



ANDRZEJ IWAN and CZESŁAW WÓWK (Szczecin)

Basic part of Witt rings of elementary type

Introduction. In an abstract Witt ring R , the existence of a birigid element is equivalent to R being a group ring. Thus, it is of importance to be able to determine whether or not birigid elements exist in a Witt ring R . One way to answer this question is to look at the subgroup B_R of the group of units of R generated by the non-birigid elements in R . This subgroup B_R is said to be the *basic part* of R and every one-dimensional element of R which is not in B_R is birigid. Thus, knowing B_R , we are able to decide whether or not R is a group ring.

Carson and Marshall [1] proved an interesting structure result for B_R in terms of value set of binary forms. If X_1 is the value group $D \langle 1, a \rangle$ of the form $\langle 1, a \rangle$ and $X_i = \bigcup \{D \langle 1, -x \rangle : 1 \neq x \in X_{i-1}\}$, $i \geq 2$, then they prove

$$(1) \quad B_R = \pm X_1 X_3 \cup X_1 X_2 X_2,$$

provided $2 < |X_1| < \infty$ and $a \neq -1$.

Thus a given non-rigid element $a \in B_R$ generates all basic elements in R .

Looking at examples, one realizes that the structure of B_R is probably much simpler than Carson–Marshall's result (1).

K. Szymiczek [3] considered this problem for Witt rings R of typical fields with infinite group of square classes including global fields, all purely transcendental extension fields and subfields of real numbers. In all these cases, except for subfields of \mathbf{R} , he gets simply $B_R = X_2$, and, for subfields of \mathbf{R} , he proves $B_R = X_2 \cup -X_2$ or $X_3 \cup -X_3$ depending on the sign of the number a we start with.

Motivated by this, we study the structure of the basic part of Witt rings R of elementary type and prove that for R in this class we have always $B_R = X_3 \cup -X_3$ for any $a \in B_R$. We also give examples showing that for elementary Witt rings this result is best possible, that is, we exhibit Witt rings R of elementary type with

$$B_R \neq \pm X_2 \cup X_3.$$

1. Preliminaries. In this section we explain notation and terminology to

be used throughout the paper. We follow closely Marshall [2] and refer the reader to [2] for the details.

An abstract Witt ring in sense of [2] is a commutative ring with unity 1 additively generated by subgroup G_R of the group of units R^* of R and satisfying certain relations.

For $a \in G_R$, the *value set* of the form $\langle 1, a \rangle$ is defined to be

$$D \langle 1, a \rangle = \{x \in G_R: 1+a = x+ax \text{ in } R\}.$$

An $a \in G_R$ is said to be *rigid* if $D \langle 1, a \rangle = \{1, a\}$ and a is said to be *birigid* if both a and $-a$ are rigid. The set

$$B_R = \{\pm 1\} \cup \{a \in G_R: a \text{ is not birigid}\}$$

is said to be the *basic part* of R .

If $B_R = G_R$, we say R is *basic*. It is known that B_R is always a subgroup of G_R .

The class of Witt rings can be made into a category (see [2], p. 67). A Witt ring R is called *decomposable* iff there exist Witt rings R_1, R_2 such that $R = R_1 \times R_2$ and $R_i \neq \mathbb{Z}/2\mathbb{Z}$, $i = 1, 2$ (\times denotes the product in category of Witt rings). Let R be a Witt ring and Δ a non-trivial group of exponent 2. Then the group ring $S = R[\Delta]$ is again a Witt ring (see [2], Proposition 5.16). A Witt ring R is said to be of *local type* if R is realized as the Witt ring of a local field (cf. [2], Chapter 5, § 3 and p. 97). If R is a Witt ring of local type with $|G_R| > 4$, then R is basic indecomposable ([2], Theorem 5.24).

A Witt ring R with $|G_R| < \infty$ which is built up by forming products and group rings from \mathbb{Z} , $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ and Witt rings of local type which are basic indecomposable, is said to be of *elementary type*.

2. Structure of the basic part. In this section we prove the structure result for B_R mentioned in the Introduction. We begin with determining the sets X_i for a decomposable Witt ring.

For an abstract Witt ring (R, G_R) write

$$A_R = \bigcup \{D \langle 1, -x \rangle: x \in G_R \setminus \{-1\}\}.$$

Since $-x \in D \langle 1, -x \rangle$ and $-1 \in D \langle 1, -x \rangle \Leftrightarrow x \in D \langle 1, 1 \rangle$, we get

$$(2.1) \quad A_R = \begin{cases} G_R & \text{if } D \langle 1, 1 \rangle \neq \{1\}, \\ G_R \setminus \{-1\} & \text{if } D \langle 1, 1 \rangle = \{1\}. \end{cases}$$

Recall that R is said to be *Pythagorean* if $D \langle 1, 1 \rangle = \{1\}$.

Now let $a \in G_R$ be fixed and put $X_1 = D \langle 1, a \rangle$ and $X_2 = \bigcup \{D \langle 1, -x \rangle: 1 \neq x \in X_1\}$. Observe that

$$(2.2) \quad X_2 = \emptyset \Leftrightarrow X_1 = \{1\} \Leftrightarrow R \text{ is Pythagorean and } a = 1.$$

Also

$$X_2 = \emptyset \Leftrightarrow X_i = \emptyset \quad \text{for all } i \geq 2.$$

Thus if $X_2 = \emptyset$, the basic part B_R cannot be described in terms of the sets X_i . As (2.2) shows, this happens only in a very special case and even if R is Pythagorean we can start with $a \neq 1$ and use the results below. However, we cannot ignore the case (2.2) since even if R has $X_2 \neq \emptyset$, the factors of R can behave differently.

Now assume that $R = S \times T$ is a non-trivial decomposition of R . Then the fixed element a in G_R can be written $a = (b, c)$, where $b \in G_S$ and $c \in G_T$. We write $D \langle 1, b \rangle = Y_1$ and $D \langle 1, c \rangle = Z_1$ and then we have

$$(2.3) \quad X_1 = D \langle 1, a \rangle = D \langle 1, b \rangle \times D \langle 1, c \rangle = Y_1 \times Z_1.$$

Write

$$Y_{i+1} = \cup \{D \langle 1, -y \rangle : y \in Y_i \setminus \{1\}\} \quad \text{for } i \geq 1,$$

and

$$Z_{i+1} = \cup \{D \langle 1, -z \rangle : z \in Z_i \setminus \{1\}\} \quad \text{for } i \geq 1.$$

We shall need formulae similar to (2.3) for X_2 and X_3 . We have

$$\begin{aligned} X_2 &= \cup \{D \langle 1, -x \rangle : x \in Y_1 \times Z_1 \setminus \{(1, 1)\}\} \\ &= \cup \{D \langle 1, -x \rangle : x \in Y_1 \times (Z_1 \setminus \{1\})\} \cup \\ &\quad \cup \{D \langle 1, -x \rangle : x \in (Y_1 \setminus \{1\}) \times \{1\}\}. \end{aligned}$$

Hence

$$(2.4) \quad X_2 = G_S \times Z_2 \cup Y_2 \times G_T.$$

To find the formula for X_3 let us assume first that $Y_2 \neq \emptyset$ and $Z_2 \neq \emptyset$. Then

$$\begin{aligned} X_2 \setminus \{1\} &= G_S \times Z_2 \setminus \{(1, 1)\} \cup Y_2 \times G_T \setminus \{(1, 1)\} \\ &= G_S \times (Z_2 \setminus \{1\}) \cup (G_S \setminus \{1\}) \times Z_2 \cup (Y_2 \setminus \{1\}) \times G_T \cup \{1\} \times (G_T \setminus \{1\}). \end{aligned}$$

Hence

$$\begin{aligned} X_3 &= \cup \{D \langle 1, -x \rangle : x \in X_2 \setminus \{1\}\} \\ &= G_S \times Z_3 \cup A_S \times G_T \cup Y_3 \times G_T \cup G_S \times A_T. \end{aligned}$$

Thus we get

$$(2.5) \quad X_3 = G_S \times (Z_3 \cup A_T) \cup (A_S \cup Y_3) \times G_T,$$

provided $Y_2 \neq \emptyset$ and $Z_2 \neq \emptyset$.

Consider now the case $Y_2 \neq \emptyset$ and $Z_2 = \emptyset$. Then the above splitting for $X_2 \setminus \{1\}$ is to be replaced by

$$X_2 \setminus \{1\} = Y_2 \times G_T \setminus \{(1, 1)\} = (Y_2 \setminus \{1\}) \times G_T \cup \{1\} \times (G_T \setminus \{1\}).$$

In this case we get

$$(2.6) \quad X_3 = Y_3 \times G_T \cup G_S \times A_T.$$

Similarly, if $Y_2 = \emptyset$ and $Z_2 \neq \emptyset$ we get

$$(2.7) \quad X_3 = G_S \times Z_3 \cup A_S \times G_T.$$

Finally, if $Y_2 = \emptyset$ and $Z_2 = \emptyset$, then $X_2 = \emptyset$ by (2.4); hence $X_3 = \emptyset$.

Now we proceed to the basic part B_R of a decomposable Witt ring R . By Lemma 5.22 in [2], if R is decomposable and $R \neq \mathbf{Z} \times \mathbf{Z}$, then necessarily $B_R = G_R$. We prove the following result.

PROPOSITION 1. *Let R be a decomposable Witt ring, $a \in G_R$ and let the sets X_i be defined as in the Introduction. Moreover, if R is Pythagorean, assume additionally $a \neq 1$.*

- (i) *If $R = \mathbf{Z} \times \mathbf{Z}$, then $B_R = \{1, -1\}$.*
- (ii) *If $R \neq \mathbf{Z} \times \mathbf{Z}$, then $B_R = G_R = X_3 \cup -X_3$.*
- (iii) *If $R \neq \mathbf{Z} \times \mathbf{Z}$ and R is the product of two non-Pythagorean Witt rings, then $B_R = G_R = X_3$.*

Proof. (i) is proved in [2], p. 118.

(ii) We want to show $G_R = X_3 \cup -X_3$. If $R = S \times T$, where S and T are not isomorphic to $\mathbf{Z}/2\mathbf{Z}$, we use the notation set up in (2.3) through (2.7). The first case is when $Y_2 \neq \emptyset$ and $Z_2 \neq \emptyset$. Then

$$G_R \subseteq G_S \times A_T \cup -(G_S \times \{1\}) \subseteq X_3 \cup -X_3,$$

the latter by (2.5). This proves $G_R = X_3 \cup -X_3$.

Exactly the same argument applies when $Y_2 \neq \emptyset$ and $Z_2 = \emptyset$ on using (2.6), and by symmetry this proves also the result in the case $Y_2 = \emptyset$ and $Z_2 \neq \emptyset$. The case $Y_2 = \emptyset$ and $Z_2 = \emptyset$ cannot occur since then $X_2 = \emptyset$ by (2.4) and then, by (2.2), R is Pythagorean and $a = 1$, contrary to assumptions. This proves (ii).

(iii) Here $R = S \times T$, where S and T are non-Pythagorean Witt rings. By (2.1), $A_S = G_S$ and by (2.2), $Y_2 \neq \emptyset$ and $Z_2 \neq \emptyset$. Hence $G_R = G_S \times G_T = X_3$ by (2.5) and we are through.

Now we record some simple facts concerning X_i .

PROPOSITION 2. *Let $a \in G_R$ and the sets X_i be defined as in the Introduction. Then*

- (i) *$d \in X_{i+1}$ iff $D \langle 1, -d \rangle \cap X_i \neq \{1\}$, $i = 1, 2, 3, \dots$,*
- (ii) *if $|G_R| < \infty$ and for every $x \in G_R$, $|D \langle 1, x \rangle|^2 > |G_R|$, then $X_2 = G_R$.*

Proof. (i) is trivial.

(ii) Our hypothesis implies that for any $x \in G_R$, $|D \langle 1, x \rangle| |D \langle 1, a \rangle| > |G_R|$. Let us observe that for any $x \in G_R$, $D \langle 1, x \rangle \cap D \langle 1, a \rangle \neq \{1\}$. Indeed, $D \langle 1, x \rangle D \langle 1, a \rangle$ is a subgroup of G_R so $D \langle 1, x \rangle \cap D \langle 1, a \rangle = \{1\}$ implies that $|D \langle 1, x \rangle D \langle 1, a \rangle| = |D \langle 1, x \rangle| |D \langle 1, a \rangle| > |G_R|$, a contradiction. Thus (i) implies that $-x \in X_2$ for any $x \in G_R$.

Here is an application of Proposition 2 to B_R , where R is realized as the Witt ring of finite extension of \mathbb{Q}_2 . All Witt rings of local type with $|G_R| > 4$ come from the field of 2-adic numbers and its finite extensions ([2], p. 97).

PROPOSITION 3. *If R is a Witt ring of local type with $|G_R| > 4$, then $B_R = X_2$ independently of the choice of $a \in G_R$.*

Proof. By [2] (Theorem 5.24), $B_R = G_R$. So we have to show that $X_2 = G_R$. Recall that if R is a Witt ring of local type, then for any $x \in G_R$ we have $|D \langle 1, x \rangle| \geq \frac{1}{2} |G_R|$ (see [2], Chapter 5, §3). Hence Proposition 2 (ii) implies $B_R = G_R = X_2$.

Now we are ready to characterize basic part of a Witt ring of elementary type.

THEOREM. *Let R be a Witt ring of elementary type with $B_R \neq \{1, -1\}$ and let the sets X_i be defined as in the Introduction. Suppose $a \in G_R$ is not birigid and $a \neq -1$. Moreover, if R is Pythagorean assume additionally $a \neq 1$, then $B_R = X_3 \cup -X_3$.*

Proof. If R is a Witt ring of elementary type, then R is either basic indecomposable or decomposable or a group ring (cf. [2], p. 120). Thus there are three cases.

Case 1. R is basic indecomposable. Since $B_R \neq \{1, -1\}$, R is a Witt ring of local type with $|G_R| > 4$. Hence Proposition 3 applies and gives $B_R = G_R = X_2 \subset X_3 \cup -X_3$.

Case 2. R is decomposable. The basic part of $\mathbb{Z} \times \mathbb{Z}$ is equal to $\{1, -1\}$ (see [2], Corollary 5.21), so this is excluded by the hypothesis. Thus R is decomposable and $R \neq \mathbb{Z} \times \mathbb{Z}$. The result follows now from Proposition 1 (ii).

Case 3. R is a group ring. In this case there exist a basic Witt ring S and an elementary 2-group Δ such that $R = S[\Delta]$. Hence $B_R = G_S = B_S$ (see [2], Corollary 5.20). From the equality $B_R = B_S$ it follows that $B_S \neq \{1, -1\}$. The element a is not birigid in R thus it belongs to B_S (cf. [2], p. 115).

Here S is either decomposable or indecomposable. If S is indecomposable, then S is basic indecomposable, so we have case 1 for S and the equality $B_R = B_S$ implies $B_R = X_2 \subset X_3 \cup -X_3$.

If S is decomposable, then we have case 2 for S and the equality $B_R = B_S$ implies $B_R = X_3 \cup -X_3$.

Remark. The theorem applies to all finitely generated reduced Witt rings (cf. [2], Corollary 4.28 and Corollary 6.25) and, in particular, to Witt rings of Pythagorean fields with finite group of square classes. Also, Witt ring of any field with group of square classes of order at most 32, is of elementary type [1], hence its basic part is essentially $X_3 \cup -X_3$.

3. Some examples. In this section we give examples showing that for elementary Witt rings our result is best possible.

EXAMPLE 1. We first exhibit Witt rings R of elementary type with $B_R \neq X_2 \cup -X_2$.

Let R_1, R_2 be Witt rings with $4 \leq |G_{R_1}| < \infty$, $4 \leq |G_{R_2}| < \infty$. Consider group rings $S = R_1[x]$, $T = R_2[y]$ with $G_S = G_{R_1} \times \{1, x\}$ and $G_T = G_{R_2} \times \{1, y\}$.

We shall show that the Witt ring $R = S \times T$ and the element $a = (x, y) \in G_R$ satisfy $B_R \neq X_2 \cup -X_2$.

Using this notation, we have

$$X_1 = D \langle 1, (x, y) \rangle = D \langle 1, x \rangle \times D \langle 1, y \rangle = \{(1, 1), (x, 1), (1, y), (x, y)\}$$

and by formula (2.4)

$$X_2 = G_S \times \{1, -y\} \cup \{1, -x\} \times G_T.$$

Clearly, $\{1, -x\} \times \{1, -y\} \subset G_S \times \{1, -y\} \cap \{1, -x\} \times G_T$, so $|X_2| < 2|G_S| + 2|G_T|$.

Since $8 \leq |G_S| < \infty$ and $8 \leq |G_T| < \infty$, we have

$$(3.1) \quad |X_2 \cup -X_2| < 4|G_S| + 4|G_T| \leq |G_S||G_T| = |G_R|.$$

Since R is a decomposable Witt ring, Proposition 1 and inequality (3.1) above imply that $B_R = G_R \neq X_2 \cup -X_2$.

EXAMPLE 2. Now we give examples of Witt rings of elementary type such that $B_R \neq X_3 \cup -X_2 \cup X_2$.

Let $R = S[\Delta] \times T$ with $|G_S| \geq 4$, $|G_T| \geq 2$ and T Pythagorean. If $X_1 = D \langle 1, a \rangle$, where $a = (u, 1)$, $u \in \Delta$, then $X_3 \cup \pm X_2 \neq B_R = G_R$. Indeed, u is birigid in $S[\Delta]$; hence $Y_2 = \{1, -u\}$, $Y_3 = \{1, u\}$. Since $Z_2 = \emptyset$, formulas (2.4) and (2.6) imply that

$$X_2 = \{1, -u\} \times G_T, \quad X_3 = \{1, u\} \times G_T \cup G_{S[\Delta]} \times (G_T \setminus \{-1\}).$$

It is easy to see that, if $v \notin \{1, -1, u, -u\}$, then $b = (v, -1) \notin X_3 \cup X_2 \cup -X_2$.

We should like to thank Professor K. Szymiczek for commenting on the manuscript.

This paper was written while the authors were on leave from University Pedagogical College, Szczecin, and stayed at the Institute of Mathematics of Silesian University in Katowice.

References

- [1] A. Carson, M. Marshall, *Decomposition of Witt rings*, Canad. J. Math. 34 (1982), 1276–1302.
- [2] M. Marshall, *Abstract Witt rings*, Queen's papers in pure and applied math. no. 57, Kingston, Ontario 1980.
- [3] K. Szymiczek, *Structure of the basic part of a field*, J. Algebra (to appear).

INSTYTUT MATEMATYKI UNIWERSYTETU SZCZECIŃSKIEGO
INSTITUTE OF MATHEMATICS OF THE SZCZECIN UNIVERSITY
