frac{a}{2a_1}$ and that I_z is a simplectic basis.

To prove that the Siegel point (U, I_z) point is the same as $z_{\mathcal{A}\bar{\mathcal{D}}}Q_{\mathcal{B}}$ it is enough to compute the matrix of complex multiplication on the basis I_z and compare it with the complex multiplication matrix of the point $z_{\mathcal{A}\bar{\mathcal{D}}}Q_{\mathcal{B}}$, which by lemma 6.1.4 is:

$$\frac{1}{\sqrt{|N|}}\begin{pmatrix} b_1 I_2 & 2a_1 Q_{\mathcal{B}}^{-1} \\ -2c_1 Q_{\mathcal{B}} & -b_1 I_2 \end{pmatrix} = \frac{1}{\sqrt{|N|}}\begin{pmatrix} b_1 & 0 & 4a_1 c & -2a_1 b \\ 0 & b_1 & -2a_1 b & 4aa_1 \\ -4ac_1 & -2bc_1 & -b_1 & 0 \\ -2bc_1 & -4ac_1 & 0 & -b_1 \end{pmatrix}$$

This is a straight forward computation, so we will just compute $U_I(v_1)$ and $U_I(v_3)$ since the other ones are analogous. We drop the term $\frac{1}{\sqrt{|N|}}$ to make computations easier. By definition we have the equations:

$$b_1^2 - 4a_1 c_1 |D| = N \tag{6.13}$$

and:

$$b^2 - 4ac = D \tag{6.14}$$

• The vector v_1 case:

$U_I(v_1) = (-j)\left(\frac{b_1 - j}{2a_1|D|}\right)(2aw_3 + bw_4) = b_1(\frac{b_1 - j}{2a_1|D|})(2aw_3 + bw_4) - \frac{b_1^2}{2a_1|D|}(2aw_3 + bw_4) + \frac{N}{2a_1|D|}(2aw_3 + bw_4) = b_1 v_1 + \left(\frac{N - b_1^2}{2a_1|D|}\right)(2aw_3 + bw_4)$.

Using (6.13) to relate the second term, we get the equality:

$$U_I(v_1) = b_1 v_1 - 2c_1(2aw_3 + bw_4)$$

• The vector v_3 case:

$4a_1 cv_1 - 2a_1 bv_2 - b_1 w_3 = \left(\frac{b_1 - j}{2a_1|D|}\right)(8aa_1 cw_3 + 4a_1 bcw_4 - 2a_1 b^2 w_3 - 4a_1 bcw_4) - b_1 w_3 = \left(\frac{b_1 - j}{2a_1|D|}\right) 2a_1(4ac - b^2)w_3 - b_1 w_3 = -jw_3 = U_I(v_3)$.

Where the last equation comes from (6.14). □

Theorem 6.2.2. *The lattice I_z is an ideal for a maximal order.*

Proof. The strategy is to prove that the quadratic form associated to the ideal I_z is locally equivalent to the maximal order one for all primes different. We need the next lemma:

Lemma 6.2.1. *The quadratic form associated to the lattice I_z has discriminant N^2.*

Proof. The bilinear form is the same as the Siegel point $z_{\mathcal{A}\bar{\mathcal{D}}}Q_{\mathcal{B}}$ hence its bilinear form matrix is:

$$B_I = \begin{pmatrix} 2c_1 Q_{\mathcal{B}} & b_1 I_2 \\ b_1 I_2 & 2a_1 D Q_{\mathcal{B}}^{-1} \end{pmatrix} \tag{6.15}$$

Since $Q_{\mathcal{B}}$ has determinant D, it is an easy computation to prove that the determinant of this matrix is N^2 (using that $b_1^2 - 4a_1c_1|D| = N$). $\square$

For the negative prime N congruent to 1 modulo 4, the quaternion algebra $B = (-1, N)$ ramifies at $|N|$ and ∞. In this representation, a maximal ideal is given by $O = \langle \frac{1+j}{2}, \frac{i+k}{2}, j, k \rangle$ (see Proposition 5.2, page 369 of [Pi]), then the matrix of the quadratic form is:

$$B_O = \begin{pmatrix} \frac{|N|+1}{2} & 0 & |N| & 0 \\ 0 & \frac{|N|+1}{2} & 0 & |N| \\ |N| & 0 & 2|N| & 0 \\ 0 & |N| & 0 & 2|N| \end{pmatrix} \tag{6.16}$$

In particular it has discriminant N^2, and is an improperly primitive integral form. By Proposition 5.1.1 and 5.1.2 we know that the forms B_I and B_O are locally equivalent for all primes $p \neq |N|$. In particular by lemma 4.2.2 we know that $(I_z)_p$ is locally principal for all primes $p \neq |N|$.

As for the ramified prime $|N|$, by proposition 5.3.3 all ideals of discriminant p^2 are locally principal. Then I_z is locally principal and its left order has discriminant N^2 hence is maximal. $\square$

6.3 Comparing Siegel Points

In the previous section we saw one way to associate an ideal to a Siegel point. Note that if I is an ideal for a maximal order, and U a complex multiplication, the Siegel point associated to (U, I) is the same as the one associated to the point $(U, I\alpha)$ for any $\alpha \in B^\times$. Suppose two Siegel points z and z' have equivalent ideals I_z and $I_{z'}$, say $I_z = I_{z'}\alpha$ for some $\alpha \in B^\times$. Then since the complex multiplication is the same for all the ideals we construct, the two Siegel points are equivalent by proposition 6.1.4. The equivalence of the Siegel points is given by the matrix M in $Sp_4(\mathbb{Z})$ making the change of basis between the lattices I_z and $I_{z'}\alpha$.

Lemma 6.3.1. *.The matrix M of change of basis is in the subspace $\Gamma_{1,2}$.*

Proof. Let $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$. Then we know that the action of M sends the bilinear form associated to the ideal I_z to the bilinear form associated to the ideal $I_{z'}\alpha$, i.e. $M^t B_{I_z} M = B_{I_{z'}\alpha} = B_{I_{z'}}$. Let $z = \left(\frac{b_1+\sqrt{N}}{2a_1}\right) Q$ and $z' = \left(\frac{b_1'+\sqrt{N}}{2a_1'}\right) Q'$ where Q and Q' have even diagonal. Then we have:

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}^t \begin{pmatrix} 2c_2Q & b_2I_2 \\ b_2I_2 & 2a_2Q^{-1} \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} 2c_2'Q & b_2'I_2 \\ b_2'I_2 & 2a_2'Q'^{-1} \end{pmatrix} \tag{6.17}$$

By the way we choose generators, $b_i \equiv 1 \bmod 4$ $i = 1, 2$ (also $b_i' \equiv 1 \bmod 4$ $i = 1, 2$) hence $2Q \equiv \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix} \bmod 4$. Let $J := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Looking at the first 2×2 matrix of equation (6.17) modulo 4 we get:

$$2c_2A^tJA + C^tA + A^tC + 2a_2C^tJC \equiv 2J \bmod 4$$

Which means that 4 divides the diagonal of the left hand side. Note that if $A := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ then $A^tJA = \begin{pmatrix} 2ac & ad+bc \\ ad+bc & 2bd \end{pmatrix}$ hence 4 divides the diagonal of $2c_2A^tJA$ and $2a_2C^tJC$. Also A^tC is symmetric hence $A^tC + C^tA = 2A^tC$ and

we get that 2 divides the diagonal of A^tC. The proof for B^tD is analogous looking at the last 2×2 matrix. $\square$

Proposition 6.3.1. *Fixed the ideals $\mathcal{A}$ and $\mathcal{D}$, the left order of $I_{z_{\mathcal{A}\mathcal{D}}Q_{\mathcal{B}}}$ is independent of the ideal $\mathcal{B}$.*

Proof. The way we defined the ideal I_z was via embeddings $\phi : \mathbb{Q}(\sqrt{N}) \to B$ and $\psi : \mathbb{Q}(\sqrt{D}) \to B$ with a 'transversality condition':

$$Tr(\phi(\sqrt{N})\psi(\sqrt{D})) = 0$$

While defining I_z we just made a specific choice of such embeddings. If $\mathcal{B} = \langle v_1, v_2 \rangle$ (where in our notation $v_1 = \frac{b+\sqrt{D}}{2}$ and $v_2 = a$) then the ideal I_z was defined by:

$$I_z = \left\langle \phi\left(\frac{b_1 - \sqrt{N}}{2a_1|D|}\right)\psi(\sqrt{D})\psi(\bar{v_2}), \phi\left(\frac{b_1 - \sqrt{N}}{2a_1|D|}\right)\psi(\sqrt{D})\psi(\bar{v_1}), \psi(\bar{v_1}), \psi(\bar{v_2}) \right\rangle$$

We can also write it as $I_z = \left\langle \phi\left(\frac{b_1-\sqrt{N}}{2a_1|D|}\right)\psi(\sqrt{D})\psi(\bar{\mathcal{B}}), \psi(\bar{\mathcal{B}}) \right\rangle$. To see that the left order is independent of the ideal $\mathcal{B}$, we will prove that for every prime q the left order of $I_z \otimes \mathbb{Z}_q$ is independent of the ideal $\mathcal{B}$.
It is a well known result that the ideal $\mathcal{B}_q := \mathcal{B} \otimes \mathbb{Z}_q$ is principal, hence there exists an element $\delta_q \in L_q := \mathbb{Q}_q(\sqrt{D})$ such that $\mathcal{B}_q = \mathcal{O}_L\delta_q$. Then we can write $I_z = \left\langle \phi\left(\frac{b_1+\sqrt{N}}{2a_1|D|}\right)\psi(\sqrt{D})\psi(\mathcal{O}_L), \psi(\mathcal{O}_L) \right\rangle \bar{\delta}_q$ hence its left order is clearly independent of $\mathcal{B}$. $\square$

Proposition 6.3.2. *Let $\mathcal{D}$ and $\mathcal{D}'$ be two split prime ideals of $\mathbb{Q}[\sqrt{N}]$ of norms $|D|$ and $|D'|$ respectively such that $\mathcal{D}' = \mu\mathcal{D}$. Let $\mathcal{B}$ and $\mathcal{B}'$ be ideals of $\mathbb{Q}[\sqrt{D}]$ and of $\mathbb{Q}[\sqrt{D'}]$ respectively. Then the ideals $I_{z_{\mathcal{A}\mathcal{D}}Q_{\mathcal{B}}}$ and $I_{z_{\mathcal{A}\mathcal{D}'}Q_{\mathcal{B}'}}$ have the same left order if following the notation of proposition 6.2.1 we take $v' = \mu v$.*

Proof. We are abusing notation while stating this theorem, since μ is an element of $\mathbb{Q}[\sqrt{N}]$. We will denote indistinctly by μ the element in B or in $\mathbb{Q}[\sqrt{N}]$ via the identification $\sqrt{N} \mapsto j$, and the case will be clear from the context.

By proposition 6.3.1 it is enough to restrict to the case $\mathcal{B}$ and $\mathcal{B}$ principal. In this case we will prove that the ideals associated to them are slightly different and use this to prove the proposition. We can choose basis such that $\mathcal{D} = \langle |D|, \frac{b_1+\sqrt{N}}{2} \rangle$ and $\mathcal{D}' = \langle |D'|, \frac{b_1+\sqrt{N}}{2} \rangle$. If $\mu = \frac{\alpha}{|D|} + \frac{\beta}{|D|}\sqrt{N}$, since $\left(\frac{\alpha}{|D|} + \frac{\beta}{|D|}\sqrt{N}\right)\left(\frac{b_1+\sqrt{N}}{2}\right) \in \mathcal{D}'$ it follows that:

$$\frac{\alpha + \beta b_1}{|D|} \in \mathbb{Z} \tag{6.18}$$

The same argument with $\mu^{-1} = \frac{\alpha}{|D'|} - \frac{\beta}{|D'|}\sqrt{N}$ says:

$$\frac{\alpha - \beta b_1}{|D'|} \in \mathbb{Z} \tag{6.19}$$

For simplicity we will note the ideals $I_{\mathcal{D}}$ and $I_{\mathcal{D}'}$. Since $b = 1$ in both cases ($\mathcal{B}$ and $\mathcal{B}'$ are principal), we can rewrite the definition of the ideals as:

$$I_{\mathcal{D}} := \left\langle \left(\frac{b_1 - j}{2a_1|D|}\right) v, \left(\frac{b_1 - j}{2a_1|D|}\right)\left(\frac{v + |D|}{2}\right), \frac{v-1}{2}, 1 \right\rangle \tag{6.20}$$

and:

$$I_{\mathcal{D}'} := \left\langle \left(\frac{b_1 - j}{2a_1|D'|}\right) v', \left(\frac{b_1 - j}{2a_1|D'|}\right)\left(\frac{v' + |D'|}{2}\right), \frac{v'-1}{2}, 1 \right\rangle \tag{6.21}$$

where v and v' are the elements of norm $|D|$ and $|D'|$ respectively as in proposition 6.2.1. We will just compare $I_{\mathcal{D}'}$ with $I_{\mathcal{D}}$ and the other case follows from symmetry.

- $\frac{v'-1}{2}$ in terms of $I_{\mathcal{D}}$

Since j is the image of $\sqrt{N}$ in B and $\mu v = v'$,

$$\frac{v'-1}{2} = \left(\frac{\alpha + \beta j}{2|D|}\right) v - \frac{1}{2} = (-a_1\beta)\left(\frac{-j + b_1}{2a_1|D|}\right) v + \left(\frac{\beta b_1 + \alpha}{2|D|}\right) v - \frac{1}{2}$$

and by (6.18) $\frac{\beta b_1 + \alpha}{|D|} \in \mathbb{Z}$. As coordinates in the basis of I_z this is the same as $[-a_1\beta, 0, \frac{\alpha + b_1\beta}{|D|}, \frac{\alpha + b_1\beta + D}{2|D|}]$

- $\left(\frac{b_1 - j}{2a_1|D'|}\right) v'$ is in I_D. Since $\mu v = v'$, we get:

$$\left(\frac{b_1 - j}{2a_1|D'|}\right) v' = \frac{(-\beta b_1 + \alpha)}{|D'|}\left(\frac{b_1 - j}{2a_1|D|}\right) v + \beta\left(\frac{b_1^2 - N}{2a_1|D||D'|}\right) v$$

By (6.19) we know that $\frac{-\beta b_1+\alpha}{|D'|} \in \mathbb{Z}$. Since $b_1^2 - 4a_1|D||D'|c = N$ the last term can be written as $2\beta cv = 4\beta c\left(\frac{v-1}{2}\right) + 2\beta c$. As coordinates in the basis of I_z this is the same as $[\frac{\alpha-\beta b_1}{|D'|}, 0, 4\beta c, 2\beta c]$

• $\left(\frac{b_1-j}{2a_1|D'|}\right)\left(\frac{v'+|D'|}{2}\right)$ in terms of I_D.

Clearly $\left(\frac{b_1-j}{2a_1|D'|}\right)\left(\frac{v'+|D'|}{2}\right) = \left(\frac{b_1-j}{4a_1}\right) + \left(\frac{b_1-j}{2a_1|D'|}\right)\frac{v'}{2}$. Using the last case equality:

$$\left(\frac{b_1-j}{2a_1|D'|}\right)\left(\frac{v'+|D'|}{2}\right) = \left(\frac{b_1-j}{4a_1}\right)+\left(\frac{-\beta b_1+\alpha}{2|D'|}\right)\left(\frac{b_1-j}{2a_1|D|}\right)v+2\beta c\left(\frac{v-1}{2}\right)+\beta c$$

Note that $\alpha^2 + |N|\beta^2 \equiv |D||D'| \equiv 1 \bmod 4$. Since $|N| \equiv 3 \bmod 4$ it follows that α is odd and β is even. In particular $\alpha - \beta b_1 - 1$ is even, and we can rewrite the last equality as:

$$\left(\frac{\alpha-\beta b_1-|D'|}{2|D'|}\right)\left(\frac{b_1-j}{2a_1|D|}\right)v + \left(\frac{b_1-j}{2a_1|D|}\right)\left(\frac{v+|D|}{2}\right) + 2\beta c\left(\frac{v-1}{2}\right) + \beta c$$

So as coordinates in the basis of I_z it is the vector $[\frac{\alpha-\beta b_1-|D'|}{2|D'|}, 1, 2\beta c, \beta c]$.

We cannot say that the two ideals are the same, since the numbers α and β may have a 2 in the denominator, but $(I_{\mathcal{D}})_p = (I_{\mathcal{D}'})_p$ for all primes $p \neq 2$. In particular if we denote $O_{\mathcal{D}}$ and $O_{\mathcal{D}'}$ the left order of $I_{\mathcal{D}}$ and $I_{\mathcal{D}'}$ respectively, we get that $(O_D)_p = (O_{\mathcal{D}'})_p$ for all $p \neq 2$. Since the denominators are at most 2 it is easy to check that $4O_{\mathcal{D}} + \mathbb{Z} \subset O_{\mathcal{D}'}$, and has index at most 2^8. By corollary 6.2, the order $R \subset O_{\mathcal{D}'}$ with index $a_1^2|D|$, which is odd. Then $4O_D + R = O_{\mathcal{D}'}$. Also $4O_{\mathcal{D}} + R = O_{\mathcal{D}}$ hence both orders are the same. □

By theorem 3.2.3 we know that the numbers $n_{[\mathcal{A}],[\mathcal{B}],\bar{\mathcal{D}}}$ depend on the equivalence class of $\mathcal{A}$, the equivalence class of $\mathcal{D}$ and the class of $z_{\mathcal{A}\mathcal{D}}Q_{\mathcal{B}}$ modulo $Sp_4(\mathbb{Z})$. Fixed the class of $\mathcal{A}$ and the class of $\mathcal{D}$ we can associate ideals to the points $z_{\mathcal{A}\mathcal{D}}Q_{\mathcal{B}}$ such that they all have the same left order. Then we get at most $h(B)$ different points in the Siegel space.

Theorem 6.3.1. *The number of different $n_{[\mathcal{A}],[\mathcal{B}],\bar{\mathcal{D}}}$ in T is at most $h(\mathcal{O}_K)^2 t(B)$, where $t(B)$ is the type number.*

Proof. This follows from corollary of lemma 6.3.2. □

Note that this number is independent of the class number of $\mathcal{O}_L$.

Proposition 6.3.3. *Let $\mathcal{A}$ be an ideal of $\mathbb{Q}(\sqrt{N})$, then $n_{[\mathcal{A}],[\mathcal{B}],\bar{\mathcal{D}}}$ and $n_{[\mathcal{O}_K],[\mathcal{B}],\bar{\mathcal{D}}}$ differ by a unit in a quadratic extension of $\mathcal{M}$.*

Proof. Let $\sigma_{\mathcal{A}}$ be the automorphism of H corresponding to the ideal $\mathcal{A}$ via the Artin map. Then we proved that $\left(\frac{\theta(z_{\mathcal{O}_K\mathcal{D}}Q_{\mathcal{B}})}{\eta(\mathcal{D})\eta(\mathcal{O}_K)}\right)^{\sigma_A} = \frac{\theta(z_{\mathcal{A}\mathcal{D}}Q_{\mathcal{B}})}{\eta(\mathcal{A}\mathcal{D})\eta(\mathcal{A})}$. Hence $n_{[\mathcal{A}],[\mathcal{B}],\bar{\mathcal{D}}} = \left(\frac{\eta(\mathcal{A})\eta(\mathcal{A}\mathcal{D})}{\eta(\mathcal{D})\eta(\mathcal{O}_K)\psi_{\bar{\mathcal{D}}}(\mathcal{A})}\right)(n_{[\mathcal{O}_K],[\mathcal{B}],\bar{\mathcal{D}}})^{\sigma_{\mathcal{A}}}$. Note that the quotient of etas squared is in H while $\psi_{\bar{\mathcal{D}}}(\mathcal{A})$ is in T, hence $\zeta := \left(\frac{\eta(\mathcal{A})\eta(\mathcal{A}\mathcal{D})}{\eta(\mathcal{D})\eta(\mathcal{O}_K)\psi_{\bar{\mathcal{D}}}(\mathcal{A})}\right)$ is in a quadratic extension of $\mathcal{M}$. Clearly $N(\zeta) = 1$ as required. □

Chapter 7

The class number one case

In this section we will be interested in the case of imaginary quadratic fields of class number equal to one since in this case $n_{[\mathcal{A}],[\mathcal{B}],\bar{\mathcal{D}}}$ is a rational integers for any choice of $\mathcal{D}$. There are just six such cases (we exclude the case $N = -3$) so we can study all this cases by numerical computations.

7.1 Case $N = -7$

This case is the simplest one, since the class number in the quaternion algebra is also one. Then the numbers $n_{[\mathcal{A}],[\mathcal{B}],\bar{\mathcal{D}}}$ are integers and differ by a unit.

Theorem 7.1.1. *Let $N = -7$ and $\mathcal{D}$ be any ideal of prime norm congruent to 3 modulo 4. Then $L(1, \psi_{\mathcal{D}}) \neq 0$.*

Proof. By proposition 3.2.4 we know that the number associated to an ideal $\mathcal{B}$ is the same as the one associated to $\bar{\mathcal{B}}$. For a prime ideal $\mathcal{D}$ let $\Omega = \eta(\bar{\mathcal{D}})\eta(\mathcal{O}_K)\frac{2\pi}{w\sqrt{|D|}}$ where $-D = N(\mathcal{D})$ and w is the number of units in $\mathbb{Q}[\sqrt{D}]$. The formula 3.1 for $L(1, \psi)$ reads:

$$L(1,\psi) = \left(\sum_{[\mathcal{B}] \in Cl(\mathcal{O}_L)} n_{[\mathcal{O}_K],[\mathcal{B}],\bar{\mathcal{D}}} \right) \Omega = \left(n_{[\mathcal{O}_K],[\mathcal{O}_L],\bar{\mathcal{D}}} + 2\sum_{\Phi} n_{[\mathcal{O}_K],[\mathcal{B}],\bar{\mathcal{D}}} \right) \Omega \quad (7.1)$$

where the last sum is over non-principal ideals $\mathcal{B}$, with any choice of ideal representatives modulo conjugacy (since $|D|$ is prime, the class number of L is odd and we have such a representation).

Taking the maximal order O as left O-ideal representative, we see that the number associated to it is 1 up to a sign, then $\frac{L(1,\psi)}{\Omega} \equiv 1 \bmod 2$. $\square$

In the next table, we list some of the numbers $n_{[\mathcal{O}_K],[\mathcal{B}],\bar{\mathcal{D}}}$ to show the behavior of the sign.

D	$\mathcal{B}$	$n_{[\mathcal{A}],[\mathcal{B}],\bar{\mathcal{D}}}$
11	[1,-1,3]	1
23	[1, -1, 6]	1
23	[13, -17, 6]	-1
23	[13, 17, 6]	-1
43	[1, -1, 11]	-1
67	[1, -1, 17]	1
71	[1, -1, 18]	-1
71	[19, 9, 2]	-1
71	[19, -9, 2]	-1
71	[29, 33, 10]	1
71	[29, -33, 10]	1
71	[43, 141, 116]	-1
71	[43, -141, 116]	-1
79	[1, -1, 20]	-1
79	[11, -25, 16]	-1
79	[11, 25, 16]	-1
79	[19, 61, 50]	1
79	[19, -61, 50]	1

7.2 Case $N = -11$

In this case the quaternion algebra has type number 2 for maximal orders , so we get two different integers associated to different $\mathcal{D}$'s. Each number $n_{[\mathcal{O}_K],[\mathcal{B}],\bar{\mathcal{D}}}$ will be associated to an ideal class. Let $B = (-1, -11)$ be the quaternion algebra ramified at 11 and infinity. Consider the order:

$$O := \langle \frac{1}{2} + \frac{j}{2}, \frac{i}{2} + \frac{k}{2}, j, k \rangle$$

It is a maximal. We can take as left O-ideals representatives O and I_1, where

$$I_1 := \langle 1 - \frac{i}{2} + \frac{k}{2}, -2, \frac{1}{2} - i - \frac{j}{2}, \frac{1}{2} + i - \frac{j}{2} \rangle$$

Here is a table of $n_{[\mathcal{O}_K],[\mathcal{B}],\bar{\mathcal{D}}}$ for different values of D and $\mathcal{B}$, writing down the associated ideal also.

D	$\mathcal{B}$	$n_{[\mathcal{A}],[\mathcal{B}],\bar{\mathcal{D}}}$	Ideal
23	[1, -1, 6]	2	I_1
23	[13, -17, 6]	0	O
23	[13, 17, 6]	0	O
31	[1, -1, 8]	-2	I_1
31	[5, 17, 16]	0	O
31	[5, -17, 16]	0	O
47	[1, -1, 12]	0	O
47	[7, -17, 12]	2	I_1
47	[7, 17, 12]	2	I_1
47	[17, -53, 42]	0	O
47	[17, 53, 42]	0	O
59	[1, -1, 15]	2	I_1
59	[7, 9, 5]	0	O
59	[7, -9, 5]	0	O

D	$\mathcal{B}$	$n_{[\mathcal{A}],[\mathcal{B}],\bar{\mathcal{D}}}$	Ideal
67	[1, -1, 17]	2	I_1
71	[1, -1, 18]	-2	I_1
71	[19, 9, 2]	0	O
71	[19, -9, 2]	0	O
71	[29, 33, 10]	0	O
71	[29, -33, 10]	0	O
71	[43, 141, 116]	-2	I_1
71	[43, -141, 116]	-2	I_1

Note that the number 0 is associated to the principal ideal, while the number 2 is associated to I_1. With the same reasoning as in theorem 7.1.1 we can get a partial result proving that the ideals $\mathcal{D}$ such that $z_{\mathcal{D}}Q_{\mathcal{O}_L}$ is associated to the ideal I_1 have a non-vanishing L-series.

Following the method described in [Pa-Vi], taking $\{O, I_1\}$ as representatives for the maximal order and constructing the Brandt matrices for level 11^2 we get that the eigenvector associated to the modular form of weight 2 and level 11^2 is $[0, 0, 0, 1, -1, 0, 0, 0, 1, -1]$. The first three zeros correspond to the principal ideal, and the ± 1 to I_1. Then the numbers associated to each ideal are the same as the ones associated to them via $n_{[\mathcal{O}_K],[\mathcal{B}],\bar{\mathcal{D}}}$, since the eigenvector is well defined up to a constant.

7.3 Case $N = -19$

This case is similar to the previous one, since the class number for maximal orders in the quaternion algebra ramified at 19 and infinity is two. Again the values for $n_{[\mathcal{A}],[\mathcal{B}],\bar{\mathcal{D}}}$ are zero for the principal ideal and two for the non-principal one. Also the eigenvector corresponding to the modular form of weight 2 and level 19^2 has 0 in

the first five places (corresponding to the principal ideal), and alternating ± 1 in the next ten places (corresponding to the non-principal ideal).

7.4 Case $N = -43$

Let $B = (-1, -43)$ be the quaternion algebra ramified at 43 and infinity. In this case, the class number for maximal orders is 4 while the type number is 3. Consider the order:

$$O := \langle \frac{1}{2} + \frac{j}{2}, \frac{i}{2} + \frac{k}{2}, j, k \rangle$$

It is a maximal order. We can take as left O-ideals representatives $\{I_j\}_{j=1}^{4}$ where $I_1 = O$ and:

- $I_2 := \langle 2, 2i, \frac{1}{2} + i - \frac{j}{2}, 1 + \frac{i}{2} - \frac{k}{2}, \rangle$
- $I_3 := \langle 3, 3i, 1 + \frac{i}{2} - \frac{k}{2}, -1/2 + i + \frac{j}{2} \rangle$
- $I_4 := \langle 3, 3i, \frac{1}{2} + i - \frac{j}{2}, -1 + \frac{i}{2} - \frac{k}{2} \rangle$

In this case the ideals I_3 and I_4 have the same right order, then the integers associated to them have to be the same. The table for this case is:

D	$\mathcal{B}$	$n_{[\mathcal{A}],[\mathcal{B}],\bar{\mathcal{D}}}$	Ideal
11	[1, -1, 3]	-4	I_2
23	[1, -1, 6]	4	I_3
23	[13, -17, 6]	2	I_3
23	[13, 17, 6]	2	I_3
31	[1, -1, 8]	4	I_2
31	[5, 17, 16]	2	I_3
31	[5, -17, 16]	2	I_3

D	$\mathcal{B}$	$n_{[\mathcal{A}],[\mathcal{B}],\bar{\mathcal{D}}}$	Ideal
47	[1, -1, 12]	0	I_1
47	[7, -17, 12]	4	I_2
47	[7, 17, 12]	4	I_2
47	[17, -53, 42]	2	I_3
47	[17, 53, 42]	2	I_4
59	[1, -1, 15]	0	I_1
59	[7, 9, 5]	-2	I_3
59	[7, -9, 5]	-2	I_4
67	[1, -1, 17]	4	I_2
79	[1, -1, 20]	0	I_1
79	[11, -25, 16]	4	I_2
79	[11, 25, 16]	4	I_2
79	[19, 61, 50]	2	I_3
79	[19, -61, 50]	2	I_4
83	[1, -1, 21]	-4	I_2
83	[7, 1, 3]	-2	I_4
83	[7, -1, 3]	-2	I_4

Note that the eigenvector of the Brandt matrix for the modular form of weight 2 and level 43^2 has eigenvector $[0, 2, 1, 1]$ with respect to the ideals I_1, I_2, I_3, I_4, i.e. the ideals under I_1 have associated the number 0, the ones under I_2 the numbers ± 2 and so on.

7.5 Case $N = -67$

Let $B = (-1, -67)$ be the quaternion algebra ramified at 67 and infinity. In this case, the class number for maximal orders is 6 while the type number is 4. Consider

the order:

$$O := \langle 1, i, \frac{1}{2} + \frac{j}{2}, \frac{i}{2} + \frac{k}{2} \rangle$$

It is a maximal order. A set of representatives of left O-ideals is given by $\{I_j\}_{j=1}^{6}$ with $I_1 = O$ and:

- $I_2 := \langle 2, 2i, \frac{1}{2} + i + \frac{j}{2}, -1 + \frac{i}{2} + \frac{k}{2} \rangle$
- $I_3 := \langle 3, 3i, \frac{1}{2} + i + \frac{j}{2}, -1 + \frac{i}{2} + \frac{k}{2} \rangle$
- $I_4 := \langle 3, 3i, \frac{-1}{2} + i + \frac{j}{2}, -1 - \frac{i}{2} + \frac{k}{2} \rangle$
- $I_5 := \langle 4, 4i, \frac{3}{2} + i + \frac{j}{2}, -1 + \frac{3i}{2} + \frac{k}{2} \rangle$
- $I_6 := \langle 4, 4i, \frac{-3}{2} + i + \frac{j}{2}, -1 - \frac{3i}{2} + \frac{k}{2} \rangle$

In this case, the pair of ideals (I_3, I_4) and (I_5, I_6) have the same right orders, hence the integers associated to them will be the same. The table for $n_{[\mathcal{A}],[\mathcal{B}],\bar{\mathcal{D}}}$ for the first primes is:

D	$\mathcal{B}$	$n_{[\mathcal{A}],[\mathcal{B}],\bar{\mathcal{D}}}$	Ideal
19	[1, -1, 5]	6	I_2
23	[1, -1, 6]	6	I_2
23	[13, -17, 6]	4	I_5
23	[13, 17, 6]	4	I_5
47	[1, -1, 12]	6	I_2
47	[7, -17, 12]	4	I_6
47	[7, 17, 12]	4	I_5
47	[17, -53, 42]	2	I_4
47	[17, 53, 42]	2	I_4

D	$\mathcal{B}$	$n_{[\mathcal{A}],[\mathcal{B}],\bar{\mathcal{D}}}$	Ideal
59	[1, -1, 15]	-6	I_2
59	[7, 9, 5]	-2	I_3
59	[7, -9, 5]	-2	I_3
71	[1, -1, 18]	0	I_1
71	[19, 9, 2]	-6	I_2
71	[19, -9, 2]	-6	I_2
71	[29, 33, 10]	-2	I_3
71	[29, -33, 10]	-2	I_4
71	[43, 141, 116]	-4	I_5
71	[43, -141, 116]	-4	I_6
83	[1, -1, 21]	0	I_1
83	[7, 1, 3]	2	I_4
83	[7, -1, 3]	2	I_3

The eigenvector for the Brandt matrix associated to the modular form of weight 2 and level 67^2 is $[0, 3, 1, 1, -2, 2]$ with respect to the ideal representatives for the maximal order $\{I_j\}$.

7.6 Case $N = -163$

Let $B = (-1, -163)$ be the quaternion algebra ramified at 163 and infinity. In this case, the class number for maximal orders is 14 while the type number is 8. Consider the maximal order:

$$O := \langle 1, i, \frac{1}{2} + \frac{j}{2}, \frac{i}{2} + \frac{k}{2} \rangle$$

A set of representatives of left O-ideals is given by $\{I_j\}_{j=1}^{14}$ with $I_1 = O$ and:

- $I_2 := \langle 2, 2i, \frac{1}{2} + i + \frac{j}{2}, -1 + \frac{i}{2} + \frac{k}{2} \rangle$
- $I_3 := \langle 3, 3i, \frac{1}{2} + i + \frac{j}{2}, -1 + \frac{i}{2} + \frac{k}{2} \rangle$
- $I_4 := \langle 3, 3i, \frac{-1}{2} + i + \frac{j}{2}, -1 - \frac{i}{2} + \frac{k}{2} \rangle$
- $I_5 := \langle 6, 6i, \frac{1}{2} + i + \frac{j}{2}, -1 + \frac{i}{2} + \frac{k}{2} \rangle$
- $I_6 := \langle 6, 6i, \frac{-1}{2} + i + \frac{j}{2}, -1 - \frac{i}{2} + \frac{k}{2} \rangle$
- $I_7 := \langle 4, 4i, \frac{3}{2} + i + \frac{j}{2}, -1 + \frac{3i}{2} + \frac{k}{2} \rangle$
- $I_8 := \langle 4, 4i, \frac{-3}{2} + i + \frac{j}{2}, -1 - \frac{3i}{2} + \frac{k}{2} \rangle$
- $I_9 := \langle 6, 6i, \frac{5}{2} + i + \frac{j}{2}, -1 + \frac{5i}{2} + \frac{k}{2} \rangle$
- $I_{10} := \langle 6, 6i, \frac{-5}{2} + i + \frac{j}{2}, -1 - \frac{5i}{2} + \frac{k}{2} \rangle$
- $I_{11} := 5, 5i, \frac{1}{3} + 2i + \frac{j}{2}, -2 + \frac{i}{2} + \frac{k}{2} \rangle$
- $I_{12} := \langle 5, 5i, \frac{-1}{2} + 2i + \frac{j}{2}, -2 - \frac{i}{2} + \frac{k}{2} \rangle$
- $I_{13} := \langle 7, 7i, \frac{5}{2} + 3i + \frac{j}{2}, -3 + \frac{5i}{2} + \frac{k}{2} \rangle$
- $I_{14} := \langle 7, 7i, \frac{-5}{2} + 3i + \frac{j}{2}, -3 - \frac{i}{2} + \frac{k}{2} \rangle$

The pairs of ideals (I_{2j+1}, I_{2j+2}) with $j = 1, \ldots, 6$, have the same right order, hence each pair will have the same integer associated. For the table we consider the range of primes between 150 and 200 so as to get all the ideals $\{I_j\}$ associated to some number $n_{[\mathcal{O}_K],[\mathcal{B}],\bar{\mathcal{D}}}$. The table is:

D	$\mathcal{B}$	$n_{[\mathcal{A}],[\mathcal{B}],\bar{\mathcal{D}}}$	Ideal
151	[1, -1, 38]	20	I_2
151	[29, 9, 2]	14	I_8
151	[29, -9, 2]	14	I_8
151	[11, -5, 4]	8	I_{13}
151	[11, 5, 4]	8	I_{14}
151	[43, 137, 110]	4	I_{12}
151	[43, -137, 110]	4	I_{12}
167	[1, -1, 42]	0	I_1
167	[157, 33, 2]	-20	I_2
167	[157, -33, 2]	-20	I_2
167	[61, 65, 18]	-2	I_4
167	[61, -65, 18]	-2	I_3
167	[29, 93, 76]	-10	I_6
167	[29, -93, 76]	-10	I_5
167	[127, -177, 62]	-14	I_7
167	[127, 177, 62]	-14	I_8
167	[19, -21, 8]	-12	I_9
167	[19, 21, 8]	-12	I_{10}
179	[1, -1, 45]	0	I_1
179	[19, 45, 29]	2	I_3
179	[19, -45, 29]	2	I_4
179	[13, 17, 9]	4	I_{12}
179	[13, -17, 9]	4	I_{11}

D	$\mathcal{B}$	$n_{[\mathcal{A}],[\mathcal{B}],\bar{\mathcal{D}}}$	Ideal
199	[1, -1, 50]	0	I_1
199	[31, -69, 40]	-20	I_2
199	[31, 69, 40]	-20	I_2
199	[43, -133, 104]	-4	I_{12}
199	[43, 133, 104]	-4	I_{11}
199	[13, 29, 20]	-14	I_8
199	[13, -29, 20]	-14	I_7
199	[131, 453, 392]	-8	I_{14}
199	[131, -453, 392]	-8	I_{13}

The eigenvector for the Brandt matrices corresponding to the form of weight 2 and level 167^2 is given by the vector $[0, 10, 1, 1, 5, -5, 7, -7, -6, 6, 2, 2, -4, 4]$ with respect to the maximal order representatives $\{I_j\}$.

Since we consider all the class number 1 imaginary quadratic fields, the numerical information proves:

Theorem 7.6.1. *Let E be a CM elliptic curve over $\mathbb{Q}$ of level p^2. Then the coordinates of the eigenvector of the Brandt matrices associated to E are given up to a sign by $n_{[\mathcal{O}_K],[\mathcal{B}],\bar{\mathcal{D}}}$*

Bibliography

[Bu-Gr] Joe Buhler and Benedict Gross, *Arithmetic on elliptic curves with complex multiplication II* Inventiones mathematicae 79, 11-29 Springer-Verlag 1985

[Cas] J. W. S. Cassels, *Rational Quadratic Forms* Academic Press Inc. (London) LTD 1978

[Ei] Martin Eichler, *Lectures on modular correspondences* Bombay, Tata Institute of Fundamental Research, 1955-56

[Ei2] Martin Eichler, *The Basis Problem for Modular Forms and the Traces of the Hecke Operators* Lecture Notes in Mathematics 320, 75-151 Springer-Verlag 1973

[Gr] Benedict Gross, *Arithmetic on Elliptic Curves with Complex Multiplication* Lecture Notes in Mathematics vol. 776. Berlin Heidelberg New York: Springer 1980

[Gr2] Benedict Gross, *Heights and the Special Values of L-series* Conference Proceedings of the CMS Vol. 7, 115-187 AMS 1986

[Ha-Vi] Farshid Hajir and Fernando Rodriguez-Villegas, *Explicit elliptic units, I* Duke Mathematical Journal v. 90, No 3 Duke University Press 1997

[La] Serge Lang, *Algebraic number Theory* Graduate text in Mathematics. Springer-Verlag 1970

[Mu] David Mumford, *Tata Lectures on Theta I* Progress in Mathematics v. 28 Birkhäuser 1983

[Ogg] Andrew Ogg, *Modular Forms and Dirichlet Series* New York, W. A. Benjamin, 1969

[Pa-Vi] Ariel Pacetti and Fernando Rodrigeuz-Villegas *Computing weight 2 modular forms of level p^2* Submited to Math. Comp.

[Pi] Arnold Pizer, *An Algorithm for Computing Modular Forms on* $\Gamma_0(N)$ Journal of Algebra 64, 340-390 (1980)

[Pi2] Arnold Pizer, *Theta Series and Modular Forms of Level p^2M* Compositio Mathematica, Vol. 40, Fasc. 2 177-241, 1980

[Pi3] Arnold Pizer, *On the arithmetic of quaternion algebras II* J. Math. Soc. Japan 28, 676-688, 1976

[Se] Jean-Pierre Serre, *A course in Arithmetic*, Graduate text in mathematics. Berlin: Springer, 1973

[Sh] Goro Shimura, *On the Holomorphy of certain Dirichlet Series* Proceedings of the London Mathematical Society (3) 31 (1975) 79-98

[St] Harold Stark, *L-Functions at s=1. IV. First Derivatives at s=0* Advances in Mathematics 35, 197-235 (1980)

[Vig] Marie France Vigneras, *Arithmetique des Algebres de quaternions* Lecture Notes in Mathematics 800. Springer-Verlag 1980

[Vi] Fernando Rodriguez-Villegas, *On the square root of special values of certain L-series*, Inventiones Mathematicae 106, 549-573 Springer-Verlag 1991

[Wa] Lawrence Washington, *Introduction to Cyclotomic Fields* Graduate text in mathematics. Springer-Verlag 1982