

COMBINATORIAL TECHNIQUES AND ABSTRACT WITT RINGS III

ROBERT W. FITZGERALD

We introduce an equivalence relation on maximal elements (i.e., $D\langle 1, -x \rangle$ is maximal). We present a form theoretic proof of Marshall's classification of reduced Witt rings, thus providing a possible outline for proving the full elementary type conjecture. The same relation restricted to elements of index two yields characterizations of Witt rings with a factor either of local type or a group ring extension of a totally degenerate Witt ring.

(R, G, q) will denote a finitely generated (abstract) Witt ring R , its associated group of one-dimensional forms G and the associated quaternionic mapping q . As in [7, 8] we use the abstract Witt ring as defined by Marshall-Yucas [13] rather than Marshall's modification in [12]. The technique introduced here is the formation of equivalence classes of maximal elements ($x \in G$ with $D\langle 1, -x \rangle$ maximal). While forming classes is not combinatorial, it does blend well with the techniques of the previous two papers in this series.

We start by discussing a four step approach to the elementary type conjecture, two of which are statements about classes of maximal elements. The four steps can be verified when R is reduced, thus giving a new, form-theoretic, proof of Marshall's classification theorem [11]. Each step is valid for Witt rings of elementary type (as opposed to the main steps in Marshall's proof or in the proofs for $|G| \leq 32$). And, when restricted to maximal elements with $[G : D\langle 1, -x \rangle] = 2$, the proposed approach leads to new results clarifying the structure of such Witt rings. The first section concludes with a verification (with some details omitted) of the four steps when R is reduced. Of interest here is the identification, when R is reduced, of the quotient structure defined in [8] with a Pfister quotient as defined by Marshall in [12].

For non-reduced R , maximal elements and their classes are difficult to handle. In the second section we consider only elements of index two ($x \in G$ with $i_G D\langle 1, -x \rangle = 2$). The restricted equivalence classes behave well and occur in two types. Using classes of type 1, we slightly

improve the characterization of local type factors in [6]. Working with classes of type 2 yields an analogous result for factors which are group rings over totally degenerate Witt rings (called S -rings here).

The last section takes up two extreme cases. First we consider the case where there are two classes of elements of index 2, one of each type, which generate $B \equiv q(G, G)$. We show R is then a product of two Witt rings, one of local type and the other an S -ring. Then, since many of the previous results involve conditions of the form $Q(x) \cap Q(y) = 1$, we consider the case where some $Q(x)$ is contained in all $Q(y)$. Under quite general conditions (satisfied if x has index 2, for example) we show R is of local type.

The notation is the same as in [7, 8]. Thus for any group H , H' denotes $H - \{1\}$. For $a \in G$, $Q(a) = \{q(a, x) | x \in G\}$ and $Y_R = \{Q(a) | a \in G'\}$. B denotes the image of q , $q(G, G)$. The value set of $\langle 1, -x \rangle$ is $D\langle 1, -x \rangle = \{y \in G | q(x, y) = 1\}$. The radical of G is $\text{rad}(G) = \{x \in G | D\langle 1, -x \rangle = G\}$. We say R is degenerate if $\text{rad} G \neq \{1\}$ and totally degenerate if $\text{rad} G = G$. We will assume throughout that R is non-degenerate.

R is of local type if $|B| = 2$. We let Δ_n denote the group of exponent two and order 2^n . The group ring $R[\Delta_n]$ is again a Witt ring. The direct product in the category of Witt rings is the fiber product over \mathbb{Z}_2 , which we will denote by the usual product symbol. Thus:

$$R_1 \times R_2 = \{(r_1, r_2) | r_i \in R_i \text{ and } \dim r_1 \equiv \dim r_2(2)\}.$$

R is of elementary type if it can be built from \mathbb{Z}_2 , \mathbb{Z}_4 and Witt rings of local type by a succession of group ring extensions and products. We will often use orthogonal decompositions as defined in [3]. Subgroups H_1, \dots, H_n of G yield an orthogonal decomposition (denoted $H_1 \perp \dots \perp H_n$) if $G = H_1 \times \dots \times H_n$ and $x_i \in D\langle 1, -x_j \rangle$ for all $x_i \in H_i$, $x_j \in H_j$, $i \neq j$.

1. Reduced Witt rings. The two notions which form the basis for all three sections are:

DEFINITION. An element $m \in G'$ is *maximal* if $D\langle 1, -m \rangle \subset D\langle 1, -x \rangle$ implies $x = 1$ or $D\langle 1, -m \rangle = D\langle 1, -x \rangle$. The collection of maximal elements of G will be denoted by M .

DEFINITION. For $a, b \in M$ write $a \sim b$ if $a = b$ or $ab \in M$. We say a and b are *equivalent*, and write $a \approx b$, if there exist $c_1, \dots, c_k \in M$ such that: $a \sim c_1 \sim c_2 \sim \dots \sim c_k \sim b$.

Equivalence is clearly an equivalence relation. Denote by $C(a)$ the equivalence class of $a \in M$. Let $H(a)$ be the subgroup of G generated by $C(a)$.

Recall the quotient structure of [8]. For $g \in G$ let $Q(g) = \{q(g, h) | h \in G\}$ and $H(Q(g)) = \{h \in G | Q(h) \subset Q(g)\}$. Set $G/g = G/H(Q(g))$ and define:

$$q_g : G/g \times G/g \rightarrow B/Q(g), \\ (aH, bH) \mapsto q(a, b)Q(g).$$

If q_g is linked the resulting Witt ring is denoted R/g . We consider a possible outline for proving the elementary type conjecture:

- (1.1) (a) G is generated by M .
 (b) If $a \not\approx b$, where $a, b \in M$, and if $x \in H(a)$, $y \in H(b)$ then $x \in D(1, -y)$.
 (c) q_a is linked for all $a \in M$.
 (d) If $G = H(a)$ for some $a \in M$ and if R/b is of elementary type for all $b \in M$ then R is of local type or a group ring.

Proving these four steps would prove the elementary type conjecture. The first two steps show there is an orthogonal decomposition (cf. [3]) $G = H(a_1) \perp \cdots \perp H(a_t)$, where $C(a_1), \dots, C(a_t)$ are the distinct equivalence classes. Each $H(a)$ generates a Witt ring, if each of these Witt rings is of elementary type then so is R [3, 3.8]. We may thus assume $G = H(a)$ for some $a \in M$. Steps (c) and (d) constitute an induction argument on $|G|$ which completes the proof.

There is some evidence for the truth of the elementary type conjecture. It holds if R is reduced (proven for abstract Witt rings by Marshall [11], simplified in [12]; cf. [2], [4], [9] for the field case) and if $|G| \leq 32$ (proven by a variety of unrelated counting arguments). There is also some evidence that (1.1) will yield a proof of the elementary type conjecture. First, the four steps of (1.1) can be proven if R is reduced, thus given a new proof of Marshall's result. Second, each of the four statements of (1.1) are true for Witt rings of elementary type. This may appear to be an insignificant advantage. However, none of the intermediate results in Marshall's proof of the reduced case are valid for non-reduced Witt rings. Only reduced Witt rings are determined by their space of orderings. Also, very few of the counting arguments used for $|G| \leq 32$ yield information about larger Witt rings. Third, (1.1) can be followed partially for maximal elements with $[G : D(1, -x)] = 2$ yielding significant improvements over previous results (see §2, 3). Unfortunately, we have been unable to prove any new cases of the elementary type conjecture via (1.1).

The remainder of this section is devoted to sketching the proofs of (1.1)(a)–(d) if R is reduced. Thus for this section (R, G, q) will denote a finitely generated, reduced Witt ring. Then $D\langle 1, 1 \rangle = \{1\}$ and as a result, if $a \in D\langle 1, b \rangle$ then $D\langle 1, a \rangle \subset D\langle 1, b \rangle$.

LEMMA 1.2. *Let $a, b \in G$.*

(i) *If $D\langle 1, a \rangle = D\langle 1, b \rangle$ then $a = b$.*

(ii) *a is maximal iff a is rigid.*

(iii) *For any $g \in G$, g is a product of elements of $D\langle 1, g \rangle \cap M$. In particular, G is generated by M .*

Proof. (i) $D\langle 1, a \rangle = D\langle 1, b \rangle \subset D\langle 1, -ab \rangle$. Thus $a, b, -ab$, and hence -1 , lie in $D\langle 1, -ab \rangle$. R reduced implies $ab = 1$.

(ii) $\{x \in G \mid D\langle 1, -a \rangle \subset D\langle 1, -x \rangle\} = \{x \in G \mid x \in D\langle 1, a \rangle\}$ since R is reduced. Then a is maximal iff this set is $\{1, a\}$ iff a is rigid.

(iii) If $|D\langle 1, g \rangle| = 2$ then $g \in M$ by (ii). If $|D\langle 1, g \rangle| > 2$ write $D\langle 1, g \rangle = \{1, g, x_3, \dots, x_t\}$. Then $g = x_3 \cdots x_t$. $D\langle 1, x_i \rangle \subsetneq D\langle 1, g \rangle$ by (i), so by induction each x_i is a product of elements in $M \cap D\langle 1, x_i \rangle \subset M \cap D\langle 1, g \rangle$. \square

LEMMA 1.3. *Let $a, b \in M$. Then either:*

(i) $D\langle 1, -ab \rangle = D\langle 1, -a \rangle \cap D\langle 1, -b \rangle$,

or

(ii) $a \approx b$.

In particular, if $a \not\approx b$, $x \in H(a)$ and $y \in H(b)$ then $x \in D\langle 1, -y \rangle$.

Proof. Suppose first that $1 \in D\langle a, b \rangle$. Then $a, b \in D\langle 1, ab \rangle$ and $-ab \in D\langle 1, -a \rangle \cap D\langle 1, -b \rangle$. We obtain (i), since R is reduced. Next suppose that $1 \notin D\langle a, b \rangle$. Then $D\langle a, b \rangle \subset M$ by [1, I 1.2] and (1.2)(ii). We may choose $c \in M \cap D\langle 1, ab \rangle$ by (1.2)(iii). Hence $c \in M$ and $ac, bc \in D\langle a, b \rangle \subset M$. So $a \sim c \sim b$. \square

The following is of some interest independent of (1.1). We show that when R is reduced, the quotient defined in [8] is the same as the Pfister quotient defined by Marshall in [12].

LEMMA 1.4. *Let $a \in M$. Then:*

(i) $H(Q(a)) = \{1, a\} = D\langle 1, a \rangle$,

(ii) R/a is well defined, and

(iii) R/a is reduced.

Proof. (i) Let $h \in H(Q(a))$. Then $q(-1, h) \in Q(h) \subset Q(a)$. By linkage (on G) there exists $z \in G$ with:

$$q(-1, h) = q(-1, z) = q(a, z).$$

Thus $h \in zD\langle 1, 1 \rangle = \{z\}$ and $z \in D\langle 1, a \rangle$. So $H(Q(a)) \subset D\langle 1, a \rangle = \{1, a\}$. We have equality since clearly $1, a \in H(Q(a))$.

(ii) Let I be the fundamental ideal of R . Since R is reduced we may assume [12, 3.23] that $q : G \times G \rightarrow I^2/I^3$ is given by $q(x, y) = \langle\langle -x, -y \rangle\rangle + I^3$. Thus $Q(a) = \langle 1, -a \rangle I + I^3$ and by (i):

$$\begin{aligned} q_a : G/D\langle 1, a \rangle \times G/D\langle 1, a \rangle &\rightarrow I^2/\langle 1, -a \rangle I + I^3, \\ q_a(\bar{x}, \bar{y}) &= \langle\langle -x, y \rangle\rangle + (\langle 1, -a \rangle I + I^3). \end{aligned}$$

There is a well-defined Pfister quotient $R/\text{ann}\langle 1, a \rangle$ [12, 4.24] which is reduced [12, 6.10]. Note that

$$\text{ann}\langle 1, a \rangle = (\{\langle 1, -x \rangle \mid x \in D\langle 1, a \rangle\}) = (\langle 1, -a \rangle).$$

Set $J = I/(\langle 1, -a \rangle)$. The quaternionic map for $R/\text{ann}\langle 1, a \rangle$ is:

$$\begin{aligned} q^* : G/D\langle 1, a \rangle \times G/D\langle 1, a \rangle &\rightarrow J^2/J^3, \\ q^*(\bar{x}, \bar{y}) &= \langle\langle -x, -y \rangle\rangle + (\langle 1, -a \rangle) + J^3. \end{aligned}$$

Map $\alpha : I^2 \rightarrow J^2/J^3$ by $\alpha(\varphi) = \varphi + (\langle 1, -a \rangle) + J^3$. This is clearly a surjective homomorphism with $\langle 1, -a \rangle I + I^3 \subset \ker \alpha$. If $\varphi \in \ker \alpha$ then $\varphi - \eta \in (\langle 1, -a \rangle)$, for some $\eta \in I^3$. Thus $\varphi - \eta = \langle 1, -a \rangle \chi$ for some form χ , and indeed $\chi \in I$ as $\varphi - \eta \in I^2$. Hence $\varphi \in \langle 1, -a \rangle I + I^3$.

Thus α is an isomorphism and the linkage of q^* implies q_a is linked.

(iii) Let $\bar{y} = yD\langle 1, a \rangle$ and suppose $q_a(-1, \bar{y}) = 1$. Then $q(-1, y) \in Q(a)$ and as in the proof of (i) we obtain $y \in D\langle 1, a \rangle$. Hence $\bar{y} = \bar{1}$ in $G/D\langle 1, a \rangle$ and so R/a is reduced. \square

The proof of (1.1)(d) is long and tedious. We present one part of the proof both to give the flavor of the whole and because a weaker version of this result holds generally for Gorenstein Witt rings (see [5]).

PROPOSITION 1.5. *Let $a \in G$ be maximal. Suppose $G = H(a)$ and R/a is a group ring. Then R is a group ring.*

Proof. We may write $\bar{G} = \bar{G}_0 \times \{1, \bar{t}\}$, where $\{1, a\} \subset G_0 \subset G = G_0 \cdot \{1, t\}$, and \bar{t} is two-sided rigid in R/a . Write $G_0 = \{1, a\} \cdot H_0$ where $a \notin H_0$ and $-1 \in H_0$.

We will assume R is not a group ring and first show that $D\langle 1, -s \rangle$ has index 2 in G . Let $h_0 \in H_0$. Then $\overline{h_0 t}, \overline{-h_0 t} \in M^*$, the maximal elements of \overline{G} . The value set in \overline{G} , $D\langle 1, \overline{x} \rangle$, is

$$D\langle 1, -x \rangle D\langle 1, -ax \rangle / \{1, a\}.$$

If $\overline{x} \in M^*$ then either:

- (i) $x, ax \in M$
or
- (ii) $x \in M$ and $D\langle 1, ax \rangle = \{1, a, x, ax\}$
or
- (iii) $ax \in M$ and $D\langle 1, s \rangle = \{1, a, x, ax\}$.

Now if $\pm h_0 t \in M$ or $\pm ah_0 t \in M$ then R has two-sided rigid elements (1.2) and is thus a group ring. Otherwise, one of two cases occurs:

- (i) $h_0 t \in M$, $D\langle 1, ah_0 t \rangle = \{1, h_0 t, a, ah_0 t\}$, $-ah_0 t \in M$ and $D\langle 1, -h_0 t \rangle = \{1, -h_0 t, a, -ah_0 t\}$ or
- (ii) $ah_0 t \in M$, $D\langle 1, h_0 t \rangle = \{1, h_0 t, a, ah_0 t\}$, $-h_0 t \in M$ and $D\langle 1, -ah_0 t \rangle = \{1, -h_0 t, a, -ah_0 t\}$.

We see then that for all $h_0 \in H_0$ either $h_0 t$ or $-h_0 t$ lies in $D\langle 1, -a \rangle$. In particular, taking $h_0 = 1$, we have t or $-t$ lies in $D\langle 1, -a \rangle$. Thus

$$|D\langle 1, -a \rangle \cap H_0| = \frac{1}{2}|H_0|.$$

If $t \in D\langle 1, -a \rangle$ then $G = \{1, -a, t, -at\}H_0$ and $i_G D\langle 1, -a \rangle = 2$. Similarly, $i_G D\langle 1, -a \rangle = 2$ if $-t \in D\langle 1, -a \rangle$.

We now obtain the desired contradiction by showing that $G = H(a)$ implies $D\langle 1, -a \rangle$ does not have index 2 in G . Note that R/a being a group ring implies $|M^*| \geq 2$ and so $|M| \geq 2$. Since $G = H(a)$, there exists $m \in M - \{a\}$ with $am \in M$. Now $-1 \notin D\langle 1, -a \rangle$ since R is reduced, so either m or $-m$ lies in $D\langle 1, -a \rangle$ (since $i_G D\langle 1, -a \rangle = 2$). But $-m \in D\langle 1, a \rangle$ implies $D\langle 1, -m \rangle \subset D\langle 1, -a \rangle$ and $m \notin M$. And $m \in D\langle 1, -a \rangle$ implies $D\langle 1, -am \rangle \subset D\langle 1, -a \rangle$ and $am \notin M$. Thus we have contradicted the initial assumption that R is not a group ring. \square

2. Elements of index 2. We now drop the assumption that R is reduced. (R, G, q) will denote a finitely generated non-degenerate Witt ring. Let $i(x)$ denote the index of $D\langle 1, -x \rangle$ in G (this is a slightly different use of $i(x)$ than in [6]). Maximal elements in an arbitrary Witt ring are difficult to work with. If, however, we restrict our attention to those maximal elements with $i(x) = 2$ then the equivalence relation of §1 is a useful tool.

Set $T = \{x \in G \mid i(x) = 2\}$ and take the same relation of §1 on T , namely, for $x, y \in T$ write $x \sim y$ if $x = y$ or $xy \in T$. Thus for $x, y \in T$, $x \sim y$ iff $i(xy) \leq 2$. In what follows we will frequently use Marshall's result [12, 5.2]:

$$|D\langle 1, -xy \rangle / D\langle 1, -x \rangle \cap D\langle 1, -y \rangle| = |Q(x) \cap Q(y)|.$$

LEMMA 2.1. *Let $x, y \in T$ and suppose $x \not\sim y$. Then:*

- (1) $i(xy) = 4$,
- (2) $D\langle 1, -xy \rangle = D\langle 1, -x \rangle \cap D\langle 1, -y \rangle$,
- (3) $Q(xy) = Q(x)Q(y)$.

Proof. By definition, $i(xy) \geq 4$ while $D\langle 1, -x \rangle \cap D\langle 1, -y \rangle \subset D\langle 1, -xy \rangle$ and $i_G(D\langle 1, -x \rangle \cap D\langle 1, -y \rangle) \leq 4$. This proves (1) and (2). Further, $2 = |D\langle 1, -y \rangle / D\langle 1, -x \rangle \cap D\langle 1, -xy \rangle| = |Q(x) \cap Q(xy)|$. Thus $Q(x) \subset Q(xy)$, as $|Q(x)| = 2$. Similarly, $Q(y) \subset Q(xy)$. Then $Q(x)Q(y) \subset Q(xy) \subset Q(x)Q(y)$ which gives (3). \square

LEMMA 2.2. *Let $x, y \in T$ and suppose $x \sim y$. Then either $D\langle 1, -x \rangle = D\langle 1, -x \rangle = D\langle 1, -y \rangle$ or $Q(x) = Q(y)$. Further, if both occur then $x = y$.*

Proof. Suppose $D\langle 1, -x \rangle \neq D\langle 1, -y \rangle$. Then

$$|D\langle 1, -xy \rangle / D\langle 1, -x \rangle \cap D\langle 1, -y \rangle| \geq 2.$$

Hence $|Q(x) \cap Q(y)| = 2$ and $Q(x) = Q(y)$. If $D\langle 1, -x \rangle = D\langle 1, -y \rangle$ and $Q(x) = Q(y)$ then

$$2 = |Q(x) \cap Q(y)| = |D\langle 1, -xy \rangle / D\langle 1, -x \rangle|$$

shows $i(xy) = 1$ and $x = y$. \square

THEOREM 2.3. *\sim is an equivalence relation on T .*

Proof. We need only check transitivity. Suppose $x, y, z \in T$ with $x \sim y$ and $y \sim z$. We may assume $x \neq y$, $x \neq z$ and $y \neq z$, so that $i(xy) = i(yz) = 2$. We show $i(xz) = 2$.

Suppose not. Then $x \not\sim z$ and $xy \not\sim yz$. By (2.1), $D\langle 1, -xz \rangle$ is contained in $D\langle 1, -x \rangle$, $C\langle 1, -z \rangle$, $D\langle 1, -xy \rangle$, $D\langle 1, -yz \rangle$ and hence $D\langle 1, -y \rangle$. Now $D\langle 1, -x \rangle \neq D\langle 1, -z \rangle$ since otherwise $D\langle 1, -x \rangle = D\langle 1, -xz \rangle$ and $i(xz) = 2$. There can only be three distinct subgroups of index 2 containing $D\langle 1, -xz \rangle$, as $i(xz) = 4$. We must have $D\langle 1, -x \rangle = D\langle 1, -y \rangle$ or $D\langle 1, -y \rangle = D\langle 1, -z \rangle$.

We will assume $D\langle 1, -x \rangle = D\langle 1, -y \rangle = D\langle 1, -xy \rangle$, the other case being similar.

We thus have $D\langle 1, -y \rangle = D\langle 1, -x \rangle \neq D\langle 1, -z \rangle$ and so $Q(y) = Q(z)$ by (2.2). We claim $i(xyz) = 4$. Otherwise, $D\langle 1, -xz \rangle \subset D\langle 1, -y \rangle$ implies $D\langle 1, -xz \rangle$ is contained in $D\langle 1, -y \rangle$, $D\langle 1, -z \rangle$, $D\langle 1, -yz \rangle$ and $D\langle 1, -xyz \rangle$, all of index 2. Again there are only three distinct subgroups of index 2 containing $D\langle 1, -xz \rangle$. So $D\langle 1, -xyz \rangle$ equals one of $D\langle 1, -y \rangle$, $D\langle 1, -z \rangle$ or $D\langle 1, -yz \rangle$, which we know are distinct. But $D\langle 1, -y \rangle = D\langle 1, -xyz \rangle$ implies $D\langle 1, -y \rangle = D\langle 1, -xz \rangle$ and $i(xz) = 2$, $D\langle 1, -z \rangle = D\langle 1, -xyz \rangle$ implies $D\langle 1, -z \rangle = D\langle 1, -xy \rangle = D\langle 1, -y \rangle$. And $D\langle 1, -yz \rangle = D\langle 1, xyz \rangle$ implies $D\langle 1, -yz \rangle = D\langle 1, -x \rangle = D\langle 1, -y \rangle = D\langle 1, -z \rangle$. All three possibilities are impossible which proves the claim.

We thus have $i(xyz) = 4$ and $D\langle 1, -xz \rangle \subset D\langle 1, -y \rangle$. So $D\langle 1, -xz \rangle = D\langle 1, -xyz \rangle \subset D\langle 1, -y \rangle$, $D\langle 1, -z \rangle$. Hence:

$$1 = \left| \frac{D\langle 1, -xz \rangle}{D\langle 1, -xyz \rangle \cap D\langle 1, -y \rangle} \right| = |Q(xyz) \cap Q(y)|,$$

$$2 = \left| \frac{D\langle 1, -xy \rangle}{D\langle 1, -xyz \rangle \cap D\langle 1, -z \rangle} \right| = |Q(xyz) \cap Q(z)|,$$

which is impossible as $Q(y) = Q(z)$.

NOTATION. For $a \in T$ let $C^*(a)$ denote the class of a in T under the relation \sim . Let $C(a) = C^*(a) \cup \{1\}$.

LEMMA 2.4. For each $a \in T$, $C(a)$ is a subgroup of G .

Proof. Let $x, y \in C(a)$. If x or y equals 1 then $xy \in C(a)$, so suppose $x, y \in C^*(a)$. Then $x \sim y$ and so $i(xy) \leq 2$. If $i(xy) = 1$ then $xy = 1 \in C(a)$. If $i(xy) = 2$ then $xy \in T$, and $xy \sim x \sim a$. Hence $xy \in C(a)$. \square

PROPOSITION 2.5. Let $a \in T$. Then either:

- (1) $Q(a) = Q(x)$ for all $x \in C^*(a)$, or
- (2) $D\langle 1, -a \rangle = D\langle 1, -x \rangle$ for all $x \in C^*(a)$.

Proof. Set $C_1(a) = \{x \in C^*(a) | Q(x) = Q(a)\} \cup \{1\}$ and $C_2(a) = \{x \in C^*(a) | D\langle 1, -x \rangle = D\langle 1, -a \rangle\} \cup \{1\}$. We first claim that $C_1(a)$ is a subgroup of $C(a)$. If $x, y \in C_1(a)$ and $x \neq 1, y \neq 1$ then $Q(x) = Q(a) = Q(y)$. So $Q(xy) \subset Q(x)Q(y) = Q(a)$. Hence either

$xy = 1$ or $Q(xy) = Q(a)$. In either case, $xy \in C_1(a)$. Next we claim $C_2(a)$ is a subgroup of $C(a)$. If $x, y \in C_2(a)$ with $x \neq 1$, $y \neq 1$ then $D\langle 1, -x \rangle = D\langle 1, -y \rangle \subset D\langle 1, -xy \rangle$. So either $xy = 1$ or $D\langle 1, -xy \rangle = D\langle 1, -a \rangle$ and so $xy \in C_2(a)$.

Now $C(a) = C_1(a) \cup C_2(a)$ by (2.2). Hence either $C(a) = C_1(a)$, yielding (1), or $C(a) = C_2(a)$, yielding (2). \square

DEFINITION. Let $a \in G$ have index 2 (i.e. $a \in T$). We say a has *type 1* if $Q(a) = Q(x)$ for all $x \in C'(a)$. We say a has *type 2* if $D\langle 1, -a \rangle = D\langle 1, -x \rangle$ for all $x \in C'(a)$ and $|C(a)| \geq 4$.

Every $a \in T$ thus has type 1 or type 2 (but not both, by the restriction that $|C(a)| \geq 4$ for type 2). We observe that if a has type 2 then $C(a) \subset D\langle 1, -a \rangle$ (namely, if $m \in C'(a)$, $m \neq a$ then $D\langle 1, -m \rangle = D\langle 1, -a \rangle = D\langle 1, -am \rangle$). In particular, $-1 \in D\langle 1, -a \rangle$. Hence $C(a) \subset D\langle 1, -a \rangle$.

Elements of index 2 having type 1 have appeared in the literature before. We reformulate two such results in this language.

PROPOSITION 2.6 (Marshall [12]). *Suppose G is generated by elements of index 2. Then R is a fiber product of Witt rings of local type.*

Proof. We have $G = C(a_1) \cdot \dots \cdot C(a_k)$, where the $C'(a_i)$ are the distinct classes in T . If $x \in C(a_i)$, $y \in C(a_j)$ with $i \neq j$ then $x \in D\langle 1, -y \rangle$ by (2.1). In particular, no $C(a_i)$ has type 2, else all the $C(a_j)$ are contained in $D\langle 1, -a_i \rangle$ and so $G \subset D\langle 1, -a_i \rangle$. We thus have $G = C(a_1) \times \dots \times C(a_k)$ and $Q(C(a_i)) \cap Q(C(a_j)) = \{1\}$ if $i \neq j$. Thus R is a fiber product with the i th factor generated by $C(a_i)$. Since $|Q(C(a_i))| = 2$ (a has type 1) each factor is of local type. \square

PROPOSITION 2.7 (Fitzgerald-Yucas [6]). *Let $a \in T$ have type 1. Set $H = C(a)$ and $K = \bigcap_{h \in H} D\langle 1, -h \rangle$.*

(1) *If $H \cap K = \{1\}$ then $G = H \perp K$ is an orthogonal decomposition.*

(2) *If, further, $Q(a) \notin Q(K)$ then $R = R_1 \times R_2$ is a fiber product with R_1 of local type.*

Proof. We refer to [6]. $C'(a) = -M$ and $C(a) = M^2$. The conclusion of (1) is Proposition 2.12(1)–(4) which depends only on

Proposition 2.11 which in turn depends only on the assumption that $H \cap K = \{1\}$. Thus (1) holds; statement (2) is Theorem 1.1. \square

We note that, in (2.7), if K generates a Witt ring of elementary type (as in an inductive argument) then condition (1) is sufficient to show R is a fiber product with one factor of local type [3, 3.8].

We turn now to elements of index 2 having type 2. Among Witt rings of elementary type these arise from fiber products $R_1 \times R_2$ where $R_1 = S[\Delta]$, S a degenerate Witt ring with radical D_S satisfying $|D_S| \geq 4$ and $|\Delta| = 2$. Here any $a = (g, 1) \in D_S \times 1$ has type 2 and $C(a) = D_S \times 1$. One difficulty is that here the class does not generate a factor of R . In the simplest case where S is totally degenerate (i.e. $D_S = G_S$) then the element $(t, 1)$ (where $\Delta = (1, t)$) is required along with $C(a)$ to generate R_1 . Note that $Q(t, 1) = Q(C(a))$.

DEFINITION. A Witt ring R is an S -ring if R is a group ring extension $S[\Delta]$ where S is a totally degenerate Witt ring, $|G_S| \geq 4$ and $|\Delta| = 2$.

DEFINITION. Let $a \in T$ have type 2. An element $t \in G$ is a *cap* for a if $Q(t) = Q(C(a))$.

We will concentrate on the easiest case of type 2 elements. We seek conditions on an $a \in T$ having type 2 analogous to (2.7) which will yield an S -ring factor.

In what follows we will often use the observation that $Q(a) \subset Q(b)$ iff $G = D\langle 1, -a \rangle D\langle 1, -ab \rangle$.

LEMMA 2.8. *Let $a \in T$ have type 2.*

- (1) $Q(C(a)) = \bigcup_{m \in C(a)} Q(m)$.
- (2) *For any $g \in G$ and $m, m' \in C(a)$ we have $Q(m) \subset Q(g)$ iff $Q(m') \subset Q(mm'g)$.*

Proof. (1) We check that the union is a group. Let $p_1 \in Q(m_1)$ and $p_2 \in Q(m_2)$ where $m_1, m_2 \in C(a)$. If either $p_1 = 1$ or $p_2 = 1$ then $p_1 p_2 \in Q(m_1) \cup Q(m_2)$. Suppose $p_1 \neq 1, p_2 \neq 1$. Then $p_1 = q(m_1, y)$ for some $y \notin D\langle 1, -m_1 \rangle = D\langle 1, -m_2 \rangle$, since a has type 2. Thus $p_2 = q(m_2, y)$ and $p_1 p_2 = q(m_1 m_2, y) \in Q(m_1 m_2)$ with $m_1 m_2 \in C(a)$.

(2) $Q(m) \subset Q(g)$ iff $G = D\langle 1, -m \rangle D\langle 1, -mg \rangle$ iff $G = D\langle 1, -m' \rangle D\langle 1, -mg \rangle$ (as $D\langle 1, -m \rangle = D\langle 1, -m' \rangle$) if $Q(m') \subset Q(mm'g)$. \square

PROPOSITION 2.9. *Let $a \in T$ have type 2 and set $P = Q(C(a))$. For any $g \in G$ either:*

- (1) $Q(g) \cap P = \{1\}$, or
- (2) $Q(g) \cap P = Q(m)$, for some $m \in C^*(a)$, or
- (3) $P \subset Q(g)$.

Proof. Suppose $Q(g) \cap P \neq \{1\}$ or P . Then there exist m_1 and $m_2 \in C^*(a)$ with $Q(m_1) \subset Q(g)$ and $Q(m_2) \not\subset Q(g)$ by (2.8). Set $H_1 = H(Q(g))$ and $H_2 = H(Q(m_1 m_2 g))$. We wish to show $H_1 \cap C(a) = \{1, m_1\}$. Now $m_2 \in H_2$ and $m_1 \notin H_2$ by (2.8). Let $m_3 \in H_1 \cap C^*(a)$ so that $Q(m_3) \subset Q(g)$. Applying (2.8) with $m = m_3$ and $m' = m_1 m_2 m_3$ yields $Q(m_1 m_2 m_3) \subset Q(m_1 m_2 g)$. Thus $m_1 m_2 m_3$, and so $m_1 m_3$, lies in H_2 . This shows $m_1(H_1 \cap C^*(a)) \subset H_2$.

If $|H_1 \cap C^*(a)| \neq 1$ then there exist distinct $x, y \in H_1 \cap C^*(a)$. So $m_1 x, m_1 y, m_1 x y \in H_2$ and hence $m_1 \in H_2$, a contradiction. Thus $H_1 \cap C^*(a) = \{m_1\}$ as desired. \square

We can now re-derive a result of Kula [10]. We use the counting formula of [7]:

$$(*) \quad \sum_{x \neq 1, z} \frac{1}{|Q(x) \cap Q(z)|} \cdot \frac{1}{|Q(xz)|} = \frac{-2}{|Q(z)|} + \sum_{y \in D\langle 1, -z \rangle} \frac{1}{|Q(y)|}.$$

COROLLARY 2.10 (Kula). *Let $a \in T$ have type 2 and set $P = Q(C(a))$. If $Q(G) = P$ then R is an S -ring.*

Proof. Choose $b \notin C(a)$ and apply (*) with $z = b$. We split the left-hand sum into sums over $C^*(a)$, $bC^*(a)$ and $G \setminus \{1, b\}C(a)$. For any $x \notin C(a)$ we have $Q(x) = P$ by (2.9). Set $g = |G|$ and $c = |C(a)| = |P|$. We obtain:

$$\text{LHS} = \frac{c-1}{2c} + \frac{c-1}{2c} + \frac{g-2c}{c^2}.$$

We split the right-hand sum into sums over $\{1\}$, $C^*(a) \cap D\langle 1, -b \rangle$ and $D\langle 1, -b \rangle \setminus C(a)$. We obtain:

$$\text{RHS} = \frac{-2}{c} + 1 + \frac{d-1}{2} + \frac{(g/c) - d}{c},$$

where $d = |D\langle 1, -b \rangle \cap C(a)|$. Equating the two sides gives:

$$\begin{aligned} -1/c &= (d-1)/2 - d/c, \\ c-2 &= d(c-2) \end{aligned}$$

and so $d = 1$. Thus for all $b \notin C(a)$, $D\langle 1, -b \rangle \cap C(a) = \{1\}$. In particular, $C(a) \subset D\langle 1, -a \rangle \subset C(a)$ and so $D\langle 1, -a \rangle = C(a)$.

Fix $b \notin C(a)$. Since $i_G C(a) = i(a) = 2$ and $D\langle 1, -b \rangle \cap C(a) = \{1\}$ we get $D\langle 1, -b \rangle = \{1, -b\}$. Further, $-1 \in D\langle 1, -a \rangle$ (cf. the remarks after (2.5)) and so $D\langle 1, b \rangle = \{1, b\}$ also. Thus b is 2-sided rigid and $E = S[\Delta]$ is a group ring extension. We have $|\Delta| = 2$ and $D\langle 1, -a \rangle = G_S$ since $i(a) = 2$. Moreover we have shown that if $x \in G_S$ then $x \in D\langle 1, -a \rangle = C(a)$ and so $D\langle 1, -x \rangle = D\langle 1, -a \rangle = G_S$. Thus S is totally degenerate. Finally, by definition of type 2, $|G_S| = |C(a)| \geq 4$. So R is an S -ring. \square

We refine (2.9):

COROLLARY 2.11. *Let $a \in T$ have type 2 and set $P = Q(C(a))$. Let $g \in G$.*

(1) *If $Q(g) \cap P = Q(m)$ for some $m \in C^*(a)$ then $Q(mg) \cap P = \{1\}$.*

(2) *If $P \subset Q(g)$ then $Q(g) = Q(mg)$ for all $m \in C(a)$.*

Proof. (1) $Q(m) \subset Q(g)$ implies $Q(mg) \subset Q(g)$. Hence if $Q(mg) \cap P \neq \{1\}$ then $Q(mg) \cap P = Q(m)$ also. Suppose this occurs and choose $n \in C^*(a) \setminus \{m\}$. Applying (2.8) with $m = m$ and $m' = n$ to $Q(m) \subset Q(g)$ gives $Q(n) \subset Q(mng)$. Next, using $M = m$ and $m' = mn$ for $Q(m) \subset Q(mg)$ gives $Q(mn) \subset Q(mng)$. Hence $Q(m) \subset Q(mn)Q(n) \subset Q(mng)$. Apply (2.8) to this inclusion with $m = m$ and $m' = n$ to obtain $Q(n) \subset Q(g)$, which is impossible. Thus $Q(mg) \cap P = \{1\}$.

(2) Fix $m_0 \in C^*(a)$. Then $Q(mm_0) \subset Q(g)$ for all $m \in C(a)$ and so $Q(m) \subset Q(m_0g)$ by (2.8). Thus $P \subset Q(m_0g)$. From $Q(m_0) \subset Q(m_0g) \subset Q(g)$ we obtain $Q(m_0g) = Q(g)$. \square

We may do better assuming there is a cap for a .

PROPOSITION 2.12. *Let $a \in T$ have type 2 and let t be a cap for a (i.e. $Q(t) = Q(C(a))$). Set $P = Q(C(a))$, $L = \{x \in G \mid Q(x) \cap P = 1\}$ and $K = D\langle 1, -a \rangle \cap D\langle 1, -t \rangle$. Let $g \in G$. Then:*

(1) $L \subset K$.

(2) *If $Q(g) \cap P = Q(m)$ for some $m \in C^*(a)$ then $mg \in L$.*

(3) *If $P \subset Q(g)$ then either:*

(i) *There exists a unique $m \in C(a)$ with $mtg \in L$, or*

(ii) $Q(mg) = Q(m'gt)$ for all $m, m' \in C(a)$.

Proof. (1) If $Q(x) \cap Q(t) = 1$ then $D\langle 1, -xt \rangle = D\langle 1, -x \rangle \cap D\langle 1, -t \rangle$ and so $x \in D\langle 1, -t \rangle$. Also $Q(x) \cap Q(a) = 1$ so that $x \in D\langle 1, -a \rangle$. Thus $L \subset K$.

(2) is (2.11)(1). For (3) we first show there is at most one $m \in C(a)$ with $mgt \in L$. Suppose not, that is, $Q(m_1gt) \cap P = 1 = Q(m_2gt) \cap P$. then for all m , $Q(m) \cap Q(migt) = 1$ ($i = 1, 2$) and so $D\langle 1, -migt \rangle = D\langle 1, -m \rangle \cap D\langle 1, -migt \rangle$. Taking $m = m_1m_2$ and $i = 1, 2$ shows $\langle 1, -m_1gt \rangle = D\langle 1, -m_2gt \rangle$. From $Q(migt) \cap Q(t) = 1$ we obtain $D\langle 1, -m_1 \rangle = D\langle 1, -t \rangle \cap D\langle 1, -m_1gt \rangle = D\langle 1, -t \rangle \cap D\langle 1, -m_2gt \rangle = D\langle 1, -m_2g \rangle$. Further, $Q(m_1g) = Q(m_2g)$ by (2.11) and hence $m_1 = m_2$.

Suppose now that (i) does not occur. Then $P \subset Q(mgt)$ for all $m \in C(a)$ by (2.11)(1). So $Q(mgt) = Q(m'g)$ for all $m, m' \in C(a)$ by (2.11)(2). \square

There are no examples of Case 3(ii) of (2.12) occurring among Witt rings of elementary type. The possibility that it might occur is the major obstacle to showing every a of type 2 with a cap arises from a fiber product where one factor is an S -ring.

We do however have a result analogous to (2.7).

PROPOSITION 2.13. *Let $a \in T$ have type 2 with a cap t . Set $H = \{1, t\}C(a)$ and $K = D\langle 1, -a \rangle \cap D\langle 1, -t \rangle$.*

(1) *If $t \notin D\langle 1, -a \rangle$ then $G = H \perp K$ is an orthogonal decomposition.*

(2) *If further $Q(t) \cap Q(K) = 1$ then $R = R_1 \times R_2$ where R_1 is an S -ring.*

Proof. (1) Let $g \in G$. Either g or $gt \in D\langle 1, -a \rangle$ as $i(a) = 2$. Further, $C(a) \cap D\langle 1, -t \rangle = 1$ and $|C(a)||D\langle 1, -t \rangle| = |G|$ by (2.8). Thus $G = \bigcup_{m \in C(a)} mD\langle 1, -t \rangle$. There exists then an $m \in C(a)$ such that mg or mgt is an $D\langle 1, -a \rangle \cap D\langle 1, -t \rangle = K$ and so $g \in HK$.

If $g \in H \cap K$ then $K \subset D\langle 1, -g \rangle$ since $g \in H$. For all $m \in C(a)$, $g \in D\langle 1, -m \rangle = D\langle 1, -a \rangle$ and $g \in D\langle 1, -t \rangle$, since $g \in K$. Hence $H \subset D\langle 1, -g \rangle$. Then $G = HK \subset D\langle 1, -g \rangle$ and $g = 1$. Thus $H \cap K = 1$ and $G = H \perp K$ is an orthogonal product.

(2) follows from (1) by [3, 3.4]. \square

We again note that if K in (2.13) generates a Witt ring of elementary type then condition (1) yields $R = R_1 \times R_2$ with R_1 an S -ring by [3, 3.8].

We may combine (2.7) and (2.13) with a change in hypotheses.

THEOREM 2.14. *Let $a \in G$ have index 2. Set $P = Q(C(a))$. Suppose:*

- (1) *There exists $x \in G$ with $Q(x) = P$, and*
- (2) *For no y is $Q(my) = Q(m'xy)$ for all $m, m' \in C(a)$.*

Then $R = R_1 \times R_2$ with R_1 of local type if a has type 1 and R_1 an S -ring if a has type 2.

Proof. Set $H = \{1, x\}C(a)$, $L = \{y \in G \mid Q(y) \cap P = 1\}$ and $K = \bigcap_{h \in H} D\langle 1, -h \rangle$. We first note that $L \subset K$. If a has type 2 then this is (2.12). If a has type 1 and $y \in L$ then $Q(m) \cap Q(y) = 1$ for all $m \in C(a)$, as $Q(m) = Q(a) = P$. Thus $D\langle 1, -my \rangle = D\langle 1, -my \rangle \cap D\langle 1, -y \rangle$ and $y \in D\langle 1, -m \rangle$ for all $m \in C(a)$. Then $y \in K$ as $Q(x) = Q(a)$ implies $x \in C(a)$ and $H = C(a)$.

We next show $G = HL$. If a has type 2 then this is (2.12) combined with assumption (2) which eliminates Case 3(ii). Suppose a has type 1. If $g \in G$, $g \notin L$ then $Q(a) \subset Q(g)$ since $|Q(a)| = 2$. Assume, by way of contradiction, that $g \notin HL$. Then $Q(a) \subset Q(mg)$ for all $m \in C(a)$. So $Q(m) \subset Q(mg) \subset Q(m)Q(g) = Q(g)$, which implies $Q(mg) = Q(g)$ for all $m \in C(a)$. Again noting that the x of assumption (1) lies in $C(a)$, we see that assumption (2) is contradicted. So $G = HL$.

We thus have $G = HK$ as well and (by [6, 1.2]) that $H \cap K = 1$. Then $G = H \times K$, $L \subset K$ and $G = HL$ imply that $L = K$. Thus $G = H \perp K$ and $P \cap Q(k) = 1$ for all $k \in K$. We obtain that $R = R_1 \times R_2$ with R_1 generated by H . If a has type 1 then $|Q(H)| = 2$ shows R_1 is of local type, while if a has type 2 then (2.10) shows R_1 is an S -ring. \square

3. Extreme cases. As before, T is the set of $x \in G$ with $i_G D\langle 1, -x \rangle = 2$. We consider the simplest of cases where T has both elements with type 1 and type 2.

THEOREM 3.1. *Suppose $Q(G)$ is generated by the $Q(x)$ with $x \in T$. Suppose further that $T = C^*(a) \cup C^*(b)$, where a has type 2 and b has type 1. Then $R = R_1 \times R_2$ where R_1 is an S -ring and R_2 is of local type.*

Proof. Set $P = Q(C(a))$ and $B = Q(G)$.

Step 1. For all $g \in G^*$, $Q(g) = Q(b)$, $Q(m)$, $Q(m)Q(b)$, P or B , for some $m \in C^*(a)$.

There are three possibilities for $Q(g) \cap P$ by (2.9). First suppose $Q(g) \cap P = 1$. Then $[B : P] = 2$ implies $|Q(g)| = 2$. Thus $g \in T = C^*(a) \cup C^*(b)$ and certainly $g \notin C^*(a)$ so that $Q(g) = Q(b)$ (as b has type 1).

Next suppose $Q(g) \cap P = Q(m)$ for some $m \in C^*(a)$. Then $Q(gm) \cap P = 1$ by (2.11), and so $gm = 1$ or $gm \in C^*(b)$. In the first case $Q(g) = Q(m)$ and in the second case $Q(g) = Q(bm) = Q(b)Q(m)$ by (2.1). Lastly, suppose $P \subset Q(g)$. Again $[B : P] = 2$ implies $Q(g) = P$ or B .

Step 2. There exists $t \in G$ with $Q(t) = P$.

Suppose otherwise. Then for any $g \in G$ either $g \in C(a)C(b)$ or $Q(g) = B$, by Step 1. We again use the counting formula from [7]:

$$\sum_{x \neq 1, a} \frac{1}{|Q(x) \cap Q(a)|} \cdot \frac{1}{|Q(ax)|} = \frac{-2}{|Q(a)|} + \sum_{y \in D\langle 1, -a \rangle} \frac{1}{|Q(y)|}.$$

Set $e = |C(b)|$, $g = |G|$ and $c = |C(a)| = |P|$. We note that $H(Q(m)) = \{1, m\}$ and $H(Q(bm)) = \{1, m\}C(b)$ for $m \in C(a)$. Further, $C(a)C(b) \subset D\langle 1, -a \rangle$, by (2.1) and the remark after (2.5). We split the left-hand sum into sums over $C^*(a) \setminus \{a\}$, $C^*(b)$, $aC^*(b)$, $(C^*(a) \setminus \{a\})C^*(b)$ and $G \setminus C(a)C(b)$. We obtain:

$$\text{LHS} = \frac{c-2}{2} + \frac{e-1}{4} + \frac{e-1}{4} + \frac{(c-2)(e-1)}{4} + \frac{g-ce}{4c}.$$

We split the right-hand sum into sums over $\{1\}$, $C^*(a)$, $C^*(b)$, $C^*(a)C^*(b)$ and $D\langle 1, -a \rangle \setminus C(a)C(b)$. We obtain:

$$\text{RHS} = -1 + 1 + \frac{c-1}{2} + \frac{e-1}{2} + \frac{(c-1)(e-1)}{4} + \frac{(g/2) - ce}{2c}.$$

Equating the two sides gives:

$$\begin{aligned} \frac{c-2}{2} + \frac{e-1}{4} - \frac{3}{4} &= \frac{c-2}{2} + \frac{e-1}{4} - \frac{e}{2}, \\ -5/4 &= -3/2, \end{aligned}$$

a contradiction.

Step 3. There is a cap t for a with $t \notin D\langle 1, -a \rangle$.

Set $F = H(P)$. We will show $F \not\subset D\langle 1, -a \rangle$, since then if $t \in F \setminus D\langle 1, -a \rangle$ we must have $Q(t) = P$ lest $t \in C(a) \subset D\langle 1, -a \rangle$. Let $f = |F|$ and $i = |F \cap D\langle 1, -a \rangle|$. We use the same formula as Step 2. On the left-hand side we need only replace the sum over $G \setminus C(a)C(b)$

by sums over $F \setminus C(a)$ and $G \setminus (C(a)C(b) \cup F)$. We obtain:

$$\begin{aligned} \text{LHS} = & \frac{c-2}{2} + \frac{e-1}{4} + \frac{e-1}{4} + \frac{(c-2)(e-1)}{4} \\ & + \frac{f-c}{2c} + \frac{g-ce-f+c}{4c}. \end{aligned}$$

On the right-hand side we need only replace the sum over $D(1, -a) \setminus C(a)C(b)$ by sums over $(F \cap D(1, -a)) \setminus C(a)$ and $D(1, -a) \setminus (C(a)C(b) \cup F)$. We obtain:

$$\text{RHS} = \frac{c-1}{2} + \frac{e-1}{2} + \frac{(c-1)(e-1)}{4} + \frac{i-c}{c} + \frac{(g/2) - ce - i + c}{2c}.$$

Equating the two sides gives:

$$\begin{aligned} -1 + \frac{e-1}{4} + \frac{f-c}{2c} + \frac{c-ce-f}{4c} &= \frac{-1}{2} + \frac{e-1}{2} + \frac{i-c}{c} + \frac{c-ce-i}{2c}, \\ f/4c &= i/2c, \\ f &= 2i. \end{aligned}$$

Thus $F \not\subset D(1, -a)$ as desired

Step 4. Finish.

Let t be the cap of Step 3. Set $H = \{1, t\}C(a)$ and $K = D(1, -a) \cap D(1, -t)$. Then $G = H \perp K$ by (2.13). Arguing as in Step 1, we see that if $k \in K$ then $Q(k) = Q(b)$, P or B . Hence (in the notation of [8]) $|Y_K| \leq 3$ and the Witt ring R_2 generated by K is of elementary type [8, 3.7]. Indeed, R_2 is of local type since otherwise R_2 is a product of two local factors and $|P| = 2$, which is impossible ($|P| = |C(a)| \geq 4$ since a has type 2). Thus $R = R_1 \times R_2$ by [3, 3.4], R_2 is of local type and R_1 , generated by H , is an S -ring by (2.10). \square

Both (2.7) and (2.13) require a condition of the form $Q(x) \not\subset Q(K)$, where $i(x) = 2$, to deduce that x arises from a fiber product. We consider the case of extreme failure of this condition, namely $Q(x) \subset Q(y)$ for all $y \in G$. When $i(x) = 2$ we will show that $Q(x) \subset Q(y)$ for all y , implies R is of local type.

LEMMA 3.2. *Suppose $Q(w) \subset Q(g)$ for all $g \in G$. Let $H = H(Q(w))$. In the quotient R/w set $\bar{z} = zH$ and $Q(\bar{z}) = Q(z)/Q(w)$. Then:*

$$(1) \quad \sum_{\bar{z} \in D(1, -a)} \frac{(h/q) - \varepsilon(\bar{z})|D(1, -a) \cap H|}{|Q(\bar{z})|} = - \left(1 - \frac{1}{q}\right) \frac{2}{|Q(\bar{a})|},$$

where $A \in G \setminus H$, $h = |H|$, $q = |Q(w)|$ and:

$$\varepsilon(\bar{z}) = \begin{cases} 0, & \text{if } zH \cap D\langle 1, -a \rangle = \emptyset, \\ 1, & \text{if } zH \cap D\langle 1, -a \rangle \neq \emptyset. \end{cases}$$

Proof. R/w is well defined by [8, 2.4]. We start with the counting formula of [7] for both (R, G) and $(R/w, \bar{G})$:

$$(2) \quad \sum_{x \neq 1, a} \frac{1}{|Q(x) \cap Q(a)|} \cdot \frac{1}{|Q(ax)|} = \frac{-2}{|Q(a)|} + \sum_{y \in D\langle 1, -a \rangle} \frac{1}{|Q(y)|},$$

$$(3) \quad \sum_{\bar{x} \neq \bar{1}, \bar{a}} \frac{1}{|Q(\bar{x}) \cap Q(\bar{a})|} \cdot \frac{1}{|Q(\bar{a}\bar{x})|} = \frac{-2}{|Q(\bar{a})|} + \sum_{\bar{y} \in D\langle 1, -\bar{a} \rangle} \frac{1}{|Q(\bar{y})|}.$$

Note that for all $g \in G$ and $h \in H$, we have $Q(g) = Q(gh)$. Namely, $Q(gh) \subset Q(g)Q(h) = Q(g)Q(w) = Q(g)$ and similarly $Q(g) \subset Q(gh)$. Then:

$$\begin{aligned} \text{LHS}(2) &= \sum_{x \in H} \frac{1}{|Q(x) \cap Q(a)|} \cdot \frac{1}{|Q(ax)|} \\ &\quad + \sum_{x \in aH} \frac{1}{|Q(x) \cap Q(a)|} \cdot \frac{1}{|Q(ax)|} \\ &\quad + \sum_{\bar{z} \neq \bar{1}, \bar{a}} \sum_{x \in zH} \frac{1}{|Q(x) \cap Q(a)|} \cdot \frac{1}{|Q(ax)|} \\ &= \frac{h-1}{q|Q(a)|} + \frac{h-1}{q|Q(a)|} + \sum_{\bar{z} \neq \bar{1}, \bar{a}} \frac{1}{|Q(\bar{z}) \cap Q(\bar{a})|} \cdot \frac{1}{|Q(\bar{a}\bar{z})|}. \end{aligned}$$

Now $|Q(g)| = |Q(\bar{g})|q$ and $|Q(x) \cap Q(a)| = |Q(\bar{x}) \cap Q(\bar{a})|q$. Thus:

$$\begin{aligned} \text{LHS}(2) &= \frac{2(h-1)}{q^2|Q(\bar{a})|} + \sum_{\bar{z} \neq \bar{1}, \bar{a}} \frac{h}{q^2|Q(\bar{z}) \cap Q(\bar{a})||Q(\bar{a}\bar{z})|} \\ &= \frac{h}{q^2} \left[\frac{2}{|Q(\bar{a})|} + \sum_{\bar{z} \neq \bar{1}, \bar{a}} \frac{1}{|Q(\bar{z}) \cap Q(\bar{a})||Q(\bar{a}\bar{z})|} \right] \\ &\quad - \frac{2}{q^2|Q(\bar{a})|}. \end{aligned}$$

Equation (3) then implies:

$$\text{LHS}(2) = \frac{h}{q^2} \left(\sum_{\bar{z} \in D\langle 1, -\bar{a} \rangle} \frac{1}{|Q(\bar{z})|} \right) - \frac{2}{q^2|Q(\bar{a})|}.$$

We turn now to the right-hand side of (2):

$$\begin{aligned} \text{RHS}(2) &= \frac{-2}{|Q(a)|} + \sum_{\bar{z} \in \bar{G}} \sum_{y \in D(1, -a) \cap zH} \frac{1}{|Q(y)|} \\ &= \frac{-2}{|Q(a)|} + \sum_{\bar{z} \in \bar{G}} \frac{|D(1, -a) \cap zH|}{|Q(z)|}. \end{aligned}$$

If $\varepsilon(\bar{z}) = 1$ then $D(1, -a) \cap zH = x(D(1, -a) \cap H)$ for some $x \in zH$. Thus $|D(1, -a) \cap zH| = \varepsilon(\bar{z})|D(1, -a) \cap H|$. Further, since $D(1, -\bar{a}) = D(1, -a)D(1, -aw)/H$, if $\bar{z} \notin D(1, -\bar{a})$ then $D(1, -a) \cap zH = \emptyset$. We obtain:

$$\begin{aligned} \text{RHS}(2) &= \frac{-2}{|Q(a)|} + \sum_{\bar{z} \in D(1, -\bar{a})} \frac{\varepsilon(\bar{z})|D(1, -a) \cap H|}{|Q(z)|} \\ &= \frac{-2}{q|Q(\bar{a})|} + \sum_{\bar{z} \in D(1, -\bar{a})} \frac{\varepsilon(\bar{z})|D(1, -a) \cap H|}{q|Q(\bar{z})|}. \end{aligned}$$

Equating the two expressions for LHS(2) and RHS(2) (and multiplying by q) gives:

$$\begin{aligned} \frac{h}{q} \left(\sum_{\bar{z} \in D(1, -\bar{a})} \frac{1}{|Q(\bar{z})|} \right) - \frac{2}{q|Q(\bar{a})|} \\ = \left(\sum_{\bar{z} \in D(1, -\bar{a})} \frac{\varepsilon(\bar{z})|D(1, -a) \cap H|}{|Q(\bar{z})|} \right) - \frac{2}{|Q(\bar{a})|}. \end{aligned}$$

This is easily seen to be equivalent to (1). \square

THEOREM 3.3. *Suppose $Q(w) \subset Q(g)$ for all $g \in G$. Set $H = H(Q(w))$. If $|Q(w)| \leq |H|$ then R is of local type.*

Proof. Let $q = |Q(w)|$, $h = |H|$, $\bar{z} = zH$ and $Q(\bar{z}) = Q(z)/Q(w)$. We assume, if possible, that $g \neq H$. Set $g = |G|$. If there exists an $a \in G \setminus H$ such that $|D(1, -a) \cap H| \leq h/q$ then LHS(1) ≥ 0 while RHS(1) < 0 , a contradiction. Hence for all $a \in G \setminus H$ we have $|D(1, -a) \cap H| \geq 2h/q$.

We now count, in two ways, the number N of pairs (a, x) where $a \in G \setminus H$, $x \in H$ and $a \in D(1, -x)$. If we fix x , the number of pairs with this x is

$$\begin{aligned} |D(1, -x) \cap (G \setminus H)| &= |D(1, x)| = |D(1, -x) \cap H| \\ &= (g/q) - |D(1, -x) \cap H|. \end{aligned}$$

Thus

$$N = \frac{(h-1)g}{q} - \sum_{x \in H} |D\langle 1, -x \rangle \cap H|.$$

Denote this last sum by β .

Next, if we fix $a \in G \setminus H$ the number of pairs with this a is

$$|D\langle 1, -a \rangle \cap H| = |D\langle 1, -a \rangle \cap H| - 1.$$

So:

$$N = \sum_{a \in G \setminus H} (|D\langle 1, -a \rangle \cap H| - 1) \geq \frac{(g-h)2h}{q} - (g-h).$$

Comparing the two expressions for N yields:

$$\begin{aligned} \frac{(g-h)2h}{q} - (g-h) &\leq \frac{(h-1)g}{q} - \beta, \\ (g-h)2h - (g-h)q &\leq (h-1)g - \beta q. \end{aligned}$$

Now $\beta = \sum_{x \in H} |D\langle 1, -x \rangle \cap H| \geq (h-1)$. Thus:

$$\begin{aligned} (g-h)2h - (g-h)q + (h-1)q &\leq (h-1)g, \\ gh - gq + g &\leq 2h^2 - 2hq + q, \\ g(h-q+1) &\leq 2h(h-q) + q. \end{aligned}$$

Note that $h-q+1 \geq 1$ since $h \geq q$. Thus:

$$g \leq \frac{2h(h-q) + q}{(h-q) + 1} < 2h,$$

since $q < 2h$. Thus $g = h$ and so $G = H$. Then $Q(g) = Q(w)$ for all $g \in G$. R is then of local type [7, Th. 5]. \square

The condition $q = |Q(w)| \leq |H| = h$ in (3.3) can be viewed as follows: In the quotient R/w , let $\bar{a} = aH$. Then $|D\langle 1, -\bar{a} \rangle| = |D\langle 1, -a \rangle|q/h$. Thus if $q \leq h$, no value group increases in size upon passing to the quotient.

COROLLARY 3.4. *Suppose $i_G D\langle 1, -w \rangle = 2$ and $Q(w) \subset Q(g)$ for all $g \in G$. Then R is of local type.*

Proof. Clearly $|Q(w)| = 2 \leq |H(Q(w))|$, so apply (3.3). \square

COROLLARY 3.5. *Suppose $Q(w) \subset Q(g)$ for all $g \in G$. Suppose further that the counting coefficients of the Hasse diagram for Y_R (cf. [7, p. 49]) are positive. Then R is of local type.*

Proof. Here we get $|Q(w)| = 2$ by [7, Th. 13], so apply (3.4). \square

REFERENCES

- [1] R. Bos, *Quadratic Forms, Orderings and Abstract Witt Rings*. Thesis, Rijksuniversiteit, 1984.
- [2] L. Bröcker, *Über die anzahl der anordnungen eines kommutative körpers*, Archiv. Der Math., **29** (1977), 458–464.
- [3] A. Carson and M. Marshall, *Decomposition of Witt rings*, Canad. J. Math., **34** (1982), 1276–1302.
- [4] T. Craven, *Characterizing reduced Witt rings of fields*, J. Algebra, **53** (1978), 68–77.
- [5] R. Fitzgerald, *Gorenstein Witt rings*, Canad. J. Math., **40** (1988), 1186–1202.
- [6] R. Fitzgerald and J. Yucas, *Local factors of finitely generated Witt rings*, Rocky Mountain J. Math., **16** (1986), 619–627.
- [7] ———, *Combinatorial techniques and abstract Witt rings, I*, J. Algebra, **114** (1988), 40–52.
- [8] ———, *Combinatorial techniques and abstract Witt rings, II*, Rocky Mountain J. Math., to appear.
- [9] M. Kula, *Fields with prescribed quadratic form schemes*, Math. Zeit., **167** (1979), 201–212.
- [10] ———, private communication.
- [11] M. Marshall, *Classification of finite spaces of orderings*, Canad. J. Math., **31** (1979), 320–330.
- [12] ———, *Abstract Witt Rings*, Queen's Papers in Pure and Applied Math. #57, Queen's University, Kingston, Ontario, Canada, 1980.
- [13] M. Marshall and J. Yucas, *Linked quaternionic mappings and their associated Witt rings*, Pacific J. Math., **95** (1981), 411–425.

Received September 30, 1988 and in revised form January 18, 1990.

SOUTHERN ILLINOIS UNIVERSITY
CARBONDALE, IL 62901-4408