2001

Bounding the wild set (counting the minimum number of wild primes in Hilbert symbol equivalent number fields)

Marius M. Somodi
Louisiana State University and Agricultural and Mechanical College, msomod1@lsu.edu

BOUNDING THE WILD SET
(COUNTING THE MINIMUM NUMBER OF WILD PRIMES IN HILBERT SYMBOL EQUIVALENT 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
Marius M. Somodi
Graduation Diploma, Bucharest University, 1993
M.S., Louisiana State University, 1998
August 2001

Acknowledgments

My first and greatest debt is to the Department of Mathematics of Louisiana State University for giving me the opportunity to pursue my interest in the field of algebraic number theory.

I am grateful to my high-school mathematics teacher, Dr. M. Tena, for making me realize how beautiful abstract algebra is.

I would like to thank to all my professors in the Department of Mathematics at the University of Bucharest, Romania, for helping me construct a solid mathematical background.

I am indebted to the Soros Foundation for an Open Society which supported me to travel in the United States of America for graduate studies in mathematics.

I wish to thank Dr. L. Richardson for introducing me to the graduate program in mathematics at Louisiana State University and for advising me during the first years of graduate study.

I am grateful to all my professors in the Department of Mathematics at Louisiana State University, whose assistance, guidance and devotion made my time spent in the graduate program a gratifying experience.

Most of all, I wish to express my sincere appreciation to Dr. Robert Perlis for his relentless guidance, helpful suggestions, openness and endless patience without which this work would not have been possible.

I would like to thank Dr. P.E. Conner who originally posed the problem solved in this dissertation.

Finally I would like to thank my spouse, Rodica, and my parents, Ion and Stela, for encouraging me continuously to improve my knowledge.

Table of Contents

Abstract

This dissertation makes a contribution to the study of Witt rings of quadratic forms over number fields. To every pair of algebraic number fields with isomorphic Witt rings one can associate a number, called the *minimum number of wild primes*. The situation is particularly nice when this number is 0; often it is not 0. Earlier investigations have established lower bounds for this number. In this dissertation an analysis is presented that expresses the minimum number of wild primes in terms of the number of wild dyadic primes. This formula not only gives immediate upper bounds, but can be considered to be an exact formula for the minimum number of wild primes.

Chapter 1. Introduction

The abstract theory of symmetric bilinear forms over fields took a major turn in 1937, when Witt constructed a new object, today known as the *Witt ring*. As this object can be associated to any field, number theorist have been interested in understanding the Witt ring of number fields. To describe explicitly the Witt ring of an arbitrary number field is a difficult problem. Another problem in algebraic theory of quadratic forms and number theory is to describe the situation when two number fields have isomorphic Witt rings (in this case the number fields are called *Witt equivalent*). In 1994, R. Perlis, K. Szymiczek, P.E. Conner, and R. Litherland ([12]) solved this problem. They proved that two number fields are Witt equivalent if and only if there is a *reciprocity equivalence* between the fields. Later the terminology has changed and *reciprocity equivalence* has been renamed *Hilbert symbol equivalence*. A Hilbert symbol equivalence is a pair of maps: a bijection between the sets of (finite and infinite) primes and an isomorphism between the square class groups of the two number fields such that the Hilbert symbols agree. In 1991, K. Szymiczek proved that there is a Hilbert symbol equivalence between two number fields if and only if the two number fields have the same level, the same number of real embeddings, and there is a bijection between the dyadic primes of the two fields so that the corresponding dyadic completions have the same level and degree over $\mathbb{Q}_2$ ([14]).

Constructing a Hilbert symbol equivalence between Witt equivalent number fields is not a simple task. Since one wants to define maps between infinite sets, in the absence of a systematic method this is an infinite task. However, in the same paper ([12]) the authors reduced this problem to the problem of constructing a finite object involving finitely many primes and called a *small equivalence*. So far small equivalence is the only tool employed to construct Hilbert symbol equivalences.

Whenever a Hilbert symbol equivalence between two number fields is considered, a partition of the set of prime ideals can be constructed: a prime ideal P is called *tame* if the isomorphism between the square class groups preserves the parity of the order at P of any square class, and *wild* if it is not tame; the partition consists of the set of tame primes and the set of wild primes. In [12] it is shown that any small equivalence can be extended to a Hilbert symbol equivalence by adding only tame primes. One consequence is that between Witt equivalent number fields one can always construct Hilbert symbol equivalences that have finitely many wild primes. P.E. Conner posed the question: how small can the set of wild primes be? A lower bound for the minimum number of wild primes can be found in [2]: this number is not less than the difference in 2-ranks of the corresponding ideal class groups and the difference in 2-ranks of the corresponding narrow ideal class groups. Here is the complete statement found in [2]:

Proposition 1.1. *Let (t, T) be a Hilbert symbol equivalence between number fields K and L with finite wild set W=Wild(K,L). Let S be any finite subset of primes of K containing all infinite primes. Then:*

$$|rk_2C_K(S) - rk_2C_L(TS)| \leq |W \setminus S|$$

and

$$|rk_2C_K^+(S) - rk_2C_L^+(TS)| \leq |W \setminus S|.$$

If two number fields are Witt equivalent, then one can consider the restriction of an arbitrary Hilbert symbol equivalence to a finite set of primes containing all infinite and dyadic primes, and call this a *correspondence*. In this dissertation we show that any corresponcence can be extended to a small equivalence (and then to a Hilbert symbol equivalence) and we present a method of extending a correspondence to a Hilbert symbol equivalence with a minimum number of wild primes among all Hilbert symbol equivalences that extend the correspondence. In particular we present a formula that expresses the minimum number of wild primes in *any* Hilbert symbol equivalence in terms of the number of dyadic wild primes:

Theorem 1.2. *Let K and L be Witt equivalent number fields, and let S be a set that contains all infinite and dyadic primes in K. Any correspondence $\mathcal{C}$ defined on S can be extended to a Hilbert symbol equivalence between K and L whose wild set has the size equal to*

$$\delta + |W| + |rk_2(C_K(S)) - rk_2(C_L(TS))|,$$

where $W = W(\mathcal{C}) \subseteq S$ is the set of wild primes of $\mathcal{C}$ and $\delta = \delta(\mathcal{C})$ is a non-negative integer called the defect of the correspondence. Moreover, any other extension of $\mathcal{C}$ to a Hilbert symbol equivalence between K and L has a wild set of size not less than $\delta + |W| + |rk_2(C_K(S)) - rk_2(C_L(TS))|$.

In particular, if one wants to construct a Hilbert symbol equivalence with a minimum number of wild primes then one has to consider all (finitely many) correspondences that can be defined on the set of infinite and dyadic primes, and determine for each one of them the number of wild dyadic primes ($|W|$) and the defect (δ). When the sum of these two numbers is minimum then any particular correspondence for which this minimum is achieved can be extended to a Hilbert symbol equivalence with a minimum number of wild primes. This number is $\delta + |W| + |rk_2(C_K(D)) - rk_2(C_L(D'))|$, where D and D' are the sets of dyadic primes in K and L respectively.

The formula that we present gives the exact minimum number of wild primes. However, computing explicitly this number for arbitrary number fields might be difficult. Upper and lower bounds for the minimum number of wild primes might be useful. Here they are:

Corollary 1.3. *Let W=Wild(K,L) be a minimum wild set for two Witt equivalent number fields K and L. Let D and D' be the sets of dyadic primes in K and L respectively, r and s be the number of real embeddings and pairs of complex embeddings respectively of K. Then:*

$$|rk_2C_K(D) - rk_2C_L(D')| \leq |W| \leq |rk_2C_K(D) - rk_2C_L(D')| + 2|D| + r + s.$$

In Chapter 2 we present background definitions and results from the algebraic theory of quadratic forms and algebraic number theory.

In Chapter 3 we discuss Hilbert symbol equivalences of number fields. As the first two chapters are background chapters, we don't give proofs for the results presented, but we include references to papers or books where proofs can be found.

Chapter 4 contains the main results. We present a method of extending a correspondence to a small equivalence by adding a minimum number of wild primes. In order to accomplish this we follow a two-step procedure. If at least one of the fields has an even S-class number then as a first step we add primes to the correspondence until both class numbers become odd. Then

we proceed to the second step, where we employ J. Carpenter's ([1]) method of extending to a small equivalence the particular type of correspondence (which she called *suitable*) that gives odd S-class numbers for both fields. We also prove that her method produces at the end the minimum number of wild primes.

Chapter 2. Quadratic Forms and Algebraic Number Fields

2.1 Symmetric Bilinear Forms and Quadratic Forms

This chapter contains standard material about quadratic forms and algebraic number fields.

Let K be a field of characteristic different from 2 and V be a finite dimensional vector space over K of dimension n. By a *symmetric bilinear form* on V we understand any map $B : V \times V \to K$ that has the following properties:

$$B(x, y) = B(y, x),\ \forall x, y \in V$$

$$B(x, y_1 + y_2) = B(x, y_1) + B(x, y_2),\ \forall x, y_1, y_2 \in V$$

$$B(kx, y) = kB(x, y),\ \forall x, y \in V,\ k \in K.$$

A symmetric bilinear form B is said to be *non-degenerate* if there is no element $x \neq 0$ such that $B(x, y) = 0,\ \forall y \in V$. To any symmetric bilinear form B one associates a *quadratic map* $Q : V \to K$ defined by $Q(x) = B(x, x),\ \forall x \in V$. The pair (V, Q) is called a *quadratic space*. This map has the following properties (see [10], page 83):

$$Q(kx) = k^2 Q(x) \tag{2.1}$$

$$Q(x + y) = Q(x) + Q(y) + 2B(x, y) \tag{2.2}$$

$$Q(\sum_{i=1}^{t} k_i x_i) = \sum_{i=1}^{t} k_i^2 Q(x_i) + 2 \sum_{i<j} k_i k_j B(x_i, x_j). \tag{2.3}$$

In particular, identity (2.2) shows that distinct symmetric bilinear forms on V define distinct quadratic maps on V. It follows that there is a one-to-one correspondence between the symmetric bilinear forms on V and the quadratic maps on V.

Two n-dimensional quadratic spaces over K, (V, Q) and (V', Q'), are called *isometric* if there is an isomorphism of K-vector spaces $i : V \to V'$ such that $Q(x) = Q'(i(x)),\ \forall x \in V$.

If we choose a basis $x_1, ..., x_n$ for V, we can associate to any symmetric bilinear form B on V a symmetric $n \times n$ matrix $A = (a_{ij})$ whose entries are defined by $a_{ij} = B(x_i, x_j)$. Conversely, given the symmetric $n \times n$ matrix A, we can define a symmetric bilinear form on V by the previous formula. According to [15], Theorem 3.1.1, if we fix the basis then we have a one-to-one correspondence between the symmetric bilinear forms on V and the symmetric $n \times n$ matrices with entries in K. By changing the basis via the linear transformation T, the matrix A will change into a congruent matrix: $P^t AP$, where P is the (invertible) transition matrix associated to T. In fact any matrix congruent to A is the matrix defined by the same symmetric bilinear form in a certain basis. According to [15], Theorem 4.1.1, two quadratic spaces (V, Q) and (V', Q') are isometric if and only if they have the same matrix relative to suitably chosen bases of V and V'. If we combine this result to the previous observation we get the following proposition:

Proposition 2.1. *There is a one-to-one correspondence between isometry classes of n-dimensional quadratic spaces over K and congruence classes of $n \times n$ symmetric matrices with entries in K.*

By an n-ary quadratic form we understand any polynomial $\phi \in K[X_1, ..., X_n]$ of degree 2:

$$\phi(X_1, ..., X_n) = \sum_{i,j=1}^{n} a_{ij} X_i X_j.$$

The representation of ϕ like above is not unique, but it becomes unique if we ask that $a_{ij} = a_{ji}$. We can associate to ϕ a symmetric matrix denoted by A, whose (i, j) entry is a_{ij}. We have $\phi(X) = X^t AX$, and there is a one-to-one correspondence between n-ary quadratic forms over K and symmetric $n \times n$ matrices with entries in K.
Let us denote by $X = (X_1, ..., X_n)$. Two n-ary quadratic forms ϕ and ϕ' are called *equivalent* if there is a $n \times n$ invertible matrix T with entries in K such that $\phi(X) = \phi'(TX)$. We denote equivalence of quadratic forms by $\simeq$. Since equivalent quadratic forms give rise to congruent symmetric matrices, we get:

Proposition 2.2. *There is a one-to-one correspondence between equivalence classes of n-ary quadratic forms over K and congruence classes of $n \times n$ symmetric matrices with coefficients in K.*

Because of these one-to-one correspondence we will often switch between symmetric matrices, quadratic forms, and quadratic spaces.

2.2 The Witt Ring

We can add two quadratic spaces (V, Q) and (V', Q') of arbitrary dimensions as follows: $(V, Q) \oplus (V', Q') = (W, Q^*)$, where $W = V \oplus V'$ as vector spaces, and $Q^*((x, y)) = Q(x) + Q'(y)$. What we get is a new quadratic space over K whose dimension is the sum of the dimensions of V and V' over K. We call (W, Q^*) the *orthogonal sum* of (V, Q) and (V', Q'). The following result from [13] (Theorem 1.8) is fundamental in the algebraic theory of quadratic forms:

Theorem 2.3. *Every quadratic space over a field of characteristic different from 2 is an orthogonal sum of 1-dimensional spaces.*

The consequence of this theorem is that every quadratic form ϕ is equivalent to a *diagonal* quadratic form, i.e. a form that can be represented as $\psi(X) = \sum_{i=1}^{n} a_i X_i^2$ with $a_i \in K$. The standard notation in this case is $\phi \sim< a_1, ..., a_n >$. It is clear that a quadratic space (or a quadratic form) is non-degenerate if none of the a_i's is 0. Moreover, the orthogonal sum of two quadratic forms in diagonal form satisfies the following identity:

$$< a_1, ..., a_n > \oplus < b_1, ..., b_m > \simeq < a_1, ..., a_n, b_1, ..., b_m >$$

From now on all quadratic forms will be non-degenerate (because degenerate quadratic forms over K can be seen as non-degenerate quadratic forms over K of a lower dimension).

Let (V, Q) be a quadratic space over K, and $x \in V$, $x \neq 0$. We say that x is *isotropic* if $Q(x) = 0$, otherwise x is called *anisotropic*. The quadratic space V is called *isotropic* if it contains isotropic vectors; if all non-zero vectors in V are isotropic then V is called *totally isotropic*, while if no vector in V is isotropic then V is called *anisotropic*. By convention, the zero vector space $V = \{0\}$ with the zero form $Q(0) = 0$ is also called anisotropic. One can easily

check that the 2-dimensional quadratic space whose matrix is $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is non-degenerate and isotropic. This particular quadratic space is called a *hyperbolic plane*. The diagonal form of a hyperbolic plane is $< 1, -1 >$. The following result holds:

Proposition 2.4. *(42:9 from [10]) The following are equivalent for a 2-dimensional quadratic space V:*
(1) V is isotropic and non-degenerate,
(2) V is a hyperbolic plane.

Since all quadratic spaces that we consider are non-degenerate, it follows that there is only one isometry class of 2-dimensional isotropic quadratic spaces: the isometry class of the hyperbolic plane. It is easy to see that the hyperbolic plane is isometric to the two dimensional quadratic space $(K^2,\ 2x_1x_2)$ and consequently the quadratic map that defines the hyperbolic plane is takes on every element of K as a value. A quadratic form (map) with this property is called *universal*. In [10], 42:10, the following more general result is proved:

Proposition 2.5. *Every non-degenerate isotropic quadratic space is split by a hyperbolic plane, hence it is universal.*

Consequently, every (non-degenerate) isotropic quadratic space is split by hyperbolic planes until it is reduced to 0 or an anisotropic form. This observation is the key of the *Witt decomposition theorem*:

Theorem 2.6. *([13]) Every (non-degenerate) quadratic form ϕ over K has an orthogonal decomposition*

$$\phi \simeq < 1, -1 > \oplus ... \oplus < 1, -1 > \oplus \phi_0$$

where ϕ_0 is an anisotropic quadratic form, and the number of times $< 1, -1 >$ shows up in the above decomposition is a non-negative integer.

The quadratic form ϕ_0 is unique up to an equivalence of quadratic forms, and will be called the *anisotropic part of* ϕ. The number of times the hyperbolic plane $< 1, -1 >$ shows up in the decomposition of ϕ is called the *Witt index* of ϕ, and it is unique. The proof of the Witt decomposition theorem is based on *Witt's cancellation theorem*:

Theorem 2.7. *([13], Theorem 1.1, p.19) If $\phi,\ \phi_1,\ \phi_2$ are quadratic forms over K such that*

$$\phi \oplus \phi_1 \simeq \phi \oplus \phi_2$$

then $\phi_1 \simeq \phi_2$.

This theorem leads to a new definition: two (non-degenerate) quadratic forms are called *similar* if they have equivalent anisotropic parts. The symbol used for similarity is $\sim$. It is easy to see that similarity of quadratic forms is an equivalence relation. The set of all similarity classes of (non-degenerate) quadratic forms over K is denoted by $W(K)$. Theorem 2.6 along with Theorem 2.7 show that two non-equivalent anisotropic quadratic forms live in distinct similarity classes, so $W(K)$ can be seen as the set of anisotropic non-degenerate quadratic forms over K.

So far we defined an operation with quadratic forms: the orthogonal sum. There is another operation that can be defined on $W(K)$: the *tensor product* of quadratic forms. If $\phi \simeq < a_1, ..., a_n >$

and $\psi \simeq < b_1, ..., b_m >$ then the tensor product of ϕ and ψ is defined to be the form

$$\phi \otimes \psi =< ..., a_i b_j, ... >_{1 \leq i \leq n,\ 1 \leq j \leq m} .$$

In 1937 Witt has proved that the orthogonal sum and the tensor product are well-defined as operations with similarity classes rather than equivalence classes of quadratic forms. The similarity class of the hyperbolic plane is the additive identity for the orthogonal sum, while the similarity class of $< 1 >$ is the multiplicative identity for the tensor product. So:

Theorem 2.8. *(Witt 1937):* $(W(K), \oplus, \otimes)$ *is a commutative ring with unit.*

This ring is called the *Witt ring of non-degenerate quadratic forms of* K, or simply the Witt ring of K. When we wish to refer to the additive structure only we speak of the Witt group.

Here are a few examples of Witt rings or groups:

$$W(\mathbb{C}) \simeq \mathbb{F}_2,\ W(\mathbb{R}) \simeq \mathbb{Z}.$$

If K is the field with p elements and p is a prime of the form $4k-1$ then as groups

$$(W(K), \oplus) \simeq (\mathbb{Z}/4\mathbb{Z}, +),$$

while if p is a prime of the form $4k+1$ then as groups

$$(W(K), \oplus) \simeq (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +).$$

2.3 Invariants

When studying quadratic forms, some invariants can be helpful. Let $\phi =< a_1, ..., a_n >$ be a non-degenerate quadratic form over K. We consider the following invariants.

1. Dimension. The *dimension* of ϕ is the number n. From the definition of equivalence of quadratic forms, any two equivalent quadratic forms have the same dimension.

2. Discriminant. The *determinant* of ϕ, denoted $det(\phi)$, is defined to be the square class of $\prod_{i=1}^{n} a_i$ in k^*/K^{*2}. Equivalent quadratic forms have the same determinant. The *discriminant* of ϕ is defined to be $(-1)^{n(n-1)/2} det(\phi)$. Equivalent quadratic forms have the same discriminant.

The importance of the first two invariants is illustrated by the following

Theorem 2.9. *Let K be a finite field (of characteristic different from 2). Two non-degenerate quadratic forms over K are equivalent if and only if they have the same dimension and discriminant.*

3. Witt index. The Witt index has been defined right after Theorem 2.6. Equivalent quadratic forms have the same Witt index.

None of the above invariants is, in general, preserved under similarity. In order to study the Witt ring $W(K)$ other invariants are necessary:

4. Dimension parity. The *dimension parity* of a similarity class is the dimension mod 2 of any element in the class. It is well-defined for the dimensions of any two similar quadratic forms differ by a multiple of 2. In other words the following map is well-defined:

$$e_0 : W(K) \to \mathbb{Z}/2\mathbb{Z}, \quad e_0(\phi) = \dim(\phi)\ (mod\ 2).$$

e_0 is a surjective ring homomorphism. The kernel of e_0 is a (maximal) ideal of index 2 (it is in fact the only ideal of index 2 in $W(K)$) which is called the *fundamental ideal* and denoted $I(K)$. The fundamental ideal consists of all similarity classes of even-dimensional (non-singular) quadratic forms. As an additive group it is generated by all similarity classes of quadratic forms $< 1, a >$, where $a \neq 0$.

5. Restricted discriminant. The discriminant is a map from $W(K)$ to K^*/K^{*2}; in general the discriminant does not preserve sums. However the discriminant preserves sums when we restrict it to $I(K)$. This gives rise to a map $e_1 : I(K) \to K^*/K^{*2}$ which is surjective and whose kernel is $I(K)^2$. We get a group isomorphism between $I(K)/I(K)^2$ and the square class group of K. The square of the fundamental ideal is generated additively by similarity classes of quadratic forms $< 1, a > \otimes < 1, b >$, where $a, b \neq 0$. Note that $< 1, a > \otimes < 1, b >=< 1, a, b, ab >$.

A theorem proved by Arason and Pfister in 1971 shows that the only element in the Witt ring which belongs to all powers of the fundamental ideal is the zero element.

6. Level. The *level* of a field K (denoted by $s(K)$) is defined in the following way:

$$s(k) = min\{d : \ -1 = x_1^2 + ... + x_d^2 \text{ has solutions in } K\}.$$

If -1 cannot be represented as a sum of squares in the field K then by definition $s(K) = \infty$.

Here are a few examples of levels of particular fields:

$$s(\mathbb{C}) = 1, \ s(\mathbb{R}) = \infty.$$

If p is a odd prime and K is the finite field with p elements then:

$$s(K) \in \{1, \ 2\}.$$

If K is a finite extension of $\mathbb{Q}$ then

$$s(K) \in \{1, \ 2, \ 4, \ \infty\}.$$

2.4 Algebraic Number Fields

Algebraic number fields are finite extensions of $\mathbb{Q}$ (so they are fields of characteristic equal to 0). If K is an algebraic number field then let's denote by O_K the set of all elements of K that are roots of monic polynomials with coefficients in $\mathbb{Z}$ (these numbers are called *algebraic integers*). Then O_K is a commutative ring which is called *the ring of integers of K*. In fact, according to the corollary to theorem 5 from [5] O_K is a Dedekind domain, i.e. it is an integral domain with the following properties:

i) O_K is a Noetherian ring;

ii) O_K is integrally closed in K;

iii) all non-zero prime ideals of O_K are maximal.

One of the basic properties of Dedekind domains is that every non-zero ideal can be written as a product of prime ideals (see Theorem 2 from [5]). Now if I is an ideal in O_K and $a \in K$ then we can look at $aI = \{ax | \ x \in I\}$. This is an O_K-submodule of K and is called a *fractional ideal* of K. Fractional ideals of the form aO_K, with $a \in K$, are called *principal* and denoted by (a). Clearly $(a)(b) = (ab)$. A fractional ideal A is called *invertible* if there is a fractional ideal B

such that $AB = O_K$. It turns out that all non-zero fractional ideals are invertible. In fact every non-zero fractional ideal A can be written uniquely as a product

$$A = \prod_{i=1}^{r} P_i^{r_i}$$

where $r_i \in \mathbb{Z}$ and the P_i's are distinct prime ideals of K. In particular, if $a \in K^*$ then

$$aO_K = \prod_{i=1}^{r} P_i^{r_i}.$$

For such a factorization we use the notation $ord_{P_i}(a)$ for the exponent r_i.

Now if we multiply two non-zero fractional ideals we get a non-zero fractional ideal. In this way, the set of non-zero fractional ideals of K forms an abelian group, denoted by I_0, with (1) serving as the neutral element. The set of all non-zero principal fractional ideals of K forms a subgroup of I_0 that will be denoted by P_0.

Definition 2.10. *The ideal class group of K is defined to be the group*

$$C_K = I_0/P_0.$$

The order of the ideal class group is denoted by h_K and is called the class number of K.

The ideal class group is always finite, so h_K is finite (see Corollary 2 to Theorem 35 from [9]).

If $p \in \mathbb{Z}$ is a non-zero integer then pO_K is an ideal in O_K, so it can be factored uniquely as

$$pO_K = P_1^{e_1} P_2^{e_2} ... P_g^{e_g}$$

with the P_i's distinct primes of K and the e_i's positive integers. The prime ideals P_i are precisely the prime ideals in K that contain pO_K. Each prime ideal P_i has finite index in O_K, so the field O_K/P_i is a finite field extension of $\mathbb{Z}/p\mathbb{Z}$ whose degree is denoted by $f_i = f(P_i|p)$ and is called the *inertial degree* of P_i over p. The exponent $e_i = e(P_i|p)$ is called the *ramification index* of P_i over p. The following identity holds:

$$\sum_{i=1}^{g} e_i f_i = n,$$

where $n = [K : \mathbb{Q}]$. When K is a normal extension of $\mathbb{Q}$, the Galois group $Gal(K|\mathbb{Q})$ acts transitively on the set of P_i's, so all primes lying over p have the same inertial degree (denoted by f) and the same ramification index (denoted by e), and the previous identity becomes:

$$efg = n.$$

If $e_1 = e_2 = ... = e_g$ then the prime p is called *unramified* in K. According to Corollary 3 to Theorem 24 from [9], all but finitely many prime integers are unramified in K.

A *valuation* of K is a map $v : K \to \mathbb{R} \cup \{\infty\}$ with the following properties:
i) $v(a) = \infty$ iff $a = 0$;
ii) $v(ab) = v(a) + v(b)$;
iii) $v(a + b) \geq inf\{v(a),\ v(b)\}$.

For every prime ideal P of K we can define a function $v_P : K^* \to \mathbb{Z}$ by

$$v_P(a) = ord_P(a).$$

Extend v_P to a function defined on K and denoted again by v_P, in the following way: $v_P(0) = \infty$. Then v_P is a valuation of K.

If λ is any positive number then any valuation v_P defines a new function $|\ |_P : K \to (0, \infty)$ in the following way:

$$|a|_P = \lambda^{-v_P(a)}.$$

This function is called an *absolute value* on K as it satisfies the condition of the following general definition:

Definition 2.11. *A function $|\ |$ from K to the set of non-negative real numbers is called an absolute value if for all a, b in K:*
i)$|a| = 0$ *iff* $a = 0$*;*
ii) $|ab| = |a||b|$*;*
iii) $|a + b| \leq |a| + |b|$.

If the last condition in the above definition is replaced by the stronger condition:
iii') $|a + b| \leq sup\{|a|, |b|\}$
then we call $|\ |$ an *ultrametric*.

An example of ultrametric on K is the *trivial* absolute value: $|a| = 0$ if $a = 0$, and $|a| = 1$ if $a \neq 0$.

If v is a valuation on K and λ is a positive number then the function defined by $|a|_v = \lambda^{v(a)}$ is an ultrametric on K (so it is an absolute value).

If the image of K^* under $|\ |$ is a discrete subgroup of $((0, \infty), \cdot)$ then $|\ |$ is called a *discrete absolute value*. In this case the image of K^* under $|\ |$ will be a cyclic subgroup of $((0, \infty), \cdot)$.

If $n = [K : \mathbb{Q}]$ then K has n embeddings into $\mathbb{C}$. Some of these embeddings may be real embeddings (and let r be the number of real embeddings) and the remaining are pairs of conjugate complex embeddings (and let s be the number of pairs of conjugate complex embeddings of K). Clearly $n = r + 2s$. The composition of the absolute value on $\mathbb{R}$ with each one of the real embeddings of K (if any) gives an absolute value on K, while the composition of the complex modulus with each one of the complex embeddings of K gives an absolute value on K. Two absolute values $|\ |_1$, $|\ |_2$ on K are called *equivalent* if there is a positive number α such that $|a|_1^\alpha = |a|_2$ for all $a \in K$. Any absolute value on K which is equivalent to the absolute value induced by a real or complex embedding of K is called *archimedian*. If an absolute value on K is not archimedian then it is called *non-archimedian*. We have seen that every non-zero prime ideal P in K defines a valuation on K which, for every positive number λ, induces an absolute value on K. The absolute value depends on the choice of the parameter λ, but different λ's induce equivalent absolute values on K. Consequently, we will not make a distinction between absolute values induced by the same valuation.

Any number field has n archimedian absolute values and any prime ideal in K induces a non-archimedian absolute value. Distinct prime ideals induce distinct absolute values, so we will often identify the prime ideal P with the absolute value $|\ |_P$ induced by P. For uniformity we will call the real and complex embeddings of K *infinite primes* in K and we will use the same

notation (P) for them, while the prime ideals will be *finite primes*. In the simple situation when $K = \mathbb{Q}$, Ostrowski's theorem describes all absolute values on K (see Theorem 9 [5]):

Theorem 2.12. *Let $|\ |$ be a non-trivial absolute value on $\mathbb{Q}$. Then $|\ |$ is equivalent to exactly one of either $|\ |_{\mathbb{R}}$ or $|\ |_p$ for some prime integer p.*

Here $|a|_p = p^{-v_p(a)}$ for all $a \in \mathbb{Q}$, where if $a = p^d a/b$ with $a, b \in \mathbb{Z}$ relatively prime to p then $v_p(a) = r$ (this is the so called *p-adic* absolute value on $\mathbb{Q}$).

Any valued field $(K, |\ |)$ has a completion which is a valued field $(K', |\ |')$ with the following properties (see Theorem 10 from [5]):
i) $|\ |'$ extends $|\ |$;
ii) K is dense in K';
iii) $(K', |\ |')$ is the smallest field with these two properties.
The completion of a valed field is unique up to an isomorphism of valued fields.

If p is a prime integer then the completion of $(\mathbb{Q}, |\ |_p)$ is denoted by $\mathbb{Q}_p$ and is called *the field of p-adic numbers*. Clearly, the completion of $\mathbb{Q}$ with the real absolute value is the field of real numbers.

If K is an arbitrary number field and P is a prime ideal in K then the completion $(K_P, |\ |_P)$ of $(K, |\ |_P)$ is a valued field extension of $(\mathbb{Q}_p, |\ |_p)$ (where p is the prime integer lying under P, i.e. the prime p such that $P \cap \mathbb{Z} = p\mathbb{Z}$). The "local" degree of the field extension is $[K_P : \mathbb{Q}_p] = e(P|p)f(P|p)$ (this follows from Theorem 15:3 [10])and for every $p \in \mathbb{Z}$ the sum of the local degrees equals the global degree n.

Now fix a prime P (finite or infinite) of K and consider the field K_P. If $a, b \in K_P^*$ we define the Hilbert symbol $(a, b)_P$ as being equal to 1 when $< a, b >$ represents 1 over K_P, and -1 otherwise. Note that if P is an infinite complex prime then the Hilbert symbol is always equal to 1, while if P is an infinite real prime then $(a, b)_P = -1$ iff $a < 0,\ b < 0$. In all cases, the Hilbert symbol has the following properties:

Proposition 2.13. *For any a,b in K_P^*:*

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

$$(a, bc)_P = (a, b)_P \cdot (a, c)_P,$$

and if $a \neq 1$ then

$$(a, 1 - a)_P = 1.$$

The Hilbert symbol has another important property (see 63:13 in [10]):

Proposition 2.14. *Given any non-square $b \in K_P^*$ there is $a \in K_P^*$ such that*

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

Finally, the following result (known as the *Hilbert reciprocity law*) holds (see Theorem 71:18 [10]):

Theorem 2.15. *Let a and b be two non-zero elements of an algebraic number field K. Then their Hilbert symbol equals 1 for almost all primes P, and*

$$\prod_P (a, b)_P = 1.$$

Chapter 3. Hilbert Symbol Equivalence of Algebraic Number Fields

3.1 Witt Equivalence

This chapter contains a synopsis of the state of knowledge before the dissertation.

The general problem that we want to discuss in this chapter is when two algebraic number fields have isomorphic Witt rings of quadratic forms. Let's consider two fields, K and L, of characteristic different than 2, that have isomorphic Witt rings, and let $\phi : W(K) \to W(L)$ be a ring isomorphism. In this case we say that K and L are *Witt equivalent*.

If two number fields are Witt equivalent (via a map ϕ) then ϕ maps I_K to I_L, I_K^2 to I_L^2, and I_K^3 to I_L^3, hence it induces group isomorphisms $t : I_K/I_K^2 \to I_L/I_L^2$ and $u : I_K^2/I_K^3 \to I_L^2/I_L^3$ that make the following diagram commutative:

$$\begin{array}{ccccc} I_K/I_K^2 & \times & I_K/I_K^2 & \longrightarrow & I_K^2/I_K^3 \\ t\downarrow & & \downarrow t & & \downarrow u \\ I_L/I_L^2 & \times & I_L/I_L^2 & \longrightarrow & I_L^2/I_L^3 \end{array} \tag{3.1}$$

As we have seen in the introduction, the discriminant gives canonical group isomorphisms $I_K/I_K^2 \to K^*/K^{*2}$ and $I_L/I_L^2 \to L^*/L^{*2}$, so the above diagram becomes:

$$\begin{array}{ccccc} K^*/K^{*2} & \times & K^*/K^{*2} & \longrightarrow & I_K^2/I_K^3 \\ t\downarrow & & \downarrow t & & \downarrow u \\ L^*/L^{*2} & \times & L^*/L^{*2} & \longrightarrow & I_L^2/I_L^3 \end{array} \tag{3.2}$$

where the horizontal maps send (a, b) to $< 1, -a > \otimes < 1, -b > \ (mod\ I^3)$.

A first solution to the problem of deciding when fields K and L are Witt equivalent was given by D. Harrison who found necessary and sufficient conditions for two number fields to be Witt equivalent. Here is Harrison's result:

Theorem 3.1. *[6] The following are equivalent:*
1. K and L are Witt equivalent.
2. There is a group isomorphism $t : I_K/I_K^2 \to I_L/I_L^2$ that sends -1 to -1, and a group isomorphism $u : I_K^2/I_K^3 \to I_L^2/I_L^3$ such that diagram 3.2 commutes.
3. There is a group isomorphism $t : I_K/I_K^2 \to I_L/I_L^2$ that sends -1 to -1, and the quadratic form $< a, b >$ represents 1 over K if and only if the quadratic form $< t(a), t(b) >$ represents 1 over L.

In [12] it is shown that any isomorphism of Witt rings induces canonically a map t between that square class groups of the two fields that satisfies condition (3) from Theorem 3.1, and any such map t induces an isomorphism between the Witt rings of the fields. These constructions are not inverse to each other.
Theorem 3.1 is very powerful, but it does not give explicit conditions in terms of the fields invariants.

In 1985 Perlis, Szymiczek, Conner, and Litherland defined a new concept that was related to the problem: *Hilbert symbol equivalence* (the initial terminology was *reciprocity equivalence*,

but it was changed by the authors in 1997). A Hilbert symbol equivalence between two number fields is a pair of maps (t, T), where

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

is a group isomorphism and

$$T : \Omega_K \to \Omega_L$$

is a bijection between the sets of primes of K and L respectively, such that the Hilbert symbols are preserved:

$$(a, b)_P = (t(a), t(b))_{T(P)}, \quad \forall P \in \Omega_K.$$

In [12] it is shown that two number fields are Witt equivalent if and only if they are Hilbert symbol equivalent. It is also shown the existence of a local-global principle:

Theorem 3.2. *Two number fields are Witt equivalent if and only if their primes can be paired so that the corresponding completions are Witt equivalent.*

The two maps that form a Hilbert symbol equivalence are not independent to each other. In fact there is a very strong correlation between them: in [11] it is shown that if (t, T) is a Hilbert symbol equivalence then the map t determines T up to the action on complex primes, and vice-versa, the map T determines t. In fact a stronger result holds:

Theorem 3.3. *If (t_1, T_1) and (t_2, T_2) are two Hilbert symbol equivalences between two number fields such that T_1 and T_2 agree on a set of primes of positive density then $t_1 = t_2$ and T_1 and T_2 may differ only at complex primes.*

We conclude this section with the following result from [12]:

Proposition 3.4. *If (t,T) is a Hilbert-symbol equivalence then T maps real primes to real primes, non-archimedian primes to non-archimedian primes, and dyadic primes to dyadic primes.*

3.2 Tame and Wild Primes

In this section we will define and present background information concerning a refinement of the concept of Hilbert symbol equivalence. The next chapter is entirely dedicated to this topic. Let (t, T) be a Hilbert symbol equivalence between two number fields K and L. If P is an arbitrary prime of K the square class group K_P^*/K_P^{*2} of the completion of K with respect to P is a vector space over $\mathbb{F}_2$ (the field with 2 elements) of dimension:

$$\begin{cases} 0, & \text{if } P \text{ is complex;} \\ 1, & \text{if } P \text{ is real;} \\ 2, & \text{if } P \text{ is non-archimedian and non-dyadic;} \\ d+2, & \text{if } P \text{ is dyadic} \end{cases}$$

where d is the degree of K_P over $\mathbb{Q}_2$.

Definition 3.5. *A non-archimedian prime P of K is called tame if*

$$ord_P(a) \equiv ord_{T(P)}(t(a)) \pmod 2$$

for any square class a.

A non-archimedian prime that is not tame is called *wild*.

It turns out that when P is a finite non-dyadic prime and when -1 is not a local square at P then the local square-class map is forced to be tame. So wild prime P can only occur at finite non-dyadic primes at which $-\bar{1} = \bar{1}$, or at dyadic primes.

3.3 Small Equivalence

The concept of Hilbert symbol equivalence made it easier to understand when two number fields have isomorphic Witt rings. In [12] it is shown that two number fields are Witt equivalent if and only if they are Hilbert symbol equivalent. In fact if two number fields have isomorphic Witt rings, there may be different Hilbert symbols equivalences between them. A natural question is how to construct Hilbert symbol equivalences between two Witt equivalent number fields. In [12] the authors showed how to construct a Hilbert symbol equivalence if a certain object called *small equivalence* was given. A small equivalence consists of:

1. A bijection T between a sufficiently large set S of primes in K and a sufficiently large set $T(S)$ of primes in L (where a sufficiently large set of primes S consists of finitely many elements such that the class number of the ring of S-integers is odd).
2. A group isomorphism t_S between the square class groups of the groups of S-units of K and L.
3. For each $P \in S$ a Hilbert symbol preserving group isomoprphism t_P between the square class groups of the completions of K and L with respect to P (K_P^*/K_P^{*2}) and to $T(P)$ $((L_{TP}^*/L_{TP}^{*2}))$ respectively.
4. A commutative diagram:

$$\begin{array}{ccc} U_K^S/(U_K^S)^2 & \longrightarrow & \prod_{P\in S} K_P^*/K_P^{*2} \\ t_S \downarrow & & \downarrow \prod_{P\in S} t_P \\ U_L^{T(S)}/(U_L^{T(S)})^2 & \longrightarrow & \prod_{P\in S} L_{T(P)}^*/L_{T(P)}^{*2} \end{array}$$

where $U_K^S/(U_K^S)^2$ is the square class group of the group of S-units in K and $U_L^{T(S)}/(U_L^{T(S)})^2$ is the square class group of the group of $T(S)$-units in L.

They presented a method of extending any small equivalence to a Hilbert symbol equivalence and proved the following theorem:

Theorem 3.6. *Any small equivalence between two Witt equivalent number fields can be extended tamely to a Hilbert symbol equivalence.*

The existence of a small equivalence is rather difficult to prove directly. In 1992 J. Carpenter (see [1]) gave an alternative set of conditions:

Theorem 3.7. *There is a small equivalence (and thus a Hilbert symbol equivalence) between two number fields K and L if and only if:*
1. -1 is a square in both K and L or in neither;
2. K and L have the same number of real primes;
3. there is a bijection between the dyadic primes of K and L such that the corresponding dyadic completions have the same local degree over $\mathbb{Q}_2$ and the same level.

The following result was proved in [14]:

Theorem 3.8. *Two number fields K and L are Hilbert symbol equivalent if and only if:*
1. K and L have the same level ;
2. K and L have the same number of real primes;
3. there is a bijection between the dyadic primes of K and L such that the corresponding dyadic completions have the same local degree over $\mathbb{Q}_2$ and the same level.

The following result is also true:

Theorem 3.9. *Two number fields are Hilbert symbol equivalent if and only if there exists a small equivalence between them.*

Concerning the property of being a tame prime a few natural questions were raised:
1. Are there Hilbert symbol equivalences that have finitely many wild primes?
The answer was given by J. Carpenter in [1]. She proved that *any* Hilbert symbol equivalence can be replaced by a Hilbert symbol equivalence that is tame outside a finite set. The following result (Theorem 2 from [12]) emphasizes a strong connection with small equivalences:

Theorem 3.10. *A small equivalence with set S between number fields K and L can be extended to a Hilbert symbol equivalence that is tame outside S.*

The existence of a small equivalence between two number fields is equivalent to the existence of a Hilbert symbol equivalence that is tame outside a finite set (see Corollary 3 from [12]).
2. Are there Hilbert symbol equivalences that have infinitely many wild primes?
The answer is "yes", and it was given by T. Palfrey in [11].
3. How small can the wild set be?
In [2] the authors give a lower bound for the size of the wild set:

Proposition 3.11. *Let (t,T) be a Hilbert symbol equivalence between number fields K and L with finite wild set W. Let S be any finite subset of primes of K that contains all archimedian primes. Then:*

$$|rk_2C_K(S) - rk_2C_L(T(S))| \leq |W \setminus S|$$

and

$$|rk_2C_K^+(S) - rk_2C_L^+(T(S))| \leq |W \setminus S|.$$

In particular, by taking $S = S_\infty$ to be the set of archimedian primes of K,

$$|rk_2C_K - rk_2C_L| \leq |W|$$

and

$$|rk_2C_K^+ - rk_2C_L^+| \leq |W|.$$

The following chapter is devoted entirely to answering question 3 above. We are able to provide an exact formula for the minimum number of wild primes that any Hilbert symbol equivalence between two number fields can have. Our result involves the difference in 2-ranks of the ideal S-class groups, but we will see that an extra term shows up in the formula.
4. How can one describe the situation when the wild set of a Hilbert symbol equivalence is empty? (this type of equivalence is called *tame*).
First we need to point out that the previous observations lead to the following

Corollary 3.12. *([2]) If K and L are tamely Hilbert symbol equivalent, then*

$$C_K/C_K^2 \simeq C_L/C_L^2.$$

In the quadratic case, an extensive study of this situation can be found in [4]. The author characterizes tame Hilbert symbol equivalence of quadratic number fields by a set of 10 conditions. In the general case, the problem is open.

5. How many classes of tamely Hilbert symbol equivalent number fields of a certain degree are? The answer in the case of quadratic number fields is due to A. Czogala (see [4]): while every quadratic number field is Hilbert symbol equivalent to one of the following seven number fields:

$$\mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{\pm 2}),\ \mathbb{Q}(\sqrt{\pm 7}),\ \mathbb{Q}(\sqrt{\pm 17}),$$

there are infinitely many classes of tamely Hilbert symbol equivalent quadratic number fields. No answer is known in the general case.

Chapter 4. The Main Results

4.1 Definitions and Notations

From now on, K and L will denote two algebraic number fields that are Hilbert symbol equivalent.

As before we will denote by r the number of real embeddings of K, and by s the number of pairs of complex embeddings of K. Similarly, r' and s' are the corresponding notations for L.

We denote by Ω_K the set of primes of K, by Ω_L the set of primes of L, and let

$$S = \{P_1, P_2, ..., P_n\} \subset \Omega_K$$

be a finite set of primes of K that contains all archimedian primes of K. When S also contains all dyadic primes of K, we will say S is decent.

By O_K^* we denote the group of units of O_K. If the set S is defined as above, we denote by $O_K(S)$ the ring of S-integers of O_K. More precisely,

$$O_K(S) = \{x \in K : \ ord_P(x) \geq 0, \ \forall P \notin S\}.$$

The units of the ring of S-integers are called the S-units of K, and they form a multiplicative group $O_K^*(S)$. An element $x \in K$ is in $O_K^*(S)$ if and only if

$$ord_P(x) = 0, \ \forall P \notin S.$$

Clearly, if $S_1 \subseteq S_2$ then $O_K(S_1) \subseteq O_K(S_2)$ and $O_K^*(S_1) \subseteq O_K^*(S_2)$. In particular, $O_K \subset O_K(S)$ and $O_K^* \subset O_K^*(S)$ for any finite set of primes S chosen as above.

We denote by C_K the ideal class group of K, and by $\rho = rk_2(C_K)$ its 2-rank.

Let $C_K(S)$ be the S-class group of K:

$$C_K(S) = C_K/H_K(S),$$

where $H_K(S)$ is the subgroup of C_K generated by the classes of the ideals in S.
Equivalently, $C_K(S)$ consists of the S-classes of integral ideals in K, where two integral ideals I and J are in the same S-class if there exist S-integers x and y such that $xI = yJ$. We will denote by $\theta(S)$ the 2-rank of $rk_2(H(S))$. Observe that $\theta(S)$ is the dimension over $\mathbb{F}_2$ of the subspace of C_K/C_K^2 generated by the cosets of ideal classes of primes in S and $rk_2(C_K(S)) = \rho - \theta(S)$. We may assume that the primes in S are numbered so that $P_1, \ ..., \ P_{\theta(S)}$ are linearly independent in C_K/C_K^2.

We will denote by $C_{K,2}(S)$ the 2-primary subgroup of $C_K(S)$, which consists of all elements in $C_K(S)$ of order equal to 2.

The image of an ideal I of K in any of the above ideal class groups will be denoted by $[I]$.

The following notations (which generalize some objects defined in [4]) will be used throughout this chapter:

$$K_0(S) = \{x \in K^* : \ ord_P(x) \equiv 0 \ (mod \ 2), \ \forall P \in \Omega_K \setminus S\}$$

$$K_{ev} = \{x \in K^* : \ ord_P(x) \equiv 0 \ (mod \ 2), \ \forall P \text{ non-archimedian}\}$$

$$K_{sq}(S) = \{x \in K_0(S) : \ x \in K_P^{*2}, \ \forall P \in S\}$$
$$U_K(S) = \{\bar{x} \in K^*/K^{*2} : \ x \in O_K^*(S)\}$$
$$E_K(S) = \{\bar{x} \in K^*/K^{*2} : \ ord_P(x) \equiv 0 \ (mod\ 2), \ \forall P \notin S\}$$
$$G_K(S) = \prod_{P \in S} K_P^*/K_P^{*2}.$$

The following inclusions hold:

$$K^{*2} \subset K_{sq}(S) \subset K_{ev} \subset K_0(S).$$

4.2 Preliminary Results

Lemma 4.1. *1. $U_K(S)$ is a subgroup of $E_K(S)$.*
2. $U_K(S)$ is a finite abelian 2-group of order $2^{|S|}$. Hence

$$rk_2(U_K(S)) = |S|.$$

3. There is an exact sequence:

$$1 \to U_K(S) \to E_K(S) \to C_{K,2}(S) \to 1.$$

Proof. 1. Obvious.
2. By Dirichlet's unit theorem:

$$O_K^*(S) \simeq W_K(S) \times Z^{|S|-1}$$

where $W_K(S)$ is a cyclic group of finite even order. Then:

$$|O_K^*(S)/O_K^*(S)^2| = 2^{|S|}$$

and the claim follows from the observation that $O_K^*(S)/O_K^*(S)^2 \simeq U_K(S)$.
3. Let $\bar{x} \in E_K(S)$. Then:

$$xO_K = Q_1^{2\alpha_1} Q_2^{2\alpha_2} ... Q_r^{2\alpha_r} P_1^{\beta_1} ... P_n^{\beta_n},$$

with $\alpha_1, \ ..., \ \alpha_r, \ \beta_1, \ ..., \ \beta_n \in \mathbb{Z}$, and $Q_1, \ ..., \ Q_r$ outside S. Define a map:

$$\Psi_S : E_K(S) \to C_{K,2}(S)$$

by

$$\Psi_S(\bar{x}) = [Q_1]^{\alpha_1} [Q_2]^{\alpha_2} ... [Q_r]^{\alpha_r}.$$

Clearly, Ψ_S is a well-defined map, and a group homomorphism. Moreover,

$$Ker(\Psi_S) = U_K(S), \quad Im(\Psi_S) \leq C_{K,2}(S).$$

To see that Ψ_S is in fact surjective, note that if $[Q_1]^{\alpha_1} [Q_2]^{\alpha_2} ... [Q_r]^{\alpha_r} \in C_{K,2}(S)$ then

$$([Q_1]^{\alpha_1} [Q_2]^{\alpha_2} ... [Q_r]^{\alpha_r})^2 = 1$$

in $C_K(S)$, hence one can find $\alpha_1', \ ..., \ \alpha_r', \ \beta_1, \ ..., \ \beta_n \in \mathbb{Z}$ and $x \in K$ such that

$$xO_K = Q_1^{2\alpha_1'} Q_2^{2\alpha_2'} ... Q_r^{2\alpha_r'} P_1^{\beta_1} ... P_n^{\beta_n},$$

which means that $\bar{x} \in E_K(S)$. $\square$

Corollary 4.2. $rk_2(E_K(S)) = |S| + rk_2(C_K(S))$

Proof. The equality follows directly from Lemma 4.1 (parts 2 and 3) and the fact that $rk_2(C_{K,2}(S)) = rk_2(C_K(S))$. □

Let S be a set of primes of K containing the archimedian and dyadic primes, and let P be a prime outside S. Let $S_1 = S \cup \{P\}$. Denote by $cl_S(P)$ the class of P in $C_K(S)/C_K(S)^2$.

Lemma 4.3. *1.* $E_K(S) \leq E_K(S_1)$.
2. $E_K(S) = E_K(S_1)$ *if and only if* $cl_S(P) \neq 1$.
3. $[E_K(S_1) : E_K(S)] = 2$ *if and only if* $cl_S(P) = 1$. *In this case, if we define* $\Phi : E_K(S_1) \to \mathbb{Z}/2\mathbb{Z}$ *by*

$$\Phi(\bar{x}) = ord_P(x) \ (mod\ 2),$$

there is a short exact sequence:

$$1 \to E_K(S) \to E_K(S_1) \to Z/2Z \to 0.$$

Proof. 1. Obvious.
2, 3. Note that $cl_S(P) = 1$ if and only if there exists $x^* \in K$ such that

$$P = x^* Q_1^{2\alpha_1} Q_2^{2\alpha_2} ... Q_j^{2\alpha_j} P_1^{\beta_1} ... P_l^{\beta_l}.$$

This is equivalent to the existence of an element $\bar{x^*} \in E_K(S_1)$ such that $ord_P(\bar{x^*}) = 1$ $(mod\ 2)$. But that means that there exists an element $x^* \in K$ which is a uniformizer locally at P and such that $\bar{x^*} \in E_K(S_1)$. In other words, $cl_S(P) = 1$ if and only if $E_K(S_1) \setminus E_K(S)$ is non-empty.

On the other hand, it follows from Corollary 4.2 that $[E_K(S_1) : E_K(S)] \leq 2$ since $|S_1| = |S|+1$ and $rk_2(C_K(S_1)) \leq rk_2(C_K(S))$. Consequently, $cl_S(P) = 1$ if and only if $[E_K(S_1) : E_K(S)] = 2$. The sequence is exact: Φ is well-defined, the kernel of Φ consists of those elements of $E_K(S_1)$ that are local units at P, i.e. are in $E_K(S)$, and Φ is onto $\mathbb{Z}/\mathbb{Z}_2$ for it maps the element $x^* \in K$ to 1. □

Lemma 4.4. *1.* $rk_2(C_K(S_1)) = rk_2(C_K(S))$ *if and only if* $cl_S(P) = 1$.
2. $rk_2(C_K(S_1)) = rk_2(C_K(S)) - 1$ *if and only if* $cl_S(P) \neq 1$.

Proof. The results are direct consequences of Lemma 4.3 and Corollary 4.2. □

Definition 4.5. *Let F be an algebraic number field. A finite subset S of Ω_F is called decent if S contains all archimedian and all dyadic primes of F.*

Definition 4.6. *A system $(S, S', T, (t_P)_{P \in S})$ consisting of:*
1. a pair of decent sets: $S \subset \Omega_K$ and $S' \subset \Omega_L$;
2. a bijection $T : S \to S'$;
3. for any prime $P \in S$ a local isomorphism,

$$t_P : (K_P^*)/(K_P^*)^2 \to (L_{TP}^*)/(L_{TP}^*)^2$$

such that

$$(a, b)_P = (t_P(a), t_P(b))_{TP}, \quad \forall a, b \in (K_P^*)/(K_P^*)^2$$

is called a correspondence between K and L.

Remark 4.7. *If $(S, S', T, (t_P)_{P\in S})$ is a correspondence between K and L then the map*

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

is a group isomorphism $t_S : G_K(S) \to G_L(S')$.

Define now the following map:

$$\nu_S = \nu_K(S) : E_K(S) \to G_K(S)$$

by

$$\nu_S(\bar{x}) = (x_{P_1}, x_{P_2}, ..., x_{P_n}) = (x)_S$$

where, for any $P \in S$, x_P denotes the image of the global square class $\bar{x}$ in $(K_P^*)/(K_P^*)^2$.
This map is well-defined. Let $\omega_K(S)$ denote the image $Im(\nu_S)$.

The following two result turns out to be very important in describing the 2-rank of the kernel and the image of ν_S.

Theorem 4.8. *([7], Theorem 169) Let $\mu_1, \mu_2, ..., \mu_m$ be integers in K such that a product of powers $\mu_1^{x_1}...\mu_m^{x_m}$ is the square of a number in K only if all exponents $x_1, ..., x_m$ are even. Let $c_1, ..., c_m$ be arbitrary values ± 1. Then there are infinitely many prime ideals P in K which satisfy the m conditions*

$$(\frac{\mu_1}{P}) = c_1, ..., \ (\frac{\mu_m}{P}) = c_m.$$

Before we continue our investigation, we would like to present an obvious generalization of a result due to Czogala (see [4]):

Corollary 4.9. *Suppose $b_1, ..., b_l \in K_{sq}(S)$ are linearly independent in $K_{sq}(S)/K^{*2}$ and let $R_1, ..., R_l$ be primes outside S, in K, such that*

$$(\frac{b_i}{R_i}) = -1, \quad (\frac{b_j}{R_i}) = 1, \quad \forall i \neq j \in \{1, ..., l\}.$$

Then the classes $[R_1], ..., [R_l]$ are linearly independent in C_K/C_K^2, and so are $[P_1], ..., [P_{\theta(S)}], [R_1], ..., [R_l]$.

Lemma 4.10. *1. $rk_2(Ker(\nu_S)) = rk_2(C_K(S))$.*
2. $rk_2(\omega_K(S)) = |S|$.

Proof. Regard $G_K(S)$ as an $\mathbb{F}_2$-inner product space, with the inner product B defined as the product of Hilbert symbols:

$$B((x)_S, (y)_S) = \prod_{P\in S} (x_P, y_P)_P.$$

According to [1], $rk_2(G_K(S)) = 2|S|$. Note that ω_S is a totally isotropic subspace of $G_K(S)$. To prove this we see that for any prime $P \notin S$, any elements $\bar{x}$, $\bar{y}$ in $E_K(S)$ map to local units at P, so the Hilbert symbol satisfies $(x, y)_P = 1$. Then:

$$1 = \prod_{P\in\Omega_K} (x, y)_P = B((x)_S, (y)_S) \cdot 1 = B((x)_S, (y)_S).$$

According to Corollary 4.4 page 16 from [8],

$$rk_2(\omega_K(S)) \leq \frac{1}{2} \cdot rk_2(G_K(S)) = |S|.$$

Now since $E_K(S)$ is a group of exponent 2, it can be regarded as an $\mathbb{F}_2$-vector space. Since $Ker(\nu_S)$ is a subgroup of $E_K(S)$, it can be regarded as a subspace of $E_K(S)$. Fix $\{\bar{x}_1, ..., \bar{x}_q\}$ an F_2-basis for $Ker(\nu_S)$. If we use repeatedly Theorem 4.8, we can find primes $Q_1, ..., Q_q$ outside S such that $\bar{x}_i$ is a local square at Q_j, $\forall j \neq i$, and $\bar{x}_i$ is a local non-square unit at Q_i, $\forall i \in \{1, ..., q\}$. If the ideal classes of Q_i were linearly dependent in C_K/C_K^2 then we would get a relation of the form

$$xO_K = Q_1...Q_l J^2$$

for some $x \in K$ (after renumbering the ideals if necessary). But then x is a local uniformizer at Q_1 and x_1 is a local non-square unit at Q_1, hence $(x, x_1)_{Q_1} = -1$, while $(x, x_1)_Q = 1,\ \forall Q \neq Q_1$ because when $Q \notin \{Q_2,\ ...,\ Q_l\}$ both x and x_1 are local units at Q and when $Q = Q_i$ for some $i \neq 1$, x_1 is a local square at Q. This contradicts Hilbert's reciprocity law.
Hence $[Q_1], ..., [Q_q]$ are linearly independent in $C_K(S)/C_K(S)^2$, which implies:

$$rk_2(Ker(\nu_S)) \leq rk_2(C_K(S)).$$

Finally,

$$|S| + rk_2(C_K(S)) = rk_2(E_K(S)) = rk_2(Ker(\nu_S)) + rk_2(\omega_K(S)) \leq rk_2(C_K(S)) + |S|$$

which proves both parts of the lemma. □

If $(S, S', T, (t_P)_{P \in S})$ is a correspondence, define

$$H_S = \{(x)_S \in \omega_K(S) :\ t_S((x)_S) \in \omega_L(S')\}$$

and

$$H_{S'} = \{(x)_{S'} \in \omega_L(S') :\ t_{S'}((x)_{S'}) \in \omega_K(S)\}.$$

Observe that H_S is a subgroup of $\omega_K(S)$ and $H_{S'}$ is a subgroup of $\omega_L(S')$.

Definition 4.11. *If $\mathcal{C} = (S, S', T, (t_P)_{P \in S})$ is a correspondence, we define the defect of $\mathcal{C}$ to be the number $\delta = \delta_{\mathcal{C}}$ given by*

$$\delta_{\mathcal{C}} = rk_2(\omega_K(S)/H_S).$$

The $\delta = rk_2(\omega_K(S)) - rk_2(H_S)$ and thus, according to Lemma 4.10,

$$\delta = |S| - rk_2(H_S).$$

Let us note that since t_S induces a group isomorphism between H_S and $H_{S'}$, the defect of the correspondence can be also expressed as

$$\delta = rk_2(\omega_L(S')/H_{S'}).$$

At this point we wish to relate the defect of a correspondence to another invariant, $d_{S,S'}$, called the *obstruction* in J. Carpenter's paper [1]. In that paper, she studies a correspondence

$(S, S', T, (t_P)_{P\in S})$ with the additional assumption that both class numbers $h_K(S)$ and $h_L(S')$ are odd. She notationally supresses the maps T and $(t_P)_{P\in S}$ and refers to such a correspondence as a *suitable pair* (S, S'). We wish to observe that when $\mathcal{C} = (S, S')$ is a suitable pair, then the defect $\delta_{\mathcal{C}}$ is exactly the same as the defect of the pair $d_{S,S'}$. The details are as follows.

Consider the restriction of the map ν_S to $U_K(S)$, denoted by i_S. This map is studied in [1]. J. Carpenter proves that, when the class number $h_K(S)$ is odd, i_S is a group monomorphism, and thus

$$rk_2(i_S(U_K(S))) = rk_2(U_K(S)) = |S|.$$

This observation combined with Lemma 4.10 shows that

$$rk_2(i_S(U_K(S))) = rk_2(\omega_K(S)).$$

On the other hand,

$$i_S(U_K(S)) = \nu_S(U_K(S)) \subseteq \nu_S(E_K(S)) = \omega_K(S)$$

which imply

$$i_S(U_K(S)) = \omega_K(S).$$

In [1] one defines

$$\bar{H}_S = \{x \in U_K(S) :\ t_S(i_S(x)) \in i_{S'}(U_L(S'))\}.$$

Note that if $x \in \bar{H}_S$ then $\nu_S(x) = i_S(x)$ has the property that $t_S(i_S(x)) \in i_{S'}(U_L(S')) = \omega_L(S')$, which implies that $i_S(x) \in H_S$. Hence $i_S(\bar{H}_S) \subseteq H_S$.
On the other hand, if $(x)_S \in H_S$ then $(x)_S \in \omega_K(S) = i_S(U_K(S))$ which means that actually $(x)_S \in i_S(\bar{H}_S)$. This observations prove:

Lemma 4.12. *$i_S(\bar{H}_S) = H_S$.*

J. Carpenter defines the ostruction of a suitable pair (S, S') in the following way:

$$d_{S,S'} = dim_{F_2}(U_K(S)/\bar{H}_S).$$

Since the groups involved in the definition of the obstruction are finite and have the exponent equal to 2,

$$d_{S,S'} = rk_2(U_K(S)/\bar{H}_S) = rk_2(U_K(S)) - rk_2(\bar{H}_S) =$$
$$= rk_2(i_S(U_K(S))) - rk_2(i_S(\bar{H}_S)) = rk_2(\omega_K(S)) - rk_2(H_S) = \delta.$$

Remark 4.13. *The above equalities show that when both class numbers $h_K(S)$ and $h_L(S')$ are odd, the defect and the obstruction coincide.*

Lemma 4.14. *([1]) Given a suitable correspondence involving (S, S') with $d_{S,S'} > 0$, there exist primes $P_{n+1} \in \Omega_K \setminus S$ and $P'_{n+1} \in \Omega_L \setminus S'$ such that $(S_1 = S \cup \{P_{n+1}\}, S'_1 = S' \cup \{P'_{n+1}\})$ is also a suitable pair for K and L and*

$$d_{S_1,S'_1} < d_{S,S'}.$$

A consequence of the above "obstruction-killing lemma" is the fact that any suitable correspondence between K and L can be extended to a small equivalence between K and L. Since any small equivalence can be extended to a Hilbert symbol equivalence between K and L which is tame outside the sets that define the small equivalence, it follows that the only wild primes in

K (if any), outside S, of the Hilbert symbol equivalence are among the primes that are adjoined by the procedure described in the proof of the obstruction-killing lemma. We recall here that J. Carpenter's procedure presented in [1] shows that:

- all the primes adjoined to S are wild;
- the number of such primes does not exceed $d_{S,S'}$.

This ends our digression. We now return to the study of the defect $\delta_{\mathcal{C}}$ of an arbitrary correspondence $\mathcal{C}$ and we no longer assume anything about the parity of $h_K(S)$ and $h_L(S')$. We shall prove now that no matter how we extend the correspondence $\mathcal{C}$ by adding a pair of primes (P_{n+1}, P'_{n+1}) subject to the restriction that -1 is a local square at P_{n+1} iff -1 is a local square at P'_{n+1}, the defect decreases by at most 1. Let $S_1 = S \cup \{P_{n+1}\}$ and $S'_1 = S' \cup \{P'_{n+1}\}$. Let $\mathcal{C}' = (S_1, S'_1, T', (t_P)_{P \in S'})$ be an extension of $\mathcal{C}$. Denote by δ_1 the defect of $\mathcal{C}'$.

Before we continue we will define the following subgroups:

$$F_S = \{(x)_{S_1} : \ x_{P_{n+1}} = 1\}$$

and

$$F_{S'} = \{(y)_{S'_1} : \ y_{P'_{n+1}} = 1\}.$$

Then F_S is a subgroup of H_{S_1} and $F_{S'}$ is a subgroup of $H_{S'_1}$.

Proposition 4.15. *Suppose P_{n+1} is tame. In the above notations,*

$$\delta_1 \geq \delta.$$

Proof. We will consider two cases:
Case 1. At least one of $[P_{n+1}]$ and $[P'_{n+1}]$ is a non-square in the corresponding ideal S-class group.
Case 2. Both $[P_{n+1}]$ and $[P'_{n+1}]$ are squares in the corresponding ideal S-class groups.
Suppose we are in Case 1 and let's say that $[P_{n+1}]$ is not a square in $C_K(S)$. Then, by Lemma 4.3, we get $E_K(S_1) = E_K(S)$. Any element $(x)_{S_1} \in H_{S_1}$ has $x_{P_{n+1}}$ a unit.
By hypothesis, P_{n+1} is tame so $t_{P_{n+1}}(x_{P_{n+1}})$ is a unit. Define $\bar{y} \in E_L(S')$ by $\bar{y} = (t_P(x_P))_{P \in S_1}$. Hence we get a well-defined map $\lambda_S : H_{S_1} \to H_S$ defined by $\lambda_S((x)_{S_1}) = (x)_S$. Moreover, there is a short exact sequence:

$$1 \to Ker(\lambda_S) \to H_{S_1} \to Im(\lambda_S) \to 1 \tag{4.1}$$

hence

$$rk_2(H_{S_1}) = rk_2(Ker(\lambda_S)) + rk_2(Im(\lambda_S)). \tag{4.2}$$

Then

$$\delta_1 = |S| + 1 - rk_2(Ker(\lambda_S)) - rk_2(Im(\lambda_S)). \tag{4.3}$$

We need to study the properties of the map λ_S. They are presented in Lemma 4.16.

Lemma 4.16. *Suppose that one extends tamely a correspondence (C) by adding a pair of primes such that at least one of them is not a square in the corresponding ideal S-class group.*
1. If λ_S is not injective then $Ker(\lambda_S) \simeq C_2$, hence $rk_2(Ker(\lambda_S)) = 1$.
2. If λ_S is not surjective then $[H_S : Im(\lambda_S)] = 2$.
3. If λ_S is not injective then it is surjective.

According to 4.3, if λ_S is injective then

$$\delta_1 = |S| + 1 - rk_2(Im(\lambda_S)) \geq |S| + 1 - rk_2(H_S) = \delta + 1 > \delta.$$

Thus $\delta_1 \geq \delta$.

On the other hand, if λ_S is not injective, then by Lemma 4.16 it is surjective and according to 4.3

$$\delta_1 = |S| + 1 - 1 - rk_2(H_S) = \delta,$$

so $\delta_1 \geq \delta$ in this case as well. This completes the study of the first case.

Suppose now that we are in Case 2, so both $[P_{n+1}]$ and $[P'_{n+1}]$ are squares in the corresponding ideal S-class groups. Then, by Lemma 4.3, we get:

$$E_K(S_1) = E_K(S) \ \cup \ \bar{x}_0 E_K(S)$$

for some $\bar{x}_0 \in E_K(S_1) \setminus E_K(S)$, and

$$E_L(S'_1) = E_L(S') \ \cup \ \bar{y}_0 E_L(S')$$

for some $\bar{y}_0 \in E_L(S'_1) \setminus E_L(S')$.
Since $\bar{x}_0 \in E_K(S_1) \setminus E_K(S)$, $(x_0)_{P_{n+1}} =$ is a non-unit, and $(y_0)_{P'_{n+1}}$ is a non-unit as $\bar{y}_0 \in E_L(S'_1) \setminus E_L(S')$.
Define the following set:

$$J_S = \{(x)_{S_1} \in H_{S_1} : \ x_{P_{n+1}} \text{ is a unit}\}.$$

J_S is a subgroup of H_{S_1}.

We claim that if $(x)_{S_1} \in J_S$ then $(x)_S \in H_S$. To prove the claim, observe that by the definition of H_{S_1} we can find $\bar{y} \in E_L(S'_1)$ such that

$$(y)_S = t_S((x)_S), \quad y_{P'_{n+1}} = t_{P_{n+1}}(x_{P_{n+1}}).$$

By hypothesis P_{n+1} is tame, so $y_{P_{n+1}}$ is a unit. Then $\bar{y} \in E_L(S')$ and since $\bar{x} \in E_K(S)$, it follows that $(x)_S \in H_S$.
Then the map $\lambda_S : H_{S_1} \to H_S$ defined by $\lambda_S((x)_{S_1}) = (x)_S$ is a well defined group homomorphism.

Now we will consider two subcases:
Subcase 2.1. There exists an element $(x^*)_{S_1} \in H_{S_1}$ such that $x^*_{P_{n+1}}$ is the square class of a non-unit. Since P_{n+1} is tame, one can find an element $(y^*)_{S'_1} \in H_{S'_1}$ such that $y^*_{P'_{n+1}}$ is the square class of a non-unit (and $t_{P_{n+1}}(x^*_{n+1}) = y^*_{n+1}$). Without loss of generality we can replace $\bar{x}_0$ by $\bar{x}^*$ and $\bar{y}_0$ by $\bar{y}^*$.

Then

$$H_{S_1} = J_S \ \cup \ (x^*)_{S_1} J_S$$

so

$$rk_2(H_{S_1}) = rk_2(J_S) + 1. \tag{4.4}$$

Claim: λ_S is injective. Indeed, if $(1, \ ..., \ 1, \ a) \in Ker(\lambda_S)$ and $(1, \ ..., \ 1, \ a) \neq (1, \ ..., \ 1, \ 1)$ then a is the square class of a non-square unit. Pick $\bar{a} \in E_K(S_1)$ such that $\nu_{S_1}(\bar{a}) = (1, \ ..., \ 1, \ a)$. Then

$(\bar{a}, \bar{x}^*)_P = 1$ for all $P \neq P_{n+1}$ and $(\bar{a}, \bar{x}^*)_{P_{n+1}} = -1$, and that contradicts Hilbert's reciprocity law.

Since λ_S is injective, $rk_2(J_S) \leq rk_2(H_S)$ and if we use 4.4 we get:

$$\delta_1 = |S| + 1 - rk_2(H_{S_1}) = |S| + 1 - rk_2(J_S) - 1 \geq |S| - rk_2(H_S) = \delta,$$

which proves the inequality.

Subcase 2.2. There are no elements $(x)_{S_1} \in H_{S_1}$ such that $x_{P_{n+1}}$ is a non-unit. Then, $J_S = H_{S_1}$. If λ_S is injective then $rk_2(J_S) \leq rk_2(H_S)$ hence

$$\delta_1 = |S| + 1 - rk_2(H_{S_1}) = |S| + 1 - rk_2(J_S) \geq |S| + 1 - rk_2(H_S) \geq \delta + 1,$$

so the inequality $\delta_1 \geq \delta$ holds.

If λ_S is not injective, then pick $\bar{a} \in E_K(S_1)$ with $\nu_{S_1}(\bar{a}) = (1,\ ...,\ 1,\ u) \in J_S$. We claim that in this situation λ_S is surjective. Indeed, if $(x)_S \in H_S$, let $\bar{x} \in E_K(S)$ and $\bar{y} \in E_L(S')$ such that $\nu_S(\bar{x}) = (x)_S$ and $\nu_{S'}(\bar{y}) = t_S((x)_S)$. Since $E_K(S) \subset E_K S_1$, $\bar{x} \in E_K(S_1)$. If $x_{P_{n+1}} \neq y_{P'_{n+1}}$ then $x_{P_{n+1}} a = y_{P'_{n+1}}$ and thus $\bar{x}\bar{a} \in E_K S_1$ and $\nu_{S_1}(\bar{x}\bar{a}) \in J_S$ is such that $\lambda_S(\nu_{S_1}(\bar{x}\bar{a})) = (x)_S$. So λ_S is surjective.

Since λ_S is surjective we get $rk_2(J_S) = rk_2(H_S) + rk_2(Ker(\lambda_S))$. Thus, since λ_S is not injective, $Ker(\lambda_S)$ is a cyclic group with 2 elements (generated by $(1,\ ...,\ 1,\ u)$) hence $rk_2(J_S) = rk_2(H_S) + 1$. We get:

$$\delta_1 = |S| + 1 - rk_2(H_{S_1}) = |S| + 1 - rk_2(J_S) = |S| + 1 - rk_2(H_S) - 1 = \delta$$

which proves the inequality $\delta_1 \geq \delta$. □

Proof of lemma 4.16. By hypothesis, at least one of $[P_{n+1}]$ and $[P_{n+1}]$ is not a square, in its respective class group. Let us say that $[P_{n+1}]$ is not a square in $C_K(S)$.

1. Since $E_K(S_1) = E_K(S)$, if $(x)_{S_1} \in Ker(\lambda_S)$ and $(x)_S = (1)_S$ then $x_{P_{n+1}} \in \{1, u\}$.

This means that

$$Ker(\lambda_S) = \{(1, ..., 1, 1),\ (1, ..., 1.u)\} \simeq C_2.$$

2. Suppose that λ_S is not surjective, and let $(x_0)_S \in H_S \setminus Im(\lambda_S)$. Then one of the following two situations occurs:

a) any element $\bar{x} \in E_K(S_1) = E_K(S)$ with $(x)_S = (x_0)_S$ has $x_{P_{n+1}} = 1$ and any element $\bar{y} \in E_L(S'_1)$ with $(y)_{S'} = t_S((x_0)_S)$ has $y_{P'_{n+1}} = u'$,

or

b) any element $\bar{x} \in E_K(S_1) = E_K(S)$ with $(x)_S = (x_0)_S$ has $x_{P_{n+1}} = u$ and any element $\bar{y} \in E_L(S'_1)$ with $(y)_{S'} = t_S((x_0)_S)$ has $y_{P'_{n+1}} = 1$.

We will give the details in case *a*); case *b*) follows by symmetry.

Let $(z)_S \in H_S \setminus Im(\lambda_S)$. Since $(z)_S \in H_S$, one can find $\bar{z} \in E_K(S)$ such that $\nu_S(\bar{z}) = (z)_S$ and one can find $\bar{w} \in E_L(S')$ such that $\nu_{S'}(\bar{w}) = t_S((z)_S)$.

Without loss of generality, suppose that $w_{P'_{n+1}} = u$ and $z_{P_{n+1}} = 1$.

If $x_{P_{n+1}} = 1$ and $y_{P'_{n+1}} = u'$ then $\bar{x}\bar{z} \in E_K(S)$, $\bar{y}\bar{w} \in E_L(S')$, and

$$(xz)_S = (x)_S(z)_S \in H_S,$$

$$(yw)_{S'} = (y)_{S'}(w)_{S'} = t_S((x)_S)t_S((z)_S) = t_S((xz)_S),$$

and

$$(xz)_{P_{n+1}} = 1,\ (yw)_{P'_{n+1}} = 1.$$

That means: $(x)_S(z)_S \in Im(\lambda_S)$.
Thus $[H_S : Im(\lambda_S)] = 2$.

3. Suppose that λ_S is non-injective. It is to be shown that λ_S is surjective. By hypothesis, λ_S is non-injective, so one can find $\bar{x}_0 \in E_K(S_1) = E_K(S)$ such that

$$\nu_{S_1}(\bar{x}_0) = (1, ..., 1, u).$$

If λ_S were non-surjective, we again have the two cases *a*) and *b*) as in the proof of part 2. Let us say, for instance, that we are in case *a*). For such $\bar{x} \in E_K(S_1)$ and $\bar{y} \in E_L(S')$ with $x_{P_{n+1}} = 1$ and $y_{P_{n+1}} = u'$, consider $\bar{x} \cdot \bar{x}_0$. Then

$$\nu_{S_1}(\bar{x} \cdot \bar{x}_0) = ((x)_S, u)$$

so that

$$\lambda_S((x \cdot x_0)_{S_1}) = (x)_S$$

which means that λ_S would be in fact surjective, contradiction. □

Proposition 4.17. *For any P_{n+1}, tame or wild, the following inequality holds:*

$$\delta_1 \geq \delta - 1.$$

Proof. When P_{n+1} is tame, we already know that $\delta_1 \geq \delta$, by Proposition 4.15, so it remains to handle the case when P_{n+1} is wild. In the proof we don't actually use the assumption that P_{n+1} is wild. We shall prove that *no matter how* we extend the correspondence (tamely or wildly) subject only to the condition that -1 is locally a square at P_{n+1} if and only if it is a square locally at P'_{n+1}, then the defect decreases by at most 1.

Define:

$$F_S = \{(x)_{S_1} \in H_{S_1} :\ x_{P_{n+1}} = 1\}$$

and

$$F_{S'} = \{(y)_{S'_1} \in H_{S'_1} :\ y_{P'_{n+1}} = 1\}.$$

Since $(1)_{S_1} \in F_S$, F_S and $F_{S'}$ are non-empty. F_S is a subgroup of H_{S_1} and $F_{S'}$ is a subgroup of $H_{S'_1}$.
If $(x)_{S_1} \in H_{S_1} \setminus F_S$ then $x_{P_{n+1}} = u$ or π or $u\pi$, where u is the square class of the non-square unit, and π is the square class of a non-unit. Without loss of generality we will assume that $x_{P_{n+1}} = u$ (the other cases can be treated similarly).
Note that if $(x)_{S_1},\ (x')_{S_1} \in H_{S_1} \setminus F_S$ have both $x_{P_{n+1}} = x'_{P_{n+1}} = u$ then $(x)_{S_1} \cdot (x')_{S_1} \in F_S$, so the last component of any element in H_{S_1} identifies the class modulo F_S to which the element belongs. Since there are at most 4 such classes, it follows that

$$|H_{S_1}/F_S| \leq 4.$$

In fact $|H_{S_1}/F_S| = 1, 2$, or 4, and in all casses $0 \leq rk_2(H_{S_1}/F_S) \leq 2$ or

$$0 \leq rk_2(H_{S_1}) - rk_2(F_S) \leq 2.$$

Claim: The map $\zeta : F_S \to H_S$, defined by $\zeta((x)_{S_1}) = (x)_S$, is a will-defined and injective homomorphism.
Once we check well-definedness, then the injectivity is clear. We have to check that the map is well-defined.
Let $(x)_{S_1} \in F_S$ and pick $\bar{x} \in E_K(S_1)$ such that $\nu_{S_1}(\bar{x}) = (x)_{S_1}$. Let x be a representative in K for $\bar{x}$. Then x is a locally a square at P_{n+1} and this implies that $\bar{x} \in E_K(S)$.
By definition, $t_{P_{n+1}}(1) = 1$, so that

$$t_{S_1}(x_{P_1}, ..., x_{P_n}, 1) = (t_{P_1}(x_{P_1}), ..., t_{P_n}(x_{P_n}), 1) \in \omega_L(S_1')$$

hence there exists an element $\bar{y} \in E_L(S_1')$ such that

$$\nu_{S_1'}(\bar{y}) = (t_{P_1}(x_{P_1}), ..., t_{P_n}(x_{P_n}), 1).$$

As before, any representative in L of $\bar{y}$ will be a square locally at P'_{n+1} and this implies that, in fact, $\bar{y} \in E_L(S')$.
Since $\nu_{S_1'}(\bar{y}) = t_S(\nu_S(\bar{x}))$, we deduce that $(x)_S \in H_S$, so the map ζ is well-defined, so the claim is proved.

Then $rk_2(F_S) \leq rk_2(H_S)$ and since $0 \leq rk_2(H_{S_1}) - rk_2(F_S) \leq 2$, it follows

$$rk_2(H_{S_1}) - rk_2(H_S) \leq 2$$

and thus

$$\delta_1 = rk_2(\omega_K(S_1)) - rk_2(H_{S_1}) = |S_1| - rk_2(H_{S_1}) =$$
$$= |S| + 1 - rk_2(H_{S_1}) \geq |S| + 1 - rk_2(H_S) - 2 = \delta - 1.$$

Thus, in all cases $\delta_1 \geq \delta - 1$. □

Proposition 4.15 and Proposition 4.17 show that if one extends a correspondence tamely then its defect will not decrease (it might in fact increase) and the wild set is unchanged, while if one extends the corresponcence wildly, the defect may decrease by at most 1 and the size of the wild set will increase by 1.

The proof of the obstruction-killing lemma uses the assumption that the S-class number of K and the S'-class number of L are odd numbers. In the next section we will focus on the case of suitable correspondences, trying to obtain more precise results concerning the minimum number and the type (tame/wild) of primes added to a correspondence in the process of obtaining a small equivalence.

4.3 Suitable Correspondences

In this section we use the construction presented in [1] to show how to extend a suitable correspondence to a small equivalence in a way guaranteed to minimize the number of additional wild primes introduced in the small equivalence.

Let $\mathcal{C} = (S, S', T, (t_P)_{P\in S})$ be a suitable correspondence between K and L, i.e. a correspondence such that the S-class number of K and the S'-class number of L are odd. J. Carpenter's obstruction-killing lemma shows that any suitable correspondence can be extended to a small equivalence by adding at most $\delta(= d_{S,S'})$ pairs of wild primes. Carpenter's analysis [1] allows the possibility that additional such pairs of primes could be less than δ. However, the following proposition shows that the minimum number of pairs of primes that must be added to a suitable correspondence in order to obtain a small equivalence between the two fields is equal to the defect.

Proposition 4.18. *Any suitable correspondence $\mathcal{C} = (S, S', T, (t_P)_{P\in S})$ between K and L can be extended to a small equivalence between K and L by adding exactly δ wild primes.*

Proof. Let W' be the set of wild primes added to S by the obstruction-killing procedure. We know that $|W'| \leq \delta$.

In order to prove the other inequality, it is enough to show that by adding a pair of primes to an existing suitable correspondence like in the obstruction killing procedure, the defect decreases by at most 1. In the obstruction killing procedure J. Carpenter adds a pair of primes (P_{n+1}, P'_{n+1}) (i.e. $T(P_{n+1}) = P'_{n+1}$) whose classes in the corresponding ideal S-class groups are squares and one defines the local map $t_{P_{n+1}}$ wildly. J. Carpenter also shows that the defect decreases by at least 1 for the choice of the pair (P_{n+1}, P'_{n+1}). Proposition 4.17 shows that in this case the defect decreases by at most 1. Consequently in Carpenter's construction we see that the defect decreases by exact one.

So, in order to make the defect 0 (i.e. to obtain a small equivalence between K and L) we need to add exactly δ pairs of primes. □

Proposition 4.18 shows that if the obstruction killing technique is applied to extend a suitable correspondence to a small equivalence then, at each step, the size of the wild set increases by 1 while the defect drops by 1. We have seen that, in terms of defect decreasing, this is the best one can get. At the end of the procedure we obtain a small equivalence with $|W(\mathcal{C})| + \delta(\mathcal{C})$ wild primes, where $W((C))$ denotes the wild set of the given correspondence. We summarize this remark:

Corollary 4.19. *Any suitable correspondence $\mathcal{C}$ between two algebraic number fields K and L can be extended to a Hilbert symbol equivalence by adding $|W(\mathcal{C})| + \delta(\mathcal{C})$ pairs of wild primes.*

4.4 Non-suitable Correspondences

Some of the results presented in this section are generalizations of A. Czogala's results from [4]. We extended Czogala's ideas to a more general situation.

A non-suitable correspondence is a correspondence that is not suitable. More precisely:

Definition 4.20. *A correspondence $\mathcal{C} = (S, S', T, (t_P)_{P\in S})$ is called non-suitable if at least one of the numbes $h_K(S) = |C_K(S)|$ and $h_L(S') = |C_L(S')|$ is even.*

Without loss of generality we will assume that $h_K(S)$ is even.

We will present a method to extend a non-suitable correspondence to a suitable correspondence, a method that minimizes the number of pairs of wild primes added to the correspondence.

Let $\mathcal{C} = (S, S', T, (t_P)_{P\in S})$ be a non-suitable correspondence. We will use the notations from Section 4.1. The following 3 results are immediate generalizations of A. Czogala's results from [4]. Their proofs follow closely Czogala's proofs.

Lemma 4.21. *1.* $dim_{F_2}(K_{ev}/K^{*2}) = r + s + \rho$.
2. $dim_{F_2}(K_0(S)/K_{ev}) = |S| - \theta(S)$, *where* $\theta(S)$ *is the* F_2*-dimension of the subspace of* C_K/C_K^2 *generated by the cosets of ideal classes of primes in* S.

Proof. 1. See Czogala's Lemma 2.4 from [4].
2. Without loss of generality assume that $[P_1], ..., [P_{\theta(S)}]$ is a maximal set of linearly independent elements in C_K/C_K^2. The map $K_0(S) \to F_2^{|S|-\theta(S)}$, defined by

$$x \to (ord_{Q_{\theta(S)+1}}(a) \ (mod\ 2), ..., ord_{Q_g}(a) \ (mod\ 2))$$

is a surjective group homomorphism. Furthermore the kernel of the map is K_{ev}. Indeed, every element in K_{ev} is in the kernel. Conversely, if an element $a \in K_0(S)$ is in the kernel then it has even order at all primes $P_{\theta(S)+1}, ..., P_n$. Since $a \in K_0(S)$, it has even order at all primes outside S. The only primes where a might have odd order are $P_1, ..., P_{\theta(S)}$, but that contradicts the linear independence of these primes. □

Corollary 4.22. $dim_{F_2}(K_0(S)/K^{*2}) = r + s + \rho + |S| - \theta(S)$.

Proof. Obvious. □

Lemma 4.23. *1.* $dim_{F_2}(K_{sq}(S)/K^{*2}) = \rho - \theta(S)$.
2. $dim_{F_2}(K_0(S)/K_{sq}(S)) = r + s + |S|$.

Proof. According to Corollary 4.9,

$$dim_{F_2}(K_{sq}(S)/K^{*2}) \leq \rho - \theta(S) \tag{4.5}$$

because otherwise C_K/C_K^2 would have more than ρ linearly independent elements, false.
In the proof of Corollary 4.9 we have seen that $G_K(S)$ is an $\mathbb{F}_2$-inner product space, with the inner product defined by the product of Hilbert symbols. Moreover, $K_0(S)/K_{sq}(S)$ can be seen as a subspace of $G_K(S)$ with the inner product

$$(\bar{x}, \bar{y}) = \prod_{P\in S} (x, y)_P.$$

It is easy to see that $K_0(S)/K_{sq}(S)$ is totally isotropic, because all elements in $K_0(S)$ are local units at the primes outside S, hence the product of Hilbert symbols at primes in S is 1 (this follows from Hilbert reciprocity).
Again Corollary 4.4 page 16 from [8] implies

$$dim_{F_2} K_0(S)/K_{sq}(S) \leq dim_{F_2} G_K(S) = r + s + |S|. \tag{4.6}$$

The equalities from this lemma follow from 4.5, 4.6, and Corollary 4.22. □

Now let $[P_1], ..., [P_{\theta(S)}]$ be the representatives of the cosets of primes in S that are linearly independent in C_K/C_K^2.

Let $\{a_1, ..., a_m\}$ (with $m = r+s+|S|$ according to Lemma 4.23) be an $\mathbb{F}_2$-basis for $K_0(S)/K_{sq}(S)$, and $b_1, ..., b_l$ (with $l = \rho - \theta(S)$, according to Lemma 4.23) be an F_2-basis of K_{sq}/K^{*2}. When constructing the basis $b_1, ..., b_n$, we pick $b_1 = -1$, if possible (i.e. if $-1 \in K_{sq}(S) \setminus K^2$).

Similarly, let $\{a'_1, ..., a'_{m'}\}$ (with $m' = r' + s' + |S'|$ according to Lemma 4.23) be an F_2-basis for $L_0(S')/L_{sq}(S')$, and $b'_1, ..., b'_{l'}$ (with $l' = \rho' - \theta'(S')$, according to Lemma 4.23) be an F_2-basis of $L_{sq}(S')/L^{*2}$. Like before, when constructing the basis $b'_1, ..., b'_{l'}$, we pick $b'_1 = -1$, if possible.

Since $\mathcal{C}$ is a corespondence, for any P in S -1 is a local square at P if and only if -1 is a local square at TP, hence $b_1 = -1$ if and only if $b'_1 = -1$.

Since K and L are Hilbert symbol equivalent, $r = r'$, $s = s'$, and $|S| = |S'|$ hence $m = m'$. Without loss of generality we will assume that $l \leq l'$.

Use Theorem 4.8 to pick primes $R_1, ..., R_l$ outside S, in K, such that

$$(\frac{b_i}{R_i}) = -1, \ \forall i \in \{1, ..., l\}$$

$$(\frac{b_j}{R_i}) = 1, \ \forall j \neq i \in \{1, ..., l\}$$

$$(\frac{a_j}{R_i}) = 1, \ \forall j \in \{1, ..., m\}, \ \forall i \in \{1, ..., l\}.$$

We know that $\{a_1, ..., a_m, b_1, ..., b_l\}$ is an $\mathbb{F}_2$-basis for $K_0(S)/K^2$. If $-1 \notin K_0(S)$ then we can take $a_1 = -1$, so

$$(\frac{-1}{R_i}) = 1, \ \forall i \in \{1, ..., l\}.$$

Similarly, pick non-dyadic primes $R'_1, ..., R'_{l'}$ outside S', in L, such that

$$(\frac{b'_i}{R'_i}) = -1, \ \forall i \in \{1, ..., l'\}$$

$$(\frac{b'_j}{R'_i}) = 1, \ \forall j \neq i \in \{1, ..., l'\}$$

$$(\frac{a'_j}{R'_i}) = 1, \ \forall j \in \{1, ..., m'\}, \ \forall i \in \{1, ..., l'\}.$$

We also know that $\{a'_1, ..., a'_{m'}, b'_1, ..., b'_{l'}\}$ is an $\mathbb{F}_2$-basis for $L_0(S')/L^2$. If $-1 \notin L_0(S')$ then we can take $a'_1 = -1$, so

$$(\frac{-1}{R'_i}) = 1, \ \forall i \in \{1, ..., l'\}.$$

It follows that for any $i \in \{1, ..., l\}$ -1 is a local square at R_i iff -1 is a local square at R'_i.

We will add to (S, S') the pair (R_1, R'_1), and we define the local map

$$t_{R_1} : (K^*_{R_1})/(K^*_{R_1})^2 \to (L^*_{R'_1})/(L^*_{R'_1})^2$$

by $1 \to 1$, $b_1 \to b'_1$, and arbitrarily on the remaining two classes. Note that the this local map is tame, for b_1 and b'_1 are simultaneously non-square units (by construction).

Let us notice that, according to Corollary 4.9, R_1 is not a square in $C_K(S)$, so we can use the construction made in Case 1 of the proof of Proposition 4.15: we can define the projection map

$$\lambda_S : H_{S\cup\{R_1\}} \to H_S.$$

Note that $(1) \neq (b_1)_{S_1} \in Ker(\lambda_S)$ because b_1 is a square at all primes in S and it is a non-square at R_1. Hence λ_S is non-injective and, by Lemma 4.16 it is surjective. The proof of Proposition 4.15 shows that in this case $\delta_1 = \delta$.

To sum up: we extend the correspondence tamely and the wild set and the defect remain unchanged.

Now continue to add pairs (R_i, R_i') to the correspondence and define tame local maps as above. If both S-class numbers become odd at a certain step, we stop adding the remaining pairs, for we got a suitable correspondence. During this process the wild set and the defect are unchanged.

Let us suppose now that after we added all possible pairs:

$$(R_1, R_1'), ..., (R_l, R_l')$$

the S'-class numbers is still even. Lemma 4.23 and Corollary 4.9 show that

$$\{[P_1], ..., [P_{\theta(S)}], [R_1], ..., [R_l]\}$$

is a basis for C_K/C_K^2. If $S^* = S \cup \{R_1, ..., R_l\}$ then $h_K(S^*)$ is odd.

Note first that in this case $l < l'$. For if $l = l'$ then, as above, the S^*-class number of L would be odd, false.

The idea is to consider other primes in K to make pairs with the remaining primes $R_{l+1}', ..., R_{l'}'$. We will use the following result (a proof of this result can be found in [12]):

Lemma 4.24. *If S is a finite set of primes in K such that $h_K(S)$ is odd and for each $P \in S$ we fix $x_P \in (K_P^*)/(K_P^*)^2$ then there are infinitely many primes Q with the property that there is an $x \in K^*$ such that:*

$$x \equiv x_P, \ \forall P \in S;$$

$$ord_Q(x) = 1;$$

$$ord_P(x) = 0, \ \forall P \notin S \cup \{Q\}.$$

We use Lemma 4.24 to obtain primes $R_{l+1}, ..., R_{l'}$ and elements $b_{l+1}, ..., b_{l'}$ in K^* such that

$$b_{l+i} = 1 \text{ in } (K_P^*)/(K_P^*)^2, \quad \forall P \in S \cup \{R_1, ..., R_{l+i-1}\};$$

$$b_{l+i} = \pi \text{ in } (K_{R_{l+i}}^*)/(K_{R_{l+i}}^*)^2;$$

$$ord_P(b_{l+i}) = 0, \quad \forall P \notin S \cup \{R_1, ..., R_{l+i}\}.$$

It is necessary to observe that -1 is a local square at all primes $R_{l+1}, ..., R_{l'}$ for otherwise one contradicts Hilbert's reciprocity law.

Now add (R_{l+1}, R_{l+1}') to $(S^* = S \cup \{R_1, ..., R_l\}, (S')^* = S' \cup \{R_1', ..., R_l'\})$, define $T(R_{l+1}) = R_{l+1}'$, and define the local map wildly:

$$1 \to 1, \quad u \to \pi', \quad \pi \to u', \quad u\pi \to u'\pi'.$$

Note that b'_{l+1} is the local non-square unit at R'_{l+1}, and b_{l+1} is the local uniformizer at R_{l+1}.

Now let $S_1^* = S^* \cup \{R_{l+1}\}$, and $(S')_1^* = (S')^* \cup \{R'_{l+1}\}$. Note that $[R_{l+1}]$ has odd order (hence it is a square) in $C_K(S^*)$ (we have seen that $ord(C_K(S^*))$ is odd for the 2-rank is 0). Moreover, $[R'_{l+1}]$ is a non-square in $C_L((S')^*)$ because $[R'_1], ..., [R'_l], [R'_{l+1}]$ are linearly independent in C_L/C_L^2, so that $E_L((S')^*) = E_L((S')_1^*)$. Hence if $x \in H_{S_1^*}$ then $x_{R_{l+1}} = 1$ or π (see the definition of $t_{R_{l+1}}$). Consequently, we can write

$$H_{S^*1} = F_{S^*} \cup (x_0)_{S_1^*} F_{S^*}$$

where $(x_0)_{S_1^*} \in H_{S_1^*}$ is such that $x_{0,R_{l+1}} = \pi$ and, as usually,

$$F_{S_1^*} = \{(x) \in H_{S_1^*} : \ x_{R_{l+1}} = 1\}.$$

Note that we can take

$$(x_0)_{S_1^*} = (1, ..., 1, \pi) = t_{S_1^*}^{-1}(\nu_{(S')_1^*}((b'_{l+1})_{(S')_1^*})) = (b_{l+1})_{S_1^*}.$$

Thus

$$[H_{S_1^*} : F_{S^*}] = 2.$$

On the other hand, if $(x)_{S^*} \in H_{S^*}$ has $x_{R_{l+1}} = u$ then

$$\prod_{P \in \Omega_K} (x, b_{l+1})_P = \prod_{P \in S^*} (x, b_{l+1})_P \cdot (x, b_{l+1})_{R_{l+1}} \cdot \prod_{P \notin S_1^*} (x, b_{l+1})_P =$$

$$= \prod_{P \in S^*} (x, 1)_P \cdot (u, \pi)_{R_{l+1}} \cdot \prod_{P \notin S_1^*} (x, b_{l+1})_P = 1 \cdot (-1) \cdot 1 = -1,$$

which contradicts Hilbert's reciprocity law.

We conclude that any element $\bar{x} \in E_K(S^*)$ which maps to an element in H_{S^*} has $x_{R_{l+1}} = 1$.

We claim that in fact any such $\bar{x} \in E_K(S^*)$ maps to an element in $H_{S_1^*}$.

Indeed, if all elements $\bar{y} \in E_L((S')^*)$ such that

$$t_{S^*}(\nu_{S^*}(\bar{x})) = \nu_{(S')^*}(\bar{y})$$

have $y_{R'_{l+1}} = u'$ (the square class of the non-square unit), then let's multiply any such $\bar{y}$ by b'_{l+1}. Note that $\bar{y}b'_{l+1} \in E_L((S')^*) = E_L((S')_1^*)$, and and

$$\nu_{(S')^*}(\bar{y}b'_{l+1}) = \nu_{(S')^*}(\bar{y}) = t_{S^*}(\nu_{S^*}(\bar{x})),$$

which means that $\bar{y}b'_{l+1}$ has all the same properties as $\bar{y}$ except that the local component at R'_{l+1} for this element is 1. This is a contradiction. Consequently $x_{S_1^*} \in H_{S_1^*}$.

In this way we get a group homomorphism $H_{S^*} \to F_{S^*}$ which is an isomorphism. We have seen that $[H_{S_1^*} : F_{S^*}] = 2$, so that

$$rk_2(H_{S_1^*}) = rk_2(H_{S^*}) + 1.$$

We get:

$$\delta_{S_1^*} = |S^*| + 1 - rk_2(H_{S_1^*}) = |S^*| + 1 - rk_2(H_{S^*}) - 1 = \delta_{S^*}.$$

So the defect is preserved, which is the best one can get when for exactly one of the primes in the pair (R_{l+1} in or case) the class in the ideal $S*$-class group is a square (see Lemma 4.25 below). Note that the ideal class of any prime outside S^* is a square in $C_K(S^*)$, so the procedure described above is optimal in terms of defect. Certainly, it does increase the size of the wild set but, according to Proposition 4.15, any tentative of extending tamely the correspondence will result in increasing the defect so overall there would be no gain.

Lemma 4.25. *Let $\mathcal{C} = (S, S', T, (t_P)_{P\in S})$ be a non-suitable correspondence of defect δ. Pick $Q \in \Omega_K \setminus S$ and $Q' \in \Omega_L \setminus S'$ such that:*
1. -1 is a local square at Q iff -1 is a local square at Q';
2. $[Q]$ is a square in $C_K(S)$ and $[Q']$ is not a square in $C_L(S')$.
Define $T(Q) = Q'$ and a local wild map $t_Q : (K_Q^*)/(K_Q^*)^2 \to (L_{Q'}^*)/(L_{Q'}^*)^2$. Then the defect of the new correspondence δ_1 satisfies the inequality:

$$\delta_1 \geq \delta.$$

Proof. Let $S_1 = S \cup \{Q\}$ and $S_1' = S' \cup \{Q'\}$.
Since $[Q']$ is not a square in $C_L(S')$ and $[Q]$ is a square in $C_K(S)$, we have

$$E_L(S') = E_L(S_1'), \quad E_K(S_1) = E_K(S) \cup \bar{x}_0 E_K(S),$$

for $\bar{x}_0 \in E_K(S_1)$ with $x_{0,Q} = \pi$. Without loss of generality suppose that $t_Q(\pi) = u'$. If $(y)_{S_1'} \in H_{S_1'}$ then $y_{Q'} = 1, u'$, hence $H_{S_1'} = F_{S'}$ or $[H_{S_1'} : F_{S'}] = 2$. We have seen in the proof of Proposition 4.17 that the map $\zeta : F_{S'} \to H_{S'}$, defined by $\zeta((y)_{S_1'}) = (y)_{S'}$, is an injective homomorphism.
It follows that

$$rk_2(H_{S_1'}) \leq rk_2(F_S) + 1 \leq rk_2(H_{S'}) + 1$$

and thus

$$\delta_1 = |S| + 1 - rk_2(H_{S_1'}) \geq |S| - rk_2(H_{S'}) = \delta.$$

□

The result that we have proved can be stated in the following

Proposition 4.26. *Let $\mathcal{C} = (S, S', T, (t_P)_{P\in S})$ be a non-suitable correspondence. Then $\mathcal{C}$ can be extended to a suitable correspondence $\mathcal{C}'$ that has the same defect and such that*

$$|W(\mathcal{C}')| = |W(\mathcal{C})| + |rk_2(C_L(S')) - rk_2(C_K(S))|.$$

Proof. The procedure of obtaining $\mathcal{C}'$ has been presended above. We have seen that the defect was unchanged.
We have

$$|W(\mathcal{C}')| = |W(\mathcal{C})| + |rk_2(C_L) - \theta(S') - rk_2(C_K) + \theta(S)|.$$

But

$$|rk_2(C_L) - \theta(S') - rk_2(C_K) + \theta(S)| = |rk_2(C_L(S')) - rk_2(C_K(S))|.$$

The inequality is a consequence of the discussion preceeding this proposition. □

Theorem 4.27. *Any correspondence $\mathcal{C} = (S, S', T, (t_P)_{P\in S})$ between two number fields K and L, of defect δ and wild set W, can be extended to a Hilbert symbol equivalence between K and L whose wild set has the size*

$$\delta + |W| + |rk_2(C_K(S)) - rk_2(C_L(S'))|.$$

Moreover, any other extension of $\mathcal{C}$ to a Hilbert symbol equivalence between K and L has a wild set of size no less that $\delta + |W| + |rk_2(C_K(S)) - rk_2(C_L(S'))|$.

Proof. The first part follows from Proposition 4.18 and Proposition 4.26.
For the second part, here are the details. Let $\mathcal{C}'$ be a Hilbert symbol equivalence with a finite wild set that extends $\mathcal{C} = (S, S', T, (t_P)_{P\in S})$. Then if one gathers S, the wild set of $\mathcal{C}'$ and the generators of the S-ideal class group of K and considers the restriction of the Hilbert symbol equivalence to this subset, one gets a small equivalence called $S.E.$. The Hilbert symbol equivalence $\mathcal{C}'$ is obtained by extending tamely this small equivalence. Now this small equivalence is a correspondence with the same number of wild primes like $\mathcal{C}'$. If we consider the subset of the small equivalence that contains S and the generators of the $C_K(S)$, it is a suitable correspondence (denoted $S.C.$) that extends $\mathcal{C}$. This correspondence has a certain defect δ, and it can be extended to a small equivalence by adding δ wild primes. Since the defect of $S.E.$ is equal to 0, at least δ of the primes added to $S.C.$ to get $S.E.$ will be wild (because at every step the defect decreases by at most 1, and it only decreases when the prime added to the correspondence is wild). Finally, consider the correspondence $\mathcal{C}$. By adding to S the generators of $C_K(S)$ one gets a suitable correspondence. $S.C.$ above defined can be obtained from $\mathcal{C}$ by adding at least $rk_2(C_K(S)) - rk_(C_L(S'))$ wild primes (because at every step the defect remains unchanged or it increases, and it only stays the same when the primes are wild). Consequently $\mathcal{C}'$ has no less than $\delta + |W| + |rk_2(C_K(S)) - rk_2(C_L(S'))|$ wild primes. □

The above theorem describes completely the size of the minimal wild set that a Hilbert symbol equivalence between K and L which extends a given correspondence can have.

In some situations, computing the defect of a correspondence may be difficult. It might be interesting to find bounds for the minimum number of wild primes in Hilbert symbol equivalences between two number fields. If D is the set of dyadic primes in K and S consists of D and the infinite primes, then we obtain directly:

Corollary 4.28. *Let W be a minimum set of wild primes of Witt equivalent number fields K and L. Then:*

$$|rk_2C_K(D) - rk_2C_L(TD)| \leq |W \setminus D| \leq |rk_2C_K(D) - rk_2C_L(TD)| + |S|.$$

The above corollary gives bounds for the number of non-dyadic primes in a minimum wild set. In particular, when K and L are Witt equivalent non-real number fields, this number exceeds the difference in 2-ranks of the D-ideal class groups by at most $5n/2$ (the number of complex places is $n/2$ and the number of dyadic primes is at most n). The splitting of 2 in K affects strongly this deviation, as if 2 stays inert in K then the number of wild non-dyadic primes in the minimum wild set exceeds the difference in 2-ranks by at most $n/2 + 2$.

From the above corollary we obtain immediately:

Corollary 4.29. *Let W=Wild(K,L) be a minimum wild set for two Witt equivalent number fields K and L. Let D and D' be the sets of dyadic primes in K and L respectively. Then:*

$$|rk_2C_K(D) - rk_2C_L(D')| \leq |W| \leq |rk_2C_K(D) - rk_2C_L(D')| + 2|D| + r + s.$$

Finally, if we combine this result with proposition 2.10 we obtain:

Proposition 4.30. *If K and L are Witt equivalent number fields then*

$$|rk_2^+C_K(D) - rk_2^+C_L(D')| \leq |rk_2C_K(D) - rk_2C_L(D')| + 2|D| + r + s.$$

4.5 Example

Let d_1 and d_2 be two square-free positive integers such that $d_1 \equiv 3 \pmod 8$ and $d_2 \equiv 3 \pmod 8$, and define $K = \mathbb{Q}(\sqrt{-d_1})$ and $L = \mathbb{Q}(\sqrt{-d_2})$. According to [4], these two number fields are Witt equivalent. The discriminants of K and L are $-d_1$ and $-d_2$ respectively. Since the discriminants are congruent to 5 (mod 8), the rational prime 2 is inert in both fields:

$$2O_K = P, \quad 2O_L = P',$$

with $f(P|2) = f(P'|2) = 2$. Then the completions K_P and $L_{P'}$ are unramified quadratic extensions of $\mathbb{Q}_2$. It is known that $\mathbb{Q}_2$ has a unique unramified quadratic extension: $\mathbb{Q}_2(\sqrt{-3})$ (see Proposition 6-5-5 from [16]), hence $K_P = L_{P'} = \mathbb{Q}_2(\sqrt{-3})$ which means that $(K_P^*)/(K_P^*)^2$ and $(L_{P'}^*)/(L_{P'}^*)^2$ are the same.

Let $S = \{P,\ P_\infty\}$ and $S' = \{P',\ P'_\infty\}$, where P_∞ and P'_∞ are the infinite complex primes in K and L respectively. For this choice, $G_K(S) = K_P^*/K_P^{*2}$ and $G_L(S') = L_{P'}^*/L_{P'}^{*2}$ which are canonically identified ("equal") by the identity map. Let T be the map that sends P_∞ to P'_∞ and P to P', and define $t_P : K_P^*/K_P^{*2} \to L_{P'}^*/L_{P'}^{*2}$ to be the identity map.

Therefore we have an example of a simple correspondence $\mathcal{C} = (S, S', T, (id, id))$.

Since the local map is the identity, the correspondence has no wild primes.

We wish to show next that the defect of this correspondence equals 0. To show that, observe that $\bar{1}$, $-\bar{1}$, and $\bar{2}$ are distinct linearly independent classes in $(K_P^*)/(K_P^*)^2$ and in fact $\bar{1},\ -\bar{1},\ \bar{2} \in \omega_K(S)(= Im(\nu_S))$. But remember that $rk_2(\omega_K(S)) = |S| = 2$, and thus $\{-\bar{1},\ \bar{2}\}$ is an $\mathbb{F}_2$-basis for $\omega_K(S)$. Similarly one can show that $\{-\bar{1},\ \bar{2}\}$ is an $\mathbb{F}_2$-basis for $\omega_L(S')$, and henceforth $\omega_K(S) = \omega_L(S')$ which implies that the defect equals 0.

For $\mathcal{C}$, the number of wild primes is 0, the defect is equal to 0, so this correspondence can be extended to a Hilbert symbol equivalence that has $|rk_2(C_K(S)) - rk_2(C_L(S'))|$ wild primes. This is the minimum number of wild primes that *any* Hilbert symbol equivalence can have. Since in the ideal class groups both $P = 2O_K$ and $P' = 2O_L$ are trivial, $C_K(S) = C_K$ and $C_L(S') = C_L$. Thus the minimum number of wild primes is $|rk_2(C_K) - rk_2(C_L)|$. But according to Gauss the 2-rank of C_K is $k-1$, where k is the number of distinct prime divisors of $-d_1$, and the 2-rank of C_L is $l-1$, where l is the number of distinct prime divisors of $-d_2$. By choosing $d_1 = 3$ we have $rk_2(C_K) = 0$, and by choosing $d_2 = 3p_1...p_N$, with $p_1,\ p_2,\ ...,\ p_N$ distinct rational primes congruent to 1(mod 8), it follows directly that for any non-negative integer N there are pairs of (quadratic) Witt equivalent number fields for which the minimum number of wild primes is equal to N. On the other hand, by choosing $k = l$, one can construct infinitely many pairs of tamely equivalent number fields with no wild primes.

Chapter 5. Conclusions

The problem of when two algebraic number fields have isomorphic Witt rings of quadratic forms has been studied in the last 15 years. Complete characterizations in terms of the invariants of the number fields are known. It is also known that this property is equivalent to the existence of Hilbert symbol equivalences between the number fields. With respect to these equivalences the prime ideals can have a particularly nice behavior (tame) or not (wild). Before this dissertation, it was known that if there is a Hilbert symbol equivalence between two number fields then one can construct another one with respect to which only finitely many primes are wild. Lower bounds for the number of wild primes in Hilbert symbol equivalences have been presented in 1997. The problem that we studied in this dissertation was: what is the minimum number of wild primes in Hilbert symbol equivalences between two fixed number fields? We presented an exact formula for this minimal number. It involves the difference in 2-ranks of the dyadic-ideal class groups of the two fields, and an invariant (called defect) of a certain correspondence based on dyadic and infinite primes only. In some situations it is still difficult to compute the defect precisely, so we also presented lower and upper bounds for the minimum number of wild primes.

References

[1] J. Carpenter, *Finiteness theorems for forms over global fields*, Math. Z. **209** (1992), 153–166.

[2] P.E. Conner, R. Perlis, K. Szymiczek *Wild sets and 2-ranks of class groups*, Acta Arith. **79** (1997), 83–91.

[3] D.A. Cox, *Primes of the Form* $x^2 + ny^2$, John Wiley and Sons, Inc., 1989.

[4] A. Czogala, *On reciprocity equivalence of quadratic number fields*, Acta Arith. **58** (1991), 29–46.

[5] A. Frohlich, M.J. Taylor, *Algebraic Number Theory*, Cambridge University Press, 1991.

[6] D. Harrison, *Witt Rings*, University of Kentucky Notes, Lexington, KY, 1970.

[7] E. Hecke, *Lectures on the Algebraic Numbers*, Springer-Verlag, 1981.

[8] T.Y. Lam, *The Algebraic Theory of Quadratic Forms*, W.A. Benjamin, Inc., 1973.

[9] D. Marcus, *Number Fields*, Springer-Verlag, 1977.

[10] O.T. O'Meara, *Introduction to Quadratic Forms*, Springer-Verlag, 1973.

[11] T. Palfrey, *Density theorems for reciprocity equivalences*, Annales Mathematicae Silesianae, **12**, 161-172, Silesian University, 1998.

[12] R. Perlis, K. Szymiczek, P.E. Conner, and R. Litherland, *Matching Witts with Global Fields*, Contemp. Math. **155** (1994), 365–387.

[13] A. Pfister, *Quadratic Forms with Applications to Algebraic Geometry and Topology* , Cambridge University Press, 1995.

[14] K. Szymiczek, *Witt equivalence of global fields*, Comm. Algebra **19** (1991), 1125–1149.

[15] K. Szymiczeck, *Bilinear Algebra: An Introduction to the Algebraic Theory of Quadratic Forms*, Gordon and Breach Science Publishers, 1997.

[16] E. Weiss, *Algebraic Number Theory*, Dover Publications, 1998.

Vita

Marius Marian Somodi was born in Zimnicea, Romania, on the 10th day of November, 1968. He graduated from the Mathematics and Physics High School No. 4, Bucharest, in 1987. He entered the Bucharest University in 1987, where he received the Graduation Diploma in Mathematics in 1993. Between 1993 and 1996 he worked as a computer programmer at the Research Institute for Informatics, Bucharest, Romania.

In January 1997 he entered the graduate program in mathematics at Louisiana State University, Baton Rouge, Louisiana. In 1998 he received the degree of Master of Science from Louisiana State University. In the Summer he will earn the degree of Doctor of Philosophy.