Scientific Research of the Institute of Mathematics and Computer Science, 1(10) 2011, 231-237

AUTOMORPHISMS OF WITT RINGS AND QUATERNIONIC STRUCTURES

Marcin Ryszard Stępień

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

Abstract. M. Marshall introduced the notion of quaternionic structure and he showed that the categories of Witt rings and quaternionic structures are naturally equivalent. Quaternionic structures turn out to bea useful tool for the investigation of Witt rings, since it suffices to handle the structure of a group. In our paper we shall describe precisely the one-to-one correspondence between automorphisms of quaternionic structures and strong the automorphisms of Witt rings.

Introduction

The notion of a Witt ring originated in 1937 with a paper [1] by E. Witt, then developed slowly until the 1960s, and then rapidly progressed as a consequence of a series of significant papers [2-4] by A. Pfister. Nowadays, the theory of Witt rings is an important part of bilinear algebra. An intelligible introduction to that field of algebra can be found for example in [5, 6]. In this paper we deal with the abstract Witt rings introduced in 1970s as an axiomatic treatment of the subject holding the most of original results of the theory. A comprehensive study of that theory can be found in the book by M. Marshall [7]. Together with abstract Witt rings, Marshall introduced the notion of quaternionic structures and showed that the categories of Witt rings and quaternionic structures are naturally equivalent. This fact enables one to investigate a rather more simple structure of a group instead the structure of a ring. In our paper we shall describe precisely the one-to-one correspondence between Witt rings and quaternionic structures in a special case: the correspondence between the automorphisms of quaternionic structures and strong automorphisms of Witt rings. The result theorem (Theorem 2.1) allows us to describe the groups of automorphisms of quaternionic structures instead the groups of strong automorphisms of suitable abstract Witt rings. We shall present the application of this method in the last section.

For the convenience of the reader, we recall some facts from [7].

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.

Definition 1.1. The triplet (G,Q,q) is called a *quaternionic structure* if for every $a,b,c,d \in G$ map q fulfills:
Q_1: $q(a,b)=q(b,a)$
Q_2: $q(a,-a)=\theta$
Q_3: $q(a,b)=q(a,c) \Leftrightarrow q(a,bc)=\theta$
Q_4: If $q(a,b)=q(c,d)$, then it exists such $x \in G$ that $q(a,b)=q(a,x)$ and $q(c,d)=q(c,x)$.

Remark 1.2. Directly from the above definition we get the following consequences:
1. $q(a,1)=\theta$ (since $q(a,1)=q(a,1)$, so by axiom Q_3, $q(a,1^2)=q(a,1)=\theta$).
2. $q(a,a)=q(a,-1)$ (as above it follows from $q(a,(-1)a)=q(a,-a)=\theta$).
3. $q(a,-ab)=q(a,b)$ (since $q(a,-ab^2)=q(a,-a)=\theta$).

Let (G,Q,q) be an arbitrary quaternionic structure. *(Quadratic) form of dimension* $n \geq 1$ over G is an n-tuple $f=(a_1,\mathrm{K},a_n)$, where $a_1,\mathrm{K},a_n \in G$. The form of dimension 2 is called a *binary form*. Form $(1,-1)$ is called the *binary hyperbolic form*. The sum and product of forms $f=(a_1,\mathrm{K},a_n)$ and $g=(b_1,\mathrm{K},b_m)$ are defined as follows:
$f \oplus g=(a_1,\mathrm{K},a_n) \oplus (b_1,\mathrm{K},b_m)=(a_1,\mathrm{K},a_n,b_1,\mathrm{K},b_m)$
$f \otimes g=(a_1,\mathrm{K},a_n) \otimes (b_1,\mathrm{K},b_m)=(a_1b_1,\mathrm{K},a_1b_m,\mathrm{K},a_nb_1,\mathrm{K},a_nb_m)$.
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) $n>2$, $(a_1,\mathrm{K},a_n) \cong (b_1,\mathrm{K},b_n) \Leftrightarrow$ there exist $a,b,c_3\mathrm{K},c_n \in G$ such that $(a_2,\mathrm{K},a_n) \cong (a,c_3,\mathrm{K},c_n)$, $(a_1,a) \cong (b_1,b)$ and $(b_2,\mathrm{K},b_n) \cong (b,c_3,\mathrm{K},c_n)$.

Form $(1,a_1) \otimes \Lambda \otimes (1,a_n)$, where $a_1,\mathrm{K},a_n \in G$, $n>0$ is called *n-fold Pfister form*. We say that form f represents element $a \in G$ if there exist $a_2,\mathrm{K},a_n \in G$ such that $f \cong (a,a_2,\mathrm{K},a_n)$. We denote the set of all elements represented by form f (*value set of the form f*) by $D(f)$. We have $f \cong g \Rightarrow D(f)=D(g)$. M. Marshall showed that $b \in D(1,-a) \Leftrightarrow q(a,b)=0$.

For f to be a form over G and $n>0$, we denote by $n \times f$ to be the form $f \oplus \Lambda \oplus f$ (n terms). Two forms f and g are called *similar* (or *Witt equivalent*), denoted by $f \approx g$, if there exist numbers $k,l \in \mathrm{N}$, such that $f \oplus k \times (1,-1) \cong g \oplus l \times (1,-1)$. The similarity class of the form $f=(a_1,\mathrm{K},a_n)$ will be denoted by $\langle f \rangle = \langle a_1,\mathrm{K},a_n \rangle$.

Let (G,Q,q) be a quaternionic structure and let W be the set all equivalence classes of forms with respect to the similarity relation. Thus the sum and product of forms induce binary operations on the similarity classes of forms. In this way we get a commutative ring with $W = W(G,Q,q)$, which we will call the *Witt ring associated to quaternionic structure* (G,Q,q). The zero element in $W(G,Q,q)$ is class $\langle 1,-1\rangle$ of hyperbolic forms and the unit element is class $\langle 1\rangle$. Group G generates $W(G,Q,q)$ additively and all axioms of the abstract Witt ring defined by Marshall in [7] are fulfilled. M. Marshall proved that the categories of Witt rings and quaternionic structures are naturally equivalent (cf. [7, Theorem 4.5, Chapter 4]).

In this paper we shall investigate the automorphisms of Witt rings and quaternionic structures.

Definition 1.3. A map σ is called an *automorphism of quaternionic structure* (G,Q,q), which we denote $\sigma \in Aut(G,Q,q)$, if for all $a,b \in G$ it fulfills the following conditions:

1. $\sigma(-1) = -1$,
2. $q(a,b) = \theta \Leftrightarrow q(\sigma(a),\sigma(b)) = \theta$.

One can show (cf. [7]) that the second requirement is equivalent to the following: $q(a,b) = q(c,d) \Leftrightarrow q(\sigma(a),\sigma(b)) = q(\sigma(c),\sigma(d))$.

Lemma 1.4. Let (G,Q,q) *be a quaternionic structure and let* $\sigma : G \to G$ *be an automorphism of group G. Then* σ *is an automorphism of quaternionic structure* (G,Q,q) *iff the following conditions hold:*

1. $\sigma(-1) = -1$,
2. $\sigma(D(1,a)) = D(1,\sigma(a))$ *for all* $a \in G$.

Proof. It follows from the fact that $b \in D(1,-a)$ iff $q(a,b) = \theta$ for all $a,b \in G$.

Definition 1.5. Let W be a Witt ring. We say that φ is a (*strong*) *automorphism of Witt ring* W if $\varphi(G) = G$.

One can notice that we consider only such automorphisms of ring W, which preserves the dimension of forms (or automorphisms mapping one-dimensional forms to one-dimensional forms).

1. Main theorem

Theorem 2.1. Let (G,Q,q) *be a quaternionic structure and* $W = W(G,Q,q)$ *associated Witt ring. Then:*

1. Every automorphism σ of (G,Q,q) induces a unique strong automorphism φ of Witt ring $W(G,Q,q)$, such that $\sigma(a)=\varphi(a)$ for all $a\in G$.

2. $Aut(G,Q,q)\cong Aut(W)$.

Proof. 1. Let W be the set of all similarity classes of forms over G. For $\sigma\in Aut(G,Q,q)$ we define map $\varphi: W\to W$ as follows:

$$\varphi(\langle a_1,\mathrm{K},a_n\rangle):=\langle\sigma(a_1),\mathrm{K},\sigma(a_n)\rangle.$$

We shall prove that φ is a group isomorphism between $Aut(W)$ and $Aut(G,Q,q)$.

First notice that φ is well-defined. Induction on n. Assume that $(a_1,\mathrm{K},a_n)\cong(b_1,\mathrm{K},b_n)$. For $n=1$ we have $(a_1)\cong(b_1)\Leftrightarrow a_1=b_1$, hence $\sigma(a_1)=\sigma(b_1)$. Let $n=2$. Then by the definition of the equivalence of forms we have $(a_1,a_2)\cong(b_1,b_2)\Leftrightarrow a_1a_2=b_1b_2$ and $q(a_1,a_2)=q(b_1,b_2)$. It follows that $\sigma(a_1a_2)=\sigma(b_1b_2)$ and then $q(\sigma(a_1),\sigma(a_2))=q(\sigma(b_1),\sigma(b_2))$. Next, using the properties of σ we get $\sigma(a_1)\sigma(a_2)=\sigma(b_1)\sigma(b_2)$, hence $(\sigma(a_1),\sigma(a_2))\cong(\sigma(b_1),\sigma(b_2))$.

Assume that the hypothesis holds for $n-1$. Using equivalence $(a_1,\mathrm{K},a_n)\cong(b_1,\mathrm{K},b_n)$ it follows that there exist such $a,b,c_3,\mathrm{K},c_n\in G$, that $(a_1,a)\cong(b_1,b)$, $(a_2,\mathrm{K},a_n)\cong(a,c_3,\mathrm{K},c_n)$ and $(b_2,\mathrm{K},b_n)\cong(b,c_3,\mathrm{K},c_n)$. Next by the above proof for $n=2$ we have $(\sigma(a_1),\sigma(a))\cong(\sigma(b_1),\sigma(b))$. Using induction we obtain $(\sigma(a_2),\mathrm{K},\sigma(a_n))\cong(\sigma(a),\sigma(c_3),\mathrm{K},\sigma(c_n))$ and

$(\sigma(b_2),\mathrm{K},\sigma(b_n))\cong(\sigma(b),\sigma(c_3),\mathrm{K},\sigma(c_n))$.

Using again the equivalence of forms we get $(\sigma(a_1),\mathrm{K},\sigma(a_n))\cong(\sigma(b_1),\mathrm{K},\sigma(b_n))$, which means that the map is well-defined on equivalent forms.

Now notice that the image of hyperbolic form is a hyperbolic form. In fact, we have $\varphi(\langle 1,-1,\mathrm{K},1,-1\rangle)=(\langle\sigma(1),\sigma(-1),\mathrm{K},\sigma(1),\sigma(-1)\rangle)=\langle 1,-1,\mathrm{K},1,-1\rangle$.

Let $\langle a_1,\mathrm{K},a_n\rangle=\langle b_1,\mathrm{K},b_m\rangle$. Then using the definition of similarity of forms we can assume, that $f=(a_1,\mathrm{K},a_n,1,-1,\mathrm{K},1,-1)$, $g=(b_1,\mathrm{K},b_m,1,-1,\mathrm{K},1,-1)$ and $f\cong g$.

Then $\varphi(\langle f\rangle)=\varphi(\langle a_1,\mathrm{K},a_n,1,-1,\mathrm{K},1,-1\rangle)=\langle\sigma(a_1),\mathrm{K},\sigma(a_n),1,-1,\mathrm{K},1,-1\rangle$ and $\varphi(\langle g\rangle)=\varphi(\langle b_1,\mathrm{K},b_m,1,-1,\mathrm{K},1,-1\rangle)=\langle\sigma(b_1),\mathrm{K},\sigma(b_m),1,-1,\mathrm{K},1,-1\rangle$,

hence by the fact that φ is well-defined on the equivalence classes of forms and on the similarity classes of hyperbolic forms we get $\varphi(\langle f\rangle)=\varphi(\langle g\rangle)$.

Let $f=(a_1,\mathrm{K},a_n)$ and $g=(b_1,\mathrm{K},b_m)$. We have

$$\varphi(\langle f\rangle\oplus\langle g\rangle)=\varphi(\langle a_1,\mathrm{K},a_n\rangle\oplus\langle b_1,\mathrm{K},b_m\rangle)=\varphi(\langle a_1,\mathrm{K},a_n,b_1,\mathrm{K},b_m\rangle)=$$
$$=\langle\sigma(a_1),\mathrm{K},\sigma(a_n),\sigma(b_1),\mathrm{K},\sigma(b_m)\rangle=\langle\sigma(a_1),\mathrm{K},\sigma(a_n)\rangle\oplus\langle\sigma(b_1),\mathrm{K},\sigma(b_m)\rangle=$$
$$=\varphi(\langle a_1,\mathrm{K},a_n\rangle)\oplus\varphi(\langle b_1,\mathrm{K},b_m\rangle)=\varphi(\langle f\rangle)\oplus\varphi(\langle g\rangle)\text{ and}$$

$$\varphi(\langle f\rangle\otimes\langle g\rangle)=\varphi(\langle a_1,\mathrm{K},a_n\rangle\otimes\langle b_1,\mathrm{K},b_m\rangle)=\varphi(\langle a_1b_1,\mathrm{K},a_1b_m,\mathrm{K},a_nb_1,\mathrm{K},a_nb_m\rangle)=$$
$$=\langle\sigma(a_1b_1),\mathrm{K},\sigma(a_1b_m),\mathrm{K}.\sigma(a_nb_1),\mathrm{K},\sigma(a_nb_m)\rangle=$$
$$=\langle\sigma(a_1)\sigma(b_1),\mathrm{K},\sigma(a_1)\sigma(b_m),\mathrm{K},\sigma(a_n)\sigma(b_1),\mathrm{K},\sigma(a_n)\sigma(b_m)\rangle=$$
$$=\langle\sigma(a_1),\mathrm{K},\sigma(a_n)\rangle\otimes\langle\sigma(b_1),\mathrm{K},\sigma(b_m)\rangle=\varphi(\langle f\rangle)\otimes\varphi(\langle g\rangle),$$

therefore φ is a ring homomorphism.

We define map $\psi:W\to W$ by $\psi(\langle a_1,\mathrm{K},a_n\rangle):=\langle\sigma^{-1}(a_1),\mathrm{K},\sigma^{-1}(a_n)\rangle$.

Then

$$(\psi\circ\varphi)(\langle a_1,\mathrm{K},a_n\rangle)=\psi(\langle\sigma(a_1),\mathrm{K},\sigma(a_n)\rangle)=\langle\sigma^{-1}(\sigma(a_1)),\mathrm{K},\sigma^{-1}(\sigma(a_n))\rangle=$$
$$=\langle a_1,\mathrm{K},a_n\rangle,$$

hence φ is a bijection, which means it is a ring automorphism. Moreover from the definition of φ it follows, that $\varphi(G)=G$, thus φ is a strong automorphism of Witt ring W.

2. Define map $\Phi:Aut(G,Q,q)\to Aut(W)$ like this: $\Phi(\sigma)=\varphi_\sigma$, where $\varphi_\sigma(\langle a_1,\mathrm{K},a_n\rangle):=\langle\sigma(a_1),\mathrm{K},\sigma(a_n)\rangle$, for every $\sigma\in Aut(G,Q,q)$.

Let $\sigma,\rho\in Aut(G,Q,q)$. We shall show that $\Phi(\sigma\circ\rho)=\Phi(\sigma)\circ\Phi(\rho)$.

In fact, we have

$$\varphi_\sigma\circ\varphi_\rho(\langle a_1,\mathrm{K},a_n\rangle)=\varphi_\sigma(\varphi_\rho(\langle a_1,\mathrm{K},a_n\rangle))=\varphi_\sigma(\langle\rho(a_1),\mathrm{K},\rho(a_n)\rangle)=$$
$$=\langle\sigma(\rho(a_1)),\mathrm{K},\sigma(\rho(a_n))\rangle=\langle(\sigma\circ\rho)(a_1),\mathrm{K},(\sigma\circ\rho)(a_n)\rangle=\varphi_{\sigma\circ\rho}(\langle a_1,\mathrm{K},a_n\rangle),$$

thus Φ is a group homomorphism.

Let φ be an automorphism of Witt ring $W(G,Q,q)$, i.e. $\varphi(G)=G$ and let σ be the restriction of φ to group G. We shall show that σ is an automorphism of quaternionic structure, i.e. $q(a,b)=\theta\Leftrightarrow q(\sigma(a),\sigma(b))=\theta$ for all $a,b\in G$. Notice, that $\theta=q(a,b)=q(1,ab)$ (see Remark 1.2), hence by the definition of the equivalence of binary forms we get $(a,b)\cong(1,ab)$. Since φ is an automorphism of a Witt ring, thus $\varphi(\langle a,b\rangle)=\varphi(\langle 1,ab\rangle)$. We have

$$\varphi(\langle a,b\rangle)=\varphi(\langle a\rangle)\oplus\varphi(\langle b\rangle)=\langle\sigma(a)\rangle\oplus\langle\sigma(b)\rangle=\langle\sigma(a),\sigma(b)\rangle$$

and

$$\varphi(\langle 1,ab\rangle)=\varphi(\langle 1\rangle)\oplus\varphi(\langle ab\rangle)=\langle 1\rangle\oplus\langle\sigma(ab)\rangle=\langle 1,\sigma(ab)\rangle$$

Therefore forms $(\sigma(a),\sigma(b))$ and $(1,\sigma(ab))$ are equivalent and consequently $q(\sigma(a),\sigma(b))=q(1,\sigma(ab))=\theta$.

Finally routine calculation shows, that $\ker\Phi=\{id_{Aut(G,Q,q)}\}$, which means that Φ is a bijection.■

2. Application

The best examples are often the simplest ones. We shall present some applications of our theorem in simple cases.

1. Let us consider the smallest Witt ring $W\cong Z/2Z$. Then group G is trivial, so identity is the only automorphism.
2. There are 3 non-isomorphic Witt rings with the two-element group G, namely $W_1\cong Z$, $W_2\cong Z/4Z$ and $W_3\cong Z/2Z$ [C_2]. By the definition of the automorphism of quaternionic structure it follows that $Aut(G_i,Q_i,q_i)=\{id_{G_i}\}$ for all W_i, $1\le i\le 3$.
3. Let $W_1\cong Z/4Z$ [C_2] and $W_2\cong Z/2Z[C_4]$, so-called Witt rings of the local type.

The quaternionic structures associated to Witt rings W_i, $i=1,2$ are triplets (G_i,Q_i,q_i), where $G_1=\{1,-1,x,-x\}$ $(-1\neq 1$ in $G_1)$, $G_2=\{1,x,y,xy\}$ $(-1=1$ in $G_2)$ and $|Q_i|=2$, say $Q_i=\{1,z\}$ and maps q_i are defined as follows:

q_1	1	−1	x	−x
1	θ	θ	θ	θ
−1	θ	θ	z	z
x	θ	z	z	θ
−x	θ	z	θ	z

q_2	1	x	y	xy
1	θ	θ	θ	θ
x	θ	θ	z	z
y	θ	z	θ	z
xy	θ	z	z	θ

One can calculate that $Aut(G_1,Q_1,q_1)=\{id_{G_1},\sigma\}$, where σ is such an automorphism of (G_1,Q_1,q_1) that $\sigma(x)=-x$ and $Aut(G_2,Q_2,q_2)\cong Aut(G)$.

More examples of groups of automorphisms of Witt rings described with the use of their one-to-one correspondence to groups of automorphisms of quaternionic structures can be found in [8], [9] and [10].

References

[1] Witt E., Theorie de quadratishen Formen in beliebigen Körpern, J. Reine Angew. Math. 1937, 176, 31-44.

[2] Pfister A., Zur Darstellung von -1 als Summe von Quadraten in einem Körper, J. London Math. Soc. 1965, 40, 159-165.

[3] Pfister A., Quadratishe Formen in beliebigen Körpern. Invent. Math. 1966. 1.116-132.

[4] Pfister A., Zur Darstellung definiter Funktionen als Summe von Quadraten. Invent. Math. 1967. 4. 229-237.

[5] 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.

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

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

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

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

[10] Stępień M.R., Automorphisms of Witt rings of finite fields. Scientific Issues. Mathematics. XVI. Jan Długosz University. Częstochowa 2011. 67-70.