PACIFIC JOURNAL OF MATHEMATICS
Vol. 128, No. 2, 1987

DERIVATION ALGEBRAS OF FINITELY GENERATED WITT RINGS

ROBERT W. FITZGERALD

We consider derivations of an abstract Witt ring R. Denote the collection of derivations by $\mathrm{Der}(R)$; it is a Lie algebra under the usual bracket operation. The structure of $\mathrm{Der}(R)$ is closely related to the structure of the torsion part of R, which is the part least understood. After a lengthy computation of $\mathrm{Der}(R)$ for finitely generated Witt rings of elementary type, we classify the Witt rings in the following cases: (i) $\mathrm{Der}(R) = 0$, (ii) $\mathrm{Der}(R)$ is a simple algebra, and (iii) the fundamental ideal of R is not differentiable.

All Witt rings considered here will be finitely generated abstract Witt rings (in the sense of Marshall [**5**]). The most important examples are the Witt rings WF of non-degenerate quadratic forms over a field F with $\mathrm{char}\, F \neq 2$ and $\dot{F}/\dot{F}^2$ a finite group. The basic problem is to classify these Witt rings. To date this has been done only for Witt rings that are small in some sense (e.g., the number of generators is ≤ 32) and for torsion-free Witt rings. Indeed the part of a Witt ring R that is least understood is its torsion ideal R_t.

We study here the derivations of a Witt ring R, namely, additive maps $D\colon R \to R$ such that $D(rs) = sD(r) + rD(s)$ for all $r, s \in R$. We denote by $\mathrm{Der}(R)$ the collection of all derivations of R. $\mathrm{Der}(R)$ is a Lie algebra, called the derivation algebra of R, under the usual bracket operation: if $D, D' \in \mathrm{Der}(R)$ then $[D, D'] = D \circ D' - D' \circ D \in \mathrm{Der}(R)$.

The usefulness of derivations appears to stem from the (easily checked) fact that the image of any derivation of R lies in R_t. Thus the structure of the derivation algebra $\mathrm{Der}(R)$ sheds some light on the structure of R_t. We have obtained only some partial results however. We do classify the Witt rings in the following cases: (i) $\mathrm{Der}(R) = 0$, (ii) $\mathrm{Der}(R)$ is a simple algebra, (iii) the fundamental ideal I_R is not differentiable (i.e., $D(I_R) \not\subset I_R$ for some $D \in \mathrm{Der}(R)$), and (iv) every derivation on R is integrable (but here we require some restrictions on R).

All of our classification results are special cases of a general classification of finitely generated Witt rings proposed by Marshall. We describe this. Start with the *fundamental Witt rings* $\mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/4\mathbf{Z}$, $\mathbf{Z}$ and certain

Witt rings of local type, namely, $L_{2n,0}$, $L_{2n,1}$ and L_{2n-1}, $(n \geq 2)$. The last three families arise as the Witt rings of suitable local fields (see [5] for details). We can form new Witt rings from old in two ways. If R is a Witt ring and Δ is a (finite) group of exponent 2 then the group ring $R[\Delta]$ is again a Witt ring. If R_1, R_2 are Witt rings then the *Witt product* (or fibre product over $\mathbf{Z}/2\mathbf{Z}$) is $R_1 \times_w R_2 = \{(r_1, r_2) \mid r_1 \in R_1,\ r_2 \in R_2 \text{ and } \dim r_1 \equiv \dim r_2 \pmod 2\}$, which is also a Witt ring. A Witt ring is of *elementary type* if it can be built up from the fundamental Witt rings listed above by a sequence of group ring extensions and Witt products. The proposed classification is simply that every finitely generated Witt ring is of elementary type.

The first section of this paper presents elementary results and reduction theorems. The second section computes the derivation algebra for any Witt ring of elementary type. An important step here is deriving some short exact sequences relating $\mathrm{Der}(L_{2n,0})$, $\mathrm{Der}(L_{2n,1})$ and $\mathrm{Der}(L_{2n-1})$.

The third section examines some examples. We give an example of two non-isomorphic Witt rings on 8 generators with Lie isomorphic derivation algebras. We also give an example of derivations arising naturally in the theory of quadratic forms. Let $F \subset K$ be a quadratic field extension and let s_* denote the usual Scharlau transfer and i_* denote the map on Witt rings induced by inclusion. Then, in many cases i_*s_*: $WK \to WK$ is a derivation.

The fourth section is devoted to proving $L = \mathrm{Der}(R)$ is a simple algebra iff R is a group ring over $\mathbf{Z}/2\mathbf{Z}$ and $L = W_n$, the generalized Witt algebra, for some n.

The fifth section examines when a derivation on a Witt ring R is integrable (in the sense of Matsumura [6]). We show that if R is of elementary type then every derivation is integrable iff R is not a group ring extension of a ring of characteristic two.

The notation for Witt rings generally follows [5]. R will always denote a finitely generated Witt ring. There is an associated group G (of one dimensional forms) with distinguished element -1. Every element of R may be expressed as a *form* $\langle g_1, \ldots, g_n \rangle$ with each $g_i \in G$. There is also an associated linked quaternionic mapping q: $G \times G \to B$, where B is some set. If there is a group H and a linked quaternionic mapping q: $H \times H \to B'$ onto some set B', then there is induced a Witt ring which we will denote WH. I_R denotes the fundamental ideal of R, that is, the collection of even dimensional forms.

If $r = \langle g_1, \ldots, g_n \rangle \in R$ then $D\langle g_1, \ldots, g_n \rangle$ (or $D_R\langle g_1, \ldots, g_n \rangle$ if the ring R needs to be specified) is the set of elements of G represented by r.

This should be distinguished from $D(\langle g_1, \ldots, g_n \rangle)$—note the parentheses—which will indicate the image of r under the derivation D.

We will write $\mathbf{Z}_n$ for $\mathbf{Z}/n\mathbf{Z}$. Δ_n will always denote a group of exponent 2 and order 2^n. A *universal round form* in R is a form $r \in R$ such that $gr = r$ for all g in the associated group G. We let $\mathrm{ur}(R)$ denote the collection of all universal round forms; $\mathrm{ur}(R)$ is an ideal. If $I \subset R$ is an ideal, $\mathrm{ann}_R I$ denotes the annihilator of I in R.

1. Reductions. We begin an elementary observation:

LEMMA 1.1. *Let* $D \in \mathrm{Der}(R)$. *Then*:
(1) $D(1) = D(-1) = 0$;
(2) $D(R) \subset \mathrm{ann}(\langle 1, 1 \rangle)$.

Proof. (1) $D(1) = D(1 \cdot 1) = D(1) + D(1)$, so $D(1) = 0$. And $0 = D(0) = D(\langle 1, -1 \rangle) = D(1) + D(-1)$, so $D(-1) = 0$.

(2) It suffices to show $D(x) \in \mathrm{ann}(\langle 1, 1 \rangle)$ for all $x \in G$. Now $0 = D(1) = D(x \cdot x) = xD(x) + xD(x)$. Hence $\langle 1, 1 \rangle D(x) = 0$. □

It will frequently be easier to define a map on G and show it extends to a derivation on R. The appropriate restrictions on the map on G are in the following:

DEFINITION. Let R be a Witt ring and G its associated group. A *G-derivation* is a map $d\colon G \to R$ such that
(i) $d(-1) = 0$;
(ii) $d(xy) = xd(y) + yd(x)$, for all $x, y \in G$;
(iii) $d(xy) = d(x) + d(y)$ if $x \in D\langle 1, y \rangle$.
Let $\mathrm{Der}(G)$ denote the collection of G-derivations. Note that for $d \in \mathrm{Der}(G)$, $d(1) = 0$ and $d(G) \subset \mathrm{ann}(\langle 1, 1 \rangle)$ (namely, the proof of (1.1) carries over).

PROPOSITION 1.2. *Every G-derivation induces a derivation on R. In particular, there is a bijection* $\mathrm{Der}(G) \leftrightarrow \mathrm{Der}(R)$.

Proof. Let $d \in \mathrm{Der}(G)$ and define $D\colon R \to R$ by $D(\langle a_1, \ldots, a_n \rangle) = d(a_1) + \cdots + d(a_n)$. Note that $D(\langle 1, -1 \rangle) = 0$. To show D is well-defined it suffices to check on binary forms (cf. [**5**, p. 31]). Suppose $\langle x_1, x_2 \rangle = \langle y_1, y_2 \rangle$ in R. Then $x_1 x_2 = y_1 y_2$ and $x_1 y_1 \in D\langle 1, x_1 x_2 \rangle$. Then

$d(x_2y_1) = d(x_1y_1 \cdot x_1x_2) = d(x_1y_1) + d(x_1x_2)$, and $d(x_2y_1) = d(x_1y_2)$. Expanding these equations yields:

$$x_1d(y_2) + y_2d(x_1) = x_1d(y_1) + y_1d(x_1) + x_1d(x_2) + x_2d(x_1),$$
$$x_1(d(y_1) + d(y_2)) = \langle y_1, y_2, -x_2\rangle d(x_1) + x_1d(x_2),$$
$$x_1D(\langle y_1, y_2\rangle) = x_1D(\langle x_1, x_2\rangle),$$
$$D(\langle y_1, y_2\rangle) = D(\langle x_1, x_2\rangle).$$

(In the second step we have used $d(z) = -d(z)$ for any $z \in G$.)

Now D is clearly additive. And

$$D(\langle x_1, \ldots, x_n\rangle \cdot \langle y_1, \ldots, y_m\rangle) = \sum d(x_iy_j) = \sum \big(x_id(y_j) + y_jd(x_i)\big)$$
$$= \langle x_1, \ldots, x_n\rangle D(\langle y_1, \ldots, y_m\rangle) + \langle y_1, \ldots, y_m\rangle D(\langle x_1, \ldots, x_n\rangle).$$

Hence $D \in \mathrm{Der}(R)$.

Lastly, suppose $D \in \mathrm{Der}(R)$ and set $d = D|_G$. Then d is a G-derivation. Namely, condition (i) holds by (1.1), condition (ii) holds by definition and if $x \in D\langle 1, y\rangle$ then $D(x) + D(xy) = D(x \cdot \langle 1, y\rangle) = D(\langle 1, y\rangle) = D(y)$. Thus $d(xy) = d(x) + d(y)$, since $D(x) = -D(x)$ by (1.1). □

REMARKS. (1) We will identity G-derivations with derivations on R.

(2) Combining conditions (ii) and (iii) for a G-derivation yields:

If $x \in D\langle 1, y\rangle$ then $\langle 1, x\rangle d(y) = \langle 1, y\rangle d(x)$. This will be used frequently.

DEFINITION. Let β be a Pfister form of R such that $i_G(D(\beta)) \leq 2$ and $\langle 1, 1\rangle\beta = 0$. Let H be a subgroup of index 2 in G containing -1 and contained in $D(\beta)$. For $x, y \in G$ define:

$$d(H, x\beta)(y) = \begin{cases} x\beta & \text{if } y \notin H, \\ 0 & \text{if } y \in H. \end{cases}$$

The derivation (induced by) $d(H, x\beta)$ is the *derivation of H and $x\beta$*.

We check this definition makes sense.

LEMMA 1.3. *$d(H, x\beta)$ is a derivation.*

Proof. Let d denote $d(H, x\beta)$; $d(-1) = 0$. Let $y_1, y_2 \in G$. We check conditions (ii) and (iii) for a G-derivation at the same time. Since we may switch the roles of y_1, y_2 there are three cases to consider:

Case 1. $y_1, y_2 \in H$.

Here $d(y_1) = d(y_2) = d(y_1y_2) = 0$. So $d(y_1y_2) = y_1d(y_2) + y_2d(y_1) = d(y_1) + d(y_2)$.

Case 2. $y_1 \notin H$, $y_2 \in H$.

Here $d(y_1) = x\beta$, $d(y_2) = 0$ and $d(y_1y_2) = x\beta$. Note that since $y_2 \in H \subset D(\beta)$, $y_2 x\beta = x\beta$. Thus we have:

$$d(y_1y_2) = y_1d(y_2) + y_2d(y_1) = d(y_1) + d(y_2).$$

Case 3. $y_1 \notin H$, $y_2 \notin H$.

Here $y_1y_2 \in H$ since $i_G(H) = 2$. We hae $d(y_1) = x\beta = d(y_2)$ and $d(y_1y_2) = 0 = x \cdot \langle 1,1\rangle\beta = d(y_1) + d(y_2)$. Since $y_1y_2 \in D(\beta)$, $y_1d(y_2) + y_2d(y_1) = y_1(d(y_2) + d(y_1)) = 0 = d(y_1y_2)$. □

PROPOSITION 1.4. $\mathrm{Der}(R) = 0$ *iff* R *is reduced or* $R \cong \mathbf{Z}_2$ *or* $R \cong \mathbf{Z}_4$. *In particular*, R *is of elementary type.*

Proof. If R is reduced then $\mathrm{Der}(R) = 0$ by (1.1)(2), and if $R \cong \mathbf{Z}_2$ or $\mathbf{Z}_4$ then $G \subset \{\pm 1\}$ and so $\mathrm{Der}(R) = 0$ by (1.1)(1). Now suppose R is not reduced, $\mathbf{Z}_2$ or $\mathbf{Z}_4$.

Since R is not reduced we can choose $w \in D\langle 1,1\rangle \setminus \{1\}$. Then $\beta_0 = \langle 1, -w\rangle \in \mathrm{ann}(\langle 1,1\rangle)$ and $\beta_0 \neq 0$. We can find a non-zero Pfister form β, divisible by β_0, such that $D(\beta) = G$. Namely, suppose otherwise and choose a non-zero Pfister form β with $D(\beta)$ maximal among those divisible by β_0 (β exists since $|G| < \infty$). If $D(\beta) \neq G$ take $x \in G \setminus D(\beta)$. Then $\langle 1, -x\rangle\beta \neq 0$, β_0 divides $\langle 1, -x\rangle\beta$ and $-1, -x$, $D(\beta) \subset D(\langle 1, -x\rangle\beta)$, so $\{1, x\}D(\beta) \subset D(\langle 1, -x\rangle\beta)$, contradicting the maximality of β.

Now $G \not\subset \{1, -1\}$, since $G \subset \{1, -1\}$ implies R is isomorphic to $\mathbf{Z}_2$, $\mathbf{Z}_4$ or $\mathbf{Z}$ [**5**, p. 41–42] and $\mathbf{Z}$ is reduced. Choose $a \in G \setminus \{1, -1\}$ and choose H a subgroup of index 2 in G containing -1 but not a. Then $d(H, \beta)$ is a derivation (1.3) and non-zero since $d(H, \beta)(a) = \beta$. Thus $\mathrm{Der}(R) \neq 0$. □

We begin the computation of $\mathrm{Der}(R)$ for R of elementary type by decomposing $\mathrm{Der}(R)$ when R is a group ring or a Witt product.

PROPOSITION 1.5. *Let* $R = R_0[\Delta_1]$ *with* $\Delta = \{1, t\}$ *and let* G_0 *be the group associated to* R_0. *Set*:

$$L_0 = \{D \in \mathrm{Der}(R) \mid D(t) = 0 \text{ and } D(G_0) \subset R_0\},$$

$$L_1 = \{D \in \mathrm{Der}(R) \mid D(G_0) = 0 \text{ and } D(t) \in R_0\}.$$

Then: (1) L_0 *is a subalgebra of* $\mathrm{Der}(R)$ *isomorphic to* $\mathrm{Der}(R_0)$;

(2) L_1 *is an abelian subalgebra isomorphic to* $\mathrm{ann}_{R_0}(\langle 1,1\rangle)$;

(3) $\mathrm{Der}(R) = L_0 \oplus tL_0 \oplus L_1 \oplus tL_1$.

Proof. (1) L_0 is closed under addition and if $D_1, D_2 \in L_0$ then $(D_1 \circ D_2)(t) = 0$ and $(D_1 \circ D_2)(G_0) \subset D_1(R_0) \subset R_0$. So L_0 is a subalgebra. If $D \in L_0$ then $D|_{R_0} \in \mathrm{Der}(R_0)$. Let $d \in \mathrm{Der}(R_0)$ and define $D(r_0 + tr_1) = d(r_0) + td(r_1)$, for $r_0, r_1 \in R_0$. This is well-defined since each $r \in R$ uniquely determines $r_0, r_1 \in R_0$ with $r = r_0 + tr_1$. It is straightforward to check $D \in \mathrm{Der}(R)$. Since $D(t) = td(1) = 0$ and $d(G_0) \subset R_0$ we have $D \in L_0$. Also $D|_{R_0} = d$ and so L_0 is isomorphic to $\mathrm{Der}(R_0)$.

(2) L_1 is closed under addition and if $D_1, D_2 \in L_1$ then $(D_1 \circ D_2)(G) = D_1(D_2(tG_0)) \subset D_1(R_0) = 0$. Thus L_1 is an abelian subalgebra.

For $w \in \mathrm{ann}_{R_0}(\langle 1,1\rangle)$ define $d(w)\colon G \to R$ by $d(w)(g_0) = 0$ and $d(w)(g_0 t) = g_0 w$, for all $g_0 \in G_0$. We check that $d(w)$ is a derivation. First, $d(w)(-1) = 0$. Next, let $x, y \in G$. If $x, y \in G_0$ then $yd(w)(x) + xd(w)(y) = 0 + 0 = d(w)(xy)$. If $x = g_0 t \in tG_0$, $y \in G_0$ then $yd(w)(x) + xd(w)(y) = yg_0 w = d(w)(xy)$. And if $x = g_0 t$, $y = g_1 t$, with $g_0, g_1 \in G_0$ then $yd(w)(x) + xd(w)(y) = g_0 g_1 tw + g_0 g_1 tw = 0 = d(w)(xy)$, since $\langle 1,1\rangle w = 0$.

Now suppose $x, y \in G$ and $x \in D\langle 1, y\rangle$. Then either $x, y \in G_0$ or $x = y \in tG_0$, since t is 2-sided rigid [**5**, 5.19]. If $x, y \in G_0$ then $d(w)(x) + d(w)(y) = 0 = d(w)(xy)$. And if $x = y$ then $d(w)(x) + d(w)(y) = \langle 1,1\rangle d(w)(x) = 0 = d(w)(xy)$. Thus $d(w)$ is a derivation.

We have inverse homomorphisms $L_1 \to \mathrm{ann}_{R_0}(\langle 1,1\rangle)$ by $D \mapsto D(t)$ and $\mathrm{ann}_{R_0}(\langle 1,1\rangle) \to L_1$ by $w \mapsto d(w)$. Hence L_1 is isomorphic to $\mathrm{ann}_{R_0}(\langle 1,1\rangle)$.

(3) It suffices to show $\mathrm{Der}(R) = L_0 + tL_0 + L_1 + tL_1$ since the sum can easily be shown to be direct. Let $D \in \mathrm{Der}(R)$. If $r \in R_0$ there exist unique $r_1, r_2 \in R_0$ such that $D(r) = r_1 + tr_2$. Let $d_1(r) = r_1$ and $d_2(r) = r_2$. Extend these maps to R by setting $d_i(r + r't) = d_i(r) + td_i(r')$, where $i = 1,2$ and $r, r' \in R_0$. Also, by (1.1), there exist unique $w_1, w_2 \in \mathrm{ann}_{R_0}(\langle 1,1\rangle)$ such that $D(t) = w_1 + tw_2$. Then $D = d_1 + td_2 + d(w_1) + td(w_2)$, where the $d(w_i)$, $i = 1,2$, are the derivations defined in (2). So it suffices to show $d_1, d_2 \in L_0$.

Now d_1 and d_2 are additive and $d_i(t) = 0$, $d_i(G_0) \subset R_0$ $(i = 1,2)$. Let $r, r' \in R_0$. Then:

$$D(rr') = rD(r') + r'D(r),$$

$$d_1(rr') + td_2(rr') = rd_1(r') + trd_2(r') + r'd_1(r) + tr'd_2(r),$$

$$d_i(rr') = rd_i(r') + r'd_i(r), \qquad (i = 1,2).$$

Hence $d_i|_{R_0} \in \mathrm{Der}(R_0)$ and, as in (1), $d_i \in L_0$ $(i = 1,2)$. □

COROLLARY 1.6. $|\mathrm{Der}(R_0[\Delta_1])| = |\mathrm{Der}(R_0)|^2 |\mathrm{ann}_{R_0}(\langle 1,1\rangle)|^2$. □

DEFINITION. An ideal $I \subset R$ is *differentiable* if $D(I) \subset I$ for all $D \in \mathrm{Der}(R)$.

THEOREM 1.7. *I_R is not differentiable iff* $\mathrm{char}(R) = 2$ *and R is a group ring.*

Proof. ($\rightarrow$). Let $r = \langle a_1, \ldots, a_{2n} \rangle$ and $d \in \mathrm{Der}(R)$ such that $D(r) \notin I_R$. Then for some a_i, say a_1, $D(a_1) \notin I_R$. By (1.1), $\langle 1, 1 \rangle D(a_1) = 0$. Since $\dim D(a_1)$ is odd, $\langle 1, 1 \rangle = 0$ [**4**, p. 250] and so $\mathrm{char}(R) = 2$. Now let $x \in D\langle 1, a_1 \rangle$. Then

$$\langle 1, a_1 \rangle D(x) = \langle 1, x \rangle D(a_1).$$

Since $D(a_1)$ is odd dimensional, the discriminant of $\langle 1, x \rangle D(a_1)$ is x. But the discriminant of $\langle 1, a_1 \rangle D(x)$ is 1 or a_1. Hence $x = 1$ or a_1. So $D\langle 1, a_1 \rangle = \{1, a_1\}$.

Further, $D(a_1) = D(-a_1) \notin I_R$ so the same argument shows $D\langle 1, -a_1 \rangle = \{1, -a_1\}$. Hence a_1 is two-sided rigid and by [**5**, 51.9] R is a group ring.

($\leftarrow$) Let $R = R_0[\Delta_1]$ where $\Delta_1 = \{1, t\}$; note that t is two-sided rigid. Now $\mathrm{char}(R) = 2$ implies $1 \in \mathrm{ann}_{R_0}(\langle 1, 1 \rangle)$. Let $D = td(1)$, where $d(1)$ is the derivation constructed in (1.5) with $d(1)(R_0) = 0$ and $d(1)(t) = \langle 1 \rangle$. Then $D(\langle 1, 1 \rangle) = \langle t \rangle \notin I_R$. □

We next consider Witt products. Let $R = R_1 \times_w R_2$ with corresponding groups $G = G_1 \times G_2$. Let $L = \mathrm{Der}(R)$. We form the following subsets of L:

$$L_1 = \{ D \in L \mid D(1 \times G_2) = 0,\ D(G_1 \times 1) \subset I_{R_1} \times 0 \},$$

$$L_2 = \{ D \in L \mid D(G_1 \times 1) = 0,\ D(1 \times G_2) \subset 0 \times I_{R_2} \},$$

$$E_1 = \{ D \in L \mid D(1 \times G_2) = 0,\ D(G_1 \times 1) \subset 0 \times I_{R_2} \},$$

$$E_2 = \{ D \in L \mid D(G_1 \times 1) = 0,\ D(1 \times G_2) \subset I_{R_1} \times 0 \}.$$

Suppose $\mathrm{char}(R) \neq 2$. R_1 and R_2 cannot both have characteristic 2; we will assume $\mathrm{char}(R_1) \neq 2$. Then $(-1, 1) \neq (1, 1)$ in G. Fix a subgroup B of index 2 in G with $(-1, 1) \notin B$. Set:

$$F = \{ D \in L \mid D(B) = 0 \}.$$

PROPOSITION 1.8. *Let* $R = R_1 \times_w R_2$ *and* $L = \mathrm{Der}(R)$. *With the notations given above, we have*:

(1) L_i *is a subalgebra isomorphic to*

$$\{ D \in \mathrm{Der}(R_i) \mid D(R_0) \subset I_{R_i} \} \text{ for } i = 1, 2.$$

(2) E_1 *and* E_2 *are abelian subalgebras and*

$$E_1 \cong \mathrm{Hom}(G_1/\{\pm 1\}, \mathrm{ur}(R_2))$$

$$E_2 \cong \mathrm{Hom}(G_2/\{\pm 1\}, \mathrm{ur}(R_1)).$$

(3) *If* $\mathrm{char}(R) \neq 2$ *then* F *is a subalgebra isomorphic* (*as a group*) *to* $\mathrm{ur}(R)$.

(4) *If* $\mathrm{char}(R) \neq 2$ *then* $L = L_1 \oplus L_2 \oplus E_1 \oplus E_2 \oplus F$.

(5) *If* $\mathrm{char}(R) = 2$ *then* $L = L_1 \oplus L_2 \oplus E_1 \oplus E_2$.

Proof. (1) Straightforward.

(2) We prove the result for E_1; the case for E_2 is similar. Let $D, D' \in E_1$. Then $(D \circ D')(G) \subset D(0 \times I_{R_2}) = 0$. Thus E_1 is an abelian subalgebra. Now $D(-1,1) = D(1,-1) = 0$ and $D(G) \subset 0 \times \mathrm{ur}(R_2)$. Namely, if $h \in G_1$ and $k \in G_2$ then since $(1,k) \in D\langle (1,1), -(h,1)\rangle$ we have

$$\langle (1,1), -(1,k)\rangle D(h,1) = \langle (1,1), -(h,1)\rangle D(1,k) = 0.$$

So if $D(h,1) = (0,r)$, with $r \in I_{R_2}$, then $\langle 1, -k\rangle r = 0$ for all $k \in G_2$ and so $r \in \mathrm{ur}(R_2)$.

We thus have $D(-1,1) = 0$ and $D(G_1 \times 1) \subset 0 \times \mathrm{ur}(R_2)$. So D induces a map e: $G_1/\{\pm 1\} \to \mathrm{ur}(R_2)$. Lastly,

$$\begin{aligned} 0 \times e(hh') &= D(hh',1) = (h,1)D(h',1) + (h',1)D(h,1) \\ &= D(h',1) + D(h,1) = 0 \times e(h') + 0 \times e(h). \end{aligned}$$

Hence $e \in \mathrm{Hom}(G_1/\{\pm 1\}, \mathrm{ur}(R_2))$.

Conversely, let $e \in \mathrm{Hom}(g_1/\{\pm 1\}, \mathrm{ur}(R_2))$; e lifts to a unique map $\bar{e}$ in $\mathrm{Hom}(G_1, \mathrm{ur}(R_2))$ sending -1 to 0. Define $D(g_1, g_2)$ to be $(0, \bar{e}(g_1))$, for all $g_1 \in G_1$, $g_2 \in G_2$. Then $D(-1) = 0$ and

$$\begin{aligned} D(g_1 g_1', g_2 g_2') &= (0, \bar{e}(g_1 g_1')) = (0, \bar{e}(g_1)) + (0, \bar{e}(g_1')) \\ &= D(g_1, g_2) + D(g_1', g_2') = (g_1', g_2')D(g_1, g_2) + (g_1, g_2)D(g_1', g_2'), \end{aligned}$$

since $D(G) \subset 0 \times \mathrm{ur}(R_2)$. By (1.2) $D \in L$ and clearly D induces e.

(3) That F is a subalgebra follows from the definitions. We map $\mathrm{ur}(R) \to F$ by $w \mapsto d(B,w)$, where $d(B,w)$ is the derivation of B and w. The map is additive and injective. To show the map is surjective we first

prove the

Claim. If $D \in L$ then $D(-1,1) \in \mathrm{ur}(R)$.

Let $h \in G_1$ and let $D(h,1) = (r_1, r_2)$ with $r_i \in R_i$. Then $(h,1) \in D\langle(1,1), (-1,1)\rangle$ implies $\langle(1,1), (h,1)\rangle D(-1,1) = \langle(1,1), (-1,1)\rangle D(h,1) = (\langle -1,1\rangle r_1, \langle 1,1\rangle r_2) = 0$, using (1.1). Similarly, if $k \in G_2$ then $(1,k) \in D\langle(1,1), (1,-1)\rangle$, $D(1,-1) = D(-1,1)$ and $\langle(1,1), (1,k)\rangle D(-1,1) = \langle(1,1), (1,-1)\rangle D(1,k) = 0$. Thus $\langle 1,g\rangle D(-1,1) = 0$ for all $g \in G_1 \times 1 \cup 1 \times G_2$ and hence for all $g \in G$. Then $D(-1,1) \in \mathrm{ur}(R)$ as claimed.

Now if $D \in F$ and $D(-1,1) = w$ then for any $b \in G$, $D(b) = 0$ and $(b \cdot (-1,1)) = bw = w$, since $w \in \mathrm{ur}(R)$. Hence $D = d(B,w)$ with $w \in \mathrm{ur}(R)$ and the map is surjective.

(4), (5) It is easily verified that the sums involved are direct. Let $D \in L$. If $D(-1,1) \neq 0$ then $\mathrm{char}(R) \neq 2$ and $D(-1,1) \in \mathrm{ur}(R)$ by the claim in (3). By (3) we can find $D_5 \in F$ such that $D(-1,1) = D_5(-1,1)$. It thus remains to show that if $D \in L$ and $D(-1,1) = 0$ then $D \in L_1 + L_2 + E_1 + E_2$.

The only Witt product that is also a group ring is $\mathbf{Z} \times_w \mathbf{Z}$ [**5**, 5.22] which is reduced. Hence by (1.7), $D(G) \subset I_R$. Let π_1, π_2 be the projections from I_R to $I_{R_1} \times 0$, $0 \times I_{R_2}$, respectively. Let ρ_1, ρ_2 be the projections from G to $G_1 \times 1$, $1 \times G_2$, respectively. Set $D_1 = \pi_1 D \rho_1$, $D_2 = \pi_2 D \rho_2$, $D_3 = \pi_2 D \rho_1$ and $D_4 = \pi_1 D \rho_2$. Then we claim $D_1 \in L_1$, $D_2 \in L_2$, $D_3 \in E_1$ and $D_4 \in E_2$. We check this only for D_1 and D_3.

For $g, g' \in G$,

$$\begin{aligned} D_1(gg') &= \pi_1 D\big(\rho_1(g)\rho_1(g')\big) \\ &= \pi_1\big(\rho_1(g')D(\rho_1(g)) + \rho_1(g)D(\rho_1(g'))\big) \\ &= \rho_1(g')D_1(g) + \rho_1(g)D_1(g') = g'D_1(g) + gD_1(g'), \end{aligned}$$

since $D_1(G) \subset I_{R_1} \times 0$ implies $(1,y)D(x) = D(x)$ for any $y \in G_2$, $x \in G$. If $g \in D\langle 1, g'\rangle$ then $\rho_1(g) \in D\langle 1, \rho_1(g')\rangle$ and so

$$D_1(gg') = \pi_1\big(D(\rho_1(g)) + D(\rho_2(g'))\big) = D_1(g) + D_1(g').$$

Thus $D_1 \in L_1$.

Now

$$\begin{aligned} D_3(gg') &= \pi_2\big(D(\rho_1(g))\rho_1(g')\big) \\ &= \pi_2\big(\rho_1(g')D(\rho_1(g)) + \rho_1(g)D(\rho_1(g'))\big) = D_3(g) + D_3(g'). \end{aligned}$$

We thus only need to show that $g'D_3(g) = D_3(g)$ for all $g, g' \in G$. Fix $g \in G$. Since $D_3(g) \subset 0 \times I_{R_2}$, $g'D_3(g) = D_3(g)$ if $g' \in G_1 \times 1$. If $g' = (1, k') \in 1 \times G_2$ then $g' \in D\langle 1, -\rho_1(g)\rangle$ so $\langle 1, -g'\rangle D(\rho_1(g)) = \langle 1, -\rho_1(g)\rangle D(g')$. Now $\pi_1(\langle 1, -g'\rangle D(\rho_1(g))) = \langle 1, -1\rangle(\pi_1 D\rho_1)(g) \times 0 = 0$. And

$$\pi_2\big(\langle 1, -g'\rangle D(\rho_1(g))\big) = \pi_2\big(\langle 1, -\rho_1(g)\rangle D(g')\big)$$
$$= 0 \times \langle 1, -1\rangle(\pi_2 D)(g') = 0.$$

Hence $g'D(\rho_1(g)) = D(\rho_1(g))$ if $g' \in 1 \times G_2$. That is, we have $g'D_3(g) = D_3(g)$ for all $g' \in G_1 \times 1 \cup 1 \times G_2$ and hence for all $g' \in G$. Thus, $D_3 \in E_1$.

Lastly, we show $D = D_1 + D_2 + D_3 + D_4$. For any $g \in g$. $\rho_1(g) \in D\langle 1, -\rho_2(g)\rangle$. So $D(g) = D(\rho_1(g)\rho_2(g)) = D(\rho_1(g)) + D(\rho_2(g))$. That is,

$$D = D\rho_1 + D\rho_2 = \pi_1 D\rho_1 + \pi_2 D\rho_1 + \pi_1 D\rho_2 + \pi_2 D\rho_2$$
$$= D_1 + D_3 + D_4 + D_2. \qquad \square$$

The simplest case of (1.8) yields

COROLLARY 1.9. *Suppose* $\operatorname{char} R_1 \neq 2$, *and* $\operatorname{char} R_2 \neq 2$. *Let* $R = R_1 \times_w R_2$ *and let* G *be the group associated to* R. *Then taking* $\mathbf{Z}_2$*-dimensions*:

$$\dim \operatorname{Der}(R) = \dim \operatorname{Der}(R_1) + \dim \operatorname{Der}(R_2) + (\dim G)(\dim \operatorname{ur}(R)).$$

Proof. We use the notations of (1.8). By (1.7), $L_i = \operatorname{der}(R_i)$ for $i = 1, 2$. We have by (1.8)

$$\dim E_1 = (\dim G - 1)\dim \operatorname{ur}(R_1)$$
$$\dim E_2 = (\dim G - 1)\dim \operatorname{ur}(R_2)$$
$$\dim F = \dim \operatorname{ur}(R_1) + \dim \operatorname{ur}(R_2)$$

(This last since $\operatorname{ur}(R) = \operatorname{ur}(R_1) \times \operatorname{ur}(R_2)$). The decomposition $\operatorname{Der}(R) = L_1 \oplus L_2 \oplus E_1 \oplus E_2 \oplus F$ then yields the result. $\square$

2. Derivation algebras for fundamental Witt rings. To complete the computation of $\operatorname{Der}(R)$ for R of elementary type we need to consider derivations on the fundamental Witt rings. These Witt rings are (cf. [**5**, 5.24]) $\mathbf{Z}$, $\mathbf{Z}_2$, $\mathbf{Z}_4$ and $L_{2n,0}$, $L_{2n,1}$, L_{2n-1} for $n \geq 2$. The latter three classes are Witt rings of local type.

By (1.4), $\mathrm{Der}(R) = 0$ for $R = \mathbf{Z}_1\mathbf{Z}_2$ and $\mathbf{Z}_4$. So for the rest of this section we will consider Witt rings of local type. Such Witt rings possess a *unique non-trivial 2-fold Pfister form, to be denoted* ρ throughout this section. Further, for each $x \neq -1$, $D\langle 1, x\rangle$ is a subgroup of index 2 in G. The converse also holds, which we separate for future reference:

LEMMA 2.1. *Let R be a Witt ring of local type with (finite) group G. For every subgroup H of index 2 in G there exists an $x \in G$ with $H = D\langle 1, x\rangle$.*

Proof. There are $|G| - 1$ subgroups of index 2 in G. There are $|G| - 1$ elements $x \in G \setminus \{-1\}$, each of which yields a (distinct) subgroup $D\langle 1, x\rangle$ of index 2. Hence the result holds. □

LEMMA 2.2. *Let R be a Witt ring of local type with group G. Assume $R \neq \mathbf{Z}$.*

(1) *If* $\mathrm{char}(R) \neq 2$ *then* $\mathrm{ann}_R\langle 1, 1\rangle = \{0, \rho\} \cup \{\langle 1, x\rangle,\ y\langle 1, x\rangle \mid -x \in D\langle 1, 1\rangle \setminus \{0\}$ *and* $y \notin D\langle 1, x\rangle\}$. *In particular,* $|\mathrm{ann}_R\langle 1, 1\rangle| = |G|$.

(2) *If* $\mathrm{char}(R) = 2$ *then* $\mathrm{ann}_R\langle 1, 1\rangle \cap I_R = \{0, \rho\} \cup \{\langle 1, x\rangle, y\langle 1, x\rangle \mid x \in G \setminus \{1\},\ y \notin D\langle 1, x\rangle\}$. *In particular,* $|\mathrm{ann}_R\langle 1, 1\rangle \cap I_R| = 2|G|$.

Proof. If $\mathrm{char}(R) \neq 2$ then $\mathrm{ann}_R\langle 1, 1\rangle \subset I_R$. Thus it suffices to find $\mathrm{ann}_R\langle 1, 1\rangle \cap I_R$ in both cases. We will show I_R consists of 0, ρ and binary forms. From this (1) and (2) follow quickly.

Let $q \in I_R$, and let $d = d(q)$. If $d = 1$ then $q \in I_R^2 = \{0, \rho\}$. Otherwise, we may write $q = \langle 1, -d\rangle + q_0$, with $q_0 \in I_R^2$. If $q_0 = 0$ we are done. If $q_0 = \rho$, let $e \notin D\langle 1, -d\rangle$. Then $\langle\langle -d, -e\rangle\rangle = \rho$ and we obtain

$$q = \langle 1, -d\rangle \cdot \langle 1, 1, -e\rangle = e \cdot \langle 1, -d\rangle + \langle\langle 1, -e, -d\rangle\rangle = e \cdot \langle 1, -d\rangle,$$

since $\langle\langle 1, -e, -d\rangle\rangle \in I_r^3 = 0$. □

LEMMA 2.3. *Let R be a Witt ring of local type with group G and* $\mathrm{char}(R) \neq 2$. *Let $D \in \mathrm{Der}(R)$ and $g \in G$. If $D(g) = 0$ then $\langle 1, -g\rangle D(x) = 0$ for all $x \in G$.*

Proof. Let $x \in G$. By (1.1), $D(x) \in \mathrm{ann}_R\langle 1, 1\rangle$ and the result is clear if $D(x) = 0$ or ρ. (Note that $D \equiv 0$ if $R = \mathbf{Z}$.) By (2.2) we may thus assume $D(x) = \langle 1, -y\rangle$ for some $y \in D\langle 1, 1\rangle$. If $x \in D\langle 1, -g\rangle$ then

$\langle 1, -g\rangle D(x) = \langle 1, -x\rangle D(g) = 0$. We thus suppose $x \notin D\langle 1, -g\rangle$; in particular, $g \neq 1$.

Now $\operatorname{char}(R) \neq 2$ implies $D\langle 1,1\rangle \neq G$. We claim that $D\langle 1, x\rangle \cap D\langle 1, g\rangle \setminus D\langle 1,1\rangle \neq \varnothing$. Otherwise, $D\langle 1, x\rangle \cap D\langle 1, g\rangle \subset D\langle 1,1\rangle$. But $D\langle 1, x\rangle \cap D\langle 1, g\rangle$ is a subgroup of index 4 in G, thus contained in only three subgroups of index 2. These three subgroups are $D\langle 1, x\rangle$, $D\langle 1, g\rangle$ and $D\langle 1, -xg\rangle$. This implies that one of x, g, $-xg$ is 1. Each possibility contradicts our previous assumptions, which proves the claim.

Let $z \in D\langle 1, x\rangle \cap D\langle 1, g\rangle \setminus D\langle 1,1\rangle$. Then $z \notin D\langle 1, -g\rangle$ lest $z \in D\langle 1, g\rangle \cap D\langle 1, -g\rangle \subset D\langle 1, 1\rangle$. Also, since $x \notin D\langle 1, -g\rangle$ and $D\langle 1, -g\rangle$ is a group of index 2, we have $xz \in D\langle 1, -g\rangle$. Lastly, $x, z \in D\langle 1, x\rangle$ implies $xz \in D\langle 1, x\rangle \cap D\langle 1, -g\rangle \subset D\langle 1, gx\rangle$, so $-gx \in D\langle 1, -xz\rangle$. We have:

$$\langle 1, -xz\rangle D(xg) = \langle 1, -xg\rangle D(xz),$$

$$\langle 1, -xz\rangle D(x) = \langle 1, -xg\rangle D(x) + \langle 1, -xg\rangle D(z),$$

since $D(xg) = gD(x)$, $\langle 1, -xz\rangle D(x) = 0$ or ρ and so $g\langle 1, -xz\rangle D(x) = \langle 1, -xz\rangle D(x)$. Also, $z \in D\langle 1, x\rangle$ implies $D(xz) = D(x) + D(z)$. Now

$$\begin{aligned}\langle 1, -xz\rangle D(x) &= x \cdot \langle x, -z\rangle D(x) = \langle x, -z\rangle D(x) \\ &= \langle 1, -x\rangle D(x) + \langle 1, -z\rangle D(x),\end{aligned}$$

since $\langle 1,1\rangle D(x) = 0$. Working the same way with $\langle 1, -xg\rangle D(x)$ and $\langle 1, -xg\rangle D(z)$ yields:

$$\begin{aligned}&\langle 1, -x\rangle D(x) + \langle 1, -z\rangle D(x) \\ &\quad = \langle 1, -x\rangle D(x) + \langle 1, -g\rangle D(x) + \langle 1, -x\rangle D(z) + \langle 1, -g\rangle D(z).\end{aligned}$$

$$(*)\quad \langle 1, -z\rangle D(x) = \langle 1, -g\rangle D(x) + \langle 1, -x\rangle D(z) + \langle 1, -g\rangle D(z).$$

But $z \in D\langle 1, x\rangle$ implies $\langle 1, -z\rangle D(x) = \langle 1, -x\rangle D(z)$, and $z \in D\langle 1, g\rangle$ implies $\langle 1, -g\rangle D(z) = \langle 1, -z\rangle D(g) = 0$. Then $(*)$ yields $\langle 1, -g\rangle D(x) = 0$. □

REMARK. Lemma 2.3 does not hold for Witt rings R of local type and characteristic 2. For example, we may describe $L_{4,0}$ by taking $G = (a, b, c, d)$—here (S) denotes the group generated by S—and $D\langle 1, a\rangle = (a, b, c)$, $D\langle 1, b\rangle = (a, b, cd)$, $D\langle 1, c\rangle = (a, c, bd)$ and $D\langle 1, d\rangle = (ab, ac, d)$. The map given by $D(a) = \langle 1, a\rangle$, $D(b) = \langle 1, b\rangle$, $D(c) = \langle 1, a\rangle$ and $D(d) = 0$ induces a derivation. But $D(d) = 0$ while $\langle 1, -d\rangle D(a) \neq 0$.

PROPOSITION 2.4. *Let R be $L_{2n,1}$ or L_{2n+1}, $(n \geq 1)$ and let G be the associated group. Then* $\mathrm{Der}(R)$ *is generated by the derivations $d(H, \beta)$ (cf.* (1.3)). *Here H is a subgroup of index 2 in G containing -1 and β is a scalar multiple of a Pfister form with $H \subset xD(\beta)$, for some $x \in G$.*

Proof. Let $0 \neq D \in \mathrm{Der}(R)$ and let $K = \ker(D|_G)$. Suppose first that $i_G(K) = 2$. Let $x \notin K$ and $\beta = D(x)$. Note that β is a scalar multiple of a Pfister form by (1.1) and (2.2). By (2.3), if $k \in K$ then $\langle 1, -k\rangle D(x) = 0$ so that K is contained in a multiple of the value set of β. Also, $D(k) = 0$ and $D(kx) = kD(x) = D(x)$. Thus $D = d(K, \beta)$.

Now suppose $i_G(K) \geq 4$. Fix $x \notin K$ and let $D(x) = \beta$. We will complete the proof by showing there exists D', a sum of $d(H, \alpha)$'s, such that $\ker((D - D')|_G) \supset K \cup xK$.

By (2.2), $\beta = \rho$, $\langle 1, -y\rangle$ or $z\langle 1, -y\rangle$, where $y \in D\langle 1, 1\rangle$ and $z \notin D\langle 1, -y\rangle$. If $\beta = \rho$, write $G = \{1, x\}H$, with $K \subset H$ and $i_G(H) = 2$. Then $K \cup xK \subset \ker((D - d(H, \rho))|_G)$. If $\beta = \langle 1, -y\rangle$ and $x \notin \langle 1, -y\rangle$ then (2.3) implies $K \subset D\langle 1, -y\rangle$ and so

$$K \cup xK \subset \ker\big((D - d(D\langle 1, -y\rangle, \langle 1, -y\rangle))|_G\big).$$

Now suppose $\beta = \langle 1, -y\rangle$ and $x \in D\langle 1, -y\rangle$. Let H be a subgroup of index 2 in G, containing K but not x. Then $H = D\langle 1, -w\rangle$, for some $w \in G$, by (2.1). We have $x \notin D\langle 1, -w\rangle$ and so $x \notin D\langle 1, -wy\rangle$. Also $K \subset D\langle 1, -y\rangle \cap D\langle 1, -yw\rangle$ by (2.3). Set $D' = d(D\langle 1, -wy\rangle, \langle 1, -wy\rangle) + d(H, -y\langle 1, -w\rangle)$. Then $D'(x) = \langle 1, -wy\rangle \perp -y\langle 1, -w\rangle = \langle 1, -y\rangle = \beta$ and $D'(K) = 0$. So $\ker((D - D')|_G) \supset K \cup xK$.

Lastly, suppose $\beta = z\langle 1, -y\rangle$. By the above argument, there exists D', a sum of $d(H, \alpha)$'s, such that $K \cup xK \subset \ker((zD - D')|_G)$. But zD' is still a sum of $d(H, \alpha)$'s and $K \cup xK \subset \ker((D - zD')|_G)$. □

COROLLARY 2.5. *Let R be $L_{2n,1}$ or L_{2n+1}, $(n \geq 1)$ with associated group G. Then* $\mathrm{Der}(R) \subset \mathrm{Hom}(G, R)$. *That is, if $D \in \mathrm{Der}(R)$ and $x, y \in G$ then $D(xy) = D(x) + D(y)$.*

Proof. This holds for $D = d(H, \beta)$ and hence for all derivations by (2.4). □

REMARKS. (1) (2.4) and (2.5) fail for Witt rings of local type and characteristic 2. The example given after (2.3) has $d(ad) = dD(a) \neq D(a) + D(d)$, contradicting (2.5) and hence (2.4).

(2) There are relations among the $d(H, \beta)$'s which are difficult to determine explicitly. We will compute $\mathrm{Der}(L_{2n,1})$, $\mathrm{Der}(L_{2n+1})$, $n \geq 1$, by an inductive argument instead.

We note that $L_1 = \mathbf{Z}$.

LEMMA 2.6. *Let R be $L_{2n,1}$ or L_{2n+1}, $(n \geq 1)$ and let G be the group associated to R. Let S be the Witt ring of local type with group K where $2|K| = |G|$ and $\mathrm{char}(S) \neq 2$ (i.e. S is L_{2n-1} or $L_{2n,1}$). Fix $a \in G \setminus \{1\}$ with $-1 \notin D\langle 1, a\rangle$.*

(1) *$D\langle 1, a\rangle$ has the induced quaternionic structure and $S \cong W(D\langle 1, a\rangle)$.*

(2) *There is a (group) isomorphism:*

$$\alpha\colon \mathrm{ann}_S\langle 1,1\rangle \to \mathrm{ann}_R\langle 1,1\rangle \cap \mathrm{ann}_R\langle 1, a\rangle$$

with $\alpha(kq) = k\alpha(q)$ for all $q \in \mathrm{ann}_S\langle 1,1\rangle$ and $k \in K$ (K is identified with $D\langle 1, a\rangle$).

Proof. There is an orthogonal decomposition $G = \{1, -a\} \perp D\langle 1, a\rangle$ and so $D\langle 1, a\rangle$ inherits a quaternionic structure with a as the distinguished element (cf. [**1**]). The Witt ring of $D\langle 1, a\rangle$ clearly is of local type, $a \neq 1$ and $2|D\langle 1, a\rangle| = |G|$, so $S \cong W(D\langle 1, a\rangle)$. We now identify S with $W(D\langle 1, a\rangle)$ and K with $D\langle 1, a\rangle$.

Define $\alpha_0\colon I_S \to I_R$ by $\Sigma_i\langle y_{2i-1}, y_{2i}\rangle \mapsto \Sigma_i\langle y_{2i-1}, -ay_{2i}\rangle$. To show α_0 is well-defined, it suffices to check on binary forms, by Witt's theorem on chain equivalence [**5**, p. 31]. Suppose $\langle y_1, y_2\rangle = \langle x_1, x_2\rangle$ in S. Then $y_1y_2 = x_1x_2$ and $x_1y_1 \in D_S\langle 1, y_1y_2\rangle$. Since $x_1, y_1 \in K = D_R\langle 1, a\rangle$ we have $x_1, y_1 \in D_R\langle 1, y_1y_2\rangle \cap D_R\langle 1, a\rangle \subset D_R\langle 1, -ay_1y_2\rangle$. Thus $\langle y_1, -ay_2\rangle = \langle x_1, -ax_2\rangle$ in R. Note that α_0 is clearly a (group) homomorphism and that $\alpha_0(kq) = k\alpha_0(q)$ for all $k \in K$, $q \in I_S$. Further,

$$\langle 1, a\rangle\alpha_0\Big(\sum_i \langle y_{2i-1}, y_{2i}\rangle\Big) = \sum_i y_{2i-1}\langle\langle a, -y_{2i-1}y_{2i}\rangle\rangle = 0,$$

since $y_{2i-1}y_{2i} \in D\langle 1, a\rangle$. Hence $\alpha_0(I_S) \subset \mathrm{ann}_R\langle 1, a\rangle$.

Let α be the restriction of α_0 to $\mathrm{ann}_S\langle 1,1\rangle$. Then $\alpha\colon \mathrm{ann}_S\langle 1,1\rangle \to \mathrm{ann}_R\langle 1,1\rangle \cap \mathrm{ann}_R\langle 1, a\rangle$. Now $|\mathrm{ann}_S\langle 1,1\rangle| = |K| = \frac{1}{2}|G|$, by (2.2). Using (2.2) again shows $\mathrm{ann}_R\langle 1,1\rangle \cap \mathrm{ann}_R\langle 1, a\rangle$ consists of 0, ρ and pairs $\langle 1, x\rangle$, $x'\langle 1, x\rangle$ where $-x \in D_R\langle 1,1\rangle \cap D_R\langle 1, a\rangle \setminus \{1\}$, $x' \notin D\langle 1, x\rangle$. Thus

$$|\mathrm{ann}_R\langle 1,1\rangle \cap \mathrm{ann}_R\langle 1, a\rangle| = 2|D_R\langle 1,1\rangle \cap D_R\langle 1, a\rangle| = \tfrac{1}{2}|G|.$$

To complete the proof then, we need only show α is injective.

Suppose $y, y' \in K$ with $\langle 1, y\rangle \in \operatorname{ann}_S\langle 1,1\rangle$ and $\alpha(y'\langle 1, y\rangle) = 0$. Then $\langle 1, -ay\rangle = 0$ in R, $a = y$ and $\langle 1, y\rangle = 0$ in S. Let $y, y' \in K$, $q = \langle\langle y, -y'\rangle\rangle$ and suppose $\alpha(q) = 0$. Then $\langle 1, -ay\rangle \perp -y'\langle 1, -ay\rangle = 0$, $y' \in D_R\langle 1, -ay\rangle \cap D_R\langle 1, a\rangle \subset D_R\langle 1, y\rangle$. But then $y' \in D_S\langle 1, y\rangle$ and $q = 0$ in S. By (2.2), $\operatorname{ann}_S\langle 1,1\rangle$ consists of such $y'\langle 1, y\rangle$, $\langle\langle y, -y'\rangle\rangle$ and so α is injective. □

Denote the inverse of α by β. Note that $\beta(kq) = k\beta(q)$ for all $k \in D_R\langle 1, a\rangle$ and $q \in \operatorname{ann}_R\langle 1,1\rangle \cap \operatorname{ann}_R\langle 1, a\rangle$. Note also under the identification of K with $D\langle 1, a\rangle$, S is a subring of R. We continue with the notations of (2.6).

COROLLARY 2.7. *Let* $A = \{D \in \operatorname{Der}(R) \mid D(a) = 0\}$. *Then* β_*: $A \to \operatorname{Der}(S)$ *is a Lie algebra isomorphism, where* $\beta_*(D) = \beta(D|_S)$.

Proof. We first show β_* is well-defined. If $x \in G$ and $D \in A$ then $\langle 1, a\rangle D(x) = 0$ by (2.3). Thus $D(R) \subset \operatorname{ann}_R\langle 1,1\rangle \cap \operatorname{ann}_R\langle 1, a\rangle$, the domain of β. Further, if $q_1, q_2 \in S$ then

$$\begin{aligned}\beta_*(D)(q_1q_2) &= \beta(D(q_1q_2)) = \beta(q_1D(q_2) + q_2D(q_1))\\ &= q_1\beta_*(D)(q_2) + q_2\beta_*(D)(q_1),\end{aligned}$$

since $\beta(kq) = k\beta(q)$ for any $k \in K$, $q \in \operatorname{ann}_R\langle 1,1\rangle \cap \operatorname{ann}_R\langle 1, a\rangle$. Thus $\beta_*(D) \in \operatorname{Der}(S)$ for all $D \in A$.

Now β_* is additive and if $D_1, D_2 \in A$ and $k \in K$ write $D_2(k) = \Sigma_i\langle y_{2i-1}, y_{2i}\rangle \in S$. Then:

$$\begin{aligned}\beta_*(D_1)\circ\beta_*(D_2)(k) &= \beta_*(D_1)\Big(\beta\Big(\sum_i\langle y_{2i-1}, y_{2i}\rangle\Big)\Big)\\ &= \beta_*(D_1)\Big(\sum_i\langle y_{2i-1}, -ay_{2i}\rangle\Big) = \beta\Big(\sum D_1\langle y_{2i-1}, -ay_{2i}\rangle\Big)\\ &= \beta\Big(\sum D_1\langle y_{2i-1}, y_{2i}\rangle\Big)\end{aligned}$$

since $D_1(ay_{2i}) = aD_1(y_{2i}) = D_1(y_{2i})$ by (2.3). Thus $\beta_*(D_1)\circ\beta_*(D_2) = \beta_*(D_1\circ D_2)$. In particular, $\beta_*([D_1, D_2]) = [\beta_*D_1, \beta_*D_2]$ and β_* is a Lie algebra homomorphism.

If, for $D \in A$, $\beta_*(D) = 0$ then $D|_K = 0$, since β is an isomorphism. Hence $G = \{1, -a\}K \subset \ker(D|_G)$ and $D = 0$. Thus β_* is injective. To show β_* is surjective it suffices to show that the generators $d(H, \alpha)$ of $\operatorname{Der}(S)$ (2.4) are in the image of β. Let H be a subgroup of index 2 in K containing a. By (2.1), $H = D_S\langle 1, x\rangle$. Let α be $\langle 1, x\rangle$, $x'\langle 1, x\rangle$ or ρ,

where $x' \notin D_S\langle 1, x\rangle$ and $\rho = \langle\langle x, ax'\rangle\rangle$. We need to show $d(H, \alpha)$ is in the image of β_*. We check this only for $\alpha = \langle 1, x\rangle$, the other cases being similar.

Set $H' = D_R\langle 1, -ax\rangle$. Note that $H\{1, -1\} \subset H'$, since $H \subset D_R\langle 1, a\rangle \cap D_R\langle 1, x\rangle$ and $x \in K = D_R\langle 1, a\rangle$, $a \in H \subset D_R\langle 1, x\rangle$ implies $-1 \in D_R\langle 1, -ax\rangle$. Then $\beta_*(d(H', \langle 1, -ax\rangle) = d(H, \langle 1, x\rangle)$. □

THEOREM 2.8. *Let R be $L_{2n,1}$ or L_{2n+1} with $n \geq 1$, and let G be the associated group. Let $a \in G$ with $-a \notin D\langle 1, 1\rangle$. Let $A = \{D \in \mathrm{Der}(R) \mid D(a) = 0\}$. Let $S = L_{2n-1}$ if $R = L_{2n,1}$ and $S = L_{2n,1}$ if $R = L_{2n+1}$.*

(1) *There is an exact sequence of groups*:

$$0 \to A \to \mathrm{Der}(R) \xrightarrow{e} \mathrm{ann}_R\langle 1, 1\rangle \to 0$$

where $e(D) = D(a)$ and A is Lie isomorphic to $\mathrm{Der}(S)$.

(2) $\dim \mathrm{Der}(R) = \frac{1}{2}(n + 2)(n - 1)$.

Proof. (1) We need only show e is surjective by (2.7). Let $\alpha \in \mathrm{ann}_R\langle 1, 1\rangle$. If $\alpha = \rho$, $\langle 1, -x\rangle$ or $x'\langle 1, -x\rangle$ where $x' \notin D_R\langle 1, -x\rangle$ and $a \notin D_R\langle 1, -x\rangle$ then $e(d(D\langle 1, -x\rangle, \alpha)) = \alpha$. By (2.2) we may thus assume $\alpha = \langle 1, -x\rangle$ with $a \in D_R\langle 1, -x\rangle$. Choose z such that $a \notin D_R\langle 1, -z\rangle$. Then

$$e\big(d(D\langle 1, -xz\rangle, \langle 1, -xz\rangle) - xd(D\langle 1, -z\rangle, \langle 1, -z\rangle)\big) = \langle 1, -xz\rangle + -x\langle 1, -z\rangle = \alpha.$$

(2) $\dim(\mathrm{Der}(R)) = \dim(\mathrm{Der}(S)) + n$, by (1) and (2.2). Since $\mathrm{Der}(L_1) = \mathrm{Der}(\mathbf{Z}) = 0$ we have

$$\dim(\mathrm{Der}(R)) = n + (n - 1) + \cdots + 2 = \tfrac{1}{2}(n + 2)(n - 1). \qquad \square$$

We turn now to the Witt rings $L_{2n,0}$ with $n \geq 2$. Let G be the group associated to $L_{2n,0}$ and let q: $G \times G \to \mathbf{Z}_2$ be the associated linked quaternionic map. We require the following construction:

Fix $a, b \in G$ with $a \notin D\langle 1, b\rangle$. There is an orthogonal sum $G = \{1, a, b, ab\} \perp D\langle 1, a\rangle \cap D\langle 1, b\rangle$. Set $H = \{1, a, b, ab\}$ and $K = D\langle 1, a\rangle \cap D\langle 1, b\rangle$. By [1] G induces a quaternionic structure on H and K. In particular, for $k \in K$ we write $D_K\langle 1, k\rangle = D_R\langle 1, k\rangle \cap K$.

Embed K into a group $\overline{K}$ with $|\overline{K}| = 2|K|$; say $\overline{K} = \{1, c\}K$. For $k \in K \setminus \{1\}$ define:

$$D_{\overline{K}}\langle 1, k\rangle = \{1, ck'\}D_K\langle 1, k\rangle, \quad \text{where } k' \in K \setminus D_K\langle 1, k\rangle,$$
$$D_{\overline{K}}\langle 1, ck\rangle = \{1, c\}D_K\langle 1, k\rangle.$$

We also set $D_{\bar{K}}\langle 1,1\rangle = K$ and $D_{\bar{K}}\langle 1,c\rangle = \bar{K}$. We further define $\bar{q}$: $\bar{K}\times\bar{K}\to \mathbf{Z}_2$ by $\bar{q}(x,y)=0$ iff $y\in D_{\bar{K}}\langle 1,cx\rangle$. (We are thus taking c to be the distinguished element of $\bar{K}$.)

LEMMA 2.9. (1) *$\bar{q}$ is a linked quaternionic mapping.*
(2) $W\bar{K}\cong L_{2n-1}$.

Proof. (1) Note that $x\in D_{\bar{K}}\langle 1,x\rangle$ for all $x\in\bar{K}$. Suppose $x\in D_{\bar{K}}\langle 1,y\rangle$. We will show $cy\in D_{\bar{K}}\langle 1,cx\rangle$ for the case $y\in K$ (the case $y\in cK$ is similar). If $x\in D_K\langle 1,y\rangle$ then $x\in D_R\langle 1,y\rangle$, $y\in D_R\langle 1,x\rangle$ since $-1=1$ in G, and so $y\in D_K\langle 1,x\rangle$. Hence $cy\in D_{\bar{K}}\langle 1,cx\rangle$. If $x=cy'x'$ with $y'\in K\setminus D_K\langle 1,y\rangle$ and $x'\in D_K\langle 1,y\rangle$ then $y\in K\setminus D_K\langle 1,x'y'\rangle$. So $cy\in D_{\bar{K}}\langle 1,x'y'\rangle = D_K\langle 1,cx\rangle$.

We lastly check $\bar{q}$ is linked. Suppose $\bar{q}(x_1,y_1)=\bar{q}(x_2,y_2)$, with $x_i,y_j\in\bar{K}$, $(i,j=1,2)$. If $\bar{q}(x_i,y_i)=0$, $i=1,2$, then $\bar{q}(x_1,y_1)=\bar{q}(x_1,1)=\bar{q}(x_2,1)=\bar{q}(x_2,y_2)$. If $\bar{q}(x_i,y_i)\neq 0$, for $i=1,2$, then $y_1\neq 1$ and $y_2\neq 1$. Since $\bar{K}$ cannot be written as the union of two proper subgroups, there exists $w\notin D_{\bar{K}}\langle 1,cx_1\rangle\cup D_{\bar{K}}\langle 1,cx_2\rangle$. Then $\bar{q}(x_1,y_1)=\bar{q}(\bar{x}_1,w)=\bar{q}(x_2,w)=\bar{q}(x_2,y_2)=1$.

(2) $\bar{q}$ has a range of two elements, so the Witt ring $W\bar{K}$ it induces is of local type. Since the distinguished element c is not 1 and $|\bar{K}|=2|K|=\frac{1}{2}|G|$, $W\bar{K}\cong L_{2n-1}$. □

We continue with all of the notations introduced before (2.9) but now writing $\bar{R}$ for $W\bar{K}\cong L_{2n-1}$.

LEMMA 2.10. *There is an additive group isomorphism*

$$\alpha\colon \operatorname{ann}_{\bar{R}}\langle 1,1\rangle\to \operatorname{ann}_R\langle 1,a\rangle\cap\operatorname{ann}_R\langle 1,b\rangle$$

such that $\alpha(yq)=y\alpha(q)$ for all $y\in\bar{K}$, $q\in\operatorname{ann}_{\bar{R}}\langle 1,1\rangle$.

Proof. Since $D_{\bar{K}}\langle 1,1\rangle = K$, a form in $\operatorname{ann}_{\bar{R}}\langle 1,1\rangle$ looks like $\Sigma_i\langle y_{2i-1},cy_{2i}\rangle$, with each $y_j\in K$ (2.2). Define α by:

$$\alpha\Big(\sum_i\langle y_{2i-1},cy_{2i}\rangle\Big)=\sum_i\langle y_{2i-1},y_{2i}\rangle.$$

To show α is well-defined it suffices to check on binary forms. Suppose $\langle y_1,cy_2\rangle=\langle y_3,cy_4\rangle$ in $\bar{R}$. Then $y_1y_2=y_3y_4$ and $y_1y_3\in D_{\bar{K}}\langle 1,cy_1y_2\rangle=\{1,c\}D_K\langle 1,y_1y_2\rangle$. Since $y_1y_3\in K$ we get $y_1y_3\in D_K\langle 1,y_1y_2\rangle\subset D_R\langle 1,y_1y_2\rangle$, so $\langle y_1,y_2\rangle=\langle y_3,y_4\rangle$ in R. Also, since each $y_j\in K=D\langle 1,a\rangle\cap D\langle 1,b\rangle$, $\langle 1,a\rangle\cdot\langle y_{2i-1},y_{2i}\rangle=0=\operatorname{ann}_R\langle 1,a\rangle\cap\operatorname{ann}_R\langle 1,b\rangle$.

Now α is clearly a homomorphism and $\alpha(yq) = y\alpha(q)$ for all $y \in \overline{K}$ and $q \in \operatorname{ann}_{\overline{R}}\langle 1, 1\rangle$. To show α is an isomorphism we first

Claim. $\operatorname{ann}_R\langle 1, a\rangle \cap \operatorname{ann}_R\langle 1, b\rangle = \{0, \rho\} \cup \{\langle 1, k\rangle,\ k'\langle 1, k\rangle \mid k \in K$ and $k' \in K \setminus D_R\langle 1, k\rangle\}$.

Let S be the set on the right-hand side. Since $K = D\langle 1, a\rangle \cap D\langle 1, b\rangle$ and $-1 = 1$ in G we have $S \subset \operatorname{ann}_R\langle 1, a\rangle \cap \operatorname{ann}_R\langle 1, b\rangle$. Let $q \in \operatorname{ann}_R\langle 1, a\rangle \cap \operatorname{ann}_R\langle 1, b\rangle$. If q is not a binary form then $q = 0$ or ρ, since $q \in I_R$. So suppose $q = y \cdot \langle 1, x\rangle$, with $x, y \in G$. Then $\langle 1, a\rangle \cdot \langle 1, x\rangle = 0 = \langle 1, b\rangle \cdot \langle 1, x\rangle$ implies $x \in K$. If $y \in D\langle 1, x\rangle$ then $y\langle 1, x\rangle = \langle 1, x\rangle \in S$. Suppose then that $y \notin D\langle 1, x\rangle$. Now K is a subgroup of index 4 in G. K is then contained in precisely three subgroups of index 2, namely $D\langle 1, x\rangle$, $D\langle 1, b\rangle$ and $D\langle 1, ab\rangle$. If $K \subset D\langle 1, x\rangle$ then $x \in \{a, b, ab\} = H \setminus \{1\}$, which is impossible since $x \in K$ and $K \cap H = \{1\}$. Thus $K \not\subset D\langle 1, x\rangle$. Choose $k' \in K \setminus D\langle 1, x\rangle$. Then $q = y\langle 1, x\rangle = k'\langle 1, x\rangle \in S$. This proves the claim.

The claim quickly yields that α is surjective since fror $k, k' \in K$, $\alpha(\langle k', k'kc\rangle) = k'\langle 1, k\rangle$, and if $k' \notin D\langle 1, k\rangle$ then $\alpha(\langle 1, ck\rangle + k'\langle 1, ck\rangle) = \langle\langle k, k'\rangle\rangle = \rho$. Further the claim shows $|\operatorname{ann}_R\langle 1, a\rangle \cap \operatorname{ann}_R\langle 1, b\rangle| = 2|K| = |\overline{K}|$. By (2.2), $|\operatorname{ann}_{\overline{R}}\langle 1, 1\rangle| = |\overline{K}|$ also. Thus α is an isomorphism. □

LEMMA 2.11. *Let* $R = L_{2n,0}$ *and* $\overline{R} = W\overline{K} \cong L_{2n-1}$ $(n \geq 2)$ *as before. Let* $A = \{D \in \operatorname{Der}(R) \mid D(a) = D(b) = 0\}$. *Then* A *is Lie isomorphic to* $\operatorname{Der}(\overline{R})$.

Proof. We first show that for $D \in A$, $D(R) \subset \operatorname{ann}_R\langle 1, a\rangle \cap \operatorname{ann}_R\langle 1, b\rangle$. For $g \in G$, if $g \in D\langle 1, a\rangle$ then $\langle 1, a\rangle D(g) = \langle 1, g\rangle D(a) = 0$. If $g \notin D\langle 1, a\rangle$ then $bg \in D\langle 1, a\rangle$, since $b \notin D\langle 1, a\rangle$. Hence $\langle 1, a\rangle D(bg) = \langle 1, bg\rangle D(a) = 0$. So $0 = b\langle 1, a\rangle D(g) + g\langle 1, a\rangle D(b)$. Since $D(b) = 0$ also $\langle 1, a\rangle D(g) = 0$. Thus in each case $D(g) \in \operatorname{ann}_R\langle 1, a\rangle$. Similarly, $D(g) \in \operatorname{ann}_R\langle 1, b\rangle$.

For $D \in A$ define $\overline{D}$: $\overline{K} \to \operatorname{ann}_R\langle 1, a\rangle \cap \operatorname{ann}_R\langle 1, b\rangle$, by $\overline{D}(k) = \overline{D}(ck) = D(k)$, for all $k \in K$. Let $\beta = \alpha^{-1}$, where α is the isomorphism of (2.10). Note $\beta(kq) = k\beta(q)$ for all $k \in K$, $q \in \operatorname{ann}_R\langle 1, a\rangle \cap \operatorname{ann}_R\langle 1, b\rangle$. Define β_*: $A \to \operatorname{Der}(\overline{R})$ by:

$$\beta_*(D) = \beta \circ \overline{D}.$$

Note that we have already shown the image of $\overline{D}$ is in the domain of β.

We next show $\beta_*(D) \in \operatorname{Der}(\overline{R})$. First, $\beta_*(D)(c) = \beta_*(\overline{D}(c)) = \beta(D(1)) = 0$. Let $x_1, x_2 \in \overline{K}$ and write $x_i = c^{\varepsilon_i} y_i$, where $\varepsilon_i \in \{0, 1\}$ and

$y_i \in K$. Then

$$\beta_*(D)(x_1x_2) = \beta(D(y_1y_2)) = \beta(y_1D(y_2) + y_2D(y_1))$$
$$= y_1\beta(D(y_2)) + y_2\beta(D(y_1)) = y_1\beta_*(D)(x_2) + y_2\beta_*(D)(x_1)$$
$$= x_1\beta_*(D)(x_2) + x_2\beta_*(D)(x_1),$$

since $\langle 1,1\rangle\beta(D(z)) = 0$ in $\overline{R}$, for any $z \in \overline{K}$, implies $c\beta(D(z)) = \beta(D(z))$.

Next suppose $x_1 \in D_{\overline{R}}\langle 1, x_2\rangle$. Then, by our construction, $y_1 \in D_K\langle 1, y_2\rangle$ unless $x_1 = cy_1$, $x_2 = y_2$. If $y_1 \in D_K\langle 1, y_2\rangle$ then $D(y_1y_2) = D(y_1) + D(y_2)$ and so $\beta_*(D)(x_1x_2) = \beta_*(D)(x_1) + \beta_*(D)(x_2)$. So suppose $y_1, y_2 \in K$ with $cy_1 \in D_{\overline{R}}\langle 1, y_2\rangle$ and $y_1 \notin D_{\overline{R}}\langle 1, y_2\rangle$. Then $y_1 \notin D_R\langle 1, by_2\rangle$, since $y_1 \in K \subset D_R\langle 1, b\rangle$. Also, $a \in D_R\langle 1, y_2\rangle$, $a \notin D_R\langle 1, b\rangle$ imply $a \notin D_R\langle 1, by_2\rangle$. Thus $ay_1 \in D_R\langle 1, by_2\rangle$ and $D(aby_1y_2) = D(ay_1) + D(by_2)$. Now $D(ab) = 0$ implies $D(aby_1y_2) = abD(y_1y_2)$. And $abD(y_1y_2) = D(y_1y_2)$ since $D(R) \subset \operatorname{ann}_R\langle 1, a\rangle \cap \operatorname{ann}_R\langle 1, b\rangle$. Thus $D(aby_1y_2) = D(y_1y_2)$ and similarly $D(ay_1) = D(y_1)$ and $D(by_2) = D(y_2)$. We thus have $D(y_1y_2) = D(y_1) + D(y_2)$ and $\beta_*(D)(x_1x_2) = \beta_*(D)(x_1) + \beta_*(D)(x_2)$. By (1.2) this completes the proof that $\beta_*(D) \in \operatorname{Der}(\overline{R})$.

Clearly β_* is an additive map. Let $D_1, D_2 \in A$ and $x = c^\varepsilon y \in \overline{K}$, with $\varepsilon \in \{0,1\}$ and $y \in K$. Let $D_2(y) = \sum_i \langle z_{2i-1}, z_{2i}\rangle$, with all $z_j \in K$. Then

$$\beta_*(D_1)\circ\beta_*(D_2)(x) = \beta_*(D_1)\Big(\beta\Big(\sum_i \langle z_{2i-1}, z_{2i}\rangle\Big)\Big)$$
$$= \beta_*(D_1)\Big(\sum_i \langle z_{2i-1}, cz_{2i}\rangle\Big) = \beta\Big(D_1\Big(\sum \langle z_{2i-1}, z_{2i}\rangle\Big)\Big)$$
$$= \beta_*(D_1\circ D_2)(x).$$

Hence $\beta_*[D_1, D_2] = [\beta_*D_1, \beta_*D_2]$.

Since β is an isomorphism, β_* is clearly injective. To show β_* is surjective, it suffices to show the generators of $\operatorname{Der}(\overline{R})$ given in (2.4) are in the image of β_*. A generator is $d(L,\gamma)$, where $\gamma \in \overline{R}$ and L is a subgroup of index 2 in $\overline{K}$ containing c and contained in a scalar multiple of $D_{\overline{R}}(\gamma)$. By (2.1) $L = D_{\overline{R}}\langle 1, x\rangle$, for some $x \in \overline{K}$ and $c \in D_{\overline{K}}\langle 1, x\rangle$, hence $cx \in D_{\overline{R}}\langle 1,1\rangle = K$. Then γ is either $\langle 1, x\rangle$, $x'\langle 1, x\rangle$ where $x' \notin D\langle 1, x\rangle$, or ρ the unique non-trivial 2-fold Pfister form in $\overline{R}$ (2.2).

We will show $d(L,\gamma)$ with $\gamma = \langle 1, cy\rangle$, $y \in K$ and $L = D_{\overline{R}}\langle 1, cy\rangle$ is in the image of β_*. The other cases are similar. Let $D = d(D\langle 1, y\rangle, \langle 1, y\rangle) \in \operatorname{Der}(r)$. Since $y \in D\langle 1, a\rangle \cap D\langle 1, b\rangle$, $a, b \in D\langle 1, y\rangle$ and so

$D \in A$. For $\varepsilon \in \{0,1\}$ and $x \in K$ we have $\beta_*(D)(c^\varepsilon x) = \beta(D(x))$, which is 0 if $x \in D_R\langle 1, y\rangle \cap K$, and is $\beta(\langle 1, y\rangle) = \gamma$ if $x \notin D_R\langle 1, y\rangle$. Thus the image $\beta_*(D)(\bar{K})$ is $\{0,\gamma\}$ and the kernel (in $\bar{K}$) is $\{1,c\}D_K\langle 1, y\rangle = D_{\bar{R}}\langle 1, cy\rangle$. Hence $\beta_*(D) = d(L,\gamma)$. □

LEMMA 2.12. *Let G be the group associated to $R = L_{2n,0}$ where $n \geq 1$. Then there exist subgroups G_1, G_2 of G such that*:

(1) $G = G_1 \times G_2$;

(2) $x_1 \in D_R\langle 1, x_2\rangle$, *for all* $x_1, x_2 \in G_1$;

(3) $y_1 \in D_R\langle 1, y_2\rangle$, *for all* $y_1, y_2 \in G_2$.

Further, if we fix $x_0, y_0 \in G$ with $x_0 \notin D_R\langle 1, y_0\rangle$ then we may assume $x_0 \in G_1$ and $y_0 \in G_2$.

Proof. If $n = 1$ then $G = \{1, x_0, y_0, x_0y_0\}$ and the result is clear. Let $n \geq 2$ and fix $x_0, y_0 \in G$ with $x_0 \notin D_R\langle 1, y_0\rangle$. There is an orthogonal decomposition $G = \{1, x_0, y_0, x_0y_0\} \perp D_R\langle 1, x_0\rangle \cap D_R\langle 1, y_0\rangle$. Here $K = D_R\langle 1, x_0\rangle \cap D_R\langle 1, y_0\rangle$ inherits a quaternionic structure and its Witt ring is $L_{2n-2,0}$. By induction there exist $K_1, K_2 \subset K$ satisfying conditions (1)–(3). Set $G_1 = \{1, x_0\}K_1$ and $G_2 = \{1, y_0\}K_2$. Then $G = G_1 \times G_2$.

We check condition (2) (the proof of (3) is similar). Let $x_1, x_2 \in G_1$ and write $x_i = x_0^{\varepsilon_i}x_i'$ where, for $i = 1,2$, $\varepsilon_i \in \{0,1\}$ and $x_i' \in K_1$. Then $x_1' \in D_K\langle 1, x_2'\rangle$ and so $x_1' \in D_R\langle 1, x_2'\rangle$. Since $x_1', x_2' \in K \subset D\langle 1, x_0\rangle$ we also have $x_1 \in D_R\langle 1, x_2\rangle$ as desired. □

THEOREM 2.13. *Let $R = L_{2n,0}$ with $n \geq 2$ and let G be the associated group. Fix $a, b \in G$ with $a \notin D_R\langle 1, b\rangle$. Let $A = \{ D \in \mathrm{Der}(R) \mid D(a) = D(b) = 0\}$.*

(1) *There is an exact sequence of groups*

$$0 \to A \to \mathrm{Der}(R) \xrightarrow{e} I_R \times I_R \to 0$$

where $e(D) = (D(a), D(b))$ and A is a subalgebra Lie isomorphic to $\mathrm{Der}(L_{2n-1})$.

(2) $\dim(\mathrm{Der}(R)) = (2n + 2)(2n + 1)/2$.

Proof. (1) By (2.11) we need only show e is surjective. By symmetry it is enough to show $0 \times I_R \subset \mathrm{im}(e)$. Then, since e is additive and $xD \in \mathrm{Der}(R)$ for all $x \in G$, $D \in \mathrm{Der}(R)$, it suffices to show $(0, \langle 1, g\rangle) \in \mathrm{im}(e)$ for all $g \in G$.

If $g \in D\langle 1, a\rangle \setminus D\langle 1, b\rangle$ then $e(d(D\langle 1, g\rangle, \langle 1, g\rangle)) = (0, \langle 1, g\rangle)$, where $d(D\langle 1, g\rangle, \langle 1, g\rangle)$ is the derivation of (1.3). If $g \in D\langle 1, a\rangle \cap D\langle 1, b\rangle$ then $ag \in D\langle 1, a\rangle \setminus D\langle 1, b\rangle$ and

$$e\big(d(D\langle 1, a\rangle, \langle 1, a\rangle) + d(D\langle 1, ag\rangle, \langle 1, ag\rangle)\big)$$
$$= (0, \langle 1, a\rangle) + (0, \langle 1, ag\rangle) = (0, \langle a, ag\rangle) = (0, \langle 1, g\rangle),$$

since $a \in D\langle 1, g\rangle$. Thus $(0, \langle 1, g\rangle) \in \mathrm{im}(e)$ for all $g \in D\langle 1, a\rangle$. Since $D\langle 1, a\rangle$ has index 2 in G and $b \notin D\langle 1, a\rangle$ it suffices to show $(0, \langle 1, b\rangle) \in \mathrm{im}(e)$.

Write $G = G_1 \times G_2$ with subgroups G_1, G_2 satisfying (2.12) and with $a \in G_1$, $b \in G_2$. Define D: $G \to I_R$ by $D(xy) = x\langle 1, y\rangle$, for all $x \in G_1$, $y \in G_2$. Note that $D(a) = 0$ and $D(b) = \langle 1, b\rangle$. We will be done if we show D is a derivation.

We check the conditions of (1.2). Clearly $D(1) = 0$. If $x_1, x_2 \in G_1$ and $y_1, y_2 \in G_2$ then

$$x_1y_1D(x_2y_2S) + x_2y_2D(x_1y_1) = x_1x_2y_1\langle 1, y_2\rangle + x_1x_2y_2\langle 1, y_1\rangle$$
$$= x_1x_2\langle y_1, y_2, y_1y_2, y_1y_2\rangle = x_1x_2\langle 1, y_1y_2\rangle,$$

since $\langle 1, 1\rangle = 0$ in I_R and $y_1 \in D\langle 1, y_1y_2\rangle$. Thus $D(x_1y_1x_2y_2) = x_1y_1D(x_2y_2) + x_2y_2D(x_1y_1)$. Now suppose $x_1y_1 \in D\langle 1, x_2y_2\rangle$. We have:

$$(*) \qquad \begin{aligned} D(x_1y_1x_2y_2) &= x_1x_2\langle 1, y_1y_2\rangle, \\ D(x_1y_1) + D(x_2y_2) &= x_1x_2(x_2\langle 1, y_1\rangle + x_1\langle 1, y_2\rangle). \end{aligned}$$

There are two cases. If $x_1 \in D\langle 1, y_2\rangle$ then since $x_1 \in D\langle 1, x_2\rangle$ we have $y_1 \in D\langle 1, x_2y_2\rangle$. So $x_1y_1 \in D\langle 1, x_2y_2\rangle$ implies $y_1 \in D\langle 1, x_2y_2\rangle \cap D\langle 1, y_2\rangle \subset D\langle 1, x_2\rangle$, and $x_2 \in D\langle 1, y_1\rangle$. Using $(*)$ gives $D(x_1y_1) + D(x_2y_2) = x_1x_2\langle 1, 1, y_1, y_2\rangle = D(x_1y_1x_2y_2)$.

Lastly, if $x_1 \notin D\langle 1, y_2\rangle$ then, arguing as above, we obtain $x_2 \notin D\langle 1, y_1\rangle$. Choose $z \notin D\langle 1, y_1\rangle \cup D\langle 1, y_2\rangle$, which is possible since G cannot be the union of two proper subgroups. Since $D\langle 1, x\rangle$ has index 2 in G we have $y_1y_2 \in D\langle 1, z\rangle$ and $z = D\langle 1, y_1y_2\rangle$. Then $x_2\langle 1, y_1\rangle = z\langle 1, y_1\rangle$, and $x_1\langle 1, y_2\rangle = z\langle 1, y_2\rangle$. Using $(*)$} gives

$$D(x_1y_1) + D(x_2y_2) = x_1x_2\langle y_1, y_2, z, z\rangle = D(x_1y_1x_2y_2).$$

(2) We apply (2.8):

$$\dim \mathrm{Der}(R) = \dim \mathrm{Der}(L_{2n-1}) + 2 \dim I_R$$
$$= \tfrac{1}{2}(2n + 1)(2n - 2) + 2(2n + 1) = \tfrac{1}{2}(2n + 2)(2n + 1).$$

□

3. Examples. Sections 1 and 2 can be used to compute the derivation algebra for any Witt ring of elementary type. Below we give $\dim(\mathrm{Der}(R))$ for every non-reduced Witt ring R where the associated group has order at most 8 (cf. [**5**, p. 122–124]).

$\mathbf{Z}_2$	0	$\mathbf{Z}_4 \times_w \mathbf{Z}_4 \times_w \mathbf{Z}_4$	6
$\mathbf{Z}_4$	0	$\mathbf{Z}_4 \times_w \mathbf{Z}_4[\Delta_1]$	5
$\mathbf{Z}_2[\Delta_1]$	2	$\mathbf{Z}_4 \times_w \mathbf{Z}_2[\Delta_2]$	8
$\mathbf{Z} \times_w \mathbf{Z}_4$	1	$\mathbf{Z}_2[\Delta_1] \times_w \mathbf{Z}_2[\Delta_1] \times_w \mathbf{Z}_2[\Delta_1]$	9
$\mathbf{Z}_4 \times_w \mathbf{Z}_4$	2	$\mathbf{Z}_2[\Delta_1] \times_w \mathbf{Z}_2[\Delta_2]$	10
$\mathbf{Z}_2[\Delta_1] \times_w \mathbf{Z}_2[\Delta_1]$	4	$(\mathbf{Z} \times_w \mathbf{Z}_4)[\Delta_1]$	4
$\mathbf{Z}_4[\Delta_1]$	2	$(\mathbf{Z}_4 \times_w \mathbf{Z}_4)[\Delta_1]$	8
$\mathbf{Z}_2[\Delta_2]$	8	$(\mathbf{Z}_2[\Delta_1] \times_w \mathbf{Z}_2[\Delta_1])[\Delta_1]$	14
$\mathbf{Z}[\Delta_1] \times_w \mathbf{Z}_4$	2	$\mathbf{Z}_4[\Delta_2]$	8
$\mathbf{Z} \times_w \mathbf{Z}_4 \times_w \mathbf{Z}_4$	4	$\mathbf{Z}_2[\Delta_3]$	28
$\mathbf{Z} \times_w \mathbf{Z}_4[\Delta_1]$	3	L_3	5
$\mathbf{Z} \times_w \mathbf{Z}_2[\Delta_2]$	6		

Any two reduced Witt rings have Lie isomorphic derivation algebras, namely 0 (1.4). To get a non-trivial example we consider the four Witt rings listed above with 2-dimensional derivation algebras.

PROPOSITION 3.1. (1) $(\mathrm{Der}(\mathbf{Z}_4[\Delta_1])$ *is abelian.*

(2) $\mathrm{Der}(\mathbf{Z}_2[\Delta_1])$, $\mathrm{Der}(\mathbf{Z}_4 \times_w \mathbf{Z}_4)$ *and* $\mathrm{Der}(\mathbf{Z} \times_w \mathbf{Z} \times_w \mathbf{Z}_4)$ *are non-abelian and Lie isomorphic.*

Proof. Up to isomorphism there is a unique non-abelian 2-dimensional Lie algebra [**2**, p. 11], so we need only check if the algebras are abelian or not.

$\mathbf{Z}_4[\Delta_1]$ can be realized by $W(\mathbf{Z}_3((t)))$, hence by (1.5), $\mathrm{Der}(\mathbf{Z}_4[\Delta_1])$ is generated by $d(\langle 1,1\rangle)$ and $d(t\langle 1,1\rangle)$ (where $d(w)$ sends ± 1 to 0 and $\pm t$ to w). Then

$$[d(\langle 1,1\rangle), d(t\langle 1,1\rangle)](t) = d(\langle 1,1\rangle)(t\langle 1,1\rangle) = t\langle\langle 1,1\rangle\rangle = 0.$$

So $\mathrm{Der}(\mathbf{Z}_4[\Delta_1])$ is abelian.

$\mathbf{Z}_2[\Delta_1]$ can be realized by $W(\mathbf{Z}_5)$. Let $\bar{a} = a + 5\mathbf{Z}$ for $a \in \mathbf{Z}$. Then $\mathrm{Der}(\mathbf{Z}_2[\Delta_1])$ is generated by $d(\bar{1})$ and $d(\bar{2})$ (where $d(\bar{a})$ sends $\bar{1}$ to 0 and $\bar{2}$ to $\bar{a}$). Then $[d(\bar{1}), d(\bar{2})] = d(\bar{1})$ and $\mathrm{Der}(\mathbf{Z}_2[\Delta_1])$ is non-abelian.

$\mathbf{Z}_4 \times_w \mathbf{Z}_4$ can be realized by the Witt ring of the group $G = \{\pm 1, \pm a\}$ with $D\langle 1, g\rangle = G$ for all $g \in G$. Using (1.8) we get $\mathrm{Der}(\mathbf{Z}_4 \times_w \mathbf{Z}_4)$

is generated by $d(\langle 1,1\rangle)$ and $d(\langle 1,a\rangle)$, where $d(w)$ sends ± 1 to 0 and $\pm a$ to w. Then $[d(\langle 1,1\rangle), d(\langle 1,a\rangle)] = d(\langle 1,1\rangle)$ and the algebra is non-abelian.

Lastly, $\mathbf{Z} \times_w \mathbf{Z} \times_w \mathbf{Z}_4$ can be realized by the Witt ring of the group $G = \{\pm 1, \pm a, \pm b, \pm ab\}$ with $D\langle 1,1\rangle = \{1, -ab\}$, $D\langle 1,a\rangle = \{1, a, -b, -ab\}$ and $D\langle 1,b\rangle = \{1, b, -a, -ab\}$. Using (1.8) we get $\mathrm{Der}(\mathbf{Z} \times_w \mathbf{Z} \times_w \mathbf{Z}_4)$ is generated by D_1 which sends a to $\langle 1, ab\rangle$, b to 0, and by D_2 which sends a to 0 and b to $\langle 1, ab\rangle$. Then $[D_1, D_2] = D_1 + D_2$ and the algebra is non-abelian. □

Note that the Witt rings of (3.1)(2) with Lie isomorphic derivation algebras have non-isomorphic associated groups. However, it is possible for non-isomorphic Witt rings to have isomorphic associated groups and non-trivial Lie isomorphic derivation algebras. An example is $\mathbf{Z} \times_w \mathbf{Z}_2[\Delta_2]$ and $\mathbf{Z}_4 \times_w \mathbf{Z}_4 \times_w \mathbf{Z}_4$. We sketch the computations required to verify this.

$\mathbf{Z}_4 \times_w \mathbf{Z}_4 \times_w \mathbf{Z}_4$ can be realized by the Witt ring of $G = \{\pm 1, \pm a, \pm b, \pm ab\}$, where $D\langle 1, g\rangle = G$ for all $g \in G$. The following is a basis for the derivation algebra:

$$D_1\colon a \mapsto \langle 1,1\rangle,\ b \mapsto 0, \quad D_4\colon a \mapsto 0,\ b \mapsto \langle 1,1\rangle,$$
$$D_2\colon a \mapsto \langle 1,a\rangle,\ b \mapsto 0, \quad D_5\colon a \mapsto 0,\ b \mapsto \langle 1,a\rangle,$$
$$D_3\colon a \mapsto \langle 1,b\rangle,\ b \mapsto 0, \quad D_6\colon a \mapsto \langle 1,a\rangle,\ b \mapsto \langle 1,b\rangle.$$

$\mathbf{Z} \times_w \mathbf{Z}_2[\Delta_2]$ can be realized by the Witt ring of the same G but with $D\langle 1,1\rangle = \{1, a, b, ab\}$, $D\langle 1,a\rangle = \{1, a\}$, $D\langle 1,b\rangle = \{1, b\}$ and $D\langle 1, ab\rangle = \{1, ab\}$. The following is a basis for the derivation algebra:

$$d_1\colon a \mapsto \langle\langle -a, -b\rangle\rangle,\ b \mapsto 0, \quad d_4\colon a \mapsto 0,\ b \mapsto \langle\langle -a, b\rangle\rangle,$$
$$d_2\colon a \mapsto \langle\langle -a, b\rangle\rangle,\ b \mapsto \langle 1, -b\rangle, \quad d_5\colon a \mapsto 0,\ b \mapsto b\langle 1, -a\rangle,$$
$$d_3\colon a \mapsto \langle 1, -b\rangle,\ b \mapsto 0, \quad d_6\colon a \mapsto b\langle 1, -a\rangle,\ b \mapsto \langle 1, -b\rangle.$$

The map $D_i \mapsto d_i$ gives a Lie isomorphism from $\mathrm{Der}(\mathbf{Z}_4 \times_w \mathbf{Z}_4 \times_w \mathbf{Z}_4)$ to $\mathrm{Der}\, \mathbf{Z} \times_w \mathbf{Z}_2[\Delta_2])$ as can be easily, if not quickly, checked.

We close this section with an example of a derivation which arises naturally in the theory of quadratic forms. We use the following set-up: Let F be a field of characteristic not 2, $e \in \dot{F} \setminus \dot{F}^2$ and $E = F(\sqrt{e})$. Let $\bar{}$ denote the involution on E with $\overline{a + b\sqrt{e}} = a - b\sqrt{e}$, and also the induced involution on WE. Let $s\colon E \to F$ be the F-linear functional defined by $s(1) = 0$, $s(\sqrt{e}) = 1$. We denote the Scharlau transfer of s by s_*, and the map $WF \to WE$ induced by inclusion by i_*.

LEMMA 3.2. *Let* $E = F(\sqrt{e})$ *and* $s^* = i_* s_*$: $WE \to WE$. *Then for all* $q_1, q_2 \in WE$:

$$s^*(q_1 q_2) = \bar{q}_1 s^*(q_2) + q_2 s^*(q_1).$$

Proof. We need only check this for $x, y \in \dot{E}$ since s^* is additive. Let t: $E \to F$ be the trace functional. If $z = \frac{1}{2}\sqrt{e}$ then $t(xz) = s(x)$ for all $x \in \dot{E}$. Let $t^* = i_* t_*$. By the trace formula of Scharlau-Knebusch [**4**, p. 212], $t^*(q) = q + \bar{q}$ for all $q \in WE$. We obtain:

$$\begin{aligned} \bar{y}s^*(x) + xs^*(y) &= \bar{y}t^*(xz) + xt^*(yz) \\ &= \bar{y}\langle xz, \overline{xz}\rangle + x\langle yz, \overline{yz}\rangle = \langle xyz, \overline{xyz}\rangle + x\bar{y}\langle z, \bar{z}\rangle \\ &= t^*(xyz) + x\bar{y}\langle \tfrac{1}{2}\sqrt{e}, -\tfrac{1}{2}\sqrt{e}\rangle = s^*(xy). \end{aligned}$$

□

COROLLARY 3.3. *Let* $E = F(\sqrt{e})$ *and suppose that for all* $x, y \in \dot{E}$ $N_{E/F}(y) \in D_E\langle 1, -N_{E/F}(x)\rangle$. *Then* $s^* = i_* s_*$: $WE \to WE$ *is a derivation.*

Proof. By an easy computation (cf. [**4**, p. 202]), if $x \in \dot{E}$ then $s^*(x) = z\langle 1, -N_{E/F}(x)\rangle$, for some $z \in \dot{F}$. By assumption, for all $y \in \dot{E}$, $\langle 1, -N_{E/F}(y)\rangle s^*(x) = 0$ and so $\bar{y}s^*(x) = ys^*(x)$. The result thus follows from (3.2).

EXAMPLES. We give some examples of fields F for which the condition of (3.3) is satisfied for all quadratic extensions.

(i) Finite fields. In this case binary forms represent all of $\dot{F}$.

(ii) Local fields. here either $\langle\langle -N_{E/F}(x), -N_{E/F}(y)\rangle\rangle$ is 0 in WF or $\langle\langle -e, -f\rangle\rangle$ for some $f \in \dot{F} \setminus D_F\langle 1, -e\rangle$, since WF has a unique non-trivial 2-fold Pfister form. In either case, $\langle\langle -N_{E/F}(x), -N_{E/F}(y)\rangle\rangle \otimes E = 0$ gives the condition of (3.3).

(iii) If the condition of (3.3) holds for every quadratic extension of F_1 and F_2 then it holds for every quadratic extension of the field F constructed by Kula [**3**] with $WF = WF_1 \times_w WF_2$.

4. Simple derivation algebras. We begin with a simple observation:

LEMMA 4.1. *Let* R *be a Witt ring,* $D \in \mathrm{Der}(R)$ *and suppose* $D(I_R) \subset I_R^m$, *for some* $m \geq 1$. *Then for all* $k \geq 1$, $D(I_R^k) \subset I_R^{m+k-1}$.

Proof. We use induction on k, the case $k = 1$ being trivial. Suppose $k > 1$; we need only check the value of D on k-fold Pfister forms.

$$\begin{aligned} D(\langle\langle a_1, \ldots, a_k\rangle\rangle) &= \langle 1, a_k\rangle D(\langle\langle a_1, \ldots, a_{k-1}\rangle\rangle) \\ &\quad + \langle\langle a_1, \ldots, a_{k-1}\rangle\rangle D(\langle 1, a_k\rangle). \end{aligned}$$

Now $D(\langle 1, a_k\rangle) \subset I_R^m$ and by induction $D(\langle\langle a_1, \ldots, a_{k-1}\rangle\rangle) \subset I_R^{m+k-2}$. Thus $D(\langle\langle a_1, \ldots, a_k\rangle\rangle) \in I_R^{m+k-1}$ as desired. □

The generalized Witt algebra W_n is the derivation algebra of $\mathbf{Z}_2[t_1, \ldots, t_n]/(t_1^2, \ldots, t_n^2)$ (cf. [7]). Since the Witt ring $\mathbf{Z}_2[\Delta_n]$ is isomorphic to $\mathbf{Z}_2[t_1, \ldots, t_n]/(t_1^2, \ldots, t_n^2)$ we have $W_n = \mathrm{Der}(\mathbf{Z}_2[\Delta_n])$. We will show this is the only example of a simple derivation algebra of a finitely generated Witt ring.

THEOREM 4.2. *Let R be a finitely generated Witt ring and suppose $L = \mathrm{Der}(R) \neq 0$. The following are equivalent*:

(1) *L is simple*;

(2) *L is semi-simple*;

(3) *L has no (non-zero) abelian ideals*;

(4) *$L \cong W_n$ and $R \cong \mathbf{Z}_2[\Delta_n]$, for some n.*

Proof. We need only show (3) → (4). So suppose L has no (non-zero) abelian ideals. Let G be the group associated to R. Write $R = R_0[\Delta]$, for some group Δ of exponent 2 and Witt ring R_0 which is not a group ring. Let G_0 be the group associated to R_0.

Step 1. $I_{R_0}^2$ is torsion-free.

Suppose otherwise and choose $m \geq 2$ such that $I_{R_0}^m$ is not torsion-free but $I_{R_0}^{m+1}$ is torsion-free (this is possible as R_0 is finitely generated, cf. [5, 9.4]). Note that a torsion form in $I_{R_0}^m$ is universally round. Let $J = R \cdot I_{R_0}^m$ and $I = \{D \in L \mid D(R) \subset J\}$. $I \neq 0$ by (1.3). We will obtain a contradiction by showing I is an abelian ideal.

Clearly I is closed under addition. Choose $D \in I$, $D' \in L$ and $g \in G$. By (1.5) $L = \Delta L_1 + L_2$, where $L_1 = \{D \in L \mid D(\Delta) = 0,\ D(R_0) \subset R_0\}$ and $L_2 = \{D \in L \mid D(R_0) = 0\}$. Since R_0 is not a group ring extension, (1.7) implies $D(R_0) \subset I_{R_0}$ for $D \in L_1$. Write $D' = (\sum \delta_i D_i) + D''$, with $\delta_i \in \Delta$, $D_i \in L_1$ and $D'' \in L_2$. Write $D(g) = \sum \gamma_i \varphi_i$, with $\gamma_i \in \Delta$ and $\varphi_i \in I_{R_0}^m$. We obtain:

$$[D, D'](g) = D(D'(g)) + \sum D'(\gamma_i \varphi_i)$$

$$= D(D'(g)) + \sum \varphi_i D'(\gamma_i) + \sum_i \gamma_i \left(\sum_j \delta_j D_j(\varphi_i) \right) + D''(\varphi_i).$$

Now $D(D'(g)) \in J$ since $D \in I$, $\varphi_i D'(\gamma_i) \in R \cdot I_{R_0}^m = J$, $D''(\varphi_i) = 0$ since $D'' \in L_2$ and $\gamma_i \delta_j D_j(\varphi_i) \in R \cdot I_{R_0}^m = J$ by (4.1). Hence $[D, D'] \in I$ and I is an ideal.

Lastly, we show I is abelian. If $D_1, D_2 \in I$ and $g \in D$ then

$$D_1(D_2(g)) \in D_1(R \cdot I_{R_0}^m) \subset RD_1(I_{R_0}^m) + I_{R_0}^m D_1(R) \subset R \cdot I_{R_0}^{2m-1}$$

by (4.1). Then since $m \geq 2$, (1.1) implies $D_1(D_2(g)) \subset R \cdot I_{R_0}^{2m-1} \cap R_t = 0$. Hence $[I, I] = 0$.

Step 2. $R \neq R_0$.

Suppose $R = R_0$. If I_R is torsion-free then either R is reduced or $\mathbf{Z}_2$, and in both cases $L = \mathrm{Der}(R) = 0$ by (1.4). So we may assume I_R is not torsion-free, in particular, that $D\langle 1,1\rangle \neq \{1\}$. If $x \in D\langle 1,1\rangle$ then $\langle 1, -x\rangle \in \mathrm{ur}(R)$ since $\langle 1, -x\rangle$ is torsion and I_R^2 is torsion-free by Step 1. We consider four cases. In each case we obtain a contradiction by construction of non-zero abelian ideal.

Case 1. $G \neq \{1, -1\}D\langle 1,1\rangle$ and $1 \neq -1$.

Fix a subgroup H of index 2 in G such that H contains $\{1, -1\}D\langle 1,1\rangle$. Set $I = \{d(H, \langle 1, -x\rangle) \mid x \in D\langle 1,1\rangle\}$, using the notation of (1.3). $I \neq 0$ since $D\langle 1,1\rangle \neq \{1\}$.

Now $d(H, \langle 1, -x\rangle) + d(H, \langle 1, -y\rangle) = d(H, \langle 1, -xy\rangle)$, so I is closed under addition. Let $D \in L$ and $g \in G$. Then $D(g) \in \mathrm{ann}_R\langle 1,1\rangle = I_R \cap R_t$, since $-1 \neq 1$. We can find an $e \in G$ such that $D(g) + \langle 1, -e\rangle \in I_R^2$. Then $\langle\langle 1, -e\rangle\rangle = \langle 1,1\rangle D(g) + \langle\langle 1, -e\rangle\rangle \in I_R^3$ and so $\langle\langle 1, -e\rangle\rangle = 0$. Thus $D(g) + \langle 1, -e\rangle \in I_R^2 \cap R_t = 0$, by Step 1. Hence for every $g \in G$ there exists an $e \in D\langle 1,1\rangle$ such that $D(g) = \langle 1, -e\rangle$.

We now complete the proof that I is an ideal. $[D, d(H, \langle 1, -x\rangle)](g) = D(d(H, \langle 1, -x\rangle)(g))$, since $D(g) = \langle 1, -e\rangle$ with $e \in D\langle 1,1\rangle \subset H$. In particular, $[D, d(H, \langle 1, -x\rangle)](g) = 0$ if $g \in H$. If $g \notin H$ and $D(x) = \langle 1, -y\rangle$ for some $y \in D\langle 1,1\rangle$ then $[D, d(H, \langle 1, -x\rangle)](g) = D(\langle 1, -x\rangle) = \langle 1, -y\rangle$. Hence $[D, d(H, \langle 1, -x\rangle)] = d(H, \langle 1, -y\rangle) \in I$.

Lastly, we show I is abelian. Since the image of $d(H, \langle 1, -x\rangle)$ is $\{0, \langle 1, -x\rangle\}$ and $x \in D\langle 1,1\rangle \subset H$, the composition of any two derivations in I is 0. Thus $[I, I] = 0$.

Case 2. $G = \{1, -1\}D\langle 1,1\rangle$ and $-1 \notin D\langle 1,1\rangle$.

For $g \in G$ define $D(g) = D\langle 1, -g\rangle$ if $g \in D\langle 1,1\rangle$, and $D(g) = \langle 1, g\rangle$ if $-g \in D\langle 1,1\rangle$. Note that $D(g) = D(-g)$ for all g and $D(-1) = 0$. To show $D \in L$ we need only check $D(gg') = D(g) + D(g')$ for all $g, g' \in G$, since $D(g) \in \mathrm{ur}(R)$ for all $g \in G$. Now:

$$\begin{aligned} D(g) \perp D(g') &= \langle 1, \varepsilon_1 g\rangle + \langle 1, \varepsilon_2 g'\rangle, \quad \text{for some } \varepsilon_1, \varepsilon_2 \in \{1, -1\} \\ &= \langle -\varepsilon_2 g', -\varepsilon_1\varepsilon_2 gg'\rangle + \langle 1, \varepsilon_2 g'\rangle, \quad \text{as } \langle 1, \varepsilon_1 g\rangle \in \mathrm{ur}(R) \\ &= \langle 1, -\varepsilon_1\varepsilon_2 gg'\rangle = D(gg'). \end{aligned}$$

Let $D' \in L$ and $g \in G$ be arbitrary. As in Case 1 $D'(g) = \langle 1, -x\rangle$ for some $x \in D\langle 1,1\rangle$. Then

$$[D', D](g) = D'(\langle 1, \varepsilon g\rangle) + D(\langle 1, -x\rangle) = D'(g) + D(x)$$
$$= \langle 1, -x\rangle + \langle 1, -x\rangle = 0 \quad (\text{where } \varepsilon \in \{1, -1\}).$$

Hence $\{0, D\}$ is an abelian ideal.

Case 3. $G = D\langle 1,1\rangle$ and $-1 \neq 1$.

Here we have $\langle 1,1\rangle \in \mathrm{ur}(R)$. Set $I = \{D \in L \mid D(R) \subset \{0, \langle 1,1\rangle\}\}$. $I \neq 0$ by (1.3). Since for any derivation $D' \in L$, $D'(1) = 0$, we have for $D \in I$ that $[D, D'](R) \subset D(D'(R)) \subset \{0, \langle 1,1\rangle\}$. Thus I is an ideal. Further, I is abelian since the composition of any two derivations in I is 0.

Case 4. $-1 = 1$.

Since $R = R_0$ by assumption and $I_{R_0}^2$ is torsion-free by Step 1, we have $I_R^2 = 0$ and $\mathrm{ann}_R\langle 1,1\rangle = \{\langle 1, x\rangle \mid x \in G\} \subset \mathrm{ur}(R)$. We define D: $G \to R$ by $D(x) = \langle 1, x\rangle$. Then $D(1) = 0$ and $D(xy) = \langle 1, xy\rangle = \langle 1, x\rangle + \langle 1, y\rangle = D(x) + D(y) = yD(x) + xD(y)$, since $\langle 1, x\rangle$, $\langle 1, y\rangle \in \mathrm{ur}(R)$. So D is a derivation. Further, for any $D' \in L$, $g \in G$ we have $[D, D'](g) = D(D'(g)) + D'(D(g)) = D'(g) + D'(g) = 0$ by (1.1). Thus $\{0, D\}$ is an abelian ideal.

Step 3. I_{R_0} is torsion-free.

By Step 2, $|\Delta| = 2^n$ with $n \geq 1$. Let $t_1, \ldots, t_n$ generate Δ. By (1.5), $L = \Delta L_1 + L_2$ where $L_1 = \{D \in L \mid D(\Delta) = 0,\ D(R_0) \subset R_0\}$ and $L_2 = \{D \in L \mid D(R_0) = 0\}$. Note that if $D \in L_1$ then $D(R_0) \subset I_{R_0}$ by (1.7). For $\alpha_1, \ldots, \alpha_n \in \mathrm{ann}_R\langle 1,1\rangle$ let $d(\alpha_1, \ldots, \alpha_n)$ be the derivation sending R_0 to 0 and t_i to α_i $(1 \leq i \leq n)$. Then $L_2 = \{d(\alpha_1, \ldots, \alpha_n) \mid \alpha_i \in \mathrm{ann}_R\langle 1,1\rangle\}$.

Suppose I_{R_0} is not torsion-free. Then $I_{R_0} \cap R_t \subset \mathrm{ann}_R\langle 1,1\rangle$, since $I_{R_0}^2$ is torsion-free by Step 1. Set $J = R(I_{R_0} \cap R_t)$ and $I = \{d(\alpha_1, \ldots, \alpha_n) \mid \alpha_i \in J\}$. I is closed under addition. We will obtain a contradiction by showing I is an abelian ideal.

First, if $\delta \in \Delta$, $D \in L_1$ and $d(\alpha_1, \ldots, \alpha_n) \in I$ then for $g \in G_0$ we have

$$[\delta D, d(\alpha_1, \ldots, \alpha_n)](g) = d(\alpha_1, \ldots, \alpha_n)(\delta D(g))$$
$$= D(g)d(\alpha_1, \ldots, \alpha_n)(\delta) \in I_{R_0} \cdot R(I_{R_0} \cap R_t) \subset R(I_{R_0}^2 \cap R_t) = 0.$$

And $[\delta D, d(\alpha_1, \ldots, \alpha_n)](t_i) = \delta D(\alpha_i) \in R(I_{R_0} \cap R_t) = J$. Hence $[\delta D, d(\alpha_1, \ldots, \alpha_n)] = d(\delta D(\alpha_1), \ldots, \delta D(\alpha_n)) \in I$ and $[\Delta L_1, I] \subset I$.

Next, choose $d(\beta_1, \ldots, \beta_n) \in L_2$ and $d(\alpha_1, \ldots, \alpha_n) \in I$. Write $\alpha_i = \sum_j \delta_{ij}\varphi_{ij}$, for some $\delta_{ij} \in \Delta$ and $\varphi_{ij} \in I_{R_0} \cap R_t$. Then $[d(\beta_1, \ldots, \beta_n), d(\alpha_1, \ldots, \alpha_n)]$ sends R_0 to 0 and sends t_i to

$$d(\alpha_1, \ldots, \alpha_n)(\beta_i) + d(\beta_1, \ldots, \beta_n)(\alpha_i)$$

$$= d(\alpha_1, \ldots, \alpha_n)(\beta_i) + \sum_j \varphi_{ij} d(\beta_1, \ldots, \beta_n)(\delta_{ij}).$$

Now $d(\alpha_1, \ldots, \alpha_n)(\beta_i) \in J$ and $\varphi_{ij} d(\beta_1, \ldots, \beta_n)(\delta_{ij}) \in (I_{R_0} \cap R_t) \cdot R = J$. Thus $[L_2, I] \subset I$ and so $[L, I] \subset I$.

Lastly, to show I is abelian choose $d(\alpha_1, \ldots, \alpha_n)$, $d(\beta_1, \ldots, \beta_n) \in I$. Then $d(\alpha_1, \ldots, \alpha_n) \circ d(\beta_1, \ldots, \beta_n)$ sends R_0 to 0 and t_i to $d(\alpha_1, \ldots, \alpha_n)(\beta_i)$. Write $\beta_i = \sum \delta_j \varphi_j$ with $\delta_j \in \Delta$ and $\varphi_j \in I_{R_0} \cap R_t$. Then

$$d(\alpha_1, \ldots, \alpha_n)(\beta_i) = \sum_j \varphi_j d(\alpha_1, \ldots, \alpha_n)(\delta_j)$$

$$\in (I_{R_0} \cap R_t) \cdot R(I_{R_0} \cap R_t) \subset R(I_{R_0}^2 \cap R_t) = 0.$$

Hence $[d(\alpha_1, \ldots, \alpha_n), d(\beta_1, \ldots, \beta_n)] = 0$ and $[I, I] = 0$.

We now complete the proof. We have $R = R_0[\Delta_n]$ with $n \geq 1$ and I_{R_0} torsion-free. In particular, $D\langle 1, 1\rangle = \{1\}$. Thus either R_0 is reduced or $R_0 \cong \mathbf{Z}_2$. But if R_0 is reduced so is R and $L = \mathrm{Der}(R) = 0$. So $R_0 \cong \mathbf{Z}_2$, $R \cong \mathbf{Z}_2[\Delta_n]$ and $L = \mathrm{Der}(R) \cong W_n$. □

REMARK. Manin has shown [7, p. 106] that every restricted Lie algebra can be embedded in a generalized Witt algebra. Hence if R is a finitely generated Witt ring there exists an n such that $\mathrm{Der}(R)$ embeds in $\mathrm{Der}(\mathbf{Z}_2[\Delta_n])$.

5. Integrable derivations. We follow the terminology of Matsumura [6]. If R is a commutative ring with identity then a derivation D of R into itself is *integrable* if there exists a homomorphism $E\colon R \to R[[t]]$ such that $E(r) \equiv r + tD(r) \pmod{t^2}$ for all $r \in R$. The map E is an *integral* of D. An integral E arises from a collection of maps $\underline{D} = (D_0, D_1, D_2, \ldots)$ where $D_0 = \mathrm{id}_R$, $D_1 = D$ and $E(r) = \sum_i D_i(r)t^i$ for all $r \in R$. If $\underline{D} = (1, D_1, D_2, \ldots)$ and $\underline{D}' = (1, D_1', D_2', \ldots)$ yield integrals for the derivations D and D' then:

$$\underline{DD'} = \left(1, D_1 + D_1', D_2 + D_1D_1' + D_2', \ldots, \sum_i D_i D_{n-i}', \ldots\right)$$

yields an integral for $D + D'$. Indeed the set of integrable derivations form an R-submodule of $\mathrm{Der}(R)$.

Let R be a Witt ring and let $D \in \mathrm{Der}(R)$. We say D is *I_R-integrable* if D has an integral E such that $E(r) - r \in I_R[[t]]$ for all $r \in R$. Equivalently, we require $\underline{D} = (1, D_1, D_2, \ldots)$ to give an integral of D with $D_i(R) \subset I_R$ for $i \geq 2$. The composition $\underline{DD'}$ above shows the set of I_R-integrable derivations also forms a subgroup of $\mathrm{Der}(R)$.

LEMMA 5.1. *Let R be a Witt ring and $D \in \mathrm{Der}(R)$. If $D(R)^2 = 0$ then D is I_R-integrable.*

Proof. $D(R)^2 = 0$ implies $D(R) \subset I_R$. Define E: $R \to R[[t]]$ by $E(r) = r + \sum_{i=1}^{\infty} D(r)t^i$. E is additive, $E(r) - r \in I_R[[t]]$ and for $r, s \in R$,:

$$E(r)E(s) = rs + \sum_i \left(rD(s) + \sum_{j=1}^{i-1} D(r)D(s) + sD(r) \right) t^i$$

$$= rs + \sum_i D(rs)t^i = E(rs),$$

using that $D(r)D(s) = 0$. □

LEMMA 5.2. *Let R be $\mathbf{Z}_2$, $\mathbf{Z}_4$ or an indecomposable finitely generated Witt ring of local type. Then every derivation of R is I_R-integrable.*

Proof. If R is $\mathbf{Z}_2$, $\mathbf{Z}_4$ or $\mathbf{Z}$ then $\mathrm{Der}(R) = 0$ (1.4). Suppose $R = L_{2n,1}$ or L_{2n-1} for $n \geq 2$. Then, by (2.4), $\mathrm{Der}(R)$ is generated by derivations of the form $d(H, \beta)$ (cf. (1.3)). Here $d(H, \beta)(R) = R\beta$, with $\beta \in \mathrm{ann}_R\langle 1, 1\rangle$. Hence (2.2) implies β is $y\langle 1, x\rangle$ or ρ, where $-x \in D\langle 1, 1\rangle$, $y \in G$ and ρ is the unique non-trivial 2-fold Pfister form of R. In either case $\beta^2 = 0$. So $d(H, \beta)$ is I_R-integrable by (5.1) and then every derivation of R is I_R-integrable.

Now suppose $R = L_{2n,0}$ with $n \geq 2$. Let G be the group associated to R and fix $a_0, b_0 \in G$ with $a_0 \notin D\langle 1, b_0\rangle$. Write $G = A \times B$ with $a_0 \in A$, $b_0 \in B$ and satisfying $a_1 \in D\langle 1, a_2\rangle$, $b_1 \in D\langle 1, b_2\rangle$ for all $a_1, a_2 \in A$, $b_1, b_2 \in B$. This is possible by (2.12). Define D_A on G by $D_A(ab) = b\langle 1, a\rangle$, with $a \in A$, $b \in B$. This is a derivation, as shown in the proof of (2.13). Note that $D_A(R)^2 = \{\langle\langle a_1, a_2\rangle\rangle \mid a_i \in A\} = 0$ so that D_A is I_R-integrable by (5.1).

Let $D \in \mathrm{Der}(R)$. The proof of (2.13) shows that there exists a derivation D_1 in the subgroup generated by D_A and $\{d(D\langle 1, x\rangle, y\langle 1, x\rangle) \mid y \in G,\ x \in D\langle 1, b_0\rangle\}$ such that $D_1(a_0) = D(a_0)$ and $D_1(b_0) = 0$.

Further, D_1 is I_R-integrable. Similarly, there exists I_R-integrable D_2 such that $D_2(a_0) = 0$ and $D_2(b_0) = D(b_0)$.

By replacing D by $D - D_1 - D_2$ if necessary, we see it suffices to show if $D \in L = \{D \in \mathrm{Der}(R) \mid D(a_0) = D(b_0) = 0\}$ then D is I_R-integrable. Now L is isomorphic to $\mathrm{Der}(L_{2n-1})$ by (2.11). Let γ_*: $\mathrm{Der}(L_{2n-1}) \to L$ be an isomorphism (take the inverse of the map in (2.11)). The proof of (2.11) showed that $\gamma_*(d(H,\alpha)) = d(K,\beta)$, where $d(H,\alpha)$, $d(K,\beta)$ are of the type discussed in (1.3). Thus the derivations $d(K,\beta) \in L$ generate L by (2.4). As argued above, $d(K,\beta)$ is I_R-integrable. Hence D is I_R-integrable. □

LEMMA 5.3. *Let R_0 be a (finitely generated) Witt ring and let $R = R_0[\Delta_1]$. Suppose every derivation of R_0 is I_{R_0}-integrable and $D \in \mathrm{Der}(R)$ satisfies $D(R_0) \subset I_{R_0}$. Then D is I_R-integrable.*

Proof. Let $\Delta_1 = \{1, t\}$. By (1.5) $D = D' + tD'' + D'''$, where $D', D'' \in L_1 = \{D \in \mathrm{Der}(R) \mid D(\Delta_1) = 0, \quad D(R_0) \subset R_0\}$ and $D'''(R_0) = 0$. The restriction to R_0 gives an isomorphism between L_1 and $\mathrm{Der}(R_0)$ so D' and D'' are I_R-integrable. We may thus assume $D = D'''$.

Let $w = D(t)$. By assumption, $w \in \mathrm{ann}_R\langle 1, 1\rangle \cap I_R$. For $r \in R_0$, $D(r) = 0$ and $D(rt) = rw$. If $\mathrm{char}\, R = 2$ then since $w^2 \in 2I_R = 0$, $D(R)^2 = (wR)^2 = 0$ and D is I_R-integrable by (5.1). So we may assume $\mathrm{char}\, R \neq 2$. For non-negative even integers k we dfine $w_k \in I_R$ inductively by:

(i) $w_0 = w$

(ii) If $k = 4i$ then $w_{2i} \in I_R$ and $w_{2i}^2 \in 2I_R$. Choose $w_k \in I_R$ such that:

$$-2tw_k = w_{2i}^2 + 2\left(\sum_{j=1}^{i-1} w_{2j}w_{k-2j}\right).$$

(iii) If $k = 4i + 2$ then $w_0^2 \in 2I_R$. Choose a $w_k \in I_R$ such that:

$$-2tw_k = w_0^2 + 2\left(\sum_{j=1}^{i} w_{2j}w_{k-2j}\right).$$

We note the following identities:

$$-2tw_k = \sum_{j=1}^{k/2-1} w_{2j}w_{k-2j} \qquad \text{if } k \equiv 0 \pmod 4,$$

$$-2tw_k = w_0^2 + \sum_{j=1}^{k/2} w_{2j}w_{k-2j} \qquad \text{if } k \equiv 2 \pmod 4.$$

For odd integers k, set $D_k = D$. Let $D_0 = \mathrm{id}_R$ and for even $k \geq 2$ define D_k: $R \to R$ by $D_k(r_1 + r_2 t) = r_2 w_k$, for all $r_1, r_2 \in R_0$. Note that $D_i(R) \subset I_R$ for $i \geq 1$. Define E: $R \to R[[s]]$ by $E(r) = \sum D_k(r) s^k$. To show E is the integral of D it suffices to check for all $x, y \in G$ (G the group associated to R) that:

$$(*) \qquad D_k(xy) = \sum_{i=0}^{k} D_i(x) D_{k-i}(y).$$

Suppose k is odd.Then $D_k(xy) = xD(y) + yD(x) = D_0(x)D_k(y) + D_0(y)D_k(x)$. Thus $(*)$ becomes:

$$0 = D(x)\left(\sum_{j=1}^{(k-1)/2} D_{2j}(y)\right) + D(y)\left(\sum_{j=1}^{(k-1)/2} D_{2j}(x)\right).$$

This clearly holds if x or y are in G_0, the group associated to R_0. So suppose $x = gt$, $y = g't$ for some $g, g' \in G_0$. Then:

$$\begin{aligned} &D(x)\Big(\sum D_{2j}(y)\Big) + D(y)\Big(\sum D_{2j}(x)\Big) \\ &\quad = gw_0\Big(g'\sum w_{2j}\Big) + g'w_0\Big(g\sum w_{2j}\Big) \\ &\quad = 2gg'w_0\Big(\sum w_{2j}\Big) = 0. \end{aligned}$$

Now suppose k is even. Let $\varepsilon_k = 0$ if $k \equiv 0 \pmod 4$ and $\varepsilon_k = 1$ if $k \equiv 2 \pmod 4$. Then $(*)$ becomes

$$(**) \qquad D_k(xy) = \sum_{j \text{ odd}} D_j(x) D_{k-j}(y) + \sum_{j \text{ even}} D_j(x) D_{k-j}(y)$$

$$\begin{aligned} D_k(xy) &= \varepsilon_k D(x)D(y) + xD_k(y) + yD_k(x) \\ &\quad + \sum_{j=1}^{k/2-1} D_{2j}(x) D_{k-2j}(y). \end{aligned}$$

The equation $(**)$ holds if x or y are in G_0. So suppose $x = gt$, $y = g't$ for some $g, g' \in G_0$. We want to show the right hand side of $(**)$ is 0 since $D_k(xy) = D_k(gg') = 0$. First consider the case $k \equiv 0 \pmod 4$. The right hand side of $(**)$ is:

$$\begin{aligned} gtg'w_k + g'tgw_k + \sum gw_{2j}g'w_{k-2j} &= gg'\Big(2tw_k + \sum w_{2j}w_{k-2j}\Big) \\ &= 0, \quad \text{by construction of } w_k. \end{aligned}$$

If $k \equiv 2 \pmod 4$ the right hand side of $(**)$ is:

$$\begin{aligned} &gg'w_0^2 + gtg'w_k + g'tgw_k + gg'\sum w_{2j}w_{k-2j} \\ &\quad = gg'\Big(w_0^2 + 2tw_k + \sum w_{2j}w_{k-2j}\Big) \\ &\quad = 0, \quad \text{again by construction of } w_k. \end{aligned}$$

□

LEMMA 5.4. *Let* R_1, R_2 *be (finitely generated) Witt rings and let* $R = R_1 \times_w R_2$. *Let* $L_i^* = \{D \in \mathrm{Der}(R_i) \mid D(R_i) \subset I_{R_i}\}$ *for* $i = 1, 2$. *Suppose every derivation in* L_i^* *is* I_{R_i}*-integrable* $(i = 1, 2)$. *Then every derivation of* R *is* I_R*-integrable.*

Proof. Let G_i be the group associated to R_i $(i = 1, 2)$; $G = G_1 \times G_2$ is the group associated to R. We use the notation of (1.8). If $D \in L_1$ then there exists $D' \in L_1^*$ such that for all $(g_1, g_2) \in G$, $D(g_1, g_2) = (D'(g_1), 0)$. Let $\underline{D}' = (1, D_1', D_2', \dots)$ yield an integral for D' with $D_i'(R_1) \subset I_{R_1}$ for $i \geq 2$. Define, for $i \geq 2$, D_i: $R \to R$ by $D_i(r_1, r_2) = (D_i'(r_1), 0)$. Then $\underline{D} = (1, D, D_2, \dots)$ yields an integral for D. Similarly, if $D \in L_2$ then D is I_R-integrable.

If D is in E_1, E_2 or F then $D(R) \subset \mathrm{ur}(R)$ by (1.8). Hence, $D(R)^2 = 0$ and D is I_R-integrable by (5.1). Since L_1, L_2, E_1, E_2 and F generate $\mathrm{Der}(R)$, by (1.8), we have that every derivation on R is I_R-integrable. □

THEOREM 5.5. *Let* R *be a finitely generated Witt ring of elementary type. The following are equivalent*:

(1) *There exists* $D \in \mathrm{Der}(R)$ *with* $D(I_R) \not\subset I_R$;

(2) *There exists* $D \in \mathrm{Der}(R)$ *that is not integrable*;

(3) *There exists* $D \in \mathrm{Der}(R)$ *that is not* I_R*-integrable*;

(4) R *is a group ring and* $\mathrm{char}(R) = 2$.

Proof. (1) ↔ (4) is (1.7) and (2) → (3) is clear.

(4) → (2): Write $R = R_0[\Delta_1]$ with $\Delta_1 = \{1, t\}$. There is a derivation D with $D(R_0) = 0$ and $D(t) = 1$ (cf. (1.5)). Suppose $\underline{D} = (1, D, D_2, \dots)$ yields an integral of D. Then $D_2(1) = 0$ and

$$0 = D_2(t \cdot t) = tD_2(t) + D(t)D(t) + tD_2(t)$$

$$0 = \langle 1 \rangle + 2tD_2(t),$$

which is impossible, as $2tD_2(t) \in I_R$ but $\langle -1 \rangle \notin I_R$.

(3) → (4): We use induction on $|G|$, where G is the group associated to R. By (5.2), R is not indecomposable. Suppose R is a product $R_1 \times_w R_2 \times_w \cdots \times_w R_n$, with each R_i indecomposable or a group ring. If R_i is indecomposable then every derivation on R_i is I_{R_i}-integrable. If R_i is a group ring then $R_i = S_i[\Delta]$ with S_i indecomposable or a Witt product. By induction, every derivation on S_i is I_{S_i}-integrable. Hence any derivation on R_i mapping I_{R_i} into itself is I_{R_i}-integrable (5.3). Then (5.4) implies every derivation on R is I_R-integrable, a contradiction.

We thus have that R is a group ring extension. Write $R = S[\Delta]$, with S indecomposable or a Witt product. Again induction yields that every derivation on S is I_S-integrable. If $\text{char}(R) \neq 2$ then any derivation on R maps I_R into itself (1.7). So (5.3) implies every derivation on R is I_R-integrable, contrary to our assumption. Thus R is a group ring and $\text{char}(R) = 2$. □

References

[1] A. Carson and M. Marshall, *Decomposition of Witt rings*, Canad. J. Math., **34** (6) (1982), 1276–1302.
[2] N. Jacobson, *Lie Algebras*, Dover Pub., New York, 1979.
[3] M. Kula, *Fields with prescribed quadratic form schemes*, Math. Zeit., **167** (1979), 201–212.
[4] T. Y. Lam, *The Algebraic Theory of Quadratic Forms*, W. A. Benjamin, Reading, Massachusetts, 1973.
[5] M. Marshall, *Abstract Witt Rings*, Queen's Papers in Pure and Applied Math. **57**, Queen's University, Kingston, Ontario, 1980.
[6] H. Matsumura, *Integrable derivations*, Nagoya Math. J., **87** (1982), 227–245.
[7] G. Seligman, *Modular Lie Algebras*, Springer, New York, 1967.

Received March 28, 1986.

SOUTHERN ILLINOIS UNIVERSITY
CARBONDALE, IL 62901