Jan Długosz University in Częstochowa
Scientific Issues, Mathematics XVI, Częstochowa 2011

AUTOMORPHISMS OF WITT RINGS OF FINITE FIELDS

Marcin Ryszard Stępień

Kielce University of Technology
al. Tysiąclecia Państwa Polskiego 7, 25-314 Kielce, Poland
e-mail: mstepien@tu.kielce.pl

Abstract. The problem of general description of the group of automorphisms of any Witt ring W seems to be very difficult to solve. However, there are many types of Witt rings, which automorphism are described precisely (e.g. [1], [2], [4], [5], [6], [7], [8]). In our paper we characterize automorphisms of abstract Witt rings (cf. [3]) isomorphic to powers of Witt rings of quadratic forms with coeffitients in finite fields with characteristic different from 2.

1. Introduction

A Witt ring of quadratic forms is one of the centaral notion in bilinear algebra. Investigation of automorphisms of Witt rings is a natural problem, when we consider such objects. The special property of automorphisms of a Witt ring W is the fact that every automorphism of W has to preserve the dimension of forms or, in other words, it has to send one-dimensional forms to one-dimensional forms. In the abstract Witt ring theory an automorphism of a Witt ring $W = (R, G)$ is such an automorphism σ of the ring R that $\sigma(G) = G$. Introducing abstract Witt rings in [3], Marshall showed that every Witt ring of quadratic forms over a field F fulfills axioms of abstract Witt rings contained in his book [3], where as a distinguished group G one can take the group F^*/F^{*2} of square classes of the feld F. We say that an abstract Witt ring $W = (R, G)$ is *realized by a field* F if there exist a Witt ring of quadratic forms over the field F and such a ring isomorphism between W and $W(F)$, which maps the group G into the group F^*/F^{*2}. In our paper we consider Witt rings which are powers of Witt rings realized by finite fields with characteristic different from 2 and we investigate their groups of automorphisms.

In proofs of our results we use the notion of quaternionic structure (G, Q, q) associated to a Witt ring $W = (R, G)$. Here q is a surjection $q\colon G \times G \to \mathrm{Q}$ and four suitable axioms hold (for details see [3, Chapter 2]). By the theory presented in [3], categories of Witt rings and quaternionic structures are naturally equivalent. Therefore, the group of automorphisms of quaternionic structure is isomorphic to the group of automorphisms of associated Witt ring. By Marshall (cf. [3]), $\sigma \in \mathrm{Aut}(G)$ is an automorphism of quaternionic structure (G, Q, q) if q fulfills the following conditions:

1. $\sigma(-1) = -1$,
2. $q(a, b) = 0 \Leftrightarrow q(\sigma(a), \sigma(b)) = 0$.

Hence, we can investigate group automorphisms $\sigma \in \mathrm{Aut}(G)$ instead of automorphisms of a Witt ring $W = (R, G)$.

Let $W = (R, G)$ be a Witt ring realized by a finite field with characteristic different from 2 and let (G, Q, q) be the quaternionic structure associated to W. There are two cases.

1) $W \cong \mathbb{Z}/2\mathbb{Z}[C_2] \cong W(\mathbb{F}_5)$, where $\mathbb{Z}/2\mathbb{Z}[C_2]$ denotes the group ring of 2-element cyclic group C_2 with coefficients in the ring $\mathbb{Z}/2\mathbb{Z}$. Then the group G is isomorphic to $\mathbb{F}_5^*/\mathbb{F}_5^{*2} = \{1, x\}$ and the distinguished element is $-1 = 1$.
2) $W \cong \mathbb{Z}/4\mathbb{Z} \cong W(\mathbb{F}_3)$. Then the group G is isomorphic to $\mathbb{F}_3^*/\mathbb{F}_3^{*2} = \{1, -1\}$ $(-1 \neq 1)$.

In both cases the set $\mathrm{Q} = \{0\}$, hence $q(a, b) = 0$ for all $a, b \in G$.

2. Witt rings of finite fields and their powers

Theorem 1. *Let $W = (R, G)$ be a Witt ring realized by a finite field with characteristic different from 2. Then every automorphism of the group G^k, $k \in \mathbb{N}$, mapping the distinguished element -1 into itself induces an automorphism of a Witt ring W^k.*

Proof.
Since $q(a, b) = 0$ for all $a, b \in G$, it follows that quaternionic map q does not influence on the form and the number of automorphisms of quaternionic structure (G, Q, q). This means that every automorphism of the group G such that $\sigma(-1) = -1$ is an automorphism of (G, Q, q).

Finally, by the construction of powers of Witt rings and quaternionic structures (see [3, Chapter 5, §4]), we conclude that every automorphism of the group G^k, $k \in \mathbb{N}$, mapping the distinguished element $-1 \in G^k$ into itself is an automorphism of quaternionic structure (G^k, Q^k, q^k), consequently it induces an automorphism of a Witt ring W^k.

Corollary 1. *Let $W = (R, G)$ be a Witt ring realized by the Galois field $\mathbb{F}_5$. Then the group of automorphisms of the Witt ring $W' = (W^k, G^k)$ is isomorphic to $GL(k, \mathbb{F}_2)$.*

Proof. Let $W' = (W^k, G^k)$. Then $1 = -1$ in G and consequently in G^k, hence any automorphism of the group G^k is an automorphism of the quaternionic structure (G^k, Q^k, q^k). In fact, the group G^k is a vector space over the two-element Galois field $\mathbb{F}_2$ and $\dim_{\mathbb{F}_2} G^k = k$. Let $\mathcal{B} = \{b_1, \ldots, b_k\}$ be a basis of the vector space of G^k over $\mathbb{F}_2$ and let $\sigma \in \mathrm{Aut}(G, \mathrm{Q}, q)$. Then a system of vectors $\{\sigma(b_1), \ldots, \sigma(b_k)\}$ is another basis of the vector space G^k over $\mathbb{F}_2$. Every $\sigma(b_i)$, $1 \leq i \leq k$ can be represented as a combination of vectors from basis $\mathcal{B}$ as follows: $\sigma(b_i) = \alpha_{i1} b_1 + \ldots + \alpha_{ik} b_k$. Define a map $\Phi\colon \mathrm{Aut}(G^k, \mathrm{Q}^k, q^k) \to \mathrm{GL}(k, \mathbb{F}_2)$ by the following formula:

$$\Phi(\sigma) = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1k} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2k} \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_{k1} & \alpha_{k2} & \ldots & \alpha_{kk} \end{bmatrix}.$$

The map Φ is a group isomorphism (this follows from uniqueness of representation of vectors $\sigma(b_i)$ in the basis $\mathcal{B}$).

Corollary 2. *Let $W = (R, G)$ be a Witt ring realized by the Galois field $\mathbb{F}_3$. Then the group of automorphisms of the Witt ring $W' = (W^k, G^k)$ is isomorphic to the affine group* $\mathrm{Aff}(k-1, \mathbb{F}_2)$.

Proof. Let $W' = (W^k, G^k)$. In this case we have $1 \neq -1$ in G. Consider the map Φ defined in the previous proof. We want to find all $\sigma \in \mathrm{Aut}(G^k)$ such that $\sigma(-1) = -1$, thus we fix the last vector in the basis $\mathcal{B}$ as $b_k = -1$. For all the automorphisms which preserve that vector, we get the following form of the map Φ:

$$\Phi(\sigma) = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1k} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2k} \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_{k-1,1} & \alpha_{k-1,2} & \ldots & \alpha_{k-1,k} \\ 0 & 0 & \ldots & 1 \end{bmatrix}.$$

So in this case we have block matrices of the form $\begin{bmatrix} A & a \\ 0 & 1 \end{bmatrix}$. Let us examine the form of the product of this kind of matrices:

$$\begin{bmatrix} A & a \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} B & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} AB & bA + a \\ 0 & 1 \end{bmatrix}.$$

On the other hand, affine transformations have the form: $f(x) = xA + a$ and $g(x) = xB + b$, hence the composition of them has the form: $f(g(x)) = f(xB + b) = (xB + b)A + a = AB + (bA + a)$.

Therefore, the map given by $f(\Phi) = \begin{bmatrix} A & a \\ 0 & 1 \end{bmatrix}$ is a group isomorphism between $\mathrm{Aut}(G, \mathrm{Q}, q)$ and $\mathrm{Aff}(k-1, \mathbb{F}_2)$.

Summarizing the results of the paper, we can write out the groups of automorphisms of Witt rings of two types:

$\mathrm{Aut}((\mathbb{Z}/2\mathbb{Z}[C_2])^k) \cong \mathrm{Aut}((W(\mathbb{F}_5))^k) \cong GL(k, \mathbb{F}_2)$,

$\mathrm{Aut}((\mathbb{Z}/4\mathbb{Z})^k) \cong \mathrm{Aut}((W(\mathbb{F}_3))^k) \cong \mathrm{Aff}(k-1, \mathbb{F}_2) \cong \mathbb{F}_2^{k-1} \ltimes GL(k-1, \mathbb{F}_2)$.

References

[1] R. Baeza, R. Moresi. On the Witt-equivalence of fields of characteristic 2. *Journal of Algebra*, **92**, 446–453, 1985.

[2] A. Czogała. On reciprocity equivalence of quadratic number fields. *Acta Arithmetica*, **58**, No. 1, 27–46, 1981.

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

[4] R. Perlis, K. Szymiczek, P.E. Conner, R. Litherland. Matching Witts with global fields. In: W.B. Jacob, T.-Y. Lam, R.O. Robson (Eds.), *Recent Advances in Real Algebraic Geometry and Quadratic Forms*, (Proceedings of the RAGSQUAD Year, Berkeley 1990–1991), *Contemporary Mathematics*, **155**, 365–387, Amer. Math. Soc. Providence, Rhode Island 1994.

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

[6] M. Stępień. Automorphisms of Witt rings of elementary type. *Mathematica. Proc. XI^{th} Slovak-Polish-Czech Mathematical School, Catholic University in Ružomberok*, **10**, 62–67, 2004.

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

[8] R. Ware. Automorphisms of Pythagorean fields and their Witt rings. *Commutative Algebra*, **17**, No. 4, 945-969, 1989.