Can. J. Math. Vol. **45** (6), 1993 pp. 1184–1199

ABSTRACT WITT RINGS WHEN CERTAIN BINARY FORMS REPRESENT EXACTLY FOUR ELEMENTS

CRAIG M. CORDES

ABSTRACT An abstract Witt rıng (R, G) of posıtıve characterıstıc ıs known to be a group rıng $S[\Delta]$ wıth $\{1\} \neq \Delta \subseteq G$ ıf and only ıf ıt contaıns a form $\langle 1,x\rangle$, $x \neq \pm 1$, whıch represents only the two elements 1 and x Carson and Marshall have characterızed all Wıtt rıngs of characterıstıc 2 whıch contaın bınary forms representıng exactly four elements Such results whıch show R ıs ısomorphıc to a product of smaller rıngs are helpful ın settlıng the conjecture that every fınıtely generated Wıtt rıng ıs of elementary type Here, some specıal sıtuatıons are consıdered In partıcular ıf $\mathrm{char}(R) = 8$, $|D\langle 1,1\rangle| = 4$, and R contaıns no rıgıd elements, then R ıs ısomorphıc to the Wıtt rıng of the 2-adıc numbers If $\mathrm{char}(R) = 4$, $|D\langle 1,a\rangle| = 4$ where $a \in D\langle 1,1\rangle$, and R contaıns no rıgıd elements, then R ıs eıther a rıng of order 8 or ıs the specıfıed product of two Wıtt rıngs at least one of whıch ıs a group rıng In several cases R ıs realızed by a fıeld

1. **Introduction.** The quadratic form structure of a field of characteristic not two is given by its Witt ring, and this concept has been generalized by M. Marshall [8] to abstract Witt rings. Various attempts have been made to characterize abstract Witt rings, but so far their deepest structural properties remain unknown. One attack that has been used successfully both for fields and in the abstract setting is an analysis of situations in which there exist binary forms whose value sets are small. For example in [1, 2, 8] are investigations of situations where there is such a value set containing exactly two elements. In [3] Carson and Marshall characterized Witt rings of characteristic 2 for which there is an associated binary form representing at most four elements, and Marshall extended this result in [9].

Here we consider the special cases when the Witt ring R has characteristic 4 or 8 and the binary form $\langle 1, 1\rangle$ (or close to it) represents exactly four elements. The main results are listed in Theorems 2.6, 3.1, and 4.1. When $\mathrm{char}(R) = 8$, R turns out to be a group ring of the Witt ring of the 2-adic numbers and a group of exponent 2.

This is the content of Section 2. In Section 3 we assume $\langle 1, 1\rangle$ represents four elements and $\mathrm{char}(R) = 4$. It is shown that the basic part of R is either a ring of order 8 or a product of two special group rings. Finally in Section 4 the same situation as in Section 3 is considered except that the binary form is $\langle 1,a\rangle$ where $a \in D\langle 1, 1\rangle - \{\pm 1\}$. Here the situation is more complex, but the results are similar to when $a = 1$. Much of the proofs in Sections 3 and 4 follow closely the proof of Theorem 3.10 in [3].

Suppose F and K are fields in which $D\langle 1, 1\rangle = \{1, -1\}$ and $s(F) = s(K) = 2$. The product of $W(F)$ and $W(K)$ in the category of Witt rings satisfies the hypothesis of

Received by the editors February 5, 1992
AMS subject classification 11E81

© Canadian Mathematical Society 1993

https://doi.org/10.4153/CJM-1993-066-7 Published online by Cambridge University Press

Theorem 3.1, and the main result in Section 3 is that every "non-degenerate" (in the sense of the radical being 1 and there existing no rigid elements) such R, *i.e.* also satisfying the hypothesis of Theorem 3.1, is isomorphic to one of these products. Similarly the non-degenerate R in Theorem 4.1 are formed from a Witt ring T of characteristic 2 containing a rigid element x and by using the F above. Then $R \cong T \times W(F)$ where a corresponds to $(x, 1)$ in $G_T \times F^* / F^{*2}$.

The hypotheses are rather restricted here, but the proofs do not seem to generalize readily. In fact the small change in hypothesis from Section 3 to 4 demands substantially more work even though the approaches were the same. What Carson's and Marshall's work [3] and the efforts in this paper seem to indicate is that studying binary forms representing exactly four elements is complicated.

Throughout, the terminology and notation are as in [8]. In particular R is an abstract Witt ring with distinguished subgroup G (of exponent 2) of units. The associated quaternionic pairing is given by $q\colon G \times G \longrightarrow Q$, and $D\langle a_1, \ldots, a_n\rangle$ denotes the subset of G corresponding to the value set of the form $\langle a_1, \ldots, a_n\rangle$. The radical of R is $D_R = \{a \in G \mid D\langle 1, -a\rangle = G\}$. The subgroup generated by $a_i \in G$ for $i \in I$ is denoted by $\langle\{a_i\}\rangle, i \in I$.

In Sections 3 and 4, the hypotheses of the main theorems specify there are no rigid elements. This restriction does not affect the generality of the results since by Corollary 5.20 [8], such elements can always be separated out via group rings. Moreover, since it is assumed here char$(R) > 0$, we have at our disposal the well-known result that for $x \neq \pm 1$, $|D\langle 1, x\rangle| \geq 4$ if and only if $|D\langle 1, -x\rangle| \geq 4$. That is, x is basic if and only if x is not rigid.

In the following, repeated use is made of several elementary results. These appear below as lemmas. Sometimes they are referred to directly, but frequently they are tacitly assumed. Note that Lemma 1.1 is used in this paper only for $n = 2$ and 3.

LEMMA 1.1. *If $H_1, \cdots, H_n$ are subgroups of a group G and if $b \in a_1H_1 \cap \cdots \cap a_nH_n$ for some $b, a_i \in G$, then $\bigcap a_iH_i = b \bigcap H_i$, $1 \leq i \leq n$.*

LEMMA 1.2. *If H, K are subgroups of a group and if $H \cup K$ is a subgroup also, then at least one of H and K contains the other.*

LEMMA 1.3. *If H, K, L are subgroups of a group, then $HK \cap HL = H(K \cap HL)$.*

LEMMA 1.4. *If R is an abstract Witt ring and if $a, b \in G$, then $D\langle 1, a, b, ab\rangle = \bigcup D\langle 1, a\rangle D\langle 1, bc\rangle$ where c runs through $D\langle 1, a\rangle$. Also $D\langle 1, a\rangle \cap D\langle 1, b\rangle \subseteq D\langle 1, -ab\rangle$.*

2. **The case** $s = 4$. Assume in this section that R is an abstract Witt ring with $s = 4$ and $D\langle 1, 1\rangle = \{1, a, b, ab\}$ where $a, b \in G$. If we denote $\langle 1, 1, 1, 1\rangle$ by ψ, then $D(\psi) = \bigcup D\langle 1, 1\rangle D\langle 1, x\rangle$, $x \in D\langle 1, 1\rangle$. That is

$$D(\psi) = \{1, a, b, ab\}(D\langle 1, a\rangle \cup D\langle 1, b\rangle \cup D\langle 1, ab\rangle).$$

Also

$$D\langle 1, 1, 1\rangle = \bigcup D\langle 1, x\rangle, \quad x \in D\langle 1, 1\rangle;$$

https://doi.org/10.4153/CJM-1993-066-7 Published online by Cambridge University Press

and so

$$D\langle 1,1,1\rangle = D\langle 1,a\rangle \cup D\langle 1,b\rangle \cup D\langle 1,ab\rangle.$$

Since $s=4, -1 \in D(\psi)-D\langle 1,1,1\rangle \subseteq bD\langle 1,a\rangle \cup aD\langle 1,b\rangle \cup aD\langle 1,ab\rangle$. It is straightforward to check that -1 is in any one of these 3 sets if and only if it is in all of them. Thus, $-b \in D\langle 1,a\rangle$, $-a \in D\langle 1,b\rangle$, and $-a \in D\langle 1,ab\rangle$. Note that $b \notin D\langle 1,a\rangle$ for otherwise $-1 \in D\langle 1,a\rangle$ which implies $-a \in D\langle 1,1\rangle$, and so $-1 \in D\langle 1,1\rangle$. Contradiction to $s=4$. Summarizing the above and similar results, we have

PROPOSITION 2.1. *With notation as above, the following hold:*

$$a,-b \in D\langle 1,a\rangle\ ; \quad -a,b \in D\langle 1,b\rangle\ ; \quad -a,-b \in D\langle 1,ab\rangle$$
$$-1,b \notin D\langle 1,a\rangle\ ; \quad -1,a \notin D\langle 1,b\rangle\ ; \quad -1,a,b \notin D\langle 1,ab\rangle.$$

By Lemma 1.4, $D\langle 1,a\rangle \cap D\langle 1,-a\rangle \subseteq D\langle 1,1\rangle = \{1,a,b,ab\}$. But $b \notin D\langle 1,a\rangle$ then shows $D\langle 1,a\rangle \cap D\langle 1,-a\rangle = \{1,a\}$. In a like fashion, we obtain the other two equalities in

PROPOSITION 2.2. *With notation as above, the following hold:* $D\langle 1,a\rangle \cap D\langle 1,-a\rangle = \{1,a\}$, $D\langle 1,b\rangle \cap D\langle 1,-b\rangle = \{1,b\}$, *and* $D\langle 1,ab\rangle \cap D\langle 1,-ab\rangle = \{1,ab\}$.

Also from Proposition 2.1 we have that $\{1,a,b,ab\}D\langle 1,x\rangle = \pm D\langle 1,x\rangle$ for each of $x=a,b,ab$. Thus

PROPOSITION 2.3. *With notation as above,*

$$D(\psi) = \pm(D\langle 1,a\rangle \cup D\langle 1,b\rangle \cup D\langle 1,ab\rangle) = \pm D\langle 1,1,1\rangle.$$

By Lemma 1.4 and Proposition 2.2,

$$D\langle 1,a\rangle \cap D\langle 1,b\rangle \cap D\langle 1,ab\rangle \subseteq D\langle 1,-ab\rangle \cap D\langle 1,ab\rangle = \{1,ab\}.$$

But also

$$D\langle 1,a\rangle \cap D\langle 1,b\rangle \cap D\langle 1,ab\rangle \subseteq D\langle 1,a\rangle \cap D\langle 1,-a\rangle = \{1,a\}.$$

Hence, we obtain

PROPOSITION 2.4. *With notation as above,*

$$D\langle 1,a\rangle \cap D\langle 1,b\rangle \cap D\langle 1,ab\rangle = \{1\}.$$

THEOREM 2.5. *If R is a Witt ring as above, then* $D\langle 1,a\rangle = \langle\{a,-b\}\rangle$, $D\langle 1,b\rangle = \langle\{-a,b\}\rangle$, $D\langle 1,ab\rangle = \langle\{-a,-b\}\rangle$, $D\langle 1,-a\rangle = \langle\{-1,a\}\rangle$, $D\langle 1,-b\rangle = \langle\{-1,b\}\rangle$, $D\langle 1,-ab\rangle = \langle\{-1,ab\}\rangle$, *and* $D\langle 1,1,1,1\rangle = \langle\{-1,a,b\}\rangle$.

PROOF. The proof will be given in four steps.

https://doi.org/10.4153/CJM-1993-066-7 Published online by Cambridge University Press

STEP 1. Choose

$$c \in D\langle 1,a\rangle \cap D\langle 1,b\rangle - \{1\},$$
$$d \in D\langle 1,a\rangle \cap D\langle 1,ab\rangle - \{1\},$$
$$e \in D\langle 1,b\rangle \cap D\langle 1,ab\rangle - \{1\}.$$

This can always be done as $c = -ab, d = -b$, and $e = -a$ show. Clearly $cde \in D(\psi)$, and also $cde \notin D\langle 1,a\rangle \cup D\langle 1,b\rangle \cup D\langle 1,ab\rangle = D\langle 1,1,1\rangle$. Hence, $cde \in -D\langle 1,1,1\rangle$ by Proposition 2.3.

Suppose $cde \in -D\langle 1,a\rangle$. Then $e \in -D\langle 1,a\rangle$, and so

$$e \in D\langle 1,b\rangle \cap D\langle 1,ab\rangle \cap -D\langle 1,a\rangle = -a(D\langle 1,b\rangle \cap D\langle 1,ab\rangle \cap D\langle 1,a\rangle) = \{-a\}.$$

Similarly cde lying in $-D\langle 1,b\rangle$ or $-D\langle 1,ab\rangle$ yields $d = -b$ and $c = -ab$ respectively. Thus, at least one of the following must hold:

$$D\langle 1,a\rangle \cap D\langle 1,b\rangle = \{1,-ab\},$$
$$D\langle 1,a\rangle \cap D\langle 1,ab\rangle = \{1,-b\},$$
$$D\langle 1,b\rangle \cap D\langle 1,ab\rangle = \{1,-a\}.$$

Without loss of generality, assume $D\langle 1,a\rangle \cap D\langle 1,b\rangle = \{1,-ab\}$.

Now consider $x \in D\langle 1,a\rangle - D\langle 1,b\rangle$ and $y \in D\langle 1,b\rangle - D\langle 1,a\rangle$. This is possible as $x = a$ and $y = b$ illustrate. Again $xy \in D(\psi)$, but $xy \notin D\langle 1,a\rangle \cup D\langle 1,b\rangle$. Could $xy \in -D\langle 1,a\rangle$? If so, then $y \in D\langle 1,b\rangle \cap -D\langle 1,a\rangle = -a(D\langle 1,b\rangle \cap D\langle 1,a\rangle) = \{-a,b\}$. Similarly $xy \in -D\langle 1,b\rangle$ implies $x \in \{a,-b\}$. Consequently, if there are $x \in D\langle 1,a\rangle - \langle\{-a,b\}\rangle$ and $y \in D\langle 1,b\rangle - \langle\{a,-b\}\rangle$, then $xy \in \pm D\langle 1,ab\rangle$.

CLAIM. Suppose $D\langle 1,a\rangle \cap D\langle 1,b\rangle = \{1,-ab\}$ and $|D\langle 1,a\rangle|$ and $|D\langle 1,b\rangle|$ are at least 8. Then $\pm D\langle 1,a\rangle \subseteq \pm D\langle 1,ab\rangle$ if and only if $\pm D\langle 1,b\rangle \subseteq \pm D\langle 1,ab\rangle$.

If $\pm D\langle 1,a\rangle \subseteq \pm D\langle 1,ab\rangle$, then $D(\psi) = \pm D\langle 1,b\rangle \cup \pm D\langle 1,ab\rangle$. Hence, $\pm D\langle 1,b\rangle \subseteq \pm D\langle 1,ab\rangle$ or $\pm D\langle 1,ab\rangle \subseteq \pm D\langle 1,b\rangle$. If the latter holds, then $D\langle 1,a\rangle = D\langle 1,a\rangle \cap D(\psi) = D\langle 1,a\rangle \cap \pm D\langle 1,b\rangle = \{1,-b\}(D\langle 1,a\rangle \cap D\langle 1,b\rangle) = \{1,a,-b,-ab\}$. Contradiction to $|D\langle 1,a\rangle| \geq 8$. So $\pm D\langle 1,b\rangle \subseteq \pm D\langle 1,ab\rangle$ must be the case. The other direction follows in exactly the same way, and the Claim is established.

STEP 2. Suppose that $|D\langle 1,b\rangle| \geq 8$ and also that $|D\langle 1,a\rangle| \geq 16$. Choose any $z \in D\langle 1,a\rangle - \langle\{a,-b\}\rangle$. Then let $x \in D\langle 1,a\rangle - \langle\{a,-b,z\}\rangle$ and set $x' = xz$. If $y \in D\langle 1,b\rangle - D\langle 1,a\rangle$, then by Step 1 we have $xy, x'y \in \pm D\langle 1,ab\rangle$. So $z = (xy)(x'y) \in \pm D\langle 1,ab\rangle$. Since $\langle\{a,-b\}\rangle \subseteq \pm D\langle 1,ab\rangle$, the above then yields $D\langle 1,a\rangle \subseteq \pm D\langle 1,ab\rangle$. By the Claim, it follows that

$$D(\psi) = \pm D\langle 1,ab\rangle.$$

Now $-a \in D\langle 1,b\rangle \subseteq D\langle 1,1,1\rangle$ shows $D\langle 1,-a\rangle \subseteq D(\psi)$. Similarly $D\langle 1,-b\rangle$, $D\langle 1,-ab\rangle \subseteq D(\psi)$.

https://doi.org/10.4153/CJM-1993-066-7 Published online by Cambridge University Press

Hence

$$D\langle 1,-a\rangle = D\langle 1,-a\rangle \cap \pm D\langle 1,ab\rangle = \{1,-1\}(D\langle 1,-a\rangle \cap D\langle 1,ab\rangle) \subseteq \pm D\langle 1,b\rangle$$

Similarly $D\langle 1,-b\rangle \subseteq \pm D\langle 1,a\rangle$ and $D\langle 1,-ab\rangle \subseteq \pm D\langle 1,1\rangle$ The last inequality yields more though because $D\langle 1,1\rangle = \{1,a,b,ab\}$ In fact since $-1, ab \in D\langle 1,-ab\rangle$ and $-a \notin D\langle 1,-ab\rangle$ (see Propositions 2 1 and 2 2), we must have $D\langle 1,-ab\rangle = \{1,-1,ab,-ab\}$

$D(\psi)$ can be computed again but in a slightly different manner Since $\langle 1,1,1,1\rangle \cong \langle 1,-ab,a,-b\rangle$, $D(\psi) = \cup D\langle 1,-ab\rangle D\langle 1,ax\rangle$, $x \in D\langle 1,-ab\rangle$ So

$$D(\psi) = \pm\{1,ab\}(D\langle 1,a\rangle \cup D\langle 1,-a\rangle \cup D\langle 1,b\rangle \cup D\langle 1,-b\rangle)$$

But

$$abD\langle 1,a\rangle = -D\langle 1,a\rangle \text{ and } abD\langle 1,b\rangle = -D\langle 1,b\rangle,$$

and by the last paragraph

$$abD\langle 1,-a\rangle \subseteq \pm abD\langle 1,b\rangle = \pm D\langle 1,b\rangle \text{ and } abD\langle 1,-b\rangle \subseteq \pm D\langle 1,a\rangle$$

Consequently, $D(\psi) = \pm D\langle 1,a\rangle \cup \pm D\langle 1,b\rangle$, and so $\pm D\langle 1,a\rangle \subseteq \pm D\langle 1,b\rangle$ or $\pm D\langle 1,b\rangle \subseteq \pm D\langle 1,a\rangle$ Both possibilities yield contradictions to $|D\langle 1,a\rangle|$ and $|D\langle 1,b\rangle| \geq 8$ just as in the proof of the Claim

The above shows it is impossible for $|D\langle 1,a\rangle| \geq 16$ and $|D\langle 1,b\rangle| \geq 8$ Similarly the situation $|D\langle 1,a\rangle| \geq 8$ and $|D\langle 1,b\rangle| \geq 16$ cannot occur

STEP 3 Assume now that $|D\langle 1,a\rangle| = |D\langle 1,b\rangle| = 8$ Then there are c,d such that $D\langle 1,a\rangle = \langle\{a,-b,c\}\rangle$ and $D\langle 1,b\rangle = \langle\{-a,b,d\}\rangle$ Note that $c \notin \langle\{-1,a,b\}\rangle$ for otherwise, $D\langle 1,a\rangle = \langle\{-1,a,b\}\rangle$ which contradicts Proposition 2 1 Also $d \notin \langle\{-1,a,b,c,\}\rangle$ or else $D\langle 1,b\rangle \subseteq \pm D\langle 1,a\rangle$ As has been seen before, this yields $|D\langle 1,b\rangle| = 4$ which is a contradiction Thus, $-1,a,b,c,d$ are independent in G

It follows that

$$D(\psi) = \langle\{-1,a,b,c,d\}\rangle \cup \pm D\langle 1,ab\rangle$$

So

$$\langle\{-1,a,b,c,d\}\rangle \subseteq \pm D\langle 1,ab\rangle$$

or

$$\pm D\langle 1,ab\rangle \subseteq \langle\{-1,a,b,c,d\}\rangle$$

If $c \in \pm D\langle 1,ab\rangle$, then $D\langle 1,a\rangle \subseteq \pm D\langle 1,ab\rangle$, and by the Claim, $D\langle 1,b\rangle \subseteq \pm D\langle 1,ab\rangle$ A contradiction is reached as in Step 2 Hence, it must be the case that $c \notin \pm D\langle 1,ab\rangle$, and so

$$\pm D\langle 1,ab\rangle \subseteq \langle\{-1,a,b,c,d\}\rangle = D(\psi)$$

Moreover, $cd \notin \pm D\langle 1,a\rangle \cup \pm D\langle 1,b\rangle$ implies $cd \in \pm D\langle 1,ab\rangle$ So $-a,-b,\delta cd \in D\langle 1,ab\rangle$ where δ is either 1 or -1, and also $\{-1,c,-c\} \cap D\langle 1,ab\rangle = \phi$ Therefore,

$$D\langle 1,ab\rangle = \langle\{-a,-b,\delta cd\}\rangle$$

https://doi.org/10.4153/CJM-1993-066-7 Published online by Cambridge University Press

As was shown in Step 2, $D\langle 1,-a\rangle \subseteq D(\psi)$. Also $D\langle 1,-a\rangle \cap D\langle 1,a\rangle = \{1,a\}$ from Proposition 2.2. But since $D\langle 1,a\rangle = \langle\{a,-b,c\}\rangle$, this means $D\langle 1,-a\rangle \cap \langle\{-b,c\}\rangle = \{1\}$.

In addition $D\langle 1,b\rangle \cap D\langle 1,ab\rangle = \langle\{-a,b,d\}\rangle \cap \langle\{a,-b,\delta cd\}\rangle = \{1,-ab\}$. From Lemma 1.4, $D\langle 1,b\rangle \cap D\langle 1,ab\rangle = D\langle 1,-a\rangle \cap D\langle 1,b\rangle = D\langle 1,-a\rangle \cap D\langle 1,ab\rangle$.

Consequently,

$$D\langle 1,-a\rangle \cap \langle\{b,d\}\rangle = \{1\}$$

and

$$D\langle 1,-a\rangle \cap \langle\{-b,\delta cd\}\rangle = \{1\}.$$

Since $\langle\{-1,a\}\rangle \subseteq D\langle 1,-a\rangle$, the above shows $D\langle 1,-a\rangle \cap \langle\{b,c,d\}\rangle = \{1\}$; and so $D\langle 1,-a\rangle = \langle\{-1,a\}\rangle$. Using the same technique, we can show $D\langle 1,-b\rangle = \langle\{-1,b\}\rangle$ and $D\langle 1,-ab\rangle = \langle\{-1,ab\}\rangle$.

Since $c \in D\langle 1,a\rangle$, $-ac \in D\langle -a,-1\rangle$. So $-ac \in D\langle -a,-ab,1\rangle$ because $-1 \in D\langle -ab,1\rangle$ (see 2.10 in [8]). However,

$$\begin{aligned} D\langle -a,-ab,1\rangle = D\langle -ab,-a,1\rangle &= \bigcup D\langle -ab,x\rangle, \\ x \in D\langle -a,1\rangle &= \{1,-1,a,-a\}. \end{aligned}$$

So

$$\begin{aligned} D\langle -ab,-a,1\rangle &= D\langle -ab,1\rangle \cup D\langle -ab,-1\rangle \cup D\langle -ab,a\rangle \cup D\langle -ab,-a\rangle \\ &= D\langle 1,-ab\rangle \cup -D\langle 1,ab\rangle \cup aD\langle 1,-b\rangle \cup -aD\langle 1,b\rangle \\ &= \{\pm 1,\pm ab\} \cup -\langle\{-a,-b,\delta cd\}\rangle \cup a\{\pm 1,\pm b\} \cup \langle\{-a,b,d\}\rangle. \end{aligned}$$

Clearly $-ac \notin D\langle -ab,-a,1\rangle$. Contradiction. Thus, it is false to assume $|D\langle 1,a\rangle| = |D\langle 1,b\rangle| = 8$.

STEP 4. We know now that at least one of $|D\langle 1,a\rangle|$ and $D|\langle 1,b\rangle|$ must be 4. Without loss of generality assume $|D\langle 1,a\rangle| = 4$, *i.e.* $D\langle 1,a\rangle = \{1,a,-b,-ab\}$. From Proposition 2.3, it then follows that

$$D(\psi) = \pm D\langle 1,b\rangle \cup \pm D\langle 1,ab\rangle.$$

So

$$\pm D\langle 1,b\rangle \subseteq \pm D\langle 1,ab\rangle \text{ or } \pm D\langle 1,ab\rangle \subseteq \pm D\langle 1,b\rangle.$$

Suppose that the former is true. Then

$$D(\psi) = \pm D\langle 1,ab\rangle,$$

and

$$\begin{aligned} D\langle 1,-b\rangle = D\langle 1,-b\rangle \cap \pm D\langle 1,ab\rangle &= \{1,b\}(D\langle 1,-b\rangle \cap D\langle 1,ab\rangle) \\ &\subseteq \{1,b\}D\langle 1,a\rangle = \langle\{-1,a,b\}\rangle. \end{aligned}$$

https://doi.org/10.4153/CJM-1993-066-7 Published online by Cambridge University Press

But $-1, b \in D\langle 1,-b\rangle$ and $-a \notin D\langle 1,-b\rangle$ (or else $b \in D\langle 1,a\rangle$) then yıeld $D\langle 1,-b\rangle = \{1,-1,b,-b\}$ Sımılarly begınnıng wıth $D\langle 1,-ab\rangle = D\langle 1,-ab\rangle \cap \pm D\langle 1,ab\rangle$ gıves $D\langle 1,-ab\rangle = \{1,-1,ab,-ab\}$

$D\langle 1,-b\rangle$ and $D\langle 1,-ab\rangle$ turn out to be the same subgroups calculated basıcally the same way, ıf ınstead we assume $\pm D\langle 1,ab\rangle \subseteq \pm D\langle 1,b\rangle$ To complete the proof, we must compute $D\langle 1,-a\rangle$, $D\langle 1,b\rangle$, and $D\langle 1,ab\rangle$

Sınce $\psi \cong \langle 1,a,1,a\rangle$, $D(\psi) = \bigcup D\langle 1,a\rangle D\langle 1,ax\rangle$, $x \in D\langle 1,a\rangle$ Thus,

$$D(\psi) = \{1,a,-b,-ab\}(D\langle 1,a\rangle \cup D\langle 1,1\rangle \cup D\langle 1,-ab\rangle \cup D\langle 1,-b\rangle) = \langle\{-1,a,b\}\rangle$$

From Proposıtıon 2 1 and from the fact that $D\langle 1,-a\rangle$, $D\langle 1,b\rangle$ and $D\langle 1,ab\rangle$ all lıe ın $D(\psi)$, we obtaın

$$D\langle 1,-a\rangle = \{1,-1,a,-a\},$$
$$D\langle 1,b\rangle = \{1,-a,b,-ab\},$$

and

$$D\langle 1,ab\rangle = \{1,-a,-b,ab\}$$ ■

After successfully calculatıng the value sets, $D\langle 1,x\rangle$, for $x \in D\langle 1,1,1,1\rangle$, we are ın a posıtıon to characterıze all Wıtt rıngs satısfyıng $|D\langle 1,1\rangle| = 4$ and $4 \leq s < \infty$ It ıs known that every abstract Wıtt rıng ıs a quadratıc form scheme (see [7]) From Theorem 3 5 [10], ıt ıs seen that $|D\langle 1,1\rangle| \geq s$ So the above condıtıons ımply $s = 4$ It ıs ınterestıng to note that all these rıngs are realızed as Wıtt rıngs of fıelds

THEOREM 2 6 *Let R be an abstract Wıtt rıng satısfyıng* $s = 4$ *and* $|D\langle 1,1\rangle| = 4$ *Then R ıs ısomorphıc ın the category of Wıtt rıngs to a group rıng* $S[\Delta]$ *where S ıs the Wıtt rıng of the* 2-*adıc numbers and* Δ *ıs a group of exponent* 2

PROOF Suppose $D\langle 1,1\rangle = \{1,a,b,ab\}$ By Corollary 2 6 of [3], the basıc part B of R ıs gıven by $B = \pm X_1X_3 \cup X_1X_2^2$ where we can choose $X_1 = D\langle 1,1\rangle$, and

$$X_i = \bigcup\{D\langle 1,-x\rangle \mid x \in X_{i\ 1} - \{1\}\}$$

for $i = 2,3$

Thus $X_2 = D\langle 1,-a\rangle \cup D\langle 1,-b\rangle \cup D\langle 1,-ab\rangle$ whıch ıs equal to $\langle\{-1,a,b\}\rangle$ by Theorem 2 5 It also follows from Theorem 2 5 that $X_3 = \langle\{-1,a,b\}\rangle$, and so $B = \langle\{-1,a,b\}\rangle = D\langle 1,1,1,1\rangle$ It ıs straıghtforward to see that the Wıtt rıng assocıated wıth B ıs ısomorphıc to the Wıtt rıng of the 2-adıc numbers The result now follows from Theorem 5 19 and Corollary 5 20 of [8] ■

Note that Theorem 2 6 gıves a new characterızatıon of fıelds whıch are quadratıcally equıvalent (see [4]) to the 2-adıc numbers

COROLLARY 2 7 *A fıeld F ıs equıvalent wıth respect to quadratıc forms to the 2 adıc numbers ıf and only ıf F contaıns no rıgıd elements,* $|\langle D1,1\rangle| = 4$ *and* $4 \leq s < \infty$

3. **The first case for s = 2.** *In this section the Witt ring R satisfies the properties that $s = 2$ and $|D\langle 1,1\rangle| = 4$. Assume throughout that $D\langle 1,1\rangle = \{1,-1,a,-a\}$.*

Let us consider first the situation where the radical D_R of R is not 1, *i.e.* R is degenerate. If $D_R \neq 1$, then there are two possibilities: (1) $D_R = G$ and (2) $D_R \neq G$. In case (1) $-1 \in D_R$ implies $|G| = 4 = |D\langle 1,1\rangle|$; and it is easy to see R is isomorphic to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ in the category of Witt rings, *i.e.* the Witt ring of a field with $s = 2 = u$ and $q = 4$. In case (2) we must have $-1 \notin D_R$. For otherwise R would satisfy the properties that $|G_R| = 4$ and also $D_R = \{1,-1\} \subseteq G = \{1,-1,a,-a\}$. Thus $-1 \in D\langle 1,a\rangle$ implies $D\langle 1,a\rangle = G$ which contradicts $D_R \neq G$.

Since we are assuming $D_R \neq G$, it follows that $|D\langle 1,x\rangle| \geq 2|D_R|$ for all $x \in G$ in exactly the same way the corresponding result for fields was proved [5, Theorem 1]. Applying this result to $x = 1$ shows $|D_R| = 2$. So in case (2) we have that

$$D\langle 1,1\rangle = D_R \cup -D_R.$$

Let H be any subgroup of G containing -1 such that $G = D_R \times H$. Then by Theorem 5.8 [8], there are Witt rings S and T in R with G_S and G_T corresponding to D_R and H respectively such that $R \cong S \times T$. Moreover, it is clear that $S \cong \mathbb{Z}/2\mathbb{Z}[x]$. Also it must be true that $D_T\langle 1,1\rangle = \{1,-1\}$. By Corollary 2.8 [3], $T \cong \mathbb{Z}/4\mathbb{Z}[G_T/\{\pm 1\}]$, *i.e* T is isomorphic to the Witt ring of an iterated power series field over a finite field of 3 elements. Note that $S \times T$ is the same up to isomorphism regardless of whether $S \cong \mathbb{Z}/2\mathbb{Z}[x]$ or $S \cong \mathbb{Z}/4\mathbb{Z}$ (see Lemma 5.11 [8]).

Now we are in a position to characterize Witt rings R satisfying $\text{char}(R) = 4$ and $D\langle 1,1\rangle = \{1,-1,a,-a\}$. Much of the argument follows Carson's and Marshall's proof of Theorem 3.10 [3] where they consider the case $\text{char}(R) = 2$. We assume G contains no rigid elements because such R can always be "shrunk" to this case (see Corollary 5.20 [8]). In the theorem below, cases (1) and (2) occur when $D_R \neq 1$; and their proof is above. Case (3) reflects what happens when the radical is 1, and it is this situation that demands the most work to prove.

THEOREM 3.1. *Suppose* $\text{char}(R) = 4$ *and G_R contains no rigid elements. Then* $|D\langle 1,1\rangle| = 4$ *if and only if R is isomorphic to one of the following Witt rings:*

(1) the Witt ring of a field F satisfying $s(F) = u(F) = 2$ and $q(F) \equiv |F^*/F^{*2}| = 4$,

(2) the product in the category of Witt rings of either $\mathbb{Z}/2\mathbb{Z}[x]$ or $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}[\Delta]$ where Δ is a group of exponent 2, or

(3) the product of $\mathbb{Z}/4\mathbb{Z}[\Delta_1]$ and $\mathbb{Z}/4\mathbb{Z}[\Delta_2]$ where Δ_1 and Δ_2 are groups of exponent 2.

PROOF. From the above we may assume $D_R = 1$. $D\langle 1,1\rangle = \{\pm 1, \pm a\}$ implies that $D\langle 1,a\rangle \cap D\langle 1,-a\rangle = D\langle 1,1\rangle$. Since $D_R = \{1\}$, Lemma 1.2 shows $D\langle 1,a\rangle \cup D\langle 1,-a\rangle \neq G$. The bulk of Carson's and Marshall's proof of Theorem 3.10 [3] consists of 5 major claims. The first 4 of those apply to the proof here with slightly amended statements, but their verifications are identical to those in [3] after the adjustments. Consequently, only the statements themselves along with some useful clarifications will be provided.

https://doi.org/10.4153/CJM-1993-066-7 Published online by Cambridge University Press

CLAIM 1. If $t \in G$, then $D\langle 1,t\rangle \cap D\langle 1,1\rangle D\langle 1,at\rangle = \{1,t\}(D\langle 1,t\rangle \cap D\langle 1,-a\rangle)$.

We will want to consider henceforth only $t \in G-(D\langle 1,a\rangle \cup D\langle 1,-a\rangle)$. Note these t are precisely those for which $D\langle 1,1\rangle \cap D\langle 1,-t\rangle = \{1\}$.

CLAIM 2. If $t \notin D\langle 1,a\rangle \cup D\langle 1,-a\rangle$, then

$$D\langle 1,t\rangle \cap D\langle 1,1\rangle D\langle 1,-t\rangle = \{1,t\} \text{ or } \{1,t,u,tu\}$$

where $u \in D\langle 1,a\rangle$ and $tu \in D\langle 1,-a\rangle$.

The proof of this claim is broken down into two cases, one where $v=-1$ and one where $v \neq -1$. Following [3], the v comes from $D\langle 1,1\rangle$.

If $T = D\langle 1,1\rangle D\langle 1,t\rangle \cap D\langle 1,1\rangle D\langle 1,-t\rangle$, then by Lemma 1.3, $T = D\langle 1,1\rangle(D\langle 1,t\rangle \cap D\langle 1,1\rangle D\langle 1,-t\rangle)$. So by Claim 2, $T = D\langle 1,1\rangle\{1,t\}$ or $D\langle 1,1\rangle\{1,t,u,tu\}$. Continuing as in [3], we see that

$$T = D\langle 1,1\rangle D\langle 1,t\rangle \cap D\langle 1,1\rangle D\langle 1,-t\rangle = D\langle 1,1\rangle D\langle 1,at\rangle \cap D\langle 1,1\rangle D\langle 1,-at\rangle.$$

Consider $\rho = \langle 1,1\rangle \otimes \langle 1,t\rangle$. Then

$$D(\rho) = \bigcup D\langle 1,1\rangle D\langle 1,xt\rangle, \quad x \in D\langle 1,1\rangle.$$

CLAIM 3. One of the groups $D\langle 1,1\rangle D\langle 1,xt\rangle$, for $x \in D\langle 1,1\rangle$, is equal to T.

Again paralleling Carson and Marshall, we may assume $H_t \cap H_{at} \neq 1$ where H_{xt} is defined to be $D\langle 1,1\rangle D\langle 1,xt\rangle/T$. There arise two cases in the proof to consider: $e=1$ or a and $e=-1$ or $-a$ (see [3]).

CLAIM 4. There exists $x \in D\langle 1,1\rangle$ such that $|D\langle 1,xt\rangle| = 4$; and for any such x, $D\langle 1,xt\rangle = \{1,xt,u,xtu\}$ where $u \in D\langle 1,a\rangle$ and $xtu \in D\langle 1,-a\rangle$. Moreover,

$$D\langle 1,a\rangle D\langle 1,-a\rangle = G.$$

It is shown in [3] that for the x in Claim 3, $|D\langle 1,xt\rangle| \leq 4$. Equality holds since by assumption G contain no rigid elements. The remainder of this claim follows by noting that $D\langle 1,xt\rangle \subseteq T \subseteq D\langle 1,1\rangle D\langle 1,-xt\rangle$ and by applying Claim 2 with t replaced by xt.

Let $\{u_\iota \mid i \in I\}$ and $\{v_k \mid k \in K\}$ be bases of $D\langle 1,a\rangle$ and $D\langle 1,-a\rangle$ modulo $D\langle 1,1\rangle$ respectively. Then $u_\iota v_k \notin D\langle 1,a\rangle \cup D\langle 1,-a\rangle$ for all $i \in I, k \in K$. Multiplying $u_\iota v_k$ by a suitable element of $D\langle 1,1\rangle$ and applying Claim 4 shows there exist $u_{\iota k} \in D\langle 1,a\rangle$, $v_{\iota k} \in D\langle 1,-a\rangle$ such that $D\langle 1,u_{\iota k}v_{\iota k}\rangle = \{1,u_{\iota k},v_{\iota k},u_{\iota k}v_{\iota k}\}$ with $u_\iota v_k \equiv u_{\iota k}v_{\iota k} \pmod{D\langle 1,1\rangle}$. From this it follows that $v_{\iota k} \equiv v_k \pmod{D\langle 1,1\rangle}$ and $u_{\iota k} \equiv u_\iota \pmod{D\langle 1,1\rangle}$.

Although the amended Claim 5 of [3] is true (it will be our Claim 6), the proof does not work. First we need an intermediate step.

CLAIM 5. Suppose $D\langle 1,xy\rangle = \{1,x,y,xy\}$ where $x \in D\langle 1,a\rangle - D\langle 1,1\rangle$ and $y \in D\langle 1,-a\rangle - D\langle 1,1\rangle$. Then $D\langle 1,x\rangle = \{1,x,-a,-ax\}$ and $D\langle 1,y\rangle = \{1,y,a,ay\}$.

Since $-1 \in D\langle 1,a\rangle \cap D\langle 1,-a\rangle$, the assumptions imply

$$(3.2) \qquad -a \in D\langle 1,x\rangle \text{ and } a \in D\langle 1,y\rangle.$$

Consider $\varphi = \langle 1, xy, 1, xy\rangle$. $D(\varphi) = \bigcup D\langle 1, xy\rangle D\langle 1, z\rangle$, $z \in D\langle 1, xy\rangle$. Thus $D(\varphi) = D\langle 1, xy\rangle(D\langle 1,1\rangle \cup D\langle 1,x\rangle \cup D\langle 1,y\rangle \cup D\langle 1,xy\rangle)$.

By (3.2)

$$\pm aD\langle 1,xy\rangle \subseteq D\langle 1,xy\rangle(D\langle 1,x\rangle \cup D\langle 1,y\rangle),$$

and so

$$D(\varphi) = -D\langle 1,xy\rangle \cup D\langle 1,xy\rangle(D\langle 1,x\rangle \cup D\langle 1,y\rangle).$$

Note that $-y \notin D\langle 1,x\rangle$ for otherwise $-xy \in D\langle 1,x\rangle$, and then $-x \in D\langle 1,xy\rangle$ which implies $-1 \in D\langle 1,xy\rangle$. Contradiction. Also then $-x \notin D\langle 1,y\rangle$.

Let $z \in D\langle 1,x\rangle \cap D\langle 1,y\rangle$. Then $-1, z \in D(\varphi)$ yields

$$-z \in D(\varphi) = -D\langle 1,xy\rangle \cup \{1,y\}D\langle 1,x\rangle \cup \{1,x\}D\langle 1,y\rangle.$$

But $-z \notin D\langle 1,x\rangle \cup D\langle 1,y\rangle$ or else $-1 \in D\langle 1,x\rangle \cup D\langle 1,y\rangle$ implies x or $y \in D\langle 1,1\rangle$. Also $-z \notin yD\langle 1,x\rangle$ for otherwise $z \in D\langle 1,x\rangle \cap -yD\langle 1,x\rangle$ which is empty by the last paragraph. Similarly $-z \notin xD\langle 1,y\rangle$. Thus it must be the case that $z \in D\langle 1,xy\rangle$, and so

$$z \in D\langle 1,x\rangle \cap D\langle 1,y\rangle \cap D\langle 1,xy\rangle \subseteq D\langle 1,1\rangle.$$

But $D\langle 1,1\rangle \cap D\langle 1,xy\rangle = \{1\}$ then shows $D\langle 1,x\rangle \cap D\langle 1,y\rangle = \{1\}$. It now follows that

$$\{1,y\}D\langle 1,x\rangle \cap \{1,x\}D\langle 1,y\rangle = \{1,x,y,xy\}(D\langle 1,x\rangle \cap D\langle 1,y\rangle) = D\langle 1,xy\rangle.$$

Clearly both $\{1,y\}D\langle 1,x\rangle$ and $\{1,x\}D\langle 1,y\rangle$ contain at least eight elements. Let $c \in \{1,y\}D\langle 1,x\rangle - D\langle 1,xy\rangle$ and $d \in \{1,x\}D\langle 1,y\rangle - D\langle 1,xy\rangle$. Then $cd \in D(\varphi)$ and $cd \notin \{1,y\}D\langle 1,x\rangle \cup \langle 1,x\rangle D\langle 1,y\rangle$ show $cd \in -D\langle 1,xy\rangle$. Thus for a fixed c, there exist at most four such d, *i.e.* $|\{1,x\}D\langle 1,y\rangle - D\langle 1,xy\rangle| \leq 4$. Hence, $|D\langle 1,y\rangle| \leq 4$, and by (3.2) $D\langle 1,y\rangle = \{1,y,a,ay\}$. Similarly $D\langle 1,x\rangle = \{1,x,-a,-ax\}$, and Claim 5 is established.

CLAIM 6. Let $i,j \in I$; $k,\ell \in K$ where I and K are defined above. Then $u_{\imath k} \equiv u_{\imath\ell} \pmod{\{1,a\}}$ and $v_{\imath k} \equiv v_{jk} \pmod{\{1,-a\}}$.

Set $u = u_{\imath k}, u' = u_{\imath\ell}, v = v_{\imath k}, v' = v_{\imath\ell}$. Then

$$D\langle 1,uv\rangle = \{1,u,v,uv\} \text{ and } D\langle 1,u'v'\rangle = \{1,u',v',u'v'\}. \tag{3.3}$$

By Claim 5, we also have

$$\begin{aligned} D\langle 1,u\rangle &= \{1,u,-a,-au\} \text{ and } D\langle 1,v\rangle = \{1,v,a,av\} \\ D\langle 1,u'\rangle &= \{1,u',-a,-au'\} \text{ and } D\langle 1,v'\rangle = \{1,v',a,av'\}. \end{aligned} \tag{3.4}$$

We know already that $u \equiv u' \pmod{D\langle 1,1\rangle}$. Suppose $u' = -u$. Then

$$D\langle 1,u'v'\rangle = D\langle 1,-uv'\rangle = \{1,-u,v',-uv'\}$$

by (3.3). From (3.4), $v' \in D\langle 1,v'\rangle \cap D\langle 1,-uv'\rangle \subseteq D\langle 1,u\rangle$ gives a contradiction. Suppose $u' = -au$. Then

$$v' \in D\langle 1,-auv'\rangle \cap D\langle 1,v'\rangle \cap D\langle 1,-a\rangle \subseteq D\langle 1,u\rangle,$$

again a contradiction. Consequently, $u' \in \{1, a\}u$, and the first half of Claim 6 is proved. The second half is done in an analogous manner.

Now set $H_1 = \langle \{u_{ik}\}, a \rangle$ and $H_2 = \langle \{v_{ik}\}, -a \rangle$ for all $i \in I, k \in K$. Clearly $q(u_{ik}, -a) = q(v_{ik}, a) = 0$. By Claim 6, $q(u_{ik}, v_{j\ell}) = q(u_{ik}, v_{i\ell}) = q(u_{i\ell}, v_{i\ell}) = 0$ since $\langle u_{i\ell}, v_{i\ell} \rangle \cong \langle 1, u_{i\ell}v_{i\ell} \rangle$. Thus $q(x, y) = 0$ for all $x \in H_1$ and $y \in H_2$, and using Claim 4 we obtain $G = H_1 \perp H_2$.

Since $-1 = a(-a)$, a is the distinguished element of H_1 and $-a$ is the distinguished element for H_2. Moreover, $D\langle 1, 1 \rangle \cap H_1 = \{1, a\}$ and $D\langle 1, 1 \rangle \cap H_2 = \{1, -a\}$. If R_1 and R_2 are the Witt rings in R associated with H_1 and H_2, then it follows from Theorems 5.8 and 5.13 [8] that $R \cong R_1 \times R_2$ in the category of Witt rings. By Corollary 2.8 [3], $R_i \cong \mathbb{Z}/4\mathbb{Z}[\Delta_i]$ for $i = 1, 2$; and the proof of Theorem 3.1 is complete. ■

It is interesting to observe that by using the results in Kula [6], we see that every Witt ring satisfying $s = 2$ and $|D\langle 1, 1 \rangle| = 4$ is realized by a field.

4. The second case for s = 2.

In this section the Witt ring R satisfies the properties that $s = 2$ and that $|D\langle 1, a \rangle| = 4$ for some $a \in D\langle 1, 1 \rangle - \{1, -1\}$. Consequently,

$$D\langle 1, a \rangle = \{1, -1, a, -a\} \text{ and } D\langle 1, 1 \rangle \cap D\langle 1, -a \rangle = D\langle 1, a \rangle.$$

As in Section 3, we first consider the situation where $D_R \neq 1$. If $D_R = G$, then virtually the same argument for this previous case works again to show $R \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. If $D_R \neq G$, then also as before $-a \notin D_R$, $|D_R| = 2$, and $D\langle 1, a \rangle = D_R \cup -aD_R$. In fact we must have $D_R = \{1, -1\}$ or $\{1, a\}$. If the latter is true, then

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

Thus Section 3 applies, and $R \cong S \times T$ where $S \cong \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z}[x]$ and $T \cong \mathbb{Z}/4\mathbb{Z}[G_T/\{\pm 1\}]$.

If the former is true, then let H be any subgroup containing a such that $G = D_R \times H$. By Theorem 5.8 [8], there are Witt rings S, T in R with G_S, G_T corresponding to D_R, H respectively such that $R \cong S \times T$. Clearly $S \cong \mathbb{Z}/4\mathbb{Z}$. $D\langle 1, a \rangle \cap H = \{1, a\}$, and so a is rigid in H. Moreover, $-1 \in D_R$ implies $s(T) = 1$. Thus, T is a group ring with $\mathrm{char}(T) = 2$.

In the theorem below, the first 3 cases correspond to the above situations when $D_R \neq 1$. Case (4) occurs when $D_R = 1$, and the remainder of the proof is dedicated to showing this.

THEOREM 4.1. *Suppose* $\mathrm{char}(R) = 4$ *and G contains no rigid elements. Then there is an* $a \in D\langle 1, 1 \rangle - \{1\}$ *satisfying* $|D\langle 1, a \rangle| = 4$ *if and only if R is isomorphic to one of the following Witt rings:*

(1) the Witt ring of a field F satisfying $s(F) = u(F) = 2$ *and* $q(F) = 4$,

(2) the product in the category of Witt rings of either $\mathbb{Z}/2\mathbb{Z}[x]$ *or* $\mathbb{Z}/4\mathbb{Z}$ *and* $\mathbb{Z}/4\mathbb{Z}[\Delta]$ *where* Δ *is a group of exponent* 2,

(3) the product of $\mathbb{Z}/4\mathbb{Z}$ *and any group ring of characteristic* 2, *or*

https://doi.org/10.4153/CJM-1993-066-7 Published online by Cambridge University Press

(4) *the product of a group ring of characteristic* 2 *and* $\mathbb{Z}/4\mathbb{Z}[\Delta]$ *where* Δ *is a group of exponent* 2.

Note: There is some overlap in these possibilities.

PROOF. From the above we may assume $D_R = 1$. $D\langle 1,a\rangle = \{\pm 1, \pm a\}$ implies that $D\langle 1,1\rangle \cap D\langle 1,-a\rangle = D\langle 1,a\rangle$. We follow the same pattern as in the proof of Theorem 3.1, but some of the steps will require slightly more in this case.

CLAIM 1. $D\langle 1,t\rangle \cap D\langle 1,a\rangle D\langle 1,-t\rangle = \{1,t\}(D\langle 1,t\rangle \cap D\langle 1,1\rangle)$.

CLAIM 1a. If $t \notin D\langle 1,1\rangle$, then

$$D\langle 1,t\rangle \cap D\langle 1,a\rangle D\langle 1,at\rangle = \{1,t\}(D\langle 1,t\rangle \cap D\langle 1,-a\rangle).$$

Claim 1 is proved as in [3], but Claim 1a (which will be needed in addition to Claim 1 to verify Claim 3 below) requires a new proof.

It follows from Lemma 1.1 and 1.4 that

$$\begin{aligned} D\langle 1,t\rangle \cap \{1,a\}D\langle 1,at\rangle &= \{1,t\}(D\langle 1,t\rangle \cap D\langle 1,at\rangle) \\ &= \{1,t\}(D\langle 1,t\rangle \cap D\langle 1,-a\rangle). \end{aligned}$$

So Claim 1a will be established if $D\langle 1,t\rangle \cap \{-1,-a\}D\langle 1,at\rangle = \phi$.

Let $u \in D\langle 1,t\rangle \cap -D\langle 1,at\rangle$. Then $q(u,-t) = q(-u,-at) = 0$. Thus $q(-1,-at) = q(u,-at)$ which yields $q(-1,t) = q(u,a)$. By the linkage property of q, there exists x satisfying $q(-1,t) = q(-1,x)$ and $q(u,a) = q(x,a)$. Hence $q(x,-a) = 0 = q(-1,tx)$, and $x \in D\langle 1,a\rangle$ and $tx \in D\langle 1,1\rangle$. It follows that $t = x(tx) \in D\langle 1,a\rangle D\langle 1,1\rangle = D\langle 1,1\rangle$. Contradiction and we must have $D\langle 1,t\rangle \cap -D\langle 1,at\rangle = \phi$.

Now suppose $u \in D\langle 1,t\rangle \cap -aD\langle 1,at\rangle$. Then $q(u,-t) = 0 = q(-au,-at)$, and so $q(-a,-at) = q(u,-at)$. Thus $q(-a,t) = q(u,a)$. By linkage there exists x satisfying $q(-a,t) = q(-a,x)$ and $q(u,a) = q(x,a)$. It follows that $x \in D\langle 1,1\rangle$ and $tx \in D\langle 1,a\rangle$, and these imply once again the contradiction of $t \in D\langle 1,1\rangle$. So $D\langle 1,t\rangle \cap -aD\langle 1,at\rangle = \phi$.

REMARK. Actually Claim 1a holds for all $t \in G$, but we will not need this generality.

CLAIM 2. If $t \notin D\langle 1,1\rangle \cup D\langle 1,-a\rangle$, then $D\langle 1,t\rangle \cap D\langle 1,a\rangle D\langle 1,-at\rangle = \{1,t\}$ or $\{1,t,u,tu\}$ where $u \in D\langle 1,1\rangle$ and $tu \in D\langle 1,-a\rangle$.

As for Theorem 3.1, the proof of this claim is broken down into two cases, one where $v \in D\langle 1,a\rangle$ is equal to $-a$ and one where $v \neq -a$.

Using Claim 2, we can establish that $T = D\langle 1,a\rangle D\langle 1,t\rangle \cap D\langle 1,a\rangle D\langle 1,-at\rangle = D\langle 1,a\rangle D\langle 1,-t\rangle \cap D\langle 1,a\rangle D\langle 1,at\rangle$. If $\rho = \langle 1,a\rangle \otimes \langle 1,t\rangle$, then $D(\rho) = \bigcup D\langle 1,a\rangle D\langle 1,xt\rangle$, $x \in D\langle 1,a\rangle$. Also $T \subseteq D\langle 1,a\rangle D\langle 1,xt\rangle$ by the above for each $x \in D\langle 1,a\rangle$.

CLAIM 3. $T = D\langle 1,a\rangle D\langle 1,xt\rangle$ for some $x \in D\langle 1,a\rangle$.

To prove this claim, as in [3], consider $H = D(\rho)/T$ and set $H_{xt} = D\langle 1,a\rangle D\langle 1,xt\rangle/T$ for $x \in D\langle 1,a\rangle$. Following [3] exactly, we may assume there exist $x \neq y$ such that $H_{xt} \cap H_{yt} \neq 1$. By the above we further can assume $x \in \{1,-a\}$ and $y \in \{-1,a\}$. Replacing

https://doi.org/10.4153/CJM-1993-066-7 Published online by Cambridge University Press

t with $-at$ if necessary, we can set $x = 1$. However, as opposed to both Carson's and Marshall's theorem and Theorem 3.1, it is not possible to reduce y to just one case. If $y = -1$, then the proof proceeds as in [3] using Claim 1 above. If $y = a$, then everything is exactly the same; but Claim 1a is required in place of Claim 1.

CLAIM 4. If $t \notin D\langle 1,1\rangle \cup D\langle 1,-a\rangle$, then there exists $x \in D\langle 1,a\rangle$ such that $|D\langle 1,xt\rangle| = 4$; and for any such $x, D\langle 1,xt\rangle = \{1,xt,u,xtu\}$ where $u \in D\langle 1,1\rangle$ and $xtu \in D\langle 1,-a\rangle$. Moreover, $D\langle 1,1\rangle D\langle 1,-a\rangle = G$.

This claim can be used just as in Section 3 to find bases $\{u_i \mid i \in I\}, \{v_k \mid k \in K\}$ for $D\langle 1,1\rangle$ and $D\langle 1,-a\rangle \bmod D\langle 1,a\rangle$ respectively as well as the associated $\{u_{ik}\}$ and $\{v_{ik}\}$ which satisfy $u_i \equiv u_{ik} \pmod{D\langle 1,a\rangle}$ and $v_k \equiv v_{ik} \pmod{D\langle 1,a\rangle}$. Again before verifying Carson's and Marshall's next claim, we need an intermediate step.

CLAIM 5. Suppose $D\langle 1,xy\rangle = \{1,x,y,xy\}$ where $x \in D\langle 1,1\rangle - D\langle 1,a\rangle$ and $y \in D\langle 1,-a\rangle - D\langle 1,a\rangle$. Then $D\langle 1,x\rangle = \{1,-1,x,-x\}, D\langle 1,ay\rangle = \{1,a,y,ay\}$ and $D\langle 1,-ay\rangle = \{1,a,-y,-ay\}$.

Note that $x \in D\langle 1,1\rangle \cap D\langle 1,xy\rangle \subseteq D\langle 1,-xy\rangle$, and so $xy \in D\langle 1,-x\rangle$. But $-1 \in D\langle 1,-x\rangle$ then implies $\pm y \in D\langle 1,-x\rangle$ (or equivalently $x \in D\langle 1,\pm y\rangle$). It also is immediate that $x,-y \in D\langle 1,-xy\rangle$. Moreover, $y \notin D\langle 1,x\rangle$ for otherwise $x,-x \in D\langle 1,-y\rangle$ which yields $y \in D\langle 1,1\rangle$. Contradiction. Summarizing, we obtain

$$\begin{gathered} x \in D\langle 1,\pm y\rangle, \quad x \in D\langle 1,-xy\rangle, \quad y \notin D\langle 1,x\rangle, \\ -1 \in D\langle 1,\pm x\rangle - D\langle 1,\pm y\rangle, \quad a \in D\langle 1,\pm y\rangle - D\langle 1,\pm x\rangle. \end{gathered} \tag{4.2}$$

Consider $\sigma = \langle 1,xy,1,xy\rangle$. Then $D(\sigma) = \bigcup D\langle 1,xy\rangle D\langle 1,z\rangle$, $z \in D\langle 1,xy\rangle$. So

$$D(\sigma) = D\langle 1,xy\rangle (D\langle 1,1\rangle \cup D\langle 1,x\rangle \cup D\langle 1,y\rangle).$$

From (4.2) $\{1,x\} \subseteq D\langle 1,x\rangle \cap D\langle 1,y\rangle$. In fact equality holds. Let $u \in D\langle 1,x\rangle \cap D\langle 1,y\rangle$. Then $-au \in D(\sigma)$. Could $-au \in D\langle 1,xy\rangle D\langle 1,x\rangle$? If so, then $\{a,ax,ay,axy\} \cap D\langle 1,x\rangle \neq \phi$. But if either a or $ax \in D\langle 1,x\rangle$, then $-a \in D\langle 1,x\rangle$ which yields $x \in D\langle 1,a\rangle$. Contradiction. Also if ay or $axy \in D\langle 1,x\rangle$, then it follows that $-axy \in D\langle 1,x\rangle \cap D\langle 1,-y\rangle \subseteq D\langle 1,xy\rangle$. Hence $-a \in D\langle 1,xy\rangle$. Contradiction. So $-au \notin D\langle 1,xy\rangle D\langle 1,x\rangle$, and similarly $-au \notin D\langle 1,xy\rangle D\langle 1,y\rangle$. Thus, it must be the case that $-au \in D\langle 1,xy\rangle D\langle 1,1\rangle$ which yields $u \in D\langle 1,xy\rangle D\langle 1,1\rangle$. So $u \in D\langle 1,x\rangle \cap D\langle 1,y\rangle \cap \{1,x,y,xy\} D\langle 1,1\rangle \subseteq D\langle 1,-xy\rangle \cap \{1,x,y,xy\} D\langle 1,1\rangle = \{1,x,-y,-xy\}(D\langle 1,-xy\rangle \cap D\langle 1,1\rangle) \subseteq \langle\{-1,x,y\}\rangle$. Since $x \in D\langle 1,y\rangle$ and $-1 \notin D\langle 1,y\rangle$, $u \neq -1,-x,-y,-xy$. Also since $y \notin D\langle 1,x\rangle$, it is impossible for u to be either y or xy. Thus $u \in \{1,x\}$, and $D\langle 1,x\rangle \cap D\langle 1,y\rangle = \{1,x\}$.

By (4.2) $D\langle 1,xy\rangle \subseteq D\langle 1,y\rangle$. So $D\langle 1,xy\rangle D\langle 1,x\rangle \cap D\langle 1,xy\rangle D\langle 1,y\rangle = D\langle 1,xy\rangle (D\langle 1,x\rangle \cap D\langle 1,xy\rangle D\langle 1,y\rangle)$ (by Lemma 1.3) = $D\langle 1,xy\rangle (D\langle 1,x\rangle \cap D\langle 1,y\rangle) = D\langle 1,xy\rangle$.

Also

$$D\langle 1,xy\rangle D\langle 1,x\rangle = \{1,y\} D\langle 1,x\rangle$$

and

$$D\langle 1,xy\rangle D\langle 1,1\rangle = \{1,y\} D\langle 1,1\rangle.$$

https://doi.org/10.4153/CJM-1993-066-7 Published online by Cambridge University Press

Now choose $u \in \{1,y\}D\langle 1,x\rangle - D\langle 1,xy\rangle$ and $v \in D\langle 1,y\rangle - D\langle 1,xy\rangle$ Then $uv \in D(\sigma) - D\langle 1,xy\rangle(D\langle 1,x\rangle \cup D\langle 1,y\rangle)$ implies $uv \in \{1,y\}D\langle 1,1\rangle$ In particular if $v = a$, then the last statement gives

$$\{1,y\}D\langle 1,x\rangle - D\langle 1,xy\rangle \subseteq \{1,y\}D\langle 1,1\rangle$$

But $x \in D\langle 1,1\rangle$ shows $D\langle 1,xy\rangle \subseteq \{1,y\}D\langle 1,1\rangle$, so $\{1,y\}D\langle 1,x\rangle \subseteq \{1,y\}D\langle 1,1\rangle$ Starting with $u = -1$ we see also that $D\langle 1,y\rangle \subseteq \{1,y\}D\langle 1,1\rangle$ Consequently,

$$D\langle 1,xy,1,xy\rangle = \{1,y\}D\langle 1,1\rangle \tag{4 3}$$

Now suppose $w \in D\langle 1,1\rangle$ Then since

$$\begin{aligned}\sigma \cong \langle 1,wy,1,wy\rangle, D\langle 1,wy\rangle &= D\langle 1,wy\rangle \cap \{1,y\}D\langle 1,1\rangle \\ &= \{1,wy\}(D\langle 1,wy\rangle \cap D\langle 1,1\rangle) \subseteq \{1,wy\}D\langle 1,-wy\rangle \\ &= \{1,-1\}D\langle 1,-wy\rangle\end{aligned}$$

Replacing w by $-w$ leads to

$$\{1,-1\}D\langle 1,wy\rangle = \{1,\ -1\}D\langle 1,-wy\rangle \text{ for all } w \in D\langle 1,1\rangle \tag{4 4}$$

Let $\tau = \langle 1,a,y,ay\rangle$ Then $D(\tau) = D\langle 1,a\rangle(D\langle 1,y\rangle \cup D\langle 1,-y\rangle \cup D\langle 1,ay\rangle \cup D\langle 1,-ay\rangle)$ But using (4 4) with $w = 1$ and a, we see that $D(\tau) = D\langle 1,a\rangle D\langle 1,y\rangle \cup D\langle 1,a\rangle D\langle 1,ay\rangle$ By (4 2), $x \in D\langle 1,y\rangle$ Suppose also that $x \in D\langle 1,a\rangle D\langle 1,ay\rangle$ Then $\{\pm x, \pm ax\} \cap D\langle 1,ay\rangle \neq \phi$ But if either x or $ax \in D\langle 1,ay\rangle$, then $x \in D\langle 1,ay\rangle$ since $a \in D\langle 1,ay\rangle$ by (4 2) Thus $-ay \in D\langle 1,-x\rangle$, and so $-a \in D\langle 1,-x\rangle$ which gives $x \in D\langle 1,a\rangle$ Contradiction On the other hand if either $-x$ or $-ax \in D\langle 1,ay\rangle$, then $-ax \in D\langle 1,ay\rangle$, and so $-ay \in D\langle 1,ax\rangle \cap D\langle 1,-ay\rangle \subseteq D\langle 1,xy\rangle$ Contradiction Hence, by Lemma 1 2

$$D(\tau) = D\langle 1,a\rangle D\langle 1,y\rangle = \{1,-1\}D\langle 1,y\rangle$$

Using (4 4) then, we see $D\langle 1,ay\rangle \subseteq D(\tau)$ implies $D\langle 1,ay\rangle = D\langle 1,ay\rangle \cap \{1,-1\}D\langle 1,-y\rangle = \{1,y\}(D\langle 1,ay\rangle \cap D\langle 1,-y\rangle) \subseteq \{1,y\}D\langle 1,a\rangle = \langle\{-1,a,y\}\rangle$

Since $y \in D\langle 1,ay\rangle$ and $-1 \notin D\langle 1,ay\rangle$, we obtain $D\langle 1,ay\rangle = \{1,a,y,ay\}$ Using (4 2), (4 4) and $-1 \notin D\langle 1,-ay\rangle$, we also see $D\langle 1,-ay\rangle = \{1,a,-y,-ay\}$ This establishes part of Claim 5

Now consider $\psi = \langle 1,xy,a,axy\rangle$ Then using $D\langle 1,a\rangle = \{\pm 1, \pm a\}, -1 \in D\langle 1,ax\rangle$, and $D\langle 1,ay\rangle = \{1,a,y,ay\}$, we see $D(\psi) = \bigcup D\langle 1,xy\rangle D\langle 1,az\rangle$, $z \in D\langle 1,xy\rangle$, and so

$$D(\psi) = D\langle 1,xy\rangle(D\langle 1,ax\rangle \cup D\langle 1,axy\rangle)$$

Suppose $-1 \in D\langle 1,xy\rangle D\langle 1,axy\rangle$ Then $\{-1,-x,-y,-xy\} \cap D\langle 1,axy\rangle \neq \phi$, but all four possibilities lead to quick contradictions Thus by Lemma 1 2, $D\langle 1,xy,a,axy\rangle = D\langle 1,xy\rangle D\langle 1,ax\rangle$

https://doi.org/10.4153/CJM-1993-066-7 Published online by Cambridge University Press

Now $x \in D\langle xy, ax\rangle$ and $ax \in D\langle a, axy\rangle$, so $D\langle 1,x\rangle \subseteq D(\psi)$. Consequently,

$$D\langle 1,x\rangle = D\langle 1,x\rangle \cap \{1,x,y,xy\}D\langle 1,ax\rangle. \tag{4.5}$$

Suppose $w \in D\langle 1,x\rangle \cap yD\langle 1,ax\rangle$. Then $q(w,-x) = 0 = q(wy,-ax)$. Thus $q(wy,a) = q(wy,-x)$ which implies $q(w,a) = q(y,-x)$. By the linkage property there exists z such that $q(w,a) = q(z,a)$ and $q(y,-x) = q(y,z)$. So $z \in D\langle 1,-ay\rangle = \{1,a,-y,-ay\}$, and $wx \in D\langle 1,-a\rangle$. It follows that $w \in D\langle 1,-a\rangle$. Hence,

$$w \in D\langle 1,-a\rangle \cap D\langle 1,x\rangle \cap yD\langle 1,ax\rangle \subseteq D\langle 1,ax\rangle \cap yD\langle 1,ax\rangle.$$

But by (4.2) $y \notin D\langle 1,x\rangle$ which yields $-x \notin D\langle 1,-y\rangle, -ax \notin D\langle 1,-y\rangle$, and finally $y \notin D\langle 1,ax\rangle$. Thus we have shown $D\langle 1,x\rangle \cap yD\langle 1,ax\rangle = \phi$.

In a similar fashion it can be demonstrated that $D\langle 1,x\rangle \cap xyD\langle 1,ax\rangle = \phi$. Consequently,

$$D\langle 1,x\rangle = D\langle 1,x\rangle \cap \{1,x\}D\langle 1,ax\rangle = \{1,x\}(D\langle 1,x\rangle \cap D\langle 1,ax\rangle) \subseteq \{1,x\}D\langle 1,-a\rangle.$$

From (4.3), $D\langle 1,x\rangle \subseteq \{1,y\}D\langle 1,1\rangle$. Using the above then we see $D\langle 1,x\rangle \subseteq \{1,x\}D\langle 1,-a\rangle \cap \{1,y\}D\langle 1,1\rangle = \{1,y,x,xy\}(D\langle 1,-a\rangle \cap D\langle 1,1\rangle) = \langle\{-1,a,x,y\}\rangle$.

From (4.2) and the earlier computations of $D\langle 1,\pm ay\rangle$, it follows that $-1,x \in D\langle 1,x\rangle$ and $\{a,y,ay\} \cap D\langle 1,x\rangle = \phi$. Hence, $D\langle 1,x\rangle = \{\pm 1,\pm x\}$; and Claim 5 is established.

CLAIM 6. Let $i,j \in I$ and $k, \ell \in K$ where I and K are defined above. Then $u_{ik} \equiv u_{i\ell}$ (mod $\{1,a\}$) and $v_{ik} \equiv v_{jk}$ (mod $\{1,-1\}$).

Set $u = u_{ik}, u' = u_{jk}, v = v_{ik}, v' = v_{jk}$. Then

$$D\langle 1,uv\rangle = \{1,u,v,uv\} \text{ and } D\langle 1,u'v'\rangle = \{1,u',v',u'v'\}. \tag{4.6}$$

From Claim 5, it is also the case that

$$\begin{aligned} &D\langle 1,u\rangle = \{\pm 1,\pm u\} \text{ and } D\langle 1,\pm av\rangle = \{1,a,\pm v,\pm av\} \quad \text{(corresponding signs)}\\ &D\langle 1,u'\rangle = \{\pm 1,\pm u'\} \text{ and } D\langle 1,\pm av'\rangle = \{1,a,\pm v',\pm av'\}. \end{aligned} \tag{4.7}$$

We know already that $v \equiv v'$ (mod $D\langle 1,a\rangle$). Suppose $v' = av$. Then from (4.6) and (4.7), $u' \in D\langle 1,au'v\rangle \cap D\langle 1,u'\rangle \subseteq D\langle 1,-av\rangle$. Contradiction. Now assume $v' = -av$. Then $u' \in D\langle 1,-au'v\rangle \cap D\langle 1,u'\rangle \subseteq D\langle 1,av\rangle$, again a contradiction. So $v' \in \{1,-1\}v$. Showing $u \equiv u'$ (mod $\{1,a\}$) is done similarly, and Claim 6 is proved.

Now set $H_1 = \langle\{u_{ik}\} \cup \{a\}\rangle$ and $H_2 = \langle\{v_{ik}\} \cup \{-1\}\rangle$. Just as in Section 3, $G = H_1 \perp H_2$. It is also easy to see that $1,-1$ are the distinguished elements of H_1, H_2 respectively and that $D\langle 1,a\rangle \cap H_1 = \{1,a\}, D\langle 1,1\rangle \cap H_2 = \{1,-1\}$. The theorem now follows just as Theorem 3.1 did. ■

One might ask is it possible for the hypotheses of Theorems 3.1 and 4.1 to be true simultaneously. If so, then $D\langle 1,1\rangle = D\langle 1,a\rangle \subseteq D\langle 1,-a\rangle$. But the proofs of Claim 4 in each of Sections 3 and 4 only relied on $D\langle 1,1\rangle \cup D\langle 1,a\rangle \cup D\langle 1,-a\rangle \neq G$. In particular the only way both hypotheses can hold is if $a \in D_R$; and this possibility occurs only in (1) and (2) of Theorems 3.1 and 4.1.

REFERENCES

1. L Berman, C Cordes and R Ware, *Quadratıc forms, rıgıd elements, and formal power serıes fields*, J Algebra **66**(1980), 123–133

2. R Bos, *Quadratıc forms, orderıngs, and abstract Wıtt rıngs*, Dıssertatıon, Utrecht (1984)

3. A Carson and M Marshall, *Decomposıtıon of Wıtt rıngs*, Can J Math **34**(1982), 1276–1302

4. C Cordes, *The Wıtt group and the equıvalence of fields wıth respect to quadratıc forms*, J Algebra **26**(1973), 400–421

5. ———, *Kaplansky's radıcal and quadratıc forms over non-real fields*, Acta Arıth **28**(1975), 253–261

6. M Kula, *Fıelds wıth prescrıbed quadratıc form schemes*, Math Zeıt **167**(1979), 202–212

7. M Kula, L Szczepanık and K Szymıczek, *Quadratıc form schemes and quaternıonıc schemes*, Fund Math **130**(1988), 181–190

8. M Marshall, *Abstract Wıtt rıngs*, Queen's Papers ın pure and applıed Math **57**, Queen's Unıv (1980)

9. ———, *Decomposıng Wıtt rıngs of characterıstıc two*, Rocky Mountaın J Math **19**(1989), 793–806

10. L Szczepanık, *Quadratıc form schemes wıth non-trıvıal radıcal*, Colloquıum Math **49**(1985), 143–160

Department of Mathematıcs
Louısıana State Unıversıty
Baton Rouge, Louısıana 70803
U S A

https://doi.org/10.4153/CJM-1993-066-7 Published online by Cambridge University Press