Theta Inversion and the Law of Quadratic Reciprocity for Arbitrary Number Fields

By

Ryan Morrill

A thesis submitted in partial fulfillment of the requirements for the degree of

Master of Science

in

Mathematics

Department of Mathematical and Statistical Sciences

University of Alberta

Abstract

In this thesis, we formulate and prove the theorem of quadratic reciprocity for an arbitrary number field. We follow Hecke and base our argument on analytic techniques and especially on an identity of theta functions called theta inversion. From this inversion formula and a limiting argument, we obtain an identity of Gauss sums which is central to our proof of quadratic reciprocity. The statement of the law of quadratic reciprocity in this generality contains unevaluated Gauss sums which we will make explicit in the examples $\mathbb{Q}, \mathbb{Q}[i]$, and $\mathbb{Q}[\sqrt{2}]$.

Acknowledgements

I would like to thank my supervisor Manish Patnaik for his guidance. He has been an excellent mentor and I am very grateful for his efforts and for the funding he was able to obtain. His input and insight has been greatly appreciated.

I would also like to thank the department, particularly Andy Liu and Sean Graves, for their support.

Contents

1 Introduction

1.1 Motivation

1.1.1. The law of quadratic reciprocity is a deep and rich topic in number theory. Given a quadratic equation in modular arithmetic

$$x^2 \equiv a \mod b \quad a, b \in \mathbb{Z}, \tag{1.1}$$

the law of quadratic reciprocity allows us to determine its solvability using a very elegant formula first proved by Gauss [6]. If (1.1) is solvable in x then we say a is a quadratic residue modulo b. Otherwise we say a is a quadratic non-residue modulo b. We can define the Legendre symbol for p a prime number as follows,

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \not\equiv 0 \pmod{p} \text{ and } a \text{ is a quadratic residue mod } p, \\ -1 & \text{if } a \not\equiv 0 \pmod{p} \text{ and } a \text{ is a quadratic non-residue mod } p, \\ 0 & \text{if } a \equiv 0 \pmod{p}. \end{cases} \tag{1.2}$$

It is easy to see this symbol has the important property,

$$\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right). \tag{1.3}$$

The law of quadratic reciprocity is the more subtle set of relations,

Theorem. *Let p and q be distinct odd primes. Then,*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}, \tag{1.4}$$

and,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}. \tag{1.5}$$

Equations (1.4) and (1.5) allow us to compute Legendre symbols through successive reductions. For example,

$$\left(\frac{34}{47}\right) = \left(\frac{2}{47}\right)\left(\frac{17}{47}\right) = \left(\frac{17}{47}\right) = \left(\frac{47}{17}\right) = \left(\frac{13}{17}\right) = \left(\frac{17}{13}\right) = \left(\frac{4}{13}\right) = 1. \tag{1.6}$$

1.1.2. While there are various proofs for Theorem 1.1.1, we will focus on one which relies on analytic methods. Defining the theta function for $z \in \mathbb{C}$ with positive imaginary part as,

$$\theta(z) = \sum_{n=-\infty}^{\infty} e^{\pi i n^2 z}, \tag{1.7}$$

which converges absolutely. By looking at the Fourier expansion of (1.7) we obtain its functional equation,

$$\theta\left(-\frac{1}{z}\right)=\left(\frac{z}{i}\right)^{1/2}\theta(z). \tag{1.8}$$

By letting $z=p/q+i\varepsilon$ for $\varepsilon>0$ and p,q prime numbers and looking at the limit as ε goes to 0 of each side of (1.8), we obtain the following identity,

$$\frac{1}{\sqrt{q}}\sum_{r=1}^{q-1}e^{\frac{\pi ir^2p}{q}}=\frac{e^{\frac{\pi i}{4}}}{\sqrt{p}}\sum_{k=1}^{p-1}e^{\frac{-\pi ik^2q}{p}}. \tag{1.9}$$

Defining the quadratic Gauss sum,

$$G(p,q)=\sum_{r=1}^{q-1}e^{\frac{2\pi ir^2p}{q}} \tag{1.10}$$

one may observe that,

$$G(1,pq)=G(p,q)G(q,p) \tag{1.11}$$

and the connection to the Legendre symbol,

$$G(n,p)=\left(\frac{n}{p}\right)G(1,p)\quad\text{such that } p \text{ does not divide } n. \tag{1.12}$$

From (1.9) we obtain, for odd number m,

$$G(1,m)=i^{(m-1)^2}\sqrt{m}. \tag{1.13}$$

With (1.11), (1.12) and (1.13) one is able to prove (1.4) and (1.5).

1.1.3. While this is the story for $\mathbb{Z}$, a reasonable question to ask is how may this be generalized. A natural generalization from $\mathbb{Q}$ with ring of integers $\mathbb{Z}$, is to consider a finite extension of $\mathbb{Q}$. Such a finite extension is called a number field, which may be denoted as K with ring of integers denoted $\mathscr{O}_K$.

Hecke generalized this theorem for an arbitrary number field [1]. This generalization is not at all obvious and it contains unevaluated analogues to the Gauss sums defined in (1.10). There are various special cases which simplify the statement significantly, but in order to obtain a concise statement one has to look at a particular number field. Hecke proved the law of quadratic reciprocity by looking at a Fourier expansion of a modified theta function for which he obtained an analogue of the classical theta inversion relation (1.8). Looking at the limits of both sides of this theta inversion, produced an identity of Gauss sums, an analogue to (1.9). Finally, using properties of these Gauss sums, Hecke was able to prove the law quadratic reciprocity for an arbitrary number field.

1.2 This Thesis

In this thesis we will give an alternate but similar approach to Hecke's proof of the law of quadratic reciprocity. We will also provide some discussion on Hecke's theta function and how it is a special case of the Siegel-Jacobi theta function given by Mumford in [2]. Here we will provide two approaches to obtain Hecke's theta inversion. The first shows that theta inversion is really a consequence of viewing the Siegel-Jacobi theta function as a modular form. The second closely echoes Hecke's approach but we avoid directly taking the Fourier expansion of his theta function. Instead, our approach is motivated by Karlsson's proof of the law of quadratic reciprocity in $\mathbb{Q}$ where he took Fourier expansion of the heat kernel to obtain theta inversion [6]. In addition, some worked examples of the law of quadratic reciprocity for the fields $\mathbb{Q}$, $\mathbb{Q}[i]$ and $\mathbb{Q}[\sqrt{2}]$ will be included.

This thesis is divided into 6 chapters. Chapters 2 and 3 provide some background. Chapter 2 will provide some basic notation and background from linear algebra, whereas Chapter 3 focuses on algebraic number theory. It is in Chapter 3 where the different ideal and the notion of a dual ideal is introduced. As theta inversion relates a theta series over an ideal to a theta series over the dual of that ideal, the notion of a dual is critical.

In Chapter 4 we introduce an analogue Gauss sum to the Gauss sum in (1.10) and their important properties. In order to keep the discussion of Gauss sums in a single chapter, the main identity, i.e. the analogue to (1.9), of Gauss sums will be used here, but the proof is omitted until the end of Chapter 6. This chapter will prove the statement of the law of quadratic reciprocity, i.e. the analogue to (1.4), modulo the main identity on Gauss sums. As the general form of the law of quadratic reciprocity still involves unevaluated Gauss sums, we will provide three examples, one in the familiar field $\mathbb{Q}$, one for the complex field $\mathbb{Q}[i]$ and one for the totally real field $\mathbb{Q}[\sqrt{2}]$. In each case we will give a compact and practical formula for the law of quadratic reciprocity.

Chapter 5 introduces the analogue to (1.7), the general theta function. It will also introduce the functional equation of the Siegel-Jacobi theta function as a modular form which will be instrumental for obtaining theta inversion. This chapter will also give some small discussion on relating these functions to a heat kernel.

Chapter 6 is where we introduce Hecke's theta function and obtain its theta inversion. This is the analogue to (1.8) which will be used to prove the main identity of Gauss sums. We will show that Hecke's theta function is a special case of the Siegel-Jacobi theta function, then shows that theta inversion is obtained exactly from a special case of the functional equation. Using some limiting arguments, this chapter concludes by giving the proof of the main identity on Gauss sums that was used in Chapter 4.

2 Basic Notation and Preliminaries from Linear Algebra

In this section, we collect some basic notation which will be adopted throughout this thesis.

2.1 Basic notations

- We define the **Kronecker delta function**,

$$\delta_{pq} = \begin{cases} 1 & \text{if } p = q \\ 0 & \text{otherwise.} \end{cases} \tag{2.1}$$

- We define the **signum function**, $\mathsf{sgn} : \mathbb{R}/\{0\} \longrightarrow \{\pm\}$,

$$\mathsf{sgn}\,\alpha = \begin{cases} 1 & \text{if } \alpha > 0 \\ -1 & \text{if } \alpha < 0\,. \end{cases} \tag{2.2}$$

- For a complex number $z = x + iy$, where $i = \sqrt{-1}$, we denote its real part $\Re(z) = x$ and its imaginary part $\Im(z) = y$.
- Let $M_{n,m}(\mathbb{R})$ be the set of all $m \times n$ real matrices, and $M_{n,m}(\mathbb{C})$ be the set of all $m \times n$ complex matrices. For a complex matrix C, we may write $C = A + Bi$ where A, B are real matrices. In this case, we refer to $A = \Re(C)$ and $B = \Im(C)$.

2.2 Preliminaries from Linear Algebra

2.2.1. Recall we have a map

$$\det : M_{n\times n}(\mathbb{R}) \to \mathbb{R}\,. \tag{2.3}$$

Let A and B be $n \times n$ matrices, c a scalar, and 0 the $n \times n$ zero matrix. The determinant has the following properties,

(a) $\det(AB) = \det(A)\det(B)$

(b) $\det(A^\top) = \det(A)$

(c) $\det(cA) = c^n \det(A)$

(d) $\det\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} = \det(A)\det(B)$

2.2.2. Given a matrix A, its **transpose** can be defined as the matrix $A^\top$ whose entries are obtained by reflecting the entries of A by the main diagonal. We have,

(a) $(A^\top)^\top = A$

(b) $(AB)^{\top} = B^{\top}A^{\top}$

2.2.3. A matrix S is said to be **symmetric** if it is equal to its transpose, or equivalently if its entries are symmetric with respect to the main diagonal.

Remark. *Let S and A be square matrices such that S is symmetric. Then $A^{\top}SA$ is also symmetric.*

2.2.4. We say that a real $n \times n$ symmetric matrix M is **positive definite** if for any non-zero vector $x \in \mathbb{R}^n$, regarded as an $n \times 1$ matrix, we have

$$x^{\top}Mx > 0\,. \tag{2.4}$$

An example of a positive definite matrix is,

$$M = \begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{pmatrix} \tag{2.5}$$

as

$$\begin{pmatrix} x & y & z \end{pmatrix} M \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2x-y & -x+2y-z & -y+2z \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = x^2 + (x-y)^2 + (y-z)^2 + z^2 \tag{2.6}$$

which is a sum of squares, hence clearly non-negative and equal to zero if and only if $x = y = z = 0$.

2.2.5. The inverse to square matrix A is denoted A^{-1} and is defined as the matrix such that $AA^{-1} = I$ where I is the identity matrix. It has the important properties,

(a) $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}^{-1} = \begin{pmatrix} A^{-1} & 0 \\ 0 & B^{-1} \end{pmatrix}$

(b) for $a_1, \ldots, a_n \in \mathbb{C}$,

$$\begin{pmatrix} a_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & a_n \end{pmatrix}^{-1} = \begin{pmatrix} \frac{1}{a_1} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \frac{1}{a_n} \end{pmatrix}\,. \tag{2.7}$$

If a matrix has an inverse, we say it is **invertible**. The set of all $n \times n$ invertible matrices with real coefficients form a group under multiplication and we denote this group as $GL_n(\mathbb{R})$.

2.2.6. We define call a $2g \times 2g$ matrix M **symplectic** if it satisfies

$$M^{\top}JM = J \quad \text{where} \quad J = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}\,. \tag{2.8}$$

Let the set of all $2g \times 2g$ symplectic matrices with entries in $\mathbb{Z}$ be denoted $Sp(2g, \mathbb{Z})$.

Claim. *The set $Sp(2g,\mathbb{Z})$ forms a group under matrix multiplication.*

Proof. To see the set is closed under multiplication, let $M_1, M_2 \in Sp(2g,\mathbb{Z})$. Then,

$$(M_1 M_2)^\top J M_1 M_2 = M_2^\top M_1^\top J M_1 M_2 = M_2^\top J M_2 = J\,. \tag{2.9}$$

The inverse to any $M \in Sp(2g,\mathbb{Z})$ is

$$M^{-1} = J^{-1} M^\top J\,. \tag{2.10}$$

To see this is the inverse,

$$\big(J^{-1} M^\top J\big) M = J^{-1}\big(M^\top J M\big) = J^{-1} J = I\,. \tag{2.11}$$

To see this is in $Sp(2g,\mathbb{Z})$, note that $J^{-1} = J^\top$. Then,

$$\big(J^\top M^\top J\big)^\top J \big(J^\top M^\top J\big) = J M J^\top J J^\top M^\top J = J M J^\top M^\top J = J\big(M^\top J M\big)^\top J = J J^\top J = J\,. \tag{2.12}$$

□

3 Basic Notions of Algebraic Number Theory

Here we will review some basic background concerning algebraic number theory. We will define what an ideal is, and look at some of their important properties. We will also look at some important ideals such as the ring of integers, the different ideal, and the dual ideal. This subsection concludes by going through some simple examples.

3.1 Number fields and the ring of integers

3.1.1. We say a complex number is an **algebraic number** if it is a root of a polynomial with coefficients in $\mathbb{Q}$. We define an algebraic number field K to be a finite extension over $\mathbb{Q}$. Since K is a finite extension, then by the primitive element theorem [13, pg.595] there must exist some element θ such that $K = \mathbb{Q}(\theta)$, the smallest subfield of the complex numbers which contains $\mathbb{Q}$ and θ. Among all polynomials with rational coefficients with the algebraic number θ as a root there is a monic one of smallest degree, call it f_θ. The degree n of the polynomial is called the **degree of** K. Since $\mathbb{Q}$ is characteristic 0, f_θ has no repeated roots. We call the n distinct roots of f_θ the **conjugates** of θ, and write these roots with superscripts as $\theta^{(1)}, \ldots \theta^{(n)}$. Furthermore every element in $\mathbb{Q}(\theta)$=$\mathbb{Q}[X]/f_\theta$ can be written as a sum of powers in θ, such as $\alpha = c_0 + c_1\theta + c_2\theta^2 + \cdots + c_{n-1}\theta^{n-1}$.

Replacing θ by one of its n conjugates gives us the following automorphisms,

$$\sigma^{(p)} : \mathbb{Q}(\theta) \longrightarrow \mathbb{Q}(\theta)\,,\ \theta \longmapsto \theta^{(p)}\,, \quad \text{for } p = 1, \ldots, n \tag{3.1}$$

For α in $K = \mathbb{Q}(\theta)$ we define $\alpha^{(p)}$ for $p = 1, \ldots, n$ to be

$$\alpha^{(p)} = \sigma^{(p)}(\alpha)\,, \tag{3.2}$$

and we call these the conjugates of α. If $\theta^{(p)}$ is complex, then its complex conjugate $\overline{\theta^{(p)}}$ must be another root of f_θ, say $\theta^{(p')}$ for some $p' \in \{1, \ldots, n\}$. Further, if α is a complex number, its complex conjugate,

$$\begin{aligned} \overline{\alpha^{(p)}} &= \overline{c_0 + c_1\theta^{(p)} + \cdots + c_n\theta^{(p)n-1}} = c_0 + c_1\overline{\theta^{(p)}} + \cdots + c_{n-1}\overline{\theta^{(p)}}^{\,n-1} \\ &= c_0 + c_1\theta^{(p')} + \cdots + c_{n-1}{\theta^{(p')}}^{n-1} = \sigma^{(p')}(\alpha)\,. \end{aligned} \tag{3.3}$$

Therefore the complex conjugates of α always come in pairs. We further organize the n conjugates of α by defining r_1, r_2 non-negative integers with $r_1 + 2r_2 = n$ such that,

$$\begin{aligned} \alpha^{(p)}\,&\text{is real for}\, p = 1, \ldots, r_1 \\ \alpha^{(p+r_2)}\,&\text{is the complex conjugate to}\, \alpha^{(p)}\, \text{for}\, p = r_1 + 1, \ldots, r_1 + r_2\,. \end{aligned} \tag{3.4}$$

We call a number α in K **totally positive** if the numbers $\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(r_1)}$ are all positive, with r_1 as in (3.4). If $r_1 = 0$, then each number in K is said to be totally positive.

3.1.2. We say that an algebraic number is **integral** over a number field K if it is a root of some monic polynomial with coefficients in $\mathbb{Z}$. All such numbers form a ring [11, p.7], and we call this the **ring of integers**, denoted $\mathscr{O}_K$. We will henceforth refer to numbers which are integral over a number field K as integers, and elements of $\mathbb{Z}$ as rational integers.

Claim. *Any $\beta \in K$ can be written as $b\alpha$ where $b \in \mathbb{Q}$ and $\alpha \in \mathscr{O}_K$.*

Proof. If $\beta \in K$ then let $f_\beta(X) \in \mathbb{Q}[X]$ be the minimal degree monic polynomial with β as a root. Let m be the degree of f_β and let d be the least common multiple of the denominators of all the coefficients of f_β. Then, $d^m f_\beta(\frac{X}{d})$ is a monic polynomial with integer coefficients with βd as a root. Therefore $\beta d \in \mathscr{O}_K$ and $\beta = \frac{\alpha}{d}$ for $\alpha \in \mathscr{O}_K$ and $d \in \mathbb{Z}$. □

3.2 Determinant and discriminant

Given n algebraic numbers ω_i, and recalling our notation in (3.2) for ordering the conjugates, we define,

$$\Delta(\omega_1, \ldots, \omega_n) = \det \begin{pmatrix} \omega_1^{(1)} & \omega_1^{(2)} & \omega_1^{(3)} & \cdots & \omega_1^{(n-1)} \\ \omega_2^{(1)} & \omega_2^{(2)} & \omega_2^{(3)} & \cdots & \omega_2^{(n-1)} \\ \omega_3^{(1)} & \omega_3^{(2)} & \omega_3^{(3)} & \cdots & \omega_3^{(n-1)} \\ & \vdots & \vdots & & \vdots \\ \omega_n^{(1)} & \omega_n^{(2)} & \omega_n^{(3)} & \cdots & \omega_n^{(n-1)} \end{pmatrix}$$

If $\omega_1, \cdots \omega_n$ forms a basis for the field K, then we call the number $d_K = \Delta^2(\omega_1, \ldots, \omega_n)$ the **discriminant of the field**.

3.3 Ideals

3.3.1. A set S of numbers in $\mathscr{O}_K$ is said to be an **ideal** if for any α, β in S, then $\lambda\alpha + \mu\beta$ is also in S, for any λ, μ in $\mathscr{O}_K$. We will denote ideals of K with the letters $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ etc. We say that an ideal S is generated by the $\alpha_1, \ldots, \alpha_r \in \mathscr{O}_K$ if every every element of S can be written as a linear combination of the $\alpha_i, i = 1, \ldots, r$ with $\mathscr{O}_K$ coefficients. We denote this ideal as $(\alpha_1, \ldots, \alpha_r)$. An ideal is called **principal** if it is generated by a single element α. These are denoted as (α), though for brevity we will write it as α when no confusion can arise. The ideal consisting of the single element $\{0\}$ is called the **zero ideal**. It is easy to see that the ring of integers $\mathscr{O}_K$ is the ideal generated by 1.

3.3.2. An ideal can also be regarded as an abelian group, i.e. as a $\mathbb{Z}$-module, by forgetting its multiplicative structure. Clearly it is a free $\mathbb{Z}$-module since we are working in characteristic zero. A **basis of the ideal** will mean a basis as a $\mathbb{Z}$-module i.e., a basis of the ideal $\mathfrak{a}$ is a set of elements whose linear combination with coefficients in $\mathbb{Z}$ produce all elements of ideal $\mathfrak{a}$, and such that the these elements are linearly independent over $\mathbb{Z}$.

From [11, Proposition 2.10], $\mathcal{O}_K$ (regarded as an ideal) has a basis consisting of $n = [K : \mathbb{Q}]$ elements $\omega_1, \dots, \omega_n$. It follows that every ideal $\mathfrak{a} \subset \mathcal{O}_K$ also has a basis of size exactly n: indeed, a subgroup of a free abelian groups are free of rank n has rank at most n. On the other hand, for any $\alpha \in \mathfrak{a}$, the eleents $\alpha\omega_1, \dots, \alpha\omega_n$ are linearly independent over $\mathbb{Z}$, so that a basis of $\mathfrak{a}$ must have at least n elements.

3.3.3. We define the product $\mathfrak{ab}$ of two ideals $\mathfrak{a} = (\alpha_1, \dots, \alpha_r)$ and $\mathfrak{b} = (\beta_1, \dots, \beta_s)$ to be the ideal generated by all combination of products of their generators,

$$\mathfrak{ab} = (\alpha_1\beta_1, \dots, \alpha_r\beta_s)\,. \tag{3.5}$$

We say that an ideal $\mathfrak{a}$ **divides** the ideal $\mathfrak{b}$ if there exists an ideal $\mathfrak{c}$ such that,

$$\mathfrak{b} = \mathfrak{ac}\,. \tag{3.6}$$

We write $\mathfrak{a} \mid \mathfrak{b}$ in this case. Note that if $\mathfrak{a} \mid \mathfrak{b}$, then $\mathfrak{b} \subset \mathfrak{a}$. In fact the reverse is also true (see [11, §3]), so that

$$\mathfrak{b} \subset \mathfrak{a} \iff \mathfrak{a} \mid \mathfrak{b}. \tag{3.7}$$

We may also define the sum of two ideals $\mathfrak{a}$ and $\mathfrak{b}$ as,

$$\mathfrak{a} + \mathfrak{b} = \{a + b \,|\, a \in \mathfrak{a}, b \in \mathfrak{b}\} \tag{3.8}$$

It is easy to see that the ideal $\mathfrak{a} + \mathfrak{b}$ is the smallest ideal which contains both of them.

3.3.4. We say an ideal $\mathfrak{p}$ is **prime** if for any α, β in $\mathcal{O}_K$ such that $\alpha\beta \in \mathfrak{p}$ then α or β must also be in $\mathfrak{p}$. The letter $\mathfrak{p}$ will be reserved for denoting a prime ideal. We have unique prime factorization [1, pg.85].

Theorem. *For every ideal different from the zero ideal and $\mathcal{O}_K$ can be written uniquely as a product of prime ideals, up to permutation.*

We say that the **greatest common divisor** between two ideals $\mathfrak{a}$ and $\mathfrak{b}$ is the smallest ideal which divides both of them, denoted $(\mathfrak{a}, \mathfrak{b})$. It is easy to see from (3.8) that as the sum $\mathfrak{a} + \mathfrak{b}$ is the smallest ideal which contains both of them, that is

$$\mathfrak{a} + \mathfrak{b} = (\mathfrak{a}, \mathfrak{b}) \tag{3.9}$$

We say two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are **relatively prime** if they share no prime ideal factors. As two relatively prime ideals $\mathfrak{a}$ and $\mathfrak{b}$ have greatest common divisor $\mathcal{O}_K$, then they are relatively prime if and only if $\mathfrak{a} + \mathfrak{b} = \mathcal{O}_K$. If ideals $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime we write $(\mathfrak{a}, \mathfrak{b}) = 1$.

Corollary. *Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime if and only if there exists $\alpha \in \mathfrak{a}$ and $\beta \in \mathfrak{b}$ such that $\alpha + \beta = 1$.*

Proof. If $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime, then $\mathfrak{a}+\mathfrak{b}=\mathscr{O}_K$. As $1\in\mathscr{O}_K$, there exists $\alpha\in\mathfrak{a}$ and $\beta\in\mathfrak{b}$ such that $\alpha+\beta=1$. If $\alpha+\beta=1$, then $\mathfrak{a}+\mathfrak{b}\supseteq\mathscr{O}_K$. As every element of $\mathfrak{a}+\mathfrak{b}$ is in $\mathscr{O}_K$, we have $\mathfrak{a}+\mathfrak{b}\subseteq\mathscr{O}_K$. □

We say that the integer $\alpha\in\mathscr{O}_K$ is **relatively prime** to the ideal $\mathfrak{b}$ if the principal ideal (α) is relatively prime to the ideal $\mathfrak{b}$. Similarly we say that two integers $\alpha,\beta\in\mathscr{O}_K$ are **relatively prime** if they are relatively prime as principal ideals.

An integer in $\mathscr{O}_K$ or an ideal is said to be **odd** if it is relatively prime with the principal ideal (2).

3.3.5. We have the Chinese remainder theorem [5, pg.9],

Theorem. *(Chinese Remainder Theorem)*

Given ideals $\mathfrak{a}_1\dots,\mathfrak{a}_n$ such that $\mathfrak{a}_i+\mathfrak{a}_j=\mathscr{O}_K$ for any $i\neq j$ then for $\mathfrak{a}=\mathfrak{a}_1\cdots\mathfrak{a}_n$,

$$\mathscr{O}_K/\mathfrak{a}\cong\mathscr{O}_K/\mathfrak{a}_1\times\cdots\times\mathscr{O}_K/\mathfrak{a}_n \tag{3.10}$$

Remark. *The Chinese remainder theorem implies that for pairwise relatively prime ideals $\mathfrak{a}_1\dots,\mathfrak{a}_n$ the system of equations,*

$$\begin{aligned} x&\equiv c_1\ (mod\ \mathfrak{a}_1)\\ &\vdots\\ x&\equiv c_n\ (mod\ \mathfrak{a}_n)\end{aligned} \tag{3.11}$$

for constants $c_1,\dots,c_n\in\mathscr{O}_K$ admits a unique solution x modulo $\mathfrak{a}_1\cdots\mathfrak{a}_n$.

3.3.6. A set S of numbers in K is said to be a **fractional ideal** if:

1. For any α,β in S, then $\lambda\alpha+\mu\beta$ is also in S for arbitrary integers $\lambda,\mu\in\mathscr{O}_K$.
2. There exists a non-zero integer $\nu\in\mathscr{O}_K$ such that the product of ν with any number in S is in $\mathscr{O}_K$.

Products of fractional ideals are defined in the same way: if $\mathfrak{a}$ and $\mathfrak{b}$ are fractional ideals then,

$$\mathfrak{a}\mathfrak{b}=\left\{\sum_{i=1}^{k}\alpha_i\beta_i\mid\alpha_i\in\mathfrak{a},\beta_i\in\mathfrak{b},k\geq 0\right\} \tag{3.12}$$

which is easily seen to be fractional ideal.

For any ideal $\mathfrak{a}$, we define the set

$$\mathfrak{a}^{-1}=\{r\in K\,|\,r\mathfrak{a}\subset\mathscr{O}_K\}. \tag{3.13}$$

One may prove (see [11, §3]) that this forms a fractional ideal with the property $\mathfrak{a}\mathfrak{a}^{-1}=\mathscr{O}_K$. From this we can write $\mathfrak{a}^{-1}=\frac{1}{\mathfrak{a}}$ and call $\mathfrak{a}^{-1}$ the **inverse** of $\mathfrak{a}$.

For any fractional ideal $\mathfrak{g}$ and by property (2) of fractional ideals, there exists $\nu \in \mathscr{O}_K$ such that

$$\nu\mathfrak{g} \subset \mathscr{O}_K \tag{3.14}$$

hence

$$\mathfrak{g} = \frac{\mathfrak{c}}{\nu} \quad \text{for some ideal } \mathfrak{c}. \tag{3.15}$$

Therefore any fractional ideal $\mathfrak{g}$ may be represented as

$$\mathfrak{g} = \frac{\mathfrak{b}}{\mathfrak{a}} \quad \text{for relatively prime ideals } \mathfrak{a} \text{ and } \mathfrak{b}. \tag{3.16}$$

3.3.7. We will look at some important existence statements concerning ideals.

Lemma. *For every ideal $\mathfrak{a}$ and any $x \in \mathfrak{a}$, there exists a non-zero ideal $\mathfrak{b}$ such that their product $\mathfrak{a}\mathfrak{b}$ is the principal ideal (x).*

Proof. For any $x \in \mathfrak{a}$ let $\mathfrak{b} = x\mathfrak{a}^{-1}$. For any $r \in \mathfrak{a}^{-1}$ we have $rx \in \mathscr{O}_K$ by (3.13), so $\mathfrak{b}$ is an ideal. Moreover,

$$\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{a}^{-1}x = (x)\,. \tag{3.17}$$

□

Proposition. *For any ideals $\mathfrak{a}$ and $\mathfrak{c}$ there exists an ideal $\mathfrak{b}$ relatively prime to $\mathfrak{c}$ such that $\mathfrak{a}\mathfrak{b}$ is principal.*

Proof. Let the prime ideals that divide $\mathfrak{a}$ or $\mathfrak{c}$ be $\mathfrak{p}_1, \ldots, \mathfrak{p}_d$. Then let $\mathfrak{a}$ and $\mathfrak{c}$ factor as,

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_d^{e_d} \quad \text{and} \quad \mathfrak{c} = \mathfrak{p}_1^{f_1} \cdots \mathfrak{p}_d^{f_d} \tag{3.18}$$

for rational integers $e_i, f_i \geq 0$, and $\mathfrak{p}_i^{e_i} = \mathscr{O}_k$ when $e_i = 0$. Since $\mathfrak{p}^{e_i}$ is strictly contains $\mathfrak{p}^{e_i+1}$, we can always find some $x_i \in \mathfrak{p}^{e_i} \backslash \mathfrak{p}^{e_i+1}$. With these x_i we obtain equations in x,

$$x \equiv x_i \pmod{\mathfrak{p}^{e_i+1}} \quad \text{for } i = 1, \ldots, d \tag{3.19}$$

which are solvable by the Chinese remainder theorem (Theorem 3.3.5). Since $x \in \mathfrak{p}_i^{e_i}$, then $x\mathfrak{p}_i^{-e_i} \subset \mathscr{O}_K$ for any $i = 1, \ldots, d$. Therefore

$$x\mathfrak{a}^{-1} = x\mathfrak{p}_1^{-e_1} \cdots \mathfrak{p}_d^{-e_d} \subset \mathscr{O}_K \tag{3.20}$$

To see that $\mathfrak{b} := x\mathfrak{a}^{-1}$ is relatively prime to $\mathfrak{c}$, notice that ${\mathfrak{p}_\mathfrak{i}}^{e_i+1}$ does not divide (x) for any $i = 1, \ldots, d$. Since $x = \mathfrak{a}\mathfrak{b}$, there are no factors of $\mathfrak{p}_i$ in $\mathfrak{b}$. □

Corollary. *For any ideals $\mathfrak{f}$ and $\mathfrak{c}$, there exists $\omega \in K$ such that*

$$\omega = \frac{\mathfrak{b}}{\mathfrak{f}} \quad \textit{where } \mathfrak{b} \textit{ is an ideal relatively prime to } \mathfrak{c}. \tag{3.21}$$

Proof. For any $\delta \in \mathfrak{f}$ the set

$$\frac{\delta}{\mathfrak{f}} \quad \text{is an ideal.} \tag{3.22}$$

Therefore by Proposition 3.3.7 we can take some ideal $\mathfrak{b}$ relatively prime to $\mathfrak{c}$ such that,

$$\frac{\delta \mathfrak{b}}{\mathfrak{d}} = \delta' \quad \text{for } \delta' \in \mathscr{O}_K. \tag{3.23}$$

Hence $\omega = \delta'/\delta \in K$ works. □

3.4 Norms and Traces

3.4.1. We can define the **norm** and **trace** of a number $\alpha \in K$ respectively, recalling our notation for conjugates as in (3.4),

- $N : K \longrightarrow \mathbb{Q}$, $\alpha \longmapsto \alpha^{(1)} \cdots \alpha^{(p)}$
- $\mathrm{tr} : K \longrightarrow \mathbb{Q}$, $\alpha \longmapsto \alpha^{(1)} + \cdots + \alpha^{(p)}$.

We define the **trace of the signum function**, with the conjugates of ω ordered as in (3.4),

$$\mathrm{tr}(\mathsf{sgn}\,\omega) = \begin{cases} \mathsf{sgn}\,\omega^{(1)} + \cdots + \mathsf{sgn}\,\omega^{(r_1)} & \text{if } r_1 > 0 \\ 0 & \text{if } r_1 = 0\,. \end{cases} \tag{3.24}$$

One finds,

$$N(\alpha\beta) = N(\alpha)N(\beta) \quad \text{and} \quad \mathrm{tr}(\alpha + \beta) = \mathrm{tr}(\alpha) + \mathrm{tr}(\beta)\,. \tag{3.25}$$

We also define the **norm of an ideal** $\mathfrak{a}$, written $N(\mathfrak{a})$, as the number of residue classes $\pmod{\mathfrak{a}}$, ie $|\mathscr{O}/\mathfrak{a}|$. If $\alpha_1, \dots \alpha_n$ is a basis for $\mathfrak{a}$, then from [1, pg.87] and recalling our notation from 3.2,

$$N(\mathfrak{a}) = |\Delta(\alpha_1, \dots \alpha_n)/\sqrt{d_K}| \tag{3.26}$$

where d_K is the discriminant for the number field K.

Corollary. *For a principal ideal* $\mathfrak{a} = (\alpha)$*, the norm* $N(\mathfrak{a}) = |N(\alpha)|$

Proof. If $\omega_1, \dots, \omega_n$ is a basis for the number field, then a basis for $\mathfrak{a}$ is $\alpha\omega_1, \dots, \alpha\omega_n$ so

$$\Delta(\alpha\omega_1, \dots, \alpha\omega_n) = N(\alpha)\Delta(\omega_1, \dots, \omega_n) = N(\alpha)\sqrt{d_K}\,. \tag{3.27}$$

□

Proposition. *The ideal norm is multiplicative:* $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$.

Proof. By the Chinese remainder theorem (Theorem 3.3.5), we have for dinstinct primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$,

$$|\mathscr{O}/\mathfrak{p}_1\mathfrak{p}_2| = |\mathscr{O}/\mathfrak{p}_1 \times \mathscr{O}/\mathfrak{p}_2| = |\mathscr{O}/\mathfrak{p}_1| \cdot |\mathscr{O}/\mathfrak{p}_2|\,. \tag{3.28}$$

Hence it suffices to prove $N(\mathfrak{p}^r) = N(\mathfrak{p})^r$. We will prove by induction. The base case when $r = 1$ is trivial. The map

$$\mathscr{O}_K/\mathfrak{p}^{r+1} \to \mathscr{O}_K/\mathfrak{p}^r \tag{3.29}$$

is surjective with kernel $\mathfrak{p}^r/\mathfrak{p}^{r+1}$ which has norm $N(\mathfrak{p})$. By the first isomorphism theorem [13, pg.243],

$$(\mathscr{O}_K/\mathfrak{p}^{r+1})/(\mathfrak{p}^r/\mathfrak{p}^{r+1}) \cong \mathscr{O}_K/\mathfrak{p}^r, \tag{3.30}$$

hence,

$$N(\mathfrak{p}^{r+1}) = N(\mathfrak{p}^r)N(\mathfrak{p}) \tag{3.31}$$

so by our inductive assumption

$$N(\mathfrak{p}^{r+1}) = N(\mathfrak{p})^r N(\mathfrak{p}) = N(\mathfrak{p})^{r+1} \tag{3.32}$$

□

3.4.2. Furthermore if $\mathfrak{c} = \mathfrak{a}/\mathfrak{b}$ is a fractional ideal, then we define $N(\mathfrak{c}) = N(\mathfrak{a})/N(\mathfrak{b})$. If the basis for fractional ideal $\mathfrak{c}$ (i.e., a basis of the fractional ideal regarded as an abelian group) is $\gamma_1, \dots, \gamma_n$, then $N(\mathfrak{c}) = |\Delta(\gamma_1, \dots \gamma_n)/\sqrt{d_K}|$. To see this take an integer $\nu \neq 0$ such that $\nu\mathfrak{c}$ is an ideal $\mathfrak{b}$ with basis $\beta_1, \dots, \beta_n$. Then $\beta_1/\nu, \dots, \beta_n/\nu$ is a basis for $\mathfrak{c}$ and

$$N(\mathfrak{c}) = \frac{N(\mathfrak{b})}{N(\nu)} = \frac{|\Delta(\beta_1, \dots, \beta_n)|}{|N(\nu)\sqrt{d_K}|} = \left|\frac{\Delta(\beta_1/\nu, \dots, \beta_n/\nu)}{\sqrt{d_K}}\right|, \tag{3.33}$$

giving us our conclusion.

3.5 The different of an ideal

Lemma. *Let K be an algebraic number field, and $\mathfrak{a} \subset \mathscr{O}_K$ be an ideal. Define the set*

$$\mathfrak{a}^\vee := \{\lambda \in K \mid \operatorname{tr}(\lambda\alpha) \in \mathbb{Z} \text{ for all } \alpha \in \mathfrak{a}\}. \tag{3.34}$$

*Then if $\alpha_1, \dots, \alpha_n$ form a basis for $\mathfrak{a}$ then $\mathfrak{a}^\vee = \oplus_{i=1}^n \mathbb{Z}\alpha_i^\vee$ where $\alpha_1^\vee, \dots, \alpha_n^\vee$ is the dual basis given by $\operatorname{tr}(\alpha_i\alpha_j^\vee) = \delta_{ij}$. This implies $\mathfrak{a}^\vee$ is a fractional ideal, which we call the **dual** of $\mathfrak{a}$.*

Proof. Take any $\omega \in K$. Then we may find $c_1, \dots, c_n \in \mathbb{Q}$ such that $\omega = \sum_{i=1}^n c_i\alpha_i^\vee$. For any α_i we have

$$\operatorname{tr}(\omega\alpha_i) = c_i \tag{3.35}$$

Hence $\omega \in \mathfrak{a}^\vee$ if and only if $c_i \in \mathbb{Z}$ for all $i = 1, \dots, n$. □

Corollary. *If $\alpha_1, \dots, \alpha_n$ define a basis for $\mathfrak{a}$, with a basis $\beta_1, \dots, \beta_n$ for $\mathfrak{a}^\vee = 1/\mathfrak{a}\mathfrak{d}$ which, along with their conjugates, are determined by the n^2 equations*

$$\mathrm{tr}(\beta_i \alpha_k) = \delta_{ik} \tag{3.36}$$

for all $i, k = 1, \dots, n$ and δ is the Kronecker delta function as in (2.1)*, then*

$$\sum_{i=1}^{n} \alpha_i^{(q)} \beta_i^{(p)} = \delta_{pq}\,. \tag{3.37}$$

also holds.

Proof. We will first show that $\beta_1, \dots, \beta_n$ really belong to K. On one hand,

$$\sum_{i=1}^{n} \alpha_i^{(q)} \,\mathrm{tr}(\alpha_k \beta_i) = \sum_{i=1}^{n} \alpha_i^{(q)} \sum_{p=1}^{n} \alpha_k^{(p)} \beta_i^{(p)} = \sum_{p=1}^{n} \alpha_k^{(p)} \sum_{i=1}^{n} \alpha_i^{(q)} \beta_i^{(p)}\,, \tag{3.38}$$

and on the other,

$$\sum_{i=1}^{n} \alpha_i^{(q)} \,\mathrm{tr}(\alpha_k \beta_i) = \sum_{i=1}^{n} \alpha_i^{q} \delta_{ki} = \alpha_k^{(q)} = \sum_{p=1}^{n} \alpha_k^{(p)} \delta_{pq}\,, \tag{3.39}$$

so since (3.38) is equal to (3.39),

$$\sum_{p=1}^{n} \alpha_k^{(p)} \sum_{i=1}^{n} \alpha_i^{(q)} \beta_i^{(p)} = \sum_{p=1}^{n} \alpha_k^{(p)} \delta_{pq}\,. \tag{3.40}$$

Therefore we may conclude

$$\sum_{i=1}^{n} \alpha_i^{(q)} \beta_i^{(p)} = \delta_{pq}\,. \tag{3.41}$$

□

Theorem. *Let K be an algebraic number field, and $\mathfrak{a} \subset \mathscr{O}_K$ be an ideal with $\mathfrak{a}^\vee$ its dual ideal. The product $\mathfrak{a}^\vee\,\mathfrak{a}$ is independent of $\mathfrak{a}$; in fact, it is the inverse of an ideal which we call the* ***different*** *and denote as $\mathfrak{d}$.*

Proof. Consider dual of the ring of integers, which is an ideal by Lemma 3.5,

$$\mathscr{O}_K^\vee = \{\lambda \in K \mid \mathrm{tr}(\lambda\,\xi) \in \mathbb{Z} \text{ for } \xi \in \mathscr{O}_K\}. \tag{3.42}$$

We will show that

$$\mathfrak{a}\,\mathfrak{a}^\vee = \mathscr{O}_K^\vee. \tag{3.43}$$

To show the inclusion $\mathfrak{a}\,\mathfrak{a}^\vee \subset \mathscr{O}_K^\vee$, choose $\lambda \in \mathfrak{a}^\vee$ and $\alpha \in \mathfrak{a}$. Then for each $\xi \in \mathscr{O}_K$, we have $\mathrm{tr}(\lambda\alpha\xi) = \mathrm{tr}(\lambda(\alpha\xi)) \in \mathbb{Z}$, thus implying $\lambda\alpha \in \mathfrak{m}_{\mathscr{O}}$. Now we turn to the reverse inclusion. Let

$\mu \in \mathfrak{m}_{\mathscr{O}}$. Also, let $\rho_1, \dots, \rho_n$ denote a basis for the fractional ideal $1/\mathfrak{a}$. Then for $\alpha \in \mathfrak{a}$, we have $\alpha\rho_j \in \mathscr{O}_K$ for any $1 \le j \le n$, and hence $\mathrm{tr}(\mu\rho_k\alpha)$ is a rational integer. This means that the product of μ with any element in $1/\mathfrak{a}$ yields an element of $\mathfrak{a}^\vee$, hence μ belongs to $\mathscr{O}_K^\vee$. Thus we have shown (3.43).

Since $1 \in \mathscr{O}_K^\vee$, we can conclude that if $\alpha \in \frac{1}{\mathscr{O}_K^\vee}$ then $\alpha \in \mathscr{O}_K$, i.e. $\mathscr{O}_K^\vee$ is the reciprocal of some ideal. □

Theorem 3.5 tells us that the different is the inverse of the dual of the ring of integers,

$$\mathfrak{d} = (\mathscr{O}_K^\vee)^{-1} = \{x \in K : x\mathscr{O}_K^\vee \subset \mathscr{O}_K\}. \tag{3.44}$$

This also means that for any ideal $\mathfrak{a}$,

$$\mathfrak{a}^\vee = \frac{1}{\mathfrak{a}\mathfrak{d}} \tag{3.45}$$

Proposition. *Let $\mathfrak{d}$ be the different and d_K be the discriminant for the field K. Then,*

$$N(\mathfrak{d}) = |d_K|. \tag{3.46}$$

Proof. For nonzero fractional ideals we have $\mathfrak{a}\mathfrak{c}/\mathfrak{b}\mathfrak{c} = \mathfrak{a}/\mathfrak{b}$ for $\mathfrak{a} \subset \mathfrak{b}$. Letting $\mathfrak{a} = \mathfrak{c}^{-1}$ and $\mathfrak{b} = \mathscr{O}_K$ gives $\mathscr{O}_K/\mathfrak{c} = \mathfrak{c}^{-1}/\mathscr{O}_K$ Therefore the index $[\mathscr{O}_K : \mathfrak{c}] = [\mathfrak{c}^{-1} : \mathscr{O}_K]$. Therefore we have,

$$N(\mathfrak{d}) = [\mathscr{O}_K : \mathfrak{d}] = [\mathfrak{d}^{-1} : \mathscr{O}_K] = [\mathscr{O}_K^\vee : \mathscr{O}_K]. \tag{3.47}$$

Let $e_1, \dots, e_n$ be a $\mathbb{Z}$-basis for $\mathscr{O}_K$ so that $\mathscr{O}_K = \oplus_{i=1}^n \mathbb{Z}e_i$ and $\mathscr{O}_K^\vee = \oplus_{i=1}^n \mathbb{Z}e_i^\vee$ where $e_i^\vee$ is the dual basis given by $\mathrm{tr}(e_ie_j^\vee) = \delta_{ij}$. If $e_j = \sum_{i=1}^n a_{ij}e_i^\vee$ then $a_{ij} = \mathrm{tr}(e_je_i) = \mathrm{tr}(e_ie_j)$. Therefore $(a_{ij}) = (\mathrm{tr}(e_je_i))$. The determinant of the left hand side matrix is $N(\mathfrak{d})$ and the determinant of the right hand side matrix is $|d_K|$, giving us the result. □

3.6 Examples of various fields

3.6.1. When $K = \mathbb{Q}$ then $\mathscr{O}_K = \mathbb{Z}$ a principal ideal domain. Hence all ideals are principal, so all the prime ideals are exactly those generated by rational primes. Here the discriminant $d_K = 1$. Since $\mathscr{O}_K = \mathscr{O}_K^\vee = \mathbb{Z}$. This means that $\mathfrak{d} = \mathbb{Z}$.

3.6.2. When $K = \mathbb{Q}(\sqrt{m})$ for m squarefree and $m \equiv 2,3 \pmod 4$. Here the ring of integers $\mathscr{O}_K = \mathbb{Z}[\sqrt{m}] = \mathbb{Z} + \sqrt{m}\mathbb{Z}$.

The discriminant may be calculated,

$$d_K = \det\begin{pmatrix} 1 & 1 \\ \sqrt{m} & -\sqrt{m} \end{pmatrix}^2 = (\sqrt{m} + \sqrt{m})^2 = 4m. \tag{3.48}$$

For any $a+b\sqrt{m}\in K$, we have $a+b\sqrt{m}\in \mathscr{O}_K^\vee$ when both

$$\mathrm{tr}(a+b\sqrt{m})\in\mathbb{Z} \quad \text{and} \quad \mathrm{tr}((a+b\sqrt{m})\sqrt{m}) = \mathrm{tr}(mb+a\sqrt{m})\in\mathbb{Z}\,. \tag{3.49}$$

This is equivalent to $2a\in\mathbb{Z}$ and $2bm\in\mathbb{Z}$ respectively. Therefore

$$\mathscr{O}_K^\vee = \frac{1}{2}\mathbb{Z}+\frac{\sqrt{m}}{2m}\mathbb{Z} = \frac{1}{2}\mathbb{Z}+\frac{1}{2\sqrt{m}}\mathbb{Z} = \frac{1}{2\sqrt{m}}\big(\mathbb{Z}+\sqrt{m}\mathbb{Z}\big) = \frac{1}{2\sqrt{m}}\mathscr{O}_K = \frac{1}{2\sqrt{m}}\mathbb{Z}[\sqrt{m}]\,. \tag{3.50}$$

Hence we have the different, $\mathfrak{d} = 2\sqrt{m}\mathbb{Z}[\sqrt{m}]$.

3.6.3. When $K=\mathbb{Q}(\sqrt{m})$ for m squarefree and $m\equiv 1 \pmod 4$. Here the ring of integers $\mathscr{O}_K = \mathbb{Z}[\frac{1+\sqrt{m}}{2}] = \mathbb{Z}+\frac{1+\sqrt{m}}{2}\mathbb{Z}$.

The discriminant may be calculated,

$$d_K = \det\begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{m}}{2} & \frac{1-\sqrt{m}}{2}\end{pmatrix}^2 = \Big(\frac{1+\sqrt{m}}{2}-\frac{1-\sqrt{m}}{2}\Big)^2 = m\,. \tag{3.51}$$

For any $a+b\sqrt{m}$ in K, we have $a+b\sqrt{m}$ in $\mathscr{O}_K^\vee$ when both $\mathrm{tr}(a+b\sqrt{m})\in\mathbb{Z}$ and $\mathrm{tr}((a+b\sqrt{m})\frac{1+\sqrt{m}}{2}) = \mathrm{tr}(\frac{a+bm}{2}+\frac{a+b}{2}\sqrt{m})\in\mathbb{Z}$. This is equivalent to $2a\in\mathbb{Z}$ and $a+bm\in\mathbb{Z}$ respectively. So if we let, for rational integers x,y,

$$\begin{aligned} 2a &= x \\ a+bm &= y\,, \end{aligned} \tag{3.52}$$

then,

$$\begin{aligned} a &= \frac{x}{2} \\ b &= \frac{1}{m}\left(y-\frac{x}{2}\right). \end{aligned} \tag{3.53}$$

Therefore

$$\mathscr{O}_K^\vee = \Big(\frac{1}{2}-\frac{1}{2m}\sqrt{m}\Big)\mathbb{Z}+\frac{\sqrt{m}}{m}\mathbb{Z} = \frac{1}{\sqrt{m}}\Big((\frac{\sqrt{m}}{2}-\frac{1}{2})\mathbb{Z}+\mathbb{Z}\Big) = \frac{1}{\sqrt{m}}\Big(\frac{1+\sqrt{m}}{2}\mathbb{Z}+\mathbb{Z}\Big) = \frac{1}{\sqrt{m}}\mathscr{O}_K = \frac{1}{\sqrt{m}}\mathbb{Z}[\sqrt{m}]\,. \tag{3.54}$$

Hence we have the different, $\mathfrak{d} = \sqrt{m}\mathbb{Z}[\sqrt{m}]$.

3.6.4. In the special case of 3.6.2 when $K=\mathbb{Q}(i)$ we have the ring of integers $\mathscr{O}_K = \mathbb{Z}[i] = \mathbb{Z}+i\mathbb{Z}$. Since $\mathbb{Z}[i]$ is a principal ideal domain, all ideals are principal, so all the prime ideals are generated by the Gaussian primes. In order for the number $a+bi$ to be a Gaussian Prime, it must satisfy one of the following three conditions,

(a) $a\neq 0, b\neq 0, a^2+b^2$ is a rational prime

(b) $a\neq 0, b=0, |a|$ is a rational prime with $|a|\equiv 3 \pmod 4$

(c) $a = 0, b \neq 0, |b|$ is a rational prime with $|b| \equiv 3 \pmod 4$

We may calculate the discriminant $d_K = -4$, and the different $\mathfrak{d} = 2i\mathbb{Z}[i] = 2\mathbb{Z}[i]$.

3.6.5. In another special case of 3.6.2 when $K = \mathbb{Q}(\sqrt{2})$ we have the ring of integers $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \sqrt{2}\mathbb{Z}$. We may calculate the discriminant $d_K = 8$, and the different $\mathfrak{d} = 2\sqrt{2}\mathbb{Z}[\sqrt{2}]$.

4 Gauss Sums and the Law of Quadratic Reciprocity

Fix a number field K, $\alpha \in \mathscr{O}_K$, and ideal $\mathfrak{m} \subset \mathscr{O}_K$. An interesting question to ask is whether or not

$$\alpha \equiv x^2 \pmod{\mathfrak{m}} \tag{4.1}$$

has a solution $x \in \mathscr{O}_K$. If there is a solution, we call α a quadratic residue mod $\mathfrak{m}$, and we call it a quadratic non-residue otherwise. To determine whether or not an integer is a quadratic residue one uses the theorem of the law of quadratic reciprocity. To prove this law, we will need to define and discuss some important properties of an interesting class of functions, called Gauss sums. We will formulate many properties of these Gauss sums, however the proof for the main identity we need about them will be deferred to section 6.4, where it will be established using analytic techniques. We prove in section 4.4 how to obtain the law of quadratic reciprocity using the stated properties of Gauss sums. At the end of this section, we will look at some concrete examples to really see the power of the law of quadratic reciprocity in action.

4.1 Quadratic Residues

4.1.1. Let $\mathfrak{p} \subset \mathscr{O}_K$ be an odd prime ideal, i.e. relatively prime to (2), and $\alpha \in \mathscr{O}_K$ such that $\alpha \not\equiv 0 \pmod{\mathfrak{p}}$, i.e. $\mathfrak{p} \not| (\alpha)$. We call α a **quadratic residue mod** $\mathfrak{p}$ if there exists an integer $\xi \in \mathscr{O}_K$ such that $\alpha \equiv \xi^2 \pmod{\mathfrak{p}}$. If there does not exist such an integer ξ, then we say α a **quadratic non-residue mod** $\mathfrak{p}$. We define the **Legendre symbol** as

$$\left[\frac{\alpha}{\mathfrak{p}}\right]_2 = \begin{cases} 1, & \text{if } \alpha \not\equiv 0 \pmod{\mathfrak{p}} \text{ and } \alpha \text{ is a quadratic residue mod } \mathfrak{p}, \\ -1, & \text{if } \alpha \not\equiv 0 \pmod{\mathfrak{p}} \text{ and } \alpha \text{ is a quadratic non-residue mod } \mathfrak{p}, \\ 0 & \text{if } \alpha \equiv 0 \pmod{\mathfrak{p}}. \end{cases} \tag{4.2}$$

For integers $\alpha, \beta \in \mathscr{O}_K$ it is easy to see that we have

$$\left[\frac{\alpha}{\mathfrak{p}}\right]_2 = \left[\frac{\beta}{\mathfrak{p}}\right]_2, \quad \text{if } \alpha \equiv \beta \pmod{\mathfrak{p}} \tag{4.3}$$

$$\left[\frac{\alpha \cdot \beta}{\mathfrak{p}}\right]_2 = \left[\frac{\alpha}{\mathfrak{p}}\right]_2 \left[\frac{\beta}{\mathfrak{p}}\right]_2. \tag{4.4}$$

Given an ideal $\mathfrak{m}$ with prime decomposition $\mathfrak{m} = \mathfrak{p}_1{}^{a_1}\mathfrak{p}_2{}^{a_2}\cdots\mathfrak{p}_{\mathfrak{r}}{}^{a_r}$ with a_i positive integers for $i = 1, \ldots, r$, then for $\alpha \in \mathscr{O}_K$ we define the **Jacobi Symbol** as,

$$\left[\frac{\alpha}{\mathfrak{m}}\right]_2 = \left[\frac{\alpha}{\mathfrak{p}_1}\right]_2^{a_1} \cdot \left[\frac{\alpha}{\mathfrak{p}_2}\right]_2^{a_2} \cdots \left[\frac{\alpha}{\mathfrak{p}_{\mathfrak{r}}}\right]_2^{a_r}. \tag{4.5}$$

For $\alpha, \beta \in \mathscr{O}_K$, the symbol $\left[\frac{\alpha}{\beta}\right]_2$ is viewing β as the principal ideal generated by β. In essence,

$$\left[\frac{\alpha}{\beta}\right]_2 = \left[\frac{\alpha}{(\beta)}\right]_2 \tag{4.6}$$

It is easy to see that this definition of the Legendre symbol agrees with the one in (1.2).

4.2 Quadratic Gauss Sums

4.2.1. Let ω in K be some non-zero algebraic number. Let $\mathfrak{d}$ be the different of K as defined in 3.5, and write $\mathfrak{d}\omega$ (recall here ω refers to the principal ideal (ω)) as the quotient of relatively prime ideals $\mathfrak{a}$ and $\mathfrak{b}$, i.e.,

$$\mathfrak{d}\omega = \frac{\mathfrak{b}}{\mathfrak{a}}. \tag{4.7}$$

Note that ω uniquely determines $\mathfrak{a}$ and $\mathfrak{b}$. We call $\mathfrak{a}$ the **denominator** of $\mathfrak{d}\omega$.

4.2.2. By Theorem 3.5, for any ideal $\mathfrak{a}$ one has its dual ideal $\mathfrak{a}^\vee = \mathfrak{a}^{-1}\mathfrak{d}^{-1}$. Furthermore, since $\omega = \beta\lambda'$ for some $\beta \in \mathfrak{b}$ and some number λ' in $\mathfrak{a}^\vee$, then

$$\mathrm{tr}(\mu\omega) = \mathrm{tr}(\mu\beta\lambda') \in \mathbb{Z} \quad \text{for any } \mu \in \mathfrak{a}. \tag{4.8}$$

This means that the number $e^{2\pi i\,\mathrm{tr}(\nu\omega)}$ depends only on the residue class $\nu \pmod{\mathfrak{a}}$. The simplest sum we could consider is the sum over residues modulo $\mathfrak{a}$. However,

Lemma. *Let $\mathfrak{d}\omega$ have denominator $\mathfrak{a} \neq 1$. Then,*

$$\sum_{\mu \bmod \mathfrak{a}} e^{2\pi i\,\mathrm{tr}(\mu\omega)} = 0. \tag{4.9}$$

Proof. For any $\alpha \in \mathscr{O}_K$, as μ runs though a system of residues mod $\mathfrak{a}$, then $\mu + \alpha$ also runs through a system of residues mod $\mathfrak{a}$. Then by letting the sum in (4.9) be equal to A, we have for any $\alpha \in \mathscr{O}_K$,

$$A = A \cdot e^{2\pi i\,\mathrm{tr}(\alpha\omega)}. \tag{4.10}$$

Since $\mathfrak{a} \neq 1$ then $\omega \notin \mathfrak{d}^{-1}$. However by (3.44) we have $\mathfrak{d}^{-1} = \mathscr{O}_K^\vee$ so there exists some $\alpha \in \mathscr{O}_K$ such that $\mathrm{tr}(\alpha\omega) \notin \mathbb{Z}$. For this α we have $e^{2\pi i\,\mathrm{tr}(\alpha\omega)} \neq 0$, so $A = 0$ in (4.10). □

4.2.3. As the sum in (4.9) is not interesting, this motivates us to define a new sum,

$$\mathbb{g}(\omega) = \sum_{\mu \bmod \mathfrak{a}} e^{2\pi i\,\mathrm{tr}(\mu^2\omega)}. \tag{4.11}$$

We call this sum a **quadratic Gauss sum in** K. When we refer to the denominator of the Gauss sum, we are referring to the ideal $\mathfrak{a}$, the denominator of $\mathfrak{d}\omega$. It is easy to see that Gauss sums of denominator 1 are identically 1.

4.3 Properties of Gauss sums

The following summarizes the properties of Gauss sums we will need.

Theorem. *Let $\omega \in K$ and write $\mathfrak{d}\omega = \mathfrak{b}\mathfrak{a}^{-1}$ for relatively prime ideals $\mathfrak{b}$ and $\mathfrak{a}$. Then,*

(a) if $\beta \in \mathcal{O}_K$ relatively prime to $\mathfrak{a}$ and $\chi \equiv \beta^2 \pmod{\mathfrak{a}}$ then,

$$\mathbb{g}(\omega) = \mathbb{g}(\chi\omega)\,. \tag{4.12}$$

(b) If $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2$ relatively prime ideals, then we may write $\mathbb{g}(\omega)$ as a product of two Gauss sums with denominators $\mathfrak{a}_1$ and $\mathfrak{a}_2$ respectively. Moreover, if $\alpha_1 \in \mathfrak{a}_1$ and $\alpha_2 \in \mathfrak{a}_2$ are relatively prime, setting

$$\beta = \omega\alpha_1\alpha_2\,, \tag{4.13}$$

gives,

$$\mathbb{g}(\omega) = \mathbb{g}\left(\frac{\beta}{\alpha_1\alpha_2}\right) = \mathbb{g}\left(\frac{\beta\alpha_2}{\alpha_1}\right)\mathbb{g}\left(\frac{\beta\alpha_1}{\alpha_2}\right), \tag{4.14}$$

where $\mathbb{g}\left(\frac{\beta\alpha_2}{\alpha_1}\right)$ has denominator $\mathfrak{a}_1$ and $\mathbb{g}\left(\frac{\beta\alpha_1}{\alpha_2}\right)$ has denominator $\mathfrak{a}_2$.

(c) Let $\mathfrak{a} = \mathfrak{p}^a$ where $\mathfrak{p}$ is an odd prime ideal and $a \geq 2$. Take $\alpha \in \mathfrak{p}/\mathfrak{p}^2$. Setting

$$\beta = \omega\alpha^a \tag{4.15}$$

we have,

$$\mathbb{g}(\omega) = \mathbb{g}\left(\frac{\beta}{\alpha^a}\right) = \begin{cases} N(\mathfrak{p})^{a/2}, & \textit{if } a \textit{ is even,} \\ N(\mathfrak{p})^{(a-1)/2}\mathbb{g}\left(\dfrac{\beta}{\alpha}\right), & \textit{if } a \textit{ is odd,} \end{cases} \tag{4.16}$$

where $\mathbb{g}\left(\frac{\beta}{\alpha}\right)$ has denominator $\mathfrak{p}$.

(d) For every integer $\chi \in \mathcal{O}_K$ which is relatively prime to $\mathfrak{a}$ we have,

$$\mathbb{g}(\chi\omega) = \left[\frac{\chi}{\mathfrak{a}}\right]_2 \mathbb{g}(\omega)\,. \tag{4.17}$$

(e) Let $\mathfrak{b}_1$ be the denominator of $\mathfrak{a}/4\mathfrak{b}$, γ an arbitrary number in K such that $\mathfrak{d}\gamma$ is relatively prime to $\mathfrak{b}_1$, and $\mathrm{tr}(\mathsf{sgn}\,\omega)$ as defined in (3.24). Then we have the reciprocity,

$$\frac{\mathbb{g}(\omega)}{|\sqrt{N(\mathfrak{a})}|} = \left|\frac{\sqrt{N(2\mathfrak{b})}}{N(\mathfrak{b}_1)}\right| e^{(\pi i/4)\,\mathrm{tr}(\mathsf{sgn}\,\omega)}\mathbb{g}\left(\frac{-\gamma^2}{4\omega}\right). \tag{4.18}$$

(f) Gauss sums of odd denominator or denominator 4 are non-zero.

The proof of part (e) will be left to the section 6.4. The remaining proofs are as follows.

4.3.1. *Proof of Theorem 4.3, part (a).* Let $\beta \in \mathscr{O}_K$ be relatively prime to $\mathfrak{a}$. As μ goes through all of the residues mod $\mathfrak{a}$, then $\mu\beta$ also goes through all of the residues mod $\mathfrak{a}$. Therefore

$$\mathbb{g}(\omega) = \mathbb{g}(\beta^2\omega)\,. \tag{4.19}$$

For any $\mu \in \mathscr{O}_K$, and since $\beta^2 - \chi \in \mathfrak{a}$, we have

$$\operatorname{tr}(\mu^2\beta^2\omega) - \operatorname{tr}(\mu^2\chi\omega) = \operatorname{tr}(\mu^2\beta^2\omega - \mu^2\chi\omega) = \operatorname{tr}(\mu^2\omega(\beta^2 - \chi)) \in \mathbb{Z}\,, \tag{4.20}$$

hence we may conclude that

$$e^{2\pi i \operatorname{tr}(\mu^2\beta^2\omega)} = e^{2\pi i \operatorname{tr}(\mu^2\chi\omega)}\,. \tag{4.21}$$

Therefore by (4.19) and (4.21),

$$\mathbb{g}(\omega) = \mathbb{g}(\beta^2\omega) = \sum_{\mu\in\mathfrak{a}} e^{2\pi i \operatorname{tr}(\mu^2\beta^2\omega)} = \sum_{\mu\in\mathfrak{a}} e^{2\pi i \operatorname{tr}(\mu^2\chi\omega)} = \mathbb{g}(\chi\omega)\,. \tag{4.22}$$

□

4.3.2. *Proof of Theorem 4.3, part (b).* We will first prove (4.14). As $(\mathfrak{a}_1, \mathfrak{a}_2) = 1$, we may choose $\alpha_1 \in \mathfrak{a}_1$ and $\alpha_2 \in \mathfrak{a}_2$ such that

$$\alpha_1 \equiv 1 \pmod{\mathfrak{a}_2}\,, \quad \alpha_2 \equiv 1 \pmod{\mathfrak{a}_1}\,. \tag{4.23}$$

Let

$$\mu = \rho_1\alpha_2 + \rho_2\alpha_1\,. \tag{4.24}$$

As ρ_1 and ρ_2 run through residue classes mod $\mathfrak{a}_1$ and $\mathfrak{a}_2$ respectively, we obtain $N(\mathfrak{a}_1)N(\mathfrak{a}_2) = N(\mathfrak{a})$ distinct residue classes mod $\mathfrak{a}$. Therefore μ runs through a complete system of residue classes mod $\mathfrak{a}$. By (4.13) and (4.24),

$$\mu^2\omega = \rho_1^2\frac{\alpha_2\beta}{\alpha_1} + 2\rho_1\rho_2\beta + \rho_2^2\frac{\alpha_1\beta}{\alpha_2}\,. \tag{4.25}$$

Now taking $\mathfrak{c}_1, \mathfrak{c}_2$ ideals as in Lemma 3.3.7 such that,

$$\mathfrak{a}_1\mathfrak{c}_1 = \alpha_1\,, \qquad \mathfrak{a}_2\mathfrak{c}_2 = \alpha_2\,, \tag{4.26}$$

and using (4.13) and $\omega = \mathfrak{b}\mathfrak{a}^{-1}\mathfrak{d}^{-1}$, we obtain,

$$\beta = \omega\alpha_1\alpha_2 = \omega\mathfrak{a}_1\mathfrak{a}_2\mathfrak{c}_1\mathfrak{c}_2 = \omega\mathfrak{a}\mathfrak{c}_1\mathfrak{c}_2 = \frac{\mathfrak{b}\mathfrak{c}_1\mathfrak{c}_2}{\mathfrak{d}}\,. \tag{4.27}$$

Turning to the final assertion of Theorem 4.3 part (b). Consider (4.27) and (4.26) which give,

$$\frac{\beta\alpha_2}{\alpha_1} = \frac{\alpha_2\mathfrak{b}\mathfrak{c}_1\mathfrak{c}_2}{\alpha_1\mathfrak{d}} = \frac{\alpha_2\mathfrak{b}\mathfrak{c}_2}{\mathfrak{d}\mathfrak{a}_1}\,. \tag{4.28}$$

From (4.28), as $(\alpha_1, \alpha_2) = 1$ implies $(\mathfrak{a}_1, \mathfrak{c}_2) = 1$, we can see $\mathbb{g}\left(\frac{\beta\alpha_2}{\alpha_1}\right)$ has denominator $\mathfrak{a}_1$. By a similar calculation, $\mathbb{g}\left(\frac{\beta\alpha_1}{\alpha_2}\right)$ has denominator $\mathfrak{a}_2$.

As $\beta\mathfrak{d}$ has denominator 1, so $\mathrm{tr}(2\rho_1\rho_2\beta) \in \mathbb{Z}$ and by (4.25),

$$e^{2\pi i \,\mathrm{tr}(\mu^2\omega)} = e^{2\pi i \,\mathrm{tr}(\rho_1^2\alpha_2\beta/\alpha_1)} e^{2\pi i \,\mathrm{tr}(\rho_2^2\alpha_1\beta/\alpha_2)}. \tag{4.29}$$

Therefore

$$\begin{aligned} \mathbb{g}\left(\frac{\beta}{\alpha_1\alpha_2}\right) &= \sum_{\mu\in\mathfrak{a}} e^{2\pi i \,\mathrm{tr}(\mu^2\omega)} \\ &= \sum_{\rho_1\in\mathfrak{a}_1}\sum_{\rho_2\in\mathfrak{a}_2} e^{2\pi i \,\mathrm{tr}(\rho_1^2\alpha_2\beta/\alpha_1)} e^{2\pi i \,\mathrm{tr}(\rho_2^2\alpha_1\beta/\alpha_2)} \\ &= \sum_{\rho_1\in\mathfrak{a}_1} e^{2\pi i \,\mathrm{tr}(\rho_1^2\alpha_2\beta/\alpha_1)} \sum_{\rho_2\in\mathfrak{a}_2} e^{2\pi i \,\mathrm{tr}(\rho_2^2\alpha_1\beta/\alpha_2)} \\ &= \mathbb{g}\left(\frac{\beta\alpha_2}{\alpha_1}\right)\mathbb{g}\left(\frac{\beta\alpha_1}{\alpha_2}\right), \end{aligned} \tag{4.30}$$

proving (4.14). □

4.3.3. *Proof of Theorem 4.3, part (c).* This part handles Gauss sums with denominator a power of a prime ideal. We apply a similar approach as part (b). By Proposition 3.3.7 we know there exists an ideal $\mathfrak{c}$ relatively prime to $\mathfrak{p}$ such that,

$$\mathfrak{p}\mathfrak{c} = \alpha. \tag{4.31}$$

So by (4.15),

$$\beta = \omega\alpha^a = \omega\mathfrak{p}^a\mathfrak{c}^a = \frac{\mathfrak{b}\mathfrak{c}^a}{\mathfrak{d}}. \tag{4.32}$$

We will show $\mathbb{g}(\beta/\alpha^k)$ for $k < a$ has denominator $\mathfrak{p}^k$. Consider (4.31) and (4.32) which imply,

$$\frac{\beta}{\alpha^k} = \frac{\mathfrak{b}\mathfrak{c}^{a-k}}{\mathfrak{p}^k\mathfrak{d}}. \tag{4.33}$$

As $(\mathfrak{c}, \mathfrak{p}) = 1$, the Gauss sum $\mathbb{g}(\beta/\alpha^k)$ has denominator $\mathfrak{p}^k$.

First notice that

$$\mu + \rho\alpha^{a-1} \tag{4.34}$$

runs through $N(\mathfrak{p})N(\mathfrak{p}^{a-1}) = N(\mathfrak{p}^a)$ distinct residues mod $\mathfrak{p}^a$ as μ and ρ run through a complete system of residues mod $\mathfrak{p}^{a-1}$ and $\mathfrak{p}$ respectively. Therefore (4.34) runs through a complete system of residues modulo $\mathfrak{p}^a$.

Then,

$$\begin{aligned}\mathbb{g}\left(\frac{\beta}{\alpha^a}\right) &= \sum_{\mu \bmod \mathfrak{p}^{a-1}} \sum_{\rho \bmod \mathfrak{p}} \exp\left\{2\pi i \operatorname{tr}\left(\frac{(\mu+\rho\alpha^{a-1})^2\beta}{\alpha^a}\right)\right\} \\ &= \sum_{\mu \bmod \mathfrak{p}^{a-1}} \left(\exp\left\{2\pi i \operatorname{tr}\left(\frac{\mu^2\beta}{\alpha^a}\right)\right\} \sum_{\rho \bmod \mathfrak{p}} \exp\left\{2\pi i \operatorname{tr}\left(\frac{2\mu\rho\beta}{\alpha}\right)\right\}\right).\end{aligned} \tag{4.35}$$

Consider the sum over ρ. If μ is in $\mathfrak{p}$, then each term is equal to 1, giving a sum of $N(\mathfrak{p})$. Otherwise, we may apply Lemma 4.2.2 so the sum is zero. Therefore we have,

$$\mathbb{g}\left(\frac{\beta}{\alpha^a}\right) = N(\mathfrak{p}) \sum_{\substack{\mu \bmod \mathfrak{p}^{a-1} \\ \mu \equiv 0 \pmod{\mathfrak{p}}}} \exp\left\{2\pi i \operatorname{tr}\left(\frac{\mu^2\beta}{\alpha^a}\right)\right\}. \tag{4.36}$$

However μ running through all residue classes mod $\mathfrak{p}^{a-1}$ such that $\mu \equiv 0 \pmod{\mathfrak{p}}$ is equivalent to $\nu\alpha$ where ν runs through all residue classes mod $\mathfrak{p}^{a-2}$. Indeed, if both run through $N(\mathfrak{p}^{a-1})/N(\mathfrak{p}) = N(\mathfrak{p}^{a-2})$ residue classes. Further more if ν_1, ν_2 are distinct mod $\mathfrak{p}^{a-2}$, ie $\nu_1 - \nu_2 \notin \mathfrak{p}^{a-2}$, then since $\alpha \in \mathfrak{p}/\mathfrak{p}^2$ then $\alpha(\nu_1 - \nu_2) \notin \mathfrak{p}^{a-1}$. Therefore $\nu\alpha$ runs through distinct residue classes mod $\mathfrak{p}^{a-1}$. Therefore,

$$\mathbb{g}\left(\frac{\beta}{\alpha^a}\right) = N(\mathfrak{p}) \sum_{\nu \bmod \mathfrak{p}^{a-2}} \exp\left\{2\pi i \operatorname{tr}\left(\frac{\nu^2\beta}{\alpha^{a-2}}\right)\right\}. \tag{4.37}$$

Therefore the sum on the right hand side of (4.37) is a Gauss sum with denominator $\mathfrak{p}^{a-2}$ giving us the recursion,

$$\mathbb{g}\left(\frac{\beta}{\alpha^a}\right) = N(\mathfrak{p})\mathbb{g}\left(\frac{\beta}{\alpha^{a-2}}\right). \tag{4.38}$$

If a is odd, then applying this recursion as many times as needed allows us to reduce Gauss sums with denominator a power of a prime ideal, to a Gauss sum with denominator a prime ideal. On the other hand, if a is even, then applying this recursion eventfully yields the sum $\mathbb{g}(\beta)$.

Therefore $\mathbb{g}(\beta)$ has denominator 1, so $\mathbb{g}(\beta) = 1$. □

4.3.4. *Proof of Theorem 4.3, part (d).* We will now see the connection between Gauss sums and quadratic residues. We begin with a lemma.

Lemma. *Suppose the denominator of $\mathfrak{d}\omega$ is the prime ideal $\mathfrak{p}$. Then,*

$$\mathbb{g}(\omega) = \sum_{\mu\, mod\, \mathfrak{p}} \left[\frac{\mu}{\mathfrak{p}}\right]_2 e^{2\pi i \operatorname{tr}(\mu\omega)}. \tag{4.39}$$

Proof. Applying Lemma 4.2.2 gives us,

$$\sum_{\mu \bmod \mathfrak{p}} \left[\frac{\mu}{\mathfrak{p}}\right]_2 e^{2\pi i \operatorname{tr}(\mu\omega)} = \sum_{\mu \bmod \mathfrak{p}} \left(\left[\frac{\mu}{\mathfrak{p}}\right]_2 + 1\right) e^{2\pi i \operatorname{tr}(\mu\omega)}. \tag{4.40}$$

We have that $\left[\frac{\mu}{\mathfrak{p}}\right]_2 + 1$ is equal to 0 whenever μ is a quadratic non-residue and equal to 1 when μ is in the residue class 0 mod $\mathfrak{p}$. Therefore the sum becomes, for $\nu^2 = \omega$ a quadratic residue,

$$\sum_{\mu \bmod \mathfrak{p}} \left[\frac{\mu}{\mathfrak{p}}\right]_2 e^{2\pi i \operatorname{tr}(\mu\omega)} = 1 + 2 \sum_{\substack{\nu \bmod \mathfrak{p} \\ \left[\frac{\nu}{\mathfrak{p}}\right]_2 = 1}} e^{2\pi i \operatorname{tr}(\nu\omega)} = \sum_{\mu \bmod \mathfrak{p}} e^{2\pi i \operatorname{tr}(\mu^2\omega)}, \tag{4.41}$$

where the last equality of (4.41) follows since each square mod $\mathfrak{p}$ except 0 occurs exactly twice. The lemma is proved as the last sum is $\mathbb{g}(\omega)$. □

To prove part (d) of Theorem 4.3, we consider first the case when the denominator of $\mathfrak{d}\omega$ is a prime ideal. Replacing ω with $\chi\omega$ for some integer $\chi \in \mathscr{O}_K$ relatively prime to $\mathfrak{p}$ in Lemma 4.3.4 gives,

$$\mathbb{g}(\chi\omega) = \sum_{\mu \bmod \mathfrak{p}} \left[\frac{\mu}{\mathfrak{p}}\right]_2 e^{2\pi i \operatorname{tr}(\chi\mu\omega)}, \tag{4.42}$$

and multiplying by $1 = \left[\frac{\chi^2}{\mathfrak{p}}\right]_2$ gives,

$$\mathbb{g}(\chi\omega) = \left[\frac{\chi}{\mathfrak{p}}\right]_2 \sum_{\mu \bmod \mathfrak{p}} \left[\frac{\chi\mu}{\mathfrak{p}}\right]_2 e^{2\pi i \operatorname{tr}(\chi\mu\omega)}. \tag{4.43}$$

However the sum on the right hand side of (4.43) is invariant under the action of changing μ to $\chi\mu$ for χ relatively prime with $\mathfrak{p}$. Therefore,

$$\mathbb{g}(\chi\omega) = \left[\frac{\chi}{\mathfrak{p}}\right]_2 \sum_{\mu \bmod \mathfrak{p}} \left[\frac{\mu}{\mathfrak{p}}\right]_2 e^{2\pi i \operatorname{tr}(\mu\omega)} = \left[\frac{\chi}{\mathfrak{p}}\right]_2 \mathbb{g}(\omega), \tag{4.44}$$

which proves part (d) when $\mathfrak{a}$ is prime. To prove part (d) when $\mathfrak{a}$ is a prime power $\mathfrak{p}^a$, we will apply part (c) of Theorem 4.3. If a is even, then

$$\left[\frac{\chi}{\mathfrak{p}^a}\right]_2 = \left[\frac{\chi}{\mathfrak{p}}\right]_2^a = 1, \tag{4.45}$$

and by part (c) we have $\mathbb{g}(\chi\omega) = \mathbb{g}(\omega)$. On the other hand, if a is odd, then

$$\left[\frac{\chi}{\mathfrak{p}^a}\right]_2 = \left[\frac{\chi}{\mathfrak{p}}\right]_2^a = \left[\frac{\chi}{\mathfrak{p}}\right]_2. \tag{4.46}$$

By part (c) where $\omega = \beta/\alpha^a$,

$$\mathbb{g}\left(\frac{\beta}{\alpha^a}\right) = N(\mathfrak{p})^{(a-1)/2} \mathbb{g}\left(\frac{\beta}{\alpha^a}\right) \tag{4.47}$$

and

$$\begin{aligned}\mathfrak{g}\left(\frac{\chi\beta}{\alpha^a}\right) &= N(\mathfrak{p})^{(a-1)/2}\mathfrak{g}\left(\frac{\chi\beta}{\alpha}\right) \\ &= N(\mathfrak{p})^{(a-1)/2}\left[\frac{\chi}{\mathfrak{p}}\right]_2\mathfrak{g}\left(\frac{\beta}{\alpha}\right) \\ &= \left[\frac{\chi}{\mathfrak{p}}\right]_2\mathfrak{g}\left(\frac{\beta}{\alpha^a}\right).\end{aligned} \tag{4.48}$$

Hence part (d) holds for when the denominator of $\mathfrak{g}(\omega)$ is a prime power. Applying part (b) of Theorem 4.3 proves part (d) for all odd denominators. □

4.3.5. *Proof of Theorem 4.3, part (f).* We will assume property (e). First, we need a lemma.

Lemma. *Given two numbers $\omega_1, \omega_2 \in K$ such that the denominator of $\mathfrak{d}\omega_1$ is equal to the denominator of $\mathfrak{d}\omega_2$, there exists some $\nu \in \mathscr{O}_K$ such that $\mathfrak{d}(\nu\omega_1 - \omega_2)$ is an ideal.*

Proof. We may write write

$$(\omega_1) = \frac{\mathfrak{b}_1}{\mathfrak{a}\mathfrak{d}}, \qquad (\omega_2) = \frac{\mathfrak{b}_2}{\mathfrak{a}\mathfrak{d}}, \tag{4.49}$$

where $(\mathfrak{a}, \mathfrak{b}_1) = 1$ and $(\mathfrak{a}, \mathfrak{b}_2) = 1$. By Lemma 3.3.7 we may find an ideal $\mathfrak{c}$ such that

$$\mathfrak{c}\mathfrak{a}\mathfrak{d} = (\xi) \quad \text{for } \xi \in \mathscr{O}_K, \tag{4.50}$$

so we obtain the ideals,

$$\omega_1\xi = \mathfrak{b}_1\mathfrak{c}, \tag{4.51}$$

$$\omega_2\xi = \mathfrak{b}_2\mathfrak{c}, \tag{4.52}$$

and

$$\xi\mathfrak{d}^{-1} = \mathfrak{a}\mathfrak{c}. \tag{4.53}$$

By (4.51) and (4.53) and since $\mathfrak{b}_1$ and $\mathfrak{a}$ are relatively prime,

$$(\omega_1\xi) + \xi\mathfrak{d}^{-1} = \mathfrak{c}. \tag{4.54}$$

Therefore, since $\omega_2\xi \in \mathfrak{c}$ by (4.52), there exists $\nu \in \mathscr{O}_K$ and $\delta \in \mathfrak{d}^{-1}$ such that

$$\nu\omega_1\xi + \delta\xi = \omega_2\xi. \tag{4.55}$$

Cancelling ξ from both sides yields

$$\nu\omega_1 - \omega_2 = -\delta \in \mathfrak{d}^{-1}. \tag{4.56}$$

Therefore by (3.13) any number in $\mathfrak{d}(\nu\omega_1 - \omega_2)$ is in $\mathscr{O}_K$. □

Corollary. *Let $\mathbb{g}(\omega)$ have denominator $\mathfrak{a}$. Then all other Gauss sums with denominator $\mathfrak{a}$ must be in the form $\mathbb{g}(\nu\omega)$ for some $\nu \in \mathscr{O}_K$.*

Proof. If $\mathbb{g}(\omega')$ also belongs to the denominator $\mathfrak{a}$, then by Lemma 4.3.5 we may take an integer $\nu \in \mathscr{O}_K$ such that

$$\mathfrak{d}(\nu\omega - \omega') \quad \text{is an ideal.} \tag{4.57}$$

Therefore, for any $\mu \in \mathscr{O}_K$,

$$\operatorname{tr}(\mu^2\nu\omega) - \operatorname{tr}(\mu^2\omega') = \operatorname{tr}(\mu^2(\nu\omega - \omega')) \in \mathbb{Z} \tag{4.58}$$

which gives us that,

$$e^{2\pi i \operatorname{tr}(\mu^2\nu\omega)} = e^{2\pi i \operatorname{tr}(\mu^2\omega')}, \tag{4.59}$$

or that $\mathbb{g}(\nu\omega) = \mathbb{g}(\omega')$. □

Remark. *In Corollary* (4.3.5), *ν must be relatively prime to $\mathfrak{a}$. Indeed, if ν was not relatively prime to $\mathfrak{a}$, then $\mathbb{g}(\nu\omega)$ and $\mathbb{g}(\omega)$ would not belong to the same denominator.*

We will now show that Gauss sums of odd denominator or denominator 4 are nonzero.

Proof. We will show that Gauss sums of odd denominator are nonzero first. Let $\mathbb{g}(\omega)$ have odd denominator $\mathfrak{a}$. From Corollary 4.3.5 we know every Gauss sum of odd denominator $\mathfrak{a}$ may be written in the form $\mathbb{g}(\nu\omega)$ for $\nu \in \mathscr{O}_K$ and by Theorem 4.17 we know that $\mathbb{g}(\nu\omega)$ differs from $\mathbb{g}(\omega)$ by a factor of ± 1, so it suffices to show that just one Gauss sum with denominator $\mathfrak{a}$ is nonzero.

By Proposition 3.3.7 we may take an ideal $\mathfrak{c}$ such that $\mathfrak{a}\mathfrak{d}\mathfrak{c} = \chi$ for $\chi \in \mathscr{O}_K$ with $\mathfrak{c}$ relatively prime to $2\mathfrak{a}$. Now by (4.14) we can write the sum $\mathbb{g}(1/4\chi)$ as the product of the three Gauss sums with denominators 4, $\mathfrak{a}$ and $\mathfrak{c}$ as the ideals $(4), \mathfrak{a}, \mathfrak{c}$ are pairwise relatively prime. To show that some Gauss sum with denominator $\mathfrak{a}$ is nonzero, it therefore suffices to show that $\mathbb{g}(1/4\chi)$ is nonzero. If we let $\omega = 1/4\chi$ then by part (e) we see that, where $\gamma \in K$ is such that $\mathfrak{d}\gamma$ is an ideal relatively prime to the denominator of $\mathfrak{a}/4\mathfrak{b} = \mathfrak{a}/4$,

$$\mathbb{g}\left(\frac{1}{4\chi}\right) = \left|\frac{\sqrt{N(2\mathfrak{b})N(\mathfrak{a})}}{N(\mathfrak{b}_1)}\right| e^{(\pi i/4)\operatorname{tr}(\mathsf{sgn}\,\omega)} \mathbb{g}\left(\frac{-\gamma^2\chi}{1}\right) \tag{4.60}$$

which is clearly non-zero since the Gauss sum on the right hand side has denominator 1, and hence is equal to 1. This proves Gauss sums of odd denominator are non-zero.

For Gauss sums of denominator 4, by Proposition 3.3.7 we may find an odd ideal $\mathfrak{a}$ (i.e. relatively prime to 2) such that

$$\mathfrak{a}\mathfrak{d} = (\chi) \quad \text{for } \chi \in \mathscr{O}_K. \tag{4.61}$$

Let $\mu \in \mathscr{O}_K$ be an arbitrary odd integer, then

$$\mathfrak{d}\frac{1}{\mu\chi} = \frac{1}{\mu\mathfrak{a}} \tag{4.62}$$

Since $\mu\mathfrak{a}$ is odd, and since Gauss sums of odd denominator are non-zero, we have $\mathfrak{g}(1/\mu\chi)$ is nonzero. Therefore applying part (e) (with γ as in the statement) we get that

$$\mathfrak{g}(-\gamma^2\chi\mu/4) \neq 0. \tag{4.63}$$

Claim. $\mathfrak{d}\gamma$ *is an odd ideal.*

Proof. Let

$$\mathfrak{d}\frac{1}{\mu\chi} = \frac{\mathfrak{b}'}{\mathfrak{a}'} \quad \text{where } \mathfrak{a}' \text{ and } \mathfrak{b}' \text{ are relatively prime ideals.}$$

By (4.62), $\mathfrak{a}'$ is odd. Therefore the denominator of $\frac{\mathfrak{a}'}{4\mathfrak{b}'}$ is $4\mathfrak{b}'$. From part (e) $\gamma \in K$ is an arbitrary number such that $\mathfrak{d}\gamma$ is an ideal relatively prime to denominator of $\frac{\mathfrak{a}'}{4\mathfrak{b}'}$, ie $4\mathfrak{b}'$. □

Using (4.61), the ideal

$$\frac{\mathfrak{d}\gamma^2\chi}{4} = \frac{\mathfrak{d}^2\gamma^2\mathfrak{a}}{4} = \frac{(\mathfrak{d}\gamma)^2\mathfrak{a}}{4}, \tag{4.64}$$

has an odd numerator from claim 4.3.5, hence has denominator 4. Take $\varphi \in K$ such that $\mathfrak{d}\varphi$ has denominator 4. Therefore by Corollary 4.3.5 there exists an integer $\mu \in \mathscr{O}_K$ (with remark 4.3.5 to ensure μ is odd) such that

$$\mathfrak{g}(\varphi) = \mathfrak{g}\left(\frac{-\gamma^2\chi\mu}{4}\right), \tag{4.65}$$

which is non-zero from (4.63). □

4.4 The Law of Quadratic Reciprocity

4.4.1. We will introduce the law of quadratic reciprocity. First we will define for $\alpha,\beta) \in K$,

$$v(\alpha,\beta) := (-1)^{\sum_{p=1}^{r_1}((\operatorname{sgn}\alpha^{(p)}-1)/2(\operatorname{sgn}\beta^{(p)}-1))/2}. \tag{4.66}$$

Theorem. *Let $\alpha,\beta \in \mathscr{O}_K$ be odd relatively prime integers. Then,*

A. (Quadratic Reciprocity)

For any $\omega \in K$ such that $\mathfrak{d}\omega$ is an ideal relatively prime to $\alpha\beta$ then,

$$\left[\frac{\alpha}{\beta}\right]_2 \cdot \left[\frac{\beta}{\alpha}\right]_2 = v(\alpha,\beta)\frac{\mathfrak{g}\left(\frac{-\omega\alpha}{4}\right)\mathfrak{g}\left(\frac{-\omega\beta}{4}\right)}{\mathfrak{g}\left(\frac{-\omega\alpha\beta}{4}\right)\mathfrak{g}\left(\frac{-\omega}{4}\right)}. \tag{4.67}$$

B. (Corollary of Quadratic Reciprocity)

If at least one of α or β is is odd and congruent to the square of a number in K modulo 4 then,

$$\left[\frac{\alpha}{\beta}\right]_2 \cdot \left[\frac{\beta}{\alpha}\right]_2 = v(\alpha, \beta)\,. \tag{4.68}$$

C. *(Supplement to Quadratic Reciprocity)*

Let $\lambda \in \mathscr{O}_K$ be even and $\alpha \in \mathscr{O}_K$ an odd integer relatively prime to λ. Then for any $\omega \in K$ such that $\mathfrak{d}\omega$ is an odd ideal we have,

$$\left[\frac{\lambda}{\alpha}\right]_2 = v(\alpha, \lambda) \frac{\mathfrak{g}\left(\frac{-\omega\alpha}{4\lambda}\right)\mathfrak{g}\left(\frac{-\omega}{4}\right)}{\mathfrak{g}\left(\frac{-\omega}{4\lambda}\right)\mathfrak{g}\left(\frac{-\omega\alpha}{4}\right)}\,. \tag{4.69}$$

4.4.2. To prove part part A of the law of quadratic reciprocity, (4.67), we will need some preliminary calculations.

Lemma. *Let $\alpha, \beta \in \mathscr{O}_K$ be relatively prime odd integers. and $\omega \in K$ such that*

$$\omega = \frac{\mathfrak{b}}{\mathfrak{d}} \tag{4.70}$$

where $\mathfrak{b}$ is an ideal relatively prime to $\alpha\beta$. Then,

(a) With $\alpha, \beta \in \mathscr{O}_K$ relatively prime and odd, and ω as in (4.70)*,*

$$\left[\frac{\alpha}{\beta}\right]_2 \left[\frac{\beta}{\alpha}\right]_2 = \frac{\mathfrak{g}\left(\frac{\omega}{\alpha}\right)\mathfrak{g}\left(\frac{\omega}{\beta}\right)}{\mathfrak{g}\left(\frac{\omega}{\alpha\beta}\right)}\,. \tag{4.71}$$

(b) With γ as in part (d) of Theorem 4.3 and $v(\alpha, \beta)$ as in (4.66)*,*

$$\frac{\mathfrak{g}\left(\frac{\omega}{\alpha}\right)\mathfrak{g}\left(\frac{\omega}{\beta}\right)}{\mathfrak{g}\left(\frac{\omega}{\alpha\beta}\right)} = v(\alpha, \beta) \frac{\mathfrak{g}\left(-\frac{\gamma^2\alpha}{4\omega}\right)\mathfrak{g}\left(-\frac{\gamma^2\beta}{4\omega}\right)}{\mathfrak{g}\left(-\frac{\gamma^2\alpha\beta}{4\omega}\right)\mathfrak{g}\left(-\frac{\gamma^2}{4\omega}\right)}\,. \tag{4.72}$$

(c) With $\mu \in \mathfrak{b}$ odd and $\chi = \mu\gamma^2\frac{1}{\omega}$,

$$\frac{\mathfrak{g}\left(-\frac{\gamma^2\alpha}{4\omega}\right)\mathfrak{g}\left(-\frac{\gamma^2\beta}{4\omega}\right)}{\mathfrak{g}\left(-\frac{\gamma^2\alpha\beta}{4\omega}\right)\mathfrak{g}\left(-\frac{\gamma^2}{4\omega}\right)} = \frac{\mathfrak{g}\left(\frac{-\chi\mu\alpha}{4}\right)\mathfrak{g}\left(\frac{-\chi\mu\beta}{4}\right)}{\mathfrak{g}\left(\frac{-\chi\mu\alpha\beta}{4}\right)\mathfrak{g}\left(\frac{-\chi\mu}{4}\right)}\,. \tag{4.73}$$

Proof. For part (a), by (4.14) and Theorem 4.17 we have

$$\mathbb{g}\left(\frac{\omega}{\alpha\beta}\right) = \mathbb{g}\left(\frac{\beta\omega}{\alpha}\right)\mathbb{g}\left(\frac{\alpha\omega}{\beta}\right) = \left[\frac{\alpha}{\beta}\right]_2\left[\frac{\beta}{\alpha}\right]_2\mathbb{g}\left(\frac{\omega}{\alpha}\right)\mathbb{g}\left(\frac{\omega}{\beta}\right), \tag{4.74}$$

so that,

$$\left[\frac{\alpha}{\beta}\right]_2\left[\frac{\beta}{\alpha}\right]_2 = \frac{\mathbb{g}\left(\frac{\omega}{\alpha}\right)\mathbb{g}\left(\frac{\omega}{\beta}\right)}{\mathbb{g}\left(\frac{\omega}{\alpha\beta}\right)}, \tag{4.75}$$

proving part (a) (4.71). While this does give a representation for the law of quadratic reciprocity, the problem is that these Gauss sums have variable denominators, ie the denominators depend on α, β. This makes it very difficult to produce a concrete formula. Hence we will apply various identities of Gauss sums to reduce the denominator, as shown in parts (b) and (c).

For part (b), consider the sum $\mathbb{g}(\omega/\alpha)$ with ω as in (4.70). The denominator of $\mathbb{g}(\omega/\alpha)$ is the principal ideal (α). Also, since α is odd and relatively prime to $\mathfrak{b}$, then the denominator of $\frac{\alpha}{4\mathfrak{b}}$ is $4\mathfrak{b}$. Therefore, with $\mathfrak{b}_1$ as in part (d) of Theorem 4.3, we have

$$\mathfrak{b}_1 = 4\mathfrak{b}. \tag{4.76}$$

Therefore,

$$\frac{\sqrt{N(2\mathfrak{b})}}{N(\mathfrak{b}_1)} = \frac{\sqrt{N(2\mathfrak{b})}}{N(4\mathfrak{b})} = \frac{1}{\sqrt{N(8\mathfrak{b})}}. \tag{4.77}$$

Therefore applying part (d) of Theorem 4.3 to $\mathbb{g}(\omega/\alpha)$ (with $\gamma \in K$ an arbitrary number such that $\mathfrak{d}\gamma$ is relatively prime to the denominator of $\frac{\mathfrak{d}\omega}{4\alpha}$) gives,

$$\mathbb{g}\left(\frac{\omega}{\alpha}\right) = \left|\frac{\sqrt{N(\alpha)}}{\sqrt{N(8\mathfrak{b})}}\right| e^{(\pi i/4)\,\mathrm{tr}(\mathsf{sgn}\,\omega\alpha)}\mathbb{g}\left(-\frac{\gamma^2\alpha}{4\omega}\right), \tag{4.78}$$

where we used $\mathsf{sgn}\,(\omega/\alpha) = \mathsf{sgn}\,(\omega\alpha)$. We can see the argument is identical if we replace α with β or $\alpha\beta$. Now if we apply this to the Gauss sums in (4.71) we obtain,

$$\frac{\mathbb{g}\left(\frac{\omega}{\alpha}\right)\mathbb{g}\left(\frac{\omega}{\beta}\right)}{\mathbb{g}\left(\frac{\omega}{\alpha\beta}\right)} = \frac{1}{|\sqrt{N(8\mathfrak{b})}|}\frac{\mathbb{g}\left(-\frac{\gamma^2\alpha}{4\omega}\right)\mathbb{g}\left(-\frac{\gamma^2\beta}{4\omega}\right)}{\mathbb{g}\left(-\frac{\gamma^2\alpha\beta}{4\omega}\right)} \cdot e^{(\pi i/4)\,\mathrm{tr}(\mathsf{sgn}\,\omega\alpha+\mathsf{sgn}\,\omega\beta-\mathsf{sgn}\,\omega\alpha\beta)} \tag{4.79}$$

If we were to set $\alpha = 1$ in (4.78) we obtain,

$$\mathbb{g}(\omega) = \left|\frac{1}{\sqrt{N(8\mathfrak{b})}}\right| e^{(\pi i/4)\,\mathrm{tr}(\mathsf{sgn}\,\omega)}\mathbb{g}\left(-\frac{\gamma^2}{4\omega}\right). \tag{4.80}$$

However since $\mathbb{g}(\omega)$ has denominator 1, then $\mathbb{g}(\omega) = 1$, therefore,

$$\sqrt{N(8\mathfrak{b})} = e^{(\pi i/4)\,\mathrm{tr}(\mathsf{sgn}\,\omega)}\mathbb{g}\left(-\frac{\gamma^2}{4\omega}\right). \tag{4.81}$$

Putting this into (4.79) yields,

$$\frac{\mathbb{g}\left(\frac{\omega}{\alpha}\right)\mathbb{g}\left(\frac{\omega}{\beta}\right)}{\mathbb{g}\left(\frac{\omega}{\alpha\beta}\right)} = \frac{\mathbb{g}\left(-\frac{\gamma^2\alpha}{4\omega}\right)\mathbb{g}\left(-\frac{\gamma^2\beta}{4\omega}\right)}{\mathbb{g}\left(-\frac{\gamma^2\alpha\beta}{4\omega}\right)\mathbb{g}\left(-\frac{\gamma^2}{4\omega}\right)} \cdot e^{(\pi i/4)\,\mathrm{tr}(\mathsf{sgn}\,\omega\alpha + \mathsf{sgn}\,\omega\beta - \mathsf{sgn}\,\omega\alpha\beta - \mathsf{sgn}\,\omega)} \tag{4.82}$$

We will simplify the exponential first. Notice,

$$\mathsf{sgn}\,\omega\alpha + \mathsf{sgn}\,\omega\beta - \mathsf{sgn}\,\omega\alpha\beta - \mathsf{sgn}\,\omega = -\mathsf{sgn}\,\omega(\mathsf{sgn}\,\alpha - 1)(\mathsf{sgn}\,\beta - 1). \tag{4.83}$$

Since $(\mathsf{sgn}\,\alpha - 1)$ and $(\mathsf{sgn}\,\beta - 1)$ are each divisible by 2, then

$$\begin{aligned} e^{(\pi i/4)(-\mathsf{sgn}\,\omega^{(p)})(\mathsf{sgn}\,\alpha^{(p)}-1)(\mathsf{sgn}\,\beta^{(p)}-1)} &= e^{(\pi i)(-\mathsf{sgn}\,\omega^{(p)})(\mathsf{sgn}\,\alpha^{(p)}-1)/2(\mathsf{sgn}\,\beta^{(p)}-1)/2} \\ &= (-1)^{(-\mathsf{sgn}\,\omega^{(p)})(\mathsf{sgn}\,\alpha^{(p)}-1)/2(\mathsf{sgn}\,\beta^{(p)}-1)/2}, \end{aligned} \tag{4.84}$$

and because $(-1)^{-\mathsf{sgn}\,\omega} = -1$,

$$e^{(\pi i/4)(-\mathsf{sgn}\,\omega^{(p)})(\mathsf{sgn}\,\alpha^{(p)}-1)(\mathsf{sgn}\,\beta^{(p)}-1)} = (-1)^{(\mathsf{sgn}\,\alpha^{(p)}-1)/2(\mathsf{sgn}\,\beta^{(p)}-1)/2}. \tag{4.85}$$

Therefore,

$$e^{(\pi i/4)\,\mathrm{tr}(\mathsf{sgn}\,\omega\alpha + \mathsf{sgn}\,\omega\beta - \mathsf{sgn}\,\omega\alpha\beta - \mathsf{sgn}\,\omega)} = (-1)^{\Sigma_{p=1}^{r_1}((\mathsf{sgn}\,\alpha^{(p)}-1)/2(\mathsf{sgn}\,\beta^{(p)}-1))/2} = v(\alpha,\beta) \tag{4.86}$$

where $v(\alpha,\beta)$ is as in (4.66). This allows us to rewrite (4.82) as,

$$\frac{\mathbb{g}\left(\frac{\omega}{\alpha}\right)\mathbb{g}\left(\frac{\omega}{\beta}\right)}{\mathbb{g}\left(\frac{\omega}{\alpha\beta}\right)} = v(\alpha,\beta)\frac{\mathbb{g}\left(-\frac{\gamma^2\alpha}{4\omega}\right)\mathbb{g}\left(-\frac{\gamma^2\beta}{4\omega}\right)}{\mathbb{g}\left(-\frac{\gamma^2\alpha\beta}{4\omega}\right)\mathbb{g}\left(-\frac{\gamma^2}{4\omega}\right)}, \tag{4.87}$$

proving part (b) (4.72).

For part (c), since γ is as in part (d) of Theorem (4.3), we obtain

$$\mathfrak{d}\gamma = \mathfrak{c} \quad \text{for } \mathfrak{c} \text{ an ideal.} \tag{4.88}$$

Furthermore, since $\mathfrak{b}_1 = 4\mathfrak{b}$ by (4.76), then $\mathfrak{c}$ and $4\mathfrak{b}$ are relatively prime.

Take $\mu \in \mathfrak{b}$ such that μ is odd. By Lemma (3.3.7) we obtain an ideal $\mathfrak{m}$ such that,

$$\mathfrak{b}\mathfrak{m} = \mu\,. \tag{4.89}$$

We define the number χ as,

$$\chi = \mu\frac{\gamma^2}{\omega} \tag{4.90}$$

so by replacing ω, γ, and μ with (4.70), (4.88) and (4.89) respectively,

$$\chi = \mathfrak{b}\mathfrak{m}\frac{\mathfrak{c}^2}{\mathfrak{d}^2}\frac{\mathfrak{d}}{\mathfrak{b}} = \frac{\mathfrak{m}\mathfrak{c}^2}{\mathfrak{d}}\,. \tag{4.91}$$

By (4.90),

$$\mathbb{g}\left(\frac{-\gamma^2\alpha}{4\omega}\right) = \mathbb{g}\left(\frac{-\chi\alpha}{4\mu}\right), \tag{4.92}$$

and by (4.14) we have,

$$\mathbb{g}\left(\frac{-\gamma^2\alpha}{4\omega}\right) = \mathbb{g}\left(\frac{-\chi\mu\alpha}{4}\right)\mathbb{g}\left(\frac{-4\chi\alpha}{\mu}\right). \tag{4.93}$$

By (4.89) and (4.91),

$$\frac{\chi}{\mu} = \frac{\mathfrak{c}^2}{\mathfrak{b}\mathfrak{d}}, \tag{4.94}$$

so $\mathbb{g}(\frac{-4\chi\alpha}{\mu})$ has denominator $\mathfrak{b}$. By applying Theorem 4.17 to $\mathbb{g}(\frac{-4\chi\alpha}{\mu})$ in (4.93),

$$\mathbb{g}\left(\frac{-\gamma^2\alpha}{4\omega}\right) = \left[\frac{\alpha}{\mathfrak{b}}\right]_2\mathbb{g}\left(\frac{-\chi\mu\alpha}{4}\right)\mathbb{g}\left(\frac{-4\chi}{\mu}\right). \tag{4.95}$$

Continuing this idea with α replaced with $1, \beta, \alpha\beta$ gives us,

$$\mathbb{g}\left(\frac{-\gamma^2}{4\omega}\right) = \left[\frac{1}{\mathfrak{b}}\right]_2\mathbb{g}\left(\frac{-\chi\mu}{4}\right)\mathbb{g}\left(\frac{-4\chi}{\mu}\right) \tag{4.96}$$

$$\mathbb{g}\left(\frac{-\gamma^2\beta}{4\omega}\right) = \left[\frac{\beta}{\mathfrak{b}}\right]_2\mathbb{g}\left(\frac{-\chi\mu\beta}{4}\right)\mathbb{g}\left(\frac{-4\chi}{\mu}\right) \tag{4.97}$$

$$\mathbb{g}\left(\frac{-\gamma^2\alpha\beta}{4\omega}\right) = \left[\frac{\alpha\beta}{\mathfrak{b}}\right]_2\mathbb{g}\left(\frac{-\chi\mu\alpha\beta}{4}\right)\mathbb{g}\left(\frac{-4\chi}{\mu}\right). \tag{4.98}$$

This means that,

$$\frac{\mathbb{g}\left(-\frac{\gamma^2\alpha}{4\omega}\right)\mathbb{g}\left(-\frac{\gamma^2\beta}{4\omega}\right)}{\mathbb{g}\left(-\frac{\gamma^2\alpha\beta}{4\omega}\right)\mathbb{g}\left(-\frac{\gamma^2}{4\omega}\right)} = \frac{\mathbb{g}\left(\frac{-\chi\mu\alpha}{4}\right)\mathbb{g}\left(\frac{-\chi\mu\beta}{4}\right)}{\mathbb{g}\left(\frac{-\chi\mu\alpha\beta}{4}\right)\mathbb{g}\left(\frac{-\chi\mu}{4}\right)}, \tag{4.99}$$

which proves (c), (4.73). □

4.4.3. *Proof of Theorem 4.4.1, part (a).*

By the three parts of Lemma 4.4.2 together we obtain,

$$\left[\frac{\alpha}{\beta}\right]_2\left[\frac{\beta}{\alpha}\right]_2 = \nu(\alpha,\beta)\frac{\mathfrak{g}\left(\dfrac{-\chi\mu\alpha}{4}\right)\mathfrak{g}\left(\dfrac{-\chi\mu\beta}{4}\right)}{\mathfrak{g}\left(\dfrac{-\chi\mu\alpha\beta}{4}\right)\mathfrak{g}\left(\dfrac{-\chi\mu}{4}\right)}. \tag{4.100}$$

By (4.89) and (4.91),

$$\mu = \frac{\mathfrak{m}\mathfrak{c}^2}{\mathfrak{d}}\mathfrak{b}\mathfrak{m} = \omega\mathfrak{m}^2\mathfrak{c}^2. \tag{4.101}$$

However, $\mathfrak{m}\mathfrak{c}$ is a principal ideal by (4.88), (4.89) and (4.70)

$$\mathfrak{m}\mathfrak{c} = \mu\gamma\frac{\mathfrak{d}}{\mathfrak{b}} = \frac{\mu\gamma}{\omega}. \tag{4.102}$$

Since $\mathfrak{m}$ and $\mathfrak{c}$ are ideals, $\frac{\mu\gamma}{\omega}$ is equal to some integer $\sigma \in \mathscr{O}_K$. Then by (4.101) gives us

$$\chi\mu = \omega\sigma^2, \tag{4.103}$$

so in (4.100)

$$\left[\frac{\alpha}{\beta}\right]_2\left[\frac{\beta}{\alpha}\right]_2 = \nu(\alpha,\beta)\frac{\mathfrak{g}\left(\dfrac{-\omega\sigma^2\alpha}{4}\right)\mathfrak{g}\left(\dfrac{-\omega\sigma^2\beta}{4}\right)}{\mathfrak{g}\left(\dfrac{-\omega\sigma^2\alpha\beta}{4}\right)\mathfrak{g}\left(\dfrac{-\omega\sigma^2}{4}\right)}. \tag{4.104}$$

Therefore by part (a) of Theorem 4.3, (4.12), we have proved part (a) of Theorem 4.4.1. □

4.4.4. *Proof of Theorem 4.4.1, part (b).*

This part is really just a corollary of part (a). If we make the assumption that one of α or β is odd and congruent to a square modulo 4, say it is α, then by (4.12)

$$\mathfrak{g}\left(\frac{-\omega\alpha\beta}{4}\right) = \mathfrak{g}\left(\frac{-\omega\beta}{4}\right); \quad \mathfrak{g}\left(\frac{-\alpha}{4}\right) = \mathfrak{g}\left(\frac{-1}{4}\right), \tag{4.105}$$

and part(b) of Theorem 4.4.1 has been shown. □

4.4.5. *Proof of Theorem 4.4.1, part (c).*

This supplementary theorem comes from when one of the α or β is no longer odd. Consider any even integer $\lambda \in \mathscr{O}_K$. Let the principal ideal (λ) factor as two ideals $\mathfrak{l}\mathfrak{r}$ where $\mathfrak{r}$ is odd and $\mathfrak{l}$ contains no odd prime factor. Let $\alpha \in \mathscr{O}_K$ be relatively prime to λ and by Corollary 3.3.7 take $\omega \in K$ such that $\mathfrak{d}\omega$ is an ideal relatively prime to $2\alpha\lambda$. Let $\mathfrak{b}$ be this ideal.

By Theorem 4.17 we have,

$$\mathfrak{g}\left(\frac{\lambda\omega}{\alpha}\right) = \left[\frac{\lambda}{\alpha}\right]_2\mathfrak{g}\left(\frac{\omega}{\alpha}\right), \tag{4.106}$$

and applying the reciprocity from part (d) of Theorem 4.3 where again $\mathfrak{b}_1 = 4\mathfrak{b}$ gives

$$\mathfrak{g}\left(\frac{\lambda\omega}{\alpha}\right) = \left|\frac{\sqrt{N(\alpha)}}{\sqrt{N(8\lambda\mathfrak{b})}}\right| e^{(\pi i/4)\,\mathrm{tr}(\mathrm{sgn}\,\lambda\omega\alpha)} \mathfrak{g}\left(\frac{-\gamma^2\alpha}{4\lambda\omega}\right), \tag{4.107}$$

$$\mathfrak{g}\left(\frac{\omega}{\alpha}\right) = \left|\frac{\sqrt{N(\alpha)}}{\sqrt{N(8\mathfrak{b})}}\right| e^{(\pi i/4)\,\mathrm{tr}(\mathrm{sgn}\,\omega\alpha)} \mathfrak{g}\left(\frac{-\gamma^2\alpha}{4\omega}\right). \tag{4.108}$$

Therefore we have

$$\left[\frac{\lambda}{\alpha}\right]_2 = \frac{\mathfrak{g}\left(\frac{\lambda\omega}{\alpha}\right)}{\mathfrak{g}\left(\frac{\omega}{\alpha}\right)} = \frac{\mathfrak{g}\left(\frac{-\gamma^2\alpha}{4\lambda\omega}\right)}{\mathfrak{g}\left(\frac{-\gamma^2\alpha}{4\omega}\right)} \frac{e^{(\pi i/4)\,\mathrm{tr}(\mathrm{sgn}\,\lambda\omega\alpha - \mathrm{sgn}\,\omega\alpha)}}{|\sqrt{N(\lambda)}|}. \tag{4.109}$$

The problem with this simplification is that the denominator of the Gauss sums is dependant on α, so it is hard to obtain a precise representation of the supplementary law. To remove the variable Gauss sum denominator of (4.109), we specialize for $\alpha = 1$ to obtain,

$$1 = \frac{\mathfrak{g}\left(\frac{-\gamma^2}{4\lambda\omega}\right)}{\mathfrak{g}\left(\frac{-\gamma^2}{4\omega}\right)} \frac{e^{(\pi i/4)\,\mathrm{tr}(\mathrm{sgn}\,\lambda\omega - \mathrm{sgn}\,\omega)}}{|\sqrt{N(\lambda)}|}. \tag{4.110}$$

By taking $\mu \in \mathfrak{b}$ odd and the number χ as,

$$\chi = \mu\frac{\gamma^2}{\omega}, \tag{4.111}$$

By the same method as we obtained (4.95),

$$\mathfrak{g}\left(\frac{-\gamma^2\alpha}{4\omega}\right) = \left[\frac{\alpha}{\mathfrak{b}}\right]_2 \mathfrak{g}\left(\frac{-\chi\mu\alpha}{4}\right) \mathfrak{g}\left(\frac{-4\chi}{\mu}\right). \tag{4.112}$$

And using the same method as for (4.95), but with 4 replaced with 4λ,

$$\mathfrak{g}\left(\frac{-\gamma^2\alpha}{4\omega\lambda}\right) = \left[\frac{\alpha}{\mathfrak{b}}\right]_2 \mathfrak{g}\left(\frac{-\chi\mu\alpha}{4\lambda}\right) \mathfrak{g}\left(\frac{-4\lambda\chi}{\mu}\right). \tag{4.113}$$

Dividing sums (4.112) and (4.113) when $\alpha = 1$ gives

$$\frac{\mathfrak{g}\left(\frac{-\gamma^2}{4\omega\lambda}\right)}{\mathfrak{g}\left(\frac{-\gamma^2}{4\omega}\right)} = \frac{\mathfrak{g}\left(\frac{-\chi\mu}{4\lambda}\right)\mathfrak{g}\left(\frac{-4\lambda\chi}{\mu}\right)}{\mathfrak{g}\left(\frac{-\chi\mu}{4}\right)\mathfrak{g}\left(\frac{-4\chi}{\mu}\right)}, \tag{4.114}$$

so dividing sums (4.112) and (4.113) for arbitrary α yields,

$$\frac{\mathbb{g}\left(\frac{-\gamma^2\alpha}{4\omega\lambda}\right)}{\mathbb{g}\left(\frac{-\gamma^2\alpha}{4\omega}\right)} = \frac{\mathbb{g}\left(\frac{-\chi\mu\alpha}{4\lambda}\right)\mathbb{g}\left(\frac{-4\lambda\chi}{\mu}\right)}{\mathbb{g}\left(\frac{-\chi\mu\alpha}{4}\right)\mathbb{g}\left(\frac{-4\chi}{\mu}\right)}. \tag{4.115}$$

Subbing (4.114) into the right hand side of (4.115) yeilds,

$$\frac{\mathbb{g}\left(\frac{-\gamma^2\alpha}{4\omega\lambda}\right)}{\mathbb{g}\left(\frac{-\gamma^2\alpha}{4\omega}\right)} = \frac{\mathbb{g}\left(\frac{-\chi\mu\alpha}{4\lambda}\right)}{\mathbb{g}\left(\frac{-\chi\mu\alpha}{4}\right)} \cdot \frac{\mathbb{g}\left(\frac{-\gamma^2}{4\omega\lambda}\right)\mathbb{g}\left(\frac{-\chi\mu}{4}\right)}{\mathbb{g}\left(\frac{-\gamma^2}{4\omega}\right)\mathbb{g}\left(\frac{-\chi\mu}{4\lambda}\right)}. \tag{4.116}$$

Since $\chi\mu = \omega\sigma^2$ then the right hand side of (4.116) becomes,

$$\frac{\mathbb{g}\left(\frac{-\gamma^2\alpha}{4\omega\lambda}\right)}{\mathbb{g}\left(\frac{-\gamma^2\alpha}{4\omega}\right)} = \frac{\mathbb{g}\left(\frac{-\omega\alpha}{4\lambda}\right)\mathbb{g}\left(\frac{-\gamma^2}{4\omega\lambda}\right)\mathbb{g}\left(\frac{-\omega}{4}\right)}{\mathbb{g}\left(\frac{-\omega\alpha}{4}\right)\mathbb{g}\left(\frac{-\gamma^2}{4\omega}\right)\mathbb{g}\left(\frac{-\omega}{4\lambda}\right)}, \tag{4.117}$$

and finally dividing by (4.110) gives us,

$$\frac{\mathbb{g}\left(\frac{-\gamma^2\alpha}{4\omega\lambda}\right)}{\mathbb{g}\left(\frac{-\gamma^2\alpha}{4\omega}\right)} = \frac{\mathbb{g}\left(\frac{-\omega\alpha}{4\lambda}\right)\mathbb{g}\left(\frac{-\omega}{4}\right)}{\mathbb{g}\left(\frac{-\omega\alpha}{4}\right)\mathbb{g}\left(\frac{-\omega}{4\lambda}\right)} \frac{|\sqrt{N(\lambda)}|}{e^{(\pi i/4)\operatorname{tr}(\operatorname{sgn}\lambda\,\omega - \operatorname{sgn}\omega)}}. \tag{4.118}$$

Subbing (4.118) into (4.109) gives us the final result. □

4.5 The Law of Quadratic Reciprocity for Rational Integers

In this section we will show that we may obtain the familiar quadratic reciprocity for the rational integers.

4.5.1. Let $K = \mathbb{Q}$. We know here the ring of integers $\mathscr{O}_K = \mathbb{Z}$ a principal ideal domain. Suppose α and β are both positive odd rational primes. Since they are positive, we always have $\operatorname{sgn}\alpha = \operatorname{sgn}\beta = 1$. In the rationals $r_1 = 1$ and $r_2 = 0$ as in (3.4) so,

$$(-1)^{\sum_{p=1}^{r_1}((\operatorname{sgn}\alpha^{(p)}-1)/2)((\operatorname{sgn}\beta^{(p)}-1)/2)} = 1 \tag{4.119}$$

for any α and β. Furthermore, an integer is odd and congruent to a square modulo 4 if and only if it is congruent to 1 (mod 4). If we assume at least one of α or β is odd and congruent toto a square modulo 4, then by (4.69) ,

$$\left[\frac{\alpha}{\beta}\right]_2 \cdot \left[\frac{\beta}{\alpha}\right]_2 = (-1)^0 = 1\,. \tag{4.120}$$

It is left to consider when both α and β are not congruent to a square modulo 4, i.e. congruent to 3 (mod 4). Since we know that $\mathfrak{d} = \mathbb{Z}$ for the rational integers. This means that (4.67) reduces to,

$$\left[\frac{\alpha}{\beta}\right]_2 \cdot \left[\frac{\beta}{\alpha}\right]_2 = \frac{\mathfrak{g}\left(\frac{\alpha}{4}\right)\mathfrak{g}\left(\frac{\beta}{4}\right)}{\mathfrak{g}\left(\frac{1}{4}\right)\mathfrak{g}\left(\frac{\alpha\beta}{4}\right)}\,. \tag{4.121}$$

To evaluate these Gauss sums we apply the following formula for a,b relatively prime rational integers, [3, pg.15,26],

$$\mathfrak{g}\left(\frac{a}{b}\right) = \sum_{\mu=0}^{b-1} e^{2\pi i\mu^2 a/b} = \begin{cases} 0 & \text{if } b \equiv 2 \pmod 4 \\ \varepsilon_b\sqrt{b}\left(\frac{a}{b}\right) & \text{if } b \text{ is odd} \\ (1+i)\varepsilon_a^{-1}\sqrt{b}\left(\frac{b}{a}\right) & \text{if } a \text{ is odd, } 4|b\,, \end{cases} \tag{4.122}$$

where,

$$\varepsilon_m = \begin{cases} 1 & \text{if } m \equiv 1 \pmod 4 \\ i & \text{if } m \equiv 3 \pmod 4\,, \end{cases} \tag{4.123}$$

and

$$\left(\frac{a}{b}\right) \quad \text{is the legendre symbol for the rational integers}\,. \tag{4.124}$$

From this we can see that, assuming both α and β are not congruent to a square modulo 4,

$$\left[\frac{\alpha}{\beta}\right]_2 \cdot \left[\frac{\beta}{\alpha}\right]_2 = \frac{(1+i)\sqrt{4}(1+i)\sqrt{4}}{(1+i)\sqrt{4}(-i)(1+i)\sqrt{4}(-i)} = -1\,. \tag{4.125}$$

Putting these two results together gives us the following expression for quadratic reciprocity in the rational integers.

Theorem. ***Rational integers: Quadratic Reciprocity***
Let α and β be odd rational primes. Then,

$$\left[\frac{\alpha}{\beta}\right]_2 \cdot \left[\frac{\beta}{\alpha}\right]_2 = (-1)^{(\alpha-1)/2}(-1)^{(\beta-1)/2}\,, \tag{4.126}$$

4.5.2. The supplementary law can be shown as, taking $\lambda = 2$. If α is an odd rational prime, then by Theorem 6.2.1 we have,

$$\left[\frac{2}{\alpha}\right]_2 = \frac{\mathbb{g}\left(\frac{-\alpha}{8}\right)\mathbb{g}\left(\frac{-1}{4}\right)}{\mathbb{g}\left(\frac{-1}{8}\right)\mathbb{g}\left(\frac{-\alpha}{4}\right)}\,. \tag{4.127}$$

To evaluate $\left[\frac{2}{\alpha}\right]_2$ exactly, We have to consider α mod 8. The easy case is when $\alpha \equiv 1 \pmod 8$. By (4.127),

$$\left[\frac{2}{\alpha}\right]_2 = \frac{\mathbb{g}\left(\frac{-1}{8}\right)\mathbb{g}\left(\frac{-1}{4}\right)}{\mathbb{g}\left(\frac{-1}{8}\right)\mathbb{g}\left(\frac{-1}{4}\right)} = 1\,. \tag{4.128}$$

Since the squares modulo 8 are 0,0,4,4,1,1,1,1 counting multiplicity, we may calculate an arbitrary Gauss sum with denominator 8 as,

$$\mathbb{g}\left(\frac{-\alpha}{8}\right) = 2e^{-2\pi i 0\cdot\alpha/8} + 2e^{-2\pi i 4\alpha/8} + 4e^{-2\pi i\alpha/8}\,. \tag{4.129}$$

So if $\alpha \equiv 7 \pmod 8$ then,

$$\mathbb{g}\left(\frac{-\alpha}{8}\right) = 2 - 2 + 4e^{-\pi i/4} = (1+i)\sqrt{8}\,, \tag{4.130}$$

and if $\alpha \equiv 3 \pmod 8$ then,

$$\mathbb{g}\left(\frac{-\alpha}{8}\right) = 2 - 2 + 4e^{-3\pi i/4} = -(1+i)\sqrt{8}\,, \tag{4.131}$$

and if $\alpha \equiv 5 \pmod 8$ then,

$$\mathbb{g}\left(\frac{-\alpha}{8}\right) = 2 - 2 + 4e^{3\pi i/4} = i(1+i)\sqrt{8}\,. \tag{4.132}$$

Finally, the squares modulo 4 are 0,0,1,1, counting multiplicity, so if $\alpha \equiv 1 \pmod 4$ then,

$$\begin{aligned}\mathbb{g}\left(\frac{-\alpha}{4}\right) &= 2e^{-2\pi i 0\cdot\alpha/4} + 2e^{-2\pi i\alpha/4} \\ &= 2 + 2e^{-\pi i/2} = \sqrt{4}(-i)(1+i)\,,\end{aligned} \tag{4.133}$$

and if $\alpha \equiv 3 \pmod 4$ then,

$$\mathbb{g}\left(\frac{-\alpha}{4}\right) = 2 + 2e^{\pi i/2} = \sqrt{4}(1+i)\,. \tag{4.134}$$

Putting all this together in (4.127) tells us that if $\alpha \equiv 7 \pmod 8$ then,

$$\left[\frac{2}{\alpha}\right]_2 = \frac{(1+i)\sqrt{8}(1+i)(-i)\sqrt{4}}{(1+i)(-i)\sqrt{8}(1+i)\sqrt{4}} = 1\,, \tag{4.135}$$

and if $\alpha \equiv 3 \pmod 8$ then,

$$\left[\frac{2}{\alpha}\right]_2 = \frac{-(1+i)\sqrt{8}(1+i)(-i)\sqrt{4}}{(1+i)(-i)\sqrt{8}(1+i)\sqrt{4}} = -1\,, \tag{4.136}$$

and if $\alpha \equiv 5 \pmod 8$ then,

$$\left[\frac{2}{\alpha}\right]_2 = \frac{i(1+i)\sqrt{8}(1+i)(-i)\sqrt{4}}{(1+i)(-i)\sqrt{8}(-i)(1+i)\sqrt{4}} = -1\,. \tag{4.137}$$

Putting (4.128), (4.135), (4.136) and (4.137) together gives the following supplement to quadratic reciprocity for when 2 is a quadratic residue.

Theorem. ***Rational integers: Quadratic Reciprocity Supplement***
For odd rational integer α,

$$\left[\frac{2}{\alpha}\right]_2 = (-1)^{(\alpha^2-1)/8}\,. \tag{4.138}$$

4.6 The Law of Quadratic Reciprocity for Gaussian Integers

We will compute Gauss sums to quadratic reciprocity for the Gaussian integers in a compact form.

4.6.1. Let $K = \mathbb{Q}[i]$. From 3.6.4 we have the ring of integers $\mathscr{O}_K = \mathbb{Z}[i]$, a principal ideal domain. Since $r_1 = 0$ and $r_2 = 1$ as in (3.4) we have,

$$(-1)^{\sum_{p=1}^{r_1}((\operatorname{sgn}\alpha^{(p)}-1)/2)((\operatorname{sgn}\beta^{(p)}-1)/2)} = 1 \tag{4.139}$$

for any α and β.

If $\alpha = a+bi$ is an odd prime, it suffices to consider it in the form $a+bi$ where a is odd and b is even. Indeed, if both a and b are even, then α is not odd. If both a and b are odd, then by 3.6.4, a^2+b^2 is even, so α divisible by $(1+i)$ which is not odd. If a is even and b odd, then

$$a+bi = i(b-ai)\,, \tag{4.140}$$

so we can instead consider the integer $-i\alpha = b-ai$.

We need to find which of the primes as identified in 3.6.4 are odd and congruent to a square modulo 4. To do this, we check the squares of every element modulo 4,

$$\begin{array}{cccc} (1+i)^2 \equiv 2i & (3+i)^2 \equiv 2i & (2+i)^2 \equiv -1 & i^2 \equiv -1 \\ (1+2i)^2 \equiv 1 & (3+2i)^2 \equiv 1 & (2+2i)^2 \equiv 0 & (2i)^2 \equiv 0 \\ (1+3i)^2 \equiv 2i & (3+3i)^2 \equiv 2i & (2+3i)^2 \equiv -1 & (3i)^2 \equiv -1 \\ 1^2 \equiv 1 & 3^2 \equiv 1 & 2^2 \equiv 0 & (4i)^2 \equiv 0 \end{array} \tag{4.141}$$

which tells us that the only numbers which are odd and congruent to a square modulo 4 in the Gaussian integers are those congruent to 1 or -1 modulo 4.

Let α, β be odd Gaussian Primes. If at least one of them is congruent to 1 or -1 modulo 4, then we have by 4.17,

$$\left[\frac{\alpha}{\beta}\right]_2 \cdot \left[\frac{\beta}{\alpha}\right]_2 = 1\,. \tag{4.142}$$

We have dealt with when at least one of α and β belong to the residue classes 1 or -1 modulo 4 so all that is left is when they both belong to residue classes $1+2i$ or $3+2i$. For this we will have to turn to the Gauss sums.

The different of the Gaussian integers is the ideal $2\mathbb{Z}[i]$. For $\omega\mathfrak{d}$ to be a ideal, relatively prime to $\alpha\beta$, we can take $\omega = \frac{1}{2}$. Then for odd primes α, β we get,

$$\left[\frac{\alpha}{\beta}\right]_2 \cdot \left[\frac{\beta}{\alpha}\right]_2 = \frac{\mathfrak{g}\left(\frac{-\alpha}{8}\right)\mathfrak{g}\left(\frac{-\beta}{8}\right)}{\mathfrak{g}\left(\frac{-\alpha\beta}{8}\right)\mathfrak{g}\left(\frac{-1}{8}\right)}\,. \tag{4.143}$$

Since the different is the principal ideal generated by the number 2, then by (4.7) we can see that the denominator of each of the Gauss sums is the principal ideal generated by the number 4. Therefore we will consider the exponent in the Gauss sum modulo 4.

To evaluate these sums, first notice that the squares of elements modulo 4 computed in (4.141) only take values $0, 1, -1, 2i$. As ν runs through all residue classes modulo 4, then ν^2 runs through each of these squares exactly 4 times.

Therefore, if $\gamma \equiv 1+2i \pmod 4$ or $1 \pmod 4$ then,

$$\begin{aligned} \mathfrak{g}\left(\frac{\gamma}{8}\right) &= 4e^{2\pi i \operatorname{tr}(-\gamma/8)} + 4e^{2\pi i \operatorname{tr}(\gamma/8)} + 4e^{2\pi i \operatorname{tr}(0\cdot\gamma/8)} + 4e^{2\pi i \operatorname{tr}(2i\gamma/8)} = \\ &= 4(e^{-\pi i/2} + e^{\pi i/2} + e^{0} + e^{2\pi i}) = 8\,. \end{aligned} \tag{4.144}$$

Similarly, if $\gamma \equiv 3+2i \pmod 4$ or $3 \pmod 4$ then,

$$\begin{aligned}\mathbb{g}\left(\frac{\gamma}{8}\right) &= 4e^{2\pi i\,\mathrm{tr}(-\gamma/8)} + 4e^{2\pi i\,\mathrm{tr}(\gamma/8)} + 4e^{2\pi i\,\mathrm{tr}(0\cdot\gamma/8)} + 4e^{2\pi i\,\mathrm{tr}(2i\gamma/8)} = \\ &= 4(e^{-3\pi i/2} + e^{3\pi i/2} + e^{0} + e^{2\pi i}) = 8\,.\end{aligned} \tag{4.145}$$

Therefore we get the following reciprocity.

Theorem. ***Gaussian Integers: Quadratic Reciprocity***
If $\alpha = a + bi$ and $\beta = c + di$ where a, c are odd and b, d are even, then

$$\left[\frac{\alpha}{\beta}\right]_2 \cdot \left[\frac{\beta}{\alpha}\right]_2 = 1\,. \tag{4.146}$$

4.6.2. Next compute $\left[\frac{i}{\beta}\right]_2$. Let $\beta = c + di$ where c is odd and $d \equiv 0 \pmod 4$. Take any odd prime α, then by (4.142) since β is odd and congruent to a square modulo 4,

$$\left[\frac{i}{\beta}\right]_2 = \left[\frac{i}{\beta}\right]_2 \left[\frac{\alpha}{\beta}\right]_2 \left[\frac{\beta}{\alpha}\right]_2 = \left[\frac{i\alpha}{\beta}\right]_2 \left[\frac{\beta}{i\alpha}\right]_2 = 1\,. \tag{4.147}$$

On the other hand, let $\beta = c + di$ where c is odd and $d \equiv 2 \pmod 4$. Then by (4.142) for $\alpha = 3$,

$$\left[\frac{i}{\beta}\right]_2 = \left[\frac{i}{\beta}\right]_2 \left[\frac{3}{\beta}\right]_2 \left[\frac{\beta}{3}\right]_2, \tag{4.148}$$

and using that

$$\left[\frac{\beta}{3}\right]_2 = \left[\frac{\beta}{3i}\right]_2, \tag{4.149}$$

we have that

$$\left[\frac{i}{\beta}\right]_2 = \left[\frac{3i}{\beta}\right]_2 \left[\frac{\beta}{3i}\right]_2 = \frac{\mathbb{g}\left(\frac{-3i}{8}\right)\mathbb{g}\left(\frac{-\beta}{8}\right)}{\mathbb{g}\left(\frac{-3i\beta}{8}\right)\mathbb{g}\left(\frac{-1}{8}\right)}\,. \tag{4.150}$$

From (4.144) and (4.145) we have that $\mathbb{g}\left(\frac{-1}{8}\right) = \mathbb{g}\left(\frac{-\beta}{8}\right) = 8$ so it suffices to solve for the remaining two Gauss sums. Using the same idea we have,

$$\begin{aligned}\mathbb{g}\left(\frac{-3i}{8}\right) &= 4(e^{2\pi i\,\mathrm{tr}(-3i/8)} + e^{2\pi i\,\mathrm{tr}(3i/8)} + e^{2\pi i\,\mathrm{tr}(-2i3i/8)} + 1) \\ &= 4(1 + 1 + e^{3\pi i} + 1) \\ &= 8\,,\end{aligned} \tag{4.151}$$

and

$$\begin{aligned}\mathfrak{g}\left(\frac{-3i\beta}{8}\right) &= 4(e^{2\pi i\,\mathrm{tr}(-3i\beta/8)} + e^{2\pi i\,\mathrm{tr}(3i\beta/8)} + e^{2\pi i\,\mathrm{tr}(-2i3i\beta/8)} + 1) \\ &= 4(e^{3\pi i} + e^{-3\pi i} + e^{c\pi i} + 1) \\ &= -8\,.\end{aligned} \tag{4.152}$$

Therefore we have by (4.150)

$$\left[\frac{i}{\beta}\right]_2 = -1\,. \tag{4.153}$$

Putting (4.147) together with (4.153) gives us the following theorem.

Theorem. ***Gaussian Integers: Quadratic Reciprocity Supplement 1***
If $\beta = c + di$ where c is odd and d is even, then,

$$\left[\frac{i}{\beta}\right]_2 = (-1)^{d/2}\,. \tag{4.154}$$

4.6.3. We finally need to handle elements which are not odd, or relatively prime to 2. Since 2 has the decomposition $2 = (1+i)^2$, it suffices to find a method to determine

$$\left[\frac{1+i}{\beta}\right]_2, \quad \text{for } \beta = c + di \text{ where } c \text{ is odd and } d \text{ is even.} \tag{4.155}$$

By (4.69), with $\mathfrak{d} = (2)$ so we may take $\omega = \frac{1}{2}$ and we get,

$$\left[\frac{1+i}{\beta}\right]_2 = \frac{\mathfrak{g}\left(\frac{-\beta}{8(1+i)}\right)\mathfrak{g}\left(\frac{-1}{8}\right)}{\mathfrak{g}\left(\frac{-1}{8(1+i)}\right)\mathfrak{g}\left(\frac{-\beta}{8}\right)}\,. \tag{4.156}$$

Using calculations earlier $g(\frac{-1}{8}) = g(\frac{-\beta}{8})$ so,

$$\left[\frac{1+i}{\beta}\right]_2 = \frac{\mathfrak{g}\left(\frac{-\beta}{8(1+i)}\right)}{\mathfrak{g}\left(\frac{-1}{8(1+i)}\right)}\,, \tag{4.157}$$

which means that we need to evaluate Gauss sums with denominator $4(1+i)$.

Claim. *The set*

$$G = \{a + bi\} \quad \textit{such that } a = 0, 1, \ldots, 7 \textit{ and } b = 0, 1, 2, 3\,, \tag{4.158}$$

runs through a system of residues modulo $4(1+i)$.

Proof. The number of residue classes modulo 4 is $4 \cdot 4 = 16$ and the number of residue classes modulo (1+i) is 2. Therefore the number of residue classes modulo $4(1+i) = 16 \cdot 2 = 32$. The set G has 32 elements, so it suffices to show that each element is distinct modulo $4(1+i)$. First notice that every element in the ideal generated by $4(1+i)$ must be in the form $a+bi$ where either $a \equiv b \equiv 0 \pmod 8$ or $a \equiv b \equiv 4 \pmod 8$. To see this, let $c+di$ be an arbitrary integer. Then $(c+di)(4+4i) = 4(c-d)+4(c+d)i.$ Since $(c-d)$ and $(c+d)$ have the same parity, therefore $4(c-d) \equiv 4(c+d) \equiv 0$ or 4 (mod 8).

Now suppose two distinct elements in G lie in the same residue class modulo $4(1+i)$. Let them be $a+bi$, $c+di$. Then,

$$(a+bi)-(c+di) = (a-c)+(b-d)i \in (4+4i)\,, \tag{4.159}$$

Therefore $a-c \equiv 0,1,2,3,4,5,6,7 \pmod 8$ and $b-d \equiv 0,1,2,3,5,6,7 \pmod 8$. The only way the difference is inside the ideal generated by $4(1+i)$ is if $a-c \equiv b-d \equiv 0 \pmod 8$, however this contradicts the assumption that $a+bi$ and $c+di$ were different. Therefore since no two elements in G lie in the same residue class, we can conclude that G is a complete residue system modulo $4(1+i)$. □

Considering the square of each residue gives us

$$\begin{array}{rrrr}
0^2 \equiv 0 & i^2 \equiv 7 & (2i)^2 \equiv 4 & (3i)^2 \equiv 7 \\
1^2 \equiv 1 & (1+i)^2 \equiv 2i & (1+2i)^2 \equiv 1 & (1+3i)^2 \equiv 6i \\
2^2 \equiv 4 & (2+i)^2 \equiv 7 & (2+2i)^2 \equiv 0 & (2+3i)^2 \equiv 7 \\
3^2 \equiv 1 & (3+i)^2 \equiv 6i & (3+2i)^2 \equiv 1 & (3+3i)^2 \equiv 2i \\
4^2 \equiv 0 & (4+i)^2 \equiv 7 & (4+2i)^2 \equiv 4 & (4+3i)^2 \equiv 7 \\
5^2 \equiv 1 & (5+i)^2 \equiv 2i & (5+2i)^2 \equiv 1 & (5+3i)^2 \equiv 6i \\
6^2 \equiv 4 & (6+i)^2 \equiv 7 & (6+2i)^2 \equiv 0 & (6+3i)^2 \equiv 7 \\
7^2 \equiv 1 & (7+i)^2 \equiv 6i & (7+2i)^2 \equiv 1 & (7+3i)^2 \equiv 2i
\end{array}$$

This means that the squares modulo $4(1+i)$, with multiplicity, are four 0's, four 4's, eight 1's, eight 7's, four 2i's, and four 6i's. Therefore we have that the Gauss sum,

$$\begin{aligned}
\mathfrak{g}\left(\frac{-\beta}{8(1+i)}\right) =& 4+4e^{2\pi i \operatorname{tr}(-4\beta/8(1+i))}+8e^{2\pi i \operatorname{tr}(-\beta/8(1+i))}+8e^{2\pi i \operatorname{tr}(\beta/8(1+i))}+ \\
&+4e^{2\pi i \operatorname{tr}(-2i\beta/8(1+i))}+4e^{2\pi i \operatorname{tr}(-6i\beta/8(1+i))}\,,
\end{aligned} \tag{4.160}$$

and since $\frac{1}{1+i} = \frac{1-i}{2}$ we get,

$$\mathbb{g}\left(\frac{-\beta}{8(1+i)}\right) = 4 + 4e^{\frac{\pi i}{2}\operatorname{tr}(-\beta(1-i))} + 8e^{\frac{\pi i}{8}\operatorname{tr}(-\beta(1-i))} + 8e^{\frac{\pi i}{8}\operatorname{tr}(\beta(1-i))} + \\ + 4e^{\frac{\pi i}{4}\operatorname{tr}(-\beta(1-i))} + 4e^{\frac{\pi i}{4}\operatorname{tr}(\beta(1-i))}. \tag{4.161}$$

Since $8 = 4(1+i) - 4i(1+i) \equiv 0$ and $8i = 4(1+i) + 4i(1+i) \equiv 0$, then for $\beta = c + di$ it suffices to consider c and d modulo 8 in the rationals. Therefore we can compute the Gauss sums as follows.

When $c \equiv \pm 1$ and $d \equiv 0$ modulo 8,

$$\begin{aligned} \mathbb{g}\left(\frac{-\beta}{8(1+i)}\right) &= 4 + 4e^{\frac{\pi i}{2}\operatorname{tr}(-(1-i))} + 8e^{\frac{\pi i}{8}\operatorname{tr}(-(1-i))} + 8e^{\frac{\pi i}{8}\operatorname{tr}((1-i))} + 4e^{\frac{\pi i}{4}\operatorname{tr}(-(1-i))} + 4e^{\frac{\pi i}{4}\operatorname{tr}((1-i))} \\ &= 4 + 4e^{-\pi i} + 8e^{\frac{\pi i}{4}} + 8e^{-\frac{\pi i}{4}} + 4e^{-\frac{\pi i}{2}} + 4e^{\frac{\pi i}{2}} \\ &= 8\sqrt{2} \end{aligned} \tag{4.162}$$

When $c \equiv \pm 3$ and $d \equiv 0$ modulo 8,

$$\begin{aligned} \mathbb{g}\left(\frac{-\beta}{8(1+i)}\right) &= 4 + 4e^{\frac{-3\pi i}{2}\operatorname{tr}((1-i))} + 8e^{\frac{3\pi i}{8}\operatorname{tr}(-(1-i))} + 8e^{\frac{3\pi i}{8}\operatorname{tr}((1-i))} + 4e^{\frac{3\pi i}{4}\operatorname{tr}(-i(1-i))} + 4e^{\frac{3\pi i}{4}\operatorname{tr}(i(1-i))} \\ &= 4 + 4e^{3\pi i} + 8e^{\frac{3\pi i}{4}} + 8e^{-\frac{3\pi i}{4}} + 4e^{-\frac{3\pi i}{2}} + 4e^{\frac{3\pi i}{2}} \\ &= -8\sqrt{2} \end{aligned} \tag{4.163}$$

When $c \equiv 1$ and $d \equiv 2$ modulo 8, then $\beta(1-i) = 3 + i$ so

$$\begin{aligned} \mathbb{g}\left(\frac{-\beta}{8(1+i)}\right) &= 4 + 4e^{\frac{\pi i}{2}\operatorname{tr}((3+i))} + 8e^{\frac{-\pi i}{8}\operatorname{tr}(-(3+i))} + 8e^{\frac{-\pi i}{8}\operatorname{tr}((3+i))} + 4e^{\frac{-\pi i}{4}\operatorname{tr}(-i(3+i))} + 4e^{\frac{-\pi i}{4}\operatorname{tr}(i(3+i))} \\ &= 4 + 4e^{-3\pi i} + 8e^{\frac{-3\pi i}{4}} + 8e^{\frac{3\pi i}{4}} + 4e^{\frac{\pi i}{2}} + 4e^{-\frac{\pi i}{2}} \\ &= -8\sqrt{2} \end{aligned} \tag{4.164}$$

When $c \equiv 3$ and $d \equiv 2$ modulo 8, then $\beta(1-i) = 5 - i$ so

$$\begin{aligned} \mathbb{g}\left(\frac{-\beta}{8(1+i)}\right) &= 4 + 4e^{\frac{\pi i}{2}\operatorname{tr}((5-i))} + 8e^{\frac{-\pi i}{8}\operatorname{tr}(-(5-i))} + 8e^{\frac{-\pi i}{8}\operatorname{tr}((5-i))} + 4e^{\frac{-\pi i}{4}\operatorname{tr}(-i(5-i))} + 4e^{\frac{-\pi i}{4}\operatorname{tr}(i(5-i))} \\ &= 4 + 4e^{-5\pi i} + 8e^{\frac{-5\pi i}{4}} + 8e^{\frac{5\pi i}{4}} + 4e^{\frac{\pi i}{2}} + 4e^{-\frac{\pi i}{2}} \\ &= -8\sqrt{2} \end{aligned} \tag{4.165}$$

When $c \equiv 5$ and $d \equiv 2$ modulo 8, then $\beta(1-i) = 7-3i$ so

$$\begin{aligned} \mathfrak{g}\left(\frac{-\beta}{8(1+i)}\right) &= 4+4e^{\frac{\pi i}{2}\operatorname{tr}((7-3i))}+8e^{\frac{-\pi i}{8}\operatorname{tr}(-(7-3i))}+8e^{\frac{-\pi i}{8}\operatorname{tr}((7-3i))}+4e^{\frac{-\pi i}{4}\operatorname{tr}(-i(7-3i))}+4e^{\frac{-\pi i}{4}\operatorname{tr}(i(7-3i))} \\ &= 4+4e^{-7\pi i}+8e^{\frac{-7\pi i}{4}}+8e^{\frac{7\pi i}{4}}+4e^{\frac{3\pi i}{2}}+4e^{-\frac{3\pi i}{2}} \\ &= 8\sqrt{2} \end{aligned} \tag{4.166}$$

When $c \equiv 7$ and $d \equiv 2$ modulo 8, then $\beta(1-i) = 1+3i$ so

$$\begin{aligned} \mathfrak{g}\left(\frac{-\beta}{8(1+i)}\right) &= 4+4e^{\frac{\pi i}{2}\operatorname{tr}((1+3i))}+8e^{\frac{\pi i}{8}\operatorname{tr}(-(1+3i))}+8e^{\frac{\pi i}{8}\operatorname{tr}((1+3i))}+4e^{\frac{\pi i}{4}\operatorname{tr}(-i(1+3i))}+4e^{\frac{\pi i}{4}\operatorname{tr}(i(1+3i))} \\ &= 4+4e^{\pi i}+8e^{\frac{\pi i}{4}}+8e^{-\frac{\pi i}{4}}+4e^{-\frac{3\pi i}{2}}+4e^{\frac{3\pi i}{2}} \\ &= 8\sqrt{2} \end{aligned} \tag{4.167}$$

From (4.162), (4.166) and (4.167), if $c \equiv \pm 1; d \equiv 0$ or $c \equiv 5,7; d \equiv 2$ we have that $c+d \equiv \pm 1 \pmod 8$. It also means that $g(\frac{-\beta}{8(1+i)}) = 8\sqrt{2}$, therefore,

$$\left[\frac{1+i}{\beta}\right]_2 = \frac{\mathfrak{g}\left(\dfrac{-\beta}{8(1+i)}\right)}{\mathfrak{g}\left(\dfrac{-1}{8(1+i)}\right)} = 1\,. \tag{4.168}$$

On the other hand from (4.163), (4.164) and (4.165), if $c \equiv \pm 3; d \equiv 0$ or $c \equiv 1,3; d \equiv 2$ we have that $c+d \equiv \pm 3 \pmod 8$. Similarly, it means that $g(\frac{-\beta}{8(1+i)}) = -8\sqrt{2}$, therefore,

$$\left[\frac{1+i}{\beta}\right]_2 = \frac{\mathfrak{g}\left(\dfrac{-\beta}{8(1+i)}\right)}{\mathfrak{g}\left(\dfrac{-1}{8(1+i)}\right)} = -1\,. \tag{4.169}$$

Therefore we get the following.

Theorem. ***Gaussian Integers: Quadratic Reciprocity Supplement 2***
For $\beta = c+di$ where c is odd and d is even, we have,

$$\left[\frac{1+i}{\beta}\right]_2 = (-1)^{\frac{(c+d)^2-1}{8}}\,. \tag{4.170}$$

Putting the reciprocity together with supplements 1 and 2 gives us a complete picture for the Gaussian integers. Let $\alpha = a+bi$ and $\beta = c+di$. If a,c are odd and b,d are even we can apply the reciprocity (4.146).

On the other hand, if a is even and b is even then multiplying by $-i$ reverses the parity, and we can use supplement 1 (4.154) as follows,

$$\left[\frac{\alpha}{\beta}\right]_2 = \left[\frac{-i\alpha}{\beta}\right]_2 \left[\frac{i}{\beta}\right]_2 = \left[\frac{-i\alpha}{\beta}\right]_2 (-1)^{d/2}. \tag{4.171}$$

And lastly if a and b have the same parity then either α is not prime so we may factor it, or $\alpha = 1+i$ and we can apply (4.170).

4.7 The Law of Quadratic Reciprocity for the Integers with the square root of 2 adjoined.

We will compute Gauss sums to obtain the law of quadratic reciprocity for the totally real field $\mathbb{Q}[\sqrt{2}]$.

4.7.1. From 3.6.5 integers in $\mathbb{Z}[\sqrt{2}]$ take the form $\alpha = a + b\sqrt{2}$ where $a, b \in \mathbb{Z}$. The conjugate of α will be denoted $\bar{\alpha} = a - b\sqrt{2}$. If a is even, then

$$a + b\sqrt{2} = 2\tilde{a} + b\sqrt{2} = \sqrt{2}(b + \tilde{a}\sqrt{2}), \tag{4.172}$$

so it suffices to consider only for odd a.

We need to find which integers are odd and congruent to a square modulo 4. To do this, we check the squares of every element modulo 4,

$$\begin{array}{rrrr}
(1+\sqrt{2})^2 \equiv 3+2\sqrt{2} & (3+\sqrt{2})^2 \equiv 3+2\sqrt{2} & (2+\sqrt{2})^2 \equiv 2 & \sqrt{2}^2 \equiv 2 \\
(1+2\sqrt{2})^2 \equiv 1 & (3+2\sqrt{2})^2 \equiv 1 & (2+2\sqrt{2})^2 \equiv 0 & (2\sqrt{2})^2 \equiv 0 \\
(1+3\sqrt{2})^2 \equiv 3+2\sqrt{2} & (3+3\sqrt{2})^2 \equiv 3+2\sqrt{2} & (2+3\sqrt{2})^2 \equiv 2 & (3\sqrt{2})^2 \equiv 2 \\
1^2 \equiv 1 & 3^2 \equiv 1 & 2^2 \equiv 0 & 0^2 \equiv 0,
\end{array}$$

which tells us that the only integers odd and congruent to the square modulo 4 are those congruent to 1 or $3+2\sqrt{2}$ modulo 4.

Since $r_1 = 2, r_2 = 0$ we have that

$$(-1)^{\sum_{p=1}^{r_1}((\mathsf{sgn}\,\alpha^{(p)}-1)/2)((\mathsf{sgn}\,\beta^{(p)}-1)/2)} = (-1)^{(\mathsf{sgn}\,\alpha-1)(\mathsf{sgn}\,\beta-1)/4}(-1)^{(\mathsf{sgn}\,\bar{\alpha}-1)(\mathsf{sgn}\,\bar{\beta}-1)/4}. \tag{4.173}$$

Let

$$S = ((\mathsf{sgn}\,\alpha - 1)(\mathsf{sgn}\,\beta - 1) + (\mathsf{sgn}\,\bar{\alpha} - 1)(\mathsf{sgn}\,\bar{\beta} - 1))/4. \tag{4.174}$$

So by (4.68) we have for integers α, β such that α is congruent to 1 or $3+2\sqrt{2}$ modulo 4,

$$\left[\frac{\alpha}{\beta}\right]_2 \cdot \left[\frac{\beta}{\alpha}\right]_2 = (-1)^S. \tag{4.175}$$

From 3.6.5 the different for the number field $\mathbb{Q}(\sqrt{2})$ is the principal ideal $(2\sqrt{2})$, so for $\mathfrak{d}\omega$ to be an ideal relatively prime to $\alpha\beta$, we may take $\omega = \frac{1}{2\sqrt{2}}$. By (4.67) for odd integers α, β we get,

$$\left[\frac{\alpha}{\beta}\right]_2 \cdot \left[\frac{\beta}{\alpha}\right]_2 = (-1)^S \frac{\mathbb{g}\left(\frac{-\alpha}{8\sqrt{2}}\right)\mathbb{g}\left(\frac{-\beta}{8\sqrt{2}}\right)}{\mathbb{g}\left(\frac{-\alpha\beta}{8\sqrt{2}}\right)\mathbb{g}\left(\frac{-1}{8\sqrt{2}}\right)}. \tag{4.176}$$

Since the different is the principal ideal generated by the number $2\sqrt{2}$, then by (4.7) we can see that the denominator of each of the Gauss sums is the principal ideal generated by the number 4. Therefore it suffices to consider each number in the Gauss sum modulo 4.

To evaluate these sums, first notice that the squares of elements modulo 4 only take values $0, 1, 3+2\sqrt{2}, 2$ and more specifically, as v runs through all residue classes modulo 4, then v^2 runs through each of these squares exactly 4 times. Therefore,

$$\begin{aligned} \mathbb{g}\left(\frac{\gamma}{8\sqrt{2}}\right) &= 4e^{2\pi i \operatorname{tr}(0\cdot\gamma/8\sqrt{2})} + 4e^{2\pi i \operatorname{tr}(\gamma/8\sqrt{2})} + 4e^{2\pi i \operatorname{tr}((3+2\sqrt{2})\gamma/8\sqrt{2})} + 4e^{2\pi i \operatorname{tr}(2\gamma/8\sqrt{2})} \\ &= 4(1 + e^{\frac{\pi i}{4}\operatorname{tr}(\gamma/\sqrt{2})} + e^{\frac{\pi i}{4}\operatorname{tr}((3+2\sqrt{2})\gamma/\sqrt{2})} + e^{\frac{\pi i}{4}\operatorname{tr}(2\gamma/\sqrt{2})}), \end{aligned} \tag{4.177}$$

so that,

$$\mathbb{g}\left(\frac{1}{8\sqrt{2}}\right) = 4(1+1+e^{\pi i}+1) = 8, \quad \mathbb{g}\left(\frac{1+\sqrt{2}}{8\sqrt{2}}\right) = 4(1+e^{\pi i/2}+e^{\pi i/2}+e^{\pi i}) = 8i$$

$$\mathbb{g}\left(\frac{1+2\sqrt{2}}{8\sqrt{2}}\right) = 4(1+e^{\pi i}+1+1 = 8, \quad \mathbb{g}\left(\frac{1+3\sqrt{2}}{8\sqrt{2}}\right) = 4(1+e^{-\pi i/2}+e^{-\pi i/2}+e^{\pi i}) = -8i$$

$$\mathbb{g}\left(\frac{3}{8\sqrt{2}}\right) = 4(1+1+e^{\pi i}+1) = 8, \quad \mathbb{g}\left(\frac{3+\sqrt{2}}{8\sqrt{2}}\right) = 4(1+e^{\pi i/2}+e^{\pi i/2}+e^{\pi i}) = 8i$$

$$\mathbb{g}\left(\frac{3+2\sqrt{2}}{8\sqrt{2}}\right) = 4(1+e^{\pi i}+1+1 = 8, \quad \mathbb{g}\left(\frac{3+3\sqrt{2}}{8\sqrt{2}}\right) = 4(1+e^{-\pi i/2}+e^{-\pi i/2}+e^{\pi i}) = -8i$$

which tells us that for $\alpha = a + b\sqrt{2}$ with a odd,

$$\mathfrak{g}\left(\frac{-\alpha}{8\sqrt{2}}\right) = \begin{cases} 8 & \text{if } b \text{ even} \\ -8i & \text{if } b \equiv 1 \pmod 4 \\ 8i & \text{if } b \equiv 3 \pmod 4. \end{cases} \tag{4.178}$$

Theorem. $\mathbb{Z}[\sqrt{2}]$***: Quadratic Reciprocity***
Let $\alpha = a + b\sqrt{2}$ and $\beta = c + d\sqrt{2}$ such that a, c are odd with S as in (4.174). *Then*

(a) if b, d are both even then,

$$\left[\frac{\alpha}{\beta}\right]_2 \cdot \left[\frac{\beta}{\alpha}\right]_2 = (-1)^S. \tag{4.179}$$

(b) if b, d are both odd then,

$$\left[\frac{\alpha}{\beta}\right]_2 \cdot \left[\frac{\beta}{\alpha}\right]_2 = (-1)^{S+\frac{b-d}{2}+1}. \tag{4.180}$$

(c) if b even and d odd then,

$$\left[\frac{\alpha}{\beta}\right]_2 \cdot \left[\frac{\beta}{\alpha}\right]_2 = (-1)^{S+\frac{b+a-1}{2}}. \tag{4.181}$$

Proof. Letting $\alpha = a + b\sqrt{2}$ and $\beta = c + d\sqrt{2}$ gives $\alpha\beta = (ac + 2bd) + (ad + bc)\sqrt{2}$.

Suppose a, c are odd. Then $ac + 2bd$ is also odd.

If b, d are even then $ad + bc$ is even. Therefore by (4.178),

$$\left[\frac{\alpha}{\beta}\right]_2 \cdot \left[\frac{\beta}{\alpha}\right]_2 = (-1)^S \frac{\mathfrak{g}\left(\frac{-\alpha}{8\sqrt{2}}\right)\mathfrak{g}\left(\frac{-\beta}{8\sqrt{2}}\right)}{\mathfrak{g}\left(\frac{-\alpha\beta}{8\sqrt{2}}\right)\mathfrak{g}\left(\frac{-1}{8\sqrt{2}}\right)} = (-1)^S \frac{8 \cdot 8}{8 \cdot 8} = (-1)^S \tag{4.182}$$

proving part (a).

If b, d are odd then $ad + bc$ is even. Furthermore, if $b \equiv d \pmod 4$ then by (4.178),

$$\left[\frac{\alpha}{\beta}\right]_2 \cdot \left[\frac{\beta}{\alpha}\right]_2 = (-1)^S \frac{\mathfrak{g}\left(\frac{-\alpha}{8\sqrt{2}}\right)\mathfrak{g}\left(\frac{-\beta}{8\sqrt{2}}\right)}{\mathfrak{g}\left(\frac{-\alpha\beta}{8\sqrt{2}}\right)\mathfrak{g}\left(\frac{-1}{8\sqrt{2}}\right)} = (-1)^S \frac{8i \cdot 8i}{8 \cdot 8} = (-1)^{S+1}. \tag{4.183}$$

On the other hand if $b \not\equiv d \pmod 4$ then by (4.178),

$$\left[\frac{\alpha}{\beta}\right]_2 \cdot \left[\frac{\beta}{\alpha}\right]_2 = (-1)^S \frac{\mathfrak{g}\left(\frac{-\alpha}{8\sqrt{2}}\right)\mathfrak{g}\left(\frac{-\beta}{8\sqrt{2}}\right)}{\mathfrak{g}\left(\frac{-\alpha\beta}{8\sqrt{2}}\right)\mathfrak{g}\left(\frac{-1}{8\sqrt{2}}\right)} = (-1)^S \frac{-8i \cdot 8i}{8 \cdot 8} = (-1)^S. \tag{4.184}$$

This is equivalent to saying

$$\left[\frac{\alpha}{\beta}\right]_2 \cdot \left[\frac{\beta}{\alpha}\right]_2 = (-1)^{S+\frac{b-d}{2}+1}, \tag{4.185}$$

proving part (b).

If b, d have different parity, we may assume that b is even and d is odd. This implies that $ad+bc$ is odd, but we need to investigate if it is congruent to 1 or -1 modulo 4. Let

$$f = ad + bc. \tag{4.186}$$

Since b even and c odd,

$$f \equiv ad + b \pmod 4). \tag{4.187}$$

If $b \equiv 0$, $a \equiv 1$ or $b \equiv 2$, $a \equiv 3$ modulo 4 then by (4.187), $f \equiv d \pmod 4$ and,

$$\left[\frac{\alpha}{\beta}\right]_2 \cdot \left[\frac{\beta}{\alpha}\right]_2 = (-1)^S \frac{\mathbb{g}\left(\frac{-\alpha}{8\sqrt{2}}\right)\mathbb{g}\left(\frac{-\beta}{8\sqrt{2}}\right)}{\mathbb{g}\left(\frac{-\alpha\beta}{8\sqrt{2}}\right)\mathbb{g}\left(\frac{-1}{8\sqrt{2}}\right)} = (-1)^S \frac{8\cdot\mathbb{g}\left(\frac{-(c+d\sqrt{2})}{8\sqrt{2}}\right)}{\mathbb{g}\left(\frac{-(f+d\sqrt{2})}{8\sqrt{2}}\right)\cdot 8} = (-1)^S. \tag{4.188}$$

On the other hand, if $b \equiv 0$, $a \equiv 3$ or $b \equiv 2$, $a \equiv 1$ modulo 4 then by (4.187), $f \equiv -d \pmod 4$ and,

$$\left[\frac{\alpha}{\beta}\right]_2 \cdot \left[\frac{\beta}{\alpha}\right]_2 = (-1)^S \frac{\mathbb{g}\left(\frac{-\alpha}{8\sqrt{2}}\right)\mathbb{g}\left(\frac{-\beta}{8\sqrt{2}}\right)}{\mathbb{g}\left(\frac{-\alpha\beta}{8\sqrt{2}}\right)\mathbb{g}\left(\frac{-1}{8\sqrt{2}}\right)} = (-1)^S \frac{8\cdot\mathbb{g}\left(\frac{-(c+d\sqrt{2})}{8\sqrt{2}}\right)}{\mathbb{g}\left(\frac{-(f-d\sqrt{2})}{8\sqrt{2}}\right)\cdot 8} = (-1)^{S+1}. \tag{4.189}$$

This proves part (c) by giving,

$$\left[\frac{\alpha}{\beta}\right]_2 \cdot \left[\frac{\beta}{\alpha}\right]_2 = (-1)^{S+\frac{b+a-1}{2}}. \tag{4.190}$$

□

4.7.2. Applying (4.69) for $\lambda = \sqrt{2}$ gives,

$$\left[\frac{\sqrt{2}}{\alpha}\right]_2 = (-1)^{(\operatorname{sgn}\bar{\alpha}-1)/2} \frac{\mathbb{g}\left(\frac{-\alpha}{16}\right)\mathbb{g}\left(\frac{-1}{8\sqrt{2}}\right)}{\mathbb{g}\left(\frac{-1}{16}\right)\mathbb{g}\left(\frac{-\alpha}{8\sqrt{2}}\right)}. \tag{4.191}$$

We need to investigate the Gauss sums $\mathbb{g}\left(\frac{-\alpha}{16}\right)$ and $\mathbb{g}\left(\frac{-1}{16}\right)$, since the other two sums may be determined by (4.178). Since $\mathfrak{d} = (2\sqrt{2})$, the sums $\mathfrak{g}\left(\frac{-\alpha}{16}\right)$ and $\mathfrak{g}\left(\frac{-1}{16}\right)$ have denominator

$$\frac{16}{2\sqrt{2}} = 4\sqrt{2}\,. \tag{4.192}$$

Claim. *The set*

$$G = \{a + b\sqrt{2}\} \quad \textit{such that } a = 0, 1, \ldots, 7 \textit{ and } b = 0, 1, 2, 3\,, \tag{4.193}$$

runs through a system of residues modulo $4\sqrt{2}$*.*

Proof. Since $8 \equiv 0$ and $4\sqrt{2} \equiv 0$ modulo $4\sqrt{2}$, then every integer is congruent to an element in G. It suffices to show that G has the correct number of elements. The number of residue classes modulo 4 is $4 \cdot 4 = 16$ and the number of residue classes modulo $\sqrt{2}$ is 2. Therefore the number of residue classes modulo $4(1+i) = 16 \cdot 2 = 32$. The set G has 32 elements, so its element must form all the distinct residue classes. □

Considering the square of each residue gives us

$$\begin{array}{llll}
0^2 \equiv 0 & \sqrt{2}^2 \equiv 2 & (2\sqrt{2})^2 \equiv 0 & (3\sqrt{2})^2 \equiv 2 \\
1^2 \equiv 1 & (1+\sqrt{2})^2 \equiv 3+2\sqrt{2} & (1+2\sqrt{2})^2 \equiv 1 & (1+3\sqrt{2})^2 \equiv 3+2\sqrt{2} \\
2^2 \equiv 4 & (2+\sqrt{2})^2 \equiv 6 & (2+2\sqrt{2})^2 \equiv 4 & (2+3\sqrt{2})^2 \equiv 6 \\
3^2 \equiv 1 & (3+\sqrt{2})^2 \equiv 3+2\sqrt{2} & (3+2\sqrt{2})^2 \equiv 1 & (3+3\sqrt{2})^2 \equiv 3+2\sqrt{2} \\
4^2 \equiv 0 & (4+\sqrt{2})^2 \equiv 2 & (4+2\sqrt{2})^2 \equiv 0 & (4+3\sqrt{2})^2 \equiv 2 \\
5^2 \equiv 1 & (5+\sqrt{2})^2 \equiv 3+2\sqrt{2} & (5+2\sqrt{2})^2 \equiv 1 & (5+3\sqrt{2})^2 \equiv 3+2\sqrt{2} \\
6^2 \equiv 4 & (6+\sqrt{2})^2 \equiv 6 & (6+2\sqrt{2})^2 \equiv 4 & (6+3\sqrt{2})^2 \equiv 6 \\
7^2 \equiv 1 & (7+\sqrt{2})^2 \equiv 3+2\sqrt{2} & (7+2\sqrt{2})^2 \equiv 1 & (7+3\sqrt{2})^2 \equiv 3+2\sqrt{2}
\end{array}$$

This means that the squares modulo $4\sqrt{2}$, with multiplicity, are four 0, four 4, four 2, four 6, eight $3+2\sqrt{2}$, eight 1. This gives the Gauss sum,

$$\begin{aligned}
\mathfrak{g}\left(\frac{-\beta}{16}\right) =& 4 + 4e^{2\pi i \operatorname{tr}(-4\beta/8\sqrt{2})} + 4e^{2\pi i \operatorname{tr}(-2\beta/8\sqrt{2})} + 4^{2\pi i \operatorname{tr}(-6\beta/8\sqrt{2})} + \\
&+ 8e^{2\pi i \operatorname{tr}(-(3+2\sqrt{2})\beta/8\sqrt{2})} + 8e^{2\pi i \operatorname{tr}(-\beta/8\sqrt{2})} \\
=& 4 + 4e^{\frac{-\pi i}{2}\operatorname{tr}(\beta\sqrt{2})} + 4e^{\frac{-\pi i}{4}\operatorname{tr}(\beta\sqrt{2})} + 4^{\frac{-3\pi i}{4}\operatorname{tr}(\beta\sqrt{2})} + \\
&+ 8e^{\frac{-\pi i}{8}\operatorname{tr}((4+3\sqrt{2})\beta)} + 8e^{\frac{-\pi i}{8}\operatorname{tr}(\beta\sqrt{2})}\,,
\end{aligned} \tag{4.194}$$

If $\alpha = a + b\sqrt{2}$ then $(4+3\sqrt{2})\beta = 4a+6b+(3a+4b)\sqrt{2}$ so,

$$\begin{aligned} \mathbb{g}\left(\frac{-\alpha}{16}\right) &= 4+4e^{-2\pi ib}+4e^{-\pi ib}+4^{-3\pi ib}+8e^{\frac{-\pi i(2a+3b)}{2}}+8e^{\frac{-\pi ib}{2}} \\ &= 8+8e^{\pi ib}+8e^{-\frac{\pi i}{2}(2a+3b)}+8e^{-\frac{\pi i}{2}b}. \end{aligned} \tag{4.195}$$

Restricting a to be odd gives,

$$\mathbb{g}\left(\frac{-\alpha}{16}\right) = 8+8e^{\pi ib}+8e^{\pi i(\frac{b}{2}-1)}+8e^{-\frac{\pi i}{2}b}, \tag{4.196}$$

which allows us to calculate,

$$\mathbb{g}\left(\frac{-\alpha}{16}\right) = \begin{cases} 16 & \text{if } b \equiv 0 \pmod 4 \\ -16i & \text{if } b \equiv 1 \pmod 4 \\ 16 & \text{if } b \equiv 2 \pmod 4 \\ 16i & \text{if } b \equiv 3 \pmod 4. \end{cases} \tag{4.197}$$

Therefore applying (4.178) and (4.197) to (4.191), we obtain the supplementary theorem.

Theorem. $\mathbb{Z}[\sqrt{2}]$***: Quadratic Reciprocity Supplement***
Let $\alpha = a + b\sqrt{2}$ for a, b rational integers with a odd. Then,

$$\left[\frac{\sqrt{2}}{\alpha}\right]_2 = (-1)^{(sgn\,\bar{\alpha}-1)/2}. \tag{4.198}$$

5 Theta Series

Before we get to the proof of part (e) of Theorem 4.3, we will need to develop the theory of theta series. In this section we will first introduce the theta function in one dimension, then give a generalization as in Mumford in [2]. We demonstrate that the series converges to a function in some domain and we also give a discussion of some of the interesting transformation properties of this function.

5.1 Quadratic forms and Convergence Results

5.1.1. Let a_{ik} be a sequence of complex constants for $1 \leq i,k \leq n$ such that and $a_{ik} = a_{ki}$, i.e. $A = (a_{ik})$ is symmetric. We call the expression

$$Q_A(x_1,\dots x_n) = \sum_{i,k=1}^{n} a_{ik}x_ix_k = a_{11}x_1^2 + 2a_{12}x_1x_2 + \cdots , \tag{5.1}$$

a **quadratic form in** n **variables**. For a quadratic form Q_A, we can split the real and imaginary parts, $Q_{\Re}, Q_{\Im}$ respectively, such that $Q = Q_{\Re} + iQ_{\Im}$. A quadratic form with real coefficients called **positive definite** if the matrix A is positive definite. That is, if $Q(x_1,\dots x_n) \geq 0$ for all $x_1,\dots,x_n \in \mathbb{R}$ with equality if and only if $x_1 = \cdots = x_n = 0$.

Lemma. *For any positive definite form $Q_A(x_1,\dots x_n)$ there is a number $c > 0$ such that for all real $x_1,\dots,x_n$*

$$Q_A(x_1,\dots x_n) \geq c(x_1^2 + x_2^2 + \cdots + x_n^2). \tag{5.2}$$

Proof. Take $y_1,\dots,y_n$ as coordinates on the unit sphere $y_1^2 + \cdots + y_n^2 = 1$. Then since Q_A is positive definite we have $Q_A(y_1,\dots,y_n) > 0$. Since Q is continuous, it must have a positive minimum value c on the sphere. Hence for $(y_1,\dots,y_n)$ on the sphere we have,

$$Q_A(y_1,\dots y_n) \geq c. \tag{5.3}$$

If we set

$$y_i = \frac{x_i}{\sqrt{x_1^2 + \cdots x_n^2}}, \tag{5.4}$$

then

$$Q_A(x_1,\dots,x_n) = Q_A(y_1,\dots,y_n)(x_1^2 + \cdots + x_n^2) \geq c(x_1^2 + \cdots + x_n^2). \tag{5.5}$$

□

5.1.2. Let $A = (a_{ij})$ as above and let $Q := Q_A$ a quadratic form. Define the quadratic theta series as the formal sum

$$\theta_Q(u_1,\dots,u_n) := \sum_{m_1,\dots m_n=-\infty}^{\infty} e^{-\pi Q(m_1+u_1,\dots,m_n+u_n)}, \tag{5.6}$$

where the $u_1, \dots, u_n$ are real variables.

Theorem. *Let $Q_{\mathfrak{R}}$ be positive definite, then its theta series $\theta_Q(u_1, \dots, u_n)$ and its derivatives are absolutely convergent for any $u_1, \dots, u_n \in \mathbb{R}$ and periodic with period 1, i.e.*

$$\theta_Q(u_1, \dots, u_n) = \theta_Q(u_1 + m_1, \dots, u_n + m_n) \quad \text{for } m_i \in \mathbb{Z}. \tag{5.7}$$

Proof. We will show θ_Q is converges absolutely. By Lemma 5.1.1 we have that

$$Q_{\mathbb{R}}(m_1 + u_1, \dots, m_n + u_n) \geq c\big((m_1 + u_1)^2 + \cdots + (m_n + u_n)^2\big), \tag{5.8}$$

for some positive c. Therefore,

$$|e^{-\pi Q}| = e^{-\pi Q_{\mathbb{R}}} \leq e^{-\pi c \sum_{i=1}^{n} (m_i + u_1)^2}. \tag{5.9}$$

Restricting the real numbers u_i to a domain $|u_i| \leq C/2$ for some positive C gives, for the constant $K = C^2 \pi c/4$,

$$|e^{-\pi Q}| \leq \exp\big\{-\pi c \sum_{i=1}^{n} (m_i^2 - C|m_i|) + K\big\}. \tag{5.10}$$

For any real numbers $m_1, \dots, m_n$ and positive integer n the following inequality holds.

$$|m_1| + \cdots + |m_n| \leq \sqrt{n(m_1^2 + \cdots + m_n^2)}. \tag{5.11}$$

For any $\varepsilon > 0$ we may take $m_1, \dots, m_n$ large enough such that

$$m_1^2 + \cdots + m_n^2 > \frac{1}{\varepsilon^2} \tag{5.12}$$

therefore (5.11) and (5.12) give,

$$|m_1| + \cdots + |m_n| \leq \sqrt{n(m_1^2 + \cdots + m_n^2)} \leq \varepsilon \sqrt{n}(m_1^2 + \cdots + m_n^2). \tag{5.13}$$

If we take ε small enough such that $a := c(1 - \varepsilon C\sqrt{n}) > 0$, then almost all the terms in θ_Q will be smaller in absolute value than their corresponding terms in some constant times the following series,

$$\sum_{m_1, \dots m_n = -\infty}^{\infty} e^{-\pi a (m_1^2 + \cdots + m_n^2)}. \tag{5.14}$$

Since this series converges absolutely, then we can say that θ_Q also converges absolutely.

We now look at the derivatives of θ_Q. Since,

$$Q(m_1 + u_1, \dots, m_n + u_n) = Q(m_1, \dots, m_n) + 2 \sum_{i,k=1}^{n} a_{ik} m_i u_k + Q(u_1, \dots, u_n) \tag{5.15}$$

then

$$\theta_Q(u_1,\ldots,u_n) = e^{-\pi Q(u_1,\ldots,u_n)} \sum_{m_1,\ldots m_n=-\infty}^{\infty} \exp\big\{-\pi Q(m_1,\ldots,m_n) - 2\pi \sum_{i,k=1}^{n} a_{ik} m_i u_k\big\}, \tag{5.16}$$

so it suffices to show absolute convergence of the derivatives of

$$\sum_{m_1,\ldots m_n=-\infty}^{\infty} \exp\big\{-\pi Q(m_1,\ldots,m_n) - 2\pi \sum_{i,k=1}^{n} a_{ik} m_i u_k\big\}. \tag{5.17}$$

As we take various partial derivatives with respect to the u_i, the exponential does not change but we introduce various coefficients to the exponential. For example, should we differentiate once with respect to u_j for $j \in \{1,\ldots,n\}$, this coefficient will be,

$$a_{1j}m_1 + \ldots + a_{nj}m_n. \tag{5.18}$$

which means it suffices consider n different sums,

$$a_{pj} \sum_{m_1,\ldots m_n=-\infty}^{\infty} m_p \exp\big\{-\pi Q(m_1,\ldots,m_n) - 2\pi \sum_{i,k=1}^{n} a_{ik} m_i u_k\big\} \quad \text{for } p = 1,\ldots,n. \tag{5.19}$$

The product of the constant terms a_{ik} and their exponents is inconsequential to the convergence of the series. Hence to show that any derivative of (5.17) is absolutely convergent, it suffices to show the absolute convergence of,

$$\sum_{m_1,\ldots m_n=-\infty}^{\infty} |m_1^{c_1}\cdots m_n^{c_n}| \exp\big\{-\pi Q(m_1,\ldots,m_n) - 2\pi \sum_{i,k=1}^{n} a_{ik} m_i u_k\big\} \quad \text{for } c_i \in \mathbb{Z} \text{ non-negative.} \tag{5.20}$$

From $|m| < e^{|m|}$ with $R := \max\{c_1,\ldots,c_n\}$ we have

$$|m_1^{c_1}\cdots m_n^{c_n}| < e^{c_1|m_1|+\cdots+c_n|m_n|} < e^{R(|m_1|+\cdots+|m_n|)}. \tag{5.21}$$

Therefore the summands in (5.20) are bounded above by,

$$\exp\big\{-\pi Q(m_1,\ldots,m_n) - 2\pi \sum_{i,k=1}^{n} a_{ik} m_i u_k + R\sum_{k=1}^{n} |m_k|\big\} \tag{5.22}$$

which by (5.15) is equal to

$$e^{\pi Q(u_1,\ldots,u_n)} \exp\big\{-\pi Q(m_1+u_1,\ldots,m_n+u_n) + R\sum_{k=1}^{n} |m_k|\big\}. \tag{5.23}$$

By Lemma 5.1.1 there exists a $c \geq 0$ such that (5.23) is bounded above by,

$$e^{\pi Q(u_1,\dots,u_n)}\exp\big\{-\pi c\sum_{i=1}^{n}(m_i+u_i)^2+R\sum_{k=1}^{n}|m_k|\big\}. \tag{5.24}$$

Exactly as in (5.10), restricting the real numbers u_i to a domain $|u_i|\leq C/2$ gives us (5.24) is bounded above by

$$e^{\pi Q(u_1,\dots,u_n)}\exp\big\{-\pi c\sum_{i=1}^{n}m_i^2+(R+C)\sum_{k=1}^{n}|m_k|+K\big\}, \tag{5.25}$$

where $K=C^2\pi c/4$. By mirroring the steps taken from (5.10) to (5.14) we obtain that (5.25) is bounded above by

$$e^{\pi Q(u_1,\dots,u_n)}\exp\big\{-\pi c(1-\varepsilon(C+R)\sqrt{n})(m_1^2+\cdots+m_n^2)+K\big\}. \tag{5.26}$$

Again, by taking ε sufficiently small, we can ensure $a:=(1-\varepsilon(C+R)\sqrt{n})>0$ which tells us that (5.20) is absolutely convergent as

$$\sum_{m_1,\dots m_n=-\infty}^{\infty} e^{-\pi a(m_1^2+\cdots+m_n^2)}, \tag{5.27}$$

clearly converges.

To see that this the function has period 1, consider replacing the summation index m_i by m_i-1. This doesn't change the value of the sum, so $\theta_Q(\dots,u_i,\dots)=\theta_Q(\dots,u_i+1,\dots)$. □

5.2 Theta function in one dimension

5.2.1. To help give motivation to more general theta functions we will introduce the notion of a theta function in one dimension. Take the variables $s\in\mathbb{C}$ and $\tau\in H$ where H is the upper half complex plane, so the imaginary part of τ is positive. Then we may define

$$\theta(s,\tau)=\sum_{n\in\mathbb{Z}}\exp\big\{\pi in^2\tau+2\pi ins\big\} \tag{5.28}$$

If we restrict $s=0$ then this series converges absolutely by Theorem 5.1.2. To see this take $u=0$ and $Q(x)=-i\tau x^2$ as in the theorem. Even for general s, one can show this series converges absolutely [2, pg.1]. To see this, set real numbers c and ε such that

$$|\Im(s)|<c \quad\text{and}\quad \Im(\tau)>\varepsilon>0 \tag{5.29}$$

then

$$|\exp\big\{\pi in^2\tau+2\pi ins\big\}|<\exp\big\{-\pi\varepsilon\big\}^{n^2}\exp\big\{2\pi c\big\}^{n}. \tag{5.30}$$

By choosing $n_0 \in \mathbb{Z}$ large enough such that

$$\exp\{-\pi\varepsilon\}^{n_0}\exp\{2\pi c\} < 1 \tag{5.31}$$

implies the inequality

$$|\exp\{\pi i n^2\tau + 2\pi i n s\}| < \exp\{-\pi\varepsilon\}^{n^2}\exp\{-\pi\varepsilon\}^{-nn_0} = \exp\{-\pi\varepsilon\}^{n(n-n_0)}, \tag{5.32}$$

which shows that the series (5.28) converges absolutely.

5.3 Theta Inversion and the Heat Equation in one dimension

5.3.1. For $t > 0$ and $x \in \mathbb{R}$ the periodic heat kernel $K(x,t)$ is the unique solution to the periodic heat equation,

$$\frac{\partial K}{\partial t} + \frac{1}{4\pi}\frac{\partial^2 K}{\partial x^2} = 0\,. \tag{5.33}$$

subject to the periodic conditions in x,

$$K(x+1,t) = K(x,t)\,., \tag{5.34}$$

and the initial conditions,

$$\lim_{t\to 0}\int_0^1 K(x,t)f(x)dx = f(0)\,. \tag{5.35}$$

It turns out that θ is such a solution for the above initial value problem. We restrict the variables s,τ to $s = x \in \mathbb{R}$ and $\tau = it$ where $t \in \mathbb{R}$, $t \geq 0$. Clearly the periodic condition is satisfied. so we are left to check it satisfies differential equation,

$$\frac{\partial}{\partial t}\big(\theta(x,it)\big) = -\pi\sum_{n\in\mathbb{Z}} n^2\exp\{-\pi n^2 t + 2\pi i n x\} \tag{5.36}$$

and,

$$\frac{\partial^2}{\partial x^2}\big(\theta(x,it)\big) = -4\pi^2\sum_{n\in\mathbb{Z}} n^2\exp\{-\pi n^2 t + 2\pi i n x\}\,. \tag{5.37}$$

Therefore θ is the unique solution to the differential equation (5.33). To verify the initial conditions, we integrate θ against a test periodic function,

$$f(x) = \sum_{m\in\mathbb{Z}} a_m e^{2\pi i m x} \tag{5.38}$$

so we get,

$$\begin{aligned}\int_0^1 \theta(x,it)f(x)dx &= \sum_{n\in\mathbb{Z}}\sum_{m\in\mathbb{Z}} a_m e^{-\pi n^2 t} e^{2\pi i(n+m)x} dx \\ &= \sum_{n\in\mathbb{Z}}\sum_{m\in\mathbb{Z}} a_m e^{-\pi n^2 t} \int_0^1 e^{2\pi i(n+m)x} dx\,.\end{aligned} \tag{5.39}$$

However,

$$\int_0^1 e^{2\pi ikx} = 0 \quad \text{for any nonzero } k \in \mathbb{Z} \tag{5.40}$$

so all the terms in the sum drop out except when $n = -m$. Therefore,

$$\int_0^1 \theta(x,it)f(x)dx = \sum_{n\in\mathbb{Z}} a_{-n} e^{-\pi n^2 t} = \sum_{n\in\mathbb{Z}} a_n e^{-\pi n^2 t}\,, \tag{5.41}$$

so,

$$\begin{aligned}\lim_{t\to 0}\int_0^1 \theta(x,it)f(x)dx &= \lim_{t\to 0}\sum_{n\in\mathbb{Z}} a_n e^{-\pi n^2 t} \\ &= \sum_{n\in\mathbb{Z}} a_n \\ &= f(0)\,.\end{aligned} \tag{5.42}$$

Hence the limit converges to a sum of delta functions at all integral points $x \in \mathbb{Z}$, showing (5.35).

5.3.2. On the other hand the differential equation, for $t > 0, x \in \mathbb{R}$,

$$\frac{\partial K}{\partial t}(x,t) = \frac{1}{4\pi}\frac{\partial^2}{\partial^2 x}K(x,t) \tag{5.43}$$

where,

$$\lim_{t\to 0} K(x,t) = \delta(x) \quad \text{the dirac-delta function,} \tag{5.44}$$

has the well known unique solution called the heat kernel,

$$K(x,t) = \frac{1}{\sqrt{t}} e^{\frac{-x^2}{4t}}\,. \tag{5.45}$$

If we periodize this function in the space variable on the circle $\mathbb{R}/\mathbb{Z}$, denoted S, we get the new heat kernel,

$$K^S(x,t) = \sum_{m=-\infty}^{\infty} K^S(x+m,t) = \frac{1}{\sqrt{t}}\sum_{m\in\mathbb{Z}} \exp\left\{\frac{-\pi(x-m)^2}{t}\right\}. \tag{5.46}$$

Therefore this periodic solution also satisfies (5.33), (5.34) and (5.35). Since $\theta(x,it)$ and the periodic heat kernel in (5.46) are both unique solutions to the boundary value problem, they must be equal,

$$\sum_{n\in\mathbb{Z}} \exp\{-\pi n^2 t\}\exp\{2\pi i n x\} = \frac{1}{\sqrt{t}}\sum_{m\in\mathbb{Z}} \exp\left\{\frac{-\pi(x-m)^2}{t}\right\}. \tag{5.47}$$

Expanding the square on the right hand side yields,

$$\begin{aligned}\sum_{m\in\mathbb{Z}} \exp\left\{\frac{-\pi(x-m)^2}{t}\right\} &= \exp\{-\pi x^2/t\}\sum_{m\in\mathbb{Z}} \exp\{-\pi n^2/t + 2\pi n x/t\} \\ &= \exp\{-\pi x^2/t\}\theta(x/it, i/t)\,.\end{aligned} \tag{5.48}$$

So we get the one dimensional theta inversion,

$$\theta(x,it) = \frac{1}{\sqrt{t}}\exp\left\{-\frac{\pi x^2}{t}\right\}\theta\left(\frac{x}{it},\frac{i}{t}\right). \tag{5.49}$$

Written out as a sum,

$$\sum_{n\in\mathbb{Z}} \exp\{-\pi n^2 t + 2\pi i x n\} = \frac{1}{\sqrt{t}}\exp\{-\pi x^2/t\}\sum_{m\in\mathbb{Z}} \exp\left\{\frac{-\pi m^2 + 2\pi x m}{t}\right\} \tag{5.50}$$

In particular, when we restrict $x = 0$ we get the identity,

$$\sum_{n\in\mathbb{Z}} \exp\{-\pi n^2 t\} = \frac{1}{\sqrt{t}}\sum_{m\in\mathbb{Z}} \exp\left\{\frac{-\pi m^2}{t}\right\}. \tag{5.51}$$

This identity is exactly what is used in [6, pg.3] to prove the law of quadratic reciprocity when $K = \mathbb{Q}$.

5.4 Siegel-Jacobi Theta Functions

5.4.1. We will obtain another generalization of the Theta Function in this section. The higher dimensional analogue of s as in Section 5.2 is the n-tuple $\vec{s} = (s_1,\ldots,s_n) \in \mathbb{C}^n$. The higher dimensional analogue of τ is the matrix Ω which is a symmetric $n\times n$ complex matrix whose imaginary part is positive definite. We can define $\mathfrak{H}_n$ to be the set of all such Ω. Let $\vec{m}$ be the n-tuple $(m_1,\ldots,m_n) \in \mathbb{Z}^n$. Then the **Siegel theta function** is,

$$\Theta(s,\Omega) = \sum_{\vec{m}\in\mathbb{Z}^n} \exp\left\{\pi i \vec{m}^\top \Omega \vec{m} + 2\pi i \vec{m}^\top \cdot \vec{s}\right\}. \tag{5.52}$$

As in Section 5.2, when $\vec{s} = 0$ the series converges absolutely by Theorem 5.1.2, since $-i\vec{m}^\top\Omega\vec{m}$ admits a positive definite quadratic form. In fact, $\Theta(0,\Omega) = \theta_Q(\vec{0})$ where $Q := Q_\Omega$ is the quadratic form with coefficients given by the matrix Ω. This series also converges absolutely in general by

[2, pg.118]. To see this, let $\Omega_{\Im}$ be the imaginary part of Ω. Then,

$$\vec{m}^{\top}\Omega_{\Im}\vec{m} = Q(m_1,\dots,m_n) \quad \text{for } Q \text{ a positive definite quadratic form,} \tag{5.53}$$

hence by Lemma 5.1.1 we can find a number $c_1 > 0$ such that

$$\vec{m}^{\top}\Omega_{\Im}\vec{m} \geq c_1(m_1^2 + m_2^2 + \cdots + m_n^2)\,. \tag{5.54}$$

Setting $c_2 > 0$ such that

$$\max_{i=1,\dots,n} |\Im(s_i)| < \frac{c_2}{2\pi} \tag{5.55}$$

gives the inequality

$$\big|\exp\left\{\pi i\vec{m}^{\top}\Omega\vec{m} + 2\pi i\vec{m}^{\top}\cdot\vec{s}\right\}\big| \leq \exp\Big\{-\pi c_1\sum_{i=1}^{n} m_i^2 + c_2\sum_{i=1}^{n}|m_i|\Big\} = \prod_{i=1}^{n}\exp\left\{-\pi c_1 m_i^2 + c_2|m_i|\right\}. \tag{5.56}$$

Therefore since

$$\sum_{m=0}^{\infty}\exp\{-\pi c_1 m^2 + c_2 m\} \tag{5.57}$$

converges absolutely, we have $\Theta(s,\Omega)$ also converges absolutely.

5.4.2. The final generalization to the theta function will be considering the vectors $\vec{a},\vec{b} \in \mathbb{Q}^n$. We can view these as the "shift" of the lattice we are summing over. We define the **Siegel-Jacobi theta function**,

$$\Theta\begin{bmatrix}\vec{a}\\ \vec{b}\end{bmatrix}(\vec{s},\Omega) = \sum_{\vec{m}\in\mathbb{Z}^n}\exp\Big\{\pi i(\vec{m}+\vec{a})^{\top}\Omega(\vec{m}+\vec{a}) + 2\pi i(\vec{m}+\vec{a})^{\top}(\vec{s}+\vec{b})\Big\}. \tag{5.58}$$

Factoring yields how this relates to the Siegel theta function in (5.52),

$$\Theta\begin{bmatrix}\vec{a}\\ \vec{b}\end{bmatrix}(\vec{s},\Omega) = \exp\{\pi i\vec{a}^{\top}\Omega\vec{a} + 2\pi i\vec{a}^{\top}(\vec{s}+\vec{b})\}\Theta(\vec{s}+\Omega\vec{a}+\vec{b},\Omega)\,. \tag{5.59}$$

It is easy to see how we can get back to the original Siegel theta function,

$$\Theta\begin{bmatrix}0\\ 0\end{bmatrix}(\vec{s},\Omega) = \Theta(\vec{s},\Omega)\,. \tag{5.60}$$

For integral vectors $\vec{m}_1,\vec{m}_2 \in \mathbb{Z}^n$,

$$\Theta\begin{bmatrix}\vec{a}+\vec{m}_1\\ \vec{b}+\vec{m}_2\end{bmatrix}(\vec{s},\Omega) = \exp\left\{2\pi i\vec{a}^{\top}\cdot\vec{m}_2\right\}\Theta\begin{bmatrix}\vec{a}\\ \vec{b}\end{bmatrix}(\vec{s},\Omega)\,. \tag{5.61}$$

5.5 Modular properties for Siegel Theta Functions

5.5.1. A modular form is a function analytic in the upper half plane satisfying a certain functional equation with respect to the group action of the modular group. The Siegel theta function is such a modular form with functional equation shown in [2, pg.189]. We will state the functional equation without proof as,

Proposition. *For ξ_γ some eighth root of 1, and*

$$\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \quad Sp(2n, \mathbb{Z}) \tag{5.62}$$

such that the diagonal of $A^\top C$ and the diagonal of $B^\top D$ are both even. Then,

$$\Theta\Big((C\Omega+D)^{-1\top}\cdot\vec{s}, (A\Omega+B)(C\Omega+D)^{-1}\Big) = \xi_\gamma \det(C\Omega+D)^{1/2}\exp\{\pi i\vec{s}^\top\cdot(C\Omega+D)^{-1}C\cdot\vec{s}\}\Theta(\vec{s},\Omega). \tag{5.63}$$

We will not use this property in its entirety so we will omit its proof. The specialized case when

$$\gamma = \begin{pmatrix} 0_n & -I_n \\ I_n & 0_n \end{pmatrix} \qquad \text{so} \quad A = D = (0); \quad C = -B = I_n, \tag{5.64}$$

is of interest to us. It turns out that for this γ then ξ is the eighth root of 1 such that,

$$\xi \det(\Omega)^{1/2} = \det(\Omega/i)^{1/2}. \tag{5.65}$$

so that we get

$$\Theta(\Omega^{-1}\vec{s}, -\Omega^{-1}) = \det(\Omega/i)^{1/2}\exp\left\{\pi i s^\top\Omega^{-1}s\right\}\Theta(\vec{s},\Omega). \tag{5.66}$$

5.5.2. We will formally prove (5.66). We start by stating the Poisson summation formula.

Proposition. *For f a smooth function on $\mathbb{R}^n$ which goes to zero fast enough at infinity we have,*

$$\sum_{m\in\mathbb{Z}^n} f(m) = \sum_{m\in\mathbb{Z}^n} \hat{f}(m) \tag{5.67}$$

where $\hat{f}$ is the Fourier transform of f given by,

$$\hat{f}(\xi) = \int_{\mathbb{R}^n} f(x)\exp\{2\pi i x^\top\cdot\xi\}dx_1\cdots dx_n \tag{5.68}$$

for x the n-tuple $(x_1,\ldots,x_n)$.

We require a computation.

Lemma. *For all $\Omega \in \mathfrak{H}_n$and $s \in \mathbb{C}^n$ we have the following integral,*

$$\int_{\mathbb{R}^n} \exp\{\pi i x^\top\Omega x + 2\pi i x^\top\cdot s)dx_1\cdots dx_n = (\det\Omega/i)^{-1/2}\exp\{-\pi i s^\top\Omega^{-1}s\}. \tag{5.69}$$

Proof. To evaluate this integral we will reduce it to a Gaussian integral. First notice that

$$\begin{aligned}(x+\Omega^{-1}s)^\top\Omega(x+\Omega^{-1}s) &= (x^\top+s^\top\Omega^{-1})\Omega(x+\Omega^{-1}s)\\ &= (x^\top+s^\top\Omega^{-1})(\Omega x+s)\\ &= x^\top\Omega x+x^\top s+s^\top x+s^\top\Omega^{-1}s\\ &= x^\top\Omega x+2x^\top s+s^\top\Omega^{-1}s\end{aligned} \tag{5.70}$$

where in the first equality we use the fact that Ω^{-1} is symmetric. Therefore we may rewrite the integral in (5.69) as,

$$\begin{aligned}\int_{\mathbb{R}^n}\exp\{\pi i x^\top\Omega x+2\pi i x^\top\cdot s)dx_1\cdots dx_n &= \int_{\mathbb{R}^n}\exp\{\pi i(x^\top\Omega x+2x^\top s+s^\top\Omega^{-1}s-s^\top\Omega^{-1}s)\}dx_1\cdots dx_n\\ &= \int_{\mathbb{R}^n}\exp\{\pi i(x+\Omega^{-1}s)^\top\Omega(x+\Omega^{-1}s)-\pi i s^\top\Omega^{-1}s\}dx_1\cdots dx_n\\ &= \exp\{-\pi i s^\top\Omega^{-1}s\}\int_{\mathbb{R}^n}\exp\{\pi i(x+\Omega^{-1}s)^\top\Omega(x+\Omega^{-1}s)\}dx_1\cdots dx_n\,.\end{aligned} \tag{5.71}$$

Claim. *Let $f(s_1,\dots,s_g)$ be a holomorphic function in each of its variables. If $f(i\mathbb{R},\dots,i\mathbb{R})=0$, then $f(s_1,\dots,s_g)=0$ for all $s_1,\dots,s_n$.*

Proof. We prove for $g=2$. For any $x\in\mathbb{R}$, considering $f(ix,s_2)$ as a holomorphic function in s_2, we have that $f(ix,s_2)$ is zero for s_2 on the imaginary axis, therefore $f(ix,s_2)=0$. Fix $z\in\mathbb{C}$ and consider $f(s_1,z)$ as a holomorphic function in s_1. Similarly, as $f(s_1,z)$ is zero for s_1 on the imaginary axis, we have $f(s_1,z)=0$. As z was arbitrary, $f(s_1,s_2)=0$. The general case follows by induction. □

As both sides of (5.69) are holomorphic in s and Ω, by Claim 5.5.2 it suffices to prove it when s and Ω are both purely imaginary, i.e. when

$$\Omega = iA^\top A\,,\quad \text{for } A \text{ a real positive definite matrix} \tag{5.72}$$

$$s = iy\,,\quad \text{for } y\in\mathbb{R}. \tag{5.73}$$

$$\tag{5.74}$$

Therefore it suffices to evaluate

$$\exp\{-\pi i s^\top\Omega^{-1}s\}\int_{\mathbb{R}^n}\exp\{-\pi(x+(A^\top A)^{-1}y)^\top iA^\top A(x+(A^\top A)^{-1}y)\}dx_1\cdots dx_n\,. \tag{5.75}$$

We make the substitution $x\to x+(A^\top A)^{-1}y$ so we may rewrite the integral as,

$$\exp\{-\pi i s^\top\Omega^{-1}s\}\int_{\mathbb{R}^n}\exp\{-\pi x^\top A^\top AAx\}dx_1\cdots dx_n\,. \tag{5.76}$$

Additionally, after making the substitution $w = Ax$ our integral (5.76) becomes

$$\exp\{-\pi i s^\top \Omega^{-1} s\} \int_{\mathbb{R}^n} \exp\{-\pi w^\top w\}(\det A)^{-1})dw_1 \cdots dw_n \tag{5.77}$$

$$= \exp\{-\pi i s^\top \Omega^{-1} s\}(\det A \cdot A)^{-1/2} \prod_{i=1}^{n} \int_{-\infty}^{\infty} \exp\{-\pi w_i^2\} dw_i \tag{5.78}$$

$$= \exp\{-\pi i s^\top \Omega^{-1} s\}(\det \Omega / i)^{-1/2} \tag{5.79}$$

where the last inequality follows from

$$A \cdot A = A^\top A = \Omega / i \quad \text{because } A \text{ is symmetric,} \tag{5.80}$$

and

$$\int_{-\infty}^{\infty} e^{-\pi w^2} dw = 1\,. \tag{5.81}$$

□

Now we prove (5.66). Let

$$f(x) = \exp\{\pi i x^\top \Omega x + 2\pi i x^\top s\} \tag{5.82}$$

so that

$$\sum_{n \in \mathbb{Z}^n} f(n) = \Theta(s, \Omega)\,. \tag{5.83}$$

To apply Proposition 5.5.2, we need to calculate $\hat{f}$ as given by (5.68). By Lemma 5.5.2,

$$\begin{aligned} \hat{f}(\xi) &= \int_{\mathbb{R}^n} \exp\{\pi i x^\top \Omega x + 2\pi i x^\top s\} \exp\{2\pi i x^\top \xi\} dx_1 \cdots dx_n \\ &= \int_{\mathbb{R}^n} \exp\{\pi i x^\top \Omega x + 2\pi i x^\top (s + \xi)\} dx_1 \cdots dx_n \\ &= (\det \Omega / i)^{-1/2} \exp\{-\pi i (s + \xi)^\top \Omega^{-1} (s + \xi)\}\,. \end{aligned} \tag{5.84}$$

Therefore, using again (5.70) to factor the exponent,

$$\begin{aligned} \sum_{m \in \mathbb{Z}^n} \hat{f}(m) &= (\det \Omega / i)^{1/2} \exp\{-\pi i s^\top \Omega^{-1} s\} \sum_{m \in \mathbb{Z}^n} \exp\{-\pi i m^\top \Omega^{-1} m - 2\pi i m^\top \Omega^{-1} s\} \\ &= (\det \Omega / i)^{1/2} \exp\{-\pi i s^\top \Omega^{-1} s\} \Theta(\Omega^{-1} s, -\Omega^{-1})\,. \end{aligned} \tag{5.85}$$

By (5.83) and the Poisson summation formula (Proposition 5.5.2), we have shown (5.66).

5.6 A connection to the Heat Equation

We can prove (5.66) for a special case using the heat equation developed in section 5.3.

Proposition. *Let Ω be the diagonal matrix,*

$$\Omega = \begin{pmatrix} it_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & it_g \end{pmatrix}, \tag{5.86}$$

where $t_1, \ldots, t_n$ are positive real numbers. Then,

$$\Theta(\Omega^{-1}\vec{x}, -\Omega^{-1}) = \det\left(\frac{\Omega}{i}\right)^{1/2} \exp\{\pi i x^\top \Omega^{-1} x\} \Theta(\vec{x}, \Omega), \tag{5.87}$$

where $\vec{x} = (x_1, \ldots, x_g) \in \mathbb{R}^g$.

Proof. The inverse to the matrix Ω is,

$$\begin{pmatrix} -\frac{i}{t_1} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & -\frac{i}{t_g} \end{pmatrix}. \tag{5.88}$$

Then, by factoring $\Theta(\vec{x}, \Omega)$,

$$\begin{aligned} \Theta(\vec{x}, \Omega) &= \sum_{n_1,\ldots,n_g} \exp\{\pi i (it_1 n_1^2 + \cdots + it_g n_g^2)\} \exp\{2\pi i (x_1 n_1 + \cdots x_g n_g)\} \\ &= \sum_{n_1,\ldots,n_g} \exp\{-\pi (t_1 n_1^2 + \cdots + t_g n_g^2)\} \exp\{2\pi i (x_1 n_1 + \cdots x_g n_g)\} \\ &= \sum_{n_1 \in \mathbb{Z}} \exp\{-\pi t_1 n_1^2 + 2\pi i x_1 n_1\} \sum_{n_2,\ldots,n_g} \exp\{-\pi (t_2 n_2^2 + \cdots + t_g n_g^2)\} \exp\{2\pi i (x_2 n_2 + \cdots x_g n_g)\}. \end{aligned} \tag{5.89}$$

Applying (5.50) on the exponential in the sum over n_1 gives,

$$\Theta(\vec{x}, \Omega) = \frac{1}{\sqrt{t_1}} \exp\{-\pi x_1^2 / t_1\} \sum_{m_1 \in \mathbb{Z}} \exp\left\{\frac{-\pi m_1^2 + 2\pi x_1 m_1}{t_1}\right\} \sum_{n_2,\ldots,n_g} \exp\{-\pi (t_2 n_2^2 + \cdots + t_g n_g^2)\}. \tag{5.90}$$

Iterating this process for the sums over $n_2, \ldots, n_g$ gives,

$$\Theta(\vec{x}, \Omega) = \frac{1}{\sqrt{t_1 \cdots t_g}} \exp\{-\pi x_1^2 / t_1 - \cdots - \pi x_g^2 / t_g\} \sum_{m_1,\ldots,m_g} \exp\left\{\frac{-\pi m_1^2}{t_1} + \cdots + \frac{-\pi m_g^2}{t_g}\right\} \exp\left\{\frac{2\pi x_1 m_1}{t_1} + \cdots + \frac{2\pi x_g m}{t_g} \right. \tag{5.91}$$

Using that the determinant of a diagonal matrix is the product of the diagonal entries we compute,

$$\det\left(\frac{\Omega}{i}\right) = t_1 \cdots t_g. \tag{5.92}$$

By simple computation we also obtain

$$x^\top \Omega^{-1} x = \frac{x_1^2}{it_1} + \cdots + \frac{x_g^2}{it_g}\,, \tag{5.93}$$

so by (5.91), (5.92) and (5.93),

$$\det\left(\frac{\Omega}{i}\right)^{1/2} \exp\{\pi i x^\top \Omega^{-1} x\}\Theta(\vec{x},\Omega) = \sum_{m_1,\ldots,m_n} \exp\left\{\frac{-\pi m_1^2}{t_1} + \cdots + \frac{-\pi m_g^2}{t_g}\right\} \exp\left\{\frac{2\pi x_1 m_1}{t_1} + \cdots + \frac{2\pi x_g m_g}{t_g}\right\} \tag{5.94}$$

giving the right hand side of (5.87).

On the other hand

$$\Omega^{-1}\vec{x} = \begin{pmatrix} x_1/it_1 \\ \vdots \\ x_g/it_g \end{pmatrix} = \frac{1}{i}\begin{pmatrix} x_1/t_1 \\ \vdots \\ x_g/t_g \end{pmatrix} \tag{5.95}$$

so,

$$\Theta(\Omega^{-1}\vec{x}, -\Omega^{-1}) = \sum_{m_1,\ldots,m_n} \exp\left\{\frac{-\pi m_1^2}{t_1} + \cdots + \frac{-\pi m_g^2}{t_g}\right\} \exp\left\{\frac{2\pi x_1 m_1}{t_1} + \cdots + \frac{2\pi x_g m_g}{t_g}\right\} \tag{5.96}$$

giving the left hand side of (5.87).

□

6 Hecke's Theta Function and the Main Gauss Sum Identity

In this section we will look at a specialized case of the Siegel Theta function, which we will call Hecke's Theta Function. In this section we will obtain Hecke's theta inversion, using the modular properties of section 5.5. Afterwards we will examine the limits of Hecke's theta function. Since these curious functions are closely related to Gauss sums, our theta inversion will eventually give us that main identity (property (d) of Theorem 4.3).

6.1 Hecke's Theta Function

6.1.1. Let K be an arbitrary number field with dimension of n and let $\mathfrak{a}$ be an ideal or fractional ideal. We will number the conjugates for any $\mu \in K$ as in (3.4).

Define t_p such that $t_p > 0$ for all $p = 1, \dots, n$ and $t_{p+r_2} = t_p$ for all $p = r_1+1, \dots, r_1+r_2$ and take $z, \omega \in K$.

We define Hecke's theta function, where t represents the n-tuple $(t_1, \dots, t_n)$, as,

$$\theta_H(t,z,\omega;\mathfrak{a}) = \sum_{\mu \in \mathfrak{a}} \exp\left\{ -\pi \sum_{p=1}^{n} t_p |\mu^{(p)} + z^{(p)}|^2 + 2\pi i \sum_{p=1}^{n} (\mu^{(p)} + z^{(p)})^2 \omega^{(p)} \right\}. \tag{6.1}$$

Let $\alpha_1, \dots, \alpha_n$ be a basis for $\mathfrak{a}$ with conjugates ordered as in (3.4), so

$$\mu = \sum_{k=1}^{n} \alpha_k m_k \quad \text{for } m_1, \dots, m_n \in \mathbb{Z} \tag{6.2}$$

then as μ runs through all numbers in $\mathfrak{a}$, then $m_1, \dots, m_n$ run through all integers in $\mathbb{Z}$. Hence by Theorem 5.1.2, Hecke's theta function (6.1) converges absolutely.

It is easy to see how it is periodic in z, as

$$\theta_H(t,z,\omega;\mathfrak{a}) = \theta_H(t,z+\mu',\omega;\mathfrak{a}) \tag{6.3}$$

for any $\mu' \in \mathfrak{a}$.

6.1.2. If we take $n = 1$, $z = 0$ and $\mathfrak{a} = \mathbb{Z}$ it is easy to see how θ_H reduces to the one-dimensional theta function discussed in section 5.2. Namely,

$$\theta_H(t,0,\omega;\mathbb{Z}) = \theta(0, it + 2\omega). \tag{6.4}$$

To get a better idea where Hecke's theta function comes from. Each summand of the series gives us a vector in the complex plane where t gives the length of that vector and ω gives the rotation of that vector. For larger n, we are summing over a higher dimensional lattice. Summing over the ideal $\mathfrak{a}$ is akin to a *stretch* of the lattice over $\mathbb{Z}^n$ to another isomorphic one. Where summing over an ideal is like a stretch, the z component is a *shift* of the lattice over $\mathfrak{a}$ to another isomorphic one.

6.1.3. We can also view Hecke's theta function as a special case of the Siegel-Jacobi Theta Function. In order to obtain Hecke's Theta Function we define $\Omega_0 \in \mathfrak{H}_n$ to be the matrix,

$$\Omega_0 := (a_{kj}) \quad \text{where} \quad a_{kj} = \begin{cases} it_k + 2\omega^{(k)} & \text{for } k = j \leq r_1 \\ 2\omega^{(k)} & \text{for } k = j > r_1 \\ it_k & \text{for } k, j > r_1; \;\; k = j \pm r_2 \\ 0 & \text{otherwise.} \end{cases} \tag{6.5}$$

Here is an example for $r_1 = 2$, $r_2 = 3$,

$$\begin{pmatrix} it_1 + 2\omega^{(1)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & it_2 + 2\omega^{(2)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2\omega^{(3)} & 0 & 0 & it_3 & 0 & 0 \\ 0 & 0 & 0 & 2\omega^{(4)} & 0 & 0 & it_4 & 0 \\ 0 & 0 & 0 & 0 & 2\omega^{(5)} & 0 & 0 & it_5 \\ 0 & 0 & it_3 & 0 & 0 & 2\omega^{(6)} & 0 & 0 \\ 0 & 0 & 0 & it_4 & 0 & 0 & 2\omega^{(7)} & 0 \\ 0 & 0 & 0 & 0 & it_5 & 0 & 0 & 2\omega^{(8)} \end{pmatrix}. \tag{6.6}$$

It is easy to see that Ω_0 is symmetric with positive imaginary part, so it really is inside $\mathfrak{H}_n$.

For the number field K let the basis for the ideal $\mathfrak{a}$ be $\alpha_1, \dots, \alpha_n$ with the conjugates ordered as in (3.4). We define the matrix

$$A = \begin{pmatrix} \alpha_1^{(1)} & \alpha_1^{(2)} & \cdots & \alpha_1^{(n)} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_n^{(1)} & \alpha_n^{(2)} & \cdots & \alpha_n^{(n)} \end{pmatrix} \tag{6.7}$$

First notice that

$$A\vec{m} = \begin{pmatrix} \alpha_1^{(1)} & \alpha_2^{(1)} & \cdots & \alpha_n^{(1)} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{(n)} & \alpha_2^{(n)} & \cdots & \alpha_n^{(n)} \end{pmatrix} \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} \alpha_1^{(1)} m_1 + \cdots + \alpha_n^{(1)} m_n \\ \vdots \\ \alpha_1^{(n)} m_1 + \cdots + \alpha_n^{(n)} m_n \end{pmatrix} = \begin{pmatrix} \mu^{(1)} \\ \vdots \\ \mu^{(n)} \end{pmatrix}, \tag{6.8}$$

where μ as in (6.2) is an arbitrary number in $\mathfrak{a}$. If we let

$$\vec{\mu} := \begin{pmatrix} \mu^{(1)} \\ \vdots \\ \mu^{(n)} \end{pmatrix} = A\vec{m} \tag{6.9}$$

with the conjugates of μ are ordered as in (3.4), then as $m_1, \dots, m_n$ run through all integers in $\mathbb{Z}$, then μ runs through all numbers in the ideal $\mathfrak{a}$.

Proposition. *The matrix $A^\top \Omega_0 A$ belongs to $\mathfrak{H}_n$ and*

$$\Theta(0, A^\top \Omega_0 A) = \theta_H(t, 0, \omega; \mathfrak{a})\,. \tag{6.10}$$

where Ω_0 is as in (6.5) *and A is as in* (6.7).

Proof. We must verify that $A^\top \Omega_0 A$ is symmetric, and its imaginary part is positive definite. The symmetric part follows immediately since Ω_0 is symmetric.

To see it is positive definite we need to compute the product $\vec{m}^\top A^\top \Omega_0 A \vec{m}$. Since as $m_1, \ldots, m_n$ run through the rational integers, then by (6.9) we have $A\vec{m} = \vec{\mu}$ and $\vec{m}^\top A^\top = \vec{\mu}^\top$ run through all $\mu \in \mathfrak{a}$. Therefore we are left to compute the product $\vec{\mu}^\top \Omega_0 \vec{\mu}$.

Consider the first r_1 terms from the upper left corner of Ω_0,

$$\sum_{p=1}^{r_1} \left[\mu^{(p)}(it_p + 2\omega^{(p)})\mu^{(p)}\right] = \sum_{p=1}^{r_1} \left[(it_p + 2\omega^{(p)})\mu^{(p)^2}\right] = \sum_{p=1}^{r_1} \left[it_p|\mu^{(p)}|^2 + 2\omega^{(p)}\mu^{(p)^2}\right]. \tag{6.11}$$

Using the fact that $\mu^{(p+r_2)}$ and $\mu^{(p)}$ are complex conjugates for $p = r_1+1, \ldots, r_1+r_2$, the remaining $2r_2$ terms from the bottom right corner of Ω_0 are,

$$\sum_{p=r_1+1}^{n} \left[it_p \mu^{(p)}\overline{\mu^{(p)}} + 2\omega^{(p)}\mu^{(p)^2}\right] = \sum_{p=r_1+1}^{n} \left[it_p|\mu^{(p)}|^2 + 2\omega^{(p)}\mu^{(p)^2}\right]. \tag{6.12}$$

From here it is easy to see that the imaginary part is positive for arbitrary rational integers $m_1, \ldots, m_n$. Therefore $A^\top \Omega_0 A \in \mathfrak{H}_n$, proving the first part of the theorem. Furthermore from this computation we can see immediately the relation to Hecke's Theta Function. Namely, the exponent in $\Theta(0, A^\top \Omega_0 A)$ is

$$i\pi \sum_{p=1}^{n} \left[it_p|\mu^{(p)}|^2 + 2\omega^{(p)}\mu^{(p)^2}\right] = -\pi \sum_{p=1}^{n} \left[t_p|\mu^{(p)}|^2 + 2i\omega^{(p)}\mu^{(p)^2}\right], \tag{6.13}$$

which is exactly the exponent to Hecke's theta function. □

6.1.4. We can see how (6.1) relates to the Siegel-Jacobi theta function in (5.58). Take $u_1, \ldots, u_n \in \mathbb{Q}$ as the unique solution to the n equations given by

$$z^{(p)} = \sum_{k=1}^{n} \alpha_k^{(p)} u_k \qquad \text{for } p = 1, \ldots, n. \tag{6.14}$$

Then for $\vec{u} = (u_1, \ldots, u_n) \in \mathbb{Q}^n$ and by Proposition 6.1.3 we have,

$$\Theta\begin{bmatrix}\vec{u}\\0\end{bmatrix}(0, A^\top \Omega_0 A) = \theta_H(t, z, \omega; \mathfrak{a})\,. \tag{6.15}$$

6.2 Using Modular properties to obtain Hecke's Theta Inversion

6.2.1. Using the modular property in (5.66) we wish to show Hecke's theta inversion. First we need a lemma.

Lemma. *Let $\Omega = A^\top \Omega_0 A$ with A as in* (6.7) *and Ω_0 as in* (6.5). *Then,*

(a)

$$\det\left(\frac{\Omega}{i}\right)^{1/2} = N(a)|\sqrt{d_K}| \prod_{p=1}^{r_1} \sqrt{t_p - 2i\omega^{(p)}} \cdot \prod_{p=r_1+1}^{r_1+r_2} \sqrt{t_p^2 + 4|\omega^{(p)}|^2}, \tag{6.16}$$

(b)

$$-\Omega^{-1} = B^\top \Omega_1 B \tag{6.17}$$

where B is the matrix,

$$B = \begin{pmatrix} \beta_1^{(1)} & \beta_1^{(2)} & \cdots & \beta_1^{(n)} \\ \vdots & \vdots & \vdots & \vdots \\ \beta_n^{(1)} & \beta_n^{(2)} & \cdots & \beta_n^{(n)} \end{pmatrix}, \tag{6.18}$$

with $\beta_1, \dots, \beta_n$ and their conjugates are a basis for $\mathfrak{a}^\vee$ obtained as in Corollary 3.5 and Ω_1 is the matrix (b_{kj}),

$$b_{kj} = \begin{cases} i\tau_k + 2\chi^{(k)} & \textit{for } k = j \le r_1 \\ 2\chi^{(k)} & \textit{for } k = j > r_1 \\ i\tau_k & \textit{for } k, j > r_1; \;\; k = j \pm r_2 \\ 0 & \textit{otherwise,} \end{cases} \tag{6.19}$$

where

$$\tau_p = \frac{t_p}{t_p^2 + 4|\omega^{(p)}|^2} \qquad \chi^{(p)} = -\frac{\overline{\omega^{(p)}}}{t_p^2 + 4|\omega^{(p)}|^2}. \tag{6.20}$$

Proof. For computation (a) we wish to find the determinant,

$$\det\left(\frac{1}{i}\Omega\right) = \det(A^\top)\det\left(\frac{\Omega_0}{i}\right)\det(A) = \det(A)^2 \det\left(\frac{\Omega_0}{i}\right). \tag{6.21}$$

By (3.26) we have the determinant of A is,

$$\left(\det(A)^2\right)^{1/2} = |\Delta(\alpha_1, \dots \alpha_n)| = N(a)|\sqrt{d_K}|. \tag{6.22}$$

To compute the determinant of $\frac{\Omega_0}{i}$, we have by (6.5) this is exactly the matrix $(\frac{1}{i}a_{kj})$ where,

$$\frac{1}{i}a_{kj} = \begin{cases} t_k - 2i\omega^{(k)} & \text{for } k = j \leq r_1 \\ -2i\omega^{(k)} & \text{for } k = j > r_1 \\ t_k & \text{for } k, j > r_1;\ \ k = j \pm r_2 \\ 0 & \text{otherwise.} \end{cases} \tag{6.23}$$

Let C be a diagonal $r_1 \times r_1$ matrix and D_p be a 2×2 matrix for $p = r_1 + 1, \dots, r_1 + r_2$ such that,

$$C = \begin{pmatrix} t_1 - 2i\omega^{(1)} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & t_{r_1} - 2i\omega^{(r_1)} \end{pmatrix} \qquad D_p = \begin{pmatrix} -2i\omega^{(p)} & t_p \\ t_p & -2i\omega^{(p+r_2)} \end{pmatrix} \tag{6.24}$$

Using the property,

$$\det \begin{pmatrix} E & 0 \\ 0 & F \end{pmatrix} = \det(E)\det(F) \qquad \text{for square matricies } E, F \tag{6.25}$$

we get

$$\begin{aligned} \det\left(\frac{\Omega_0}{i}\right) &= \det(C) \prod_{p=r_1+1}^{r_1+r_2} \det(D_p) \\ &= \prod_{p=1}^{r_1} t_p - 2i\omega^{(p)} \cdot \prod_{p=r_1+1}^{r_1+r_2} t_p^2 - (i^2\omega^{(p)}\omega^{(p+r_2)}) \\ &= \prod_{p=1}^{r_1} t_p - 2i\omega^{(p)} \cdot \prod_{p=r_1+1}^{r_1+r_2} t_p^2 + |\omega^{(p)}|^2, \end{aligned} \tag{6.26}$$

therefore by (6.22) and (6.26) we can compute the determinant in (6.21),

$$\det\left(\frac{\Omega}{i}\right)^{1/2} = N(a)|\sqrt{d_K}| \prod_{p=1}^{r_1} \sqrt{t_p - 2i\omega^{(p)}} \cdot \prod_{p=r_1+1}^{r_1+r_2} \sqrt{t_p^2 + 4|\omega^{(p)}|^2}, \tag{6.27}$$

concluding part (a).

For part (b) we need to find the inverse to the matrix $\Omega = A^\top \Omega_0 A$. Using the matrix B in (6.18), by Corollary 3.5, we have $AB^\top = I$ as,

$$\begin{pmatrix} \alpha_1^{(1)} & \alpha_1^{(2)} & \cdots & \alpha_1^{(n)} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_n^{(1)} & \alpha_n^{(2)} & \cdots & \alpha_n^{(n)} \end{pmatrix} \begin{pmatrix} \beta_1^{(1)} & \beta_2^{(1)} & \cdots & \beta_n^{(1)} \\ \vdots & \vdots & \vdots & \vdots \\ \beta_1^{(n)} & \beta_2^{(n)} & \cdots & \beta_n^{(n)} \end{pmatrix} = \begin{pmatrix} S(\alpha_1\beta_1) & S(\alpha_1\beta_2) & \cdots & S(\alpha_1\beta_n) \\ \vdots & \vdots & \vdots & \vdots \\ S(\alpha_n\beta_1) & S(\alpha_n\beta_2) & \cdots & S(\alpha_n\beta_n) \end{pmatrix} \tag{6.28}$$

which by Corollary 3.5 is exactly the identity matrix. Similarly we get $A^\top B = I$, but here we use the property (3.37).

We will compute the inverse to Ω_0. Using matrices C and D_p as in (6.24) we may compute their inverses. For C we find the inverse,

$$C^{-1} = \begin{pmatrix} \frac{1}{t_1 - 2i\omega^{(1)}} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \frac{1}{t_{r_1} - 2i\omega^{(r_1)}} \end{pmatrix} = \begin{pmatrix} \frac{t_1 + 2i\omega^{(1)}}{t_1^2 + 4|\omega^{(1)}|^2} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \frac{t_{r_1} + 2i\omega^{(r_1)}}{t_{r_1}^2 + 4|\omega^{(r_1)}|^2} \end{pmatrix} \tag{6.29}$$

where we used, for $p = 1, \dots, r_1$ so $\omega^{(p)}$ real,

$$\frac{1}{t_p - 2i\omega^{(p)}} = \frac{1}{t_p - 2i\omega^{(p)}} \frac{t_p + 2i\omega^{(p)}}{t_p + 2i\omega^{(p)}} = \frac{t_p + 2i\omega^{(p)}}{t_p^2 + 4|\omega^{(p)}|^2} \quad \text{for } p = 1, \dots, r_1\,. \tag{6.30}$$

For D_p where $p = r_1 + 1, \dots, r_1 + r_2$ we find the inverse,

$$D_p^{-1} = \frac{1}{-4|\omega^{(p)}|^2 - t_p^2} \begin{pmatrix} -2i\omega^{(p+r_2)} & -t_p \\ -t_p & -2i\omega^{(p)} \end{pmatrix} = \frac{1}{t_p^2 + 4|\omega^{(p)}|^2} \begin{pmatrix} 2i\omega^{(p+r_2)} & t_p \\ t_p & 2i\omega^{(p)} \end{pmatrix} \tag{6.31}$$

However, recall the matrices C, D_p from (6.24) were blocks to the matrix $\frac{1}{i}\Omega_0$. Therefore iC and iD_p are the matrices which form the same blocks in Ω_0. The property

$$\begin{pmatrix} E & 0 \\ 0 & F \end{pmatrix}^{-1} = \begin{pmatrix} E^{-1} & 0 \\ 0 & F^{-1} \end{pmatrix} \qquad \text{for invertible matricies } E, F \tag{6.32}$$

tells us that since iC and iD_p form blocks in Ω_0, then

$$(iC)^{-1} = -iC^{-1}\,, \qquad (iD_p)^{-1} = -iD_p^{-1} \tag{6.33}$$

form the blocks of Ω_0^{-1}. Using (6.29) and (6.31) we obtain the inverse to Ω_0 as $\Omega_0^{-1} = (-b_{kj})$ where b_{kj} is as in (6.34). In essence,

$$-b_{kj} = \begin{cases} -\dfrac{it_k - 2\omega^{(k)}}{t_k^2 + 4|\omega^{(k)}|^2} & \text{for } k = j \leq r_1 \\[2ex] -\dfrac{-2\overline{\omega^{(k)}}}{t_k^2 + 4|\omega^{(k)}|^2} & \text{for } k = j > r_1 \\[2ex] -\dfrac{it_k}{t_k^2 + 4|\omega^{(k)}|^2} & \text{for } k, j > r_1; \;\; k = j \pm r_2 \\[2ex] \qquad 0 & \text{otherwise.} \end{cases} \tag{6.34}$$

If we take *tau* and *chi* as in (6.20) then we get,

$$b_{kj} = \begin{cases} i\tau_k + 2\chi^{(k)} & \text{for } k = j \leq r_1 \\ 2\chi^{(k)} & \text{for } k = j > r_1 \\ i\tau_k & \text{for } k, j > r_1;\ \ k = j \pm r_2 \\ 0 & \text{otherwise.} \end{cases} \tag{6.35}$$

Therefore by (6.18) and (6.34) we have

$$A^\top \Omega_0 A B^\top \Omega_0^{-1} B = I \tag{6.36}$$

so that

$$\Omega^{-1} = (A^\top \Omega_0 A)^{-1} = B^\top \Omega_0^{-1} B, \tag{6.37}$$

which implies, defining $\Omega_1 := -\Omega_0^{-1} = (b_{kj})$ with b_{kj} as in (6.35),

$$-\Omega^{-1} = B^\top \Omega_1 B, \tag{6.38}$$

concluding part (b). □

We can now prove Hecke's theta inversion in the following theorem.

Theorem. *With τ representing the n-tuple $(\tau_1, \ldots, \tau_n)$, $\chi \in K$ and $t, \omega, \mathfrak{a}$ as in* (6.1)*, we have,*

$$\theta_H(\tau, 0, \chi; \mathfrak{a}^\vee) = N(\mathfrak{a})|\sqrt{d_K}|W(t,\omega)\theta_H(t, 0, \omega; \mathfrak{a}), \tag{6.39}$$

where

$$W(t,\omega) = \prod_{p=1}^{r_1} \sqrt{t_p - 2i\omega^{(p)}} \cdot \prod_{p=r_1+1}^{r_1+r_2} \sqrt{t_p^2 + 4|\omega^{(p)}|^2}, \tag{6.40}$$

$$\tau_p = \frac{t_p}{t_p^2 + 4|\omega^{(p)}|^2}, \qquad \chi^{(p)} = \frac{-\overline{\omega}^{(p)}}{t_p^2 + 4|\omega^{(p)}|^2}. \tag{6.41}$$

Proof. From (5.66) with $\vec{s} = 0$ we have,

$$\Theta(0, -\Omega^{-1}) = \det(\Omega/i)^{1/2}\Theta(0, \Omega). \tag{6.42}$$

We will let $\Omega = A^\top \Omega_0 A$ with A as in (6.7) and Ω_0 as in (6.5). By Proposition 6.1.3,

$$\Theta(0, \Omega) = \Theta(0, A^\top \Omega_0 A) = \theta_H(t, 0, \omega; \mathfrak{a}). \tag{6.43}$$

Using (6.35) and that $\beta_1, \ldots, \beta_n$ form a basis for the ideal $1/\mathfrak{a}\mathfrak{d} = \mathfrak{a}^\vee$ gives

$$\Theta(0, -\Omega^{-1}) = \Theta(0, B^\top \Omega_0^{-1} B) = \theta_H(\tau, 0, \chi; \mathfrak{a}^\vee), \tag{6.44}$$

This, along with Lemma 6.2.1 in (6.42), complete the proof. □

6.3 Limits of the Theta Series

Lemma. *Let $\sigma_p = t_p c^{(p)}$ for $c \in K$ with conjugates ordered as in* (3.4)*. Then,*

$$\lim_{t\to 0}\sqrt{t_1 t_2\cdots t_n}\,\theta_H(t,z,t\sigma;\mathfrak{a}) = \frac{1}{N(\mathfrak{a})|\sqrt{d_K}|}\,. \tag{6.45}$$

Proof. By (5.59) we have,

$$\Theta\begin{bmatrix}\vec{u}\\0\end{bmatrix}(0,\Omega) = e^{\pi i\vec{u}^\top\Omega\vec{u}}\Theta(\Omega\vec{u},\Omega) \tag{6.46}$$

and by (5.66),

$$\Theta(\vec{s},\Omega) = \det(\Omega/i)^{-1/2}\Theta(\Omega^{-1}\vec{s},-\Omega^{-1})e^{-\pi i\vec{s}^\top\Omega^{-1}\vec{s}} \tag{6.47}$$

therefore

$$\begin{aligned} e^{\pi i\vec{u}^\top\Omega\vec{u}}\Theta(\Omega\vec{u},\Omega) &= e^{\pi i\vec{u}^\top\Omega\vec{u}}\det(\Omega/i)^{-1/2}\Theta\big(\Omega^{-1}(\Omega\vec{u}),-\Omega^{-1}\big)e^{-\pi i(\Omega\vec{u})^\top\Omega^{-1}(\Omega\vec{u})}\\ &= \det(\Omega/i)^{-1/2}\Theta(\vec{u},-\Omega^{-1})e^{\pi i\vec{u}^\top\Omega\vec{u}}e^{-\pi i\vec{u}^\top\Omega\vec{u}}\\ &= \det(\Omega/i)^{-1/2}\Theta(\vec{u},-\Omega^{-1})\,. \end{aligned} \tag{6.48}$$

So by (6.46) and (6.48),

$$\Theta\begin{bmatrix}\vec{u}\\0\end{bmatrix}(0,\Omega) = \det(\Omega/i)^{-1/2}\Theta\big(\vec{u},-\Omega^{-1}\big)\,. \tag{6.49}$$

If we take $\Omega = A^\top\Omega_0 A$ as in Proposition 6.1.3 we have by (6.15), where

$$z^{(p)} = \sum_{k=1}^{n}\alpha_k^{(p)}u_k\,, \tag{6.50}$$

then,

$$\Theta\begin{bmatrix}\vec{u}\\0\end{bmatrix}(0,\Omega) = \theta_H(t,z,\omega;\mathfrak{a})\,. \tag{6.51}$$

Furthermore by part (a) of Lemma 6.2.1,

$$\det(\Omega/i)^{1/2} = N(\mathfrak{a})|\sqrt{d_K}|W(t,t\sigma)\,, \tag{6.52}$$

hence,

$$\theta_H(t,z,\omega;\mathfrak{a}) = \frac{1}{N(\mathfrak{a})|\sqrt{d_K}|W(t,t\sigma)}\Theta\big(\vec{u},-\Omega^{-1}\big)\,. \tag{6.53}$$

Therefore with $\omega^{(p)} = t_p\sigma_p$, written for brevity as $\omega = t\sigma$, we have,

$$\lim_{t\to 0}\sqrt{t_1t_2\cdots t_n}\,\theta_H(t,z,t\sigma;\mathfrak{a}) = \lim_{t\to 0}\frac{\sqrt{t_1t_2\cdots t_n}}{N(\mathfrak{a})|\sqrt{d_K}|W(t,t\sigma)}\Theta\big(\vec{u},-\Omega^{-1}\big)$$
$$= \frac{1}{N(\mathfrak{a})|\sqrt{d_K}|}\lim_{t\to 0}\left(\frac{\sqrt{t_1t_2\cdots t_n}}{W(t,t\sigma)}\right)\lim_{t\to 0}\Theta\big(\vec{u},-\Omega^{-1}\big)\,. \tag{6.54}$$

However since,

$$\lim_{t\to 0}\frac{\sqrt{t_1t_2\cdots t_n}}{W(t,t\sigma)} = \lim_{t\to 0}\frac{\sqrt{t_1t_2\cdots t_n}}{\prod_{p=1}^{r_1}\sqrt{t_p-2it_p\overline{\sigma_p}}\cdot\prod_{p=r_1+1}^{r_1+r_2}\sqrt{t_p^2+4t_p|\sigma_p|^2}}$$
$$= \lim_{t\to 0}\frac{1}{\prod_{p=1}^{r_1}\sqrt{1-2\overline{\sigma_p}}\cdot\prod_{p=r_1+1}^{r_1+r_2}\sqrt{1+4|\sigma_p|^2}} = 1\,, \tag{6.55}$$

we are left to consider

$$\lim_{t\to 0}\Theta\big(\vec{u},-\Omega^{-1}\big)\,. \tag{6.56}$$

We start with a claim.

Claim. *For any $\vec{m}\in\mathbb{Z}^n/\{0\}$, with Ω as in Proposition 6.1.3 and $\omega = t\sigma$,*

$$\lim_{t\to 0} e^{-\vec{m}^\top\Omega^{-1}\vec{m}} = 0 \tag{6.57}$$

Proof. Using Ω^{-1} as in part (b) of Lemma 6.2.1, we obtain, for some $\lambda\in\mathfrak{a}^\vee$,

$$e^{-\vec{m}^\top\Omega^{-1}\vec{m}} = \exp\left\{-\pi\sum_{p=1}^{n}\left(\frac{t_p}{t_p^2+4|t_p\sigma_p|^2}|\lambda^{(p)}|^2+\frac{2it_p\overline{\sigma_p}}{t_p^2+4|t_p\sigma_p|^2}\lambda^{(p)^2}\right)\right\}$$
$$= \exp\left\{-\pi\sum_{p=1}^{n}\left(\frac{1}{t_p(1+4|\sigma_p|^2)}|\lambda^{(p)}|^2+\frac{2i\overline{c^{(p)}}}{1+4|\sigma_p|^2}\lambda^{(p)^2}\right)\right\} \tag{6.58}$$

which clearly converges to 0 as t_p approaches 0 from the right for all $p = 1,\ldots,n$. □

Consider the limit,

$$\begin{aligned}\lim_{t\to 0}\left|\Theta(\vec{u},-\Omega^{-1})-1\right| &= \lim_{t\to 0}\left|\sum_{\vec{m}\in\mathbb{Z}^n}\exp\{-\pi i\vec{m}^\top\Omega^{-1}\vec{m}+2\pi i\vec{m}^\top\vec{u}\}-1\right| \\ &= \lim_{t\to 0}\left|\sum_{\vec{m}\in\mathbb{Z}^n/\{0\}}\exp\{-\pi i\vec{m}^\top\Omega^{-1}\vec{m}+2\pi i\vec{m}^\top\vec{u}\}\right| \\ &= \lim_{t\to 0}\left|\sum_{\vec{m}\in\mathbb{Z}^n/\{0\}}\exp\{-\pi i\vec{m}^\top\Omega^{-1}\vec{m}\}\right| \\ &= 0\end{aligned} \tag{6.59}$$

where the final line follows from Claim 6.3. Therefore

$$\lim_{t\to 0}\Theta\big(\vec{u},-\Omega^{-1}\big)=1\,. \tag{6.60}$$

Therefore from (6.54) using (6.55) and (6.60) for the limits, we have that

$$\lim_{t\to 0}\sqrt{t_1t_2\cdots t_n}\,\theta_H(t,z,t\sigma;\mathfrak{a})=\frac{1}{N(\mathfrak{a})|\sqrt{d_K}|}\,. \tag{6.61}$$

□

6.4 Proof of Main Identity on Gauss Sums

Take ω to be a non-zero number in K and let $\mathfrak{d}\omega$ be writen as,

$$\mathfrak{d}\omega=\frac{\mathfrak{b}}{\mathfrak{a}}\,, \tag{6.62}$$

for relatively prime ideals $\mathfrak{a},\mathfrak{b}$. We will call the denominator of $\frac{\mathfrak{a}}{4\mathfrak{b}}$ the ideal $\mathfrak{b}_1$. By Corollary 3.3.7 there exists a $\gamma\in K$ such that

$$\mathfrak{d}\gamma=\mathfrak{c}_1 \quad \text{where } \mathfrak{c}_1 \text{ is an ideal relatively prime to } \mathfrak{b}_1. \tag{6.63}$$

6.4.1. We will first investigate the right hand side of (6.39), when we sum over the ring of integers. We can write μ as it runs through all elements in $\mathscr{O}_k$ as $\mu=\nu+\rho$ as ν runs through all elements in $\mathfrak{a}$ and ρ runs through all residue classes mod $\mathfrak{a}$. Then,

$$\begin{aligned}\theta_H(t,0,\omega;\mathscr{O}_K) &= \sum_{\mu\in\mathscr{O}_k} \exp\left\{-\pi\sum_{p=1}^{n} t_p|\mu^{(p)}|^2 + 2\pi i\sum_{p=1}^{n}\omega^{(p)}(\mu^{(p)})^2\right\}\\ &= \sum_{\rho \bmod \mathfrak{a}}\left\{\sum_{\nu\in\mathfrak{a}}\exp\left\{-\pi\sum_{p=1}^{n} t_p|\nu^{(p)}+\rho^{(p)}|^2 + 2\pi i\sum_{p=1}^{n}\omega^{(p)}(\nu^{(p)}+\rho^{(p)})^2\right\}\right\},\end{aligned} \tag{6.64}$$

and since $e^{2\pi i\,\mathrm{tr}(\eta\omega)}$ only depends on the residue class η (mod $\mathfrak{a}$),

$$\begin{aligned}\theta_H(t,0,\omega;\mathscr{O}_K) &= \sum_{\rho \bmod \mathfrak{a}}\left\{\sum_{\nu\in\mathfrak{a}}\exp\left\{-\pi\sum_{p=1}^{n} t_p|\nu^{(p)}+\rho^{(p)}|^2\right\}e^{2\pi i\,\mathrm{tr}(\rho^2\omega)}\right\}\\ &= \sum_{\rho \bmod \mathfrak{a}}\theta_H(t,\rho,0;\mathfrak{a})e^{2\pi i\,\mathrm{tr}(\rho^2\omega)}.\end{aligned} \tag{6.65}$$

Taking the limit as t approaches 0, interchanging the sum and the limit gives,

$$\lim_{t\to 0}\sqrt{t_1\cdots t_n}\,\theta_H(t,0,\omega;\mathscr{O}_K) = \sum_{\rho \bmod \mathfrak{a}}\lim_{t\to 0}\sqrt{t_1\cdots t_n}\,\theta_H(t,\rho,0;\mathfrak{a})e^{2\pi i\,\mathrm{tr}(\rho^2\omega)}. \tag{6.66}$$

Applying Lemma 6.3 to the left hand side of (6.66) gives

$$\lim_{t\to 0}\sqrt{t_1\cdots t_n}\,\theta_H(t,0,\omega;\mathscr{O}_K) = \sum_{\rho \bmod \mathfrak{a}}\frac{1}{N(\mathfrak{a})|\sqrt{d_K}|}e^{2\pi i\,\mathrm{tr}(\rho^2\omega)} = \frac{1}{N(\mathfrak{a})|\sqrt{d_K}|}\sum_{\rho \bmod \mathfrak{a}}e^{2\pi i\,\mathrm{tr}(\rho^2\omega)} \tag{6.67}$$

so using the definition of the Gauss sum as in (4.11),

$$\lim_{t\to 0}\sqrt{t_1\cdots t_n}\,\theta_H(t,0,\omega;\mathscr{O}_K) = \frac{\mathbb{g}(\omega)}{N(\mathfrak{a})|\sqrt{d_K}|}. \tag{6.68}$$

6.4.2. Now we will investigate the right hand side of (6.39). As the dual of $\mathscr{O}_K$ is $\frac{1}{\mathfrak{d}}$ by (3.44), then our sum will be over all numbers in $\frac{1}{\mathfrak{d}}$. By Proposition 3.3.7 we introduce an ideal $\mathfrak{c}$ such that,

$$\mathfrak{c}\mathfrak{d} = \delta \quad \text{where } \delta\in\mathscr{O}_K \text{ and } \mathfrak{c} \text{ is relatively prime to } \mathfrak{b}_1. \tag{6.69}$$

Since $\frac{1}{\mathfrak{d}} = \frac{\mathfrak{c}}{\delta}$, then $\mu = \frac{\nu}{\delta}$ runs though all numbers in $\frac{1}{\mathfrak{d}}$ as ν runs though all numbers in $\mathfrak{c}$. Therefore,

$$\begin{aligned}\theta_H\left(\tau, 0, \chi; \frac{1}{\mathfrak{d}}\right) &= \sum_{\mu \in \frac{1}{\mathfrak{d}}} \exp\left\{-\pi \sum_{p=1}^{n} \tau_p |\mu^{(p)}|^2 + 2\pi i \sum_{p=1}^{n} \chi^{(p)} (\mu^{(p)})^2\right\} \\ &= \sum_{\nu \in \mathfrak{c}} \exp\left\{-\pi \sum_{p=1}^{n} \tau_p \left|\frac{\nu^{(p)}}{\delta^{(p)}}\right|^2 + 2\pi i \sum_{p=1}^{n} \chi^{(p)} \left(\frac{\nu^{(p)}}{\delta^{(p)}}\right)^2\right\} \\ &= \theta_H\left(\frac{\tau}{|\delta|^2}, 0, \frac{\chi}{\delta^2}; \mathfrak{c}\right).\end{aligned} \tag{6.70}$$

For any $\nu \in \mathfrak{c}$ we may view it as a residue modulo $\mathfrak{b}_1$. Since $\mathfrak{c}$ is relatively prime to $\mathfrak{b}_1$, then as η runs though all integers in $\mathfrak{b}_1\mathfrak{c}$ and ρ runs though residue classes mod $\mathfrak{b}_1$ with $\rho \in \mathfrak{c}$ then $\nu = \eta + \rho$ runs through all integers in $\mathfrak{c}$. Therefore,

$$\begin{aligned}\theta_H\left(\frac{\tau}{|\delta|^2}, 0, \frac{\chi}{\delta^2}; \mathfrak{c}\right) &= \sum_{\nu \in \mathfrak{c}} \exp\left\{-\pi \sum_{p=1}^{n} \frac{\tau_p}{|\delta^{(p)}|^2} |\nu^{(p)}|^2 + 2\pi i \sum_{p=1}^{n} \frac{\chi^{(p)}}{\delta^{(p)2}} (\nu^{(p)})^2\right\} \\ &= \sum_{\substack{\rho \bmod \mathfrak{b}_1 \\ \rho \equiv 0 (\mathfrak{c})}} \sum_{\eta \in \mathfrak{b}_1\mathfrak{c}} \exp\left\{-\pi \sum_{p=1}^{n} \frac{\tau_p}{|\delta^{(p)}|^2} |\eta^{(p)} + \rho^{(p)}|^2 + 2\pi i \sum_{p=1}^{n} \frac{\chi^{(p)}}{\delta^{(p)2}} (\eta^{(p)} + \rho^{(p)})^2\right\} \\ &= \sum_{\substack{\rho \bmod \mathfrak{b}_1 \\ \rho \equiv 0 (\mathfrak{c})}} \theta_H\left(\frac{\tau}{|\delta|^2}, \rho, \frac{\chi}{\delta^2}; \mathfrak{b}_1\mathfrak{c}\right).\end{aligned} \tag{6.71}$$

Defining $\sigma_p = t_p / 4\omega^{(p)}$, then from (6.20),

$$\chi^{(p)} = \frac{-\overline{\omega}}{t_p^2 + 4|\omega^{(p)}|^2} = -\frac{1}{\omega^{(p)}} + \frac{t_p^2}{4\omega^{(p)}(t_p^2 + 4|\omega^{(p)}|^2)} = -\frac{1}{4\omega^{(p)}} + \tau_p \sigma_p, \tag{6.72}$$

which means

$$\begin{aligned}\theta_H\left(\frac{\tau}{|\delta|^2}, \rho, \frac{\chi}{\delta^2}; \mathfrak{b}_1\mathfrak{c}\right) &= \theta_H\left(\frac{\tau}{|\delta|^2}, \rho, -\frac{1}{4\omega\delta^2} + \frac{\tau\sigma}{\delta^2}; \mathfrak{b}_1\mathfrak{c}\right) \\ &= e^{2\pi i \operatorname{tr}(-\rho^2/4\omega\delta^2)} \theta_H\left(\frac{\tau}{|\delta|^2}, \rho, \frac{\tau\sigma}{\delta^2}; \mathfrak{b}_1\mathfrak{c}\right).\end{aligned} \tag{6.73}$$

Combining (6.70), (6.71) and (6.73) gives,

$$\theta_H\left(\tau, 0, \chi; \frac{1}{\mathfrak{d}}\right) = \sum_{\substack{\rho \bmod \mathfrak{b}_1 \\ \rho \equiv 0 (\mathfrak{c})}} e^{2\pi i \operatorname{tr}(-\rho^2/4\omega\delta^2)} \theta_H\left(\frac{\tau}{|\delta|^2}, \rho, \frac{\tau\sigma}{\delta^2}; \mathfrak{b}_1\mathfrak{c}\right). \tag{6.74}$$

After multiplying both sides of (6.74) by

$$\sqrt{\frac{\tau_1 \cdots \tau_n}{\delta^{(1)} \dots \delta^{(n)}}} = \sqrt{\frac{\tau_1 \cdots \tau_n}{N(\delta)^2}} \tag{6.75}$$

and taking the limit as t approaches zero while swapping the sum and limit we have,

$$\lim_{t\to 0} \sqrt{\frac{\tau_1 \cdots \tau_n}{N(\delta)^2}} \theta_H \left(\tau, 0, \chi; \frac{1}{\mathfrak{d}} \right) = \sum_{\substack{\rho \bmod \mathfrak{b}_1 \\ \rho \equiv 0 (\mathfrak{c})}} e^{2\pi i \operatorname{tr}(-\rho^2/4\omega\delta^2)} \lim_{t\to 0} \sqrt{\frac{\tau_1 \cdots \tau_n}{N(\delta)^2}} \theta_H \left(\frac{\tau}{|\delta|^2}, \rho, \frac{\tau\sigma}{\delta^2}; \mathfrak{b}_1\mathfrak{c} \right) \tag{6.76}$$

By (6.20) as t tends to zero then so does τ, hence applying Lemma 6.3 to the right hand side of (6.76) gives,

$$\lim_{t\to 0} \sqrt{\frac{\tau_1 \cdots \tau_n}{N(\delta)^2}} \theta_H \left(\tau, 0, \chi; \frac{1}{\mathfrak{d}} \right) = \frac{1}{N(\mathfrak{b}_1\mathfrak{c}) |\sqrt{d_K}|} \sum_{\substack{\rho \bmod \mathfrak{b}_1 \\ \rho \equiv 0 (\mathfrak{c})}} e^{2\pi i \operatorname{tr}(-\rho^2/4\omega\delta^2)} . \tag{6.77}$$

We wish to show that the sum in (6.77) is really a Gauss sum. By (6.62) and (6.69),

$$\mathfrak{b}_1 \text{ is the denominator of } \frac{\mathfrak{a}}{4\mathfrak{b}} = \frac{\mathfrak{d}\mathfrak{c}^2}{4\omega\delta^2} . \tag{6.78}$$

Let

$$\alpha := \gamma\delta \tag{6.79}$$

so by (6.69) and (6.63)

$$\alpha = \gamma\delta = \mathfrak{d}\mathfrak{c}\gamma = \mathfrak{c}_1\mathfrak{c} \tag{6.80}$$

Therefore $\alpha \in \mathfrak{c}$ and $\alpha/\mathfrak{c}$ is relatively prime to $\mathfrak{b}_1$, so we may replace ρ by $\rho\alpha$ in the sum in (6.77) and let ρ run though a complete system of residues mod $\mathfrak{b}_1$. Then we get the Gauss sum,

$$\sum_{\substack{\rho \bmod \mathfrak{b}_1 \\ \rho \equiv 0 (\mathfrak{c})}} e^{2\pi i \operatorname{tr}(-\rho^2/4\omega\delta^2)} = \sum_{\rho \bmod \mathfrak{b}_1} e^{2\pi i \operatorname{tr}(-\alpha^2\rho^2/4\omega\delta^2)} = \mathfrak{g}\left(-\frac{1}{4\omega} \frac{\alpha^2}{\delta^2} \right), \tag{6.81}$$

so by (6.79)

$$\sum_{\substack{\rho \bmod \mathfrak{b}_1 \\ \rho \equiv 0 (\mathfrak{c})}} e^{2\pi i \operatorname{tr}(-\rho^2/4\omega\delta^2)} = \ vg\left(-\frac{1}{4\omega}\gamma^2 \right). \tag{6.82}$$

By (6.20),

$$\lim_{t\to 0} \sqrt{\tau_1 \cdots \tau_n} = \frac{\lim_{t\to 0} \sqrt{t_1 \cdots t_n}}{N(2\omega)} , \tag{6.83}$$

and by (6.69) and Proposition (3.5),

$$N(\mathfrak{b}_1\mathfrak{c}) = \frac{N(\mathfrak{b}_1)N(\mathfrak{d})}{N(\delta)} = \frac{N(\mathfrak{b}_1)\sqrt{d_K}}{N(\delta)}. \tag{6.84}$$

Introducing (6.82), (6.83) and (6.84) into (6.77) gives us,

$$\lim_{t\to 0}\sqrt{t_1\cdots t_n}\,\theta_H\left(\tau, 0, \chi; \frac{1}{\mathfrak{d}}\right) = \left|\frac{N(2\omega)}{N(\mathfrak{b}_1)}\sqrt{d_K}\right| \mathfrak{g}\left(\frac{-\gamma^2}{4\omega}\right). \tag{6.85}$$

which is the right hand side of (6.39).

6.4.3. We want to put everything together now. If $p = 1, \ldots, r_1$ then

$$\sqrt{-2i\omega^{(p)}} = \sqrt{-2i(\operatorname{sgn}\omega^{(p)})|\omega^{(p)}|} = e^{(-\pi i/4)\operatorname{sgn}\omega^{(p)}}\sqrt{2|\omega^{(p)}|}, \tag{6.86}$$

which means that

$$\lim_{t\to 0} W(t,\omega) = |\sqrt{N(2\omega)}|e^{(-\pi i/4)\,\mathrm{tr}(\operatorname{sgn}\omega)}, \tag{6.87}$$

where $\mathrm{tr}(\operatorname{sgn}\omega)$ is as in (3.24) and $W(t,\omega)$ as in (6.40). By (6.62) and Proposition 3.5 we simplify the norm,

$$N(2\omega) = \frac{N(2\mathfrak{b})}{N(\mathfrak{a})N(\mathfrak{d})} = \frac{N(2\mathfrak{b})}{N(\mathfrak{a})}\frac{1}{\sqrt{d_K}}. \tag{6.88}$$

Therefore by Theorem 6.2.1 with the left hand side (6.68) together with the right hand side (6.85) gives,

Theorem. *Let* $\mathfrak{a}$ *and* $\mathfrak{b}$ *be relatively prime ideals,* $\omega = \mathfrak{b}/\mathfrak{a}\mathfrak{d}$, $\mathfrak{b}_1$ *the denominator of* $\mathfrak{a}/4\mathfrak{b}$, γ *an arbitrary number in* K *such that* $\mathfrak{d}\gamma$ *is an ideal relatively prime to* $\mathfrak{b}_1$, *and* $\mathrm{tr}(\mathit{sgn}\,\omega)$ *as defined in* (3.24). *Then we have the reciprocity,*

$$\frac{\mathfrak{g}(\omega)}{|\sqrt{N(\mathfrak{a})}|} = \left|\frac{\sqrt{N(2\mathfrak{b})}}{N(\mathfrak{b}_1)}\right| e^{(\pi i/4)\,\mathrm{tr}(\mathit{sgn}\,\omega)}\mathfrak{g}\left(\frac{-\gamma^2}{4\omega}\right). \tag{6.89}$$

References

[1] Erich Hecke, *Lectures on the theory of algebraic numbers*, Graduate Texts in Mathematics, vol. 77, Springer-Verlag, New York-Berlin, 1981. Translated from the German by George U. Brauer, Jay R. Goldman and R. Kotzen. MR638719

[2] David Mumford, *Tata Lectures on Theta I*, Progress in Mathematics, vol. 28, Birkhauser Basel, 1983. Edited by J. Coates and S. Helgason.

[3] Bruce Berndt, *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, vol. 21, Wiley, 1998.

[4] Keith Conrad, *The Different Ideal*, 11. http://www.math.uconn.edu/ kconrad/blurbs/gradnumthy/different.pdf.

[5] ———, *Ideal Factorization*, 23. http://www.math.uconn.edu/ kconrad/blurbs/gradnumthy/idealfactor.pdf.

[6] Anders Karlsson, *Applications of heat kernels on abelian groups: $\zeta(2n)$, quadratic reciprocity, Bessel integrals*, 13. https://people.kth.se/ akarl/langmemorial.pdf.

[7] Pierre Samuel, *Algebraic Theory of Numbers*, Dover Publications Inc., 2008. Translated from the French by Allan J. Silberger.

[8] Serge Lang, *Undergraduate Analysis*, Springer, 2005.

[9] Jean-Pierre Serre, *A Course in Arithmetic*, Graduate Texts in Mathematics, vol. 7, Springer-Verlag New York Inc., 1973.

[10] J. David Logan, *Applied Partial Differential Equations*, Undergraduate texts in Mathematics, Springer International Publishing, 2015.

[11] Jurgen Neukirch, *Algebraic Number Theory*, Grundlehren der mathematischen Wissenschaften, vol. 322, Springer-Verlag Berlin Heidelberg, 1999.

[12] M. Ram Murty and Pacelli, *Quadratic reciprocity via theta functions* (2004), 107-116. http://www.mast.queensu.ca/ murty/recip-theta.pdf.

[13] D. Dummit and Foote, *Abstract Algebra*, John Wiley and Sons, Inc., 2003.

[14] James S. Milne, *Algebraic Number Theory (v3.07)* (2017), 165. Available at www.jmilne.org/math/.