Journal of Algebra, Number Theory: Advances and Applications
Volume 8, Number 1-2, 2012, Pages 57-80

TRACE FORMS OF ABELIAN EXTENSIONS OF NUMBER FIELDS OF TYPE (1, 1)

KARLI MORRIS

University of Montevallo
Alabama 35115
Montevallo
USA
e-mail: kmorris5@montevallo.edu

Abstract

This article is concerned with describing bilinear trace forms associated with finite abelian extensions $N|K$ of an algebraic number field K. These abelian trace forms are described up to Witt equivalence, that is, they are described as elements in the Witt ring $W(K)$. When the base field K has exactly one dyadic prime and one real embedding, it is shown that the Witt class of every abelian trace form over K is a product of Witt classes of eight specified types.

1. Introduction

For a field K and a finite separable extension F of K, the trace form of F over K is the symmetric K-bilinear form $\mathrm{tr}_{F|K} : F \times F \to K$ given by $\mathrm{tr}_{F|K}(x, y) = \mathrm{trace}_{F|K}(xy)$ for all $x, y \in F$. Trace forms were studied in detail in [1]. A number field with d dyadic primes (primes containing the natural number 2) and r real infinite primes will be said to have type (d, r). Trace forms of abelian extensions of number fields of type (1, 0)

2010 Mathematics Subject Classification: 11E81, 11E12.

Keywords and phrases: trace forms, Witt ring, Witt equivalence, symmetric bilinear forms.

Received October 9, 2012

were discussed in [4]. In this article, we look specifically at trace forms of abelian extensions of number fields of type (1, 1), i.e., number fields with one dyadic prime and one real infinite prime. These fields are interesting because they generalize the field of rational numbers. Fields of type (1, 1) have odd degree over $\mathbb{Q}$, and for any odd number n, a field of degree n and type (1, 1) is obtained by adjoining an n-th root of 2 to $\mathbb{Q}$. Now fix K of type (1, 1). In this article, eight Witt classes in the Witt ring $W(K)$ are produced with the property that the Witt classes of finite abelian extensions of K are precisely the finite products of classes in $W(K)$ with these eight types. In other words, we give a set of multiplicative generators of the abelian classes. For the explicit statements, see Theorems 3.8, 4.3, and 4.4 below, together with Lemma 3.11.

2. Background Material

For a quick but elementary introduction to Witt rings over number fields, see the Introduction to [4]. For details, see Chapter 1 of [3], Subsection 1.2 of [1]. Here, we give some background information that will be helpful in the subsequent chapters.

Let R be a commutative ring with 1. An *inner product space* over R is a pair (V, b), where V is a nonzero finitely generated projective left module over R, and $b : V \times V \to R$ is a non-singular symmetric bilinear form.

Let W be an R-submodule of the inner product space (V, b). Then we have an associated submodule

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

If W is a direct summand of V and if $W = W^{\perp}$, then W is called a *metabolizer* for (V, b). Two inner product spaces (V, b) and (V', b') are *Witt equivalent* when the direct sum space $(V, b) \oplus (V', -b')$ has a metabolizer.

Witt equivalence is an equivalence relation. The equivalence class of the inner product space (V, b) is called the *Witt class* of (V, b), and is denoted by $\langle V, b\rangle$, with diamond brackets. The collection of all Witt classes over R forms the *Witt ring* $W(R)$.

We now introduce trace forms.

Definition 2.1. Let $F|K$ be a finite separable field extension. Then the trace form of $F|K$ is the symmetric K-bilinear form

$$\mathrm{tr}_{F|K} : F \times F \to K,$$

given by $\mathrm{tr}_{F|K}(x, y) = \mathrm{trace}_{F|K}(xy)$ 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 $(F, \mathrm{tr}_{F|K})$ in the Witt ring $W(K)$. We will occasionally use the notation $\langle F\rangle_K$, when the field K needs to be specified.

Bilinear forms over algebraic number fields are determined up to Witt equivalence by four invariants, which we now discuss.

The first invariant is the *rank*. 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.

To define the *discriminant* of a symmetric bilinear form b on a vector space V, 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-singular. The discriminant of the Witt class $\langle V, b\rangle$ is the element of K^*/K^{*2} defined by

$$dis\langle V, b\rangle = (-1)^{n(n-1)/2} \det(B).$$

This is read in K^*/K^{*2}. The factor involving the power of -1 makes this a Witt class invariant.

For a diagonalized form $\langle a_1, \ldots, a_n\rangle$, the discriminant is

$$dis\langle a_1, \ldots, a_n\rangle = (-1)^{n(n-1)/2}(a_1 \cdots a_n),$$

modulo the squares in K^*.

The two invariants *rk* and *dis* together give us a map

$$W(K) \to Z/2Z \times K^*/K^{*2},$$

and we put a ring structure on the Cartesian product to make this map a ring homomorphism. Let (e, d) and (e', d') be any two elements in the Cartesian product. Define addition by declaring

$$(e, d) + (e', d') = (e + e', (-1)^{ee'} dd'),$$

and define multiplication by

$$(e, d)(e', d') = (ee', d^{e'} d'^{e}).$$

Then, there is an exact sequence

$$0 \to J^2 \to W(K) \to Z/2Z \times K^*/K^{*2} \to 0.$$

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

Now, let $N|K$ be a finite Galois extension of fields of characteristic not 2. Then, the pair $(N, \mathrm{tr}_{N|K})$ is an inner product space over K and defines an element $\langle N\rangle$ in the Witt ring $W(K)$. In addition to the discriminant $dis\langle N\rangle$ of this Witt class, there is also the discriminant $Dis(N|K)$ of the field extension $N|K$, which is also read in the square-class group K^*/K^{*2}. These two discriminants are related by

$$Dis(N|K) = (-1)^{n(n-1)/2} \cdot dis\langle N\rangle.$$

These two discriminants coincide when $n(n-1)$ is a multiple of 4. This happens, in particular, when $n = 2^k$ with $k \geq 2$. The next theorem tells us when the field discriminant is non-trivial in K^*/K^{*2}.

Theorem 2.2 (see [1], Theorem I.3.4)**.** *Let $N|K$ be a finite normal field extension of characteristic different than 2. Then the field discriminant $Dis(N|K)$ is not 1 in K^*/K^{*2} if and only if the Galois group $G = Gal(N|K)$ has a non-trivial cyclic Sylow 2-subgroup. In particular, $Dis(N|K) = 1$, whenever $Gal(N|K)$ has odd order, and $Dis(N|K) \neq 1$ if $Gal(N|K)$ has even order not divisible by 4.*

In connection with Theorem 2.2 above, we note that the field discriminant of a normal extension $N|K$ is always trivial in the square-class group N^*/N^{*2} of the overfield N. Thus, N always contains $K(\sqrt{Dis(N|K)})$.

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 a signature to each ordering of K. 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

$$\operatorname{sgn}\langle V, b\rangle = s - (n - s) = 2s - n.$$

If the algebraic number field K has more than one embedding into the real numbers, then each embedding gives us an ordering of K, and each ordering corresponds to a signature. So, we have a *total signature*

$$\operatorname{Sgn} : W(K) \to Z^r,$$

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

The final invariant is the *Hasse-Witt invariant*. This is actually not a single invariant but a countably infinite family of invariants, which are referred to as *Hasse symbols*, or *Hasse-Witt symbols*. For a Witt class $X \in W(K)$, there is an invariant $c_P(X)$ for every prime P in K, finite and infinite. When the field K needs to be specified, we will use the notation $c_P(X)_K$. This invariant is $+1$ or -1. For details, concerning the calculation of these Hasse symbols, please see [1] and [4]. There is a theorem due to Hasse that summarizes the four invariants:

Theorem 2.3 (see [1], 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. Note 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 2.4. *Let K be an algebraic number field and P be a real infinite prime. Then for X in $W(K)$, we have*

(1) $\operatorname{sgn}_P(X) \equiv rk(X)$ *in* $Z / 2Z$.

(2) $dis(X) > 0$ *in the ordering associated to P if and only if* $\operatorname{sgn}_P(X) \equiv 0$ *or* 1 (mod 4).

(3) *If* $\operatorname{sgn}_P(X) \equiv 0, 1, 6,$ *or* 7 (mod 8), *then* $c_P(X) = 1$. *If* $\operatorname{sgn}_P(X) \equiv 2,$ 3, 4, *or* 5 (mod 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, $\operatorname{sgn}_P(X)$ has the form $2s - n$, and $2s - n \equiv -n \equiv n \pmod 2$. So $\operatorname{sgn}_P(X) \equiv rk(X)$ in $Z / 2Z$.

(2) First of all, X can be diagonalized, so we can write $X = \langle a_1, \ldots, a_n \rangle$. Assume $\operatorname{sgn}_P(X) \equiv 0 \pmod 4$. Then, we can write $\operatorname{sgn}_P(X) = 2s - n = 4k$ 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 $\operatorname{sgn}_P(X) \equiv 1 \pmod 4$. Then $\operatorname{sgn}_P(X) = 2s - n = 4k + 1$ 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 $\text{sgn}_P(X) \equiv 2 \pmod 4$. Then $\text{sgn}_P(X) = 2s - n = 4k + 2$ 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 $\text{sgn}_P(X) \equiv 3 \pmod 4$. Then $\text{sgn}_P(X) = 2s - n = 4k + 3$ for some integer k, so $n = 2s - 4k - 3$. Then,

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

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

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

First, let $\text{sgn}_P(X) \equiv 0 \pmod 8$. Let $X = \langle a_1, \ldots, a_s, b_1, \ldots, b_r \rangle$, where $a_i > 0$ for $1 \le i \le s$, and $b_j < 0$ for $1 \le j \le r$, 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 know that to compute Hasse symbols we must have $n \equiv 0$ 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 $1 \le i < j \le 4q$. 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 $\operatorname{sgn}_P(X) \equiv 4 \pmod 8$. 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 $1 \le i < j \le 2q$. 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 $Z/2Z$, b is in K^*/K^{*2}, and c is a function which assigns a value of 1 or -1 to each prime of K, finite or infinite, 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. (This is called *reciprocity*.)

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

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

thus the additive identity is $(0, 1, 1)$. Multiplication in $Sym(K)$ is

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

and the multiplicative identity is $(1, 1, 1)$. 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 the function, which assigns to each prime P the value of the Hasse symbol $c_P(X)$.

Theorem I.2.5 in [1] states that for any number field K, there is a short exact sequence

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

By Theorem 2.3, an element of $W(K)$ is completely determined once, we know its image in $Sym(K)$ and its total signature. Elements of J^3 are completely determined by total signature alone. If K is purely complex, then there are no signatures, so $J^3 = 0$ and $W(K) \cong Sym(K)$. If K has r real infinite primes, $r > 0$, then the total signature gives us the isomorphism $Sgn : J^3 \cong 8Z^r$.

When K is replaced by its completion K_P at a finite prime P, there is a *local symbol ring* $Sym(K_P)$, consisting of triples (a, b, c), where a is in $Z/2Z$, b is in K_P^* / K_P^{*2}, and $c = \pm 1$. The local Witt ring $W(K_P)$ maps to $Sym(K_P)$ by sending X in $W(K_P)$ to the triple $(rk(X), dis(X), c_P(X))$. The exact sequence above remains valid when K_P replaces K and when the fundamental ideal of $W(K_P)$ replaces J.

Now, we give a theorem 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 $Sym(K)$. One checks directly that a torsion class in $Sym(K)$ has 2-power order.

Theorem 2.5. *Every class in* $Sym(K)$ *has additive order dividing* 8. *The elements of order* 8 *are precisely the elements of odd rank.*

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

$$(a, b, c) + (a, b, c) = (0, (-1)^a, [-1, (-1)^a][b, b]) = (0, 1, 1).$$

We see that $(-1)^a = 1$, so $a = 0$.

Now, let $(e, f, g) \in Sym(K)$ have order 4. So, we have $2(e, f, g) = (a, b, c) = (0, b, c)$. Calculating in $Sym(K)$, 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 $(j, k, l) \in Sym(K)$ have order 8. Then we have $2(j, k, l) = (e, f, g) = (0, f, g)$. As in the previous steps, calculating in $Sym(K)$ 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 $(m, n, p) \in Sym(K)$ 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 $(j, k, l) \in Sym(K)$ have order 8. Then $2(j, k, l) = (e, f, g) = (1, f, g)$. This will lead to $0 = 1$, clearly, a contradiction.

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

Corollary 2.6. *A torsion class in* $W(K)$ *must have order dividing* 8. *Every torsion class of even rank has order dividing* 4.

Definition 2.7. For any field K, an element of $W(K)$ is *algebraic* if it can be represented by the trace form of a finite separable extension of K. 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. Let K be a number field and $F|K$ be a finite separable extension of K. Let $\sigma : K \to R$ be an embedding of K into the real numbers. Then $\text{sgn}_\sigma\langle F\rangle$ is equal to the number of extensions τ of σ to a mapping from F to R. From this formulation, we see that if $F|K$ is a normal extension, then $\text{sgn}\langle F\rangle = 0$ or $[F : K]$.

This article characterizes the Witt classes of trace forms of abelian extensions of an algebraic number field K, when K has type (1, 1). (See Theorems 3.8, 4.3, and 4.4 below, together with Lemma 3.11.) Type (1, 1) means that K has one signature and one *dyadic* prime (a prime ideal of K containing the rational number 2).

In general, computation of the Hasse symbol at a dyadic prime can be difficult; when there is exactly one dyadic prime, P, the Hasse symbol there can be determined from the symbols at all the other primes, by reciprocity. In the remainder of this article, a *non-dyadic prime* will refer to a *finite* prime that is not a dyadic prime.

3. Getting Started

In this section, we collect various loosely connected or disconnected pieces used to prove our main results in the next section. The reader may choose to jump ahead to the next section and return to this one when necessary. Most of the results of this section are stated without proof, but include a reference to the proof.

Theorem 3.1 (see [1], 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 $\langle EF\rangle$*

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

Theorem 3.2 (see [1], Corollary I.6.5)**.** *Let K be a number field and $F|K$ be a finite extension. If the normal closure of $F|K$ has odd degree over K, then in $W(K)$,*

$$\langle F\rangle = [F : K]\langle 1\rangle.$$

Corollary 3.3 (see [4], Corollary 3.8)**.** *Let K be a number field. Then the Witt classes of finite abelian extensions of odd degree over K coincide with the Witt classes $n\langle 1\rangle$ with n odd.*

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 3.4 (see [1], Theorem I.9.1)**.** *Let $F|Q$ be a normal extension of even degree. If the Sylow 2-subgroups of $Gal(F|Q)$ 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 $\langle F \rangle = [F : Q]\langle 1 \rangle$, or*

(2) *F is purely complex and $\langle F \rangle = 0$.*

Theorem 3.5 (see [1], 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 $\operatorname{sgn}(X) = 0$ or 4, then X can be represented by the trace form of a biquadratic extension of K.*

Theorem 3.6 (Realization by Hilbert symbols, see Theorem 71:19 of [5]; notation has been modified to be consistent with this article)**.** *Let T be a set consisting of an even number of finite or real infinite primes of an algebraic number field K. Then, there are α, β in K^* such that*

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

Moreover, β can be any element of K^* that is a local non-square at all places in T.

Proposition 3.7 (see [2], Proposition 3.20; notation has been modified to be consistent with this article)**.** *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, then E_1E_2 and $E_1 \cap E_2$ are Galois over F, and*

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

is an isomorphism of $Gal(E_1E_2|F)$ onto the subgroup

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

of $Gal(E_1|F) \oplus Gal(E_2|F)$.

The next theorem characterizes the Witt classes of abelian extensions of K of degree 2.

Theorem 3.8 (see [4], Lemma 3.11)**.** *If* $s \neq 1$ *in* K^*/K^{*2}, *then* $\langle 2, 2s\rangle$ *is abelian and is represented by the trace form of* $K(\sqrt{s})|K$.

The following theorems and lemmas, which apply to all number fields, will help us in our classification of trace forms of abelian extensions of number fields of type (1, 1), which we undertake in the next chapter.

Theorem 3.9 (see [4], Theorem 3.12)**.** *Let* K *be a number field. Then* $0 \in W(K)$ *is abelian.*

Lemma 3.10 (see [4], Lemma 3.13)**.** *Every abelian class in* $W(K)$ *is a product of cyclic classes in* $W(K)$.

Lemma 3.11 (see [1], Lemma I.11.2)**.** *A Witt class* $X \in W(K)$ *is abelian if and only if* $X = n\langle F\rangle$ *for an abelian extension* F *of* K *of degree* 2^k, $k \geq 0$, *and an odd positive integer* n.

Theorem 3.12. *If* $k \geq 3$, *then* $2^k\langle 1\rangle$ *is abelian in* $W(K)$.

Proof. We begin by working in $W(Q)$. Take $k \geq 3$ real quadratic fields, whose discriminants are distinct primes. By Theorem 3.4, the trace form of the compositum represents $2^k\langle 1\rangle$.

Now, for $W(K)$, take $k \geq 3$ fields, whose discriminants are distinct primes such that $K^\sigma \cap Q(\sqrt{p_i}) = Q$ for all K^σ 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 $W(K)$. □

4. 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 3.3, and those of degree 2 are classified in Theorem 3.8. Our next task is to prove that when K is of type (1, 1), the abelian classes in $W(K)$ are closed under multiplication. We begin with

Theorem 4.1. *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 2.4, we see that $\operatorname{sgn}(X) \equiv 0 \pmod 4$. The first two possibilities are $\operatorname{sgn}(X) = 0$ and $\operatorname{sgn}(X) = 4$. For these cases, Theorem 3.5 implies that X is abelian. So we will assume that $\operatorname{sgn}(X) > 4$. We can write $\operatorname{sgn}(X) = 2^{k+2}(2n+1)$, with $k \geq 0$ and $n \geq 0$. Let $Y = X - \operatorname{sgn}(X)\langle 1\rangle$. Then $\operatorname{sgn}(Y) = 0$, so Y is a torsion class. By Corollary 2.6, Y has order dividing 4. If $2n+1 \equiv 1 \pmod 4$, then $(2n+1)Y = Y$, and

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

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 $Sym(K)$ 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 3.11 tells us that it suffices to prove our theorem for $X \in J^2$ with $\operatorname{sgn}(X) = 2^{k+2} > 4$. Note that $k \geq 1$.

Now suppose that X lies in J^3. Then $\text{sgn} : J^3 \cong 8Z$ gives us $X = \text{sgn}(X)\langle 1\rangle$, so by Theorem 3.12, X is abelian.

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

We have $rk(X) \equiv 0 \pmod 2$ and $dis(X) = 1 \in K^*/K^{*2}$. Since $\text{sgn}(X) \equiv 0 \pmod 8$, Lemma 2.4 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 ζ 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 [1], $dis\langle F\rangle = q$. 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 $\text{sgn}\langle FK\rangle = 2^{k+1}$.

By realization by Hilbert symbols (Theorem 3.6), there is an $r \in K^*$ such that $(r, q)_P = c_P(X)$ for all primes P of K. We must analyze $K(\sqrt{-r})$. First, we need to show that $r \neq -1$ in K^*/K^{*2}. Let P be a non-dyadic prime with $c_P(X) = -1$. If $r = -1$ in K^*/K^{*2}, 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

$$(-qr, q)_P = (-q, q)_P(r, q)_P = (r, q)_P = c_P(X),$$

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 $[FK : K] = 2^{k+1}$, and $[K(\sqrt{-r}) : K] = 2$. So,

$$\begin{aligned}[(FK) \cdot K(\sqrt{-r}) : K] &= [FK(\sqrt{-r}) : K] \\ &\leq [FK : K][K(\sqrt{-r}) : K] = 2^{k+2}.\end{aligned}$$

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 $-r = q \in K^*/K^{*2}$. 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 3.7, $Gal(FK(\sqrt{-r})|K) \cong Gal(FK|K) \oplus Gal(K(\sqrt{-r})|K)$, so $Gal(FK(\sqrt{-r})|K)$ is an abelian group. Therefore, $\langle FK(\sqrt{-r})\rangle \in W(K)$ is abelian. By Theorem 3.1,

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

so in $Sym(K)$, we have

$$\begin{aligned}\alpha_K(\langle FK(\sqrt{-r})\rangle) &= \alpha_K(\langle FK\rangle)\alpha_K(\langle K(\sqrt{-r})\rangle)\\ &= (0, q, c\langle FK\rangle)(0, r, c\langle K(\sqrt{-r})\rangle)\\ &= (0, 1, [q, r]) = (0, 1, c(X)).\end{aligned}$$

Also, $\operatorname{sgn}\langle FK(\sqrt{-r})\rangle = 2 \cdot 2^{k+1} = 2^{k+2} = \operatorname{sgn}(X)$. So we have $X = \langle FK(\sqrt{-r})\rangle$, which 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, so $XY = mn\langle 1\rangle$, which is abelian by Corollary 3.3.

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 3.11. □

Theorem 4.3. *Let K be a number field of type* (1, 1) *and $N|K$ be a cyclic extension of degree $n = 2^k \geq 8$. Let $m = dis\langle N\rangle$. Then $m \neq 1 \in K^*/K^{*2}$. Moreover, if the exponent k is odd, then*

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

and if k is even, then

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

Proof. The discriminant m of the Witt class $\langle N\rangle$ equals the discriminant of the field extension $N|K$ multiplied by $(-1)^{n(n-1)/2}$. Since $n = 2^k \geq 8$, the discriminants are the same. By Theorem 2.2, we see that $m \neq 1$ in K^*/K^{*2}. Moreover, $\sqrt{m}$ lies in the normal overfield N and therefore generates a quadratic extension $K(\sqrt{m})|K$.

We will compare the invariants of the Witt classes in question. We see that $\langle N\rangle$ has even rank, as do both $\langle 2, -2m\rangle + (\text{sgn}\langle N\rangle)\langle 1\rangle$ and $\langle 1, -m\rangle + (\text{sgn}\langle N\rangle)\langle 1\rangle$. Also, we see that $dis\langle 2, -2m\rangle = 4m \equiv m \in K^*/K^{*2}$, and $dis\langle 1, -m\rangle = m \in K^*/K^{*2}$. Since $m = dis\langle N\rangle$, the discriminants agree. Since $N|K$ is cyclic and therefore normal, Remark 1 gives us that

$\text{sgn}\langle N\rangle = 0$ or 2^k. So $\text{sgn}\langle N\rangle \equiv 0 \pmod 8$, and by Lemma 2.4, $dis\langle N\rangle = m > 0$. This implies that the Witt classes $\langle 2, -2m\rangle$ and $\langle 1, -m\rangle$ both have signature 0, so $\langle 2, -2m\rangle + (\text{sgn}\langle N\rangle)\langle 1\rangle$ and $\langle 1, -m\rangle + (\text{sgn}\langle N\rangle)\langle 1\rangle$ each have signature $\text{sgn}\langle N\rangle$.

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 in [4], and a simple calculation in $Sym(K)$ gives us that

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

and

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

So, we just need the symbols for the real infinite prime and the dyadic prime. Let Q be the real infinite prime. Since $\text{sgn}\langle N\rangle \equiv 0 \pmod 8$, Lemma 2.4 gives us $c_Q\langle N\rangle = 1$. Also, since $\langle 2, -2m\rangle + (\text{sgn}\langle N\rangle)\langle 1\rangle$ and $\langle 1, -m\rangle + (\text{sgn}\langle N\rangle)\langle 1\rangle$ both have signature $\text{sgn}\langle N\rangle$, we get

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

and

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

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

Theorem 4.4. *Let K be a number field of type* (1, 1) *and $N|K$ be a cyclic extension of degree* 4. *Then $\langle N\rangle = \langle 1, -m\rangle + (\text{sgn}\langle N\rangle)\langle 1\rangle + X$, where $m = dis\langle N\rangle \neq 1 \in K^*/K^{*2}$, 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 *that ramify in* $K(\sqrt{m})$.

(2) $c_P(X) = 1$ *for all non-dyadic* P *that are 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. We know that $m \neq 1$ from Theorem 2.2.

Now put $X = \langle N\rangle + \langle -1, m\rangle + (\text{sgn}\langle N\rangle)\langle -1\rangle$. As in Theorem 4.6 in [4], calculations in $Sym(K)$ give us $X \in J^2$, as required. Consequently, $\langle N\rangle$ and $\langle 1, -m\rangle + (\text{sgn}\langle N\rangle)\langle 1\rangle + X$ both have even rank and discriminant m. Since $N|K$ is normal, Remark 1 gives us that $\text{sgn}\langle N\rangle = 0$ or 4. So $\text{sgn}\langle N\rangle \equiv 0 \pmod 4$, and by Lemma 2.4, $dis\langle N\rangle = m > 0$. 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

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

has signature $\text{sgn}\langle N\rangle$.

The calculations of the Hasse symbols of $\langle N\rangle$ and of $\langle 1, -m\rangle + (\text{sgn}\langle N\rangle)\langle 1\rangle + X$ for finite, non-dyadic prime ideals are identical to those in the proof of Theorem 4.6 in [4]. So, we just need the symbols for the real infinite prime and the dyadic prime. Let Q be the real infinite prime.

Case 1. $\text{sgn}\langle N\rangle = 0$. Then $\text{sgn}\langle N\rangle \equiv 0 \pmod 8$, so Lemma 2.4 gives us $c_Q\langle N\rangle = 1$. We also get

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

Case 2. $\text{sgn}\langle N\rangle = 4$. Then $\text{sgn}\langle N\rangle \equiv 4 \pmod 8$, and by Lemma 2.4, we have $c_Q\langle N\rangle = -1$. Also,

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

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

We now summarize our findings by describing the trace form of an abelian extension $F|K$ of degree n over number fields of type (1, 1):

If n is odd, then $\langle F\rangle = n\langle 1\rangle$, (Corollary 3.3).

If n is even, write $n = r \cdot 2^k$, 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 3.11).

The abelian extension $N|K$ of degree 2^k gives an abelian Witt class $\langle N\rangle$, which is a product of cyclic Witt classes by Lemma 3.10. The Witt classes $\langle N\rangle$ in $W(K)$ arising from cyclic extensions $N|K$ of degree 2^k with $k \geq 1$ are described in Theorems 3.8, 4.4, and 4.3. Putting this together shows that when K has type (1, 1), then every abelian class in $W(K)$ is a finite product of Witt classes of the following forms (the Witt class 0 coming from the empty product):

(1) $n\langle 1\rangle$; n odd (Corollary 3.3);

(2) $\langle 2, 2m\rangle$; $m \neq 1 \in K^*/K^{*2}$ (Theorem 3.8);

(3) $\langle 1, -m\rangle + X$; $m \neq 1 \in K^*/K^{*2}$; $X \in J^2$; $c_P(X)$ given by Theorem 4.4;

(4) $\langle 1, -m\rangle + 4\langle 1\rangle + X$; $m \neq 1 \in K^*/K^{*2}$; $X \in J^2$; $c_P(X)$ given by Theorem 4.4;

(5) $\langle 2, -2m\rangle$; $m \neq 1 \in K^*/K^{*2}$ (Theorem 4.3);

(6) $\langle 2, -2m\rangle + 2^k\langle 1\rangle$; $m \neq 1 \in K^*/K^{*2}$ (Theorem 4.3);

(7) $\langle 1, -m\rangle$; $m \neq 1 \in K^*/K^{*2}$ (Theorem 4.3);

(8) $\langle 1, -m\rangle + 2^k\langle 1\rangle$; $m \neq 1 \in K^* / K^{*2}$ (Theorem 4.3).

Also note that abelian Witt classes in $W(K)$ are closed under products by Corollary 4.2.

References

[1] P. E. Conner and R. Perlis, A Survey of Trace Forms of Algebraic Number Fields, World Scientific, Singapore, 1984.

[2] J. S. Milne, Fields and Galois Theory, 4th Version, Creative Commons License, 2005.

[3] J. Milnor and D. Husemoller, Symmetric Bilinear Forms, Springer-Verlag, Berlin, 1973.

[4] K. Morris and R. Perlis, Trace forms of abelian extensions of number fields of type (1, 0), Linear and Multilinear Algebra, Published online 29 March 2012, pages 1-21. DOI:10.1080/03081087.2012.671818

[5] O. T. O'Meara, Introduction to Quadratic Forms, 2nd Printing, Springer-Verlag, Heidelberg, 1971.

■