Please cite this article as:
Marcin Ryszard Stępień, Uncountability of the group of strong automorphisms of Witt ring of rational numbers, Scientific Research of the Institute of Mathematics and Computer Science, 2012, Volume 11, Issue 1, pages 117-128.
The website: http://www.amcm.pcz.pl/

UNCOUNTABILITY OF THE GROUP OF STRONG AUTOMORPHISMS OF WITT RING OF RATIONAL NUMBERS

Marcin Ryszard Stępień

Kielce University of Technology, Poland
mstepien@tu.kielce.pl

Abstract. We use the notion of rational self-equivalence which is a special case of Hilbert-symbol equivalence of fields, where both fields are considered to be the field $\mathbb{Q}$ of rational numbers. We define a small self-equivalence of the field $\mathbb{Q}$ as a special case of small equivalence of fields - a tool for constructing Hilbert-symbol equivalence of fields. We shall show, that one can choose initial sets of prime numbers and then control the processes of extending of small self-equivalence such that uncountable many rational self-equivalences can be constructed. The final conclusion is the corollary deciding that the group of strong automorphisms of Witt ring $W(\mathbb{Q})$ of rational numbers is uncountable.

Introduction

In this paper we shall show, how uncountalbly many strong automorphisms of Witt ring $W(\mathbb{Q})$ can be constructed.

We will use the notion of Hilbert-symbol equivalence of fields considered in [1], [2] and [3]. The ideas contained in these works are the base of our constructions. The restriction to the field $\mathbb{Q}$ of rational numbers allows us to simplify many details, therefore instead of frequent reference to literature we try to present the solution of the problem in the most complete way. In this section we shall outline the notions and facts which will be used in the paper. We use properties and facts from number theory, which can be found in [2], [4], [5] or [6].

Consider the field $\mathbb{Q}$ of rational numbers. Let $\mathbb{P}$ denote the set of prime numbers together with the symbol ∞. In the follow we consider its two subsets:

$$\mathbb{P}_1 = \{p \in \mathbb{P} \setminus \{\infty\} : p \equiv 1 \pmod 4\}, \qquad \mathbb{P}_3 = \{p \in \mathbb{P} \setminus \{\infty\} : p \equiv 3 \pmod 4\}.$$

For each prime number p there exists a completion $\mathbb{Q}_p$ of the field $\mathbb{Q}$ with respect to p-adic valuation v_p called the field of p-adic numbers. Moreover we assume that $\mathbb{Q}_\infty = \mathbb{R}$ is a completion of $\mathbb{Q}$ with respect to usual absolute value (see [4]). Let t be an automorphism of the group of square classes $t: \mathbb{Q}^*/\mathbb{Q}^{*2} \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ and let T be an invertible map $T: \mathbb{P} \to \mathbb{P}$ preserving Hilbert symbols in the sense that $(a,b)_p = (t(a),t(b))_{T(p)}$ for all $a,b \in \mathbb{Q}^*/\mathbb{Q}^{*2}$ and for all $p \in \mathbb{P}$. The pair of maps

(T,t) we will call the *Hilbert-symbol rational self-equivalence* or shortly just *rational self-equivalence*. The notion of rational self-equivalence is a special case of a more general notion of *Hilbert-symbol equivalence of fields*, where the prime numbers are replaced by prime ideals of global fields (see [2, 3]).

Two number fields have isomorphic Witt rings of quadratic forms if and only if there is a Hilbert-symbol equivalence between them (comp. [3]). Namely the bijection t fulfilling the above conditions induces a strong isomorphism of Witt rings.

Constructing of Hilbert-symbol equivalence between Witt equivalent number fields is not an easy problem. The task of defining maps between infinite sets is difficult since there is no method of doing this in a finite number of steps. In [3] the authors reduced this problem to the problem of constructing so called *small equivalence*, which requires defining maps between finite sets of prime ideals. For more details the reader is referred to [3]. We use these ideas in order to construct the set of rational self-equivalences. There was shown in [7] that the set of rational self-equivalences is infinite and the effective construction of rational self-equivalences was presented. In this paper we shall prove that the set of rational self-equivalences is, in fact, uncountable.

Let p and q be two elements in the set $\mathbb{P}$. Every group isomorphism $t_{lok} : \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \to \mathbb{Q}_q^*/\mathbb{Q}_q^{*2}$ preserving Hilbert symbols will be called *local isomorphism*. The local isomorphism t_{lok} is an isomorphism of quaternionic structures of local fields $\mathbb{Q}_p$ and $\mathbb{Q}_q$ (for more information about quaternionic structures and their isomorphisms see [8, 9]). If p and q are prime numbers, then the local isomorphism $t_{lok} : \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \to \mathbb{Q}_q^*/\mathbb{Q}_q^{*2}$ is called *tame* if $v_q(t_{lok}(\mathrm{x})) \equiv v_p(x) \pmod 2$. It is well-known that if the prime numbers p and q are equivalent to 3 modulo 4, then -1 is not a square in fields $\mathbb{Q}_p$ and $\mathbb{Q}_q$ and every local isomorphism maps -1 to -1. In this case every local isomorphism is tame. It is easy to notice that exactly two local isomorphisms exist for such a prime numbers p and q. The first one fulfilling $t_{lok}(p) = q$ we call *simple local isomorphism* and the other one $t_{lok}(p) = -q$ we call *skew local isomorphism*.

By [3] p. 376 it follows that the rational self-equivalence (T,t) determines the family of local isomorphisms $t_p : \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \to \mathbb{Q}_{T(p)}^*/\mathbb{Q}_{T(p)}^{*2}$ fulfilling the condition $t_p(a\mathbb{Q}_p^{*2}) = t(a)\mathbb{Q}_{T(p)}^{*2}$.

Let $S = \{p_1,\ldots,p_k\}$ be any finite subset of $\mathbb{P}$ containing 2 and ∞. Let us fix that $p_1 = \infty$ and $p_2 = 2$. We define the *set of S-singular elements* as follows:

$$E_S = \{\mathrm{x} \in \mathbb{Q}^* : v_p(x) \equiv 0 \pmod 2 \text{ for every } p \notin S\}$$

Notice that E_S is a subgroup of the multiplicative group of the field $\mathbb{Q}$ containing all squares of non-zero rational numbers. Therefore the quotient group $E_S/\mathbb{Q}^{*2}$ is a subgroup of the group of square classes $\mathbb{Q}^*/\mathbb{Q}^{*2}$.

For any element $p \in \mathbb{P}$ the group $G_p = \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ (of exponent 2) can be viewed as a vector space over the two-element field $\mathbb{F}_2$ and the Hilbert symbol determines

non-degenerate bilinear form $\beta_p : G_p \times G_p \to \mathbb{F}_2$ such that $(a,b)_p = (-1)^{\beta_p(a,b)}$. For given finite subset $S \subset \mathbb{P}$ we create a bilinear space (G_S,β_S), where

$$G_S = \prod_{p\in S} G_p = \prod_{p\in S} \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \qquad \beta_S\left([a_p]_{p\in S},[b_p]_{p\in S}\right) = \sum_{p\in S}\beta_p(a_p,b_p).$$

The space (G_S,β_S) is an orthogonal sum of non-degenerate bilinear subspaces, hence it is also non-degenerate.

For every $p \in \mathbb{P}$ the natural imbedding of the field $\mathbb{Q}$ in $\mathbb{Q}_p$ induces the group homomorphism i_p: $\mathbb{Q}^*/\mathbb{Q}^{*2} \to \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ which is surjective. For given finite set $S = \{p_1,\ldots,p_n\} \subset \mathbb{P}$ we get the diagonal homomorphism $\mathrm{diag}_S : \mathbb{Q}^*/\mathbb{Q}^{*2} \to G_S$ defined by $\mathrm{diag}_S(a\mathbb{Q}^{*2}) = [i_{p_1}(a),\ldots, i_{p_n}(a)] = [a\mathbb{Q}_{p_1}^{*2},\ldots, a\mathbb{Q}_{p_n}^{*2}]$ for all $a \in \mathbb{Q}$. In order to simplify the notation the rational number a will be often identified with its class of squares $a\mathbb{Q}^{*2}$ and we will use the notation $\bar{a} = \mathrm{diag}_S(a\mathbb{Q}^{*2})$. The restriction of the homomorphism diag_S to the set of square classes of S-singular elements we denote by i_S.

Lemma 1.1. *If* $S = \{\infty,2,p_3,\ldots,p_n\} \subset \mathbb{P}$, *then*

1. $\{-1\mathbb{Q}^{*2}, 2\mathbb{Q}^{*2}, p_3\mathbb{Q}^{*2}, \ldots, p_n\mathbb{Q}^{*2}\}$ *is a basis of the space* $E_S/\mathbb{Q}^{*2}$.
2. $\dim(E_S/\mathbb{Q}^{*2}) = |S|$.
3. i_S *is a group monomorphism.*
4. $\dim G_S = 2|S|$.
5. *The subspace* $i_S(E_S/\mathbb{Q}^{*2})$ *is equal to its orthogonal completion in the linear space* (G_S,β_S).

Proof. By the definition of the set E_S it follows that prime numbers which are not in S can appear in decomposition of x only with even exponents. Let $x = (-1)^{e_1} 2^{2k_2+e_2} p_3^{2k_3+e_3} \cdots p_n^{2k_n+e_n} q_1^{2l_1} \cdots q_m^{2l_m}$ where $q_1,q_2,\ldots,q_n \notin S$ are prime numbers, $k_i,l_i \in \mathbb{Z}$ and $e_i \in \{0,1\}$ be a canonical decomposition of any nonzero rational number x. Then $x\mathbb{Q}^{*2} = (-1)^{e_1} 2^{e_2} p_3^{e_3} \cdots p_n^{e_n} \mathbb{Q}^{*2}$. Hence the elements of the group $E_S/\mathbb{Q}^{*2}$ are uniquely represented by integers of the form $(-1)^{e_1} 2^{e_2} p_3^{e_3} \cdots p_n^{e_n}$. In particular the elements $-1\mathbb{Q}^{*2}$, $2\mathbb{Q}^{*2}$, …, $p_3\mathbb{Q}^{*2}$, $p_n\mathbb{Q}^{*2}$ create a basis of linear space $E_S/\mathbb{Q}^{*2}$ over $\mathbb{F}_2$ and $\dim E_S/\mathbb{Q}^{*2} = |S|$. This finishes the proof of 1 and 2.

3. If $x \in \ker i_S$, then x is a square in each p-adic field for $p \in S$ and it follows that $x > 0$ since the squares in the field $\mathbb{Q}_\infty = \mathbb{R}$ are positive numbers and $v_p(x) \equiv 0 \pmod 2$ for prime numbers in S. It shows that x is a product of prime

numbers with even exponents, hence x is a square of a rational number. Therefore $\ker i_S = \{\mathbb{Q}^{*2}\}$.

4. It suffices to notice that $\dim G_S = \sum_{p\in S} \dim G_p = 1+3+2(n-2) = 2n$ since $\dim G_\infty = \dim \mathbb{R}^*/\mathbb{R}^{*2} = 1$, $\dim G_2 = \dim \mathbb{Q}_2^*/\mathbb{Q}_2^{*2} = 3$ and $\dim G_p = \dim \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} = 2$ for odd prime numbers p.

5. Let $x, y \in E_S$. By Hilbert reciprocity law $\prod_{p\in\mathbb{P}} (x,y)_p = 1$ we get

$$\prod_{p\in S} (x,y)_p = \prod_{p\in \mathbb{P}\setminus S} (x,y)_p .$$

For every $p \in \mathbb{P}\setminus S$ the elements x, y are p-adic units, hence $(x,y)_p = 1$. Therefore

$$(-1)^{\beta_S(x,y)} = \prod_{p\in S} (-1)^{\beta_p(x,y)} = \prod_{p\in S} (x,y)_p = 1$$

Thus we get $\beta_S(x,y) = 0$. It follows that for $F = i_S(E_S/\mathbb{Q}^{*2})$ we have $F \subseteq F^\perp$ and consequently $\dim F \le \dim F^\perp$. Since i_S is a monomorphism, hence $\dim F = \dim E_S/\mathbb{Q}^{*2} = |S|$. It is well-known that the bilinear space (G_S, β_S) is non-degenerate, thus by the orthogonal complement theorem we get $\dim F^\perp = \dim G_S - \dim F = 2|S| - |S| = n$. Since the subspaces F and $F^\perp$ have the same dimensions and one of them is contained in the second one, thus $F = F^\perp$.

Definition 1.2. A *small self-equivalence of the field* $\mathbb{Q}$ *defined on the set* S is a triplet $\Re = (S, T, \{t_p\}_{p\in S})$ where

1) S is a finite subset of $\mathbb{P}$ and ∞, $2 \in S$;
2) $T : S \to \mathbb{P}$ is an injection;
3) $\{t_p\}_{p\in S}$ is a family of local isomorphisms $t_p : \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \to \mathbb{Q}_{T(p)}^*/\mathbb{Q}_{T(p)}^{*2}$ preserving Hilbert symbols, i.e. $(a,b)_p = (t_p(a), t_p(b))_{T(p)}$ for all $a,b \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$.

The above definition of small self-equivalence imposes some restrictions on the map T. Namely $T(\infty) = \infty$, since $p = \infty$ is the only element of the set $\mathbb{P}$ such that $\dim \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} = 1$. Similarly $T(2) = 2$, since $p = 2$ is the only element of the set $\mathbb{P}$ such that $\dim \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} = 3$. Moreover by preserving the Hilbert symbol by the isomorphism $t_p : \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \to \mathbb{Q}_{T(p)}^*/\mathbb{Q}_{T(p)}^{*2}$ it follows that the quaternionic structures of the fields $\mathbb{Q}_p$ i $\mathbb{Q}_{T(p)}$ are isomorphic, what holds if and only if $T(p) \equiv p \pmod 4$. Conversely, if the injection $T : S \to \mathbb{P}$ fulfills these conditions, thus for any

choice of local isomorphisms $t_p : \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \to \mathbb{Q}_{T(p)}^*/\mathbb{Q}_{T(p)}^{*2}$ for $p \in S$ the triplet $(S, T, \{t_p\}_{p\in S})$ is a small self-equivalence.

Let us denote $S' = T(S)$. By injectivity of the map T it follows that the sets S and S' have the same cardinality. A small self-equivalence defined on S induces group isomorphism $\tau_S : G_S \to G_{S'}$ which is a product of the family of local isomorphisms determined by the equivalence. If $[\alpha_1,\ldots,\alpha_n] \in G_S$, then $\tau_S([\alpha_1,\ldots,\alpha_n]) = [t_{p_1}(\alpha_1),\ldots,t_{p_n}(\alpha_n)]$. Any small self-equivalence determines two sets

$$H_S = \{\alpha \in E_S/\mathbb{Q}^{*2} : \tau_S \circ i_S(\alpha) \in i_{S'}(E_{S'}/\mathbb{Q}^{*2})\} \subseteq E_S/\mathbb{Q}^{*2},$$

$$H_{S'} = \{\gamma \in E_{S'}/\mathbb{Q}^{*2} : \tau_S^{-1} \circ i_{S'}(\gamma) \in i_S(E_S/\mathbb{Q}^{*2})\} \subseteq E_{S'}/\mathbb{Q}^{*2}.$$

Since the maps i_S, $i_{S'}$, τ_S are monomorphisms, then $t_S = i_{S'}^{-1} \circ \tau_S \circ i_S\big|_{H_S}$ maps H_S isomorphically into $H_{S'}$. The situation is presented on the following diagram

$$\begin{array}{ccc} H_S \subseteq E_S/\mathbb{Q}^{*2} & \xrightarrow{\ i_S\ } & G_S \\ \Big\downarrow t_S & & \Big\downarrow \tau_S \\ H_{S'} \subseteq E_{S'}/\mathbb{Q}^{*2} & \xrightarrow{\ i_{S'}\ } & G_{S'} \end{array}$$

Lemma 1.3. *For any small self-equivalence defined on the set S the following conditions are equivalent:*
1. $H_S = E_S/\mathbb{Q}^{*2}$.
2. $H_{S'} = E_{S'}/\mathbb{Q}^{*2}$.
3. $\tau_S \circ i_S(E_S/\mathbb{Q}^{*2}) = i_{S'}(E_{S'}/\mathbb{Q}^{*2})$.

Proof. It suffices to notice that by lemma 1.1 $\dim i_S(E_S/\mathbb{Q}^{*2}) = \dim i_{S'}(E_{S'}/\mathbb{Q}^{*2})$, because the sets S and S' are equinumerous.

If at least one of the conditions of the above lemma 1.3 is fulfilled, then the small self-equivalence $\mathfrak{R}$ will be called *regular*. In the other case we say that small self-equivalece is *irregular* and the number $\operatorname{def}\mathfrak{R} = \dim E_S/\mathbb{Q}^{*2} - \dim H_S$ we call *defect* of small self-equivalence. If the small self-equivalence defined on the set S is regular, then t_S is a group isomorphism between $E_S/\mathbb{Q}^{*2}$ and $E_{S'}/\mathbb{Q}^{*2}$ and the equality $\tau_S \circ i_S = i_{S'} \circ t_S$ holds.

Definition 1.4. We say that the small self-equivalence $\mathfrak{R}_1 = (S_1, T_1, \{t_p^{(1)}\}_{p\in S_1})$ is an *extension of the small self-equivalence* $\mathfrak{R} = (S, T, \{t_p\}_{p\in S})$ if

1) $S \subseteq S_1$;
2) the map T_1 is an extension of the map T;
3) $t_p = t_p^{(1)}$ for all $p \in S$;
4) $H_S \subseteq H_{S_1}$ and the global isomorphism t_{S_1} is an extension of the isomorphism t_S.

We say that the extension $\Re_1 = (S_1, T_1, \{t_p^{(1)}\}_{p \in S_1})$ of the small self-equivalence $\Re = (S, T, \{t_p\}_{p \in S})$ is determined by $q, q' \in \mathbb{P}$ and the local isomorphism $t_q : \mathbb{Q}_q^*/\mathbb{Q}_q^{*2} \to \mathbb{Q}_{q'}^*/\mathbb{Q}_{q'}^{*2}$ where $S_1 = S \cup \{q\}$ and T_1 is an extension of T such that $T_1(q) = q'$ and $\{t_p^{(1)}\}_{p \in S_1} = \{t_p\}_{p \in S} \cup \{t_q\}$.

We shall show that any regular small self-equivalence defined on arbitrary finite subset of $\mathbb{P}$ containing 2 and ∞ can be extended to a rational self-equivalence. Next we will notice that the map $t : \mathbb{Q}^*/\mathbb{Q}^{*2} \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ obtained in such a construction induces a strong automorphism of the Witt ring $W(\mathbb{Q})$ of rational numbers. We shall show how to control the construction in order to get uncountably many rational self-equivalences or uncountably many strong automorphisms of Witt ring $W(\mathbb{Q})$.

1. The construction of rational self-equivalences

Lemma 2.1 *Assume that* $S \subset \mathbb{P}$ *is a finite set,* $\infty, 2 \in S$ *and* $\alpha \in G_S$. *Then there exists a prime number* $q \notin S$ *and an element* $c \in E_S$ *such that* $\mathrm{diag}_S(cq\mathbb{Q}^{*2}) = \alpha$.

Proof. Let $a_1, \ldots, a_n$ be integers, which are not squares and let $\alpha = [a_1\mathbb{Q}_{p_1}^{*2}, a_2\mathbb{Q}_{p_2}^{*2}, \ldots, a_n\mathbb{Q}_{p_n}^{*2}]$. We can assume that $a_1 \in \{1, -1\}$. By the Chinese remainder theorem it follows that there exists a natural number b such that $b \equiv a_1 a_2 \pmod{16}$ and $b \equiv a_1 a_i \pmod{p_i^2}$ for $i = 3, \ldots, n$. Let us denote by $M = (4p_3 \cdots p_n)^2$ and $d = \gcd(b, M)$. Then the numbers $\frac{b}{d}$ and $\frac{M}{d}$ are coprime and by Dirichlet's theorem it follows that the arithmetic progression $(\frac{b}{d} + k\frac{M}{d})_{k \in \mathbb{N}}$ contains infinitely many prime numbers. Let q be one such number coprime to M, thus $q \notin S$. Let us denote $a = a_1 dq$. It is obvious that $a \equiv a_1 b \pmod{M}$, hence $a \equiv a_1 b \pmod{p_i^2}$ and $qd \equiv b \pmod{M}$ thus by transitivity of congruence relation we have $qd \equiv a_1 a_i \pmod{p_i^2}$ and consequently $a_1 dq \equiv a_i \pmod{p_i^2}$. Assume that $c = a_1 d$.

Therefore we have $cq \equiv a_i \pmod{p_i^2}$. Since $d|M$ hence $d \in E_S$ and it follows that the element $c = a_1 d$ is in E_S.

Notice that the numbers cq and a_1 are both positive or both negative. Moreover $v_2(a_i) = v_2(cq) < 2$, $4 \le v_2(cq - a_2)$ and $v_{p_i}(a_i) = v_{p_i}(cq) < 2 \le v_{p_i}(cq - a_i)$, then by Hensel's lemma it follows that $cq\mathbb{Q}_{p_i}^{*2} = a_i\mathbb{Q}_{p_i}^{*2}$ for $i = 2,\ldots,n$. Therefore we get $i_S(cq\mathbb{Q}^{*2}) = \alpha$. □

Lemma 2.2. *For any regular small self-equivalence $\Re = (S, T, \{t_p\}_{p\in S})$ and for any prime number $q \in \mathbb{P} \setminus S$ there exists such a prime number $q' \notin S'$ that for any tame local isomorphism $t_q : G_q \to G_{q'}$ the extension of the small self-equivalence $\Re$ determined by elements q, q', t_q has a defect not bigger than 1. Moreover, there exists a tame local isomorphism $t_q^{\bullet} : G_q \to G_{q'}$ such that the extension of self-equivalence $\Re$ determined by elements q, q', $t_q^{\bullet}$ is a regular small self-equivalence.*

Proof. Let us fix $S' = T(S)$ and $S_1 = S \cup \{q\}$. If $\Re$ is a regular small self-equivalence, then $\tau_S \circ i_S = i_{S'} \circ t_S$. Using lemma 2.1 there exists a prime number $q' \notin S'$ and an integer $a \in E_{S'}$ such that $\overline{aq'} = \tau_S(\bar{q})$. We define $S'_1 = S' \cup \{q'\}$ and $T_1(p) = T(p)$ for $p \in S$ and $T_1(q) = q'$. Take any element $x \in E_S$. Since $\Re$ is regular, then there exists an element $x' \in E_{S'}$ such that $\tau_S(\bar{x}) = \overline{x'}$. Since $i_{S_1}(x) = [\bar{x}, i_q(x)] \in i_{S_1}(E_{S_1})$, then according to lemma 1.1 $\beta_{S_1}\left([\bar{x}, i_q(x)], [\bar{q}, i_q(q)]\right) =$ $= \beta_S(\bar{x}, \bar{q}) + \beta_q\left(i_q(x), i_q(q)\right) = 0$. Similarly $i_{S'_1}(x') = [\overline{x'}, i_{q'}(x')] \in i_{S'_1}(E_{S'_1})$, hence according to lemma 1.1 $\beta_{S'_1}\left([\overline{x'}, i_{q'}(x')], [\overline{q'}, i_{q'}(q')]\right) = \beta_{S'}(\overline{x'}, \overline{q'}) + \beta_{q'}\left(i_{q'}(x'), i_{q'}(q')\right) =$ $= 0$. Using the first formula and the fact that τ_S maps isometrically the space (G_S, β_S) into $(G_{S'}, \beta_{S'})$ we get $\beta_q(x, q) = \beta_S(\bar{x}, \bar{q}) = \beta_{S'}\left(\tau_S(\bar{x}), \tau_S(\bar{q})\right) = \beta_{S'}(\bar{x}, \overline{aq'})$. Using again lemma 1.1 for elements $x', a \in E_{S'}$ and the second formula above we get $\beta_{S'}(\bar{x}', \overline{aq'}) = \beta_{S'}(\bar{x}', \bar{a}) + \beta_{S'}(\bar{x}', \bar{q}') = \beta_{S'}(\bar{x}', \bar{q}') = \beta_{q'}(\bar{x}', \bar{q}')$. In this way we have shown that

$$\beta_q(x, q) = \beta_{q'}(x', q'). \tag{1}$$

In particular for $x = -1$ we have $\beta_q(-1, q) = \beta_{q'}(-1, q')$, which means $\left(\frac{-1}{q}\right) = \left(\frac{-1}{q'}\right)$, which is equivalent to $q \equiv q' \pmod 4$. The last fact implies existing the local isomorphisms of groups of square classes of q-adic and q'-adic fields $\mathbb{Q}_q^*/\mathbb{Q}_q^{*2}$ and

$\mathbb{Q}_{q'}{}^*/\mathbb{Q}_{q'}{}^{*2}$. Let $t_q : \mathbb{Q}_q{}^*/\mathbb{Q}_q{}^{*2} \to \mathbb{Q}_{q'}{}^*/\mathbb{Q}_{q'}{}^{*2}$ be any tame local isomorphism. By definition t_q maps q-adic units to q'-adic units. Moreover since q is not a q-adic unit, then $t_q(q) \in \{q', u'q'\}$. We shall show that q, q' and t_q determine the extension $\Re_1$ of the small self-equivalence $\Re$. We have to show, that $E_S/\mathbb{Q}^{*2} = H_S \subseteq H_{S_1}$.

Since $\Re$ is regular, then the global isomorphism t_S determined by $\Re$ is defined on whole group $E_S/\mathbb{Q}^{*2}$. Take any element $x \in H_S = E_S/\mathbb{Q}^{*2}$. There are two cases possible: 1. if $t_q(q) = q'$, then $\beta_q(x,q) = \beta_{q'}(t_q(x), t_q(q)) = \beta_{q'}(t_q(x), q')$ and 2. if $t_q(q) = u'q'$, then $\beta_q(x,q) = \beta_{q'}(t_q(x), t_q(q)) = \beta_{q'}(t_q(x), u'q') = \beta_{q'}(t_q(x), u') + \beta_{q'}(t_q(x), q') = \beta_{q'}(t_q(x), q')$, because $t_q(x)$ and u' are q'-adic units. Therefore $\beta_{q'}(t_q(x), u') = 0$. Using the formula (1) for $x' = t_S(x)$ in both cases we get $\beta_{q'}(t_S(x), q') = \beta_{q'}(t_q(x), q')$ and consequently $t_S(x) = t_q(x)$ in the group $\mathbb{Q}_{q'}{}^*/\mathbb{Q}_{q'}{}^{*2}$. Therefore we have shown that $\tau_{S1}(i_{S1}(x)) = i_{S_1'}(t_S(x)) \in i_{S'}(E_{S'}/\mathbb{Q}^{*2})$, hence $x \in H_{S1}$. The defect of rational small self-equivalence $\Re_1$ is $\operatorname{def}(\Re_1) = \dim E_{S_1}/\mathbb{Q}^{*2} - \dim H_{S1} \le \dim E_{S_1}/\mathbb{Q}^{*2} - \dim H_S = |S_1| - |S| = 1$.

Now we will show that for properly chosen local isomorphism we will get a regular extension of small self-equivalence $\Re$. Assume that $\mathbb{Q}_q{}^*/\mathbb{Q}_q{}^{*2} = \{1, u, q, uq\}$ and $\mathbb{Q}_{q'}{}^*/\mathbb{Q}_{q'}{}^{*2} = \{1, u', q', u'q'\}$. We define the local isomorphism $t_q^\bullet : \mathbb{Q}_q{}^*/\mathbb{Q}_q{}^{*2} \to \mathbb{Q}_{q'}{}^*/\mathbb{Q}_{q'}{}^{*2}$ by $t_q^\bullet(u) = u'$ and $t_q^\bullet(q) = aq'$. The remaining values of $t_q^\bullet$ are uniquely determined: $t_q^\bullet(1) = 1$ and $t_q^\bullet(uq) = u'aq'$. We can see that $t_q^\bullet$ is tame. If a is a square in $\mathbb{Q}_{q'}$, then $t_q^\bullet$ is a simple local isomorphism, in the other case $t_q^\bullet$ is a skew local isomorphism.

It is easy to notice that $E_{S_1}/\mathbb{Q}^{*2} = E_S/\mathbb{Q}^{*2} \cup qE_S/\mathbb{Q}^{*2}$. In order to show that the small rational self-equivalence $\Re_1$ determined by $\Re$ and the elements q, q' and $t_q^\bullet$ is regular it suffices to check if $q \in H_{S1}$, that means if the extension t_{S_1} of global isomorphism t_S can be defined for element $q \in E_{S_1}/\mathbb{Q}^{*2}$. Easy calculation $\tau_{S_1}(i_{S_1}(q)) = \tau_{S_1}([\bar{q}, q]) = [\tau_S(\bar{q}), t_q^\bullet(q)] = [\overline{aq'}, aq'] = i_{S_1'}(aq') \in i_{S_1'}(E_{S_1'})$ shows that $t_{S_1}(q) = aq'$. In general $\tau_{S_1}(xq^e) = t_S(x)(aq')^e$ for all $x \in E_S$ and $e \in \{0,1\}$.

Lemma 2.3. *For every rational small self-equivalence $\Re = (S, T, \{t_p\}_{p \in S})$ with defect equal to 1 there exist prime numbers q, q'∈ ℙ and a local isomorphism $t_q : G_q \to G_{q'}$ such that the extension of $\Re$ determined by q, q', t_q is a regular small self-equivalence.*

Proof. Let us denote by $S' = T(S)$. Let t_S be a fixed global monomorphism determined by $\mathfrak{R}$. According to hypothesis dim $E_S/\mathbb{Q}^{*2}$ – dim H_S =1, hence there exists S-singular element x such that $\tau_S(\bar{x}) \notin i_{S'}(E_S/\mathbb{Q}^{*2})$. By lemma 1.1 it follows that $i_{S'}(E_{S'}/\mathbb{Q}^{*2})$ equals to its orthogonal completion, hence every element, which does not belong to this set can not be orthogonal to all its elements. This means that there exists S'-singular element $y \in \mathbb{Q}^*$ such that $\beta_{S'}(\tau_S(\bar{x}), \bar{y}) = 1$.

For any $z \in E_S$ we have $\beta_{S'}(\tau_S(\bar{x}), \tau_S(\bar{z})) = \beta_S(\bar{x}, \bar{z}) = 0$, hence $y \notin H_{S'}$. Next we have $\beta_S(\tau_S^{-1}(\bar{y}), \bar{x}) = \beta_{S'}(\bar{y}, \tau_S(\bar{x})) = 1$, thus $\tau_S^{-1}(\bar{y}) \notin i_S(E_S/\mathbb{Q}^{*2})$. By lemma 2.1 there exists a prime number $q \notin S$ and the number $a \in E_S$, such that $\overline{aq} = \tau_S^{-1}(\bar{y})$. Similarly there exists a prime number $q' \notin S'$ and the number $a' \in E_{S'}$, such that $\overline{a'q'} = \tau_S(\bar{x})$. We define two sets $S_1 = S \cup \{q\}$ and $S_1' = S' \cup \{q'\}$. First we notice that if $z\mathbb{Q}^{*2} \in H_S$, then $z \in \mathbb{Q}_q{}^{*2}$. In fact, since z and aq are S_1-singular elements, therefore by lemma 1.1 it follows that $\beta_S(\bar{z}, \overline{aq}) = 0$ and consequently we get $\beta_q(z, aq) = \beta_S(\bar{z}, \overline{aq}) = \beta_S(\bar{z}, \tau_S^{-1}(\bar{y})) = \beta_{S'}(\tau_S(\bar{z}), \bar{y}) = 0$. The last equality follows from $\tau_S(\bar{z}), \bar{y} \notin i_{S'}(E_S/\mathbb{Q}^{*2})$. Since z is q-adic unit modulo $\mathbb{Q}^{*2}$, hence by equalities $v_q(aq) = 1$ and $\beta_q(z, aq) = 0$ it follows that $z \in \mathbb{Q}_q{}^{*2}$.

Analogously taking any S'-singular element z' such that $z'\mathbb{Q}^{*2} \in H_{S'}$ and using equalities $\beta_{q'}(z', aq') = \beta_{S'}(\bar{z}, \tau_S(\bar{x})) = \beta_S(\tau_S^{-1}(z'), \bar{x}) = 0$ we find that $z' \in \mathbb{Q}_q{}^{*2}$. Since $-1 \in H_S$ and $-1 \in H_{S'}$, thus in particular it follows that $-1 \in \mathbb{Q}_q{}^{*2}$ and $-1 \in \mathbb{Q}_{q'}{}^{*2}$. This shows that $q, q' \in \mathbb{P}_1$.

We extend the small self-equivalence $\mathfrak{R}$ to equivalence $\mathfrak{R}_1 = (S_1, T_1, \{t_p\}_{p \in S_1})$ by extending bijection T to the set S_1 and setting $T_1(q) = q'$. It remains to define a local isomorphism $t_q : \mathbb{Q}_q{}^*/\mathbb{Q}_q{}^{*2} \to \mathbb{Q}_{q'}{}^*/\mathbb{Q}_{q'}{}^{*2}$. Let u be a q-adic unit such that $\beta_q(u, aq) = 1$ and let u' be a q'-adic unit such that $\beta_{q'}(u', a'q') = 1$. The classes of squares of elements u and aq make the basis of $\mathbb{Q}_q{}^*/\mathbb{Q}_q{}^{*2}$ and the classes of squares of elements u' and $a'q'$ make the basis of $\mathbb{Q}_{q'}{}^*/\mathbb{Q}_{q'}{}^{*2}$. We define the isomorphism t_q by $t_q(u) = a'q'$, $t_q(aq) = u'$.

Since -1 is a square in fields $\mathbb{Q}_q$ and $\mathbb{Q}_{q'}$ it follows that every group isomorphism mapping the group $\mathbb{Q}_q{}^*/\mathbb{Q}_q{}^{*2}$ into $\mathbb{Q}_{q'}{}^*/\mathbb{Q}_{q'}{}^{*2}$ preserves Hilbert symbols, thus in particular for t_q defined above we have $(x, y)_q = (t_q(x), t_q(y))_{q'}$ for all x, y $\in \mathbb{Q}_q{}^*/\mathbb{Q}_q{}^{*2}$. By adding t_q to the family of local isomorphisms determined by the small self-equivalence $\mathfrak{R}$ we finish the construction of small self-equivalence $\mathfrak{R}_1$.

It suffices to show that $\Re_1$ is an extension of $\Re$. Notice that $H_S \subset H_{S_1}$. In fact, let $z\mathbb{Q}^{*2} \in H_S$ and let $t_S(z) = z'$, that means $\tau_S(\bar{z}) = \bar{z'}$. Then $z'\mathbb{Q}^{*2} \in H_{S'}$. Since $z = 1$ in group $\mathbb{Q}_q^*/\mathbb{Q}_q^{*2}$ and $z' = 1$ in $\mathbb{Q}_{q'}^*/\mathbb{Q}_{q'}^{*2}$, then $t_q(z) = z'$ and it follows $\tau_{S_1}(\bar{z}) = \bar{z'}$ in G_{S_1} and consequently $z\mathbb{Q}^{*2} \in H_{S_1}$.

It follows by above argumentation that if $z\mathbb{Q}^{*2} \in H_S$, then $\tau_{S_1}(\bar{z}) = \overline{\tau_S(z)}$. Therefore the global monomorphism t_{S_1} for small self-equivalence $\Re_1$ is an extension of t_S. This finishes the proof that $\Re_1$ is an extension of $\Re$.

Now we shall show, that the square classes of elements x and aq are in H_{S_1}. Since x and aq are S_1-singular, then by lemma 1.1 we get equality $\beta_{S_1}(\bar{x}, \overline{aq}) = 0$. Thus we have $\beta_q(x, aq) = \beta_S(\bar{x}, \overline{aq}) = \beta_S(\bar{x}, \tau_S^{-1}(\bar{y})) = \beta_{S'}(\tau_S(\bar{x}), \bar{y}) = 1$, hence $x = u$ in group $\mathbb{Q}_q^*/\mathbb{Q}_q^{*2}$. By definition of t_q we have $t_q(x) = a'q'$. With the fact $\tau_S(\bar{x}) = \overline{a'q'}$ we get $\tau_{S_1}(\bar{x}) = \overline{a'q'}$ in $G_{S_1'}$. Now since $a'q' \in E_{S_1'}/\mathbb{Q}_q^{*2}$, then $x\mathbb{Q}^{*2} \in H_{S_1}$. Similarly y and $a'q'$ are S_1'-singular, then we have $\beta_{q'}(y, a'q') = \beta_{S'}(\bar{y}, \overline{a'q'}) = \beta_{S'}(\bar{y}, \tau_S(\bar{x})) = \beta_{S'}(\tau_S(\bar{x}), \bar{y}) = 1$. Therefore $y = u'$ in the group $\mathbb{Q}_{q'}^*/\mathbb{Q}_{q'}^{*2}$ and by the definition of isomorphism t_q we have $aq = t_q^{-1}(u') = t_q^{-1}(y)$. On the other hand $\overline{aq} = \tau_S^{-1}(\bar{y})$, hence we get $\overline{aq} = \tau_{S_1}^{-1}(\bar{y})$ in G_{S_1}. The element y is S-singular, thus it is S_1-singular too, hence $aq\mathbb{Q}^{*2} \in H_{S_1}$. As a consequence we get the inclusion $H_S \cup \{x\mathbb{Q}^{*2}, aq\mathbb{Q}^{*2}\} \subset H_{S_1}$.

By definition of elements x, aq it follows that $x\mathbb{Q}^{*2} \in E_S/\mathbb{Q}^{*2} \setminus H_S$ and $aq\mathbb{Q}^{*2} \notin E_S/\mathbb{Q}^{*2}$, hence $\dim H_{S_1} \geq \dim H_S + 2$. The set S_1 was constructed by adding one prime number to the set S, thus $\dim E_{S_1}/\mathbb{Q}^{*2} = \dim E_S/\mathbb{Q}^{*2} + 1$. Finally we get inequality $\operatorname{def}\Re_{S_1} = \dim E_{S_1}/\mathbb{Q}^{*2} - \dim H_{S_1} \leq (\dim E_S/\mathbb{Q}^{*2} + 1) - (\dim H_S + 2) = \dim E_S/\mathbb{Q}^{*2} - \dim H_S - 1 = \operatorname{def}\Re_S - 1 = 0$.

This finishes the proof of regularity of the rational small self-equivalence $\Re_{S_1}$.

Theorem 2.4. *For every subset $A \subseteq \mathbb{P}_3$ there exists a rational self-equivalence (T,t) such that induced local isomorphism $t_q : \mathbb{Q}_q^*/\mathbb{Q}_q^{*2} \to \mathbb{Q}_{T(q)}^*/\mathbb{Q}_{T(q)}^{*2}$ is simple (i. e. it fulfills condition $t_q(q\mathbb{Q}_q^{*2}) = T(q)\mathbb{Q}_{T(q)}^{*2}$) if and only if $q \in A$.*

Proof. The rational self-equivalence will be constructed on some fixed small rational self-equivalence defined on the set $S = \{\infty, 2\}$ by adding suitable prime numbers. On each step of construction we have to control local isomorphisms as-

sociated to prime numbers from $\mathbb{P}_3$. If starting small-equivalence is not regular, then by lemma 2.3 it can be extended to a regular small self-equivalence on the set S enlarged with one prime number from the set $\mathbb{P}_1$. The small self-equivalence obtained in such a way we denote by $\Re_0 = (S_0, T_0, \{t_p\}_{p\in S_0})$.

Assume that after m-th step we get a regular small self-equivalence $\Re_m = (S_m, T_m, \{t_p\}_{p\in S_m})$.

Step A. Let q be the smallest prime number such that $q \notin S_m$. If $q \in \mathbb{P}_1$, then by lemma 2.2 there exists a prime number $q' \in T_m(S_m)$ such that with the proper choice of local isomorphism t_q the extension $\Re_{m+1}$ of the small self-equivalence $\Re_m$ determined by q, q' and t_q will be a regular small self-equivalence.

If $q \in \mathbb{P}_3$, then by lemma 2.2 $\Re_m$ can be extended to some small self-equivalence $\Re_*$ with any choice of local isomorphism t_q. Therefore if $q \in A$, then we assume that t_q is a simple local isomorphism and in the other case we choose a skew local isomorphism for t_q. If the obtained extension is regular, then we take $\Re_{m+1} = \Re_*$ and we go to the next step. If the defect of small self-equivalence $\Re_*$ equals 1, then by lemma 2.3 by adding suitable chosen prime numbers $q, q' \in \mathbb{P}_1$ we get some regular small self-equivalence, which we denote by $\Re_{m+1}$.

Step B. We proceed as before with small self-equivalence inverse to $\Re_{m+1}$, which we denote $\Re' = (S', T', \{t'_{p'}\}_{p'\in S'})$. We choose the smallest prime number $q' \notin S'$. As previously if $q' \in \mathbb{P}_1$, then adding q' and properly chosen prime number $q \in \mathbb{P}_1 \setminus T'(S')$ to $\Re'$ and suitable local isomorphism we get regular small self-equivalence $\Re''$.

If $q' \in \mathbb{P}_3 \setminus S'$, then there exists a prime number $q \in \mathbb{P}_3 \setminus T'(S')$ which for any local isomorphism $t'_{q'} : G_{q'} \to G_q$ gives the extension of small self-equivalence $\Re'$ with a defect equal to 1. Similarly as before we choose a simple local isomorphism if $q \in A$ and we choose a skew isomorphism in the other case. If the obtained extension is not regular, then by adding properly chosen prime numbers from $\mathbb{P}_1$ to the sets S' and $T'(S')$ we get a regular small self-equivalence. Regular small self-equivalence $\Re''$ obtained in this step is an extension of small self-equivalence inverse to $\Re_{m+1}$. The small self-equivalence inverse to $\Re''$ we denote by $\Re_{m+2}$ and go to step A. Of course the small self-equivalence $\Re_{m+2}$ is an extension of $\Re_{m+1}$.

Continue this procedure we get one-to-one bijection of the set $\mathbb{P}$ into itself. In order to define an automorphism t of the group of square classes $\mathbb{Q}^*/\mathbb{Q}^{*2}$ notice that every regular small self-equivalence $(S_m, T_m, \{t_p\}_{p\in S_m})$ defines isomorphism $t_{S_m} : E_{S_m}/\mathbb{Q}^{*2} \to E_{S'_m}/\mathbb{Q}^{*2}$ preserving Hilbert symbols. Every nonzero rational

number a is a finite product of prime numbers with integer exponents, hence $a \in E_{S_m}$ for some $m \in \mathbb{N}$. It suffices to assume that $t(a\mathbb{Q}^{*2}) = t_{S_m}(a\mathbb{Q}^{*2})$. It is obvious that the value of $t(a\mathbb{Q}^{*2})$ does not depend on the choice of m. In fact, assume that $a \in E_{S_{m_1}}$ and $a \in E_{S_{m_2}}$. We can assume that $m_1 \le m_2$. Then $E_{S_{m_1}} \subseteq E_{S_{m_2}}$ and by the fact that $t_{S_{m_2}}$ is an extension of $t_{S_{m_1}}$ we have $t_{S_{m_2}}(a\mathbb{Q}^{*2}) = t_{S_{m_1}}(a\mathbb{Q}^{*2})$.

We have shown that the pair (T,t) is a rational self-equivalence.

Theorem 2.5. The group of strong automorphisms of Witt rings of rational numbers is uncountable.

Proof. It known (as follows from [1], [3] and [7]) that there exists one-to-one correspondence between rational self-equivalences and strong automorphisms of Witt rings (comp. [1],[3] and [7]). On the other hand every rational self-equivalence uniquely determines the set of this prime numbers with simple local isomorphisms. Since every subset (from the uncountably family of subsets) of $\mathbb{P}_3$ is a set of prime numbers, which induces simple local isomorphisms, hence the group of strong automorphisms of Witt ring W($\mathbb{Q}$) is uncountable.

References

[1] Czogała A., On reciprocity equivalence of quadratic number fields, Acta Arith. 1981, 58 (1), 27-46.

[2] Czogała A., Hilbert-symbol equivalence of global fields, Prace Naukowe Uniwersytetu Śląskiego w Katowicach vol. 1969, Wyd. Uniwersytetu Śląskiego, Katowice 2001 (in Polish).

[3] Czogała A., Hilbert-symbol equivalence of global function fields, Mathematica Slovaca 2001, 51, 4, 383-401.

[4] Browkin J., Field theory, Biblioteka Matematyczna 49, PWN, Warsaw 1978 (in Polish).

[5] Cassels J.W.S., Fröhlich A. (ed.), Algebraic Number Theory, Academic Press, London, New York 1967.

[6] Serre J.-P., A Course in Arithmetic, Springer-Verlag, New York, Heidelberg, Berlin 1973.

[7] Stępień M., A construction of infinite set of rational self-equivalences, Scientific Issues. Mathematics, XIV: 117-132, Jan Długosz University, Częstochowa 2009.

[8] Marshall M., Abstract Witt Rings, volume 57 of Queen's Papers in Pure and Applied Math. Queen's University, Ontario 1980.

[9] Stępień M. R., Automorphisms of Witt rings and quaternionic structures, Scientific Research of the Institute of Mathematics and Computer Science Częstochowa University of Technology 2011, 1(10), 231-237.