ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 19, Number 3, Summer 1989

DECOMPOSING WITT RINGS OF CHARACTERISTIC TWO

MURRAY MARSHALL

The Witt rings considered here are the abstract Witt rings in the sense of [**6**]. A major problem is the following: Is every finitely generated Witt ring necessarily of elementary type? We restrict our attention to Witt rings of characteristic 2. This simplifies matters considerably. Just as an example, the classification of Witt rings with a 1-sided rigid element is pretty complicated [**2**]. If the characteristic is 2, then 1-sided rigids are automatically 2-sided so the classification is comparatively easy [**1**].

The main result here is to give necessary and sufficient conditions for a Witt ring of characteristic 2 to be a product (in the category of Witt rings) of group rings (see Theorem 1) or group rings and dyadic local types (see Theorem 2). This has similarities with the problem tackled in [**4**]. However the motivation here is different: we try to generalize the characterization of a product of two group rings given in [**3**, Theorem 3.10]. Once this result is established, it is used to obtain a characterization of elementary Witt rings of characteristic 2 (see Theorems 7 and 8). It is not clear how to generalize any of this to the characteristic $\neq 2$ case.

An earlier version of this paper [**7**] was submitted for publication and then later withdrawn in favor of the present paper. The results presented here, although they still leave something to be desired, are a substantial improvement over the results in [**7**].

Terminology and notation are as in [**3**, **6**, **8**]. Throughout, R denotes a Witt ring of characteristic 2, and G denotes the distinguished subgroup of units of R. The associated quaternionic pairing is denoted by $q : G \times G \to Q$. For $a \in G$, $D\langle 1, a\rangle$ denotes the value group of the 1-fold Pfister form $\langle 1, a\rangle$, i.e., $D\langle 1, a\rangle = \{x \in G | q(x, a) = 0\}$. Of course, we are assuming $\text{char}(R) = 2$, so $-a = a$ holds for all $a \in G$.

Received by the editors on October 3, 1986 and in revised form on April 15, 1987.

1. The decomposition criterion. Define the *radical* of an element $a \in G$ to be the set of all $b \in G$ satisfying $D\langle 1, a\rangle \subseteq D\langle 1, b\rangle$. This is a subgroup of G which we denote by $\operatorname{rad}(a)$. Clearly $\{1, a\} \subseteq \operatorname{rad}(a) \subseteq D\langle 1, a\rangle$. Observe that $\operatorname{rad}(1) = \{x \in G | q(x, y) = 0 \ \forall\ y \in G\}$. $\operatorname{rad}(1)$ is sometimes referred to as the Kaplansky radical of q.

Suppose now that there is some element $1 \neq a \in G$ with $|D\langle 1, a\rangle|$ finite. Of all such elements a pick one with $|D\langle 1, a\rangle|$ smallest possible, say $|D\langle 1, a\rangle| = 2^m$. If $m = 1$, then $D\langle 1, a\rangle = \{1, a\}$, i.e., a is rigid, so by [**1**] (or [**6**]), R is a group ring. If $m = 2$, then $D\langle 1, a\rangle = \{1, a, b, ab\}$ for some $b \in G$, so, by [**3**], R is a product of two group rings.

If $m = 1$ or 2, then clearly $\operatorname{rad}(a) = D\langle 1, a\rangle$. However, if $m = 3$ there are two possibilities. Either (1) $\operatorname{rad}(a) = D\langle 1, a\rangle$ or (2) $\operatorname{rad}(a) = \{1, a\}$. (One checks that these are the only possibilities.) In case (1) one might expect that R is the product of 3 group rings. In case (2) one might expect that R is the dyadic local type $L_{4,0}$. Neither of these results has been proved.

Define $n \geq 1$ by $|\operatorname{rad}(a)| = 2^n$. (Conceivably, this depends on our choice of $a \in G$.) Thus, for example, if R is a group ring, $D\langle 1, a\rangle = \{1, a\} = \operatorname{rad}(a)$ and $m = n = 1$. Also, if R is a dyadic local type, say $R = L_{2v,0}$, then $D\langle 1, a\rangle$ has index 2 in G and $\operatorname{rad}(a) = \{1, a\}$ so $m = 2v - 1$, $n = 1$. More generally, suppose R is the product of Witt rings $R_1, \ldots R_\ell$ and that $R_i = L_{2v_i,0}$ for $i \leq k$ and that R_i is a group ring for $i \rangle k$. Then $m = \sum_1^k (2v_i - 1) + (\ell - k)$ and $n = \ell$. Thus, in general, one might expect n (not m) to reflect the number of factors of R in its decomposition as a product. Also, one might expect the case when $m = n$ (i.e., when $\operatorname{rad}(a) = D\langle 1, a\rangle$) to correspond to the case when R is a product of n group rings. Of course, there is no proof of these assertions in general.

Suppose $m \geq 2$. Then, by [**1**], the basic part of G is all of G. Define $X_1 = D\langle 1, a\rangle$ and for $i \geq 2$ define X_i inductively by $X_i = \cup\{D\langle 1, x\rangle | x \in X_{i-1},\ x \neq 1\}$. According to [**3**], $G = X_1 X_2^2 \cup X_1 X_3$. This is the best general result known and is valid for any $a \in G$, $a \neq 1$. There is some evidence (e.g., see [**5**] and [**9**]) that this result is not best possible. Since the element $a \in G$ being considered has been chosen so that $|D\langle 1, a\rangle| = 2^m$ is smallest possible, there is even hope that a much stronger result may hold, namely:

$$(*) \qquad G = D\langle 1, b\rangle D\langle 1, ab\rangle \quad \text{for all} \quad b \in D\langle 1, a\rangle.$$

For example, this is true if R is of elementary type. Also observe that (*) is true (trivially) if $m = 1$. The proof of (*) in case $m = 2$ was an important step in the proof that R is a product of two group rings in this case. Another case where (*) holds will be considered in the next section.

We are now ready to state the main results:

THEOREM 1. *Suppose R is a Witt ring of characteristic 2. Then, in the category of Witt rings, R is a product of n group rings if and only if there exists an element $1 \neq a \in G$ satisfying:*

(i) $\operatorname{rad}(a) = D\langle 1, a\rangle$ *has* 2^n *elements and*

(ii) $D\langle 1, b\rangle D\langle 1, ab\rangle = G$ *holds for all* $b \in \operatorname{rad}(a)$.

THEOREM 2. *Suppose R is a Witt ring of characteristic 2. Then, in the category of Witt rings, R is a (finite) product of Witt rings which are either group rings of dyadic local types if and only if $\exists$ an element $1 \neq a \in G$ satisfying:*

(i) $D\langle 1, a\rangle$ *is finite and $\exists$ a set $B \subseteq D\langle 1, a\rangle$ which is a basis for $D\langle 1, a\rangle$ modulo* $\operatorname{rad}(a)$ *such that $D\langle 1, b\rangle$ has index 2 in G for all $b \in B$; and*

(ii) $D\langle 1, b\rangle D\langle 1, ab\rangle = G$ *holds for all* $b \in \operatorname{rad}(a)$.

In both of the above Theorems, one implication is easy. For suppose R is the product of n Witt rings $R_1, \ldots, R_n$ where each R_i is either a group ring or a dyadic local type. Thus $G = G_1 \times \cdots \times G_n$ where G_i denotes the distinguished subgroup of units in R_i. Fix an element $a_i \in G_i$ such that $a_i \neq 1$ and a_i is rigid if R_i is a group ring. Take $a = (a_1, \ldots, a_n)$. (i) and (ii) are now straightforward to check.

The non-trivial portion of the proof of Theorems 1 and 2 is deferred until §3.

2. Characterization of elementary types. Fix $a \in G$. For each $y \in G$ define $H_y = D\langle 1, a\rangle D\langle 1, y\rangle$. For fixed $x \in G$, the union of the groups H_{bx}, $b \in D\langle 1, a\rangle$, is precisely the value set of the 2-

fold Pfister form $\langle 1, a, x, ax\rangle$ and is thus itself a group. In case R is of elementary type, the explanation of this fact is easy enough: In this case the set $\{H_{bx} | b \in D\langle 1, a\rangle\}$ actually has a largest element (with respect to inclusion). For R of elementary type, the set $\{H_{bx} | b \in \mathrm{rad}(a)\}$ also has a largest element and both of these sets are closed under intersection so also have smallest elements. All these facts are easy (but tedious) to check, e.g., see [7]. The proofs are omitted.

The results which follow show the importance of determining to what extent the above properties hold in case R is arbitrary, i.e., not necessarily of elementary type. To date, very little is known. Here is one general result.

LEMMA 3. *For any* $b \in \mathrm{rad}(a)$, $H_x \cap H_{ax} \subseteq H_{bx}$.

PROOF. Let $y \in H_x \cap H_{ax}$, $b \in \mathrm{rad}(a)$. Then $y = cz$ where $c \in D\langle 1, a\rangle$ and $z \in D\langle 1, x\rangle \cap D\langle 1, a\rangle D\langle 1, ax\rangle$. Thus $\exists\ d \in D\langle 1, a\rangle$ such that $q(dz, ax) = 0$, and so $q(z, a) = q(d, x)$. Since $b \in \mathrm{rad}(a)$, $q(ab, d) = 0$ implies $q(d, x) = q(d, abx)$. Then $q(z, a) = q(d, abx)$, and, by linkage, $\exists\ e \in D\langle 1, a\rangle$ such that $q(z, a) = q(ez, a) = q(ez, abx) = q(d, abx)$. Thus $ez \in D\langle 1, bx\rangle$, giving $y = cz = (ce)(ez) \in D\langle 1, a\rangle D\langle 1, bx\rangle = H_{bx}$. □

LEMMA 4. (i) *The set* $\{H_{bx} | b \in \mathrm{rad}(a)\}$ *has a smallest element if and only if* $\exists\ c \in \mathrm{rad}(a)$ *such that* $H_{cx} \subseteq H_{acx}$ *(in which case* H_{cx} *is the smallest element).*

(ii) *If the set* $\{H_{bx} | b \in \mathrm{rad}(a)\}$ *has a largest element, then it also has a smallest element.*

PROOF. The first assertion is immediate from Lemma 3. For the second assertion, if H_{acx} is the largest element, then, by (i), H_{cx} is the smallest element. □

The next two results indicate how the lattice structure of $\{H_{bx} | b \in D\langle 1, a\rangle\}$ relates the property (*) considered in §1.

LEMMA 5. *Suppose* $1 \neq a \in G$ *is chosen so that* $|D\langle 1,a\rangle| = 2^m$ *is finite and smallest possible. Suppose further that* $x \in G$ *satisfies* $H_x \subseteq H_{ax}$. *Then* $|D\langle 1,x\rangle| = 2^m$ *and, for each* $b \in D\langle 1,a\rangle$, $x \in D\langle 1,b\rangle D\langle 1,ab\rangle$.

PROOF. To begin let $a,x \in G$ be arbitrary. If $t \in D\langle 1,x\rangle \cap D\langle 1,a\rangle D\langle 1,ax\rangle$, then $\exists c \in D\langle 1,a\rangle$ such that $q(ct,ax) = 0$ and so $c = (t)(ct) \in D\langle 1,a\rangle \cap D\langle 1,x\rangle D\langle 1,ax\rangle$. Conversely, each $c \in D\langle 1,a\rangle \cap D\langle 1,x\rangle D\langle 1,ax\rangle$ arises in this way for some $t \in D\langle 1,x\rangle \cap D\langle 1,a\rangle D\langle 1,ax\rangle$. Observe that $c \in D\langle 1,x\rangle \Leftrightarrow c \in D\langle 1,ax\rangle \Leftrightarrow t \in D\langle 1,ax\rangle \Leftrightarrow t \in D\langle 1,a\rangle$. We have a group isomorphism

$$\frac{D\langle 1,x\rangle \cap D\langle 1,a\rangle D\langle 1,ax\rangle}{D\langle 1,a\rangle \cap D\langle 1,x\rangle} \cong \frac{D\langle 1,a\rangle \cap D\langle 1,x\rangle D\langle 1,ax\rangle}{D\langle 1,a\rangle \cap D\langle 1,x\rangle} \tag{**}$$

induced by $t \leftrightarrow c$.

Now suppose that x,a satisfy the special hypothesis in the statement of the lemma. Then $H_x \subseteq H_{ax}$ so $D\langle 1,x\rangle \subseteq D\langle 1,a\rangle D\langle 1,ax\rangle$. Since $D\langle 1,x\rangle$ has at least 2^m elements (by choice of m), (**) implies that $D\langle 1,x\rangle$ has exactly 2^m elements and further that $D\langle 1,a\rangle \subsetneq D\langle 1,x\rangle D\langle 1,ax\rangle$. Finally, suppose $b \in D\langle 1,a\rangle$ is arbitrary. Then $\exists\, t \in D\langle 1,x\rangle$ with $q(bt,ax) = 0$, i.e., $q(b,x) = q(t,a)$. Thus, by linkage $\exists\, d \in D\langle 1,a\rangle$ such that $q(t,a) = q(dt,a) = q(dt,b) = q(x,b)$ so $dt \in D\langle 1,ab\rangle$ and $dt\,x \in D\langle 1,b\rangle$. Therefore $x = (dt\,x)(dt) \in D\langle 1,b\rangle D\langle 1,ab\rangle$. □

LEMMA 6. *Suppose* $1 \neq a \in G$ *is chosen so that* $|D\langle 1,a\rangle| = 2^m$ *is finite and smallest possible. Suppose further that, for each* $x \in G$, *the set* $\{H_{cx} | c \in \operatorname{rad}(a)\}$ *has a smallest element (with respect to inclusion). Then, for each* $b \in D\langle 1,a\rangle$, $D\langle 1,b\rangle D\langle 1,ab\rangle = G$.

PROOF. Let $y \in G$, $b \in D\langle 1,a\rangle$ be arbitrary. By assumption $\exists c \in \operatorname{rad}(a)$ such that $x := cy$ satisfies $H_x \subseteq H_{ax}$. Thus, by Lemma 5, $x \in D\langle 1,b\rangle D\langle 1,ab\rangle$. Since $c \in \operatorname{rad}(a) \subseteq D\langle 1,b\rangle$, this implies that $y = cx$ is also in $D\langle 1,b\rangle D\langle 1,ab\rangle$. □

We introduce some notation. Denote by $\mathcal{E}_0$ (respectively $\mathcal{E}_1$) the smallest class of Witt rings containing $\mathbf{Z}/2$ (respectively $\mathbf{Z}/2$ and all the dyadic local types $L_{2v,0}, v \geq 2$) and closed under the following two operations:

(1) group ring formation $R \to R[C_2]$, C_2 cyclic of order 2 and

(2) product formation $(R, S) \to R \times S$.

Thus $\mathcal{E}_1$ is just the class of elementary types of characteristic 2. According to [**3**, Corollary 4.4], $\mathcal{E}_1$ is also characterized as the smallest class of Witt rings containing $\mathbf{Z}/2$ and closed under operation (1) and under the formation of *weak* products.

THEOREM 7. *Suppose R has characteristic 2, $|G| < \infty$. Then R belongs to the class $\mathcal{E}_0$ if and only if the following two conditions hold for all elements $1 \neq a \in G$ with $D\langle 1, a\rangle$ minimal (with respect to inclusion):*

(i) $D\langle 1, a\rangle = \operatorname{rad}(a)$;

(ii) *For all $x \in G$, the set $\{H_{bx} | b \in \operatorname{rad}(a)\}$ has a smallest element.*

Caution. $D\langle 1, a\rangle$ can be minimal without $|D\langle 1, a\rangle|$ being minimal.

THEOREM 8. *Suppose R has characteristic 2 and $|G| < \infty$. Then R belongs to the class $\mathcal{E}_1$ if and only if the following two conditions hold for all $a \in G$ with $D\langle 1, a\rangle$ minimal:*

(i) *$D\langle 1, a\rangle$ is generated by elements $b \in D\langle 1, a\rangle$ such that the group $D\langle 1, b\rangle \cap D\langle 1, a\rangle$ has index 1 or 2 in $D\langle 1, a\rangle$;*

(ii) *For all $x \in G$, the set $\{H_{bx} | b \in \operatorname{rad}(a)\}$ has a smallest element.*

Note. If $b \in D\langle 1, a\rangle$, then $D\langle 1, b\rangle \cap D\langle 1, a\rangle$ has index 1 in $D\langle 1, a\rangle$ if and only if $b \in \operatorname{rad}(a)$. Thus condition (i) of Theorem 8 is just a bit weaker than the corresponding condition of Theorem 7.

PROOF. One implication is easy so the proof is omitted. For the other, assume hypotheses (i) and (ii) hold for all $1 \neq a \in G$ with $D\langle 1, a\rangle$ minimal. Choose an element $1 \neq a \in G$ with $|D\langle 1, a\rangle|$ smallest

possible. Then $D\langle 1,a\rangle$ is obviously minimal, so, by (ii) and Lemma 6, $D\langle 1,b\rangle D\langle 1,ab\rangle = G$ holds for all $b \in D\langle 1,a\rangle$. By (i) there is a basis B of $D\langle 1,a\rangle$ modulo $\mathrm{rad}(a)$ such that $D\langle 1,b\rangle \cap D\langle 1,a\rangle$ has index 2 in $D\langle 1,a\rangle$ for all $b \in B$. (Of course, $B = 0$ if $\mathrm{rad}(a) = D\langle 1,a\rangle$.) By (ii), each $b \in B$ can be modified by multiplying by a suitable element of $\mathrm{rad}(a)$ so as to satisfy $H_{ab} \subseteq H_b$. This doesn't change the index of $D\langle 1,b\rangle \cap D\langle 1,a\rangle$ so we may as well assume, to begin with, that this holds for all $b \in B$. Thus we have $D\langle 1,b\rangle D\langle 1,ab\rangle = G$ and $D\langle 1,ab\rangle \subseteq D\langle 1,a\rangle D\langle 1,b\rangle$, so $D\langle 1,a\rangle D\langle 1,b\rangle = G$. Then $D\langle 1,b\rangle$ has index 2 in G for each $b \in B$, and, by Theorem 2, $R = R_1 \times \cdots \times R_n$ where each R_i is a group ring or a dyadic local type. (If $\mathrm{rad}(a) = D\langle 1,a\rangle$, apply Theorem 1 instead to conlcude that all the R_i are group rings in this case.) The desired conclusion now follows by induction on $|G|$. To be able to apply induction one has to make sure that if R_i is a group ring, say $R_i = S_i[C_2]$, then (i) and (ii) hold for each $x_i \in H_i$ (= the distinguished group of units of S_i) with $D_i\langle 1,x_i\rangle$ minimal. The reason this works is that any such x_i is the i-th component of some $x \in G$ with $D\langle 1,x\rangle$ minimal. □

3. End of proofs. First we give a proof of Theorem 2, assuming Theorem 1. This turns out to be fairly easy.

Thus we suppose that R has characteristic 2 and that there exists an element $1 \neq a \in G$ satisfying conditions (i) and (ii) of Theorem 2. Suppose $B \neq 0$, say $b_1 \in B$. Since $b_1 \notin \mathrm{rad}(a)$, there exists $b_2 \in B$ with $q(b_1,b_2) \neq 0$. Thus G decomposes as $G = [b_1,b_2] \perp \overline{G}$ where $\overline{G} = D\langle 1,b_1\rangle \cap D\langle 1,b_2\rangle$. (Here, $[b_1,b_2]$ denotes the subgroup generated by b_1,b_2.) Continuing in this way, working with the induced quaternionic structure on $\overline{G}$, one sees that $|B|$ is even, say $|B| = 2s$, and G has a decomposition

$$G = [b_1,b_2] \perp \cdots \perp [b_{2s-1},b_{2s}] \perp G'.$$

Observe that $a \in G'$ and that $\mathrm{rad}(a) = \mathrm{rad}'(a) = D'\langle 1,a\rangle$. Also, $D'\langle 1,b\rangle D'\langle 1,ab\rangle = G'$ for all $b \in D'\langle 1,a\rangle$. Thus, by Theorem 1, the Witt ring of G' is a product of group rings. Clearly the Witt ring of each $[b_{2i-1},b_{2i}]$ is the local type $L_{2,0}$. Thus R is a weak product of local types and group rings so the result follows from [**3**, Corollary 3.8 and Remark 3.9].

It remains to prove Theorem 1. This takes up the remainder of the paper. Assume R has characteristic 2 and that there exists an element $a \in G$ satisfying (i) and (ii) of Theorem 1. We want to show that R is the product of n group rings. If R is degenerate (i.e., if $\exists\, x \in G,\ x \neq 1$ such that $D\langle 1, x\rangle = G$), then R decomposes as a Witt product, namely $R \cong R' \times \mathbf{Z}/2[C_2], C_2$ cyclic of order 2. Denote by a' the component of a in $G' \subseteq R'$. Then a' has all the properties of a except that now $D'\langle 1, a'\rangle$ has order 2^{n-1}. Thus, by induction on n, R' is the Witt product of $n-1$ group rings and we are done. Thus we may as well assume to begin with that R is non-degenerate. The proof is by means of several lemmas.

LEMMA 9. *Suppose* $\beta \in D\langle 1, a\rangle$, $x \in G$. *Suppose* $x = x_1 x_2$ *is a decomposition of* x *with* $x_1 \in D\langle 1, \beta\rangle$, $x_2 \in D\langle 1, a\beta\rangle$. *Then* $D\langle 1, x\rangle \cap D\langle 1, a\rangle$ *is a subgroup of* $D\langle 1, x_i\rangle \cap D\langle 1, a\rangle$, $i = 1, 2$.

PROOF. Let $\alpha \in D\langle 1, x\rangle \cap D\langle 1, a\rangle$. Then $q(x, \alpha\beta) = q(x, \beta) = q(x_2, \beta) = q(x_2, a)$. By linkage, $\exists\, \gamma \in D\langle 1, a\rangle$ such that $q(x_2, a) = q(\gamma x_2, a) = q(\gamma x_2, \alpha\beta) = q(x, \alpha\beta)$. Thus $q(\gamma x_1, \alpha\beta) = 0$. By (i), $q(\gamma, \alpha\beta) = 0$, so this implies that $q(x_1, \alpha\beta) = 0$. Since $q(x_1, \beta) = 0$, this in turn implies that $q(x_1, \alpha) = 0$. Finally, $q(x, \alpha) = 0$, so this implies $q(x_2, \alpha) = 0$, too. □

LEMMA 10. *Under the hypothesis of Lemma* 9, *suppose* $q(x, \beta) \neq 0$, $q(x, a\beta) \neq 0$. *Then* $q(x_i, a) \neq 0$, $i = 1, 2$, *and the inclusions in Lemma* 9 *are proper.*

PROOF. If $q(x_1, a) = 0$, then $q(x, a\beta) = q(x_1, a\beta) = q(x_1, a) = 0$, a contradiction. Thus $q(x_1, a) \neq 0$. Similarly, since $q(x, \beta) \neq 0$, it follows that $q(x_2, a) \neq 0$. The second assertion is clear since $\beta \in D\langle 1, x_1\rangle$ but $\beta \notin D\langle 1, x\rangle$ and $a\beta \in D\langle 1, x_2\rangle$ but $a\beta \notin D\langle 1, x\rangle$. □

We will say $x \in G \backslash D\langle 1, a\rangle$ is *maximal* if the group $D\langle 1, x\rangle \cap D\langle 1, a\rangle$ is maximal with respect to inclusion. It follows from Lemmas 9 and 10 that

(1) $x \in G \backslash D\langle 1, a\rangle$ is maximal if and only if $D\langle 1, x\rangle \cap D\langle 1, a\rangle$ has

index 2 in $D\langle 1,a\rangle$ and

(2) Each element $x \in G\backslash D\langle 1,a\rangle$ is a finite product of maximal elements. (This follows by induction on the index of $D\langle 1,x\rangle \cap D\langle 1,a\rangle$ in $D\langle 1,a\rangle$.)

Put an equivalence relation on the set of maximal elements by declaring $x \sim y$ to mean $D\langle 1,x\rangle \cap D\langle 1,a\rangle = D\langle 1,y\rangle \cap D\langle 1,a\rangle$. Note:

(3) If $\alpha \in D\langle 1,a\rangle$ and x is maximal, then αx is also maximal and $\alpha x \sim x$. (This is immediate from hypothesis (i).)

(4) If x, y are maximal and $x \sim y$, then either $xy \in D\langle 1,a\rangle$ or xy is maximal and $xy \sim x$.

It follows from (3) and (4) that, for any maximal $x \in G\backslash D\langle 1,a\rangle$, the set

$$\Delta = \{y : y \text{ is maximal and } y \sim x\} \cup D\langle 1,a\rangle$$

is a subgroup of G. □

LEMMA 11. *If $t_1, \ldots, t_s$ are pairwise inequivalent maximal elements, then*

(1) *$t_1, \ldots, t_s$ are linearly independent modulo $D\langle 1,a\rangle$ and*

(2) $D\langle 1, t_1, \ldots, t_s\rangle \cap D\langle 1,a\rangle = \cap_i D\langle 1,t_i\rangle \cap D\langle 1,a\rangle$.

PROOF. For (1) we show, by induction on s, that if $s \geq 1$ then $q(t_1 \ldots t_s, a) \neq 0$. Suppose to the contrary that $q(t_1 \ldots t_s, a) = 0$. Then $s \geq 2$. Since t_1 and t_s are inequivalent there is some $\beta \in D\langle 1,a\rangle$ such that $q(t_s, \beta) = 0$ and $q(t_1, a\beta) = 0$. Rearranging $t_1, \ldots, t_s$ we have $1 \leq k < s$ such that $q(t_i a\beta) = 0$ for $i \leq k$ and $q(t_i, \beta) = 0$ for $i > k$. Thus $q(t_1 \ldots t_k, \beta) = q(t_1 \ldots t_k, a)$ and $q(t_{k+1} \ldots t_s, \beta) = 0$, so $q(t_1 \ldots t_s, \beta) = q(t_1 \ldots t_k, a)$. On the other hand, since $q(t_1 \ldots t_s, a) = 0$, it follows from (i) that $q(t_1 \ldots t_s, \beta) = 0$. Thus $q(t_1 \ldots t_k, a) = 0$. Since $1 \leq k < s$ this is a contradiction.

For (2) suppose to the contrary that $\beta \in D\langle 1,a\rangle$ $q(t_1 \ldots t_s, \beta) = 0$, but $q(t_1, a\beta) = 0$. Then, rearranging $t_1, \ldots, t_s$, we have $1 \leq k \leq s$ such that $q(t_i, a\beta) = 0$ for $i \leq k$ and $q(t_i, \beta) = 0$ for $i\rangle k$. Then $q(t_1 \ldots t_k, a) = q(t_1 \ldots t_k, \beta) = q(t_1 \ldots t_s, \beta) = 0$. This contradicts (1). □

Suppose there are s equivalence classes of maximal elements so we have pairwise inequivalent maximal elements $t_1, \ldots, t_2$ and every maximal t is equivalent to one of these. Let $\Delta_1, \ldots, \Delta_s$ be the corresponding subgroups of G. Thus $G = \Delta_1 \ldots \Delta_s$ and, by Lemma 11, this product is direct modulo $D\langle 1, a\rangle$. Since there are $2^n - 1$ subgroup of index 2 in $D\langle 1, a\rangle$ it follows that $s < 2^n$. We want to show that $s = n$. We do this by showing that the t_i correspond to linearly independent characters on $D\langle 1, a\rangle$. The proof uses the following Lemma which will also be used later.

LEMMA 12. *Suppose* $x \in D\langle 1, \beta\rangle$, $y \in D\langle 1, a\beta\rangle$ *for some* $\beta \in D\langle 1, a\rangle$. *Then* $\exists\ \gamma \in D\langle 1, a\rangle$ *such that* $q(\gamma x, \gamma y) = 0$.

PROOF. $q(xy, \beta) = q(y, \beta) = q(y, a)$, so, by linkage, $\exists\, \delta \in D\langle 1, a\rangle$ such that $q(y, a) = q(\delta y, a) = q(\delta y, xy) = q(xy, \beta)$. Thus $q(xy, \delta\beta y) = 0$. Since $q(\delta\beta y, \delta\beta y) = 0$, this implies $q(\delta\beta x, \delta\beta y) = 0$. Now take $\gamma = \delta\beta$. □

LEMMA 13. *Suppose* $t_1, \ldots, t_s$ *are pairwise inequivalent maximal elements. Then the group* $\cap_i D\langle 1, t_i\rangle \cap D\langle 1, a\rangle$ *has index* 2^s *in* $D\langle 1, a\rangle$. *In particular,* $s \leq n$.

PROOF. It is clear that this index is $\leq 2^s$ and that it is equal to 2^s if $s = 1$ or 2. By induction on s we can assume that $s \geq 2$, that $H := \cap_i D\langle 1, t_i\rangle \cap D\langle 1, a\rangle$ has index 2^s and that t is some maximal element such that $H \subseteq D\langle 1, t\rangle$. We must show this implies $t \sim t_i$ for some $i \in \{1, \ldots, s\}$. Since H has index 2^s, $\exists$ elements $\beta_1, \ldots, \beta_s \in D\langle 1, a\rangle$ satisfying $q(t_i, a\beta_i) = 0$ and $q(t_j, \beta_i) = 0$ for $j \neq i$. In particular, $\beta_1, \ldots, \beta_s$ generate $D\langle 1, a\rangle$ modulo H. Now $q(t, a\beta_i) = 0$ for some i. (Otherwise $q(t, \beta_i) = 0$ for all i, so $q(t, \beta) = 0$ for all $\beta \in D\langle 1, a\rangle$, a contradiction.) Without loss of generality, we can assume $q(t, a\beta_s) = 0$. Then $q(tt_s, a\beta_s) = 0$ and $q(t_1 \ldots t_{s-1}, \beta_s) = 0$. Take $x = t_1 \ldots t_{s-1}$, $y = tt_s$. Thus, by Lemma 12, $\exists \gamma \in D\langle 1, a\rangle$ such that $q(\gamma x, \gamma y) = 0$. Replacing t_1 by γt_1 and t_s by γt_s we can assume $\gamma = 1$ so that $q(x, y) = 0$. Also, for each $i = 1, \ldots, s - 1$, we can apply Lemma 12 again (but to the elements $x, \beta_i y$ instead

of x, y) to get an element $\alpha \in D\langle 1, a\rangle$ (depending on i) such that $q(\alpha x, \alpha\beta_i y) = 0$. Expanding, this yields $q(\alpha, xy) = q(\beta_i, x)$. Now $q(\beta_i, x) = q(\beta_i, t_1 \dots t_{s-1}) = q(\beta_i, t_i) = q(a, t_i)$. Say $\alpha = \Pi_j \beta_j^{e_j} \delta$, $\delta \in H$, $e_j \in \{0,1\}$. Thus $q(\alpha, xy) = q(\alpha, t_1, \dots t_s t) = q(a, t_1^{e_1} \dots t_s^{e_s} t^f)$ where $f \in \{0,1\}$ is defined by $q(\alpha, t) = q(a, t^f)$. Then the equation $q(\alpha, xy) = q(\beta_i, x)$ reduces to $q(a, t_1^{e_1} \dots t_i^{e_i+1} \dots t_s^{e_s} t^f) = 0$. According to Lemma 11 this can only hold if $e_i = 1$, $e_j = 0$, for $j \neq i$, and $f = 0$. This gives $\alpha \equiv \beta_i \bmod H$ and $q(\beta_i, t) = q(\alpha, t) = 0$ (since $f = 0$). Thus $q(\beta_i, t) = 0$ for $i = 1, \dots, s-1$. Since $q(a\beta_s, t) = 0$ and $q(\delta, t) = 0$ for all $\delta \in H$, this implies that $t \sim t_s$.

Now suppose $t_1, \dots, t_s$ is a maximal set of pairwise inquivalent maximal elements and that $\Delta_1, \dots, \Delta_s$ are the associated subgroups of G. Thus $H = \cap_i D\langle 1, t_i\rangle \cap D\langle 1, a\rangle$ has index 2^s in $D\langle 1, a\rangle$ so that $s \leq n$. For any $\beta \in H$, $q(\beta, t_i) = 0$ for $i = 1, \dots, s$ so $q(\beta, t) = 0$ for all $t \in G$. Since we are assuming R is non-degenerate this implies $H = 1$, $s = n$. □

LEMMA 14. *Suppose t, u are inequivalent maximal elements. Then exactly one of the following holds*:

$$q(t,u) = 0,\ q(at,u) = 0,\ q(t,au) = 0,\ q(at,au) = 0.$$

PROOF. Since t, u are inequivalent $\exists \beta \in D\langle 1, a\rangle$ such that $q(t, \beta) = 0$, $q(u, a\beta) = 0$ (so $q(t, a\beta) \neq 0$, $q(u, \beta) \neq 0$). By Lemma 12, $\exists \gamma \in D\langle 1, a\rangle$ such that $q(\gamma t, \gamma u) = 0$. Since t, u are maximal, there are 4 possibilities:

(1) $q(\gamma, t) = 0$, $q(\gamma, u) = 0$;

(2) $q(\gamma, t) = 0$, $q(a\gamma, u) = 0$;

(3) $q(a\gamma, t) = 0$, $q(\gamma, u) = 0$;

(4) $q(a\gamma, t) = 0$, $q(a\gamma, u) = 0$.

Expanding the equation $q(\gamma t, \gamma u) = 0$ in each of these 4 cases yields the 4 possibilities listed in the statement of the Lemma. Using $q(t, a) \neq 0$, $q(u, a) \neq 0$, and $q(tu, a) \neq 0$, one verifies easily that these 4 possibilities are mutually exclusive.

Now let $\Delta_1, \dots, \Delta_n$ be the subgroups of G corresponding to the n equivalence classes of maximal elements. Thus $D\langle 1, a\rangle \subseteq \Delta_i$ and

$t_i \in \Delta_i$ is maximal if and only if $t_i \notin D\langle 1, a\rangle$. Let us say that a maximal element $t_i \in \Delta_i$ is Δ_j-*compatible* ($j \neq i$) if $q(t_i, t_j) = 0$ or $q(t_i, at_j) = 0$ for all maximal $t_j \in \Delta_j$.

LEMMA 15. *For each $i, j, i \neq j$ and each maximal $t_i \in \Delta_i$, either t_i or at_i is Δ_j-compatible.*

PROOF. If the result is false, then there exist maximal $t_j, u_j \in \Delta_j$ such that $q(t_i, t_j) = 0$, $q(at_i, u_j) = 0$. Consider the element $t_j u_j \in \Delta_j$. If this is maximal, then, by Lemma 14, we either have

$$q(t_i, a^e t_j u_j) = 0 \tag{1}$$

or

$$q(at_i,\ a^f t_j u_j) = 0 \tag{2}$$

for suitable $e, f \in \{0, 1\}$. In case (1), $q(t_i, a^e u_j) = 0$ and $q(at_i, u_j) = 0$, contradicting Lemma 14. Similarly, in case (2), $q(at_i, a^f t_j) = 0$ and $q(t_i, t_j) = 0$, contradicting Lemma 14. The other possibility is that $t_j u_j$ is not maximal so $t_j u_j \in D\langle 1, a\rangle$. In this case (1) and (2) both hold for suitable e, f and again we have a contradiction to Lemma 14.

Let $\beta_1, \ldots, \beta_n$ denote the canonical basis for $D\langle 1, a\rangle$ as in the proof of Lemma 13. Thus, if t_i is any maximal element in Δ_i, then $q(t_i, a\beta_i) = 0$ and $q(t_i, \beta_j) = 0$ if $j \neq i$. □

LEMMA 16. *For given i and given maximal $t_i \in \Delta_i$ there are exactly two elements t, u in the coset of t_i modulo $D\langle 1, a\rangle$ which are Δ_j-compatible for all $j \neq i$. Further $tu = \beta_i$.*

PROOF. We are looking for the elements $\alpha = \beta_1^{e_1} \ldots \beta_n^{e_n}$ in $D\langle 1, a\rangle$ which satisfy $q(\alpha t_i, t_j) = 0$ for all Δ_i-compatible maximal elements $t_j \in \Delta_j$, $j = 1, \ldots, n$, $j \neq i$. Now $q(\alpha t_i, t_j) = q(\beta_j^{e_j} t_i, t_j) = q(a^{e_j} t_i, t_j)$. Then, for $i \neq j$, we must have $e_j = 0$ if t_i is Δ_j-compatible and $e_j = 1$ if at_i is Δ_j-compatible. There is no restriction on $e_i \in \{0, q\}$. Thus there are exactly two elements t, u of the form $t = \alpha t_i$, $u = \alpha\beta_i t_i$ satisfying the required conditions. □

Let S_i denote the set of maximal elements in Δ_i which are Δ_j-compatible for all $j \neq i$. Observe that if $t_i \in S_i$, $t_j \in S_j$, then $q(t_i, t_j) = 0$. Thus if $t_i, u_i \in S_i$, $t_j \in S_j$, then $q(t_i u_i, t_j) = 0$. If $t_i u_i$ is maximal, this implies $t_i u_i$ is Δ_j-compatible for all $j \neq i$ so $t_i u_i \in S_i$. If $t_i u_i$ is not maximal, then $t_i u_i \in D\langle 1, a\rangle$. Since $q(t_i u_i, t_j) = 0$ for all $j \neq i$ we are forced to conclude that $t_i u_i = 1$ or β_i. From these observations it is clear that

$$G_i := S_i \cup \{1, \beta_i\}$$

is a subgroup of Δ_i.

Now consider $G_1 \dots G_n \subseteq \Delta_1 \dots \Delta_n = G$. Since $\beta_i \in G_i$ we have $D\langle 1, a\rangle \subseteq G_1 \dots G_n$. By Lemma 16, $\Delta_i \subseteq G_i D\langle 1, a\rangle$. Taken together these two results imply that $G = G_1 \dots G_n$. Suppose $t_i \in G_i$ and $t_1 \dots t_n = 1$. Since the product $G = \Delta_1 \dots \Delta_n$ is direct modulo $D\langle 1, a\rangle$ this implies $t_i \in D\langle 1, a\rangle$, so $t_i = 1$ or β_i. Since $\beta_1, \dots, \beta_n$ are linearly independent, $t_i = 1$ for $i = 1, \dots, n$. Thus the product $G = G_1 \dots G_n$ is direct.

We have also seen that $q(t_i, t_j) = 0$ whenever $t_i \in G_i$, $t_j \in G_j$, $i \neq j$. Thus $G = G_1 \times \cdots \times G_n$ is an orthogonal decomposition. Thus q induces a quaternionic structure on G_i. Denote the associated Witt ring by R_i. Suppose $t_i \in G_i$, $q(t_i, \beta_i) = 0$. Since $q(t_i, \beta_j) = 0$ for $j \neq i$, this implies that $q(t_i, a) = 0$. Thus $t_i \in D\langle 1, a\rangle \cap G_i = \{1, \beta_i\}$. This shows that $\beta_i \in G_i$ is rigid so R_i is a group ring, $i = 1, \dots, n$. According to [**3**, Theorem 3.4] this implies that the induced map $\rho : R_1 \times \cdots \times R_n \to R$ is an isomorphism. This completes the proof of Theorem 1. □

REFERENCES

1. L. Berman, C. Cordes and R. Ware, *Quadratic forms, rigid elements, and formal power series fields*, J. Algebra **66** (1980), 123-133.

2. R. Bos, *Quadratic forms, orderings, and abstract Witt rings*, dissertation, Utrecht (1984).

3. A. Carson and M. Marshall, *Decomposition of Witt rings*, Can. J. Math. **34** (1982), 1276-1302.

4. R. Fitzgerald and J. Yucas, *Local factors of finitely generated Witt rings*, Rocky Mountain J. Math. **16** (1986), 619-627.

5. A. Iwan and C. Wowk, *Basic part of Witt rings of elementary type*, preprint.

6. M. Marshall, *Abstract Witt rings*, Queen's Papers in pure and applied Math. **57**, Queen's Univ. (1980).

7. ———, *Intersection properties of value groups of quadratic form schemes*, unpublished.

8. ——— and J. Yucas, *Linked quaternionic mappings and their associated Witt rings*, Pac. J. Math. **95** (1981), 411-425.

9. K. Szymiczek, *Structure of the basic part of a field*, J. Algebra **99** (1986), 422-429.

UNIVERSITY OF SASKATCHEWAN, SASKATOON, SASKATCHEWAN, S7N 0W0, CANADA