ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 16, Number 3, Summer 1986

LOCAL FACTORS OF FINITELY GENERATED WITT RINGS

ROBERT FITZGERALD AND JOSEPH YUCAS

ABSTRACT. The Witt rings considered here are the abstract Witt rings in the sense of Marshall [3]. A local Witt ring is one with a unique non-trivial 2-fold Pfister form. Our main result gives necessary and sufficient conditions for a finitely generated Witt ring to be a product (in the category of Witt rings) of two Witt rings, one of which is local. The basic motivation is to develop a tool for the study of whether every finitely generated Witt ring is of elementary type (that is, can be built from local Witt rings $\mathbf{Z}/4\mathbf{Z}$ and $\mathbf{Z}/2\mathbf{Z}$ by a succession of products and group ring extensions), cf. [**3**; problem 4, p. 123].

1. Introduction. R will always denote a non-degenerate finitely generated Witt ring and G will be the multiplicative subgroup of one-dimensional forms in R. The category of Witt rings is equivalent to the category of quaternionic structures and also to that of the quaternionic schemes defined in [**1**]. We let q denote the quaternionic mapping associated with R. For $a \in G$, $D\langle 1, a\rangle = \{b \in G | q(b, -a) = 0\}$ is the value set of the form $\langle 1, a\rangle$; $i(a)$ will denote the index of $D\langle 1, a\rangle$ in G. For a subset K of G, we let $Q(K) = \{q(k, x) \mid k \in K, x \in G\}$. If $K = \{k\}$, we write $Q(k)$ for $Q(K)$. We will be mainly concerned with the existence of elements $a \in G$ such that $i(a) = 2$, equivalently, such that $|Q(-a)| = 2$.

For Witt rings R_1 and R_2 we let $R_1 \times_w R_2$ denote the product of R_1 and R_2 in the category of Witt rings. We say R_1 is a local factor of R if $R \cong R_1 \times_w R_2$ with R_1 a local Witt ring. C_2 denotes the group of order 2 and $R[C_2]$ denotes the group ring of C_2 with coefficients in R. Details on products and group rings of Witt rings may be found in [**3**].

For $a \in G$, we let $M(a) = \{m \in G | i(m) = 2,\ i(-am) = 2$ and $D\langle 1, m\rangle \neq D\langle 1, a\rangle\} \cup \{a\}$, and we let $H(a) = \bigcap_{m \in M(a)} D\langle 1, m\rangle$. We say a is a local element if $i(a) = 2$ and $\rho \notin Q(H(a))$, where ρ is the unique non-trivial element in $Q(-a)$. The main goal of this paper is to prove the following

THEOREM 1.1. *Let R be a finitely generated non-degenerate Witt ring. R has a local factor if and only if R has a local element.*

We take a moment here to motivate our definition of local element.

Received by the editors on August 27, 1984 and in revised form on December 7, 1984.

The Witt rings of elementary type which contain an element a with $i(a) = 2$ are of two types.

1. $R \times_w L$, where R is of elementary type and L is local. Here we can choose a to be any element of the form $(-1, x)$, $x \neq -1$.

2. $R \times S[C_2]$, where R is of elementary type and S is degenerate with $|G_S| > 2$. Here we can choose a to be any element of the form $(-1, -x)$ with $x \neq 1$ and in the radical of S.

Thus to classify Witt rings with local factors a further condition on a is needed to distinguish between these two types. The element $\rho \notin Q(H(a))$ does just that. In the first case $H(a) = G_R$ and $-a \in G_L$ so clearly $\rho \notin Q(H(a))$. In the second case, $H(a) = G_R \times G_S$ thus $-a \in H(a)$ and $\rho \in Q(H(a))$.

§2 is devoted to the proof of (1.1). We close this section with a preliminary result which characterizes the subgroups of G which yield Witt ring factors of R. For a subgroup H of G, we let $C(H) = \bigcap_{h\in H} D\langle 1, -h\rangle = \{k \in G | H \subseteq D\langle 1, -k\rangle\}$.

LEMMA 1.2. *Let H be a subgroup of G.*

i) $H \subseteq C(C(H))$.

ii) *If $G = H \cdot C(H)$, then $H \cap C(H) = \{1\}$ and $H = C(C(H))$.*

iii) *If $h \in H$, $k \in C(H)$, then $D\langle 1, hk\rangle \cap H = D\langle 1, h\rangle \cap H$ and $D\langle 1, hk\rangle \cap C(H) = D\langle 1, k\rangle \cap C(H)$.*

PROOF. i). If $k \in C(H)$, then $H \subseteq D\langle 1, -k\rangle$; hence $H \subseteq \bigcap_{k\in C(H)} D\langle 1, -k\rangle = C(C(H))$.

ii). Let $x \in H \cap C(H)$. Then $x \in C(H)$ and $x \in C(C(H))$ and so H, $C(H) \subseteq D\langle 1, -x\rangle$. But then $G = H \cdot C(H) \subseteq D\langle 1, -x\rangle$ and R non-degenerate implies $x = 1$. To show $H = C(C(H))$, let $x \in C(C(H))$ and write $x = hk$, $h \in H$, $k \in C(H)$. Then $C(H) \subseteq D\langle 1, -hk\rangle$ and $C(H) \subseteq D\langle 1, -h\rangle$, hence, $C(H) \subseteq D\langle 1, -k\rangle$. But $H \subseteq D\langle 1, -k\rangle$, thus, $G = H \cdot C(H) \subseteq D\langle 1, -k\rangle$. Since R is non-degenerate, $k = 1$ and $x \in H$.

iii). Let $h' \in H$. Since $k \in C(H)$, $h' \in D\langle 1, -k\rangle$. Consequently $h' \in D\langle 1, hk\rangle$ if and only if $h' \in D\langle 1, h\rangle$. Similarly if $k' \in C(H)$, then $k' \in D\langle 1, -h\rangle$; thus, $k' \in D\langle 1, hk\rangle$ if and only if $k' \in D\langle 1, k\rangle$.

We introduce more notation. If $D\langle 1, -x\rangle \subseteq D\langle 1, -y\rangle$ we write $x \leqq y$, and for a subgroup H of G we set $H_x = \{h \in H | x \leqq h\}$. As in **[4]**, the radical of an $x \in G$ is defined by $\text{rad}(x) = \{y \in G | x \leqq y\} = \bigcap_{z\in D\langle 1, -x\rangle} D\langle 1, -z\rangle$. Notice that $H_x = \text{rad}(x) \cap H$, and if $H = D\langle 1, -x\rangle$,then $C(H) = \text{rad}(x)$.

THEOREM 1.3. *For a subgroup H of G the following statements are equivalent:*

(1) *For all $x \in G$, $xH_x \cap C(H) \neq \varnothing$;*

(2) *For all $x \in G$, $xH \cap \text{rad}(x) \cap C(H) \neq \varnothing$;*

(3) *For all* $y \in G$, $x \in D\langle 1, y\rangle$ *implies* $xH \cap D\langle 1, y\rangle \cap C(H) \neq \varnothing$; *and*

(4) *The collections* $\{D\langle 1, h\rangle \cap H | h \in H\}$ *and* $\{D\langle 1, k\rangle \cap C(H) | k \in C(H)\}$ *are quaternionic schemes on* H *and* $C(H)$, *respectively, yielding Witt rings* R_1 *and* R_2 *such that* $R \cong R_1 \times_w R_2$.

PROOF. (1) $\Rightarrow$ (2). Since $H_x = \text{rad}(x) \cap H$ we have $xH_x = x(\text{rad}(x) \cap H) = \text{rad}(x) \cap xH$. (2) now follows from (1).

(2) $\Rightarrow$ (3). Let $y \in G$ and $x \in D\langle 1, y\rangle$. Notice that $\text{rad}(x) = \bigcap_{-z \in D\langle 1, -x\rangle} D\langle 1, z\rangle = \bigcap_{x \in D\langle 1, z\rangle} D\langle 1, z\rangle$. By (2), there is an $h \in H$ such that $xh \in \text{rad}(x) \cap C(H)$. Since $x \in D\langle 1, y\rangle$ and $xh \in \bigcap_{x \in D\langle 1, z\rangle} D\langle 1, z\rangle$, we see that $xh \in D\langle 1, y\rangle$. This proves (3).

(3) $\Rightarrow$ (4). First note that $G = H \cdot C(H)$. Namely, for any $y \in G$, $y \in D\langle 1, y\rangle$ and (3) imply that $yH \cap D\langle 1, y\rangle \cap C(H) \neq \varnothing$. Thus there exists an $h \in H$ such that $yh \in C(H)$, that is, $y \in H \cdot C(H)$. By (1.2) we thus also have $H \cap C(H) = \{1\}$.

Let $D_H\langle 1, a\rangle = D\langle 1, a\rangle \cap H$. To show that $\{D_H\langle 1, a\rangle | a \in H\}$ is a quaternionic scheme on H we must show, for all $a, b, c, d \in H$:

i) $a \in D_H\langle 1, a\rangle$;

ii) There is an $\alpha \in H$ such that $x \in D_H\langle 1, a\rangle \Rightarrow \alpha a \in D_H\langle 1, \alpha x\rangle$; and

iii) $bD_H\langle 1, \alpha a\rangle \cap D_H\langle 1, \alpha ac\rangle \cap dD_H\langle 1, \alpha c\rangle \neq \varnothing \Rightarrow aD_H\langle 1, \alpha b\rangle \cap D_H\langle 1, \alpha bd\rangle \cap cD_H\langle 1, \alpha d\rangle \neq \varnothing$.

(i) is obvious. For (ii), since $-1 \in G = H \cdot C(H)$ we may write $-1 = \alpha\beta$, with $\alpha \in H$ and $\beta = -\alpha \in C(H)$. Suppose $x \in D_H\langle 1, a\rangle$; then x, $a \in H$ and $-a \in D\langle 1, -x\rangle$. Since $-\alpha \in C(H)$, we have $-\alpha \in D\langle 1, -x\rangle$ and thus $\alpha a \in D\langle 1, -x\rangle$, $x \in D\langle 1, -\alpha a\rangle$. But $\alpha a \in H$, so $-\alpha \in D\langle 1, -\alpha a\rangle$ and $-\alpha x \in D\langle 1, -\alpha a\rangle$. Consequently, $\alpha a \in D_H\langle 1, \alpha x\rangle$.

To prove (iii) we first make the following

Claim. For $x, y \in H$, $x \in D_H\langle 1, \alpha y\rangle$ if and only if $x \in D\langle 1, -y\rangle$.

Namely, $D\langle 1, -y\rangle \cap H = D\langle 1, \alpha\beta y\rangle \cap H = D\langle 1, \alpha y\rangle \cap H$ by (1.2) (iii).

Thus $bD\langle 1, -a\rangle \cap D\langle 1, -ac\rangle \cap dD\langle 1, -c\rangle \neq \varnothing$. Since (iii) holds for G, there exists $y \in aD\langle 1, -b\rangle \cap D\langle 1, -bd\rangle \cap cD\langle 1, -d\rangle$. Since $y \in D\langle 1, -bd\rangle$ we have, by (3), that there exists an $h \in H$ with $yh \in D\langle 1, -bd\rangle \cap C(H)$. Consequently, $h \in D\langle 1, -bd\rangle$ and $yh \in D\langle 1, -z\rangle$, for all $z \in H$. Now, ya, $yh \in D\langle 1, -b\rangle$, hence $ah \in D\langle 1, -b\rangle$. Also, yc, $yh \in D\langle 1, -d\rangle$, hence $ch \in D\langle 1, -d\rangle$. This shows $aD\langle 1, -b\rangle \cap D\langle 1, -bd\rangle \cap cD\langle 1, -d\rangle \cap H \neq \varnothing$. The Claim then implies (iii).

To show $\{D\langle 1, k\rangle \cap C(H) | k \in C(H)\}$ is a quaternionic scheme on $C(H)$, it suffices to show $C(H)$ satisfies (3). Multiplying, (3) applied to H, by x yields $H \cap D\langle 1, y\rangle \cap x\,C(H) \neq \varnothing$. Since $H \subseteq C(C(H))$ by (1.2), (3) holds for $C(H)$.

Now we have $G = H \times C(H)$ as groups and the distinguished element of $C(H)$ is $\beta = -\alpha$, where α is the distinguished element of H. So it remains to show only that $D\langle 1, y\rangle = D_H\langle 1, y\rangle \cdot D_{C(H)}\langle 1, y\rangle$, for all $y \in G$. Let $z \in D\langle 1, y\rangle$. By (3), $zH \cap D\langle 1, y\rangle \cap C(H) \neq \varnothing$ so there exists an $h \in H$ with $h \in D\langle 1, y\rangle$, $zh \in D\langle 1, y\rangle$ and $zh \in C(H)$. Consequently $z = h(zh)$, $h \in D_H\langle 1, y\rangle$, and $zh \in D_{C(H)}\langle 1, y\rangle$. And, finally, if $h \in D_H\langle 1, y\rangle$ and $k \in D_{C(H)}\langle 1, y\rangle$, then clearly $hk \in D\langle 1, y\rangle$.

(4) $\Rightarrow$ (1). For an $x \in G$, (4) implies $x = hk$, for some $h \in H$, $k \in C(H)$. Notice that $k = xh \in xH \cap C(H)$, so it suffices to show that $D\langle 1, -x\rangle \subseteq D\langle 1, -h\rangle$. Now $D\langle 1, -x\rangle = D\langle 1, -hk\rangle = D_H\langle 1, -hk\rangle D_{C(H)}\langle 1, -hk\rangle$, by (4). Let $z \in D\langle 1, -x\rangle$. Write $z = z_1 z_2$ where $z_1 \in D\langle 1, -hk\rangle \cap H$ and $z_2 \in D\langle 1, -hk\rangle \cap C(H)$. Now $z_2 \in D(H)$ implies $z_2 \in D\langle 1, -h\rangle$, and $z_1 \in H \subseteq C(C(H))$, by (1.2), implies $z_1 \in D\langle 1, -k\rangle$. Thus $z_1 \in D\langle 1, -k\rangle \cap D\langle 1, -hk\rangle \subseteq D\langle 1, -h\rangle$, and so $z = z_1 z_2 \in D\langle 1, -h\rangle$.

2. Local elements and local factors. Throughout, we fix a local element $a \in G$. We will write M for $M(a)$ and H for $H(a)$. We begin with the case $|M| = 1$.

PROPOSITION 2.1. *If $M = \{a\}$, then $-1 \notin D\langle 1, a\rangle$ and $D\langle 1, a\rangle = \bigcup_{x \in D\langle 1, a\rangle} D\langle 1, x\rangle$.*

PROOF. If $-1 \in D\langle 1, a\rangle$, then a cannot be a local element, since $-a \in D\langle 1, a\rangle = H \Rightarrow \rho \in Q(H)$. Hence $-1 \notin D\langle 1, a\rangle$. Assume there exist $x \in D\langle 1, a\rangle$ and $y \in D\langle 1, x\rangle$ with $y \notin D\langle 1, a\rangle$. We have $\langle 1, a\rangle \simeq \langle x, xa\rangle$, $\langle 1, x\rangle \simeq \langle y, xy\rangle$. Since $i(a) = 2$ and $-1 \notin D\langle 1, a\rangle$, $\langle 1, 1, a, a\rangle \simeq \langle 1, a, -y, -ay\rangle$. On the other hand $\langle 1, 1, a, a\rangle \simeq \langle 1, a, x, xa\rangle \simeq \langle a, xa, y, xy\rangle$. Thus $\langle 1, a, -y, -ay\rangle \simeq \langle a, xa, y, xy\rangle$; hence, $\langle 1, a, -xy, -xa\rangle \simeq \langle y, y, ay, a\rangle$. Upon multiplying by ya, we obtain $\langle ya, y, -xa, -xy\rangle \simeq \langle a, a, 1, y\rangle$. After cancelling $\langle y\rangle$ we see that ya is represented by the pure part of $\langle\langle 1, a\rangle\rangle$. Consequently, $\rho = q(-1, -a) = q(-ya, z)$, for some $z \in G$. Now $-ya \in D\langle 1, a\rangle = H$; thus $\rho \in Q(H)$, contradicting the fact that a is a local element.

COROLLARY 2.2. *If $M = \{a\}$, then $R \cong \mathbf{Z} \times_w S$ for some nondegenerate Witt ring S.*

PROOF. Let $K = \{1, -a\}$. We show first that (1.3) (3) is satisfied. Notice that $C(K) = D\langle 1, a\rangle$. Let $y \in G$, $x \in D\langle 1, y\rangle$. If $x \in D\langle 1, a\rangle$, then clearly $x \in xK \cap D\langle 1, y\rangle \cap D\langle 1, a\rangle$. Suppose $x \notin D\langle 1, a\rangle$. By (2.1), $-1 \notin D\langle 1, a\rangle$, and, since $i(a) = 2$, we have $-x \in D\langle 1, a\rangle$. Now $-y \in D\langle 1, -x\rangle$, so $-y \in D\langle 1, a\rangle$ by (2.1). Consequently, $-xa \in xK \cap D\langle 1, y\rangle \cap D\langle 1, a\rangle$. Now since $q(-a, -a) \neq 0$, it follows from [3, p. 42, Case 4] that the Witt ring associated with K is $\mathbf{Z}$.

The statement and proof of (2.2) are implicit in [5, 3.3].

From this point on we assume $M \neq \{a\}$, that is we assume $|M| > 1$. We begin a study of the structure of M.

LEMMA 2.3. *Let G be an arbitrary group with subgroups H_1, H_2, H_3 of index 2. If $H_1 \cap H_2 = H_1 \cap H_3$ and $H_2 \neq H_3$, then $G = H_1 \cup H_2 \cup H_3$.*

PROOF. Suppose $g \in G$ with $g \notin H_1 \cup H_2 \cup H_3$. We show $H_2 = H_3$, contradicting our hypothesis. Let $h \in H_2$. If $h \in H_1$, $h \in H_1 \cap H_2 \subseteq H_3$. If $h \notin H_1$, then $gh \in H_1$. Notice that $gh \notin H_3$, for, otherwise, $gh \in H_1 \cap H_3 \subseteq H_2$, implying that $g \in H_2$. Consequently, $h = g(gh) \in H_3$ and $H_2 \subseteq H_3$. Since H_2 and H_3 are subgroups of the same index, $H_2 = H_3$.

LEMMA 2.4. *Let $m, m' \in M$, $m \neq m'$. Then*:
(1) $Q(-m) = Q(-a) = Q(-m')$;
(2) $D\langle 1, m\rangle \neq D\langle 1, m'\rangle$;
(3) $i(-mm') = 2$; *and*
(4) $G = D\langle 1, m\rangle \cup D\langle 1, m'\rangle \cup D\langle 1, -mm'\rangle$.

PROOF. To prove (1), it suffices to show that $Q(-m) = Q(-a)$. Clearly we may assume $m \neq a$. Since $m \in M$, $i(a) = i(m) = i(-am) = 2$, $D\langle 1, -am\rangle \cap D\langle 1, a\rangle = D\langle 1, -am\rangle \cap D\langle 1, m\rangle$ and $D\langle 1, a\rangle \neq D\langle 1, m\rangle$. By (2.3), $G = D\langle 1, a\rangle \cup D\langle 1, m\rangle \cup D\langle 1, -am\rangle$. Since G is not the union of two proper subgroups, there exists $x \notin D\langle 1, a\rangle \cup D\langle 1, m\rangle$, $x \in D\langle 1, -am\rangle$. This implies that $q(x, -a) \neq 0$, $q(x, -m) \neq 0$ and $q(x, am) = 0$. But $q(x, am) = 0$ forces $q(x, -a) = q(x, -m)$. Since $i(a) = i(m) = 2$, $|Q(-a)| = |Q(-m)| = 2$; hence, $Q(-a) = Q(-m)$. To prove (2) and (3), notice that $|Q(-m) \cap Q(-m')| = 2$, so by [3, 5.2], $D\langle 1, m\rangle \cap D\langle 1, m'\rangle$ has index 2 in $D\langle 1, -mm'\rangle$. Since $D\langle 1, m\rangle \cap D\langle 1, m'\rangle$ has index 2 or 4 in G, this forces $D\langle 1, m\rangle \cap D\langle 1, m'\rangle$ to have index 4 in G and thus $D\langle 1, -mm'\rangle$ must have index 2 in G. Statement (4) now follows from (2), (3) and (2.3).

LEMMA 2.5. *Let $x_1, x_2, x_3 \in G$ and suppose*:
(a) $i(x_1) = i(x_2) = i(x_3) = 2$;
(b) $i(-x_1x_2) = i(-x_1x_3) = i(-x_2x_3) = 2$; *and*
(c) $D\langle 1, x_i\rangle \neq D\langle 1, x_j\rangle$, for $i \neq j$.
Then $i(x_1x_2x_3) \leqq 2$.

PROOF. Since $D\langle 1, x_1\rangle \cap D\langle 1, -x_2x_3\rangle \subseteq D\langle 1, x_1x_2x_3\rangle$ we have $i(x_1x_2x_3) \leqq 4$. Assume $i(x_1x_2x_3) = 4$. In this case $D\langle 1, x_1x_2x_3\rangle = D\langle 1, x_1\rangle \cap D\langle 1, -x_2x_3\rangle$, so, in particular, $D\langle 1, x_1x_2x_3\rangle \subseteq D\langle 1, x_1\rangle$. Similarly, $D\langle 1, x_1x_2x_3\rangle \subseteq D\langle 1, x_2\rangle$ and $D\langle 1, x_1x_2x_3\rangle \subseteq D\langle 1, x_3\rangle$. By (c), we get $D\langle 1, x_1x_2x_3\rangle = D\langle 1, x_i\rangle \cap D\langle 1, x_j\rangle$, for $i \neq j$. But then $D\langle 1, x_1\rangle \cap D\langle 1, x_2\rangle = D\langle 1, x_1\rangle \cap D\langle 1, x_3\rangle$, so, by (2.3), $G = D\langle 1, x_1\rangle \cup D\langle 1, x_2\rangle \cup D\langle 1, x_3\rangle$. Since G is not the union of two proper subgroups, there exists $g \in D\langle 1, x_3\rangle$, $g \notin D\langle 1, x_1\rangle \cup D\langle 1, x_2\rangle$. Recall that $D\langle 1, x_1\rangle \cap D\langle 1, -x_2x_3\rangle = D\langle 1, x_1x_2x_3\rangle = D\langle 1, x_1\rangle \cap D\langle 1, x_2\rangle$. Also, $D\langle 1, -x_2x_3\rangle \neq D\langle 1, x_2\rangle$, else $D\langle 1, x_3\rangle = D\langle 1, x_2\rangle$; by (2.3), $G = D\langle 1, x_1\rangle \cup D\langle 1, x_2\rangle \cup D\langle 1, -x_2x_3\rangle$. Consequently, $g \in D\langle 1, -x_2x_3\rangle$. Then $g \in D\langle 1, x_3\rangle \cap D\langle 1, -x_2x_3\rangle \subseteq D\langle 1, x_2\rangle$, a contradiction.

LEMMA 2.6. *Let $x, y, z \in G, z \neq -xy$, with $i(x) = i(y) = i(z) = i(-yz) = 2$. If $D\langle 1, -xy\rangle = D\langle 1, z\rangle$, then $D\langle 1, x\rangle = D\langle 1, y\rangle = D\langle 1, z\rangle$.*

PROOF. If $D\langle 1, y\rangle = D\langle 1, z\rangle$, then $D\langle 1, y\rangle = D\langle 1, -xy\rangle = D\langle 1, x\rangle$; so assume $D\langle 1, y\rangle \neq D\langle 1, z\rangle$. Also, $D\langle 1, z\rangle = D\langle 1, -xy\rangle \cap D\langle 1, z\rangle \subseteq D\langle 1, xyz\rangle$; thus $D\langle 1, z\rangle = D\langle 1, xyz\rangle$, since $i(z) = 2$ and $z \neq -xy$. Now, $D\langle 1, -yz\rangle \cap D\langle 1, y\rangle = D\langle 1, -yz\rangle \cap D\langle 1, z\rangle$; thus, by (2.3), $G = D\langle 1, y\rangle \cup D\langle 1, z\rangle \cup D\langle 1, -yz\rangle$. Consequently, $D\langle 1, x\rangle = D\langle 1, x\rangle \cap D\langle 1, y\rangle \cup D\langle 1, x\rangle \cap D\langle 1, z\rangle \cup D\langle 1, x\rangle \cap D\langle 1, -yz\rangle$. Now $D\langle 1, x\rangle \cap D\langle 1, y\rangle \subseteq D\langle 1, -xy\rangle = D\langle 1, z\rangle$ and $D\langle 1, x\rangle \cap D\langle 1, -yz\rangle \subseteq D\langle 1, xyz\rangle = D\langle 1, z\rangle$, so $D\langle 1, x\rangle \subseteq D\langle 1, z\rangle$. Since $i(x) = i(z)$, $D\langle 1, x\rangle = D\langle 1, z\rangle$ and $D\langle 1, x\rangle = D\langle 1, -xy\rangle = D\langle 1, y\rangle$, a contradiction.

LEMMA 2.7. *Let $m_1, m_2 \in M$. Then*
(1) $-m_1m_2 \in M \cup \{-1\}$; and
(2) $am_1m_2 \in M \cup \{-1\}$.

PROOF. (1). First note that if $m_1 = m_2$, then $-m_1m_2 = -1 \in M \cup \{-1\}$. If $m_1 = a$ and $m_2 \neq a$, then $i(-m_1m_2) = i(-am_2) = 2$, since $m_2 \in M$ and $i(am_1m_2) = i(m_2) = 2$. If $D\langle 1, -m_1m_2\rangle = D\langle 1, a\rangle$, then $D\langle 1, -am_2\rangle = D\langle 1, a\rangle = D\langle 1, m_2\rangle$, a contradiction. So in this case, (1) is true. Similarly, if $m_1 \neq a$ and $m_2 = a$, the result is true. If $-m_1m_2 = a$, then clearly $-m_1m_2 \in M$ so we may assume that $m_1 \neq m_2, m_1 \neq a$, $m_2 \neq a$ and $-m_1m_2 \neq a$. By (2.4) (3), $i(-m_1m_2) = 2$. Notice that $i(a) = i(m_1) = i(m_2) = 2$, $i(-am_1) = i(-am_2) = i(-m_1m_2) = 2$ and $D\langle 1, a\rangle \neq D\langle 1, m_1\rangle$, $D\langle 1, a\rangle \neq D\langle 1, m_2\rangle$, and by (2.4) (2), $D\langle 1, m_1\rangle \neq D\langle 1, m_2\rangle$. So by (2.5), $i(am_1m_2) \leqq 2$. But if $i(am_1m_2) = 1$, then $-m_1m_2 = a$, contradicting our assumption; thus, $i(am_1m_2) = 2$. If $D\langle 1, -m_1m_2\rangle = D\langle 1, a\rangle$, then $D\langle 1, m_1\rangle = D\langle 1, m_2\rangle$, by (2.6), a contradiction. Hence $i(-m_1m_2) = 2$, $i(am_1m_2) = 2$, and $D\langle 1, -m_1m_2\rangle \neq D\langle 1, a\rangle$, so $-m_1m_2 \in M$.

(2). By (1), $-m_1m_2 \in M \cup \{-1\}$. If $-m_1m_2 = -1$, then $am_1m_2 = a \in M$. If $-m_1m_2 \in M$, then $am_1m_2 = -(a)(-m_1m_2) \in M \cup \{-1\}$, by (1).

PROPOSITION 2.8. (1) *If $m_1, m_2, \ldots, m_{2n+1} \in M \cup \{-1\}$, then $m_1 \cdot m_2 \cdot \cdots \cdot m_{2n+1} \in M \cup \{-1\}$.*

(2) *If* $m_1, m_2, \ldots, m_{2n} \in M \cup \{-1\}$, *then* $-m_1 \cdot m_2 \cdot \cdots \cdot m_{2n} \in M \cup \{-1\}$.

PROOF. (1). It sufficies to do the case $n = 1$, for then $m_1 \cdot m_2 \cdot \cdots \cdot m_{2n+1} = (m_1m_2m_3)m_4 \cdot \cdots \cdot m_{2n+1}$ is a product of $(2n-1)$ elements of $M \cup \{-1\}$. Thus we must show $m_1m_2m_3 \in M \cup \{-1\}$. First notice that we may assume that the m_i are distinct, for otherwise it is trivial. We may also assume that $m_i \neq a$, $i = 1, 2, 3$, since then $m_1m_2m_3 \in M \cup \{-1\}$ by (2.7) (2). Further, we may assume $m_1 \neq -m_2m_3$, since then $-1 = m_1m_2m_3 \in M \cup \{-1\}$. Finally, we may assume that $m_i \neq -1$, for then the result is either trivial or follows from (2.7) (1). Now, by (2.4) (2) and (3), $i(-m_im_j) = 2$ and $D\langle 1, m_i\rangle \neq D\langle 1, m_j\rangle$, for $i \neq j$. By (2.5), with $x_i = m_i$, $i(m_1m_2m_3) \leqq 2$. Strict inequality holds only if $m_1 = -m_2m_3$ which we are assuming is not so, thus $i(m_1m_2m_3) = 2$. We now want to apply (2.5) with $x_i = -am_i$. Now $m_i \neq a$, so $x_i \in M$ by (2.7) (1). Also $x_i \neq a$, since $m_i \neq -1$. Applying (2.5), we get $i(-am_1m_2m_3) \leqq 2$. Again, $i(-am_1m_2m_3) = 2$, else $m_1m_2m_3 = a \in M$. It remains only to show that $D\langle 1, m_1m_2m_3\rangle \neq D\langle 1, a\rangle$. If this is not so, then, by (2.6), $D\langle 1, m_1\rangle = \langle 1, -m_2m_3\rangle = D\langle 1, a\rangle$, a contradiction.

(2). Again it suffices to do only the case $n = 1$, for then $-m_1 \cdot m_2 \cdot \cdots \cdot m_{2n} = (-m_1m_2)m_3 \cdot \cdots \cdot m_{2n}$ which is a product of $(2n-1)$ elements of $M \cup \{-1\}$ and by (1) must be in $M \cup \{-1\}$. If $m_1, m_2 \in M$, then $-m_1m_2 \in M \cup \{-1\}$ by (2.7) (1). If $m_1 = -1$ and/or $m_2 = -1$, the result is trivial.

PROPOSITION 2.9. (1) *M^2 is a subgroup of G.*

(2) $M^2 = -M \cup \{1\}$.

PROOF. (1). Let $m_1m_2, m_3m_4 \in M^2$. Then $(m_1m_2)(m_3m_4) = m_1(m_2m_3m_4) \in M \cdot (M \cup \{-1\}) = M^2 \cup -M$, by (2.8) (1). Thus it suffices to show $-M \subseteq M^2$. Let $-m \in -M$. There exists $m_1 \in M$ with $m_1 \neq m$ (otherwise $M = \{a\}$, contrary to the assumption made after (2.2)), and so $-m = m_1(-mm_1) \in M^2$ by (2.7) (1).

(2). As in (1), $-M \subseteq M^2$ and so $-M \cup \{1\} \subseteq M^2$. On the other hand, $-M^2 \subseteq M \cup \{-1\}$ by (2.7), so $M^2 \subseteq -M \cup \{1\}$.

We turn now to the relationships among M, H and $C(H)$.

COROLLARY 2.10. $M^2 \cap H = \{1\}$.

PROOF. Let $x \in M^2 \cap H$. By (2.9) (2) we may assume $-x = m \in M$. Then by (2.4) (1), $Q(x) = Q(-a)$, that is, $\rho \in Q(x)$ and $x \in H$, contradicting our basic assumption.

For $g \in G$, let $S(g) = \{-m \in -M | g \in D\langle 1, m\rangle\} \cup \{1\}$.

PROPOSITION 2.11. (1) *For each $g \in G$, $S(g)$ is a subgroup of M^2.*

(2) *$S(g)$ has index $\leqq 2$ in M^2 with equality holding if and only if $g \notin H$.*
(3) *For $x, y \in -M^2$, $x \neq y$, we have $S(x) \neq S(y)$.*

PROOF. (1). Notice that $S(g) = (-M \cup \{1\}) \cap D\langle 1, -g\rangle$, so (1) follows from (2.9).

(2). Suppose $x, y \in M^2 - S(g)$. We show $xy \in S(g)$. Clearly we may assume $x \neq y$. Now $x, y \in -M$ by (2.9) (2), so $g \notin D\langle 1, -x\rangle \cup D\langle 1, -y\rangle$, and thus $g \in D\langle 1, -xy\rangle$. Also, $-xy \in M$ by (2.7) (1); hence, $xy \in S(g)$. This shows that $|M^2/S(g)| \leqq 2$. Notice that $M^2 = S(g)$ if and only if $g \in H$.

(3). Suppose $S(x) = S(y)$. Then, for all $m \in M$, either x and y are in $D\langle 1, m\rangle$ or x and y are not in $D\langle 1, m\rangle$. Since $i(m) = 2$, we see that in either case $xy \in D\langle 1, m\rangle$; hence, $xy \in H$. Recall that $-M^2 = M \cup \{-1\}$. If $x \in M$ and $y = -1$, then $x \in -H \cap M$. By (2.4)(1), $Q(-a) = Q(-x)$, and then $\rho \in Q(-x)$ and $-x \in H$, contradicting our basic assumption. If $x \in M$ and $y \in M$, then $xy \in M^2 \cap H = \{1\}$, by (2.10), again a contradiction.

We thank M. Kula for simplifying an earlier version of (2.11 (1)).

PROOOSITION 2.12. (1) $G = M^2H$.
(2) $G = H \cdot C(H)$.
(3) $H \cap C(H) = \{1\}$.
(4) $C(H) = M^2$.
(5) $Q(C(H)) = \{0, \rho\}$.

PROOF. (1). Let $|M^2| = 2^k$. By (2.11) (1) (2), $\{S(x) \mid x \in -M^2\}$ is a collection of 2^k distinct subgroups of M^2, all of index $\leqq 2$. Since there are only $2^k - 1$ subgroups of index 2 in M^2, the collection $\{S(x) | x \in -M^2\}$ consists of all subgroups of M^2 of index $\leqq 2$. Now let $g \in G$. Then $S(g)$ is a subgroup of M^2 of index $\leqq 2$. Hence there exists $x \in -M^2$ such that $S(g) = S(x)$. But then, as in the proof of (2.11) (3), $gx \in H$. Consequently, $g \in xH \subseteq -M^2H$. That is, $G = -M^2H$ and so $G = M^2H$.

(2). $M^2 = -M \cup \{1\}$ by (2.9) (2). Thus if $x \in M^2$, $H \subseteq D\langle 1, -x\rangle$ and so $x \in C(H)$. That is, $M^2 \subseteq C(H)$. Hence (2) follows from (1).

(3). This follows from (2) by (1.2).

(4). We have shown $M^2 \subseteq C(H)$. Parts (2) and (3) imply $|G| = |H| \cdot |C(H)|$. If $M^2 \neq C(H)$, then $|G| > |H| \cdot |M^2|$, which contradicts (1).

(5). $Q(C(H)) = \{q(c, x) \mid c \in C(H), x \in G\} = \{q(-m, x) \mid m \in M, x \in G\}$ by (4) and (2.9) (2). But $q(-m, x) = 0$ or ρ by (2.4) (1). Hence $Q(C(H)) = \{0, \rho\}$.

PROOF OF THEOREM 1.1. Recall that if $|M| = 1$, we have already proved the result in Corollary 2.2. For $|M| > 1$, we first show that $D\langle 1, mh\rangle \subseteq D\langle 1, m\rangle$, for every $h \in H$. Let $x \in D\langle 1, mh\rangle$. Then $q(x, -mh) = 0$, hence, $q(x, -m) = q(x, h)$. If $q(x, -m) = 0$, then $x \in D\langle 1, m\rangle$ as desired. If $q(x, -m) \neq 0$, then $q(x, -m) = \rho$ by (2.4) (1). Consequently, $q(x, h) = \rho$ and thus $\rho \in Q(H)$, contradicting our basic assumption. Now, to prove that $G = H \times_w C(H)$, we need only show that statement (1) of (1.3) is satisfied. Let $x \in G$. We must show $xH_x \cap C(H) \neq \emptyset$. By (2.12) (2), $x = hc$ for some $h \in H$, $c \in C(H)$. By (2.12) (4) and (2.9) (2), $c \in -M \cup \{1\}$. If $c = 1$, then $x = h$; clearly $1 \in xH_x \cap C(H)$. Suppose then that $c \in -M$. Write $c = -m$, for some $m \in M$. Then $x = hc = -hm$. Since $xh \in C(H)$, it suffices to show that $xh \in xH_x$. That is, we will show $h \in H_x$. Let $y \in D\langle 1, -x\rangle = D\langle 1, hm\rangle$. By the first part of our proof we see that $y \in D\langle 1, m\rangle \cap D\langle 1, hm\rangle \subseteq D\langle 1, -h\rangle$. Consequently, $D\langle 1, -x\rangle \subseteq D\langle 1, -h\rangle$ and $h \in H_x$. Finally, by (2.12) (5) we see that $C(H)$ is a local factor.

To illustrate the use of (1.1) we close with a proof of a result due to Kaplansky **[2]**.

COROLLARY 2.13. *If* $|G| > 1$ *and* $i(a) = 2$, *for every* $a \in G - \{-1\}$, *then* $|Q(G)| = 2$.

PROOF. Let $a \in G$. We have $M(a) = \{m \in G | D\langle 1, m\rangle \neq D\langle 1, a\rangle\} \cup \{a\}$. Notice that if $-1 \neq g \in G - M(a)$, then $D\langle 1, g\rangle = D\langle 1, m\rangle$, for some $m \in M(a)$. Hence $H(a) = \bigcap_{m \in M(a)} D\langle 1, m\rangle = \bigcap_{g \in G} D\langle 1, g\rangle = \{1\}$, since R is non-degenerate. Thus $C(H) = \bigcap_{h \in H(a)} D\langle 1, -h\rangle = G$. Clearly a is a local element, so (1.1) implies $|Q(G)| = |Q(C(H))| = 2$.

REFERENCES

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

2. I. Kaplansky, *Fröhlich's local quadratic froms*, J. Reine Angew. Math. **239** (1969), 74–77.

3. M. Marshall, *Abstract Witt Rings*, Queen's Papers in Pure and Applied Math. No. **57**, Queen's Univ. Kingston, Ontario, Canada (1980).

4. ———, *Intersection properties of value groups of quadratic form schemes*, preprint.

5. J. Yucas, *Witt rings and associated Boolean rings*. J. Algebra **71** (1981), 40–49.

SOUTHERN ILLINOIS UNIVERSITY AT CARBONDALE, CARBONDALE, IL. 62901