Can. J. Math. Vol. **49** (3), 1997 pp. 499–519

GORENSTEIN WITT RINGS II

ROBERT W. FITZGERALD

ABSTRACT. The abstract Witt rings which are Gorenstein have been classified when the dimension is one and the classification problem for those of dimension zero has been reduced to the case of socle degree three. Here we classify the Gorenstein Witt rings of fields with dimension zero and socle degree three. They are of elementary type.

The elementary type conjecture, stated by Marshall [11] in 1980, is a proposed classification of noetherian Witt rings R. There is still little evidence for its validity; the basic known cases are when R is reduced or has at most 32 generators. The case of Gorenstein Witt rings was first studied in [5], primarily because it seemed tractable. They also have particularly simple Ext-algebras and often arise in that context (*cf.* [6], [7]).

Let R denote a noetherian, abstract (in the sense of Marshall [11]) Witt ring. The only important examples are Witt rings of fields F with $F^\bullet/F^{\bullet 2}$ finite. The elementary type conjecture for the Gorenstein case is:

(C)

If R is a Gorenstein Witt ring then R is a group ring extension of a Witt ring of local type (*i.e.* a Witt ring of a local field).

(C) was shown in [5] to hold in the following cases:

(1) $\dim R \neq 0$.

(2) $\dim R = 0$ and the socle degree, $\sigma(R)$, is at most two.

(3) If (C) holds for all R with $\dim R = 0$ and $\sigma(R) = 3$, then (C) holds for all R.

In this paper we show that (C) holds when $\dim R = 0$, $\sigma(R) = 3$ and R is the Witt ring of a field.

The proof of our result uses quadratic field extensions, a technique not available in the abstract setting. More importantly, the reduction step (3) used Pfister quotients which are not known to exist in the category of Witt rings of fields. Thus our result does not imply the classification of all Gorenstein Witt rings of fields. Still it gives the most important example of the only open case. Further, we are able to classify certain 2-Hilbert fields, introduced by Szymiczek [13].

From now on R is a Gorenstein Witt ring with $\dim R = 0$ and $\sigma(R) = 3$. Let G be the associated group of one dimensional forms and q the associated quaternionic mapping. R Gorenstein and zero-dimensional means, by Bass' criterion, that $\dim(\operatorname{ann} I_R) = 1$. R having socle degree three means that $\operatorname{ann} I_R = \{0, \sigma\}$, for some anisotropic 3-fold Pfister

Received by the editors June 3, 1996.
AMS subject classification: Primary: 11E81; Secondary: 13H10.

form σ. Some simple consequences are that $I_R^4 = 0, I_R^3 = \{0, \sigma\}$ and every anisotropic 2-fold Pfister form represents half of G. Two less obvious consequences are:

(0.0.1) $\operatorname{ann}(\operatorname{ann} I) = I$, for any ideal $I \subset R$.

(0.0.2) $|D\langle 1, -x\rangle|\,|D\langle 1, -y\rangle|\,|D\langle 1, -xy\rangle| = g|D\langle 1, -x\rangle \cap D\langle 1, -y\rangle|^2$, for any $x, y \in G$.

(0.0.1) is [5, 2.8] and (0.0.2) is [5, 2.17]. We will also often use the Block Design Counting formula:

(0.0.3)
$$\sum_{x\in A} |D\langle 1, -x\rangle \cap B| = \sum_{y\in B} |D\langle 1, -y\rangle \cap A|,$$

for sets $A, B \subset G$. Both sides of (0.0.3) count the number of pairs (x, y) with $x \in A$, $y \in B$ and $x \in D\langle 1, -y\rangle$. A different version of this first appeared in [8] while the above version is from [10].

F will denote a field of characteristic not two. We are only concerned with the case that $\operatorname{char} WF \neq 0$ so we always assume that F is non-formally real. Let g denote $|G|$. E_n denotes the elementary abelian group of exponent 2 and order 2^n. For a multiplicative group H we use $H^\bullet$ to denote $H \setminus \{1\}$. The index of an element $x \in G$, $i(x)$, is the index of $D\langle 1, -x\rangle$ in G. We will work in as great a generality as is convenient. In particular, we will work with abstract Witt rings in the first two sections and switch to the field case in the last two sections. We close this introduction with a statement of the usual way to verify conjecture (C) for our Gorenstein Witt rings of socle degree three.

PROPOSITION 0.1. *The following are equivalent:*

(1) G has a rigid element.

(2) $R = L[E_1]$ for some Witt ring L of local type.

(3) R is of elementary type.

PROOF. (1)⟶(2): Let $t \in G$ be a rigid element. Then, since $\operatorname{char} R \neq 0$, t is birigid by [1, Corollary to Theorem 1] (the proof in [1] is valid for abstract Witt rings, see [12, 4.15]). Thus $R = S[E_1]$, for some Witt ring S, by [11, 5.19]. S is isomorphic to the Pfister quotient $R/\operatorname{ann}\langle 1, -t\rangle$. So S is Gorenstein of socle degree two by [5, 2.6], and hence of local type by [5, 2.5].

(2)⟶(3) is clear. (3)⟶(1): R is not of local type since $I_R^3 \neq 0$. If R is a product then $G \approx H \times K$, for some non-trivial subgroups H and K of G. For each $h \in H$, $k \in K$ we have:

$$D\langle 1, -hk\rangle = D\langle 1, -h\rangle \cap D\langle 1, -k\rangle,$$

by [11, pp. 100-101]. In particular, if $h \neq 1$, $k \neq 1$ then $D\langle 1, -hk\rangle \subset D\langle 1, -h\rangle$, so that, by definition, $h \in \operatorname{rad}(hk)$. But $\operatorname{rad}(hk) = \{1, hk\}$ by [5, 2.9] which forces $h = 1$ or $h = hk$. Either case contradicts the supposition that $h \neq 1$, $k \neq 1$. Hence R is not a product. R being of elementary type then implies that R is a group ring extension. Thus G has a rigid element by [11, pp. 115-116]. ∎

https://doi.org/10.4153/CJM-1997-023-1 Published online by Cambridge University Press

1. **Elements of Index 4.** The case where G has an element of index 4 will be the first step in the induction argument proving our result. However, it requires a different treatment than the other cases. We begin that study here for abstract Witt rings. Set:

$$B_k = \{x \in G \mid i(x) = 2^k\}$$
$$B_2^+ = B_2 \cup \{1\}.$$

LEMMA 1.1. *(1) B_2^+ is a subgroup of G.*
(2) $B_2B_k \subset B_k$. In particular, B_k is a union of cosets of B_2^+.
(3) If $a \in B_2$ and $x \neq 1$, a then $|D\langle 1,-a\rangle \cap D\langle 1,-x\rangle| = \frac{1}{2}|D\langle 1,-x\rangle|$.

PROOF. We start with (3). $D\langle 1,-x\rangle$ is not a subset of $D\langle 1,-a\rangle$ [5, 2.9] and $i(a) = 4$ implies that $|D\langle 1,-a\rangle \cap D\langle 1,-x\rangle| = \frac{1}{2}|D\langle 1,-x\rangle|$ or $\frac{1}{4}|D\langle 1,-x\rangle|$. Suppose that $|D\langle 1,-a\rangle \cap D\langle 1,-x\rangle| = \frac{1}{4}|D\langle 1,-x\rangle|$. Then by (0.0.2):

$$\frac{g}{4} \cdot |D\langle 1,-x\rangle| \cdot |D\langle 1,-ax\rangle| = g \cdot \frac{1}{16}|D\langle 1,-x\rangle|^2$$
$$|D\langle 1,-ax\rangle| = \frac{1}{4}|D\langle 1,-x\rangle|$$
$$= |D\langle 1,-a\rangle \cap D\langle 1,-x\rangle|.$$

But then $D\langle 1,-ax\rangle = D\langle 1,-a\rangle \cap D\langle 1,-x\rangle \subset D\langle 1,-a\rangle$, which is impossible by [5, 2.9]. This proves (3).

Now suppose that $x \in B_k$. Again using (0.0.2):

$$\frac{g}{4} \cdot |D\langle 1,-x\rangle| \cdot |D\langle 1,-ax\rangle| = g\Big(\frac{1}{2}|D\langle 1,-x\rangle|\Big)^2$$
$$|D\langle 1,-ax\rangle| = |D\langle 1,-x\rangle|.$$

So $ax \in B_k$ giving (2). When $k = 2$ this is (1). ∎

Fix $a \in B_2$ and $b_1, b_2, b_3 = b_1b_2$ such that $G = \{1, b_1, b_2, b_3\}D\langle 1,-a\rangle$. Set $\rho_i = q(a, b_i)$ for $i = 1, 2, 3$. Then $Q(a) = \{1, \rho_1, \rho_2, \rho_3\}$. Further, we will always assume that:

$$|D\langle 1,-b_1\rangle| \geq |D\langle 1,-b_2\rangle| \geq |D\langle 1,-b_3\rangle|.$$

LEMMA 1.2. *Let $\alpha, \beta \in D\langle 1,-a\rangle$ and let $i \neq j$ for $1 \leq i, j \leq 3$. Then $D\langle 1,-b_i\alpha\rangle \cap D\langle 1,-b_j\beta\rangle = \{1\}$.*

PROOF. If $x \in D(\rho_i') \cap D(\rho_j')$ then $\rho_i, \rho_j \in Q(x) \cap Q(a)$. Hence $Q(a) \subset Q(x)$ and $x = a$. That is,

$$D(\rho_i') \cap D(\rho_j') = \{-a\}.$$

Let $y \in D\langle 1,-b_i\alpha\rangle \cap D\langle 1,-b_j\beta\rangle$. Then $\rho_i = q(a, b_i) = q(ay, b_i\alpha)$ and $\rho_j = q(a, b_j\beta) = q(ay, b_j\beta)$. Thus $-ay \in D(\rho_i') \cap D(\rho_j') = \{-a\}$ and so $y = 1$. ∎

https://doi.org/10.4153/CJM-1997-023-1 Published online by Cambridge University Press

LEMMA 1.3. *If R is not of elementary type then $B_2 \subset D\langle 1, -a\rangle$ for all $a \in B_2$.*

PROOF. Let $x \in B_2 \setminus D\langle 1, -a\rangle$. We may assume that $x \in b_1 D\langle 1, -a\rangle$. By (1.2) $D\langle 1, -x\rangle \cap D\langle 1, -b_2\rangle = \{1\}$ and so by (0.0.2):

$$|D\langle 1, -x\rangle|\,|D\langle 1, -b_2\rangle|\,|D\langle 1, -xb_2\rangle| = g.$$

Since $x \in B_2$, $|D\langle 1, -b_2\rangle|\,|D\langle 1, -xb_2\rangle| = 4$. So b_2 and xb_2 are rigid and R is of elementary type by (0.1). ∎

THEOREM 1.4. *Let R be a Gorenstein Witt ring of dimension zero and socle degree three. Suppose $a \in G$ has index 4. If R is not of elementary type then there exists an $m \geq 3$, such that:*

(1)
$$B_2, \ldots, B_{m-1} \subset D\langle 1, -a\rangle,$$
$$B_m \not\subset D\langle 1, -a\rangle,$$

(2)
$$b_1 D\langle 1, -a\rangle \subset B_m$$
$$b_2 D\langle 1, -a\rangle \subset B_r$$
$$b_3 D\langle 1, -a\rangle \subset B_s,$$

for some $s \geq r \geq m$.

PROOF. Let $b = b_1, b_2$ or b_3. We will show that for all $\alpha \in D\langle 1, -a\rangle$ we have $|D\langle 1, -b\rangle| = |D\langle 1, -b\alpha\rangle|$. This proves the result since this omits only the statement that $m \geq 3$, which follows from (1.3). We may assume, without loss of generality, that $b = b_1$. We have by (1.2) and (0.0.1):

$$|D\langle 1, -b_1\alpha\rangle|\,|D\langle 1, -b_2\beta\rangle|\,|D\langle 1, -b_3\alpha\beta\rangle| = |G|$$

for all $\alpha, \beta \in D\langle 1, -a\rangle$. Replacing in turn α and β by 1; β alone by 1; β by α; and α by 1, β by α gives:

$$|D\langle 1, -b_1\rangle|\,|D\langle 1, -b_2\rangle|\,|D\langle 1, -b_3\rangle| = |G|$$
$$|D\langle 1, -b_1\alpha\rangle|\,|D\langle 1, -b_2\rangle|\,|D\langle 1, -b_3\alpha\rangle| = |G|$$
$$|D\langle 1, -b_1\alpha\rangle|\,|D\langle 1, -b_2\alpha\rangle|\,|D\langle 1, -b_3\rangle| = |G|$$
$$|D\langle 1, -b_1\rangle|\,|D\langle 1, -b_2\alpha\rangle|\,|D\langle 1, -b_3\alpha\rangle| = |G|.$$

Thus:

(i) $|D\langle 1, -b_1\rangle|\,|D\langle 1, -b_3\rangle| = |D\langle 1, -b_1\alpha\rangle|\,|D\langle 1, -b_3\alpha\rangle|$
(ii) $|D\langle 1, -b_1\rangle|\,|D\langle 1, -b_2\rangle| = |D\langle 1, -b_1\alpha\rangle|\,|D\langle 1, -b_2\alpha\rangle|$
(iii) $|D\langle 1, -b_2\rangle|\,|D\langle 1, -b_3\rangle| = |D\langle 1, -b_2\alpha\rangle|\,|D\langle 1, -b_3\alpha\rangle|$.

Suppose $|D\langle 1, -b_1\rangle| < |D\langle 1, -b_1\alpha\rangle|$. Then (i) gives $|D\langle 1, -b_2\rangle| > |D\langle 1, -b_2\alpha\rangle|$ and (ii) gives $|D\langle 1, -b_3\rangle| > |D\langle 1, -b_3\alpha\rangle|$. But this contradicts (iii). Thus we have that $|D\langle 1, -b_1\rangle| = |D\langle 1, -b_1\alpha\rangle|$. ∎

https://doi.org/10.4153/CJM-1997-023-1 Published online by Cambridge University Press

2. **Improvements when -1 is a sum of two squares.** The goal of this section is to refine (1.4). The additional assumption that -1 is a sum of two squares will turn out not to be restrictive in the field case. However, we continue to work here with abstract Witt rings.

LEMMA 2.1. $g \equiv |D\langle 1, -x\rangle| \pmod 3$ *iff* $x \in D(4)$.

PROOF. $(R/\operatorname{ann}\langle 1, -x\rangle, G/D\langle 1, -x\rangle)$ is Gorenstein of socle degree two [5, 2.6], hence of local type [5, 2.5]. Then $g \equiv |D\langle 1, -x\rangle| \pmod 3$ iff $|G/D\langle 1, -x\rangle| = 2^{2k}$ for some k iff -1 is a sum of two squares in $R/\operatorname{ann}\langle 1, -x\rangle$ iff $\langle\langle 1, 1, -x\rangle\rangle = 0$ iff $x \in D(4)$. ∎

From now on suppose that $-1 \in D(2)$. We thus have that $g \equiv |D\langle 1, -x\rangle| \pmod 3$ for all x in G. Set

$$A_k = \{x \in G^\bullet \mid i(x) = 2^{2k}\}$$
$$A_1^+ = A_1 \cup \{1\}.$$

Thus, in terms of the notation in the last section, $A_k = B_{2k}$.

PROPOSITION 2.2. *Suppose G has an element a of index 4. Then $g \equiv 2 \pmod 3$.*

PROOF. Let $a \in A_1$ and $g = 2^k$. We count using (0.0.3), with $A = G$ and $B = D\langle 1, -a\rangle$. For each $x \in A_i$, $x \neq 1$ we have by (1.1) that $|D\langle 1, -a\rangle \cap D\langle 1, -x\rangle| = \frac{1}{2}|D\langle 1, -x\rangle| = 2^{k-2i-1}$. Thus:

$$\text{(LHS)} \sum_{x\in G} |D\langle 1, -a\rangle \cap D\langle 1, -x\rangle| = 2 \cdot 2^{k-2} + (|A_1^+| - 2)2^{k-3} + \sum_{i=2}^{n} |A_i| 2^{k-2i-1}$$

where $n < \frac{m-2}{2}$. Using $G = A_1^+ \cup \bigcup A_i$:

$$\text{(LHS)} = 2^{k-2} + 2^{2k-2n-1} + (2^{k-3} - 2^{k-2n-1})|A_1^+| + \sum_{i=2}^{n-1}(2^{k-2i-1} - 2^{k-2n-1})|A_i|.$$

And thus we have:

$$\text{(LHS)} \equiv 2 + 2^{k-2} \pmod 3.$$

Next we have:

$$\text{(RHS)} \sum_{y\in D\langle 1,-a\rangle} |D\langle 1, -y\rangle| = 2^k + (|A_1^+ \cap D\langle 1, -a\rangle| - 1)2^{k-2} + \sum_{i=2}^{n} |A_i \cap D\langle 1, -a\rangle| 2^{k-2i}.$$

Using $D\langle 1, -a\rangle = (A_1^+ \cap D\langle 1, -a\rangle) \cup \bigcup (A_i \cap D\langle 1, -a\rangle)$:

$$\text{(RHS)} = 2^k - 2^{k-2} + 2^{2k-2n} + (2^{k-2} - 2^{k-2n})|A_1^+ \cap D\langle 1, -a\rangle| + \sum_{i=2}^{n-1}(2^{k-2i} - 2^{k-2n})|A_i \cap D\langle 1, -a\rangle|.$$

And so we have:

$$\text{(RHS)} \equiv 1 \pmod 3.$$

Since LHS = RHS, we have $2^{k-2} + 2 \equiv 1 \pmod 3$, $2^k \equiv -4 \pmod 3$ and so $g = 2^k \equiv 2 \pmod 3$. ∎

https://doi.org/10.4153/CJM-1997-023-1 Published online by Cambridge University Press

COROLLARY 2.3. *If G has an element of index 4 then $|D\langle 1,-x\rangle| \neq 4$ for all $x \in G$.*

PROOF. We have that $G = D(4)$ so that for any $x \in G$ (2.1) and (2.2) combine to give:

$$|D\langle 1,-x\rangle| \equiv g \equiv 2 \pmod 3.$$

Thus $|D\langle 1,-x\rangle| \neq 4$. ∎

We recall the setup and result of (1.4). We continue to assume that $-1 \in D(2)$, and that G has an element a of index 4. Fix $b_1, b_2, b_3 = b_1b_2$ such that $G = \{1, b_1, b_2, b_3\}D\langle 1,-a\rangle$. Set $\rho_i = q(a, b_i)$ for $i = 1, 2, 3$. Then $Q(a) = \{1, \rho_1, \rho_2, \rho_3\}$. Now using (1.3) set $g = 2^{2k+1}$. Further, we assume that:

$$|D\langle 1,-b_1\rangle| \geq |D\langle 1,-b_2\rangle| \geq |D\langle 1,-b_3\rangle|.$$

(1.4) said that there are $s \geq r \geq m \geq 2$ such that:

$$\begin{gathered} A_1, \ldots, A_{m-1} \subset D\langle 1,-a\rangle, \\ A_m \not\subset D\langle 1,-a\rangle, \\ b_1D\langle 1,-a\rangle \subset A_m, \\ b_2D\langle 1,-a\rangle \subset A_r, \\ b_3D\langle 1,-a\rangle \subset A_s. \end{gathered}$$

(Note that, as written, (1.4) in fact says $m \geq 3$, but that refers to the index of B_i while we are now working with $A_i = B_{2i}$. So in this notation we have only that $m \geq 2$).

THEOREM 2.4. *Suppose R is not of elementary type. Then there exists an odd $m \geq 3$ such that $A_1, \ldots, A_{m-1} \subset D\langle 1,-a\rangle$ and $A_m \not\subset D\langle 1,-a\rangle$. Further:*

(1) $2^{3m} < g \leq 2^{4m-1}$ *(or, equivalently,* $\frac{1}{2}(3m-1) < k \leq 2m-1$*).*

(2)

$$\begin{gathered} D\langle 1,-a\rangle \subset A_1^+ \cup A_2 \cup \cdots \cup A_m \\ b_1D\langle 1,-a\rangle \subset A_m \\ \{b_2, b_3\}D\langle 1,-a\rangle = A_r \quad \text{where } r = k - \frac{m-1}{2}. \end{gathered}$$

(3) If $t \notin [1, m] \cup \{r\}$ then $A_t = \emptyset$.

PROOF. Set $p = 2k - 2r + 1$ and $q = 2k - 2s + 1$. Then $|D\langle 1,-b_2\rangle| = g/2^{2r} = 2^p$ and $|D\langle 1,-b_3\rangle| = g/2^{2s} = 2^q$. Note that $p \geq q$. Also, from (2.1) and (2.2) we have that p and q are odd. (1.2) gives:

$$\begin{gathered} |D\langle 1,-b_1\rangle|\,|D\langle 1,-b_2\rangle|\,|D\langle 1,-b_3\rangle| = g \\ 2^{p+q} = 2^{2m} \\ p + q = 2m. \end{gathered}$$

https://doi.org/10.4153/CJM-1997-023-1 Published online by Cambridge University Press

Since $p \geq q$, this implies $m \geq q$. Further, for $1 \neq \beta \in D\langle 1, -a\rangle$ then (0.0.2) gives:

$$|D\langle 1,-\beta\rangle|\,|D\langle 1,-b_3\rangle|\,|D\langle 1,-b_3\beta\rangle| = g|D\langle 1,-\beta\rangle \cap D\langle 1,-b_3\rangle|^2 \geq g$$
$$|D\langle 1,-\beta\rangle| \geq 2^{2k+1-2q}$$
$$i(\beta) \leq 2q.$$

So $D\langle 1,-a\rangle \subset A_1^+ \cup A_2 \cup \cdots \cup A_q$. If $x \in A_t$ where $t \notin [1,q] \cup \{r,s,m\}$ then $x \notin D\langle 1,-a\rangle$, $x \notin b_1 D\langle 1,-a\rangle \subset A_m$, $x \notin b_2 D\langle 1,-a\rangle \subset A_r$ and $x \notin b_3 D\langle 1,-a\rangle \subset A_s$. Thus $A_t = \emptyset$.

STEP 1. $m = q$ and $r = s$.

We have $s \geq r \geq m \geq q$ and $2m = p + q$. Thus $m = q$ iff $q = p$ iff $r = s$. Suppose that $m > q$. Then:

$$s > r \geq m > q.$$

We claim that:

(i) $D\langle 1,-a\rangle = A_1^+ \cup \cdots \cup A_q$

(ii) $\{b_1, b_2\} D\langle 1,-a\rangle = A_m \cup A_r$

(iii) $b_3 D\langle 1,-a\rangle = A_s$.

Namely,

$$A_1^+ \cup \cdots \cup A_{m-1} \subset D\langle 1,-a\rangle \subset A_1^+ \cup \cdots \cup A_q$$

and $m > q$ implies:

$$A_1^+ \cup \cdots \cup A_q \subset A_1^+ \cup \cdots \cup A_{m-1}.$$

Thus (i) holds. If $x \in A_s$ then $x \notin D\langle 1,-a\rangle$ by (i), and $x \notin \{b_1, b_2\} D\langle 1,-a\rangle$ by (1.4). So $x \in b_3 D\langle 1,-a\rangle$. This proves (iii). And (ii) follows from (i) and (iii).

We use block design counting (0.0.3) with $A = D\langle 1,-a\rangle$ and $B = G \setminus D\langle 1,-a\rangle$. We break the sum on the left into sums over $b_i D\langle 1,-a\rangle$, for $i = 1,2,3$, each of size $g/4 = 2^{2k-1}$. Recall from (1.1) that for $z \neq 1, a$ we have $|D\langle 1,-a\rangle \cap D\langle 1,-z\rangle| = \frac{1}{2}|D\langle 1,-z\rangle|$. We thus get on the left:

$$\sum_{z \notin D\langle 1,-a\rangle} |D\langle 1,-z\rangle \cap D\langle 1,-a\rangle| = 2^{2k-1}(2^{2k-2m} + 2^{p-1} + 2^{q-1}).$$

The right hand side sums over $D\langle 1,-a\rangle$. Working with sums over $1, a, A_1 \setminus \{a\}, A_2, \ldots, A_q$ and again using (1.1)(3) gives:

$$\begin{aligned}\sum_{w \in D\langle 1,-a\rangle} |D\langle 1,-w\rangle \setminus D\langle 1,-a\rangle| &= 3 \cdot 2^{2k-1} + (|A_1| - 1)2^{2k-2} + \sum_{i=2}^{q} |A_i| 2^{2k-2i} \\ &= 5 \cdot 2^{2k-2} + \sum_{i=1}^{q} |A_i| 2^{2k-2i} \\ &= 5 \cdot 2^{2k-2} + 2^{4k-2q-1} - 2^{2k-2q} \\ &\quad + \sum_{i=1}^{q-1} |A_i|(2^{2k-2i} - 2^{2k-2q}),\end{aligned}$$

https://doi.org/10.4153/CJM-1997-023-1 Published online by Cambridge University Press

where the last equation comes from $\cup A_i = D\langle 1,-a\rangle \setminus \{1\}$, and so $\sum |A_i| = 2^{2k-1}-1$. Equating the two sides of (0.0.3) and dividing by 2^{2k-2q} gives:

$$\begin{aligned} &2^{2q-1}(2^{2k-2m}+2^{p-1}+2^{q-1}) \\ &\qquad = 5\cdot 2^{2q-2}+2^{2k-1}-1+\sum_{i=1}^{q-1}|A_i|(2^{2q-2i}-1). \end{aligned} \tag{2.4.1}$$

We have $2^{2q-1}(2^{2k-2m}+2^{p-1}+2^{q-1}) > 2^{2k-1}$. Divide by 2^{2q-1} to get:

$$2^{2k-2m}+2^{p-1}+2^{q-1}-1 > 2^{2k-2q}.$$

Since $p > q$:

$$\begin{aligned} 2^p &> 2^{p-1}+2^{q-1} \\ &> 2^{2k-2q}-2^{2k-2m} \\ &> 2^{2k-2q-1}. \end{aligned}$$

Thus $p > 2k-2q-1$ and $\frac{p-1}{2} > k-q-1$. Thus $r = k-(\frac{p-1}{2}) < k-(k-q-1) = q+1$. But $r > q$, a contradiction.

Hence $m = q$ and $r = s$.

We summarize. We have m is odd since $m = q$. By (1.3) $m \neq 1$ so that $m \geq 3$. Combining (1.4) and Step 1 gives:

$$\begin{aligned} D\langle 1,-a\rangle &\subset A_1^+ \cup \cdots \cup A_m \\ b_1 D\langle 1,-a\rangle &\subset A_m \\ \{b_2,b_3\}D\langle 1,-a\rangle &\subset A_r, \end{aligned}$$

where $r = k-(\frac{m-1}{2}) = s$. Also, (3) was verified in the last sentence before Step 1. To prove (2) we need only show $\{b_2,b_3\}D\langle 1,-a\rangle = A_r$. Nearly all of (1) remains to be shown. At this point, we can only show that $2^{3m} \leq g$. Namely, $p = 2k+1-2r$, by definition, and $r \geq m$ by (1.4). Thus $p \leq 2k+1-2m$. Step 1 gives that $p = m = q$, so $2k+1 \geq 3m$ (and $g = 2^{2k+1}$ by definition of k).

STEP 2. $2^{3m} < g$ and $\{b_2,b_3\}D\langle 1,-a\rangle = A_r$.

First note that if $g > 2^{3m}$ then $2k+1 > 3m$ and $r = k-(\frac{m-1}{2}) > \frac{3m-1}{2} - \frac{m-1}{2} = m$. If $x \in A_r$ then $x \notin \{1,b_1\}D\langle 1,-a\rangle \subset A_1^+ \cup \cdots \cup A_m$. So $x \in \{b_2,b_3\}D\langle 1,-a\rangle$. Thus to complete Step 3 we need only show $g \neq 2^{3m}$.

Suppose $g = 2^{3m}$. Then $r = m$. Also $A_m \cap D\langle 1,-a\rangle = \emptyset$. Otherwise, if $x \in A_m \cap D\langle 1,-a\rangle$ and $b \notin D\langle 1,-a\rangle$ then

$$|D\langle 1,-x\rangle|\,|D\langle 1,-b\rangle|\,|D\langle 1,-bx\rangle| = 2^{3m}|D\langle 1,-x\rangle \cap D\langle 1,-b\rangle|^2$$

hence $|D\langle 1,-x\rangle \cap D\langle 1,-b\rangle| = 1$. This shows that if $b \notin D\langle 1,-a\rangle$ then $-b \notin D\langle 1,-x\rangle$ (else $-b \in D\langle 1,-x\rangle \cap D\langle 1,-b\rangle$). Thus $D\langle 1,-x\rangle \cap -\{b_1,b_2,b_3\}D\langle 1,-a\rangle = \emptyset$. Now $a \in A_1 \subset D\langle 1,-a\rangle$, so $-1 \in D\langle 1,-a\rangle$. Thus $D\langle 1,-x\rangle \cap \{b_1,b_2,b_3\}D\langle 1,-a\rangle$ is empty and $D\langle 1,-x\rangle \subset D\langle 1,-a\rangle$, a contradiction.

https://doi.org/10.4153/CJM-1997-023-1 Published online by Cambridge University Press

Thus $D\langle 1,-a\rangle = A_1^+ \cup \cdots \cup A_{m-1}$ and $G \setminus D\langle 1,-a\rangle = A_m$. Apply (2.4.1) with $m = p = q$ and $2k+1 = 3m$:

$$2^{2m-1}(2^{m-1}+2^{m-1}+2^{m-1}) = 5\cdot 2^{2m-2} + 2^{3m-2} - 1 + \sum_{i=1}^{m-1} |A_i|(2^{2m-2i}-1)$$

(2.4.2)

$$2^{3m-1} - 5\cdot 2^{2m-2} + 1 = \sum_{i=1}^{m-1} |A_i|(2^{2m-2i}-1).$$

Now $|A_1| + \cdots + |A_{m-1}| = |D\langle 1,-a\rangle| - 1 = 2^{3m-2} - 1$. Solve for $|A_{m-1}|$ and plug into (2.4.2). Since the coefficient of $|A_{m-1}|$ is 3 we have:

$$2^{3m-1} - 5\cdot 2^{2m-2} + 1 = 3\cdot 2^{3m-2} - 3 + \sum_{i=1}^{m-2} |A_i|(2^{2m-2i}-4)$$

$$4 - 2^{3m-2} - 5\cdot 2^{2m-2} = \sum_{i=1}^{m-2} |A_i|(2^{2m-2i}-4).$$

But the sum on the right is non-negative while the left is negative since $m \geq 3$. This contradiction proves Step 2. Thus the proof of (2) is complete. To finish the proof of (1), and hence of the Theorem, we need:

STEP 3. $g \leq 2^{4m-1}$.

Fix $c \in \{b_2, b_3\}D\langle 1,-a\rangle$. Then $i(c) = r = k - (\frac{m-1}{2})$ so that $|D\langle 1,-c\rangle| = 2^m$. For any $x \in D\langle 1,-a\rangle$:

$$|D\langle 1,-x\rangle|\,|D\langle 1,-c\rangle|\,|D\langle 1,-cx\rangle| = 2^{2k+1}|D\langle 1,-x\rangle \cap D\langle 1,-c\rangle|^2$$

$$|D\langle 1,-x\rangle| = 2^{2k-2m+1}|D\langle 1,-x\rangle \cap D\langle 1,-c\rangle|^2$$

$$|D\langle 1,-x\rangle \cap D\langle 1,-c\rangle| = 2^{m-i} \quad \text{for } x \in A_i.$$

We will use block design counting (0.0.3) for $A = D\langle 1,-a\rangle$ and $B = D\langle 1,-c\rangle$. Summing over $\{1\}, A_1, \ldots, A_{m-1}$, and $A_m \cap D\langle 1,-a\rangle$ gives:

$$\text{(LHS)} \sum_{x\in D\langle 1,-a\rangle} |D\langle 1,-x\rangle \cap D\langle 1,-c\rangle| = 2^m + \sum_{i=1}^{m-1} |A_i|2^{m-i} + |A_m \cap D\langle 1,-a\rangle|.$$

Since $\sum_{i=1}^{m-1} |A_i| + |A_m \cap D\langle 1,-a\rangle| = |D\langle 1,-a\rangle| - 1 = 2^{2k-1} - 1$ we have:

$$\text{LHS} = 2^{2k-1} + 2^m - 1 + \sum_{i=1}^{m-1} (2^{m-i}-1)|A_i|.$$

Now if $y \in D\langle 1,-c\rangle$ and $y \neq 1$, then $|D\langle 1,-y\rangle \cap D\langle 1,-a\rangle| = \frac{1}{2}|D\langle 1,-y\rangle|$ by (1.1)(3). Thus:

$$\begin{aligned}\text{(RHS)} \sum_{y\in D\langle 1,-c\rangle} |D\langle 1,-y\rangle \cap D\langle 1,-a\rangle| = 2^{2k-1} &+ \sum_{i=1}^{m-1} |A_i \cap D\langle 1,-c\rangle|2^{2k-2i} \\ &+ |A_m \cap D\langle 1,-a\rangle \cap D\langle 1,-c\rangle|2^{2k-2m} \\ &+ |b_1 D\langle 1,-a\rangle \cap D\langle 1,-c\rangle|2^{2k-2m} \\ &+ |\{b_2,b_3\}D\langle 1,-a\rangle \cap D\langle 1,-c\rangle|2^{m-1}.\end{aligned}$$

https://doi.org/10.4153/CJM-1997-023-1 Published online by Cambridge University Press

Now $b_1D\langle 1,-a\rangle \cap D\langle 1,-c\rangle = \emptyset$ by (1.2) and $|\{b_2,b_3\}D\langle 1,-a\rangle \cap D\langle 1,-c\rangle| = \frac{1}{2}|D\langle 1,-c\rangle| = 2^{m-1}$. So:

$$\begin{aligned}\text{RHS} &= 2^{2k-1} + 2^{2m-2} + \sum_{i=1}^{m-1} |A_i \cap D\langle 1,-c\rangle| 2^{2k-2i} \\ &\quad + |A_m \cap D\langle 1,-a\rangle \cap D\langle 1,-c\rangle| 2^{2k-2m}.\end{aligned}$$

Since $\sum_{i=1}^{m-1} |A_i \cap D\langle 1,-c\rangle| + |A_m \cap D\langle 1,-a\rangle \cap D\langle 1,-c\rangle| = |D\langle 1,-a\rangle \cap D\langle 1,-c\rangle| - 1 = 2^{m-1} - 1$,

$$\text{RHS} = 2^{2k-1} + 2^{2m-2} + 2^{2k-m-1} - 2^{2k-2m} + 2^{2k-2m} \sum_{i=1}^{m-1} (2^{2m-2i} - 1)|A_i^+ \cap D\langle 1,-c\rangle|.$$

Equating LHS=RHS and cancelling 2^{2k-1} gives:

$$\begin{aligned}2^m - 1 + \sum_{i=1}^{m-1} (2^{m-i} - 1)|A_i| &= 2^{2k-m-1} + 2^{2m-2} - 2^{2k-2m} \\ &\quad + 2^{2k-2m} \sum_{i=1}^{m-1} (2^{2m-2i} - 1)|A_i \cap D\langle 1,-c\rangle|.\end{aligned} \tag{2.4.3}$$

Dividing (2.4.2) by 3 gives:

$$|A_{m-1}| = \frac{1}{3}(2^{3m-1} - 5 \cdot 2^{2m-2} + 1) - \sum_{i=1}^{m-2} \frac{1}{3}(2^{2m-2i} - 1)|A_i|.$$

Plugging into (2.4.3) gives:

$$\begin{aligned}\frac{1}{3}(2^{3m-1} - 5 \cdot 2^{2m-2} + 1) + 2^m - 1 + 2^{2k-2m} &= 2^{2m-2} + 2^{2k-m-1} \\ &\quad + \sum_{i=1}^{m-2} \Big(\frac{1}{3}(2^{2m-2i} - 1) - (2^{m-i} - 1)\Big)|A_i| \\ &\quad + 2^{2k-2m} \sum_{i=1}^{m-1} (2^{2m-2i} - 1)|A_i \cap D\langle 1,-c\rangle|.\end{aligned}$$

We thus have:

$$\begin{aligned}\frac{1}{3}(2^{3m-1} - 5 \cdot 2^{2m-2}) + 2^m + 2^{2k-2m} &> 2^{2m-2} + 2^{2k-m-1} \\ \frac{1}{3}(2^{3m-1} - 2^{2m}) - \frac{1}{3}2^{2m-2 + m-1} - 2^{2m-2} + 2^{m-1} &> 2^{2k-m-1} - 2^{2k-2m} \\ \frac{1}{3}2^{2m}(2^{m-1} - 1) - 2^{m-1}(2^{m-1} - 1) + 2^{m-1} - \frac{1}{3}2^{2m-2} &> 2^{2k-2m}(2^{m-1} - 1).\end{aligned}$$

Now $2^{m-1} - \frac{1}{3}2^{2m-2} < 0$, since $m \geq 3$ implies that $2^{2m-2} = (2^{m-1})^2 > 3 \cdot 2^{m-1}$. Thus:

$$\begin{aligned}(2^{m-1} - 1)\Big(\frac{1}{3}2^{2m} - 2^{m-1}\Big) &> (2^{m-1} - 1)2^{2k-2m} \\ \frac{1}{3}2^{2m} - 2^{m-1} &> 2^{2k-2m} \\ 2^{2m-2} &\geq 2^{2k-2m},\end{aligned}$$

https://doi.org/10.4153/CJM-1997-023-1 Published online by Cambridge University Press

and so $k \leq 2m-1$ and $g \leq 2^{4m-1}$. ∎

REMARK. By a detailed analysis of equations (2.4.2), (2.4.3) and similar equations one can show that if $-1 \in D(2)$, G has an element of index 4 and R is not of elementary type then $m \geq 9$ and $g \geq 2^{29}$. Unfortunately, we are unable to eliminate this case completely. To improve these results further requires the use of field techniques.

3. **Quadratic Extensions.** The key to better results for Witt rings of fields is the result [5, 2.6] that if WF is Gorenstein of socle degree k then $WF(\sqrt{w})$ is also Gorenstein of socle degree k.

We will be working with several fields at once, so for clarity we now write G_F for $F^\bullet/F^{\bullet 2}$, $D_F(q)$ for the values represented by a quadratic form q defined over F, and $i_F(x)$ for the index $[G_F : D_F\langle 1, -x\rangle]$. We begin with two results valid for any field F (of characteristic not two).

LEMMA 3.1. *Let ρ be a Pfister form over F and let $K = F(\sqrt{w})$. Let N denote the restriction of $N_{K/F}$ to $D_K(\rho)$. Then:*

$$1 \longrightarrow \frac{D_K(\rho) \cap G_F}{\{1, w\}F^{\bullet 2}} \xrightarrow{\ i\ } D_K(\rho) \xrightarrow{\ N\ } D_F(\rho) \cap D_F\langle 1, -w\rangle \longrightarrow 1$$

is exact.

PROOF. The map i induced by inclusion is clearly injective and its image is the kernel of N. That N maps into $D_F(\rho) \cap D_F\langle 1, -w\rangle$ follows from Scharlau's Norm Principle [9, VII 4.3]. Thus we need only show that N is surjective. Pick an $a \in D_F(\rho) \cap D_F\langle 1, -w\rangle$. Then there is a $z \in K$ such that $N(z) = a$, since the norm maps onto $D_F\langle 1, -w\rangle$ by [9, VII 3.4]. Then $s_*(\rho \otimes \langle 1, -z\rangle) = \rho \otimes s_*(\langle 1, -z\rangle) = \rho \otimes s_*(\langle -z\rangle)$, using Frobenius reciprocity [9, VII 1.3]. So for some $b \in F$, we have $s_*(\rho \otimes \langle 1, -z\rangle) = \langle b\rangle\rho \otimes \langle 1, -N(z)\rangle = \langle b\rangle\rho \otimes \langle 1, -a\rangle = 0$. Thus $\rho \otimes \langle 1, -z\rangle$ is defined over F. By [3, 2.11], $\rho \otimes \langle 1, -z\rangle = \rho \otimes \langle 1, -c\rangle \otimes K$, for some $c \in F$. Then $cz \in D_K(\rho)$ and (modulo squares) $N(cz) = N(z) = a$. ∎

COROLLARY 3.2. *Let $K = F(\sqrt{w})$ and let $x \in F^\bullet$.*

(1) $|D_K\langle 1, -x\rangle| = \frac{1}{2}|D_F\langle 1, -x\rangle|\,|D_F\langle 1, -xw\rangle|$.

(2) If x has finite index in G_F then:

$$i_K(x) = i_F(x)\frac{|D_F\langle 1, -xw\rangle|}{|D_F\langle 1, -w\rangle|}.$$

PROOF. We begin with the

CLAIM. $D_K\langle 1, -x\rangle \cap G_F = D_F\langle 1, -x\rangle D_F\langle 1, -xw\rangle$.

Namely, $z \in D_K\langle 1, -x\rangle \cap i(G_F/\{1, w\})$ if and only if $\langle\langle -x, -z\rangle\rangle \otimes F(\sqrt{w}) = 0$ if and only if $\langle 1, -w\rangle$ divides $\langle\langle -x, -z\rangle\rangle$ if and only if $-w \in D_F\langle -x, -z, xz\rangle$ if and only if $-w \in D_F\langle -x, z\alpha\rangle$ for some $\alpha \in D_F\langle 1, -x\rangle$ if and only if $z\alpha \in D_F\langle -x, w\rangle$ if and only if $zw \in D_F\langle 1, -x\rangle D_F\langle 1, -xw\rangle$ if and only if $z \in D_F\langle 1, -x\rangle D_F\langle 1, -xw\rangle$.

https://doi.org/10.4153/CJM-1997-023-1 Published online by Cambridge University Press

The Claim combined with (3.1) gives:

$$|D_K\langle 1,-x\rangle| = \frac{1}{2}|D_F\langle 1,-x\rangle \cap D_F\langle 1,-w\rangle|\,|D_F\langle 1,-x\rangle D_F\langle 1,-xw\rangle|$$
$$= \frac{1}{2}|D_F\langle 1,-x\rangle|\,|D_F\langle 1,-xw\rangle|.$$

Also $|G_K| = \frac{1}{2}|G_F|\,|D_F\langle 1,-w\rangle|$ by [9, VII 3.4]. So:

$$i_K(x) = \frac{\frac{1}{2}|G_F|\,|D_F\langle 1,-w\rangle|}{\frac{1}{2}|D_F\langle 1,-x\rangle|\,|D_F\langle 1,-xw\rangle|}$$
$$= i_F(x)\frac{|D_F\langle 1,-w\rangle|}{|D_F\langle 1,-xw\rangle|}.$$ ∎

PROPOSITION 3.3. *Suppose WF is Gorenstein of socle degree $k+2$ for some $k \geq 1$. Suppose further that $WF(\sqrt{w}) \approx L[E_k]$, for some Witt ring of local type L. Then $WF \approx L'[E_k]$ for some Witt ring of local type L'.*

PROOF. First suppose that $k \geq 2$. Let $t, s, ts \in G_K$, where $K = F(\sqrt{w})$, be birigid. Then $\langle\langle t,s\rangle\rangle \simeq \langle\langle x,\alpha\rangle\rangle$ for some $x \in F$, by [2, Lemma 2]. But then $x \in D\langle t,s,ts\rangle = \{t,s,ts\}$. Thus some $x \in F$ is birigid in K. That is, $|D_K\langle 1,-x\rangle| = 2$. Then (3.2) implies that $|D_F\langle 1,-x\rangle|\,|D_F\langle 1,-xw\rangle| = 4$. But then either x or xw is rigid. So, as char $WF \neq 0$, either x or xw is birigid by [1, Corollary to Theorem 1] (or [12, 4.15]). WF is then a group ring extension and a simple induction argument shows WF is in fact a group ring extension of a Witt ring of local type.

Now suppose that $k = 1$. We may assume $|D_K\langle 1,-x\rangle| \neq 2$ as in the previous paragraph. Since $WK = L[E_1]$, we must have $i_K(x) = 4$. Thus $|D_K\langle 1,-x\rangle| = |G_K|/4 = |G_F|\,|D_F\langle 1,-w\rangle|/8$ using [9, VII 3.4] again. Hence, multiplying (3.2)(1) by $|D_F\langle 1,-w\rangle|$:

$$\frac{1}{8}|G_F|\,|D_F\langle 1,-w\rangle|^2 = \frac{1}{2}|D_F\langle 1,-x\rangle|\,|D_F\langle 1,-xw\rangle|\,|D_F\langle 1,-w\rangle|.$$

Now apply (0.0.2):

$$|D_F\langle 1,-w\rangle|^2 = 4|D_F\langle 1,-x\rangle \cap D_F\langle 1,-w\rangle|^2$$
$$|D_F\langle 1,-w\rangle| = 2|D_F\langle 1,-x\rangle \cap D_F\langle 1,-w\rangle|.$$

We use block design counting (0.0.3) for $A = G_F, B = D_F\langle 1,-w\rangle$. Break the sum over G_F into sums over $\{1,w\}$ and $G_F \setminus \{1,w\}$. Set $d = |D_F\langle 1,-w\rangle|$.

$$\text{(LHS)}\ \sum_{x\in G}|D_F\langle 1,-x\rangle \cap D_F\langle 1,-w\rangle| = 2d + \frac{1}{2}(g-2)d = d\Big(\frac{g}{2}+1\Big),$$
$$\text{(RHS)}\ \sum_{z\in D_F\langle 1,-w\rangle}|D_F\langle 1,-z\rangle| = g + \sum_{z\in D_F^\bullet\langle 1,-w\rangle}|D_F\langle 1,-z\rangle|.$$

Thus:

$$\sum_{z\in D_F^\bullet\langle 1,-w\rangle}|D_F\langle 1,-z\rangle| = g\Big(\frac{d}{2}-1\Big)+d.$$

https://doi.org/10.4153/CJM-1997-023-1 Published online by Cambridge University Press

Thus there exists $1 \neq z \in D_F\langle 1, -w\rangle$ such that:

$$|D_F\langle 1, -z\rangle| \geq \frac{g\left(\frac{d}{2} - 1\right) + d}{d-1}.$$

We claim that $|D_F\langle 1, -z\rangle| \geq \frac{g}{2}$, which is impossible (as then $\langle 1, -z\rangle \in \operatorname{ann} IF$) and so finishes the proof. If not then:

$$\frac{g}{4}(d-1) \geq g\left(\frac{d}{2} - 1\right) + d$$
$$\frac{3g}{4} \geq \frac{gd}{4} + d$$
$$3g \geq gd + 4d > gd.$$

Hence $3 > d$ and $d = |D_F\langle 1, -w\rangle| = 2$, which implies that WF is of elementary type by (0.1). ∎

We will concentrate on the socle degree three case even though the reduction of the general case to this one is not known to be valid in the category of Witt rings of fields.

THEOREM 3.4. *Let $R = WF$ be a Gorenstein Witt ring of a field F. Suppose R has dimension zero, socle degree three and an element of index 4. Then R is of elementary type.*

PROOF. Suppose R is not of elementary type. Let $a \in F$ be an element of index 4. We first show that we may assume -1 is a square in F. If not, set $L = F(\sqrt{-1})$. By (1.1) $|D_F\langle 1, a\rangle| = |D_F\langle 1, 1\rangle|$, so by (3.2) $i_L(a) = 4$ also. WL is still Gorenstein of socle degree three by [5, 2.6]. If we show that WL is of elementary type then so is WF by (3.3). Thus we may replace F by L if necessary and assume that -1 is a square.

We review the notation and results of §2 for a field E satisfying our conditions (WE is Gorenstein of socle degree three, not of elementary type, with an element of index 4 and having -1 a square). Choose $b_1, b_2, b_3 = b_1b_2$ with $G_E = \{1, b_1, b_2, b_3\}D_E\langle 1, a\rangle$, and $|D_E\langle 1, b_1\rangle| \geq |D_E\langle 1, b_2\rangle| \geq |D_E\langle 1, b_3\rangle|$. Set $A_i(E) = \{x \in G_E \mid i_E(x) = 2^{2i}\}$. Write $G_E = 2^{2k(E)+1}$. Then there exists an odd $m(E) \geq 3$ such that:

(i) $A_1(E), \ldots, a_{m(E)-1}(E) \subset D_E\langle 1, a\rangle; A_{m(E)}(E) \not\subset D_E\langle 1, a\rangle$.
(ii) $b_1D_E\langle 1, a\rangle \subset A_{m(E)}(E)$.
(iii) $\{b_2, b_3\}D_E\langle 1, a\rangle = A_{r(E)}(E)$, with $r(E) = k(E) - \frac{m(E)-1}{2}$.
(iv) $\frac{1}{2}\left(3m(E) + 1\right) < k(E) \leq 2m(E) - 1$.

Set $K = F(\sqrt{b_2})$. Again (1.1) gives $|D_F\langle 1, b_2\rangle| = |D_F\langle 1, ab_2\rangle|$ so that (3.2) gives $i_K(a) = 4$. WK is not of elementary type by (3.3). So (2.4) applies to WK as well as to WF. Note:

$$|G_K| = \frac{1}{2}|G_F|\,|D_F\langle 1, b_2\rangle| = 2^{4k(F)-2r(F)+1}.$$

Thus $k(K) = 2k(F) - r(F)$.

CLAIM. $m(F) < m(K)$. Suppose instead that $m(F) \leq m(K)$. By (iv) $2^{2(K)+1} \leq 2^{4m(K)-1}$. So $\frac{1}{2}\left(k(K) + 1\right) \leq m(K) \leq m(F)$. Now $k(K) = 2k(F) - r(F)$ so that:

$$k(F) - \frac{1}{2}r(F) + \frac{1}{2} \leq m(F).$$

https://doi.org/10.4153/CJM-1997-023-1 Published online by Cambridge University Press

By definition $r(F) = k(F) - \frac{1}{2}\big(m(F) - 1\big)$ so

$$k(F) - \frac{1}{2}k(F) + \frac{1}{4}m(F) - \frac{1}{4} + \frac{1}{2} \leq m(F)$$
$$\frac{1}{2}k(F) + \frac{1}{4} \leq \frac{3}{4}m(F)$$
$$2k(F) + 1 \leq 3m(F).$$

But (iv) gives $3m(F) < 2k(F) + 1$. This proves the Claim.

Let $x \in b_1 D_F\langle 1, a\rangle$. Then $b_2, b_2x \in \{b_2, b_3\}D_F\langle 1, a\rangle = A_{r(F)}(F)$, and so we have that $|D_F\langle 1, b_2\rangle| = |D_F\langle 1, b_2x\rangle|$. By (3.2) $i_K(x) = i_F(x)$ and $i_F(x) = 2^{2m(F)}$ by (ii). Thus $x \in A_{m(F)}(K)$. By the Claim $m(F) < m(K)$, so $x \in D_K\langle 1, a\rangle$ by (i). Thus $\{1, b_1\}D_F\langle 1, a\rangle \subset D_K\langle 1, a\rangle$. Since b_2 is, by construction, a square in K, $b_2 D_F\langle 1, a\rangle \subset D_K\langle 1, a\rangle$ also. Thus $G_F \subset D_K\langle 1, a\rangle$. But then $\big\langle\langle -a, -x\rangle\big\rangle \otimes F(\sqrt{b_2}) = 0$, for all $x \in G_F$. Then $Q(a) \subset Q(b_2)$, contradicting [5, 2.16]. ∎

4. **The Field Case.** Throughout this section we will assume that $R = WF$ is a Gorenstein Witt ring of dimension zero and socle degree three. We begin with a generalization of (1.1).

LEMMA 4.1. *Suppose that among all R with -1 a square in F and R not of elementary type we know $A_1 = \cdots A_{p-1} = \emptyset$ for some $p \geq 1$. Then for such an R:*

(1) $A_p A_m \subset A_m$, for all $m \geq p$.

(2) If $a \in A_p$ and $x \neq 1, a$ then $|Q(a) \cap Q(x)| = 2^p$.

PROOF. We use induction on m. The case $m = p - 1$ is vacuous. Fix $a \in A_p$ and $x \in A_m$, where we assume $a \neq x$ if $m = p$. We note that $ax \in A_l$ for $l < m$. When $m = p$ this is true by the assumption that $A_1 = \cdots = A_{p-1} = \emptyset$. When $m > p$ this is by induction: if $ax \in A_l$ with $l < m$ then $x = a(ax) \in A_l$, not A_m. So suppose $ax \in A_k$ with $k \geq m$. We get by (0.0.2):

$$\frac{g}{2^{2p}}\frac{g}{2^{2m}}\frac{g}{2^{2k}} = g|D\langle 1, a\rangle \cap D\langle 1, x\rangle|^2 \tag{4.1.1}$$
$$\frac{g}{2^{p+m+k}} = |D\langle 1, a\rangle \cap D\langle 1, x\rangle|.$$

Now $|D\langle 1, ax\rangle| > |D\langle 1, a\rangle \cap D\langle 1, x\rangle|$, since otherwise $D\langle 1, ax\rangle = D\langle 1, a\rangle \cap D\langle 1, x\rangle \subset D\langle 1, a\rangle$, contradicting [5, 2.9]. So $g/2^{2k} > g/2^{p+k+m}$ and $p+m > k \geq m$. Write $k = m+i$. Set $K = F(\sqrt{ax})$. Then by (3.2)(2):

$$i_K(a) = i_F(a)\frac{|D_F\langle 1, ax\rangle|}{|D_F\langle 1, x\rangle|} = \frac{i_F(a)}{2^i}.$$

This implies that $a \in A_{p-i}(K)$. Now K has -1 a square and WK is not of elementary type by (3.3). Thus our hypothesis applies to WK and we have $A_{p-i}(K) = \emptyset$ for all $i > 0$. Hence $i = 0$ and $ax \in A_m$ as desired.

https://doi.org/10.4153/CJM-1997-023-1 Published online by Cambridge University Press

For statement (2), (4.1.1) gives $D\langle 1,a\rangle \cap D\langle 1,x\rangle| = g/2^{p+2m}$. So:

$$|Q(a)\cap Q(x)| = \frac{|D\langle 1,ax\rangle|}{|D\langle 1,a\rangle\cap D\langle 1,x\rangle|} = \frac{g/2^{2m}}{g/2^{p+2m}} = 2^p.$$

■

(4.1) is not known to hold in the category of abstract Witt rings. The following result is valid for abstract Witt rings.

LEMMA 4.2. *Let (R,G,B) be an abstract Witt ring that is Gorenstein of socle degree three. For any $a_1,\dots,a_s,b_1,\dots,b_t$ in G:*

$$\Big|\prod_{i=1}^{s} Q(a_i)\cap\prod_{i=1}^{t} Q(b_i)\Big| = |G|/\Big|\Big(\bigcap_{i=1}^{s} D\langle 1,-a_i\rangle\Big)\Big(\bigcap_{i=1}^{t} D\langle 1,-b_i\rangle\Big)\Big|.$$

PROOF. For any set S in G, let I_S be the ideal in R generated by $\{\langle 1,-a\rangle \mid a\in S\}$. To avoid confusion, in this proof we will denote the fundamental ideal of R by IR. Let J_S be the ideal in R generated by all $\varphi\in I^2$ such that $G(\varphi)$ contains S. Here $G(\varphi) = \{x\in G \mid \langle 1,-x\rangle\varphi = 0\}$. Further, let $C(S)$ denote the intersection of all $D\langle 1,-a\rangle$, for $a\in S$.

We begin with results that appeared at least implicitly in [5].

CLAIM 1.

(i) $\operatorname{ann} I_S = I_{C(S)} + J_S$.

(ii) If $S\subset G$ is a subgroup then $|J_S| = 2|G|/|S|$.

(iii) If $S\subset G$ is a subgroup then $\operatorname{ann} J_S = I_S + I^2R$.

(iv) If $S,T\subset G$ are subgroups then $J_S\cap J_T = J_{ST}$.

(v) $|I_S\cap I_T\cap I^2R| = 2|\prod_{a\in S} Q(a)\cap\prod_{b\in T} Q(b)|$.

(i) Let $\psi\in\operatorname{ann} I_S$ and write $\psi = \langle 1,-d\rangle + \varphi$, where $d = \operatorname{dis}\psi$ and $\varphi\in I^2R$. Then $\langle 1,-d\rangle$ and φ are in $\operatorname{ann} I_S$. Thus $\langle 1,-d\rangle\langle 1,-a\rangle = 0$ for all $a\in S$ and so $d\in C(S)$. Also $S\subset G(\varphi)$ so $\varphi\in J_S$. Thus $\psi\in I_{C(S)} + J_S$. The reverse inclusion is easy to check.

(ii) Let $\mathcal{A} = \{H\subset G \mid H \text{ a subgroup of index at most } 2, S\subset H\}$. Then $|\mathcal{A}| = |G|/|S|$. Map:

$$\alpha\colon J_S/I^3R\to\mathcal{A} \quad \text{by}$$
$$\varphi + I^3R\mapsto G(\varphi).$$

That $G(\varphi)\in\mathcal{A}$ for $\varphi\in J_S$ is part of [5, 2.11]. Also, $I^3R = \{0,\sigma\}$ with σ universal, so that $G(\varphi) = G(\varphi+\sigma)$ and α is well-defined. α is surjective by the second part of [5, 2.11]. If $G(\varphi) = G(\psi)$, for some forms $\varphi,\psi\in I^2R$, then $\operatorname{ann}(\varphi) = I_{G(\varphi)} + I^2R = \operatorname{ann}(\psi)$.

https://doi.org/10.4153/CJM-1997-023-1 Published online by Cambridge University Press

Taking annihilators of both sides and applying (0.0.1) yields $(\varphi) = (\psi)$. Thus $\varphi = x\psi = \psi + \langle x, -1\rangle\psi$, so that $\varphi + I^3R = \psi + I^3R$. Hence α is also injective. We obtain:

$$|J_S/I^3R| = |G|/|S|$$
$$|J_S| = 2|G|/|S|.$$

(iii) $J_S \subset I^2R$ and $I^4R = 0$ so $I^2R \subset \operatorname{ann} J_S$. Let $\langle 1, -a\rangle \in \operatorname{ann} J_S$. Then $\langle 1, -a\rangle\varphi = 0$ for all $\varphi \in J_S$, hence $a \in G(\varphi)$ for all $\varphi \in I^2R$ having $S \subset G(\varphi)$. From the proof of (ii) we have that $a \in H$ for all subgroups $H \subset G$ of index 2 containing S. And S equals the intersection of all subgroups of index 2 containing it (think of G as a vector space over $\mathbb{Z}_2$). Thus $a \in S$ and $\langle 1, -a\rangle \in I_S$. The inclusion $I_S \subset \operatorname{ann} J_S$ is clear.

(iv) If $\varphi \in J_S \cap J_T$ then $S \cup T \subset G(\varphi)$. Since $G(\varphi)$ is a group, $ST \subset G(\varphi)$. And if $\varphi \in J_{ST}$ then $S, T \subset G(\varphi)$ so that $\varphi \in J_S \cap J_T$.

(v) We begin with a small technical point. Since I^3R consists of 0 and a 3-fold Pfister form [5, 2.4], the Arason-Pfister property AP(3) holds trivially. Thus there is an embedding $i\colon B \longrightarrow I^2R/I^3R$, that sends $q(a, b)$ to $\langle\langle -a, -b\rangle\rangle + I^3R$, by [11, 3.16, 3.23]. We may replace B with the group it generates (inside the universal Steinberg symbol). Note that B is a multiplicative group while I^2/I^3R is an additive group. We have in particular that:

$$i\big(Q(a)\big) = \langle 1, -a\rangle IR/I^3R.$$
$$i\Big(\prod_{a\in S} Q(a)\Big) = \sum_{a\in S}\langle 1, -a\rangle IR/I^3R$$
$$= I_S \cdot IR/I^3R$$
$$= I_S \cap I^2R/I^3R,$$

where the last equality is by [4, 2.15]. (The proof in [4] uses the Arason-Pfister theorem which we have shown is valid for our abstract Witt ring. The result can also easily be proven without the Arason-Pfister theorem for any abstract Witt ring.) We thus get:

$$i\Big(\prod_{a\in S} Q(a) \cap \prod_{b\in T} Q(b)\Big) = I_S \cap I_T \cap I^2R/I^3R$$
$$\Big|\prod_{a\in S} Q(a) \cap \prod_{b\in T} Q(b)\Big| = 2|I_S \cap I_T \cap I^2R|.$$

This completes the proof of Claim 1.

CLAIM 2. $I_S \cap I^2R = J_{C(S)}$.

Let gS denote the group generated by S. Then $J_S = J_{gS}$ since $S \subset G(\varphi)$ iff $gS \subset G(\varphi)$. If $\varphi = \sum \psi_i\langle 1, -a_i\rangle$, where each $a_i \in S$, then for all $c \in C(S)$ we have $\langle 1, -c\rangle\varphi = 0$. Thus $I_S \cap I^2 \subset J_{C(S)}$. Also, $\operatorname{ann} I_S = I_{C(S)} + J_S = I_{C(S)} + J_{gS}$, by (i). So taking annihilators of both sides and applying (0.0.1) gives $I_S = \operatorname{ann}\big(I_{C(S)} + J_{gS}\big) = \big(I_{C\left(C(S)\right)} + J_{C(S)}\big) \cap (I_{gS} + I^2R)$, by (i) and (iii). Clearly $J_{C(S)} \subset I_{C\left(C(S)\right)} + J_{C(S)}$ and $J_{C(S)} \subset I_{gS} + I^2R$, so we have that $J_{C(S)} \subset I_S$. Hence $J_{C(S)} \subset I_S \cap I^2R$, as desired. This proves Claim 2.

https://doi.org/10.4153/CJM-1997-023-1 Published online by Cambridge University Press

Let $S = \{a_1, \ldots, a_s\}$ and $T = \{b_1, \ldots, b_t\}$. Then:

$$\begin{aligned}\left|\prod_{i=1}^{s} Q(a_i) \cap \prod_{i=1}^{t} Q(b_i)\right| &= \frac{1}{2}|I_S \cap I_T \cap I^2| \quad \text{by (v)}\\ &= |(I_S \cap I^2R) \cap (I_T \cap I^2R)|\\ &= \frac{1}{2}|J_{C(S)} \cap J_{C(T)}| \quad \text{by Claim 2}\\ &= \frac{1}{2}|J_{C(S)C(T)}| \quad \text{by (iv)}\\ &= \frac{|G|}{|C(S)C(T)|}, \quad \text{by (ii).}\end{aligned}$$

which completes the proof. ∎

We remark that (4.2) appears to be the key combinatorial result for Gorenstein Witt rings of socle degree three. When $s = t = 1$ (4.2) is equivalent to (0.0.2).

THEOREM 4.3. *If WF is Gorenstein of dimension zero and socle degree three then WF is of elementary type.*

PROOF. Suppose not. We may assume -1 is a square in F by passing to $F(\sqrt{-1})$, if necessary and applying (3.3) to see that the extended Witt ring is still not of elementary type. Let p be the minimal index with $A_p \neq \emptyset$ among all Gorenstein WF of socle degree three, -1 a square and not of elementary type. We note that $p \geq 2$ by (3.4). Among all Gorenstein WF of socle degree three, -1 a square, not of elementary type and $A_p \neq \emptyset$, let k be the minimal index such that $A_k \not\subset D\langle 1, a\rangle$, for some $a \in A_p$.

Let F be a field that achieves both minima, that is, with an element $a \in A_p$ and an element $b_1 \in A_k \setminus D\langle 1, a\rangle$.

STEP 1. Let $b_1, \ldots, b_{p+1}$ be independent modulo $D\langle 1, a\rangle$. Then $\bigcap_{i=1}^{p+1} D\langle 1, b_i\rangle = \{1\}$.

Set $\rho_i = \langle\langle a, b_i\rangle\rangle$. Then the ρ_i are independent modulo I^3F, since if $\sum\langle\langle a, b_{i_j}\rangle\rangle \in I^3F$ then $\langle\langle a, \prod b_{i_j}\rangle\rangle \in I^3F$. But then $\prod b_{i_j} \in D\langle 1, a\rangle$, contradicting the independence of the b_i modulo $D\langle 1, a\rangle$. In particular, the ρ_i generate a subgroup of order 2^{p+1} in $Q(a)$.

Suppose that $z \in \cap D\langle 1, b_i\rangle$. Then $z \in a \cdot \cap D(\rho_i\prime)$. Thus $\{\rho_i\} \subset Q(a) \cap Q(az)$ and so $|Q(a) \cap Q(az)| \geq 2^{p+1}$. By (4.1)(2) $az = a$ and $z = 1$. This proves Step 1.

STEP 2. For all $x, y, xy \notin \{1, b_1\}D\langle 1, a\rangle$, we have $|D\langle 1, x\rangle \cap D\langle 1, y\rangle| \leq 2^{4k}$.

Set $b_2 = x$ and $b_3 = y$. Write $G = gp(b_1, b_2, \ldots, b_{2p})D\langle 1, a\rangle$, where the notation $gp(S)$ means the group generated by S. We first Claim:

$$|D\langle 1, b_1\rangle \cap D\langle 1, b_2\rangle \cap D\langle 1, b_3\rangle| \leq 2^{2k}. \tag{4.3.1}$$

This is clear if $p = 2$ since then the left-hand side of (4.3.1) is 1, by Step 1. Suppose $p > 2$. Then:

$$\begin{aligned}\frac{g}{2^{2k}} &= |Q(b_1)|\\ &\leq |Q(b_1)Q(b_2)Q(b_3) \cap Q(b_1)Q(b_4) \cdots Q(b_{p+1})|\\ &= \frac{g}{|D\langle 1, b_1\rangle \cap D\langle 1, b_2\rangle \cap D\langle 1, b_3\rangle|\,|D\langle 1, b_1\rangle \cap D\langle 1, b_4\rangle \cap \cdots|},\end{aligned}$$

https://doi.org/10.4153/CJM-1997-023-1 Published online by Cambridge University Press

by (4.2) and Step 1. This proves (4.3.1).

Now using (4.2) again, we have:

$$\begin{aligned} 1 &\leq |Q(b_2)Q(b_3) \cap Q(b_1)| \\ &\leq \frac{g|D\langle 1, b_1\rangle \cap D\langle 1, b_2\rangle \cap D\langle 1, b_3\rangle|}{|D\langle 1, b_2\rangle \cap D\langle 1, b_3\rangle|\,|D\langle 1, b_1\rangle|} \\ 1 &\leq \frac{2^{2k}2^{2k}}{|D\langle 1, b_2\rangle \cap D\langle 1, b_3\rangle|}, \end{aligned}$$

by (4.3.1). This gives Step 2.

STEP 3. If $A_m \not\subset \{1, b_1\}D\langle 1, a\rangle$ then $2^{3m-8k} \leq g \leq 2^{3m+12k}$.

Suppose $b_2 \in A_m \setminus \{1, b_1\}D\langle 1, a\rangle$. Choose $b_3, b_4, \ldots, b_{2p}$, (recalling that $D\langle 1, a\rangle$ has index $2p$ in G), such that $G = gp(b_1, b_2, b_3, \ldots, b_{2p})D\langle 1, a\rangle$. Recall that $p \geq 2$. Now by (0.0.2):

$$|D\langle 1, b_2\rangle|\,|D\langle 1, b_3\rangle|\,|D\langle 1, b_2b_3\rangle| = g|D\langle 1, b_2\rangle \cap D\langle 1, b_3\rangle|^2.$$

Hence by Step 2:

$$\begin{aligned} g \leq |D\langle 1, b_2\rangle|\,|D\langle 1, b_3\rangle|\,|D\langle 1, b_2b_3\rangle| &\leq g \cdot 2^{8k} \\ 2^{2m} \leq |D\langle 1, b_3\rangle|\,|D\langle 1, b_2b_3\rangle| &\leq 2^{2m+8k}. \end{aligned} \tag{4.3.2}$$

Similarly:

$$2^{2m} \leq |D\langle 1, b_4\rangle|\,|D\langle 1, b_2b_4\rangle| \leq 2^{2m+8k} \tag{4.3.3}$$

$$2^{2m} \leq |D\langle 1, b_3b_4\rangle|\,|D\langle 1, b_2b_3b_4\rangle| \leq 2^{2m+8k}. \tag{4.3.4}$$

Without loss of generality we may suppose $|D\langle 1, b_3\rangle| \leq |D\langle 1, b_2b_3\rangle|$. So $|D\langle 1, b_3\rangle| \leq 2^{m+4k}$, by (4.3.2). Set $\alpha = |D\langle 1, b_4\rangle|\,|D\langle 1, b_3b_4\rangle|$ and $\beta = |D\langle 1, b_2b_4\rangle|\,|D\langle 1, b_2b_3b_4\rangle|$. Now:

$$g \leq \min\{|D\langle 1, b_3\rangle|\alpha,\ |D\langle 1, b_3\rangle|\beta\} \leq 2^{m+4k}\min\{\alpha, \beta\}, \tag{4.3.5}$$

where the first inequality is from (0.0.2) and the second is from our bound on $|D\langle 1, b_3\rangle|$. The product of (4.3.3) and (4.3.4) gives $\alpha\beta \leq 2^{4m+16k}$. Thus the minimum of α, β is at most 2^{2m+8k}. Then (4.3.5) gives $g \leq 2^{3m+12k}$.

Next, since $|D\langle 1, b_2b_3\rangle| \geq |D\langle 1, b_3\rangle|$, (4.3.2) implies $|D\langle 1, b_2b_3\rangle| \geq 2^m$. We repeat the previous trick and set $\gamma = |D\langle 1, b_4\rangle|\,|D\langle 1, b_2b_3b_4\rangle|$ and $\delta = |D\langle 1, b_2b_4\rangle|\,|D\langle 1, b_3b_4\rangle|$. Then:

$$\begin{aligned} &\max\{|D\langle 1, b_2b_3\rangle|\gamma, |D\langle 1, b_2b_3\rangle|\delta\} \\ &\qquad = \max\{g|D\langle 1, b_2b_3\rangle \cap D\langle 1, b_4\rangle|^2,\ g|D\langle 1, b_2b_3\rangle \cap D\langle 1, b_2b_4\rangle|^2\} \\ &\qquad \leq g \cdot 2^{8k}. \end{aligned}$$

https://doi.org/10.4153/CJM-1997-023-1 Published online by Cambridge University Press

The equality here is (0.0.2) while the inequality is Step 2. So $2^m \cdot \max\{\gamma, \delta\} \leq g \cdot 2^{8k}$. The product of (4.3.3) and (4.3.4) gives $\gamma\delta \geq 2^{4m}$. We obtain $\max\{\gamma, \delta\} \geq 2^{2m}$. Thus $g \geq 2^{3m-8k}$. This gives Step 3.

Write $g = 2^{9n+i}$, for some $0 \leq i \leq 8$.

STEP 4. If $x \notin \{1, b_1\}D\langle 1, a\rangle$ then:

$$2^{3n+i-6k-6} \leq |D\langle 1, x\rangle| \leq 2^{3n+i+8k}.$$

Say $x \in A_m$. Then by Step 3:

$$3m - 8k \leq 9n + i \leq 3m + 12k.$$

The first inequality gives:

$$m \leq 3n + \frac{8}{3}k + \frac{i}{3} \leq 3n + 3k + 3,$$

while the second inequality gives:

$$m \geq 3n - 4k + \frac{i}{3} \geq 3n - 4k.$$

Step 4 then follows from $|D\langle 1, x\rangle| = 2^{9n+i-2m}$.

STEP 5. $g \leq 2^{108k+125}$.

Pick $w \notin D(\rho_1)$ where $\rho_1 = \langle\langle a, b_1\rangle\rangle$. Since $b_1 w \notin D(\rho_1)$ also, we may assume that $|D\langle 1, b_1 w\rangle| \geq |D\langle 1, w\rangle|$. Set $K = F(\sqrt{w})$. We check that K satisfies our hypotheses. WK is not of elementary type since WF is not, using (3.3). -1 is a square in K since it is in F. By (4.1):

$$i_K(a) = i_F(a)|D_F\langle 1, w\rangle| / |D_F\langle 1, aw\rangle|,$$

and so $i_K(a) = i_F(a)$ by (4.2)(1). Thus $a \in A_p(K)$ and $A_p(K) \neq \emptyset$. Further:

$$i_K(b_1) = i_F(b_1)|D_F\langle 1, w\rangle| / |D_F\langle 1, b_1 w\rangle| \leq i_F(b_1) = 2k.$$

If $i_K(b_1) < 2k$ then by our minimality assumptions, $b_1 \in D_K\langle 1, a\rangle$. But then $\rho_1 \otimes F(\sqrt{w}) = 0$ and $w \in D(\rho_1')$, which is impossible as $w \notin D(\rho_1)$. Thus $i_K(b_1) = 2k$, that is, $b_1 \in A_k(K) \setminus D_K\langle 1, a\rangle$. Thus all of Steps 1–4 apply to K.

Now:

$$\begin{aligned} |D_F\langle 1, a\rangle D_F\langle 1, aw\rangle| &= |D_F\langle 1, a\rangle| \frac{|D_F\langle 1, aw\rangle|}{|D_F\langle 1, a\rangle \cap D_F\langle 1, w\rangle|} \\ &= |D_F\langle 1, a\rangle| \, |Q(a) \cap Q(w)| \\ &= 2^p |D_F\langle 1, a\rangle|. \end{aligned}$$

Thus $|D_F\langle 1, a\rangle D_F\langle 1, aw\rangle| = g/2^p$. Choose then $x \in G_F \setminus \{1, b_1\}D_F\langle 1, a\rangle D_F\langle 1, aw\rangle$, which is possible since $p \geq 2$. Then $x \notin \{1, b_1\}D_K\langle 1, a\rangle$, using the Claim of (3.2). So we can apply Step 4 to K and x.

https://doi.org/10.4153/CJM-1997-023-1 Published online by Cambridge University Press

First, however, apply Step 4 to F and w, noting that $w \notin \{1, b_1\}D\langle 1, a\rangle \subset D(\rho_1)$:

$$|G_K| = \frac{1}{2}|G_F|\,|D_F\langle 1, w\rangle| \leq \frac{1}{2}2^{9n+i}2^{3n+i+8k} \leq 2^{12n+2i+8k}.$$

Write $12n + 2i + 8k = 9N + j$, for some $0 \leq j \leq 8$. Now apply Step 4 to K and x:

$$|D_K\langle 1, x\rangle| \leq 2^{3N+j+8k}.$$

Now $3N + j + 8k = 4n + \frac{2}{3}i + \frac{8}{3}k - \frac{j}{3} + j + 8k \leq 4n + 11k + 12$, since $i, j \leq 8$. Thus $|D_K\langle 1, x\rangle| \leq 2^{4n+11k+12}$.

However, $x \notin \{1, b_1\}D_F\langle 1, a\rangle$, by constuction. Also $xw \notin \{1, b_1\}D_F\langle 1, a\rangle$, since otherwise $xw \in \{1, b_1\}D_F\langle 1, a\rangle D_F\langle 1, aw\rangle$ and $x \in \{1, b_1\}D_F\langle 1, a\rangle D_F\langle 1, aw\rangle$, contrary to our original choice of x. So using the lower bound of Step 4 applied to F, x, xw gives:

$$\begin{aligned}|D_K\langle 1, x\rangle| &= \frac{1}{2}|D_F\langle 1, x\rangle|\,|D_F\langle 1, xw\rangle| \\ &\geq \frac{1}{2}2^{6n+2i-12k-12} \\ &= 2^{6n+2i-12k-13} \\ &\geq 2^{6n-12k-13}.\end{aligned}$$

Hence:

$$\begin{aligned}6n - 12k - 13 &\leq 4n + 11k + 12 \\ 2n &\leq 23k + 25 \\ n &\leq 12k + 13.\end{aligned}$$

Thus:

$$g = 2^{9n+i} \leq 2^{9(12k+13)+8} = 2^{108k+125}.$$

STEP 6. Completion of the proof.

Out of all G such that (a) R is not of elementary type, (b) $-1 = 1$, (c) there exists an element a in A_p, and (d) $A_k \not\subset D\langle 1, a\rangle$, pick the maximal one. This is possible by Step 5. Again, if we pick $w \notin D(\rho_1)$, where $b_1 \in A_k \setminus D\langle 1, a\rangle$ and $\rho_1 = \langle\langle a, b_1\rangle\rangle$, then WK satisfies (a)–(d) as was shown in the first part of the proof of Step 5. By maximality, $|G_K| = |G_F|$. But then $|D_F\langle 1, w\rangle| = 2$, so w is rigid and WF is of elementary type, by (0.1). This contradiction to property (a) proves the result. ∎

Szymiczek [13] called a field F a *n-Hilbert field* if $|F^\bullet/D\sigma| \leq 2$ for all n-fold Pfister forms σ, with equality holding for at least one σ. We can classify certain 2-Hilbert fields.

COROLLARY 4.4. *Let F be a non-formally real linked 2-Hilbert field with trivial radical and $|F^\bullet/D\sigma| = 2$ for all anisotropic 2-fold Pfister forms. Then F is Witt equivalent (i.e. has a Witt ring isomorphic) to $K\big((t)\big)$, where K is a local field.*

PROOF. We check that WF is Gorenstein of socle degree three. $I^3F = \{0, \tau\}$, for some anisotropic 3-fold Pfister form τ by [13, 2.3]. And τ is universal by Kneser's Lemma [9, XI 4.5]. In particular, $I^4F = 0$ and WF has socle degree three.

https://doi.org/10.4153/CJM-1997-023-1 Published online by Cambridge University Press

To show WF is Gorenstein we check Bass' criterion. Let $\varphi \in \operatorname{ann} IF$. We can write:

$$\varphi = \langle 1, -x \rangle \perp \sigma \perp \psi,$$

where σ is a 2-fold Pfister form and $\psi \in I^3F$, since F is linked. Then $\langle 1, -x \rangle$ and σ are in $\operatorname{ann} IF$. But $\langle 1, -x \rangle \in \operatorname{ann} IF$ implies that $\langle\langle -x, -y \rangle\rangle = 0$ for all $y \in F^\bullet$ and so $x \in \operatorname{rad} F$. By assumption, $\operatorname{rad} F = F^{\bullet 2}$ so that $\langle 1, -x \rangle = 0$ in WF. Also $\sigma \in \operatorname{ann} IF$ implies $F^\bullet = D\sigma$, which, by our assumption, forces $\sigma = 0$ in WF. Thus $\varphi = \psi \in I^3F$ and so $\operatorname{ann} IF = I^3F$. From the first paragraph then $\dim(\operatorname{ann} IF) = 1$ and WF is Gorenstein.

Apply (4.3). $WF = L[E_1]$, for some Witt ring of local type. L is the Witt ring of some local field K by [11, p. 97]. Thus $WF \approx WK\big((t)\big)$, by [11, p. 114]. ∎

REFERENCES

1. C. Cordes and J. Ramsey, *Quadratic forms over fields with $u = q/2 < +\infty$*, Fund. Math. **99**(1978), 1–10.
2. R. Elman and T.-Y. Lam, *Classification theorems for quadratic forms over fields*, Math. Helv. **49**(1974), 373–381.
3. R. Elman, T.-Y. Lam and A. Wadsworth, *Amenable fields and Pfister extensions*, Conference on quadratic forms 1976, Queen's papers in pure and applied math. No. 46, 1977, 445–491.
4. ———, *Pfister ideals in Witt rings*, Math. Ann. **245**(1979), 219–245.
5. R. Fitzgerald, *Gorenstein Witt rings*, Canad. J. Math. **40**(1988), 1186–1202.
6. ———, *Local artinian rings and the Fröberg relation*, Rocky Mtn. J. Math., to appear.
7. ———, *Bass series of small Witt rings*, preprint.
8. R. Fitzgerald and J. Yucas, *Combinatorial techniques and abstract Witt rings I*, J. Algebra **114**(1988), 40–52.
9. T.-Y. Lam, *The Algebraic Theory of Quadratic Forms*, Benjamin, Reading, Mass., 1973.
10. M. Kula, *Finitely Generated Witt Rings*, Univwersytet Ślaski, Katowice, 1991.
11. M. Marshall, *Abstract Witt rings*, Queen's papers in pure and applied math. No. 57, Queen's University, Kingston, Ontario, 1980.
12. L. Szczepanik, *Quadratic forms schemes with non-trivial radical*. Colloq. Math. **49**(1985), 143–160.
13. K. Szymiczek, *Generalized Hilbert fields*, J. Reine Angew. Math. **329**(1981), 58–65.

Southern Illinois University
Carbondale, IL
USA 62901-4408
e-mail: rfitzg@math.siu.edu