ACTA ARITHMETICA
163.1 (2014)

Automorphisms of Witt rings of global fields

by

ALFRED CZOGAŁA and MIECZYSŁAW KULA (Katowice)

1. Introduction. The Witt ring is an algebraic structure introduced in [12] that carries information about the behaviour of all quadratic forms over a fixed field. This paper investigates automorphisms of Witt rings of global fields. We restrict our attention to global fields of characteristic different from 2. Therefore, the term *global field* will henceforth exclude fields of characteristic 2.

Intensive investigation of Witt rings of global fields began in the early 1980s. Descriptions of Witt rings of global fields in terms of fundamental invariants (Witt index, discriminant, Hasse–Witt invariants) were given in [3] and [2].

Two fields are said to be *Witt equivalent* if their Witt rings are isomorphic. In [8], [1] and [11] the problem of Witt equivalence of global fields was completely solved. It was shown that the crucial notion for solving the problem is *reciprocity equivalence*, which is now called Hilbert-symbol equivalence.

By a *Hilbert-symbol equivalence* of global fields K and L we mean a pair (T, t), where

$$T\colon \Omega(K) \to \Omega(L)$$

is a bijection between the sets of primes of these fields and

$$t\colon \dot{K}/\dot{K}^2 \to \dot{L}/\dot{L}^2$$

is an isomorphism of their square class groups which preserves Hilbert symbols with respect to the corresponding primes, i.e.

$$(a,b)_{\mathfrak{p}} = (ta,tb)_{T\mathfrak{p}} \quad \text{for all } a,b \in \dot{K}/\dot{K}^2,\ \mathfrak{p} \in \Omega(K).$$

When $K = L$, Hilbert-symbol equivalence is also called *Hilbert-symbol self-equivalence* of K.

In [8] the authors showed that two global fields have isomorphic Witt rings (they are *Witt equivalent*) if and only if they are *Hilbert-symbol equiv-*

2010 *Mathematics Subject Classification*: Primary 11E81; Secondary 19F15.
Key words and phrases: Witt ring, global field, Hilbert-symbol equivalence.

DOI: 10.4064/aa163-1-1

alent (there exists a Hilbert-symbol equivalence between them). One can observe that some isomorphisms of Witt rings preserve the dimensions of nonisotropic forms representing Witt classes of the ring. Such isomorphisms are called *strong isomorphisms* of Witt rings. It can be shown that an isomorphism $\varphi\colon WK \to WL$ of the Witt rings of the fields K and L is strong if and only if it preserves one-dimensional quadratic forms (i.e. $\varphi(\langle a\rangle) = \langle b\rangle$).

It is easy to show that if (T, t) is a Hilbert-symbol equivalence of global fields K and L, then the map $\langle a_1, \ldots, a_n\rangle \mapsto \langle ta_1, \ldots, ta_n\rangle$ induces a strong isomorphism of the Witt rings of K and L.

Conversely, it was shown in [8] that every strong isomorphism of the Witt rings of global fields K and L determines a Hilbert-symbol equivalence (T, t), where the isomorphism t is uniquely determined and the bijection T is uniquely determined on the set of non-complex primes.

In this way the problem of Witt equivalence of global fields was reduced to the existence of a Hilbert-symbol equivalence of these fields. Similarly the construction of a strong isomorphism of Witt rings can be reduced to the construction of a Hilbert-symbol equivalence.

In [1] a finite set of conditions was given ensuring the existence of Hilbert-symbol equivalence of two global fields. By applying that result, a complete set of invariants for Hilbert-symbol equivalence (and equivalently for Witt equivalence) of global fields was found in [11].

The techniques developed for the classification of Witt rings of global fields can be applied to study the structure of the Witt rings themselves. In this paper we shall deal with the automorphism group of the Witt ring of a global field which provides us with information on the inner symmetry of the ring. This idea was proposed by D. Leep and M. Marshall [5] for abstract Witt rings.

The main result of this paper is that the group of strong automorphisms of the Witt ring of a global field is uncountable (cf. Theorem 3.2). This can be considered as a first step in the study of automorphisms of Witt rings of global fields. The special case of the field of rational numbers was proved in [10].

The main result is proved by finding a set of Hilbert-symbol self-equivalences of a global field which is equinumerous to the set of all infinite 0-1 sequences, so the automorphism groups of Witt rings of global fields are uncountable. The result seems to be somewhat surprising as the automorphism groups of global fields are countable.

In the construction we shall use methods developed in [8] and [1]. In Section 2 we adapt these methods to the situation considered here. In general, we follow the standard terminology and notation of [9] but we shall slightly simplify them. Throughout the paper, $\Omega(K)$ denotes the set of all primes (archimedean or not) of a global field K. For every finite subset S in $\Omega(K)$ containing all infinite (archimedean) primes the set

$$\mathcal{O}_K(S) = \{x \in K : \mathrm{ord}_{\mathfrak{p}}\, x \geq 0 \text{ for all } \mathfrak{p} \text{ outside } S\}$$

is called the *ring of S-integers* of K. The ideal class group and the class number of $\mathcal{O}_K(S)$ will be denoted by $C_K(S)$ and $h_K(S)$, respectively. The 2-*rank* of an abelian group G is $\dim_{\mathbb{F}_2} G/G^2$. Where it is not misleading, the global square class $a\dot{K}^2$ (and also the local square class $a\dot{K}_{\mathfrak{p}}^2$) will be denoted simply as a.

2. Preliminary results. From now on, K denotes a global field. A finite nonempty set S of primes of the field K will be called a *Hasse set* if it contains all dyadic and all infinite primes of K. Moreover, if the class number $h_K(S)$ is odd, then S is called a *sufficiently large* Hasse set.

Observe that if $S \subset S'$ are Hasse sets of K, then there is a natural epimorphism $C_K(S) \to C_K(S')$. Hence if S is sufficiently large, then so is S'.

Remark 2.1. It is easy to extend an arbitrary Hasse set S to be sufficiently large. Indeed, it suffices to take a set of ideals of $\mathcal{O}_K(S)$ which are representatives of ideal classes that generate the Sylow 2-subgroups of $C_K(S)$ and add these additional primes to S. The resulting set and each of its supersets is a sufficiently large Hasse set of primes of K.

Assume that S is a Hasse set of primes of K. We denote

$$E_K(S) = \{a \in \dot{K} : \mathrm{ord}_{\mathfrak{p}}\, a \equiv 0 \pmod 2 \text{ for all } \mathfrak{p} \in \Omega(K) \setminus S\}.$$

It is easy to check that $E_K(S)$ is a subgroup of the multiplicative group $\dot{K}$ and $\dot{K}^2 \subseteq E_K(S)$. Elements of $\dot{K}$ that belong to $E_K(S)$ are said to be *S-singular*. By [9, Corollary 5] it follows that

$$\mathrm{rk}_2\, E_K(S)/\dot{K}^2 = \#S + \mathrm{rk}_2\, C_K(S). \tag{2.1}$$

In particular, if S is sufficiently large, then $\mathrm{rk}_2\, E_K(S)/\dot{K}^2 = \#S$, as $\mathrm{rk}_2\, C_K(S) = 0$.

If S is a Hasse set of primes of K, then we denote by $G_K(S)$ the product of the local square class groups of $\dot{K}_{\mathfrak{p}}/\dot{K}_{\mathfrak{p}}^2$, for all $\mathfrak{p} \in S$, that is,

$$G_K(S) = \prod_{\mathfrak{p} \in S} \dot{K}_{\mathfrak{p}}/\dot{K}_{\mathfrak{p}}^2.$$

There is a natural homomorphism

$$\mathrm{diag}_S \colon \dot{K}/\dot{K}^2 \to G_K(S).$$

Its restriction induces a homomorphism $i_S \colon E_K(S)/\dot{K}^2 \to G_K(S)$. We write $\bar{x} = \mathrm{diag}_S(x\dot{K}^2)$. Note that $(G_K(S), \beta_S)$ is a nondegenerate inner product space over the field $\mathbb{F}_2$, where

$$\beta_S(\bar{x},\bar{y}) = \prod_{\mathfrak{p}\in S}(x,y)_{\mathfrak{p}}.$$

By [8, Lemma 5] and [1, Metabolizer Lemma] we obtain

PROPOSITION 2.2. *If S is a sufficiently large Hasse set of primes of K, then:*

(i) *The homomorphism $i_S\colon E_K(S)/\dot{K}^2 \to G_K(S)$ is injective.*
(ii) *The subspace $i_S(E_K(S)/\dot{K}^2)$ is self-dual (a metabolizer) in the inner product space $(G_K(S),\beta_S)$.*

The next lemma enables representing an arbitrary element of $G_K(S)$ as a value of diag_S restricted to the set of S_1-singular elements where S_1 is obtained by adding a suitable prime to S.

LEMMA 2.3. *Let S be a Hasse set of primes of K and let $(\alpha_{\mathfrak{p}}\dot{K}_{\mathfrak{p}}^2)_{\mathfrak{p}\in S} \in G_K(S)$. Then there exist $\mathfrak{q}\in\Omega(K)\setminus S$ and $q\in\dot{K}$ such that*

- $q\dot{K}_{\mathfrak{p}}^2 = \alpha_{\mathfrak{p}}\dot{K}_{\mathfrak{p}}^2$ *for all* $\mathfrak{p}\in S$,
- $\mathrm{ord}_{\mathfrak{q}}\, q = 1$,
- $\mathrm{ord}_{\mathfrak{p}}\, q \equiv 0 \pmod 2$ *for every* $\mathfrak{p}\in\Omega(K)\setminus(S\cup\{\mathfrak{q}\})$.

Proof. The lemma follows from [6, Lemma 2.1] immediately. ∎

COROLLARY 2.4. *Let S be a Hasse set of primes of K and $\alpha\in G_K(S)$. Then there exist $\mathfrak{q}\in\Omega(K)\setminus S$ and $q\in\dot{K}$ such that*

- $\mathrm{diag}_S(q\dot{K}^2) = \alpha$,
- $\mathrm{ord}_{\mathfrak{q}}\, q = 1$,
- $q\in E_K(S\cup\{\mathfrak{q}\})$.

LEMMA 2.5. *Let S be a sufficiently large Hasse set of primes of K and $\mathfrak{q}\in\Omega(K)\setminus S$. Moreover let $S_1 = S\cup\{\mathfrak{q}\}$. Then there exists $x\in E_K(S_1)$ such that $x\notin\dot{K}_{\mathfrak{q}}^2$.*

Proof. Assume that $E_K(S_1)\subseteq\dot{K}_{\mathfrak{q}}^2$. Then for all $x\in E_K(S_1)$ and all $\mathfrak{p}\in\Omega(K)\setminus\{S\}$ the number $\mathrm{ord}_{\mathfrak{p}}\, x$ is even, which implies $E_K(S_1)\subseteq E_K(S)$. We get a contradiction since by (2.1),

$$\mathrm{rk}_2\, E_K(S_1)/\dot{K}^2 = \#S+1 > \#S = \mathrm{rk}_2\, E_K(S)/\dot{K}^2. \ ∎$$

The construction of Hilbert-symbol self-equivalences to be presented in Section 3 is performed by defining bijections T_S on increasingly growing sequences of finite sets of primes S accompanied with determining isomorphisms t_S on increasingly larger groups $E_K(S)/\dot{K}^2$. The description of this procedure uses the notion of correspondence and small equivalence introduced in [1] and [8], which we shall adapt to our situation.

Let S be a Hasse set of primes of K. Let us consider an injection $T_S\colon S \to TS \subseteq \Omega(K)$ and a family of isomorphisms

$$t_{\mathfrak{p}}\colon \dot{K}_{\mathfrak{p}}/\dot{K}_{\mathfrak{p}}^2 \to \dot{K}_{T_S\mathfrak{p}}/\dot{K}_{T_S\mathfrak{p}}^2, \qquad \mathfrak{p} \in S,$$

which preserve Hilbert symbols, i.e.

$$(a,b)_{\mathfrak{p}} = (t_{\mathfrak{p}}a, t_{\mathfrak{p}}b)_{T_S\mathfrak{p}}, \qquad a,b \in \dot{K}_{\mathfrak{p}}/\dot{K}_{\mathfrak{p}}^2,\ \mathfrak{p} \in S.$$

It is easy to observe (cf. [8]) that

- if $\mathfrak{p}$ is a dyadic prime, then so is $T_S\mathfrak{p}$,
- if $\mathfrak{p}$ is a real prime, then so is $T_S\mathfrak{p}$,
- if $\mathfrak{p}$ is a complex prime, then so is $T_S\mathfrak{p}$,
- $t_{\mathfrak{p}}(-1\dot{K}_{\mathfrak{p}}^2) = -1\dot{K}_{T_S\mathfrak{p}}^2$.

If both S and $T_S S$ are sufficiently large, then the pair $\mathcal{R} = (T_S, \tau_S)$, where $\tau_S = \prod_{\mathfrak{p}\in S} t_{\mathfrak{p}}$, will be referred to as a *correspondence over* S (in [9], $\mathcal{R}$ is called a *suitable correspondence*).

Remark 2.6. Let $\mathfrak{p}, \mathfrak{q}$ be finite and nondyadic primes of K. The local square class groups $\dot{K}_{\mathfrak{p}}/\dot{K}_{\mathfrak{p}}^2$ and $\dot{K}_{\mathfrak{q}}/\dot{K}_{\mathfrak{q}}^2$ have four elements each. One can show that every bijection $t\colon \dot{K}_{\mathfrak{p}}/\dot{K}_{\mathfrak{p}}^2 \to \dot{K}_{\mathfrak{q}}/\dot{K}_{\mathfrak{q}}^2$ such that $t(\dot{K}_{\mathfrak{q}}^2) = \dot{K}_{\mathfrak{q}}^2$ and $t(-1\dot{K}_{\mathfrak{p}}^2) = -1\dot{K}_{\mathfrak{q}}^2$ is an isomorphism which preserves Hilbert symbols. The proof is easy but slightly tedious. If -1 is a square in $K_{\mathfrak{p}}$, then the mapping t satisfies only one restriction $t(\dot{K}_{\mathfrak{q}}^2) = \dot{K}_{\mathfrak{q}}^2$, so every permutation of the set of all three square classes different from 1 determines a local isomorphism, thus we get six possibilities for t. When -1 is not a square in $K_{\mathfrak{p}}$, there are two possible local isomorphisms.

From now on, only sufficiently large Hasse sets will be considered, so we will omit the term "sufficiently large" most of the time when dealing with Hasse sets. To simplify notation, we shall often write T instead of T_S if it does not cause misunderstanding.

Notice also that every correspondence over S determines the diagram

$$\begin{array}{ccccc} 1 & \longrightarrow & E_K(S)/\dot{K}^2 & \xrightarrow{i_S} & G_K(S) \\ & & & & \Big\downarrow{\scriptstyle \tau_S} \\ 1 & \longrightarrow & E_K(TS)/\dot{K}^2 & \xrightarrow{i_{TS}} & G_K(TS) \end{array} \tag{2.2}$$

and the subgroups

$$H_S(\tau_S) = \{a \in E_K(S)/\dot{K}^2 : \tau_S \circ i_S(a) \in i_{TS}(E_K(TS)/\dot{K}^2)\},$$

$$H_{TS}(\tau_S) = \{b \in E_K(TS)/\dot{K}^2 : \tau_S^{-1} \circ i_{TS}(b) \in i_S(E_K(S)/\dot{K}^2)\}.$$

By standard group theory, there exists a unique global isomorphism $t_S : H_S(\tau_S) \to H_{TS}(\tau_S)$ such that the following diagram commutes:

$$\begin{array}{ccccc} 1 & \longrightarrow & H_S(\tau_S) & \xrightarrow{i_S} & G_K(S) \\ & & \big\downarrow{\scriptstyle t_S} & & \big\downarrow{\scriptstyle \tau_S} \\ 1 & \longrightarrow & H_{TS}(\tau_S) & \xrightarrow{i_{TS}} & G_K(TS) \end{array} \tag{2.3}$$

The isomorphism t_S preserves Hilbert symbols with respect to primes in S, i.e.

$$(x,\, y)_{\mathfrak{p}} = (t_S x, t_S y)_{T\mathfrak{p}} \quad \text{for all } x, y \in H_S(\tau_S) \text{ and } \mathfrak{p} \in S.$$

Let S and S' be Hasse sets of primes, and $\mathcal{R}_S = (T, \tau_S)$ and $\mathcal{R}_{S'} = (T', \tau'_{S'})$ be correspondences over S and S', respectively with $\tau_S = \prod_{\mathfrak{p}\in S} t_{\mathfrak{p}}$ and $\tau'_S = \prod_{\mathfrak{p}\in S'} t'_{\mathfrak{p}}$. We say that $\mathcal{R}_{S'}$ is an *extension* of $\mathcal{R}_S$ if

- $S \subseteq S'$,
- T' is an extension of T,
- $t_{\mathfrak{p}} = t'_{\mathfrak{p}}$ for each $\mathfrak{p} \in S$,
- $H_S(\tau_S) \subseteq H_{S'}(\tau_{S'})$ (i.e. $t_{S'}$ is an extension of t_S).

In what follows we shall often denote both T' and T by T.

If $H_S(\tau_S) = E_K(S)/\dot{K}^2$, then the correspondence will be called a *small equivalence over* S. Obviously, in this case t_S is defined on $E_K(S)/\dot{K}^2$ and the following diagram commutes:

$$\begin{array}{ccccc} 1 & \longrightarrow & E_K(S)/\dot{K}^2 & \xrightarrow{i_S} & G_K(S) \\ & & \big\downarrow{\scriptstyle t_S} & & \big\downarrow{\scriptstyle \tau_S} \\ 1 & \longrightarrow & E_K(TS)/\dot{K}^2 & \xrightarrow{i_{TS}} & G_K(TS) \end{array}$$

Now we shall prove a modification of [1, Obstruction Killing Lemma] (cf. also [9, p. 174]).

Theorem 2.7. *Every correspondence over a Hasse set S can be extended to a small equivalence over a set $\hat{S}$ with $S \subseteq \hat{S}$.*

Proof. Let $\mathcal{R}_S = (T, \tau_S)$ be a fixed correspondence over S and let $t_S : H_S(\tau_S) \to H_{TS}(\tau_S)$ be the global isomorphism determined by $\mathcal{R}_S$ (cf. (2.3)). Assume that $H_S(\tau_S) \subsetneq E_K(S)/\dot{K}^2$. Let x be an S-singular element of K such that $\tau_S\bar{x} \notin i_{S'}(E_K(S')/\dot{K}^2)$. It follows from Proposition 2.2 that there exists an S'-singular $y \in \dot{K}$ such that $\beta_{S'}(\tau_S\bar{x}, \bar{y}) = -1$. For every $z \in E_S(K)$ we have $\beta_{S'}(\tau_S\bar{x}, \tau_S\bar{z}) = \beta_S(\bar{x}, \bar{z}) = 1$, so $\bar{y} \notin H_{S'}(\tau_{S'})$. Consequently,

$$\beta_S(\tau_S^{-1}\bar{y}, \bar{x}) = \beta_{S'}(\bar{y}, \tau_S\bar{x}) = -1, \tag{2.4}$$

so $\tau_S^{-1}\bar{y} \notin i_S(E_K(S)/\dot{K}^2)$.

From Corollary 2.4 it follows that there exist $\mathfrak{q} \in \Omega(K) \setminus S$ and $q \in \dot{K}$ such that

- $\bar{q} = \tau_S^{-1}\bar{y}$,
- $\operatorname{ord}_{\mathfrak{q}} q = 1$,
- $q \in E_K(S_1)$, where $S_1 = S \cup \{\mathfrak{q}\}$.

Similarly, there are $\mathfrak{q}' \in \Omega(K) \setminus S'$ and $q' \in \dot{K}$ such that

- $\bar{q'} = \tau_S \bar{x}$,
- $\operatorname{ord}_{\mathfrak{q}'} q' = 1$,
- $q' \in E_K(S_1')$, where $S_1' = S' \cup \{\mathfrak{q}'\}$.

First observe that if $z\dot{K}^2 \in H_S(\tau_S)$, then $z = 1 \bmod \dot{K}_{\mathfrak{q}}^2$. Indeed, since z and q are S_1-singular, Proposition 2.2 shows that $\beta_{S_1}(\bar{z}, \bar{q}) = 1$, and this yields

$$(z, q)_{\mathfrak{q}} = \beta_S(\bar{z}, \bar{q}) = \beta_S(\bar{z}, \tau_S^{-1}\bar{y}) = \beta_{S'}(\tau_S\bar{z}, \bar{y}) = 1.$$

The final equality follows from $\tau_S\bar{z}, \bar{y} \in i_{S'}(E_K(S')/\dot{K}^2)$. Since z is a $\mathfrak{q}$-adic unit modulo $\dot{K}_{\mathfrak{q}}^2$, from (2.2) and $(z, q)_{\mathfrak{q}} = 1$ we get $z \in \dot{K}_{\mathfrak{q}}^2$.

Analogously, considering any S'-singular element z' such that $z'\dot{K}^2$ is in $H_{S'}(\tau_{S'})$ and applying

$$(z', q')_{\mathfrak{q}'} = \beta_{S'}(\bar{z'}, \tau_S\bar{x}) = \beta_S(\tau_S^{-1}\bar{z'}, \bar{x}) = 1$$

we conclude that $z' = 1 \bmod \dot{K}_{\mathfrak{q}'}^2$.

Since $-1 \in H_S(\tau_S)$ and $-1 \in H_{S'}(\tau_{S'})$, it follows in particular that $-1 \in \dot{K}_{\mathfrak{q}}^2$ and $-1 \in \dot{K}_{\mathfrak{q}'}^2$.

Now we shall extend $\mathcal{R}_S$ to a correspondence over S_1.

For this purpose we extend the bijection T onto S_1 by setting $T\mathfrak{q} = \mathfrak{q}'$. It remains to define a local isomorphism $t_{\mathfrak{q}} : \dot{K}_{\mathfrak{q}}/\dot{K}_{\mathfrak{q}}^2 \to \dot{K}_{\mathfrak{q}'}/\dot{K}_{\mathfrak{q}'}^2$. Consider a $\mathfrak{q}$-adic unit u and a $\mathfrak{q}'$-adic unit u' which are not local squares. According to Remark 2.6, the mapping defined by $t_{\mathfrak{q}}1 = 1$, $t_{\mathfrak{q}}u = q'$, $t_{\mathfrak{q}}q = u'$ and $t_{\mathfrak{q}}uq = u'q'$ is the required isomorphism.

Thus the correspondence $\mathcal{R}_{S_1} = (T, \tau_{S_1})$ is constructed. To prove that $\mathcal{R}_{S_1}$ extends $\mathcal{R}_S$ it suffices to show that $H_S(\tau_S) \subset H_{S_1}(\tau_{S_1})$. For this purpose, assume $z\dot{K}^2 \in H_S(\tau_S)$ and let $t_S z = z'$, i.e. $\tau_S\bar{z} = \bar{z'}$. Then $z'\dot{K}^2 \in H_{S'}(\tau_{S'})$. Since $z = 1$ in $\dot{K}_{\mathfrak{q}}^2$ and $z' = 1$ in $\dot{K}_{\mathfrak{q}'}^2$, it follows that $t_{\mathfrak{q}}z = z'$, and consequently $\tau_{S_1}\bar{z} = \bar{z'}$ in $G_{S_1'}(K)$. As a result we have $z\dot{K}^2 \in H_{S_1}(\tau_{S_1})$.

Now we shall show that the square classes of x and q belong to $H_{S_1}(\tau_{S_1})$. Recall that x and q are S_1-singular, so by Proposition 2.2 we get $\beta_{S_1}(\bar{x}, \bar{q}) = 1$. By (2.4) we have

$$(x, q)_{\mathfrak{q}} = \beta_S(\bar{x}, \bar{q}) = \beta_S(\bar{x}, \tau_S^{-1}\bar{y}) = \beta_{S'}(\tau_S\bar{x}, \bar{y}) = -1,$$

so $x = u \bmod \dot{K}_{\mathfrak{q}}^2$. In this case $t_{\mathfrak{q}}x = q'$. As $\tau_S\bar{x} = \bar{q'}$, we see that $\tau_{S_1}\bar{x} = \bar{q'}$ in $G(S_1')$. Consequently, since $q'\dot{K}^2 \in E_K(S_1')/\dot{K}^2$, it follows that $x\dot{K}^2$ is in $H_{S_1}(\tau_{S_1})$.

Similarly q' and y are S_1'-singular, so by (2.4) we have

$$(y, q')_{\mathfrak{q}'} = \beta_{S'}(\bar{y}, \bar{q'}) = \beta_{S'}(\bar{y}, \tau_S \bar{x}) = \beta_{S'}(\tau_S \bar{x}, \bar{y}) = -1.$$

As a result, $y = u'$ in $\dot{K}_{\mathfrak{q}'}^2$ and this implies $q = t_{\mathfrak{q}}^{-1} y$. However $\bar{q} = \tau_S^{-1} \bar{y}$, so $\bar{q} = \tau_{S_1}^{-1} \bar{y}$ in $G_{S_1}(K)$. As y is S-singular, it is also S_1-singular, and thus $q\dot{K}^2 \in H_{S_1}(\tau_{S_1})$.

As a consequence, we get $H_S(\tau_S) \cup \{x\dot{K}^2, q\dot{K}^2\} \subset H_{S_1}(\tau_{S_1})$.

By the choice of x and q we have $x\dot{K}^2 \in E_K(S)/\dot{K}^2 \setminus H_S(\tau_S)$ and $q\dot{K}^2 \notin E_K(S)/\dot{K}^2$, so $\operatorname{rk}_2 H_{S_1}(\tau_{S_1}) \geq \operatorname{rk}_2 H_S(\tau_S) + 2$. The set S_1 is obtained by adding one prime to S, so

$$\operatorname{rk}_2 E_K(S_1)/\dot{K}^2 = \operatorname{rk}_2 E_K(S)/\dot{K}^2 + 1.$$

Finally we get

$$\operatorname{rk}_2 (E_K(S_1)/\dot{K}^2)/H_{S_1}(\tau_{S_1}) \leq \operatorname{rk}_2 (E_K(S)/\dot{K}^2)/H_S(\tau_S) - 1.$$

Repeating this construction at most $n = \operatorname{rk}_2 (E_K(S)/\dot{K}^2)/H_S(\tau_S)$ times, we get a correspondence over $\hat{S}$ which is an extension of $\mathcal{R}_S$ such that $\operatorname{rk}_2 (E_K(\hat{S})/\dot{K}^2)/H_{\hat{S}}(\tau_{\hat{S}}) = 0$. ■

The following lemma shows that any correspondence can be extended by adjoining given primes of K.

Lemma 2.8. *Let $\mathfrak{q}, \mathfrak{r}$ be finite nondyadic primes of K. Any correspondence over S can be extended to a correspondence over $\hat{S}$ such that $\mathfrak{q} \in \hat{S}$ and $\mathfrak{r} \in T\hat{S}$.*

Proof. Let $\mathcal{R}_S = (T, \tau_S)$ be a fixed correspondence over S, and define $S' = TS$.

If $\mathfrak{q} \in S$ and $\mathfrak{r} \in S'$, then the statement of the lemma is obvious. Assume that this is not the case.

Assume that $\mathfrak{q} \notin S$ and denote $S_1 = S \cup \{\mathfrak{q}\}$. The class number $h = h_K(S)$ is odd. The ideal $\mathfrak{q}^h$ is principal in $\mathcal{O}_S(K)$. Denote a generator of the ideal by q. Then $\operatorname{ord}_{\mathfrak{q}} q \equiv 1 \pmod 2$ and $\operatorname{ord}_{\mathfrak{p}} q = 0$ for every $\mathfrak{p} \in \Omega(K) \setminus (S \cup \{\mathfrak{q}\})$.

It follows from Corollary 2.4 that there exist a prime $\mathfrak{q}'$ of K such that $\mathfrak{q}' \notin S' = TS$ and an element $q' \in \dot{K}$ with the following properties:

- $\tau_S \bar{q} = \bar{q'}$,
- $\operatorname{ord}_{\mathfrak{q}'} q' = 1$,
- $q' \in E_{S_1'}(K)$, where $S_1' = S' \cup \{\mathfrak{q}'\}$.

Let us extend $\mathcal{R}_S$ to a correspondence over S_1. To do this we extend T to a bijection on S_1 by setting $T\mathfrak{q} = \mathfrak{q}'$. Before we define a local isomorphism we have to show the equality $(-1, q)_{\mathfrak{q}} = (-1, q')_{\mathfrak{q}'}$, otherwise $\dot{K}_{\mathfrak{q}}/\dot{K}_{\mathfrak{q}}^2$ and $\dot{K}_{\mathfrak{q}'}/\dot{K}_{\mathfrak{q}'}^2$ are not isomorphic. First observe that the choice of q' implies $(-1, q)_{\mathfrak{p}} = (-1, q')_{T\mathfrak{p}}$ for every $\mathfrak{p} \in S$. Moreover, q and q' are $\mathfrak{p}$-adic units (modulo squares) for every prime $\mathfrak{p} \notin S_1$, hence $(-1,q)_{\mathfrak{p}} = 1 = (-1,q')_{\mathfrak{p}}$. By the above arguments and by the Hilbert reciprocity law it follows that

$$(-1,q)_{\mathfrak{q}} \prod_{\mathfrak{p}\in S} (-1,q)_{\mathfrak{p}} = 1 = (-1,q')_{\mathfrak{q}'} \prod_{\mathfrak{p}\in S} (-1,q')_{T\mathfrak{p}}.$$

Therefore $(-1,q)_{\mathfrak{q}} = (-1,q')_{\mathfrak{q}'}$, i.e. -1 is or is not a square in $K_{\mathfrak{q}}$ and $K_{\mathfrak{q}'}$ simultaneously. Fix a $\mathfrak{q}$-adic unit $u \in K$ and a $\mathfrak{q}'$-adic unit $u' \in K$ which are not local squares ($u = -1$ whenever -1 is not a square in $K_{\mathfrak{q}}$). It is easy to observe that the square classes determined by u and q form a basis of the vector space $\dot{K}_{\mathfrak{q}}/\dot{K}_{\mathfrak{q}}^2$ over $\mathbb{F}_2$. The mapping defined by $t_{\mathfrak{q}}(u) = u'$ and $t_{\mathfrak{q}}(q) = q'$ can be uniquely extended to a group isomorphism $t_{\mathfrak{q}} : \dot{K}_{\mathfrak{q}}/\dot{K}_{\mathfrak{q}}^2 \to \dot{K}_{\mathfrak{q}'}/\dot{K}_{\mathfrak{q}'}^2$. Remark 2.6 implies that $t_{\mathfrak{q}}$ preserves Hilbert symbols. This proves that $\mathcal{R}_{S_1} = (T, \tau_{S_1})$, where $\tau_{S_1} = \tau_S \times t_{\mathfrak{q}}$, is a correspondence over S_1.

We shall show that $H_S(\tau_S) \subseteq H_{S_1}(\tau_{S_1})$.

Let $x \in H_S(\tau_S)$. The correspondence $\mathcal{R}_S$ determines a global isomorphism $t_S\colon H_S(\tau_S) \to H_{TS}(\tau_S)$, so there exists an $x' \in H_{S'}(\tau_S)$ such that $t_S\bar{x} = \bar{x}'$. Since $x, q \in E_K(S_1)$, the elements x and q are $\mathfrak{p}$-adic units (modulo squares) for each prime $\mathfrak{p} \notin S_1$. By the Hilbert reciprocity law we have $\prod_{\mathfrak{p}\in S_1} (x,q)_{\mathfrak{p}} = 1$, which implies $(x,q)_{\mathfrak{q}} = \prod_{\mathfrak{p}\in S} (x,q)_{\mathfrak{p}}$. Similarly, we show that $(x',q')_{\mathfrak{q}'} = \prod_{\mathfrak{p}\in S'} (x',q')_{\mathfrak{p}}$.

The elements x, x' are $\mathfrak{q}$-adic and $\mathfrak{q}'$-adic units (modulo $\dot{K}_{\mathfrak{q}}^2$ and $\dot{K}_{\mathfrak{q}'}^2$), respectively. Hence $x = u^k \bmod \dot{K}_{\mathfrak{q}}^2$ and $x' = (u')^l \bmod \dot{K}_{\mathfrak{q}'}^2$ for some $k, l \in \{0,1\}$. Thus

$$(-1)^k = (x,q)_{\mathfrak{q}} = \prod_{\mathfrak{p}\in S} (x,q)_{\mathfrak{p}} = \prod_{\mathfrak{p}\in S'} (x',q')_{\mathfrak{p}} = (x',q')_{\mathfrak{q}'} = (-1)^l.$$

Therefore $k = l$, which means $t_{\mathfrak{q}}x = x'$ in $\dot{K}_{\mathfrak{q}'}/\dot{K}_{\mathfrak{q}'}^2$. On the other hand, $\tau_S\bar{x} = \bar{x}'$ in $G_{S'}(K)$. This shows that $\tau_{S_1}\bar{x} = \bar{x}'$, so $x \in H_{S_1}$. Thus we have proved that $\mathcal{R}_{S_1} = (T, \tau_{S_1})$ is an extension of $\mathcal{R}_S$.

If $\mathfrak{r} \in S_1'$, then we set $\hat{S} = S_1$ and the proof is completed.

Assume that $\mathfrak{r} \notin S_1'$. It is easily seen that $\mathcal{R}_{S_1'} = (T^{-1}, \tau_{S_1}^{-1})$ is a correspondence over S_1'. By similar arguments we can extend it to a correspondence over $S_2' = S_1' \cup \{\mathfrak{r}\}$. Thus we can define a correspondence over $S_2 = S_1 \cup \{\mathfrak{q}_1\}$ with $T\mathfrak{q}_1 = \mathfrak{r}$ which extends $\mathcal{R}_{S_1}$. We set $\hat{S} = S_2$, which completes the proof. ∎

Theorem 2.7 combined with Lemma 2.8 yields the following corollary.

Corollary 2.9. *Assume that $\mathfrak{q}$, $\mathfrak{r}$ are finite nondyadic primes of K. Any correspondence over a Hasse set S can be extended to a small equivalence $\mathcal{R} = (T, \tau)$ over a Hasse set $\hat{S}$ such that $\mathfrak{q} \in \hat{S}$ and $\mathfrak{r} \in T\hat{S}$.*

Proof. Let $\mathcal{R}_0 = (T, \tau_0)$ be a correspondence over S and let $\mathfrak{q}, \mathfrak{r}$ be primes of K. According to Lemma 2.8 there exists a correspondence $\mathcal{R}' = (T, \tau')$ over $S' \subset \Omega(K)$ with $S \subseteq S'$ that is an extension of $\mathcal{R}_0$ with $\mathfrak{q} \in S'$, $\mathfrak{r} \in TS'$. Applying Theorem 2.7 completes the proof. ∎

3. The main construction. In this section we shall prove our main result. To do this we need an operation of splitting of small equivalences. For a given nondyadic finite prime $\mathfrak{p}$ of K, we denote by $\pi_{\mathfrak{p}}$ a fixed $\mathfrak{p}$-adic uniformizer and by $u_{\mathfrak{p}}$ a fixed $\mathfrak{p}$-adic unit which is not a square in $K_{\mathfrak{p}}$.

The local square class group $\dot{K}_{\mathfrak{p}}/\dot{K}_{\mathfrak{p}}^2$ is generated by the square classes $\pi_{\mathfrak{p}}\dot{K}_{\mathfrak{p}}^2$ and $u_{\mathfrak{p}}\dot{K}_{\mathfrak{p}}^2$.

Assume that $\mathfrak{p}$, $\mathfrak{q}$ are fixed finite nondyadic primes of K such that -1 is a local square with respect to these primes (i.e. $-1 \in \dot{K}_{\mathfrak{p}}^2$ and $-1 \in \dot{K}_{\mathfrak{q}}^2$).

We shall consider the isomorphisms

$$t^0_{\mathfrak{p}\mathfrak{q}},\, t^1_{\mathfrak{p}\mathfrak{q}} \colon \dot{K}_{\mathfrak{p}}/\dot{K}_{\mathfrak{p}}^2 \to \dot{K}_{\mathfrak{q}}/\dot{K}_{\mathfrak{q}}^2$$

such that

$$\begin{aligned} t^0_{\mathfrak{p}\mathfrak{q}}(\pi_{\mathfrak{p}}) &= \pi_{\mathfrak{q}}, & t^0_{\mathfrak{p}\mathfrak{q}}(u_{\mathfrak{p}}) &= u_{\mathfrak{q}},\\ t^1_{\mathfrak{p}\mathfrak{q}}(\pi_{\mathfrak{p}}) &= u_{\mathfrak{q}}, & t^1_{\mathfrak{p}\mathfrak{q}}(u_{\mathfrak{p}}) &= u_{\mathfrak{q}}\pi_{\mathfrak{q}}. \end{aligned}$$

It is easy to check that the isomorphisms preserve Hilbert symbols. Observe that

$$t^0_{\mathfrak{p}\mathfrak{q}}(x) \neq t^1_{\mathfrak{p}\mathfrak{q}}(x) \quad \text{for every } x \notin \dot{K}_{\mathfrak{p}}^2. \tag{3.1}$$

Assume that K is an arbitrary global field. Let S be a fixed (sufficiently large) Hasse set of primes of K (the existence of such a set was shown in Section 2).

Let $\mathcal{R} = (T, \tau)$ be a small equivalence over S. For every finite nondyadic prime $\mathfrak{r}$ of K we construct two extensions of $\mathcal{R}$ denoted by $\mathcal{R}_0 = (T, \tau_0)$ over a set S_0 and $\mathcal{R}_1 = (T, \tau_1)$ over a set S_1 such that $\mathfrak{r}$ is contained in each of the sets S_0, TS_0, S_1, TS_1.

Let $a_1, \ldots, a_n$ form a basis of $E_K(S)/\dot{K}^2$ over $\mathbb{F}_2$. According to [4, Satz 169] and [7, 65:17], there exist infinitely many nondyadic finite primes $\mathfrak{p}$ of K such that $\left(\frac{a_i}{\mathfrak{p}}\right) = 1$ for every $i \in \{1, \ldots, n\}$. Let $\mathfrak{q}, \mathfrak{q}' \in \Omega(K) \setminus S$ be two such primes. Then in particular $-1 \in \dot{K}_{\mathfrak{q}}^2$ and $-1 \in \dot{K}_{\mathfrak{q}'}^2$. Denote $\tilde{S} = S \cup \{\mathfrak{q}\}$. Let us build two correspondences $\tilde{\mathcal{R}}_0 = (T_0, \tau_0)$, $\tilde{\mathcal{R}}_1 = (T_1, \tau_1)$ over $\tilde{S}$. In both, $T_0 = T_1$ is the extension of T such that $T_0(\mathfrak{q}) = T_1(\mathfrak{q}) = \mathfrak{q}'$, whereas $\tau_0 = \tau \times t^0_{\mathfrak{q}\mathfrak{q}'}$ and $\tau_1 = \tau \times t^1_{\mathfrak{q}\mathfrak{q}'}$.

Observe that

$$t^0_{\mathfrak{q}\mathfrak{q}'}(x) = 1 \bmod \dot{K}_{\mathfrak{q}}^2 \quad \text{and} \quad t^1_{\mathfrak{q}\mathfrak{q}'}(x) = 1 \bmod \dot{K}_{\mathfrak{q}}^2$$

for every $x \in E_K(S)$. Therefore $E_K(S)/\dot{K}^2 \subseteq H_{\tilde{S}}(\tau_0)$ and $E_K(S)/\dot{K}^2 \subseteq H_{\tilde{S}}(\tau_1)$, which means that $\tilde{\mathcal{R}}_0$ and $\tilde{\mathcal{R}}_1$ are extensions of $\mathcal{R}$. According to Corollary 2.9 they can be extended to small equivalences over suitable Hasse sets S_0, S_1 such that $\mathfrak{r}$ belongs to each of the sets S_0, TS_0, S_1, TS_1. The prime $\mathfrak{q}$ will be called a *splitting prime* of the small equivalence $\mathcal{R}$.

Remark 3.1. Lemma 2.5 implies that in the above construction there exists $x \in E_K(\tilde{S}) \subset E_K(S_0) \cap E_K(S_1)$ such that $x \notin \dot{K}^2_{\mathfrak{q}}$.

Now we are in a position to prove the main result of the paper.

Theorem 3.2. *The group of strong automorphisms of the Witt ring of any global field has the cardinality of the continuum.*

Proof. The Witt ring of a global field is countable, so the cardinality of the group of its automorphisms does not exceed the cardinality of the continuum. It suffices to prove that the group of strong automorphisms of the Witt ring of a global field is uncountable.

First we take a (sufficiently large) Hasse set S (cf. Remark 2.1). It is clear that $\mathcal{R} = (T, \tau)$, where T and τ are the identity mappings on S and $G_K(S) = \prod_{\mathfrak{p} \in S} \dot{K}_{\mathfrak{p}}/\dot{K}^2_{\mathfrak{p}}$ respectively, is a small equivalence over S. Let us arrange all the primes in $\Omega(K) \setminus S$ into a sequence $(\mathfrak{p}_i)_{i\in\mathbb{N}}$.

For every infinite binary sequence $\epsilon = (\epsilon_i)_{i\in\mathbb{N}} \in \{0,1\}^{\mathbb{N}}$ we shall construct an increasing sequence of Hasse sets $S_{\epsilon_1} \subseteq S_{\epsilon_1,\epsilon_2} \subseteq \cdots \subseteq S_{\epsilon_1,\dots,\epsilon_k} \subseteq \cdots$ and a sequence of small equivalences $\mathcal{R}_{\epsilon_1}, \mathcal{R}_{\epsilon_1,\epsilon_2}, \dots, \mathcal{R}_{\epsilon_1,\dots,\epsilon_k}, \dots$ such that

- $\mathcal{R}_{\epsilon_1,\dots,\epsilon_k} = (T, \tau_{\epsilon_1,\dots,\epsilon_k})$ is a small equivalence over $S_{\epsilon_1,\dots,\epsilon_k}$ for all $k \in \mathbb{N}$.
- $\mathcal{R}_{\epsilon_1,\dots,\epsilon_k}$ is an extension of $\mathcal{R}_{\epsilon_1,\dots,\epsilon_{k-1}}$ for all $k \geq 2$.
- $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ belong to both $S_{\epsilon_1,\dots,\epsilon_k}$ and $TS_{\epsilon_1,\dots,\epsilon_k}$.

The sequences are built recursively. If $k = 1$, we assume that $\hat{\mathcal{R}} = \mathcal{R}$ and $\hat{S} = S$. Assume that for a given $k \geq 2$ we have already constructed a small equivalence $\hat{\mathcal{R}} = \mathcal{R}_{\epsilon_1,\dots,\epsilon_{k-1}}$ over $\hat{S} = S_{\epsilon_1,\dots,\epsilon_{k-1}}$. Applying the splitting operation to $\hat{\mathcal{R}}$ and $\mathfrak{p}_k$ yields two small equivalences $\hat{\mathcal{R}}_0$ and $\hat{\mathcal{R}}_1$ over suitable $\hat{S}_0$ and $\hat{S}_1$, respectively, with $\mathfrak{p}_k \in \hat{S}_i, T\hat{S}_i$ for $i = 0, 1$. Setting $\mathcal{R}_{\epsilon_1,\dots,\epsilon_k} = \hat{\mathcal{R}}_{\epsilon_k}$ and $S_{\epsilon_1,\dots,\epsilon_k} = \hat{S}_{\epsilon_k}$ completes the kth step.

It remains to show that every binary sequence determines a Hilbert self-equivalence, and that the Hilbert self-equivalences determined by different sequences are different. To do this, we need to define a bijection $T\colon \Omega(K) \to \Omega(K)$ and a global group automorphism t of $\dot{K}/\dot{K}^2$.

For simplicity of notation, we write $E_K(\gamma)$, t_γ instead of $E_K(S_\gamma)$, t_{S_γ}, respectively (γ is a finite binary sequence).

Fix a sequence $\omega = (\epsilon_i)_{i\in\mathbb{N}} \in \{0,1\}^{\mathbb{N}}$. For any prime $\mathfrak{p} \in \Omega(K)$ there exists a sequence $\gamma = (\epsilon_1, \dots, \epsilon_k)$ such that $\mathfrak{p} \in S_\gamma$. We define $T\mathfrak{p} = T_\gamma\mathfrak{p}$. Since $\mathcal{R}_{\epsilon_1,\dots,\epsilon_{k+1}}$ is an extension of $\mathcal{R}_{\epsilon_1,\dots,\epsilon_k}$ for every $k \in \mathbb{N}$, the mapping T

is well defined. It is easily seen that T is an injection, as $T_{\epsilon_1,\dots,\epsilon_k}$ is, for every $k \geq 1$. Since $\{\mathfrak{p}_1,\dots,\mathfrak{p}_k\} \subseteq T_{\epsilon_1,\dots,\epsilon_k} S_{\epsilon_1,\dots,\epsilon_k}$ for $k \in \mathbb{N}$, T is a surjection.

To define the automorphism t observe that for every $x \in \dot{K}$ the set of primes $\mathfrak{p}$ such that $\operatorname{ord}_{\mathfrak{p}} x \neq 0$ is finite. Thus $\operatorname{ord}_{\mathfrak{p}} x = 0$ for all $\mathfrak{p} \in \Omega(K) \setminus (S \cup \{\mathfrak{p}_1,\dots,\mathfrak{p}_k\})$ if $k \in \mathbb{N}$ is large enough. This implies $x \in E_K(\epsilon_1,\dots,\epsilon_k)$. Define $tx = t_{\epsilon_1,\dots,\epsilon_k} x$. Since for every $k \in \mathbb{N}$ the small equivalence $\mathcal{R}_{\epsilon_1,\dots,\epsilon_{k+1}}$ is an extension of $\mathcal{R}_{\epsilon_1,\dots,\epsilon_k}$, the mapping t is well defined. Since every $t_{\epsilon_1,\dots,\epsilon_k}$ is a group isomorphism, so is t.

For any $x, y \in \dot{K}$ there exists $k \in \mathbb{N}$ such that $x, y \in E_K(S_{\epsilon_1,\dots,\epsilon_k})$. Then for every $\mathfrak{p} \in S_{\epsilon_1,\dots,\epsilon_k}$ we have

$$(x,y)_{\mathfrak{p}} = (t_{\epsilon_1,\dots,\epsilon_k} x, t_{\epsilon_1,\dots,\epsilon_k} y)_{T_{\epsilon_1,\dots,\epsilon_k}\mathfrak{p}} = (tx,ty)_{T\mathfrak{p}}.$$

Moreover, for every prime $\mathfrak{r} \notin S_{\epsilon_1,\dots,\epsilon_k}$ the square classes of x, y are $\mathfrak{r}$-adic units, whereas the square classes of tx, ty are $T\mathfrak{r}$-adic units modulo squares, thus

$$(x,y)_{\mathfrak{r}} = 1 = (tx,ty)_{T\mathfrak{r}},$$

so t preserves Hilbert symbols. This means that (T,t) is a Hilbert self-equivalence of K.

It remains to show that two Hilbert-symbol equivalences (T,t) and (T',t') corresponding (in the construction) to two different sequences $\omega = (\epsilon_i)_{i\in\mathbb{N}} \in \{0,1\}^{\mathbb{N}}$ and $\omega' = (\epsilon'_i)_{i\in\mathbb{N}} \in \{0,1\}^{\mathbb{N}}$ are different.

Let k be the smallest integer such that $\epsilon_k \neq \epsilon'_k$. We can assume that $\epsilon_k = 0$ and $\epsilon'_k = 1$. Let $\mathfrak{q}$ be a splitting prime of $\mathcal{R}_{\epsilon_1,\dots,\epsilon_{k-1}}$ over $S_{\epsilon_1,\dots,\epsilon_{k-1}}$ and $T_{\epsilon_1,\dots,\epsilon_{k-1}}\mathfrak{q} = \mathfrak{q}'$. By the splitting construction and Remark 3.1 there exists $x \in E_K(\epsilon_1,\dots,\epsilon_k) \cap E_K(\epsilon'_1,\dots,\epsilon'_k)$ such that $x \notin \dot{K}^2_{\mathfrak{q}}$.

Then

$$\begin{aligned} t(x) &= t_{(\epsilon_1,\dots,\epsilon_k)}(x) = t^0_{\mathfrak{q}\mathfrak{q}'}(x) \bmod \dot{K}^2_{\mathfrak{q}'}, \\ t'(x) &= t_{(\epsilon'_1,\dots,\epsilon'_k)}(x) = t^1_{\mathfrak{q}\mathfrak{q}'}(x) \bmod \dot{K}^2_{\mathfrak{q}'}. \end{aligned}$$

According to (3.1) we have $t^0_{\mathfrak{q}\mathfrak{q}'}(x) \neq t^1_{\mathfrak{q}\mathfrak{q}'}(x)$, hence $t(x) \neq t'(x)$.

We established a one-to-one correspondence between the set of all binary sequences and a subset of the group of all Hilbert equivalences of K. Since the cardinality of the former set is $\mathfrak{c}$, the proof is complete. ∎

4. Conclusion. Let $W(F)$ be the Witt ring of a global field F. The cardinality of the set $\mathcal{B}(W(F))$ of all bijections of $W(F)$ does not exceed $\mathfrak{c}$. Furthermore we proved in Theorem 3.2 that the cardinality of the group $\operatorname{SAut}(W(F))$ of all strong automorphisms of $W(F)$ is $\mathfrak{c}$. Thus

$$\mathfrak{c} = \operatorname{card}(\operatorname{SAut}(W(F))) \leq \operatorname{card}(\operatorname{Aut}(W(F))) \leq \operatorname{card}(\mathcal{B}(W(F))) \leq \mathfrak{c},$$

where $\operatorname{Aut}(W(F))$ denotes the group of all automorphisms of $W(F)$. This proves that the cardinality of $\operatorname{Aut}(W(F))$ is $\mathfrak{c}$.

In this paper we have restricted our attention to global fields of characteristic different from 2. The case of characteristic 2 requires a different approach, but we conjecture that the result is the same.

Acknowledgements. We thank Marcin Stępień for his help with editing a preliminary version of this paper. We also thank the anonymous referee for the careful reading of our manuscript and helpful comments.

References

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

[2] A. Czogała and A. Sładek, *Witt rings of global fields*, Comm. Algebra 31 (2003), 3195–3205.

[3] F. DeMeyer, D. Harrison and R. Miranda, *Quadratic forms over* $\mathbb{Q}$ *and Galois extensions of commutative rings*, Mem. Amer. Math. Soc. 77 (1989), no. 394.

[4] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Leipzig, 1923.

[5] D. Leep and M. Marshall, *Isomorphisms and automorphisms of Witt rings*, Canad. Math. Bull. 31 (1988), 250–256.

[6] D. B. Leep and A. R. Wadsworth, *The Hasse norm theorem mod squares*, J. Number Theory 42 (1992), 337–348.

[7] O. T. O'Meara, *Introduction to Quadratic Forms*, Springer, Berlin, 1973.

[8] R. Perlis, K. Szymiczek, P. Conner and R. Litherland, *Matching Witts with global fields*, in: Contemp. Math. 155, Amer. Math. Soc., 1994, 365–387.

[9] M. Somodi, *On the size of the wild set*, Canad. J. Math. 57 (2005), 180–203.

[10] M. R. Stępień, *Uncountability of the group of strong automorphisms of Witt ring of rational numbers*, Scientific Research of the Institute of Mathematics and Computer Science, Częstochowa Univ. of Technology 1 (2012), 117–128.

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

[12] E. Witt, *Teorie der quadratischen Formen in beliebigen Körpern*, J. Reine Angew. Math. 176 (1937), 31–44.

Alfred Czogała, Mieczysław Kula
Institute of Mathematics
University of Silesia
Bankowa 14
40-007 Katowice, Poland
E-mail: alfred.czogala@us.edu.pl
mieczyslaw.kula@us.edu.pl

Received on 22.12.2012
and in revised form on 5.8.2013 (7297)