Acta Mathematica et Informatica Universitatis Ostraviensis

Kazimierz Szymiczek

A characterization of tame Hilbert-symbol equivalence

Acta Mathematica et Informatica Universitatis Ostraviensis, Vol. 6 (1998), No. 1, 191--201

Persistent URL: `http://dml.cz/dmlcz/120533`

A characterization of tame Hilbert-symbol equivalence

Kazimierz Szymiczek

Abstract: We prove that two number fields are tamely Hilbert-symbol equivalent if and only if they have isomorphic Knebusch-Milnor exact sequences for the Witt groups of quadratic forms.

Key Words: Hilbert symbol, Knebusch-Milnor sequence, Witt ring.

Mathematics Subject Classification: 11E81, 11E12.

1. Introduction

A Hilbert-symbol equivalence between number fields K and L is a pair of maps (t, T) in which

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

is an isomorphism of square-class groups, and

$$T : \Omega_K \longrightarrow \Omega_L$$

is a bijection between the set of places of K and those of L, preserving Hilbert symbols in the sense that

$$(a, b)_\mathfrak{p} = (ta, tb)_{T\mathfrak{p}}$$

for all square-classes $a, b \in K^*/K^{*2}$ and all places $\mathfrak{p}$ of K.

We recall that there is a Hilbert-symbol equivalence between K and L if and only if the Witt rings $W(K)$ and $W(L)$ of quadratic forms are isomorphic ([5]). If (t, T) is a Hilbert-symbol equivalence, then T always maps real infinite places to real infinite places, finite places to finite places, and dyadic places to dyadic places (see Lemma 4 of [5]).

The equivalence (t, T) is said to be *tame at the finite place* $\mathfrak{p}$ if

$$\mathrm{ord}_\mathfrak{p}\, a \equiv \mathrm{ord}_{T\mathfrak{p}}\, ta \pmod 2$$

Supported by the State Committee for Scientific Research (KBN) of Poland under Grant 2 P03A 024 12.

for all square classes $a \in K^*/K^{*2}$; otherwise (t,T) is *wild* at $\mathfrak{p}$. We say that (t,T) is *tame* when it is tame at *every* finite place $\mathfrak{p}$ of K.

It was an early observation that tamely equivalent fields produce isomorphic Knebusch-Milnor exact sequences. ¿From this it follows immediately that tame Hilbert-symbol equivalence preserves the integral Witt rings of the fields and also the 2-ranks of ideal class groups. In this paper we prove the converse: if two number fields have isomorphic Knebusch-Milnor exact sequences, then they are tamely Hilbert-symbol equivalent. Thus we get a complete characterization of tame Hilbert-symbol equivalence in terms of the Knebusch-Milnor sequences.

2. Knebusch-Milnor exact sequence and tame equivalence

Tame Hilbert-symbol equivalence between number fields K and L can be naturally interpreted in terms of the Knebusch-Milnor exact sequences for K and L. In this section we explain the Knebusch-Milnor sequence and we discuss in detail the connection with tame Hilbert-symbol equivalence.

Knebusch-Milnor sequence

For a number field K let $\mathcal{O}_K$ be its ring of integers and $C(K)$ the ideal class group of K. Write Ω_K for the set of all finite places of K. For each $\mathfrak{p} \in \Omega_K$, let $K_\mathfrak{p}$ be the $\mathfrak{p}$-adic completion of K, and $\overline{K_\mathfrak{p}}$ the residue class field of $K_\mathfrak{p}$. Then, with $\mathfrak{p}$ running over all finite places of K we have the following *Knebusch-Milnor sequence* for the Witt groups $W(\mathcal{O}_K), W(K)$ and $W(\overline{K_\mathfrak{p}})$:

$$0 \to W(\mathcal{O}_K) \xrightarrow{i} W(K) \xrightarrow{\partial_K} \coprod_{\mathfrak{p}} W(\overline{K_\mathfrak{p}}) \xrightarrow{\lambda} C(K)/C(K)^2 \to 0. \qquad (1)$$

Here i is the natural injection. We recall now the definition of ∂_K. First consider the composition

$$\partial_\mathfrak{p} : W(K) \longrightarrow W(K_\mathfrak{p}) \xrightarrow{\partial''_\mathfrak{p}} W(\overline{K_\mathfrak{p}})$$

where the first arrow is the natural surjection and the second arrow is the *second residue class homomorphism.* The latter can be defined only after fixing a prime element π in $K_\mathfrak{p}$. Then every element $\alpha \in W(K_\mathfrak{p})$ can be written as

$$\alpha = \langle a_1, \dots, a_k, b_1\pi, \dots, b_m\pi \rangle,$$

where a_i, b_j are units in $K_\mathfrak{p}$, and we set

$$\partial''_\mathfrak{p}(\alpha) = \langle \bar{b}_1, \dots, \bar{b}_m \rangle \in W(\overline{K_\mathfrak{p}}),$$

where $\bar{b}$ is the canonical image of the $\mathfrak{p}$-adic unit b in the residue class field $\overline{K_\mathfrak{p}}$. Notice that this construction does not distinguish between dyadic and nondyadic primes. When $\mathfrak{p}$ is a dyadic prime, then $W(\overline{K_\mathfrak{p}}) = \{0,1\} = \mathbf{Z}/2\mathbf{Z}$, and

$$\partial''_\mathfrak{p}(\alpha) \;=\; \mathrm{ord}_\mathfrak{p} \operatorname{dis} \alpha + 2\mathbf{Z} \;=\; m + 2\mathbf{Z},$$

where $\operatorname{dis}\alpha$ is the discriminant (signed determinant) of α. For any fixed $\alpha \in W(K)$ we have $\partial_{\mathfrak{p}}(\alpha) = 0$ for almost all primes $\mathfrak{p}$. Hence the map

$$\partial_K : W(K) \longrightarrow \coprod_{\mathfrak{p}} W(\overline{K_{\mathfrak{p}}}), \quad \partial_K(\alpha) = (\partial_{\mathfrak{p}}(\alpha))$$

is well defined and is said to be the *boundary* homomorphism.

It remains to recall the definition of λ. Let $\eta = (\eta_{\mathfrak{p}}) \in \coprod_{\mathfrak{p}} W(\overline{K_{\mathfrak{p}}})$. We set

$$\lambda(\eta) = [\prod_{\mathfrak{p}} \mathfrak{p}^{e(\eta_{\mathfrak{p}})}]\, C(K)^2.$$

Here $e : W(\overline{K_{\mathfrak{p}}}) \to \mathbf{Z}/2\mathbf{Z}$ is the *dimension-index* homomorphism, and the square brackets are used to denote the ideal class in $C(K)$.

The proof of the exactness of the Knebusch-Milnor sequence is found in [4] and [6]. Milnor and Husemoller concentrate on the exactness of the sequence (1) at $W(K)$ (cf. [4], Cor. (3.3), p. 93) and give hints on how to prove the exactness at the next group in the sequence. Scharlau ([6], Theorem 6.11, p.227) gives a proof for the latter.

Tame equivalence

When the equivalence (t, T) is *tame*, then we have the following commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 \to & W(\mathcal{O}_K) & \to & W(K) & \xrightarrow{\partial_K} & \coprod_{\mathfrak{p}} W(\overline{K_{\mathfrak{p}}}) & \to & C(K)/C(K)^2 & \to 1 \\ & \downarrow & & \downarrow \varphi & & \downarrow \overline{\varphi} & & \downarrow & \\ 0 \to & W(\mathcal{O}_L) & \to & W(L) & \xrightarrow{\partial_L} & \coprod_{\mathfrak{p}} W(\overline{L_{T\mathfrak{p}}}) & \to & C(L)/C(L)^2 & \to 1 \end{array} \tag{2}$$

where the first two vertical arrows are ring isomorphisms and the remaining two vertical arrows are *group* isomorphisms. The isomorphism $\overline{\varphi}$ sends the group $W(\overline{K_{\mathfrak{p}}})$ of the upper coproduct onto the group $W(\overline{L_{T\mathfrak{p}}})$ of the lower coproduct. Thus $\overline{\varphi}$ acts coordinate-wise according to the matching of coordinates supplied by the map T. This is one of the results proved in earlier versions of [5] and omitted in its final printed version. Czogała reproduces this proof in his recent paper [2]. Czogała asked the following question:

Suppose K and L are Hilbert-symbol equivalent fields and there is a commutative diagram (2). Does it then follow that K and L are *tamely* Hilbert-symbol equivalent?

It turns out that in order to answer this question it is necessary to make it more specific. First of all, the isomorphism $\overline{\varphi}$ (defined in a 1989 version of [5]) has always been viewed as a *group* isomorphism. The truth, however, is that $\overline{\varphi}$ is a *ring* isomorphism. The coproduct $\coprod_{\mathfrak{p}} W(\overline{K_{\mathfrak{p}}})$ has the ring structure with multiplication defined coordinate-wise. Although ∂_K certainly is not a ring homomorphism, when K and L are tamely Hilbert-symbol equivalent one can easily show that the additive isomorphism $\overline{\varphi}$ is a ring isomorphism (see Remark 2 below). Hence we are led to the following modification of Czogała's question:

Suppose K and L are Hilbert-symbol equivalent fields and there is a commutative diagram (2) in which φ and $\overline{\varphi}$ are *ring* isomorphisms. Does it then follow that K and L are *tamely* Hilbert-symbol equivalent?

The answer is yes, and this will be shown in section 4. Here we recall some fundamentals about Hilbert-symbol equivalence and we explain why $\overline{\varphi}$ is a ring isomorphism.

Lemma 1. *Let (t, T) be a Hilbert-symbol equivalence between K and L.*

(a) *There is an associated ring isomorphism $\varphi : W(K) \to W(L)$ satisfying $\varphi\langle a\rangle = \langle ta\rangle$ for all $a \in K^*$.*

(b) *For each $\mathfrak{p} \in \Omega_K$ there is an induced ring isomorphism $\varphi_\mathfrak{p} : W(K_\mathfrak{p}) \to W(L_{T\mathfrak{p}})$ satisfying $\varphi_\mathfrak{p}\langle a\rangle = \langle ta\rangle$ for all $a \in K^*$.*

Proof. For any $\mathfrak{p} \in \Omega_K$ the group isomorphism t induces a map

$$t_\mathfrak{p} : K_\mathfrak{p}^*/K_\mathfrak{p}^{*2} \to L_{T\mathfrak{p}}^*/L_{T\mathfrak{p}}^{*2}$$

which is a local symbol-preserving group isomorphism. Now t and $t_\mathfrak{p}$ can be used to define the associated ring isomorphisms φ and $\varphi_\mathfrak{p}$ satisfying $\varphi\langle a\rangle = \langle ta\rangle$ and $\varphi_\mathfrak{p}\langle a\rangle = \langle t_\mathfrak{p} a\rangle$ for all $a \in K^*$. For details, see Lemma 4(a) and Corollary 1 in [5]. □

Lemma 2. *Let (t, T) be a Hilbert-symbol equivalence between K and L and let $\varphi : W(K) \to W(L)$ be the associated Witt ring isomorphism. Let $\mathfrak{p} \in \Omega_K$ be a fixed prime. The following are equivalent.*

(a) *There is a commutative diagram*

$$\begin{array}{ccc} W(K) & \xrightarrow{\partial_\mathfrak{p}} & W(\overline{K_\mathfrak{p}}) \\ \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\overline{\varphi_\mathfrak{p}}} \\ W(L) & \xrightarrow{\partial_{T\mathfrak{p}}} & W(\overline{L_{T\mathfrak{p}}}) \end{array} \tag{3}$$

where $\overline{\varphi_\mathfrak{p}}$ is a ring isomorphism.

(b) *There is a commutative diagram* (3), *where $\overline{\varphi_\mathfrak{p}}$ is a group isomorphism.*

(c) *The equivalence (t, T) is tame at $\mathfrak{p}$.*

Proof. (a) $\Rightarrow$ (b) is trivial so we begin with (b) $\Rightarrow$ (c). Consider a square class $a \in K^*/K^{*2}$. Then, for the 1-dimensional class $\langle a\rangle \in W(K)$, we have

$$\begin{aligned} \operatorname{ord}_\mathfrak{p} a \equiv 0 \pmod 2 \quad &\Longleftrightarrow \quad \partial_\mathfrak{p}\langle a\rangle = 0 &&\Longleftrightarrow \quad \overline{\varphi_\mathfrak{p}}\partial_\mathfrak{p}\langle a\rangle = 0 \\ &\Longleftrightarrow \quad \partial_{T\mathfrak{p}}\varphi\langle a\rangle = 0 &&\Longleftrightarrow \quad \partial_{T\mathfrak{p}}\langle ta\rangle = 0 \\ &\Longleftrightarrow \quad \operatorname{ord}_{T\mathfrak{p}} ta \equiv 0 \pmod 2. \end{aligned}$$

This proves that (t, T) is tame at $\mathfrak{p}$.

(c) $\Rightarrow$ (a) First assume that $\mathfrak{p}$ is a nondyadic prime of K. We fix a local prime class $\pi \in K_\mathfrak{p}^*/K_\mathfrak{p}^{*2}$, and then we have the direct sum decomposition

$$W(K_\mathfrak{p}) = UW(K_\mathfrak{p}) \oplus \langle\pi\rangle UW(K_\mathfrak{p})$$

of the additive group $W(K_{\mathfrak{p}})$, where $UW(K_{\mathfrak{p}})$ is the subring of $W(K_{\mathfrak{p}})$ generated by the classes $\langle u\rangle$ of the local units u in $K_{\mathfrak{p}}$ (see [3], Cor. 1.6, p. 145). Since (t,T) is tame at $\mathfrak{p}$, the element $t_{\mathfrak{p}}(\pi)$ in $L^*_{T\mathfrak{p}}/L^{*2}_{T\mathfrak{p}}$ can be chosen as the square class of a prime at $T\mathfrak{p}$ and again we have

$$W(L_{T\mathfrak{p}}) = UW(L_{T\mathfrak{p}}) \oplus \langle t_{\mathfrak{p}}(\pi)\rangle UW(L_{T\mathfrak{p}}).$$

For the induced ring isomorphism $\varphi_{\mathfrak{p}} : W(K_{\mathfrak{p}}) \to W(L_{T\mathfrak{p}})$ of Lemma 1 we have

$$\varphi_{\mathfrak{p}}(UW(K_{\mathfrak{p}})) = UW(L_{T\mathfrak{p}}) \quad \text{and} \quad \varphi_{\mathfrak{p}}(\langle\pi\rangle UW(K_{\mathfrak{p}})) = \langle t_{\mathfrak{p}}(\pi)\rangle UW(L_{T\mathfrak{p}}).$$

We use π and $t_{\mathfrak{p}}(\pi)$ to define the second residue class homomorphisms $\partial''_{\mathfrak{p}}$ and $\partial''_{T\mathfrak{p}}$, respectively. Then $\partial''_{\mathfrak{p}}$ restricted to $\langle\pi\rangle UW(K_{\mathfrak{p}})$ becomes a group isomorphism

$$\partial''_{\mathfrak{p}} : \langle\pi\rangle UW(K_{\mathfrak{p}}) \to W(\overline{K_{\mathfrak{p}}}),$$

and similarly

$$\partial''_{T\mathfrak{p}} : \langle t_{\mathfrak{p}}(\pi)\rangle UW(L_{T\mathfrak{p}}) \to W(\overline{L_{\mathfrak{q}}})$$

is a group isomorphism. Hence there is a unique group isomorphism $\overline{\varphi_{\mathfrak{p}}}$ fitting into the commutative diagram

$$\begin{array}{ccccc} W(K_{\mathfrak{p}}) & \to & \langle\pi\rangle UW(K_{\mathfrak{p}}) & \xrightarrow{\partial''_{\mathfrak{p}}} & W(\overline{K_{\mathfrak{p}}}) \\ \downarrow\varphi_{\mathfrak{p}} & & \downarrow\varphi_{\mathfrak{p}} & & \downarrow\overline{\varphi_{\mathfrak{p}}} \\ W(L_{T\mathfrak{p}}) & \to & \langle t_{\mathfrak{p}}(\pi)\rangle UW(L_{T\mathfrak{p}}) & \xrightarrow{\partial''_{T\mathfrak{p}}} & W(\overline{L_{T\mathfrak{p}}}) \end{array} \tag{4}$$

of additive group homomorphisms. Here the unlabelled horizontal arrows are the projections with the kernels $UW(K_{\mathfrak{p}})$ and $UW(L_{T\mathfrak{p}})$, respectively.

We extend the diagram (4) to the left by inserting the natural ring homomorphisms $W(K) \to W(K_{\mathfrak{p}})$ and $W(L) \to W(L_{T\mathfrak{p}})$. We obtain

$$\begin{array}{ccccc} W(K) & \to & W(K_{\mathfrak{p}}) & \xrightarrow{\partial''_{\mathfrak{p}}} & W(\overline{K_{\mathfrak{p}}}) \\ \downarrow\varphi & & \downarrow\varphi_{\mathfrak{p}} & & \downarrow\overline{\varphi_{\mathfrak{p}}} \\ W(L) & \to & W(L_{T\mathfrak{p}}) & \xrightarrow{\partial''_{T\mathfrak{p}}} & W(\overline{L_{T\mathfrak{p}}}) \end{array}$$

which produces the commutative diagram (3). It remains to show that $\overline{\varphi_{\mathfrak{p}}}$ is, in fact, a *ring* isomorphism. This follows from the following computation for the additive generators $\langle\bar{u}\rangle, \langle\bar{v}\rangle \in W(\overline{K_{\mathfrak{p}}})$, where $u, v \in K_{\mathfrak{p}}$ are $\mathfrak{p}$-adic units:

$$\begin{aligned} \overline{\varphi_{\mathfrak{p}}}(\langle\bar{u}\rangle \cdot \langle\bar{v}\rangle) &= \overline{\varphi_{\mathfrak{p}}}\langle\bar{u}\bar{v}\rangle &&= \overline{\varphi_{\mathfrak{p}}}\partial''_{\mathfrak{p}}(\langle uv\pi\rangle) \\ &= \partial''_{T\mathfrak{p}} \circ \varphi_{\mathfrak{p}}(\langle uv\pi\rangle) &&= \partial''_{T\mathfrak{p}}\langle t_{\mathfrak{p}}(uv\pi)\rangle \\ &= \partial''_{T\mathfrak{p}}\langle t_{\mathfrak{p}}u \cdot t_{\mathfrak{p}}v \cdot t_{\mathfrak{p}}\pi\rangle &&= \langle\overline{t_{\mathfrak{p}}u}\rangle \cdot \langle\overline{t_{\mathfrak{p}}v}\rangle \\ &= \overline{\varphi_{\mathfrak{p}}}\langle\bar{u}\rangle \cdot \overline{\varphi_{\mathfrak{p}}}\langle\bar{v}\rangle, \end{aligned}$$

where the second last equality uses the tameness of (t,T) at $\mathfrak{p}$.

Now assume that $\mathfrak{p}$ is a dyadic prime of K. Then for any $\alpha \in W(K)$ we have

$$\partial_{\mathfrak{p}}(\alpha) \;=\; \operatorname{ord}_{\mathfrak{p}} \operatorname{dis} \alpha \pmod 2.$$

Since (t, T) is tame at $\mathfrak{p}$, we have

$$\partial_{\mathfrak{p}}(\alpha) \equiv \operatorname{ord}_{\mathfrak{p}} \operatorname{dis} \alpha \equiv \operatorname{ord}_{T\mathfrak{p}} t(\operatorname{dis} \alpha) \equiv \operatorname{ord}_{T\mathfrak{p}} \operatorname{dis} \varphi(\alpha) = \partial_{T\mathfrak{p}}(\varphi(\alpha)) \pmod 2.$$

With $\overline{\varphi_{\mathfrak{p}}}$ the identity map on $W(\overline{K_{\mathfrak{p}}}) = \mathbf{Z}/2\mathbf{Z} = W(\overline{L_{T\mathfrak{p}}})$, this proves the commutativity of (3). □

Remark 1. The equivalence of (a) and (b) is a trivial matter since the Witt rings of finite fields are isomorphic (as rings) if and only if their additive groups are isomorphic. Moreover, if a ring isomorphism exists, it is unique.

Remark 2. Now we can show that in the case when (t, T) is a tame Hilbert-symbol equivalence the isomorphism $\overline{\varphi}$ in the commutative diagram (2) is a *ring* isomorphism. It is defined as the coproduct of the homomorphisms $\overline{\varphi_{\mathfrak{p}}}$. But by Lemma 2, these isomorphisms are ring isomorphisms, hence so is their coproduct.

3. An abstract lemma

In this section we will describe all isomorphisms between the rings

$$P(K) := \coprod_{\mathfrak{p}} W(\overline{K_{\mathfrak{p}}}) \quad \text{and} \quad P(L) := \coprod_{\mathfrak{q}} W(\overline{L_{\mathfrak{q}}}).$$

We will view the coproducts $P(K)$ and $P(L)$ as the *internal* direct sums of the subrings $W(\overline{K_{\mathfrak{p}}})$ and $W(\overline{L_{\mathfrak{q}}})$, respectively. These direct summands are orthogonal in the sense that

$$W(\overline{K_{\mathfrak{p}_1}}) \cdot W(\overline{K_{\mathfrak{p}_2}}) = 0$$

for $\mathfrak{p}_1, \mathfrak{p}_2 \in \Omega_K$ and $\mathfrak{p}_1 \neq \mathfrak{p}_2$, and similarly for the summands of $P(L)$. Observe also that each $W(\overline{K_{\mathfrak{p}}})$ is a ring with identity element but $P(K)$ does not have an identity element. It is fairly obvious how to construct some special ring isomorphisms $\Phi : P(K) \to P(L)$. Clearly, when $\tau : \Omega_K \to \Omega_L$ is a bijective map such that for $\mathfrak{p} \in \Omega_K$ and $\mathfrak{q} = \tau(\mathfrak{p}) \in \Omega_L$ there is a ring isomorphism $\Phi_{\mathfrak{p}} : W(\overline{K_{\mathfrak{p}}}) \to W(\overline{L_{\mathfrak{q}}})$, then

$$\Phi = \coprod_{\mathfrak{p}} \Phi_{\mathfrak{p}} : P(K) \to P(L)$$

is a ring isomorphism. We now show that these are the only ring isomorphisms between $P(K)$ and $P(L)$.

Lemma 3. *Let K and L be algebraic number fields and let $\Phi : P(K) \to P(L)$ be a ring isomorphism. Then there is a bijective map*

$$\tau : \Omega_K \longrightarrow \Omega_L$$

such that for each $\mathfrak{p} \in \Omega_K$ and $\mathfrak{q} = \tau(\mathfrak{p})$ we have

$$\Phi(W(\overline{K_{\mathfrak{p}}})) = W(\overline{L_{\mathfrak{q}}}).$$

Proof. We choose and fix an arbitrary prime $\mathfrak{p} \in \Omega_K$ and we will match $\mathfrak{p}$ with a suitably chosen prime $\mathfrak{q} \in \Omega_L$. We write $1_\mathfrak{p}$ for the identity element in $W(\overline{K_\mathfrak{p}})$. Clearly,

$$W(\overline{K_\mathfrak{p}}) = 1_\mathfrak{p} \cdot P(K),$$

hence taking the images under the ring isomorphism Φ we get

$$\Phi(W(\overline{K_\mathfrak{p}})) = \Phi(1_\mathfrak{p} \cdot P(K)) = \Phi(1_\mathfrak{p}) \cdot \Phi(P(K)) = \Phi(1_\mathfrak{p}) \cdot P(L). \tag{5}$$

We begin with three general remarks. First, $\Phi(1_\mathfrak{p})$ is a nonzero idempotent in $P(L)$. Second, $\Phi(1_\mathfrak{p})$ has at most two nonzero coordinates. For if

$$\Phi(1_\mathfrak{p}) = \beta_1 + \cdots + \beta_k, \quad \text{where} \quad 0 \neq \beta_i \in W(\overline{L_{\mathfrak{q}_i}}),$$

then according to (5),

$$\Phi(W(\overline{K_\mathfrak{p}})) = \Phi(1_\mathfrak{p}) \cdot P(L) = \beta_1 \cdot W(\overline{L_{\mathfrak{q}_1}}) \oplus \cdots \oplus \beta_k \cdot W(\overline{L_{\mathfrak{q}_k}}) \tag{6}$$

and this has only 2 or 4 elements. But each of the direct summands has 2 or 4 elements so that we must have $k \leq 2$.

Third, when $\mathfrak{p}$ is a dyadic prime, then $k = 1$. Indeed, $\#W(\overline{K_\mathfrak{p}}) = 2$ for a dyadic prime $\mathfrak{p}$ and the direct summands in the decomposition (6) have at least 2 elements each. Hence $k = 1$.

Now consider the case when $k = 1$. Then there is a unique $\mathfrak{q} \in \Omega_L$ and an element $\beta = \Phi(1_\mathfrak{p}) \in W(\overline{L_\mathfrak{q}})$ such that

$$\Phi(W(\overline{K_\mathfrak{p}})) = \beta \cdot P(L) = \beta \cdot W(\overline{L_\mathfrak{q}}). \tag{7}$$

If $\mathfrak{p}$ is a nondyadic prime, then $\#W(\overline{K_\mathfrak{p}}) = 4$, and (7) forces that $\mathfrak{q}$ is a nondyadic prime and $\beta \cdot W(\overline{L_\mathfrak{q}}) = W(\overline{L_\mathfrak{q}})$. Now we set $\tau(\mathfrak{p}) = \mathfrak{q}$, and then we have $\Phi(W(\overline{K_\mathfrak{p}})) = W(\overline{L_\mathfrak{q}})$, as required.

If $\mathfrak{p}$ is a dyadic prime and $\mathfrak{q}$ is nondyadic, then $\#W(\overline{K_\mathfrak{p}}) = 2$, and (7) forces that β is a nilpotent element in $W(\overline{L_\mathfrak{q}})$ (the nonzero elements are either invertible or nilpotent). Then, however, $\Phi(1_\mathfrak{p}) = \beta$ is impossible, since $\Phi(1_\mathfrak{p})$ is a nonzero idempotent. Thus, if $\mathfrak{p}$ is a dyadic prime, so is $\mathfrak{q}$ and $\Phi(1_\mathfrak{p}) = 1_\mathfrak{q}$ (as $1_\mathfrak{q}$ is the only nonzero element in $W(\overline{L_\mathfrak{q}})$). It follows that for the dyadic prime $\mathfrak{p}$ we can set $\tau(\mathfrak{p}) = \mathfrak{q}$, and then also $\Phi(W(\overline{K_\mathfrak{p}})) = W(\overline{L_\mathfrak{q}})$, as required.

It remains to consider the case when $k = 2$, that is, when

$$\Phi(1_\mathfrak{p}) = \beta_1 + \beta_2, \quad 0 \neq \beta_i \in W(\overline{L_{\mathfrak{q}_i}}), \quad i = 1, 2.$$

We will show that this case cannot occur. Otherwise we have

$$\Phi(W(\overline{K_\mathfrak{p}})) = \Phi(1_\mathfrak{p}) \cdot P(L) = \beta_1 \cdot W(\overline{L_{\mathfrak{q}_1}}) \oplus \beta_2 \cdot W(\overline{L_{\mathfrak{q}_2}}),$$

and by our third remark $\mathfrak{p}$ is a nondyadic prime. If $\mathfrak{q}_1$ or $\mathfrak{q}_2$ is nondyadic, then either β_1 or β_2 is not invertible, since otherwise the RHS would have more than 4 elements. Hence at least one of them, say β_1, is nilpotent with vanishing square, and so

$$\Phi(1_{\mathfrak{p}}) = \Phi(1_{\mathfrak{p}}^2) = \beta_1^2 + \beta_2^2 = \beta_2^2,$$

a contradiction (we would have $k = 1$). Hence necessarily $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are dyadic primes and then we must have $\beta_1 = 1_{\mathfrak{q}_1}, \beta_2 = 1_{\mathfrak{q}_2}$. But then we consider the ring isomorphism Φ^{-1} and as above we find unique dyadic primes $\mathfrak{p}_1, \mathfrak{p}_2 \in \Omega_K$ such that

$$\Phi^{-1}(1_{\mathfrak{q}_1}) = 1_{\mathfrak{p}_1} \quad \text{and} \quad \Phi^{-1}(1_{\mathfrak{q}_2}) = 1_{\mathfrak{p}_2}.$$

Then it follows

$$1_{\mathfrak{p}} = \Phi^{-1}(\beta_1 + \beta_2) = \Phi^{-1}(1_{\mathfrak{q}_1}) + \Phi^{-1}(1_{\mathfrak{q}_2}) = 1_{\mathfrak{p}_1} + 1_{\mathfrak{p}_2},$$

which is inconsistent with the direct sum decomposition of $P(K)$. This shows that $k = 2$ is impossible.

Summing up, given a ring isomorphism $\Phi : P(K) \to P(L)$ we have defined a map $\tau : \Omega_K \to \Omega_L$ satisfying

$$\tau(\mathfrak{p}) = \mathfrak{q} \quad \Longleftrightarrow \quad \Phi(W(\overline{K_{\mathfrak{p}}})) = W(\overline{L_{\mathfrak{q}}})$$

for all $\mathfrak{p} \in \Omega_K$. It remains to show that τ is a bijective map. For this we consider the inverse ring isomorphism $\Phi^{-1} : P(L) \to P(K)$. Then by the above result there is a map $\tau_1 : \Omega_L \to \Omega_K$ satisfying

$$\tau_1(\mathfrak{q}) = \mathfrak{p} \quad \Longleftrightarrow \quad \Phi^{-1}(W(\overline{L_{\mathfrak{q}}})) = W(\overline{K_{\mathfrak{p}}}).$$

for all $\mathfrak{q} \in \Omega_L$. Combinig the two equivalences we have

$$\tau(\mathfrak{p}) = \mathfrak{q} \quad \Longleftrightarrow \quad \tau_1(\mathfrak{q}) = \mathfrak{p},$$

that is, τ_1 is the inverse map for τ. Hence τ is bijective, as desired. □

4. Main result

We are now in a position to give a characterization of tame Hilbert-symbol equivalences in terms of commuting diagrams

$$\begin{array}{ccc} W(K) & \xrightarrow{\partial_K} & \coprod_{\mathfrak{p}} W(\overline{K_{\mathfrak{p}}}) \\ \downarrow \varphi & & \downarrow \Phi \\ W(L) & \xrightarrow{\partial_L} & \coprod_{\mathfrak{q}} W(\overline{L_{\mathfrak{q}}}) \end{array} \tag{8}$$

Theorem. *Let (t, T) be a Hilbert-symbol equivalence between number fields K and L and let $\varphi : W(K) \to W(L)$ be the associated Witt ring isomorphism. The following are equivalent.*

(a) *The equivalence (t, T) is tame.*

(b) *There is a commutative diagram* (8), *where* Φ *is a ring isomorphism.*

Proof. (a) $\Rightarrow$ (b) When (t, T) is a tame Hilbert-symbol equivalence between K and L, then for each finite prime $\mathfrak{p}$ of K there is a commutative diagram (3) of Lemma 2, where $\overline{\varphi_{\mathfrak{p}}} : W(\overline{K_{\mathfrak{p}}}) \to W(\overline{L_{\mathfrak{q}}})$ is a ring isomorphism. Then $\Phi := \coprod_{\mathfrak{p}} \overline{\varphi_{\mathfrak{p}}}$ is a ring isomorphism, and we obtain a commutative diagram (8).

(b) $\Rightarrow$ (a) According to Lemma 3 there is a bijective map $\tau : \Omega_K \to \Omega_L$ such that for each $\mathfrak{p} \in \Omega_K$ and $\mathfrak{q} = \tau(\mathfrak{p})$ we have $\Phi(W(\overline{K_{\mathfrak{p}}})) = W(\overline{L_{\mathfrak{q}}})$. We will show that $\tau = T$, that is, $\tau(\mathfrak{p}) = T(\mathfrak{p})$ for all $\mathfrak{p} \in \Omega_K$. We distinguish two cases.

Case 1. $\mathfrak{p}$ is a nondyadic prime.

Suppose $\mathfrak{q} := \tau(\mathfrak{p}) \neq T(\mathfrak{p})$. Then there are $a, b \in K^*/K^{*2}$ such that

$$(a, b)_{\mathfrak{p}} = (ta, tb)_{T\mathfrak{p}} = 1 \quad \text{and} \quad (ta, tb)_{\mathfrak{q}} = -1.$$

Thus $\langle 1, -a, -b, ab \rangle = 0 \in W(K_{\mathfrak{p}})$ and we have

$$\Phi\partial_{\mathfrak{p}}\langle 1, -a, -b, ab \rangle = \Phi(0) = 0.$$

On the other hand, $\langle 1, -ta, -tb, tab \rangle$ is anisotropic over $L_{\mathfrak{q}}$, hence isometric to the unique anisotropic quaternary quadratic form $\langle 1, -u, -\pi, u\pi \rangle$ over $L_{\mathfrak{q}}$, where u is a $\mathfrak{q}$-adic unit and π is a $\mathfrak{q}$-adic prime. Hence

$$\partial_{\mathfrak{q}}\varphi\langle 1, -a, -b, ab \rangle = \partial_{\mathfrak{q}}\langle 1, -ta, -tb, tab \rangle = \partial_{\mathfrak{q}}\langle 1, -u, -\pi, u\pi \rangle = \langle -1, \bar{u} \rangle \neq 0,$$

contradicting the commutativity of (8). Hence $\tau(\mathfrak{p}) = T(\mathfrak{p})$, as desired.

Case 2. $\mathfrak{p}$ is a dyadic prime.

We say that $a \in K^*$ is an *isolated dyadic nonsquare* (IDN, for short) if there is a dyadic prime $\mathfrak{p}$ of K such that $a \notin K_{\mathfrak{p}}^{*2}$ and $a \in K_{\mathfrak{P}}^{*2}$ for the remaining dyadic primes $\mathfrak{P}$ of K. Then we also say that a is an IDN at $\mathfrak{p}$.

Clearly, $a \in K^*$ is an IDN at $\mathfrak{p}$ if and only if ab^2 is IDN at $\mathfrak{p}$ for all $b \in K^*$. Hence we can speak of IDN square classes aK^{*2}.

Isolated dyadic nonsquares exist: a number $a \in K^*$ close to a nonsquare at $\mathfrak{p}$ and close to 1 at remaining dyadic primes is an IDN at $\mathfrak{p}$.

An application of Lemma 1(b) shows that

if $a \in K^*/K^{*2}$ is an IDN at $\mathfrak{p}$, then $ta \in L^*/L^{*2}$ is an IDN at $T\mathfrak{p}$.

In fact, $\langle ta \rangle = \varphi_{\mathfrak{p}}\langle a \rangle \neq 1_{T\mathfrak{p}}$, hence ta is a nonsquare at $T\mathfrak{p}$, and $\langle ta \rangle = \varphi_{\mathfrak{P}}\langle a \rangle = 1_{T\mathfrak{P}}$ for dyadic $\mathfrak{P} \neq \mathfrak{p}$, hence ta is a square at $T\mathfrak{P}$.

Now choose $a \in K^*$ to be a local prime element at $\mathfrak{p}$ and a square at all the remaining dyadic primes of K. Then a is an IDN at $\mathfrak{p}$. We use the prime element a to define the second residue homomorphism $\partial_{\mathfrak{p}}$. By the commutativity of (8),

$$\partial_{\tau(\mathfrak{p})}\langle ta \rangle = \partial_{\tau(\mathfrak{p})}\varphi\langle a \rangle = \Phi\partial_{\mathfrak{p}}\langle a \rangle = \Phi(1_{\mathfrak{p}}) = 1_{\tau(\mathfrak{p})}.$$

Hence ta is a nonsquare at $\tau(\mathfrak{p})$, and as observed above, ta is an IDN at $T(\mathfrak{p})$. Hence $\tau(\mathfrak{p}) = T(\mathfrak{p})$, as desired.

Summing up the results of the two cases we have proved that $\tau = T$. Thus in the commutative diagram (8) we have $\Phi(W(\overline{K_{\mathfrak{p}}})) = W(\overline{L_{T\mathfrak{p}}})$, and at the $\mathfrak{p}$−th coordinate of the coproduct $\coprod_{\mathfrak{p}} W(\overline{K_{\mathfrak{p}}})$ the diagram (8) reduces to the commutative diagram (3). By Lemma 2, it follows that (t, T) is tame. □

We make one final comment on the diagram (3). Lemma 3 asserts that the existence of such a diagram is equivalent to the tameness of the given Hilbert-symbol equivalence at $\mathfrak{p}$. It is of some importance to realize that a similar diagram, with Witt rings of residue class fields replaced by Witt rings of the local fields, characterizes the Hilbert-symbol equivalence itself.

Proposition. *Let (t, T) be a Hilbert-symbol equivalence between number fields K and L and let $\varphi : W(K) \to W(L)$ be the associated Witt ring isomorphism. Let $\mathfrak{p} \in \Omega_K$ be a fixed prime. The following are equivalent.*

(a) *There is a commutative diagram*

$$\begin{array}{ccc} W(K) & \to & W(K_{\mathfrak{p}}) \\ \downarrow\varphi & & \downarrow\psi \\ W(L) & \to & W(L_{\mathfrak{q}}) \end{array} \tag{9}$$

where $\mathfrak{q} \in \Omega_L$ and ψ is a ring isomorphism.

(b) *$K_{\mathfrak{p}}$ and $L_{\mathfrak{q}}$ are Hilbert-symbol equivalent in the sense that*

$$(a, b)_{\mathfrak{p}} = (ta, tb)_{\mathfrak{q}} \quad \text{for all} \quad a, b \in K^*.$$

(c) $\mathfrak{q} = T(\mathfrak{p})$.

Proof. (a) ⇒ (b) For $a \in K^*$ we have $\varphi\langle a\rangle = \langle ta\rangle$, so that by commutativity of (9) we get $\psi\langle aK_{\mathfrak{p}}^{*2}\rangle = \langle taL_{\mathfrak{q}}^{*2}\rangle$. Hence for all $a, b \in K^*$,

$$\psi\langle 1, -a, -b, ab\rangle = \langle 1, -ta, -tb, tab\rangle,$$

and so

$$\begin{aligned} (a, b)_{\mathfrak{p}} = 1 \quad &\Longleftrightarrow \quad \langle 1, -a, -b, ab\rangle = 0 \in W(K_{\mathfrak{p}}) \\ &\Longleftrightarrow \quad \langle 1, -ta, -tb, tab\rangle = 0 \in W(L_{\mathfrak{q}}) \\ &\Longleftrightarrow \quad (ta, tb)_{\mathfrak{q}} = 1. \end{aligned}$$

(b) ⇒ (c) By the Hilbert-symbol equivalence, $(a, b)_{\mathfrak{p}} = (ta, tb)_{T\mathfrak{p}}$ for all $a, b \in K^*$. Hence

$$(ta, tb)_{\mathfrak{q}} = (ta, tb)_{T\mathfrak{p}} \quad \text{for all} \quad ta, tb \in L^*/L^{*2},$$

and $\mathfrak{q} = T\mathfrak{p}$ follows.

(c) ⇒ (a) Take $\psi = \varphi_{\mathfrak{p}}$ and apply Lemma 1. □

References

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

[2] A. Czogała, *On integral Witt equivalence of algebraic number fields.* Acta Math. Inform. Univ. Ostrav. **4** (1996), 7–21.

[3] T. Y. Lam, *The Algebraic Theory of Quadratic Forms.* Mathematics Lecture Note Series, Benjamin/Cummings Publ. Co., Reading, Mass. 1973.

[4] J. Milnor and D. Husemoller, *Symmetric Bilinear Forms.* Ergebnisse der Mathematik und ihrer Grenzgebiete **73**, Springer-Verlag, Berlin Heidelberg New York 1973.

[5] R. Perlis, K. Szymiczek, P. E. Conner, and R. Litherland, *Matching Witts with global fields.* Contemporary Mathematics **155** (1994), 365–387.

[6] W. Scharlau, *Quadratic and Hermitian Forms.* Grundlehren der mathematischen Wissenschaften **270**, Springer-Verlag, Berlin Heidelberg New York Tokyo 1985.

Received: October 8, 1997