JAM CM Journal of Applied Mathematics and Computational Mechanics 2015, 14(3), 109-119
www.amcm.pcz.pl p-ISSN 2299-9965
DOI: 10.17512/jamcm.2015.3.12 e-ISSN 2353-0588

AUTOMORPHISMS OF WITT RINGS OF LOCAL TYPE

Marcin Ryszard Stępień

Department of Mathematics and Physics, Kielce University of Technology
Kielce, Poland
mstepien@tu.kielce.pl

Abstract. We present a description of the group of strong automorphisms of Witt rings of local type (Witt rings of local fields) using quaternionic structures.

Keywords: *quadratic forms, Witt ring, quaternionic structures*

1. Introduction

The Witt ring of quadratic forms with coefficients in a field is a fundamental notion in the theory of quadratic forms. Since 1937, when E. Witt introduced the notion in [1], Witt rings have been the subject of much research and their structure and properties are described in detail in numerous articles and books. It turns out that the structure and properties of Witt ring $W(K)$ depend strongly on the field K of coefficients of quadratic forms. Therefore the problem of classification of Witt rings with respect to the fields of their coefficients was one of the most interesting in the theory of quadratic forms. Two Witt rings $W(K)$ and $W(L)$ over the fields K and L respectively are called *strong isomorphic* (and the fields K and L are called *Witt equivalent*), if there exists a ring isomorphism $\varphi: W(K) \to W(L)$ which preserves the dimension of nonisotropic forms representing Witt classes, i.e. such that $\varphi(\langle a\rangle) = \langle b\rangle$. The problem of classification of fields with respect to Witt equivalence (and the classification of Witt rings) has been extensively studied since the early 70s of the twentieth century and the review of the results was presented in the book [2].

In this article we consider the problem of research of strong automorphisms of the Witt ring, that is strong isomorphisms, where $K = L$. The diversity of Witt rings causes that there was not found one universal description of automorphisms of any Witt ring, but the groups of strong automorphisms are described for many broad classes of Witt rings (cf. [3-10]). In the paper we present the description of the groups of strong automorphisms of Witt rings of local fields.

We refer to the concept of an abstract Witt ring defined by Marshall in [11] as an abstract equivalent of well-known Witt rings of quadratic forms, which have the same algebraic properties as the original object.

Definition 1.1. Following Marshall, a *Witt ring* is a pair $W = (R, G)$, where R is a commutative ring with unity 1 and G is a subgroup of the multiplicative group R^* which has exponent 2 and contains distinguished element -1 (where, as usual in a ring $-r$ denotes the additive inverse of r). Furthermore, the following axioms hold.
$\mathcal{W}_1$: G generates R additively.
$\mathcal{W}_2$: The following Arason-Pfister property holds for $k = 1$ and $k = 2$:
If $r = a_1 + a_2 + \cdots + a_n \in I^k$, where I denotes the fundamental ideal of R generated by elements $r = a + b$, $a, b \in G$, $n < 2^k$, then $r = 0$.
$\mathcal{W}_3$: If $a_1 + a_2 + \cdots + a_n = b_1 + b_2 + \cdots + b_n$ and $n \geq 3$, then $\exists_{a,b,c_3,\ldots,c_n \in G}$ such that $a_2 + \cdots + a_n = a + c_3 + \cdots + c_n$, $a_1 + a = b_1 + b$ (and, hence, $b_2 + \cdots + b_n = b + c_3 + \cdots + c_n$).

We will say that φ is a (*strong*) *isomorphism* of Witt rings $W_1 = (R_1, G_1)$ and $W_2 = (R_2, G_2)$ if $\varphi: R_1 \to R_2$ is a ring isomorphism such that $\varphi(G_1) = G_2$. A *strong automorphism of Witt ring* W is a strong isomorphism of W onto itself.

Since we will use quaternionic structures, below we recall the definition.

Definition 1.2. Let G be a group of exponent 2, i.e. $a^2 = 1$ for all $a \in G$ with distinguished element $-1 \in G$ and let us denote $-a = -1 \cdot a$. Let Q be the set with distinguished element θ and let $q: G \times G \to Q$ be a surjective map. The triplet (G, Q, q) is called a *quaternionic structure* if for every $a, b, c, d \in G$ the map q fulfills:
Q_1: $q(a, b) = q(b, a)$
Q_2: $q(a, -a) = \theta$
Q_3: $q(a, b) = q(a, c) \Rightarrow q(a, bc) = \theta$
Q_4 If $q(a, b) = q(c, d)$, then there exists such $x \in G$ that $q(a, b) = q(a, x)$ and $q(c, d) = q(c, x)$.

Two quaternionic structures (G_1, Q_1, q_1) and (G_2, Q_2, q_2) are *isomorphic* if there exists a group isomorphism $\sigma: G_1 \to G_2$ such that $\sigma(-1) = -1$ and $q_1(a, b) = \theta_1 \Rightarrow q_2\big(\sigma(a), \sigma(b)\big) = \theta_2$ for all $a, b \in G_1$. By *automorphism of a quaternionic structure* (G, Q, q) we understand any isomorphism $\sigma: (G, Q, q) \to (G, Q, q)$.

Now we shall present some definitions of notions of the theory of quadratic forms, which we will use in this paper.

Let (G, Q, q) be a quaternionic structure. A (*quadratic*) *form of dimension* $n \geq 1$ over G is *n*-tuple $f = (a_1, \ldots, a_n)$, where $a_1, \ldots, a_n \in G$. A form f of dimension 2 is called *binary form*. Two forms of dimension n are called *equivalent* (or *isometric*) if:
(1) $n = 1$, $(a) \cong (b) \Leftrightarrow a = b$
(2) $n = 2$, $(a, b) \cong (c, d) \Leftrightarrow ab = cd$ and $q(a, b) = q(c, d)$
(3) $n > 2$, $(a_1, \ldots, a_n) \cong (b_1, \ldots, b_n) \Leftrightarrow \exists a, b, c_3, \ldots, c_n \in G$ such that $(a_2, \ldots, a_n) \cong (a, c_3, \ldots, c_n)$, $(a_1, a) \cong (b_1, b)$ and $(b_2, \ldots, ab_n) \cong (b, c_3, \ldots, c_n)$.

We say that form *f represents element* $a \in G$ if there exist $a_2, \dots, a_n \in G$, such that $f \cong (a, a_2, \dots a_n)$. We denote the set of all elements represented by form f (*value set of the form f*) by $D(f)$. We have $f \cong g \Rightarrow D(f) = D(g)$. Notice that there exists a formula that expresses the set of elements represented by binary form $(1, a)$ by means of quaternionic mapping, namely $b \in D(1, a) \Leftrightarrow q(a, b) = \theta$ ([11], p.74).

Let $W = (R, G)$ be an abstract Witt ring. According to [11, Theorem 4.5] Witt rings are in one-to-one correspondence with quaternionic structures. The natural one-to-one correspondence means that for every Witt ring $W = (R, G)$ there exists a quaternionic structure (G, Q, q) associated to it and conversely for given quaternionic structure (G, Q, q) one can construct related Witt ring $W = (R, G)$. This fact provides to use quaternionic structures in order to study properties of Witt rings when it is convenient. Let (G, Q, q) denote the quaternionic structure associated to Witt ring $W = (R, G)$. According to ([12, Theorem 2.1] the groups of strong automorphisms of Witt rings are isomorphic to the groups of all automorphisms of associated quaternionic structures (compare [11, Chapter 4, §1]).

Let $W = (R, G)$ be a Witt ring and let (G, Q, q) be the quaternionic structure associated to it. Then two forms $(a_1, \dots, a_n)$ and $(b_1, \dots, b_m)$ are equivalent if $a_1 + a_2 + \dots + a_n = b_1 + b_2 + \dots + b_m$ in R and $m = n$. In many situations there is more convenient to use forms instead elements of ring R.

Definition 1.3. We will say that quaternionic structure (G, Q, q) is of *local type* if the group G is finite and $|D(1, -a)| = \frac{1}{2}|G|$ for all $1 \neq a \in G$. The Witt ring $W = (R, G)$ associated to quaternionic structure (G, Q, q) of local type will be called a *Witt ring of local type*.

Witt rings of local type are realized by local fields, especially by p-adic fields $\mathbb{Q}_p$ and their finite extensions. More information about local fields, quadratic forms with coefficients in local fields and about structures of Witt rings of local type the reader can find in books [11] and [13-15].

It follows that in the case of Witt ring $W = (R, G)$ of local type we can investigate automorphisms of associated quarternionic structure (G, Q, q) instead of strong automorphisms of Witt ring W.

In this paper we present a complete description of groups of strong automorphisms of all kinds of Witt rings of local type. We use one-to-one correspondence between strong automorphisms of Witt rings of local type and isometries of bilinear spaces over two-element field $\mathbb{F}_2$ created by quaternionic structures associated to that Witt rings. Quaternionic structures corresponding to Witt rings of local type create three different types of bilinear spaces over $\mathbb{F}_2$ with respect to properties of quaternionic map q treated as a bilinear functional. In each of these cases we give description of group of isometries of suitable bilinear space, which is equivalent that we get description of groups of strong automorphisms of Witt rings of local type.

Remark 1.4. According to above definition the Witt ring $(\mathbb{Z},\{1,-1\})$, which is isomorphic to the Witt ring $W(\mathbb{R})$ of the field of real numbers is a Witt ring of local type, since $D(1,1)=\{1\}$.

2. Quaternionic structures associated to Witt rings of local type as bilinear spaces

If (G,Q,q) is a quaternionic structure of a local type, then $|G|=2^n$ and the value set of quaternionic map q can be viewed as two-element field $\mathbb{F}_2$. It follows from axioms of quaternionic structure that the quaternionic map q is bilinear (cf. [11, Chapter 2, §1]), hence q is nonsingular bilinear functional in vector space G over the field $\mathbb{F}_2$ ([11, Chapter 5, §3]). Therefore automorphisms of quaternionic structure associated to a Witt ring of local type can be treated as isometries of nonsingular bilinear space over $\mathbb{F}_2$ of dimension n, i.e. vector space with nonsingular bilinear functional q.

Although the group G has multiplicative notation, from now in the paper it will be more convenient to use additive operation in G in order to emphasize the function of G as a bilinear space. Let V be a finitely generated bilinear space over the two-element field $\mathbb{F}_2$ and let $\beta: V\times V\to\mathbb{F}_2$ be a symmetrical and nonsingular bilinear functional. The pair (V,β) is a nonsingular bilinear space. If U is a subspace of V, then the restriction $\beta\restriction_{U\times U}$ we denote by β_U. Let $\operatorname{rad}V$ denote the *radical of bilinear space* V defined as $\operatorname{rad}V=\{w\in V:\beta(w,u)=0 \text{ for all } u\in V\}$ (compare [2]).We shall prove that $(V,\mathbb{F}_2,\beta)$ is a quaternionic structure of local type (see Corollary 2.2).

Theorem 2.1. *Let (V,β) be a nonsingular bilinear space over the field $\mathbb{F}_2$ and let $\dim V=n$. Then:*
1. $U=\{u\in V:\beta(u,u)=0\}$ is a subspace of V and $\dim U\geq n-1$.
2. There exists exactly one element $\hat{v}\in V$ such that

$$\beta(v,\hat{v}+v)=0 \tag{1}$$

for all $v\in V$.
3. $U^{\perp}=lin(\hat{v})$.
4. For every isometry σ of space (V,β) it holds $\sigma(U)=U$ and $\sigma(\hat{v})=\hat{v}$.

Proof: 1. We define a quadratic map $\varphi: V\to\mathbb{F}_2$ by $\varphi(v)=\beta(v,v)$ (the quadratic form determined by a functional β). Take

$$\varphi(v_1+v_2)=\beta(v_1,v_1)+\beta(v_1,v_2)+\beta(v_2,v_1)+\beta(v_2,v_2)=\varphi(v_1)+\varphi(v_2).$$

Homogeneity of the map φ is obvious in view of the field structure, hence the map φ is a linear functional.

Let $v \in \ker\varphi$, this is to say $\varphi(v) = 0$, and that is equivalent to $\beta(v,v) = 0$ or $U = \ker\varphi$. On the other hand, $\ker\varphi$ is a subspace of the vector space V and $\dim V = \dim\ker\varphi + \dim\operatorname{im}\varphi$ holds. There are two possible cases:
a) $\operatorname{im}\varphi = \{0\}$. Then $U = \ker\varphi = V$, hence $\dim U = n$ and the functional β is alternating.
b) $\operatorname{im}\varphi = \mathbb{F}_2$. Then $\dim\operatorname{im}\varphi = 1$ and it follows $\dim U = \dim\ker\varphi = n - 1$.

2 and 3. We start from showing the uniqueness of element $\hat{v}$ holding (1). Suppose that the elements $\hat{u}, \hat{v} \in V$ fulfill $\beta(v, \hat{u} + v) = 0$ and $\beta(v, \hat{v} + v) = 0$ for every $v \in V$. Then

$$\beta(v, \hat{u} + \hat{v}) = \beta(v, (\hat{u} + v) + (\hat{v} + v)) = \beta(v, \hat{u} + v) + \beta(v, \hat{v} + v) = 0$$

for every $v \in V$. Since the functional β is nonsingular, it follows that $\hat{u} + \hat{v} = 0$, thus $\hat{u} = \hat{v}$.

The proof of existence requires a few cases. If $\dim U = n$, then β is an alternating functional, thus $\hat{v} = 0$ fulfills (1). Since functional β is nonsingular, therefore $U^{\perp} = 0 = \operatorname{lin}\{0\}$.

Suppose that $\dim U = n - 1$. We assume that $\hat{v}$ is a nonzero element in subspace $U^{\perp}$. Of course $\operatorname{lin}(\hat{v}) = U^{\perp}$, since $\dim U^{\perp} = 1$ (by the dimension theorem 5.2.1 in [2]). Notice that if $u \in U$, then $\beta(u, \hat{v} + u) = \beta(u, \hat{v}) + \beta(u, u) = 0 + 0 = 0$.

If the bilinear space (U, β_U), where β_U denotes the restriction of functional β to the subspace U, is nonsingular, then by the orthogonal complement theorem (cf. [2, Theorem 5.2.2]) we have $V = U \oplus U^{\perp}$. Therefore, if $v \in V \backslash U$, then there exists $u \in U$ such that $v = \hat{v} + u$, and it follows $\beta(v, \hat{v} + v) = \beta(\hat{v} + u, \hat{v} + \hat{v} + u) = \beta(\hat{v} + u, u) = 0$.

If the bilinear space (U, β_U) is singular, then $U^{\perp} \subseteq U$. By the fact that the functional β is nonsingular on V it follows that $(U^{\perp})^{\perp} = U$, that means $\beta(v, \hat{v}) = 1$ for all $v \in V \setminus U$. Therefore $\beta(v, \hat{v} + v) = \beta(v, \hat{v}) + \beta(v, v) = 1 + 1 = 0$. Hence in both cases $\hat{v}$ fulfills (1).

4. Let $\hat{v}$ be the element holding (1). If σ is an isometry of bilinear space (V, β), then $\beta(\sigma(v), \sigma(\hat{v}) + \sigma(v)) = 0$ for all $v \in V$. It shows that $\sigma(\hat{v})$ also fulfills (1), hence by the uniqueness of element $\hat{v}$ it follows that $\sigma(\hat{v}) = \hat{v}$.

In the sequel we assume that the bilinear space (V, β) is nonsingular, the set of all isotropic vectors in V we will denote by U, and the unique element fulfilling (1) will be denoted by $\hat{v}$.

Recall that for every $v \in V$ the mapping $\beta(v,\cdot): V \to \mathbb{F}_2$ such that $x \to \beta(v, x)$ for all $x \in V$ is a linear functional. If $v \neq 0$, then $\ker\beta(v,\cdot) = \{x \in V: \beta(v, x) = 0\}$ is a subspace of V with dimension $\dim V - 1$. Of course $\beta(0,\cdot)$ is zero functional.

Corollary 2.2. *If* (V,β) *is nonsingular bilinear space over two-element field* $\mathbb{F}_2$ *and* $\dim V < \infty$, *then* $(V,\mathbb{F}_2,\beta)$ *is a quaternionic structure of local type and* $\mathrm{Aut}(V,\mathbb{F}_2,\beta) = Izom(V,\beta)$ *where* $Izom(V,\beta)$ *denotes the group of all isometries of bilinear space* (V,β).

Proof: First we shall show that the axioms $Q_1 - Q_4$ of the definition of quaternionic structure are fulfilled.

The condition Q_1 (symmetry) is fulfilled, since the bilinear functional β is symmetrical.

The condition Q_2 follows by the theorem 2.1 §2. The vector $\hat{v}$ is the distinguished element of the group V in the quaternionic structure $(V,\mathbb{F}_2,\beta)$.

In order to show the condition Q_3 (weak bilinearity) it suffices to notice that by bilinearity of functional β the equality $\beta(x,y) = \beta(x,z)$ holds if and only if $\beta(x,y+z) = 0$ for all $x,y,z \in V$.

It remains to check the condition Q_4 (linkage): if $\beta(u,y) = \beta(w,z)$, then there exists an element $x \in V$ such that $\beta(u,y) = \beta(u,x)$ and $\beta(w,z) = \beta(w,x)$. Let us consider two cases. If $\beta(u,y) = \beta(w,z) = 0$, then it suffices to set $x = 0$. If $\beta(u,y) = \beta(w,z) = 1$, then vectors u,w are nonzero. Let us denote $T = \ker\beta(u,\cdot)$ and $W = \ker\beta(w,\cdot)$. By nonsingularity of functional β it follows that $|T| = |W| = 2^{n-1}$. Therefore $y \notin T$ and $z \notin W$, hence $0 \notin (y+T) \cup (z+W)$. It follows that $|(y+T) \cap (z+W)| = |(y+T)| + |z+W| - |(y+T) \cup (z+W)| \geq 2 \cdot 2^{n-1} - (2^n - 1) = 1$. This shows that there exists $x \in (y+T) \cap (z+W)$. With such a choice of element x there exist $t_1 \in T$ and $t_2 \in W$ such that $x = y + t_1$ and $x = z + t_2$. Then $\beta(u,x) = \beta(u,y+t_1) = \beta(u,y) + \beta(u,t_1) = \beta(u,y)$. Similarly $\beta(w,x) = \beta(w,z+t_2) = \beta(w,z)$, hence Q_4 holds, which finishes the proof that $(V,\mathbb{F}_2,\beta)$ is a quaternionic structure.

According to [1] $q(a,b) = 0 \Leftrightarrow 1 - a = b(1-a) \Leftrightarrow b \in D(1-a)$ for every quaternionic structure (G,Q,q) (compare [1, Ch. 4 §3, p. 74]). It follows that the value set of binary form $(0,\hat{v}+v)$ equals to $\ker\beta(v,\cdot)$, therefore for all $v \neq 0$ it has 2^{n-1} elements. This shows that $(V,\mathbb{F}_2,\beta)$ is the quaternionic structure of local type.

3. Groups of isometries of bilinear spaces created by quaternionic structures of local type

In theorem below we use the notion of a *symplectic group*, i.e. the group of isometries of nonsingular alternating space. One can find more about properties of symplectic groups over finite fields in the book by E. Artin [16].

Theorem 3.1. *Suppose that* $(V,\mathbb{F}_2,\beta)$ *is a quaternionic structure and the dimension of* V *as a vector space over* $\mathbb{F}_2$ *equals to* $\dim V = n$.
1. If n *is odd number, then the functional* β *is not alternating and*

$$Aut(V, \mathbb{F}_2, \beta) \cong Sp(n-1, \mathbb{F}_2)$$

2. If n is an even number and the functional β is alternating, then

$$Aut(V, \mathbb{F}_2, \beta) \cong Sp(n, \mathbb{F}_2)$$

3. If n is an odd number and the functional β is not alternating then the group $Aut(V, \mathbb{F}_2, \beta)$ is isomorphic to the group $(U \times Sp(n-2, \mathbb{F}_2), *)$, with operation $*$ defined by

$$(u_2, \bar{\tau}_2) * (u_1, \bar{\tau}_1) = (w, \bar{\tau}_2 \bar{\tau}_1),$$

where w is an element of subspace U determined by u_1, u_2 and $\bar{\tau}_2$ (see (2)).

Proof: 1. If the dimension of the space is odd and the functional is nonsingular, then the functional cannot be alternating, since by [2, Corollary 6.2.3] the dimension is the only invariant needed to classify nonsingular alternating spaces up to isometry. Therefore $\dim U = n-1$ and the functional β_U is alternating. Suppose that the functional β_U is singular. Then $\operatorname{rad} U = U^{\perp} \cap U$ is not trivial, thus $1 \leq \dim \operatorname{rad} U \leq \dim U^{\perp} = 1$. By [2, Theorem 5.3.1] $U = U_1 \oplus \operatorname{rad} U$ for some nonsingular subspace U_1 contained in U. This is a contradiction, since U_1 is nonsingular alternating space with odd dimension. Therefore U is alternating nonsingular space and $V = U \oplus U^{\perp}$ and by theorem 2.1 we have $U^{\perp} = \{0, \hat{v}\}$.

By the corollary 2.2 the group of all automorphisms of a quaternionic structure is isomorphic to the group of isometries of bilinear space (V, β). If σ is an isometry of the space (V, β), then by theorem 2.1 §4 we have $\sigma(U) = U$ for the subspace U, hence the restriction $\sigma \restriction_U$ is an isometry of space (U, β_U). Therefore we get the map $\operatorname{Izom}(V, \beta) \to \operatorname{Izom}(U, \beta_U) \cong Sp(n-1, \mathbb{F}_2)$. It is obvious that such a map is a group homomorphism. Since the subspace (U, β_U) is nonsingular, then $V = \operatorname{lin}(\hat{v}) \oplus U$. Every element $v \in V$ can be expressed in form $v = a\hat{v} + u$, where $a \in \mathbb{F}_2$ and $u \in U$. If $\sigma \restriction_U$ is an identity map, then $\sigma(a\hat{v} + u) = a\sigma(\hat{v}) + \\ + \sigma(u) = v$, thus σ is identity map, hence the mapping is a monomorphism. Moreover, every isometry $\tau \in \operatorname{Izom}(U, \beta_U)$ can be uniquely extended to the isometry of the space (V, β) defined by $\sigma(a\hat{v} + u) = a\hat{v} + \tau(u)$. Therefore $Aut(V, \mathbb{F}_2, \beta) = \\ = \operatorname{Izom}(V, \beta) \cong \operatorname{Izom}(U, \beta_U) = Sp(n-1, \mathbb{F}_2)$.

2. It follows by corollary 2.2.

3. If n is an even number and the functional β is not alternating, then similarly as in the first case $\dim U = n-1$, i.e. the subspace U has odd dimension, thus it is singular. By theorem 2.1 we have $\hat{v} \in U^{\perp} \subseteq U$. Moreover, $(U^{\perp})^{\perp} = U$ hence $\beta(v, \hat{v}) = 1$ for all $v \in V \setminus U$. If $v \in V \setminus U$ and $W = \operatorname{lin}(v, \hat{v})$, then the matrix of bilinear functional $\beta_W : W \times W \to \mathbb{F}_2$ (which is the restriction of β to the subspace W) relative to the basis $(v, \hat{v})$ has the following form $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, hence the subspace W is nonsingular.

Consider the quotient space $\overline{U} = U/U^{\perp}$ and the canonical epimorphism $\kappa\colon U \to \overline{U}$ defined by $\kappa(u) = u + U^{\perp}$. Notice that $u + U^{\perp} = \{u, u + \hat{v}\}$. Since $\beta(u_1 + a_1\hat{v}, u_2 + a_2\hat{v}) = \beta(u_1, u_2)$ for all $u_1, u_2 \in U$ and $a_1, a_2 \in \mathbb{F}_2$, hence the alternating bilinear functional β_U induces the natural alternating functional $\bar{\beta}\colon \overline{U} \times \overline{U} \to \mathbb{F}_2$ defined by $\bar{\beta}(u_1 + U^{\perp}, u_2 + U^{\perp}) = \beta_U(u_1, u_2)$ for all $u_1, u_2 \in U$. Similarly, every isometry τ of the space U uniquely induces the isometry $\bar{\tau}$ of bilinear space $(\overline{U}, \bar{\beta})$ defined by $\bar{\tau}(u + U^{\perp}) = \bar{\tau}(u) + U^{\perp}$. Of course $\bar{\tau} \in \mathrm{Izom}(\overline{U}, \bar{\beta}) \cong Sp(n-2, \mathbb{F}_2)$. For every subspace $W \subseteq U$ such that $U = U^{\perp} \oplus W$ we have $W \cap \ker\kappa = W \cap U^{\perp} = \{0\}$, hence the restriction of canonical epimorphism $\kappa\restriction_W\colon W \to \overline{U}$ is an isometry of bilinear spaces.

Now we shall show that with arbitrary element $v_0 \in V \setminus U$ there exists a bijection Φ between the set of all isometries of space (V, β) and the set $U \times \mathrm{Izom}(\overline{U}, \bar{\beta})$. For an isometry σ of the space (V, β) we assume that $u = \sigma(v_0) + v_0$. Since U is a subgroup of the group V with index 2 and $\sigma(v_0), v_0 \notin U$ hence $u \in U$. Moreover, we have $\sigma(U) = U$, thus $\tau = \sigma\restriction_U$ is an isometry of alternating space $U/\mathrm{rad}\, U$. The map τ uniquely determines an isometry $\bar{\tau}$ of space $(\overline{U}, \bar{\beta})$. It is easy to show that the mapping $\sigma \to \bar{\tau}$ is a homomorphism of the groups $\mathrm{Izom}(V, \beta)$ and $Sp(\overline{U}, \bar{\beta})$. In this way we define $\Phi(\sigma) = (\mathrm{u}, \bar{\tau})$.

Conversely for each pair $(\mathrm{u}, \bar{\tau}) \in \mathrm{U} \times \mathrm{Izom}(\overline{U}, \bar{\beta})$ we will define an isometry σ in the space V such that $\Phi(\sigma) = (u, \bar{\tau})$. Since the subspace $\mathrm{lin}(v_0, \hat{v})$ is nonsingular, hence $V = \mathrm{lin}(v_0, \hat{v}) \oplus U'$, where $U' = \mathrm{lin}(v_0, \hat{v})^{\perp}$. Similarly the subspace $\mathrm{lin}(v_0 + u, \hat{v})$ is nonsingular, hence $V = \mathrm{lin}(v_0 + u, \hat{v}) \oplus U''$, where $U'' = \mathrm{lin}(v_0 + u, \hat{v})^{\perp}$. The restrictions $\kappa' = \kappa\restriction_{U'}$ and $\kappa'' = \kappa\restriction_{U''}$ of the canonical map κ are isomorphisms of spaces. Therefore the map $\tau = \kappa''^{-1} \circ \bar{\tau} \circ \kappa'$ is an isometry mapping from the subspace U' to U''. It is easy to check that there exists exactly one isometry $\mu\colon \mathrm{lin}(v_0, \hat{v}) \to \mathrm{lin}(v_0 + u, \hat{v})$ such that $\mu(v_0) = v_0 + u$. Every vector of V can be uniquely expressed in the form $v = t + u$, where $t \in \mathrm{lin}(v_0, \hat{v})$ and $u \in U'$, hence the linear map σ can be uniquely defined by $\sigma(v) = \mu(t) + \tau(u)$. It suffices to show that σ is an isometry. Let us consider $v_1 = t_1 + u_1$ and $v_2 = t_2 + u_2$, where $t_1, t_2 \in \mathrm{lin}(v_0, \hat{v})$ and $u_1, u_2 \in U'$ hence $\beta(t_i, u_j) = 0$ and $\beta(\mu(t_i), \tau(u_j)) = 0$ for $i, j \in \{1,2\}$. We calculate

$\beta\big(\sigma(v_1), \sigma(v_2)\big) = \beta\big(\mu(t_1) + \tau(u_1), \mu(t_2) + \tau(u_2)\big) = \beta\big(\mu(t_1), \mu(t_2)\big) +$
$+\beta\big(\tau(u_1), \tau(u_2)\big) = \beta(t_1, t_2) + \beta(u_1, u_2) = \beta(t_1 + u_1, t_2 + u_2) = \beta(v_1, v_2).$

It is easy to check that $\Phi(\sigma) = (u, \bar{\tau})$.

In order to define an operation in $U \times \mathrm{Izom}(\overline{U}, \bar{\beta})$ let us consider two pairs $(u_1, \bar{\tau}_1)$, $(u_2, \bar{\tau}_2)$ and corresponding isometries σ_1 and σ_2, respectively. Then $\Phi(\sigma_2 \circ \sigma_1) = (w, \bar{\tau}_2 \circ \bar{\tau}_1)$, where $w = \sigma_2 \circ \sigma_1(v_0) + v_0 = \sigma_2(v_0 + u_1) + v_0 = = \sigma_2(v_0) + \sigma_2(u_1) + v_0 = v_0 + u_2 + \sigma_2(u_1) + v_0 = u_2 + \sigma_2(u_1)$. Assume that $u_1 \in U' = \mathrm{lin}(v_0, \hat{v})^{\perp}$. Then $w = u_2 + \sigma_2(u_1) = u_2 + \kappa''^{-1}\bar{\tau}_2\kappa'(u_1)$. If $u_1 \notin U'$, then there exists an element $u_1' \in U'$ such that $u_1 = u_1' + \hat{v}$ and then $w = u_2 + + \sigma_2(u_1) = u_2 + \sigma_2(u_1' + \hat{v}) = u_2 + \sigma_2(u_1') + \hat{v} = u_2 + \kappa''^{-1}\bar{\tau}_2\kappa'(u_1) + \hat{v}$.

Finally we get

$$w = \begin{cases} u_2 + \kappa''^{-1}\bar{\tau}_2\kappa'(u_1) & \text{if } u_1 \in U' \\ u_2 + \kappa''^{-1}\bar{\tau}_2\kappa'(u_1) + \hat{v}\,, & \text{if } u_1 \notin U' \end{cases} \tag{2}$$

Notice, that in both cases w depends alike on $\bar{\tau}_2$ and u_1 and u_2.

Corollary 3.2. *Let* $(V, \mathbb{F}_2, \beta)$ *be a quaternionic structure and let* $\dim_{\mathbb{F}_2} V = n$. *Then:*
1. If n *is odd number, then*

$$|Aut(V, \mathbb{F}_2, \beta)| = 2^{(n-1)^2/4} \cdot \prod_{i=1}^{(n-1)/2} (2^{2i} - 1).$$

2. If n *is even number and the functional* β *is alternating, then*

$$|Aut(V, \mathbb{F}_2, \beta)| = 2^{n^2/4} \cdot \prod_{i=1}^{n/2} (2^{2i} - 1).$$

3. If n *is odd number and the functional* β *is not alternating, then*

$$|Aut(V, \mathbb{F}_2, \beta)| = 2^{n^2/4} \cdot \prod_{i=1}^{(n-2)/2} (2^{2i} - 1).$$

Proof: In cases 1. and 2. the groups of automorphisms are isomorphic to a suitable symplectic group. The order of those groups can be calculated by using the formula contained in [16, p. 201].
3. By the previous theorem it follows that $|Aut(V, \mathbb{F}_2, \beta)| = |U| \cdot |Sp(n - -2, \mathbb{F}_2)| = 2^{n-1} \cdot 2^{(n-2)^2/4} \cdot \prod_{i=1}^{(n-2)/2}(2^{2i} - 1) = 2^{n^2/4} \cdot \prod_{i=1}^{(n-2)/2}(2^{2i} - 1)$.

4. Groups of strong automorphisms of Witt rings of p-adic fields

Using facts proved above we shall describe the groups of all strong automorphisms for Witt rings of local type with the most simple structure.

The simplest Witt ring of a local type is a ring isomorphic to the ring $\mathbb{Z}$ of all integers. The Witt ring $\mathbb{Z}$ is realized by the field $\mathbb{R}$ of real numbers. In this case the group $G \cong \mathbb{R}^*/\mathbb{R}^{*2} = \{1, -1\}$ and the only strong automorphism of $W(\mathbb{R})$ is the identity map.

Let us consider now the Witt rings of local type realized by the fields $\mathbb{Q}_p$ of p-adic numbers. More information about fields of p-adic numbers, their Witt rings

and associated quaternionic structures one can find in [11], [13] and [14]. We will consider three possible cases.

1. Let W be the Witt ring realized by the 2-adic field $\mathbb{Q}_2$. The abstract Witt ring isomorphic to $W(\mathbb{Q}_2)$ has an 8-element group of square classes $G = \mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ (see [14] or [11] where this abstract Witt ring is denoted by $\mathbb{L}_3$). In this case the quaternionic structure associated with Witt ring can be viewed as bilinear space over $\mathbb{F}_2$ with dimension $n = 3$, the suitable functional is not alternating and according to theorem 3.1 §1 we get $Aut\big(W(\mathbb{Q}_2)\big) \cong Sp(2, \mathbb{F}_2)$. Scrupulous calculation shows that $Aut\big(W(\mathbb{Q}_2)\big)$ is isomorphic to the symmetric group $S(3)$ (group of all permutations of 3-element set).

2. Let us consider Witt ring W realized by any p-adic field $\mathbb{Q}_p$, where $p \equiv 1 \pmod 4$, for example $\mathbb{Q}_5$. It is isomorphic to the ring $\mathbb{Z}/2\mathbb{Z}[C_4]$ of the cyclic 4-element group with coefficients in 2-element ring $\mathbb{Z}/2\mathbb{Z}$ (see [11]). The group of square classes of the field $\mathbb{Q}_p$ has 4 elements: $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} = \{1, p, u, up\}$ ([14, Theorem 2.2, p. 152], compare [11, Theorem 3.18]). The suitable bilinear space V over $\mathbb{F}_2$ is alternating therefore by theorem 3.1 §2 we have $Aut\left(W\left(\mathbb{Q}_p\right)\right) \cong Sp(2, \mathbb{F}_2)$ as in the previous case.

3. Let W be a Witt ring of local type realized by any p-adic field $\mathbb{Q}_p$, where $p \equiv 3 \pmod 4$, for example $\mathbb{Q}_3$. It is isomorphic to the group ring $\mathbb{Z}/4\mathbb{Z}[C_2]$ of the cyclic 2-element group with coefficients in 4-element ring $\mathbb{Z}/4\mathbb{Z}$ (see [11]).

In this case $1 \neq -1 \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$, hence $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} = \{1, -1, p, -p\}$ ([14], Chapter VI, Theorem 2.2). We have $\dim V = 2$ and the suitable functional is not alternating, hence we are in a position described in theorem 3.1 §3. Since $\dim(U, \beta_U) = n - 1 = 1$ and assume that $\hat{v} = -1$, hence $U = \{1, -1\}$. Therefore we have a group isomorphism $U \cong C_2$ and $v_0 = p$. In this case, the second factor of the Cartesian product vanishes, thus $Aut\left(W\left(\mathbb{Q}_p\right)\right) \cong C_2$ that is to say $Aut\left(W\left(\mathbb{Q}_p\right)\right)$ where $p \equiv 3 \pmod 4$ is the 2-element cyclic group.

Witt rings of local type with more complex structure are realized by extensions of the field of 2-adic numbers $\mathbb{Q}_2$ (compare [11, Chapter V, §3]). Let k denote the extension degree of the field K over $\mathbb{Q}_2$.Then the cardinality of the group of square classes K^*/K^{*2} equals $2k + 2$ [cf. [11]). If the extension degree k is an odd number, then there exists exactly one Witt ring of local type with the group of square classes with cardinality $2k + 2$. On the other hand if k is even, there are two non-isomorphic Witt rings of local type depending on that whether $\sqrt{-1} \in F$ or not. In the first case we have $-1 = 1$ and in the second case $-1 \neq 1$. The exact structure of these Witt rings is described in [11, Prop. 5.6].

5. Consequences and future works

Witt rings of local type create an important family of finitely generated Witt rings. Namely, we know that every finitely generated Witt ring can be expressed in terms of $\mathbb{Z}/2\mathbb{Z}$ and so called *basic indecomposable Witt rings* using the operations of group ring formation and direct products (see [11, Theorem 5.23]). Next we notice that most known basic indecomposables are Witt rings of local type (cf. [11, Theorem 5.24]) and we know the description of the groups of strong automorphisms of products of Witt rings of local type (cf. [5]) and the description of the groups of strong automorphisms of Witt rings which are group rings (cf. [6]). These facts make description of groups of strong automorphisms of Witt rings of local type very important for investigation of strong automorphisms of other (possibly all) finitely generated Witt rings.

References

[1] Witt E., Teorie der Quadratischen Formen in Beliebigen Körpern, J. Reine Angew. Math. 1937, 176, 31-44.

[2] Szymiczek K., Bilinear Algebra: An Introduction to the Algebraic Theory of Quadratic Forms. Algebra, Logic and Applications Series Vol. 7, Gordon and Breach Science Publishers, Amsterdam 1997.

[3] Leep D., Marshall M., Isomorphisms and automorphisms of Witt rings, Canad. Math. Bul. 1988, 31 (2), 250-256.

[4] Ware R., Automorphisms of Pythagorean fields and their Witt rings, Comm. Algebra 1989, 17 (4), 945-969.

[5] Stępień M., Automorphisms of products of Witt rings of local type, Acta Mathematica et Informatica Universitatis Ostraviensis 2002, 10, 125-131.

[6] Stępień M., Automorphisms of Witt rings of elementary type. Mathematica. Proc. XIth Slovak-Polish-Czech Mathematical School, Pedagogical Faculty Catholic University in Ružomberok, June 2nd – 5th 2004, 62-67.

[7] Stępień M., Automorphisms of Witt Rings of Finite Fields, Scientific Issues. Mathematics, XVI, Jan Długosz University, Częstochowa 2011, 67-70.

[8] Stępień M.R., Stępień L., On automorphisms of products of Witt rings (I), Journal of Applied Mathematics and Computational Mechanics 2013, 12 (3), 123-133.

[9] Stępień M. R., Stępień L. On automorphisms of products of Witt rings (II), Journal of Applied Mathematics and Computational Mechanics 2013, 12 (4), 119-125.

[10] Czogała A., Kula M., Automorphisms of Witt rings of global fields. Acta Arith. 2014, 163 (1), 1-13.

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

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

[13] Browkin J., Teoria ciał, Biblioteka Matematyczna vol.49, PWN, Warsaw 1978.

[14] Lam T.Y., Introduction to Quadratic Forms over Fields. Graduate Studies in Mathematics vol. 67, American Mathematics Society, 2005.

[15] Lang S., Algebra. Graduate Texts in Mathematics vol. 211, Revised Third Edition, Springer 2002.

[16] Artin E., Geometric Algebra, Interscience Tracts in Pure and Applied Mathematics vol. 3, Interscience Publishers, New York, London 1957.