Acta Mathematica et Informatica Universitatis Ostraviensis

Alfred Czogała

On integral Witt equivalence of algebraic number fields

Acta Mathematica et Informatica Universitatis Ostraviensis, Vol. 4 (1996), No. 1, 7--21

Persistent URL: `http://dml.cz/dmlcz/120498`

Acta Mathematica et Informatica Universitatis Ostraviensis 4(1996) 7–20

On integral Witt equivalence of algebraic number fields

ALFRED CZOGALA

Abstract. Two algebraic number fields K and L are said to be *integrally Witt equivalent* if there exists a Witt ring isomorphism $W(K) \to W(L)$ mapping the Witt ring $W(\mathcal{O}_K)$ of the ring of integers $\mathcal{O}_K$ of K onto the Witt ring $W(\mathcal{O}_L)$ of the ring of integers $\mathcal{O}_L$ of L. The paper connects integral Witt equivalence with Hilbert-symbol equivalence of number fields, and gives a complete classification of quadratic number fields with respect to the integral Witt equivalence.

1991 Mathematics Subject Classification: Primary 11E81, Secondary 11E12

1 Introduction

The notion of the Witt ring of a field plays a central role in the algebraic theory of quadratic forms. While asking for a description of the isomorphism type of the Witt ring $W(K)$ of a general field K as an exclusive question, asking for criteria differentiating between nonisomorphic Witt rings turns out to be a menageable problem. Two fields with isomorphic Witt rings are said to be *Witt equivalent* and the problem consists in classifying fields with respect to Witt equivalence.

When K is an algebraic number field, there is another Witt ring to be considered, the Witt ring $W(\mathcal{O}_K)$ of symmetric bilinear forms over the ring $\mathcal{O}_K$ of integers of K. We call $W(\mathcal{O}_K)$ the *integral Witt ring* of K.

The extension of scalars yields the ring homomorphism $W(\mathcal{O}_K) \longrightarrow W(K)$ which is known to be injective (cf. [4, Cor.3.3]). For this reason we will view the integral Witt ring of K as a *subring* of the Witt ring of K.

In this paper we consider Witt equivalent number fields K and L and the isomorphisms $\phi : W(K) \to W(L)$ of their Witt rings inducing isomorphisms of their integral Witt rings $W(\mathcal{O}_K)$ and $W(\mathcal{O}_L)$. If for fields K and L such an isomorphism ϕ of Witt rings exists, then we say that K and L are *integrally Witt equivalent.*

We will be even more restrictive and will consider only the so called *strong isomorphisms* of Witt rings, i. e., isomorphisms preserving the dimensions of anisotropic forms. It follows from the Harrison's Criterion (see [6]) that strong isomorphisms of isomorphic Witt rings always exist.

In [6] there has been introduced the concept of a reciprocity equivalence of two number fields as a necessary and sufficient condition for the fields to be Witt equivalent. Following [9] and [2] we will use the name *Hilbert-symbol equivalence* instead of reciprocity equivalence.

Recall that two algebraic number fields K and L are said to be *Hilbert-symbol equivalent* if there is a pair of maps (t, T), where

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

is a group isomorphism and

$$T : \Omega(K) \longrightarrow \Omega(L)$$

is a bijection of the set all primes of K onto the set of all primes of L, preserving Hilbert symbols in the sense that

$$(a,\, b)_P = (ta,\, tb)_{TP}$$

for all $a, b \in \dot{K}/\dot{K}^2$ and $P \in \Omega(K)$. One of the main results in [6] (see also [8], [9]) asserts that *two global fields are Witt equivalent iff they are Hilbert-symbol equivalent.*

In this paper we give a necessary and sufficient condition for integral Witt equivalence of number fields. The condition, called here the *even-order-preserving Hilbert-symbol equivalence* (EOP-Hilbert-symbol equivalence, or EOP equivalence, for short) is a special type of Hilbert-symbol equivalence defined as follows.

For a number field K we set

$$\dot{K}_{ev} = \{x \in \dot{K} : \mathrm{ord}_P\, x \equiv 0 \pmod 2 \ \text{ for every finite prime } P \text{ of } K\ \}.$$

We say that a given Hilbert-symbol equivalence (t, T) between two number fields K and L is *even-order-preserving*, whenever

$$t(\dot{K}_{ev}/\dot{K}^2) \;=\; \dot{L}_{ev}/\dot{L}^2.$$

In Section 2 we prove the following result.

Theorem 1. *Two algebraic number fields K and L are integrally Witt equivalent if and only if they are EOP-Hilbert-symbol equivalent.*

For a number field K, let $\Omega_0(K)$ be the set of all infinite and all dyadic primes of K, and let K_P be the completion of K at the prime P.

The following theorem gives a finiteness condition for the integral Witt equivalence. For a proof, see Section 3.

Theorem 2. *Two number fields K and L are integrally Witt equivalent if and only if there is a bijective map $T : \Omega_0(K) \longrightarrow \Omega_0(L)$ and a group isomorphism $t : \dot{K}_{ev}/\dot{K}^2 \longrightarrow \dot{L}_{ev}/\dot{L}^2$ satisfying the following conditions:*

1. *P is infinite real iff TP is infinite real.*
2. *P is dyadic iff TP is dyadic; moreover $[K_P : \mathbb{Q}_2] = [L_{TP} : \mathbb{Q}_2]$.*
3. *$t(-1) = -1$.*

4. *x is positive at P iff tx is positive at TP, for all $x \in \dot{K}$ and all infinite real primes P.*

5. *For every dyadic prime P of K, the map t induces a Hilbert-symbol preserving group isomorphism*

$$t : K_{ev}\dot{K}_P/\dot{K}_P^2 \longrightarrow L_{ev}\dot{L}_{TP}/\dot{L}_{TP}^2.$$

Theorem 2 allows us to give a complete classification of quadratic number fields with respect to integral Witt equivalence (EOP-Hilbert-symbol equivalence).
For a number field K, we write $g(K)$ for the number of dyadic primes of K, $r(K)$ for the number of real embeddings of K, $N(K)$ for the norm group of the extension $K/\mathbb{Q}$, $l(K)$ for the number of distinct prime divisors of the discriminant of K.
Theorem 3. *Let K and L be quadratic number fields and let P and Q be arbitrary dyadic prime ideals in K and L, respectively. The fields K and L are integrally Witt equivalent if and only if the following nine conditions are satisfied:*

(0) $-1 \in \dot{K}^2 \iff -1 \in \dot{L}^2$.
(I) $r(K) = r(L)$.
(II) $g(K) = g(L)$.
(III) $-1 \in \dot{K}_P^2 \iff -1 \in \dot{L}_Q^2$.
(IV) $l(K) = l(L)$.
(V) $-1 \in N(K) \iff -1 \in N(L)$.
(VI) *2 is prime in K or* $2 \in |N(K)| \iff$ *2 is prime in L or* $2 \in |N(L)|$.
(VII) *If* $-1 \notin N(K)$, *then* $-2 \in N(K) \iff -2 \in N(L)$.
(VIII) *If* $g(K) = 2$ *and* $-1 \in N(K)$, *then* $(2, a)_P = (2, a')_Q$,

where a, a' are elements of K_{ev} and L_{ev}, respectively, with negative norms.

Theorem 3 implies that there are infinitely many classes of integrally Witt equivalent quadratic number fields because fields with distinct numbers of prime factors of the discriminants are not integrally Witt equivalent. However, if we fix the number of prime factors of the discriminant, then from Theorem 3 it follows that there are at most 18 classes of integrally Witt equivalent quadratic number fields with the given number of prime factors of the discriminant. For example, the following fields $\mathbb{Q}(\sqrt{d})$, $d = -1, -2, -7, 2, 17, 41$, represent quadratic number fields with exactly one prime factor of the discriminant.
The integral Witt equivalence of fields K and L is a sufficient condition for the existence of a strong isomorphism of Witt rings $W(\mathcal{O}_K) \to W(\mathcal{O}_L)$. Unfortunately, this condition is not necessary. We know from [5] that the integral Witt rings of the fields $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{7})$ are strongly isomorphic but, on other hand, these fields are not integrally Witt equivalent, according to Theorem 3.

EOP-Hilbert-symbol equivalence of number fields is closely related to *tame* Hilbert-symbol equivalence. We recall the definition. Let $P \in \Omega(K)$ be any finite prime. The Hilbert-symbol equivalence (t, T) is said to be *tame* at P if

$$\mathrm{ord}_P\, a \equiv \mathrm{ord}_{TP}\, ta \pmod 2$$

for all $a \in \dot{K}/\dot{K}^2$. The equivalence (t, T) is said to be *tame* when it is tame for all finite primes of K.

It is clear that a tame equivalence is also an EOP equivalence. A preliminary version of the paper [6] contained the proof of the fact that *tame equivalence implies integral Witt equivalence* of number fields. This result has been omitted in the printed version of the paper. We also remark that an analogue of Theorem 2 for Hilbert-symbol equivalence has been proved in [1, Theorem 3.1] and for tame equivalence in [3, Theorem 2.1].

2 Hilbert-symbol equivalence versus integral Witt equivalence

If K is an algebraic number field, then we have the Knebusch-Milnor exact sequence (cf. [4, p. 93, 3.3, 3.4]):

$$0 \longrightarrow W(\mathcal{O}_K) \longrightarrow W(K) \xrightarrow{\partial} \sum_P W(\overline{K}_P) \longrightarrow C(K)/C(K)^2 \longrightarrow 1$$

Here the sum runs over all finite primes of K, whereas $\overline{K}_P$ and $C(K)$ denote the residue class field of the completion K_P of K at P and the ideal class group of K, respectively. The additive group homomorphism $\partial = \partial_K$ is the direct sum of the second residue class homomorphisms $\partial_P : W(K) \longrightarrow W(\overline{K}_P)$.

Although the homomorphism ∂_P depends on the choice of the local uniformizer at P, the kernel $\ker \partial_P$ doesn't depend on that choice. Hence the kernel of the homomorphism ∂_K doesn't depend on the choices of local uniformizers. Throughout the paper we will identify the ring $W(\mathcal{O}_K)$ with the kernel of ∂_K. Recalling the definition we can say, that *two algebraic number fields K and L are integrally Witt equivalent iff there exists a strong isomorphism $\phi : W(K) \longrightarrow W(L)$ such that $\phi(\ker \partial_K) = \ker \partial_L$.*

In the proof of the Theorem 1 we use the following auxiliary facts from [7, Prop. 2.4]. Let $q \in W(K)$ and $a \in \dot{K}$. Then:

(1) $q \in W(\mathcal{O}_K) \Longrightarrow \operatorname{dis} q \in K_{ev}$,

(2) $\langle a \rangle \in W(\mathcal{O}_K) \iff a \in K_{ev}$.

Proof of the Theorem 1: (Necessity). Let ϕ be a strong isomorphism of Witt rings of K and L such that $\phi(W(\mathcal{O}_K)) = W(\mathcal{O}_L)$. The isomorphism ϕ induces canonically a Harrison map t_ϕ such that $\phi(\langle a \rangle) = \langle t_\phi a \rangle$ for all $a \in \dot{K}/\dot{K}^2$. From [6] it follows that there exists a Hilbert-symbol equivalence (t, T) from K to L satisfying $t = t_\phi$. Now $a \in K_{ev}$ implies that $\phi(\langle a \rangle) \in W(\mathcal{O}_L)$, hence $ta \in L_{ev}$. This proves that the equivalence (t, T) is even-order-preserving. □

To prove the converse statement we need some auxiliary results. Lemmas 2.1, 2.2 and Proposition 2.1 have been reproduced from the unpublished preliminary 1989 version of [6].

Let (t, T) be a Hilbert-symbol equivalence of algebraic number fields K and L. Pick a prime P of K. There exists a natural group epimorphism $\dot{K}/\dot{K}^2 \to \dot{K}_P/\dot{K}_P^2$ whose kernel is $\ker_1 = \{a \in \dot{K}/\dot{K}^2;\ (a, x)_P = 1 \text{ for every } x \in \dot{K}/\dot{K}^2\}$. Consider the diagram

$$\begin{tikzcd} \ker_1 \arrow[r] & \dot{K}/\dot{K}^2 \arrow[r] \arrow[d, "t"] & \dot{K}_P/\dot{K}_P^2 \arrow[r] \arrow[d, dashed, "t_P"] & 1 \\ \ker_2 \arrow[r] & \dot{L}/\dot{L}^2 \arrow[r] & \dot{L}_{TP}/\dot{L}_{TP}^2 \arrow[r] & 1 \end{tikzcd}$$

The map t preserves Hilbert symbols, hence t sends $\ker_1$ to $\ker_2$ and we obtain the following result.

Lemma 2.1. *The map t induces a local Hilbert-symbol-preserving isomorphism*

$$t_P : \dot{K}_P/\dot{K}_P^2 \longrightarrow \dot{L}_{TP}/\dot{L}_{TP}^2.$$

From the above lemma and Harrison's Criterion (see [6]) it follows that t induces a global Witt ring isomorphism $\phi = \phi_t$ and a local Witt ring isomorphism ϕ_P making the following diagram commute

$$\begin{tikzcd} W(K) \arrow[r] \arrow[d, "\phi"] & W(K_P) \arrow[d, "\phi_P"] \\ W(L) \arrow[r] & W(L_{TP}) \end{tikzcd}$$

The horizontal arrows are the canonical ring homomorphisms and the vertical arrows are ring isomorphisms mapping the class of $\langle a \rangle$ to the class of $\langle ta \rangle$ (resp. $\langle t_P a \rangle$).

Lemma 2.2. *If the Hilbert-symbol equivalence (t, T) is tame at P, then there exists an isomorphism $\overline{\phi}_P : W(\overline{K}_P) \longrightarrow W(\overline{L}_{TP})$ such that the following diagram is commutative*

$$\begin{tikzcd} W(K) \arrow[r] \arrow[d, "\phi"] & W(K_P) \arrow[r, "\partial_P"] \arrow[d, "\phi_P"] & W(\overline{K}_P) \arrow[d, "\overline{\phi}_P"] \\ W(L) \arrow[r] & W(L_{TP}) \arrow[r, "\partial_{TP}"] & W(\overline{L}_{TP}) \end{tikzcd}$$

(with appropriate choices of the uniformizers).

PROOF: Assume that the finite prime P is non-dyadic. Choose a local prime square class $\pi \in \dot{K}_P/\dot{K}_P^2$, that is, the square class of a local uniformizing parameter at P. From the congruence $\mathrm{ord}_P\, \pi \equiv \mathrm{ord}_{TP}\, t_P\pi \pmod 2$ it follows that $t_P\pi$ is

a local prime class in $\dot{L}_{TP}/\dot{L}_{TP}^2$. We choose the prime class $t_P\pi$ in $\dot{L}_{TP}/\dot{L}_{TP}^2$ to define the map ∂_{TP}.
The map ∂_P is a left inverse to the injection $j_P : W(\overline{K}_P) \longrightarrow W(K_P)$ mapping $\langle \overline{u}_1, \dots, \overline{u}_n\rangle$ in $W(\overline{K}_P)$ to $\langle \pi u_1, \dots, \pi u_n\rangle$ in $W(K_P)$. We define $\overline{\phi}_P = \partial_{TP} \circ \phi_P \circ j_P$. Then ϕ_P produces the desired commutative diagram.
Now consider a dyadic prime P. Then TP is also dyadic (see [6]), and the Witt rings of the residue class fields are isomorphic to $\mathbb{Z}/2\mathbb{Z}$. The second residue class homomorphism becomes $\partial_P(q) \equiv \operatorname{ord}_P(\operatorname{dis} q) \pmod 2$. In this case we define $\phi_P = \mathrm{id}$ to be the identity map. Since t_P preserves orders modulo 2, this produces the necessary commutative diagram. □

Corollary 2.1. *Assume that the Hilbert-symbol equivalence $(t,\, T)$ is tame at P and $q \in W(K)$. Then $\partial_P(q) = 0$ iff $\partial_{TP}(q) = 0$.* □

Proposition 2.1. *If the Hilbert-symbol equivalence $(t,\, T)$ of K and L is tame, then the integral Witt rings $W(\mathcal{O}_K)$ and $W(\mathcal{O}_L)$ are isomorphic and ideal class groups modulo squares $C(K)/C(K)^2$ and $C(L)/C(L)^2$ are isomorphic.*

PROOF: It suffices to consider the following commutative diagram obtained from Knebusch-Milnor sequences and Lemma 2.2:

$$\begin{array}{ccccccccc}
0 \to W(\mathcal{O}_K) & \longrightarrow & W(K) & \xrightarrow{\partial_K} & \sum_P W(\overline{L}_{TP}) & \longrightarrow & C(K)/C(K)^2 & \longrightarrow & 1 \\
 & & \Big\downarrow \phi & & \Big\downarrow \overline{\phi} & & & & \\
0 \to W(\mathcal{O}_L) & \longrightarrow & W(L) & \xrightarrow{\partial_L} & \sum_P W(\overline{L}_{TP}) & \longrightarrow & C(L)/C(L)^2 & \longrightarrow & 1
\end{array}$$

Here $\overline{\phi} = \sum_P \overline{\phi}_P$. □

Proposition 2.2. *If P is a finite non-dyadic prime of K with $-1 \notin \dot{K}_P^2$, then the Hilbert-symbol equivalence $(t,\, T)$ is tame at P.*

PROOF: From [6] it follows that the prime TP of L is finite and non-dyadic and -1 is not a local square at TP. The quadratic extensions $K_P(\sqrt{-1})/K_P$ and $L_{TP}(\sqrt{-1})/L_{TP}$ are unramified. Then we have

$$(-1,\, a)_P = (-1)^{\operatorname{ord}_P a} \quad \text{and} \quad (-1,\, ta)_{TP} = (-1)^{\operatorname{ord}_{TP} ta}$$

for every $a \in \dot{K}$. Now the equality of Hilbert symbols $(-1,\, a)_P = (-1,\, ta)_{TP}$ proves that the equivalence $(t,\, T)$ is tame at P. □

PROOF OF THEOREM 1: (Sufficiency). Let $(t,\, T)$ be an EOP-Hilbert-symbol equivalence between K and L, and $\phi = \phi_t$ be the Witt ring homomorphism induced by t. Consider $q \in W(\mathcal{O}_K)$ and assume that q is anisotropic over K. Then $\operatorname{dis} q \in K_{ev}$ implies $\operatorname{dis} \phi q \in L_{ev}$.
Now we show that $\partial_{TP}(\phi q) = 0$ for all finite primes P of K.

(1) First consider a dyadic prime P. Then TP is also dyadic, and the Witt ring of the residue class field $\overline{L}_{TP}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. The second residue homomorphism ∂_{TP} yields

$$\partial_{TP}(\phi q) = \mathrm{ord}_{TP}(\mathrm{dis}\, \phi q) \bmod 2 = 0$$

(2) If P is nondyadic with $-1 \notin \dot{K}_P^2$, then from Cor. 2.3 and Prop. 2.2 it follows that $\partial_{TP}(\phi\, q) = 0$.
(3) Finally consider a finite non-dyadic prime P at which -1 is a local square. If $q = 0$ in $W(K_P)$, then $\partial_{TP}(\phi\, q) = 0$.
Now suppose that $q \neq 0$ in $W(K_P)$. Let $q = \langle a_1, \ldots, a_n \rangle$. The square class group of K_P consists of 4 elements, hence after renumbering $a_1, \ldots, a_n$ (if necessary) we have the following decomposition over K

$$q = \langle a_1, \ldots, a_k \rangle \perp \langle a_{k+1}, a_{k+2} \rangle \perp \langle a_{n-1}, a_n \rangle,$$

where $1 \leq k \leq 4$, the square classes of $a_1, \ldots, a_k$ are pairwise distinct in $\dot{K}_P/\dot{K}_P^2$ and $a_i = a_{i+1} \bmod \dot{K}_P^2$ for $i = k+1,\, k+3,\, \ldots,\, n-1$.
The form $q_1 = \langle a_1, \ldots, a_k \rangle$ is anisotropic over K_P and all $\langle a_i,\, a_{i+1} \rangle$ are hyperbolic over K_P. Thus we can decompose the form q over K into the sum $q = q_1 \perp q_2$, where q_1 and q_2 are anisotropic and hyperbolic over K_P, respectively (of course, $\dim q \leq 4$). It is clear that $\partial_P(q_2) = 0$, and this implies $\partial_P(q_1) = 0$. Analyzing the anisotropic forms over K lying in the kernel of the second residue class homomorphism we deduce that q_1 can be written as $\langle a \rangle$, $\langle b \rangle$ or $\langle a,\, b \rangle$, where $a, b \in \dot{K}$ are P-adic units modulo squares and $a \in \dot{K}_P^2$, $b \notin \dot{K}_P^2$. We also have the decomposition $\phi q = \phi q_1 \perp \phi q_2$ over the field L. Moreover, ϕq_1 and ϕq_2 are anisotropic and hyperbolic over L_{TP}, respectively. Thus $\mathrm{dis}(\phi q_2)$ is a local square at TP. Hence $\mathrm{ord}_{TP}(\mathrm{dis}\phi q_1)$ is even. When q_1 is a one-dimensional form, we get $\partial_{TP}(\phi q_1) = 0$. If $q_1 = \langle a,\, b \rangle$, then $\phi q_1 = \langle ta,\, tb \rangle$. Because $\mathrm{ord}_{TP} tatb$ is even and $(ta,\, tb)_{TP} = (a,\, b)_P = 1$, we get $\partial_{TP}(\phi q_1) = 0$.
In both cases we have $\partial_{TP}(\phi q) = \partial_{TP}(\phi q_1) = 0$.
Now consider the EOP-Hilbert-symbol equivalence $(t^{-1},\, T^{-1})$, and let ψ be the Witt ring isomorphism induced by t^{-1}. From the above it follows that $\psi(W(\mathcal{O}_L)) \subseteq W(\mathcal{O}_K)$. As a result we get $\phi(W(\mathcal{O}_K)) = W(\mathcal{O}_L)$. □

3 Integral Witt equivalence

In this section we prove the characterization of the integral Witt equivalence given in Theorem 2. According to Theorem 1, we can switch to even-order-preserving Hilbert-symbol equivalence. We begin with introducing some notation. For a number field K let K_+ denote the set of totally positive elements of K and let

$$K_{sq} = \{x \in K_{ev} :\ x \in \dot{K}_P^2 \ \text{for every prime}\ P \in \Omega_0(K)\}.$$

We write $\rho = \rho(K)$ for the 2-rank of the ideal class group $C(K)$ of K, $\sigma = \sigma(K)$ for the 2-rank of the subgroup of $C(K)$ generated by the classes of dyadic ideals of K and $c = c(K)$ for the number of infinite complex primes of K. According to [3] we have

$$\dim_{\mathbf{F}_2} \dot{K}_{ev}/\dot{K}^2 = r + c + \rho,$$

$$\dim_{\mathbf{F}_2} K_{sq}/\dot{K}^2 = \rho - \sigma.$$

Proposition 3.1. *Let (t, T) be an EOP-Hilbert-symbol equivalence between K and L. Then t induces the following group isomorphisms.*
(a) $K_{ev} \cap K_+/\dot{K}^2 \cong L_{ev} \cap L_+/\dot{L}^2$.
(b) $K_{sq}/\dot{K}^2 \cong L_{sq}/\dot{L}^2$.

PROOF: . This follows from [6]. □

Clearly EOP equivalence preserves all those properties of fields which are preserved by a plain Hilbert-symbol equivalence (the degree over $\mathbb{Q}$, the number of real embeddings, the number of dyadic primes, etc; cf. [6]). Now we apply Prop. 3.1 to show that an EOP equivalence preserves some additional arithmetic properties of fields.

Corollary 3.1. *If K and L are EOP-Hilbert-symbol equivalent, then*
(i) *the ideal class groups of K and L have the same 2-ranks;*
(ii) *the narrow ideal class groups of K and L have the same 2-ranks;*
(iii) *the subgroups of ideal class groups of K and L generated by the classes of dyadic ideals have the same 2-ranks.*

PROOF: (i) and (iii) follow from Prop. 3.1. If K is a number field and $\hat{\rho}(K)$ denotes 2-rank of the narrow ideal class group of K, then [4] states that the order of the group $K_{ev} \cap K_+/\dot{K}^2$ is equal to $2^{c(K)}\hat{\rho}(K)$. Thus (ii) follows from Prop. 3.1. □ □

PROOF OF THEOREM 2: (Necessity.) Let (t, T) be an EOP-Hilbert-symbol equivalence between K and L. Restricting T to $\Omega_0(K)$ and t to $K_{ev}/\dot{K}^2$ we obtain the maps t and T as stated in Theorem 2. Then, according to [6], (1) – (5) are satisfied. □

In the proof of the sufficiency part of Theorem 2 we use the concept of a *small equivalence* (cf. [6]). According to [6] we say that a finite set S of primes of K is *sufficiently large* when S contains all infinite and dyadic primes, and when the class number $h^S(K)$ of the ring of S–integers of K is odd. We write $U_K(S)$ for the group of S-units of K. The S-unit square class group $U_K(S)/U_K(S)^2$ will be identified with its image under the natural embedding $U_K(S)/U_K(S)^2 \longrightarrow \dot{K}/\dot{K}^2$. The following statement follows from [6, Lemma 5].
If S is a sufficiently large set of primes of K, then a square class a in $\dot{K}/\dot{K}^2$ is represented by an S-unit iff $\operatorname{ord}_P a \equiv 0 \pmod 2$ *for every finite $P \in \Omega(K) \setminus S$.*

Corollary 3.2. *If S is a sufficiently large set of primes of K, then the group $\dot{K}_{ev}/\dot{K}^2$ is a subgroup of $U_K(S)/U_K(S)^2$.*

Let S be a sufficiently large set of primes of K and consider the direct product of the groups $\dot{K}_P/\dot{K}_P^2$ over all $P \in S$,

$$G(S) = \prod_{P \in S} \dot{K}_P/\dot{K}_P^2.$$

The Lemma 5 in [6] states that the map $i_s : U_K(S)/U_K(S)^2 \longrightarrow G(S)$ which maps the square class of $y \in \dot{K}$ to the tuple $(y, \ldots, y)$ where the $P-$th coordinate represents the image of the global square class y in $\dot{K}_P/\dot{K}_P^2$, is injective.

In the sequel we use the same symbol for $x \in \dot{K}$ and its canonical image in $\dot{K}/\dot{K}^2$. We will do the same with cosets of $\dot{K}$ modulo some other subgroups of $\dot{K}$.

PROOF OF THEOREM: 2. (Sufficiency.) Let t and T denote maps satisfying the conditions (1) – (5) in Theorem 2. We first observe that K and L have the same degree over $\mathbb{Q}$ and $r(K) = r(L)$, $c(K) = c(L)$, $g(K) = g(L)$. Thus $\rho(K) = \rho(L)$. From (4) and (5) it follows that t induces the isomorphism $K_{sq}/\dot{K}^2 \cong L_{sq}/\dot{L}^2$. Therefore we have $\sigma(K) = \sigma(L)$. Write $m = \rho - \sigma$, $n = r + c + \sigma$. Let $\{a_1, \ldots, a_n\}$ and $\{b_1, \ldots, b_m\}$ be bases for K_{ev}/K_{sq} and $K_{sq}/\dot{K}^2$, resp., where we choose $b_1 = -1$ whenever $-1 \in K_{sq} \setminus \dot{K}^2$. Then the set $B_K = \{a_1, \ldots, a_n, b_1, \ldots, b_m\}$ is a basis for $K_{ev}/\dot{K}^2$ and the set $B_L = \{ta_1, \ldots, ta_n, tb_1, \ldots, tb_m\}$ is a basis for $L_{ev}/\dot{L}^2$, and moreover, $\{ta_1, \ldots, ta_n\}$ is a basis for L_{ev}/L_{sq}, $\{tb_1, \ldots, tb_m\}$ is a basis for $L_{sq}/\dot{L}^2$ and $tb_1 = -1$ whenever $-1 \in L_{sq} \setminus \dot{L}^2$.

We pick up non-dyadic prime ideals $Q_1, \ldots, Q_m$ in K and $R_1, \ldots, R_m$ in L such that

$$\left(\frac{b_i}{Q_i}\right) = \left(\frac{tb_i}{R_i}\right) = -1\,, \quad \left(\frac{x}{Q_i}\right) = \left(\frac{tx}{R_i}\right) = 1$$

for each $x \in B \setminus \{b_i\}$, $i = 1, 2, \ldots, m$.

From [3, Lemma 2.6] it follows that the sets of primes $S = \Omega_0(K) \cup \{Q_1, \ldots, Q_m\}$ and $S' = \Omega_0(L) \cup \{R_1, \ldots, R_m\}$ are sufficiently large in K and L, respectively. Thus the groups $\dot{K}_{ev}/\dot{K}^2$ and $\dot{L}_{ev}/\dot{L}^2$ are subgroups of $U_K(S)/U_K(S)^2$ and $U_L(S')/U_L(S')^2$, respectively. We extend T to a map $T : S \to S'$ by putting $T(Q_i) = R_i$. Then our choice of Q_i, R_i implies that t induces a group isomorphism

$$t_P : K_{ev}\dot{K}_P/\dot{K}_P^2 \longrightarrow L_{ev}\dot{L}_{TP}/\dot{L}_{TP}^2$$

for each $P \in \{Q_1, \ldots, Q_m\}$.

From [3, Lemma 2.9] it follows that, for $P \in S$, the group isomorphism t_P can be extended to a group isomorphism $t_P : \dot{K}_P/\dot{K}_P^2 \longrightarrow \dot{L}_{TP}/\dot{L}_{TP}^2$ in a symbol preserving way. In this situation, the pair S, S' is called a *suitable pair* for K and L, according to [1].

Let τ_S be the product of isomorphisms t_P for $P \in S$. We have the following diagram

$$\begin{array}{ccccc} 1 & \longrightarrow & U_K(S)/U_K(S)^2 & \xrightarrow{i_S} & G(S) \\ & & & & \downarrow \tau_S \\ 1 & \longrightarrow & U_L(S')/U_L(S')^2 & \xrightarrow{i_{S'}} & G(S') \end{array}$$

According to [1] we put

$$H_S = \{\alpha \in U_K(S)/U_K(S)^2;\ \tau_s \circ i_s(\alpha) \in i_{S'}(U_L(S')/U_L(S')^2)\},$$

$$H_{S'} = i_{S'}^{-1} \circ \tau_S \circ i_S(H_S),$$

$$d_{SS'} = \dim_{\mathbf{F}_2} U_K(S)/U_K(S)^2/H_S.$$

We have $\tau_S \circ i_S(a) = i_{S'}(ta)$ for each $a \in \dot{K}_{ev}/\dot{K}^2$. Therefore the groups $\dot{K}_{ev}/\dot{K}^2$ and $\dot{L}_{ev}/\dot{L}^2$ are subgroups of H_S and $H_{S'}$, respectively. By the Obstruction-Killing Lemma (see [1]), there exists a suitable pair S_1, S_1' for K and L with $S \subseteq S_1$, $S' \subseteq S_1'$ and $d_{SS'} < d_{S_1 S_1'}$. An analysis of the proof of [1, Obstruction-Killing Lemma] shows that

$$\tau_{S_1} \circ i_{S_1}(a) = i_{S_1'}(ta)$$

for each $a \in \dot{K}_{ev}/\dot{K}^2$.
Indeed, in the proof $S_1 = S \cup \{P_1\}$ and $S_1' = S' \cup \{P_1'\}$ where P_1 and P_1' are suitably chosen primes in K and L, respectively. Moreover, it follows from the proof that each element of H_S is a local square at P_1 and each element of $H_{S'}$ is a local square at P_1'. Thus putting

$$G(S_1) = G(S) \times \dot{K}_{P_1}/\dot{K}_{P_1}^2\,, \quad G(S_1') = G(S') \times \dot{L}_{P_1'}/\dot{L}_{P_1'}^2$$

and

$$\tau_{S_1} = \tau_S \times t_{P_1},$$

we have

$$\tau_{S_1} \circ i_{S_1}(a) = \tau_{S_1}(i_S(a),\, 1) = (\tau_S \circ i_S(a),\, 1) = (i_{S'}(ta),\, 1) = i_{S_1'}(ta)$$

for all $a \in \dot{K}_{ev}/\dot{K}^2$.
Continuing the process (at most $d_{SS'}$ times) we obtain a suitable pair S_d, S_d' for K and L such that

$$H_{S_d} = U_K(S_d)/U_K(S_d)^2$$

and

$$\tau_{S_d} \circ i_{S_d}(a) = i_{S_d'}(ta)$$

for all $a \in \dot{K}_{ev}/\dot{K}^2$.
Now we put $\hat{t} = i_{S_d'}^{-1} \circ \tau_{S_d} \circ i_{S_d}$. Then we have the following commutative diagram

$$\begin{tikzcd} U_K(S_d)/U_K(S_d)^2 \arrow[r] \arrow[d, "\hat{t}"] & G(S_d) \arrow[d, "\tau_{S_d}"] \\ U_L(S'_d)/U_L(S'_d)^2 \arrow[r] & G(S'_d) \end{tikzcd}$$

and moreover $\hat{t}a = ta$ for every $a \in \dot{K}_{ev}/\dot{K}^2$.
In this situation we say that there is a small S_d-equivalence between K and L. From [6] it follows that the S_d-equivalence can be extended to a Hilbert-symbol equivalence of K and L which is tame outside S_d. The equivalence is even-order-preserving. This proves Theorem 2. □

4 Integral Witt equivalence of quadratic number fields

In this section we prove Theorem 3. As in the previous section we use Theorem 1 to replace integral Witt equivalence by even-order-preserving Hilbert-symbol equivalence. From [6] it follows that the field $\mathbb{Q}(\sqrt{-1})$ constitutes a singleton class of Hilbert-symbol equivalence. Thus in this section we assume that K and L are quadratic fields distinct from $\mathbb{Q}(\sqrt{-1})$.
The proof of Theorem 3 will be based on some properties of the following groups: $\dot{K}_{ev}/\dot{K}^2$, $K_{ev}/K_{ev} \cap K_+$ and $K_{ev} \cap K_+/\dot{K}^2$.
Assume that $K = \mathbb{Q}(\sqrt{d})$, where d is a square-free integer $\neq 1$. Let $\{p_1, \ldots, p_l\}$ be the pairwise distinct prime divisors of the discriminant of K; we agree that $p_1 = 2$, whenever $d \equiv 3 \pmod 4$. The order of the group $K_{ev} \cap K_+/\dot{K}^2$ is equal to 2^{c+l-1} and one of the sets

$$\{-1, p_1, \ldots, p_{l-1}\} \quad \text{if} \quad d < 0,$$

$$\{p_1, \ldots, p_{l-1}\} \quad \text{if} \quad d > 0,$$

forms a basis for $K_{ev} \cap K_+/\dot{K}^2$, (cf. [4]). From [3, Prop. 3.3] it follows that the 2-rank $\sigma(K)$ of the subgroup of the ideal class group of K generated by the classes of dyadic ideals is equal to 0 when 2 is prime in K or $2 \in |N(K)|$, and is equal to 1 otherwise.
The Gauss Genus Theory states that the 2-rank $\rho(K)$ of the ideal class group of K is equal to $l-1$ when K is non-real or $-1 \in N(K)$, and is equal to $l-2$ when K is real and $-1 \notin N(K)$.

Lemma 4.1. *Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field with $-1 \notin N(K)$, $\sigma(K) = 0$ and let P be arbitrarily chosen dyadic prime in K. Then $-1 \in (K_{ev} \cap K_+)\dot{K}_P^2/\dot{K}_P^2$ iff $-2 \notin N(K)$.*

PROOF: From $-1 \notin N(K)$ it follows that there is a prime divisor p of the discriminant of K congruent to 3 or 7 mod 8. If $p \equiv 7 \pmod 8$, then $-p$ is a local

square at P. If $p \equiv 3 \pmod 8$, then $2 \notin N(K)$. It follows that 2 is prime in K (i.e., $d \equiv 5 \pmod 8$)). Thus $-p$ is a square in the field $K_P = \mathbb{Q}_2(\sqrt{d})$.
Now assume that $-2 \in N(K)$. Then every prime divisor of d is congruent to 1, 2 or 3 mod 8. Therefore $d \equiv 1, 2, 3, 6 \pmod 8$. Moreover, $a \equiv 1, 2, 3, 6 \pmod 8$ and $da \equiv 1, 2, 3, 6 \pmod 8$ for each $a \in K_{ev} \cap K_+$. This proves that $-a \notin \dot{K}_P^2$ for each element a of $K_{ev} \cap K_+$. □

If K is non-real, then $K_{ev} = K_{ev} \cap K_+$. If K is real, then the group $K_{ev}/K_{ev} \cap K_+$ is 2-element with basis $\{-1\}$, or is 4-element with basis $\{-1, a\}$ depending on whether $-1 \notin N(K)$ or $-1 \in N(K)$, where a is an element of K with negative norm.

PROOF OF THEOREM 3: Assume that (t, T) is an EOP-Hilbert-symbol equivalence between K and L. The conditions (0) – (III) are consequences of Hilbert-symbol equivalence of K and L (cf. [6]).
The condition (IV) follows from Prop. 3.1.
The map t induces a group isomorphism $K_{ev}/K_{ev} \cap K_+ \cong L_{ev}/L_{ev} \cap L_+$ hence (V) holds.
Corollary 3.1 and Gauss Genus Theory imply the condition (IV).
The condition (VI) follows from Cor. 3.1.
From Theorem 2 and Prop. 3.1 it follows that the map t induces a group isomorphism

$$(K_{ev} \cap K_+)\dot{K}_P^2/\dot{K}_P^2 \cong (L_{ev} \cap L_+)\dot{L}_{TP}^2/\dot{L}_{TP}^2$$

for every dyadic prime P. Since TP is dyadic, (VII) follows from Lemma 4.1.
Now we prove (VIII). First we show that the Hilbert symbols in question do not depend on the choice of elements a and a' and on the choice of dyadic primes P, Q. Let a be an element of K with negative norm. Then $N(a) \in -\dot{\mathbb{Q}}^2$ and

$$(2,\, a)_P = (2,\, \bar{a})_{\bar{P}} = (2,\, -a)_{\bar{P}} = (2,\, a)_{\bar{P}}$$

(here $\bar{P}$ is the conjugate ideal of P and $\bar{a}$ is the conjugate element of a). The assumptions in (VIII) imply that every prime factor p of the discriminant of K is congruent to 1 mod 8. Hence $K_{ev} \cap K_+ = K_{sq}$. If a_1 is any element of K_{ev} with negative norm, then $\pm a_1 a \in K_{ev} \cap K_+$. Thus $a_1 = \pm a$ in $\dot{K}_P/\dot{K}_P^2$. This implies the equality of the Hilbert symbols

$$(2,\, a_1)_P = (2,\, \pm a)_P = (2,\, a)_P.$$

To prove (VIII) we can assume that $TP = Q$ since, as we have already shown, the Hilbert symbols in question do not depend on the choice of dyadic primes. Let a be an element of K_{ev} with negative norm. The Prop. 3.1 implies that the element ta of L_{ev} has negative norm. The above yields that without loss of generality we can assume $a' = ta$. Thus we get

$$(2,\, a)_P = (2,\, ta)_{TP} = (2,\, a')_Q$$

Now we prove the sufficiency of (0) - (VIII) íbr K and L to be EOP equivalent. Thus, we assume that A' and L satisfy (0) - (VIII), and we construct two maps T and t satisfying the hypothesis of Theorem 2.

If — 1 *(£ N(K)* we define T to be an arbitrary bijection that sends infinite reál primes and dyadic primes of K onto infinite reál primes and dyadic primes of L. respectively.

Now assume that —1 £ *N(K).* First we choose elements a and a' of K_{ev} and L_{ev}, resp., with negative norms. We write $P_{OQl)}$ Poo_2 $^{an<}$^ Qoo_{15} Qoo_2 ^{Ior} the two infinite reál primes of A and L, respectively. We can assume that a is positive at P_{n01} and negative at POQ_2 and sirnilarly that a' is positive at Q_{OQl} and negative at Qoo_2- We put rPoo, = Qoo_x and 7\Poo$_2$ = Qoo_2>

H g(K) — i and P, Q are the unique dyadic primes in /l and L, respectively, then we put *TP — Q.*

Let ^(/í) = 2 and let P, $P^/$ and Q, Q' be distinct dyadic primes of K and L, respectively. By Hilbert reciprocity (—1, a)p/ = —(—1, *a)p* and (— 1, a^r)g' = -(— 1, *(I')Q.* We can assume (— 1, *a)p* — (—1, a^g = 1, Then we put *TP — Q* and *TP' — Q'.* The elements a and a' chosen above will be uśed in the construction *oit.*

The isomorphism t will be defined on a suitably chosen basis of the group K_{ev} / K^1. We construct this basis in the samé way as the basis in the proof of [3, Thm 1]. We use the isomorphism

$$K_{ev}/K^2 \;=\; K_{ev}/K_{ev} \;\; \mathrm{O} \;\; K+ \;\; 0 \;\; K_{ev} \;\; \mathrm{n} \;\; K+/K_{sq} \;\; 0 \;\; K_{sq}/I<^2\text{-}$$

The conditions (I) - (VII) irnply that the orders of the direct surnmands are equal to the orders of the corresponding direct surnmands in the decomposition

$$L_{ev}/L^2 \;\; \wedge \;\; Lev\, I\, Lev \;\; \mathrm{H} \;\; L_+ \;\; 0 \;\; L_{ev} \;\; \mathrm{n} \;\; L+/L_{8q} \;\; 0 \;\; L_{sq}/L^2.$$

First we define t on K_{sq}/K^2. Let $\{6i,\dots,6_m\}$ and $\{6i,\dots,6\wedge)$ be bases for K_{sq}/K^2 and $L_{sq}/L^2{}_y$ where &i = 6^ = — 1, whenever —1 E $Á'_{5g}$. Then we put í6j = 6J- for ? — $1,2,\dots,m$.

The group K_{ev}/K_{ev} D A+ is non-trivial only when /i is reál and has basis {— 1} when -1 £ A^(A^r), and {-l,a} when -1 e A^r(A'). We put /(-l) = -1 and *ta — a".*

Now we choose a basis P^ of $/i_{eí}$, O $K+/K_{sq}$. We consider two cases depending on the number of dyadic primes.

Part I. *g(K)* — 1. The group $Á'_{et;}$ fi $K+/K_{sq}$ is canonically isornorphic to (A'_{ev} O K_+*)kl/ki.*

1.1. If A is non-real, the group $A'_{eí}$, O $K+/K_{sq}$ has a basis {v} or {v, ?i} depending on whether *a(K)* is equal 0 or l. In both cases we can assume that v — -T, whenever —1 is not locally a square at P.

1.2. When -1 £ *N(K),* the group K_{ev} D $K+/K_{sq}$ is nontrivial only if cr(A^r) = 1 and it has order 2. Let {u} be a basis of K_{ev} $C\backslash$ $K+/K_{sq}$ in the nontrivial čase. The Hilbert reciprocity implies that (—1, *á)p* — (—1, *—a)p* — —1, thus { —l,a}

are independent in $\dot{K}_P/\dot{K}_P^2$. Moreover $(-1, u)_P = (a, u)_P = 1$, hence -1, a, u are independent in $\dot{K}_P/\dot{K}_P^2$, if $\sigma(K) = 1$.
I.3. Now assume that K is real and $-1 \notin N(K)$. The group $K_{ev} \cap K_+/K_{sq}$ has a basis $\{v\}$ if $\sigma(K) = 0$, and $\{v, u\}$ if $\sigma(K) = 1$. If $\sigma(K) = 1$, then the subspace of the dyadic unit square class group U_P/U_P^2 (with the Hilbert symbol as inner product) generated by -1, u, v is totally isotropic, hence -1, u, v are dependent in $\dot{K}_P/\dot{K}_P^2$. Thus we can assume that $v \in -\dot{K}_P^2$ whenever -1 is not a square at P. When $\sigma(K) = 0$, the Lemma 4.1 guarantees that we can assume $v \in -\dot{K}_P^2$ when $-2 \notin N(K)$ and $-1 \notin \dot{K}_P^2$, and $v \notin -\dot{K}_P^2$ in the remaining cases.
Part II. $g(K) = 2$. In this case $\sigma(K) = 0$ iff $2 \in |N(K)|$.
II.1. Assume that K is non-real. When $2 \notin N(K)$, there is a prime divisor p of the discriminant of K congruent to 3 or 5 mod 8.
Take $p_1 = \pm p \equiv 5 \pmod 8$. Thus $K_{ev} \cap K_+/K_{sq}$ has the basis $\{-1\}$ or $\{-1, p_1\}$ depending on whether $2 \in N(K)$ or $2 \notin N(K)$, respectively.
II.2. Assume that K is real and $-1 \notin N(K)$. Then there exists a prime divisor p of the discriminant of K congruent to 3 or 7 mod 8. When $2 \notin |N(K)|$ there exists a divisor q of the discriminant of K congruent to 5 mod 8. We choose $p_1 = p$ or pq, whichever satisfies $p_1 \equiv 7 \pmod 8$. Then $\{p_1, q\}$ is a basis of the group $K_{ev} \cap K_+/K_{sq}$. When $2 \in N(K)$ or $-2 \in N(K)$ we find a basis $\{p_2\}$ of $K_{ev} \cap K_+/K_{sq}$, where p_2 is congruent to 7 mod 8 when $2 \in N(K)$ and p_2 is congruent to 3 mod 8 when $-2 \in N(K)$.
II.3. Now assume that $-1 \in N(K)$. The group $K_{ev} \cap K_+/K_{sq}$ is nontrivial when $2 \notin N(K)$. In this case we choose a basis $\{p\}$ of $K_{ev} \cap K_+/K_{sq}$, where $p \equiv 5 \pmod 8$. The equality $(-1, a)_P = 1$ implies that a is equal to 1 or 5 in the group $\dot{K}_P/\dot{K}_P^2$. In the case when $2 \notin N(K)$, by replacing a with pa, if necessary, we get $a = 1$ in $\dot{K}_P/\dot{K}_P^2$ (then $a = -1$ in $\dot{K}_{P'}/\dot{K}_{P'}^2$). In case $2 \in N(K)$ we have a equal to 1 or 5 in $\dot{K}_P/\dot{K}_P^2$ depending on whether the Hilbert symbol $(2, a)_P$ is equal to 1 or -1, respectively.
Analogously we construct a basis B_L of the group $L_{ev} \cap L_+/L_{sq}$ and we define the mapping t by assigning elements of B_K to corresponding elements of B_L. This definition guarantees that t induces the group isomorphism

$$K_{ev}\dot{K}_P/\dot{K}_P^2 \longrightarrow L_{ev}\dot{L}_{TP}/\dot{L}_{TP}^2,$$

for every dyadic prime P. Moreover, in the case $g(K) = 2$, it follows immediately from the construction that t preserves the Hilbert symbols for dyadic primes. And in the case $g(K) = 1$, it follows from the construction that t preserves the Hilbert symbols for all infinite primes and all non-dyadic primes. The Hilbert symbols for dyadic primes are equal by Hilbert reciprocity (cf. [3]). □

References

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

[2] Conner, P. E., Perlis, R., Szymiczek, K., *Wild sets and 2-ranks of class groups*, Acta Arith., (to appear).

[3] Czogała, A., *On reciprocity equivalence of quadratic number fields*, Acta arith. **58** (1991), 365–387.

[4] Milnor, J., Husemoller, D., *Symmetric Billinear Forms*, Springer Verlag, Berlin, 1973.

[5] Münstermann, R., *Der Wittring des Ring der ganzen Zahlen eines Quadratischen Zahlkörpers*, Diplomarbeit, Bielefeld, 1983.

[6] Perlis, R., Szymiczek, K., Conner, P., Litherland, R., *Matching Witts with global fields*, Contemp. Math. **155** (1994), 365–387.

[7] Shastri, P., *Witt groups of algebraic integers*, J. of Number Theory **30** (1988), 243–266.

[8] Szymiczek, K., *Matching Witts locally and globally*, Math. Slovaca **41** (1991), 315–330.

[9] Szymiczek, K., *Hilbert-symbol equivalence of number fields*, Tatra Mount. Math. Publ., 11 (to appear).

Address: Instytut Matematyki, Uniwersytet Śląski, 40 007 Katowice, Poland

Talk at the First Czech–Polish Conference on Number Theory, University of Ostrava, Ostrava, Czech Republic, May 30, 1996.
Supported by the State Committee for Scientific Research (KBN) of Poland under Grant 2 1063 91 01.