Finiteness Theorems for Forms Over Number Fields.

Jenna Price Carpenter

Louisiana State University and Agricultural & Mechanical College

Follow this and additional works at: https://repository.lsu.edu/gradschool_disstheses

Recommended Citation

https://repository.lsu.edu/gradschool_disstheses/4701

This Dissertation is brought to you for free and open access by the Graduate School at LSU Scholarly Repository. It has been accepted for inclusion in LSU Historical Dissertations and Theses by an authorized administrator of LSU Scholarly Repository. For more information, please contact gradetd@lsu.edu.
INFORMATION TO USERS

The most advanced technology has been used to photograph and reproduce this manuscript from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book. These are also available as one exposure on a standard 35mm slide or as a 17" x 23" black and white photographic print for an additional charge.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

UMI
University Microfilms International
A Bell & Howell Information Company
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
313/761-4700 800/521-0600
Finiteness theorems for forms over number fields

Carpenter, Jenna Price, Ph.D.

The Louisiana State University and Agricultural and Mechanical Col., 1989

Copyright ©1990 by Carpenter, Jenna Price. All rights reserved.
FINITENESS THEOREMS
FOR
FORMS OVER NUMBER FIELDS

A Dissertation
Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy
in
The Department of Mathematics

by
Jenna Price Carpenter
B.S., Louisiana Tech University, 1983
M.S., Louisiana State University, 1986
May 1989
ACKNOWLEDGEMENTS

I would like to thank my major professor, Robert V. Perlis, for directing this dissertation, as well as much of my mathematical education. His help, guidance, and advice have been greatly appreciated.

I am grateful to Pierre E. Conner for sharing his insight and suggestions, and for explaining the concepts which led to the development of Chapter II.

I would like to express my appreciation to the Department of Mathematics, the Graduate School, and the Louisiana State University Alumni Federation for four years of financial support in the form of a Louisiana State University Alumni Federation Fellowship.

I am deeply indebted to my husband, Walter Carpenter, for countless hours of technical assistance, in addition to his general support and understanding.

Finally, I must thank my parents, Birtrum M. and Virginia S. Price, for their love and encouragement, and for instilling in me at an early age the importance of education.
# TABLE OF CONTENTS

**ACKNOWLEDGEMENTS** .......................................................... ii

**ABSTRACT** ................................................................. v

**INTRODUCTION** ............................................................. 1

**CHAPTER I - Preliminaries** .................................................. 5

§I.1 Introduction ................................................................. 5
§I.2 A Review of Basic Form Theory ........................................ 5
§I.3 Some Fundamental Results from Number Theory ................. 7
§I.4 Hilbert Symbols and Reciprocity Equivalence .................... 9
§I.5 The S-Ideal Class Group ............................................... 10

**CHAPTER II - Local Inner Product Spaces** ......................... 12

§II.1 Introduction ............................................................... 12
§II.2 The Inner Product Space \((K_p^*/K_p^2, ( , )_p)\) .................... 12
§II.3 Isometry and Kaplansky’s Lemma .................................. 13
§II.4 The Inner Product Space \(G(S)\) ...................................... 16
§II.5 The Subspace \(i_S(U_K(S)/U_K(S)^2)\) of \(G(S)\) ............... 19
§II.6 The Cokernel of \(i_S\) .................................................... 20

**CHAPTER III - Small Equivalence of Number Fields** .......... 30

§III.1 Introduction ............................................................ 30
§III.2 Suitable Pairs and Small Equivalence ............................ 30
§III.3 Removing the Obstruction ......................................... 32
§III.4 The Existence of a Suitable Pair ................................. 42
ABSTRACT

In 1932, E. Witt showed how the collection of bilinear forms over a field $E$ can be made into a ring called the Witt ring, $W(E)$, of $E$. Properties of bilinear forms over a field often are reflected in the algebraic properties of its Witt ring. Perlis, Szymiczek, and Conner give criteria for global fields to be Witt equivalent; that is, to have isomorphic Witt rings. We refine these criteria to obtain finite, necessary and sufficient conditions to insure Witt equivalence of number fields. These conditions yield several finiteness statements for forms over number fields. Among them, for a fixed degree $n \in \mathbb{N}$, the number of Witt equivalence classes of number fields of degree $n$ is finite.
INTRODUCTION

In 1932, E. Witt showed how the collection of bilinear forms over a field $E$ can be made into a ring, called the Witt ring, $W(E)$, of $E$. Often, properties of bilinear forms over $E$ are reflected in the properties of its Witt ring. In [P-S-C], Perlis, Szymiczek, and Conner study Witt equivalence, or isomorphism of Witt rings, for global fields (number fields or function fields in one variable over finite fields) of characteristic not 2. They define an equivalence of the laws of Hilbert symbol reciprocity, or reciprocity equivalence, for these global fields; moreover, they prove that these global fields are Witt equivalent if and only if they are reciprocity equivalent.

In this dissertation we simplify the criteria of [P-S-C] to obtain finite, necessary and sufficient conditions for number fields to be Witt equivalent. Namely, given number fields $K$ and $L$, their Witt rings $W(K)$ and $W(L)$ are isomorphic if and only if:

A) $r_1(K) = r_1(L)$
B) $-1 \in K^{*2} \iff -1 \in L^{*2}$
C) there exists a bijection

\[
\begin{align*}
\text{Dyadic Prime Ideals of } K & \leftrightarrow \text{Dyadic Prime Ideals of } L \\
\end{align*}
\]

such that if $P \leftrightarrow Q$, then

\[
[K_P : Q_2] = [L_Q : Q_2]
\]

and $-1 \in K_P^{*2} \iff -1 \in L_Q^{*2}$

where $r_1(K)$ denotes the number of distinct embeddings of the field $K$ into the field of real numbers. These conditions are simple enough to allow one to quickly read off whether or not two given number fields are Witt equivalent. In addition, they yield more general results about forms over number fields, two of which are finiteness statements.

Fix a degree $n \in \mathbb{N}$. Witt equivalence partitions the set of number fields of degree $n$ into classes; that is, two fields are in the same class if and only if they have
isomorphic Witt rings. The first finiteness theorem states that the number of Witt equivalence classes of number fields of degree $n$ is finite.

The second finiteness result concerns the classification of reciprocity equivalences into two types, tame and wild, which are defined as follows. [P-S-C] shows that a reciprocity equivalence canonically induces isomorphisms between the local square-class groups. If such a local map sends the square class of a local prime element to the square class of a local unit, then the reciprocity equivalence is wild at the (finite) place $P$ which corresponds to the given localization; otherwise, it is tame at $P$. The wild set of a reciprocity equivalence consists of all (finite) places at which the equivalence is wild. It is conjectured that reciprocity equivalences with infinite wild sets really do exist. We do not discuss this here; however, we do show for our second finiteness result that whenever a reciprocity equivalence exists (infinite wild set or not), it can be replaced by another equivalence whose wild set is finite.

Chapter II focuses on equivalence at the local level. Namely, given a number field $K$ and a place $P$ of $K$, we study the local square-class group $K_P^*/K_P^{*2}$ as an inner product space over $F_2$, where the inner product is given by the local Hilbert symbol. Kaplansky has classified inner product spaces over $F_2$. For our spaces, Kaplansky's results imply that these local inner product spaces are classified, up to isometry, by the number of square classes and whether or not $-1$ is a local square. Next, we take a finite set $S$ of places of $K$ where $S$ contains $S_\infty$, the set of all infinite places of $K$. If we let $G(S)$ denote the direct product of the local square-class groups $K_P^*/K_P^{*2}$ over all places $P$ of $S$, then there is a natural map $i_S$ from the group $U_K(S)/U_K(S)^2$ of $S$-units of $K$ modulo squares to $G(S)$. Our main technical lemma is, for suitable sets $S$, to identify the image of the $S$-units modulo squares in $G(S)$ or, equivalently, to identify the cokernel of the map $i_S$; this is our Cokernel Lemma.

[P-S-C] shows how to obtain a reciprocity equivalence between two number fields $K$ and $L$, assuming one is presented with a small equivalence; that is, a commutative diagram

$$
\begin{array}{ccc}
U_K(S)/U_K(S)^2 & \overset{i_S}{\longrightarrow} & G(S) \\
\downarrow t_{SS'} & & \downarrow \prod t_P \\
U_L(S')/U_L(S')^2 & \overset{i_{S'}}{\longrightarrow} & G(S')
\end{array}
$$
where $S, S'$ is a pair of suitable sets of places of $K, L$ respectively, and $t_P$ is a group isomorphism of the local square-class groups $K_p^*/K_p^{*2}$ and $L_T^*/L_T^{*2}$ (for some bijection $T : S \rightarrow S'$). Chapter III is devoted to proving that the conditions A), B), and C) imply the existence of a small equivalence. The idea is as follows: we begin with the sets $S, S'$ of all infinite and dyadic places of $K, L$ respectively, and determine the obstruction to this pair yielding a small equivalence. First, we must guarantee that the maps $i_S$ and $i_{S'}$ are injective. It turns out that this is forced when the $S$— and $S'$—class numbers of $K$ and $L$ are odd; to accomplish this, we add finitely many prime ideals to each of $S, S'$. Next, it is clear that we can define an isomorphism $t_{SS'}$ yielding a small equivalence if and only if the image of $(\prod_{P \in S} t_P) \circ i_S$ in $G(S)$ lies in the image of $i_{S'}$. For this, we let $H(S)$ be the set of all elements $x$ in $U_K(S)/U_K(S)^2$ whose image in $G(S')$ lies in the group $i_{S'}(U_L(S')/U_L(S')^2)$. The pair $S, S'$ gives a small equivalence if and only if $H(S) = U_K(S)/U_K(S)^2$; that is, if and only if
\[
\dim_{F_2} \left( \frac{U_K(S)/U_K(S)^2}{H(S)} \right) = 0.
\]
In general, this obstruction is non-zero (although it is always finite). The key is to prove that each of $S$ and $S'$ can be augmented in such a way as to make the obstruction decrease; the Obstruction-Killing Lemma does this. Repeating this process finitely many times, we obtain a small equivalence, hence by [P-S-C, Theorem 1], a reciprocity equivalence between $K$ and $L$.

At this point, we have shown that the conditions A), B), and C) are sufficient for the existence of a small equivalence which, in turn, is sufficient for the existence of a reciprocity equivalence. One easily shows that reciprocity equivalent fields satisfy the conditions A), B), and C). Thus the weakest criteria, conditions A), B), and C), are seen to be necessary and sufficient for the existence of a reciprocity equivalence. We combine these observations in Chapter IV to conclude:

**Theorem.** Let $K$ and $L$ be number fields. The following are equivalent:

1. $K$ and $L$ are Witt equivalent.
2. $K$ and $L$ are reciprocity equivalent.
3. There is a small equivalence between $K$ and $L$.
4. $K$ and $L$ satisfy conditions A), B), and C).
The remainder of Chapter IV is devoted to the study of consequences of this theorem. To illustrate the power of the conditions A), B), and C), we classify the quadratic number fields up to Witt equivalence; they had been classified previously by A. Czogała up to tame equivalence (see [Cz]).
CHAPTER I
Preliminaries

§1.1. Introduction

As the title suggests, this chapter is essentially a review of basic concepts and results. No attempt is made to prove the material presented here, although references are given in most cases. A brief perusal of this chapter is encouraged, as we establish much of our notation in these sections. In addition, we include several observations which may be of interest in subsequent chapters.

§1.2. A Review of Basic Form Theory

Let $E$ be a field and $(V, \beta)$ be an inner product space over $E$. That is, $V$ is an $E$-vector space and $\beta$ a symmetric bilinear form over $E$.

Definition 1.1: The $E$-inner product space $(V, \beta)$ is regular or non-degenerate if the map

$$\text{Ad}_{\beta} : V \rightarrow \text{Hom}_E(V, E)$$

$$x \mapsto \beta(x, x)$$

is an $E$-vector space isomorphism (where $\text{Hom}_E(V, E)$ denotes the vector space dual of $V$).

In this dissertation, it is to be understood that all inner product spaces are regular, whether explicitly stated or not.

Let $(V, \beta)$ be an $E$-inner product space and $W$ a subspace of $V$. 

5
Definition 1.2: The orthogonal complement, $W^\perp$, of $W$ is the subspace of $V$ defined by

$$W^\perp = \{x \in V \mid \beta(x, W) = 0\}.$$ 

We observe that $(W, \beta)$ is an $E$-inner product space if and only if

$$W \cap W^\perp = \{0\}$$

(where "\beta" is understood to mean $\beta$ restricted to $W$). It is always true, however, that

$$\dim_E W + \dim_E W^\perp = \dim_E V,$$

for any subspace $W$ of $V$ (where $\dim_E W$ denotes the dimension of the subspace $W$ over the field $E$). As we indicated above, the subspaces $W$ and $W^\perp$ of $V$ do not have to be distinct. In fact, when $W = W^\perp$, we make the following definition:

Definition 1.3: The subspace $W$ is called a metabolizer of $(V, \beta)$ if $W = W^\perp$.

Let $(V_1, \beta_1)$ and $(V_2, \beta_2)$ be inner product spaces over $E$. In Chapter II, we will be interested in determining when two inner products are the "same" in the following sense:

Definition 1.4: The spaces $(V_1, \beta_1)$ and $(V_2, \beta_2)$ are said to be isometric if there exists an $E$-linear isomorphism

$$\tau : V_1 \rightarrow V_2$$

such that

$$\beta_1(x, y) = \beta_2(\tau x, \tau y) \quad \text{for all} \ x, y \in V_1.$$ 

The isomorphism $\tau$ is called an isometry of $(V_1, \beta_1)$ and $(V_2, \beta_2)$.

Given two $E$-inner product spaces $(V_1, \beta_1)$ and $(V_2, \beta_2)$, we can add them as follows. Let $(V_1, \beta_1) \oplus (V_2, \beta_2)$ denote the $E$-inner product space

$$(V_1 \oplus V_2, \beta_1 \oplus \beta_2),$$
where $V_1 \oplus V_2$ is the direct sum of the vector spaces $V_1$ and $V_2$; since every vector $w$ in $V_1 \oplus V_2$ can be written uniquely as $w = v_1 \oplus v_2$ with $v_i \in V_i$ for $i = 1, 2$, we define

$$(\beta_1 \oplus \beta_2)(w) = \beta_1(v_1) + \beta_2(v_2).$$

Two spaces $(V_1, \beta_1)$ and $(V_2, \beta_2)$, are said to be *equivalent*, $(V_1, \beta_1) \sim (V_2, \beta_2)$, if $(V_1, \beta_1) \oplus (V_2, -\beta_2)$ has a metabolizer (observe that isometric spaces are equivalent). This relation forms an equivalence relation on the set of all isometry classes of $E$-inner product spaces. This set of equivalence classes has a natural ring structure; this ring is called the *Witt ring*, $W(E)$, of $E$.

One way to compare forms over a number field $K$ with those over another number field $L$ is to determine whether or not their Witt rings are isomorphic. Since isomorphism of Witt rings induces an equivalence relation on the set of all number fields, we make the following definition:

**Definition 1.5**: Let $K$ and $L$ be number fields. Then $K$ and $L$ are said to be *Witt equivalent*,

$$K \sim \omega L,$$

if and only if $W(K) \cong W(L)$.

§I.3. Some Fundamental Results from Number Theory

Let $K$ be a number field and $O_K$ its ring of integers. A *place* of $K$ is an equivalence class of valuations on $K$, represented by either an embedding of $K$ into the field of real numbers, a pair of complex conjugate embeddings of $K$ into the complex numbers, or a prime ideal of $O_K$. The first two represent archimedean valuations of $K$ and are called *infinite places* or *infinite primes* of $K$. The third is referred to as a *finite place* of $K$ and represents a non-archimedean valuation of $K$. Therefore a place of $K$ is either a prime ideal of $O_K$ or an infinite prime of $K$. By a "prime ideal of $K" we mean a prime ideal of $O_K$. We write $\Omega_K$ to denote the set of all places of $K$. $S_\infty$ is defined to be the set of all infinite places of $K$. 
The following list consists of three basic results from number theory which we use frequently throughout this paper. No attempt is made to prove them here; we state them primarily for the sake of clarity.

1. Let $r_1(K)$ represent the number of real infinite primes of $K$ and $r_2(K)$ the number of complex infinite primes of $K$. These two quantities are related in the following way:

$$r_1(K) + 2 \cdot r_2(K) = [K : \mathbb{Q}]$$

where $[K : \mathbb{Q}]$ denotes the degree of $K$ over $\mathbb{Q}$, the field of rational numbers.

2. Let $L/K$ be a finite extension of number fields and $\mathfrak{p}$ a prime ideal of $K$. The $O_L$-ideal $\mathfrak{p} \cdot O_L$ uniquely factors in $O_L$ as a product of prime $O_L$-ideals, say

$$\mathfrak{p} \cdot O_L = P_1^{e_1} P_2^{e_2} \cdots P_g^{e_g}$$

where $\{P_i\}_{i=1}^g$ are distinct prime $O_L$-ideals and $e_i \geq 1$ for all $i = 1, 2, \ldots, g$.

The Fundamental Equality of (Algebraic) Number Theory (see [Mc, Theorem 21]) states that

$$\sum_{i=1}^g [L_{P_i} : K_{\mathfrak{p}}] = [L : K]$$

where $L_{P_i}$ and $K_{\mathfrak{p}}$ denote the $p$-adic completions of $L$ at $P_i$ (for all $i = 1, 2, \ldots, g$) and $K$ at $\mathfrak{p}$, respectively.

3. The Hasse-Minkowski Principle (see [Lm, Pgs. 168-171]) is a well-known result for forms over global fields (number fields or function fields in one variable over finite fields). In Chapter IV we refer to the following corollary of the Hasse-Minkowski Principle, called the Global Square Theorem:

**Global Square Theorem.** Let $K$ be a number field and $a \in K^*$. Then

$$a \in K^{*2} \iff a \in K_{P}^{*2} \quad \text{for all places } P \text{ in } \Omega_K.$$

In other words, the element $a$ is a square in $K$ if and only if it is a square in the $p$-adic field $K_P$ for every place $P$ of $K$. 
§I.4. Hilbert Symbols and Reciprocity Equivalence

Let $E$ be a field. By an element $a$ of the square-class group $E^*/E^{*2}$ of $E$, we mean the square class of the element $a$ in $E^*$.

Given a number field $K$, fix a place $P$ of $K$ and elements $a, b \in K^*/K^{*2}$.

**Definition 1.6**: The *Hilbert symbol* $(a, b)_P$ is defined by

$$ (a, b)_P = \begin{cases} +1 & \text{if there exist } x, y \in K_P \text{ for which } ax^2 + by^2 = 1 \\ -1 & \text{otherwise.} \end{cases} $$

Below we recall several important properties of Hilbert symbols. The first is essential to the development of the local inner product spaces which we study in Chapter II:

**Non-degeneracy of the Hilbert Symbol**. Fix a place $P$ of the number field $K$. Given any element $a \in K^*/K^{*2}$, we have

$$(a, b)_P = 1 \text{ for all } b \in K^*/K^{*2} \iff a \in K_P^{*2};$$

that is, if and only if $a$ is a local square at $P$.

In particular, $a \neq 1$ in $K^*/K^{*2}$ implies that there exists an element $b \in K^*/K^{*2}$ for which $(a, b)_P = -1$ (see [LM, Theorem VI.2.16]).

From the definition, one easily shows that Hilbert symbols are symmetric:

1) $(a, b)_P = (b, a)_P$

and bi-multiplicative:

2) $(a, bc)_P = (a, b)_P (a, c)_P$

3) $(ab, c)_P = (a, c)_P (b, c)_P$.

Similarly, one can establish:

4) $(a, 1)_P = 1$ for all $a \in K^*/K^{*2}$

and

5) $(a, a)_P = (a, -1)_P$ for all $a \in K^*/K^{*2}$.

We remark that whenever $a, b \in K^*/K^{*2}$, then $(a, b)_P = 1$ for almost all places $P$ of $K$. With this in mind, we state perhaps the most important property of Hilbert symbols, the reciprocity law:
HILBERT’S RECIPROCITY LAW. Let $K$ be a number field and $a, b \in K^*$. Then

$$\prod_{P \in \Omega_K} (a, b)_P = 1.$$  

This relationship between the symbols $\{(a, b)_P\}_{P \in \Omega_K}$ is useful for calculating either one symbol $(a, b)_P$ at a particular place $P$ or a product $\prod_{P \in S} (a, b)_P$ of symbols (where $S$ is some proper subset of $\Omega_K$), provided the product of the remaining symbols is known.

We are now in a position to define an equivalence of Hilbert symbol reciprocity laws, or reciprocity equivalence, between two number fields. (see [P-S-C, Introduction]):

**Definition 1.7:** A reciprocity equivalence between number fields $K$ and $L$ is a pair of maps $(\tau, \tau)$ where

$$T : \Omega_K \rightarrow \Omega_L$$

is a bijection between the set $\Omega_K$ of all places of $K$ and the set $\Omega_L$ of all places of $L$ and

$$t : K^*/K^{*2} \rightarrow L^*/L^{*2}$$

is a group isomorphism of the square-class groups $K^*/K^{*2}$ and $L^*/L^{*2}$, which together preserve the Hilbert symbols

$$(a, b)_P = (\tau a, \tau b)_{\tau P}$$

for all elements $a, b \in K^*/K^{*2}$ and for all places $P \in \Omega_K$.

§I.5. The S-Ideal Class Group

Let $K$ be a number field and $S \subseteq \Omega_K$ a finite set of places of $K$ with $S_{\infty} \subseteq S$. The ring, $O_K(S)$, of $S$-integers in $K$ consists of all elements of $K$ which are integers at every prime ideal $P$ of $O_K$ not in $S$:

$$O_K(S) = \{x \in K \mid ord_P(x) \geq 0 \text{ for all prime ideals } P \not\in S\}.$$
Observe that the ring $O_K$ of integers of $K$ is contained in the ring $O_K(S)$ of $S$-integers of $K$, since $x \in O_K$ implies $ord_P(x) \geq 0$ for all prime ideals $P$ of $O_K$. The group $U_K(S)$ of $S$-units of $K$ is the subgroup of $O_K(S)$ consisting of all $S$-integers which are units at every prime ideal $P$ not in $S$. That is, $x \in O_K(S)$ is an $S$-unit if and only if $ord_P(x) = 0$ for all prime ideals $P \in \Omega_K \setminus S$. As with the rings of integers, the group $U_K(S)$ is always contained in the group $U_K(S)$ of $S$-units of $K$. We will use the notation $U_K(S)/U_K(S)^2$ to denote the group of $S$-units of $K$ modulo squares.

Given a number field $K$, recall that the set of fractional $O_K$-ideals, modulo the principal $O_K$-ideals, forms a group called the ideal class group, $C(K)$, of $K$. It is a finite group for every number field $K$. The order of the ideal class group is called the ideal class number, $h(K)$, of $K$.

Given $S \subseteq \Omega_K$ a finite set of places of $K$ with $S_\infty \subseteq S$, we can make a similar construction. The set of all fractional $O_K(S)$-ideals forms a multiplicative group. If we mod out by the subgroup of principal $O_K(S)$-ideals, we obtain a group called the $S$-ideal class group, $C^S(K)$, of $K$. The order of this group is also finite and denoted by $h^S(K)$, the $S$-ideal class number of $K$. There is a natural epimorphism

$$C(K) \longrightarrow C^S(K) \longrightarrow 1$$

which implies

$$h^S(K) \mid h(K).$$

That is, the $S$-ideal class number of $K$ divides the ideal class number of $K$. 
CHAPTER II
Local Inner Product Spaces

§II.1. Introduction

Let $K$ be a number field and $P$ a place of $K$; then the local square-class group $K_P^*/K_P^{*2}$ is an $\mathbb{F}_2$-vector space. The Hilbert symbol $(\ , )_P$ can be viewed as an $\mathbb{F}_2$-valued inner product on $K_P^*/K_P^{*2}$ if $\mathbb{F}_2$ is identified with the multiplicative group $\{\pm 1\}$. From this perspective, we can use the theory of inner product spaces to examine local equivalence. For example, Kaplansky classifies $\mathbb{F}_2$-inner product spaces in [Ka]. Interpreting these results for the spaces $(K_P^*/K_P^{*2}, (\ , )_P)$, we see that they are classified, up to isometry, by the number of square classes and whether or not $-1$ is a local square. This observation, which we call Kaplansky's Lemma, turns out to be one of our most valuable tools, as its frequent use illustrates.

Next, given a finite set $S$ of places of $K$ with $S_\infty \subseteq S$, put

$$G(S) = \prod_{P \in S} K_P^*/K_P^{*2} \quad \text{and} \quad \langle \ , \rangle_S = \prod_{P \in S} (\ , )_P.$$ 

Then $(G(S), \langle \ , \rangle_S)$ is an $\mathbb{F}_2$-inner product space in the obvious way. There is a natural map $i_S$ from the group $U_K(S)/U_K(S)^2$ of $S$-units of $K$ modulo squares to $G(S)$. The main technical result of this dissertation is, for suitable sets $S$, to identify the cokernel of the map $i_S$. The Cokernel Lemma, which concludes Chapter II, accomplishes this by describing the cokernel of $i_S$ in terms of the generalized ideal class group of $K$ associated to a cycle on $K$ canonically determined by $S$.

§II.2. The Inner Product Space $(K_P^*/K_P^{*2}, (\ , )_P)$

Let $K$ be a number field and $P$ a place of $K$. As we noted above, the local square-class group $K_P^*/K_P^{*2}$ can be viewed as an $\mathbb{F}_2$-vector space. We define the
following map on $K_P^*/K_P^{*2} \times K_P^*/K_P^{*2}$:

$$(,)_P : K_P^*/K_P^{*2} \times K_P^*/K_P^{*2} \longrightarrow F_2$$

where $F_2$ is identified with the multiplicative group $\{\pm 1, \times\}$. This map is well-defined since the local Hilbert symbol $(a,b)_P$ depends only on the square classes of the elements $a$ and $b$ in $K_P^*$. Moreover, $(,)_P$ is a non-degenerate symmetric bilinear form on $K_P^*/K_P^{*2}$. Therefore, $(K_P^*/K_P^{*2},(,)_P)$ is a regular $F_2$-inner product space.

There exists the notion of a regular inner product space $(K_P^*/K_P^{*2},(,)_P)$ being "trivial" in the sense that $(a,a)_P = 1$ for all $a \in K_P^*/K_P^{*2}$ (observe that this does not necessarily imply that the inner product $(,)_P$ is the trivial map on $K_P^*/K_P^{*2} \times K_P^*/K_P^{*2}$; by the non-degeneracy of the Hilbert symbol, it is trivial if and only if $K_P^*/K_P^{*2} = \{1\}$). We make the following definition.

Definition 2.1: The space $(K_P^*/K_P^{*2},(,)_P)$ is totally isotropic if and only if

$$(a,a)_P = 1 \quad \text{for all } a \in K_P^*/K_P^{*2}$$

and not totally isotropic otherwise; that is, if there exists an element $a \in K_P^*/K_P^{*2}$ for which $(a,a)_P = -1$.

We claim that the inner product space $(K_P^*/K_P^{*2},(,)_P)$ is totally isotropic if and only if $-1$ is a square in $K_P^*$. Namely, recalling that $(a,a)_P = (a,-1)_P$ for all $a$ in $K_P^*/K_P^{*2}$ and for all places $P$, we have

$$(K_P^*/K_P^{*2},(,)_P) \text{ is totally isotropic} \iff (a,a)_P = 1 \text{ for all } a \in K_P^*/K_P^{*2}$$

$$\iff (a,-1)_P = 1 \text{ for all } a \in K_P^*/K_P^{*2}$$

$$\iff -1 = 1 \in K_P^{*2} \text{ or } -1 \in K_P^{*2}.$$
isometry of \((K_p^*/K_{p^2}^*, (\cdot, \cdot)_P)\) and \((L_Q^*/L_{Q^2}^*, (\cdot, \cdot)_Q)\) is an isomorphism of the local square-class groups \(K_p^*/K_{p^2}^2\) and \(L_Q^*/L_{Q^2}^2\) which preserves the local Hilbert symbol. Such maps have the following property (see [P-S-C, Lemma 1]):

**Lemma 2.1.** If \(t : K_p^*/K_{p^2}^2 \cong L_Q^*/L_{Q^2}^2\) is an isometry, then \(t(-1) = -1\).

**Proof of Lemma 2.1:** Let \(t(-1) = c\). Then

\[
(a, a)_P = (a, -1)_P = (ta, t(-1))_Q = (ta, c)_Q \\
= (ta, -1)_Q(ta, -c)_Q \\
= (ta, ta)_Q(ta, -c)_Q \\
= (a, a)_P(ta, -c)_Q \quad \text{for all } a \in K_p^*/K_{p^2}^2.
\]

Thus, \((ta, -c)_Q = 1\) for all \(a \in K_p^*/K_{p^2}^2\), or equivalently, \((b, -c)_Q = 1\) for all \(b \in L_Q^*/L_{Q^2}^2\). By the non-degeneracy of the Hilbert symbol, this implies that

\[-c = 1 \in L_Q^*/L_{Q^2}^2 \quad \text{or} \quad c = -1 \in L_Q^*/L_{Q^2}^2.\]

That is, \(t(-1) = c = -1 \in L_Q^*/L_{Q^2}^2\). \(\blacksquare\)

Assume that the inner product spaces \((K_p^*/K_{p^2}^2, (\cdot, \cdot)_P)\) and \((L_Q^*/L_{Q^2}^2, (\cdot, \cdot)_Q)\) are isometric. Then \(K_p^*/K_{p^2}^2\) and \(L_Q^*/L_{Q^2}^2\) are isomorphic as finite-dimensional \(\mathbb{F}_2\)-vector spaces, so

\[
\text{(2.1)} \quad \dim_{\mathbb{F}_2} K_p^*/K_{p^2}^2 = \dim_{\mathbb{F}_2} L_Q^*/L_{Q^2}^2.
\]

Moreover, by Lemma 2.1,

\[
\text{(2.2)} \quad -1 \in K_{p^2}^2 \iff -1 \in L_{Q^2}^2.
\]

That is, given an isometry \(t\), we obtain

\[-1 \in K_{p^2}^2 \iff (a, -1)_P = 1 \quad \text{for all } a \in K_p^*/K_{p^2}^2 \]

\[-1 \in K_{p^2}^2 \iff (ta, t(-1))_Q = 1 \quad \text{for all } a \in K_p^*/K_{p^2}^2 \]

\[-1 \in K_{p^2}^2 \iff (ta, -1)_Q = 1 \quad \text{for all } a \in K_p^*/K_{p^2}^2 \quad \text{by Lemma 2.1} \]

\[-1 \in K_{p^2}^2 \iff (b, -1)_Q = 1 \quad \text{for all } b \in L_Q^*/L_{Q^2}^2 \]

\[-1 \in K_{p^2}^2 \iff -1 \in L_{Q^2}^2.\]
Hence, both spaces are either totally isotropic or not totally isotropic. Thus, we have established that

\[
\left( \frac{K^*_P}{K^*_P}, (,)_P \right) \cong_{\text{isometric}} \left( \frac{L^*_Q}{L^*_Q}, (,)_Q \right) \Rightarrow
\]

\[(1) \ dim_{F_2} K^*_P/K^*_P = dim_{F_2} L^*_Q/L^*_Q \]
\[(2) -1 \in K^*_P \iff -1 \in L^*_Q.\]

We claim that the converse is also true. To see this, we consider a pair of theorems from [Ka]. Given a totally isotropic inner product space \((K^*_P/K^*_P, (,)_P)\), [Ka, Theorem 19] guarantees the existence of an \(F_2\)-basis for \(K^*_P/K^*_P\) whose associated matrix of inner products is of the form

\[
\begin{pmatrix}
0 & I_m \\
-I_m & 0
\end{pmatrix}
\]

where \(I_m\) denotes the \((m \times m)\)-identity matrix and \(2m = dim_{F_2} K^*_P/K^*_P\). In particular, any two such totally isotropic spaces having the same dimension must be isometric.

On the other hand, if the inner product space \((K^*_P/K^*_P, (,)_P)\) is not totally isotropic, [Ka, Theorem 20] states that \(K^*_P/K^*_P\) has an orthogonal \(F_2\)-basis. The matrix of inner products corresponding to this basis is the \((n \times n)\)-identity matrix \(I_n\) (where \(n = dim_{F_2} K^*_P/K^*_P\)). Once again we see that any two such not totally isotropic spaces of the same dimension must be isometric.

Combining these observations, we conclude that the \(F_2\)-inner product space \((K^*_P/K^*_P, (,)_P)\) is classified by its dimension over \(F_2\) and whether or not it is totally isotropic. In particular, two such inner product spaces \((K^*_P/K^*_P, (,)_P)\) and \((L^*_Q/L^*_Q, (,)_Q)\) satisfying (2.1) and (2.2) must be isometric. The following lemma summarizes these remarks.

**Lemma 2.2 (Kaplansky’s Lemma).** Let \(K, L\) be number fields and \(P, Q\) places of \(K, L\), respectively. Then

\[
\left( \frac{K^*_P}{K^*_P}, (,)_P \right) \cong_{\text{isometric}} \left( \frac{L^*_Q}{L^*_Q}, (,)_Q \right) \text{ if and only if}
\]

\[(1) \ dim_{F_2} K^*_P/K^*_P = dim_{F_2} L^*_Q/L^*_Q \]
\[(2) -1 \in K^*_P \iff -1 \in L^*_Q.\]
We note that $\dim_{\mathbb{F}_2} K_P^*/K_P^{*2} = \dim_{\mathbb{F}_2} L_Q^*/L_Q^{*2}$ if and only if $K_P^*/K_P^{*2}$ and $L_Q^*/L_Q^{*2}$ have the same order. Namely,

$$\#(K_P^*/K_P^{*2}) = \begin{cases} 
1 & \text{when } P \text{ is a complex infinite prime} \\
2 & \text{when } P \text{ is a real infinite prime} \\
4 & \text{when } P \text{ is a non-dyadic prime ideal} \\
2^{|K_P:Q_2|+2} \geq 8 & \text{when } P \text{ is a dyadic prime ideal.}
\end{cases}$$

Hence

$$\dim_{\mathbb{F}_2}[K_P^*/K_P^{*2}] = \begin{cases} 
0 & \text{when } P \text{ is a complex infinite prime} \\
1 & \text{when } P \text{ is a real infinite prime} \\
2 & \text{when } P \text{ is a non-dyadic prime ideal} \\
[K_P:Q_2] + 2 & \text{when } P \text{ is a dyadic prime ideal.}
\end{cases}$$

§II.4. The Inner Product Space $G(S)$

Let $K$ be a number field and $S$ a finite set of places of $K$ satisfying

$$\text{(2.4)} \quad \text{(1) } S \text{ contains } S_\infty \text{ and all dyadic prime ideals of } K;$$

$$\text{(2) } \text{the } S - \text{class number of } K \text{ is odd.}$$

We write $y \in U_K(S)/U_K(S)^2$ where $y$ represents the square class of the element $y \in K^*$ in the group $U_K(S)/U_K(S)^2$ of $S$-units of $K$ modulo squares. We put

$$G(S) = \prod_{P \in S} K_P^*/K_P^{*2}.$$ 

One easily shows that $U_K(S)/U_K(S)^2$ and $G(S)$ are finite-dimensional $\mathbb{F}_2$-vector spaces. In fact, we have

**Lemma 2.3 (Dimension Lemma).**

1) $\dim_{\mathbb{F}_2} G(S) = 2(\#S)$

2) $\dim_{\mathbb{F}_2} U_K(S)/U_K(S)^2 = (\#S)$.

**Proof of Lemma 2.3:** By definition of $G(S)$, we have

$$\dim_{\mathbb{F}_2} G(S) = \sum_{P \in S} \dim_{\mathbb{F}_2}[K_P^*/K_P^{*2}].$$
Combining (2.3) and (2.5), we obtain

$$dim_{F_2}G(S) = r_1(K) \cdot 1 + r_2(K) \cdot 0 + \sum_{P \in S} (n_P + 2) + m \cdot 2$$

where $m$ denotes the number of non-dyadic prime ideals in $S$, $r_1(K)$ the number of real infinite primes of $K$, and $r_2(K)$ the number of complex infinite primes of $K$. Letting $g_2(K)$ denote the number of dyadic prime ideals of $K$, we see that

$$dim_{F_2}G(S) = r_1(K) + \sum_{P \in S} [K_P : Q_2] + 2 \cdot g_2(K) + 2m.$$

Using the Fundamental Equality of Number Theory,

$$\sum_{P \in S} [K_P : Q_2] = [K : Q],$$

along with the fact that

$$[K : Q] = r_1(K) + 2 \cdot r_2(K),$$

we obtain

$$dim_{F_2}G(S) = 2 [r_1(K) + r_2(K) + g_2(K) + m]$$

or

$$dim_{F_2}G(S) = 2 \cdot (\#S).$$

To prove the second equality, let $S = S_\infty$. The group $U_K(S_\infty)$ of $S_\infty$-units is actually the group $U_K$ of units of $K$. Now Dirichlet's Unit Theorem (see [I-R]) states that $U_K$ can be written as the product of a finite cyclic group of even order (the roots of unity in $K$) and a free group of rank $(\#S_\infty - 1)$. Thus, the group $U_K(S_\infty)/U_K(S_\infty)^2$ of $S_\infty$-units of $K$ modulo squares is isomorphic to the direct product of $(\#S_\infty)$ copies of $\mathbb{Z}/2\mathbb{Z}$:

$$U_K(S_\infty)/U_K(S_\infty)^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z},$$

which implies that

$$dim_{F_2}U_K(S_\infty)/U_K(S_\infty)^2 = (\#S_\infty).$$

Let $S = \{ \text{finite sets } S \mid S_\infty \subseteq S \subseteq \Omega_K \}$. We make the following claim.
CLAIM: \( \dim_{F_2} \frac{U_K(S)}{U_K(S)^2} = (\#S) \) for all \( S \) in \( S \).

By (2.6), \( S_\infty \) satisfies the claim. Assume it holds for all \( S \in S \) of order \( \ell \) where \( \ell \geq (\#S_\infty) \). Fix a set \( S \in S \) with \( (\#S) = \ell + 1 \). It remains to show that \( \dim_{F_2} \frac{U_K(S)}{U_K(S)^2} = \ell + 1 \). Now \( (\#S) > (\#S_\infty) \) implies that there exists a prime ideal \( P \) of \( K \) in the set \( S \). Fixing such a prime ideal \( P \), we can write \( S = \hat{S} \cup \{P\} \) where \( \hat{S} \in S \) has order \( \ell \). By induction, the claim holds for \( \hat{S} \):

\[
\dim_{F_2} \frac{U_K(\hat{S})}{U_K(\hat{S})^2} = (\#\hat{S}) = (\#S - 1).
\]

If we fix a prime element \( \pi \in K^* \) for \( P \), then we can express \( \frac{U_K(S)}{U_K(S)^2} \) as the disjoint union

\[
\frac{U_K(S)}{U_K(S)^2} = \frac{U_K(\hat{S})}{U_K(\hat{S})^2} \cup \pi \cdot \frac{U_K(\hat{S})}{U_K(\hat{S})^2}.
\]

From this we obtain that

\[
\dim_{F_2} \frac{U_K(S)}{U_K(S)^2} = (\#\hat{S} + 1) = (\#S),
\]

or the claim holds for \( S \). By induction, it must hold for all \( S \in S \). \( \blacksquare \)

An element \( a \) in

\[
G(S) = \prod_{P \in S} \frac{K^*_P}{K_{P^2}}
\]

is a tuple \((a, a, \ldots, a)\) where the \( P^{th} \) coordinate represents the image of the element \( a \in K^* \) in the local square-class group \( \frac{K^*_P}{K_{P^2}} \). \( G(S) \) can be made into an \( F_2 \)-inner product space. We define the map \( \langle \, , \, \rangle_S \) on \( G(S) \times G(S) \) as follows:

\[
\langle \, , \, \rangle_S : G(S) \times G(S) \rightarrow F_2
\]

\[
(a, b) \mapsto \prod_{P \in S} (a, b)_P
\]

where \((F_2, +)\) is identified with \( (\{\pm 1\}, \times) \). The fact that each of the Hilbert symbols \( (\, , \,)_P \) is well-defined implies that \( \langle \, , \, \rangle_S \) is also a well-defined map. Moreover, \( \langle \, , \, \rangle_S \) is a non-degenerate symmetric bilinear form on \( G(S) \), since the Hilbert symbol \( (\, , \,)_P \) is a non-degenerate symmetric bilinear form on \( \frac{K^*_P}{K_{P^2}} \) for each \( P \in S \). Hence, \( (G(S), \langle \, , \, \rangle_S) \) is a regular \( F_2 \)-inner product space.
§11.5. The Subspace $i_S \left( \mathbf{U}_K(S)/\mathbf{U}_K(S)^2 \right)$ of $G(S)$

Let $K$ be a number field and $S$ a finite set of places of $K$ satisfying conditions (1) and (2) of (2.4). Then the group $\mathbf{U}_K(S)/\mathbf{U}_K(S)^2$ can be diagonally embedded into $G(S)$ as follows:

$$i_S : \mathbf{U}_K(S)/\mathbf{U}_K(S)^2 \rightarrow G(S)$$

$$y \rightarrow y = (y, y, \ldots, y).$$

The map $i_S$ is well-defined; for if $z \in K^*$ is another representative of the class of $y$ in $\mathbf{U}_K(S)/\mathbf{U}_K(S)^2$, then

$$z = y \cdot w^2 \quad \text{in } K^*$$

for some $S$-unit $w$. Therefore, we have

$$z = y \cdot w^2 \quad \text{in } K^*_P \quad \text{for all } P \in S$$

or

$$z = y \quad \text{in } G(S).$$

One easily checks that $i_S$ is a homomorphism. Using the assumption that $h^S(K)$ is odd, [P-S-C, Lemma 4] shows that $i_S$ is also injective.

Next let us consider $i_S \left( \mathbf{U}_K(S)/\mathbf{U}_K(S)^2 \right)$ as a subspace of the $\mathbb{F}_2$-inner product space $(G(S), \langle , \rangle_S)$. The non-degeneracy of $(G(S), \langle , \rangle_S)$ implies that

$$\dim_{\mathbb{F}_2} [i_S (\mathbf{U}_K(S)/\mathbf{U}_K(S)^2)] + \dim_{\mathbb{F}_2} \left[ i_S \left( \mathbf{U}_K(S)/\mathbf{U}_K(S)^2 \right)^\perp \right] = \dim_{\mathbb{F}_2} G(S).$$

Lemma 2.3 (Dimension Lemma) and the injectivity of $i_S$ guarantee that

$$\dim_{\mathbb{F}_2} \left[ i_S (\mathbf{U}_K(S)/\mathbf{U}_K(S)^2) \right] = \frac{1}{2} \dim_{\mathbb{F}_2} G(S).$$

Combining (2.7) and (2.8), we obtain

$$\dim_{\mathbb{F}_2} \left[ i_S (\mathbf{U}_K(S)/\mathbf{U}_K(S)^2) \right] = \dim_{\mathbb{F}_2} \left[ i_S (\mathbf{U}_K(S)/\mathbf{U}_K(S)^2)^\perp \right].$$

We claim that $i_S \left( \mathbf{U}_K(S)/\mathbf{U}_K(S)^2 \right)$ is a metabolizer in $G(S)$. 
Lemma 2.4. \( i_S (U_K(S)/U_K(S)^2) \subseteq G(S) \) is a metabolizer in the \( F_2 \)-inner product space \( (G(S), (\cdot, \cdot)_S) \).

Proof of Lemma 2.4: By Definition 1.2, we must show

\[
i_S (U_K(S)/U_K(S)^2) = i_S (U_K(S)/U_K(S)^2)^{\perp}.
\]

It suffices, however, to prove:

\[
(2.10) \quad i_S (U_K(S)/U_K(S)^2) \subseteq i_S (U_K(S)/U_K(S)^2)^{\perp}
\]

since \( (2.9) \) and \( (2.10) \), together with the fact that the common dimension in \( (2.9) \) is finite, yield the desired result.

To establish \( (2.10) \), recall that

\[
i_S (U_K(S)/U_K(S)^2)^{\perp} = \{ b \in G(S) : \langle a, b \rangle_S = 1 \text{ for all } a \in i_S (U_K(S)/U_K(S)^2) \}.
\]

Fix \( b \in i_S (U_K(S)/U_K(S)^2) \). By Hilbert’s reciprocity law, we have the following for all \( a \in i_S (U_K(S)/U_K(S)^2) \):

\[
1 = \prod_{P \in \Omega_K} (a, b)_P
= \prod_{P \in S} (a, b)_P \cdot \prod_{P \notin S} (a, b)_P.
\]

Now \( (a, b)_P = 1 \) for all \( P \notin S \); that is, \( P \) is a non-dyadic prime ideal and \( a, b \) as elements of \( i_S (U_K(S)/U_K(S)^2) \) are units at \( P \). Therefore, we have

\[
1 = \prod_{P \in S} (a, b)_P \cdot 1
= \prod_{P \in S} (a, b)_P = \langle a, b \rangle_S.
\]

Hence, \( b \in i_S (U_K(S)/U_K(S)^2)^{\perp} \), and \( (2.10) \) holds. \( \square \)

§II.6. The Cokernel of \( i_S \)

As before, let \( K \) be a number field and \( S \) a finite set of places of \( K \) satisfying \( (2.4) \). We noted earlier that \( i_S : U_K(S)/U_K(S)^2 \to G(S) \) is injective. The fact
that
\[
dim_{F_2} \left[ i_S \left( U_K(S)/U_K(S)^2 \right) \right] = \frac{1}{2} \dim_{F_2} G(S) > 0
\]
guarantees that it is not surjective. In particular, \( i_S \left( U_K(S)/U_K(S)^2 \right) \) is a proper subspace of \( G(S) \). To analyze the concept of small equivalence of number fields in Chapter III, we need a characterization of the subspace \( i_S \left( U_K(S)/U_K(S)^2 \right) \) of \( G(S) \) or, equivalently, the

Cokernel of \( i_S = G(S)/i_S \left( U_K(S)/U_K(S)^2 \right) \).

We proceed as follows:

**Definition 2.2:** Given a finite set \( S \) of places of \( K \), the cycle \( c_S \) of \( K \) is defined by

\[
c_S = \prod_{P \in S} P^{m_P}
\]

where

\[
m_P = \begin{cases} 
1 & \text{if } P \text{ is a real infinite prime or non-dyadic prime ideal} \\
0 & \text{if } P \text{ is a complex infinite prime} \\
2e_P(K) + 1 & \text{if } P \text{ is a dyadic prime ideal}
\end{cases}
\]

and \( e_p(K) \) denotes the ramification index of \( P \) in \( K \).

**Definition 2.3:** Given \( a \in K^* \), we say

\[
a \equiv 1 \pmod{c_S}
\]

if \( a \equiv 1 \pmod{P^{m_P}} \) for all \( P \in S \). That is, \( a = 1 \) in \( K^*_P/K^*_P \) for all \( P \in S \). In particular, for \( P \) a real infinite prime, it implies that \( a \) is positive in the embedding \( K \hookrightarrow \mathbb{R} \) corresponding to \( P \). For \( P \) a prime ideal, it says that \( a \) is a local unit at \( P \) or \( \text{ord}_P(a) = 0 \).

Let \( I(K, c_S) \) denote the set of fractional \( O_K \)-ideals which are prime to \( c_S \) and \( P(K, c_S) \) the principal \( O_K \)-ideals \( A \) for which there exists a generator \( x \in K^* \) with \( x \equiv 1 \pmod{c_S} \).
Definition 2.4: The generalized ideal class group, \( \mathcal{C}(K,c_S) \), associated to the cycle \( c_S \) is the group
\[
\mathcal{C}(K,c_S) = I(K,c_S)/P(K,c_S).
\]

The Cokernel of \( i_S \) can be described using this generalized ideal class group. Namely,

Lemma 2.5 (Cokernel Lemma).
\[
\mathcal{C}(K,c_S)/\mathcal{C}(K,c_S)^2 \cong G(S)/i_S(U_K(S)/U_K(S)^2)
\]

via the map \([\overline{A}] \mapsto (\alpha, \alpha, \ldots, \alpha) \mod i_S(U_K(S)/U_K(S)^2)\), where \( A \in I(K,c_S) \) is an integral \( O_K \)-ideal for which there exists an element \( \alpha \) (unique up to an \( S \)-unit) in \( O_K(S) \) such that
\[
A^{h_S(K)} \cdot O_K(S) = \alpha \cdot O_K(S).
\]

Remarks:
1. As \( O_K \)-ideals, recall that \( A^{h_S(K)} = \alpha \cdot A \), where \( A \) is an \( O_K \)-ideal containing only ideals in \( S \).
2. The symbol \([\overline{A}]\) is to be interpreted as follows:
   i) \( \overline{A} \) denotes the class of the ideal \( A \in I(K,c_S) \) in the generalized ideal class group, \( \mathcal{C}(K,c_S) = I(K,c_S)/P(K,c_S) \), associated to \( c_S \).
   ii) \([\overline{A}]\) denotes the square class of the element \( \overline{A} \in \mathcal{C}(K,c_S) \) in the square-class group \( \mathcal{C}(K,c_S)/\mathcal{C}(K,c_S)^2 \).

Proof of Lemma 2.5 (Cokernel Lemma):
First, we define a map
\[
\phi: \mathcal{C}(K,c_S) \longrightarrow G(S)/i_S(U_K(S)/U_K(S)^2)
\]
and verify that it is a well-defined, surjective homomorphism. Next, we observe that \( \phi \) can be extended to a surjective homomorphism
\[
\overline{\phi}: \mathcal{C}(K,c_S)/\mathcal{C}(K,c_S)^2 \longrightarrow G(S)/i_S(U_K(S)/U_K(S)^2)
\]
since
\[
\mathcal{C}(K,c_S)^2 \subseteq \text{kernel}(\phi).
\]
Lastly, we prove that \( \overline{\phi} \) is injective.

Define \( \phi \) as follows:

\[
\phi : \text{Cl}(K, c_S) \longrightarrow G(S) / i_S(U_K(S)/U_K(S)^2)
\]

\[
\overline{A} \longmapsto \alpha = (\alpha, \ldots, \alpha) \mod i_S(U_K(S)/U_K(S)^2)
\]

where \( A \in I(K, c_S) \) and \( \alpha \in O_K(S) \) (unique up to an \( S \)-unit) are such that

\[
A^{h^S(K)} \cdot O_K(S) = \alpha \cdot O_K(S) \text{ as } O_K(S) - \text{ideals.}
\]

**CLAIM**: \( \phi \) is well-defined.

In the process of defining \( \phi \), we made two choices: (1) the representative \( A \) of \( I(K, c_S) \) for the generalized ideal class \( \overline{A} \in \text{Cl}(K, c_S) \), and (2) the element \( \alpha \) of \( O_K(S) \) (unique only up to an \( S \)-unit) which satisfies

\[
A^{h^S(K)} \cdot O_K(S) = \alpha \cdot O_K(S).
\]

First, we claim \( \phi \) is independent of the choice of \( \alpha \). Let \( u \) be an \( S \)-unit which satisfies

\[
(u\alpha) \cdot O_K(S) = A^{h^S(K)} \cdot O_K(S).
\]

Then by definition of \( \phi \), we can map

\[
\overline{A} \longmapsto u\alpha \mod i_S(U_K(S)/U_K(S)^2).
\]

Now

\[
u\alpha = (u\alpha, \ldots, u\alpha) = (u, \ldots, u) \cdot (\alpha, \ldots, \alpha) = u \cdot \alpha \text{ in } G(S).
\]

Since \( u \) an \( S \)-unit,

\[
u = 1 \mod i_S(U_K(S)/U_K(S)^2),
\]

thus

\[
u\alpha = 1 \cdot \alpha = \alpha \mod i_S(U_K(S)/U_K(S)^2)
\]

or

\[
u\alpha = \alpha \text{ in } G(S).
\]

Hence \( \phi \) is independent of the choice of \( \alpha \) in \( O_K(S) \), up to an \( S \)-unit.
Secondly, we must show that \( \phi \) does not depend on the choice of the representative for the generalized ideal class \( \overline{A} \). Let \( x \cdot \mathcal{O}_K(S) \) be an element of \( P(K, cs) \). Then \( x \cdot A \in \overline{A} \) and

\[
(x \cdot A)^{h^s(K)} \cdot \mathcal{O}_K(S) = (\alpha \cdot x^{h^s(K)}) \cdot \mathcal{O}_K(S).
\]

According to the definition of \( \phi \), we can map

\[
\overline{A} \mapsto \alpha \cdot x^{h^s(K)} = (\alpha \cdot x^{h^s(K)}, \ldots, \alpha \cdot x^{h^s(K)}) \mod i_S(U_K(S)/U_K(S)^2).
\]

The fact that \( x \cdot \mathcal{O}_K \in P(K, cs) \) implies that \( x \equiv 1 \pmod{cs} \) or \( x = 1 \) in \( K^*_P/K^*_P^2 \) for all places \( P \) in \( S \). Thus \( x^{h^s(K)} = 1 \) in \( K^*_P/K^*_P^2 \) for all \( P \in S \), or

\[
x^{h^s(K)} = (x^{h^s(K)}, \ldots, x^{h^s(K)}) = (1, \ldots, 1) = 1 \quad \text{in } G(S).
\]

Therefore, we have

\[
\alpha \cdot x^{h^s(K)} = \alpha \cdot 1 = \alpha \mod i_S(U_K(S)/U_K(S)^2).
\]

This implies \( \phi \) is independent of the choice of representative for the generalized ideal class \( \overline{A} \) in \( \mathcal{Cl}(K, cs) \). Hence, \( \phi \) is well-defined, as claimed.

The fact that \( \phi \) is a homomorphism is clear. Namely, given elements \( \overline{A}, \overline{B} \) of \( \mathcal{Cl}(K, cs) \) we can write

\[
A^{h^s(K)} \cdot \mathcal{O}_K(S) = \alpha \cdot \mathcal{O}_K(S) \quad \text{and} \quad B^{h^s(K)} \cdot \mathcal{O}_K(S) = \beta \cdot \mathcal{O}_K(S)
\]

where \( A \in \overline{A}, B \in \overline{B} \) and \( \alpha, \beta \in \mathcal{O}_K(S) \). Therefore

\[
\overline{A} \cdot \overline{B} \mapsto \alpha \beta = \alpha \cdot \beta
\]

since we can write \((A \cdot B)^{h^s(K)} \cdot \mathcal{O}_K(S) = \alpha\beta \cdot \mathcal{O}_K(S)\). Thus, \( \phi(\overline{A} \cdot \overline{B}) = \phi(\overline{A}) \cdot \phi(\overline{B}) \).

Next we would like to prove that \( \phi \) is a surjective homomorphism. For each place \( P \) in \( S \), fix a square class \( y_P \in K^*_P/K^*_P^2 \). Let

\[
y = (y_P, \ldots, y_P) \in G(S)
\]

and \( n_y \) denote the number of coordinates \( y_P \) which satisfy

\[\text{ord}_P(y_P) \equiv 1 \pmod{2}.\]

We proceed by induction on \( n_y \).
Case 1: $y \in \text{Image}(\phi)$ if $n_y = 0$.

By the Approximation Theorem (see [Ws, 1-2-3]), there exists an element $z$ of $O_K^*$ (hence $O_K(S)$) such that

a) $z = y_P$ in $K_P^*/K_P^2$ for each $P \in S$,

or $z = y$ in $G(S)$, and for which

b) $z \cdot O_K \in I(K, c_S)$.

In other words, $z \cdot O_K$ represents a class in $\mathcal{C}(K, c_S)$. So we obtain

$$\phi: z \cdot O_K \mapsto z^{h^S(K)} = z = y \mod \left(\frac{U_K(S)}{U_K(S)^2}\right)$$

since $h^S(K)$ is odd and we can write

$$z^{h^S(K)} \cdot O_K(S) = \left(z^{h^S(K)}\right) \cdot O_K(S) \text{ and } z^{h^S(K)} \in O_K(S).$$

Therefore $y \in \text{Image}(\phi)$ and Case 1 holds.

Case 2: $y \in \text{Image}(\phi)$ if $n_y = 1$.

Now $n_y = 1$ implies that there exists a place $\varphi \in S$ such that

$$\text{ord}_\varphi(y_\varphi) \equiv 1 \pmod{2}$$

(2.11)

and

$$\text{ord}_P(y_\varphi) \equiv 0 \pmod{2} \quad \text{for all } P \in S, P \neq \varphi.$$

Consider the ideal class $c\ell(\varphi^{-1})$ in the ideal class group, $\mathcal{C}(K)$, of $K$. $S$ being a finite set of places, we can find an integral ideal $Q \in c\ell(\varphi^{-1})$ which is prime to $c_S$; that is, $Q \in I(K, c_S)$. By our choice of $Q$, the ideal $Q \cdot \varphi$ is a principal $O_K$-ideal, hence,

$$Q \cdot \varphi = x \cdot O_K \quad \text{as } O_K - \text{ideals}$$

for some $x \in K^*$. From this we see that

$$\text{ord}_\varphi(x) \equiv 1 \pmod{2}$$

(2.12)

and

$$\text{ord}_P(x) \equiv 0 \pmod{2} \quad \text{for all } P \in S, P \neq \varphi.$$

Combining (2.11) and (2.12) yields

$$\text{ord}_P(xy) \equiv 0 \pmod{2} \quad \text{for all } P \in S,$$
including \( P = \varphi \) or
\[
n_{xy} = 0.
\]

This means we can apply Case 1 to the element \( xy \in G(S) \) to obtain an element \( z \) of \( O_K^* \) for which \( z \cdot O_K \in I(K, c_S) \) and
\[
\phi : z \cdot O_K \mapsto xy \mod i_S(U_K(S)/U_K(S)^2).
\]

**Claim:** \( \phi : z \cdot Q \mapsto y \mod i_S(U_K(S)/U_K(S)^2) \).

First note that
\[
z \cdot Q \cdot \varphi = z \cdot O_K \quad \text{as} \quad O_K - \text{ideals},
\]
so we have
\[
z \cdot Q = z \cdot Q \cdot \varphi = zx \cdot O_K(S) \quad \text{as} \quad O_K(S) - \text{ideals}.
\]

This forces
\[
(z \cdot Q)^{h^s(K)} \cdot O_K(S) = (zx)^{h^s(K)} \cdot O_K(S).
\]

Also observe that \((zx)^{h^s(K)} \in O_K(S)\) and \( z \cdot Q \in I(K, c_S) \). Therefore, \( z \cdot Q \) represents a class in \( \mathcal{C}(K, c_S) \) and
\[
\phi : z \cdot Q \mapsto (zx)^{h^s(K)} = z \cdot x = y \mod i_S(U_K(S)/U_K(S)^2),
\]
which proves both our claim and Case 2.

Now assume for some integer \( \ell > 1 \) we have \( y \in \text{Image}(\phi) \) whenever \( n_y < \ell \). It remains to show:

**Case 3:** \( y \in \text{Image}(\phi) \) if \( n_y = \ell \).

The condition \( \ell > 1 \) guarantees the existence of a place \( \varphi \in S \) for which
\[
\text{ord}_{\varphi}(y) \equiv 1 \pmod{2}.
\]

Define elements \( w, t \in G(S) \) as follows:
\[
w_P = y_P \quad \text{and} \quad t_P = 1 \quad \text{in} \quad K^*_P/K^*_P^2
\]
\[
w_P = 1 \quad \text{and} \quad t_P = y_P \quad \text{in} \quad K^*_P/K^*_P^2 \quad \text{for all} \quad P \in S, P \neq \varphi.
\]
Since $n_w = 1$ and $n_t = \ell - 1$, there must exist ideals $\mathcal{A}, \mathcal{B} \in I(K, c_S)$ satisfying

$$\phi : \overline{\mathcal{A}} \mapsto w \mod i_S(U_K(S)/U_K(S)^2)$$

and

$$\phi : \overline{\mathcal{B}} \mapsto t \mod i_S(U_K(S)/U_K(S)^2).$$

Hence

$$\phi : \overline{\mathcal{A}}\overline{\mathcal{B}} \mapsto w \cdot t = y \mod i_S(U_K(S)/U_K(S)^2).$$

Thus, Case 3 holds, proving that $y \in \text{Image}(\phi)$ for all values of $n_y$, hence $\phi$ is surjective.

We note that $\phi$ extends to a surjective homomorphism

$$\overline{\phi} : \text{Cl}(K, c_S)/\text{Cl}(K, c_S)^2 \longrightarrow G(S)/i_S(U_K(S)/U_K(S)^2)$$

since the cokernel of $i_S$ is an elementary abelian 2-group; that is,

$$\text{Cl}(K, c_S)^2 \subseteq \text{kernel}(\phi).$$

Lastly, we prove that $\overline{\phi}$ is an injective homomorphism. Let us suppose $[\overline{\mathcal{A}}]$ is in $\text{Cl}(K, c_S)/\text{Cl}(K, c_S)^2$ and

$$(2.13) \quad \overline{\phi} : [\overline{\mathcal{A}}] \mapsto 1 = (1, \ldots, 1) \mod i_S(U_K(S)/U_K(S)^2).$$

It remains to show $[\overline{\mathcal{A}}] = [\overline{1}]$ in $\text{Cl}(K, c_S)/\text{Cl}(K, c_S)^2$. Let $\alpha \in O_K(S)$ satisfy

$$\mathcal{A} h^S(K) \cdot O_K(S) = \alpha \cdot O_K(S).$$

By (2.13) there exists an element $u \in U_K(S)/U_K(S)^2$ for which

$$\alpha = u \cdot 1 \quad \text{or} \quad \alpha \cdot u = 1 \quad \text{in } K^*_P/K^*_P^2 \quad \text{for all } P \in S.$$

Since $\alpha$ is unique only up to an $S$-unit, we may replace $\alpha$ with $\alpha \cdot u$ and assume that

$$\alpha = 1 \quad \text{in } K^*_P/K^*_P^2 \quad \text{for all } P \in S.$$

This implies for each $P \in S$, there exists an element $y_P \in K^*_P$ satisfying

$$\alpha = y_P^2 \quad \text{in } K^*_P.$$
$S$ being a finite set of places, we can apply the Approximation Theorem to obtain a global element $y \in K^*$ with

$$y = y_P \pmod{P^{m_P}} \quad \text{for all } P \in S.$$ 

But then

$$\alpha \cdot y^2 = y_P^2 \cdot y_P^{-2} = 1 \quad \text{in } K_P^* \quad \text{for all } P \in S;$$

that is to say, $\alpha \cdot y^{-2} \equiv 1 (\text{mod}^* c_S)$ or $\alpha \cdot y^{-2} \cdot O_K \subseteq P(K, c_S)$. Therefore

$$\overline{A} = \overline{\alpha \cdot y^{-2} \cdot A} \quad \text{in } \mathcal{C}(K, c_S).$$

Hence to show $\overline{\phi}$ injective, it suffices to show

$$\left[ \overline{\alpha \cdot y^{-2} \cdot A} \right] = \left[ \overline{1} \right] \quad \text{in } \mathcal{C}(K, c_S)/\mathcal{C}(K, c_S)^2$$

or

$$\overline{\alpha \cdot y^{-2} \cdot A} \in \mathcal{C}(K, c_S)^2.$$

Let $I_K$ denote the group of fractional $O_K$-ideals. Observe that

$$\alpha \cdot y^{-2} \cdot A = \alpha \cdot \mathcal{A}$$

$$(2.14)$$

$$= \alpha \cdot \mathcal{A} \cdot \mathcal{A}^{h_s(K) - 1}$$

$$= \alpha \cdot \mathcal{A}^{h_s(K)} \quad \text{in } I_K/I_K^2$$

since $\alpha \cdot y^{-2} = \alpha$ in the global square-class group $K^*/K^*$. Earlier we noted

$$\mathcal{A}^{h_s(K)} = \alpha \cdot \mathcal{A}$$

as $O_K$-ideals,

where $A$ is some $O_K$-ideal containing only prime ideals in $S$. Continuing (2.14), this implies that

$$\alpha \cdot y^{-2} \cdot A = \alpha \cdot \mathcal{A}^{h_s(K)}$$

$$= \alpha^2 \cdot A \quad \text{in } I_K/I_K^2$$

or

$$\alpha \cdot y^{-2} \cdot A = \alpha^2 \cdot A \cdot Q^2 \quad \text{in } I_K$$

for some fractional $O_K$-ideal $Q$. Since

$$0 = ord_P(\alpha \cdot y^{-2} \cdot A) = ord_P(\alpha^2 \cdot A \cdot Q^2) \quad \text{for all } P \in S,$$

$$(2.15)$$
we have $\alpha^2 \cdot A \cdot Q^2 \in I(K, c_S)$ or
\[
\alpha^2 \cdot A \cdot Q^2 = \bar{\alpha} \cdot y^{-2} \cdot A
\]
in $\mathcal{C}(K, c_s)$.

Thus we have reduced the problem of showing $\bar{\phi}$ is injective to that of verifying that
\[
\alpha^2 \cdot A \cdot Q^2 \in \mathcal{C}(K, c_s)^2.
\]

Now

\[
ord_P(\alpha^2 \cdot A \cdot Q^2) \equiv ord_P(A) \pmod{2} \quad \text{for all prime ideals } P \text{ of } K.
\]

Recalling that the $O_K$-ideal $A$ contains only prime ideals in $S$, we observe that
\[
\text{(2.16)} \quad ord_P(A) \equiv 0 \pmod{2} \quad \text{for all prime ideals } P \notin S.
\]

Then we are done; equations (2.15) and (2.16) tell us precisely that $\alpha^2 \cdot A \cdot Q^2$ is the square of a class in $\mathcal{C}(K, c_S)$:
\[
\alpha^2 \cdot A \cdot Q^2 \in \mathcal{C}(K, c_s)^2.
\]

Thus we have established the injectivity of $\phi$, which concludes our proof of the Cokernel Lemma. \hfill \blacksquare
§III.1. Introduction

Our goal in this chapter is to find sufficient conditions for the existence of a small equivalence between two number fields $K$ and $L$. Here we rely heavily on the theory of local inner product spaces developed in Chapter II. We define the concept of small equivalence in terms of certain "suitable" pairs of finite sets $S \subseteq \Omega_K$, $S' \subseteq \Omega_L$. Unfortunately, not all suitable pairs $S, S'$ give a small equivalence between $K$ and $L$. The task of determining the obstruction to an arbitrary suitable pair $S, S'$ yielding a small equivalence is not difficult. That of removing the obstruction is. In fact, the Obstruction-Killing Lemma is the key to our solution of the problem. Namely, suppose that $S, S'$ is a suitable pair for $K$ and $L$ with obstruction $d_{SS'} > 0$. The Obstruction-Killing Lemma allows us to augment (in a finite number of steps) the original suitable pair $S, S'$ in such a way as to obtain a new suitable pair for $K$ and $L$ which does yield a small equivalence. The remainder of Chapter III is devoted to determining precisely when a suitable pair exists for two number fields $K$ and $L$.

§III.2. Suitable Pairs and Small Equivalence

Let $K$ and $L$ be number fields and $S_0, S'_0$ the sets of all infinite and dyadic places of $K, L$ respectively. We make the following definition:

**Definition 3.1:** The finite sets $S \subseteq \Omega_K$ and $S' \subseteq \Omega_L$ are said to form a *suitable pair* for $K$ and $L$ if:

1) $S_0 \subseteq S$, $S'_0 \subseteq S'$;
ii) the S-class number, $h^S(K)$, of $K$ and the $S'$-class number, $h^{S'}(L)$, of $L$ are odd;

iii) there exists a bijection $T : S \rightarrow S'$ such that for all $P \in S$, there exists an isometry $t_P$ between the inner product spaces $(K_P^+/K_P^+, (,)_P)$ and $(L_{TP}^+/L_{TP}^+, (,)_TP)$.

Observe that conditions i) and ii) are precisely conditions (1) and (2) of (2.4).

Given a suitable pair $S, S'$ for $K$ and $L$, by condition iii) the map

$$\tau_S = \prod_{P \in S} t_P$$

is an isometry between the inner product spaces $(G(S), (,)_S)$ and $(G(S'), (,)_{S'})$.

Moreover, we have the following diagram (note $i_S$ and $i_{S'}$ are injective by ii)):

$$U_K(S)/U_K(S)^2 \xrightarrow{i_S} G(S) \xrightarrow{\tau_S} U_L(S')/U_L(S')^2 \xrightarrow{i_{S'}} G(S').$$

Given this situation, [P-S-C] makes the following definition:

**Definition 3.2:** There is a small equivalence between $K$ and $L$ if there exists a group isomorphism

$$t_{SS'} : U_K(S)/U_K(S)^2 \rightarrow U_L(S')/U_L(S')^2$$

which makes diagram (3.1) commute. That is to say,

$$i_{S'} \circ t_{SS'}(U_K(S)/U_K(S)^2) = \tau_S \circ i_S(U_K(S)/U_K(S)^2) \quad \text{in } G(S').$$

Clearly, if such a map $t_{SS'}$ exists, we have

$$i_{S'}(U_L(S')/U_L(S')^2) = \tau_S \circ i_S(U_K(S)/U_K(S)^2) \quad \text{in } G(S').$$

On the other hand, given any suitable pair $S, S'$ for which (3.2) holds, we can define a group homomorphism $t_{SS'} : U_K(S)/U_K(S)^2 \rightarrow U_L(S')/U_L(S')^2$ which makes diagram (3.1) commute; simply put

$$t_{SS'} = i_{S'}^{-1} \circ \tau_S \circ i_S.$$
Therefore we have established:

**Lemma 3.1.** If a suitable pair $S, S'$ for $K$ and $L$ satisfies (3.2), then $S, S'$ yields a small equivalence between $K$ and $L$.

### §III.3. Removing the Obstruction

Lemma 3.1 reduces the problem of establishing a small equivalence between two number fields $K$ and $L$ to that of finding a suitable pair which satisfies (3.2). In light of this, we pose the following question:

**Question:** Let $S, S'$ be an arbitrary suitable pair for $K$ and $L$. Which elements of $U_K(S)/U_K(S)^2$ (if any) map into the image of $U_L(S')/U_L(S')^2$ under $\tau_S \circ i_S$, and vice versa?

To answer this question, we make the following definition:

**Definition 3.3:** Let $S, S'$ be a suitable pair for $K$ and $L$. We define the subsets $H_S$ and $H_{S'}$ of $U_K(S)/U_K(S)^2$ and $U_L(S')/U_L(S')^2$, respectively, by

$$H_S = \{ \alpha \in U_K(S)/U_K(S)^2 | \tau_S \circ i_S(\alpha) \in i_{S'}(U_L(S')/U_L(S')^2) \}$$

and

$$H_{S'} = \{ \beta \in U_L(S')/U_L(S')^2 | i_{S'}(\beta) \in \tau_S \circ i_S(U_K(S)/U_K(S)^2) \}.$$  

Note that $H_S$ is precisely the set of elements of $U_K(S)/U_K(S)^2$ which maps into the image of $U_L(S')/U_L(S')^2$ under the map $\tau_S \circ i_S$; similarly, $H_{S'}$ is the set of elements of $U_L(S')/U_L(S')^2$ which maps into the image of $U_K(S)/U_K(S)^2$ under $i_{S'}$.

We claim that the sets $H_S$ and $H_{S'}$ are non-empty, non-trivial subgroups of $U_K(S)/U_K(S)^2$ and $U_L(S')/U_L(S')^2$, respectively. Clearly $\tau_S \circ i_S(1) = 1$ and, by
Lemma 2.1, \( \tau_S \circ i_S(-1) = -1 \). So, both \( H_S \) and \( H_{S'} \) contain the elements 1 and -1; one easily verifies that they are subgroups.

Note that these particular groups \( H_S \) and \( H_{S'} \) measure how close the pair \( S, S' \) comes to satisfying Lemma 3.1. That is,

\[
\tau_S \circ i_S(H_S) = \tau_S \circ i_S(U_K(S)/U_K(S)^2) \bigcap i_{S'}(U_L(S')/U_L(S')^2).
\]

If \( H_S = U_K(S)/U_K(S)^2 \) (hence \( H_{S'} = U_L(S')/U_L(S')^2 \)) we are done. Thus, the obstruction to a suitable pair \( S, S' \) yielding a small equivalence is the integer

\[
d_{SS'} = \dim_F(U_K(S)/U_K(S)^2/H_S).
\]

We present the following obstruction-killing lemma.

**Lemma 3.2 (Obstruction-Killing Lemma).** Given a suitable pair \( S, S' \) for \( K \) and \( L \) with obstruction \( d_{SS'} > 0 \), there exist prime ideals \( P \in \Omega_K \setminus S \) and \( P' \in \Omega_L \setminus S' \) such that \( S_1 = S \cup \{ P \}, \ S'_1 = S' \cup \{ P' \} \) is also a suitable pair for \( K \) and \( L \) and

\[
d_{S_1S'_1} < d_{SS'}.\]

From this we immediately obtain:

**Corollary 3.3.** The existence of a suitable pair for \( K \) and \( L \) implies the existence of a small equivalence between \( K \) and \( L \).

**Proof of Corollary 3.3:** Let \( S, S' \) be a suitable pair for \( K \) and \( L \). If \( d_{SS'} = 0 \), we are done. That is, by Lemma 3.1, there is a small equivalence between \( K \) and \( L \). If \( d_{SS'} > 0 \), applying Lemma 3.2 (Obstruction-Killing Lemma) at most \( d = d_{SS'} \) times, we obtain a suitable pair \( S_d, S'_d \) with obstruction zero. Therefore \( S_d, S'_d \) yields a small equivalence between \( K \) and \( L \).

Now we prove the Obstruction-Killing Lemma:

**Proof of Lemma 3.2 (Obstruction-Killing Lemma):** The proof is divided into three parts as follows:

**Part 1** - Find the prime ideals \( P_1 \) and \( P'_1 \).

**Part 2** - Verify that \( S_1, S'_1 \) is a suitable pair for \( K \) and \( L \).

**Part 3** - Check that \( d_{S_1S'_1} < d_{SS'} \).
Part 1 - Find the prime ideals $P_1$ and $P'_1$.

The fact that

$$d_{SS'} = \text{dim}_{F_2} \left( \frac{U_K(S)}{U_K(S)^2} / H_S \right) > 0$$

assures us that $\left( \frac{U_K(S)}{U_K(S)^2} / H_S \right)$ is non-empty. Thus, fix an element $x_0$ of $\left( \frac{U_K(S)}{U_K(S)^2} / H_S \right)$. By definition of $H_S$, we have

\[(3.3) \quad \tau_S x_0 \notin i_{S'} \left( \frac{U_L(S')}{U_L(S')^2} \right) \quad \text{Lemma 2.4} \quad i_{S'} \left( \frac{U_L(S')}{U_L(S')^2} \right)^\perp.
\]

This implies that there exists an element $y_0 \in \frac{U_L(S')}{U_L(S')^2}$ for which

\[(3.4) \quad \langle \tau_S x_0, y_0 \rangle_{S'} = -1;
\]

for if

$$\langle \tau_S x_0, y \rangle_{S'} = 1 \quad \text{for all} \quad y \in i_{S'} \left( \frac{U_L(S')}{U_L(S')^2} \right),$$

then $\tau_S x_0 \in i_{S'} \left( \frac{U_L(S')}{U_L(S')^2} \right)^\perp$, contradicting (3.3). Consequently, fix an element $y_0 \in \frac{U_L(S')}{U_L(S')^2}$ satisfying (3.4). We claim

\[(3.5) \quad y_0 \notin H_{S'}.
\]

Namely, if there exists an element $z_0 \in \frac{U_K(S)}{U_K(S)^2}$ for which $\tau_S z_0 = y_0$ in $G(S')$, then

$$-1 = \langle \tau_S x_0, y_0 \rangle_{S'}$$
$$= \langle \tau_S x_0, \tau_S z_0 \rangle_{S'}$$
$$= \langle x_0, z_0 \rangle_S$$
$$= 1 \quad \text{by Lemma 2.4}
$$

which is clearly a contradiction. Hence, (3.5) holds.

Now consider the element

$$x_0 \cdot \tau_S^{-1} y_0 \in G(S).$$

By Lemma 2.5 (Cokernel Lemma), there exists an $O_K$-ideal $\mathcal{A} \in I(K, e_S)$ such that

$$\bar{\phi} : [\overline{\mathcal{A}}] \mapsto x_0 \cdot \tau_S^{-1} y_0 \quad \text{in} \quad G(S)/i_S \left( \frac{U_K(S)}{U_K(S)^2} \right).$$
Every generalized ideal class \( \overline{B} \in \mathcal{C}l(K, c_S) \) contains infinitely many integral prime ideals of \( K \). Therefore, there exists an integral prime ideal \( P_1 \in \Omega_K \setminus S \) such that \( P_1 \in [\overline{B}] \) in \( \mathcal{C}l(K, c_S)/\mathcal{C}l(K, c_S)^2 \). Thus,

\[
\overline{\phi} : [P_1] \mapsto x_0 \cdot \tau_S^{-1}y_0 \quad \text{in} \quad G(S)/i_S \left( U_K(S)/U_K(S)^2 \right).
\]

Chose an element \( \pi_1 \in O_K(S) \) which satisfies

\[
P_1^{h_S(K)} \cdot O_K(S) = \pi_1 \cdot O_K(S)
\]

(recall such an element is unique only up to an \( S \)-unit). Then by definition of \( \overline{\phi} \), we must have

\[
\pi_1 = x_0 \cdot \tau_S^{-1}y_0 \quad \text{in} \quad G(S)/i_S \left( U_K(S)/U_K(S)^2 \right)
\]
or

\[
u \pi_1 = x_0 \cdot \tau_S^{-1}y_0 \quad \text{in} \quad G(S)
\]
where \( \nu \in U_K(S)/U_K(S)^2 \). Since we can replace \( \pi_1 \) by \( \nu \pi_1 \), we may assume

\[
(3.6) \quad \pi_1 = x_0 \cdot \tau_S^{-1}y_0 \quad \text{in} \quad G(S).
\]

Similarly, there exists an integral prime ideal \( P_1' \in \Omega_K \setminus S' \) and an element \( \pi_1' \in O_L(S') \), unique up to an \( S' \)-unit, such that

1) \( (P_1')^{h_S(K)} \cdot O_L(S') = \pi_1' \cdot O_L(S') \)

and

2) \( \pi_1' = \tau_Sx_0 \cdot y_0 \quad \text{in} \quad G(S'). \)

Now \( P_1 \) a non-dyadic prime ideal of \( K \) implies that

\[
K_{P_1}^*/K_{P_1}^{*2} = \{1, u_1, \pi_1, u_1\pi_1\}
\]
where \( u_1 \) denotes the class of the non-square unit. Similarly, for \( P_1' \),

\[
L_{P_1'}^*/L_{P_1'}^{*2} = \{1, u_1', \pi_1', u_1'\pi_1'\}
\]
where \( u_1' \) denotes the class of the non-square unit.

Every element of \( H_S \) is a local unit at the prime ideal \( P_1 \) since \( P_1 \notin S \). That is, given \( z \in H_S \), either \( z = 1 \) or \( z = u_1 \) in \( K_{P_1}^*/K_{P_1}^{*2} \); likewise for \( z' \) in \( H_{S'} \). We claim that \( z \in H_S \) is a local square at \( P_1 \), or \( z = 1 \) in \( K_{P_1}^*/K_{P_1}^{*2} \) (similarly for \( z' \) in \( H_{S'} \) at \( P_1' \)). Since \( (u_1, \pi_1)_{P_1} = -1 \) and \( (1, \pi_1)_{P_1} = 1 \), it suffices to show
Lemma 3.4. For all elements $z \in H_S$, 

$$(z, \pi_1)_{P_1} = 1.$$ 

Similarly, given $z'$ in $H_{S'}$, we have $(z', \pi'_1)_{P'_1} = 1$.

Proof of Lemma 3.4: Here we give the proof for $z \in H_S$ only; the proof for $z' \in H_{S'}$ is analogous.

For all prime ideals $Q$ of $K$, $Q \notin S_1$, 

$$(z, \pi_1)_Q = 1$$ 

since both $z$ and $\pi_1$ are local units at $Q$. By Hilbert's reciprocity law, this yields 

$$(z, \pi_1)_{P_1} = \prod_{P \in S} (z, \pi_1)_P = (z, \pi_1)_S.$$ 

(Observe that while $\pi_1 \notin U_K(S)/U_K(S)^2$, any element of $K^*$ can be viewed as an element of the inner product space $(G(S), \langle , \rangle_S)$). Equation (3.6) tells us that 

$$(z, \pi_1)_S = \langle z, x_0 \cdot \tau_S^{-1} y_0 \rangle_S$$ 

$$= \langle z, x_0 \rangle_S \langle z, \tau_S^{-1} y_0 \rangle_S$$ 

$$= \langle z, x_0 \rangle_S \langle \tau_S z, y_0 \rangle_{S'}$$ 

$$= 1 \quad \text{by Lemma 2.4.}$$

Therefore we obtain 

$$(z, \pi_1)_{P_1} = (z, \pi_1)_S = 1$$

as desired. 

Part 2 - Verify that $S_1, S'_1$ is a suitable pair for $K$ and $L$.

Recalling the definition of a suitable pair, we note that the pair $S_1, S'_1$ already satisfies conditions i) and ii). It remains to show:

iii) there exists a bijection $T_1 : S_1 \to S_1'$ such that for all $P \in S_1$, there exists an isometry $t_P$ between the inner product spaces $(K^*_P/K^*_P)^2, ( , )_P)$ and $(L^{*}_{T_1 P}/L^{*}_{T_1 P}, ( , )_{T_1 P})$.

To define $T_1$, extend the given bijection $T : S \to S'$ by mapping $P_1 \mapsto P'_1$. It remains to establish the existence of an isometry $t_{P_1}$ between $(K^*_P/K^*_P)^2, ( , )_{P_1})$
and \( \left( L_{P_1}^*/L_{P_1}^{*2}, \langle , \rangle_{P_1^*} \right) \). Define the map \( t_{P_1} \) as follows:

\[
\begin{align*}
t_{P_1} : K_{P_1}/K_{P_1}^{*2} & \rightarrow L_{P_1}^*/L_{P_1}^{*2} \\
1 & \mapsto 1 \\
u_1 & \mapsto u'_1 \pi'_1 \\
\pi_1 & \mapsto \pi'_1 \\
u_1 \pi_1 & \mapsto u'_1.
\end{align*}
\]

(3.7)

If \( t_{P_1} \) is to be an isometry, it must satisfy \( t_{P_1}(-1) = -1 \). Since \( P_1 \) and \( P_1' \) are non-dyadic prime ideals, \(-1\) is a local unit at both \( P_1 \) and \( P_1' \). As \(-1 \in H_s, H_{s'}\), Lemma 3.4 implies \(-1 = 1\) in \( K_{P_1}^*/K_{P_1}^{*2} \) and \(-1 = 1\) in \( L_{P_1}^*/L_{P_1}^{*2} \). That is,

\[
-1 \in K_{P_1}^{*2} \quad \text{and} \quad -1 \in L_{P_1}^{*2}.
\]

(3.8)

Thus we have \( t_{P_1}(-1) = t_{P_1}(1) = 1 = -1 \), as desired.

Note that (3.8), along with the fact that \( P_1 \) and \( P_1' \) are non-dyadic prime ideals, guarantees the existence of an isometry between \( K_{P_1}^*/K_{P_1}^{*2} \) and \( L_{P_1}^*/L_{P_1}^{*2} \) by Lemma 2.2 (Kaplansky's Lemma). However, for our purposes, we need a specific isometry (namely, the one defined in (3.7)).

One easily checks that \( t_{P_1} \) is an isomorphism. To verify that it preserves the inner product, we must show

\[
(a, b)_{P_1} = (t_{P_1} a, t_{P_1} b)_{P_1'} \quad \text{for all} \; a, b \in K_{P_1}^*/K_{P_1}^{*2}.
\]

Observe \( t_{P_1}(1) = 1 \) implies that all symbols involving \( 1 \) match up. Moreover, we recognize that

\[
(a, a)_{P_1} = (a, -1)_{P_1} = (a, 1)_{P_1} \quad \text{by (3.8)}
\]

\[
= 1
\]

and similarly, \( (c, c)_{P_1'} = 1 \) for all \( c \in L_{P_1}^*/L_{P_1}^{*2} \). Consequently, we must check only those symbols for which \( a \) and \( b \) are distinct elements of \( K_{P_1}^*/K_{P_1}^{*2} \), not equal to 1.
In particular, we must verify that

\[(u_1, \pi_1)_{P_1} = (u'_1 \pi'_1, \pi'_1)_{P'_1}\]

(3.9)

\[(u_1, u_1 \pi_1)_{P_1} = (u'_1 \pi'_1, u'_1)_{P'_1}\]

\[(\pi_1, u_1 \pi_1)_{P_1} = (\pi'_1, u'_1)_{P'_1}\].

We make the following simplification:

\[(u_1, u_1 \pi_1)_{P_1} = (u_1, u_1)_{P_1} \cdot (u_1, \pi_1)_{P_1} = 1 \cdot (u_1, \pi_1)_{P_1} = (u_1, \pi_1)_{P_1}\].

Likewise we obtain

\[(\pi_1, u_1 \pi_1)_{P_1} = (u_1, \pi_1)_{P_1}\]

\[(u'_1 \pi'_1, \pi'_1)_{P'_1} = (u'_1, \pi'_1)_{P'_1}\]

\[(u'_1 \pi'_1, u'_1)_{P'_1} = (u'_1, \pi'_1)_{P'_1}\].

Therefore (3.9) reduces to the single equation

\[(u_1, \pi_1)_{P_1} = (u'_1, \pi'_1)_{P'_1}\].

Then we are done, for

\[(u_1, \pi_1)_{P_1} = -1 = (u'_1, \pi'_1)_{P'_1}\].

Hence, \(t_{P_1}\) is an isometry and \(S_1, S'_1\) is a suitable pair for \(K\) and \(L\).

**Part 3** - Check that \(d_{S_1 S'_1} < d_{SS'}\).

Recalling Lemma 2.3 (Dimension Lemma), we see that

\[\dim_{F_2} (U_K(S_1)/U_K(S_1)^2) = (\#S_1) = (\#S) + 1 = \dim_{F_2} (U_K(S)/U_K(S)^2) + 1.\]

We make the following claim:

**CLAIM:**

(3.10) \[\dim_{F_2} H_{S_1} \geq \dim_{F_2} H_S + 2.\]
Note that Part 3 follows from (3.10). That is,
\[
d_{S,S'} = \dim_{F_2} \left( \frac{U_K(S_1)}{U_K(S_1)^2} \right) - \dim_{F_2} H_{S_1}
\]
\[
\leq \dim_{F_2} \left( \frac{U_K(S)}{U_K(S)^2} + 1 \right) - (\dim_{F_2} H_S + 2)
\]
\[
\leq \dim_{F_2} \left( \frac{U_K(S)}{U_K(S)^2} - \dim_{F_2} H_S \right) - 1
\]
\[
\leq d_{SS'} - 1 < d_{SS'}.
\]

Therefore, it remains to prove (3.10).

We contend that it suffices to show

\[(3.11) \quad H_{S,x_0,\pi_1} \subseteq H_{S_1}.
\]

Namely, given any $F_2$-basis $e_1, e_2, \ldots, e_l$ for $H_S$, the elements $e_1, e_2, \ldots, e_l$ are linearly independent over $F_2$. Since $x_0 \notin H_S$, we observe that $e_1, e_2, \ldots, e_l, x_0$ must also be linearly independent over $F_2$. Likewise, $\pi_1 \notin \frac{U_K(S)}{U_K(S)^2}$ and $e_1, e_2, \ldots, e_l, x_0 \in \frac{U_K(S)}{U_K(S)^2}$ imply that the elements $e_1, e_2, \ldots, e_l, x_0, \pi_1$ are linearly independent over $F_2$, as well. Assuming (3.11) holds, we then have a subspace of $H_{S_1}$ of dimension
\[
\dim_{F_2} H_S + 2.
\]

Subsequently, we must have
\[
\dim_{F_2} H_{S_1} \geq \dim_{F_2} H_S + 2,
\]
as claimed.

To establish (3.11), consider the diagram, analogous to (3.1), obtained upon replacing the suitable pair $S, S'$ with the suitable pair $S_1, S'_1$:

\[
\begin{array}{ccc}
U_K(S_1)/U_K(S_1)^2 & \xrightarrow{i_{S_1}} & G(S_1) = G(S) \times K_{P_1}^*/K_{P_1}^{*2} \\
\downarrow r_s \times t_{P_1} & & \\
U_L(S'_1)/U_L(S'_1)^2 & \xrightarrow{i_{S'_1}} & G(S'_1) = G(S') \times L_{P_1'}^*/L_{P_1'}^{*2}.
\end{array}
\]

(3.12)

We make the following observations:

(i) $U_K(S_1)/U_K(S_1)^2 = U_K(S)/U_K(S)^2 \cup \pi_1 \cdot U_K(S)/U_K(S)^2$,

(ii) $U_L(S'_1)/U_L(S'_1)^2 = U_L(S')/U_L(S')^2 \cup \pi'_1 \cdot U_L(S')/U_L(S')^2$. 


where \( \cup \) denotes disjoint union, and

\[(iii) \quad \tau_{S_1} = \tau_S \times t_{P_1}.\]

Clearly (i) implies \( H_S, x_0, \pi_1 \subseteq U_K(S_1)/U_K(S_1)^2. \) Similarly, from (ii) we obtain \( H_{S'}, y_0, \pi'_1 \subseteq U_L(S'_1)/U_L(S'_1)^2. \) To verify (3.11), we must show \( H_S, x_0 \) and \( \pi_1 \) map into the subspace \( i_{S_1}' \left( U_L(S'_1)/U_L(S'_1)^2 \right) \) of \( G(S'_1) \) under the map \( \tau_{S_1} \circ i_{S_1}. \)

First of all consider the set \( H_S. \) Let \( z \in H_S; \) then

\[
z \in U_K(S_1)/U_K(S_1)^2 \xrightarrow{i_{S_1}} z = (z, \ldots, z, 1) \text{ in } G(S_1),
\]

where the last coordinate of \( z \) corresponds to the image of \( z \) in \( K_{P_1}^* \) (as in diagram (3.12)). By definition of \( H_S, \) \( \tau_S(z) = z' \) in \( G(S') \) for some \( z' \in H_{S'}. \) By Lemma 3.4, \( z = 1 \) in \( K_{P_1}^*/K_{P_1}^{*2} \) and \( z' = 1 \) in \( L_{P_1}^*/L_{P_1}^{*2}. \) Thus we obtain:

\[
z \in U_K(S_1)/U_K(S_1)^2 \xrightarrow{i_{S_1}} z = (z, \ldots, z, 1) \text{ in } G(S_1) \\
\downarrow_{\tau_S \times t_{P_1}} \\
z' \in U_L(S'_1)/U_L(S'_1)^2 \xrightarrow{i_{S'_1}} z' = (z', \ldots, z', 1) \text{ in } G(S'_1).
\]

In particular, \( \tau_S \circ i_{S_1}(z) = i_{S'_1}(z') \) or \( z \in H_{S_1}. \) As \( z \) was arbitrary, we have shown \( H_S \subseteq H_{S_1}. \)

Next we focus on the element \( x_0: \)

\[
x_0 \in U_K(S_1)/U_K(S_1)^2 \xrightarrow{i_{S_1}} x_0 = (x_0, \ldots, x_0, 1) \text{ in } G(S_1).
\]

As above, we must determine the image of \( x_0 \) in \( K_{P_1}^*/K_{P_1}^{*2}. \) Since \( x_0 \) is an \( S \)-unit and \( P_1 \notin S, \) the element \( x_0 \) must be a unit at the prime ideal \( P_1; \) that is, \( x_0 = 1 \) or \( x_0 = u_1 \) in \( K_{P_1}^*/K_{P_1}^{*2}. \) To ascertain which, it suffices to evaluate the symbol \( (x_0, \pi_1)_{P_1}. \)

As both \( x_0 \) and \( \pi_1 \) are units at all prime ideals \( Q \notin S_1, \) the symbol \( (x_0, \pi_1)_Q = 1 \)
for such $Q$. Hilbert's reciprocity law then yields

$$\prod_{Q \in S} (x_0, \pi_1)_Q = (x_0, \pi_1)_S$$

$$= (x_0, x_0 \cdot \tau_S^{-1} y_0)_S \quad \text{by (3.6)}$$

$$= (x_0, x_0)_S (x_0, \tau_S^{-1} y_0)_S$$

$$= 1 \cdot (x_0, \tau_S^{-1} y_0)_S \quad \text{by Lemma 2.4}$$

$$= (\tau_S x_0, y_0)_S'$$

$$= -1 \quad \text{by (3.4)}.$$

Therefore $x_0 = u_1$ in $K_{P_1}^*/K_{P_1}^{*2}$. An analogous proof shows $(y_0, \pi_1')_{P_1} = -1$, or $y_0 = u_1'$ in $K_{P_1}^*/K_{P_1}^{*2}$. Also, note that (3.6) implies:

$$\pi_1 = x_0 \cdot \tau^{-1} y_0 \quad \text{in} \quad G(S)$$

$$(3.13)$$

$$\downarrow_{\tau_S}$$

$$\tau_S x_0 \cdot y_0 = \pi_1' \quad \text{in} \quad G(S')$$.

Combining these observations we obtain

$$x_0 \in U_K(S_1)/U_K(S_1)^2 \xrightarrow{i_{S_1}} x_0 = (x_0, \ldots, x_0, u_1) \quad \text{in} \quad G(S_1)$$

$$\downarrow_{\tau_S \times i_{P_1}}$$

$$y_0 \pi_1' \in U_L(S_1')/U_L(S_1')^2 \xrightarrow{i_{S_1'}} y_0 \pi_1' = (y_0 \pi_1', \ldots, y_0 \pi_1', u_1' \pi_1') \quad \text{in} \quad G(S_1').$$

That is to say, $\tau_{S_1} \circ i_{S_1}(x_0) = i_{S_1'}(y_0 \pi_1')$, hence $x_0 \in H_{S_1}$.

Lastly, we examine the element $\pi_1$. From (3.13) we get:

$$\pi_1 \in U_K(S_1)/U_K(S_1)^2 \xrightarrow{i_{S_1}} \pi_1 = (\pi_1, \ldots, \pi_1, \pi_1) \quad \text{in} \quad G(S_1)$$

$$\downarrow_{\tau_S \times i_{P_1}}$$

$$\pi_1' \in U_L(S_1')/U_L(S_1')^2 \xrightarrow{i_{S_1'}} \pi_1' = (\pi_1', \ldots, \pi_1', \pi_1') \quad \text{in} \quad G(S_1').$$

Thus $\tau_{S_1} \circ i_{S_1}(\pi_1) = i_{S_1'}(\pi_1')$ or $\pi_1 \in H_{S_1}$. This establishes (3.11), hence Part 3, concluding the proof of the Obstruction-Killing Lemma.
§III.4. The Existence of a Suitable Pair

We have shown that the existence of a suitable pair for $K$ and $L$ guarantees the existence of a small equivalence between them. Therefore, we would like to determine precisely when a suitable pair exists for two number fields $K$ and $L$.

Suppose $K$ and $L$ have a suitable pair $S, S'$. Then there is an associated bijection $T : S \rightarrow S'$ and, for each $P \in S$, an isometry $t_P$ between the inner product spaces $(K_P^*/K_P^{*2}, (,)_P)$ and $(L_{T_P}^*/L_{T_P}^{*2}, (,)_T)$. Moreover, $S, S'$ must contain the sets $S_0, S'_0$ of all infinite and dyadic places, respectively. By [P-S-C, Lemma 1], the given bijection $T : S \rightarrow S'$ induces a bijection between the sets $S_0$ and $S'_0$. Therefore if any suitable pair exists for $K$ and $L$,

b) there exists a bijection $T_0 : S_0 \rightarrow S'_0$ such that for every $P \in S_0$, there exists an isometry $t_P$ between the inner product spaces $(K_P^*/K_P^{*2}, (,)_P)$ and $(L_{T_0,P}^*/L_{T_0,P}^{*2}, (,)_T)$. 

(We emphasize that condition b) by itself is actually a statement about the fields themselves and not a statement about a specific suitable pair.)

We claim that condition b), along with

a) $-1 \in K^{*2} \iff -1 \in L^{*2}$,

suffices to guarantee the existence of a suitable pair for $K$ and $L$.

**Lemma 3.5.** Given number fields $K$ and $L$ which satisfy

a) $-1 \in K^{*2} \iff -1 \in L^{*2}$;

b) there exists a bijection $T_0 : S_0 \rightarrow S'_0$ such that for every $P \in S_0$, there exists an isometry $t_P$ between the inner product spaces $(K_P^*/K_P^{*2}, (,)_P)$ and $(L_{T_0,P}^*/L_{T_0,P}^{*2}, (,)_T)$;

then there exists a suitable pair for $K$ and $L$.

**Proof of Lemma 3.5:** Starting with the sets $S_0$ and $S'_0$, we build finite sets $S$ and $S'$ to satisfy the conditions i), ii) and iii) of Definition 3.1. First, we make the following observations.
Observations: Let $S$ be a finite set of places of a number field $K$ which contains all infinite and dyadic places of $K$. Recall that

\[(3.14) \quad h^S(K) \mid h(K),\]

that is, the $S$-class number of $K$ divides the ideal class number of $K$. Now suppose $S$ contains a representative from each of the ideal classes which generate the $2$-primary subgroup of the ideal class group of $K$. Then (3.14) implies

\[h^S(K) \equiv 1 \pmod{2}.\]

Moreover, given a set $S$ with $h^S(K)$ odd, adding additional prime ideals (to obtain another set, say $S_*$) will not change the parity of the resulting $S_*$-class number since

\[S \subseteq S_* \iff h^{S_*}(K) \mid h^S(K).\]

To construct $S$ and $S'$, start with the set $S_0$ and add enough (non-dyadic) prime ideals $P$ of $K$ to obtain a set $S_*$ with odd $S_*$-class number. Then we claim:

**CLAIM 1:** For each prime ideal $P$ added to $S_0$, we can add a (non-dyadic) prime ideal $P'$ of $L$ to $S_*$ (to obtain a new set $S'_*$) subject to the restriction:

\[(3.15) \quad -1 \in K^{*2} \iff -1 \in L^{*2}.\]

Fix a prime ideal $P \in S_* \setminus S_0$. The claim follows from condition a):

\[-1 \in K^{*2} \iff -1 \in L^{*2}.\]

If $-1$ is a global square in both $K$ and $L$, then it is a local square at every place of $K$ and at every place of $L$. In particular,

\[-1 \in K^{*2} \iff -1 \in L^{*2}.\]

In this case, (3.14) imposes no additional conditions on the prime ideal $P'$ other than $P' \notin S'_0$ (that is, $P'$ must be a non-dyadic prime ideal). On the other hand, if $-1$ is not a global square in either field, then the extensions

\[K(\sqrt{-1})/K \quad \text{and} \quad L(\sqrt{-1})/L\]
are quadratic. Recall

\[-1 \in K_p^* \iff P \text{ splits in } K(\sqrt{-1});\]

likewise for \(P'\) and \(L\). Thus, (3.15) is equivalent to the statement

\[(3.16) \quad P \text{ splits in } K(\sqrt{-1}) \iff P' \text{ splits in } L(\sqrt{-1}).\]

There are infinitely many (non-dyadic) prime ideals \(P'\) of \(L\) which split in \(L(\sqrt{-1})\) and infinitely many (non-dyadic) prime ideals \(P'\) of \(L\) which do not split in \(L(\sqrt{-1})\). So, we can always choose \(P'\) in such a way as to satisfy (3.16), or equivalently, (3.15); thus, CLAIM 1 holds.

If the \(S'_{\text{c}}\)-class number is odd, put \(S = S_{\ast}\) and \(S' = S'_{\ast}\). If not, we can add enough (non-dyadic) prime ideals \(Q'\) of \(L\) to the set \(S'_{\ast}\) to obtain a set \(S'\) with odd \(S'_{\text{c}}\)-class number. As before, for each prime ideal \(Q'\) added to \(S'_{\ast}\), we can add a (non-dyadic) prime ideal \(Q\) to \(S_{\ast}\) (to obtain a set \(S\)) subject to the restriction:

\[-1 \in K_p^* \iff -1 \in L_{Q'}^* .\]

Thus, we have our sets \(S\) and \(S'\). We now claim:

CLAIM 2: \(S, S'\) is a suitable pair for \(K\) and \(L\).

Recall the definition of a suitable pair. The sets \(S\) and \(S'\) satisfy conditions i) and ii) by construction. Thus it remains to show

iii) there exists a bijection \(T : S \rightarrow S'\) such that for all \(\varphi \in S\), there exists an isometry \(t_\varphi\) between the inner product spaces \((K_p^*/K_p^{*2}, (,)_p)\) and \((L_T^*/L_{T_p}^{*2}, (,)_T^p)\).

To define the bijection, we extend the given bijection \(T_0 : S_0 \rightarrow S'_0\) by mapping \(P \mapsto P'\) and \(Q \mapsto Q'\) for each added prime ideal \(P\) and \(Q\) of \(S\). Now fix \(\varphi \in S\). If \(\varphi \in S_0\), condition b) guarantees the existence of the desired isometry. If \(\varphi \in S \setminus S_0\), then \(\varphi\) and \(T\varphi\) are non-dyadic prime ideals (that is, one of the added pairs \(P, P'\) or \(Q, Q'\)). Therefore, the corresponding inner product spaces have the same dimension over \(F_2\). Moreover, \(\varphi\) and \(T\varphi\) were chosen subject to the condition

\[-1 \in K_p^* \iff -1 \in L_{T_p}^*.\]
By Lemma 2.2 (Kaplansky's Lemma), the inner product spaces \( (K^*_P/K^*_P^2, (\cdot)_P) \) and \( (L^*_P/L^*_P^2, (\cdot)_P) \) are isometric. Hence, condition iii) is satisfied, proving that \( S, S' \) is a suitable pair for \( K \) and \( L \), as desired. 

Lemma 3.5 and Corollary 3.3 together answer the question we posed at the beginning of Section 3. Namely, when does there exist a small equivalence exist between two number fields?

**Proposition 3.6.** Given two number fields \( K \) and \( L \) which satisfy the following conditions:

a) \(-1 \in K^{*2} \iff -1 \in L^{*2}\);

b) there exists a bijection \( T_0 : S_0 \to S'_0 \) such that for every \( P \in S_0 \), there exists an isometry \( t_P \) between the inner product spaces \( (K^*_P/K^*_P^2, (\cdot)_P) \) and \( (L^*_P/L^*_P^2, (\cdot)_P) \);

then there is a small equivalence between \( K \) and \( L \).
§IV.1. Introduction

Our goal in this chapter is to extend Proposition 3.6 to determine when two number fields are reciprocity equivalent. Namely, using results from [P-S-C] and an equivalent formulation of the conditions a) and b), we show:

**Theorem 4.1.** Let \( K \) and \( L \) be number fields. The following are equivalent:

I) \( K \) and \( L \) are reciprocity equivalent.

II) These conditions hold:

A) \( r_1(K) = r_1(L) \)

B) \(-1 \in K^{*2} \iff -1 \in L^{*2}\)

C) there exists a bijection

\[
\begin{align*}
\{ \text{Dyadic Prime Ideals of } K \} & \leftrightarrow \{ \text{Dyadic Prime Ideals of } L \} \\
\{ \text{Prime Ideals of } K \} & \leftrightarrow \{ \text{Prime Ideals of } L \}
\end{align*}
\]

such that if \( P \leftrightarrow Q \), then

\( [K_P : Q_2] = [L_Q : Q_2] \)

and \(-1 \in K_P^{*2} \iff -1 \in L_Q^{*2}\).

III) There exists a small equivalence between \( K \) and \( L \).

The main theorem of [P-S-C] is the statement that global fields \( K \) and \( L \) of characteristic not 2 are reciprocity equivalent if and only if they are Witt equivalent. Using this, we restate Theorem 4.1 as follows:

**Theorem 4.4.** Let \( K \) and \( L \) be number fields.
\[ W(K) \cong W(L) \iff \begin{align*}
\text{A) } & \ r_1(K) = r_1(L) \\
\text{B) } & \ -1 \in K^\times \iff -1 \in L^\times \\
\text{C) } & \text{there exists a bijection} \\
\left\{ \begin{array}{c}
\text{Dyadic} \\
\text{Prime} \\
\text{Ideals}
\end{array} \right\}_K & \leftrightarrow \\
\left\{ \begin{array}{c}
\text{Dyadic} \\
\text{Prime} \\
\text{Ideals}
\end{array} \right\}_L
\end{align*} \]

such that if \( P \leftrightarrow Q \), then
\[ [K_P : Q_2] = [L_Q : Q_2] \]
and \(-1 \in K_P^\times \iff -1 \in L_Q^\times\).

Each of these theorems yields more general results about Witt and reciprocity equivalent number fields. Among them are two finiteness statements for forms over number fields.

Section 2 is devoted to the proof of Theorem 4.1 and the corollaries which follow. The first corollary concerns reciprocity equivalences between certain quadratic extensions of \( K \) and \( L \); the second is the first finiteness statement. It deals with tame and wild (finite) places of a reciprocity equivalence. [P-S-C] shows that a reciprocity equivalence canonically induces isomorphisms between the local square-class groups. If such a local map sends the equivalence class of a local prime element to the equivalence class of a local unit, then the reciprocity equivalence is wild at the (finite) place corresponding to the given localization; otherwise, it is tame at that (finite) place. The wild set of a reciprocity equivalence consists of all (finite) places at which the equivalence is wild. [P-S-C, Theorem 1] states that every small equivalence of \( K \) and \( L \) can be extended to a reciprocity equivalence which is wild at only finitely many places of \( K \). Combining this with Theorem 4.1 yields the second corollary: a reciprocity equivalence (infinite wild set or not) can always be replaced by another equivalence which is wild at no more than finitely many places. There is a relationship between the number of places in the wild set of a reciprocity equivalence and the ideal class numbers of the two equivalent fields; namely, when the wild set is empty, the class numbers of the equivalent fields have the same parity. In light of this, one might want the number of such places to be as small as possible.

The results on Witt equivalence of number fields, Theorem 4.4 and its corollaries,
are located in Section 3. The first of these is the second finiteness statement: for fixed \( n \in \mathbb{N} \), the number of Witt equivalence classes of number fields of degree \( n \) is finite. We prove this by producing an upper bound on the number of classes of fields of degree \( n \), using the conditions A), B), and C). To illustrate the power of these conditions, we use them to show that there are exactly seven Witt equivalence classes of quadratic number fields, represented by \( \mathbb{Q}(\sqrt{-1}) \), \( \mathbb{Q}(\sqrt{2}) \), \( \mathbb{Q}(\sqrt{-2}) \), \( \mathbb{Q}(\sqrt{7}) \), \( \mathbb{Q}(\sqrt{-7}) \), and \( \mathbb{Q}(\sqrt{-17}) \) (they had been previously classified up to tame equivalence by A. Czogala in [Cz]). A brief algorithm (which arises from the proof) for determining the class of an arbitrary quadratic number field is also included. The last corollary relates Witt equivalence of number (global) fields to that of the corresponding \( p \)-adic (local) fields. Perlis, Szymiczek, and Conner note that the existence of a reciprocity equivalence \((t,T)\) between \( K \) and \( L \) implies that \( W(K_p) \cong W(L_{tp}) \) for all places \( p \) of \( K \). Given a bijection \( T: \Omega_K \rightarrow \Omega_L \) for which \( W(K_p) \) and \( W(L_{tp}) \) are isomorphic as additive groups for all \( p \in \Omega_K \), we conclude that \( W(K) \) and \( W(L) \) are isomorphic as rings.

§IV.2. Consequences of Reciprocity Equivalence

Let \( K \) and \( L \) be number fields which satisfy Proposition 3.6; then there exists a small equivalence between them. By [P-S-C, Theorem 1] a small equivalence always can be extended to a reciprocity equivalence. This, together with [P-S-C, Lemma 1], gives us:

**Theorem 4.1.** Let \( K \) and \( L \) be number fields. The following are equivalent.

I) \( K \) and \( L \) are reciprocity equivalent.

II) These conditions hold:

A) \( r_1(K) = r_1(L) \)

B) \(-1 \in K^* \iff -1 \in L^* \)

C) there exists a bijection
such that if $P \leftrightarrow Q$, then

$$[K_P : Q_2] = [L_Q : Q_2]$$

and $-1 \in K_P^* \iff -1 \in L_Q^*.$

III) There exists a small equivalence between $K$ and $L$.

Proof of Theorem 4.1: III) $\Rightarrow$ I) is [P-S-C, Theorem 1]. One easily checks I) $\Rightarrow$ II) using the definition of reciprocity equivalence (a proof can also be found in [P-S-C, Lemma 1]).

To establish II) $\Rightarrow$ III), it suffices to show that conditions A), B), and C) imply conditions a) and b) of Proposition 3.6 (we remark that A), B), and C) are, in fact, equivalent to a) and b); however, to prove the theorem we need to show only one implication). Condition a) is simply a restatement of condition B). To obtain the bijection $T_0 : S_0 \rightarrow S'_0$ in condition b), extend the given bijection between the dyadic prime ideals of $K$ and $L$ by mapping the real infinite primes of $K$ to the real infinite primes of $L$ and the complex infinite primes of $K$ to the complex infinite primes of $L$. We can do this since condition A) implies that $K$ and $L$ have the same number of real infinite primes. That is, by condition C), we obtain

$$[K : Q] = \sum_{P \text{ dyadic}} [K_P : Q_2] = \sum_{Q \text{ dyadic}} [L_Q : Q_2] = [L : Q].$$

Since $r_1(K) + 2 \cdot r_2(K) = [K : Q] = [L : Q] = r_1(L) + 2 \cdot r_2(L)$, $K$ and $L$ must also have the same number of complex infinite primes: $r_2(K) = r_2(L)$.

By way of condition C), we have

$$(K_P^* / K_P^{*2}, ( , )_P) \cong (L_{T_0 P}^* / L_{T_0 P}^{*2}, ( , )_{T_0 P})$$

for all dyadic prime ideals $P$ of $K$. Thus, it remains to check this condition for the non-dyadic places $P \in S_0$. Now if $P \in S_0$ is a non-dyadic place, both $P$ and $T_0 P$ must be either real infinite primes or complex infinite primes. In either case, the corresponding inner product spaces have the same dimension over $F_2$. Moreover, $P$
and $T_0 P$ real infinite primes means that -1 is not a local square in the corresponding $F_2$-inner product spaces; if $P$, $T_0 P$ are complex infinite primes, -1 is a local square in both spaces. Hence Lemma 2.2 (Kaplansky's Lemma) guarantees that the desired isometry exists. Therefore condition b) is satisfied, so by Proposition 3.6, there is a small equivalence between $K$ and $L$. 

Given reciprocity equivalent number fields $K$ and $L$, what, if anything, can be said about extensions of $K$ and $L$? For the simplest such extensions, quadratic extensions if $K$ and $L$, we have the following result:

**Corollary 4.2.** Let $K$ and $L$ be number fields. If $(t, T)$ is a reciprocity equivalence between $K$ and $L$, then for any $a \in K^*/K^{*2}$

$$K\left(\sqrt{a}\right) \text{ and } L\left(\sqrt{ta}\right)$$

are reciprocity equivalent.

**Proof of Corollary 4.2:** Fix $a \in K^*/K^{*2}$. By Theorem 4.1, it suffices to show $K(\sqrt{a})$ and $L(\sqrt{ta})$ satisfy conditions A), B), and C). We observe that $a \in K^{*2}$ if and only if $ta \in L^{*2}$. In particular, $a \in K^{*2}$ implies

$$K(\sqrt{a}) = K \quad \text{and} \quad L(\sqrt{ta}) = L$$

in which case, we are done. Thus we may assume $a \notin K^{*2}$ (and $ta \notin L^{*2}$).

We observe that $a$ is positive in the real embedding of $K$ (which corresponds to the real infinite prime $\wp$ of $K$) if and only if

$$(a, -1)_{\wp} = 1 \iff (ta, -1)_{T_{\wp}} = 1$$

if and only if $ta$ is positive in the real embedding of $L$ (which corresponds to the real infinite prime $T_{\wp}$ of $L$). In particular, the number of real embeddings of $K$ in which $a$ is positive is equal to the number of real embeddings of $L$ in which $ta$ is positive. Thus, since

$$r_1(K(\sqrt{a})) = 2 \left( \# \text{ real embeddings of } K \text{ in which } a \text{ is positive} \right)$$

and

$$r_1(L(\sqrt{ta})) = 2 \left( \# \text{ real embeddings of } L \text{ in which } ta \text{ is positive} \right),$$

we obtain $r_1(K(\sqrt{a})) = r_1(L(\sqrt{ta}))$, or condition A) holds.
Now we check that $K(\sqrt{a})$ and $L(\sqrt{ta})$ satisfy condition B):

$$-1 \in K(\sqrt{a})^{*2} \iff -1 \in K^{*2} \text{ or } a = -1 \text{ in } K^*/K^{*2}$$

$$\iff -1 \in L^{*2} \text{ or } ta = -1 \text{ in } L^*/L^{*2}$$

$$\iff -1 \in L(\sqrt{ta})^{*2}.$$

It remains to verify condition C). Fix an arbitrary dyadic prime ideal $\varphi$ of $K$. It suffices to show:

**CLAIM:** There exists a bijection

$$\begin{align*}
\{ \text{Dyadic Prime} & \}\text{ Ideals of } K(\sqrt{a}) \text{ lying over } \varphi \\
& \leftrightarrow \\
\{ \text{Dyadic Prime} & \}\text{ Ideals of } L(\sqrt{ta}) \text{ lying over } T\varphi
\end{align*}$$

such that if $P \leftrightarrow Q$, then

$$[K_P(\sqrt{a}) : K_\varphi] = [L_Q(\sqrt{ta}) : L_{T\varphi}]$$

and

$$-1 \in K_P(\sqrt{a})^{*2} \iff -1 \in L_Q(\sqrt{ta})^{*2}.$$

That is, each dyadic prime ideal $P$ of $K(\sqrt{a})$ lies over precisely one dyadic prime ideal of $K$ and likewise for $L(\sqrt{ta})$. Moreover, for each dyadic prime ideal $\varphi$ of $K$, we have $[K_\varphi : \mathcal{Q}_2] = [L_{T\varphi} : \mathcal{Q}_2]$. Thus, if the claim holds we have

$$[K_P(\sqrt{a}) : \mathcal{Q}_2] = [K_P(\sqrt{a}) : K_\varphi] [K_\varphi : \mathcal{Q}_2]$$

$$= [L_Q(\sqrt{ta}) : L_{T\varphi}] [L_{T\varphi} : \mathcal{Q}_2]$$

$$= [L_Q(\sqrt{ta}) : \mathcal{Q}_2].$$

To prove the claim, we begin by noting that

$\varphi$ splits in $K(\sqrt{a})$ $\iff a \in K_\varphi^{*2}$

$$\iff (a, b)_{\varphi} = 1 \text{ for all } b \in K_\varphi^*/K_\varphi^{*2}$$

$$\iff (ta, c)_{T\varphi} = 1 \text{ for all } c \in L_{T\varphi}^*/L_{T\varphi}^{*2}$$

$$\iff ta \in L_{T\varphi}^{*2}$$

$$\iff T\varphi \text{ splits in } L(\sqrt{ta}).$$
Hence $K(\sqrt{a})$ and $L(\sqrt{ta})$ have precisely the same number of dyadic prime ideals lying over $\wp$ and $T\wp$, respectively. That is, we can always define a bijection as desired.

Fix such a bijection. Suppose $\wp$ (hence $T\wp$) splits. Then if $P \leftrightarrow Q$, we must have

$$[K_P(\sqrt{a}) : K_p] = 1 = [L_Q(\sqrt{ta}) : L_{T\wp}],$$

or

$$-1 \in K_P(\sqrt{a})^{*2} \iff -1 \in K_p^{*2}$$

$$\iff -1 \in L_{T\wp}^{*2}$$

$$\iff -1 \in L_Q(\sqrt{ta})^{*2}.$$

On the other hand, if $\wp, T\wp$ are non-split prime ideals, then $P \leftrightarrow Q$ yields

$$[K_P(\sqrt{a}) : K_p] = 2 = [L_Q(\sqrt{ta}) : L_{T\wp}]$$

and

$$-1 \in K_P(\sqrt{a})^{*2} \iff -1 \in K_p^{*2} \text{ or } a = -1 \text{ in } K_p^{*}/K_p^{*2}$$

$$\iff -1 \in L_{T\wp}^{*2} \text{ or } ta = -1 \text{ in } L_{T\wp}^{*}/L_{T\wp}^{*2}$$

$$\iff -1 \in L_Q(\sqrt{ta})^{*2}.$$

Therefore, the claim holds and, by Theorem 4.1, $K(\sqrt{a})$ and $L(\sqrt{ta})$ are reciprocity equivalent. 

Given a reciprocity equivalence $(t, T)$ between the number fields $K$ and $L$, Perlis, Szymiczek, and Conner make the following definitions:

**Definition 4.1**: The reciprocity equivalence $(t, T)$ is said to be **tame** at the (finite) place $P$ of $\Omega_K$ if

$$ord_P(a) \equiv ord_T(ta) \pmod{2}$$

for all square classes $a \in K^{*}/K^{*2}$, and **wild** otherwise. The set of all (finite) places $P$ at which the equivalence is wild is call the **wild set** of $(t, T)$.

(Do not confuse this with tame and wild ramification of prime ideals in number fields.) Furthermore,
Definition 4.2: The reciprocity equivalence \((t, T)\) is called a tame equivalence if \((t, T)\) is tame at every (finite) place \(P\) of \(\Omega_K\), and a wild equivalence otherwise.

There is a relationship between tame equivalence and the ideal class numbers of \(K\) and \(L\). If \(K\) and \(L\) are tamely equivalent, then

\[ h(K) \equiv h(L) \pmod{2} \]

(see [P-S-C, Section 3] for a proof).

Certainly not every reciprocity equivalence is tame. However, if there is a small equivalence between \(K\) and \(L\), [P-S-C] shows that it can be tamely extended to a reciprocity equivalence \((t, T)\) between \(K\) and \(L\). That is to say, \((t, T)\) is tame at all places not involved in the small equivalence. Thus we can extend the small equivalence to obtain a reciprocity equivalence which has a finite wild set. Combining this fact with Theorem 4.1, we have:

Corollary 4.3. Given reciprocity equivalent number fields \(K\) and \(L\), there exists (perhaps another) reciprocity equivalence between them which is wild at only finitely many places of \(K\).

Proof of Corollary 4.3: By Theorem 4.1, \(K\) and \(L\) reciprocity equivalent implies the existence of a small equivalence between them. [P-S-C, Theorem 1] guarantees that we can tamely extend this small equivalence to (perhaps another) reciprocity equivalence of \(K\) and \(L\). Therefore, the second reciprocity equivalence could be wild only at those (finite) places which appeared in the original small equivalence. Hence, the latter reciprocity equivalence is wild at only finitely many places of \(K\).

In particular, if reciprocity equivalences with infinite wild sets really do exist, we can replace them by those which are wild at only finitely many places. Thus, if one so chooses, one can avoid equivalences with infinite wild sets, although such may have interesting properties of their own.
§IV.3. Witt Equivalence of Number Fields

The main theorem of [P-S-C] is the statement that global fields $K$ and $L$ of characteristic not 2 are reciprocity equivalent if and only if they are Witt equivalent. Using this, we restate Theorem 4.1 as follows:

**THEOREM 4.4.** Let $K$ and $L$ be number fields.

$W(K) \cong W(L) \iff$

A) $r_1(K) = r_1(L)$

B) $-1 \in K^* \iff -1 \in L^*$

C) there exists a bijection

\[
\begin{align*}
\{ \text{Dyadic} \\ \text{Prime} \\ \text{Ideals} \\ \text{of } K \} & \leftrightarrow \{ \text{Dyadic} \\ \text{Prime} \\ \text{Ideals} \\ \text{of } L \} \\
\end{align*}
\]

such that if $P \leftrightarrow Q$, then

$[K_P : Q_2] = [L_Q : Q_2]$  
and $-1 \in K_P^* \iff -1 \in L_Q^*$.

Theorem 4.4 determines when two number fields are in the same Witt equivalence class via conditions A), B), and C). Perlis, Szymiczek, and Conner prove that two Witt equivalent number fields must have the same degree over $\mathbb{Q}$ (see [P-S-C, Lemma 1 and Theorem 2]). In light of this, we pose the following question:

**QUESTION:** Fix $n \in \mathbb{N}$. What can be said about the number of Witt equivalence classes of number fields of degree $n$?

Let $K$ be an arbitrary number field of degree $n$. If $K$ is totally complex, then there are no real embeddings of $K$. On the other hand, if $K$ is totally real, then there are at most $n$ distinct embeddings of $K$ into the field of real numbers. Hence, condition A) gives us at most $(n + 1)$ different classes of number fields of degree $n$. Clearly condition B) divides each of these $(n + 1)$ possible classes into at most two more classes, depending on whether or not $-1$ is a global square. Furthermore, the
Fundamental Equality of Number Theory implies that a number field of degree $n$ can have at most $n$ dyadic prime ideals, each with a local degree of at least one and no more than $n$. Lastly, either -1 is or is not a local square at each of these dyadic prime ideals. Thus, altogether, condition C) subdivides each of the above classes into no more than $2n^2$ classes. Therefore, we have at most

$$ \text{(4.1)} \quad (n + 1)2 \cdot 2(2n^2) = 4(n + 1)n^2 $$

distinct Witt equivalence classes of number fields of degree $n$. We summarize this in the form of the following corollary:

**Corollary 4.5.** Fix $n \in \mathbb{N}$. The number of Witt equivalence classes of number fields of degree $n$ is finite.

While (4.1) suffices to establish Corollary 4.5, we were able to obtain a sharper bound; with more work we can show:

**Lemma 4.6.** Fix $n \in \mathbb{N}$. The number of Witt equivalence classes of number fields of degree $n$ is bounded by

$$ \text{(4.2)} \quad \left\lfloor \frac{n+1}{2} \right\rfloor \cdot \left( \sum_{\text{all partitions } A \text{ of } n} 2^{|A|+1} \right) $$

where $\left\lfloor \frac{n+1}{2} \right\rfloor$ denotes the least integer greater than or equal to the number $\frac{n+1}{2}$ and $|A|$ the number of terms in the partition $A$ of $n$.

We remark that this bound is not intended to be the best possible. In fact, in the case $n = 1$, the bound in (4.2) indicates that there are at most 4 Witt equivalence classes of number fields of degree 1 (while (4.1) gives a maximum of 8 classes). As there is only one number field of degree 1, namely $\mathbb{Q}$ itself, there is precisely one Witt equivalence class of number fields of degree 1. For $n = 2$, the bound given in (4.2) is 24 classes and that in (4.1) is 48. As we shall see in Corollary 4.7, there are only seven Witt equivalence classes of quadratic number fields.

**Proof of Lemma 4.6:** Conditions A), B), and C) of Theorem 4.4 divide the number fields of degree $n$ into equivalence classes. Condition A), for example, specifies that fields in the same class must have the same number of real infinite
primes. Thus, given an arbitrary number field $K$ of degree $n$, we must count the number of distinct values which $r_1(K)$ can assume.

Recalling that we can write the global degree $n$ of $K$ as the sum

$$
(4.3) \quad n = r_1(K) + 2\cdot r_2(K)
$$

we see that

$$
0 \leq r_1(K) \leq n.
$$

Clearly, $r_1(K)$ can assume at most $(n + 1)$ distinct values. However (4.3) implies that the parity of $n$ and $r_1(K)$ must be the same. Therefore, if $n$ (hence $r_1(K)$) is odd, $r_1(K)$ can assume at most $\frac{n+1}{2}$ distinct values; if $n$ (hence $r_1(K)$) is even, $r_1(K)$ can assume no more than $\frac{n+2}{2}$ distinct values. Using the notation $[\alpha]$ to denote the least integer greater than or equal to the number $\alpha$, we can combine our observations into one statement which does not mention parity. Namely, there are at most

$$
\left\lfloor \frac{n + 1}{2} \right\rfloor
$$

distinct values of $r_1(K)$.

Turning to condition B), we see that fields in which -1 is a global square cannot be equivalent to those in which -1 is not a global square. Therefore, condition B) divides each of the above groups into at most two distinct classes.

Lastly, we consider condition C). Given two equivalent fields of degree $n$, condition C) states that not only must the sets of local degrees at the dyadic prime ideals match up, but for corresponding dyadic prime ideals, -1 must be either a local square at both prime ideals or at neither. Thus, if $\delta$ represents one such set of local degrees at the dyadic prime ideals and $|\delta|$ the number of dyadic prime ideals associated with $\delta$, there are at most $2^{|\delta|}$ distinct classes of fields of degree $n$ corresponding to $\delta$. Hence, summing over all possible distinct sets $\delta$, we see that condition C) divides each of the previous groups of fields into at most

$$
\sum_{\delta} 2^{|\delta|}
$$

distinct classes of number fields of degree $n$. 
In order to describe the sets $\delta$ more explicitly, we use the Fundamental Equality of Number Theory:

\[ n = \sum_{i=1}^{g} [K_{p_i} : Q_p] \]

(4.4)

where \( \{p_1, p_2, \ldots, p_g\} \) denotes the set of all dyadic prime ideals of $K$. It is clear from (4.4) that the corresponding set of local degrees $\delta = \{[K_{p_i} : Q_p]\}_{i=1}^{g}$ form a partition of $n$. In fact, any partition of $n$ can be viewed as a (possible) set of local degrees for the dyadic prime ideals of $K$. Thus, the number of partitions of $n$ counts the number of possible sets $\delta$. Moreover, given a partition $A$ of $n$, the number of terms, $|A|$, of $A$ gives the number of dyadic prime ideals associated with $A$. Hence, condition C) yields at most

\[ \left( \sum_{\text{all partitions } A \text{ of } n} 2^{|A|} \right) \]

distinct classes of fields.

Combining the observations we have obtained from each of the three conditions A), B), and C), we arrive at an upper bound on the number of Witt equivalence classes of number fields of degree $n$. In particular, the number of classes is bounded by

\[ \left\lfloor \frac{n+1}{2} \right\rfloor \cdot (2) \cdot \left( \sum_{\text{all partitions } A \text{ of } n} 2^{|A|} \right). \]

Absorbing the term $(2)$ into the sum, we obtain

\[ \left\lfloor \frac{n+1}{2} \right\rfloor \cdot \left( \sum_{\text{all partitions } A \text{ of } n} 2^{|A|+1} \right) \]

as desired. \[ \]

Recall that $K \sim_w L$ means $W(K) \cong W(L)$. As an example, we consider the family of quadratic number fields. Applying the conditions A), B), and C) directly, we can show the following:

**Corollary 4.7.** There are exactly seven Witt equivalence classes of quadratic number fields, represented by $Q(\sqrt{-1})$, $Q(\sqrt{2})$, $Q(\sqrt{-2})$, $Q(\sqrt{7})$, $Q(\sqrt{-7})$, $Q(\sqrt{17})$,
and \(\mathbb{Q}(\sqrt{-17})\). In particular, given a quadratic number field \(K\), write \(K = \mathbb{Q}(\sqrt{n})\), where \(n \in \mathbb{Z}\) is square-free and \(n \neq 1\). Then

1. \(n = -1 \Rightarrow K = \mathbb{Q}(\sqrt{-1})\);
2. \(n \neq -1\) odd, and
   \[|n| \equiv 3, 5 \pmod{8} \Rightarrow K \sim \mathbb{Q}\left(\sqrt{-\left((-1)^{\text{sign}(n)} \cdot 2\right)}\right)\]
   \[|n| \equiv 7 \pmod{8} \Rightarrow K \sim \mathbb{Q}\left(\sqrt{-\left((-1)^{\text{sign}(n)} \cdot 7\right)}\right)\]
   \[|n| \equiv 1 \pmod{8} \Rightarrow K \sim \mathbb{Q}\left(\sqrt{-\left((-1)^{\text{sign}(n)} \cdot 17\right)}\right)\]
3. \(n\) even \(\Rightarrow K \sim \mathbb{Q}\left(\sqrt{-\left((-1)^{\text{sign}(n)} \cdot 2\right)}\right)\).

We note that the family of quadratic number fields had been classified previously up to tame equivalence by A. Czogala (see [Cz]).

Proof of Corollary 4.7: Every quadratic number field can be written in the form

\[(4.5) \quad \mathbb{Q}(\sqrt{n}) \quad \text{where } n \neq 1 \text{ is a square-free integer.}\]

Consequently, whenever we write "\(\mathbb{Q}(\sqrt{n})\)", the number "\(n\)" is understood to be as in (4.5).

Let \(K = \mathbb{Q}(\sqrt{n})\) be an arbitrary quadratic number field. If \(-1 \in K^{*2}\), then we must have \(n = -1\), since \(\mathbb{Q}(\sqrt{-1})\) is the only quadratic number field in which \(-1\) is a global square. Moreover, by condition B), we observe that \(\mathbb{Q}(\sqrt{-1})\) cannot be Witt equivalent to any other quadratic number field. In light of this, we may assume that \(n \neq -1\).

Let us consider condition A). Recall that for any number field \(K\),

\[r_1(K) + 2 \cdot r_2(K) = [K : \mathbb{Q}].\]

In particular, if \(K\) is quadratic, we have

\[r_1(K) + 2 \cdot r_1(K) = 2.\]
Hence, \( r_1(K) = 0 \) or \( r_2(K) = 2 \). More specifically,

\[
r_1(K) = 2 \iff n > 0
\]

and

\[
r_1(K) = 0 \iff n < 0.
\]

Therefore, we have

\[
\mathbb{Q}(\sqrt{n}) \sim \mathbb{Q}(\sqrt{m}) \iff \text{both } n, m > 0 \text{ or both } n, m < 0.
\]

We prove the case for \( n, m > 0 \) here, the case for \( n, m < 0 \) being identical.

Assume \( n > 0 \). The Fundamental Equality of Number Theory implies that a quadratic number field \( K \) has either one dyadic prime ideal or precisely two (distinct) dyadic prime ideals. In fact, \( K \) has two dyadic prime ideals if and only if the rational prime number 2 splits in \( K \) if and only if \( n \equiv 1 \pmod{8} \). Using condition C) of Theorem 4.4 (and assuming \( n, m > 0 \)), we obtain

\[
(4.6) \quad \mathbb{Q}(\sqrt{n}) \sim \mathbb{Q}(\sqrt{m}) \iff \text{both } n, m \equiv 1 \pmod{8} \text{ or both } n, m \not\equiv 1 \pmod{8}.
\]

Observations:

1) Since \( n \) is a square-free integer, we have

\[
n \equiv 1, 2, 3, 5, 6 \text{ or } 7 \pmod{8}
\]

(that is, \( n \not\equiv 0 \text{ or } 4 \pmod{8} \)). Thus \( n \not\equiv 1 \pmod{8} \) means \( n \equiv 2, 3, 5, 6, \text{ or } 7 \pmod{8} \).

2) The set \( \{[K_P : \mathbb{Q}_2] \}_P \text{ dyadic} \) is entirely determined by the number of dyadic prime ideals of \( K \). Namely, by the Fundamental Equality of Number Theory, \( K \) has only one dyadic prime ideal, say \( P \), if and only if \([K_P : \mathbb{Q}_2] = 2\) and two dyadic prime ideals, say \( P_1 \) and \( P_2 \), if and only if \([K_{P_i} : \mathbb{Q}_2] = 1\) for \( i = 1, 2 \). Thus, any bijection between the sets of dyadic prime ideals of two quadratic number fields automatically preserves the local degrees over \( \mathbb{Q}_2 \).

It remains to determine when -1 is a local square at a dyadic prime ideal of \( K \). By observation 2), if \( K \) has two dyadic prime ideals \( P_1 \) and \( P_2 \), then \( K_{P_i} = \mathbb{Q}_2 \) for
For $i = 1, 2$, So, $-1$ is not a local square in $K_{P_i}, i = 1, 2$. Thus assuming $n, m > 0$,

\[(4.7) \quad \text{both } n, m \equiv 1 \pmod{8} \implies Q(\sqrt{n}) \sim Q(\sqrt{m}).\]

On the other hand, if $K$ has only one dyadic prime ideal $P$, $(n \not\equiv 1 \pmod{8})$ then

\[-1 \in K_P^2 \iff Q_2(\sqrt{n}) = Q_2(\sqrt{-1})
\iff n = -1 \cdot \text{square in } Q_2
\iff (n \text{ is odd and } n \equiv -1 \equiv 7 \pmod{8}).\]

Hence, for $n, m > 0$ and $n, m \not\equiv 1 \pmod{8}$, we obtain

\[Q(\sqrt{n}) \sim Q(\sqrt{m}) \iff \text{both } n, m \equiv 7 \pmod{8} \quad \text{or} \quad \text{both } n, m \equiv 2, 3, 5 \text{ or } 6 \pmod{8}.\]

Combining this with (4.6) and (4.7), for $n, m > 0$ we have shown

\[Q(\sqrt{n}) \sim Q(\sqrt{m}) \iff \text{both } n, m \equiv 1 \pmod{8} \quad \text{or} \quad \text{both } n, m \equiv 7 \pmod{8} \quad \text{or} \quad \text{both } n, m \equiv 2, 3, 5 \text{ or } 6 \pmod{8}.\]

Similarly for $n, m < 0$ we obtain

\[Q(\sqrt{n}) \sim Q(\sqrt{m}) \iff \text{both } n, m \equiv 1 \pmod{8} \quad \text{or} \quad \text{both } n, m \equiv 7 \pmod{8} \quad \text{or} \quad \text{both } n, m \equiv 2, 3, 5 \text{ or } 6 \pmod{8}.\]

Therefore, using the conditions of Theorem 4.4, we have produced seven (distinct) Witt equivalence classes of quadratic number fields (including $Q(\sqrt{-1})$). Furthermore, our analysis shows that each of these is a full equivalence class.
We choose representatives as follows:

\[ \begin{align*}
&\text{for } n = -1, & Q(\sqrt{-1}) \\
&n > 0, n \equiv 2,3,5 \text{ or } 6 \pmod{8}, & Q(\sqrt{2}) \\
&n > 0, n \equiv 7 \pmod{8}, & Q(\sqrt{7}) \\
&n > 0, n \equiv 1 \pmod{8}, & Q(\sqrt{17}) \\
&n < 0, n \equiv 2,3,5 \text{ or } 6 \pmod{8}, & Q(\sqrt{-2}) \\
&n < 0, n \equiv 7 \pmod{8}, & Q(\sqrt{-17}) \\
&n < 0, n \equiv 1 \pmod{8}, & Q(\sqrt{-7}).
\end{align*} \]

(4.8)

Note that for \( n > 0 \), we have

\[ n \equiv |n| \pmod{8} \]

where \( |n| \) denotes the absolute value of \( n \), and for \( n < 0 \),

\[ -n \equiv |n| \pmod{8}. \]

Rewriting the congruences in (4.8) in terms of \( |n| \) and letting

\[ \text{sign}(n) = \begin{cases} 
+1 & \text{for } n > 0 \\
-1 & \text{for } n < 0 
\end{cases} \]

yields the desired algorithm.

In proving \( \text{II)} \Rightarrow \text{III)} \) of Theorem 4.1, we considered the local fields \( K_P \) and \( L_Q \), where \( P \) and \( Q \) were places of \( K \) and \( L \), respectively. With that in mind, one might ask if there is a relationship between global Witt rings and local Witt rings. By Theorem 4.4, \( W(K) \cong W(L) \) implies \( K \) and \( L \) are reciprocity equivalent, say via \( (t,T) \). It is not difficult to see that this implies that \( W(K_P) \cong W(L_{TP}) \) as rings (hence as additive groups) for all places \( P \) of \( K \). Theorem 4.4 gives the converse; that is, almost the converse. We show if there exists a bijection \( T : \Omega_K \to \Omega_L \) for which \( W(K_P) \cong W(L_{TP}) \) as additive groups for all places \( P \) of \( K \), then \( W(K) \cong W(L) \) as rings. We conclude this section with a proof of this fact.

**Corollary 4.8.** Let \( K \) and \( L \) be number fields.

If there exists a bijection \( T : \Omega_K \to \Omega_L \) such that

\[ W(K_p)_\text{GROUPS} \cong W(L_{T_P}) \text{ for all } p \in \Omega_K \]

(4.9)
then

\[ W(K) \cong W(L). \]

**Proof of Corollary 4.8**: Once again, it suffices to check conditions A), B), and C) of Theorem 4.4 for \( K \) and \( L \). We begin by observing

\[ W(K_p) = \begin{cases} \mathbb{Z}/2, & \text{if } \wp \text{ is a complex infinite prime} \\ \mathbb{Z}, & \text{if } \wp \text{ is a real infinite prime} \\ \text{finite of order } 2^{[K_p: \mathbb{Q}_2] + 4}, & \text{if } \wp \text{ is a dyadic prime ideal} \\ \text{finite of order } 16, & \text{if } \wp \text{ is a non-dyadic prime ideal} \end{cases} \]

and similarly for \( W(L_{T_p}) \). Thus \( T \) must map the set of real infinite primes of \( K \) bijectively onto the set of real infinite primes of \( L \). In particular, we obtain

\[ r_1(K) = r_1(L), \]

hence condition A) is satisfied.

Note that (4.10) also implies that \( T \) does induce a bijection between the set of dyadic prime ideals of \( K \) and the set of dyadic prime ideals of \( L \); moreover

\[ [K_p : \mathbb{Q}_2] = [L_{T_p} : \mathbb{Q}_2] \]

for each dyadic prime ideal \( \wp \) of \( K \). That is, given a dyadic prime ideal \( \wp \) of \( K \), the local degree \([K_p : \mathbb{Q}_2] \geq 1\) so

\[ \#W(K_p) = 2^{[K_p : \mathbb{Q}_2] + 4} \geq 32; \]

likewise for \( L \). Hence if \( \wp \in \Omega_K \) is a dyadic prime ideal,

\[ W(K_p) \cong \text{Groups } W(L_{T_p}) \Rightarrow [K_p : \mathbb{Q}_2] = [L_{T_p} : \mathbb{Q}_2]. \]

As for the square-class of -1 in \( K_p \) and \( L_{T_p} \), we note that for any place \( \wp \) of \( K \):

\[ -1 \in K_p^\times \iff W(K_p) \text{ has additive 2-torsion} \]

\[ \iff W(L_{T_p}) \text{ had additive 2-torsion by (4.9)} \]

\[ (4.11) \iff -1 \in L_{T_p}^\times. \]

Thus \( K \) and \( L \) satisfy condition C). Condition B) follows from (4.11) and the
Global-Square Theorem:

\[-1 \in K^{*2} \iff -1 \in K_p^{*2} \text{ for all } p \in \Omega_K \text{ by the Global-Square Theorem}\]
\[-1 \in L_{T_p}^{*2} \text{ for all } T_p \in \Omega_L \text{ by (4.11)}\]
\[-1 \in L^{*2} \text{ by the Global-Square Theorem}.\]

Therefore, \(K\) and \(L\) are Witt equivalent, or \(W(K) \cong W(L)\) (as rings).

In closing, we mention that this result is reminiscent of C.M. Cordes' Theorem (see [Co]), showing that two fields with finitely many square classes and isomorphic Witt groups often have isomorphic Witt rings.
BIBLIOGRAPHY


INDEX OF DEFINITIONS

The following is a list of terminology and the page on which it was defined.

regular or non-degenerate ... 5
orthogonal complement ... 6
metabolizer ... 6
isometric ... 6
isometry ... 6
Witt ring ... 7
Witt equivalent ... 7
place ... 7
infinite place or infinite prime ... 7
finite place ... 7
Hilbert symbol ... 9
reciprocity equivalence ... 10
ring of $S$-integers ... 10
$S$-units ... 11
group of units of $O_K$ ... 11
group of $S$-units modulo squares ... 11
ideal class group ... 11
ideal class number ... 11
$S$-ideal class group ... 11
$S$-ideal class number ... 11
totally isotropic ... 13
not totally isotropic ... 13
cycle $c_S$ of $K$ ... 21
$a \equiv 1 \pmod{mod^*c_S}$ ... 21
generalized ideal class group associated to the cycle $c_S$ ... 22
suitable pair ... 30
small equivalence ... 31
\[ H_S, H_{S'} \ldots 32 \]
tame ... 52
wild ... 52
wild set ... 52
tame equivalence ... 53
wild equivalence ... 53
The following is a list of frequently used notation and the page on which it was introduced.

\[(V, \beta) \ldots \text{inner product space, 5}\]
\[\text{Hom}_E(V, E) \ldots \text{vector space dual of } V, 5\]
\[W^\perp \ldots \text{orthogonal complement of } W, 6\]
\[W(E) \ldots \text{Witt ring of the field } E, 7\]
\[K \sim L \ldots \text{Witt equivalence, 7}\]
\[O_K \ldots \text{ring of integers of } K, 7\]
\[\Omega_K \ldots \text{set of all places of } K, 7\]
\[\mathcal{S}_\infty \ldots \text{set of all infinite places of } K, 7\]
\[r_1(K) \ldots \text{number of real infinite primes of } K, 8\]
\[r_2(K) \ldots \text{number of complex infinite primes of } K, 8\]
\[[L : K] \ldots \text{degree of the field extension } L/K, 8\]
\[Q \ldots \text{field of rational numbers, 8}\]
\[K_{\mathfrak{p}} \ldots \text{p-adic completion of } K \text{ at the place } \mathfrak{p}, 8\]
\[E^*/E^{*2} \ldots \text{group of square-classes of the field } E, 9\]
\[(a, b)_P \ldots \text{Hilbert symbol of the elements } (a, b) \text{ of } K \text{ at the place } P, 9\]
\[(t, T) \ldots \text{reciprocity equivalence, 10}\]
\[O_K(S) \ldots \text{ring of } S\text{-integers of } K, 10\]
\[U_K(S) \ldots \text{group of } S\text{-units of } K, 11\]
\[U_K \ldots \text{group of units of } K, 11\]
\[U_K(S)/U_K(S)^2 \ldots \text{group of } S\text{-units of } K \text{ modulo squares, 11}\]
\[C(K) \ldots \text{ideal class group of } K, 11\]
\[h(K) \ldots \text{ideal class number of } K, 11\]
\[C^S(K) \ldots S\text{-ideal class group of } K, 11\]
\[h^S(K) \ldots S\text{-ideal class number of } K, 11\]
\[F_2 \ldots \text{finite field with two elements, 12}\]
\[(\#S) \ldots \text{order of the finite set } S, 16\]
number of dyadic prime ideals of $K$, 17
$G(S)$ ... see Page 18
$y = (y, \ldots, y)$ ... image of the element $y$ of $K^*$ in $G(S)$, 18
$\langle , , \rangle_S$ ... see Page 18
$i_S$ ... see Page 19
$c_S$ ... cycle of $K$ associated with $S$, 21
$e_P(K)$ ... ramification index of the prime ideal $P$ in $K$, 21
$I(K, c_S)$ ... set of fractional $O_K$-ideals prime to cycle $c_S$, 21
$P(K, c_S)$ ... set of principle $O_K$-ideals with generator congruent to $1 \mod c_S$, 21
$\mathcal{C}\ell(K, c_S)$ ... generalized ideal class group associated to cycle $c_S$ of $K$, 22
$\mathcal{A}$ ... class of the ideal $\mathcal{A} \in I(K, c_S)$, in $\mathcal{C}\ell(K, c_S)$, 22
$[\mathcal{A}]$ ... square-class of $\mathcal{A}$, 22
$\phi$ ... see Page 23
$\mathcal{C}\ell(Q)$ ... class of the ideal $Q$ in the ideal class group, 25
$\mathcal{C}\ell(Q)$ ... class of the ideal $Q$ in the ideal class group, 25
$I_K$ ... group of fractional $O_K$-ideals, 28
$S, S'$ ... suitable pair for $K$ and $L$, 30
$S_0, S'_0$ ... set of all infinite and dyadic places of $K$ and $L$ respectively, 30
$\tau_S$ ... see Page 31
$H_S, H_S'$ ... see Page 32
$d_{SS'}$ ... obstruction to $S, S'$ yielding a small equivalence, 33
$u_1, \pi_1, u'_1, \pi'_1$ ... see Page 35
$[\alpha]$ ... least integer greater than or equal to $\alpha$, 55
$|A|$ ... number of terms in the partition $A$ of $n$, 55
$|n|$ ... absolute value of the number $n$, 61
$\text{sign}(n)$ ... sign of the real number $n$, 61
VITA

Jenna Sue Price was born on November 7, 1961 in Corsicana, Texas. She became Mrs. George Walter Carpenter, Jr. on August 27, 1983. In November 1983, she received a Bachelor of Science degree in Mathematics from Louisiana Tech University. She entered Louisiana State University in January 1984 and received a Master of Science degree in Mathematics in May 1986.
Candidate: Jenna Price Carpenter

Major Field: Mathematics (Algebra)

Title of Dissertation: Finiteness Theorems for Forms over Number Fields

Approved:

[Signatures of the Major Professor and Chairman, Dean of the Graduate School, and other committee members]

EXAMINING COMMITTEE:

[Signatures of the committee members]

Date of Examination:

April 21, 1989