Trace Forms of Abelian Extensions of Number Fields

Karli Smith
Louisiana State University and Agricultural and Mechanical College

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

Part of the Applied Mathematics Commons

Recommended Citation
https://repository.lsu.edu/gradschool_dissertations/3627

This Dissertation is brought to you for free and open access by the Graduate School at LSU Scholarly Repository. It has been accepted for inclusion in LSU Doctoral Dissertations by an authorized graduate school editor of LSU Scholarly Repository. For more information, please contact gradetd@lsu.edu.
TRACE FORMS OF ABELIAN EXTENSIONS OF 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
Karli Smith
B.S. in Math., California Polytechnic State University, 2003
M.S., Louisiana State University, 2005
August 2008
Acknowledgments

I would like to express my gratitude to the many people who have helped me through the years. First of all, I would like to thank my adviser Dr. Robert Perlis. He has always known just what to say to challenge me and make me think, and he’s been supportive and understanding during the ups and downs of my graduate studies. I'll never forget him telling me, “There are more important things in life than math.” I will be a better teacher and mentor to my students because of him.

I would like to thank Lisa Adams and Dr. Steve Agronsky for their faith in my mathematical abilities. If not for their encouragement to “go all the way with math”, I definitely wouldn’t be here right now.

My parents and sister deserve special thanks for their support throughout the years. They never doubted that I would make it this far.

I am grateful for my two best friends, Anthony and Paula. They have both given selflessly of themselves, and I know we will continue to be great friends no matter where life takes us.

Finally, I dedicate this dissertation to my husband Charles and my daughter Kira, the loves of my life. They helped make the last five years truly enjoyable.
# Table of Contents

Acknowledgements............................................................................................ii

Abstract..............................................................................................................iv

Chapter 1. Introduction.........................................................................................1

Chapter 2. Selected Results from Other Works..................................................14

Chapter 3. Abelian Witt Classes over Arbitrary Number Fields.......................18

Chapter 4. Abelian Witt Classes over Number Fields of Type (1, 0).................22

Chapter 5. Abelian Witt Classes over Number Fields of Type (1, 1).................33

References..........................................................................................................40

Vita......................................................................................................................41
Abstract

This dissertation is concerned with providing a description of certain symmetric bilinear forms, called trace forms, associated with finite normal extensions $N/K$ of an algebraic number field $K$, with abelian Galois group $Gal(N/K)$. These abelian trace forms are described up to Witt equivalence, that is, they are described as elements in the Witt ring $W(K)$. Complete descriptions are obtained when the base field $K$ has exactly one dyadic prime and either no real embeddings or one real embedding. For these fields $K$, the set of abelian trace forms is closed under multiplication in the Witt ring $W(K)$. 
Chapter 1
Introduction

We begin with an introduction to Witt rings, which comes mainly from Section 1.2 of [2].

Let $K$ be a field. We look at pairs $(V, b)$, where $V$ is a non-zero finite-dimensional vector space over $K$, and $b : V \times V \to K$ is a bilinear symmetric form. We say $b$ is nondegenerate if the adjoint, $Ad_b : V \to \text{Hom}_K(V, K)$, given by $Ad_b(v) = b(v, \cdot)$, is an isomorphism. When $b$ is nondegenerate, we call the pair $(V, b)$ an innerproduct space over $K$. We say that $(V, b)$ is isometrically equivalent to $(V', b')$ if and only if there is a $K$-linear isomorphism $L : V \to V'$ such that $b'(L(x), L(y)) = b(x, y)$ for all $x, y \in V$.

The orthogonal direct sum of two innerproduct spaces, $(V \oplus V', b \oplus b')$, is given by

$$(b \oplus b')(\langle x, x' \rangle, \langle y, y' \rangle) = b(x, y) + b'(x', y').$$

The tensor product is defined by

$$(b \otimes b')(x \otimes x', y \otimes y') = b(x, y)b'(x', y').$$

Let $(W, b)$ be a subspace of the inner product space $(V, b)$. Then we have an associated subspace

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

If $W = W^\perp$, then $W$ is called a metabolizer for $(V, b)$. An innerproduct space is called Witt trivial if it contains a metabolizer. Two innerproduct spaces $(V, b)$ and $(V', b')$ are Witt equivalent if $(V \oplus V', b \oplus (-b'))$ is Witt trivial.
Witt equivalence is an equivalence relation, and we will let \( \langle V, b \rangle \) denote the equivalence class of \((V, b)\). We call \( \langle V, b \rangle \) the *Witt class* of \((V, b)\). The collection of all Witt classes forms the *Witt ring* \( W(K) \). The Witt ring is a commutative ring with identity. Addition is given by

\[
\langle V, b \rangle + \langle V', b' \rangle = \langle V \oplus V', b \oplus b' \rangle,
\]
and the additive inverse of \( \langle V, b \rangle \) is

\[
-\langle V, b \rangle = \langle V, -b \rangle.
\]

Multiplication is given by

\[
\langle V, b \rangle \langle V', b' \rangle = \langle V \otimes V', b \otimes b' \rangle.
\]

Whenever \( \text{char}(K) \neq 2 \), Witt classes in \( W(K) \) can be diagonalized. So we can choose an orthogonal basis \( e_1, \ldots, e_n \) of \((V, b)\), i.e. \( b(e_i, e_j) = 0 \) whenever \( i \neq j \). Let \( b(e_i, e_i) = a_i \), and we can write \( \langle V, b \rangle \) as \( \langle a_1, \ldots, a_n \rangle \). Observe that a Witt class \( \langle a_1, \ldots, a_n \rangle \) is the sum of one-dimensional Witt classes \( \langle a_i \rangle \), with \( a_i \in K^* \), the set of nonzero elements in \( K \). Moreover, \( \langle a_i \rangle = \langle a_i z^2 \rangle \) for any \( z \in K^* \). We say that the displayed entries in \( \langle a_1, \ldots, a_n \rangle \) are determined up to (nonzero) squares, and write \( a_i \in K^*/K^{**} \), where \( K^{**} \) denotes the set \( \{ a^2, a \in K^* \} \) of squares of elements in \( K^* \). With this notation, the multiplicative identity of \( W(K) \) is \( \langle 1 \rangle \). The additive identity is a hyperbolic plane, \( \langle 1, -1 \rangle \).

Now we will introduce trace forms.

**Definition 1.1.** Let \( F/K \) be a finite separable extension of a field \( K \). Then the **trace form** of \( F \) is the symmetric \( K \)-bilinear form

\[
tr_{F/K} : F \times F \to K
\]

given by \( tr_{F/K}(x, y) = \text{trace}_{F/K}(xy) \) for all \( x, y \in F \).
If we look at $F$ as a finite-dimensional vector space over $K$, then the field $F$ is a symmetric inner product space over $K$ with respect to the trace form, and we define $\langle F \rangle$ to be the Witt class of $(F, tr_{F/K})$ in the Witt ring $W(K)$.

**Definition 1.2.** Take an extension $F/K$ and an element $s \in F^*$. Then the scaled trace form

$$tr_{F/K}(x, y)_s = trace_{F/K}(sxy)$$

defines an innerproduct structure on $F$ whose Witt class is denoted $\langle Fs \rangle$.

Although we are mainly interested in trace forms, we will now discuss four invariants of general Witt classes. The first such invariant is $dim_K V$, the dimension of $V$ as a vector space, modulo 2. We call this the *rank* of $\langle V, b \rangle$. The following theorem, due to Witt, gives a relationship between rank and isometric equivalence.

**Theorem 1.3.** (see [2], Theorem I.2.1) If $K$ does not have characteristic 2, then two innerproduct spaces over $K$ are isometrically equivalent if and only if they have the same rank and are Witt equivalent.

The rank of a Witt class is defined to be the dimension of any class representative, modulo 2: $rk\langle V, b \rangle \equiv dim_K V \pmod{2}$. As a Witt class invariant, the rank gives us a ring homomorphism

$$0 \to J \to W(K) \to Z/2Z \to 0.$$ 

The kernel, $J$, is called the *fundamental ideal* of $W(K)$, and consists of all classes of even rank.

The next invariant is the *discriminant*. We first choose any basis $e_1, \ldots, e_n$ for $V$ over $K$, and let $B$ be the matrix

$$B = (b(e_i, e_j)).$$
Then $B$ is symmetric since $b$ is symmetric, and $B$ is non-singular since $b$ is non-degenerate. Starting with another basis will give us a matrix of the form $ABA^t$, but $\det(ABA^t) = \det(B)$ in $K^*/K^{**}$. The discriminant of $\langle V, b \rangle$ is the element of $K^*/K^{**}$ defined by
\[ dis\langle V, B \rangle = (-1)^{(n-1)/2} \det(B), \]
which is well-defined in $K^*/K^{**}$. For a diagonalized form $\langle a_1, \ldots, a_n \rangle$, the discriminant is
\[ dis\langle a_1, \ldots, a_n \rangle = (-1)^{(n-1)/2} (a_1 \cdots a_n), \]
modulo the squares in $K^*$.

The two invariants $rk$ and $dis$ together form a map
\[ W(K) \to \mathbb{Z}/2\mathbb{Z} \times K^*/K^{**}. \]

This map gives us the exact sequence
\[ 0 \to J^2 \to W(K) \to \mathbb{Z}/2\mathbb{Z} \times K^*/K^{**} \to 0. \]

Here the kernel is $J^2$, which consists of all classes with even rank and discriminant 1 modulo squares.

The third invariant of $\langle V, b \rangle$ is the signature. If $K$ cannot be ordered, i.e. if $K$ has no embeddings into the real numbers, then signatures are not defined. But if $K$ can be ordered in at least one way, then we can associate each ordering of $K$ with a signature. To define this signature, first choose an orthogonal basis $e_1, \ldots, e_n$ of $(V, b)$. With respect to our chosen ordering of $K$, a certain number $s$ of these basis elements will satisfy the inequality $b(e_i, e_i) > 0$, while the other $n - s$ basis elements will satisfy $b(e_i, e_i) < 0$. The signature of $\langle V, b \rangle$ for the chosen ordering is the difference
\[ sgn\langle V, b \rangle = s - (n - s) = 2s - n. \]
Sylvester’s Theorem of Inertia guarantees that $s$ (and hence $\text{sgn}(V, b)$) is independent of the chosen orthogonal basis.

Now let’s assume that $K$ is an algebraic number field, that is, an extension of the rationals of finite degree. This number field $K$ may contain several real infinite primes, each of which corresponds to a specific embedding of $K$ into $R$. Each of these embeddings gives us a different ordering of $K$, and each ordering corresponds to a signature. So we have a total signature,

$$Sgn : W(K) \rightarrow \mathbb{Z}^r,$$

which pairs each element $X$ of $W(K)$ with an $r$-tuple of integers, where $r$ is the number of real infinite primes of $K$.

The final invariant is the Hasse-Witt invariant. This is actually a countably infinite family of invariants, also called Hasse symbols. We must first recall that for a number field $K$, a finite prime is a prime ideal in the ring of integers of $K$, a real infinite prime is an embedding of $K$ into the real numbers, and a complex infinite prime is a pair of complex conjugate embeddings of $K$ into the complex numbers. Note also that a finite prime $P$ is called dyadic when $2 \in P$; otherwise it is non-dyadic.

Now for a Witt class $X \in W(K)$, there is an invariant $c_P(X)$ for every prime $P$ in $K$, finite and infinite. This invariant is $+1$ or $-1$. We calculate these Hasse symbols as follows: If a representative $(V, b)$ of $X$ can be chosen so that $V$ is one-dimensional, then $c_P(X) = 1$ for all primes $P$. Otherwise, choose a representative $(V, b)$ with $\dim_K V \equiv 0 \text{ or } 1 \pmod{8}$. We may have to add one or more hyperbolic planes to accomplish this. Then take an orthogonal basis $e_1, \ldots, e_n$ for $(V, b)$, and let $a_i = b(e_i, e_i)$. Then

$$c_P(X) = \prod_{i < j} (a_i, a_j)_P,$$
where \((a_i, a_j)_P\) is the Hilbert symbol. Recall that a Hilbert symbol \((c, d)_P\) is defined as \((c, d)_P = 1\) if \(cx^2 + dy^2\) represents 1 in the completion \(K_P\), and \((c, d)_P = -1\) otherwise.

The properties of the Hasse symbols are

1. \(c_P(X) = 1\) for almost all primes,
2. \(c_P(X) = 1\) for all complex primes,
3. \(\prod c_P(X) = 1\) (This is called reciprocity).

There is a theorem due to Hasse that summarizes these four invariants:

**Theorem 1.4.** (see [2], Theorem I.2.2) Let \(K\) be an algebraic number field. An element of \(W(K)\) is uniquely determined by

1. the rank mod 2,
2. the discriminant mod squares,
3. the Hasse-Witt invariants,
4. the total signature, if \(K\) is not purely complex.

In other words, two elements of \(W(K)\) that have these four invariants in common are Witt equivalent. We mention without further comment that these four invariants classify forms over number fields, but not over fields in general, where the classification problem for inner product spaces is unsolved.

We also have a Lemma that shows how the invariants are dependent on one another.

**Lemma 1.5.** Let \(K\) be an algebraic number field, and let \(P\) be a real infinite prime. Then for \(X \in W(K)\), we have

1. \(\text{sgn}_P(X) \equiv \text{rk}(X) \text{ in } \mathbb{Z}/2\mathbb{Z}\).
2. \(\text{dis}(X) > 0\) in the ordering associated to \(P\) if and only if \(\text{sgn}_P(X) \equiv 0 \text{ or } 1 \pmod{4}\).
3. If \( \mathrm{sgn}_P(X) \equiv 0, 1, 6, \text{ or } 7 \pmod{8} \), then \( c_P(X) = 1 \). If \( \mathrm{sgn}_P(X) \equiv 2, 3, 4, \text{ or } 5 \pmod{8} \), then \( c_P(X) = -1 \).

Proof. Fix a representative \((V, b)\) of \( X \) with dimension \( n \), with \( n \equiv 0, 1 \pmod{8} \).

1. By definition of signature, \( \mathrm{sgn}_P(X) \) has the form \( 2s - n \), and \( 2s - n \equiv -n \equiv n \pmod{2} \). So \( \mathrm{sgn}_P(X) \equiv \mathrm{rk}(X) \pmod{2} \).

2. First of all, \( X \) can be diagonalized, so we can write \( X = \langle a_1, \ldots, a_n \rangle \). Assume \( \mathrm{sgn}_P(X) \equiv 0 \pmod{4} \). Then we can write \( \mathrm{sgn}_P(X) = 2s - n = 4k \) for some integer \( k \), so \( n = 2s - 4k \). Then

\[
dis(X) = (-1)^{(2s - 4k)(2s - 4k - 1)/2}(a_1 \cdots a_n) = (-1)^{(s - 2k)(2s - 4k - 1)}(a_1 \cdots a_n).
\]

From the definition of signature, we see that \( s \) is the number of \( a \)'s that are positive with respect to the chosen ordering, and \( n - s \) is the number of \( a \)'s that are negative. If \( s \) is even, then the exponent of \(-1\) is even, and \( n - s \) is even, so \( dis(X) > 0 \). If \( s \) is odd, then the exponent of \(-1\) is odd, and \( n - s \) is odd, so \( dis(X) > 0 \).

Now assume \( \mathrm{sgn}_P(X) \equiv 1 \pmod{4} \). Then \( \mathrm{sgn}_P(X) = 2s - n = 4k + 1 \) for some integer \( k \), so \( n = 2s - 4k - 1 \). Then

\[
dis(X) = (-1)^{(2s - 4k - 1)(2s - 4k - 2)/2}(a_1 \cdots a_n) = (-1)^{(2s - 4k - 1)(s - 2k - 1)}(a_1 \cdots a_n).
\]

If \( s \) is even, then the exponent of \(-1\) is odd, and \( n - s \) is odd, so \( dis(X) > 0 \). If \( s \) is odd, then the exponent of \(-1\) is even, and \( n - s \) is even, so \( dis(X) > 0 \).

Next we let \( \mathrm{sgn}_P(X) \equiv 2 \pmod{4} \). Then \( \mathrm{sgn}_P(X) = 2s - n = 4k + 2 \) for some integer \( k \), so \( n = 2s - 4k - 2 \). Then

\[
dis(X) = (-1)^{(2s - 4k - 2)(2s - 4k - 3)/2}(a_1 \cdots a_n) = (-1)^{(s - 2k - 1)(2s - 4k - 3)}(a_1 \cdots a_n).
\]

If \( s \) is even, then the exponent of \(-1\) is odd, and \( n - s \) is even, so \( dis(X) < 0 \). If \( s \) is odd, then the exponent of \(-1\) is even, and \( n - s \) is odd, so \( dis(X) < 0 \).
Finally we let \( sgn_P(X) \equiv 3 \pmod{4} \). Then \( sgn_P(X) = 2s - n = 4k + 3 \) for some integer \( k \), so \( n = 2s - 4k - 3 \). Then

\[
\text{dis}(X) = (-1)^{(2s-4k-3)(2s-4k-4)/2}(a_1 \cdots a_n) = (-1)^{(2s-4k-3)(s-2k-2)}(a_1 \cdots a_n).
\]

If \( s \) is even, then the exponent of \(-1\) is even, and \( n - s \) is odd, so \( \text{dis}(X) < 0 \). If \( s \) is odd, then the exponent of \(-1\) is odd, and \( n - s \) is even, so \( \text{dis}(X) < 0 \).

3. We will prove the claim for \( sgn_P(X) \equiv 0 \pmod{8} \) and \( sgn_P(X) \equiv 4 \pmod{8} \). The other cases are proved similarly.

First let \( sgn_P(X) \equiv 0 \pmod{8} \). Let \( X = \langle a_1, \ldots, a_s, b_1, \ldots, b_r \rangle \), where \( a_i > 0 \) for \( 1 \leq i \leq s \), and \( b_j < 0 \) for \( 1 \leq j \leq r \), with respect to a chosen ordering. So we have \( n = s + r \). Combining this with \( s - r = 8k \) for some integer \( k \) gives us \( n = 8k + 2r \). So we see that \( n \) is even, but we defined \( n \equiv 0 \) or \( 1 \pmod{8} \). So \( n \equiv 0 \pmod{8} \).

Let \( n = s + r = 8l \) for some integer \( l \). We can solve for \( r \) to get \( r = 4(l - k) = 4q \), where we let \( q = l - k \). Since we are calculating the Hasse symbol at a real infinite prime, the Hilbert symbol \((d_i, d_j)_P\) will only be \(-1\) if \( d_i \) and \( d_j \) are both negative. So we need to count the number of pairs of negative numbers, i.e. the number of \( i, j \) pairs such that \( 1 \leq i < j \leq 4q \). The number of such pairs is

\[
\sum_{i=1}^{4q-1} \left( \sum_{j=i+1}^{4q} 1 \right) = \sum_{i=1}^{4q-1} (4q - (i + 1) + 1) = \sum_{i=1}^{4q-1} (4q - i)
\]

\[
= 4q(4q - 1) - \frac{(4q - 1)(4q)}{2} = 8q^2 - 2q,
\]

which is even. So the number of \(-1\)'s will be even, giving us \( c_P(X) = 1 \).

Now let \( sgn_P(X) \equiv 4 \pmod{8} \). Let \( X \) be as above. Again we have \( n = s + r \), but in this case, \( s - r = 8k + 4 \) for some integer \( k \). Combining our two equalities, we see that \( n = 8k + 2r + 4 \), which is even. So we must have \( n \equiv 0 \pmod{8} \). Let \( n = s + r = 8l \) for some integer \( l \). Solving for \( r \), we get \( r = 2(2l - 2k - 1) = 2q \), where we let \( q = 2l - 2k - 1 \). Note that \( q \) is odd. As above, we need to count
the number of pairs of negative numbers, i.e. the number of \(i,j\) pairs such that \(1 \leq i < j \leq 2q\). We proceed as follows:

\[
\sum_{i=1}^{2q-1} \left( \sum_{j=i+1}^{2q} 1 \right) = \sum_{i=1}^{2q-1} (2q - (i + 1) + 1) = \sum_{i=1}^{2q-1} (2q - i) = 2q(2q - 1) - \frac{(2q - 1)(2q)}{2} = 2q^2 - q,
\]

which is odd. So the number of \(-1\)'s will be odd, giving us \(c_P(X) = -1\).

For every number field \(K\) there is an associated ring called the symbol ring of \(K\), and denoted by \(Sym(K)\). The elements of \(Sym(K)\) are triples \((a, b, c)\), where \(a\) is in \(\mathbb{Z}/2\mathbb{Z}\), \(b\) is in \(K^*/K^{**}\), and \(c\) is a function which assigns a value of 1 or \(-1\) to each prime of \(K\), with the following properties:

1. \(c\) is 1 for almost all primes,
2. \(c\) is 1 for every complex infinite prime,
3. the product of all the values of \(c\) is 1.

We will use the notation \([x, y]\) for the function assigning to each prime \(P\) the value of the Hilbert symbol \((x, y)_P\). Addition in \(Sym(K)\) is given by

\[
(a, b, c) + (a', b', c') = (a + a', (-1)^{aa'} bb', [-bb', (-1)^{aa'}][b, b'][cc']),
\]

and multiplication is

\[
(a, b, c)(a', b', c') = (aa', b^{aa'} b^{ta}, [b, b']^{1+aa'} c^a c^{ta}).
\]

There is a surjective ring homomorphism

\[
\alpha_K : W(K) \to Sym(K)
\]

such that

\[
\alpha_K(X) = (rk(X), dis(X), c(X))
\]
for every $X \in W(K)$, where $c(X)$ is a function which assigns to each prime $P$ the value of the Hasse symbol $c_P(X)$.

Note that if $X$ and $Y$ are classes in $W(K)$ that are in the fundamental ideal, $c(XY)$ is independent of $c(X)$ and $c(Y)$, and depends only on $\text{dis}(X)$ and $\text{dis}(Y)$:

$$
\alpha_K(XY) = \alpha_K(X)\alpha_K(Y) = (0, \text{dis}(X), c(X))(0, \text{dis}(Y), c(Y)) = (0, 1, [\text{dis}(X), \text{dis}(Y)]).
$$

**Theorem 1.6.** (see [2], Theorem I.2.5) For any number field $K$, there is a short exact sequence

$$
0 \to J^3 \to W(K) \to \text{Sym}(K) \to 0.
$$

By Theorem 1.4, an element of $W(K)$ is determined by its image in $\text{Sym}(K)$ and its total signature. Elements of $J^3$ are determined only by total signature. If $K$ is purely complex, then there are no signatures, so $J^3 = 0$ and $W(K) \cong \text{Sym}(K)$. If $K$ has $r$ real infinite primes, $r > 0$, then the total signature gives us the isomorphism $\text{Sgn} : J^3 \cong 8\mathbb{Z}^r$.

Now we give a theorem about the orders of classes in $\text{Sym}(K)$ and a corollary about the torsion classes in $W(K)$. We remark first that when $K$ can be ordered, the torsion classes in $W(K)$ are precisely the classes with total signature 0. Therefore torsion classes are completely determined by their image in $\text{Sym}(K)$. One checks directly that a torsion class in $\text{Sym}(K)$ has 2-power order.

**Theorem 1.7.** Every class in $\text{Sym}(K)$ has additive order dividing 8. The elements of order 8 are precisely the elements of odd rank.

**Proof.** Let $(a, b, c) \in \text{Sym}(K)$ have additive order 2. So we must have $2(a, b, c) = (0, 1, 1)$. We use the addition formula for $\text{Sym}(K)$:

$$
(a, b, c) + (a, b, c) = (0, (-1)^a, [-1, (-1)^a][b, b]) = (0, 1, 1).
$$
We see that \((-1)^a = 1\), so \(a = 0\).

Now let \((e, f, g) \in \text{Sym}(K)\) have order 4. So we have \(2(e, f, g) = (a, b, c) = (0, b, c)\). Calculating in \(\text{Sym}(K)\), we get:

\[
(e, f, g) + (e, f, g) = (0, (-1)^e, [-1, (-1)^e][f, f]) = (0, b, c).
\]

We have \((-1)^e = b\), so there are two cases.

Case 1: \(b = 1\). Then \(e = 0\). Let \((j, k, l) \in \text{Sym}(K)\) have order 8. Then we have \(2(j, k, l) = (e, f, g) = (0, f, g)\). As in the previous steps, calculating in \(\text{Sym}(K)\) gives us \((-1)^j = f\). If \(f = 1\), then \((0, f, g) = (0, 1, g)\), which has order 2. This contradicts the assumption that \((0, f, g)\) has order 4. So we must have \(f = -1\).

Thus \(j = 1\), and \((j, k, l)\) has odd rank.

Now let \((m, n, p) \in \text{Sym}(K)\) have order 16. We have \(2(m, n, p) = (j, k, l) = (1, k, l)\). But this will give us \(0 = 1\). So \((m, n, p)\) cannot have order 16.

Case 2: \(b = -1\). Then \(e = 1\). Let \((j, k, l) \in \text{Sym}(K)\) have order 8. Then \(2(j, k, l) = (e, f, g) = (1, f, g)\). This will lead to \(0 = 1\), a contradiction.

In summary, we see that a class in \(\text{Sym}(K)\) must have order dividing 8, and a class of even rank has order dividing 4.

\[ \square \]

**Corollary 1.8.** A torsion class in \(W(K)\) must have order dividing 8. Every torsion class of even rank has order dividing 4.

**Definition 1.9.** An element of \(W(K)\) is algebraic if it can be represented by the trace form of a finite separable extension of \(K\).

**Definition 1.10.** A Witt class in \(W(K)\) is abelian (resp. normal, cyclic) if it can be represented by the trace form of some abelian (resp. normal, cyclic) extension \(F/K\).
Remark 1.11. Let $K$ be a number field, and let $F/K$ be a finite separable extension of $K$. Let $\sigma : K \to R$ be an embedding of $K$ into the real numbers. Then $\text{sgn}_\sigma(F)$ is equal to the number of extensions $\tau$ of $\sigma$ to a mapping from $F$ to $R$. From this formulation, we see that if $F/K$ is a normal extension, then $\text{sgn}(F) = 0$ or $[F:K]$.

In this dissertation, we refer to a number field with $d$ dyadic primes and $r$ real infinite primes as a number field of type $(d, r)$. Chapter 4 contains a description of the abelian classes in $W(K)$ when $K$ has type $(1, 0)$, and in Chapter 5 we discuss the abelian classes in $W(K)$ when $K$ has type $(1, 1)$. At this time, determining the abelian classes in $W(K)$ when $K$ has general type $(d, r)$ remains open.

There is an extensive literature and active current research on trace forms. MathSciNet lists 91 papers with “trace form” in the title, published since 1990. None of these papers are needed for the results of this dissertation (the characterization of trace forms of abelian extensions), but we briefly discuss some of the more prominent papers on this list in order to put this dissertation in context.

The combination of the three papers of Epkenhans, Krüskemper, and Scharlau (see [3], [6], and [10]) gives a complete classification up to isometry of trace forms of algebraic extensions of number fields. Any form of rank 4 or greater is isometric to a trace form if and only if every signature is non-negative. An explicit list of forms of rank 1, 2, and 3 which are trace forms is given in [3]. These results imply that a Witt class $X$ in the Witt ring $W(K)$ of an algebraic number field $K$ is algebraic if and only if every signature is non-negative.

The paper of Serre (see [11]) contains an interesting application of trace forms to a problem in Galois Theory: Let $K$ be a field of characteristic different from 2. Given a field extension $E/K$, with Galois group $A_n$ (the alternating group),
and given a particular central group extension $\pi : \tilde{A}_n \to A_n$, does there exist a field $\tilde{E}$ containing $E$ with $Gal(\tilde{E}/K) \cong \tilde{A}_n$ for which the natural projection $Gal(\tilde{E}/K) \to Gal(E/K)$ gives the group extension $\pi$? The answer is “yes” if and only if the so-called “second Stiefel-Whitney” class of the trace form vanishes. In this paper, the author relates the second Stiefel-Whitney class to the Hasse-Witt invariant of the trace form. Hasse-Witt invariants are discussed earlier in this chapter.
Chapter 2
Selected Results from Other Works

In this chapter we collect various results from other sources that we will use in the later chapters.

**Theorem 2.1.** (see [2], Corollary I.6.3) Let $K$ be a number field. If $F/K$ is a finite normal extension and $E/K$ is any finite extension, then in $W(K)$ the product $\langle E \rangle \langle F \rangle$ is a multiple of an algebraic class; namely, $\langle E \rangle \langle F \rangle$ is a multiple of $\langle EF \rangle$:

$$\langle E \rangle \langle F \rangle = \frac{[E:K][F:K]}{[EF:K]} \cdot \langle EF \rangle.$$  

**Corollary 2.2.** (see [2], Corollary I.6.5) Let $K$ be a number field, and let $F/K$ be a finite extension. If the normal closure of $F/K$ has odd degree over $K$, then in $W(K)$

$$\langle F \rangle = \langle 1 \rangle.$$  

For the next theorem, recall that a group $G$ is metacyclic when $G$ contains a normal cyclic subgroup $N$ with cyclic quotient $G/N$. The set of all metacyclic groups includes the set of cyclic groups.

**Theorem 2.3.** (see [2], Theorem I.9.1) Let $F/Q$ be a normal extension of even degree. If the Sylow 2-subgroups of $\text{Gal}(F/Q)$ are not metacyclic, then $\langle F \rangle$ lies in the image of $W(Z)$ in $W(Q)$. Furthermore, either

1. $F$ is totally real and $\langle F \rangle = \langle F:Q \rangle \langle 1 \rangle$, or
2. $F$ is purely complex and $\langle F \rangle = 0$.

**Theorem 2.4.** (see [2], Theorem I.10.1, Corollary I.10.3, and note regarding generalization on page 57) Let $K$ be a number field. Take $X$ in $W(K)$ of even
rank. If $K$ has signatures, assume additionally that the value of any signature lies among the values 0, 2, or 4. Then $X$ is algebraic. If $X$ lies in $J^2$ and $\text{sgn}(X) = 0$ or 4, then $X$ can be represented by the trace form of a biquadratic extension of $K$.

The following theorem requires some explanation of the notation. Let $K$ be a non-dyadic local field, and let $E/K$ be an unramified extension of degree $f$. Let $O_K$ be the ring of local integers in $K$, and let $O_K^*$ denote the units of $O_K$. The group $O_K^{**}$ consists of squares of units. If $\pi$ is a prime element in $K$ and $a \neq 1$ in $O_K^*/O_K^{**}$ is a non-square local unit, then the four classes $\langle 1 \rangle$, $\langle \pi \rangle$, $\langle a \rangle$, and $\langle a\pi \rangle$ additively generate $W(K)$.

**Theorem 2.5.** (see [2], Theorem II.3.2, even degree cases; notation has been modified to be consistent with this dissertation) Let $E/K$ be an unramified local extension of degree $f$, and let $b$ be a non-square unit in $E$. Recall that $\langle E_b \rangle$, $\langle E_\pi \rangle$, and $\langle E_{b\pi} \rangle$ are the trace forms of $E$ scaled by $b$, $\pi$, and $b\pi$, respectively.

If $f$ is even and either $-1$ is a square in $K$ or $f \equiv 0 \pmod{4}$, then in $\text{Sym}(K)$,

$$\alpha_K(\langle E \rangle) = (rk\langle E \rangle, \text{dis}\langle E \rangle, c_P\langle E \rangle) = (0, a, 1),$$

$$\alpha_K(\langle E_b \rangle) = (0, 1, 1) = 0,$$

$$\alpha_K(\langle E_\pi \rangle) = (0, a, -1), \text{ and}$$

$$\alpha_K(\langle E_{b\pi} \rangle) = (0, 1, 1) = 0.$$

If $f \equiv 2 \pmod{4}$ and $-1$ is not a square in $K$, then

$$\alpha_K(\langle E \rangle) = (0, 1, 1) = 0,$$

$$\alpha_K(\langle E_b \rangle) = (0, -1, 1) = (0, a, 1),$$

$$\alpha_K(\langle E_\pi \rangle) = (0, 1, 1) = 0, \text{ and}$$

$$\alpha_K(\langle E_{b\pi} \rangle) = (0, -1, -1) = (0, a, -1).$$
Lemma 2.6. (see [2], Lemma II.6.3, even degree case; notation has been modified to be consistent with this dissertation) Let $F/E$ be a totally and tamely ramified local extension of degree $e$, with $e$ even. Then

$$\alpha_E(\langle F \rangle) = (0, \pi, (\pi, -e)_P),$$

where $\pi$ is a local uniformizer of $E$, chosen so that $F = E(\sqrt[1]{\pi})$.

Lemma 2.7. (see [2], Lemma V.7.4) Let $F/Q_p$ be a cyclic extension of the $p$-adic rationals of degree $2^{k+1} \geq 2$. Let $E$ be the unique subfield of $F$ of degree $2^k$ over $Q_p$. That is, $[F : E] = 2$. If $-1$ is not a square in $Q_p$, then $E/Q_p$ is unramified. In particular, if $F/Q_p$ is ramified then

$$e(F/Q_p) = 2.$$  

Theorem 2.8. (Approximation Theorem, page 137 of [5]) Let $K$ be a number field. Let $| \cdot |_1, \ldots , | \cdot |_n$ be nontrivial, pairwise inequivalent absolute values on $K$ and let $\beta_1, \ldots , \beta_n$ be any $n$ elements of $K$. For any positive real $\epsilon$, there is an $\alpha \in K$ such that $|\alpha - \beta_i|_i < \epsilon$ for all $i = 1, \ldots , n$.

Theorem 2.9. (Realization by Hilbert symbols, see Theorem 71:19 of [9]; notation has been modified to be consistent with this dissertation) Let $T$ be a set consisting of an even number of discrete or real spots on an algebraic number field $F$. Then there are $\alpha, \beta$ in $F$ such that

$$(\alpha, \beta)_P = \begin{cases} -1 & \text{if } P \in T, \\ 1 & \text{if } P \notin T. \end{cases}$$

Proposition 2.10. (see [7], Proposition 3.20; notation has been modified to be consistent with this dissertation) Let $F$ be a number field. Let $E_1$ and $E_2$ be field extensions of $F$ contained in some common field. If $E_1$ and $E_2$ are Galois over $F$,  

16
then $E_1E_2$ and $E_1 \cap E_2$ are Galois over $F$, and

$$
\sigma \mapsto (\sigma|_{E_1}, \sigma|_{E_2}) : \text{Gal}(E_1E_2/F) \to \text{Gal}(E_1/F) \oplus \text{Gal}(E_2/F)
$$

is an isomorphism of $\text{Gal}(E_1E_2/F)$ onto the subgroup

$$
H = \{ (\sigma_1, \sigma_2) : \sigma_1|_{E_1 \cap E_2} = \sigma_2|_{E_1 \cap E_2} \}
$$

of $\text{Gal}(E_1/F) \oplus \text{Gal}(E_2/F)$.

**Lemma 2.11.** (see [8], Corollary 3.4) If $R$ is a local ring in which 2 is a unit, then every symmetric inner product space $X$ over $R$ possesses an orthogonal basis. That is, $X$ possesses a basis $e_1, \ldots, e_k$ so that $e_i \cdot e_j = 0$ for $i \neq j$, and $e_i \cdot e_i = u_i$ for some unit $u_i$ in $R$. In other words,

$$
X \cong \langle u_1, \ldots, u_k \rangle
$$

for suitable units $u_1, \ldots, u_k$. 

17
Chapter 3
Abelian Witt Classes over Arbitrary Number Fields

The following results are true for all number fields $K$ and will be used in the remaining chapters.

**Theorem 3.1.** Let $K$ be a number field. Then $0 \in W(K)$ is abelian.

*Proof.* Case 1: If $-1$ is not a square in $K$, then $\langle K(\sqrt{-1}) \rangle = \langle 2, -2 \rangle$, which is a hyperbolic plane and therefore Witt equivalent to 0.

Case 2: If $-1$ is a square in $K$, then choose primes $p_1, p_2, p_3$ such that none of them divide $\text{Dis}(K/Q)$ and so that $[K(\sqrt{-p_1}, \sqrt{-p_2}, \sqrt{-p_3}) : K] = 8$. Theorem 2.1 gives us

$$\langle K(\sqrt{-p_1}, \sqrt{-p_2}, \sqrt{-p_3}) \rangle = \langle K(\sqrt{-p_1}) \rangle \langle K(\sqrt{-p_2}) \rangle \langle K(\sqrt{-p_3}) \rangle.$$ 

Each $\langle K(\sqrt{-p_i}) \rangle$ has even rank and is therefore in $J$, so the product of all three is in $J^3$. But $J^3$ is 0 since $K$ is totally complex, so $\langle K(\sqrt{-p_1}, \sqrt{-p_2}, \sqrt{-p_3}) \rangle$ is Witt equivalent to 0.

**Theorem 3.2.** If $s \neq 1$ in $K^*/K^{**}$, then $\langle 2, 2s \rangle$ is abelian and is represented by the trace form of $K(\sqrt{s})/K$.

*Proof.* A basis for $K(\sqrt{s})/K$ is $\{1, \sqrt{s}\}$, so an element $v$ of $K(\sqrt{s})$ can be written as $v = x + y \sqrt{s}$, with $x, y \in K$. So

$$tr_{K(\sqrt{s})/K}(v^2) = tr_{K(\sqrt{s})/K}(x^2 + 2xy\sqrt{s} + sy^2) = 2x^2 + 2sy^2 = \langle 2, 2s \rangle.$$

**Lemma 3.3.** Every abelian class in $W(K)$ is a product of cyclic classes in $W(K)$. 

Proof. Let $X \in W(K)$ be abelian, i.e. $X = \langle F \rangle$ for some abelian extension $F$ of $K$. If $F/K$ is a cyclic extension, we are done. So we will assume that $F/K$ is not cyclic.

Let $G = Gal(F/K)$. Then $G$ is abelian, so we can write $G = \bigoplus_p G_p$, where $p$ is prime and $G_p$ is a Sylow $p$-subgroup. We can further write $G = G_1 \oplus G_2$, where $G_1 = \bigoplus_{p \neq 2} G_p$, and $G_2$ is a Sylow 2-subgroup. Let $G'_1$ and $G'_2$ be the fixed fields of $G_1$ and $G_2$, respectively. We have $[G'_1 : K] = |G_2| = 2^i$, and $[G'_2 : K] = |G_1|$, which is odd. Since $[G'_1 : K]$ and $[G'_2 : K]$ are relatively prime,


So $G'_1 G'_2 = F$. By Theorem 2.1, we get

$$\langle G'_1 \rangle \langle G'_2 \rangle = \left[ \frac{G'_1 : K}{[G'_1 G'_2 : K]} \right] \cdot \langle G'_1 G'_2 \rangle = \langle G'_1 \rangle \langle G'_2 \rangle = \langle F \rangle.$$

Now $G'_2/K$ is a finite abelian extension of odd degree, so by Corollary 2.2, $\langle G'_2 \rangle = |G_1|\langle 1 \rangle$. But there is a cyclic extension $L$ of $K$ with $[L : K] = |G_1|$, and we have $\langle L \rangle = |G_1|\langle 1 \rangle = \langle G'_2 \rangle$. So $\langle G'_2 \rangle$ is a cyclic Witt class.

Now we must show that $\langle G'_1 \rangle$ is a product of cyclic classes. We have $G_2 \cong Gal(G'_1/K)$. If $G_2$ is a cyclic group, we are done. If not, we will proceed by induction. Assume $G_2 = C_1 \oplus C_2$, where $C_1$ and $C_2$ are cyclic. Let $F_1$ be the fixed field of $C_2$, and let $F_2$ be the fixed field of $C_1$. Then $F_1 \cap F_2 \subseteq G'_1$ corresponds to the subgroup of $G_2$ generated by $C_2$ and $C_1$. But $\langle C_2, C_1 \rangle = C_1 \oplus C_2 = G_2$. So $F_1 \cap F_2 = K$. This implies that

$$[F_1 F_2 : K] = [F_1 : K][F_2 : K] = |C_2||C_1| = |G_2| = [G'_1 : K].$$

So $\langle F_1 \rangle \langle F_2 \rangle = \langle F_1 F_2 \rangle = \langle G'_1 \rangle$. This gives us

$$\langle F \rangle = \langle G'_1 \rangle \langle G'_2 \rangle = \langle F_1 \rangle \langle F_2 \rangle \langle G'_2 \rangle,$$
where \( \langle F_1 \rangle, \langle F_2 \rangle, \text{ and } \langle G_2' \rangle \) are all cyclic classes.

Now assume that if we have \( G_2 = C_1 \oplus \cdots \oplus C_n \), with \( C_i \) cyclic for all \( i \), then
\[
\langle G'_1 \rangle = \langle F_1 \cdots F_n \rangle = \langle F_1 \rangle \cdots \langle F_n \rangle,
\]
where \( F_i \) is the fixed field of \( \bigoplus_{j \neq i} C_j \). Then let \( G_2 = C_1 \oplus \cdots \oplus C_n \oplus C_{n+1} \), where \( C_i \) is cyclic for all \( i \). By induction, we have
\[
\langle F_1 \rangle \cdots \langle F_n \rangle \langle F_{n+1} \rangle = \langle F_1 \cdots F_n \rangle \langle F_{n+1} \rangle.
\]

Similar to the case with two cyclic groups, \((F_1 \cdots F_n) \cap F_{n+1} \subseteq G'_1\) corresponds to the subgroup of \( G_2 \) generated by \( C_{n+1} \) and \( \bigoplus_{j \neq n+1} C_j \). But
\[
\langle C_{n+1}, \bigoplus_{j \neq n+1} C_j \rangle = C_1 \oplus \cdots \oplus C_{n+1} = G_2.
\]
So \((F_1 \cdots F_n) \cap F_{n+1} = K\). This gives us
\[
\langle F_1 \cdots F_n \rangle \langle F_{n+1} \rangle = \langle F_1 \cdots F_n F_{n+1} \rangle = \langle G'_1 \rangle.
\]
So
\[
\langle F \rangle = \langle F_1 \rangle \cdots \langle F_{n+1} \rangle \langle G'_2 \rangle,
\]
where \( \langle F_1 \rangle, \ldots, \langle F_{n+1} \rangle \), and \( \langle G'_2 \rangle \) are all cyclic classes.

\[\blacksquare\]

**Lemma 3.4.** (see [2], Lemma I.11.2) A Witt class \( X \in W(K) \) is abelian if and only if \( X = m\langle F \rangle \) for an abelian extension \( F \) of \( K \) of degree \( 2^k \), \( k \geq 0 \), and an odd positive integer \( m \).

**Proof.** We first assume that \( X \) is abelian. So let \( X = \langle E \rangle \), with \( E/K \) abelian. Then the Galois group \( \text{Gal}(E/K) \) is a direct product \( \text{Gal}(E/K) = G_1 \times G_2 \), where \( G_1 \) is a Sylow 2-subgroup of order \( 2^k \), and \( G_2 \) is a subgroup of odd order \( m \). The fixed field \( E_1 \) of \( G_2 \) is normal over \( K \) with Galois group \( G_1 \), and the fixed field \( E_2 \) of \( G_1 \) is normal with Galois group \( G_2 \). The two fields \( E_1 \) and \( E_2 \) are linearly disjoint, so by Theorem 2.1,
\[
\langle E \rangle = \langle E_1 \rangle \langle E_2 \rangle.
\]
Since $E_2/K$ is an abelian, odd degree extension, Corollary 2.2 gives us $\langle E_2 \rangle = m\langle 1 \rangle$.

So $X = \langle E \rangle = m\langle E_1 \rangle$.

Now we assume that $X = m\langle F \rangle$, where $F/K$ is an abelian extension of degree $2^k$, $k \geq 0$, and $m > 1$ is an odd integer. We first choose a prime number $p$ such that $Q(\zeta) \cap K = Q$, where $\zeta$ is a $p$-th root of unity. Then $Q(\zeta) \cdot K = K(\zeta)$, so $K(\zeta)$ contains a unique cyclic subfield $E$ of degree $m$ over $K$. Since $E$ is linearly disjoint from $F$ over $K$, the trace form of the compositum of $E$ and $F$ is $\langle EF \rangle = \langle E \rangle \langle F \rangle = m\langle F \rangle = X$. So $X$ is abelian.

\textbf{Theorem 3.5.} If $k \geq 3$, then $2^k\langle 1 \rangle$ is abelian in $W(K)$.

\textit{Proof.} We begin by working in $W(Q)$. Take $k \geq 3$ real quadratic fields whose discriminants are distinct primes. By Theorem 2.3, the trace form of the compositum represents $2^k\langle 1 \rangle$.

Now, for $W(K)$, where $K$ is any number field, take $k \geq 3$ fields whose discriminants are distinct primes such that $K^\sigma \cap Q(\sqrt{p_i}) = Q$ for all $K^\sigma$ conjugates of $K$ and for $1 \leq i \leq k$. Then the trace form of $K(\sqrt{p_1}, \ldots, \sqrt{p_k})$ represents $2^k\langle 1 \rangle$, and $Gal(K(\sqrt{p_1}, \ldots, \sqrt{p_k})/K) \cong Gal(Q(\sqrt{p_1}, \ldots, \sqrt{p_k})/Q)$. Therefore $2^k\langle 1 \rangle$ is abelian in $W(K)$. \hfill \square
Chapter 4

Abelian Witt Classes over Number Fields of Type (1, 0)

Recall that a number field $K$ of type (1, 0) has one dyadic prime and no real infinite primes, so $K$ is a totally complex field. The Witt classes of abelian extensions of odd degree are classified in Corollary 2.2, and those of degree 2 are classified in Theorem 3.2.

Now we wish to prove that the abelian classes in $W(K)$ are closed under multiplication. Then, to describe the trace forms of all abelian extensions, in light of Corollary 2.2 and Theorem 3.2 we will just have to find the classes in $W(K)$ that can be represented by the trace form of a cyclic extension of $K$ of degree $2^k$ for some $k \geq 2$.

**Theorem 4.1.** Every Witt class in the square of the fundamental ideal in $W(K)$ is abelian.

*Proof.* Let $X$ be in $J^2$. Then $rk(X)$ is even and $dis(X) = 1$ in $K^*/K^{**}$. Since $K$ is totally complex, there are no signatures, so $J^3 = 0$. If $X$ is in $J^3$, then $X$ is 0 and hence is abelian by Theorem 3.1. So assume $X \notin J^3$.

Now we must proceed with two cases.

Case 1: $-1$ is a square in $K^*$. Let

$$S_X = \{ p \mid p \text{ a prime of } K \text{ and } c_p(X) = -1 \}.$$ 

Then $S_X$ is a finite, non-empty set of even order. For every $p \in S_X$, pick $b_p \in K^*$ such that $b_p \in K_p^* \setminus K_p^{**}$. For any choice of $\epsilon_p > 0$, the Approximation Theorem (Theorem 2.8) tells us that there is an element $b \in K^*$ such that $|b - b_p|_p < \epsilon_p$ for
every $p \in S_X$. Two elements that are sufficiently close $p$-adically are in the same square class, so $b \in K_p^* \setminus K_p^{**}$ for all $p \in S_X$.

By Realization by Hilbert symbols (Theorem 2.9), there is an $a \in K^*$ such that $(a, b)_p = c_p(X)$ for all primes $p$ of $K$. We will analyze $\langle K(\sqrt{-a}) \rangle$ and $\langle K(\sqrt{-b}) \rangle$. Note that $K(\sqrt{-a})$ and $K(\sqrt{-b})$ are linearly disjoint. To see this, assume that $K(\sqrt{-a}) = K(\sqrt{-b})$. This implies that $a = b$ in $K^*/K^{**}$, so, using the fact that $-1$ is a square in $K^*$, we have

$$(a, b)_p = (b, b)_p = (b, -b)_p = 1 = c_p(X)$$

for all primes $p$ of $K$. This contradicts $c_p(X) = -1$ for $p \in S_X$, which is a nonempty set. So $K(\sqrt{-a}) \neq K(\sqrt{-b})$, and we see that $K(\sqrt{-a})$ and $K(\sqrt{-b})$ are linearly disjoint.

Case 2: $-1$ is not a square in $K^*$. Let $S_X$ be defined as in Case 1. Since $-1$ is not a square in $K^*$, there are infinitely many finite primes $q$ at which $-1$ is not a square in $K_q$. Fix such a $q$ that is both non-dyadic and not in $S_X$. So $c_q(X) = 1$. As above, for every $p \in S_X$, pick $b_p \in K^*$ such that $b_p \in K_p^* \setminus K_p^{**}$. Additionally, let $b_q$ be a local prime element at $q$. Then by Theorem 2.8, there is an element $b \in K^*$ such that $|b - b_p|_p < \epsilon_p$ for every $p \in S_X \cup \{q\}$. Again by Realization by Hilbert symbols, there is an element $a \in K^*$ such that $(a, b)_p = c_p(X)$ for all primes $p$ of $K$. We will show that $K(\sqrt{-a})$ and $K(\sqrt{-b})$ are linearly disjoint in this case. If $K(\sqrt{-a}) = K(\sqrt{-b})$, then $a = b$ in $K^*/K^{**}$. So $c_q(X) = (a, b)_q = (b, b)_q = (b, -1)_q = -1$, since $-1$ is not a square in $K_q$. But this is a contradiction, since we chose $q$ so that $c_q(X) = 1$.

At this point, the two cases converge, and we proceed as follows:
Note that \( \langle K(\sqrt{-a}) \rangle = \langle 2, -2a \rangle \), and \( \langle K(\sqrt{-b}) \rangle = \langle 2, -2b \rangle \), so we see that both \( \langle K(\sqrt{-a}) \rangle \) and \( \langle K(\sqrt{-b}) \rangle \) have rank congruent to 0 modulo 2. We also have \( \text{dis}(\langle K(\sqrt{-a}) \rangle) = 4a \equiv a \in K^*/K^{**} \), and \( \text{dis}(\langle K(\sqrt{-b}) \rangle) = 4b \equiv b \in K^*/K^{**} \).

Since \( J^3 = 0 \), there being no signatures, the surjective ring homomorphism \( \alpha_K : W(K) \to \text{Sym}(K) \) is an isomorphism, and

\[
\alpha_K(X) = (\text{rk}(X), \text{dis}(X), c(X))
\]

for every \( X \in W(K) \), where \( c(X) \) is the function which assigns to each prime \( P \) the value of the Hasse symbol \( c_P(X) \). Then \( \alpha_K(\langle K(\sqrt{-a}) \rangle) = (0, a, c\langle K(\sqrt{-a}) \rangle) \), and \( \alpha_K(\langle K(\sqrt{-b}) \rangle) = (0, b, c\langle K(\sqrt{-b}) \rangle) \). We can determine the rank, discriminant, and Hasse-Witt invariants of the product \( \langle K(\sqrt{-a}) \rangle \langle K(\sqrt{-b}) \rangle \) by calculating the product of the two corresponding elements in \( \text{Sym}(K) \):

\[
(0, a, c\langle K(\sqrt{-a}) \rangle)(0, b, c\langle K(\sqrt{-b}) \rangle) = (0, a^0 b^0, [a, b]^1 c\langle K(\sqrt{-a}) \rangle^0 c\langle K(\sqrt{-b}) \rangle^0)
\]

\[
= (0, 1, [a, b]) = (0, 1, c(X)).
\]

So \( X \) and \( \langle K(\sqrt{-a}) \rangle \langle K(\sqrt{-b}) \rangle \) are Witt equivalent in \( W(K) \). Since \( K(\sqrt{-a}) \) and \( K(\sqrt{-b}) \) are linearly disjoint, Theorem 2.1 gives us

\[
\langle K(\sqrt{-a}) \rangle \langle K(\sqrt{-b}) \rangle = \langle K(\sqrt{-a})K(\sqrt{-b}) \rangle = \langle K(\sqrt{-a}, \sqrt{-b}) \rangle.
\]

Therefore, \( X \) is abelian.

**Corollary 4.2.** The abelian classes in \( W(K) \) are closed under multiplication.

**Proof.** Let \( X \) and \( Y \) be abelian Witt classes.

Case 1: \( X \) and \( Y \) both have even rank. Then \( X \) and \( Y \) both lie in \( J \), so \( XY \) is in \( J^2 \) and is abelian by Theorem 4.1.

Case 2: \( X \) and \( Y \) both have odd rank. Then \( X = m\langle 1 \rangle \), and \( Y = n\langle 1 \rangle \), where \( m \) and \( n \) are odd, by Corollary 2.2. So \( XY = mn\langle 1 \rangle \), which is abelian by Lemma 3.4.
Case 3: Without loss of generality, suppose $X$ has odd rank and $Y$ has even rank. Then $X = m\langle 1 \rangle$, where $m$ is odd. So $XY = mY$, which is abelian by Lemma 3.4. □

**Lemma 4.3.** Let $K$ be any number field, not necessarily assumed to be of type $(1, 0)$. Let $N/K$ be a cyclic extension of degree $2^k \geq 8$. Then $c_P\langle N \rangle_K = 1$ for every finite, non-dyadic prime $P$ of $K$ that is not totally ramified in $N/K$.

**Proof.** First assume that $P$ is unramified in $N/K$. Let $PO_N = P_1 \cdots P_r$. So we have local extensions $N_{P_1}, \ldots, N_{P_r}$ of $K_P$. We can write

$$\langle N \rangle_{K_P} = \bigoplus_{i=1}^{r} \langle N_{P_i} \rangle_{K_P} = \langle a_1, \ldots, a_n \rangle,$$

where $n = 2^k$. $N_{P_i}/K_P$ is an unramified local extension, which means that the ring of integers $O_{N_{P_i}}$ becomes a symmetric inner product space over $O_{K_P}$. In other words, the field discriminant of $N_{P_i}/K_P$ is a local unit in $O_{K_P}$. Then, by Lemma 2.11, the $a_i$’s can be chosen to be units in $O_{K_P}^*$. So

$$c_P\langle N \rangle_K = \prod_{i<j} (a_i, a_j)_P = 1.$$

Now assume $P$ is ramified but not totally so, and let $e$ be the ramification index. Assume that $P$ splits into $r$ prime ideals in $N$. Let $E$ be the maximal extension of $K$ contained in $N$ such that $P$ is unramified in $E$. So $PO_E = P_1 \cdots P_r$, and each $P_i$ is totally ramified with exponent $e$ in $N/E$. Let $K' = K_P$. Let $P'$ be any fixed prime of $N$ lying over $P$, and let $N' = N_{P'}$. Take $E'$ to be the completion of $E$ at $P' \cap E$. Let $O_{K'}$ be the ring of local integers in $K'$. Let $\pi$ be a prime element in $K'$ and $a \neq 1$ in $O_{K'}^*/O_{K'}^{**}$ a non-square local unit. Let $b$ be a non-square unit in $E'$.

Since $N'/E'$ is a totally ramified extension of 2-power degree, and $P$ is non-dyadic, we see that $N'/E'$ is a totally and tamely ramified extension. As such,
$N'/E'$ is generated by a root of an Eisenstein polynomial of the form $f(x) = x^e - u\pi$, where $u$ is some unit in $E'$. So we have $N' = E'({\sqrt[1]{u\pi}})$. Assume that $u$ is a unit in $K'$. Since $N'/K'$ is cyclic, $E'({\sqrt[1]{u\pi}})/K'$ is also cyclic. But $E'({\sqrt[1]{u\pi}}) = K'({\sqrt[1]{u\pi}})E'$, which is not cyclic, giving us a contradiction. So $u$ is not a unit in $K'$.

Case 1: $-1$ is a square in $K$. We will make use of the homomorphism $\alpha_{E'}: W(E') \to Sym(E')$. By Lemma 2.6, with $F = N'$ and with $\pi$ being replaced by the current $u\pi$, we have

$$\alpha_{E'}(\langle N' \rangle_{E'}) = (0, u\pi, (u\pi, -e)_P).$$

From the comments above we exclude $u = 1$ and $u = a$, leaving $u = b$ (up to squares). Remember that we have $e|2^k$, so let $e = 2^j$. Then $c_P(\langle N' \rangle_{E'}) = (b\pi, -e)_P = (b\pi, -2^j)_P$.

Case 1a: $j$ is even. Then

$$c_P(\langle N' \rangle_{E'}) = (b\pi, -1)_P(b\pi, 2^j)_P = (b\pi, -1)_P.$$

The trace form $\langle 1, b\pi \rangle_{E'}$ is Witt equivalent to $\langle N' \rangle_{E'}$ (remembering that $-1$ is a square). So to get $\langle N' \rangle_{K'}$, we can trace $\langle 1, b\pi \rangle_{E'}$ all the way down to $K'$, and we have $\langle N' \rangle_{K'} = \langle E' \rangle_{K'} + \langle E'_{b\pi} \rangle_{K'}$, where $\langle E'_{b\pi} \rangle_{K'}$ is the trace form of $E'$ scaled by $b\pi$. We can apply Theorem 2.5 to get $\alpha_{K'}(\langle N' \rangle_{K'}) = (0, a, 1)$. Now $\langle N \rangle_K = \bigoplus_r \langle N' \rangle_{K'}$, so

$$\alpha_K(\langle N \rangle_K) = r\alpha_{K'}(\langle N' \rangle_{K'}) = r(0, a, 1)$$

$$\begin{cases} (0, a, 1) & \text{when } r = 1, \\ (0, 1, 1) & \text{when } r \geq 2. \end{cases}$$

Either way, we see that $c_P(\langle N \rangle_K) = 1$.

Case 1b: $j$ is odd. Then in $W(E')$,

$$c_P(\langle N' \rangle_{E'}) = (b\pi, -2)_P(b\pi, 2^j)_P = (b\pi, -2)_P.$$
The trace form $\langle 2, 2b\pi \rangle_{E'}$ is Witt equivalent to $\langle N' \rangle_{E'}$. We trace $\langle 2, 2b\pi \rangle_{E'}$ down to $K'$ to get $\langle N' \rangle_{K'} = \langle 2 \rangle_{K'} \langle E' \rangle_{K'} + \langle 2 \rangle_{K'} \langle E_{b\pi} \rangle_{K'}$. Again we use Theorem 2.5 to get
\[
\alpha_{K'}(\langle N' \rangle_{K'}) = (1, 2, 1)(0, a, 1) = (0, a, [2, a]) = (0, a, 1).
\]
As in Case 1a, $c_P(\langle N \rangle_K) = 1$.

Case 2: $-1$ is not a square in $K$. By Lemma 2.7, $e = 2$, and consequently $N' = E'(\sqrt{b\pi})$. By Theorem 3.2, $\langle N' \rangle_{E'} = \langle 2, 2b\pi \rangle$. If $f \geq 4$, we proceed as in Case 1b to get $c_P(\langle N \rangle_K) = 1$. If $f = 2$, we have
\[
\alpha_{K'}(\langle N' \rangle_{K'}) = (1, 2, 1)(0, a, -1) = (0, a, -[2, a]) = (0, a, -1).
\]
In this case, $r \geq 2$, so
\[
\alpha_K(\langle N \rangle_K) = r(0, a, -1) = (0, 1, 1).
\]
Again, $c_P(\langle N \rangle_K) = 1$. \hfill \Box

**Theorem 4.4.** Let $K$ be a totally complex number field with one dyadic prime, and let $N/K$ be a cyclic extension of degree $2^k \geq 8$, with $k$ odd (resp. even). Then \[\langle N \rangle = \langle 2, -2m \rangle \text{ (resp. } \langle N \rangle = \langle 1, -m \rangle)\], where $\text{dis}(\langle N \rangle) = m \neq 1 \in K^*/K^{**}$.

**Proof.** $N$ has even rank, as do both $\langle 2, -2m \rangle$ and $\langle 1, -m \rangle$. Also, we see that $\text{dis}(\langle 2, -2m \rangle) = 4m \equiv m \in K^*/K^{**}$, and $\text{dis}(\langle 1, -m \rangle) = m \in K^*/K^{**}$.

Now we must calculate the Hasse symbols.

Case 1: $k$ is odd.

Case 1a: Let $P$ be a non-dyadic prime ideal of $K$ that is ramified in $K(\sqrt{m})$. Then $P$ is totally ramified in $N/K$, and the ramification index is $e = 2^k$. Since $P$ is totally ramified, we can apply Lemma 2.6:
\[
c_P(\langle N \rangle_K) = (m, -e)_P = (m, -2^k)_P = (m, -2)_P(m, 2)^{k-1}_P = (m, -2)_P.
\]
We also calculate the symbols for $\langle 2, -2m \rangle$ by adding three hyperbolic planes:

$$c_P\langle 2, -2m, 1, -1, 1, -1, 1, -1 \rangle_K = (2, -2m)_P (2, 1)_P^3 (2, -1)_P^3 (-2m, 1)_P^3 (-2m, -1)_P^3 (1, -1)_P^3$$

$$= (2, -2m)_P (-2m, -1)_P (-1, -1)_P = (2, -2)_P (2, m)_P (-2, -1)_P (m, -1)_P (-1, -1)_P$$

$$= (2, m)_P (2m, -1)_P (2, m)_P (2, -1)_P (m, -1)_P = (m, -2)_P = c_P\langle N \rangle_K.$$

Case 1b: Let $P$ be a non-dyadic prime ideal that is not ramified in $K(\sqrt{m})$. Then $P$ is not totally ramified in $N/K$, so $c_P\langle N \rangle_K = 1$ by Lemma 4.3. Also, $c_P\langle 2, -2m \rangle_K = (m, -2)_P = 1$, so $c_P\langle N \rangle_K = c_P\langle 2, -2m \rangle_K$.

Reciprocity tells us that the symbols of $\langle N \rangle$ and $\langle 2, -2m \rangle$ at the dyadic prime must also be equal, so we find that $\langle N \rangle$ and $\langle 2, -2m \rangle$ are Witt equivalent in $W(K)$.

Case 2: $k$ is even.

Case 2a: Let $P$ be as in Case 1a. Again by Lemma 2.6, we have

$$c_P\langle N \rangle_K = (m, -e)_P = (m, -2^k)_P = (m, -1)_P (m, 2)_P^k = (m, -1)_P.$$

We calculate the symbols for $\langle 1, -m \rangle$ by again adding three hyperbolic planes:

$$c_P\langle 1, -m, 1, -1, 1, -1, 1, -1 \rangle_K = (-1, -m)_P^3 (-1, -1)_P^3$$

$$= (-1, -m)_P (-1, -1)_P = (-1, m)_P = c_P\langle N \rangle_K.$$

Case 2b: Let $P$ be as in Case 1b. Again by Lemma 4.3, $c_P\langle N \rangle_K = 1$. Also, $c_P\langle 1, -m \rangle_K = (-1, m)_P = 1$, so $c_P\langle N \rangle_K = c_P\langle 1, -m \rangle_K$.

Applying reciprocity again, we see that $\langle N \rangle$ and $\langle 1, -m \rangle$ are Witt equivalent in $W(K)$.\hfill\Box

Whereas Lemma 4.3 discussed extensions of 2-power degree $\geq 8$, we now consider extensions of degree 4.
Lemma 4.5. Let $K$ be any number field, not necessarily assumed to be of type $(1, 0)$. Let $N/K$ be a cyclic extension of degree 4. If $P$ is a non-dyadic prime ideal of $K$ that is unramified in $N/K$, then $c_P(N)_K = 1$. If $P$ is a non-dyadic prime ideal that is ramified but not totally ramified in $N/K$, then $c_P(N)_K = 1$ if $-1$ is a square in $K_P$, and $c_P(N)_K = -1$ if $-1$ is not a square in $K_P$.

Proof. First assume that $P$ is unramified in $N/K$. As in Lemma 4.3, $c_P(N)_K = 1$.

Now assume $P$ is ramified but not totally so, and let $e$ be the ramification index. Clearly we must have $e = 2$. Let $E$ be the maximal extension of $K$ contained in $N$ such that $P$ is unramified in $E$. Let $N', E'$, and $K'$ be the local fields corresponding to $N$, $E$, and $K$, respectively. Since $[N : K] = efr = 4$ and $e = 2$, we have two cases: $f = 2, r = 1$ and $f = 1, r = 2$.

Case 1: $f = 2$ and $r = 1$. Take $π$ and $b$ to be as in the proof of Lemma 4.3. By the same argument as in that lemma, we must have $N' = E'(\sqrt{bπ})$. By Theorem 3.2, $\langle N' \rangle_{E'} = \langle 2, 2bπ \rangle_{E'}$. We trace $\langle 2, 2bπ \rangle_{E'}$ down to $K'$ to get $\langle N' \rangle_{K'} = \langle 2 \rangle_{K'}\langle E' \rangle_{K'} + \langle 2 \rangle_{K'}\langle bπ \rangle_{K'}$.

Case 1a: $-1$ is a square in $K$. Again we use Theorem 2.5 to get

$$\alpha_{K'}(\langle N' \rangle_{K'}) = (1, 2, 1)(0, a, 1) = (0, a, [2, a]) = (0, a, 1).$$

So $c_P(N)_K = 1$.

Case 1b: $-1$ is not a square in $K$. Since $f = 2$, we get

$$\alpha_{K'}(\langle N' \rangle_{K'}) = (1, 2, 1)(0, a, -1) = (0, a, -[2, a]) = (0, a, -1).$$

So $c_P(N)_K = -1$.

Case 2: $f = 1$ and $r = 2$. Then $E' = K'$, so $[N' : K'] = 2$. We have $N' = K'(\sqrt{γ})$, where $γ$ is some prime element in $K'$. So $\langle N' \rangle_{K'} = \langle 2, 2γ \rangle$. We see that
\[ \alpha_{K'}(\langle N' \rangle_{K'}) = (0, -\gamma, c_P\langle N' \rangle_{K'}) \], so

\[ \alpha_K(\langle N \rangle_K) = r\alpha_{K'}(\langle N' \rangle_{K'}) = 2(0, -\gamma, c_P\langle N' \rangle_{K'}) = (0, 1, (-\gamma, -\gamma)_P) = (0, 1, (-\gamma, -1)_P). \]

If \(-1\) is a square in \(K\), we have \(c_P\langle N \rangle_K = (-\gamma, -1)_P = 1\). If \(-1\) is not a square in \(K\), we get \(c_P\langle N \rangle_K = (-\gamma, -1)_P = -1\).

**Theorem 4.6.** Let \(K\) be a totally complex number field with one dyadic prime, and let \(N/K\) be a cyclic extension of degree 4. Then \(\langle N \rangle = \langle 1, -m \rangle + X\), where \(\text{dis} \langle N \rangle = m \neq 1 \in K^*/K^{**}\), and \(X\) is a class in \(J^2\) such that \(c_P(X)\) is determined as follows:

1. \(c_P(X) = 1\) for all non-dyadic prime ideals \(P\) of \(K\) such that \(P\) is ramified in \(K(\sqrt{m})\).
2. \(c_P(X) = 1\) for all non-dyadic \(P\) such that \(P\) is unramified in \(N/K\).
3. \(c_P(X) = 1\) for all non-dyadic \(P\) for which \(-1\) is a square in \(K_P\).
4. \(c_P(X) = -1\) for all other non-dyadic prime ideals \(P\).

**Proof.** Put \(X = \langle N \rangle + \langle -1, m \rangle\). Then \(\langle N \rangle = \langle 1, -m \rangle + X\), and

\[ \alpha_K(X) = \alpha_K(\langle N \rangle) + \alpha_K(\langle -1, m \rangle) = (0, m, c\langle N \rangle) + (0, m, c\langle -1, m \rangle) = (0, 1, [m, m]c\langle N \rangle c\langle -1, m \rangle). \]

Since \(X\) has even rank and square discriminant, we see that \(X \in J^2\), as required. Consequently, \(\langle N \rangle\) and \(\langle 1, -m \rangle + X\) both have even rank and discriminant \(m\), and we just need to calculate Hasse symbols.

Case 1: Let \(P\) be a non-dyadic prime ideal that is ramified in \(K(\sqrt{m})\). Then \(P\) is totally ramified in \(N/K\) with \(e = 4\). By Lemma 2.6, we have

\[ c_P\langle N \rangle_K = (m, -e)_P = (m, -4)_P = (m, -1)_P (m, 2)^2_P = (m, -1)_P. \]
As in Case 2a of Theorem 4.4, \( c_p(1, -m)_K = (-1, m)_p \). We have \( c_p(X) = 1 \), so
\[
\alpha_K((1, -m) + X) = \alpha_K((1, -m)) + \alpha_K(X) = (0, m, (1, m)_p) + (0, 1, 1) = (0, m, (1, m)_p).
\]
So \( c_p((1, -m) + X)_K = (-1, m)_p = c_p(N)_K \).

Case 2: Let \( P \) be a non-dyadic prime ideal that is unramified in \( K(\sqrt{m}) \). Then \( P \) is not totally ramified in \( N/K \).

Case 2a: \( P \) is unramified in \( N/K \). Then by Lemma 4.5, \( c_p(N)_K = 1 \). We have \( c_p((1, -m)_K = (-1, m)_p = 1 \), and \( c_p(X) = 1 \), so
\[
\alpha_K((1, -m) + X) = (0, m, 1) + (0, 1, 1) = (0, m, 1).
\]
So we get \( c_p((1, -m) + X)_K = 1 = c_p(N)_K \).

Case 2b: \( P \) is ramified in \( N/K \) but not totally so.

Case 2bi: \(-1 \) is a square in \( K_P \). By Lemma 4.5, \( c_p(N)_K = 1 \). As in Case 2a, \( c_p((1, -m) + X)_K = 1 \).

Case 2bii: \(-1 \) is not a square in \( K_P \). By Lemma 4.5, \( c_p(N)_K = -1 \). Again we have \( c_p((1, -m)_K = 1 \), but in this case \( c_p(X) = -1 \). So
\[
\alpha_K((1, -m) + X) = (0, m, 1) + (0, 1, -1) = (0, m, -1).
\]
So \( c_p((1, -m) + X)_K = -1 = c_p(N)_K \).

Applying reciprocity to see that the symbols of \( N \) and \( (1, -m) + X \) at the dyadic prime must also be equal, we find that \( N \) and \( (1, -m) + X \) are Witt equivalent in \( W(K) \).

We now summarize the findings of this chapter by describing the trace form of an abelian extension \( F/K \) of degree \( n \):

If \( n \) is odd, then \( \langle F \rangle = n\langle 1 \rangle \). (Corollary 2.2)

If \( n \) is even, let \( n = r\cdot 2^k \), where \( r \) is odd and \( k \geq 1 \). Then \( \langle F \rangle = r\langle N \rangle \), where \( N \) is an abelian extension of \( K \) of degree \( 2^k \). (Lemma 3.4)
Since $N/K$ is abelian, the class $\langle N \rangle$ can be written as a product of cyclic classes by Lemma 3.3. Let $\text{dis} \langle N \rangle = m \in K^*$. When $N/K$ is cyclic of degree $2^k$, then $\langle N \rangle$ is given by

\[
\begin{align*}
\langle 2, -2m \rangle & \quad \text{when } k = 1 \text{ and } m \neq -1 \in K^*/K^{**} \quad \text{(Theorem 3.2);} \\
\langle 1, -m \rangle + X & \quad \text{when } k = 2 \text{ and } m \neq 1 \in K^*/K^{**} \quad \text{(Theorem 4.6);} \\
\langle 2, -2m \rangle & \quad \text{when } k \text{ odd, } k \geq 3, \text{ and } m \neq 1 \in K^*/K^{**} \quad \text{(Theorem 4.4);} \\
\langle 1, -m \rangle & \quad \text{when } k \text{ even, } k \geq 4, \text{ and } m \neq 1 \in K^*/K^{**} \quad \text{(Theorem 4.4).}
\end{align*}
\]
Chapter 5
Abelian Witt Classes over Number Fields of Type (1, 1)

Recall that a number field $K$ of type (1, 1) has one dyadic prime and one real infinite prime. Over any number field $K$, the Witt classes of abelian extensions of odd degree are classified in Corollary 2.2, and those of degree 2 are classified in Theorem 3.2. We now proceed in a manner similar to that of Chapter 4.

**Theorem 5.1.** Every Witt class of non-negative signature in the square of the fundamental ideal in $W(K)$ is abelian.

**Proof.** Let $X \in W(K)$. Assume that $X \in J^2$ and $X$ has non-negative signature.

By Lemma 1.5, we see that $\text{sgn}(X) \equiv 0 \pmod{4}$. The first two possibilities are $\text{sgn}(X) = 0$ and $\text{sgn}(X) = 4$. For these cases, Theorem 2.4 implies that $X$ is abelian. So we will assume that $\text{sgn}(X) > 4$. We can write $\text{sgn}(X) = 2^{k+2}(2n + 1)$, with $k \geq 0$ and $n \geq 0$. Let $Y = X - \text{sgn}(X)\langle 1 \rangle$. Then $\text{sgn}(Y) = 0$, so $Y$ is a torsion class. By Corollary 1.8, $Y$ has order dividing 4. If $2n + 1 \equiv 1 \pmod{4}$, then $(2n + 1)Y = Y$, and

$$(2n + 1)(2^{k+2}\langle 1 \rangle + Y) = \text{sgn}(X)\langle 1 \rangle + Y = X.$$ 

Since $X \in J^2$ and $2n+1$ is odd, we see that $2^{k+2}\langle 1 \rangle + Y$ is in $J^2$ (since a calculation in $\text{Sym}(K)$ shows us that $2^{k+2}\langle 1 \rangle + Y$ has even rank and square discriminant). If $2n + 1 \equiv 3 \pmod{4}$, then $-(2n + 1)Y = Y$, and

$$(2n + 1)(2^{k+2}\langle 1 \rangle - Y) = X.$$ 

So $2^{k+2}\langle 1 \rangle - Y$ is in $J^2$. In both cases, Lemma 3.4 tells us that it suffices to prove our theorem for $X \in J^2$ with $\text{sgn}(X) = 2^{k+2} > 4$. Note that $k \geq 1$. 

33
Now suppose that $X$ lies in $J^3$. Then $sgn : J^3 \cong 8\mathbb{Z}$ gives us $X = sgn(X)(1)$, so by Theorem 3.5, $X$ is abelian.

So we will consider $X$ in $J^2$ with $sgn(X) = 2^{k+2} \geq 8$ and $X$ not in $J^3$.

We have $rk(X) \equiv 0 \pmod{2}$ and $dis(X) = 1 \in K^*/K^{**}$. Since $sgn(X) \equiv 0 \pmod{8}$, Lemma 1.5 gives us $c_Q(X) = 1$, where $Q$ is the real infinite prime. So, since $X$ is not in $J^3$, there must be at least one non-dyadic prime ideal $P$ with $c_P(X) = -1$. Let

$$T_X = \{ P \mid P \text{ a prime of } K \text{ and } c_P(X) = -1 \}.$$ 

We take a prime $q$ such that

1. $q$ is not a square in $K_P$ for any $P \in T_X$,
2. $q$ does not divide $Dis(K/Q)$,
3. $q \equiv 1 \pmod{2^{k+2}}$,
4. $q$ is not divisible by any prime $P$ in $T_X$.

Let $\zeta$ be a primitive $q$-th root of unity. Then $Q(\zeta)/Q$ is an abelian extension of degree $q - 1$. Let $N$ be the extension of $Q$ contained in $Q(\zeta)$ that is the fixed field of complex conjugation. Then $[N:Q] = \frac{q-1}{2}$. From condition 3 above we see that $2^{k+2}|(q - 1)$, so $2^{k+1}|\frac{q-1}{2}$. Let $F$ be the extension of $Q$ contained in $N$ such that $[F:Q] = 2^{k+1}$. The field $N$ is totally real, so $F$ is totally real as well. By the remarks on page 49 of [2], $dis(F) = q$. Condition 2 above guarantees that $Q(\zeta) \cap K = Q$, which implies that $F \cap K = Q$. So $Gal(FK/K) \cong Gal(F/Q)$. This means that $FK/K$ is an abelian extension of degree $2^{k+1}$. Also, we have $sgn(FK) = 2^{k+1}$.

By Realization by Hilbert symbols (Theorem 2.9), there is an $r \in K^*$ such that $(r, q)_P = c_P(X)$ for all primes $P$ of $K$. We must analyze $K(\sqrt{-7})$. First we need to show that $r \neq -1$ in $K^*/K^{**}$. Let $P$ be a non-dyadic prime with $c_P(X) = -1$. 

34
If \( r = -1 \) in \( K^*/K^{**} \), we have

\[
c_P(X) = (r, q)_P = (-1, q)_P = 1,
\]
a contradiction.

Next, we must show that we can choose \( r \) to be negative. Note that

\[
(-qr, q)_P = (-q, q)_P = (r, q)_P = c_P(X),
\]
so we can replace \( r \) with \(-qr\) if necessary to guarantee that \( r \) is negative, and consequently \(-r\) is positive. So \( K(\sqrt{-r}) \) is a real quadratic extension.

Now we must see that \( FK \cap K(\sqrt{-r}) = K \). First of all, note that \([FK : K] = 2k+1\), and \([K(\sqrt{-r}) : K] = 2\). So

\[
[(FK) : K(\sqrt{-r}) : K] = [FK(\sqrt{-r}) : K] \leq [FK : K][K(\sqrt{-r}) : K] = 2^{k+2}.
\]

We also have \([FK : K])[FK(\sqrt{-r}) : K]\). So \([FK(\sqrt{-r}) : K] = 2^{k+1} \) or \(2^{k+2}\). Assume \( FK \cap K(\sqrt{-r}) \neq K \). Then \([FK(\sqrt{-r}) : K] \neq 2^{k+2} \), so \([FK(\sqrt{-r}) : K] = 2^{k+1} \). This implies that \( FK(\sqrt{-r}) = FK \), which gives us \( \sqrt{-r} \in FK \).

We now have \( K \subset K(\sqrt{-r}) \subset FK \). Since \( Gal(F/Q) \cong Gal(FK/K) \), and the extensions are cyclic, there is a unique quadratic extension \( Q(\sqrt{d}) \) of \( Q \) such that \( Q \subset Q(\sqrt{d}) \subset F \). We also know that \( Q(\sqrt{d}) \) is a subfield of \( Q(\zeta) \). Since \( q \) is the only totally ramified prime in \( Q(\zeta) \), the same will be true for \( Q(\sqrt{d}) \). So \( Dis(Q(\sqrt{d})/Q) = \pm q \). Since discriminants must be congruent to 0 or 1 modulo 4, and since \( q \) was chosen to be congruent to 1 modulo \( 2^{k+2} \), we see that \( q \equiv 1 \pmod{4} \), so \( Dis(Q(\sqrt{d})/Q) = q \). So \( d = q \), and our quadratic extension of \( Q \) corresponding to \( K(\sqrt{-r}) \) is \( Q(\sqrt{q}) \). This gives us

\[
K(\sqrt{-r}) = K \cdot Q(\sqrt{q}) = K(\sqrt{q}).
\]
So \(-r = q \in K^*/K^{**}\). Looking at symbols, we have

\[(r, q)_P = (r, -r)_P = 1 = c_P(X),\]

a contradiction. So we must have \(FK \cap K(\sqrt{-r}) = K\).

By Proposition 2.10, \(\text{Gal}(FK(\sqrt{-r})/K) \cong \text{Gal}(FK/K) \oplus \text{Gal}(K(\sqrt{-r})/K)\), so \(\text{Gal}(FK(\sqrt{-r})/K)\) is an abelian group. Therefore, \(\langle FK(\sqrt{-r}) \rangle \in W(K)\) is abelian. By Theorem 2.1,

\[\langle FK \rangle \langle K(\sqrt{-r}) \rangle = \langle (FK) \cdot K(\sqrt{-r}) \rangle = \langle FK(\sqrt{-r}) \rangle,\]

so in \(\text{Sym}(K)\), we have

\[\alpha_K(\langle FK(\sqrt{-r}) \rangle) = \alpha_K(\langle FK \rangle) \alpha_K(\langle K(\sqrt{-r}) \rangle) = (0, q, c\langle FK \rangle)(0, r, c\langle K(\sqrt{-r}) \rangle)\]

\[= (0, 1, [q, r]) = (0, 1, c(X)).\]

Also, \(\text{sgn}(FK(\sqrt{-r})) = 2 \cdot 2^{k+1} = 2^{k+2} = \text{sgn}(X)\). So we have \(X = \langle FK(\sqrt{-r}) \rangle\), which is abelian.

\[\square\]

**Corollary 5.2.** The abelian classes in \(W(K)\) are closed under multiplication.

**Proof.** This proof is nearly identical to that of Corollary 4.2. Just replace Theorem 4.1 with Theorem 5.1.

\[\square\]

**Theorem 5.3.** Let \(N/K\) be a cyclic extension of degree \(2^k \geq 8\), with \(k\) odd (resp. even). Then \(\langle N \rangle = \langle 2, -2m \rangle + \langle \text{sgn}(N) \rangle \langle 1 \rangle\) (resp. \(\langle N \rangle = \langle 1, -m \rangle + \langle \text{sgn}(N) \rangle \langle 1 \rangle\)), where \(\text{dis}\langle N \rangle = m \neq 1 \in K^*/K^{**}\).

**Proof.** \(N\) has even rank, as do both \(\langle 2, -2m \rangle + \langle \text{sgn}(N) \rangle \langle 1 \rangle\) and \(\langle 1, -m \rangle + \langle \text{sgn}(N) \rangle \langle 1 \rangle\).

Also, we see that \(\langle 2, -2m \rangle\) and \(\langle 1, -m \rangle\) both have discriminant \(m\) in \(K^*/K^{**}\).

Since \(N/K\) is cyclic and therefore normal, Remark 1.11 gives us that \(\text{sgn}(N) = 0\).
or $2^k$. So $\text{sgn}(N) \equiv 0 \pmod{8}$, and by Lemma 1.5, $\text{dis}(N) = m > 0$. This implies that the Witt classes $\langle 2, -2m \rangle$ and $\langle 1, -m \rangle$ both have signature 0, so $\langle 2, -2m \rangle + (\text{sgn}(N))\langle 1 \rangle$ and $\langle 1, -m \rangle + (\text{sgn}(N))\langle 1 \rangle$ each have signature $\text{sgn}(N)$.

The calculations of the Hasse symbols of $\langle N \rangle$, $\langle 2, -2m \rangle$, and $\langle 1, -m \rangle$ for finite, non-dyadic prime ideals are identical to those in the proof of Theorem 4.4, and a simple calculation in $\text{Sym}(K)$ gives us that

$$c_P(\langle 2, -2m \rangle + (\text{sgn}(N))\langle 1 \rangle) = c_P\langle 2, -2m \rangle$$

and

$$c_P(\langle 1, -m \rangle + (\text{sgn}(N))\langle 1 \rangle) = c_P\langle 1, -m \rangle.$$

So we just need the symbols for the real infinite prime and the dyadic prime. Let $Q$ be the real infinite prime. Since $\text{sgn}(N) \equiv 0 \pmod{8}$, Lemma 1.5 gives us $c_Q\langle N \rangle = 1$. Also, since $\langle 2, -2m \rangle + (\text{sgn}(N))\langle 1 \rangle$ and $\langle 1, -m \rangle + (\text{sgn}(N))\langle 1 \rangle$ both have signature $\text{sgn}(N)$, we get

$$c_Q(\langle 2, -2m \rangle + (\text{sgn}(N))\langle 1 \rangle) = 1$$

and

$$c_Q(\langle 1, -m \rangle + (\text{sgn}(N))\langle 1 \rangle) = 1.$$

By reciprocity, the symbols of any of the three classes $\langle N \rangle$, $\langle 2, -2m \rangle + (\text{sgn}(N))\langle 1 \rangle$, and $\langle 1, -m \rangle + (\text{sgn}(N))\langle 1 \rangle$ at the dyadic prime must also be equal, so we find that $\langle N \rangle = \langle 2, -2m \rangle + (\text{sgn}(N))\langle 1 \rangle$ when $k$ is odd, and $\langle N \rangle = \langle 1, -m \rangle + (\text{sgn}(N))\langle 1 \rangle$ when $k$ is even. \hfill \qedsymbol

**Theorem 5.4.** Let $N/K$ be a cyclic extension of degree 4. Then $\langle N \rangle = \langle 1, -m \rangle + (\text{sgn}(N))\langle 1 \rangle + X$, where $\text{dis}(N) = m \neq 1 \in K^*/K^{**}$, and $X$ is a torsion class in $J^2$ such that $c_P(X)$ is determined as follows:
1. \( c_P(X) = 1 \) for all non-dyadic prime ideals \( P \) of \( K \) such that \( P \) is ramified in \( K(\sqrt{m}) \).

2. \( c_P(X) = 1 \) for all non-dyadic \( P \) such that \( P \) is unramified in \( N/K \).

3. \( c_P(X) = 1 \) for all non-dyadic \( P \) for which \(-1\) is a square in \( K_P \).

4. \( c_P(X) = -1 \) for all other non-dyadic prime ideals \( P \).

**Proof.** First of all, \( X = \langle N \rangle + \langle -1, m \rangle + (\text{sgn}(N))(-1) \). As in Theorem 4.6, calculations in \( \text{Sym}(K) \) give us \( X \in J^2 \), as required. Consequently, \( \langle N \rangle \) and \( \langle 1, -m \rangle + (\text{sgn}(N))(1) + X \) both have even rank and discriminant \( m \). Since \( N/K \) is normal, Remark 1.11 gives us that \( \text{sgn}(N) \equiv 0 \pmod{4} \). So \( \text{sgn}(N) \equiv 0 \pmod{4} \), and by Lemma 1.5, \( \text{dis}(N) = m > 0 \). This implies that the Witt class \( \langle 1, -m \rangle \) has signature 0, so \( X \) is a torsion class, as claimed. Clearly we see that

\[
\langle 1, -m \rangle + (\text{sgn}(N))(1) + X \]

has signature \( \text{sgn}(N) \).

The calculations of the Hasse symbols of \( \langle N \rangle \) and of \( \langle 1, -m \rangle + (\text{sgn}(N))(1) + X \) for finite, non-dyadic prime ideals are identical to those in the proof of Theorem 4.6. So we just need the symbols for the real infinite prime and the dyadic prime. Let \( Q \) be the real infinite prime.

Case 1: \( \text{sgn}(N) = 0 \). Then \( \text{sgn}(N) \equiv 0 \pmod{8} \), so Lemma 1.5 gives us \( c_Q(N) = 1 \). We also get

\[
c_Q(\langle 1, -m \rangle + (\text{sgn}(N))(1) + X) = 1. \]

Case 2: \( \text{sgn}(N) = 4 \). Then \( \text{sgn}(N) \equiv 4 \pmod{8} \), and by Lemma 1.5 we have \( c_Q(N) = -1 \). Also,

\[
c_Q(\langle 1, -m \rangle + (\text{sgn}(N))(1) + X) = -1. \]
By reciprocity, the symbols of \( \langle N \rangle \) and of \( \langle 1, -m \rangle + (\text{sgn}(N))\langle 1 \rangle + X \) at the dyadic prime must also be equal, so we find that \( \langle N \rangle = \langle 1, -m \rangle + (\text{sgn}(N))\langle 1 \rangle + X \). 

As in Chapter 4, we summarize our findings by describing the trace form of an abelian extension \( F/K \) of degree \( n \):

If \( n \) is odd, then \( \langle F \rangle = n\langle 1 \rangle \). (Corollary 2.2)

If \( n \) is even, let \( n = r \cdot 2^k \), where \( r \) is odd and \( k \geq 1 \). Then \( \langle F \rangle = r\langle N \rangle \), where \( N \) is an abelian extension of \( K \) of degree \( 2^k \). (Lemma 3.4)

Since \( N/K \) is abelian, the class \( \langle N \rangle \) can be written as a product of cyclic classes by Lemma 3.3. Let \( \text{dis}(N) = m \in K^* \). When \( N/K \) is cyclic of degree \( 2^k \), then \( \langle N \rangle \) is given by

\[
\begin{align*}
\langle 2, -2m \rangle & \quad \text{when } k = 1 \text{ and } m \neq -1 \in K^*/K^{**} \quad \text{(Thm 3.2)}; \\
\langle 1, -m \rangle + X & \quad \text{when } k = 2; m \neq 1 \in K^*/K^{**}; \text{sgn}(N) = 0 \quad \text{(Thm 5.4)}; \\
\langle 1, -m \rangle + 4\langle 1 \rangle + X & \quad \text{when } k = 2; m \neq 1 \in K^*/K^{**}; \text{sgn}(N) = 4 \quad \text{(Thm 5.4)}; \\
\langle 2, -2m \rangle & \quad \text{when } k \text{ odd, } k \geq 3; m \neq 1 \in K^*/K^{**}; \text{sgn}(N) = 0; \\
\langle 2, -2m \rangle + 2^k\langle 1 \rangle & \quad \text{when } k \text{ odd, } k \geq 3; m \neq 1 \in K^*/K^{**}; \text{sgn}(N) = 2^k; \\
\langle 1, -m \rangle & \quad \text{when } k \text{ even, } k \geq 4; m \neq 1 \in K^*/K^{**}; \text{sgn}(N) = 0; \\
\langle 1, -m \rangle + 2^k\langle 1 \rangle & \quad \text{when } k \text{ even, } k \geq 4; m \neq 1 \in K^*/K^{**}; \text{sgn}(N) = 2^k,
\end{align*}
\]

the last four cases coming from Theorem 5.3.
References


Vita

Karli Smith was born in September 1982, in San Luis Obispo, California. She finished her undergraduate studies at California Polytechnic State University in June 2003. In August 2003 she came to Louisiana State University to pursue graduate studies in mathematics. She earned a master of science degree in mathematics from Louisiana State University in May 2005. She is currently a candidate for the degree of Doctor of Philosophy in mathematics, which will be awarded in August 2008. After graduation, Karli will move to Alabama with her husband and daughter, where she will be an assistant professor of mathematics at University of Montevallo.