RECIPROCITY LAW OF QUADRATIC EXTENSIONS

by

Filiz Tümel

B.S. in Mathematics, Boğaziçi University, 2003

Submitted to the Institute for Graduate Studies in
Science and Engineering in partial fulfillment of
the requirements for the degree of
Master of Science

Graduate Program in Mathematics

Boğaziçi University

2006

RECIPROCITY LAW OF QUADRATIC EXTENSIONS

APPROVED BY:

Prof. Ahmet Feyzioğlu (Thesis Supervisor)	.....
Assist. Prof. Müge Kanuni	.....
Prof. Hülya Şenkon	.....

DATE OF APPROVAL: 09.08.2006

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my thesis supervisor, Prof. Ahmet Feyzioğlu, for his endless support in preparation of this study. It would not be possible to complete this thesis without the patience and motivation he has provided during these two years.

I would like to thank Prof. Hülya Şenkon and Assist. Prof. Müge Kanuni for their participation in my thesis committee.

I am extremely thankful to my friends, Görkem Özkaya and Birkan Yılmaz for their technical support and to Bora Erdamar for his encouragement during the preparation of this thesis.

My special thanks are due to my family for their confidence and patience throughout my education.

ABSTRACT

RECIPROCITY LAW OF QUADRATIC EXTENSIONS

In the first chapter, basic definitions and results which will be used in the following chapters of this thesis are presented.

In the following chapter, ideal classes and classes of quadratic forms are reviewed. Then the relationship between the ideal classes of the quadratic field $\mathbb{Q}(\sqrt{D})$ with discriminant Δ and the classes of quadratic forms having discriminant Δ is established. It is proved that if two forms are equivalent, then they are constructed by two equivalent ideals and conversely equivalent ideals construct equivalent forms.

The next chapter aims to present one of the proofs of the quadratic reciprocity law which is based on the theory of quadratic number fields. Instead of developing the theory of binary quadratic forms, a proof using the ideal theoretic approach is given since the relation between ideals and forms is discussed in the previous chapter. The Hilbert's symbol for quadratic number fields is defined in this chapter and it is compared with Legendre symbol. Then genus is defined by using character sets and the quadratic reciprocity law is proved. Furthermore, the number of genera is found.

The following chapter again aims to prove the quadratic reciprocity law by using the theory of quadratic number fields. But for this chapter, we will first discuss how the strict sense equivalence change the class number. Then, we will find the number of genera by using exact sequences. It is easier than the previous section since considering strict equivalence brings all cases into one case. With these results, again a proof of the quadratic reciprocity law is given. In addition, genus character and genus field with their properties is presented.

In the last chapter, quadratic reciprocity law over $\mathbb{Q}(i)$ is presented. The proof is

based on the theory of Dirichlet number fields. The relative Hilbert symbol is defined for quadratic number fields over $\mathbb{Q}(i)$ and the number of genera of a Dirichlet number field is found by using the parallel arguments in Chapter 4. The number of genera again leads us to prove the quadratic reciprocity law over $\mathbb{Q}(i)$.

ÖZET

İKİNCİ DERECEDEN CİSİM GENİŞLEMELERİNDE RESİPROSİTE KANUNU

İlk bölümde tezin daha sonraki bölümlerinde kullanılacak olan temel tanımlar ve sonuçlar verilmiştir.

Bir sonraki bölümde ideal sınıfları ve ikinci dereceden form sınıflarına değinilmiştir. Sonrasında diskriminantı Δ olan $\mathbb{Q}(\sqrt{D})$ cisminin ideal sınıfları ile diskriminantı Δ olan ikinci dereceden formlar arasındaki ilişki incelenmiştir. İki form birbirine denk ise bu formların birbirine denk iki idealden oluştuğu ve birbirine denk ideallerin oluşturduğu formların da birbirine denk olduğu ispatlanmıştır.

4. bölümde ikinci dereceden cisim genişlemelerini kullanarak ikinci dereceden resiprosite kanununun ispatlanması hedeflenmiştir. Bir önceki bölümde formlar ve idealler arası ilişki incelendiğinden ikinci dereceden formlar ile çalşmak yerine ideal teorisi yaklaşımı kullanılarak ispat verilmiştir. Bu bölümde ikinci dereceden cisim genişlemeleri içinde Hilbert sembolü tanımlanmış ve bu sembol Legendre sembolü ile karşılaştırılmıştır. Karakter kümeleri kullanılarak cins tanımlanmış ve ikinci dereceden resiprosite kanunu ispatlanmıştır. Son olarak cins sayısı bulunmuştur.

5. bölümde de amaç ikinci dereceden cisim genişlemelerini kullanarak ikinci dereceden resiprosite kanununu ispatlamaktır. Fakat bu bölümde ilk olarak dar anlamda denklik bağıntısının sınıf sayısını nasıl değiştirdiği incelenmiştir. Cins sayısı bir önceki bölüme göre daha kolay bulunmuştur, çünkü dar anlamda denklik bizi bazı durumları incelemekten kurtarmıştır. Bu sonuçlar kullanılarak ikinci dereceden resiprosite kanununun ispatı verilmiştir. Cins karakteri ve cins cismi tanımlanmış ve özellikleri verilmiştir.

Son olarak ikinci dereceden resiprosite kanunu $\mathbb{Q}(i)$ cismi üzerinde verilmiştir. İspat Dirichlet sayı cisimleri teorisine dayanır. $\mathbb{Q}(i)$ üzerindeki ikinci dereceden cisim genişlemeleri içinde göreceli Hilbert sembolü tanımlanmış ve 4. bölümdeki yol takip edilerek Dirichlet sayı cisimlerinde cins sayısı hesaplanmıştır. Cins sayısı kullanılarak $\mathbb{Q}(i)$ üzerinde ikinci dereceden resiprosite kanunu ispatlanmıştır.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS iii
ABSTRACT iv
ÖZET vi
LIST OF FIGURES x
LIST OF TABLES xi
LIST OF SYMBOLS/ABBREVIATIONS xii
1. INTRODUCTION 1
2. PRELIMINARIES 3
3. QUADRATIC FIELDS AND QUADRATIC FORMS 5
3.1. Ideal Classes 5
3.2. Classes of Quadratic Forms 6
3.3. The Relationship between the Ideal Classes and The Classes of Quadratic Forms 7
4. QUADRATIC RECIPROCITY LAW BY QUADRATIC NUMBER FIELDS WITH HILBERT SYMBOL 19
4.1. The Integers in the Quadratic Number Field 19
4.2. The Prime Ideals in $\mathbb{Q}(\sqrt{m})$ 20
4.3. Hilbert's Symbol 24
4.4. The Character Set of an Ideal 34
4.5. Genera of Ideal Classes 39
4.6. Ambig Ideals 39
4.7. Quadratic Reciprocity Law 40
4.8. The Number of Genera 47
5. QUADRATIC RECIPROCITY LAW BY QUADRATIC NUMBER FIELDS WITH GENUS THEORY IN THE STRICT SENSE 57
5.1. Introduction 57
5.2. Class Groups 59
5.3. The Genus Class Groups 60
5.4. Quadratic Reciprocity Law 67

5.5. The Genus Character 70
6. QUADRATIC RECIPROCITY LAW BY DIRICHLET FIELDS 77
6.1. The Integers in the Dirichlet Number Field 77
6.2. The Prime Ideals of Dirichlet Fields 79
6.3. Relative Hilbert's Symbol 83
6.4. The Character Set of an Ideal 87
6.5. Genera of Ideal Classes 89
6.6. Ideal Classes in the Principle Genus 90
6.7. Ambig Ideals 98
6.8. Ambig Classes 99
6.9. The Number of Genera 105
6.10. The Reciprocity Law 106
APPENDIX A: SOME CALCULATIONS 112
APPENDIX B: SOME USEFUL THEOREMS 126
REFERENCES 129

LIST OF FIGURES

Figure 5.1. Exact sequence of class groups 59

Figure 5.2. Exact sequence of ambig ideals 62

Figure 5.3. Figure for ambig ideals to use Snake Lemma 63

Figure 5.4. Exact sequence of quotient groups 63

Figure 5.5. Exact sequence to decide the class number 75

Figure A.1. The algorithm for Lemma A.0.14 121

Figure B.1. Figure for Snake Lemma 126

LIST OF TABLES

Table 4.1. Decomposition of 2 into its prime ideals in $\mathbb{Q}(\sqrt{m})$ 23

Table 4.2. Table of $n = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha) \mod 2^3$ 32

Table 6.1. Decomposition of $1+i$ into its prime ideals in $k(\sqrt{\delta})$ 82

Table 6.2. Table of $\alpha = N_{k(\sqrt{\delta})/k}(A) \mod (1+i)^5$ 86

Table 6.3. Table of $\upsilon \equiv N_{k(\sqrt{\delta})/k}(A)$ with $\delta < 6$ 97

LIST OF SYMBOLS/ABBREVIATIONS

$\mathfrak{a}$	An ideal
$\mathfrak{a}'$	Conjugate ideal of $\mathfrak{a}$ in a quadratic number field over $\mathbb{Q}$
$[\mathfrak{a}]$	Ideal class of $\mathfrak{a}$
$\mathtt{A}$	Ideal class
$\mathtt{A}'$	Conjugate ideal class of $\mathtt{A}$
$\left(\frac{a}{p}\right)$	Legendre symbol
$\left(\frac{a}{b}\right)_J$	Jacobi symbol
$\left(\frac{a}{p:m}\right)$	Hilbert symbol
c	Length of a character set
C_2	Cyclic group of order 2 under multiplication
$\mathrm{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))$	Discriminant of $\mathbb{Q}(\sqrt{m})$ over $\mathbb{Q}$
F	A binary quadratic form
$F_{\mathfrak{a}}$	A binary quadratic form belonging to the ideal $\mathfrak{a}$
$\mathfrak{G}$	Genus
$\mathfrak{G}_0$	Principle genus
K	Number field
$Mat_{2\times 2}(\mathbb{Z})$	2×2 matrices with integer entries
$N(\alpha)$	Norm of α over $\mathbb{Q}$
$\mathfrak{O}$	Ring of integers
$\mathfrak{O}^{\times}$	The unit group of $\mathfrak{O}$
s	Number of prime divisors of the discriminant
S	Set of all ambig prime ideals
S	Relative conjugation function
$SL(2,\mathbb{Z})$	Special linear group of 2×2 matrices with integer entries
$T(\alpha)$	Trace of α over $\mathbb{Q}$
Δ	Discriminant of a binary quadratic form
ε	Unit
$\left[\frac{\sigma}{\tau}\right]$	Dirichlet symbol

$\left[\frac{\sigma}{\tau : \delta}\right]$	Relative Hilbert symbol for Dirichlet fields
Υ	Character function
χ_j	Genus character

1. INTRODUCTION

During the development of algebraic number theory from Gauss to Hilbert, the developers in this theory had two major goals in back of their minds: generalizing quadratic reciprocity and solving Diophantine equations. Quadratic reciprocity seems to belong to the theory of rational numbers. However, its generalization were a key stimulus in the creation of algebraic number theory.

The theory of "binary quadratic forms" first clarified by Lagrange (1773) after the Fermat's famous question: which primes are sums of two squares? Lagrange discovered the equivalence of forms and give the concept of class number, but understand the difficulty of finding class number. Lagrange's results refined by Gauss. He partitioned all forms of discriminant D into disjoint subsets, he called each subset a genus.

Quadratic forms threw up a problem that was too hard for 18th century mathematicians: the law of quadratic reciprocity. In investigating the prime values of quadratic forms, it turns out to be important to know which primes p are squares modulo a given prime q. Euler and Legendre observed that the answer seems to depend only the 'reciprocal' property: whether q is a square modulo p. First, Legendre (1785) proposed a proof, but it depended on the unproved assumption that there are infinitely many primes of the form $an + b$ with $(a, b) = 1$.

One of the great achievement of Gauss was to prove quadratic reciprocity, without Legendre's assumption. He gave a total of six proofs of quadratic reciprocity in his 'Disquisitiones Arithmeticae', published in 1801. The law of quadratic reciprocity was Gauss's favorite theorem, his principal goal was to find the approach that would allow generalizations to higher power. A proof in this thesis has that approach.

We must also note the correspondence between forms and fields. Our law for the splitting of rational primes in quadratic fields then leads to significant results on the representation of numbers by forms, via composition of forms, and this circle of

ideas leads naturally to Gauss's genus theory of forms. This correspondence is given in Chapter 2 in this thesis and then genus theory is used for fields in the following chapters.

The systematic development of algebraic number theory began with Gauss and his successors. Dirichlet did not first read the Disquisitiones several times, but throughout his life it was always on the table where he was working and was a source for continual study. The search for higher reciprocity laws led to the development of algebraic number theory.

In 1893, the German Mathematical Society asked David Hilbert and Hermann Minkowski to prepare a survey report on the state of the theory of numbers. Hilbert and Minkowski divided the work, deciding that the former would report on algebraic number theory and the latter on rational number theory. Minkowski never finished his report. Hilbert's report, the 'Zahlbericht' appeared in 1893. This volume, based upon the revolutionary work of Kummer, Kronecker and Dedekind, presented the ideal theoretic foundations on algebraic number theory and included many deep and important new contributions. Chapter 3 presents some work from [1].

Subsequent to the appearance of the Zahlbericht, Hilbert published a series of papers which opened up a new approach to reciprocity laws in algebraic number fields. One of these papers [2] is presented in Chapter 5.

Lastly, a 20th century view of reciprocity laws was presented by the paper by B. Wyman.

2. PRELIMINARIES

In this chapter, our aim is to present basic definitions and results which will be used in the following chapters of this thesis. The proofs of all results can be found in [3].

Let K be a number field and $\mathfrak{O}$ be its ring of integers. Uniqueness of the factorization of elements in $\mathfrak{O}$ into irreducible elements may fail. To restore the unique factorization on $\mathfrak{O}$, one studies ideals of $\mathfrak{O}$ instead of elements.

Let us recall some general facts.

Lemma 2.0.1. *Let R be a nontrivial commutative ring with identity element and $\mathfrak{a}$ be an ideal in R. Then,*
(a) $\mathfrak{a}$ is maximal if and only if $R/\mathfrak{a}$ is a field.
(b) $\mathfrak{a}$ is prime if and only if $R/\mathfrak{a}$ is an integral domain.

Corollary 2.0.2. *Let R be a commutative ring with identity element. Then every maximal ideal in R is prime.*

Definition 2.0.3. Let K be a number field. An element $\alpha \in K$ is called an *algebraic integer over* $\mathbb{Z}$, if it is a root of a monic polynomial with coefficients in $\mathbb{Z}$.

Definition 2.0.4. Let K be a number field and $\mathfrak{O}$ be its ring of integers. An element $\alpha \in K$ is called an *algebraic integer over* $\mathfrak{O}$, if it is a root of a monic polynomial with coefficients in $\mathfrak{O}$.

From now on, an integer means an algebraic integer.

Theorem 2.0.5. *Let $\mathfrak{O}$ be the ring of integers of a number field K of degree $n > 0$. Then,*
(a) $\mathfrak{O}$ is an integral domain with field of fractions K,
(b) $\mathfrak{O}$ is noetherian,
(c) $\mathfrak{O}$ is integrally closed; that is if $\alpha \in K$ is an integral over $\mathfrak{O}$, then it is an integer

over $\mathbb{Z}$,
(d) Every nonzero prime ideal is maximal in $\mathfrak{O}$.

In general, such a ring satisfying these conditions is called a *Dedekind Ring* (Julius Wihelm Richard Dedekind, 1831-1916).

Now consider ideals of $\mathfrak{O}$ as an $\mathfrak{O}$-submodule of $\mathfrak{O}$. This gives us a chance to study $\mathfrak{O}$-submodules of K.

Definition 2.0.6. Let K be a number field and $\mathfrak{O}$ be its ring of integers. An $\mathfrak{O}$-submodule $\mathfrak{a}$ of K is called a *fractional ideal* of $\mathfrak{O}$, if there exists some nonzero $c \in \mathfrak{O}$ such that $c\mathfrak{a} \subseteq \mathfrak{O}$. In other words, the fractional ideals of $\mathfrak{O}$ are subsets of the form $c^{-1}\mathfrak{b}$ where $\mathfrak{b}$ is an ideal of $\mathfrak{O}$ and c is a nonzero element of $\mathfrak{O}$.

Note that if $\mathfrak{O}$ is a principal ideal domain, then the fractional ideals are of the form $c^{-1} < d >= c^{-1}d\mathfrak{O} = \alpha\mathfrak{O}$ where $\alpha \in K$. Also note that a fractional ideal $\mathfrak{a}$ is an ideal if and only if $\mathfrak{a} \subseteq \mathfrak{O}$.

Lemma 2.0.7. *The nonzero fractional ideals of* $\mathfrak{O}$ *form an abelian group under multiplication.*

3. QUADRATIC FIELDS AND QUADRATIC FORMS

In this chapter, we are going to establish the relationship between the ideal classes of the quadratic field $\mathbb{Q}(\sqrt{D})$ with discriminant Δ and the classes of quadratic forms having discriminant Δ. We are going to prove that if two forms are equivalent, then they are constructed by two equivalent ideals and conversely equivalent ideals construct equivalent forms. Let us review first ideal classes, then classes of quadratic forms.

3.1. Ideal Classes

Definition 3.1.1. Let $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals. If there exist two principal ideals (α) and (β) such that $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$, then we say that the two ideals $\mathfrak{a}$ *and* $\mathfrak{b}$ *belong to the same ideal class*, and we write $\mathfrak{a} \sim \mathfrak{b}$.

Theorem 3.1.2. *The number of ideal classes of* $\mathbb{Q}(\theta)$ *is finite.*

Proof. The proof is given in [4]. □

Definition 3.1.3. Let $\alpha \in \mathbb{Q}(\sqrt{D})$, so $\alpha = q_1 + q_2\sqrt{D}$ for some $q_1, q_2 \in \mathbb{Q}$. Then we define *the conjugate of* α as $q_1 - q_2\sqrt{D}$ and denote by α'.

Definition 3.1.4. $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a}) := |\mathfrak{O}/\mathfrak{a}|$.

This norm definition will be used only for this chapter. We will define the norm of an ideal differently when we will study quadratic fields instead of quadratic forms.

Theorem 3.1.5. *Let* h *be the number of ideal classes of* $\mathbb{Q}(\theta)$*. Then for any ideal* $\mathfrak{a}$*, we have* $\mathfrak{a}^h \sim \mathfrak{O}$*.*

Proof. The proof is given in [4]. □

Notation 3.1.6. Let $\mathfrak{a}$ be an ideal in $\mathfrak{O}$. We choose an integral basis for $\mathfrak{a}$, say $\{\alpha_1, \alpha_2\}$. By [3], we know that

$$\det \begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_1' & \alpha_2' \end{pmatrix} = \mp N(\mathfrak{a})\sqrt{\Delta},$$

where α_1', α_2' are conjugates of α_1, α_2 respectively.

In case $\Delta > 0$, we denote the positive square root of Δ by $\sqrt{\Delta}$.

In case $\Delta < 0$, we denote $\sqrt{|\Delta|}i$ by $\sqrt{\Delta}$, which is one of the two possibilities for the symbol "$\sqrt{\Delta}$ ".

Then if necessary, we reorder α_1, α_2 to obtain

$$\det \begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_1' & \alpha_2' \end{pmatrix} = \mp N(\mathfrak{a})\sqrt{\Delta} > 0. \tag{3.1}$$

3.2. Classes of Quadratic Forms

Definition 3.2.1. Let the integer coefficient substitution

$$x = rX + sY,\ y = tX + uY,\ (ru - st = 1)$$

transform $F(x, y)$ into $G(X, Y)$. The two forms F and G are said to be *equivalent*, and we write $F \sim G$.

Definition 3.2.2. For the form $F = ax^2 + bxy + cy^2$, if its discriminant $\Delta < 0$, we have

$$4a(ax_0^2 + bx_0y_0 + cy_0^2) = (2ax_0 + by_0)^2 + |\Delta|y_0 \geq 0$$

for any $x_0, y_0 \in \mathbb{Z}$, and equal to 0 if and only if $x_0 = y_0 = 0$. Thus, the form F represents, aside from 0, either exclusively positive integers or exclusively negative integers. So we call F a *definite form*, more specifically a *positive definite form* if the nonzero integers represented by F are all positive, that is if $a > 0$, or a *negative definite form* if the nonzero integers represented by F are all negative, that is if $a < 0$.

But if the discriminant $\Delta > 0$, the form F represents positive integers as well as negative integers. So we call F an *indefinite form*.

3.3. The Relationship between the Ideal Classes and The Classes of Quadratic Forms

Given in ideal $\mathfrak{a}$ with its integral basis $\{\alpha_1, \alpha_2\}$, we construct the following quadratic form:

$$\begin{aligned} F_{\mathfrak{a}(\alpha_1,\alpha_2)} &:= \frac{N(\alpha_1 x + \alpha_2 y)}{N(\mathfrak{a})} \\ &= \frac{(\alpha_1 x + \alpha_2 y)(\alpha_1' x + \alpha_2' y)}{N(\mathfrak{a})} \\ &= \frac{\alpha_1\alpha_1'}{N(\mathfrak{a})}x^2 + \frac{\alpha_1\alpha_2' + \alpha_1'\alpha_2}{N(\mathfrak{a})}xy + \frac{\alpha_2\alpha_2'}{N(\mathfrak{a})}y^2 \\ &= \frac{N(\alpha_1)}{N(\mathfrak{a})}x^2 + \frac{T(\alpha_1\alpha_2')}{N(\mathfrak{a})}xy + \frac{N(\alpha_2)}{N(\mathfrak{a})}y^2 \\ &= ax^2 + bxy + cy^2. \end{aligned}$$

Note that a, b and c are dependent on $\mathfrak{a}$, α_1 and α_2.

Here $a, b, c \in \mathbb{Z}$, because $\mathfrak{a} \mid (\alpha_1)$ and $\mathfrak{a} \mid (\alpha_2)$ since $\alpha_1, \alpha_2 \in \mathfrak{a}$, so $N(\mathfrak{a}) \mid N(\alpha_1)$ and $N(\mathfrak{a}) \mid N(\alpha_2)$. Also $T(\alpha_1\alpha_2')^2 - 4N(\alpha_1)N(\alpha_2) = (\alpha_1\alpha_2' + \alpha_2\alpha_1')^2 - 4\alpha_1\alpha_1'\alpha_2\alpha_2' = (\alpha_1\alpha_2' - \alpha_2\alpha_1')^2 = \det \begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_1' & \alpha_2' \end{pmatrix}^2 = N(\mathfrak{a})^2 \cdot \Delta$ by Equation 3.1. Since $N(\mathfrak{a})^2 \mid 4N(\alpha_1)N(\alpha_2)$, we get $N(\mathfrak{a})^2 \mid T(\alpha_1\alpha_2')^2$, so $N(\mathfrak{a}) \mid T(\alpha_1\alpha_2')$. Also, the discriminant of the form

$F_{\mathfrak{a}(\alpha_1,\alpha_2)}(x,y)$ is

$$\begin{aligned} b^2-4ac &= \frac{(\alpha_1\alpha_2'+\alpha_2\alpha_1')^2-4(\alpha_1\alpha_1')(\alpha_2\alpha_2')}{(N(\mathfrak{a}))^2} \\ &= \frac{(\alpha_1\alpha_2'-\alpha_2\alpha_1')^2}{(N(\mathfrak{a}))^2} \\ &= \frac{\det\begin{pmatrix}\alpha_1 & \alpha_2\\ \alpha_1' & \alpha_2'\end{pmatrix}^2}{N(\mathfrak{a})^2} \\ &= \Delta. \end{aligned}$$

So $F_{\mathfrak{a}(\alpha_1,\alpha_2)}(x,y) = ax^2+bxy+cy^2$ is a quadratic form with discriminant Δ. We say that $F_{\mathfrak{a}(\alpha_1,\alpha_2)}(x,y)$ is *a quadratic form belonging to the ideal* $\mathfrak{a}$.

Note that when $\Delta < 0$, we have

$$\begin{aligned} N(r+s\sqrt{\Delta}) &= (r+s\sqrt{\Delta})(r-s\sqrt{\Delta}) \\ &= r^2-s^2\Delta \\ &= r^2+s^2|\Delta| \geq 0 \end{aligned}$$

for all $r, s \in \mathbb{Q}$. Also $N(\mathfrak{a}) > 0$ by Definition 3.1.4, so $a = \dfrac{N(\alpha_1)}{N(\mathfrak{a})} > 0$ and $F_{\mathfrak{a}(\alpha_1,\alpha_2)}(x,y)$ is positive definite.

Lemma 3.3.1. *Let* $\mathfrak{a}$ *be an ideal in* $\mathfrak{O}$. *As* α_1, α_2 *run through all of the basis for* $\mathfrak{a}$ *satisfying Equation 3.1, we obtain all quadratic forms equivalent to* $F_{\mathfrak{a}(\alpha_1,\alpha_2)}(x,y)$.

Proof. We will show that:

(i) If β_1, β_2 is another basis for $\mathfrak{a}$ satisfying Equation 3.1, then $F_{\mathfrak{a}(\alpha_1,\alpha_2)}(x,y) \sim F_{\mathfrak{a}(\beta_1,\beta_2)}(x,y)$.

(ii) If F is a quadratic form of discriminant Δ and if $F \sim F_{\mathfrak{a}(\alpha_1,\alpha_2)}(x,y)$, then there is a basis β_1, β_2 of $\mathfrak{a}$ satisfying Equation 3.1 and $F = F_{\mathfrak{a}(\beta_1,\beta_2)}(x,y)$.

Firstly, let β_1, β_2 denote another basis for $\mathfrak{a}$ satisfying Equation 3.1. Then

for some $M \in \mathrm{Mat}_{2\times 2}(\mathbb{Z})$ we have $\begin{pmatrix}\alpha_1\\ \alpha_2\end{pmatrix} = M\begin{pmatrix}\beta_1\\ \beta_2\end{pmatrix}$, so $\begin{pmatrix}\alpha_1'\\ \alpha_2'\end{pmatrix} = M\begin{pmatrix}\beta_1'\\ \beta_2'\end{pmatrix}$, then $\begin{pmatrix}\alpha_1 & \alpha_2\\ \alpha_1' & \alpha_2'\end{pmatrix} = \begin{pmatrix}\beta_1 & \beta_2\\ \beta_1' & \beta_2'\end{pmatrix} M^t$ where M^t denotes the transpose matrix of M. Also we have $\det\begin{pmatrix}\alpha_1 & \alpha_2\\ \alpha_1' & \alpha_2'\end{pmatrix} = \det\begin{pmatrix}\beta_1 & \beta_2\\ \beta_1' & \beta_2'\end{pmatrix}\det(M^t)$. By Equation 3.1, we get

$$N(\mathfrak{a})\sqrt{\Delta} = N(\mathfrak{a})\sqrt{\Delta}\det(M),$$

so $\det(M) = 1$, thus $M \in SL(2,\mathbb{Z})$.

Now, we will show that $F_{\mathfrak{a}(\alpha_1,\alpha_2)}(x,y) = \dfrac{N(\alpha_1 x+\alpha_2 y)}{N(\mathfrak{a})}$ and $F_{\mathfrak{a}(\beta_1,\beta_2)}(x,y) = \dfrac{N(\beta_1 x+\beta_2 y)}{N(\mathfrak{a})}$ are equivalent:

$$\begin{aligned} N(\beta_1 x+\beta_2 y) &= N\left((x\ y)\begin{pmatrix}\beta_1\\ \beta_2\end{pmatrix}\right)\\ &= N\left((x\ y)\cdot M^{-1}\begin{pmatrix}\alpha_1\\ \alpha_2\end{pmatrix}\right)\\ &= N\left((x\ y)M^{-1}\cdot\begin{pmatrix}\alpha_1\\ \alpha_2\end{pmatrix}\right)\\ &= N\left((X\ Y)\begin{pmatrix}\alpha_1\\ \alpha_2\end{pmatrix}\right)\\ &= N(\alpha_1 X+\alpha_2 Y) \end{aligned} \tag{3.2}$$

where $(x\ y)M^{-1} = (X\ Y)$, implying $(x\ y) = (X\ Y)M$, so $\begin{pmatrix} x \\ y \end{pmatrix} = M^t \begin{pmatrix} X \\ Y \end{pmatrix}$. Thus,

$$\begin{aligned} F_{\mathfrak{a}(\beta_1,\beta_2)} M^t \begin{pmatrix} X \\ Y \end{pmatrix} &= F_{\mathfrak{a}(\beta_1,\beta_2)} \begin{pmatrix} x \\ y \end{pmatrix} \\ &= F_{\mathfrak{a}(\alpha_1,\alpha_2)} \begin{pmatrix} X \\ Y \end{pmatrix} \text{ (by Equation 3.2)} \\ &= F_{\mathfrak{a}((\beta_1,\beta_2)M^t)} \begin{pmatrix} X \\ Y \end{pmatrix}, \end{aligned}$$

so $F^{M^t}_{\mathfrak{a}(\beta_1,\beta_2)}(X,Y) = F_{\mathfrak{a}(\alpha_1,\alpha_2)}(X,Y)$, and $F_{\mathfrak{a}(\beta_1,\beta_2)}(X,Y) \sim F_{\mathfrak{a}(\alpha_1,\alpha_2)}(X,Y)$.

Remark 3.3.2. Note that

$$F^A_{\mathfrak{a}(\beta_1,\beta_2)}(x,y) = F_{\mathfrak{a}((\beta_1,\beta_2)A)}(x,y) \tag{3.3}$$

for $A \in \mathrm{Mat}_{2\times 2}(\mathbb{Z})$.

Secondly, let F be a quadratic form of a discriminant Δ and $F \sim F_{\mathfrak{a}(\alpha_1,\alpha_2)}(x,y)$, so $F = F^A_{\mathfrak{a}(\alpha_1,\alpha_2)}(x,y)$ for some $A \in SL(2,\mathbb{Z})$, then $F = F_{\mathfrak{a}((\alpha_1,\alpha_2)A)}(x,y) = F_{\mathfrak{a}(\beta_1,\beta_2)}$ where β_1, β_2 is an integral basis for $\mathfrak{a}$ since $A \in SL(2,\mathbb{Z})$. Thus,

$$\begin{pmatrix} \beta_1 & \beta_2 \\ \beta_1' & \beta_2' \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_1' & \alpha_2' \end{pmatrix} A$$

implies that

$$\det \begin{pmatrix} \beta_1 & \beta_2 \\ \beta_1' & \beta_2' \end{pmatrix} = \det \begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_1' & \alpha_2' \end{pmatrix} \cdot \det(A) = N(\mathfrak{a}) \cdot \sqrt{\Delta} \cdot 1\,,$$

so β_1, β_2 satisfies Equation 3.1. □

Theorem 3.3.3. *Let $F(x,y) = ax^2 + bxy + cy^2$ be a binary quadratic form for some $a, b, c \in \mathbb{Z}$, and Δ be its discriminant. Assume F is indefinite or positive definite, then*

there is an ideal $\mathfrak{a}$ *in* $\mathfrak{O}$*, and a basis* α_1, α_2 *of* $\mathfrak{a}$ *such that* $F(x,y) = F_{\mathfrak{a}(\alpha_1,\alpha_2)}(x,y)$.

Proof. First we will check that $\dfrac{b-\sqrt{\Delta}}{2}$ satisfies the equation $x^2 - bx + ac = 0$, equally $x(b-x) = ac$.

$$\frac{b-\sqrt{\Delta}}{2}(b - \frac{b-\sqrt{\Delta}}{2}) = \frac{b-\sqrt{\Delta}}{2}(\frac{2b-b+\sqrt{\Delta}}{2}) = \frac{(b^2-\Delta)}{4} = \frac{b^2-b^2+4ac}{4} = ac.$$

So a and $\dfrac{b-\sqrt{\Delta}}{2}$ are algebraic integers by being roots of $x-a$ and $x^2-bx+ac$ in $\mathbb{Z}[x]$ respectively.

Claim: $a, \dfrac{b-\sqrt{\Delta}}{2}$ form an integral basis for the ideal $\mathfrak{b} = \mathfrak{O}a + \mathfrak{O}\left(\dfrac{b-\sqrt{\Delta}}{2}\right)$.

Proof of the claim: Let $1, w$ be an integral basis of $\mathfrak{O}$ in the quadratic field $\mathbb{Q}(\sqrt{D})$ where $w = \sqrt{D}$ for $D \equiv 2,3 \mod 4$ and $w = \dfrac{1+\sqrt{D}}{2}$ for $D \equiv 1 \mod 4$ by Appendix A.0.7. We have,
for $D \equiv 2,3 \mod 4$, $\dfrac{T(w)+\sqrt{\Delta}}{2} = \dfrac{\sqrt{D}-\sqrt{D}+\sqrt{4D}}{2} = \sqrt{D} = w$,
for $D \equiv 1 \mod 4$, $\dfrac{T(w)+\sqrt{\Delta}}{2} = \dfrac{\frac{1+\sqrt{D}}{2}+\frac{1-\sqrt{D}}{2}+\sqrt{D}}{2} = \dfrac{1+\sqrt{D}}{2} = w$.
Now,

$$aw = a\frac{T(w)+\sqrt{\Delta}}{2} = a\frac{T(w)+b-b+\sqrt{\Delta}}{2} = \left(\frac{T(w)+b}{2}\right)\cdot a + (-a)\cdot\frac{b-\sqrt{\Delta}}{2}$$

where $\dfrac{T(w)+b}{2}, -a \in \mathbb{Z}$, because if $\Delta = 4D$, then $T(w) = 0$, also $b^2 \equiv b^2 - 4ac = \Delta = 4D \equiv 0 \mod 4$ and thus b is even, and if $\Delta = D$, then $T(w) = 1$, also $b^2 \equiv b^2 - 4ac = \Delta = D \equiv 1 \mod 4$ and thus b is odd. Furthermore,

$$\left(\frac{b-\sqrt{\Delta}}{2}\right)w \;=\; \left(\frac{b-\sqrt{\Delta}}{2}\right)\left(\frac{T(w)+\sqrt{\Delta}}{2}\right)$$

$$\begin{aligned} &= \left(\frac{T(w)+\sqrt{\Delta}-b+b}{2}\right)\left(\frac{b-\sqrt{\Delta}}{2}\right) \\ &= \left(\frac{b+\sqrt{\Delta}}{2}\right)\left(\frac{b-\sqrt{\Delta}}{2}\right)+\left(\frac{T(w)-b}{2}\right)\left(\frac{b-\sqrt{\Delta}}{2}\right) \\ &= \left(\frac{b^2-\Delta}{4a}\right)a+\left(\frac{T(w)-b}{2}\right)\left(\frac{b-\sqrt{\Delta}}{2}\right), \end{aligned}$$

where $\frac{b^2-\Delta}{4a}, \frac{T(w)-b}{2} \in \mathbb{Z}$. Therefore,

$$\begin{pmatrix} aw \\ \frac{b-\sqrt{\Delta}}{2}w \end{pmatrix} = \begin{pmatrix} a \\ \frac{b-\sqrt{\Delta}}{2} \end{pmatrix} w = \begin{pmatrix} \frac{T(w)+b}{2} & -a \\ \frac{b^2-\Delta}{4a} & \frac{T(w)-b}{2} \end{pmatrix} \begin{pmatrix} a \\ \frac{b-\sqrt{\Delta}}{2} \end{pmatrix} \tag{3.4}$$

and

$$\begin{aligned} \mathfrak{b} &= \mathfrak{O}a+\mathfrak{O}\frac{b-\sqrt{\Delta}}{2} \\ &= (\mathbb{Z}+\mathbb{Z}w)a+(\mathbb{Z}+\mathbb{Z}w)\frac{b-\sqrt{\Delta}}{2} \\ &= \mathbb{Z}a+\mathbb{Z}\frac{b-\sqrt{\Delta}}{2}+\mathbb{Z}wa+\mathbb{Z}w\frac{b-\sqrt{\Delta}}{2} \\ &= \mathbb{Z}a+\mathbb{Z}\frac{b-\sqrt{\Delta}}{2}, \end{aligned}$$

since $\mathbb{Z}wa$, $\mathbb{Z}w\frac{b-\sqrt{\Delta}}{2} \subseteq \mathbb{Z}a+\mathbb{Z}\frac{b-\sqrt{\Delta}}{2}$ by the Equation 3.4. This proves our claim.

Now, if $a>0$, then let $\mathfrak{a}=\mathfrak{b}$, $\alpha_1=a$, $\alpha_2=\frac{b-\sqrt{\Delta}}{2}$. We will show that for these values of $\mathfrak{a}, \alpha_1, \alpha_2$, we have $F_{\mathfrak{a}(\alpha_1,\alpha_2)}(x,y)=F(x,y)=ax^2+bxy+cy^2$.

$$\begin{aligned} F_{\mathfrak{a}(\alpha_1,\alpha_2)}(x,y) &= \frac{N(\alpha_1 x+\alpha_2 y)}{N(\mathfrak{a})} \\ &= \frac{(ax+(b-\sqrt{\Delta})y/2)(ax+(b+\sqrt{\Delta})y/2)}{N(\mathfrak{b})} \end{aligned}$$

$$
\begin{aligned}
&= \frac{(ax+by/2)^2-(\sqrt{\Delta}y/2)^2}{(\alpha_1\alpha_2'-\alpha_2\alpha_1')/\sqrt{\Delta}} \\
&= \frac{a^2x^2+abxy+b^2y^2/4-\Delta y^2/4}{a(\alpha_2'-\alpha_2)/\sqrt{\Delta}} \\
&= \frac{a^2x^2+abxy+b^2y^2/4-(b^2y^2/4-acy^2)}{a(\frac{b+\sqrt{\Delta}}{2}-\frac{b-\sqrt{\Delta}}{2})/\sqrt{\Delta}} \\
&= \frac{a^2x^2+abxy+acy^2}{a} \\
&= ax^2+bxy+cy^2, \text{ with}
\end{aligned}
$$

$$
\det\begin{pmatrix}\alpha_1 & \alpha_2\\ \alpha_1' & \alpha_2'\end{pmatrix} = \det\begin{pmatrix}a & \dfrac{b-\sqrt{\Delta}}{2}\\ a & \dfrac{b+\sqrt{\Delta}}{2}\end{pmatrix} = a\sqrt{\Delta} > 0,
$$

so $\{\alpha_1, \alpha_2\}$ satisfies Equation 3.1.

But if $a < 0$, then let $\mathfrak{a} = \sqrt{\Delta}\mathfrak{b}$, $\alpha_1 = \sqrt{\Delta}a$, $\alpha_2 = \sqrt{\Delta}\dfrac{b-\sqrt{\Delta}}{2}$. Note that F is not positive definite since $a < 0$, then by assumption of the theorem F is indefinite, so $\Delta > 0$. Similarly,

$$
\begin{aligned}
F_{\mathfrak{a}(\alpha_1,\alpha_2)}(x,y) &= \frac{N(\alpha_1x+\alpha_2y)}{N(\mathfrak{a})} \\
&= \frac{\sqrt{\Delta}(ax+(b-\sqrt{\Delta})y/2)(-\sqrt{\Delta})(ax+(b+\sqrt{\Delta})y/2)}{N(\sqrt{\Delta}\mathfrak{b})} \\
&= \frac{-\Delta}{N(\sqrt{\Delta})}\,\frac{(ax+(b-\sqrt{\Delta})y/2)(ax+(b+\sqrt{\Delta})y/2)}{N(\mathfrak{b})} \\
&= \frac{-\Delta}{\sqrt{\Delta}(-\sqrt{\Delta})}(ax^2+bxy+cy^2) \\
&= ax^2+bxy+cy^2, \text{ with}
\end{aligned}
$$

$$\det\begin{pmatrix}\alpha_1 & \alpha_2\\ \alpha_1' & \alpha_2'\end{pmatrix} = \det\begin{pmatrix} a\sqrt{\Delta} & \dfrac{b-\sqrt{\Delta}}{2}\sqrt{\Delta}\\ -a\sqrt{\Delta} & -\dfrac{b+\sqrt{\Delta}}{2}\sqrt{\Delta}\end{pmatrix} = -a\sqrt{\Delta}\Delta > 0,$$

so $\{\alpha_1, \alpha_2\}$ satisfies Equation 3.1. □

To sum up, let us define

$$\begin{array}{rcl}\Phi \;:\; \{(\mathfrak{a}, B) : B \text{ is a } \mathbb{Z}\text{-basis of } \mathfrak{a} & \longrightarrow & \{F : F \text{ is not negative definite,}\\ \text{with } \det\begin{pmatrix}B\\ B'\end{pmatrix} = N(\mathfrak{a})\sqrt{\Delta} > 0\} & & \text{has disriminant } \Delta\}\\ (\mathfrak{a}, B) & \mapsto & F_{\mathfrak{a}(B)}(x, y)\end{array}$$

Φ is well defined by its construction. Also,

(i) $\Phi(\mathfrak{a}, B_1) \sim \Phi(\mathfrak{a}, B_2)$ for all $\mathfrak{a}$ in K by the first part of Lemma 3.3.1.

(ii) If $F \sim \Phi(\mathfrak{a}, B_1)$, then $F = \Phi(\mathfrak{a}, B_2)$ for some basis B_2 of $\mathfrak{a}$ by the second part of Lemma 3.3.1.

(iii) Φ is surjective by Theorem 3.3.3.

Definition 3.3.4. Let $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals in K. If there exist $\alpha, \beta \in \mathfrak{O}$ such that $\alpha\mathfrak{a} = \beta\mathfrak{b}$ and $N(\alpha\beta) > 0$, then we say that $\mathfrak{a}$ and $\mathfrak{b}$ are *equivalent in the narrower sense*, and write $\mathfrak{a} \simeq \mathfrak{b}$.

By using the Definition 3.3.4, we define a new function:

$$\begin{array}{rcl}\Phi' \;:\; \{[\mathfrak{a}] : [\mathfrak{a}] \text{ is a narrow} & \longrightarrow & \{[F] : [F] \text{ is an equivalence class of forms,}\\ \text{equivalence class in } \mathfrak{O}\} & & \text{not negative definite, has disriminant } \Delta\}\\ [\mathfrak{a}] & \mapsto & [\Phi(\mathfrak{a}, B)]\end{array}$$

for some basis B of an ideal $\mathfrak{a}$ in the narrow class $[\mathfrak{a}]$. We will show that Φ' is well defined, surjective and injective:

(i) Φ' **is well defined:** We will show that if $[\mathfrak{a}] = [\mathfrak{b}]$, then $[\Phi(\mathfrak{a}, B_1)] = [\Phi(\mathfrak{b}, B_2)]$. So let $\mathfrak{a}, \mathfrak{b}$ be two narrow equivalent ideals, and let $\{\alpha_1, \alpha_2\}$ and $\{\beta_1, \beta_2\}$ be their basis respectively. Then $\gamma\mathfrak{a} = \delta\mathfrak{b}$ for some $\gamma, \delta \in \mathfrak{O}$ with $N(\gamma\delta) > 0$. For the integral basis $\{\gamma\alpha_1, \gamma\alpha_2\}$ and $\{\delta\beta_1, \delta\beta_2\}$ of the ideal $\gamma\mathfrak{a} = \delta\mathfrak{b}$, we have

$$\begin{aligned}
\det \begin{pmatrix} \gamma\alpha_1 & \gamma\alpha_2 \\ (\gamma\alpha_1)' & (\gamma\alpha_2)' \end{pmatrix} &= \gamma\alpha_1(\gamma\alpha_2)' - (\gamma\alpha_1)'\gamma\alpha_2 \\
&= \gamma\gamma'(\alpha_1\alpha_2' - \alpha_1'\alpha_2) \\
&= N(\gamma) \det \begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_1' & \alpha_2' \end{pmatrix} \\
&= N(\gamma)N(\mathfrak{a})\sqrt{\Delta} \\
&= N(\gamma\mathfrak{a})\sqrt{\Delta}.
\end{aligned}$$

Similarly,

$$\begin{aligned}
\det \begin{pmatrix} \delta\beta_1 & \delta\beta_2 \\ (\delta\beta_1)' & (\delta\beta_2)' \end{pmatrix} &= \delta\beta_1(\delta\beta_2)' - (\delta\beta_1)'\delta\beta_2 \\
&= \delta\delta'(\beta_1\beta_2' - \beta_1'\beta_2) \\
&= N(\delta) \det \begin{pmatrix} \beta_1 & \beta_2 \\ \beta_1' & \beta_2' \end{pmatrix} \\
&= N(\delta)N(\mathfrak{b})\sqrt{\Delta} \\
&= N(\delta\mathfrak{b})\sqrt{\Delta}.
\end{aligned}$$

Therefore, $\{\gamma\alpha_1, \gamma\alpha_2\}$ and $\{\delta\beta_1, \delta\beta_2\}$ satisfy Equation 3.1. Then by the first part of Lemma 3.3.1 since $\{\gamma\alpha_1, \gamma\alpha_2\}$ and $\{\delta\beta_1, \delta\beta_2\}$ are the two basis of the same ideal $\gamma\mathfrak{a} = \delta\mathfrak{b}$, we get

$$\begin{gathered}
F_{\gamma\mathfrak{a}(\gamma\alpha_1, \gamma\alpha_2)}(x, y) \sim F_{\delta\mathfrak{b}(\delta\beta_1, \delta\beta_2)}, \\
\Phi(\gamma\mathfrak{a}, (\gamma\alpha_1, \gamma\alpha_2)) \sim \Phi(\delta\mathfrak{b}, (\delta\beta_1, \delta\beta_2)), \\
\Phi'([\gamma\mathfrak{a}]) = \Phi'([\delta\mathfrak{b}]).
\end{gathered}$$

But $\Phi'[\gamma\mathfrak{a}] = \Phi'[\mathfrak{a}]$ since,

$$\begin{aligned} F_{\gamma\mathfrak{a}(\gamma\alpha_1,\gamma\alpha_2)}(x,y) &= \frac{N(\gamma\alpha_1 x + \gamma\alpha_2 y)}{N(\gamma\mathfrak{a})} \\ &= \frac{N(\gamma)N(\alpha_1 x + \alpha_2 y)}{N(\gamma)N(\mathfrak{a})} \\ &= F_{\mathfrak{a}(\alpha_1,\alpha_2)}(x,y). \end{aligned}$$

Similarly, $\Phi'[\delta\mathfrak{b}] = \Phi'[\mathfrak{b}]$. Hence, $\Phi'([\mathfrak{a}]) = \Phi'([\mathfrak{b}])$.

(ii) Φ' **is surjective:** For every class of forms, $[F]$, consider the form F. Since Φ is surjective, there exists a pair $(\mathfrak{a}, B)$ such that $\Phi(\mathfrak{a}, B) = F$. Then by choosing that ideal $\mathfrak{a}$, we have $\Phi'([\mathfrak{a}]) = [\Phi(\mathfrak{a}, B)] = [F]$.

(iii) Φ' **is injective:** To prove that Φ' is injective, first we need a lemma.

Lemma 3.3.5. *Let $\mathfrak{a}, \mathfrak{b}$ be two ideals with integral basis $\{\lambda, \alpha\}$ and $\{\lambda, \beta\}$ respectively. If $T(\lambda\alpha') = T(\lambda\beta')$, and if $N(\alpha) = N(\beta)$, then $\alpha = \beta$.*

Proof. If $N(\alpha) = N(\beta)$, then $\alpha = \varepsilon\beta$ for some $\varepsilon \in \mathfrak{O}^\times$. Then, $\alpha \in \mathfrak{O}\beta \subseteq \mathfrak{b}$. Since $\alpha, \lambda \in \mathfrak{b}$, we get $\mathfrak{a} \subseteq \mathfrak{b}$. Similarly, $\beta = \varepsilon'\alpha$ for $\varepsilon'\varepsilon = 1$, then $\beta \in \mathfrak{O}\alpha \subseteq \mathfrak{a}$, and $\mathfrak{b} = \mathfrak{a}$. Hence, $\mathbb{Z}\lambda + \mathbb{Z}\alpha = \mathbb{Z}\lambda + \mathbb{Z}\beta$. So $\lambda = a_{11}\lambda + a_{12}\beta$ and $\alpha = a_{21}\lambda + a_{22}\beta$ with $\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = 1$ since the two basis $\{\lambda, \alpha\}$ and $\{\lambda, \beta\}$ satisfy Equation 3.1.

Now, $\lambda(1 - a_{11}) = a_{12}\beta$. If $a_{12} \neq 0$, then $\{\lambda, \beta\}$ are $\mathbb{Z}$-linearly dependent which contradicts that it is a basis, so $a_{12} = 0$. Then, $\lambda(1 - a_{11}) = 0$ implies that $a_{11} = 1$ since $\lambda \neq 0$. Also, $a_{11}a_{22} - a_{12}a_{21} = 1$ implies that $1a_{22} - 0a_{21} = a_{22} = 1$.

On the other hand, $\alpha = a_{21}\lambda + a_{22}\beta = a_{21}\lambda + \beta$. By the hypothesis of the lemma, $T(\lambda\beta') = T(\lambda\alpha') = T(\lambda(a_{21}\lambda' + \beta')) = T(a_{21}N(\lambda)) + T(\lambda\beta') = 2a_{21}N(\lambda) + T(\lambda\beta')$. Thus, $2a_{21}N(\lambda) = 0$ and we get $a_{21} = 0$ since $N(\lambda) \neq 0$.

We get $\begin{pmatrix} \lambda \\ \alpha \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \lambda \\ \beta \end{pmatrix} = \begin{pmatrix} \lambda \\ \beta \end{pmatrix}$, hence $\alpha = \beta$. □

Now we can show that Φ' is injective:
Let $[\mathfrak{a}]$ and $[\mathfrak{b}]$ be two narrow ideal classes, and assume that $\Phi'([\mathfrak{a}]) = \Phi'([\mathfrak{b}])$. Let us choose a basis $\{\alpha_1, \alpha_2\}$ and $\{\beta_1, \beta_2\}$ of $\mathfrak{a}$ and $\mathfrak{b}$ respectively satisfying Equation 3.1. Therefore,

$$\begin{gathered}[\Phi(\mathfrak{a}, (\alpha_1, \alpha_2))] = [\Phi(\mathfrak{b}, (\beta_1, \beta_2))], \\ \left[F_{\mathfrak{a}(\alpha_1,\alpha_2)}(x, y)\right] = \left[F_{\mathfrak{b}(\beta_1,\beta_2)}(x, y)\right], \\ F_{\mathfrak{a}(\alpha_1,\alpha_2)}(x, y) \sim F_{\mathfrak{b}(\beta_1,\beta_2)}(x, y).\end{gathered}$$

Then there exists a matrix $M \in SL(2, \mathbb{Z})$ such that

$$F_{\mathfrak{b}(\beta_1,\beta_2)}(x, y) = F^M_{\mathfrak{a}(\alpha_1,\alpha_2)}(x, y) = F_{\mathfrak{a}(\alpha_1,\alpha_2)M}(x, y)$$

by Remark 3.3.2. Let $(\gamma_1\, \gamma_2) := (\alpha_1\, \alpha_2)M$, then $F_{\mathfrak{b}(\beta_1,\beta_2)}(x, y) = F_{\mathfrak{a}(\gamma_1,\gamma_2)}(x, y)$ where $\{\gamma_1, \gamma_2\}$ is also an integral basis for $\mathfrak{a}$ satisfying Equation 3.1. Equality of the forms implies the equality of the coefficients of the forms, so $\dfrac{N(\gamma_1)}{N(\mathfrak{a})} = \dfrac{N(\beta_1)}{N(\mathfrak{b})}$, $N(\gamma_1)N(\beta_1) > 0$ since $N(\mathfrak{a}), N(\mathfrak{b}) > 0$. Thus, $N(\gamma_1)$ and $N(\beta_1)$ are both positive or both negative, then the two basis $\{\gamma_1\beta_1, \gamma_2\beta_1\}$ and $\{\beta_1\gamma_1, \beta_2\gamma_1\}$ both satisfy Equation 3.1 or both not. Let us denote ε the sign of $N(\gamma_1)$ and $N(\beta_1)$. Then,

$$\begin{aligned} F_{\beta_1\mathfrak{a}(\gamma_1\beta_1,\gamma_2\beta_1)}(x, y) &= \frac{N(\gamma_1\beta_1 x + \gamma_2\beta_1 y)}{N(\beta_1)N(\mathfrak{a})} \\ &= \varepsilon_{(N(\beta_1))}F_{\mathfrak{a}(\gamma_1,\gamma_2)}(x, y) \\ &= \varepsilon_{(N(\gamma_1))}F_{\mathfrak{b}(\beta_1,\beta_2)}(x, y) \\ &= F_{\gamma_1\mathfrak{b}(\beta_1\gamma_1,\beta_2\gamma_1)}(x, y). \end{aligned}$$

Again by the equality of the forms, we get $\dfrac{T(\gamma_1\beta_1(\gamma_2\beta_1)')}{N(\beta_1\mathfrak{a})} = \dfrac{T(\beta_1\gamma_1(\beta_2\gamma_1)')}{N(\gamma_1\mathfrak{b})}$, $\dfrac{N(\gamma_2\beta_1)}{N(\beta_1\mathfrak{a})} = \dfrac{N(\beta_2\gamma_1)}{N(\gamma_1\mathfrak{b})}$ and $\dfrac{N(\gamma_1\beta_1)}{N(\beta_1\mathfrak{a})} = \dfrac{N(\beta_1\gamma_1)}{N(\gamma_1\mathfrak{b})}$. The last equation implies that $N(\beta_1\mathfrak{a}) = N(\gamma_1\mathfrak{b})$. Thus, we have two ideals $\beta_1\mathfrak{a}$ and $\gamma_1\mathfrak{b}$ with basis $\{\gamma_1\beta_1, \gamma_2\beta_1\}$ and $\{\gamma_1\beta_1, \gamma_1\beta_2\}$ respectively, and $T((\gamma_1\beta_1)(\gamma_2\beta_1)') = T((\gamma_1\beta_1)(\gamma_1\beta_2)')$, $N(\gamma_2\beta_1) = N(\beta_2\gamma_1)$ by the first and second equations. So by Lemma 3.3.5, we get $\gamma_2\beta_1 = \beta_2\gamma_1$, hence $\beta_1\mathfrak{a} = \gamma_1\mathfrak{b}$ with $N(\beta_1\gamma_1) > 0$, so $\mathfrak{a} \simeq \mathfrak{b}$.

We obtained the following theorem:

Theorem 3.3.6. *Equivalent quadratic forms belong to ideals which are equivalent in the narrower sense. Conversely, quadratic forms belonging to ideals which are equivalent in the narrower sense are equivalent forms.*

4. QUADRATIC RECIPROCITY LAW BY QUADRATIC NUMBER FIELDS WITH HILBERT SYMBOL

The aim of this chapter is to present one of the proofs of the quadratic reciprocity law which is based on the theory of quadratic number fields. Instead of developing the theory of binary quadratic forms, we will give a proof using the ideal theoretic approach since we have discussed the relation between ideals and forms in the previous chapter. We will define the Hilbert's symbol for quadratic number fields in this chapter and compare it with Legendre symbol. Then we will define genus by using character sets and prove the quadratic reciprocity law. Furthermore, we will find the number of genera.

4.1. The Integers in the Quadratic Number Field

We begin by recalling some basic results. Let $m \in \mathbb{Z}$ be squarefree, $m \neq 1$, then the field $\mathbb{Q}(\sqrt{m})$ over $\mathbb{Q}$ is called a *quadratic number field*. Throughout the following chapter, we will denote the ring of integers in $\mathbb{Q}(\sqrt{m})$ by $\mathfrak{O}$. If $A \in \mathfrak{O}$, then $A\mathfrak{O}$ is the principle ideal generated by A. For short, we will denote $A\mathfrak{O}$ by A and let the context make it clear that A is a number or an ideal.

Each number $A \in \mathbb{Q}(\sqrt{m})$ can be brought into the form $\dfrac{a+b\sqrt{m}}{c}$ where the numbers $a, b, c \in \mathbb{Z}$.

We will denote the operation that changes $\sqrt{m}$ to $-\sqrt{m}$ by $'$, so for $A = \dfrac{a+b\sqrt{m}}{c}$, we have $A' = \dfrac{a-b\sqrt{m}}{c}$.

For $A \in \mathfrak{O}$, we have $A + A' = \dfrac{2a}{c} \in \mathbb{Z}$ and $A \cdot A' = \dfrac{a^2 - b^2 m}{c^2} \in \mathbb{Z}$. See [4] for proof.

Theorem 4.1.1. *The $\mathbb{Z}$-basis of the ring of integers $\mathfrak{O}$ in the quadratic number field*

$\mathbb{Q}(\sqrt{m})$ *is* $\{1, \omega\}$ *where* ω *is defined as following:*

$$\begin{aligned} \omega &= \sqrt{m}, \qquad if \quad m \equiv 2,3 \qquad \mod 4, \\ \omega &= \frac{1+\sqrt{m}}{2}, \quad if \quad m \equiv 1 \qquad \mod 4. \end{aligned}$$

We denote the discriminant of $\mathbb{Q}(\sqrt{m})$ *over* $\mathbb{Q}$ *by* $disc_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))$*, then*

$$\begin{aligned} disc_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m})) &= 4m, \quad if \quad m \equiv 2,3 \qquad \mod 4, \\ disc_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m})) &= m, \quad if \quad m \equiv 1 \qquad \mod 4. \end{aligned}$$

Proof. See [3] and Appendix A.0.7 for calculations. □

Definition 4.1.2. For each ideal $\mathfrak{a}$ in the number field $\mathbb{Q}(\sqrt{m})$, the product $\mathfrak{a}.\mathfrak{a}'$ is a set generated by a number in $\mathbb{Q}$ as shown in Appendix B.0.22, say $\mathfrak{a}\mathfrak{a}' = \mathfrak{O}x$ for $x \in \mathfrak{O}$. Then, x is denoted by $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a})$ and called *the norm of the ideal* $\mathfrak{a}$.

Note that, for $\mathfrak{a} \cdot \mathfrak{a}' = \mathfrak{O}x$, $x \in \mathbb{Q}$ is not completely determined by this condition, x is determined up to its two associates, that is if $x, y \in \mathbb{Q}$ represent $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a})$, then $x = y(-1)^a$ for some $a \in \{0, 1\}$.

4.2. The Prime Ideals in $\mathbb{Q}(\sqrt{m})$

We will first consider the prime numbers in $\mathbb{Q}$ which are different from 2 and do not divide m. There are two kinds of such primes:
i) a prime number $p \in \mathbb{Z}$ such that m is a quadratic residue modulo p in $\mathbb{Z}$,
ii) a prime number $q \in \mathbb{Z}$ such that m is a quadratic non-residue modulo q in $\mathbb{Z}$.

Lemma 4.2.1. *If* $p \in \mathbb{Z}$ *is a prime number with* $p \neq 2$*,* $p \nmid m$ *and if* m *is a quadratic residue modulo* p*, then* p *is reducible into two different prime ideals in* $\mathbb{Q}(\sqrt{m})$*. We say that* p *splits in* $\mathbb{Q}(\sqrt{m})$*.*

Proof. Let $p \in \mathbb{Z}$ be a prime number with $p \neq 2$ such that m is a quadratic residue

modulo p in $\mathbb{Z}$. Then $m \equiv e^2 \mod p$ for some number $e \in \mathbb{Z}$, and

$$\begin{aligned}(p, e+\sqrt{m})(p, e-\sqrt{m}) &= (p \cdot p, [e+\sqrt{m}]p, p\,[e-\sqrt{m}], [e+\sqrt{m}][e-\sqrt{m}]) \\ &= (p^2, p\,[e+\sqrt{m}], p\,[e-\sqrt{m}], e^2-m) \\ &= p(p, e+\sqrt{m}, e-\sqrt{m}, \frac{e^2-m}{p}) \\ &= p, \text{ since } p \text{ and } (e+\sqrt{m})+(e-\sqrt{m}) = 2e \\ &\quad \text{are in } (p, e+\sqrt{m}, e-\sqrt{m}, \frac{e^2-m}{p}), \text{ and } (p, 2e) = 1.\end{aligned}$$

Thus we have the desired result, $p = \mathfrak{b} \cdot \mathfrak{b}'$ where $\mathfrak{b} = (p, e+\sqrt{m})$ with $(p, e+\sqrt{m}) \neq (p, e-\sqrt{m})$ since $(p, e+\sqrt{m}, e-\sqrt{m}) = 1$, so $\mathfrak{b} \neq \mathfrak{b}'$. □

Lemma 4.2.2. *If $q \in \mathbb{Z}$ is a prime number with $q \neq 2$, $q \nmid m$ and if m is a quadratic non-residue modulo q, then q is prime in $\mathbb{Q}(\sqrt{m})$. We say that q is inert in $\mathbb{Q}(\sqrt{m})$.*

Proof. Let $q \in \mathbb{Z}$ be a prime number with $q \neq 2$ such that m is a quadratic non-residue modulo q in $\mathbb{Q}$. If $q = \mathfrak{a}\mathfrak{b}$ for some ideals $\mathfrak{a}, \mathfrak{b}$ in $\mathbb{Q}(\sqrt{m})$, then we can find an integer $A = \alpha + \beta\sqrt{m} \in \mathfrak{O}$ such that $q \nmid A$, but one of its prime ideal divisors in $\mathbb{Q}(\sqrt{m})$ divides A, say $\mathfrak{a} \mid A$ without loss of generality. Necessarily $(\beta, q) = 1$, because if not $(\beta, q) = q$ since q is prime, then $q \mid \beta^2$. Also $q \mid A \cdot A' = \alpha^2 - \beta^2 m$ since $\mathfrak{a}' = \mathfrak{b}$ and therefore $q \mid \alpha^2$, $q \mid \alpha$, thus $q \mid A$ which contradicts our assumption that $q \nmid A$. Again by using the fact that $q \mid A \cdot A'$, we get $\alpha^2 - \beta^2 m \equiv 0 \mod q$ where $(\beta, q) = 1$, so $m \equiv (\frac{\alpha}{\beta})^2 \mod q$ which contradicts our hypothesis that m is a quadratic non-residue modulo q in $\mathbb{Q}$. □

Now we will consider the prime numbers in $\mathbb{Q}$ which are different from 2 and divide m. Let $l_1, l_2, \ldots, l_r$ denote the prime numbers in $\mathbb{Q}$ different from 2 that divide the number m. Then $m = l_1 l_2 \ldots l_r$ or $m = 2 l_1 l_2 \ldots l_r$.

Lemma 4.2.3. *Let l be a prime number in $\mathbb{Q}$. Then the ideal $(l, \sqrt{m})$ is a prime ideal in $\mathbb{Q}(\sqrt{m})$.*

Proof. Let l be a prime number in $\mathbb{Q}$, and assume that $\mathfrak{l} = (l, \sqrt{m}) = \mathfrak{a}\mathfrak{b}$ for some

ideals $\mathfrak{a}$, $\mathfrak{b}$ in $\mathbb{Q}(\sqrt{m})$. Then, $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a})$ and $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{b})$ divides $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{l}) = (l, \sqrt{m})(l, -\sqrt{m}) = (l^2, l\sqrt{m}, m) = l(l, \sqrt{m}, \frac{m}{l}) = l$ since $(l, \frac{m}{l}) = 1$. Since $l \in \mathbb{Z}$ is prime, $\mathfrak{a} = \mathfrak{O}$ or $\mathfrak{b} = \mathfrak{O}$, therefore $\mathfrak{l}$ is a prime ideal. □

Lemma 4.2.4. *If $l \in \mathbb{Q}$ is a prime number with $l \neq 2$ and if $l \mid m$, then l is reducible into two prime ideals in $\mathbb{Q}(\sqrt{m})$, say $l = \mathfrak{l} \cdot \mathfrak{l}'$ where $\mathfrak{l}$, $\mathfrak{l}'$ are conjugate prime ideals in $\mathbb{Q}(\sqrt{m})$ and $\mathfrak{l} = \mathfrak{l}'$. We say that l ramifies in $\mathbb{Q}(\sqrt{m})$.*

Proof. Consider the ideals

$$\mathfrak{l}_1 = \mathfrak{l}'_1 = (l_1, \sqrt{m}), \mathfrak{l}_2 = \mathfrak{l}'_2 = (l_2, \sqrt{m}), \ldots, \mathfrak{l}_r = \mathfrak{l}'_r = (l_r, \sqrt{m}).$$

Then the ideals $\mathfrak{l}_1, \mathfrak{l}_2, \ldots, \mathfrak{l}_r$ are prime ideals in $\mathbb{Q}(\sqrt{m})$ by Lemma 4.2.3 and $l_1 = \mathfrak{l}_1{}^2, l_2 = \mathfrak{l}_2{}^2, \ldots, l_r = \mathfrak{l}_r{}^2$. □

Lastly we will consider the prime number 2.

Lemma 4.2.5. *If $m \equiv 5 \mod 8$, then 2 is irreducible in $\mathfrak{O}$.*

If $m \equiv 1 \mod 8$, then $2 = \mathfrak{b} \cdot \mathfrak{b}'$ where $\mathfrak{b} \neq \mathfrak{b}'$.

For the other cases, that is if $2 \mid disc_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))$, then $2 = \mathfrak{b} \cdot \mathfrak{b}'$ where $\mathfrak{b} = \mathfrak{b}'$.

Proof. First let $m \equiv 1 \mod 4$. The congruence

$$x^2 - x - \frac{m-1}{4} \equiv 0 \mod 2$$

is reducible or irreducible according as $\frac{m-1}{4}$ is congruent to 0 or 1 modulo 2, that is according as $m \equiv 1 \mod 8$ or $m \equiv 5 \mod 8$. See [5] for irreducible polynomials.

If $m \equiv 1 \mod 8$, then

$$2 = (2, \frac{1+\sqrt{m}}{2})(2, \frac{1-\sqrt{m}}{2}) = \mathfrak{b} \cdot \mathfrak{b}'$$

where $\mathfrak{b} \neq \mathfrak{b}'$ since $(2, \frac{1+\sqrt{m}}{2}, \frac{1-\sqrt{m}}{2}) = 1$.

If $2 \mid \text{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))$, then $m \equiv 2 \mod 4$ or $m \equiv 3 \mod 4$. If $m \equiv 2 \mod 4$, then $2 = (2, \sqrt{m})^2$, but if $m \equiv 3 \mod 4$, then $2 = (2, 1+\sqrt{m})^2$.

Hence, $2 = \mathfrak{l}^2$ if and only if $2 \mid \text{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))$. □

Now we get the following table:

Table 4.1. Decomposition of 2 into its prime ideals in $\mathbb{Q}(\sqrt{m})$

$m \equiv 1 \mod 8 \Rightarrow 2 = \mathfrak{b}\mathfrak{b}', \mathfrak{b} = (2, \frac{1+\sqrt{m}}{2}), \mathfrak{b} \neq \mathfrak{b}'$
$m \equiv 5 \mod 8 \Rightarrow 2 = \mathfrak{b}$ where $\mathfrak{b}$ is prime in $\mathbb{Q}(\sqrt{m})$
$m \equiv 2 \mod 4 \Rightarrow 2 = \mathfrak{l}^2$ where $\mathfrak{l} = \mathfrak{l}' = (2, \sqrt{m})$
$m \equiv 3 \mod 4 \Rightarrow 2 = \mathfrak{l}^2$ where $\mathfrak{l} = \mathfrak{l}' = (2, 1+\sqrt{m})$

Definition 4.2.6. Let $a \in \mathbb{Q}$ be arbitrary and $t \in \mathbb{Q}$ be a prime number. If $t \neq 2$, then

$$\left(\frac{a}{t}\right) = \begin{cases} +1, & \text{if} \quad a \text{ is a quadratic residue modulo } t \text{ in } \mathbb{Q}, \\ -1, & \text{if} \quad a \text{ is a quadratic nonresidue modulo } t \text{ in } \mathbb{Q}, \\ 0, & \text{if} \quad t \mid a. \end{cases}$$

If $t = 2$, then

$$\left(\frac{a}{2}\right) = \begin{cases} +1, & \text{if} \quad a \text{ is a quadratic residue modulo 8 in } \mathbb{Q}, \\ -1, & \text{if} \quad a \text{ is a quadratic nonresidue modulo 8 in } \mathbb{Q}, \\ 0, & \text{if} \quad 2 \mid a. \end{cases}$$

We have the following theorem by combining Lemma 4.2.1, Lemma 4.2.2, Lemma 4.2.4, Lemma 4.2.5 and Definition 4.2.6.

Theorem 4.2.7. *Let $\mathbb{Q}(\sqrt{m})$ be a quadratic number field over $\mathbb{Q}$ and $d = disc_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))$ be its discriminant. Let t be a prime number in $\mathbb{Q}$.*

If $\left(\frac{d}{t}\right) = +1$, then t is reducible into two different conjugate prime ideals in $\mathbb{Q}(\sqrt{m})$.

If $\left(\frac{d}{t}\right) = -1$, then t is irreducible in $\mathbb{Q}(\sqrt{m})$.

If $\left(\frac{d}{t}\right) = 0$, then t is equal to a square of a prime ideal in $\mathbb{Q}(\sqrt{m})$.

This theorem will be used repeatedly.

4.3. Hilbert's Symbol

Definition 4.3.1. Let $n, m \in \mathbb{Z}$, m be squarefree and $w \in \mathbb{Z}$ be a prime number. We define Hilbert's symbol by

$$\left(\frac{n}{w:m}\right) = \begin{cases} +1, & \text{if for all } i \in \mathbb{N}, \text{ there is } \alpha_i \in \mathbb{Q}(\sqrt{m}) \text{ such that} \\ & n \equiv N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha_i) \mod w^i, \\ -1, & \text{otherwise.} \end{cases}$$

Definition 4.3.2. Let $n, m \in \mathbb{Z}$ with m is not the square of an integer and $w \in \mathbb{Z}$ be any prime number. The integer n is called a *norm residue of $\mathbb{Q}(\sqrt{m})$ modulo w*, if $\left(\frac{n}{w:m}\right) = +1$; *a norm non-residue of $\mathbb{Q}(\sqrt{m})$ modulo w*, if $\left(\frac{n}{w:m}\right) = -1$.

Remark 4.3.3. If n is itself the norm of an integer α in the field $\mathbb{Q}(\sqrt{m})$, then we have $\left(\frac{n}{w:m}\right) = +1$, because we can write the congruence $n \equiv N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha) \mod w^i$ for all $i \in \mathbb{N}$.

Lemma 4.3.4. *Let w be an odd prime number and $w \mid m$, but $w \nmid n$. Then any of the*

congruences

$$4n \equiv (2x+y)^2 - my^2 \mod w, \tag{4.1}$$

$$n \equiv x^2 - my^2 \mod w \tag{4.2}$$

is solvable in rational integers x and y if and only if $\left(\frac{n}{w}\right) = +1$.

Proof. If $\left(\frac{n}{w}\right) = +1$, then $n \equiv x^2 \mod w$ has a solution in rational integers x. Also $w \mid m$, so $m \equiv 0 \mod w$, $-my^2 \equiv 0 \mod w$ has a solution for all rational integers y. Then, $n + 0 \equiv x^2 - my^2 \mod w$ has a solution in rational integers x and y, so does Equation 4.2. Note that $N(x+\sqrt{m}y) = x^2 - my^2$, so we have $n \equiv N(x+\sqrt{m}y) \mod w$. If $m \equiv 2, 3 \mod 4$, then $x+\sqrt{m}y$ is an integer in $\mathbb{Q}(\sqrt{m})$, so $\left(\frac{n}{w:m}\right) = +1$.

Similarly, if $\left(\frac{n}{w}\right) = +1$, then $n \equiv (\frac{2x+y}{2})^2 \mod w$ has a solution in integers. Also $w \mid m$, so $m \equiv 0 \mod w$, $-m(\frac{y}{2})^2 \equiv 0 \mod w$ has a solution for all rational integers y. Then, $n \equiv (\frac{2x+y}{2})^2 - m(\frac{y}{2})^2 \mod w$, and $4n \equiv (2x+y)^2 - my^2 \mod w$ has a solution in rational integers x and y, so Equation 4.1. Note that $N(x+y\frac{1+\sqrt{m}}{2}) = (\frac{2x+y}{2})^2 - m(\frac{y}{2})^2$, so we have $n \equiv N(x+y\frac{1+\sqrt{m}}{2}) \mod w$. If $m \equiv 1 \mod 4$, then $x+y\frac{1+\sqrt{m}}{2}$ is an integer in $\mathbb{Q}(\sqrt{m})$, so $\left(\frac{n}{w:m}\right) = +1$.

Conversely, if Equation 4.1 is solvable, then $n \equiv x^2 - my^2 \equiv x^2 \mod w$ is solvable in integers x, hence $\left(\frac{n}{w}\right) = +1$. Furthermore, note that $n \equiv x^2 \mod w^i$ is solvable for all $i \in \mathbb{N}$. Then congruences in Equation 4.1 are solvable modulo w^i for all $i \in \mathbb{N}$ by Remark 4.3.3. Hence, $\left(\frac{n}{w:m}\right) = \left(\frac{n}{w}\right)$. Similar for Equation 4.2. □

Lemma 4.3.5. *Let w be an odd prime, $w \nmid m$ and $w \nmid n$. Then the congruence*

$$n \equiv x^2 - my^2 \mod w$$

always has solutions in rational integers x and y.

Proof. **Case 1.** $\left(\frac{n}{w}\right) = +1$.
For the right hand side of this congruence, the values $x = 1, 2, \ldots, \frac{1}{2}(w-1)$ and $y = 0$ give all the quadratic residues modulo w. So we always have solutions in this case.

Case 2. $\left(\frac{n}{w}\right) = -1$.

Subcase 1. $\left(\frac{-m}{w}\right) = -1$.
Congruence gives all the quadratic non-residues modulo w for the values $x = 0$ and $y = 1, 2, \ldots, \frac{1}{2}(w-1)$, because we get $n \equiv 0 - my^2 \equiv -my^2 \mod w$, so $\left(\frac{n}{w}\right) = \left(\frac{-my^2}{w}\right) = \left(\frac{-m}{w}\right) = -1$. So we always have solutions in this case.

Subcase 2. $\left(\frac{-m}{w}\right) = +1$.
Let a be the least positive quadratic non-residue modulo w, that is $a \equiv x^2 \mod w$ has no solution with $a > 0$ and a is the minimum over this property. Then $a - 1$ is a quadratic residue. Let $y = b$ be a root of the congruence $-my^2 \equiv a - 1 \mod w$. The solution exists since $\left(\frac{-m}{w}\right) = +1$. So $a \equiv 1 - mb^2 \mod w$ and ax^2 represents all the quadratic non-residues modulo w for $x = 1, 2, \ldots, \frac{1}{2}(w-1)$, so also $x^2(1 - mb^2) = x^2 - m(bx)^2$ for $x = 1, 2, \ldots, \frac{1}{2}(w-1)$. So $n \equiv x^2 - my^2 \mod w$ has a solution in this case since $\left(\frac{n}{w}\right) = -1$. □

Theorem 4.3.6. *Let w be a prime number and $n, m \in \mathbb{Z}$ be not divisible by w. Then we have*

A. *If w is odd,*

$$\left(\frac{n}{w : m}\right) = +1, \tag{4.3}$$

$$\left(\frac{n}{w : w}\right) = \left(\frac{w}{w : n}\right) = \left(\frac{n}{w}\right). \tag{4.4}$$

B. *If w is even, i.e. $w = 2$,*

$$\left(\frac{n}{2:m}\right) = (-1)^{\frac{(n-1)(m-1)}{4}}, \tag{4.5}$$

$$\left(\frac{n}{2:2}\right) = \left(\frac{2}{2:n}\right) = (-1)^{\frac{(n^2-1)}{8}}. \tag{4.6}$$

Now, let w be a prime number and $n, n', m, m' \in \mathbb{Z}$. Then we have,

$$\left(\frac{-m}{w:m}\right) = +1, \tag{4.7}$$

$$\left(\frac{n}{w:m}\right) = \left(\frac{m}{w:n}\right), \tag{4.8}$$

$$\left(\frac{nn'}{w:m}\right) = \left(\frac{n}{w:m}\right)\left(\frac{n'}{w:m}\right), \tag{4.9}$$

$$\left(\frac{n}{w:mm'}\right) = \left(\frac{n}{w:m}\right)\left(\frac{n}{w:m'}\right). \tag{4.10}$$

Proof. Note that if $n, n' \in \mathbb{Z} \setminus \{0\}$ satisfy $\frac{n}{n'} = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\frac{\alpha}{\alpha'})$ for some integers α, α' in $\mathbb{Q}(\sqrt{m})$, then $nN_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha') = n'N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha)$, so $\left(\frac{n}{w:m}\right) = \left(\frac{n'}{w:m}\right)$ by Definition 4.3.1. So $\left(\frac{n}{w:m}\right)$ does not change, if we multiply n by a square or remove a square factor from n, because $a^2 = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(a)$ for $a \in \mathbb{Z}$. So from now on, we can assume that m and n are not divisible by the square of a prime number.

The proof of Equation (4.7): The number, $-m$ is the norm of an integer $\sqrt{m}$ in

$\mathbb{Q}(\sqrt{m})$, so

$$\left(\frac{-m}{w:m}\right) = +1$$

by Definition 4.3.1.

To prove the other equations, we need some case analysis.

Case 1. w: odd prime, $w \mid m$, Subcase 1. $w \mid n$, Subcase 2. $w \mid n$,

Case 2. w: odd prime, $w \nmid m$,Subcase 1. $w \nmid n$, Subcase 2. $w \mid n$,

Case 3. $w = 2$, Subcase 1. n is odd, Subcase 2. n is even.

Case 1. Let w be an odd prime and $w \mid m$.

1.a. Let $w \nmid n$. Then $\left(\frac{n}{w:m}\right) = \left(\frac{n}{w}\right)$ by the corollary in the proof of Lemma 4.3.4.

1.b. Let $w \mid n$.

$$\begin{aligned}\left(\frac{n}{w:m}\right) &= \left(\frac{-nm}{w:m}\right) \text{ by Equation 4.7} \\ &= \left(\frac{-nm/w^2}{w:m}\right) \\ &= \left(\frac{-nm/w^2}{w}\right) \text{ by Case 1.a, since } w \nmid \frac{-nm}{w^2}.\end{aligned}$$

Remember that m and n are squarefree.

Case 2. Let w be an odd prime and $w \nmid m$.

2.a. Let $w \nmid n$.

Lemma 4.3.5 implies that the congruence $n \equiv x^2 - my^2$ is solvable modulo every power of w. Thus, $\left(\frac{n}{w:m}\right) = +1$ for Case 2.a.

2.b. Let $w \mid n$. Note that $w^2 \nmid n$.

A solution of the congruence $n \equiv x^2 - my^2 \mod w^2$ would give rise to a number $\alpha = x - \sqrt{m}y$ of the field $\mathbb{Q}(\sqrt{m})$ for which the norm $\alpha \cdot \alpha' = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha)$ contains only w, but not w^2 as a factor. So $w \cdot z = \alpha \cdot \alpha'$ for prime w implies $w = \mathfrak{w} \cdot \mathfrak{w}'$ where $\mathfrak{w}$ and $\mathfrak{w}'$ are two distinct prime ideals in $\mathbb{Q}(\sqrt{m})$, so $\left(\frac{m}{w}\right) = +1$ by Theorem 4.2.7.

Conversely, if $\left(\frac{m}{w}\right) = +1$, then $w = \mathfrak{w} \cdot \mathfrak{w}'$ for two distinct prime ideals $\mathfrak{w}, \mathfrak{w}'$ in $\mathbb{Q}(\sqrt{m})$. Let $\alpha \in \mathbb{Q}(\sqrt{m})$ be an integer such that $w \mid \alpha$, but $\mathfrak{w}^2 \nmid \alpha$ and $\mathfrak{w}'^2 \nmid \alpha$. Then,

$$\begin{aligned}
\left(\frac{n}{w:m}\right) &= \left(\frac{nN_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha)}{w:m}\right) \\
&= \left(\frac{\frac{nN_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha)}{w^2}}{w:m}\right) \\
&= +1 \text{ by Case 2.a since } w \nmid \frac{nN_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha)}{w^2}.
\end{aligned}$$

Thus, $\left(\frac{n}{w:m}\right) = \left(\frac{m}{w}\right)$ for Case 2.b.

Now we get the equations by using all these cases.

The proof of Equation (5.3): $\left(\frac{n}{w:m}\right) = +1$ since w is an odd prime, $w \nmid m$, $w \nmid n$ by Case 2.a.

The proof of Equation (5.3): $\left(\frac{n}{w:w}\right) = \left(\frac{n}{w}\right)$ by Case 1.a and $\left(\frac{w}{w:n}\right) = \left(\frac{n}{w}\right)$ by Case 2.b.

The following equations will be proved for odd prime w.

The proof of Equation (4.8): If $w \mid m$ and $w \nmid n$, then $\left(\frac{n}{w:m}\right) = \left(\frac{n}{w}\right)$ by Case 1.a and $\left(\frac{m}{w:n}\right) = \left(\frac{n}{w}\right)$ by Case 2.b, so $\left(\frac{n}{w:m}\right) = \left(\frac{m}{w:m}\right)$.

Similar for the case $w \mid n$ and $w \nmid m$ since it is symmetric of the situation in the proof of Equation (4.8).

If $w \nmid m$ and $w \nmid n$, then $\left(\frac{n}{w:m}\right) = +1 = \left(\frac{m}{w:n}\right)$ by Case 2.a.

If $w \mid n$ and $w \mid m$, then $\left(\frac{n}{w:m}\right) = \left(\frac{-nm/w^2}{w:m}\right) = \left(\frac{-mn/w^2}{w}\right) = \left(\frac{m}{w:n}\right)$ by Case 1.b. Hence, we deduce Equation (4.8) for odd primes w by considering successively the different cases of divisibility and non-divisibility of n and m by w.

The proof of Equation (4.9): The equation $\left(\frac{nn'}{w:m}\right) = \left(\frac{n}{w:m}\right)\left(\frac{n'}{w:m}\right)$ will be shown by case analysis.

Case 1. If $w \mid m$,

1.a. If $w \nmid nn'$, then $w \nmid n$ and $w \nmid n'$. So

$$\left(\frac{nn'}{w:m}\right) = \left(\frac{nn'}{w}\right) = \left(\frac{n}{w}\right)\left(\frac{n'}{w}\right) = \left(\frac{n}{w:m}\right)\left(\frac{n'}{w:m}\right).$$

1.b. If $w \mid nn'$, then $\left(\frac{nn'}{w:m}\right) = \left(\frac{-nn'm/w^2}{w}\right)$ because of the following cases.

1.b.(i) If $w \nmid n$ and $w \mid n'$, then $\left(\frac{n}{w:m}\right) = \left(\frac{n}{w}\right)$ and $\left(\frac{n'}{w:m}\right) = \left(\frac{-n'm/w^2}{w}\right)$ since $w \nmid \frac{-n'm}{w^2}$ by Case 2.a. So $\left(\frac{nn'}{w:m}\right) = \left(\frac{-nn'm/w^2}{w}\right) = \left(\frac{n}{w}\right)\left(\frac{n'(-m)/w^2}{w}\right) = \left(\frac{n}{w:m}\right)\left(\frac{n'}{w:m}\right)$.

The case in which $w \nmid n'$ and $w \mid n$ and the case in which $w \nmid n$ and $w \mid n'$ are symmetric.

1.b.(ii) The case in which $w \mid n$ and $w \mid n'$ is not defined since $w^2 \nmid nn'$, because $\left(\frac{n}{w:m}\right)$ is defined where n and m are not divisible by a square of a prime number.

2. If $w \nmid m$,

2.a. If $w \nmid nn'$, then $\left(\frac{nn'}{w:m}\right) = +1$. Also, $w \nmid n$ and $w \nmid n'$, so $\left(\frac{n}{w:m}\right) = +1$ and $\left(\frac{n'}{w:m}\right) = +1$. Hence, $\left(\frac{n}{w:m}\right) \cdot \left(\frac{n'}{w:m}\right) = +1$.

2.b. If $w \mid nn'$, then

$$\left(\frac{nn'}{w:m}\right) = \left(\frac{m}{w}\right),$$

because if $w \mid n$ and $w \nmid n'$, then $\left(\frac{n}{w:m}\right) = \left(\frac{m}{w}\right)$ by Case 2.b and $\left(\frac{n'}{w:m}\right) = +1$. So,

$$\left(\frac{n}{w:m}\right)\left(\frac{n'}{w:m}\right) = \left(\frac{m}{w}\right).$$

The case $w \nmid n$ and $w \mid n'$ is symmetric.

We do not have the case $w \mid n$ and $w \mid n'$.

Hence we deduce Equation 4.9 for odd primes w by considering successively the different cases of divisibility and non-divisibility of n, n' by w.

The proof of Equation (4.10): Equation 4.8 and Equation 4.9 together imply Equation 4.10.

Case 3. Let $w = 2$.

Now we will consider two cases and two subcases in each case.

3.a. Let n be an odd integer. To determine the value of the symbol $\left(\frac{n}{2:m}\right)$, we have to investigate for which combinations of values of n and m, the congruence $n \equiv N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha) \mod 2^3$ is solvable for some $\alpha \in \mathfrak{O}$. After long calculations in Appendix A.0.9, we get the following table.

Table 4.2. Table of $n = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha) \mod 2^3$

m	n
1	1,3,5,7
2	1,7
3	1,5
5	1,3,5,7
6	1,3
7	1,5

3.a.(i) Let m be an odd integer. So we will show that $\left(\frac{n}{2:m}\right) = (-1)^{\frac{(n-1)(m-1)}{4}}$.

If $m \equiv 1, 5 \mod 8$, then $(-1)^{\frac{(n-1)(m-1)}{4}} = 1$ for all $n \equiv 1, 3, 5, 7 \mod 8$.

If $m \equiv 3 \mod 8$, then $(-1)^{\frac{(n-1)}{2}} = 1$ for $n \equiv 1, 5 \mod 8$ and $(-1)^{\frac{(n-1)(m-1)}{4}} = -1$ for $n \equiv 3, 7 \mod 8$.

If $m \equiv 7 \mod 8$, then $(-1)^{\frac{3(n-1)}{2}} = 1$ for $n \equiv 1, 5 \mod 8$ and $(-1)^{\frac{3(n-1)}{2}} = -1$ for $n \equiv 3, 7 \mod 8$.

3.a.(ii) Let m be an even integer, say $m = 2m'$. By using the table, we get that $\left(\frac{n}{2:2m'}\right) = (-1)^{\frac{(n^2-1)}{8}} \cdot (-1)^{\frac{(n-1)(m^2-1)}{4}}$.

So for $m' = 1$, we get Equation 4.6 where n is odd.

3.b. Let n be an even integer,say $n = 2n'$.

3.b.(i) Let m be an odd integer. So $m \equiv 1 \mod 4$ or $m \equiv 3 \mod 4$.

Firstly, if $m \equiv 1 \mod 4$, then $\mathrm{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m})) = m$ is odd, so $\left(\frac{m}{2}\right) = +1$, that is $2 = \mathfrak{p}\mathfrak{p}'$ where $\mathfrak{p} \neq \mathfrak{p}'$ by Theorem 4.2.7. So we can find $\alpha \in \mathfrak{O}$ such that $2 \mid N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha)$, but $4 \nmid N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha)$ by choosing $\alpha \in \mathfrak{O}$ with $\mathfrak{p} \mid \alpha$, $\mathfrak{p}^2 \nmid \alpha$ and $\mathfrak{p}' \nmid \alpha$. So

$$\begin{aligned}
\left(\frac{n}{2:m}\right) &= \left(\frac{2n'}{2:m}\right) \\
&= \left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha)}{2:m}\right)\left(\frac{2n'}{2:m}\right) \\
&= \left(\frac{2n'N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha)}{2:m}\right) \\
&= \left(\frac{4}{2:m}\right)\left(\frac{\frac{n'N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha)}{2}}{2:m}\right) \\
&= (+1)\left(\frac{n'r}{2:m}\right) \text{ where } n'r \text{ is odd} \\
&= +1
\end{aligned}$$

by Theorem 4.3.6. Therefore,

$$\left(\frac{2n'}{2:m}\right) = \left(\frac{m}{2}\right) = (-1)^{\frac{m^2-1}{8}}.$$

Now, if $m \equiv 3 \mod 4$, then $2n' \equiv x^2 - my^2 \mod 2^e$ is solvable if and only if $m \equiv x^2 - 2n'y^2 \mod 2^e$ is solvable. Therefore,

$$\left(\frac{2n'}{2:m}\right) = \left(\frac{m}{2:2n'}\right),$$

so again we can use the above case.

3.b.(ii) Let m also be even, then

$$\left(\frac{n}{2:m}\right) = \left(\frac{2n'}{2:2m'}\right) = \left(\frac{-2\cdot 2n'm'}{2:2m'}\right) = \left(\frac{-n'm'}{2:2m'}\right),$$

so we can use the above cases since $n'm'$ is odd. □

4.4. The Character Set of an Ideal

Definition 4.4.1. Let $\mathbb{Q}(\sqrt{m})$ be a quadratic field over $\mathbb{Q}$ and $\text{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))$ be its discriminant. Let $l_1, l_2, \ldots, l_s$ be the list of whole distinct prime numbers dividing $|\text{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))|$. Let $C_2 = \{-1, +1\}$ be a cyclic group of order 2 under multiplication. We define a function

$$\begin{array}{rccl} \Phi & : & \mathbb{Z} & \longrightarrow & C_2^s \\ & & a & \mapsto & \left(\left(\dfrac{a}{l_1 : m}\right), \ldots, \left(\dfrac{a}{l_s : m}\right)\right). \end{array}$$

The s tuple, $\Phi(a)$ is called *the character set of the number a in* $\mathbb{Q}(\sqrt{m})$.

Now we can also define the character set of an ideal $\mathfrak{a}$ by using Definition 4.1.2.

Definition 4.4.2. Let $\mathbb{Q}(\sqrt{m})$ be a quadratic field over $\mathbb{Q}$ and $\text{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))$ be its discriminant. Let $l_1, l_2, \ldots, l_s \in \mathbb{Z}$ be the s distinct prime numbers that divide $\text{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))$. Let $\mathfrak{O}$ be the ring of integers in $\mathbb{Q}(\sqrt{m})$ and $C_2 = \{-1, +1\}$ be a cyclic group under multiplication.

Case 1. If $m < 0$, we define a function

$$\begin{array}{rccl} \Psi & : & \{\mathfrak{a} : \mathfrak{a} \text{ is an ideal in } \mathfrak{O}\} & \longrightarrow & C_2^c \\ & & \mathfrak{a} & \mapsto & \left(\left(\dfrac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a})}{l_1 : m}\right), \ldots, \left(\dfrac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a})}{l_c : m}\right)\right). \end{array}$$

where $c = s$.

Case 2. If $m < 0$ and $\Phi(-1) = (+1, \ldots, +1)$, then we define a function

$$\begin{array}{rccl} \Psi & : & \{\mathfrak{a} : \mathfrak{a} \text{ is an ideal in } \mathfrak{O}\} & \longrightarrow & C_2^c \\ & & \mathfrak{a} & \mapsto & \left(\left(\dfrac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a})}{l_1 : m}\right), \ldots, \left(\dfrac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a})}{l_c : m}\right)\right). \end{array}$$

where $c = s$.

Note that this definition is well defined since $\left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a})}{l_j : m}\right) = \left(\frac{x}{l_j : m}\right) = \left(\frac{y(-1)^a}{l_j : m}\right) = \left(\frac{\mp y}{l_j : m}\right) = \left(\frac{\mp 1}{l_j : m}\right)\left(\frac{y}{l_j : m}\right) = (+1) \cdot \left(\frac{y}{l_j : m}\right) = \left(\frac{y}{l_j : m}\right)$ for all $j \in \{1, 2, \ldots, s\}$ since $\Phi(-1) = (+1, \ldots, +1)$.

Case 3. If $m < 0$ and if $\Phi(-1) \neq (+1, \ldots, +1)$, say $\left(\frac{-1}{l_s : m}\right) = -1$, then we take the value x of the principle ideal $\mathfrak{a}\mathfrak{a}' = \mathfrak{O}x$ such that $\left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a})}{l_s : m}\right) = \left(\frac{x}{l_s : m}\right) = \left(\frac{y(-1)^a}{l_s : m}\right) = \left(\frac{y}{l_s : m}\right)\left(\frac{-1}{l_s : m}\right)^a = +1$ by choosing the suitable number $a \in \{0, 1\}$. For this value $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a}) = x$, we define a function

$$\begin{array}{rcccl} \Psi & : & \{\mathfrak{a} : \mathfrak{a} \text{ is an ideal in } \mathfrak{O}\} & \longrightarrow & C_2^c \\ & & \mathfrak{a} & \mapsto & \left(\left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a})}{l_1 : m}\right), \ldots, \left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a})}{l_c : m}\right)\right). \end{array}$$

where $c = s - 1$.

Note that this definition is well defined since a is fixed first, so $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a})$ is uniquely determined.

Then $\Psi(\mathfrak{a})$ is called *the character set of the ideal* $\mathfrak{a}$ *in* $\mathbb{Q}(\sqrt{m})$.

Recall that an $\mathfrak{O}$-submodule $\mathfrak{a}$ of the field $\mathbb{Q}(\sqrt{m})$ is called a *fractional ideal* in $\mathfrak{O}$, if there exists some nonzero $\gamma \in \mathfrak{O}$ such that $\gamma\mathfrak{a} \subseteq \mathfrak{O}$. Note that we can also extend the function Ψ to the set of all fractional ideals by

$$\begin{array}{rcccl} \Psi & : & \{\mathfrak{a} : \mathfrak{a} \text{ is a fractional ideal }\} & \longrightarrow & C_2^c \\ & & \mathfrak{a} & \mapsto & \left(\left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a})}{l_1 : m}\right), \ldots, \left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a})}{l_c : m}\right)\right) \end{array}$$

where $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a}) = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{b})/N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\gamma)$ with $\gamma\mathfrak{a} = \mathfrak{b}$, $\gamma \in \mathfrak{O}$, $\mathfrak{b} \subseteq \mathfrak{O}$.

Notation 4.4.3. From now on, we will denote both the functions Φ and Ψ defined

above by Υ.

Lemma 4.4.4. $\Upsilon(\mathfrak{ab}) = \Upsilon(\mathfrak{a})\Upsilon(\mathfrak{b})$ *for all ideals* $\mathfrak{a}$, $\mathfrak{b}$ *in* $\mathfrak{O}$.

Proof. If it is the Case 1 or the Case 2 defined in Definition 4.4.1, then since

$$N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{ab}) = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a})N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{b}),$$

by Appendix B.0.23, we get $\Upsilon(\mathfrak{ab}) = \Upsilon(\mathfrak{a})\Upsilon(\mathfrak{b})$.

If it is the Case 3 defined in Definition 4.4.1, we necessarily have $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{ab}) = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a})N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{b})$, because

$$\begin{aligned}
\left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{ab})}{l_s : m}\right) &= \left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a})N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{b})}{l_s : m}\right) \\
&= \left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a})}{l_s : m}\right)\left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{b})}{l_s : m}\right) \text{ by Theorem 4.3.6} \\
&= 1 \cdot 1 = 1.
\end{aligned}$$

So $\Upsilon(\mathfrak{ab}) = \Upsilon(\mathfrak{a})\Upsilon(\mathfrak{b})$ by Definition 4.4.1. □

Lemma 4.4.5. $\Upsilon(\mathfrak{O}a) = (+1, +1, \ldots, +1)$ *for all* $a \in \mathfrak{O}$.

Proof. **Case 1.** If $m < 0$, then

$$\begin{aligned}
\Upsilon(\mathfrak{O}a) &= \left(\left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{O}a)}{l_1 : m}\right), \ldots, \left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{O}a)}{l_c : m}\right)\right) \\
&= \left(\left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(a)}{l_1 : m}\right), \ldots, \left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(a)}{l_c : m}\right)\right) \\
&= (+1, \ldots, +1),
\end{aligned}$$

by Definition 4.3.1.

Case 2. If $m > 0$ and $\Upsilon(-1) = (1, \ldots, 1)$, then also if $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{O}a) =$

$N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(a)$, we have

$$\Upsilon(\mathfrak{O}a) = \left(\left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(a)}{l_1 : m}\right), \ldots, \left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(a)}{l_c : m}\right)\right) = (+1, \ldots, +1)$$

by Definition 4.3.1.

But if $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{O}a) = -N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(a)$, we have

$$\begin{aligned}
\Upsilon(\mathfrak{O}a) &= \left(\left(\frac{-N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(a)}{l_1 : m}\right), \ldots, \left(\frac{-N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(a)}{l_c : m}\right)\right) \\
&= \left(\left(\frac{-1}{l_1 : m}\right)\left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(a)}{l_1 : m}\right), \ldots, \left(\frac{-1}{l_c : m}\right)\left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(a)}{l_c : m}\right)\right) \\
&= (1 \cdot 1, \ldots, 1 \cdot 1) = (+1, \ldots, +1).
\end{aligned}$$

by Theorem 4.3.6 and Definition 4.3.1.

Case 3. If $m > 0$ and $\Upsilon(-1) \neq (1, \ldots, 1)$, say $\left(\frac{-1}{l_s : M}\right) = -1$, then if $N(\mathfrak{O}a) = N(a)$, we have

$$\Upsilon(\mathfrak{O}a) = \left(\left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(a)}{l_1 : m}\right), \ldots, \left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(a)}{l_c : m}\right)\right) = (1, \ldots, 1)$$

by Definition 4.3.1.

But if $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{O}a) = x = -N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(a)$, we compute $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{O}a) = y = -x < 0$ since

$$\begin{aligned}
\Upsilon(\mathfrak{O}a) &= \left(\left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{O}a)}{l_1 : m}\right), \ldots, \left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{O}a)}{l_c : m}\right)\right) \\
&= \left(\left(\frac{(-1)(-N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(a))}{l_1 : m}\right), \ldots, \left(\frac{(-1)(-N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(a))}{l_c : m}\right)\right)
\end{aligned}$$

$$
\begin{aligned}
&= \left(\left(\frac{(-1)(x)}{l_1 : m}\right), \ldots, \left(\frac{(-1)(x)}{l_c : m}\right)\right) \\
&= \left(\left(\frac{y}{l_1 : m}\right), \ldots, \left(\frac{y}{l_c : m}\right)\right) \\
&= \left(\left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(a)}{l_1 : m}\right), \ldots, \left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(a)}{l_c : m}\right)\right) = (+1, \ldots, +1).
\end{aligned}
$$

□

Corollary 4.4.6. *The principal ideal* $\mathfrak{O}a \in \operatorname{Ker} \Upsilon$ *for all* $a \in \mathfrak{O}$.

Theorem 4.4.7. *The rule defined by*

$$
\begin{array}{rccl}
\overline{\Psi} & : & \{\mathtt{A} : \mathtt{A} \textit{ is an ideal class in } \mathbb{Q}(\sqrt{m})\} & \longrightarrow & C_2^c \\
 & & A = [\mathfrak{a}] & \mapsto & \Upsilon(\mathfrak{a})
\end{array}
$$

is a well defined function.

Proof. Let $\mathtt{A}, \mathtt{B}$ be ideal classes such that $\mathtt{A} = \mathtt{B}$, so $[\mathfrak{a}] = [\mathfrak{b}]$ for some $\mathfrak{a} \in \mathtt{A}$ and $\mathfrak{b} \in \mathtt{B}$. Then there exist $a, b \in \mathfrak{O}$ such that $a \cdot \mathfrak{a} = b \cdot \mathfrak{b}$. Consider $\overline{\Psi}([\mathfrak{a}])$ and $\overline{\Psi}([\mathfrak{b}])$,

$$
\begin{aligned}
\overline{\Psi}([\mathfrak{a}]) &= \Upsilon(\mathfrak{a}) \\
&= \Upsilon(a)\Upsilon(\mathfrak{a}) \text{ by Corollary 4.4.6} \\
&= \Upsilon(a\mathfrak{a}) \text{ by Lemma 4.4.4} \\
&= \Upsilon(b\mathfrak{b}) \text{ since } \Upsilon \text{ is well defined,} \\
&= \Upsilon(b\mathfrak{b}) \text{ by Lemma 4.4.4} \\
&= \Upsilon(\mathfrak{b}\mathfrak{a}) \text{ by Corollary 4.4.6} \\
&= \overline{\Psi}([\mathfrak{b}]),
\end{aligned}
$$

thus $\overline{\Psi}$ is well defined. □

4.5. Genera of Ideal Classes

Definition 4.5.1. Each coset of $\operatorname{Ker}\overline{\Psi}$ in the collection of ideal classes is called *genus*, and denoted by $\mathfrak{G}$. The set $\operatorname{Ker}\overline{\Psi}$ is called *the principal genus* and denoted by $\mathfrak{G}_0$.

Now we will check that whether the map $\overline{\Psi}$ is surjective or not.

4.6. Ambig Ideals

Definition 4.6.1. An ideal $\mathfrak{a}$ in $\mathbb{Q}(\sqrt{m})$ is called an *ambig ideal*, if $\mathfrak{a} = \mathfrak{a}'$ and $\mathfrak{a}$ is not divisible by a number in $\mathbb{Q}$.

Theorem 4.6.2. *Let $\operatorname{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))$ be the discriminant of $\mathbb{Q}(\sqrt{m})$ over $\mathbb{Q}$. A prime ideal $\mathfrak{p}$ divides $\operatorname{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))$ if and only if $\mathfrak{p}$ is an ambig prime ideal in $\mathbb{Q}(\sqrt{m})$. If $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_s$ are all the distinct prime ideals dividing $\operatorname{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))$, then*

$$S = \{\mathfrak{O}, \mathfrak{p}_1\,\mathfrak{p}_2, \ldots, \mathfrak{p}_s, \mathfrak{p}_1\mathfrak{p}_2, \ldots, \mathfrak{p}_1\mathfrak{p}_s, \ldots, \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_s\}$$

is the set of all ambig ideals in $\mathbb{Q}(\sqrt{m})$.

Proof. By the Theorem 4.2.7, for every prime $p \in \mathbb{Z}$, we have that

$$p = \begin{cases} \mathfrak{p}_1\mathfrak{p}_1', & \text{if } p \nmid \operatorname{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m})) \text{ and } \left(\dfrac{\operatorname{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))}{p}\right) = +1, \\ \mathfrak{p}_1, & \text{if } p \nmid \operatorname{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m})) \text{ and } \left(\dfrac{\operatorname{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))}{p}\right) = -1, \\ \mathfrak{p}_1{}^2, & \text{if } p \mid \operatorname{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m})). \end{cases}$$

Consider an ambig ideal $\mathfrak{a} = \mathfrak{p}_1{}^{a_1}\mathfrak{p}_2{}^{a_2} \ldots \mathfrak{p}_n{}^{a_n}$; so

$$\mathfrak{p}_1{}^{a_1}\mathfrak{p}_2{}^{a_2} \ldots \mathfrak{p}_n{}^{a_n} = \mathfrak{p}_1{}'^{a_n}\mathfrak{p}_2{}'^{a_2} \ldots \mathfrak{p}_n{}'^{a_n}$$

and $\mathfrak{a}$ has no integer divisor, that is $p \nmid \mathfrak{a}$ for all prime $p \in \mathbb{Z}$. Thus, there is no $\mathfrak{p}$ of

the second form. Also $a_i = 0$ or 1 for all $i = 1, 2, \ldots, n$. The prime number p is of the first form, so $p = \mathfrak{p}\mathfrak{p}'$. But $\mathfrak{a}$ is ambig, so $\mathfrak{a}' = \mathfrak{p}_1'\mathfrak{p}_2' \ldots \mathfrak{p}_n'$ such that $\mathfrak{p}_i = \mathfrak{p}_i'$; because if not, that is if $\mathfrak{p}_i = \mathfrak{p}_j'$ for $i \neq j$, then $\mathfrak{p}_i\mathfrak{p}_j = \mathfrak{p}_j'\mathfrak{p}_j \in \mathbb{Z}$ divides $\mathfrak{a}$ which contradicts to the Definition 4.6.1. But $\mathfrak{p} = \mathfrak{p}'$ is a contradiction for a prime number p of the first form. Hence there are at most $\mathfrak{p}^0$ or $\mathfrak{p}^1$ of the third form. So the prime ideals dividing $\text{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))$ are the only ambig prime ideals in $\mathbb{Q}(\sqrt{m})$. Thus, S is the set of all ambig ideals in $\mathbb{Q}(\sqrt{m})$ with $|S| = 2^s$. □

4.7. Quadratic Reciprocity Law

Lemma 4.7.1. *If $\text{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))$ of $\mathbb{Q}(\sqrt{m})$ has only a single prime factor, then $\mathfrak{l}$ is the only ambig ideal in $\mathbb{Q}(\sqrt{m})$ where $\mathfrak{l} = \sqrt{m}$ if $m \neq -1$ and $\mathfrak{l} = 1 + \sqrt{-1}$ if $m = -1$.*

Proof. Let l be the only prime divisor of $\text{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))$. By Theorem 4.2.7, $l = \mathfrak{p}^2$, so by Theorem 4.6.2, $\mathfrak{p}$ is the only ambig prime ideal, so only ambig ideal in $\mathbb{Q}(\sqrt{m})$. □

Lemma 4.7.2. *If $\text{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))$ of $\mathbb{Q}(\sqrt{m})$ has only a single prime factor, and if $m > 0$, then $N(\varepsilon) = -1$ where ε is a fundamental unit of $\mathbb{Q}(\sqrt{m})$.*

Proof. Proof is by contradiction. So suppose that $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\varepsilon) = +1$. By Appendix B.0.16, there exists an integer $\alpha \in \mathfrak{O}$ such that $\varepsilon = \dfrac{\alpha}{\alpha'}$, so $\alpha = \varepsilon\alpha'$. For a prime ideal $\mathfrak{p}$, if $\mathfrak{p} \mid \alpha$ then $\mathfrak{p} \mid \alpha'$ and vice versa. So $(\alpha) = (\alpha')$ implies $(\alpha) = (\alpha)'$. But by Lemma 4.7.1, $(\sqrt{m})$ is the unique ambig prime ideal in $\mathbb{Q}(\sqrt{m})$, so $\alpha = \eta a$ or $\alpha = \eta\sqrt{m}a$ where η is a unit, $a \in \mathbb{Z} \setminus \{0\}$. Thus, $\varepsilon = \dfrac{\eta a}{(\eta a)'}$ or $\varepsilon = \dfrac{\eta\sqrt{m}a}{(\eta\sqrt{m}a)'}$; so $\varepsilon = \dfrac{\eta a}{(\eta)'a} = \dfrac{\eta}{(\eta)'} = \eta^2$ or $\varepsilon = \dfrac{\eta\sqrt{m}a}{\eta'(-\sqrt{m})a} = -\dfrac{\eta}{\eta'} = -\eta^2$. But $\varepsilon = \mp\eta^2$ contradicts to ε being a fundamental unit. Hence $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\varepsilon) = -1$. □

Lemma 4.7.3. *If the discriminant $\text{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))$ of $\mathbb{Q}(\sqrt{m})$ has only a single prime factor, then the class number h of $\mathbb{Q}(\sqrt{m})$ is odd.*

Proof. Proof is by contradiction. So assume that the class number h is even, then there exists an ideal $\mathfrak{a}$, not belonging to principal class, such that $\mathfrak{a}^2 \sim 1$. So $\mathfrak{a} \sim \mathfrak{a}'$. Let

$\alpha = \dfrac{\mathfrak{a}}{\mathfrak{a}'}$, then $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha) = \dfrac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a})}{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a}')} = \mp 1$. Now, if $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha) = +1$, then let $\beta = \alpha$. If $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha) = -1$, then $\mathbb{Q}(\sqrt{m})$ is a real field, so let $\beta = \varepsilon\alpha$ where ε is a fundamental unit. Therefore, $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\beta) = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha) = +1$ for the first case and $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\beta) = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\varepsilon\alpha) = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\varepsilon)N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha) = (-1)(-1) = +1$ for the second case by Lemma 4.7.2. Also $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\dfrac{1}{\beta}) = +1$, so by Appendix B.0.16 there exists $\gamma \in \mathfrak{O}$ such that $\dfrac{1}{\beta} = \dfrac{\gamma}{\gamma'}$. Thus,

$$\begin{aligned} \frac{\gamma\mathfrak{a}}{\gamma\mathfrak{a}'} &= \frac{\frac{\gamma'}{\beta}\mathfrak{a}}{\gamma'\mathfrak{a}'} \\ &= \frac{1}{\beta}(\alpha) \\ &= (\frac{\alpha}{\beta}) \\ &= (\varepsilon) = \mathfrak{O}, \end{aligned}$$

so $\gamma\mathfrak{a} = (\gamma\mathfrak{a})'$. Then $\gamma\mathfrak{a} = a$ or $\gamma\mathfrak{a} = a\mathfrak{l}$ where $a \in \mathbb{Z}$ and $\mathfrak{l}$ is the unique nonrational prime factor of $\mathbb{Q}(\sqrt{m})$ coinciding with its conjugate. So by Lemma 4.7.1, $\mathfrak{l} = \sqrt{m}$ if $m \neq -1$ and $\mathfrak{l} = 1 + \sqrt{-1}$ if $m = -1$. Thus $\mathfrak{l} \sim 1$. So $\gamma\mathfrak{a} = a$ or $\gamma\mathfrak{a} = a\mathfrak{l}$ implies that $\mathfrak{a} \sim 1$ which contradicts our assumption for $\mathfrak{a}$. Hence h is odd. □

Theorem 4.7.4. *If $disc_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))$ of $\mathbb{Q}(\sqrt{m})$ has only a single prime factor p, then there is only one genus in $\mathbb{Q}(\sqrt{m})$.*

Proof. For $m > 0$, let ε be a fundamental unit in $\mathbb{Q}(\sqrt{m})$. So by Lemma 4.7.2, $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\varepsilon) = -1$. Thus $\left(\dfrac{-1}{p:m}\right) = +1$. So the character set for an ideal $\mathfrak{a}$ is,

$$\Upsilon(\mathfrak{a}) = \left(\left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a})}{p:m}\right)\right) \text{ since } N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\varepsilon) = -1, \text{ for } m > 0;$$

$$\Upsilon(\mathfrak{a}) = \left(\left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a})}{p:m}\right)\right), \text{ for } m < 0.$$

If $\Upsilon(\mathfrak{a}) = -1$, then

$$\left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a}^2)}{p:m}\right) = \left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a})N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a})}{p:m}\right) = \left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a})}{p:m}\right)^2 = (-1)^2 = 1.$$

So $\Upsilon(\mathfrak{a}^2) = +1$ and the collection of all ideal classes of $\mathbb{Q}(\sqrt{m})$ fall into two genera. Then the class number h is even which contradicts to Lemma 4.7.3. Hence for each ideal $\mathfrak{a}$ in $\mathbb{Q}(\sqrt{m})$, $\Upsilon(\mathfrak{a}) = (+1)$. □

Theorem 4.7.5. *(Quadratic Reciprocity Law) Let $p, q \in \mathbb{Z}$ be distinct positive odd prime numbers. Then*

(i) $\left(\dfrac{-1}{p}\right) = (-1)^{\dfrac{p-1}{2}}$,

(ii) $\left(\dfrac{2}{p}\right) = (-1)^{\dfrac{p^2-1}{8}}$ *and*

(iii) $\left(\dfrac{p}{q}\right)\left(\dfrac{q}{p}\right) = (-1)^{\dfrac{(p-1)(q-1)}{4}}$.

Proof. By Theorem 4.2.7, if p is an odd positive prime number which does not divide $\mathrm{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))$, and if $\left(\dfrac{m}{p}\right) = +1$, then $p = \mathfrak{p}\mathfrak{p}'$ where $\mathfrak{p}$ and $\mathfrak{p}'$ are distinct conjugate prime ideals. Then $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(p) = p^2$ and $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(p) = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{p}\mathfrak{p}') = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{p})N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{p}') = [N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{p})]^2$. So $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{p}) = p$ since $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{p}) > 0$.

Let $\mathbb{Q}(\sqrt{m})$ be a quadratic number field where $\mathrm{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))$ has only one distinct prime factor, say l. Then, if $\left(\dfrac{m}{p}\right) = +1$, we have $\left(\dfrac{p}{l:m}\right) = \left(\dfrac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{p})}{l:m}\right) = +1$ by Theorem 4.7.4. We shall repeatedly use this relation.

1. To prove the first assertion (i), take $m = -1$, so $\mathrm{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{-1})) = -4$, $l = 2$. For odd prime $p > 0$, if $\left(\dfrac{-1}{p}\right) = +1$, then $\left(\dfrac{p}{2:-1}\right) = +1$. But by Theorem 4.3.6 we have,

$$\left(\frac{p}{2:-1}\right) = (-1)^{\dfrac{(p-1)(-1-1)}{4}} = (-1)^{\dfrac{-(p-1)}{2}} = (-1)^{\dfrac{(p-1)}{2}}. \qquad (4.11)$$

Thus, if $\left(\frac{-1}{p}\right) = +1$ then $(-1)^{\frac{(p-1)}{2}} = +1$.

Conversely, we will prove if $(-1)^{\frac{p-1}{2}} = +1$, then $p \equiv 1 \mod 4$. Consider the field $\mathbb{Q}(\sqrt{p})$. Then, $\left(\frac{-1}{p}\right) = \left(\frac{-1}{p:p}\right)$ by Theorem 4.3.6. Here $\text{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{p})) = p$, so by Lemma 4.7.2 we have $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\varepsilon) = -1$ for the fundamental unit ε. So we have $\left(\frac{-1}{p}\right) = \left(\frac{-1}{p:p}\right) = \left(\frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\varepsilon)}{p:p}\right) = +1$.

Thus, $(-1)^{\frac{(p-1)}{2}} = +1$ holds if and only if $\left(\frac{-1}{p}\right) = +1$.

Hence, we get $\left(\frac{-1}{p}\right) = (-1)^{\frac{(p-1)}{2}}$. This proves (i).

2. Take $m = 2$ to prove the assertion (ii), so $\text{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})) = 8$, $l = 2$. For odd prime $r > 0$, if $\left(\frac{2}{r}\right) = +1$, then $\left(\frac{r}{2:2}\right) = +1$. But by Theorem 4.3.6, we have

$$\left(\frac{r}{2:2}\right) = (-1)^{\frac{(r^2-1)}{8}}.$$

Thus if $\left(\frac{2}{r}\right) = +1$, then $(-1)^{\frac{(r^2-1)}{8}} = +1$.

For the converse, let $p, q \in \mathbb{Z}$ be prime numbers such that $p \equiv 1 \mod 4$, $q \equiv 3 \mod 4$, consider the fields $\mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{-q})$. Then, $(-1)^{\frac{(p^2-1)}{8}} = +1$ implies that $\left(\frac{2}{p}\right) = \left(\frac{2}{p:p}\right) = +1$. Note that we have $2 = N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}} 1 + \sqrt{-1}$. So similarly, $(-1)^{\frac{(q^2-1)}{8}} = +1$ implies $\left(\frac{2}{q:-q}\right) = +1$, then $\left(\frac{2}{q}\right) = \left(\frac{2}{q:q}\right) \cdot (+1) = \left(\frac{2}{q:q}\right)\left(\frac{2}{q:-1}\right) = \left(\frac{2}{q:-q}\right) = +1$. Thus, $(-1)^{\frac{(p^2-1)}{8}} = +1$ implies $\left(\frac{2}{p}\right) = +1$ and $(-1)^{\frac{(q^2-1)}{8}} = +1$ implies $\left(\frac{2}{q}\right) = +1$. So we get $\left(\frac{2}{r}\right) = (-1)^{\frac{(r^2-1)}{8}}$.

This proves (ii).

Now the following steps are for the last assertion (iii).

3. Take $m = p \equiv 1 \mod 4$, so $\mathrm{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{p})) = p$, $l = p$. Let $p_1 > 0$ be a prime number $p_1 \neq p$ with $p_1 \equiv 1 \mod 4$. If $\left(\frac{p}{p_1}\right) = +1$, then $\left(\frac{p_1}{p:p}\right) = +1$. But by Theorem 4.3.6, we have

$$\left(\frac{p_1}{p:p}\right) = \left(\frac{p_1}{p}\right).$$

Thus, if $\left(\frac{p}{p_1}\right) = +1$, then $\left(\frac{p_1}{p}\right) = +1$. And by the symmetry of the argument, we get $\left(\frac{p}{p_1}\right) = \left(\frac{p_1}{p}\right)$.

4. Take $m = p \equiv 1 \mod 4$, so $\mathrm{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{p})) = p$, $l = p$. Let $q > 0$ be a prime number with $q \equiv 3 \mod 4$. If $\left(\frac{p}{q}\right) = +1$, then $\left(\frac{q}{p:p}\right) = +1$. But by Theorem 4.3.6, we have

$$\left(\frac{q}{p:p}\right) = \left(\frac{q}{p}\right).$$

Thus, if $\left(\frac{p}{q}\right) = +1$, then $\left(\frac{q}{p}\right) = +1$.

5. Take $m = -q \equiv 1 \mod 4$, so $\mathrm{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{-q})) = -q$, $l = q$. Let $p > 0$ be a prime number with $p = 1 \mod 4$. If $\left(\frac{-q}{p}\right) = +1$, then $\left(\frac{p}{q:-q}\right) = +1$. But by Theorem 4.3.6, we have

$$\left(\frac{p}{q:-q}\right) = \left(\frac{p}{q:q}\right)\left(\frac{p}{q:-1}\right) = \left(\frac{p}{q}\right)(+1) = \left(\frac{p}{q}\right).$$

Thus, if $\left(\frac{q}{p}\right) = +1$, then $\left(\frac{-q}{p}\right) = +1$ since $\left(\frac{-1}{p}\right) = (-1)^{\frac{(p-1)}{2}} = +1$ by part 1.

Thus, if $\left(\frac{q}{p}\right) = +1$, then $\left(\frac{p}{q}\right) = +1$. Hence by part 4 and 5 we get $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.

6. Take $m = -q \equiv 1 \mod 4$, so $\mathrm{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{-q})) = -q$, $l = q$. Let $q_1 > 0$ be a prime number $q_1 \neq q$ with $q_1 \equiv 3 \mod 4$. If $\left(\frac{-q}{q_1}\right) = +1$, then $\left(\frac{q_1}{q : -q}\right) = +1$. By Equation 5.3 and Equation 5.3 in Theorem 4.3.6, we have

$$\left(\frac{q_1}{q : -q}\right) = \left(\frac{q_1}{q : q}\right)\left(\frac{q_1}{q : -1}\right) = \left(\frac{q_1}{q}\right)(+1) = \left(\frac{q_1}{q}\right).$$

If $\left(\frac{q}{q_1}\right) = -1$, then $\left(\frac{-q}{q_1}\right) = +1$ since $\left(\frac{-1}{q_1}\right) = (-1)^{\frac{(q_1-1)}{2}} = -1$. Thus, if $\left(\frac{q}{q_1}\right) = -1$, then $\left(\frac{q_1}{q}\right) = +1$. And by the symmetry of the argument, we get $\left(\frac{q}{q_1}\right) = -\left(\frac{q_1}{q}\right)$.

This proves (iii). □

Using Quadratic Reciprocity Law, we now want to prove that a certain product is equal to 1.

Theorem 4.7.6. *Let $n, m \in \mathbb{Z}$, not both negative. Then*

$$\prod_{(w)} \left(\frac{n}{w : m}\right) = +1$$

where w ranges over all prime numbers in $\mathbb{N}$.

Proof. Let $p, q \in \mathbb{Z}$ be distinct odd prime numbers. Then we have,

(i) $\left(\frac{-1}{2 : 2}\right) = (-1)^{\frac{(-1)^2-1}{8}} = +1$ by Equation 4.6 in Theorem 4.3.6.

(ii) $\left(\frac{-1}{2 : p}\right)\left(\frac{-1}{p : p}\right) = (-1)^{\frac{(-1-1)(p-1)}{4}}\left(\frac{-1}{p}\right) = (-1)^{\frac{-(p-1)}{2} + \frac{p-1}{2}} = +1$ by Equation 5.3 in Theorem 4.3.6,

(iii) $\left(\frac{2}{2:2}\right) = \left(\frac{2.1}{2:2.1}\right) = \left(\frac{-1}{2:2}\right) = (-1)^{\frac{1-1}{2}} = +1$ by Case 3.b (ii) in the proof of Theorem 4.3.6,

(iv) $\left(\frac{2}{2:p}\right)\left(\frac{2}{p:p}\right) = (-1)^{\frac{p^2-1}{8}}\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}(-1)^{\frac{p^2-1}{8}} = +1$ by Equation 4.6 and Equation 5.3 in Theorem 4.3.6,

(v) $\left(\frac{p}{2:p}\right)\left(\frac{p}{p:p}\right) = (-1)^{\frac{(p-1)(p-1)}{4}}\left(\frac{\frac{-pp}{p^2}}{p}\right) = (-1)^{\frac{(p-1)^2}{4}}\left(\frac{-1}{p}\right)$
$= (-1)^{\frac{(p-1)^2+2(p-1)}{4}} = (-1)^{\frac{(p-1)(p+1)}{4}} = +1$ since $-p = N_{\mathbb{Q}(\sqrt{p})/\mathbb{Q}}(\sqrt{p})$,

(vi) $\left(\frac{p}{2:q}\right)\left(\frac{p}{p:q}\right)\left(\frac{p}{q:q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)$
$= (-1)^{\frac{(p-1)(q-1)}{2}} = +1$

by Quadratic Reciprocity Law 4.7.5.

We know by Theorem 4.3.6 that $\left(\frac{n}{w:m}\right) = +1$ for all odd prime w such that $w \nmid n$ and $w \nmid m$. So if n and m are ∓ 1 or p for some prime $p \in \mathbb{Z}$, then $\prod_{(w)}\left(\frac{n}{w:m}\right) = +1$ by all the results above for $w = m$ or $w = n$. But by Theorem 4.3.6, we also have

$$\left(\frac{nn'}{w:m}\right) = \left(\frac{n}{w:m}\right)\left(\frac{n'}{w:m}\right) \text{ and } \left(\frac{n}{w:mm'}\right) = \left(\frac{n}{w:m}\right)\left(\frac{n}{w:m'}\right),$$

so theorem is also true for composite n and m which are not both negative. □

Note that $\left(\frac{-1}{2:-1}\right) = (-1)^{-2.-2/4} = -1$. So if n, m are both negative, then $\prod_{(w)}\left(\frac{n}{w:m}\right) = -1$ since $\left(\frac{-1}{w:-1}\right) = +1$ for each odd prime w by Equation 5.3 in Theorem 4.3.6. So we define a new symbol $\left(\frac{n}{-1:m}\right)$ where it is equal to $+1$ if one of n, m is 0, and equals to -1 if both n, m are negative to preserve the Product Formula

(Here -1 stands for the infinite prime in the p-adic approach).

Note that the product of c units in $\Upsilon(\mathfrak{a})$ is $+1$ for any $\mathfrak{a}$ in $\mathbb{Q}(\sqrt{m})$. We will prove that if the product of an arbitrary c units is $+1$, then this c-tuple is in $Im(\Upsilon)$.

4.8. The Number of Genera

Theorem 4.8.1. *Let $m, n \in \mathbb{Z}$ such that m is not a square. If $\left(\frac{n}{w:m}\right) = +1$ for all primes w, then $n = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha)$ for some $\alpha \in \mathbb{Q}(\sqrt{m})$.*

Proof. Let $m, n \in \mathbb{Z}$ such that m is not a square. First we will show that $|n| = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{i})$ for some ideal $\mathfrak{i}$ by considering the prime divisors of n.

The product $\prod_{(w)} \left(\frac{n}{w:m}\right) = +1$ implies that $n > 0$ or $m > 0$. Assume n, m are not divisible by a square.

If p is a prime integer such that $p \mid n$ and $p \mid \mathrm{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))$, then $p = \mathfrak{p}_1{}^2$ by Theorem 4.2.7, so $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{p}_1) = p$.

If p is an odd prime integer such that $p \mid n$ and $p \nmid m$, then

$$\left(\frac{n}{p:m}\right) = \left(\frac{m}{p}\right) = +1$$

by Case 2.b in the proof of Theorem 4.3.6. Then $p = \mathfrak{p}_1\mathfrak{p}_1{}'$ for some ideals $\mathfrak{p}_1$, $\mathfrak{p}_1{}'$ in $\mathbb{Q}(\sqrt{m})$, so $p = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{p}_1)$.

If $p = 2$ such that $2 \mid n$ and $2 \nmid \mathrm{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))$, then

$$\left(\frac{n}{2:m}\right) = \left(\frac{2^a n'}{2:m}\right),$$

where $2 \nmid n'$, so $\left(\frac{n'}{2:m}\right) = +1$. Then,

$$\left(\frac{n}{2:m}\right) = \left(\frac{2}{2:m}\right) = (-1)^{\frac{m^2-1}{8}} = +1$$

by assumption. So $\left(\frac{m}{2}\right) = +1$ implies $2 = \mathfrak{p}_1\mathfrak{p}_1'$, so $2 = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{p}_1)$ by Theorem 4.2.7.

Therefore there is an ideal $\mathfrak{i} \subseteq \mathbb{Q}(\sqrt{m})$ such that $|n| = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{i})$. The proof will be based on induction on m with $|m| > 4$.

Let $\mathtt{A}_\mathfrak{i}$ denote the ideal class of $\mathfrak{i}$ where $|n| = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{i})$, choose $\mathfrak{j} \in \mathtt{A}_\mathfrak{i}$ such that $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{j}) \leqslant |\sqrt{\mathrm{disc}_\mathbb{Q}(\mathbb{Q}(\sqrt{m}))}|$ by Minkowski's Theorem (See Appendix B.0.18). Since $\mathfrak{i} \sim \mathfrak{j}$, there exists a number $\kappa \in \mathbb{Q}(\sqrt{m})$ such that $\mathfrak{j} = \kappa\mathfrak{i}$, so we have that $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{j}) = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{i})N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\kappa)$. Let $n' = \varepsilon N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{j})$ where $\varepsilon \in \{+1, -1\}$ is such that $n' = nN_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\kappa)$. Then,

$$|n'| = |\mp N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{j})| \leq |\sqrt{\mathrm{disc}_\mathbb{Q}(\mathbb{Q}(\sqrt{m}))}| \leq |\sqrt{4m}| = 2|\sqrt{m}| \leq |m|$$

for $|m| > 4$.

Now, $n' = nN_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\kappa)$, so $\left(\frac{n'}{w:m}\right) = \left(\frac{n}{w:m}\right) = +1$ by assumption. We have $\left(\frac{m}{w:n'}\right) = \left(\frac{n'}{w:m}\right)$ by Theorem 4.3.6, so $\left(\frac{m}{w:n'}\right) = +1$ for all primes w.

For induction, assume that for each field $\mathbb{Q}(\sqrt{m'})$ such that $|m'| < |m|$, if $\left(\frac{n}{w:m'}\right) = +1$ for all prime w, then $n = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha)$ for some $\alpha \in \mathbb{Q}(\sqrt{m})$. Note that n' is not a square, $|n'| < |m|$ and $\left(\frac{m}{w:n'}\right) = +1$ for all prime w. Then, $m = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha')$ for some $\alpha' \in \mathbb{Q}(\sqrt{n'})$. Then $m = a^2 - n'b^2$ for some $a, b \in \mathbb{Q}$, $b \neq 0$. So $n'b^2 = a^2 - m$, $n' = (\frac{a}{b})^2 - (\frac{1}{b})^2 m$ where $\frac{a}{b}, \frac{1}{b} \in \mathbb{Q}$, so $n' = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\lambda)$ for some $\lambda \in \mathbb{Q}(\sqrt{m})$. But $n' = nN_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\kappa)$, so $n = \dfrac{n'}{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\kappa)} = \dfrac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\lambda)}{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\kappa)} =$

$N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\frac{\lambda}{\kappa}) = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha)$ for $\alpha = \frac{\lambda}{\kappa} \in \mathbb{Q}(\sqrt{m})$.

If $|m| \leq 4$, it is also enough to check for n with $|n| \leq |\sqrt{\text{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))}|$ because of the same result as above, then the result follows by the following case analysis.

Note that there is no need to check for $n = 1$ since $1 = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(1)$ for $1 \in \mathbb{Q}(\sqrt{m})$ for all $m \in \mathbb{Z} \setminus \{0\}$.

(i) If $m = -3$, $\text{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{-3})) = -3$, then $0 < n \leq \sqrt{3}$, so $n = 1$ is the only value that satisfies the assumption of the theorem.

(ii) If $m = -2$, $\text{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{-2})) = -8$, then $0 < n \leq 2\sqrt{2}$, so we check $\left(\frac{n}{w : m}\right)$ values for $0 < n \leq 2\sqrt{2}$,

$$\left(\frac{2}{w : -2}\right) = +1,$$

so $n = 1, 2$ are the only values that satisfy the assumption of the theorem. For $n = 2$, $\alpha = \sqrt{-2}$ since $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\sqrt{-2}) = (\sqrt{-2})(-\sqrt{-2}) = -(-2) = 2$.

(iii) If $m = -1$, $\text{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{-1})) = -4$, then $0 < n \leq 2$, so we check $\left(\frac{n}{w : m}\right)$ values for $0 < n \leq 2$,

$$\left(\frac{1}{2 : -1}\right) = (-1)^{\frac{(1-1)(-1-1)}{2}} = +1 \text{ and } \left(\frac{1}{w : -1}\right) = +1,$$

$$\left(\frac{2}{2 : -1}\right) = \left(\frac{-1}{2}\right) = (-1)^{\frac{(1-1)}{8}} = +1 \text{ and } \left(\frac{2}{w : -1}\right) = +1,$$

so $n = 1, 2$ are the only values that satisfy the assumption of the theorem. For $n = 1$, $\alpha = \sqrt{-1}$ since $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\sqrt{-1}) = (\sqrt{-1})(-\sqrt{-1}) = -(-1) = 1$. For $n = 2$, $\alpha = 1 + \sqrt{-1}$ since $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(1 + \sqrt{-1}) = (1 + \sqrt{-1})(1 - \sqrt{-1}) = 1 - (-1) = 2$.

(iv) If $m = 2$, $\text{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{4})) = 8$, then $-2\sqrt{2} \leq n \leq 2\sqrt{2}$, so we check $\left(\frac{n}{w : m}\right)$ values

for $2 \leq n \leq 2$,

$$\left(\frac{-2}{w:2}\right) = +1, \left(\frac{-1}{2:2}\right) = (-1)^{\frac{(1-1)}{8}} = +1 \text{ and}$$

$$\left(\frac{-1}{w:2}\right) = +1, \left(\frac{2}{2:2}\right) = +1 \text{ by Equation (iii) in Theorem 4.7.6 and ,}$$

$$\left(\frac{2}{w:2}\right) = +1,$$

so $n = -2, -1, 1, 2$ are the values that satisfy the assumption of the theorem. For $n = -2$, $\alpha = \sqrt{2}$ since $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\sqrt{2}) = (\sqrt{2})(-\sqrt{2}) = -2$. For $n = -1$, $\alpha = 1 + \sqrt{2}$ since $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(1 + \sqrt{2}) = (1 + \sqrt{2})(1 - \sqrt{2}) = 1 - 2 = -1$. For $n = 2$, $\alpha = 2 + \sqrt{2}$ since $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(2 + \sqrt{2}) = (2 + \sqrt{2})(2 - \sqrt{2}) = 4 - 2 = 2$.

(v) If $m = 3$, $\text{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{3})) = 12$, then $-2\sqrt{3} \leq n \leq 2\sqrt{3}$, so we check $\left(\frac{n}{w:m}\right)$ values for $-3 \leq n \leq 3$:

$$\left(\frac{-3}{w:3}\right) = +1,$$

$$\left(\frac{-2}{2:3}\right) = \left(\frac{-1}{2:3}\right)\left(\frac{2}{2:3}\right) = (-1)^{\frac{(-2).2}{4}}(-1)^{\frac{9-1}{8}} = (-1)(-1) = +1,$$

$$\left(\frac{-2}{3:3}\right) = \left(\frac{-2}{3}\right) = \left(\frac{-1}{3}\right)\left(\frac{2}{3}\right) = (-1)^{\frac{(3-1)}{2}}(-1)^{\frac{(9-1)}{8}} = +1 \text{ and ,}$$

$$\left(\frac{-2}{w:3}\right) = +1 \text{ for all } w \neq 2, 3.$$

$$\left(\frac{-1}{3:3}\right) = \left(\frac{-1}{3}\right) = (-1)^{\frac{(3-1)}{2}} = -1.$$

$$\left(\frac{2}{3:3}\right) = \left(\frac{2}{3}\right) = (-1)^{\frac{9-1}{8}} = -1.$$

$$\left(\frac{3}{3:3}\right) = \left(\frac{-1}{3:3}\right)\left(\frac{-3}{3:3}\right) = \left(\frac{-1}{3:3}\right)(+1) = (-1)(+1) = -1.$$

So $n = -3, -2, 1$ are the values that satisfy the assumption of the theorem. For $n = -3$, $\alpha = \sqrt{3}$ since $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\sqrt{3}) = (\sqrt{3})(-\sqrt{3}) = -3$. For $n = -2$, $\alpha = 1 + \sqrt{3}$ since $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(1 + \sqrt{3}) = (1 + \sqrt{3})(1 - \sqrt{3}) = 1 - 3 = -2$. □

By Lemma 4.4.4, $\Upsilon(\mathfrak{a}^2) = \Upsilon(\mathfrak{a})\Upsilon(\mathfrak{a}) = [\Upsilon(\mathfrak{a})]^2 = (+1, +1, \ldots, +1)$, so for each ideal $\mathfrak{a} \subseteq \mathbb{Q}(\sqrt{m})$, the ideal class $[\mathfrak{a}^2]$ is in the principal genus. Now we will check the converse.

Theorem 4.8.2. *For each ideal class $\mathtt{A}$ in $\mathfrak{G}_0$, there exists an ideal class $\mathtt{B}$ such that $\mathtt{A} = \mathtt{B}^2$.*

Proof. Let $\mathtt{A}$ be an ideal class in $\mathfrak{G}_0$ of the field $\mathbb{Q}(\sqrt{m})$ and $\mathfrak{a}$ be an ideal in the class $\mathtt{A}$ such that $(\mathfrak{a}, \mathrm{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))) = 1$, and $\overline{n} = \varepsilon_{\mathfrak{a}} N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a})$. Then $\left(\frac{\overline{n}}{w:m}\right) = +1$ for all prime w since $\overline{n} \nmid \mathrm{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))$. So by Theorem 4.8.1, $\overline{n} = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha)$ for some $\alpha \in \mathbb{Q}(\sqrt{m})$. Consider $\frac{\mathfrak{a}}{\alpha} = \frac{\mathfrak{b}}{\mathfrak{c}}$ such that $(\mathfrak{b}, \mathfrak{c}) = 1$. Then $\frac{\mathfrak{b}\mathfrak{b}'}{\mathfrak{c}\mathfrak{c}'} = \frac{\mathfrak{b}}{\mathfrak{c}}(\frac{\mathfrak{b}}{\mathfrak{c}})' = (\frac{\mathfrak{a}}{\alpha})(\frac{\mathfrak{a}}{\alpha})' = \frac{\mathfrak{a}\mathfrak{a}'}{\alpha\alpha'} = \frac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a})}{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha)} = 1$, so $\mathfrak{c} = \mathfrak{b}'$.

Then, $\mathfrak{a} \sim \frac{\mathfrak{a}}{\alpha} = \frac{\mathfrak{b}}{\mathfrak{b}'} = \frac{\mathfrak{b}\mathfrak{b}}{\mathfrak{b}'\mathfrak{b}} \sim \mathfrak{b}^2$ since $\mathfrak{b}\mathfrak{b}' \sim \mathfrak{O}$. Hence $\mathfrak{a} \sim \mathfrak{b}^2$, that is $\mathtt{A} = \mathtt{B}^2$. □

Notation 4.8.3. If $\mathfrak{a} \in \mathtt{A}$, then we will denote the ideal class $[\mathfrak{a}']$ by $\mathtt{A}'$.

Definition 4.8.4. An ideal class $\mathtt{A}$ is called an *ambig ideal class*, if $\mathtt{A} = \mathtt{A}'$, that is for all $\mathfrak{a} \in \mathtt{A}$ there exists $\mathfrak{b} \in \mathtt{A}'$ such that $\mathfrak{a} = \mathfrak{b}$ and vice versa.

Note that, $\mathfrak{a}\mathfrak{a}' \sim \mathfrak{O}$ implies $\mathtt{A}\mathtt{A}' = \mathtt{I}$, so if $\mathtt{A}$ is ambig, then $\mathtt{A}^2 = \mathtt{A}\mathtt{A}' = \mathtt{I}$. Conversely, if $\mathtt{A}^2 = \mathtt{I}$, then $\mathtt{A}\mathtt{A} = \mathtt{I}$ implies $\mathtt{A} = \mathtt{A}^{-1}$, but also $\mathtt{A}' = \mathtt{A}^{-1}$, hence $\mathtt{A} = \mathtt{A}' = \mathtt{A}^{-1}$ and $\mathtt{A}$ is an ambig ideal class.

If $\mathfrak{a}$ is an ambig ideal, then $\mathtt{A} = [\mathfrak{a}]$ is clearly an ambig ideal class, so we have 2^s ambig ideals obtained by this way. Now we will check that how many of them are distinct.

Recall that a set of ideal classes, $\mathtt{c}$ is called independent if $\mathtt{I} \notin \mathtt{c}$ and $\mathtt{I} = \mathtt{A}_1^{a_1}\mathtt{A}_2^{a_2}\ldots\mathtt{A}_n^{a_n}$ for $\mathtt{A}_1, \mathtt{A}_2, \ldots, \mathtt{A}_n \in \mathtt{c}$ implies $\mathtt{A}_1^{a_1} = \mathtt{A}_2^{a_2} = \ldots = \mathtt{A}_n^{a_n} = \mathtt{I}$. See [5] for group theoretical approach.

Theorem 4.8.5. *Let s be the number of distinct ambig prime ideals in $\mathbb{Q}(\sqrt{m})$.*
If $m < 0$, then $s-1$ of them determine independent ambig classes and there are 2^{s-1} distinct ambig ideals.
If $m > 0$ and $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\varepsilon) = +1$, then $s-2$ of them determine independent ambig classes and there are 2^{s-2} distinct ambig ideals.
If $m > 0$ and $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\varepsilon) = -1$, then $s-1$ of them determine independent ambig classes and there are 2^{s-1} distinct ambig ideals.

Proof. Since two ideals belong to the same class if they differ by a principle ideal, we will check the ambig principle ideals in $\mathbb{Q}(\sqrt{m})$.

Case 1. If $m < 0$, but $m \neq -1, -3$, then let $\alpha\mathfrak{O}$ be an ambig principal ideal, so $\alpha\mathfrak{O} = (\alpha\mathfrak{O})'$ then $\dfrac{\alpha}{\alpha'}$ is a unit, so $\dfrac{\alpha}{\alpha'} = (-1)^e$ where $e = 0$ or 1 by [3]. Then

$$\frac{\alpha(\sqrt{m})^e}{(\alpha(\sqrt{m})^e)'} = \begin{cases} \dfrac{\alpha}{\alpha'} = 1, & \text{if } e = 0 \\ \dfrac{\alpha\sqrt{m}}{\alpha'(-\sqrt{m})} = -\dfrac{\alpha}{\alpha'} = 1, & \text{if } e = 1. \end{cases}$$

So $\alpha(\sqrt{m})^e = (\alpha(\sqrt{m})^e)'$, thus $(\alpha\sqrt{m})^e \in \mathbb{Z}$. So if $e = 0$, then $\alpha \in \mathbb{Z}$, $\alpha = \mp 1$ since $\alpha\mathfrak{O}$ is ambig. And if $e = 1$, then $\alpha(\sqrt{m}) \in \mathbb{Z}$, $\alpha = \mp\sqrt{m}$ since $\alpha\mathfrak{O}$ is ambig. Thus, the only ambig principal ideals are $\mathfrak{O}$ and $\mathfrak{O}\sqrt{m}$.

Case 2. If $m = -1$, then by Lemma 4.7.1, $\mathfrak{l} = 1 + \sqrt{-1}$ is the only ambig ideal in $\sqrt{-1}$.

If $m = -3$, then by Lemma 4.7.1, $\mathfrak{l} = \sqrt{-3}$ is the only ambig ideal in $\sqrt{-3}$ since 3 is the only prime divisor of $\mathrm{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{-3})) = -3$, because $-3 \equiv 1 \mod 4$.

Case 3. If $m > 0$ and $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\varepsilon) = +1$, then $\varepsilon = \dfrac{\beta}{\beta'}$ for some $\beta \in \mathfrak{O}$ by Lemma B.0.16. Choose α such that $\beta = a\alpha$ for $a \in \mathbb{Z}$ and α is not divisible by any integer, so $\alpha = \varepsilon\alpha'$ implies $\alpha\mathfrak{O} = (\alpha\mathfrak{O})$, thus $\alpha\mathfrak{O}$ is an ambig principal ideal.

We claim that $\alpha\mathfrak{O} \neq \mathfrak{O}$ and $\alpha\mathfrak{O} \neq \sqrt{m}\mathfrak{O}$. Otherwise $\alpha = \mp\varepsilon^f$ or $\alpha = \mp\varepsilon^f\sqrt{m}$ for some $f \in \mathbb{Z}$. Then $\dfrac{\alpha}{\alpha'} = (-1)^e\dfrac{\varepsilon^f}{(\varepsilon')^f}$, where $\varepsilon\varepsilon' = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\varepsilon) = 1$, so $(\varepsilon')^{-1} = \varepsilon$, so $\dfrac{\alpha}{\alpha'} = (-1)^e\varepsilon^{2f}$ where $e = 0$ or 1 respectively. But then $(-1)^e\varepsilon^{2f} = \varepsilon$ which contradicts to the fact that ε is a fundamental unit.

Let $\beta\mathfrak{O}$ be an ambig principal ideal in $\mathbb{Q}(\sqrt{m})$, then $\dfrac{\beta}{\beta'}$ is a unit, so $\dfrac{\beta}{\beta'} = (-1)^e\varepsilon^f$ for some $e, f \in \mathbb{Z}$. Then for $\gamma = \dfrac{\beta}{(\sqrt{m})^e\alpha^f}$, we have $\dfrac{\gamma}{\gamma'} = \dfrac{\beta}{(\sqrt{m})^e\alpha^f}\dfrac{(-\sqrt{m})^e\alpha'^f}{\beta'} = \dfrac{\beta}{\beta'}(-1)^e(\dfrac{\alpha'}{\alpha})^f = (-1)^e\varepsilon^f(-1)^e(\dfrac{1}{\varepsilon})^f = +1$, so $\gamma = \gamma'$ and $\gamma \in \mathbb{Q}$. Hence we get an ambig principal ideal by removing the factors of $\mathbb{Z}$ from $\sqrt{m}\alpha$, say $\mathfrak{a}$. The ambig principal ideals are $\mathfrak{O}, \mathfrak{O}\sqrt{m}, \mathfrak{O}\alpha$ and $\mathfrak{a}$.

Case 4. If $m > 0$ and $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\varepsilon) = -1$, then let $\mathfrak{O}\alpha$ be an ambig principal ideal, then $\dfrac{\alpha}{\alpha'} = (-1)^e\varepsilon^f$ for some $e, f \in \mathbb{Z}$. $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\dfrac{\alpha}{\alpha'}) = \dfrac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha)}{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha')} = \dfrac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha)}{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha)} = 1$, so $[N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\varepsilon)]^f = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}((-1)^e\dfrac{\alpha}{\alpha'}) = +1$, so $f = 2g$ for some $g \in \mathbb{Z}$ since $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\varepsilon) = -1$.

Consider $\beta = \dfrac{\alpha}{\varepsilon^g(\sqrt{m})^{e+g}}$, then $\dfrac{\beta}{\beta'} = \dfrac{\alpha}{\varepsilon^g(\sqrt{m})^{e+g}}\dfrac{(-\varepsilon)^{-g}(-\sqrt{m})^{e+g}}{\alpha'}$ since $\varepsilon\varepsilon' = -1$. Then $\dfrac{\beta}{\beta'} = (-1)^e\varepsilon^f\dfrac{(-1)^{-g}}{\varepsilon^{2g}}(-1)^{e+g} = +1$, so $\beta = \beta'$, $\beta \in \mathbb{Q}$. Hence $\mathfrak{O}$ and $\mathfrak{O}\sqrt{m}$ are the only ambig principal ideals in $\mathbb{Q}(\sqrt{m})$.

The product of all the prime ideals dividing m is equal to $\sqrt{m}$, because $m = p_1 p_2 \dots p_s$ where $p_i \in \mathbb{Z}$ are prime and since $p_i \mid \mathrm{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))$ for all $i = 1, 2, \dots, s$, we have $p_i = \mathfrak{p}_i{}^2$ for all $i = 1, 2, \dots, s$. Hence $\sqrt{m} = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_s$. Also a principal ambig ideal in $\mathbb{Q}(\sqrt{m})$ is a product of the prime ideals dividing m. So for Case 1, Case 2 and Case 4 there are $s-1$ independent ambig classes and for Case 3 there are $s-2$ independent ambig classes. □

Theorem 4.8.6. *There exists an ambig ideal class $\mathtt{A}$ in $\mathbb{Q}(\sqrt{m})$ that contains no ambig ideal if and only if $m > 0$ and $\Upsilon(-1) = (+1, +1, \dots, +1)$ and $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\varepsilon) = +1$. Furthermore, all ambig ideal classes of this type in $\mathbb{Q}(\sqrt{m})$, say $\mathtt{B}$, is of the form $\mathtt{B} = \mathtt{A}\mathtt{A}_1 \dots \mathtt{A}_n$ where $\mathtt{A}_i$'s are ambig classes such that $\mathtt{A}_i = [\mathfrak{a}_i]$ for some ambig ideal $\mathfrak{a}_i$.*

Proof. First assume that $m > 0$ and $\left(\dfrac{-1}{w:m}\right) = +1$ for all primes $w \in \mathbb{Z}$ with $w \mid m$. By Theorem 4.3.6, we have $\left(\dfrac{-1}{w:m}\right) = +1$ for all primes $w \in \mathbb{Z}$ with $w \nmid m$. So by Theorem 4.8.1, $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha) = -1$ for some $\alpha \in \mathbb{Q}(\sqrt{m})$. Since $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\varepsilon) = +1$, α cannot be a unit, so $\mathfrak{O}\alpha = \dfrac{\mathfrak{i}}{\mathfrak{j}}$ for some ideals $\mathfrak{i}, \mathfrak{j}$ with $(\mathfrak{i}, \mathfrak{j}) = 1$. So $\dfrac{\mathfrak{i}\mathfrak{i}'}{\mathfrak{j}\mathfrak{j}'} = \alpha\alpha' = 1$, $\mathfrak{j} = \mathfrak{i}'$, $\alpha = \dfrac{\mathfrak{i}}{\mathfrak{j}} = \dfrac{\mathfrak{i}}{\mathfrak{j}'}$ implying $\mathfrak{i} = \alpha\mathfrak{i}'$, then $\mathfrak{i} \sim \mathfrak{i}'$, so $\mathtt{A} = [\mathfrak{i}]$ is an ambig ideal class.

Claim: $\mathtt{A}$ does not contain an ambig ideal.

Proof of the claim: Assume $\mathfrak{a} = \mathfrak{i}\beta$ is an ambig ideal for some $\beta \in \mathbb{Q}(\sqrt{m})$, then $\dfrac{\mathfrak{a}}{\mathfrak{a}'} = \dfrac{\mathfrak{i}\beta}{\mathfrak{i}'\beta'} = \alpha\dfrac{\beta}{\beta'}$ is a unit since $\mathfrak{a} = \mathfrak{a}'$, say $\alpha\dfrac{\beta}{\beta'} = (-1)^e\varepsilon^f$ for some $e, f \in \mathbb{Z}$. Then $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha)\dfrac{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\beta)}{N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\beta')} = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(-1)^e N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\varepsilon)^f = (+1)(+1)^f = +1$, so $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha) = +1$ contradicting to $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha) = -1$.

Conversely let $\mathtt{A}$ be an ambig class containing no ambig ideal and $\mathfrak{i} \in \mathtt{A}$ such that $\mathfrak{i} \sim \mathfrak{i}'$, that is $\mathfrak{i} = \alpha\mathfrak{i}'$ for some $\alpha \in \mathbb{Q}(\sqrt{m})$ with $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha) = \mp 1$.

If $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha) = +1$, then $\dfrac{1}{\alpha} = \dfrac{\beta}{\beta'}$ for some $\beta \in \mathfrak{O}$, so $\dfrac{\mathfrak{i}\beta}{(\mathfrak{i}\beta)'} = \alpha\dfrac{1}{\alpha} = +1$. Therefore, $\mathfrak{i}\beta = \mathfrak{i}'\beta$ and $\mathfrak{i}\beta \in \mathtt{A}$ where $\mathfrak{i}\beta$ is an ambig ideal. But this contradicts to the fact that $\mathtt{A}$ does not contain an ambig ideal. If $m < 0$, then $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha) = +1$,

but this is not possible as we have mentioned. So we must have $m > 0$. If $m > 0$ and $\left(\frac{-1}{w:m}\right) = -1$ for some prime w, then -1 cannot be a norm of any integer in $\mathbb{Q}(\sqrt{m})$, so $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha) = +1$. Again we get a contradiction above, so we must have $\Upsilon(-1) = (+1, +1, \ldots, +1)$.

If $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha) = -1$ and $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\varepsilon) = -1$, then $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\varepsilon\alpha) = +1$, so similarly $\mathtt{A}$ contains an ambig ideal and we get a contradiction.

Therefore, we must have $m > 0$, $\left(\frac{-1}{w:m}\right) = +1$ for all prime $w \in \mathbb{Z}$ and $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\varepsilon) = +1$.

Now for the last part of theorem, choose $\mathfrak{i} \in \mathtt{A}$, $\mathfrak{j} \in \mathtt{B}$ where $\mathtt{A}, \mathtt{B}$ are ambig classes that do not contain ambig ideals. Then for $\frac{\mathfrak{i}}{\mathfrak{i}'} = \alpha$ and $\frac{\mathfrak{j}}{\mathfrak{j}'} = \beta$, we get $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha) = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\beta) = -1$ by above results. So $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\frac{\alpha}{\beta}) = +1$. Then $\frac{\beta}{\alpha} = \frac{\gamma}{\gamma'}$ for some $\gamma \in \mathfrak{O}$. Consider $\frac{\mathfrak{i}\gamma}{\mathfrak{j}} = b\mathfrak{a}$ where $b \in \mathbb{Q}$ and $\mathfrak{a}$ has no factor of $\mathbb{Z}$ other than ∓ 1. So $\frac{b\mathfrak{a}}{(b\mathfrak{a})'} = \frac{\mathfrak{i}\gamma}{\mathfrak{j}} \cdot \frac{\mathfrak{j}'}{\mathfrak{i}'\gamma'} = \alpha \cdot \frac{1}{\beta} \cdot \frac{\beta}{\alpha} = 1$, so $\mathfrak{a} = \mathfrak{a}'$, $\mathfrak{a}$ is ambig, $\mathfrak{i}\beta = b\beta\mathfrak{a}$ implies $\mathfrak{i} \sim \mathfrak{j}\mathfrak{a}$. □

Theorem 4.8.7. *There exist $c-1$ independent ambig classes and 2^{c-1} distinct ambig classes.*

Proof. Let s be the number of distinct prime divisors of $\mathrm{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m}))$.

Case 1. If $m < 0$, then $c = s$. So by Theorem 4.8.5 and by Theorem 4.8.6, there are 2^{s-1} ambig classes.

Case 2. If $m > 0$ and $\Upsilon(-1) = (1, 1, \ldots, 1)$, then $c = s$. So by Theorem 4.8.5 and by Theorem 4.8.6, there are 2^{s-1} ambig classes. If $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\varepsilon) = -1$, then all classes are obtained by ambig ideals. If $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\varepsilon) = +1$, then only 2^{s-2} of them are obtained by ambig ideals.

Case 3. If $m > 0$ and $\Upsilon(-1) \neq (+1, +1, \ldots, +1)$, then $c = s-1$. So by Theorem 4.8.5 and by Theorem 4.8.6, there are 2^{s-2} ambig classes all obtained by ambig ideals.

Thus, there are 2^{c-1} distinct ambig classes in all cases. □

Theorem 4.8.8. *In $\mathbb{Q}(\sqrt{m})$, let g be the number of distinct genera, then $g = 2^{c-1}$.*

Proof. Let f denote the number of ideal classes in the principal genus. By Definition 4.5.1, each genus has the same number of classes, so each genus contains f classes. Then $h = gf$ is the number of all classes in $\mathbb{Q}(\sqrt{m})$. Let $\mathtt{H}_1, \mathtt{H}_2, \ldots, \mathtt{H}_f$ be the classes in the principal genus, then by Theorem 4.8.2, $\mathtt{H}_1 = \mathtt{K}_1^2, \mathtt{H}_2 = \mathtt{K}_2^2, \ldots, \mathtt{H}_f = \mathtt{K}_f^2$ where $\mathtt{K}_1, \mathtt{K}_2, \ldots, \mathtt{K}_f$ are classes in $\mathbb{Q}(\sqrt{m})$.

Now let $\mathtt{C}$ be an arbitrary ideal class, so $\mathtt{C}^2$ is in the principal genus, so $\mathtt{C}^2 = \mathtt{K}_\alpha^2$ for a unique $\alpha \in \{1, 2, \ldots, f\}$. So the unique class $\mathtt{A} = \dfrac{\mathtt{C}}{\mathtt{K}_\alpha}$ is ambig since $\mathtt{C} = \mathtt{AK}_\alpha$ implies $\mathtt{C}^2 = \mathtt{A}^2\mathtt{K}_\alpha^2$. Then $\mathtt{A}^2 = \mathtt{I}$, that is $\mathtt{A} = \mathtt{A}^{-1}$, so $\mathtt{A} = \mathtt{A}'$ since $\mathtt{AA}' = \mathtt{I}$. So as $\mathtt{A}$ ranges over all ambig classes and $\mathtt{K}$ ranges over all $\mathtt{K}_1, \mathtt{K}_2, \ldots, \mathtt{K}_f$, then $\mathtt{AK}$ ranges over all classes. And for each ambig class $\mathtt{A}$ and for each $\mathtt{K} \in \{\mathtt{K}_1, \mathtt{K}_2, \ldots, \mathtt{K}_f\}$ there is exactly one class $\mathtt{AK}$. So $h = 2^{c-1}f$ since there exist 2^{c-1} distinct ambig classes by Theorem 4.8.7, so $h = gf = 2^{c-1}f$ implies $g = 2^{c-1}$. □

5. QUADRATIC RECIPROCITY LAW BY QUADRATIC NUMBER FIELDS WITH GENUS THEORY IN THE STRICT SENSE

5.1. Introduction

The aim of this chapter is again to prove the quadratic reciprocity law by using the theory of quadratic number fields. But for this chapter, we will first discuss how the strict sense equivalence change the class number. Then, we will find the number of genera by using exact sequences. With these results, we will give a proof of the quadratic reciprocity law. In addition, we present genus character and genus field with their properties.

Definition 5.1.1. Let $k = \mathbb{Q}(\sqrt{m})$ be a quadratic number field over $\mathbb{Q}$ and d be its discriminant. The discriminant d is called a *prime discriminant*, if it is a prime power up to sign.

Proposition 5.1.2. *Let d be the discriminant of a quadratic number field k. Then d can be written uniquely as a product of prime discriminants up to order.*

Proof. If d is a prime discriminant, then we are done. Assume d is not a prime discriminant, then there exists an odd prime p dividing d, because if all prime divisors of a discriminant are even, these discriminants are $-4, -8$ or 8 and they are prime discriminants. Then

$$d_1 = p^* = (-1)^{\frac{p-1}{2}} \; p \equiv 1 \mod 4$$

is a prime discriminant. Now, let us show that $\dfrac{d}{d_1} = d'$ is a discriminant by using Theorem 4.1.1.

Case 1. If $d \equiv 0 \mod 4$, then $d' \equiv 0 \mod 4$, so $d' = 4m$ where $m \equiv 2$

mod 4 , therefore d' is a discriminant.

Case 2. If d' is odd, then d is odd, then $d \equiv 1 \mod 4$ since it is a discriminant, then $d' \equiv 1 \mod 4$ since d_1 is, therefore d' is a discriminant.

Case 3. If $d' \equiv 4 \mod 8$, then $d = d'd_1 \equiv 4 \mod 8$ since $d_1 \equiv 1 \mod 8$, then $\frac{d}{4} \equiv 3 \mod 4$ since d is a discriminant, so $\frac{d'}{4} \equiv 3 \mod 4$ since $d_1 \equiv 1 \mod 4$, therefore d' is a discriminant.

We can proceed by induction. For uniqueness let $= d_1 d_2 ... d_n = d'_1 d'_2 ... d'_m$ be prime discriminant factorizations of d. If each prime discriminant is even, then it is $-4, -8$ or 8 and for equality they must appear equally on both sides. If there is an odd prime discriminant, say d_1, then there exists a prime discriminant, say d'_1 such that $|d_1| = |d'_1|$ since the absolute values are prime numbers. If $d_1 = -d'_1$ then one is congruent to 1 modulo 4 and other one is congruent to 3 modulo 4 which contradicts that both of d_1 and d'_1 are discriminants. Thus we have $d_1 = d'_1$. Proceeding by this way we eliminate all odd prime discriminants and get $d_i = d'_i$ for all i and $n = m$. □

Definition 5.1.3. A number $\alpha \in k = \mathbb{Q}(\sqrt{m})$ is called *totally positive*, if $m < 0$ or if $m > 0$, $\alpha > 0$ and $\alpha^\sigma > 0$ where α^σ is the algebraic conjugate of α and we write $\alpha >> 0$. A number $\alpha \in k = \mathbb{Q}(\sqrt{m})$ is called *totally negative*, if $-\alpha$ is totally positive and we write $\alpha << 0$.

Definition 5.1.4. For this chapter, we define the norm of an ideal by

$$N(\mathfrak{a}) = |N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(k)\mathbb{Q}(\mathfrak{a})|$$

where $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(k)\mathbb{Q}(\mathfrak{a})$ is the norm of $\mathfrak{a}$ defined in Definition 4.1.2.

Lemma 5.1.5. *Let $\alpha \in k = \mathbb{Q}(\sqrt{m})$, then $N(\alpha) > 0$ if and only if $\alpha >> 0$ or $-\alpha >> 0$.*

Proof. $N(\alpha) > 0$ if and only if $\alpha\alpha^\sigma > 0$, if and only if $\alpha > 0$ and $\alpha^\sigma > 0$ or $\alpha < 0$ and

$\alpha^\sigma < 0$, if and only if $\alpha > 0$ and $\alpha^\sigma > 0$ or $-\alpha > 0$ and $-\alpha^\sigma > 0$, if and only if $\alpha > 0$ and $\alpha^\sigma > 0$ or $-\alpha > 0$ and $(-\alpha)^\sigma > 0$, if and only if $\alpha >> 0$ or $-\alpha >> 0$. □

5.2. Class Groups

Now we will define some equivalence relations among ideals.

Definition 5.2.1. Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are called *equivalent*, if $\mathfrak{a} \equiv \lambda\mathfrak{b}$ for some $\lambda \in k$ and written $\mathfrak{a} \sim \mathfrak{b}$.

Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are called *equivalent in the strict sense*, if $\mathfrak{a} \equiv \lambda\mathfrak{b}$ for some $\lambda \in k$ with $\lambda >> 0$ and written $\mathfrak{a} \sim^+ \mathfrak{b}$. See Definition 3.3.4 and note the difference between strict and narrow sense equivalences.

Here $\sim$ is an equivalence relation. The equivalence class of $\mathfrak{a}$ is $[\mathfrak{a}]$ and these classes form the group $Cl(k)$ called *the class group*. The order of the class group is called *the class number* and denoted by $h(k)$.

Similarly $\sim^+$ is an equivalence relation. The equivalence class of $\mathfrak{a}$ is $[\mathfrak{a}]_+$ and these classes form the group $Cl^+(k)$ called *the class group in the strict sense*. The order of the class group is called *the class number in the strict sense* and denoted by $h^+(k)$.

Proposition 5.2.2. *Let $\langle\sqrt{d}\,\rangle$ denote the subgroup $\{\mathcal{I}_+, [(\sqrt{d}\,)]_+\}$ of the class group in the strict sense, $Cl^+(k)$. Then the Figure 5.1.*

$$1 \xrightarrow{\varphi} \langle\sqrt{d}\,\rangle \xrightarrow{i} Cl^+(k) \xrightarrow{\pi} Cl(k) \xrightarrow{\psi} 1$$

Figure 5.1. Exact sequence of class groups

where $\pi : [\mathfrak{a}]_+ \mapsto [\mathfrak{a}]$ is exact.

Proof. The identity map i is one to one, so $\mathrm{Ker}\,(i) = \{\mathfrak{1}_+\} = \mathrm{Im}\,(\varphi)$. Also $\mathrm{Im}\,(\pi) = Cl(k) = \mathrm{Ker}\,(\psi)$ since for all $[\mathfrak{a}] \in Cl(k)$, we find $[\mathfrak{a}]_+ \in Cl^+(k)$ such that $\pi([\mathfrak{a}]_+) = [\mathfrak{a}]$. And $\mathrm{Im}\,(i) = \{\mathfrak{1}_+, [(\sqrt{d})]_+\} \subseteq \mathrm{Ker}\,(\pi)$ since $\pi(\mathfrak{1}_+) = \mathfrak{1}$ and $\pi([(\sqrt{d})]_+) = [(\sqrt{d})] = \mathfrak{1}$. Now let $[\mathfrak{a}]_+ \in \mathrm{Ker}\,(\pi)$, so $\pi([\mathfrak{a}]_+) = [\mathfrak{a}] = \mathfrak{1}$, then $\mathfrak{a} \sim \mathfrak{1}$, $\mathfrak{a} = (\alpha)$ for some $\alpha \in k$.

Case 1. If $N(\alpha) > 0$, then $\alpha >> 0$ or $-\alpha >> 0$, so choose α with $\alpha >> 0$, then $\mathfrak{a} = (\alpha)$ with $\alpha >> 0$ implies $[\mathfrak{a}]_+ = \mathfrak{1}_+$.

Case 2. If $N(\alpha) > 0$, then $\alpha > 0$ and $\alpha^\sigma < 0$ or $\alpha < 0$ and $\alpha^\sigma > 0$, then $\alpha > 0$ and $\alpha^\sigma < 0$ or $-\alpha > 0$ and $(-\alpha)^\sigma < 0$, so choose α with $\alpha > 0$, then $\dfrac{\alpha}{\sqrt{d}} > 0$ and $\left(\dfrac{\alpha}{\sqrt{d}}\right)^\sigma = \dfrac{\alpha^\sigma}{-\sqrt{d}} > 0$ so we have $\dfrac{\alpha}{\sqrt{d}} >> 0$ with $\mathfrak{a} = \left(\dfrac{\alpha}{\sqrt{d}}\right)(\sqrt{d})$ implies $[\mathfrak{a}]_+ = [(\sqrt{d})]_+$ and $[\mathfrak{a}]_+ \in \langle \sqrt{d}\,\rangle = \mathrm{Im}\,(i)$.

Therefore $\mathrm{Ker}\,(\pi) \subseteq \mathrm{Im}\,(i)$. □

Corollary 5.2.3. *Let $h^+(k)$ and $h(k)$ be the orders of $Cl^+(k)$ and $Cl(k)$ respectively. If $disc(k) = d > 0$ and $N(\varepsilon) = +1$, then $h^+(k) = 2h(k)$, otherwise $h^+(k) = h(k)$.*

Proof. $h^+(k) = h(k)$ if and only if $|Cl^+(k)| = |Cl(k)|$ if and only if $|\mathrm{Ker}\,(\pi)| = 1$ where π is defined as in Proposition 5.2.2, that is if and only if $\mathrm{Im}\,(i) = \langle \sqrt{d}\,\rangle = 1$ by the exact sequence in Proposition 5.2.2, if and only if $(\sqrt{d}) = (\alpha)$ for some $\alpha >> 0$, if and only if $\alpha = \eta\sqrt{d} >> 0$ for some $\eta \in \mathfrak{O}_k^\times$. If $d < 0$, then we can take $\eta = 1$. If $d > 0$ and then $\eta\sqrt{d} >> 0$. So $N(\sqrt{d}) = -d < 0$ implies that $N(\eta) < 0$, therefore $N(\eta) < 0$, therefore $[(\sqrt{d})]_+ = \mathfrak{I}_+\ \eta \in \mathfrak{O}_k^\times$ with $N(\eta) = -1$, if and only if $N(\varepsilon) = -1$. Otherwise, $h(k) = h^+(k)/\,|\mathrm{Ker}\,(\pi)| = h^+(k)/|\langle\sqrt{d}\rangle|$ implies $h^+(k) = 2h(k)$. □

5.3. The Genus Class Groups

Now again we will define some equivalence relations:

Definition 5.3.1. Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are called *similar*, if $N(\mathfrak{a}) \equiv N(\lambda)N(\mathfrak{b})$ for some $\lambda \in k$ and written $\mathfrak{a} \approx \mathfrak{b}$.

Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are called *similar in the strict sense*, if $N(\mathfrak{a}) \equiv N(\lambda)N(\mathfrak{b})$ for some $\lambda \in k$ with $\lambda >> 0$ and written $\mathfrak{a} \approx^{+} \mathfrak{b}$.

Here $\approx$ is an equivalence relation. The equivalence class of $\mathfrak{a}$ is $[[\mathfrak{a}]]$ and these classes form the group $Cl_{gen}(k)$ called *the genus class group.*

Similarly, $\approx^{+}$ is an equivalence relation. The equivalence class of $\mathfrak{a}$ is $[[\mathfrak{a}]]_{+}$ and these classes form the group $Cl^{+}_{gen}(k)$ called *the genus class group in the strict sense.*

Proposition 5.3.2. *Let* $\mathfrak{a}$,$\mathfrak{b}$ *be two ideals in* $\mathfrak{O}$. *Then* $\mathfrak{a} \approx^{+} \mathfrak{b}$ *if and only if* $\mathfrak{a} \sim^{+} \mathfrak{b}\mathfrak{c}^2$ *for some ideal* $\mathfrak{c}$ *in* $\mathfrak{O}$.

Proof. We will prove that $\mathfrak{a} \approx^{+} \mathfrak{1}$ if and only if $\mathfrak{a} \sim^{+} \mathfrak{c}^2$ for some ideal $\mathfrak{c}$ in $\mathfrak{O}$.

First assume that $\mathfrak{a} \approx^{+} \mathfrak{1}$, then $N(\mathfrak{a}) = N(\lambda)$ for some $\lambda >> 0$, then $N(\lambda^{-1}\mathfrak{a}) = 1$. By Hilbert's Theorem 90 (See Appendix B.0.17), there exists an ideal $\mathfrak{c}$ such that $\lambda^{-1}\mathfrak{a} = \mathfrak{c}^{1-\sigma}$. We have $\mathfrak{c}\mathfrak{c}^{\sigma} = N(\mathfrak{c})$ with $N(\mathfrak{c}) > 0$, so $N(\mathfrak{c}) >> 0$, then $\mathfrak{c} = N(\mathfrak{c})\mathfrak{c}^{-\sigma}$ with $N(\mathfrak{c}) >> 0$ implies that $\mathfrak{c}^{-\sigma} \sim^{+} \mathfrak{c}$. Thus, $\lambda^{-1}\mathfrak{a} = \mathfrak{c}\mathfrak{c}^{-\sigma} \sim^{+} \mathfrak{c}^2$ implies $\mathfrak{a} \sim^{+} \mathfrak{c}^2$ since $\lambda >> 0$.

Conversely assume that $\mathfrak{a} \sim^{+} \mathfrak{c}^2$, then $\mathfrak{a} = \lambda\mathfrak{c}^2$ for some $\lambda >> 0$, then $N(\mathfrak{a}) = N(\lambda)N(\mathfrak{c}^2) = N(\lambda)N(N(\mathfrak{c})) = N(\lambda c)$ where $c = N(\mathfrak{c}) > 0$. Thus $\mathfrak{a} \approx^{+} \mathfrak{1}$. □

Corollary 5.3.3.

$$Cl^{+}_{gen}(k) \simeq Cl^{+}(k)/(Cl^{+}(k))^2$$

From now on, we will try to find the number of genera by showing that

$$\left|Cl^{+}(k)/Cl^{+}(k)^2\right| = 2^{s-1}$$

where s is the number of finite primes ramifying in k.

Definition 5.3.4. A class is called *ambiguous*, if $\mathfrak{c}^\sigma = \mathfrak{c}$ for $c \in Cl^+(k)$. The set of all ambiguous classes is denoted by Am^+ and it is a subgroup of $Cl^+(k)$.

Nota that, being ambiguous and ambig are slightly different things for ideals. See Definition 4.6.1.

Also note that, by Definition 5.3.4, the Figure 5.2.

$$1 \longrightarrow Am^+ \longrightarrow Cl^+(k) \xrightarrow{1-\sigma} Cl^+(k)^{1-\sigma} \longrightarrow 1$$

Figure 5.2. Exact sequence of ambig ideals

is exact where $1 - \sigma : c \mapsto c^{1-\sigma}$.

Proposition 5.3.5. *Let Am^+ be the subgroup of all ambiguous classes in $Cl^+(k)$. Then if $\mathfrak{c} \in Am^+$, then $\mathfrak{c} = [\mathfrak{a}]_+$ with $\mathfrak{a} = \mathfrak{a}^\sigma$.*

Proof. Let $\mathfrak{c}$ be in Am^+. Then $\mathfrak{c} = \mathfrak{c}^\sigma$ for $\mathfrak{c} = [\mathfrak{a}]$, so $\mathfrak{a}^\sigma = \lambda\mathfrak{a}$ with $\lambda >> 0$. Then $N(\mathfrak{a}^\sigma) = N(\lambda)N(\mathfrak{a})$ implies that λ is a unit, so $N(\lambda) = +1$ since it is totally positive. Then $\lambda = \alpha^{1-\sigma}$ for some $\alpha \in k$ by Hilbert's Theorem 90 (See Appendix B.0.16). Then $N(\alpha) = \alpha\alpha^\sigma = \lambda\alpha^{2\sigma} >> 0$ in k implies $N(\alpha) > 0$, that is if and only if $\alpha >> 0$ or $-\alpha >> 0$. So by choosing the suitable one we get $\mathfrak{a} \sim^+ \alpha\mathfrak{a}$. So $\mathfrak{c} = [\alpha\mathfrak{a}]$ and $\alpha\mathfrak{a}$ is ambiguous since $(\alpha\mathfrak{a})^\sigma = \alpha^\sigma\mathfrak{a}^\sigma = \alpha^\sigma\lambda\mathfrak{a} = \alpha\mathfrak{a}$. □

Note that $(Cl^+(k) : Cl^+(k)^2) = |Am^+|$ since for $\mathfrak{c} = [\mathfrak{a}]_+$, $\mathfrak{a}\mathfrak{a}^\sigma = (N(\mathfrak{a})) = \lambda$ with $\lambda >> 0$ implies $\mathfrak{a}\mathfrak{a}^\sigma \sim^+ \mathfrak{1}$, so $[\mathfrak{a}\mathfrak{a}^\sigma]_+ = 1$, so $\mathfrak{c}\mathfrak{c}^\sigma = \mathfrak{I}$ implies $\mathfrak{c}^{-\sigma} = \mathfrak{c}$, so $\mathfrak{c}^{1-\sigma} = \mathfrak{c}^2$, then $Cl^+(k)^{1-\sigma} = Cl^+(k)Cl^+(k) = Cl^+(k)^2$ and by the exactness of the Equation 5.3 since $1 - \sigma$ is onto, we get

$$Cl^+(k)/Am^+ \simeq (Cl^+(k))^{1-\sigma}. \tag{5.1}$$

Thus $|Am^+| = |Cl^+(k)| \,/\, |(Cl^+(k))^{1-\sigma}|$.

Notation 5.3.6. A : the group of fractional ambiguous ideals,

E_k : unit group of k,

E : totally positive units in $\mathfrak{O}_k^{\times}$,

I : ideals generated by rational numbers,

$H = \{\mathfrak{a} : \mathfrak{a}^{\sigma} = \mathfrak{a}, \mathfrak{a} = (\alpha), \alpha >> 0, \alpha \in k\}$.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & I & \longrightarrow & I & \longrightarrow & 1 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & H & \longrightarrow & A & \xrightarrow{\gamma} & Am^{+} & \longrightarrow & 1 \end{array}$$

Figure 5.3. Figure for ambig ideals to use Snake Lemma

where $\gamma : \mathfrak{a} \mapsto [\mathfrak{a}]_{+}$ and this diagram commutes with exact rows. So by the Snake Lemma (See Appendix B.0.19), we get the Figure 5.4.

$$1 \longrightarrow H/I \longrightarrow A/I \longrightarrow Am^{+} \longrightarrow 1.$$

Figure 5.4. Exact sequence of quotient groups

We know that $A/I \simeq (\mathbb{Z}/2\mathbb{Z})^s$ by Theorem 4.6.2. Then we will determine $|H/I|$.

If $(\alpha) \in H$, then $\alpha >> 0$ and (α) is ambiguous, so $(\alpha)^{\sigma} = (\alpha)$, so $(\alpha)^{1-\sigma} = \mathfrak{1}$ implies $\alpha^{1-\sigma} = \varepsilon$ with $\varepsilon >> 0$. Then define

$$\rho : H \longrightarrow E/E^{1-\sigma}$$

such that $\rho((\alpha)) = \varepsilon E^{1-\sigma}$. The function ρ is a well defined homomorphism and

$$\operatorname{Ker}\rho \;\; = \;\; \{(\alpha) \in H : \rho((\alpha)) = E^{1-\sigma}\}$$

$$\begin{aligned} &= \{(\alpha) \in H : \varepsilon E^{1-\sigma} = E^{1-\sigma}\} \\ &= \{(\alpha) \in H : \varepsilon = \alpha^{1-\sigma} \in E^{1-\sigma}\} \\ &= \{(\alpha) \in H : (\alpha) = (\alpha^{\sigma})\} \\ &= I. \end{aligned}$$

Also, $\operatorname{Im}\rho = E/E^{1-\sigma}$ since $\varepsilon E^{1-\sigma} \in E/E^{1-\sigma}$ implies $\varepsilon \in E$, so $N(\varepsilon) = 1$. Then $\varepsilon = \alpha^{1-\sigma}$ for some $\alpha \in k$. Then $N(\alpha) = \alpha\alpha^{\sigma} = (\varepsilon\alpha^{\sigma})\alpha^{\sigma} = \varepsilon\alpha^{2\sigma} >> 0$, so we can choose $\alpha >> 0$ by Lemma 5.1.5, so $\rho(\alpha) = \varepsilon E^{1-\sigma}$. Therefore, $H/I \simeq E/E^{1-\sigma}$.

Now, what is $(E : E^{1-\sigma})$?

Case 1. If $d < 0$, then $E = E_k = \langle\zeta\rangle$ where ζ is the root of unity with $\zeta\zeta^{\sigma} = 1$. Then $\zeta^{-\sigma} = \zeta$ implies $\zeta^{1-\sigma} = \zeta^2$, so $(E : E^{1-\sigma}) = (\langle\zeta\rangle : \langle\zeta^2\rangle) = 2$.

Case 2. If $d > 0$ and $N(\varepsilon) = +1$ where ε is the fundamental unit in k, then $\varepsilon >> 0$ or $-\varepsilon >> 0$ implies $E = \langle\varepsilon\rangle$ and $\varepsilon\varepsilon^{\sigma} = 1$ implies $\varepsilon^{-\sigma} = \varepsilon$. Then $\varepsilon^{1-\sigma} = \varepsilon^2$, so $E^{1-\sigma} = \langle\varepsilon^2\rangle$ and $(E : E^{1-\sigma}) = (\langle\varepsilon\rangle : \langle\varepsilon^2\rangle) = 2$.

Case 3. If $d > 0$ and $N(\varepsilon) = -1$ where ε is the fundamental unit in k, then $N(\varepsilon^2) = N(\varepsilon)N(\varepsilon) = 1$. Then $\varepsilon^2 >> 0$ or $-\varepsilon^2 >> 0$ implies $E = \langle\varepsilon^2\rangle$ and $\varepsilon^2\varepsilon^{2\sigma} = 1$ implies $\varepsilon^{-2\sigma} = \varepsilon^2$, so $\varepsilon^{2-2\sigma} = \varepsilon^4$, $E^{1-\sigma} = \langle\varepsilon^4\rangle$ and $(E : E^{1-\sigma}) = (\langle\varepsilon^2\rangle : \langle\varepsilon^4\rangle) = 2$.

Hence, by the exactness of the Figure 5.4. with the Equation 5.1 and by the isomorphism $A/I \simeq (\mathbb{Z}/2\mathbb{Z})^t$ and $H/I \simeq \mathbb{Z}/2\mathbb{Z}$, we proved,

Theorem 5.3.7. *$Am^+ \simeq Cl^+(k)/Cl^+(k)^2 \simeq (\mathbb{Z}/2\mathbb{Z})^{s-1}$*

Let us now consider the relation between Cl^+_{gen} and Cl_{gen}.

Proposition 5.3.8. *Let $\mathfrak{a}$,$\mathfrak{b}$ be two ideals in $\mathfrak{O}$. Then $\mathfrak{a} \approx \mathfrak{b}$ if and only if $\mathfrak{a}\sim\mathfrak{b}\mathfrak{c}^2$ for some ideal $\mathfrak{c}$ in $\mathfrak{O}$.*

Proof. We will prove that $\mathfrak{a} \approx \mathfrak{1}$ if and only if $\mathfrak{a}\sim\mathfrak{c}^2$ for some ideal $\mathfrak{c}$ in $\mathfrak{O}$.

First assume that $\mathfrak{a} \approx \mathfrak{1}$, then $N(\mathfrak{a}) = N(\lambda)$ for some $\lambda \in k$, then $N(\lambda^{-1}\mathfrak{a}) = 1$. By Hilbert's Theorem 90 (See Appendix B.0.17), there exists an ideal $\mathfrak{c}$ such that $\lambda^{-1}\mathfrak{a} = \mathfrak{c}^{1-\sigma}$. We have $\mathfrak{c}\mathfrak{c}^{\sigma} = N(\mathfrak{c})$ with $N(\mathfrak{c}) \in k$, then $\mathfrak{c} = N(\mathfrak{c})\mathfrak{c}^{-\sigma}$ implies that $\mathfrak{c}^{-\sigma} \sim \mathfrak{c}$. Thus $\lambda^{-1}\mathfrak{a} = \mathfrak{c}\mathfrak{c}^{-\sigma} \sim \mathfrak{c}^2$ implies $\mathfrak{a} \sim \mathfrak{c}^2$.

Conversely, assume that $\mathfrak{a} \sim \mathfrak{c}^2$, then $\mathfrak{a} = \lambda\mathfrak{c}^2$ for some $\lambda \in k$, then $N(\mathfrak{a}) = N(\lambda)N(\mathfrak{c}^2) = N(\lambda)N(N(\mathfrak{c})) = N(\lambda c)$ where $c = N(\mathfrak{c}) \in k$, thus $\mathfrak{a} \approx \mathfrak{1}$. □

Corollary 5.3.9.

$$Cl_{gen}(k) \simeq Cl(k)/(Cl(k))^2$$

Proposition 5.3.10. *The followings are equivalent:*
i. $Cl^{+}_{gen}(k) \simeq Cl_{gen}(k)$
ii. $(\sqrt{m}) \approx^{+} \mathfrak{1}$
iii. m *is a sum of squares.*

Proof. Consider the map

$$\begin{array}{ccccc} \pi & : & Cl^{+}_{gen}(k) & \longrightarrow & Cl_{gen}(k) \\ & & [[\mathfrak{a}]]_{+} & \mapsto & [[\mathfrak{a}]]. \end{array}$$

(i) ⇒ (ii): If $Cl^{+}_{gen}(k) \simeq Cl_{gen}(k)$, then since $(\sqrt{m}) \approx \mathfrak{1}$ in $Cl_{gen}(k)$ we have $(\sqrt{m}) \approx^{+} \mathfrak{1}$ in $Cl^{+}_{gen}(k)$.

(ii) ⇒ (i): Assume $(\sqrt{m}) \approx^{+} \mathfrak{1}$. Let $[[\mathfrak{a}]]_{+} \in \operatorname{Ker}\pi$, so $\pi([[\mathfrak{a}]]_{+}) = [[\mathfrak{a}]] = 1$ in $Cl_{gen}(k)$, that is $\mathfrak{a} \approx \mathfrak{1}$, in other words $N(\mathfrak{a}) = N((\lambda))$.

If $N(\lambda) > 0$, then we can choose λ with $\lambda >> 0$, so $N(\mathfrak{a}) = N(\lambda)$ with $\lambda >> 0$ implies $\mathfrak{a} \approx^{+} \mathfrak{1}$.

If $N(\lambda) < 0$, then $N(\frac{\lambda}{\sqrt{m}})$. Then we can choose λ with $\frac{\lambda}{\sqrt{m}} >> 0$. Since $\mathfrak{a} = \frac{\lambda}{\sqrt{m}}(\sqrt{m})$, we get $N(\mathfrak{a}) = N(\frac{\lambda}{\sqrt{m}})N((\sqrt{m}))$ with $\frac{\lambda}{\sqrt{m}} >> 0$, that implies $\mathfrak{a} \approx^+ (\sqrt{m}) \approx^+ \mathfrak{1}$ with assumption.

Note that, without the assumption $(\sqrt{m}) \approx^+ \mathfrak{1}$, we still have that $|\mathrm{Ker}\,\pi| \leq 2$.

Thus $\mathrm{Ker}\,\pi = \{1\}$ and since π is an onto homomorphism, we get the isomorphism $Cl^+_{gen}(k) \simeq Cl_{gen}(k)$.

(ii) $\Rightarrow$ (iii): If $(\sqrt{m}) \approx^+ \mathfrak{1}$, then $(\sqrt{m}) = \lambda\mathfrak{c}^2$ for some ideal $\mathfrak{c}$ with $\lambda >> 0$. Say $\lambda = \frac{1}{2}(a + b\sqrt{m})$, then $N((\sqrt{m})) = N(\lambda\mathfrak{c}^2) > 0$ gives $m = \frac{1}{4}(a^2 - b^2m)c^2$ where $c = N(\mathfrak{c})$, then $4m = (a^2 - b^2m)c^2$. Put $a = mA$, so $4m = (m^2A^2 - b^2m)c^2$ implies $4m + mb^2c^2 = m^2A^2c^2$ and $m = \frac{4}{A^2c^2} + \frac{b^2c^2}{A^2c^2} = \left(\frac{2}{Ac}\right)^2 + \left(\frac{b}{A}\right)^2$.

(iii) $\Rightarrow$ (ii): If $m = r^2 + s^2$, then for $\mathfrak{c} = (s, r + \sqrt{m})$, $\mathfrak{c}^2 = (s^2, sr + s\sqrt{m}, (r + \sqrt{m})^2) = (m - r^2, sr + s\sqrt{m}, (r + \sqrt{m})^2) = (r + \sqrt{m})(r - \sqrt{m}, s, r + \sqrt{m}) = (r + \sqrt{m})$ since $r - \sqrt{m} + r + \sqrt{m} = 2r$ and $(2r, s) = 1$. So for $(\lambda) = (r\sqrt{m} + m) = \sqrt{m}\mathfrak{c}^2$, $\lambda >> 0$ since $r\sqrt{m} + m > 0$ and $(r\sqrt{m} + m)^\sigma = m - r\sqrt{m} > 0$, because $m > r^2$. Thus, $N(\sqrt{m})N(\mathfrak{c}^2) = N(\lambda)$ with $\lambda >> 0$ implies $(\sqrt{m}) \approx^+ \mathfrak{1}$. □

Corollary 5.3.11. *If m is a sum of two squares, then $Cl_{gen}(k) \simeq (\mathbb{Z}/2\mathbb{Z})^{t-1}$, otherwise we have $Cl_{gen}(k) \simeq (\mathbb{Z}/2\mathbb{Z})^{t-2}$.*

Proof. By Corollary 5.3.3 and Theorem 5.3.7 we have $Cl^+_{gen}(k) \simeq (\mathbb{Z}/2\mathbb{Z})^{t-1}$. If m is a sum of two squares $Cl_{gen}(k) \simeq Cl^+_{gen}(k)$ by Proposition 5.3.10, so we get $Cl_{gen}(k) \simeq (\mathbb{Z}/2\mathbb{Z})^{t-1}$. Otherwise $|\mathrm{Ker}\,\pi| = 2$ again by Proposition 5.3.10, so

$$Cl_{gen}(k) \simeq Cl^+_{gen}(k)/\mathrm{Ker}\,\pi \simeq (\mathbb{Z}/2\mathbb{Z})^{s-1}/(\mathbb{Z}/2\mathbb{Z}) \simeq (\mathbb{Z}/2\mathbb{Z})^{s-2}.$$

□

5.4. Quadratic Reciprocity Law

Proposition 5.4.1. *Let k be a quadratic number field with discriminant d. Then the class number in the strict sense $h^+(k)$ is odd if and only if d is a prime discriminant, and the class number in the usual sense $h(k)$ is odd if and only if d is a prime discriminant or a product of two prime discriminants.*

Proof. First assume that d is a prime discriminant, so $s = 1$ and we get $(Cl^+(k) : Cl^+(k)^2) = 2^{s-1} = 1$. So $|(Cl^+(k)| = |Cl^+(k)^2)|$ and then

$$\begin{array}{ccccc} \varphi^+ & : & Cl^+(k) & \longrightarrow & Cl^+(k)^2 \\ & & \mathsf{c} & \mapsto & \mathsf{c}^2 \end{array}$$

is an automorphism. Thus $|Cl^+(k)| = h^+(k)$ is odd, then $|Cl(k)| = h(k)$ is odd by Corollary 5.2.3. Also see Lemma 4.7.3.

Now assume that $d = d_1 d_2$ where d_1, d_2 are negative prime discriminants. Then we have two possible values for d.
1. $d = (-4)(-p)$ where $p \equiv 3 \mod 4$,
2. $d = (-p)(-q)$ where $p \equiv q \equiv 3 \mod 4$. Since there exists a prime power of d of the form $4k+3$ that divides d with an odd exponent, d is not a sum of squares. So by Corollary 5.3.11, we get $|Cl_{gen}(k)| = 2^{s-2} = 2^{2-2} = 1$, then

$$\begin{array}{ccccc} \varphi & : & Cl(k) & \longrightarrow & Cl(k)^2 \\ & & \mathsf{c} & \mapsto & \mathsf{c}^2 \end{array}$$

is an automorphism. Thus $|Cl(k)| = h(k)$ is odd.

For the converse, assume that $|Cl^+(k)| = h^+(k)$ is odd, so φ^+ is an automorphism, then $(Cl^+(k) : Cl^+(k)^2) = 1$ implies that $2^{s-1} = 1$, so $s = 1$ and d is a prime discriminant.

Now assume that $|Cl(k)| = h(k)$ is odd, but $h^+(k)$ is even, that is $s \neq 1$, so $h(k) \neq h^+(k)$ implies $Cl^+_{gen}(k) \simeq Cl_{gen}(k)$ is not true, so by Proposition 5.3.10, m is not a sum of square. Thus, Corollary 5.3.11 implies $|Cl_{gen}(k)| = 2^{s-2} = 1$ and therefore $s = 2$. This also means that m contains a prime power of the form $4k + 3$ that divides m with an odd exponent, so also d. This is possible if and only if $d = 4p$ with $p \equiv 3 \mod 4$ or $d = p\,q$ with $p \equiv q \equiv 3 \mod 4$, in other words d is a product of two prime discriminants. □

Theorem 5.4.2. ***(Quadratic Reciprocity Law)*** *Let $p, q \in \mathbb{Z}$ be distinct positive odd prime numbers. Then*

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

(ii) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ *and*

(iii) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$.

Proof. We will prove the theorem in the following order:

Case 1. $\left(\frac{-1}{p}\right) = 1 \Leftrightarrow p \equiv 1 \mod 4$:

If $p \equiv 1 \mod 4$, then $\mathbb{Q}(\sqrt{p})$ has a unit $\varepsilon = \frac{1}{2}(x + y\sqrt{p})$ with $N(\varepsilon) = -1$. See Appendix A.0.10 for the way we find ε. So $x^2 - py^2 = -4$, $x^2 \equiv -4 \mod p$, therefore $\left(\frac{-1}{p}\right) = +1$. Then by Theorem 4.2.7, p splits in $\mathbb{Q}(\sqrt{-1})$, so $p = (a + b\sqrt{-1})(a - b\sqrt{-1})$ for some $a, b \in \mathbb{Z}$ since $\mathbb{Q}(\sqrt{-1})$ is an euclidean domain. Therefore, $p = a^2 + b^2$, so $p \equiv 1 \mod 4$ by [6].

Case 2. If $p \equiv 1 \mod 4$, then $\left(\frac{p}{q}\right) = +1 \Leftrightarrow \left(\frac{q}{p}\right) = +1$:

Fist assume that $\left(\frac{p}{q}\right) = +1$ for $p \equiv 1 \mod 4$. Then q splits in $\mathbb{Q}(\sqrt{p})$, say

$q = \mathfrak{q}\mathfrak{q}'$. By Proposition 5.4.1 and Corollary 5.2.3, $h = h(\mathbb{Q}(\sqrt{p})) = h^+(\mathbb{Q}(\sqrt{p}))$ is odd. Here, $\mathfrak{q}^h$ is a principal ideal by Theorem 3.1.5, say $\mathfrak{q}^h = (\frac{1}{2}(x + y\sqrt{p}))$. Then $q^h = \mathfrak{q}^h\mathfrak{q}'^h = \mp(\frac{1}{2}(x + y\sqrt{p}))(\frac{1}{2}(x - y\sqrt{p}))$ implies $\mp 4q^h = x^2 - py^2$, so $\mp 4q^h \equiv x^2 \mod p$. Since $\left(\frac{-1}{p}\right) = +1$ by Case 1, we get $\left(\frac{q}{p}\right) = +1$.

Conversely, assume that $\left(\frac{q}{p}\right) = +1$. Then for $q^\star = (-1)^{\frac{q-1}{2}} q \equiv 1 \mod 4$, p splits in $\mathbb{Q}(\sqrt{q^\star})$ since $\left(\frac{-1}{p}\right) = +1$ by Case 1, say $p = \mathfrak{p}\mathfrak{p}'$. By Proposition 5.4.1 and Corollary 5.2.3, $h = h(\mathbb{Q}(\sqrt{q^\star})) = h^+(\mathbb{Q}(\sqrt{q^\star}))$ is odd. Here, $\mathfrak{p}^h$ is a principal ideal by Theorem 3.1.5, say $\mathfrak{p}^h = (\frac{1}{2}(x + y\sqrt{q^\star}))$. Then $p^h = \mathfrak{p}^h\mathfrak{p}'^h = \mp(\frac{1}{2}(x + y\sqrt{q^\star}))(\frac{1}{2}(x - y\sqrt{q^\star}))$ implies $\mp 4p^h = x^2 - q^\star y^2$, so $\mp 4p^h \equiv x^2 \mod q^\star$. We get, $\left(\frac{\mp p}{q}\right) = +1$. But since negative sign holds if and only if $q^\star > 0$, that is $q \equiv 1 \mod 4$, we have in fact $\left(\frac{p}{q}\right) = +1$.

Case 3. If $p \equiv q \equiv 3 \mod 4$, then $\left(\frac{p}{q}\right) = +1 \Leftrightarrow \left(\frac{q}{p}\right) = -1$:

Consider the field $\mathbb{Q}(\sqrt{pq})$. For the ideal $\mathfrak{p} = (p, \sqrt{pq})$, we have $\mathfrak{p}^2 = (p^2, 2p\sqrt{pq}, pq) = (p)(p, 2\sqrt{pq}, q) = (p)$ since $(p, q) = 1$. So, $\mathfrak{p}^2 \sim \mathfrak{1}$ implies that $\mathfrak{p}$ is a principal ideal since $h(\mathbb{Q}(\sqrt{pq}))$ is odd by Proposition 5.4.1, say $\mathfrak{p} = (\frac{1}{2}(x + y\sqrt{pq}))$. Then, $N(\mathfrak{p}) = \mp\frac{1}{4}(x^2 - pqy^2)$ implies $\mp 4p = x^2 - pqy^2$, so x is divisible by p, say $x = pz$. By cancellation, we get $\mp 4 = pz^2 - qy^2$. If positive sign holds, then $+4 \equiv pz^2 \mod q$ and $+4 \equiv -qy^2 \mod p$, so $\left(\frac{p}{q}\right) = +1$ and $\left(\frac{q}{p}\right) = -1$ by Case 1. If negative sign holds, then $-4 \equiv pz^2 \mod q$ and $-4 \equiv -qy^2 \mod p$, that is $4 \equiv qy^2 \mod p$, so $\left(\frac{p}{q}\right) = -1$ and $\left(\frac{q}{p}\right) = +1$ by Case 1.

Case 4. $\left(\frac{2}{p}\right) = +1 \Leftrightarrow p \equiv \pm 1 \mod 8$:

First assume that $p \equiv \mp 1 \mod 8$. Consider the field $\mathbb{Q}(\sqrt{p^\star})$ where $p^\star = (-1)^{\frac{p-1}{2}} p \equiv 1 \mod 4$. By Proposition 5.4.1, $h = h(\mathbb{Q}(\sqrt{p^\star}))$ is odd. By Theorem 4.2.7

2 splits in $\mathbb{Q}(\sqrt{p^\star})$. Then 2^h splits into two principle ideals, say $\mp(\frac{1}{2}(x+y\sqrt{p^\star}))$ and $\mp(\frac{1}{2}(x-y\sqrt{p^\star}))$. Therefore, $x^2-p^\star y^2 = \mp 4\cdot 2^h$. We can only consider the positive sign since for $p\equiv 1 \mod 4$ we have a fundamental unit with $N(\varepsilon)=-1$ and for $p\equiv 3 \mod 4$ we have $x^2-p^\star y^2>0$. Therefore, $x^2\equiv 2^{h+2} \mod p$, so $\left(\frac{2}{p}\right)=+1$ since h is odd.

Conversely assume that $\left(\frac{2}{p}\right)=+1$, then p splits in $\mathbb{Q}(\sqrt{2})$ by Theorem 4.2.7, say $p=\mathfrak{p}\mathfrak{p}'$. Since $\mathbb{Q}(\sqrt{2})$ is an euclidean field, $\mathfrak{p}=(\mp\frac{1}{2}(x+y\sqrt{2}))$, so $\mp p = x^2-2y^2\equiv \mp 1 \mod 8$ since p is odd. See Appendix A.0.11 for calculations. □

5.5. The Genus Character

Definition 5.5.1. Let k be a quadratic number field and d be its discriminant with $d=d_1d_2\dots d_t$ its decomposition into prime discriminants. For each d_j, $\chi_j : Cl^+_{gen} \longrightarrow \mathbb{Z}/2\mathbb{Z}$ is defined by:

$$\chi_j([[\mathfrak{p}]]) = \begin{cases} \left(\frac{d_j}{N(\mathfrak{p})}\right)_J & \text{if } (N(\mathfrak{p}),d_j)=1, \\ \\ \left(\frac{d'_j}{N(\mathfrak{p})}\right)_J & \text{if } (N(\mathfrak{p}),d'_j)=1. \end{cases}$$

where $\mathfrak{p}$ is a prime ideal and $d'_j=\dfrac{d}{d_j}$ and called a *genus character*.

From now on, let $\chi_j(\mathfrak{p})$ denote $\chi_j([[\mathfrak{p}]])$ for short.

Proposition 5.5.2. *The character $\chi_j : Cl^+_{gen} \longrightarrow \mathbb{Z}/2\mathbb{Z}$ is well defined.*

Proof. To show that $(N(\mathfrak{p}),d_j)=(N(\mathfrak{p}),d'_j)=1$ implies $\left(\frac{d_j}{N(\mathfrak{p})}\right)_J = \left(\frac{d'_j}{N(\mathfrak{p})}\right)_J$, consider all the cases for $\mathfrak{p}$. Note that here $\mathfrak{p}\nmid d$.

Case 1. If $\mathfrak{p}=(p)$, that is if p is inert in k, then $N(\mathfrak{p})=p^2$, so $\left(\frac{d_j}{N(\mathfrak{p})}\right)_J =$

$$\left(\frac{d_j}{p^2}\right)_J = \left(\frac{d_j}{p}\right)\left(\frac{d_j}{p}\right) = \left[\left(\frac{d_j}{p}\right)\right]^2 = +1 = \left[\left(\frac{d'_j}{p}\right)\right]^2 = \left(\frac{d'_j}{p}\right)\left(\frac{d'_j}{p}\right) = \left(\frac{d'_j}{p^2}\right)_J = \left(\frac{d'_j}{N(\mathfrak{p})}\right)_J.$$

Case 2. If $\mathfrak{p}\mathfrak{p}^\sigma = (p) = N(\mathfrak{p})$, that is if p splits in k, then by Theorem 4.2.7 $\left(\frac{d}{p}\right) = 1$. Thus, $\left(\frac{d}{p}\right) = \left(\frac{d_i}{p}\right)\left(\frac{d'_i}{p}\right) = \left(\frac{d_j}{N(\mathfrak{p})}\right)\left(\frac{d'_j}{N(\mathfrak{p})}\right) = 1$, which gives that $\left(\frac{d_j}{N(\mathfrak{p})}\right)_J = \left(\frac{d'_j}{N(\mathfrak{p})}\right)_J = 1$ or $\left(\frac{d_j}{N(\mathfrak{p})}\right)_J = \left(\frac{d'_j}{N(\mathfrak{p})}\right)_J = -1$. □

Definition 5.5.3. Let $\mathfrak{a}$ be a fractional ideal and α an element of k. Then we define $\chi_j(\mathfrak{a})$ multiplicatively and $\chi_j(\alpha) = \chi_j((\alpha))$.

Lemma 5.5.4. *Let k be a quadratic number field and $\lambda \in k$ with $\lambda >> 0$. Then $\chi_j(\lambda) = 1$ for all $j = 1, 2, \ldots, t$.*

Proof. Let us prove the lemma first for λ and j with $(N(\lambda), d_j) = 1$.

Case 1. $d_j \equiv 1 \mod 4$.

Let $\lambda = \frac{1}{2}(a + b\sqrt{d})$, so $N(\lambda) = \frac{1}{4}(a^2 - db^2)$, then $4N(\lambda) = a^2 - db^2$. Here, $d_j \mid d$, but $d_j \nmid N(\lambda)$. So $d_j \nmid a$ and $N(\lambda) \equiv (\frac{a}{2})^2 \mod d_j$. Then $\chi_j(\lambda) = \left(\frac{d_j}{N(\lambda)}\right)_J = \left(\frac{N(\lambda)}{d_j}\right)_J$ by Quadratic Reciprocity Law 5.4.2 since $d_j \equiv 1 \mod 4$. Here, $\left(\frac{N(\lambda)}{d_j}\right)_J = 1$ since $N(\lambda)$ is a square modulo d_j. Also, $\left(\frac{d_j}{N(\lambda)}\right)_J$ is defined since $N(\lambda) > 0$, because $\lambda >> 0$.

Case 2. $d_j = -4$.

In this case, we must have $d = 4m$ with $m \equiv 3 \mod 4$. Let $\lambda = a + b\sqrt{m}$, so $N(\lambda) = a^2 - mb^2 \equiv a^2 + b^2 \mod 4$. Since $(N(\lambda), d_j) = 1$, $N(\lambda)$ must be odd. Thus $N(\lambda) \equiv 1 \mod 4$, since it is a sum of two squares modulo 4 by [6]. Thus $\chi_j(\lambda) = \left(\frac{d_j}{N(\lambda)}\right)_J = \left(\frac{-1}{N(\lambda)}\right)_J = (-1)^{\frac{N(\lambda)-1}{2}} = +1$ by Quadratic Reciprocity Law 5.4.2.

Case 3. $d_j = 8$.

If $d_j = 8$, then $d = 4m$ with $m \equiv 2 \mod 4$. Let $\lambda = a + b\sqrt{m}$, so $N(\lambda) = a^2 - mb^2 \equiv$

$a^2 - 2b^2 \equiv \mp 1 \mod 8$ by Appendix A.0.11 since $N(\lambda)$ is odd. So by Quadratic Reciprocity Law 5.4.2, $\chi_j(\lambda) = \left(\frac{d_j}{N(\lambda)}\right)_J = \left(\frac{2}{N(\lambda)}\right)_J = +1$.
If $d_j = -8$, then again by Quadratic Reciprocity Law 5.4.2, $\chi_j(\lambda) = \left(\frac{d_j}{N(\lambda)}\right)_J = \left(\frac{-1}{N(\lambda)}\right)_J \left(\frac{2}{N(\lambda)}\right)_J$. Again $N(\lambda)$ is odd. So if $N(\lambda) \equiv 3 \mod 4$, then $\chi_j(\lambda) = (-1)\cdot(-1) = +1$. But if $N(\lambda) \equiv 1 \mod 4$, then $\chi_j(\lambda) = (+1)\cdot(+1) = +1$.

Now to prove the lemma for an arbitrary $\lambda \in \mathfrak{O}$, not necessarily $(N(\lambda), d_j) = 1$, we will consider the ideal (λ) as $(\lambda) = \mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_t\mathfrak{b}$ where $\mathfrak{b}$ is relatively prime to d and $\mathfrak{p}_i$'s are prime ideals that divide d, that is $\mathfrak{p}_i$'s are ramified. For each $i = 1, 2, \ldots, t$, choose an ideal $\mathfrak{a}_i \in [\mathfrak{p}_i]_+^{-1}$ such that $(\mathfrak{a}_i, d) = 1$, so $\mathfrak{a}_i \sim^+ \mathfrak{p}_i^{-1}$ implies $\mathfrak{a}_i = \alpha_i\mathfrak{p}_i^{-1}$ with $\alpha_i >> 0$, so $\mathfrak{a}_i\mathfrak{p}_i = (\alpha_i)$ with $\alpha_i >> 0$. Here for the factorization of the principle ideal $(\alpha_i) = \prod \mathfrak{p}_\mathfrak{j}^{a_j}$ there exists only one ramified prime ideal, namely $\mathfrak{p}_i$, so $(\alpha, d_j) = 1$ or $(\alpha, d_j') = 1$ implies $\chi_j(\mathfrak{a}_i\mathfrak{p}_i) = \chi_j\alpha_i = 1$ for all $j = 1, 2, \ldots, s$ since $\alpha_i >> 0$ with $(\alpha_i, d_j) = 1$ without loss of generality.

$$(\lambda) = \mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_s\mathfrak{b} = \prod_{i=1}^{s}(\mathfrak{a}_i\mathfrak{p}_i)(\mathfrak{b}\prod_{i=1}^{s}(\mathfrak{a}_i)^{-1}) = \prod_{i=1}^{s}(\alpha_i)(\mathfrak{b}\prod_{i=1}^{s}(\mathfrak{a}_i)^{-1}),$$

so $\mathfrak{c} = (\mathfrak{b}\prod_{i=1}^{s}(\mathfrak{a}_i)^{-1})$ must also be a principle ideal which is relatively prime to d by the way we have chosen $\mathfrak{a}_i$'s. Thus, by the first part of our proof again we get $\chi_j(\mathfrak{c}) = \left(\frac{d_j}{N(\mathfrak{c})}\right)_J = +1$. Therefore, $\chi_j(\lambda) = +1$ for all $j = 1, 2, \ldots, s$. For an arbitrary $\lambda \in k$, we can use the multiplicativity of χ_j. □

Corollary 5.5.5. *For ideals $\mathfrak{a}, \mathfrak{b}$ in $\mathfrak{O}$, if $\mathfrak{a} \approx^+ \mathfrak{b}$, then $\chi_j(\mathfrak{a}) = \chi_j(\mathfrak{b})$ for all $j = 1, 2, \ldots, s$.*

Proof. If $\mathfrak{a} \approx^+ \mathfrak{b}$, then $N(\mathfrak{a}) = N(\lambda)N(\mathfrak{b})$ with $\lambda >> 0$, then $\chi_j(\mathfrak{a}) = \left(\frac{d_j}{N(\mathfrak{a})}\right)_J = \left(\frac{d_j}{N(\lambda)N(\mathfrak{b})}\right)_J = \left(\frac{d_j}{N(\lambda)}\right)_J \left(\frac{d_j}{N(\mathfrak{b})}\right)_J = \chi_j(\lambda)\chi_j(\mathfrak{b}) = \chi_j(\mathfrak{b})$ since $\chi_j(\lambda) = 1$ by Lemma 5.5.4. □

Theorem 5.5.6. ***(Product Formula)*** $\prod_{j=1}^{s}\chi_j = 1$

Proof. We want to show that $\prod_{j=1}^{s} \chi_j(\mathfrak{p}) = 1$ for an arbitrary prime ideal $\mathfrak{p}$.

Case 1. If $\mathfrak{p} \nmid d$, then we have two possibilities. If $N(\mathfrak{p}) = p^2$, then $\chi_j(\mathfrak{p}) = \left(\frac{d_j}{N(\mathfrak{p})}\right)_J = +1$ for all j. But if $N(\mathfrak{p}) = p$, then p splits, so $\prod_{j=1}^{s} \chi_j(\mathfrak{p}) = \prod_{j=1}^{s} \left(\frac{d_j}{N(\mathfrak{p})}\right)_J = \left(\frac{\prod_{j=1}^{s} d_j}{N(\mathfrak{p})}\right)_J = \left(\frac{d}{N(\mathfrak{p})}\right)_J = \left(\frac{d}{p}\right) = +1.$

Case 2. If $\mathfrak{p} \mid d$, then say without loss of generality say $\mathfrak{p} \mid d_1$, so $\prod_{j=1}^{t} \chi_j(\mathfrak{p}) = \left(\frac{d_1'}{N(\mathfrak{p})}\right)_J \left(\frac{d_2}{N(\mathfrak{p})}\right)_J \dots \left(\frac{d_t}{N(\mathfrak{p})}\right)_J$ where $d_1' = \frac{d}{d_1} = d_2 \dots d_t$. Thus,

$$\begin{aligned} \prod_{j=1}^{t} \chi_j(\mathfrak{p}) &= \left(\frac{d_2 \dots d_t}{N(\mathfrak{p})}\right)_J \left(\frac{d_2}{N(\mathfrak{p})}\right)_J \dots \left(\frac{d_t}{N(\mathfrak{p})}\right)_J \\ &= \left(\frac{d_2 \dots d_t}{N(\mathfrak{p})}\right)_J^2 \\ &= +1. \end{aligned}$$

□

Now, let $\chi_j(\mathfrak{c})$ denote $\chi_j([\mathfrak{c}]_+)$ for short.

Theorem 5.5.7. ***(Principle Genus Theorem)*** *Let $\mathfrak{c}$ be in $Cl^+(k)$. If $\chi_1(\mathfrak{c}) = \chi_2(\mathfrak{c}) = \dots = \chi_s(\mathfrak{c}) = +1$, then $\mathfrak{c} = \mathfrak{a}^2$ for some ideal class $\mathfrak{a}$ in $Cl^+(k)$.*

Proof. Let $\mathfrak{c} = [\mathfrak{a}]_+$ be an ideal class with $\chi_1(\mathfrak{a}) = \chi_2(\mathfrak{a}) = \dots = \chi_t(\mathfrak{a}) = +1$. We want to show that $\mathfrak{c} = [\mathfrak{a}]_+ = \mathfrak{a}^2$ for some ideal class $\mathfrak{a}$, that is $\mathfrak{a} \approx^+ \mathfrak{1}$, in other words $N(\mathfrak{a}) = N(\lambda)$ for some $\lambda \in k$ with $\lambda >> 0$. Let us choose $\mathfrak{a}$ in that way:

- $(\mathfrak{a}, 2d) = 1$,
- $z \nmid \mathfrak{a}$ for any $z \in \mathbb{Z}$,
- $\mathfrak{a}$ is square free.

For $n = N(\mathfrak{a})$, we want to show that $x^2 - dy^2 = nz^2$ has a solution in integers, because we want to find the number λ satisfying $N(\mathfrak{a}) = N(\lambda)$ by taking $\lambda = \frac{x}{z} + \frac{y}{z}\sqrt{d}$. To do that, we will show that this equation satisfies the conditions of Legendre's Theorem (See Appendix B.0.20).

Let $a = 1$, $b = -d$, $c = -n$. Here $a, b, c \in \mathbb{Z}$ such that $(1, -d) = (1, -n) = (-d, -n) = 1$, because $(\mathfrak{a}, 2d) = 1$ implies $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_t$ where $\mathfrak{p}_i$ is not ramified, so for all $p_i \mid n$, we get that $p_i \nmid d$. Furthermore, $(p_i) = \mathfrak{p}_i$ or $(p_i) = \mathfrak{p}_i\mathfrak{p}_i'$.

Now we will show that these congruences are solvable:

$$\begin{aligned} u^2 &\equiv -(-d)(-n) \qquad \text{mod } 1 \\ v^2 &\equiv -(-n)(1) \qquad \text{mod } -d \\ w^2 &\equiv -(-d)(1) \qquad \text{mod } -n \end{aligned}$$

There is no need to check the first congruence. The second congruence $v^2 \equiv n \mod -d$ is solvable by hypothesis of the theorem, because $\chi_1(c) = \chi_2(c) = \dots = \chi_t(c) = 1$ implies $\left(\frac{d_1}{n}\right)_J = \left(\frac{d_2}{n}\right)_J = \dots = \left(\frac{d_t}{n}\right)_J = 1$. The third congruence $w^2 \equiv d \mod -n$ is solvable since $(p_i) = \mathfrak{p}_i$ or $(p_i) = \mathfrak{p}_i\mathfrak{p}_i'$ for every $p_i \mid n$ implies $\left(\frac{d}{p_i}\right) = 1$, so $\left(\frac{d}{n}\right)_J = 1$. This completes the proof. □

Theorem 5.5.8. *Let k be a quadratic field and d be its discriminant with its decomposition into prime discriminants $d = d_1 d_2 \dots d_s$. Then the homomorphism defined by*

$$\begin{aligned} \Upsilon \;:\; Cl^+(k) &\longrightarrow (\mathbb{Z}/2\mathbb{Z})^s \\ \mathfrak{c} &\mapsto (\chi_1(\mathfrak{c}), \dots, \chi_s(\mathfrak{c})) \end{aligned}$$

induces an isomorphism $Cl^+_{gen}(k) \simeq (\mathbb{Z}/2\mathbb{Z})^{s-1}$.

Proof. Υ is a homomorphism by multiplicativity. Now define

$$\begin{array}{rccc} \Pi & : & (\mathbb{Z}/2\mathbb{Z})^s & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \\ & & (\varepsilon_1, \ldots, \varepsilon_t) & \mapsto & \prod_{i=1}^{s} \varepsilon_i \end{array}$$

where $\varepsilon_i \in \{-1, +1\}$. To show the isomorphism, we will prove that the sequence

$$1 \longrightarrow Cl^+(k)^2 \xrightarrow{i} Cl^+(k) \xrightarrow{\Upsilon} (\mathbb{Z}/2\mathbb{Z})^s \xrightarrow{\Pi} \mathbb{Z}/2\mathbb{Z}$$

Figure 5.5. Exact sequence to decide the class number

is exact. Since i is the identity function, it is one to one, so we have exactness at $Cl^+(k)^2$.

$\mathrm{Im}\,(i) = Cl^+(k)^2 \subseteq \mathrm{Ker}\,(\Upsilon)$ since $\chi_i(\mathfrak{c}^2) = (\chi_i(\mathfrak{c}))^2 = (\mp 1)^2 = +1$ for all $i = 1, 2, \ldots, s$. Conversely, $\mathrm{Ker}\,(\Upsilon) \subseteq \mathrm{Im}\,(i) = Cl^+(k)^2$, because $\mathfrak{c} \in \mathrm{Ker}\,(\Upsilon)$ means $\chi_1(\mathfrak{c}) = \chi_2(\mathfrak{c}) = \ldots = \chi_s(\mathfrak{c}) = +1$ and this implies $\mathfrak{c} = \mathfrak{a}^2$ for some ideal class $\mathfrak{a}$ by Principle Genus Theorem 5.5.7, so $\mathfrak{c} \in \mathrm{Im}\,(i) = Cl^+(k)^2$ and we have exactness at $Cl^+(k)$.

$\mathrm{Im}\,(\Upsilon) \subseteq \mathrm{Ker}\,(\Pi)$ by Product Formula 5.5.6 and conversely,

$$\begin{array}{lcll} (\mathbb{Z}/2\mathbb{Z})^{s-1} & \simeq & Cl^+(k)/Cl^+(k)^2 & \text{by Theorem 5.3.7,} \\ & = & Cl^+(k)/\mathrm{Ker}\,(\Upsilon) & \text{by the exactness at } Cl^+(k), \\ & \simeq & \mathrm{Im}\,(\Upsilon) & \text{by the Main Isomorphism Theorem,} \\ & \subseteq & \mathrm{Ker}\,(\Pi) & \text{by the above result of Product Formula,} \\ & \simeq & (\mathbb{Z}/2\mathbb{Z})^{s-1} & \end{array}$$

forces that $\mathrm{Im}\,(\Upsilon) = \mathrm{Ker}\,(\Pi)$ and we have exactness at $(\mathbb{Z}/2\mathbb{Z})^s$. □

Definition 5.5.9. Let k be a quadratic number field with discriminant d and $d = d_1 \ldots d_s$ be its factorization into prime discriminants. Then the field $K = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_s})$ is called the *genus field* and denoted by k_{gen}.

Proposition 5.5.10. *Let k be a quadratic number field. Then there exists a canonical isomorphism $Cl^{+}_{gen}(k) \simeq Gal(k_{gen}/k)$.*

Proof. We define a map $\Gamma : Cl^{+}_{gen}(k) \longrightarrow Gal(k_{gen}/k)$ that maps each $[\mathfrak{c}]_{+} \in Cl^{+}_{gen}(k)$ to the automorphism $\sigma \in Gal(k_{gen}/k)$ which is defined as $\sigma : \sqrt{d_i} \mapsto \chi_i(\mathfrak{c})\sqrt{d_i}$ where $\chi_i(\mathfrak{c}) \in \{-1, +1\}$. For short, let $\Gamma(\mathfrak{c})$ denote $\Gamma([\mathfrak{c}]_{+})$. Here σ's are really in $Gal(k_{gen}/k)$ since $\sigma(\sqrt{d}) = \sigma(\prod \sqrt{d_i}) = \prod(\sigma(\sqrt{d_i})) = \prod \chi_i(\mathfrak{c})\sqrt{d_i} = \prod \sqrt{d_i} = \sqrt{d}$ by Product Formula 5.5.6. Thus, σ's fix k.

We have $\mathfrak{G}(\mathfrak{c}_1\mathfrak{c}_2) = \sigma_3 : \sqrt{d_i} \mapsto \chi_i(\mathfrak{c}_3)\sqrt{d_i}$ for $\mathfrak{c}_3 = \mathfrak{c}_1\mathfrak{c}_2$ and $\mathfrak{G}(\mathfrak{c}_1)\mathfrak{G}(\mathfrak{c}_2) = \sigma_1\sigma_2$ where $\sigma_1 : \sqrt{d_i} \mapsto \chi_i(\mathfrak{c}_1)\sqrt{d_i}$ and $\sigma_2 : \sqrt{d_i} \mapsto \chi_i(\mathfrak{c}_2)\sqrt{d_i}$, so

$$\sqrt{d_i} \overset{\sigma_1}{\mapsto} \chi_i(\mathfrak{c}_1)\sqrt{d_i} \overset{\sigma_2}{\mapsto} \chi_i(\mathfrak{c}_2)(\chi_i(\mathfrak{c}_1)\sqrt{d_i}) = \chi_i(\mathfrak{c}_1\mathfrak{c}_2)\sqrt{d_i}.$$

Thus $\sigma_1\sigma_2 = \sigma_3$ and Γ is a homomorphism.

Let $\sigma \in Gal(k_{gen}/k)$ such that $\sigma : \sqrt{d_i} \mapsto \varepsilon_i\sqrt{d_i}$ where $\varepsilon_i \in \{-1, +1\}$. Since σ fixes $k = \mathbb{Q}(\sqrt{d})$, we have $\sigma(\sqrt{d}) = \sqrt{d}$, so $\sigma(\prod \sqrt{d_i}) = \prod \sqrt{d_i}$ implies $\prod \varepsilon_i = 1$ for all $\sigma \in Gal(k_{gen}/k)$ and therefore for each σ, there exists a unique class that represents a genus in $Cl^{+}_{gen}(k)$ such that for $\mathfrak{c} \in Cl^{+}(k)$ in that class $\chi_i(\mathfrak{c}) = \varepsilon_i$ by Theorem 5.5.8. Thus Γ is one to one and onto. □

6. QUADRATIC RECIPROCITY LAW BY DIRICHLET FIELDS

In this chapter, we will present biquadratic reciprocity law which is based on the theory of Dirichlet number fields. We will define the relative Hilbert symbol for quadratic number fields over $\mathbb{Q}(i)$ and find the number of genera of a Dirichlet number field by using the parallel arguments in Chapter 4. The number of genera will lead us to prove the biquadratic reciprocity law.

6.1. The Integers in the Dirichlet Number Field

In this chapter, we will denote the quadratic number field $\mathbb{Q}(i)$ by k, and its ring of integers $\mathbb{Z}[i]$ by $\mathfrak{o}$.

Let $\delta \in \mathfrak{o}$ be squarefree, $\delta \neq \mp 1$, then the biquadratic number field $k(\sqrt{\delta})$ over $\mathbb{Q}$ is called a *Dirichlet number field*. We will denote the ring of integers in $k(\sqrt{\delta})$ by $\mathfrak{O}$.

Every number $A \in k(\sqrt{\delta})$ can be brought into the form $\dfrac{\alpha+\beta\sqrt{\delta}}{\gamma}$ where the numbers $\alpha, \beta, \gamma \in \mathfrak{o}$.

We will denote the operation that changes $\sqrt{\delta}$ to $-\sqrt{\delta}$ by S, so for $A = \dfrac{\alpha+\beta\sqrt{\delta}}{\gamma}$, $\mathsf{S}A = \dfrac{\alpha-\beta\sqrt{\delta}}{\gamma}$.

For $A \in \mathfrak{O}$, we have $A + \mathsf{S}A = \dfrac{2\alpha}{\gamma} \in \mathfrak{o}$ and $A \cdot \mathsf{S}A = \dfrac{\alpha^2-\beta^2\delta}{\gamma^2} \in \mathfrak{o}$. Now we are going to determine the elements of $\mathfrak{O}$.

For $A = \dfrac{\alpha+\beta\sqrt{\delta}}{\gamma}$, let $\lambda \in k$ be a prime number with $\lambda \neq 1+i$ and $\lambda \mid \gamma$. Then $\frac{2\alpha}{\gamma} \in \mathfrak{o}$ implies $\lambda \mid \alpha$ since $\lambda \neq 1+i$. Also $\lambda^2 \mid \gamma^2$ and $\lambda^2 \mid \beta^2$ implies $\lambda \mid \beta$ since $\frac{\alpha^2-\beta^2\delta}{\gamma^2} \in \mathfrak{o}$ and δ is squarefree, then $\lambda \mid \beta$; so λ divides both the numerator and the denominator of A. Thus, λ can not appear on the denominator of A.

Let $(1+i)^3 \mid \gamma$, then $1+i \mid \alpha$ and $1+i \mid \beta$ since $(1+i)^2 \mid 2$ in $A + \mathsf{S}A = \dfrac{2\alpha}{\gamma}$, so $1+i$ divides both the numerator and the denominator of A. Thus, $(1+i)^3$ can not appear on the denominator of A.

If $\gamma = 2$, then $4 \mid \alpha^2 - \beta^2\delta$ since $A \cdot \mathsf{S}A = \dfrac{\alpha^2 - \beta^2\delta}{\gamma^2}$ and $\gamma^2 = 2^2 = 4$. If $1+i \mid \beta$ then $1+i \mid \alpha$, so $1+i$ divides both the numerator and the denominator of A. If $1+i \nmid \beta$ then $\delta \equiv \dfrac{\alpha^2}{\beta^2} \mod 4$, that means δ is a quadratic residue modulo 4 in the field k.

If $\gamma = 1+i$, then $2 \mid \alpha^2 - \beta^2\delta$ since $A \cdot \mathsf{S}A = \dfrac{\alpha^2 - \beta^2\delta}{\gamma^2}$ and $\gamma^2 = (1+i)^2 = 2i$. If $1+i \mid \beta$ then $1+i \mid \alpha$, so $1+i$ divides both the numerator and the denominator of A. If $1+i$ does not divide β then $\delta \equiv \dfrac{\alpha^2}{\beta^2} \mod 2$, that means δ is a quadratic residue modulo 2 in the field k.

Note that:

i) δ is a quadratic residue modulo 4 when $\delta \equiv \mp 1 \mod 4$.

ii) δ is a quadratic residue modulo 2, but a quadratic non-residue modulo 4 when $\delta \equiv \mp 3 + 2i \mod 4$.

iii) δ is a non-quadratic residue modulo 2 for all other cases, that is when $\delta \equiv i \mod 2$ and $\delta \equiv 0 \mod 1+i$, as we may see from the computations in Appendix A.0.12.

Thus we get the following result:

Theorem 6.1.1. *The $\mathbb{Z}$-basis of the ring of integers $\mathfrak{O}$ in the Dirichlet number field $k(\sqrt{\delta})$ is $\{1, i, \Omega, i\Omega\}$ where Ω is defined as following,*

$$\begin{aligned}
\Omega &= \frac{1+\sqrt{\delta}}{2}, \quad if \quad \delta \equiv 1 && \mod 4 \\
\Omega &= \frac{1+\sqrt{\delta}}{1+i}, \quad if \quad \delta \equiv 3+2i && \mod 4 \\
\Omega &= 1+\sqrt{\delta}, \quad if \quad \delta \equiv i && \mod 2 \\
\Omega &= \sqrt{\delta}, \quad if \quad \delta \equiv 0 && \mod 1+i.
\end{aligned}$$

We denote the relative discriminant of $k(\sqrt{\delta})$ *over* k *by* $disc_k(k(\sqrt{\delta}))$*, then*

$$\begin{aligned}
disc_k(k(\sqrt{\delta})) &= \delta, \quad if \quad \delta \equiv 1 && \mod 4 \\
disc_k(k(\sqrt{\delta})) &= -2i\delta, \quad if \quad \delta \equiv 3+2i && \mod 4 \\
disc_k(k(\sqrt{\delta})) &= 4\delta, \quad if \quad \delta \equiv i && \mod 2 \\
disc_k(k(\sqrt{\delta})) &= 4\delta, \quad if \quad \delta \equiv 0 && \mod 1+i,
\end{aligned}$$

where the computations are done in Appendix A.0.13.

The usual discriminant $\mathrm{disc}_{\mathbb{Q}}(k(\sqrt{\delta}))$ of the biquadratic field is $2^4|\mathrm{disc}_k(k(\sqrt{\delta}))|^2$ by Appendix A.0.13.

6.2. The Prime Ideals of Dirichlet Fields

We will first consider the prime numbers in k which are different from $1+i$ and do not divide δ. There are two kinds of such primes:

i) a prime number $\pi \in k$ such that δ is a quadratic residue modulo π in k,

ii) a prime number $\kappa \in k$ such that δ is a quadratic non-residue modulo κ in k.

Lemma 6.2.1. *If* $\pi \in k$ *is a prime number with* $\pi \neq 1+i$ *and if* δ *is a quadratic residue modulo* π*, then* π *is reducible into two different prime ideals in* $k(\sqrt{\delta})$*.*

Proof. Let $\pi \in k$ be a prime number with $\pi \neq 1+i$ such that δ is a quadratic residue modulo π in k. Then $\delta \equiv \eta^2 \mod \pi$ for some number $\eta \in \mathfrak{o}$, and

$$\begin{aligned}(\pi, \eta+\sqrt{\delta})(\pi, \eta-\sqrt{\delta}) &= (\pi\pi, [\eta+\sqrt{\delta}]\pi, \pi[\eta-\sqrt{\delta}], [\eta+\sqrt{\delta}][\eta-\sqrt{\delta}]) \\ &= (\pi^2, \pi[\eta+\sqrt{\delta}], \pi[\eta-\sqrt{\delta}], \eta^2-\delta) \\ &= \pi, \text{ since } \pi \text{ and } (\eta+\sqrt{\delta})+(\eta-\sqrt{\delta}) = 2\eta \\ &\quad \text{are in } (\pi, \eta+\sqrt{\delta}, \eta-\sqrt{\delta}, \frac{\eta^2-\delta}{\pi}), \text{ and } (\pi, 2\eta) = 1.\end{aligned}$$

Thus we have the desired result, $\pi = \mathfrak{B}\cdot\mathsf{S}(\mathfrak{B})$ where $\mathfrak{B} = (\pi, \eta+\sqrt{\delta})$ with $(\pi, \eta+\sqrt{\delta}) \neq (\pi, \eta-\sqrt{\delta})$, so $\mathfrak{B} \neq \mathsf{S}(\mathfrak{B})$. □

Lemma 6.2.2. *If $\kappa \in k$ is a prime number with $\pi \neq 1+i$ and if δ is a quadratic non-residue modulo κ, then κ is a prime number in $k(\sqrt{\delta})$.*

Proof. Let $\kappa \in k$ be a prime number with $\pi \neq 1+i$ such that δ is a quadratic non-residue modulo κ in k. If κ is reducible, say $\kappa = \mathfrak{P}\mathfrak{Q}$ for some ideals $\mathfrak{P}, \mathfrak{Q}$ in k, then we can find an integer $A = \alpha + \beta\sqrt{\delta} \in \mathfrak{O}$ such that $\kappa \nmid A$, but one of its prime ideal divisors in K divides A, say $\mathfrak{P} \mid A$ without loss of generality. Necessarily $(\beta, \kappa) = 1$, because if not $(\beta, \kappa) = \kappa$ since κ is prime, then $\kappa \mid \beta^2$; also $\kappa \mid A.\mathsf{S}(A) = \alpha^2 - \beta^2\delta$ since $\mathsf{S}\mathfrak{P} = \mathfrak{Q}$ and therefore $\kappa \mid \alpha^2$, $\kappa \mid \alpha$, thus $\kappa \mid A$ which contradicts our assumption that $\kappa \nmid A$. Again by using the fact that $\kappa \mid A.\mathsf{S}A$, we get $\alpha^2 - \beta^2\delta \equiv 0 \mod \kappa$ where $(\beta, \kappa) = 1$, so $\delta \equiv (\frac{\alpha}{\beta})^2 \mod \kappa$ which contradicts our hypothesis that δ is a quadratic non-residue modulo κ in k. □

Now we will consider the prime numbers in k which are different from $1+i$ and divide δ:

Let $\lambda_1, \lambda_2, \ldots, \lambda_r$ denote the prime numbers in k different from $1+i$ that divide δ. Then $\delta = \lambda_1\lambda_2\ldots\lambda_r$ or $\delta = (1+i)\lambda_1\lambda_2\ldots\lambda_r$.

Lemma 6.2.3. *Let λ be a prime number in k. Then the ideal $(\lambda, \sqrt{\delta})$ is a prime ideal in $k(\sqrt{\delta})$.*

Proof. Let λ be a prime number in k, and $\mathfrak{L} = (\lambda, \sqrt{\delta}) = \mathfrak{P}\mathfrak{Q}$ for some ideals $\mathfrak{P}, \mathfrak{Q}$ in $k(\sqrt{\delta})$. Then, $N_{k(\sqrt{\delta})/k}(\mathfrak{P})$ and $N_{k(\sqrt{\delta})/k}(\mathfrak{Q})$ divides $N_{k(\sqrt{\delta})/k}(\mathfrak{L}) = (\lambda, \sqrt{\delta})(\lambda, -\sqrt{\delta}) = (\lambda^2, \lambda\sqrt{\delta}, \delta) = \lambda(\lambda, \sqrt{\delta}, \frac{\delta}{\lambda}) = \lambda$ since $(\lambda, \frac{\delta}{\lambda}) = 1$. Since $\lambda \in k$ is prime, $\mathfrak{P} = \mathfrak{O}$ or $\mathfrak{Q} = \mathfrak{O}$, therefore $\mathfrak{L}$ is a prime ideal. □

Lemma 6.2.4. *If $\lambda \in k$ is a prime number with $\lambda \neq 1 + i$ and if $\lambda \mid \delta$, then λ is reducible into two prime ideals in $k(\sqrt{\delta})$, say $\lambda = \mathfrak{L}.\mathsf{S}\mathfrak{L}$ where $\mathfrak{L}$, $\mathsf{S}\mathfrak{L}$ are prime ideals in $k(\sqrt{\delta})$ and $\mathfrak{L} = \mathsf{S}\mathfrak{L}$.*

Proof. Consider the ideals

$$\mathfrak{L}_1 = \mathsf{S}\mathfrak{L}_1 = (\lambda_1, \sqrt{\delta}), \mathfrak{L}_2 = \mathsf{S}\mathfrak{L}_2 = (\lambda_2, \sqrt{\delta}), \ldots, \mathfrak{L}_r = \mathsf{S}\mathfrak{L}_r = (\lambda_r, \sqrt{\delta}).$$

Then the ideals $\mathfrak{L}_1, \mathfrak{L}_2, \ldots, \mathfrak{L}_r$ are prime ideals in $k(\sqrt{\delta})$ by Lemma 6.2.3 and $\lambda_1 = {\mathfrak{L}_1}^2, \lambda_2 = {\mathfrak{L}_2}^2, \ldots, \lambda_r = {\mathfrak{L}_r}^2$.

□

Lastly we will consider the prime number $1 + i$:

Lemma 6.2.5. *If $\delta \equiv 1 + 4i \mod (1 + i)^5$ then $1 + i$ is irreducible in $\mathfrak{O}$.*

If $\delta \equiv 1 \mod (1 + i)^5$ then $1 + i = \mathfrak{B}.\mathcal{S}\mathfrak{B}$ where $\mathfrak{B} \neq \mathcal{S}\mathfrak{B}$.

If $\delta \equiv 3 + 2i \mod 4$, $\delta \equiv 0 \mod 1 + i$ or $\delta \equiv i \mod 2$, that is if $1 + i \mid disc_k(k(\sqrt{\delta}))$, then $1 + i = \mathfrak{B}. \cdot \mathcal{S}\mathfrak{B}$ where $\mathfrak{B} = \mathcal{S}\mathfrak{B}$.

Proof. First let $\delta \equiv 1 \mod 4$. If also $\delta \equiv 1+4i \mod (1+i)^5$ then $1+i \neq (1+i, \Omega)(1+i, \mathsf{S}\Omega)$ since $\Omega = \frac{1+\sqrt{\delta}}{2}$ implies $\Omega\mathsf{S}\Omega = \frac{1-\delta}{4} = \frac{(1+4i)+(1+i)^5\xi}{4} = -i - (1+i)\xi$, $1 + i$ is irreducible.

But if $\delta \equiv 1 \mod (1 + i)^5$ then $1 + i = (1 + i, \Omega)(1 + i, \mathsf{S}\Omega) = \mathfrak{B} \cdot \mathsf{S}\mathfrak{B}$ since

$\Omega = \frac{1+\sqrt{\delta}}{2}$ implies $\Omega \cdot \mathsf{S}\Omega = \frac{1-\delta}{4} = \frac{(1+i)^5\xi}{-(1+i)^4} = (1+i)(-\xi)$ where $\mathfrak{B}, \mathsf{S}\mathfrak{B}$ are prime ideals in $k(\sqrt{\delta})$ by Lemma 6.2.3 with $\mathfrak{B} \neq \mathsf{S}\mathfrak{B}$.

If $\delta \equiv 3+2i \mod 4$ then $\Omega = \frac{1+\sqrt{\delta}}{1+i}$, so $\mathsf{S}\Omega = \frac{1-\sqrt{\delta}}{1+i} = \frac{2-(1+\sqrt{\delta})}{1+i} = \frac{2}{1+i} - \frac{1+\sqrt{\delta}}{1+i} = (1-i) - \Omega = (i+1)(-i) - \Omega$, thus $(1+i, \Omega) = (1+i, \mathsf{S}\Omega)$ and $1+i = (1+i,\Omega)(1+i,\mathsf{S}\Omega) = \mathfrak{B} \cdot \mathsf{S}\mathfrak{B}$ since $\Omega \cdot \mathsf{S}\Omega = \frac{1+\sqrt{\delta}}{1+i} \cdot \frac{1-\sqrt{\delta}}{1+i} = \frac{1-\delta}{2i} = \frac{1-3-2i+(1+i)\xi}{2i} = (i-1) - 2i\xi = (i+1) - (2+2i\xi) = (1+i) - 2(1+i\xi) = (1+i) + i(1+i)^2(1+i\xi) = (1+i)(1+i(1+i)(1+i\xi))$.

If $\delta \equiv i \mod 2$ then $\Omega = 1+\sqrt{\delta}$, so $\mathsf{S}\Omega = 1-\sqrt{\delta} = 2-(1+\sqrt{\delta}) = (1+i)(1-i)-\Omega$, thus $(1+i,\Omega) = (1+i,\mathsf{S}\Omega)$ and $1+i = (1+i,\Omega)(1+i,\mathsf{S}\Omega) = \mathfrak{B}\cdot\mathsf{S}\mathfrak{B}$ since $\Omega\cdot\mathsf{S}\Omega = (1+\sqrt{\delta})(1-\sqrt{\delta}) = 1-\delta = 1-i-2\xi = 1+i-2i-2\xi = (1+i)-2(i+\xi) = (1+i)+i(1+i)^2(i+\xi) = (1+i)(1+i(1+i)(i+\xi))$.

If $\delta \equiv 0 \mod 1+i$, then $\Omega = \sqrt{\delta}$, so $\mathsf{S}\Omega = -\sqrt{\delta} = -\Omega$, thus $(1+i,\Omega) = (1+i,\mathsf{S}\Omega)$ and $1+i = (1+i,\Omega)(1+i,\mathsf{S}\Omega) = \mathfrak{B}\cdot\mathsf{S}\mathfrak{B}$ since $\Omega\cdot\mathsf{S}\Omega = (\sqrt{\delta})(-\sqrt{\delta}) = -\delta = -0-(1+i)\xi = (1+i)(\xi)$.

Hence, $1+i = \mathfrak{L}^2$ if and only if $1+i \mid d$. □

Now we get the following table:

Table 6.1. Decomposition of $1+i$ into its prime ideals in $k(\sqrt{\delta})$

$\delta \equiv 1 \mod (1+i)^5 \Rightarrow 1+i = \mathfrak{B}\mathsf{S}\mathfrak{B}, \mathfrak{B} = (1+i,\Omega), \mathfrak{B} \neq \mathsf{S}\mathfrak{B}$
$\delta \equiv 1+4i \mod (1+i)^5 \Rightarrow 1+i = \mathfrak{B}$ where $\mathfrak{B}$ is prime in K
$\delta \equiv 3+2i \mod 4 \Rightarrow 1+i = \mathfrak{L}^2$ where $\mathfrak{L} = \mathsf{S}\mathfrak{L} = (1+i,\Omega)$
$\delta \equiv i \mod 2 \Rightarrow 1+i = \mathfrak{L}^2$ where $\mathfrak{L} = \mathsf{S}\mathfrak{L} = (1+i,\Omega)$
$\delta \equiv 0 \mod 1+i \Rightarrow 1+i = \mathfrak{L}^2$ where $\mathfrak{L} = \mathsf{S}\mathfrak{L} = (1+i,\Omega)$

Definition 6.2.6. Let $\alpha \in k$ be arbitrary and $\tau \in k$ be a prime number. If $\tau \neq 1+i$, then

$$\left[\frac{\alpha}{\tau}\right] = \begin{cases} +1, & \text{if} \quad \alpha \text{ is a quadratic residue modulo } \tau \text{ in } k. \\ -1, & \text{if} \quad \alpha \text{ is a quadratic nonresidue modulo } \tau \text{ in } k. \\ 0, & \text{if} \quad \tau \mid \alpha. \end{cases}$$

If $\tau = 1+i$, then

$$\left[\frac{\alpha}{1+i}\right] = \begin{cases} +1, & \text{if} \quad \alpha \text{ is a quadratic residue modulo } (1+i)^5 \text{ in } k. \\ -1, & \text{if} \quad \alpha \text{ is a quadratic nonresidue modulo } (1+i)^5 \text{ in } k. \\ 0, & \text{if} \quad 1+i \mid \alpha. \end{cases}$$

We have the following theorem by combining Lemma 6.2.1, Lemma 6.2.2, Lemma 6.2.4, Lemma 6.2.5 and Definition 6.2.6 :

Theorem 6.2.7. *Let $k(\sqrt{\delta})$ be a Dirichlet number field over k and $d = disc_k(k(\sqrt{\delta}))$ be its relative discriminant. Let τ be a prime number in k.*

If $\left[\frac{d}{\tau}\right] = +1$, then τ is reducible into two different prime ideals in $k(\sqrt{\delta})$.

If $\left[\frac{d}{\tau}\right] = -1$, then τ is irreducible in $k(\sqrt{\delta})$.

If $\left[\frac{d}{\tau}\right] = 0$, then τ is equal to a square of a prime ideal in $k(\sqrt{\delta})$.

This theorem will be used repeatedly.

6.3. Relative Hilbert's Symbol

Let $A \in \mathfrak{O}$. We denote the relative norm of A by $N_{k(\sqrt{\delta})/k}(A) = A \cdot \mathsf{S}A$. This relative norm is a number in $\mathfrak{o}$.

Lemma 6.3.1. *Let* $A = \dfrac{\alpha+\beta\sqrt{\delta}}{\gamma} \in \mathfrak{O}$ *and* $\lambda \in k$ *be a prime number with* $\lambda \neq 1+i$ *and* $\lambda \mid \delta$*, but* λ *does not divide* $\alpha+\beta\sqrt{\delta}$ *and* γ *at the same time. Then* $N_{k(\sqrt{\delta})/k}(A)$ *is a quadratic residue modulo* λ*.*

Proof. For $A = \dfrac{\alpha+\beta\sqrt{\delta}}{\gamma}$, $N_{k(\sqrt{\delta})/k}(A) = \dfrac{\alpha^2-\beta^2\delta}{\gamma^2}$ implies $N_{k(\sqrt{\delta})/k}(A) \equiv \dfrac{\alpha^2}{\gamma^2} \equiv (\dfrac{\alpha}{\gamma})^2$ mod λ since $\lambda \mid \delta$. But we need to show that $\lambda \nmid \gamma$ and $\lambda \nmid \alpha$:

For $A = \dfrac{\alpha+\beta\sqrt{\delta}}{\gamma}$ with $\alpha, \beta, \gamma \in \mathfrak{o}$, firstly assume that $\lambda \mid \gamma$, so $\lambda^2 \mid \gamma^2$. Then $\lambda^2 \mid \alpha^2 - \beta^2\delta$ since $N_{k(\sqrt{\delta})/k}(A) \in \mathfrak{o}$. Furthermore, $\lambda \mid \delta$ and $\lambda \mid \alpha^2 - \beta^2\delta$ imply together that $\lambda \mid \alpha$. Also $\lambda^2 \mid \alpha^2$ and $\lambda \mid \delta$ imply together that $\lambda \mid \beta$. Thus λ divides both the numerator and the denominator of A which contradicts our hypothesis.

Now assume that $\lambda \mid \alpha$, so $\lambda \mid \alpha^2$. Then $\lambda \mid \alpha^2$ and $\lambda \mid \delta$ imply together that $\lambda \mid \alpha^2 - \beta^2\delta$. Then $\lambda \mid \gamma^2$ since $N_{k(\sqrt{\delta})/k}(A) \in \mathfrak{o}$. Therefore, $\lambda \mid \gamma$, so $\lambda^2 \mid \gamma^2$, and $\lambda^2 \mid \alpha^2 - \beta^2\delta$, together with $\lambda^2 \mid \alpha^2$ we have $\alpha \mid \beta$.Therefore, λ divides both the numerator and the denominator of A which contradicts our hypothesis. □

Lemma 6.3.2. *Let* $\lambda \in k$ *be a prime number with* $\lambda \mid \delta$ *and* $\sigma \in k$ *be arbitrary. Then there exist* $\alpha, A \in \mathfrak{o}$ *such that*

$$\sigma = \alpha \cdot \upsilon$$

where $\lambda \nmid \alpha$ *and* $\upsilon = N_{k(\sqrt{\delta})/k}(A)$*.*

Proof. If $\lambda \nmid \sigma$ then we are done. But if $\lambda \mid \sigma$ then $\sigma = \lambda^n\gamma$ for some $n \in \mathbb{N}$ where $\lambda \nmid \gamma$. So it is enough to prove the lemma for $\sigma = \lambda$. Since $\lambda \mid \delta$, $\lambda = \mathfrak{L}^2$ for some ideal $\mathfrak{L}$ in $k(\sqrt{\delta})$. Let $A \in k(\sqrt{\delta})$ be a number such that $\mathfrak{L} \mid A$, but $\lambda = \mathfrak{L}^2 \nmid A$. Put $\upsilon = N_{k(\sqrt{\delta})/k}(A)$. Then $\lambda \mid \upsilon$ and for $\alpha := \dfrac{\lambda}{\upsilon}$, the numerator is 1 and the denominator is $\frac{\upsilon}{\lambda}$, so not divisible by λ because if $\lambda \mid \dfrac{\upsilon}{\lambda}$, $\lambda^2 \mid \upsilon = N_{k(\sqrt{\delta})/k}(A)$, $\lambda \mid A$ which contradicts

our assumption that $\lambda = \mathfrak{L}^2 \nmid A$. Thus we get $\lambda = \alpha\upsilon$ where $\alpha \in \mathfrak{o}$ with $\lambda \nmid \alpha$, and $\upsilon = N_{k(\sqrt{\delta})/k}(A)$ for some number $A \in k(\sqrt{\delta})$. □

Definition 6.3.3. Let $k(\sqrt{\delta})$ be a Dirichlet number field over k. Let $\sigma \in k$ be arbitrary and $\lambda \in k$ be a prime number with $\lambda \neq 1+i$ and $\lambda \mid \delta$. We define the *relative Hilbert symbol* by:

$$\left[\frac{\sigma}{\lambda : \delta}\right] = \begin{cases} +1, & \text{if } \sigma = N_{k(\sqrt{\delta})/k}(A) \text{ for some number } A \in k(\sqrt{\delta}) \\ \left[\frac{\alpha}{\lambda}\right], & \text{if } \sigma = \alpha\upsilon \text{ for some } \alpha, \upsilon \in k \text{ where } \alpha \in \mathfrak{o} \text{ with} \\ & \lambda \nmid \alpha, \text{ and } \upsilon = N_{k(\sqrt{\delta})/k}(A) \text{ for some number } A \in k(\sqrt{\delta}). \end{cases}$$

But we need to show that this definition is well defined:

Lemma 6.3.4. *Let $\lambda \in k$ be a prime number with $\lambda \mid \delta$ and $\sigma \in k$ be arbitrary. If $\sigma = \alpha\upsilon = \alpha_1\upsilon_1$ where $\lambda \nmid \alpha, \alpha_1$ and $\upsilon = N_{k(\sqrt{\delta})/k}(A)$, $\upsilon_1 = N_{k(\sqrt{\delta})/k}(A_1)$ for some $A, A_1 \in \mathfrak{o}$, then $\left[\frac{\alpha}{\lambda}\right] = \left[\frac{\alpha_1}{\lambda}\right]$.*

Proof. If $\alpha\upsilon = \alpha_1\upsilon_1$, then $\dfrac{\alpha}{\alpha_1} = \dfrac{\upsilon_1}{\upsilon}$ where $\dfrac{\upsilon_1}{\upsilon} = \dfrac{N_{k(\sqrt{\delta})/k}(A_1)}{N_{k(\sqrt{\delta})/k}(A)} = N_{k(\sqrt{\delta})/k}(\dfrac{A_1}{A})$. Therefore, $\left[\frac{\frac{\alpha}{\alpha_1}}{\lambda}\right] = \left[\frac{\frac{\upsilon_1}{\upsilon}}{\lambda}\right] = \left[\dfrac{N_{k(\sqrt{\delta})/k}(\frac{A_1}{A})}{\lambda}\right] = +1$ by its definition, so $\left[\frac{\alpha}{\lambda}\right] = \left[\frac{\alpha_1}{\lambda}\right]$. □

Also we have the multiplicative property:

$$\left[\frac{\sigma\sigma'}{\lambda : \delta}\right] = \left[\frac{\sigma}{\lambda : \delta}\right]\left[\frac{\sigma'}{\lambda : \delta}\right]$$

If $1+i \mid \mathrm{disc}_k(k(\sqrt{\delta}))$, then we need to examine the relative norms and their residues modulo powers of $1+i$ to define the relative Hilbert symbol. We put $i' = 3+2i$, $i'' = 1+4i$ and give the values 0 or 1 to t, t', t'', so we get by the form $\mp i^t i'^{t'}$ the whole 8 residues modulo $(1+i)^4$ if $1+i \nmid \delta$ and by the form $\mp i^t i'^{t'} i''^{t''}$ the whole 16 residues modulo $(1+i)^5$ if $1+i \mid \delta$ which are relatively prime to $1+i$. Let us denote these numbers $(i)^t(i')^{t'}$ by (tt') and the numbers $(i)^t(i')^{t'}(i'')^{t''}$ by $(tt't'')$ for short.

If $\delta \equiv (00) \mod (1+i)^4$ then $\delta \equiv 1 \mod 4$, so $\mathrm{disc}_k(k(\sqrt{\delta})) = \delta$ and $1+i \nmid \mathrm{disc}_k(k(\sqrt{\delta}))$. So it is enough to check the 7 cases: $\delta \equiv (01), (10), (11) \mod (1+i)^4$ where $1+i \nmid \delta$ and $\delta \equiv (1+i)(00), (1+i)(10), (1+i)(01)$ and $(1+i)(11) \mod (1+i)^5$ where $1+i \mid \delta$.

Let $\alpha \equiv (t_\alpha {t'}_\alpha {t''}_\alpha) \mod (1+i)^5$ with $1+i \nmid \alpha$. To determine the value of the symbol $\left[\dfrac{\alpha}{1+i:\delta}\right]$, we have to investigate for which combinations of values of α and δ, the congruence $\alpha \equiv N_{k(\sqrt{\delta})/k}(A) \mod (1+i)^5$ is solvable for some $A \in \mathfrak{O}$. After long calculations in Appendix A.0.14, we get the following table.

Table 6.2. Table of $\alpha = N_{k(\sqrt{\delta})/k}(A) \mod (1+i)^5$

δ	α
(01)	(000),(001),(010),(011)
(1,0)	(000),(001),(101),(100)
(11)	(000),(001),(110),(111)
(1+i)(00)	(000),(011),(100),(111)
(1+i)(01)	(000),(011),(101),(110)
(1+i)(10)	(000),(010),(100),(110)
(1+i)(11)	(000),(010),(101), (111)

In general, for $\delta \equiv (t_\delta {t'}_\delta)$, respectively for $\delta \equiv (t_\delta {t'}_\delta {t''}_\delta)$, α is a relative norm of a number in $k(\sqrt{\delta})$ modulo $(1+i)^5$ where $\alpha \equiv (t_\alpha {t'}_\alpha {t''}_\alpha)$ if and only if $t_\alpha {t'}_\delta + {t'}_\alpha t_\delta$ is even, respectively $t_\alpha {t'}_\delta + {t'}_\alpha t_\delta + {t'}_\alpha + {t''}_\alpha$ is even. If it is the case, then α is a relative norm of a number in $k(\sqrt{\delta})$ modulo higher powers of $1+i$.

Definition 6.3.5. Let $k(\sqrt{\delta})$ be a Dirichlet number field over k. Let $\sigma \in k$ be arbitrary with $\sigma = \alpha \equiv (t_\alpha {t'}_\alpha {t''}_\alpha)$ and $\lambda = 1+i \in k$ and $1+i \mid \mathrm{disc}_k(k(\sqrt{\delta}))$. We define *the relative Hilbert symbol* for $1+i$ by:

$$\left[\frac{\sigma}{1+i:\delta}\right] = \begin{cases} +1, & \text{if } \sigma = N_{k(\sqrt{\delta})/k}(A) \text{for some number } A \in k(\sqrt{\delta}) \\ (-1)^{t_\sigma t'_\delta + t'_\sigma t_\delta}, & \text{if } 1+i \nmid \sigma \text{ and } 1+i \nmid \delta \\ (-1)^{t_\sigma t'_\delta + t'_\sigma t_\delta + t'_\sigma + t''_\sigma}, & \text{if } 1+i \nmid \sigma \text{ and } 1+i \mid \delta \\ \left[\frac{\alpha}{1+i:\delta}\right], & \text{if } \sigma = \alpha\upsilon \text{ for some } \alpha, \upsilon \in k \text{ where } \alpha \in \mathfrak{o} \text{ with } \\ & \lambda \nmid \alpha, \text{ and } \upsilon = N_{k(\sqrt{\delta})/k}(A) \text{ for some number } \\ & A \in k(\sqrt{\delta}). \end{cases}$$

Also we have the multiplicative property:

$$\left[\frac{\sigma_1\sigma_2}{1+i:\delta}\right] = \left[\frac{\sigma_1}{1+i:\delta}\right]\left[\frac{\sigma_2}{1+i:\delta}\right]$$

where σ_1, σ_2 are arbitrary numbers in k.

6.4. The Character Set of an Ideal

Definition 6.4.1. Let $k(\sqrt{\delta})$ be a Dirichlet number field over k and $\mathrm{disc}_k(k(\sqrt{\delta}))$ be its relative discriminant; let $\lambda_1, \lambda_2, \ldots, \lambda_s$ be all the distinct prime numbers dividing $\mathrm{disc}_k(k(\sqrt{\delta}))$. Let $C_2 = \{-1, +1\}$ be a cyclic group of order 2 under multiplication. We define a function

$$\begin{aligned} \Phi \;:\; k \;&\longrightarrow\; C_2^s \\ \sigma \;&\mapsto\; \left(\left[\frac{\sigma}{\lambda_1:\delta}\right], \left[\frac{\sigma}{\lambda_2:\delta}\right], \ldots, \left[\frac{\sigma}{\lambda_s:\delta}\right]\right). \end{aligned}$$

The s tuple, $\Phi(\sigma)$ is called *the character set of* σ *in* $k(\sqrt{\delta})$.

Definition 6.4.2. For each ideal $\mathfrak{I}$ in the number field $k(\sqrt{\delta})$, the product $\mathfrak{I} \cdot \mathsf{S}\mathfrak{I}$, which is a set generated by a number in k as shown in Appendix B.0.22, is denoted by $N_{k(\sqrt{\delta})/k}(\mathfrak{I})$ and called *the relative norm of the ideal* $\mathfrak{I}$.

Note that $\mathfrak{I} \cdot \mathsf{S}\mathfrak{I} = \mathfrak{O}x$ for some $x \in k$ is not completely determined by this condition, x is determined up to its four associates, that is if $x, y \in k$ are represented by $N_{k(\sqrt{\delta})/k}(\mathfrak{I})$, then $x = yi^a$ for some $a \in \{0, 1, 2, 3\}$.

To define the character set of an ideal $\mathfrak{I}$, we first check the character set of the number i,

$$\Phi(i) = \left(\left[\frac{i}{\lambda_1 : \delta} \right], \left[\frac{i}{\lambda_2 : \delta} \right], \ldots, \left[\frac{i}{\lambda_s : \delta} \right] \right).$$

Case 1. If $\Phi(i) = (+1, +1, \ldots, +1)$, then we define a function

$$\Psi \ : \ \{\mathfrak{I} : \mathfrak{I} \text{ is an ideal in } \mathfrak{O}\} \longrightarrow C_2^r$$

$$\mathfrak{I} \mapsto \left(\left[\frac{N_{k(\sqrt{\delta})/k}(\mathfrak{I})}{\lambda_1 : \delta} \right], \left[\frac{N_{k(\sqrt{\delta})/k}(\mathfrak{I})}{\lambda_2 : \delta} \right], \ldots, \left[\frac{N_{k(\sqrt{\delta})/k}(\mathfrak{I})}{\lambda_r : \delta} \right] \right).$$

where $r = s$.

Note that this function is well defined since $\left[\frac{N_{k(\sqrt{\delta})/k}(\mathfrak{I})}{\lambda_j : \delta} \right] = \left[\frac{x}{\lambda_j : \delta} \right] = \left[\frac{yi^a}{\lambda_j : \delta} \right] = \left[\frac{\mp y(i)^m}{\lambda_j : \delta} \right] = \left[\frac{\mp 1}{\lambda_j : \delta} \right] \left[\frac{y}{\lambda_j : \delta} \right] \left[\frac{(i)^m}{\lambda_j : \delta} \right] = (+1) \cdot \left[\frac{y}{\lambda_j : \delta} \right] \cdot (+1)^m = \left[\frac{y}{\lambda_j : \delta} \right]$ for all $j \in \{1, 2, \ldots, s\}$ with a suitable $m \in \{0, 1\}$.

Case 2. If $\Phi(i) \neq (1, \ldots, 1)$, say $\left[\frac{i}{\lambda_s : \delta} \right] = -1$, then we take the value x of the relative norm $N_{k(\sqrt{\delta})/k}(\mathfrak{I}) = \mathfrak{O}x$ such that $\left[\frac{N_{k(\sqrt{\delta})/k}(\mathfrak{I})}{\lambda_s : \delta} \right] = \left[\frac{x}{\lambda_s : \delta} \right] = \left[\frac{yi^a}{\lambda_s : \delta} \right] = \left[\frac{y}{\lambda_s : \delta} \right] \left[\frac{i}{\lambda_s : \delta} \right]^a = +1$ by choosing the suitable number $a \in \{0, 1, 2, 3\}$. Then for this value $N_{k(\sqrt{\delta})/k}(\mathfrak{I}) = \mathfrak{O}x$ we define a function

$$\Psi \ : \ \{\mathfrak{a} : \mathfrak{a} \text{ is an ideal in } \mathfrak{O}\} \longrightarrow C_2^r$$

$$\mathfrak{a} \mapsto \left(\left[\frac{N_{k(\sqrt{\delta})/k}(\mathfrak{I})}{\lambda_1 : \delta} \right], \left[\frac{N_{k(\sqrt{\delta})/k}(\mathfrak{I})}{\lambda_2 : \delta} \right], \ldots, \left[\frac{N_{k(\sqrt{\delta})/k}(\mathfrak{I})}{\lambda_r : \delta} \right] \right).$$

where $r = s - 1$.

Note that this function is well defined since a is fixed first. The number a can take two values according as $\left[\frac{y}{\lambda_s : \delta}\right] = +1$ or -1, that is $a = 0, 2$ or $a = 1, 3$, so $x = \mp y$ or $x = \mp yi$. Therefore, $\left[\frac{N_{k(\sqrt{\delta})/k}(\mathfrak{I})}{\lambda_j : \delta}\right] = \left[\frac{x}{\lambda_j : \delta}\right] = \left[\frac{\mp y}{\lambda_j : \delta}\right] = (+1) \cdot \left[\frac{y}{\lambda_j : \delta}\right] = \left[\frac{y}{\lambda_j : \delta}\right]$ or $\left[\frac{N_{k(\sqrt{\delta})/k}(\mathfrak{I})}{\lambda_j : \delta}\right] = \left[\frac{x}{\lambda_j : \delta}\right] = \left[\frac{\mp yi}{\lambda_j : \delta}\right] = (+1) \cdot \left[\frac{yi}{\lambda_j : \delta}\right] = \left[\frac{yi}{\lambda_j : \delta}\right]$, which implies that $\left[\frac{N_{k(\sqrt{\delta})/k}(\mathfrak{I})}{\lambda_j : \delta}\right]$ is completely determined for all $j \in \{1, 2, \ldots, s-1\}$.

Notation 6.4.3. From now on we will denote both the functions Φ and Ψ defined above by Υ.

Ideals in the same class have the same character set since $\mathfrak{I}' = A\mathfrak{I}$ implies that

$$\begin{aligned}
\left[\frac{N_{k(\sqrt{\delta})/k}(\mathfrak{I}')}{\lambda : \delta}\right] &= \left[\frac{N_{k(\sqrt{\delta})/k}(A\mathfrak{I})}{\lambda : \delta}\right] \\
&= \left[\frac{N_{k(\sqrt{\delta})/k}(A) N_{k(\sqrt{\delta})/k}(\mathfrak{I})}{\lambda : \delta}\right] \\
&= \left[\frac{N_{k(\sqrt{\delta})/k}(A)}{\lambda : \delta}\right] \left[\frac{N_{k(\sqrt{\delta})/k}(\mathfrak{I})}{\lambda : \delta}\right] \\
&= (+1) \left[\frac{N_{k(\sqrt{\delta})/k}(\mathfrak{I})}{\lambda : \delta}\right] \\
&= \left[\frac{N_{k(\sqrt{\delta})/k}(\mathfrak{I})}{\lambda : \delta}\right]
\end{aligned}$$

for each prime divisor λ of $\mathrm{disc}_k(k(\sqrt{\delta}))$.

6.5. Genera of Ideal Classes

Definition 6.5.1. The set of all ideal classes that have the same character set is called a *genus* and denoted by $\mathfrak{G}$. The genus of ideal classes which have the character set

$(+1,+1,\ldots,+1)$ is called the *principle genus* and denoted by $\mathfrak{G}_0$.

Note that the character set of the principle class is equal to $(+1,+1,\ldots,+1)$, so it lies in the principle genus $\mathfrak{G}_0$.

6.6. Ideal Classes in the Principle Genus

By the multiplicative property of norm (See Appendix B.0.23), the character system of $\mathfrak{I}^2$ for an ideal $\mathfrak{I}$ in K, is

$$\begin{aligned}
&\left(\left[\frac{N_{k(\sqrt{\delta})/k}(\mathfrak{I}^2)}{\lambda_1:\delta}\right],\ldots,\left[\frac{N_{k(\sqrt{\delta})/k}(\mathfrak{I}^2)}{\lambda_s:\delta}\right]\right)\\
=&\left(\left[\frac{N_{k(\sqrt{\delta})/k}(\mathfrak{I})N_{k(\sqrt{\delta})/k}(\mathfrak{I})}{\lambda_1:\delta}\right],\ldots,\left[\frac{N_{k(\sqrt{\delta})/k}(\mathfrak{I})N_{k(\sqrt{\delta})/k}(\mathfrak{I})}{\lambda_s:\delta}\right]\right)\\
=&\left(\left[\frac{N_{k(\sqrt{\delta})/k}(\mathfrak{I})}{\lambda_1:\delta}\right]^2,\ldots,\left[\frac{N_{k(\sqrt{\delta})/k}(\mathfrak{I})}{\lambda_s:\delta}\right]^2\right)\\
=&\ (\mp1,\mp1,\ldots,\mp1)\\
=&\ (1,1,\ldots,1)\,.
\end{aligned}$$

where $r=s$ or $r=s-1$. Thus the class of $\mathfrak{I}^2$ lies in the principle genus. The converse is also true.

Theorem 6.6.1. *Every ideal class in the principle genus is a square of an ideal class.*

To prove the Theorem 6.6.1 we should first prove the following theorems:

Theorem 6.6.2. *If υ is equal to $N_{K_\delta/k}(\mathfrak{I})$ for some ideal $\mathfrak{I}$ in the principle genus of K_δ then δ is equal to $N_{K_\upsilon/k}(\mathfrak{J})$ for some ideal $\mathfrak{J}$ in the principle genus of K_υ.*

Proof. We will show that $\delta = N_{K_\upsilon/k}(\mathfrak{J})$ for some ideal $\mathfrak{J}$ in the principle genus by showing that λ is a product of two prime ideals for each prime divisor λ of δ and

$\left[\frac{\delta}{\pi : \upsilon}\right] = +1$ for each divisor π of υ. We will assume that υ does not contain square factors in k since a square of a number is itself a norm of that number.

Firstly, we will consider the prime divisors of υ different from $1+i$.

Case 1. Assume that $\pi \mid \upsilon$, but $\pi \nmid \mathrm{disc}_k(k(\sqrt{\delta}))$. By hypothesis, $\upsilon = N_{k(\sqrt{\delta})/k}(\mathfrak{I})$ for some ideal $\mathfrak{I}$ in $k(\sqrt{\delta})$, so π reduces into two prime ideals in $k(\sqrt{\delta})$. To prove that assume the contrary, then π must be prime in $k(\sqrt{\delta})$ since $\pi \nmid \mathrm{disc}_k(k(\sqrt{\delta}))$. But then $\pi \mid \upsilon = \mathfrak{I} \cdot \mathsf{S}\mathfrak{I}$, so $\pi \mid \mathfrak{I}$ without loss of generality, then $\pi^2 \mid \mathfrak{I} \cdot \mathsf{S}\mathfrak{I} = \upsilon$ which contradicts to the fact that υ is squarefree. Therefore, δ is a quadratic residue modulo π, so $\left[\frac{\delta}{\pi : \upsilon}\right] = \left[\frac{\delta}{\pi}\right] = +1$ since $\pi \nmid \delta$.

Case 2. Now assume that $\lambda \mid \upsilon$ and also $\lambda \mid \mathrm{disc}_k(k(\sqrt{\delta}))$. We know that $\lambda = \mathfrak{L}^2$ where $\mathfrak{L} = (\lambda, \sqrt{\delta})$ is a prime ideal in $k(\sqrt{\delta})$ by Lemma 6.2.3. So $\lambda + \sqrt{\delta}$ is divisible by $\mathfrak{L}$, but it is not divisible by λ in $k(\sqrt{\delta})$. Then for $\upsilon = \lambda\upsilon'$, $\delta = \lambda\delta'$ we get:

$$\begin{aligned}
\left[\frac{\upsilon}{\lambda : \delta}\right] &= \left[\frac{\upsilon}{\lambda : \delta}\right].(+1) = \left[\frac{\upsilon}{\lambda : \delta}\right]\left[\frac{N_{k(\sqrt{\delta})/k}(\frac{1}{\lambda+\sqrt{\delta}})}{\lambda : \delta}\right] \\
&= \left[\frac{\upsilon N_{k(\sqrt{\delta})/k}(\frac{1}{\lambda+\sqrt{\delta}})}{\lambda : \delta}\right] = \left[\frac{\frac{\upsilon}{\lambda^2-\delta}}{\lambda : \delta}\right] \\
&= \left[\frac{\frac{\lambda\upsilon'}{\lambda^2-\lambda\delta'}}{\lambda : \delta}\right] = \left[\frac{\frac{\upsilon'}{\lambda-\delta'}}{\lambda : \delta}\right] = \left[\frac{\frac{\upsilon'}{\lambda-\delta'}}{\lambda}\right] \text{ since } \lambda \nmid \frac{\upsilon'}{\lambda-\delta'} \\
&= \left[\frac{\upsilon'\delta'}{\lambda}\right]\left[\frac{\frac{1}{\delta-\delta'^2}}{\lambda}\right] = \left[\frac{\upsilon'\delta'}{\lambda}\right]\left[\frac{-N_{k(\sqrt{\delta})/k}(\frac{1}{\delta'+\sqrt{\delta}})}{\lambda}\right]
\end{aligned}$$

$$= \left[\frac{\upsilon'\delta'}{\lambda}\right]\left[\frac{-1}{\lambda}\right]\left[\frac{N_{k(\sqrt{\delta})/k}(\frac{1}{\delta'+\sqrt{\delta}})}{\lambda}\right] = \left[\frac{\upsilon'\delta'}{\lambda}\right]\left[\frac{i^2}{\lambda}\right].(+1)$$

$$= \left[\frac{\upsilon'\delta'}{\lambda}\right].(+1) = \left[\frac{\upsilon'\delta'}{\lambda}\right]$$

Similarly,

$$\left[\frac{\delta}{\lambda:\upsilon}\right] = \left[\frac{\delta}{\lambda:\upsilon}\right].(+1) = \left[\frac{\delta}{\lambda:\upsilon}\right]\left[\frac{N_{k(\sqrt{\delta})/k}(\frac{1}{\lambda+\sqrt{\upsilon}})}{\lambda:\upsilon}\right]$$

$$= \left[\frac{\delta N_{k(\sqrt{\delta})/k}(\frac{1}{\lambda+\sqrt{\upsilon}})}{\lambda:\upsilon}\right] = \left[\frac{\frac{\delta}{\lambda^2-\upsilon}}{\lambda:\upsilon}\right]$$

$$= \left[\frac{\frac{\lambda\delta'}{\lambda^2-\lambda\upsilon'}}{\lambda:\upsilon}\right] = \left[\frac{\frac{\delta'}{\lambda-\upsilon'}}{\lambda:\upsilon}\right] = \left[\frac{\frac{\delta'}{\lambda-\upsilon'}}{\lambda}\right] \text{ since } \lambda \nmid \frac{\delta'}{\lambda-\upsilon'}$$

$$= \left[\frac{\delta'\upsilon'}{\lambda}\right]\left[\frac{\frac{1}{\upsilon-\upsilon'^2}}{\lambda}\right] = \left[\frac{\upsilon'\delta'}{\lambda}\right]\left[\frac{-N_{k(\sqrt{\delta})/k}(\frac{1}{\upsilon'+\sqrt{\upsilon}})}{\lambda}\right]$$

$$= \left[\frac{\delta'\upsilon'}{\lambda}\right]\left[\frac{-1}{\lambda}\right]\left[\frac{N_{k(\sqrt{\delta})/k}(\frac{1}{\upsilon'+\sqrt{\upsilon}})}{\lambda}\right] = \left[\frac{\delta'\upsilon'}{\lambda}\right]\left[\frac{i^2}{\lambda}\right].(+1)$$

$$= \left[\frac{\delta'\upsilon'}{\lambda}\right].(+1) = \left[\frac{\delta'\upsilon'}{\lambda}\right]$$

Therefore, $\left[\frac{\upsilon}{\lambda:\delta}\right] = \left[\frac{\delta'\upsilon'}{\lambda}\right] = \left[\frac{\delta}{\lambda:\upsilon}\right]$ and by the hypothesis that $\upsilon = N_{k(\sqrt{\delta})/k}(\mathfrak{I})$

where $\mathfrak{I}$ is in the principle genus, we get

$$\left[\frac{\upsilon}{\lambda : \delta}\right] = +1 \text{ for all } \lambda \text{ that divides } \delta,$$

and then $\left[\dfrac{\delta}{\lambda : \upsilon}\right] = +1$ for all λ that divides δ and υ.

Secondly, we will consider the prime divisor $1 + i$. We have four cases to check:

(i) $1 + i$ does not divide both υ and δ,
(ii) $1 + i$ divides υ, but does not divide δ,
(iii) $1 + i$ divides δ, but does not divide υ,
(iv) $1 + i$ divides both δ and υ.

So we will show that $\left[\dfrac{\delta}{\lambda : \upsilon}\right] = +1$, if $\lambda = 1 + i \mid \text{disc}_k(k(\sqrt{\upsilon}))$ and $1 + i$ is a product of two prime ideals, if $1 + i \mid \delta$.

(i) For the first case we put $\upsilon \equiv (t_\upsilon t'_\upsilon)$ and $\delta \equiv (t_\delta t'_\delta) \mod (1 + i)^4$, and consider the two cases:

a) If t_υ, t'_υ are both even, then $\upsilon \equiv 1 \mod 4$, so $\text{disc}_k(k(\sqrt{\upsilon})) = \upsilon$ and $1 + i \nmid \text{disc}_k(k(\sqrt{\upsilon}))$. So no such symbol $\left[\dfrac{\delta}{\lambda : \upsilon}\right]$ exists with $\lambda = 1 + i$.

b) If t_υ, t'_υ are not both even, then $\text{disc}_k(k(\sqrt{\delta})) = (-2i)\upsilon$ or $\text{disc}_k(k(\sqrt{\upsilon})) = 4\upsilon$, so $1 + i \mid \text{disc}_k(k(\sqrt{\upsilon}))$. If t_δ and t'_δ are both even, then this symbol has value $+1$. If t_δ and t'_δ are not both even, then $\text{disc}_k(k(\sqrt{\delta})) = (-2i)\delta$ or $\text{disc}_k(k(\sqrt{\delta})) = 4\delta$, so $1 + i \mid \text{disc}_k(k(\sqrt{\delta}))$ and the symbol $\left[\dfrac{\upsilon}{1 + i : \delta}\right]$ is meaningful. Furthermore, $\left[\dfrac{\upsilon}{1 + i : \delta}\right] = +1$ by our hypothesis and $\left[\dfrac{\upsilon}{1 + i : \delta}\right] = (-1)^{t_\upsilon t'_\delta + t_\delta t'_\upsilon} = (-1)^{t_\delta t'_\upsilon + t_\upsilon t'_\delta} = \left[\dfrac{\delta}{1 + i : \upsilon}\right]$ by the definition of the symbol. Thus $\left[\dfrac{\delta}{1 + i : \upsilon}\right] = +1$. In addition, $\left[\dfrac{\delta}{1 + i}\right] = \left[\dfrac{\delta}{1 + i : \upsilon}\right]$, so $1 + i$ is a product of prime ideals in $k(\sqrt{\upsilon})$.

(ii) For the second case, we put $\upsilon \equiv (1+i)(t_\upsilon t'_\upsilon)$ and $\delta \equiv (t_\delta t'_\delta t''_\delta) \mod (1+i)^5$, and consider the two cases:

a) If t_δ and t'_δ are both even, then $1+i \nmid \mathrm{disc}_k(k(\sqrt{\delta})) = \delta$, so $\left[\frac{\delta}{1+i:\upsilon}\right] = \left[\frac{\delta}{1+i}\right]$. By hypothesis, $\upsilon = N_{K_\delta/k}(\mathfrak{I})$ for some ideal $\mathfrak{I}$ in $k(\sqrt{\delta})$ and $(1+i) \mid \upsilon$, so $1+i$ is a product of two different prime ideals in $k(\sqrt{\delta})$. Thus, $\left[\frac{\delta}{1+i}\right] = +1$ and we get $\left[\frac{\delta}{1+i:\upsilon}\right] = +1$.

b) If t_δ and t'_δ are not both even, then $1+i$ divides $\mathrm{disc}_k(k(\sqrt{\delta}))$. Let $\omega = \frac{\Omega \cdot \mathsf{S}\Omega}{1+i}$, so $N_{k(\sqrt{\delta})/k}(\frac{1}{\Omega}) = \frac{1}{\Omega \cdot \mathsf{S}\Omega} = \frac{1}{\omega(1+i)}$ and then we get that

$$\begin{aligned}
\left[\frac{\upsilon}{1+i:\delta}\right] &= \left[\frac{\upsilon N_{k(\sqrt{\delta})/k}(\frac{1}{\Omega})}{1+i:\delta}\right] \\
&= \left[\frac{(t_\upsilon t'_\upsilon)\frac{1}{\omega(1+i)}}{1+i:\delta}\right]\left[\frac{\omega^2}{1+i:\delta}\right] \\
&= \left[\frac{(t_\upsilon t'_\upsilon)\omega}{1+i:\delta}\right] \\
&= \left[\frac{(t_\upsilon t'_\upsilon)}{1+i:\delta}\right]\left[\frac{\omega}{1+i:\delta}\right] \\
&= (-1)^{t_\upsilon t'_\delta + t'_\upsilon t_\delta}(-1)^{t'_\delta + t''_\delta} \\
&= (-1)^{t_\upsilon t'_\delta + t'_\upsilon t_\delta + t'_\delta + t''_\delta} \\
&= \left[\frac{\delta}{1+i:\upsilon}\right]
\end{aligned}$$

by Definition 6.3.5. By hypothesis $\left[\frac{\upsilon}{1+i:\delta}\right] = +1$, thus $\left[\frac{\delta}{1+i:\upsilon}\right] = +1$.

(iii) For the third case we put $\upsilon \equiv (t_\upsilon t'_\upsilon t''_\upsilon)$ and $\delta \equiv (1+i)(t_\delta t'_\delta) \mod (1+i)^5$ and consider the two cases:

a) If t_υ and t'_υ are both even, then $1+i \nmid \mathrm{disc}_k(k(su))$. By hypothesis, $\left[\frac{\upsilon}{1+i:\delta}\right] =$

$+1$ and by Definition 6.3.5 $\left[\frac{\upsilon}{1+i:\delta}\right] = (-1)^{t_\upsilon t'_\delta + t'_\upsilon t_\delta + t'_\upsilon + t''_\upsilon} = (-1)^{t''_\upsilon}$ since t_υ and t'_υ are even. Therefore, t''_υ must be even and $\upsilon \equiv (000) \mod (1+i)^5$. Since $1+i \nmid \upsilon$, we have that $+1 = \left[\frac{\upsilon}{1+i:\delta}\right] = \left[\frac{\upsilon}{1+i}\right]$, so $1+i$ is a product of prime ideals in $k(\sqrt{\upsilon})$.

b) If t_υ and t'_υ are not both even, then $1+i \mid \mathrm{disc}_k(k(\sqrt{\upsilon}))$. We take ω as in Case ii.b) and get $\left[\frac{\delta}{1+i:\upsilon}\right] = (-1)^{t_\upsilon t'_\delta + t'_\upsilon t_\delta + t'_\upsilon + t''_\upsilon}$. But by Definition 6.3.5, this is equal to the symbol $\left[\frac{\upsilon}{1+i:\delta}\right]$ which has value $+1$ by hypothesis.

(iv) For the fourth case we put $\upsilon \equiv (1+i)(t_\upsilon t'_\upsilon t''_\upsilon)$ and $\delta \equiv (1+i)(t_\delta t'_\delta t''_\delta) \mod (1+i)^6$. Then,

$$\begin{aligned}
\left[\frac{\upsilon}{1+i:\delta}\right] &= \left[\frac{\upsilon N_{k(\sqrt{\delta})/k}(\frac{1}{\sqrt{\delta}})}{1+i:\delta}\right] = \left[\frac{\frac{\upsilon}{-\delta}}{1+i:\delta}\right] \\
&= \left[\frac{(t_\upsilon t'_\upsilon t''_\upsilon)(t_\delta t'_\delta t''_\delta)}{1+i:\delta}\right] \qquad (6.1) \\
&= (-1)^{(t_\upsilon+t_\delta)t'_\delta + (t'_\upsilon+t'_\delta)t_\delta + (t'_\delta+t'_\upsilon) + (t''_\delta+t''_\upsilon)}.
\end{aligned}$$

Similarly,

$$\begin{aligned}
\left[\frac{\delta}{1+i:\upsilon}\right] &= \left[\frac{\delta N_{k(\sqrt{\delta})/k}(\frac{1}{\upsilon})}{1+i:\upsilon}\right] = \left[\frac{(t_\delta t'_\delta t''_\delta)(t_\upsilon t'_\upsilon t''_\upsilon)}{1+i:\upsilon}\right] \\
&= (-1)^{(t_\delta+t_\upsilon)t'_\upsilon + (t'_\delta+t'_\upsilon)t_\upsilon + (t'_\delta+t'_\upsilon) + (t''_\delta+t''_\upsilon)} \\
&= (-1)^{t_\delta t'_\upsilon + t_\upsilon t'_\upsilon + t'_\delta t_\upsilon + t'_\upsilon t_\upsilon + (t'_\delta+t'_\upsilon) + (t''_\delta+t''_\upsilon)} \\
&= (-1)^{t_\delta t'_\upsilon + t'_\delta t_\upsilon + (t'_\delta+t'_\upsilon) + (t''_\delta+t''_\upsilon)}
\end{aligned}$$

$$= \left[\frac{\upsilon}{1+i:\delta}\right] \text{ by Equation 6.1}$$

$$= +1 \text{ by hypothesis.}$$

Lastly, we will consider the prime divisors λ of δ different from $1+i$ such that $\lambda \nmid \text{disc}_k(k(\sqrt{\upsilon}))$. Then $\left[\frac{\upsilon}{\lambda:\delta}\right] = \left[\frac{\upsilon}{\lambda}\right]$ and $\left[\frac{\upsilon}{\lambda}\right] = +1$ by the assumption that the character system of υ consists of $+1$. Thus λ is a product of two prime ideals in $k(\sqrt{\upsilon})$.

If $\lambda = 1+i$ for this case, then $1+i \mid \lambda$ and $1+i \nmid \text{disc}_k(k(\sqrt{\upsilon}))$, so $1+i \nmid \upsilon$. But this is the Case *(iii)*, so $1+i$ is a product of two prime ideals in $k(\sqrt{\upsilon})$.

Therefore, each prime divisor of δ is a product of two prime ideals in $k(\sqrt{\upsilon})$ with $\left[\frac{\delta}{\lambda:\upsilon}\right] = +1$ for each prime divisor λ of $\text{disc}_k(k(\sqrt{\upsilon}))$, so δ is a relative norm of an ideal in the principle genus. □

Theorem 6.6.3. *If υ is a relative norm of a number in $k(\sqrt{\delta})$, then δ is also a relative norm of a number in $k(\sqrt{\upsilon})$.*

Proof. Let $\upsilon = N_{k(\sqrt{\delta})/k}(\alpha+\beta\sqrt{\delta}) = (\alpha+\beta\sqrt{\delta})(\alpha-\beta\sqrt{\delta}) = \alpha^2-\beta^2\delta$ where $\alpha,\beta \in k$. Then $\beta^2\delta = \alpha^2+\upsilon$ implies $\delta = (\frac{\alpha}{\beta})^2 - (\frac{1}{\beta})^2\upsilon = (\frac{\alpha}{\beta}+\frac{1}{\beta}\sqrt{\upsilon})(\frac{\alpha}{\beta}+-\frac{1}{\beta}\sqrt{\upsilon}) = N_{k(\sqrt{\delta})/k}(\frac{\alpha+\sqrt{\upsilon}}{\beta})$ where $\frac{\alpha+\sqrt{\upsilon}}{\beta} \in k(\sqrt{\upsilon})$. □

Theorem 6.6.4. *If $\upsilon = N_{k(\sqrt{\delta})/k}(\mathfrak{I})$ for some ideal $\mathfrak{I}$ in the principle genus of $k(\sqrt{\delta})$, then in fact $\upsilon = N_{k(\sqrt{\delta})/k}(A)$ for some number A in $k(\sqrt{\delta})$.*

Proof. We will use Minkowski's theorem about the discriminant of general number fields (See Appendix B.0.18). Notice that in the biquadratic Dirichlet number field $k(\sqrt{\delta})$, the degree of $k(\sqrt{\delta})$ over $\mathbb{Q}$ is $n=4$, and the number of real embeddings is $r_1 = 0$, the number of complex embeddings is $r_2 = 2$. To see why, assume not. Then we get $r_1 = 2$, $r_2 = 0$, which implies that for the real embedding $\varphi : k(\sqrt{\delta}) \to \mathbb{R}$, we have $\varphi|_k : k \to \mathbb{R}$. But this is a contradiction since $\varphi|_k(i)$ can not be defined. Now, we have $M_{k(\sqrt{\delta})} = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2} = \frac{4!}{4^4}\left(\frac{4}{\pi}\right)^2 = \frac{3}{2\pi^2}$. Therefore, by Minkowski's theorem, in every

ideal class of $k(\sqrt{\delta})$ there exists an ideal $\mathfrak{I}$ such that $N_{k(\sqrt{\delta})/\mathbb{Q}}(\mathfrak{I}) \leq M_{k(\sqrt{\delta})}\sqrt{|D_{k(\sqrt{\delta})_\delta}|} = \frac{3}{2\pi^2}\sqrt{|D|}$ where $D = \mathrm{disc}_k(k(\sqrt{\delta}))$. But $D = 2^4|d|^2$ where $d = \mathrm{disc}_{\mathbb{Q}}(k(\sqrt{\delta}))$, and for all cases $\Omega \leq 1 + \sqrt{\delta}$ implying that $d \leq (1 + \sqrt{\delta} - (1 - \sqrt{\delta}))^2 = (1 + \sqrt{\delta} - 1 + \sqrt{\delta}) = (2\sqrt{\delta})^2 = 4\delta$. Thus, $D \leq 2^4|4\delta|^2 = 2^4 2^4|\delta|^2 = 2^8|\delta|^2$. Therefore,

$$N_{k(\sqrt{\delta})/\mathbb{Q}}(\mathfrak{I}) \leq \frac{3}{2\pi^2}|\sqrt{D}| = \frac{32^3}{\pi^2} \cdot \frac{1}{2^4}|\sqrt{D}| < \sqrt{6}\frac{1}{2^4}\sqrt{2^8|\delta|^2} = \sqrt{6}|\delta|.$$

But every norm is a square of a relative norm, say $N_{k(\sqrt{\delta})/\mathbb{Q}}(\mathfrak{I}) = |N_{k(\sqrt{\delta})/k}(\mathfrak{I})|^2$. Therefore, every ideal class in $k(\sqrt{\delta})$ contains an ideal $\mathfrak{I}$ with $|N_{k(\sqrt{\delta})/k}(\mathfrak{I})|^2 < \sqrt{6}|\delta|$.

Firstly, we will prove the theorem for Dirichlet fields $k(\sqrt{\delta})$ with $|\delta| < \sqrt{6}$. Let $\delta = a + bi$ with $a, b \in \mathbb{Z}$, then $|a + bi|^2 = a^2 + b^2 < 6$ implies that the whole set of possibilities for (a, b) is $\{(1, \mp 2), (2, \mp 1), (1, \mp 1), (0, \mp 1), (\mp 1, 0)\}$. Note that we do not have $\delta = \mp 2$ or $\mp 2i$ since $2i = (1+i)^2$. Also $\delta \neq 1$ since $k(\sqrt{\delta})$ is a biquadratic number field over $\mathbb{Q}$. Now by using Minkowski's equality, the value $\upsilon \in k$ which satisfies the theorem with $|\upsilon|^2 < \sqrt{6}|\delta|$ is given for each δ in the following table. The calculations are done in Appendix A.0.15.

Table 6.3. Table of $\upsilon \equiv N_{k(\sqrt{\delta})/k}(A)$ with $\delta < 6$

δ	υ
$1 \pm 2i$	$1 \mp i$
2 ± 1	$2 \mp i$
$2 \pm i$	$1 \pm i$
$1 \pm i$	$\pm i$
i	$1 + i$

Now let δ be an imaginary number with $|\delta| > \sqrt{6}$ and assume for induction that the theorem is true for all Dirichlet number fields $k(\sqrt{\delta'})$ with $|\delta'| < |\delta|$. Let $N = N_{k(\sqrt{\delta})/k}(\mathfrak{I})$ and let $\mathfrak{I}$ be in the principle genus. Then by Minkowski's theorem, there exists an ideal $\mathfrak{I}'$ in $k(\sqrt{\delta})$ which is equivalent to $\mathfrak{I}$ and for $N' = N_{k(\sqrt{\delta})/k}(\mathfrak{I}')$ we have $|N'|^2 < \sqrt{6}|\delta|$. Since $\sqrt{6} < |\delta|$, we get $|N'|^2 < |\delta|^2$, so $|N'| < |\delta|$. Here N' is the relative

norm of the ideal $\mathfrak{I}'$ which belongs to the principle genus since $\mathfrak{I}'$ and $\mathfrak{I}$ are equivalent ideals. Then by Theorem 6.6.2, $\delta = N_{k(\sqrt{\delta'})/k}(\mathfrak{J})$ for some ideal $\mathfrak{J}$ in the principle genus of $k(\sqrt{\delta'})$. But $|N'| < |\delta|$, so by induction hypothesis N' is equal to $N_{k(\sqrt{\delta})/k}(B)$ for some number B in $k(\sqrt{\delta})$. Therefore, $\mathfrak{I} = \mathfrak{I}'A$ for some number $A \in k$ implies that $N = N_{k(\sqrt{\delta})/k}(\mathfrak{I}) = N_{k(\sqrt{\delta})/k}(\mathfrak{I}'A) = N_{k(\sqrt{\delta})/k}(\mathfrak{I}')N_{k(\sqrt{\delta})/k}(A) = N'N_{k(\sqrt{\delta})/k}(A) = N_{k(\sqrt{\delta})/k}(B)N_{k(\sqrt{\delta})/k}(A) = N_{k(\sqrt{\delta})/k}(BA) = N_{k(\sqrt{\delta})/k}(C)$ for some number C in k. □

Now we can prove Theorem 6.6.1:

Proof. Let $\mathfrak{I}$ be an ideal in the principle genus of $k(\sqrt{\delta})$. Then by Theorem 6.6.4, $N_{k(\sqrt{\delta})/k}(\mathfrak{I}) = N_{k(\sqrt{\delta})/k}(A)$ for some number A in k. We put $\frac{\mathfrak{I}}{A} = \frac{\mathfrak{P}}{\mathfrak{P}'}$ where $\mathfrak{P}, \mathfrak{P}'$ are relatively prime ideals. Then $N_{k(\sqrt{\delta})/k}(\frac{\mathfrak{I}}{A}) = N_{k(\sqrt{\delta})/k}(\mathfrak{I})\ N_{k(\sqrt{\delta})/k}(A) = 1 = \frac{\mathfrak{P} \cdot \mathsf{S}\mathfrak{P}}{\mathfrak{P}' \cdot \mathsf{S}\mathfrak{P}'}$ implies $\mathfrak{P}' = \mathsf{S}\mathfrak{P}$. Since $\mathfrak{P} \cdot \mathsf{S}\mathfrak{P} = N_{k(\sqrt{\delta})/k}(\mathfrak{P}) = \alpha$ is a number in k by Appendix B.0.22, we get $\frac{\mathfrak{I}}{A} = \mathfrak{P}\frac{1}{\mathsf{S}\mathfrak{P}} = \mathfrak{P}\frac{\mathfrak{P}}{\alpha} = \frac{\mathfrak{P}^2}{\alpha}$ and $\mathfrak{I} = \frac{A}{\alpha}\mathfrak{P}^2$. Therefore, $\mathfrak{I}$ is in the ideal class of $\mathfrak{P}^2$. □

6.7. Ambig Ideals

Definition 6.7.1. An ideal $\mathfrak{I}$ in K is called an *ambig ideal*, if $\mathfrak{I} = \mathsf{S}\mathfrak{I}$ and $\mathfrak{I}$ is not divisible by a number in k.

Theorem 6.7.2. *Let d be the relative discriminant of the Dirichlet number field K. A prime ideal $\mathfrak{P}$ divides $\mathfrak{O}d$ if and only if $\mathfrak{P}$ is an ambig prime ideal of K. If $\mathfrak{P}_1, \mathfrak{P}_2 \ldots, \mathfrak{P}_s$ are all the distinct prime ideal dividing $\mathfrak{O}d$ then*

$$S = \{\mathfrak{O}, \mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_s, \mathfrak{P}_1\mathfrak{P}_2, \ldots, \mathfrak{P}_1\mathfrak{P}_s, \ldots, \mathfrak{P}_1\mathfrak{P}_2 \ldots \mathfrak{P}_s\}$$

is the set of all ambig ideals in K.

Proof. We can deduce that $\mathfrak{L}_1, \mathfrak{L}_2, \ldots, \mathfrak{L}_s$ and only these are ambig prime ideals in K

by Theorem 6.2.7, because for every prime $\tau \in k$, we have that

$$\tau\mathfrak{O} = \begin{cases} \mathfrak{B} \cdot \mathsf{S}\mathfrak{B}, & \text{if } \tau \nmid d \text{ and } \left[\frac{d}{\tau}\right] = +1 \\ \mathfrak{B}, & \text{if } \tau \nmid d \text{ and } \left[\frac{d}{\tau}\right] = -1 \\ \mathfrak{L}^2, & \text{if } \tau \mid \mathrm{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m})). \end{cases}$$

Consider an ambig ideal $\mathfrak{I} = \mathfrak{L}_1{}^{a_1}\mathfrak{L}_2{}^{a_2}\ldots\mathfrak{L}_n{}^{a_n}$; so

$$\mathfrak{L}_1{}^{a_1}\mathfrak{L}_2{}^{a_2}\ldots\mathfrak{L}_n{}^{a_n} = \mathsf{S}\mathfrak{L}_1{}^{a_1}\mathsf{S}\mathfrak{L}_2{}^{a_2}\ldots\mathsf{S}\mathfrak{L}_n{}^{a_n}$$

and $\mathfrak{I}$ has no integer divisor, that is $\tau\mathfrak{O} \nmid \mathfrak{I}$ for all prime $\tau \in k$. Thus, there is no $\mathfrak{I}$ of the second form. Also $a_i = 0$ or 1 for all $i = 1, 2, \ldots, n$. So for the first form $\tau = \mathfrak{B} \cdot \mathsf{S}\mathfrak{B}$, but $\mathfrak{I}$ is ambig, so $\mathsf{S}\mathfrak{I} = \mathsf{S}\mathfrak{L}_1\mathsf{S}\mathfrak{L}_2\ldots\mathsf{S}\mathfrak{L}_n$ such that $\mathfrak{L}_i = \mathsf{S}\mathfrak{L}_i$, because if not, that is if $\mathfrak{B}_i = \mathsf{S}\mathfrak{B}_j$ for $i \neq j$, then $\mathfrak{B}_i\mathfrak{B}_j = \mathsf{S}(\mathfrak{B}_j\mathfrak{B}_j) \in k$ divides $\mathfrak{I}$ which contradicts Definition 6.7.1. But $\mathfrak{B} = \mathsf{S}\mathfrak{B}$ is a contradiction for a prime τ of the first form. Hence there are at most $\mathfrak{B}^0$ or $\mathfrak{B}^1$ where $\mathfrak{B}$ is of the third form. So the prime ideals dividing $\mathfrak{O}d$ are the only ambig prime ideals in K. Thus S is the set of all ambig ideals in $\mathbb{Q}(\sqrt{m})$ with $|S| = 2^s$. □

6.8. Ambig Classes

Definition 6.8.1. If $\mathfrak{I}$ is an ideal in the ideal class $\mathtt{C}$, then the class containing the ideal $\mathsf{S}\mathfrak{I}$ will be denoted by SC. The ideal class $\mathtt{C}$ is called an *ambig class*, if $\mathtt{C} = \mathsf{SC}$.

Since $\mathfrak{I} \cdot \mathsf{S}\mathfrak{I}$ is equivalent to $\mathfrak{O}$, we have $\mathtt{C} \cdot \mathsf{SC} = 1$ where $\mathtt{C}$ is the ideal class containing $\mathfrak{I}$. If $\mathtt{C}$ is an ambig class then $\mathtt{C}^2 = \mathtt{C} \cdot \mathsf{SC} = 1$. Conversely, if $\mathtt{C}^2 = 1$ then $\mathtt{C} = \dfrac{1}{\mathtt{C}} = \dfrac{\mathtt{C} \cdot \mathsf{SC}}{\mathtt{C}} = \mathsf{SC}$, so $\mathtt{C}$ is an ambig class.

Our new aim is to find the all ambig classes. It is clear that the ideal class con-

taining an ambig ideal is an ambig class, so first we will check that how many of the ambig classes that are containing the 2^s ambig ideals are different.

Lemma 6.8.2. *Let E be a fundamental unit of the Dirichlet number field K. Then $N_{K/k}(E) = \mp 1$ or $\mp i$.*

Proof. Let E be a fundamental unit of K, then every unit in K is of the form $\rho E'^m$ where ρ is a root of unity and $m \in \mathbb{Z} \setminus \{0\}$. The minimal polynomial of ρ over $\mathbb{Q}$ has degree 2 or 4, then we can find that which root of unity ρ is.

$$
\begin{aligned}
\rho^2 - 1 &= (\rho - 1)(\rho + 1) = 0 && \text{is possible if } \rho = \mp 1,\\
\rho^3 - 1 &= (\rho - 1)(\rho^2 + \rho + 1) = 0 && \text{is possible if } \delta = 3,\\
\rho^4 - 1 &= (\rho^2 - 1)(\rho^2 + 1) && \text{is possible if } \rho = \mp i\\
\rho^5 - 1 &= (\rho - 1)(\rho^4 + \rho^3 + \rho^2 + \rho + 1) && \text{is not possible since}\\
& && \rho = e^{2\pi i/5} \notin k(\sqrt{\delta}),\\
\rho^6 - 1 &= (\rho^2 - 1)(\rho^4 + \rho^2 + 1) && \text{is not possible since}\\
& && \rho = \sqrt{\frac{-1 + \sqrt{3}i}{2}} \notin k(\sqrt{\delta}),\\
\rho^7 - 1 &= (\rho - 1)(\rho^6 + \rho^5 + \rho^4 + \rho^3 + \rho^2 + \rho + 1) && \text{is not possible since } 6 \neq 2, 4,\\
\rho^8 - 1 &= (\rho^4 - 1)(\rho^4 + 1) && \text{is possible if } \rho = \sqrt{i}, \delta = i.
\end{aligned}
$$

We know the values of ρ is ω for $\delta = 3$ and $\sqrt{i}$ for $\delta = i$. For all other cases $\rho = \mp 1$ or $\mp i$. The relative norm of the fundamental unit E divides the root of unity ρ in K, so $N_{K/k}(E) = \mp 1$ or $\mp i$. □

Theorem 6.8.3. *Let s be the number of distinct ambig prime ideals in $k(\sqrt{\delta})$.*

If $N_{k(\sqrt{\delta})/k}(E) = \mp 1$ for a fundamental unit E, then $s - 2$ of them determine independent ambig classes and there are 2^{s-2} distinct ambig classes.

If $N_{k(\sqrt{\delta})/k}(E) = \mp i$ for a fundamental unit E, then $s - 1$ of them determine

independent ambig classes and there are 2^{s-1} *distinct ambig classes.*

Proof. The product of the all different prime ideals that divide δ is equal to $\sqrt{\delta}$. We will show that the all ambig principle ideals can be only $\mathfrak{O}$ and $\mathfrak{O}\delta$ or there can be more if $N_{k(\sqrt{\delta})/k}(E) = \mp 1$ or $N_{k(\sqrt{\delta})/k}(E) = \mp i$ respectively.

We will assume first that $\delta \neq 3$ and $\delta \neq i$.

Firstly, let E be a fundamental unit such that $N_{k(\sqrt{\delta})/k}(E) = \mp 1$. It is enough to consider the case that $N_{k(\sqrt{\delta})/k}(E) = +1$ since for the case $N_{k(\sqrt{\delta})/k}(E) = -1$ we can take iE as a fundamental unit instead of E. Let $1 + E = \alpha A$ where $\alpha \in k$ and $A \in \mathfrak{O}$ which is not divisible by any number in k. Then
$\dfrac{A}{\mathsf{S}A} = \dfrac{\alpha A}{\alpha \mathsf{S}A} = \dfrac{\alpha A}{\mathsf{S}\alpha A} = \dfrac{1+E}{\mathsf{S}(1+E)} = \dfrac{1+E}{1+\mathsf{S}E} = \dfrac{1+E}{E\mathsf{S}E+\mathsf{S}E} = \dfrac{1+E}{\mathsf{S}E(1+E)} = \dfrac{1}{\mathsf{S}E} = \dfrac{E\mathsf{S}E}{\mathsf{S}E} = E.$

Therefore, $A = \mathsf{S}A \cdot E = \mathsf{S}A.\dfrac{1}{\mathsf{S}E} = \mathsf{S}\left(\dfrac{A}{E}\right)$ and $\mathfrak{O}A$ is a principle ambig ideal different from $\mathfrak{O}$ and $\mathfrak{O}\delta$, because if $A = \rho E^m$ and $\rho E^m\sqrt{\delta}$ then

$$E = \frac{A}{\mathsf{S}A} = \mp\left(\frac{E}{\mathsf{S}E}\right)^m = \mp E^{2m},\ m \in \mathbb{Z}$$

implying that E is a root of unity. But E is a fundamental unit, so we get a contradiction.

To prove that all principle ambig ideals are generated by $\mathfrak{O}A$ and $\mathfrak{O}\sqrt{\delta}$, let $\mathfrak{O}B$ be an arbitrary ambig principle ideal. Then $\dfrac{B}{\mathsf{S}B} = \rho E^m$ where ρ is a root of unity and $N_{k(\sqrt{\delta})/k}(\dfrac{B}{\mathsf{S}B}) = N_{k(\sqrt{\delta})/k}(\rho)N_{k(\sqrt{\delta})/k}(E)^m = N_{k(\sqrt{\delta})/k}(\rho)(+1)^m = +1$ since $\mathfrak{O}B$ is an ambig ideal. Thus, $\rho = \mp 1$. Let $\rho = (-1)^n$ where $n = 0$ or $n = 1$, so for $\Gamma = B(\sqrt{\delta})^n A^{-m}$ we have,

$$\frac{\Gamma}{\mathsf{S}\Gamma} = B(\sqrt{\delta})^n A^{-m}\frac{1}{\mathsf{S}B}\frac{1}{(-\sqrt{\delta})^n}\frac{1}{(\mathsf{S}A)^{-m}} = \rho E^m(-1)^n E^{-m} = (-1)^{2n} = +1.$$

where $\Gamma \in k$, which implies that $\mathfrak{O}B$ does not give a new ambig ideal.

Now, let E be a fundamental unit such that $N_{k(\sqrt{\delta})/k}(E) = \mp i$. It is enough to consider the case that $N_{k(\sqrt{\delta})/k}(E) = i$ since for the case $N_{k(\sqrt{\delta})/k}(E) = -i$ we can take iE as a fundamental unit instead of E. We will prove that there is no principle ambig ideal different from $\mathfrak{O}$ and $\mathfrak{O}\sqrt{\delta}$. Assume for a contradiction that there exists an ambig principle ideal $\mathfrak{U} = \mathfrak{O}A$ different from $\mathfrak{O}$ and $\mathfrak{O}\sqrt{\delta}$, then necessarily $\dfrac{A}{\mathsf{S}A} = \rho E^m$ and $N_{k(\sqrt{\delta})/k} = 1$ implying that $N_{k(\sqrt{\delta})/k}(E^m) = N_{k(\sqrt{\delta})/k}(E)^m = \mp 1$ for $m \in Z$. Since we have that $N_{k(\sqrt{\delta})/k}(E) = 1$, m must be even. Then let us define $B = AE^{-m/2}$. Then we get $\dfrac{B}{\mathsf{S}B} = \dfrac{AE^{-m/2}}{\mathsf{S}A\mathsf{S}(E)^{-m/2}} = \rho E^m(\dfrac{E}{\mathsf{S}E})^{-m/2} = \rho E^m(-i\dfrac{iE}{\mathsf{S}E})^{-m/2} = \rho E^m(-i)^{-m/2}\left(\dfrac{E\cdot\mathsf{S}(E)\cdot E}{\mathsf{S}E}\right)^{-m/2} = \rho E^m(-i)^{-m/2}(E^2)^{-m/2} = \rho(-i)^{-m/2}$. Since we know $N_{k(\sqrt{\delta})/k}(\dfrac{B}{\mathsf{S}B}) = +1$, we get that $N_{k(\sqrt{\delta})/k}(\rho(-i)^{-m/2}) = N_{k(\sqrt{\delta})/k}(\rho)N_{k(\sqrt{\delta})/k}((-i)^{-m/2}) = N_{k(\sqrt{\delta})/k}(\rho)(-i.i)^{-m/2} = N_{K/k}(\rho) = +1$ implying that $\rho = \mp 1$. Here B is not divisible by any number in k. Therefore,

(i) if $\rho = +1$ then $\dfrac{B}{\mathsf{S}B} = \rho = +1$ implies that $B = \rho = +1$,
(ii) if $\rho = -1$ then $\dfrac{B}{\mathsf{S}B} = \rho = -1$ implies that $B = \rho\sqrt{\delta} = -\sqrt{\delta}$.

If $\delta = 3$, then $\mathrm{disc}_k(k(\sqrt{\delta})) = 3$, so the only principle ambig ideal is $\mathfrak{L} = \mathfrak{O}\sqrt{3}$ and $N_{K/k}(E) = \mp i$.

If $\delta = i$, then $\mathrm{disc}_k(k(\sqrt{\delta})) = 4i$, so the only principle ambig ideal is the divisor of $1 + i = (\sqrt{i})^2(1 - \sqrt{i})(1 + \sqrt{i})$, $\mathfrak{O}\sqrt{i}$ and $N_{K/k}(\sqrt{i}) = -i$. □

Remark 6.8.4. If δ is a prime number with $\delta \equiv \mp 1 \mod (1+i)^4$, then by the results in the proof of Theorem 6.8.3 we have $s = 1$ and $N_{k(\sqrt{\delta})/k}(E) = \mp i$ where E is a fundamental unit.

Theorem 6.8.5. *In the filed K there exists an ambig class which contains no ambig ideal if and only if i is in the principle genus and $N_{k(\sqrt{\delta})/k}(E) = \mp 1$ where E is a fundamental unit in $k(\sqrt{\delta})$.*

Proof. Let $\mathtt{C}$ be an ambig class which does not contain an ambig ideal and let $\mathfrak{I}$ be an ideal in $\mathtt{C}$. Then $\mathtt{C} = \mathsf{S}\mathtt{C}$ implies that $\dfrac{\mathfrak{I}}{\mathsf{S}\mathfrak{I}}$ is a number in $k(\sqrt{\delta})$, say A. We can assume that $N_{k(\sqrt{\delta})/k}(A) = +1$ or $= +i$, because if it is -1 or $-i$, then we can take iA instead of A.

Firstly assume that $N_{k(\sqrt{\delta})/k}(A) = +1$ and let $B = 1 + \mathsf{S}A$. Then,

$$\frac{B}{\mathsf{S}B} = \frac{1+\mathsf{S}A}{1+A} = \frac{A\cdot\mathsf{S}A + \mathsf{S}A}{1+A} = \mathsf{S}A \cdot \frac{A+1}{1+A} = \frac{1}{A}$$

since $A \cdot \mathsf{S}A = 1$. Then,

$$\frac{B\mathfrak{I}}{\mathsf{S}(B\mathfrak{I})} = \frac{B}{\mathsf{S}B} \cdot \frac{\mathfrak{I}}{\mathsf{S}(\mathfrak{I})} = \frac{1}{A} \cdot A = 1$$

implying that $B\mathfrak{I} = \mathsf{S}(B\mathfrak{I})$.

Let $B\mathfrak{I} = \dfrac{\alpha}{\beta}\mathfrak{U}$ where α, β are integers in k and $\mathfrak{U}$ is an ideal not divisible by any integer in k. Therefore, $\mathfrak{U}$ is an ambig ideal and $\mathfrak{U} = \dfrac{\beta}{\alpha}B\mathfrak{I} = \dfrac{\beta}{\alpha}(1+\mathsf{S}A)\mathfrak{A} = \dfrac{\beta}{\alpha}(1+\dfrac{\mathsf{S}\mathfrak{I}}{\mathfrak{I}})\mathfrak{I} = \dfrac{\beta}{\alpha}(\mathfrak{I}+\mathsf{S}\mathfrak{I})$, so $\mathfrak{U}$ is in the ideal class $\mathtt{C}$.

Secondly, assume that $N_{k(\sqrt{\delta})/k}(A) = +i$. Then i is in the principle genus. Now $N_{k(\sqrt{\delta})/k}(E) = +1$ or $+i$ where E is a fundamental unit in $k(\sqrt{\delta})$.

If $N_{k(\sqrt{\delta})/k}(E) = +i$, then we take $\dfrac{A}{E}$ instead of A and get the first case above since $N_{k(\sqrt{\delta})/k}(\dfrac{A}{E}) = \dfrac{N_{k(\sqrt{\delta})/k}(A)}{N_{k(\sqrt{\delta})/k}(E)} = \dfrac{i}{i} = 1$.

If $N_{k(\sqrt{\delta})/k}(E) = +1$, then we will show that the ideal class $\mathtt{C}$ contains no ambig ideal. For a contradiction assume that $\mathtt{C}$ contains an ambig ideal $\mathfrak{U} = B\mathfrak{I}$ for some number $B \in k(\sqrt{\delta})$. Then $\dfrac{\mathfrak{U}}{\mathsf{S}\mathfrak{U}} = \dfrac{B}{\mathsf{S}B} \cdot \dfrac{\mathfrak{I}}{\mathsf{S}\mathfrak{I}} = \dfrac{B}{\mathsf{S}B}A$ for some number $A \in k(\sqrt{\delta})$ since $\mathtt{C}$ is an ambig class and $\mathfrak{I} \in \mathtt{C}$. But $\mathfrak{U}$ is an ambig ideal, so $\dfrac{\mathfrak{U}}{\mathsf{S}\mathfrak{U}}$ must be a unit, say ρE^m where E is a fundamental unit. Here $N_{k(\sqrt{\delta})/k}(E) = +1$, then we

get $N_{k(\sqrt{\delta})/k}(\frac{B}{\mathsf{S}B})N_{k(\sqrt{\delta})/k}(A) = N_{k(\sqrt{\delta})/k}(\rho E^m)$ implying that $\frac{B\mathsf{S}(B)}{\mathsf{S}(B)B}N_{k(\sqrt{\delta})/k}(A) = N_{k(\sqrt{\delta})/k}(\rho)N_{k(\sqrt{\delta})/k}(E)^m = (\mp 1)1^m = \mp 1$, which contradicts our assumption that $N_{k(\sqrt{\delta})/k}(A) = i$.

Conversely, assume that i is in the principle genus. Then there exists a number $A \in K$ such that $N_{K/k}(A) = i$ by Theorem 6.6.4. Here, $N_{k(\sqrt{\delta})/k}(E) = +1$ implies that A is not a unit, so A is factorizable, say $A = \frac{\mathfrak{I}}{\mathfrak{I}'}$ where $\mathfrak{I}$ and $\mathfrak{I}'$ are relatively prime ideals in $k(\sqrt{\delta})$. Then $N_{k(\sqrt{\delta})/k}(A) = A \cdot \mathsf{S}A = \frac{\mathfrak{I}\mathsf{S}(\mathfrak{I})}{\mathfrak{I}'\mathsf{S}(\mathfrak{I}')} = +1$ implies that $\mathfrak{I}' = \mathsf{S}(\mathfrak{I})$. The ideal $\mathfrak{I}$ is equivalent to $\mathsf{S}\mathfrak{I}$ since $\mathfrak{I}$ is in the ambig class $\mathtt{C}$. Thus $\mathtt{C}$ does not contain an ambig ideal. □

Theorem 6.8.6. *If there exists an ideal class $\mathtt{C}$ in the field K that does not contain any ambig ideal, and if $\mathfrak{U}$ is an ideal in $\mathtt{C}$, then all other ambig ideal classes that do not contain any ambig ideal are formed by $\mathtt{C}\mathtt{C}_1 \ldots \mathtt{C}_n$ where $\mathtt{C}_i$'s are ambig classes arising from an ambig ideal.*

Proof. The ambig classes that do not contain an ambig ideal, contain ideals $\mathfrak{I}$, $\mathfrak{I}'$ such that $\mathfrak{I}$ and $\mathfrak{I}'$ are relatively prime with $\mathfrak{I}' = \mathsf{S}(\mathfrak{I})$, and for $A = \frac{\mathfrak{A}}{\mathfrak{I}'}$, and A' $N_{K/k}(A) = N_{K/k}(\frac{\mathfrak{I}}{\mathfrak{I}'}) = N_{K/k}(\frac{\mathfrak{I}}{\mathsf{S}\mathfrak{I}}) = \mp i$ and $N_{K/k}(A') = N_{K/k}(\frac{\mathfrak{I}'}{\mathsf{S}(\mathfrak{I}')}) = N_{K/k}(\frac{\mathfrak{I}'}{\mathfrak{I}}) = N_{K/k}\frac{1}{A} = \mp i$, so $N_{K/k}(\frac{A}{A'}) = \mp 1$ and for $B = 1 + \frac{\mathsf{S}A}{\mathsf{S}A'}$ we get that

$$\frac{B}{\mathsf{S}B} = \frac{1 + \frac{\mathsf{S}A}{\mathsf{S}A'}}{1 + \frac{A}{A'}} = \frac{1 + \frac{A'}{A}}{1 + \frac{A}{A'}} = \frac{A + A'}{A}\frac{A'}{A' + A} = \frac{A'}{A}.$$

Thus, $B\frac{\mathfrak{I}}{\mathfrak{I}'} = BA = \mathsf{S}(B)A' = \mathsf{S}(B)\frac{\mathfrak{I}'}{\mathfrak{I}} = \mathsf{S}(B)\frac{\mathsf{S}(\mathfrak{I})}{\mathsf{S}(\mathfrak{I}')} = \mathsf{S}(B\frac{\mathfrak{I}}{\mathfrak{I}'})$. Let $B\frac{\mathfrak{I}}{\mathfrak{I}'} = \frac{\alpha}{\beta}\mathfrak{U}$ where α and β are integers in k, and $\mathfrak{U}$ is not divisible by any integer in k. Thus $\mathfrak{U}$ is an ambig ideal equivalent to $\frac{\mathfrak{I}}{\mathfrak{I}'}$. □

The results obtained untill now make us to guess the number of different ambig classes:

Theorem 6.8.7. *There exist $c - 1$ independent ambig classes where c is the number*

of individual characters which determine the genus of a class. The total number of distinct ambig ideal classes is thus 2^{c-1}.

Proof. If i is in the principle genus, then by Theorem 6.8.3, Theorem 6.8.5 and Theorem 6.8.6, there exist 2^{s-1} ambig classes where s is the number of distinct prime divisors of $\mathrm{disc}_k(k(\sqrt{\delta}))$ of the field $k(\sqrt{\delta})$; of these 2^{s-1} ambig classes either all or only half arise from ambig ideals according as $N_{k(\sqrt{\delta})/k}(E) = \mp i$ or ∓ 1 where E is a fundamental unit in $k(\sqrt{\delta})$.

If i is not in the principle genus, then necessarily $N_{k(\sqrt{\delta})/k}(E) = \mp 1$ where E is a fundamental unit in $k(\sqrt{\delta})$. By Theorem 6.8.3 and Theorem 6.8.5, there exist 2^{s-2} ambig classes and all arise from ambig ideals.

Let $c = s$ or $c = s - 1$ according to the fact that i is in the principle genus or not. Thus we get the desired result. □

6.9. The Number of Genera

The results obtained in Chapter 6.6, Chapter 6.7 and Chapter 6.8 make us guess the number of genera of Dirichlet number field $k(\sqrt{\delta})$. The character system of an ideal class consists of c individual characters, each one has value +1 or -1. Then there are 2^c possible character systems. We come across that question: For each of these 2^c character systems are there a genera or do only some of them represent a genus?

Theorem 6.9.1. *The number of genera is half of the all possible character systems, that is* 2^{c-1} *where* c *is the number of individual characters.*

Proof. Let g be the number of distinct genera and f be the number of classes in the principle genus. Each genus contains f many classes, so the number of all classes in the field is gf.

Let $\mathtt{H}_1, \ldots, \mathtt{H}_f$ be the classes in the principle genus, then by 6.6.1 $\mathtt{H}_1 = \mathtt{Q}_1^2, \ldots, \mathtt{H}_f = \mathtt{Q}_f^2$ for some classes $\mathtt{Q}_1, \ldots, \mathtt{Q}_f$ in K. Let $\mathtt{C}$ be an arbitrary class in K, then $\mathtt{C}^2$ is in the principle genus, so $\mathtt{C}^2 = \mathtt{Q}_r^2$ where $\mathtt{Q}_r$ for some $r \in \{1, \ldots, n\}$. Then the ideal class $\mathtt{A} = \frac{\mathtt{C}}{\mathtt{Q}_r}$ is ambig since $\mathtt{A}^2 = \mathtt{1}$ and $\mathtt{AS}(\mathtt{A}) = \mathtt{1}$ imply together that $\mathtt{A} = \mathtt{S}(\mathtt{A})$. By Theorem 6.8.7 the number of all differeent ambig classes is 2^{c-1}, so the number of all classes $\mathtt{C} = \mathtt{AQ}$ is $2^{c-1}f$ since each class of the form $\mathtt{AQ}$ represents a different class, because if not $\mathtt{AQ}_r = \mathtt{A}'\mathtt{Q}_{r'}$ for some ambig class $\mathtt{A}'$ and for some $r' \in \{1, \ldots, n\}$. Then $\mathtt{A}^2 = \mathtt{A}'^2 = \mathtt{1}$, and $\mathtt{A}^2\mathtt{Q}_r^2 = \mathtt{A}'^2\mathtt{Q}_{r'}^2$ implies $\mathtt{Q}_r^2 = \mathtt{Q}_{r'}^2$, so $\mathtt{H}_r = \mathtt{H}_{r'}$ and $r = r'$. Thus $\mathtt{A} = \mathtt{A}'$ and $\mathtt{Q}_r = \mathtt{Q}_{r'}$.

We have $2^{c-1}f = gf$ different classes, so $g = 2^{c-1}$. Thus we get the desired result. □

6.10. The Reciprocity Law

We have concluded that only half of the character systems represent a genus. Now we have a new question: Which of the character systems represent a genus? The question was answered when Dirichlet assigned the reciprocity law for integers in k.

Theorem 6.10.1. *Let κ be a prime number in k such that $\kappa \equiv (t_\kappa t'_\kappa) \mod (1+i)^4$, then $\left[\frac{i}{\kappa}\right] = (-1)^{t'_\kappa}$.*

Proof. Let $\kappa \neq 1+i$ be a prime number in k such that $\kappa \equiv (00) \mod (1+i)^4$. Then by Remark 6.8.4 $N_{k(\sqrt{\kappa})/k}(E) = \mp i$ where E is a fundamental unit in $k(\sqrt{\kappa})$, so $\left[\frac{i}{\kappa}\right] = \left[\frac{i}{\kappa : \kappa}\right] = \left[\frac{N_{k(\sqrt{\kappa}))/k}(E)}{\kappa : \kappa}\right] = +1$ by Definition 6.3.3 and i is a quadratic residue modulo κ by Definition 6.2.6.

Let $\kappa \neq 1+i$ be a prime number in k such that $\kappa \equiv (10) \mod (1+i)^4$. Then $i\kappa \equiv i.i = -1 = (00) \mod (1+i)^4$ and by Remark 6.8.4 $N_{k(\sqrt{i\kappa})/k}(E) = \mp i$ where E is a fundamental unit in $k(\sqrt{i\kappa})$, so $\left[\frac{i}{\kappa}\right] = \left[\frac{i}{\kappa : i\kappa}\right] = \left[\frac{N_{k(\sqrt{i\kappa})/k}(E)}{\kappa : i\kappa}\right] = +1$ by Definition 6.3.3 and i is a quadratic residue modulo κ by Definition 6.2.6.

We have showed that $\left[\frac{i}{\kappa}\right] = +1$, if $t'_\kappa = 0$. Conversely, assume that $\left[\frac{i}{\kappa}\right] = +1$. The discriminant $\mathrm{disc}_k(k(\sqrt{i})) = 4i$ by Theorem 6.1.1, so $1+i$ is the only prime divisor of $\mathrm{disc}_k(k(\sqrt{i}))$. We have $\left[\frac{i}{1+i:i}\right] = \left[\frac{N_{k(\sqrt{i})/k}(i\sqrt{i})}{1+i:i}\right] = +1$ by Definition 6.3.3. Then by Theorem 6.9.1, the number of genera is $2^{1-1} = 1$. Then particularly, $\left[\frac{\kappa}{1+i:i}\right] = +1$. Thus, if $\left[\frac{i}{\kappa}\right] = +1$, then $+1 = \left[\frac{\kappa}{1+i:i}\right] = (-1)^{t_\kappa t'_i + t'_\kappa t_i} = (-1)^{t_\kappa 0 + t'_\kappa 1}$ implies that $t'_\kappa = 0$.

Hence, we have shown that $\left[\frac{i}{\kappa}\right] = +1$ if and only if $t'_\kappa = 0$. So if $\left[\frac{i}{\kappa}\right] = -1$, then $t'_\kappa = 1$ and vice versa. □

Theorem 6.10.2. *Let κ be a prime number in k such that $\kappa \equiv (t_\kappa t'_\kappa t''_\kappa) \mod (1+i)^5$, then $\left[\frac{1+i}{\kappa}\right] = (-1)^{t'_\kappa + t''_\kappa}$.*

Proof. Let $\kappa \neq 1+i$ be a prime number in k such that $\kappa \equiv (000) \mod (1+i)^5$. The discriminant $\mathrm{disc}_k(k(\sqrt{\kappa})) = \kappa$ by Theorem 4.1.1, and $\left[\frac{i}{\kappa:\kappa}\right] = \left[\frac{i}{\kappa}\right] = (-1)^{t'_\kappa} = +1$. Then by Theorem 6.9.1, the number of genera is $2^{1-1} = 1$. Then particularly, $\left[\frac{1+i}{\kappa:\kappa}\right] = \left[\frac{1+i}{\kappa}\right] = (-1)^{t'_\kappa} = +1$ by Theorem 6.10.1.

Let $\kappa \neq 1+i$ be a prime number in k such that $\kappa \equiv (100) \mod (1+i)^5$. Then $i\kappa \equiv i.i = -1 = (000) \mod (1+i)^5$ and the discriminant is $\mathrm{disc}_k(k(\sqrt{i\kappa})) = i\kappa$ by Theorem 6.1.1, and $\left[\frac{i}{\kappa:i\kappa}\right] = \left[\frac{i}{\kappa}\right] = +1$. Then by Theorem 6.9.1, the number of genera is $2^{1-1} = 1$. Then particularly, $\left[\frac{1+i}{\kappa:i\kappa}\right] = \left[\frac{1+i}{\kappa}\right] = +1$.

For the converse, let us now consider first the field $k(\sqrt{1+i})$. Let $\kappa \neq 1+i$ be a prime number such that $\kappa \equiv (t_\kappa 0 t''_\kappa) \mod (1+i)^5$. Assume $\left[\frac{1+i}{\kappa}\right] = +1$. The discriminant is $\mathrm{disc}_k(k(\sqrt{1+i})) = 4(1+i)$ by Theorem 4.1.1, so $1+i$ is the only prime divisor of $\mathrm{disc}_k(k(\sqrt{1+i}))$. We have $\left[\frac{i}{1+i:1+i}\right] = \left[\frac{i}{1+i}\right] = (-1)^{t'_{1+i}} = (-1)^0 = +1$ by Theorem 6.10.1. Then by Theorem 6.9.1, the number of genera is $2^{1-1} = 1$. Then particularly, $\left[\frac{\kappa}{1+i:1+i}\right] = +1$. Thus, if $\left[\frac{1+i}{\kappa}\right] = +1$ then $(-1)^{t_\kappa t'_{1+i} + t'_\kappa t_{1+i} + t'_\kappa + t''_\kappa} = (-1)^{t_\kappa .0 + t'_\kappa .0 + 0 + t''_\kappa} = (-1)^{t''_\kappa} = +1$, so $t''_\kappa = 0$. Thus, if $t'_\kappa = 0$ then $\left[\frac{1+i}{\kappa}\right] = (-1)^{t''_\kappa}$.

Lastly, let us now consider the field $k(\sqrt{(1+i)\kappa})$. Let κ be a prime number such that $\kappa \equiv (t_\kappa 1 t''_\kappa) \mod (1+i)^5$. Assume $\left[\frac{1+i}{\kappa}\right] = +1$. The relative discriminant $\mathrm{disc}_k(k(\sqrt{(1+i)\kappa})) = 4(1+i)\kappa$ by Theorem 6.1.1, so $1+i$ and κ are the only prime divisors of $\mathrm{disc}_k(k(\sqrt{(1+i)\kappa}))$, that is $s = 2$. We have $\left[\frac{i}{1+i:(1+i)\kappa}\right] = \left[\frac{i}{1+i}\right] = (-1)^{t'_{1+i}} = (-1)^0 = +1$ by Theorem 6.10.1. Then by Theorem 6.9.1, the number of genera is $2^{2-1} = 2$. Then, $\left(\left[\frac{\kappa}{1+i:(1+i)\kappa}\right], \left[\frac{\kappa}{\kappa:(1+i)\kappa}\right]\right) = (+1,+1)$ or $(-1,-1)$. But $\left[\frac{(1+i)\kappa}{\kappa:(1+i)\kappa}\right] = \left[\frac{N_{k(\sqrt{\delta})/k}(k(\sqrt{(1+i)\kappa}))k(i\sqrt{(1+i)\kappa})}{\kappa:(1+i)\kappa}\right] = +1$ and $\left[\frac{1+i}{\kappa:(1+i)\kappa}\right] = \left[\frac{1+i}{\kappa}\right] = +1$ by assumption imply together that $\left[\frac{\kappa}{\kappa:(1+i)\kappa}\right] = +1$. So we get $\left[\frac{\kappa}{1+i:(1+i)\kappa}\right] = +1$. Thus, if $\left[\frac{1+i}{\kappa}\right] = +1$, then we get that $(-1)^{t_\kappa(t'_{1+i}+t'_\kappa)+t'_\kappa(t_{1+i}+t_\kappa)+t'_\kappa+t''_\kappa} = (-1)^{t_\kappa.(0+1)+1.(0+t_\kappa)+1+t''_\kappa} = (-1)^{1+t''_\kappa} = +1$ implies $t''_\kappa = 1$. Thus, if $t'_\kappa = 1$, then $\left[\frac{1+i}{\kappa}\right] = (-1)^{1+t''_\kappa}$. □

Theorem 6.10.3. *Let κ and π be prime numbers in k different from $1+i$ such that $\kappa \equiv (t_\kappa t'_\kappa)$ and $\pi \equiv (t_\pi t'_\pi) \mod (1+i)^4$. Then*

$$\left[\frac{\kappa}{\pi}\right]\left[\frac{\pi}{\kappa}\right] = (-1)^{t_\kappa t'_\pi + t'_\kappa t_\pi}.$$

Proof. Let κ and π be prime numbers in k different from $1+i$ such that $\kappa \equiv (t_\kappa t'_\kappa)$ and $\pi \equiv (t_\pi t'_\pi) \mod (1+i)^4$.

Firstly, let $t_\kappa = 0$ and $t_\pi = 0$.

If $\kappa \equiv (00) \mod (1+i)^4$, then $\mathrm{disc}_k(k(\sqrt{\kappa})) = \kappa$. Then by Theorem 6.9.1, the number of genera is $2^{1-1} = 1$, so every ideal is in the principle genus. Assume that $\left[\frac{\kappa}{\pi}\right] = +1$, then $\pi = \mathfrak{B}\mathsf{S}(\mathfrak{B})$ for some prime ideal $\mathfrak{B}$ in the principle genus of $k(\sqrt{\kappa})$ with $\mathfrak{B} \neq \mathsf{S}(\mathfrak{B})$. Then by Theorem 6.6.2, $\kappa = N_{k(\sqrt{\delta})/k}(\mathfrak{A})$ for some ideal $\mathfrak{A}$ in the

principl egenus of $k(\sqrt{\pi})$. Then, $\left[\frac{\pi}{\kappa}\right] = +1$ by Theorem 6.2.7. As a result, we get that,

$$\text{if } \kappa \equiv (00),\ \pi \equiv (00) \mod (1+i)^4 \text{ and } \left[\frac{\kappa}{\pi}\right] = +1,\ \text{then } \left[\frac{\pi}{\kappa}\right] = +1 \tag{6.2}$$

$$\text{if } \kappa \equiv (00),\ \pi \equiv (01) \mod (1+i)^4 \text{ and } \left[\frac{\kappa}{\pi}\right] = +1,\ \text{then } \left[\frac{\pi}{\kappa}\right] = +1 \tag{6.3}$$

Now let $\kappa \equiv (01) \mod (1+i)^4$. Then $\mathrm{disc}_k(k(\sqrt{\kappa})) = -2i\kappa$, so $s = 2$. And $\left[\frac{i}{\kappa : \kappa}\right] = \left[\frac{i}{\kappa}\right] = (-1)^{t'_\kappa} = -1$ implies that i is not in the principle genus. So by Theorem 6.9.1, the number of genera is $2^{2-2} = 1$. If $\left[\frac{\kappa}{\pi}\right] = +1$, then $\pi = \mathfrak{B}\mathsf{S}(\mathfrak{B})$ for some prime ideal $\mathfrak{B}$ in $k(\sqrt{\kappa})$ with $\mathfrak{B} \neq \mathsf{S}(\mathfrak{B})$. Then $\pi = N_{k(\sqrt{\kappa})/k}(\mathfrak{B})$, and $\left[\frac{\pi}{(1+i)\kappa}\right] = +1$ by Theorem 6.2.7. Then, $\left[\frac{\pi}{1+i : \kappa}\right] = \left[\frac{\pi}{\kappa : \kappa}\right] = \left[\frac{\pi}{\kappa}\right] = +1$ or $\left[\frac{\pi}{1+i : \kappa}\right] = \left[\frac{\pi}{\kappa : \kappa}\right] = \left[\frac{\pi}{\kappa}\right] = -1$. As a result, we get,

$$\text{if } \kappa \equiv (01),\ \pi \equiv (00) \mod (1+i)^4 \text{ and } \left[\frac{\kappa}{\pi}\right] = +1,\ \text{then } \left[\frac{\pi}{\kappa}\right] = +1 \tag{6.4}$$

$$\text{if } \kappa \equiv (01),\ \pi \equiv (01) \mod (1+i)^4 \text{ and } \left[\frac{\kappa}{\pi}\right] = +1,\ \text{then } \left[\frac{\pi}{\kappa}\right] = +1 \tag{6.5}$$

In the Equation 6.2 π and κ are symmetric, so if $\left[\frac{\kappa}{\pi}\right] = -1$ then $\left[\frac{\pi}{\kappa}\right] = -1$ where $t'_\kappa = t'_\pi = 0$.

In the Equation 6.3 if $\left[\frac{\kappa}{\pi}\right] = +1$, then $\left[\frac{\pi}{\kappa}\right] = +1$ where $t'_\kappa = 0$, $t'_\pi = 1$. Also in the Equation 6.4 if $\left[\frac{\kappa}{\pi}\right] = +1$, then $\left[\frac{\pi}{\kappa}\right] = +1$ where $t'_\kappa = 1$, $t'_\pi = 0$. Thus, if $\left[\frac{\kappa}{\pi}\right] = -1$, then $\left[\frac{\pi}{\kappa}\right] = -1$ by using Equation 6.3 and Equation 6.4.

In the Equation 6.5 π and κ are symmetric, so if $\left[\frac{\kappa}{\pi}\right] = -1$, then $\left[\frac{\pi}{\kappa}\right] = -1$ where $t'_\kappa = t'_\pi = 1$.

If $t_\kappa \neq 0$ or $t_\pi \neq 0$, then we put $(i)^{t_\kappa}\kappa$ and $(i)^{t_\pi}\pi$ instead of κ and π respectively.

□

Definition 6.10.4. If $\alpha = \prod^{\kappa} \kappa$ and $\beta = \prod^{\pi} \pi$ are relatively prime integers not divisible by $1+i$, then the Jacobi symbol for imaginary numbers is defined as

$$\left[\frac{\alpha}{\beta}\right] = \prod^{\kappa,\pi} \left[\frac{\kappa}{\pi}\right].$$

Theorem 6.10.5. *Let α and β be relatively prime numbers in k not divisible by $1+i$ such that $\alpha \equiv (t_\alpha t'_\alpha)$ and $\beta \equiv (t_\beta t'_\beta) \mod (1+i)^4$. Then*

$$\left[\frac{\alpha}{\beta}\right]\left[\frac{\beta}{\alpha}\right] = (-1)^{t_\alpha t'_\beta + t'_\alpha t_\beta}.$$

Theorem 6.10.6. *A character system represents a genus if and only if the product of all unique characters is equal to +1.*

Proof. Firstly, assume that δ is not divisible by $1+i$. Also let $\upsilon = N_{k(\sqrt{\delta})/k}(\mathfrak{I})$ for some ideal $\mathfrak{I}$ in $k(\sqrt{\delta})$ such that υ is relatively prime to δ and not divisible by $1+i$. Then by Lemma 6.3.1, δ is a quadratic residue modulo each prime divisor of υ, so $\left[\frac{\delta}{\upsilon}\right] = +1$. By Theorem 6.10.5, $\left[\frac{\upsilon}{\delta}\right] = (-1)^{t_{\delta t'_\upsilon + t_\upsilon t'_\delta}}$. Now we have two cases,

Case 1: If $\delta \equiv (00) \mod (1+i)^4$, then $\mathrm{disc}_k(k(\sqrt{\delta})) = \delta$, and if $\lambda_1, \ldots, \lambda_s$ are the all prime divisors of δ, then $\left[\frac{\upsilon}{\lambda_1 : \delta}\right] \cdots \left[\frac{\upsilon}{\lambda_s : \delta}\right] = \left[\frac{\upsilon}{\lambda_1}\right] \cdots \left[\frac{\upsilon}{\lambda_s}\right] = \left[\frac{\upsilon}{\delta}\right] = (-1)^{t_{\delta t'_\upsilon + t_\upsilon t'_\delta}} = +1$

Case 2: If $\delta \not\equiv (00) \mod (1+i)^4$, then $(1+i) \mid \mathrm{disc}_k(k(\sqrt{\delta}))$, and if we also have $\lambda_1, \ldots, \lambda_{s-1}, \lambda_s = 1+i$ are the all prime divisors of $\mathrm{disc}_k(k(\sqrt{\delta}))$, then

$$\left[\frac{\upsilon}{\lambda_1 : \delta}\right] \cdots \left[\frac{\upsilon}{\lambda_{s-1} : \delta}\right]\left[\frac{\upsilon}{\lambda_s : \delta}\right] = \left[\frac{\upsilon}{\lambda_1 : \delta}\right] \cdots \left[\frac{\upsilon}{\lambda_{s-1} : \delta}\right](-1)^{t_\upsilon t'\delta + t'_\upsilon t_\delta}$$

$$\begin{aligned} &= \left[\frac{\upsilon}{\lambda_1}\right]\cdots\left[\frac{\upsilon}{\lambda_{s-1}}\right](-1)^{t_\upsilon t'\delta+t'_\upsilon t_\delta} \\ &= \left[\frac{\upsilon}{\delta}\right](-1)^{t_\upsilon t'\delta+t'_\upsilon t_\delta} \\ &= (-1)^{2(t_\upsilon t'\delta+t'_\upsilon t_\delta)} = +1. \end{aligned}$$

Secondly, assume that δ is divisible by $1+i$. We put $\delta = (1+i)\delta'$ and υ as above, so δ is a quadratic residue modulo each prime divisor of υ, so $\left[\frac{\delta}{\upsilon}\right] = +1$. Then $\left[\frac{\delta'}{\upsilon}\right]\left[\frac{1+i}{\upsilon}\right] = \left[\frac{\delta'}{\upsilon}\right](-1)^{t'_{upsilon}+t''_\upsilon} = +1$ by Theorem 6.10.2. Thus, $\left[\frac{\delta'}{\upsilon}\right] = (-1)^{t'_{upsilon}+t''_\upsilon}$. By Theorem 6.10.5 $\left[\frac{\upsilon}{\delta'}\right]\left[\frac{\delta'}{\upsilon}\right] = (-1)^{t_{\delta'}t'_\upsilon+t'_{\delta'}t_\upsilon}$, therefore we get that $\left[\frac{\upsilon}{\delta'}\right] = (-1)^{t_{\delta'}t'_\upsilon+t'_{\delta'}t_\upsilon+t'_{upsilon}+t''_\upsilon}$. Hence,

$$\begin{aligned} \left[\frac{\upsilon}{\lambda_1:\delta}\right]\cdots\left[\frac{\upsilon}{\lambda_s:\delta}\right] &= \left[\frac{\upsilon}{\delta':\delta}\right]\left[\frac{\upsilon}{1+i:\delta}\right] \\ &= \left[\frac{\upsilon}{\delta'}\right](-1)^{t_{\delta'}t'_\upsilon+t'_{\delta'}t_\upsilon+t'_{upsilon}+t''_\upsilon} \\ &= (-1)^{2(t_{\delta'}t'_\upsilon+t'_{\delta'}t_\upsilon+t'_{upsilon}+t''_\upsilon)} \\ &= +1 \text{ by Definition 6.3.5.} \end{aligned}$$

□

APPENDIX A: SOME CALCULATIONS

Theorem A.0.7.

$$\begin{aligned} disc_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m})) &= 4m, \quad if \quad m \equiv 2,3 \pmod 4 \\ disc_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m})) &= m, \quad if \quad m \equiv 1 \pmod 4. \end{aligned}$$

Proof. $\text{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m})) = \det \begin{pmatrix} 1 & \omega \\ 1 & \omega' \end{pmatrix}^2 = (\omega - \omega')^2$, so if $m \equiv 2,3 \pmod 4$, then $\omega = \sqrt{m}$ by Theorem 4.1.1, so $\text{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m})) = \det \begin{pmatrix} 1 & \sqrt{m} \\ 1 & -\sqrt{m} \end{pmatrix}^2 = (-\sqrt{m} - \sqrt{m})^2 = 4m$. But if $m \equiv 1 \pmod 4$, then $\omega = \dfrac{1+\sqrt{m}}{2}$ by Theorem 4.1.1, so $\text{disc}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{m})) = \det \begin{pmatrix} 1 & \frac{1+\sqrt{m}}{2} \\ 1 & \frac{1-\sqrt{m}}{2} \end{pmatrix}^2 = (\dfrac{1-\sqrt{m}}{2} - \dfrac{1+\sqrt{m}}{2})^2 = (-\sqrt{m})^2 = m$. □

Lemma A.0.8. *If $f(x,y)$ is an integer polynomial, homogeneous of degree 2 in x and y, and n is an odd rational integer then, if the congruence $f(x,y) \equiv n \pmod{2^3}$ has rational integer solutions for x and y, then so do all the congruences $f(x,y) \equiv n \pmod{2^{e+1}}$ for all $e \geq 3$.*

Proof. Proof is by induction on e. So suppose that a and b are rational integers for which $n \equiv f(a,b) \pmod{2^e}$, where the exponent $e \geq 3$. If we do not also have $n \equiv f(a,b) \pmod{2^{e+1}}$, but rather than $n \equiv f(a,b) + 2^e \pmod{2^{e+1}}$, then we determine a rational integer c such that $c^2 \equiv 1 + 2^e \pmod{2^{e+1}}$ by choosing $c = 1 + 2^{e-1}$. Then,

$$\begin{aligned} f(ca,cb) &\equiv c^2 f(a,b) \pmod{2^{e+1}} \text{ since } f \text{ is homogeneous,} \\ &\equiv f(a,b) + 2^e f(a,b) \pmod{2^{e+1}} \\ &\equiv f(a,b) + 2^e - 2^e + 2^e f(a,b) \pmod{2^{e+1}} \\ &\equiv f(a,b) + 2^e + 2^e(f(a,b) - 1) \pmod{2^{e+1}} \\ &\equiv f(a,b) + 2^e \pmod{2^{e+1}} \text{ since } f(a,b) - 1 \text{ is even,} \\ &\equiv n \pmod{2^{e+1}}. \end{aligned}$$

So claim is proved. □

Lemma A.0.9. *Let n be an odd integer and m be a squarefree integer. The congruence, $n \equiv N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha) \mod 2^3$ is solvable for some $\alpha \in \mathfrak{O}$ if and only if $(m,n) = (1,1),(1,3),(1,5),(1,7),(2,1),(2,7),(3,1),(3,5),(5,1),(5,3),(5,5),(5,7),(6,1),(6,3),(7,1)$ or $(7,5)$ modulo 8.*

Proof. To investigate for which combinations of values of n and m, the congruence $n \equiv N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha) \mod 2^3$ is solvable for some $\alpha \in \mathfrak{O}$, by Theorem 4.1.1, we will investigate the congruences

$$n \equiv x^2 + xy - \frac{m-1}{4}y^2 \mod 2^3 \quad \text{if } m \equiv 1 \mod 4, \tag{A.1}$$

$$n \equiv x^2 - my^2 \mod 2^3 \quad \text{if } m \equiv 2,3 \mod 4 \tag{A.2}$$

are solvable in integers x and y. It is enough by Lemma A.0.8.

If $m \equiv 1 \mod 8$, then $n \equiv x^2 + xy \mod 8$. Then

If $(x,y) = (0,0)$, then $n \equiv 0 \mod 8$,
If $(x,y) = (0,1)$, then $n \equiv 0 \mod 8$, same as $(x,y) = (0,0)$.

If $(x,y) = (1,0)$, then $n \equiv 1 \mod 8$,
If $(x,y) = (1,1)$, then $n \equiv 1+1 = 2 \mod 8$,
If $(x,y) = (1,2)$, then $n \equiv 1+2 = 3 \mod 8$,
If $(x,y) = (1,3)$, then $n \equiv 1+3 = 4 \mod 8$,
If $(x,y) = (1,4)$, then $n \equiv 1+4 = 5 \mod 8$,
If $(x,y) = (1,5)$, then $n \equiv 1+5 = 6 \mod 8$,
If $(x,y) = (1,6)$, then $n \equiv 1+6 = 7 \mod 8$,
If $(x,y) = (1,7)$, then $n \equiv 1+7 = 0 \mod 8$.

Therefore, $n \equiv 1,3,5,7 \mod 8$.

If $m \equiv 2$,then $n \equiv x^2 - 2y^2 \mod 8$. Then

If $(x, y) = (0, 0)$, then $n \equiv 0 \mod 8$,
If $(x, y) = (0, 1)$, then $n \equiv 6 \mod 8$,
If $(x, y) = (0, 2)$, then $n \equiv 0 \mod 8$, same as $(x, y) = (0, 0)$.

If $(x, y) = (1, 0)$, then $n \equiv 1 \mod 8$,
If $(x, y) = (1, 1)$, then $n \equiv 7 \mod 8$,
If $(x, y) = (1, 2)$, then $n \equiv 1 \mod 8$, same as $(x, y) = (1, 0)$.

If $(x, y) = (2, 0)$, then $n \equiv 4 \mod 8$,
If $(x, y) = (2, 1)$, then $n \equiv 2 \mod 8$,
If $(x, y) = (2, 2)$, then $n \equiv 4 \mod 8$, same as $(x, y) = (2, 0)$.

If $(x, y) = (3, 0)$, then $n \equiv 1 \mod 8$,
If $(x, y) = (3, 1)$, then $n \equiv 7 \mod 8$,
If $(x, y) = (3, 2)$, then $n \equiv 1 \mod 8$, same as $x = 1$.

Therefore, $n \equiv 1, 7 \mod 8$.

If $m \equiv 3$, then $n \equiv x^2 - 3y^2 \mod 8$. Then

If $(x, y) = (0, 0)$, then $n \equiv 0 \mod 8$,
If $(x, y) = (0, 1)$, then $n \equiv 5 \mod 8$,
If $(x, y) = (0, 2)$, then $n \equiv 4 \mod 8$,
If $(x, y) = (0, 3)$, then $n \equiv 5 \mod 8$,
If $(x, y) = (0, 4)$, then $n \equiv 0 \mod 8$, same as $(x, y) = (0, 0)$.

If $(x, y) = (1, 0)$, then $n \equiv 1 \mod 8$,
If $(x, y) = (1, 1)$, then $n \equiv 6 \mod 8$,
If $(x, y) = (1, 2)$, then $n \equiv 5 \mod 8$,

$$\begin{array}{llll}
\text{If} & (x,y)=(1,3), & \text{then} & n\equiv 6 \mod 8, \\
\text{If} & (x,y)=(1,4), & \text{then} & n\equiv 1 \mod 8, \text{ same as } (x,y)=(1,0).
\end{array}$$

$$\begin{array}{llll}
\text{If} & (x,y)=(2,0), & \text{then} & n\equiv 4 \mod 8, \\
\text{If} & (x,y)=(2,1), & \text{then} & n\equiv 1 \mod 8, \\
\text{If} & (x,y)=(2,2), & \text{then} & n\equiv 0 \mod 8, \\
\text{If} & (x,y)=(2,3), & \text{then} & n\equiv 1 \mod 8, \\
\text{If} & (x,y)=(2,4), & \text{then} & n\equiv 4 \mod 8, \text{ same as } (x,y)=(2,0).
\end{array}$$

$$\begin{array}{llll}
\text{If} & (x,y)=(3,0), & \text{then} & n\equiv 1 \mod 8, \\
\text{If} & (x,y)=(3,1), & \text{then} & n\equiv 6 \mod 8, \\
\text{If} & (x,y)=(3,2), & \text{then} & n\equiv 0 \mod 8, \\
\text{If} & (x,y)=(3,3), & \text{then} & n\equiv 6 \mod 8, \\
\text{If} & (x,y)=(3,4), & \text{then} & n\equiv 1 \mod 8, \text{ same as } (x,y)=(3,0).
\end{array}$$

$$\begin{array}{llll}
\text{If} & (x,y)=(4,0), & \text{then} & n\equiv 0 \mod 8, \\
\text{If} & (x,y)=(4,1), & \text{then} & n\equiv 5 \mod 8, \\
\text{If} & (x,y)=(4,2), & \text{then} & n\equiv 4 \mod 8, \\
\text{If} & (x,y)=(4,3), & \text{then} & n\equiv 5 \mod 8, \\
\text{If} & (x,y)=(4,4), & \text{then} & n\equiv 0 \mod 8, \text{ same as } x=0.
\end{array}$$

Therefore, $n =\equiv 1,5 \mod 8$.

If $m \equiv 5 \mod 8$, then $n \equiv x^2+xy-y^2 \mod 8$.Then

$$\begin{array}{llll}
\text{If} & (x,y)=(0,0) & \text{then} & n\equiv 0 \mod 8, \\
\text{If} & (x,y)=(0,1) & \text{then} & n\equiv 7 \mod 8, \\
\text{If} & (x,y)=(0,2) & \text{then} & n\equiv 4 \mod 8, \\
\text{If} & (x,y)=(0,3) & \text{then} & n\equiv 7 \mod 8, \\
\text{If} & (x,y)=(0,4) & \text{then} & n\equiv 0 \mod 8, \text{ same as } (x,y)=(0,0).
\end{array}$$

$$\begin{array}{llll}
\text{If} & (x,y)=(1,0) & \text{then} & n\equiv 1 \mod 8,\\
\text{If} & (x,y)=(1,1) & \text{then} & n\equiv 1 \mod 8,\\
\text{If} & (x,y)=(1,2) & \text{then} & n\equiv 7 \mod 8,\\
\text{If} & (x,y)=(1,3) & \text{then} & n\equiv 3 \mod 8,\\
\text{If} & (x,y)=(1,4) & \text{then} & n\equiv 5 \mod 8,\\
\text{If} & (x,y)=(1,5) & \text{then} & n\equiv 5 \mod 8,\\
\text{If} & (x,y)=(1,6) & \text{then} & n\equiv 3 \mod 8,\\
\text{If} & (x,y)=(1,7) & \text{then} & n\equiv 7 \mod 8.
\end{array}$$

Therefore, $n \equiv 1, 3, 5, 7 \mod 8$.

If $m \equiv 6 \mod 8$, then $n \equiv x^2 - 6y^2 \mod 8$. Then

$$\begin{array}{llllll}
\text{If} & (x,y)=(0,0) & \text{then} & n\equiv 0 \mod 8, & & \\
\text{If} & (x,y)=(0,1) & \text{then} & n\equiv 2 \mod 8, & & \\
\text{If} & (x,y)=(0,2) & \text{then} & n\equiv 0 \mod 8, & \text{same as } (x,y)=(0,0). &
\end{array}$$

$$\begin{array}{llllll}
\text{If} & (x,y)=(1,0) & \text{then} & n\equiv 1 \mod 8, & & \\
\text{If} & (x,y)=(1,1) & \text{then} & n\equiv 3 \mod 8, & & \\
\text{If} & (x,y)=(1,2) & \text{then} & n\equiv 1 \mod 8, & \text{same as } (x,y)=(1,0). &
\end{array}$$

$$\begin{array}{llllll}
\text{If} & (x,y)=(2,0) & \text{then} & n\equiv 4 \mod 8, & & \\
\text{If} & (x,y)=(2,1) & \text{then} & n\equiv 6 \mod 8, & & \\
\text{If} & (x,y)=(2,2) & \text{then} & n\equiv 4 \mod 8, & \text{same as } (x,y)=(2,0). &
\end{array}$$

$$\begin{array}{llllll}
\text{If} & (x,y)=(3,0) & \text{then} & n\equiv 1 \mod 8, & & \\
\text{If} & (x,y)=(3,1) & \text{then} & n\equiv 3 \mod 8, & & \\
\text{If} & (x,y)=(3,2) & \text{then} & n\equiv 1 \mod 8, & \text{same as } x=1. &
\end{array}$$

Therefore, $n \equiv 1, 3$.

If $m \equiv 7 \mod 8$, then $n \equiv x^2 - 7y^2 \equiv x^2 + y^2 \mod 8$. Then

$$
\begin{array}{llllll}
\text{If} & (x,y) = (0,0) & \text{then} & n \equiv 0 & \mod 8, & \\
\text{If} & (x,y) = (0,1) & \text{then} & n \equiv 1 & \mod 8, & \\
\text{If} & (x,y) = (0,2) & \text{then} & n \equiv 4 & \mod 8, & \\
\text{If} & (x,y) = (0,3) & \text{then} & n \equiv 1 & \mod 8, & \\
\text{If} & (x,y) = (0,4) & \text{then} & n \equiv 0 & \mod 8, & \text{same as } (x,y) = (0,0).
\end{array}
$$

$$
\begin{array}{llllll}
\text{If} & (x,y) = (1,0) & \text{then} & n \equiv 1 & \mod 8, & \\
\text{If} & (x,y) = (1,1) & \text{then} & n \equiv 2 & \mod 8, & \\
\text{If} & (x,y) = (1,2) & \text{then} & n \equiv 5 & \mod 8, & \\
\text{If} & (x,y) = (1,3) & \text{then} & n \equiv 2 & \mod 8, & \\
\text{If} & (x,y) = (1,4) & \text{then} & n \equiv 1 & \mod 8, & \text{same as } (x,y) = (1,0).
\end{array}
$$

$$
\begin{array}{llllll}
\text{If} & (x,y) = (2,0) & \text{then} & n \equiv 4 & \mod 8, & \\
\text{If} & (x,y) = (2,1) & \text{then} & n \equiv 5 & \mod 8, & \\
\text{If} & (x,y) = (2,2) & \text{then} & n \equiv 0 & \mod 8, & \\
\text{If} & (x,y) = (2,3) & \text{then} & n \equiv 5 & \mod 8, & \\
\text{If} & (x,y) = (2,4) & \text{then} & n \equiv 4 & \mod 8, & \text{same as } (x,y) = (2,0).
\end{array}
$$

$$
\begin{array}{llllll}
\text{If} & (x,y) = (3,0) & \text{then} & n \equiv 1 & \mod 8, & \\
\text{If} & (x,y) = (3,1) & \text{then} & n \equiv 2 & \mod 8, & \\
\text{If} & (x,y) = (3,2) & \text{then} & n \equiv 5 & \mod 8, & \\
\text{If} & (x,y) = (3,3) & \text{then} & n \equiv 2 & \mod 8, & \\
\text{If} & (x,y) = (3,4) & \text{then} & n \equiv 1 & \mod 8, & \text{same as } x = 1.
\end{array}
$$

Therefore, $n \equiv 1, 5$. □

Lemma A.0.10. *If $p \equiv 1 \mod 4$, then $\mathbb{Q}(\sqrt{p})$ has a unit ε with $N(\varepsilon) = -1$.*

Proof. Let ε be the smallest positive unit with $N(\varepsilon) = +1$. Then, write $\varepsilon^3 = x + y\sqrt{p}$ in $\mathbb{Q}(\sqrt{p})$ with odd x. By taking norm of both sides, we get $1 = x^2 - py^2$, so $(x-1)(x+1) =$

py^2. Since p is prime, we must have

$$x - 1 = 2a^2 \text{ and } x + 1 = 2pb^2$$

or

$$x - 1 = 2pb^2 \text{ and } x + 1 = 2a^2.$$

for some $a, b \in \mathbb{Q}$. Then $a^2 - pb^2 = \mp 1$. Therefore, $a^2 - pb^2 = -1$ since ε was minimal with norm $+1$. □

Lemma A.0.11. *If an odd number p is of the $x^2 - 2y^2$ form, then $p \equiv \mp 1 \mod 8$.*

Proof. Let $p = x^2 - 2y^2$. Then x^2 and y^2 can be congruent to quadratic residues module 8, so $x^2, y^2 \in \{0, 1, 4\}$ modulo 8. Therefore, p can have the following values:

$$\begin{aligned} &p = 0 - 2 \cdot 0 = 0, \quad p = 0 - 2 \cdot 1 = 6, \quad p = 0 - 2 \cdot 4 = 0, \\ &p = 1 - 2 \cdot 0 = 1, \quad p = 1 - 2 \cdot 1 = -1, \quad p = 1 - 2 \cdot 4 = 1, \\ &p = 4 - 2 \cdot 0 = 4, \quad p = 4 - 2 \cdot 1 = 2, \quad p = 4 - 2 \cdot 4 = 4 \end{aligned}$$

modulo 8. Since p is odd, $p \equiv \mp 1 \mod 8$. □

Remark A.0.12. Let $k = \mathbb{Q}(i)$ and $\mathfrak{o} = \mathbb{Z}[i]$. Then $\mathfrak{o}/4\mathfrak{o} = \{0, 1, 2, 3, i, 1+i, 2+i, 3+i, 2i, 1+2i, 2+2i, 3+2i, 3i, 1+3i, 2+3i, 3+3i\}$. To find the quadratic residues modulo $(1+i)^5$, let us calculate squares of elements in $\mathfrak{o}/4\mathfrak{o}$.

$$\begin{aligned} &0^2 = 0, && 1^2 = 1, && 2^2 = 0, && 3^2 = 1, \\ &i^2 = -1, && (1+i)^2 = 2i, && (2+i)^2 = -1, && (3+i)^2 = 2i, \\ &(2i)^2 = 0, && (1+2i)^2 = 1, && (2+2i)^2 = 0, && (3+2i)^2 = 1, \\ &(3i)^2 = -1, && (1+3i)^2 = 2i, && (2+3i)^2 = -1, && (3+3i)^2 = 2i. \end{aligned}$$

Therefore, for some $\delta \in k$, we get that δ is a quadratic residue modulo 4, if $\delta \equiv \mp 1 \mod 4$ since $(1+i) \mid 2i$.

Similarly, $\mathfrak{o}/2\mathfrak{o} = \{0, 1, i, 1+i\}$. Then,

$$0^2 = 0, \quad 1^2 = 1,$$
$$i^2 = 1, \quad (1+i)^2 = 0.$$

Therefore, δ is a quadratic residue modulo 2, if $\delta \equiv 1 \mod 2$, that is $\delta \equiv \mp 1$ or $\mp 1 + 2i \mod 4$. Thus, δ is a quadratic residue modulo 2, but non-residue modulo 4, if $\delta \equiv \mp 1 + 2i \mod 4$.

In addition, for other cases $\delta \equiv i \mod 2$ or $\delta \equiv 0 \mod 1+i$ where δ is a quadratic non-residue modulo 2.

Remark A.0.13. To find the relative discriminant, we use that $\mathrm{disc}_k(k(\sqrt{\delta})) = \det \begin{pmatrix} 1 & \Omega \\ 1 & \mathsf{S}\Omega \end{pmatrix}^2 = (\Omega - \mathsf{S}\Omega)^2$. So,

$$\begin{aligned}
\text{If } \delta \equiv 1 \mod 4, \quad \text{then } \mathrm{disc}_k(k(\sqrt{\delta})) &= \left(\frac{1+\sqrt{\delta}}{2} - \frac{1-\sqrt{\delta}}{2}\right)^2 \\
&= \left(\frac{1-\sqrt{\delta}-1+\sqrt{\delta}}{2}\right)^2 = \delta \\
\text{If } \delta \equiv 3+2i \mod 4, \quad \text{then } \mathrm{disc}_k(k(\sqrt{\delta})) &= \left(\frac{1+\sqrt{\delta}}{1+i} - \frac{1-\sqrt{\delta}}{1+i}\right)^2 \\
&= \left(\frac{1-\sqrt{\delta}-1+\sqrt{\delta}}{1+i}\right)^2 = -2i\delta \\
\text{If } \delta \equiv i \mod 2, \quad \text{then } \mathrm{disc}_k(k(\sqrt{\delta})) &= \left(1+\sqrt{\delta}-1-\sqrt{\delta}\right)^2 \\
&= \left(1-\sqrt{\delta}-1+\sqrt{\delta}\right)^2 = 4\delta \\
\text{If } \delta \equiv 0 \mod 1+i, \quad \text{then } \mathrm{disc}_k(k(\sqrt{\delta})) &= \left(\sqrt{\delta}--\sqrt{\delta}\right)^2 = \left(\sqrt{\delta}+\sqrt{\delta}\right)^2 = 4\delta.
\end{aligned}$$

The usual discriminant $\mathrm{disc}_{\mathbb{Q}}(k(\sqrt{\delta}))$ of the biquadratic field is:

$$\begin{aligned}\mathrm{disc}_{\mathbb{Q}}(k(\sqrt{\delta})) &= \det\begin{pmatrix}1 & i & \Omega & i\Omega\\ 1 & -i & \Omega & -i\Omega\\ 1 & i & \mathsf{S}\Omega & i\mathsf{S}\Omega\\ 1 & -i & \mathsf{S}\Omega & -i\mathsf{S}\Omega\end{pmatrix}^2\\ &= 2^4(\Omega-\mathsf{S}\Omega)^2\\ &= 2^4|\mathrm{disc}_k(k(\sqrt{\delta}))|^2.\end{aligned}$$

Lemma A.0.14. *Let α be in $k(\sqrt{\delta})$. The congruence, $\alpha \equiv N_{k(\sqrt{\delta})/k}(A) \mod (1+i)^5$ is solvable for some $A \in \mathfrak{O}$ if and only if*

Case 1. $\alpha \equiv (000), (001), (010)$ *or* $(011) \mod (1+i)^5$, *for the field* $k(\sqrt{\delta})$ *with* $\delta \equiv (01) \mod (1+i)^4$,

Case 2. $\alpha \equiv (000), (001), (101)$ *or* $(100) \mod (1+i)^5$, *for the field* $k(\sqrt{\delta})$ *with* $\delta \equiv (10) \mod (1+i)^4$,

Case 3. $\alpha \equiv (000), (001), (110)$ *or* $(111) \mod (1+i)^5$, *for the field* $k(\sqrt{\delta})$ *with* $\delta \equiv (11) \mod (1+i)^4$,

Case 4. $\alpha \equiv (000), (011), (100)$ *or* $(111) \mod (1+i)^5$, *for the field* $k(\sqrt{\delta})$ *with* $\delta \equiv (1+i)(00) \mod (1+i)^5$,

Case 5. $\alpha \equiv (000), (011), (101)$ *or* $(110) \mod (1+i)^5$, *for the field* $k(\sqrt{\delta})$ *with* $\delta \equiv (1+i)(01) \mod (1+i)^5$,

Case 6. $\alpha \equiv (000), (010), (100)$ *or* $(110) \mod (1+i)^5$, *for the field* $k(\sqrt{\delta})$ *with* $\delta \equiv (1+i)(10) \mod (1+i)^5$,

Case 7. $\alpha \equiv (000), (010), (101)$ *or* $(111) \mod (1+i)^5$, *for the field* $k(\sqrt{\delta})$ *with* $\delta \equiv (1+i)(11) \mod (1+i)^5$.

Proof. To investigate for which combinations of values of α and δ, the congruence $\alpha \equiv N_{k(\sqrt{\delta})/k}(A) \mod (1+i)^5$ is solvable for some $A \in \mathfrak{O}$, by Theorem 6.1.1, we will investigate the congruence $\alpha = N_{k(\sqrt{\delta})/k}(x+y\Omega) \mod (1+i)^5$ case by case.

Case 1. For $\delta \equiv (01) \mod (1+i)^4$, $\Omega = \frac{1+\sqrt{\delta}}{1+i}$, so $\alpha = (x + \frac{1+\sqrt{\delta}}{1+i}y)(x + \frac{1-\sqrt{\delta}}{1+i}y) = x^2 + (1-i)xy - \frac{\delta-1}{2i}y^2 \equiv x^2 + (1-i)xy - (1-i)y^2 \mod (1+i)^5$. Now, for $x = a+bi$, $y = c+di$ where $a, b, c, d \in \mathbb{Z}$, we use this algorithm in Maple to get all the values for α:

```
with(GaussInt):
v := array(0..4096):
i := 0;
for a from 0 by 1 to 8 do
for b from 0 by 1 to 8 do
for c from 0 by 1 to 8 do
for d from 0 by 1 to 8 do
rmd := GIrem((a+b*I)^2+(1-I)*(a+b*I)*(c+d*I)-(1-I)*(c+d*I)^2,(1+
I)^5);.....equation line
if (GIrem(rmd, (1+I)) <> 0) then
v[i] := rmd; i := i +1;
end if
end do
end do
end do
end do;
convert(v, set);
```

Figure A.1. The algorithm for Lemma A.0.14

All other cases can be done with this algorithm by changing the equation with Ω. So let us give only the equations for each case that will be used in the equation line.

Case 2. For $\delta \equiv (10) \mod (1+i)^4$, $\Omega = 1+\sqrt{\delta}$, so $\alpha = (x + (1+\sqrt{\delta})y)(x +$

$(1-\sqrt{\delta})y) = x^2+2xy-(\delta-1)y^2 \equiv x^2+2xy+(1-i)y^2 \mod (1+i)^5$.

Case 3. For $\delta \equiv (11) \mod (1+i)^4$, $\Omega = 1+\sqrt{\delta}$, so $\alpha = (x+(1+\sqrt{\delta})y)(x+(1-\sqrt{\delta})y) = x^2+2xy-(\delta-1)y^2 \equiv x^2+2xy+(3-3i)y^2 \mod (1+i)^5$.

Case 4. For $\delta \equiv (1+i)(00) \mod (1+i)^4$, $\Omega = \sqrt{\delta}$, so $\alpha = (x+\sqrt{\delta}y)(x-\sqrt{\delta}y) = x^2-\delta y^2 \equiv x^2-(1+i)y^2 \mod (1+i)^5$.,

Case 5. For $\delta \equiv (1+i)(01) \mod (1+i)^4$, $\Omega = \sqrt{\delta}$, so $\alpha = (x+\sqrt{\delta}y)(x-\sqrt{\delta}y) = x^2-\delta y^2 \equiv x^2-(1+i)(3+2i)y^2 \equiv x^2-(1+5i)y^2 \mod (1+i)^5$.

Case 6. For $\delta \equiv (1+i)(10) \mod (1+i)^4$, $\Omega = \sqrt{\delta}$, so $\alpha = (x+\sqrt{\delta}y)(x-\sqrt{\delta}y) = x^2-\delta y^2 \equiv x^2-(i-1)y^2 \mod (1+i)^5$.

Case 7. For $\delta \equiv (1+i)(11) \mod (1+i)^4$, $\Omega = \sqrt{\delta}$, so $\alpha = (x+\sqrt{\delta}y)(x-\sqrt{\delta}y) = x^2-\delta y^2 \equiv x^2-(i-1)(3+2i)y^2 \equiv x^2-(i-5)y^2 \mod (1+i)^5$. □

Lemma A.0.15. *Let $\delta \in \{1\mp 2i, 2\mp i, 1\mp i, \mp i\}$. If $\upsilon = N_{k(\sqrt{\delta})/k}(\mathfrak{I})$ for some ideal $\mathfrak{I}$ in the principle genus of $k(\sqrt{\delta})$, then in fact $\upsilon = N_{k(\sqrt{\delta})/k}(A)$ for some number A in $k(\sqrt{\delta})$.*

Proof. Note that here $\delta \in k$ is prime for each case, then for $\upsilon = \delta$, we have $\upsilon = N_{k(\sqrt{\delta})/k}(i\sqrt{\delta}) = i\sqrt{\delta}(-i\sqrt{\delta}) = \delta$. So we do not consider the value $\upsilon = \delta$ in case analysis. Furthermore, $1 = N_{k(\sqrt{\delta})/k}(1)$, $-1 = N_{k(\sqrt{\delta})/k}(i)$, $2i = N_{k(\sqrt{\delta})/k}(1+i)$ and $2 = 2i(-i)$, so again no need to check these values.

Case 1. $\delta = 1 \pm 2i$. In each ideal class, there exists an ideal $\mathfrak{I}$ in $k(\sqrt{\delta})$ such that $N_{k(\sqrt{\delta})/\mathbb{Q}}(\mathfrak{I}) = |N_{k(\sqrt{\delta})/k}(\mathfrak{I})|^2 < \sqrt{6}|\delta| = \sqrt{6}\sqrt{5} = \sqrt{30}$. So it is enough to check the values $N_{k(\sqrt{\delta})/k}(\mathfrak{I}) = \upsilon = a+bi$ with $a^2+b^2 < \sqrt{30}$. Then, $\upsilon \in \{\mp i, 1\mp i, 1\pm 2i, 2\mp i\}$. Let us check for each υ that whether $\mathfrak{I}$ is in the principle genus or not.

$$\left[\frac{i}{1\pm 2i : 1\pm 2i}\right] = \left[\frac{i}{1\pm 2i}\right] = -1,$$

since $\mathfrak{o}/(1 \pm 2i)\mathfrak{o} = \{0, \mp 1, \mp i\}$ where ∓ 1 are quadratic residues and $\mp i$ are quadratic non-residues modulo $1 \pm 2i$. So if $\upsilon \equiv i \mod 1 \pm 2i$, then $\left[\frac{\upsilon}{1 \pm 2i : 1 \pm 2i}\right] = \left[\frac{\upsilon}{1 \pm 2i}\right] = -1$ since it is a quadratic non-residue modulo $1 + 2i$ and if $\upsilon \equiv \mp 1 \mod 1 \pm 2i$, then $\left(\frac{\upsilon}{1 \pm 2i : 1 \pm 2i}\right) = \left[\frac{\upsilon}{1 \pm 2i}\right] = +1$ since it is a quadratic non-residue modulo $1 \pm 2i$ where $1 + 2i \nmid \upsilon$, so $\mathfrak{I}$ is in the principle genus.

$$\begin{array}{lcll} 1+i & = & (1+2i)(1)-i & \equiv -i \mod 1+2i \\ 1-i & = & (1+2i)(-i)-1 & \equiv -1 \mod 1+2i \\ 1-2i & = & (1+2i)(-1-i)+i & \equiv +i \mod 1+2i \\ 2+i & = & (1+2i)(1-i)-1 & \equiv -1 \mod 1+2i \\ 2-i & = & (1+2i)(-i)+0 & \equiv 0 \mod 1+2i \end{array}$$

$$\begin{array}{lcll} 1+i & = & (1-2i)(i)-1 & \equiv -1 \mod 1-2i \\ 1-i & = & (1-2i)(1)+i & \equiv +i \mod 1-2i \\ 1+2i & = & (1-2i)(-1+i)-i & \equiv -i \mod 1-2i \\ 2+i & = & (1-2i)(i)+0 & \equiv 0 \mod 1-2i \\ 2-i & = & (1-2i)(1+i)-1 & \equiv -1 \mod 1-2i \end{array}$$

Here $\upsilon = 2 \pm i$ is a candidate, but since $\left[\frac{1 \pm 2i}{2 \pm i}\right] = -1$, the value $2 \pm i$ can not be a norm of an ideal, because it is itself prime in $k(\sqrt{\delta})$.Therefore, for $\upsilon = 1 \mp i$, the ideal $\mathfrak{I}$ is in the principle genus. Furthermore, υ is a norm of a number in $k(\sqrt{\delta})$ since

$$\begin{aligned} N_{k(\sqrt{\delta})/k}\left(\frac{1+i\sqrt{1 \pm 2i}}{1+i}\right) &= \frac{1+i\sqrt{1 \pm 2i}}{1+i} \cdot \frac{1-i\sqrt{1 \pm 2i}}{1+i} \\ &= \frac{1+(1 \pm 2i)}{2i} \\ &= \frac{2 \pm 2i}{2i} = 1 \mp i. \end{aligned}$$

From now on, the idea in the other cases is similar to Case 1, so we only check whether

υ is congruent to ∓ 1 or $\mp i$ modulo δ.

Case 2. $\delta = 2 \pm i$.

$$\begin{array}{lcll} 1+i & = & (2+i)(1)-1 & \equiv -1 \mod 2+i \\ 1-i & = & (2+i)(-i)-i & \equiv -i \mod 2+i \\ 1+2i & = & (2+i)(1+i)-i & \equiv -i \mod 2+i \\ 1-2i & = & (2+i)(-i)+0 & \equiv 0 \mod 2+i \\ 2-i & = & (2+i)(1-i)-1 & \equiv -1 \mod 2+i \end{array}$$

$$\begin{array}{lcll} 1+i & = & (2-i)(i)-1 & \equiv -1 \mod 2-i \\ 1-i & = & (2-i)(1)-1 & \equiv -1 \mod 2-i \\ 1+2i & = & (2-i)(i)+0 & \equiv 0 \mod 2-i \\ 1-2i & = & (2-i)(1-i)+i & \equiv i \mod 2-i \\ 2+i & = & (2-i)(1+i)-1 & \equiv -1 \mod 2-i \end{array}$$

Therefore, for $\upsilon = 2 \mp i$ and $\upsilon = 1 \pm i$, the ideal $\mathfrak{I}$ is in the principle genus. Furthermore, υ is a norm of a number in $k(\sqrt{\delta})$ since

$$\begin{aligned} N_{k(\sqrt{\delta})/k}(1 \mp i + i\sqrt{2 \pm i}) &= (1 \mp i + i\sqrt{2 \pm i}) \cdot (1 \mp i - i\sqrt{2 \pm i}) \\ &= (1 \mp i)^2 + (2 \pm i) \\ &= \mp 2i + 2 \pm i = 2 \mp i. \end{aligned}$$

$$\begin{aligned} N_{k(\sqrt{\delta})/k}(1 + i\sqrt{2 \pm i}) &= (1 + i\sqrt{2 \pm i}) \cdot (1 - i\sqrt{2 \pm i}) \\ &= 1 + (2 \pm i) \\ &= 1 \pm i. \end{aligned}$$

Case 3. $\delta = 1 \pm i$, so check the values for $\upsilon = a + bi$ with $a^2 + b^2 < \sqrt{6}\sqrt{2} = \sqrt{12}$.

$$\begin{aligned} 1 - i &= (1+i)(-i) - 0 \equiv 0 \mod 1+i \\ 1 + i &= (1-i)(i) + 0 \equiv 0 \mod 1+i \end{aligned}$$

Therefore, for $\upsilon = \pm i$, the ideal $\mathfrak{I}$ is in the principle genus. Furthermore, υ is a norm of a number in $k(\sqrt{\delta})$ since

$$\begin{aligned} N_{k(\sqrt{\delta})/k}(i + i\sqrt{1 \pm i}) &= (i + i\sqrt{1 \pm i}) \cdot (i - i\sqrt{1 \pm i}) \\ &= -1 + (1 \pm i) \\ &= \pm i. \end{aligned}$$

Case 4. $\delta = i$. We will check the values for $\upsilon = a + bi$ with $a^2 + b^2 < \sqrt{6}$, that is $\upsilon = 1 \mp i$. Moreover, $\left[\dfrac{1-i}{1+i:i}\right] = +1$ and $\left[\dfrac{1-+i}{1+i:i}\right] = +1$. Therefore, for $\upsilon = 1 \mp i$, the ideal $\mathfrak{I}$ is in the principle genus. Furthermore, υ is a norm of a number in $k(\sqrt{\delta})$ since

$$\begin{aligned} N_{k(\sqrt{\delta})/k}(1 + i\sqrt{i}) &= (1 + i\sqrt{i}) \cdot (1 - i\sqrt{i}) \\ &= 1 + i, \\ N_{k(\sqrt{\delta})/k}(1 + \sqrt{i}) &= (1 + \sqrt{i}) \cdot (1 - \sqrt{i}) \\ &= 1 - i. \end{aligned}$$

□

APPENDIX B: SOME USEFUL THEOREMS

Lemma B.0.16. *(Hilbert's Theorem 90) Let $x \in \mathbb{Q}(\sqrt{m})$ with $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(x) = +1$. Then there exists an integer $y \in \mathfrak{O}$ such that $x = y/y'$ where y' denotes the conjugate of y.*

Proof. Let $y = x + 1 \in \mathfrak{O}$. Then $\dfrac{x+1}{(x+1)'} = \dfrac{x+1}{x'+1} = \dfrac{x+1}{x'+xx'} = \dfrac{1}{x'} = \dfrac{xx'}{x'} = x.$ □

Lemma B.0.17. *(Hilbert's Theorem 90 for ideals) Let $\mathfrak{a}$ be an ideal in $\mathbb{Q}(\sqrt{m})$ with $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a}) = +1$. Then there exists an ideal $\mathfrak{b}$ in $\mathbb{Q}(\sqrt{m})$ such that $\mathfrak{a} = \dfrac{\mathfrak{b}}{\mathfrak{b}'}$ where $\mathfrak{b}'$ denotes the conjugate of $\mathfrak{b}$.*

Proof. By Definition 4.1.2, if $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\mathfrak{a}) = +1$, then $\mathfrak{a}\mathfrak{a}' = \mathfrak{O}$. Let $\mathfrak{b} = \mathfrak{a} + \mathfrak{O}$ in $\mathbb{Q}(\sqrt{m})$. Then $\dfrac{\mathfrak{a}+\mathfrak{O}}{(\mathfrak{a}+\mathfrak{O})'} = \dfrac{\mathfrak{a}+\mathfrak{O}}{\mathfrak{a}'+\mathfrak{O}} = \dfrac{\mathfrak{a}+\mathfrak{O}}{\mathfrak{a}'+\mathfrak{a}\mathfrak{a}'} = \dfrac{\mathfrak{O}}{\mathfrak{a}'} = \dfrac{\mathfrak{a}\mathfrak{a}'}{\mathfrak{a}'} = \mathfrak{a}.$ □

Theorem B.0.18. *(Minkowski's Theorem) Let K be a number field and let D_k be its discriminant. Let $n = r_1 + 2r_2$ be the degree of K over $\mathbb{Q}$, where r_1 and r_2 are the number of real and complex embedding functions, respectively. The class group of K is denoted by $Cl(K)$. In any ideal class $\mathfrak{c} \in Cl(K)$, there exists an ideal $\mathfrak{U} \in \mathfrak{c}$ such that*

$$|N(\mathfrak{U})| \leq M_K \sqrt{|D_K|}$$

where $N(\mathfrak{U})$ denotes the absolute norm of $\mathfrak{U}$ and $M_K = \dfrac{n!}{n^n}\left(\dfrac{4}{\pi}\right)^{r_2}$.

Theorem B.0.19. *Given a commutative diagram of abelian groups*

$$\begin{array}{ccccccccc} & & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 1 & \longrightarrow & A' & \xrightarrow{f^0} & B' & \xrightarrow{g^0} & C' & & \end{array}$$

Figure B.1. Figure for Snake Lemma

with exact rows, there exists an exact sequence

$$\ker\alpha \longrightarrow \ker\beta \longrightarrow \ker\gamma \xrightarrow{\delta} \operatorname{coker}\alpha \longrightarrow \operatorname{coker}\beta \longrightarrow \operatorname{coker}\gamma. \tag{B.1}$$

Proof. See [7] for its proof. □

Theorem B.0.20. *(Legendre's Theorem) Assume that $a, b, c \in \mathbb{Z}$ satisfy the following conditions:*

1. *(a,b) = (b,c) = (c,a) = 1,*

2. *at least one of ab, bc, ca is negative,*

3. *the following congruences are solvable:*

$$u^2 \equiv -bc \mod a,\ v^2 \equiv -ca \mod b,\ w^2 \equiv -ab \mod c\ .$$

Then the diophantine equation $ax^2 + by^2 + cz^2 = 0$ has non-trivial solutions in $\mathbb{Z}$.

Proof. See [**?**] for its proof. □

Definition B.0.21. Let K be a number field over k of degree r. For $A \in K$, *the relative norm of the number A* is

$$N_{K/k}(A) = AA'A'' \dots A^{(r-1)}$$

where $A^{(i)}$s denote the relative conjugates of A.

If $\mathfrak{J} = (A_1, \dots, A_s)$ is any ideal of K, then *the relative norm of an ideal $\mathfrak{J}$* is

$$N_{K/k}(\mathfrak{J}) = \mathfrak{J}\mathfrak{J}' \dots \mathfrak{J}^{(r-1)}$$

where $\mathfrak{J}^{(i)}$s denote the relative conjugate ideals of $\mathfrak{J}$.

Theorem B.0.22. *Let K be an algebraic field extension over k. Then for some ideal $\mathfrak{J}$ in K, $NK/k(\mathfrak{J})$ is an ideal in k.*

Proof. Let $K = k(\theta)$ be an algebraic extension over k of degree r and let f be the minimal polynomial of θ over k. Let $\theta, \theta', \theta'', \ldots, \theta^{(r-1)}$ be all roots of f in a splitting field of f, say L. Then there exists a field homomorphism $\sigma_i : K = k(\theta) \to K^{(i)} = k(\theta^{(i)})$ for each $i = 0, 1, \ldots, r-1$. Note that $L = k(\theta, \theta', \theta'', \ldots, \theta^{(r-1)})$ is normal and separable over k, so L is Galois over k.

Let $\mathfrak{J} = (A_1, \ldots, A_s)$ be an ideal in K. Then $N_{K/k}(\mathfrak{J}) = \mathfrak{J}\mathfrak{J}' \ldots \mathfrak{J}^{(r-1)}$ can be denoted by $(A_1U_1 + \ldots + A_sU_s)(A_1'U_1 + \ldots + A_s'U_s) \ldots (A_1^{(r-1)}U_1 + \ldots + A_s^{(r-1)}U_s)$ for indeterminates $U_1, \ldots, U_s$ by [1]. Now, we will show that $(A_1U_1 + \ldots + A_sU_s)(A_1'U_1 + \ldots + A_s'U_s) \ldots (A_1^{(r-1)}U_1 + \ldots + A_s^{(r-1)}U_s)$ are integers of k to prove the theorem.

For some $\lambda \in \mathrm{Aut}(L/k)$, λ fixes $(A_1U_1 + \ldots + A_sU_s)(A_1'U_1 + \ldots + A_s'U_s) \ldots (A_1^{(r-1)}U_1 + \ldots + A_s^{(r-1)}U_s)$ since it is a symmetric number in L under taking conjugates. But L is Galois over k, so the only numbers that λ fixes must be in k, so $(A_1U_1 + \ldots + A_sU_s)(A_1'U_1 + \ldots + A_s'U_s) \ldots (A_1^{(r-1)}U_1 + \ldots + A_s^{(r-1)}U_s) \in k$. Thus, $\mathfrak{O}_L(\mathfrak{J}\mathfrak{J}' \ldots \mathfrak{J}'') = (\mathfrak{O}_LA_1 + \ldots + \mathfrak{O}_LA_s)(\mathfrak{O}_LA_1' + \ldots + \mathfrak{O}_LA_s') \ldots (\mathfrak{O}_LA_1^{(r-1)} + \ldots + \mathfrak{O}_LA_s^{(r-1)}) = \mathfrak{O}_L(\mathfrak{o}_kC_1 + \ldots + \mathfrak{o}_kC_t)$ where $(\mathfrak{o}_kC_1 + \ldots + \mathfrak{o}_kC_t)$ is a k-ideal. □

Lemma B.0.23. *The relative norm function is multiplicative.*

Proof.

$$\begin{aligned} N_{k(\sqrt{\delta})/k}(\mathfrak{A}\mathfrak{B}) &= (\mathfrak{A}\mathfrak{B})\mathsf{S}((AB)) \\ &= \mathfrak{A}\mathfrak{B}\mathsf{S}(\mathfrak{A})\mathsf{S}(\mathfrak{B}) \\ &= \mathfrak{A}\mathsf{S}(\mathfrak{A})\mathfrak{B}\mathsf{S}(\mathfrak{B}) \\ &= N_{k(\sqrt{\delta})/k}(\mathfrak{A})N_{k(\sqrt{\delta})/k}(\mathfrak{B}). \end{aligned}$$

□

REFERENCES

1. Hilbert, D., *The Theory of Algebraic Number Fields*, Springer, Berlin, 1998.

2. Hilbert, D., *Über den Dirichletschen biquadratischen Zahlkörper*, Mathem. Annalen Bd. 45, S.309-340, 1894.

3. Stewart, I., D. Tall, *Algebraic Number Theory*, Chapman and Hall, New York, 1987.

4. Landau, E., *Einführung in die Elementare Zahlen Theorie*, Chelsea Pub. Co., New York, 1949.

5. Feyzioğlu, A., *A Course on Algebra*, Boğaziçi University Publication, Istanbul.

6. Niven, I., H. S. Zuckerman and H. L. Montgomery, *An Introduction to the Theory of Numbers*, pp. 164, Wiley, New York, 1991.

7. Lemmermeyer, F., *The Snake Lemma*, unpublised, Nov. 2002.