Can. J. Math., Vol. XXXIV, No. 6, 1982, pp. 1276–1302

DECOMPOSITION OF WITT RINGS

ANDREW B. CARSON AND MURRAY A. MARSHALL

We take the definition of a Witt ring to be that given in [**13**], i.e., it is what is called a strongly representational Witt ring in [**8**]. The classical example is obtained by considering quadratic forms over a field of characteristic $\neq 2$ [**17**], but Witt rings also arise in studying quadratic forms or symmetric bilinear forms over more general types of rings [**5**, **7**, **8**, **9**]. An interesting problem in the theory is that of classifying Witt rings in case the associated group G is finite. The reduced case, i.e., the case where the nilradical is trivial, is better understood. In particular, the above classification problem is completely solved in this case [**4**, **12**, or **13**, Corollary 6.25]. Thus, the emphasis here is on the non-reduced case. Although some of the results given here do not require $|G| < \infty$, they do require some finiteness assumption. Certainly, the main goal here is to understand the finite case, and in this sense this paper is a continuation of work started by the second author in [**13**, Chapter 5].

To date, all known Witt rings with $|G| < \infty$ are built up from Witt rings of finite fields and local fields of characteristic $\neq 2$ by forming products and group rings. Any Witt ring that can be built up in this fashion is said to be of elementary type. The elementary types are well understood. In particular, using certain uniqueness results in [**13**, Chapter 5], one can develop formulae for counting the number of elementary types with $|G| = 2^n$ for each integer $n \geqq 0$. This is done in Section 4. In Section 5 we prove, with the aid of a computer, that every Witt ring with $|G| \leqq 32$ is of elementary type. This extends some earlier results. For $|G| \leqq 8$, see [**2**] and [**11**]. The result in case $|G| = 16$ is due to L. Berman (unpublished) and, independently, to L. Szczepanik [**15**].

In Sections 2 and 3 we develop internal characterizations of group rings and products respectively, complimenting results in [**1**] and [**13**, Chapter 5]. In Section 2 we show how a given non-rigid element generates all non-rigid elements and use this to obtain another characterization of the basic part. This is useful for the computation in Section 5 and also yields a classification of non-real preorders as defined in [**18**]. In Section 3 we study the relationship between product decompositions of Witt rings and orthogonal decompositions of their associated groups. The results obtained are applied in Section 4 to prove that a Witt ring with $|G| < \infty$ is of elementary type if and only if it can be built up from Witt rings in the set

Received September 26, 1981.

$\{\mathbf{Z}, \mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/4\mathbf{Z}\}$ by forming group rings and weak products. Also in Section 3, we give a characterization of Witt rings of characteristic 2 which are the product of two group rings.

1. Introduction. In this section we introduce terminology and notation, recall the basic relationship between Witt rings and quaternionic structures developed in [**13**], and relate these objects to the quadratic form schemes considered in [**2**, **10**, **15**, and **16**].

R will always denote a Witt ring and G will denote the distinguished subgroup of the multiplicative group of R. Thus R is a commutative ring with 1, G has exponent 2 and $-1 \in G$, and every element of R is expressible as a finite sum of elements of G. Finally, if

$$a_1 + \ldots + a_n = b_1 + \ldots + b_m$$

where $a_1, \ldots, a_n, b_1, \ldots, b_m \in G$ and $n \geqq m \geqq 1$ and $n \geqq 2$, then $\exists\ c_1, \ldots, c_{n-1} \in G$ such that

$$a_2 + \ldots + a_n = c_1 + \ldots + c_{n-1}$$

and

$$a_1 + c_1 = b_1 + a_1b_1c_1.$$

Equivalent axioms for Witt rings are given in [**13**, Chapter 4] and [**8**].

It is clear from the definition that R is a quotient of the integral group ring $\mathbf{Z}[G]$. In fact, by [**13**, Theorem 4.3], R can be identified with $\mathbf{Z}[G]/J$ where J is the ideal of $\mathbf{Z}[G]$ generated by $[1] + [-1]$ and all elements $([1] - [a])([1] - [b])$ where $a, b \in G$ satisfy

$$(1 - a)(1 - b) = 0 \text{ (in } R).$$

Here, $[a]$ denotes the element $a \in G$, but viewed as an element of $\mathbf{Z}[G]$.

For $a, b \in G$, let

$$q(a, b) := (1 - a)(1 - b),$$

and let

$$Q = \{q(a, b) | a, b \in G\} \subseteq R.$$

Then $q: G \times G \rightarrow Q$ is a *quaternionic structure*, i.e., it satisfies

$$q(a, b) = q(b, a), q(a, -a) = 0,$$
$$q(a, b) = q(a, c) \Leftrightarrow q(a, bc) = 0,$$

and the *linkage property*:

$$q(a, b) = q(c, d) \Rightarrow \exists\ x \in G \text{ with}$$
$$q(a, b) = q(a, x) \quad \text{and} \quad q(c, d) = q(c, x).$$

For the proof, see [**13**, Proposition 4.2]. It is clear from the representation of R as a quotient of $\mathbf{Z}[G]$ that a Witt ring is completely determined once its quaternionic structure is specified.

The reader should note that the concept of a quaternionic structure may well be more general than the concept of a quaternionic mapping given in [**14**]. The relationship between these two concepts is discussed in [**13**, Chapter 3]. In any case, the main result of [**14**] carries over as follows:

(1.1) THEOREM. *Every quaternionic structure is realized as the quaternionic structure of a Witt ring.*

Proof. See [**13**, Chapter 2].

For the computation in Section 5, it is useful to have another description of quaternionic structures. To obtain this, consider the value sets $D\langle 1, a\rangle$, $a \in G$, terminology as in [**13**, Chapter 2]. Thus, in terms of q,

$$D\langle 1, a\rangle = \{x \in G | q(-a, x) = 0\}.$$

These value sets are subgroups of G and satisfy:

$$a \in D\langle 1, a\rangle \quad \text{and} \quad a \in D\langle 1, -b\rangle \Leftrightarrow b \in D\langle 1, -a\rangle.$$

Thus every quaternionic structure defines a *quadratic form scheme*, terminology as in [**2**, **10**, **15**, or **16**]. Moreover, q can be recovered from its quadratic form scheme since, by the properties of q, $q(a, b) = q(c, d)$ if and only if

$$bD\langle 1, -a\rangle \cap D\langle 1, -ac\rangle \cap dD\langle 1, -c\rangle \neq \emptyset.$$

This also shows that the quadratic form scheme associated to q satisfies:

$$\text{(1.2)} \quad bD\langle 1, -a\rangle \cap D\langle 1, -ac\rangle \cap dD\langle 1, -c\rangle \neq \emptyset$$
$$\Rightarrow aD\langle 1, -b\rangle \cap D\langle 1, -bd\rangle \cap cD\langle 1, -d\rangle \neq \emptyset.$$

In fact, this extra property characterizes quadratic form schemes associated to quaternionic structures.

(1.3) THEOREM. *An abstract quadratic form scheme defines a quaternionic structure if and only if it satisfies* (1.2).

Proof. Suppose we are given a quadratic form scheme satisfying (1.2). Let us denote

$$bD\langle 1, -a\rangle \cap D\langle 1, -ac\rangle \cap dD\langle 1, -c\rangle$$

by $V(a, b; c, d)$ for short. Define a relation $\equiv$ on $G \times G$ by

$$(a, b) \equiv (c, d) \Leftrightarrow V(a, b; c, d) \neq \emptyset.$$

Suppose $(a, b) \equiv (c, d) \equiv (e, f)$. Thus $\exists\ x \in V(a, b; c, d)$ and $y \in V(c, d; e, f)$. It follows that $c \in V(x, a; y, e)$, so by (1.2), $\exists\ z \in V(a, x;$

$e, y)$. Since $xD\langle 1, -a\rangle = bD\langle 1, -a\rangle$ and $yD\langle 1, -e\rangle = fD\langle 1, -e\rangle$, this implies $z \in V(a, b; e, f)$, and hence that $(a, b) \equiv (e, f)$. Thus $\equiv$ is transitive and hence is an equivalence relation. Now define $q(a, b)$ to be the equivalence class of (a, b) under $\equiv$. The verification that q is a quaternionic structure is now just an elementary exercise.

In view of Theorem 1.3 we will refer to quadratic form schemes which satisfy (1.2) as *quaternionic schemes*.

A *morphism of Witt rings* Ψ: $R \to S$ is just a ring homomorphism satisfying $\Psi(G_R) \subseteq G_S$. If Ψ is such a morphism, then its restriction to G_R is a *morphism of schemes*, i.e., it is a group homomorphism satisfying

$$\Psi(-1) = -1 \quad \text{and} \quad \Psi(D_R\langle 1, a\rangle) \subseteq D_S\langle 1, \Psi(a)\rangle \quad \forall\, a \in G_R.$$

Conversely, any scheme morphism Ψ: $G_R \to G_S$ lifts uniquely to a morphism of the Witt rings. In this way, the category of Witt rings and the category of quaternionic schemes (or equivalently, quaternionic structures) are equivalent. It is also worth noting that in all known cases, Witt rings which are isomorphic as rings are also isomorphic as Witt rings; see [**13**, Proposition 4.6].

One case where the theory is better understood is the reduced case. This was formulated originally in terms of spaces of orderings; see e.g., [**12**]. In terms of schemes, reduced Witt rings correspond to quaternionic schemes satisfying $D\langle 1, 1\rangle = 1$, see [**13**, Theorem 4.2].

Finally, it should be pointed out that (1.2) is not quite the same as the extra axiom for quadratic form schemes considered in [**15**, **16**]. The extra axiom in [**15**, **16**] has the same strength as the representation property for forms (see [**13**, Proposition 2.10]) and hence is a consequence of (1.2), but whether or not it is equivalent to (1.2) appears to be an open problem. In any case, since we are interested in Witt rings, we also want the cancellation property for forms (see [**13**, Proposition 2.8]), and hence will stay with (1.2).

2. Group rings, rigid elements, and non-real preorders. If S is a Witt ring and Δ is a group of exponent 2, we can form the group ring $S[\Delta]$. This is a Witt ring if we take $G_{S[\Delta]} = G_S \times \Delta$. We say the Witt ring R is a *group ring* if there exists a Witt ring S and a group Δ of exponent 2, $\Delta \neq 1$, with $R \cong S[\Delta]$ as Witt rings. A criterion for recognizing group rings is developed in [**1**]. To explain this we need some terminology. An element $a \in G$ is called *rigid* if $D\langle 1, a\rangle = \{1, a\}$. The *basic part* of R is the set $B = B_R$ defined by

(2.1) $\quad B = \{\pm 1\} \cup \{a \in G | a \text{ or } -a \text{ is not rigid}\}.$

Note, if $R = S[\Delta]$, then any $a \in G\backslash G_S$ is rigid, so $B \subseteq G_S$. Also, the quaternionic structure of S is just obtained by restricting q to G_S. Conversely, we have the following:

https://doi.org/10.4153/CJM-1982-089-1 Published online by Cambridge University Press

(2.2) THEOREM. *For any Witt ring R, B is a subgroup of G. If H is any subgroup of G with $B \subseteq H$, then the restriction of q to H defines a quaternionic structure q' on H, and $R \cong S[G/H]$ where S denotes the Witt ring corresponding to q'.*

Proof. See [**1**, or **13**, Chapter 5].

(2.3) COROLLARY. *R is a group ring if and only if $B \neq G$.*

Proof. This is clear.

We now give a result which shows how a given non-rigid element generates all non-rigid elements. This leads to a new characterization of the basic part and to the classification of non-real preorders as defined in [**18**].

(2.4) THEOREM. *Suppose $a \in G$, a is not rigid, and $|D\langle 1, a\rangle| < \infty$. Define $X_1 = D\langle 1, a\rangle$ and for $i \geqq 2$ define*

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

Finally, suppose $b \in G$, $b \notin X_1X_2^2 \cup -X_1X_3$. Then b is rigid.

Proof. $aX_1 = X_1$ since X_1 is a group and $a \in X_1$. Now suppose $x \in X_2$. Then $\exists\ y \in X_1$, $y \neq 1$, with $x \in D\langle 1, -y\rangle$. But $y \in D\langle 1, a\rangle$, so $-a \in D\langle 1, -y\rangle$. Thus $-ax \in D\langle 1, -y\rangle$. This proves that $-aX_2 = X_2$ and hence that

$$-X_1X_2 = (aX_1)(-aX_2) = X_1X_2.$$

Now fix $b \in G$, $b \notin X_1X_2^2 \cup -X_1X_3$.

Claim 1. $\forall\ x \in X_1$,

$$D\langle 1, xb\rangle \cap (X_1 \cup X_2) = 1.$$

For suppose y lies in this intersection, $y \neq 1$. Thus $-xb \in D\langle 1, -y\rangle$. If $y \in X_2$, this implies $-xb \in X_3$ so $b = -x(-xb) \in -X_1X_3$, a contradiction. If $y \in X_1$, then $-xb \in X_2$, so

$$b = -x(-xb) \in -X_1X_2 = X_1X_2 \subseteq X_1X_2^2,$$

also a contradiction.

Claim 2. If $x, y \in X_1$, $x \neq y$, then

$$D\langle 1, xb\rangle \cap D\langle 1, yb\rangle = 1.$$

For

$$D\langle 1, xb\rangle \cap D\langle 1, yb\rangle \subseteq D\langle 1, -xy\rangle \subseteq X_2,$$

so the result follows from claim 1.

Claim 3. If $x, y \in X_1$, $x \neq y$, then

$$X_1D\langle 1, xb\rangle \cap D\langle 1, yb\rangle = \{1, yb\}.$$

For suppose $z \in X_1$ and $zD\langle 1, xb\rangle \cap D\langle 1, yb\rangle \neq \emptyset$. Thus

$$\langle 1, yb\rangle \oplus -z\langle 1, xb\rangle \cong \langle 1, -z\rangle \oplus yb\langle 1, -xyz\rangle$$

is isotropic so by [**13**, Corollary 2.12] there exists $t \in D\langle 1, -xyz\rangle$ with $-tyb \in D\langle 1, -z\rangle$. If $z \neq 1, xy$, this yields $t \in X_2$, $-tyb \in X_2$, so

$$b = -yt(-tyb) \in -X_1X_2^2 = X_1X_2^2,$$

a contradiction. Thus $z = 1$ or xy so

$$\begin{aligned} X_1D\langle 1, xb\rangle \cap D\langle 1, yb\rangle &= \{1, xy\}D\langle 1, xb\rangle \cap D\langle 1, yb\rangle \\ &= \{1, yb\}D\langle 1, xb\rangle \cap D\langle 1, yb\rangle \\ &= \{1, yb\}(D\langle 1, xb\rangle \cap D\langle 1, yb\rangle) = \{1, yb\} \end{aligned}$$

using claim 2.

Claim 4. $x, y \in X_1$, $x \neq y$ implies

$$X_1D\langle 1, xb\rangle \cap X_1D\langle 1, yb\rangle = X_1\{1, b\}.$$

For

$$\begin{aligned} X_1D\langle 1, xb\rangle \cap X_1D\langle 1, yb\rangle &= X_1(X_1D\langle 1, xb\rangle \cap D\langle 1, yb\rangle) \\ &= X_1\{1, yb\} = X_1\{1, b\} \end{aligned}$$

using claim 3.

Now consider the Pfister form

$$p = \langle 1, a, b, ab\rangle \cong \langle 1, a\rangle \oplus b\langle 1, a\rangle.$$

$D(p)$ is a group by [**13**, Corollary 3.2]. Also, by [**13**, Proposition 2.10],

$$\begin{aligned} D(p) = \cup\{D\langle x, yb\rangle | x, y \in X_1\} &= \cup\{xD\langle 1, yb\rangle | x, y \in X_1\} \\ &\cup\{X_1D\langle 1, xb\rangle | x \in X_1\}. \end{aligned}$$

Let $V = D(p)/X_1\{1, b\}$ and let

$$V_x = X_1D\langle 1, xb\rangle / X_1\{1, b\}\ \forall\, x \in X_1.$$

Thus V is a group of exponent 2, V_x is a subgroup of V for all $x \in X_1$, $V = \cup\{V_x | x \in X_1\}$, and by claim 4, $V_x \cap V_y = 1$ for $x, y \in X_1$, $x \neq y$.

Claim 5. There exists $x \in X_1$ with $V_x = 1$. For suppose not. Then for all $x \in X_1$, there exists $s_x \in V_x$, $s_x \neq 1$. Let V' denote the span of $\{s_x | x \in X_1\}$ in V and let $V_x' = V' \cap V_x$. Then $|V'| < \infty$ since X_1 is finite, $V' = \cup\{V_x' | x \in X_1\}$, and $V_x' \cap V_y' = 1$ for all $x, y \in X_1$, $x \neq y$. Also $s_x \in V_x'$, so $V_x' \neq 1$ for all $x \in X_1$. Thus, by counting,

$$|V'| = \sum_{x \in X_1} (|V_x'| - 1) + 1,$$

i.e.,

$$|V'| = \sum_{x \in X_1} |V_x'| - |X_1| + 1.$$

https://doi.org/10.4153/CJM-1982-089-1 Published online by Cambridge University Press

Since $|V'|$, $|X_1|$, and all the $|V_x'|$, $x \in X_1$ are even, we have a contradiction here.

Now take x as in claim 5. By claim 1,

$$D\langle 1, xb\rangle \cap X_1 = 1,$$

and by claim 5,

$$X_1 D\langle 1, xb\rangle = X_1\{1, b\} = X_1\{1, xb\}.$$

Thus $D\langle 1, xb\rangle = \{1, xb\}$. Also

$$p = \langle 1, a, b, ab\rangle \cong \langle 1, a, xb, xab\rangle \cong \langle 1, xb\rangle \oplus a\langle 1, xb\rangle,$$

so by [**13**, Proposition 2.10],

$$D(p) = \cup \{D\langle r, as\rangle | r, s \in D\langle 1, xb\rangle\}.$$

Since $D\langle 1, xb\rangle = \{1, xb\}$, this reduces to

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

A group cannot be a union of two proper subgroups. Thus either

$$\{1, b\}D\langle 1, a\rangle \subseteq \{1, a\}D\langle 1, xab\rangle = D(p), \quad \text{or}$$
$$\{1, a\}D\langle 1, xab\rangle \subseteq \{1, b\}D\langle 1, a\rangle = D(p).$$

In the first case

$$D\langle 1, a\rangle \subseteq \{1, a\}D\langle 1, xab\rangle$$

and by claim 1,

$$D\langle 1, a\rangle \cap D\langle 1, xab\rangle = 1,$$

so $D\langle 1, a\rangle = \{1, a\}$, a contradiction. Thus we must be in the second case. Since $D\langle 1, b\rangle \subseteq D(p)$ this yields

$$D\langle 1, b\rangle \subseteq \{1, b\}D\langle 1, a\rangle.$$

But by claim 1,

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

This implies $D\langle 1, b\rangle = \{1, b\}$ and completes the proof.

A *non-real preorder* (for the Witt ring R) is defined to be a subgroup $H \subseteq G$ with $-1 \in H$ satisfying: $a \in H, a \neq -1 \Rightarrow D\langle 1, a\rangle \subseteq H$.

(2.5) *Examples*. (i) The basic part B; (ii) any subgroup H of G with $B \subseteq H$; (iii) $\{1\}$, if R has characteristic 2; (iv) $\{\pm 1\}$, if $D\langle 1, 1\rangle = 1$ (i.e., if R is reduced). Verification of these assertions is elementary. Also, if H is any subgroup of G one verifies easily that H is a non-real preorder if and only if $H \cap B$ is a non-real preorder.

Here is another elementary observation: suppose H is a non-real preorder, $a \in H$, $a \neq -1$, and the subsets $X_1, X_2, \ldots$ of G are defined as in Theorem 2.4. Then $X_1 \subseteq H$ and, by an easy induction, $X_i \subseteq H$ $\forall\, i > 1$.

(2.6) COROLLARY. *Suppose there is $a \in G$ such that $a \neq -1$, a is not rigid, and $|D\langle 1, a\rangle| < \infty$. Also suppose that the sets X_i are defined as in Theorem 2.4. Then*

$$B = \pm X_1X_3 \cup X_1X_2^2.$$

Proof. Since B is a non-real preorder, one inclusion is elementary. To prove the other note, by the proof of Theorem 2.4 $-X_1X_2 = X_1X_2$. Thus

$$\begin{aligned}\pm X_1X_3 \cup X_1X_2^2 &= \pm X_1X_3 \cup \pm X_1X_2^2 \\ &= \pm(-X_1X_3 \cup X_1X_2^2).\end{aligned}$$

Thus if $b \notin \pm X_1X_3 \cup X_1X_2^2$ then, by Theorem 2.4, b and $-b$ are both rigid, and clearly $b \neq \pm 1$. Thus

$$B \subseteq \pm X_1X_3 \cup X_1X_2^2.$$

(2.7) COROLLARY. *Suppose H is a non-real preorder in G and that there exists $a \in H$ such that $a \neq -1$, a is not rigid, and $|D\langle 1, a\rangle| < \infty$. Then $B \subseteq H$.*

Proof. Since H is a non-real preorder

$$\pm X_1X_3 \cup X_1X_2^2 \subseteq H.$$

However, by Corollary 2.6, $\pm X_1X_3 \cup X_1X_2^2 = B$.

Here is a simple application of Corollary 2.7; see also [**3**, Proposition 1].

(2.8) COROLLARY. *Suppose $D\langle 1, 1\rangle = \{\pm 1\}$ and $-1 \neq 1$ (i.e.,* char $(R) \neq 2$). *Then $B = \{\pm 1\}$ and $R \cong \mathbf{Z}/4\mathbf{Z}[G/\{\pm 1\}]$.*

Proof. Take $H = \{\pm 1\}$, $a = 1$ and apply Corollary 2.7. This yields $B \subseteq \{\pm 1\}$, so $B = \{\pm 1\}$. The assertion concerning R follows from Theorem 2.2.

The following result is implicit from results in [**1**] and [**3**]. We state it here explicitly since it serves to motivate Theorem 3.10.

(2.9) COROLLARY. *Suppose* char $(R) \neq 0$. *Then there exists $a \in G$ with $|D\langle 1, a\rangle| \leqq 2$ if and only if R is $\mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/4\mathbf{Z}$, or a group ring.*

Proof. ($\Leftarrow$) is trivial. To prove ($\Rightarrow$) assume char $(R) \neq 0$ and that there exists $a \in G$ with $|D\langle 1, a\rangle| \leqq 2$. If $a \neq 1$, this implies a is rigid, so $-a$ is also rigid. (Note that the proof of [**3**, Theorem 1] is valid in the abstract sense considered here, see [**16**, Corollary 4.15].) If $a \neq \pm 1$, this implies $B \neq G$, so R is a group ring by Corollary 2.3. If $a = -1$, then

$|G| \leqq 2$, and the result is trivial. This leaves the case $a = 1 \neq -1$. Thus $D\langle 1, 1\rangle = \{1, b\}$. If $b = -1$, then $R \cong \mathbf{Z}/4\mathbf{Z}[G/\{\pm 1\}]$ by Corollary 2.8. Suppose $b \neq -1$. By [**13**, Proposition 2.10],

$$D\langle 1, 1, 1\rangle = D\langle 1, 1\rangle \cup D\langle 1, b\rangle = D\langle 1, b\rangle,$$

and by a simple induction,

$$D(n \times \langle 1\rangle) = D\langle 1, b\rangle \ \forall\, n \geqq 3.$$

Since char $(R) \neq 0$, this implies $-1 \in D\langle 1, b\rangle$, so $-b \in D\langle 1, 1\rangle = \{1, b\}$. This contradicts $-1 \neq 1$, $b \neq -1$. Thus this case cannot occur.

(2.10) *Remarks.* (i) It may be possible to remove the hypothesis that $|D\langle 1, a\rangle| < \infty$ in Theorem 2.4 and Corollaries 2.6 and 2.7. In any case, this hypothesis is not restrictive if $|G| < \infty$.

(ii) Suppose $|G| < \infty$. Then one verifies easily using Corollary 2.7 that if H is any non-real preorder, then its intersection with B is either B or $\{\pm 1\}$. Further, the latter case can only occur if either char $(R) = 2$ or R is reduced or $B = \{\pm 1\}$. In view of a remark in 2.5, this completely classifies non-real preorders in the finite case.

3. Products and orthogonal decompositions. The product of Witt rings $R_1, \ldots, R_k$ in the category of Witt rings will be denoted by $R_1 \triangle \ldots \triangle R_k$. Thus $S = R_1 \triangle \ldots \triangle R_k$ is the subring of the usual direct product ring $R_1 \times \ldots \times R_k$ consisting of all elements $(f_1, \ldots, f_k)$ satisfying

$$\dim_2 (f_i) = \dim_2 (f_j) \ \forall\, i, j = 1, \ldots, k,$$

where $\dim_2$ denotes the mod 2 dimension mapping. Also,

$$G_S = G_{R_1} \times \ldots \times G_{R_k}.$$

Thus, any decomposition $R \cong R_1 \triangle \ldots \triangle R_k$ induces a group isomorphism

$$G \cong G_{R_1} \times \ldots \times G_{R_k}.$$

Denote by G_i the subgroup of G corresponding to G_{R_i} for $i = 1, \ldots, k$. Thus $G = G_1 \times \ldots \times G_k$ and this decomposition is orthogonal in the sense that if $x \in G_i$, $y \in G_j$, $i \neq j$, then $q(x, y) = 0$. We denote this fact by writing $G = G_1 \perp \ldots \perp G_k$. Conversely, if an arbitrary orthogonal decomposition $G_1 \perp \ldots \perp G_k$ of G is given, then $-1 \in G$ decomposes as $-1 = e_1 \ldots e_k$ with $e_i \in G_i$ and one verifies easily that the restriction of q to G_i (denote this by q_i) defines a quaternionic structure on G_i with e_i serving as the distinguished element. Denote the Witt ring associated to q_i by R_i, $i = 1, \ldots, k$, and define the subsets Q_i of Q by

$$Q_i = \{q(x, y) | x, y \in G_i\} = \{q(x, y) | x \in G_i, y \in G\}.$$

Then there is a natural morphism

$$\phi: R_1 \triangle \dots \triangle R_k \to R$$

and we have the following internal characterization of direct products:

(3.1) THEOREM. *Let $G_1 \perp \dots \perp G_k$ be an orthogonal decomposition of G. Then, with the above notation, $\phi: R_1 \triangle \dots \triangle R_k \to R$ is an isomorphism if and only if $Q_i \cap Q_j = 0$ holds for all $i, j \in \{1, \dots, k\}$, $i \neq j$.*

Proof. See [**13**, p. 107].

Any Witt ring decomposes as $R \cong R \triangle \mathbf{Z}/2\mathbf{Z}$. A Witt ring R is said to be *indecomposible* if $R \not\cong \mathbf{Z}/2\mathbf{Z}$ and if $R \cong R_1 \triangle R_2 \Rightarrow R_i \cong \mathbf{Z}/2\mathbf{Z}$ for $i = 1$ or 2. Let Δ_2 denote the cyclic group of order 2. Every group ring is indecomposible with one exception: $\mathbf{Z}[\Delta_2] \cong \mathbf{Z} \triangle \mathbf{Z}$. R is said to be *degenerate* if $\exists\ x \in G, x \neq 1$ which satisfies $q(x, y) = 0\ \forall\ y \in G$. The only degenerate indecomposible Witt rings are $\mathbf{Z}/4\mathbf{Z}$ and $\mathbf{Z}/2\mathbf{Z}[\Delta_2]$. If R is non-degenerate and expressible as a product of indecomposibles (clearly the latter is always true if $|G| < \infty$) then this expression is unique, and moreover any two such decompositions of R as a product of indecomposibles give rise to exactly the same orthogonal decomposition of G; see [**13**, Theorem 5.9]. If R is degenerate this is no longer true, for example,

$$R \triangle \mathbf{Z}/2\mathbf{Z}[\Delta_2] \cong R \triangle \mathbf{Z}/4\mathbf{Z},$$

if char $(R) \neq 2$. However, any decomposition $R \cong R_1 \triangle \dots \triangle R_k$ can be modified to satisfy

(3.2) If char $(R) \neq 2$, then no R_i is isomorphic to $\mathbf{Z}/2\mathbf{Z}[\Delta_2]$.

Any decomposition $R \cong R_1 \triangle \dots \triangle R_k$ with $R_1, \dots, R_k$ indecomposible and satisfying (3.2) is called a *normalized decomposition* of R. The main fact concerning these is the following:

(3.3) THEOREM. *If $R_1 \triangle \dots \triangle R_k$ and $S_1 \triangle \dots \triangle S_l$ are normalized decompositions of R, then $k = l$ and, after reindexing suitably, $R_i \cong S_i$ for $i = 1, \dots, k$.*

Proof. See [**13**, Theorem 5.12].

By Theorem 3.1, if $G_1 \perp \dots \perp G_k$ is an orthogonal decomposition of G which does not correspond to a product decomposition of R, then $\exists\ i, j \in \{1, \dots, k\}$, $i \neq j$, with $Q_i \cap Q_j \neq 0$. To get an example of such a decomposition, consider a non-degenerate Witt ring R with $|Q| = 2$, and $8 \leqq |G| < \infty$. Such Witt rings are completely classified; see, for example, [**13**, Chapter 5, § 3]. In particular, if R is any such Witt ring, then G has a (non-canonical) orthogonal decomposition $G_1 \perp \dots \perp G_k$ with $|G_1| = 2$ or 4 and with $|G_i| = 4$ for $i \geqq 2$. Also $Q_i = Q$ for all $i = 1, \dots, k$, so certainly $Q_i \cap Q_j \neq 0$ if $i \neq j$. In view of this example, the following result is of some interest.

(3.4) THEOREM. *Suppose* $G_1 \perp \dots \perp G_k$ *is an orthogonal decomposition of* G *and notation is as in Theorem* 3.1. *Suppose also, for each* $i \in \{1, \dots, k\}$, *that either* R_i *is an indecomposible group ring or that* $|Q_i| \leqq 2$. *Finally, suppose* $Q_i \cap Q_j \neq 0$ *for some* $i, j \in \{1, \dots, k\}$, $i \neq j$. *Then* $|Q_i| = |Q_j| = 2$.

Proof. Suppose the result is false. Then $\exists\, i, j \in \{1, \dots, k\}, i \neq j$, with $Q_i \cap Q_j \neq 0$, $|Q_i| \geqq 2$, $|Q_j| > 2$. Reindexing, we may suppose $i = 1$, $j = 2$. We can also suppose $k = 2$. Otherwise, let $H = G_1 \perp G_2$. Then

$$G = H \perp G_3 \perp \dots \perp G_k$$

so q induces a quaternionic structure on H. Now just replace R by the Witt ring associated to this quaternionic structure. Since $|Q_2| > 2$, R_2 is an indecomposible group ring. Let G_2' be any subgroup of index 2 in G_2 which contains the basic part of R_2. Note that since $|Q_2| > 2$ and R_2 is an indecomposible group ring, it follows that $|G_2| \geqq 8$, so $|G_2'| \geqq 4$. For $a \in G$, we denote the set $\{q(a, b)|b \in G\}$ by $Q(a)$ as in [**13**, p. 93]. Note that if $a \in G_i$ for $i = 1$ or 2, then $Q(a)$ is equal to

$$Q_i(a) = \{q(a, b)|b \in G_i\}.$$

This is because G_1 and G_2 are orthogonal. Since $Q_1 \cap Q_2 \neq 0$, there exist $x, y \in G_1$ with $q(x, y) \neq 0$ and $q(x, y) \in Q_2$. Thus $Q_1(x) \cap Q_2 \neq 0$. Fix any $x \in G_1$ with this property.

Claim 1. There exists $a \in G_2'$, $a \neq 1$, and $t \in G_2 \backslash G_2'$ with $q(a, t) \in Q_1(x)$. For there exists $y \in G_1$ with $q(x, y) \neq 0$, $q(x, y) \in Q_2$. Thus there exist $b, c \in G_2$ with $q(x, y) = q(b, c)$. Let e_i denote the component of -1 in G_i for $i = 1, 2$. Thus

$$e_2 \in G_2' \quad \text{and} \quad q(b, c) = q(b, e_2bc).$$

Thus, if either b or c lies in $G_2 \backslash G_2'$ we are done. This leaves the case b, $c \in G_2'$. In this case pick any $t \in G_2 \backslash G_2'$ and note that

$$\begin{aligned} q(xt, yc) = q(xt, y) * q(xt, c) &= q(x, y) * q(t, c) \\ &= q(b, c) * q(t, c) = q(bt, c) = q(xbt, c). \end{aligned}$$

For the definition of $*$, see [**13**, p. 92]. Thus, by the linkage property of q, there exists $z \in G$ satisfying

$$(3.5) \qquad q(xt, yc) = q(xt, z) = q(xbt, z) = q(xbt, c).$$

Let z_1, z_2 denote the components of z in G_1 and G_2. Thus, by (3.5), $q(b, z) = 0$, i.e., $q(b, z_2) = 0$. Since $b \neq 1$ (after all, $q(b, c) \neq 0$) it follows, using the fact that G_2' is a non-real preorder in G_2, that $z_2 \in G_2'$. Also we have, by (3.5) again, that $q(xt, cyz) = 0$, i.e., $q(x, cyz) = q(t, cyz)$, i.e., $q(x, yz_1) = q(t, cz_2)$. Take $a = cz_2$. Note $a \neq 1$, since if $a = 1$, then $z_2 = c$ so

$$0 = q(b, z_2) = q(b, c) \neq 0.$$

Since $a \in G_2'$, we are done.

Claim 2. For each $b \in G_2'$, there exists $t_b \in G_2 \backslash G_2'$ such that $q(b, t_b) \in Q_1(x)$. For choose a, t as in claim 1. Choose $y \in G_1$ such that $q(x, y) = q(a, t)$. Then

$$\begin{aligned} q(xb, yt) = q(x, yt) * q(b, yt) = q(x, y) * q(b, t) &= q(a, t) * q(b, t) \\ &= q(ab, t) = q(xab, t). \end{aligned}$$

Thus by linkage, there exists $z \in G$ with

$$(3.6) \qquad q(xb, yt) = q(xb, z) = q(xab, z) = q(xab, t).$$

Thus $q(a, z) = 0$, i.e., $q(a, z_2) = 0$. As before, this implies $z_2 \in G_2'$. Also, by (3.6) $q(xb, yzt) = 0$, i.e., $q(x, yzt) = q(b, yzt)$, i.e., $q(x, yz_1) = q(b, z_2t)$. Take $t_b = tz_2$.

Claim 3. For $a \in G_2'$, either

$$q(a, b) \in Q_1(x) \ \forall\, b \in G_2'$$

or

$$q(e_2at_a, b) \in Q_1(x) \ \forall\, b \in G_2'.$$

Here t_a is as in claim 2, and e_2 is the component of -1 in G_2. To prove this, fix $a \in G_2'$ and pick $y \in Q_1(x)$ such that $q(x, y) = q(a, t_a)$. Then for all $b \in G_2'$,

$$\begin{aligned} q(xb, ya) = q(x, ya) * q(b, ya) = q(x, y) * q(b, a) &= q(a, t_a) * q(b, a) \\ &= q(bt_a, a) = q(xbt_a, a) \end{aligned}$$

so by linkage there exists $z \in G$ with

$$(3.7) \qquad q(xb, ya) = q(xb, z) = q(xbt_a, z) = q(xbt_a, a).$$

This yields $0 = q(t_a, z) = q(t_a, z_2)$. Since e_2t_a is in $G_2 \backslash G_2'$, it is rigid in G_2, so $z_2 = 1$ or e_2t_a. Also by (3.7),

$$q(b, az_2) = q(x, yz_1) \in Q_1(x),$$

so either $q(a, b) \in Q_1(x)$ (if $z_2 = 1$) or $q(e_2at_a, b) \in Q_1(x)$ (if $z_2 = e_2t_a$). Finally,

$$\{b \in G_2' | q(a, b) \in Q_1(x)\} \quad \text{and}$$
$$\{b \in G_2' | q(b, ae_2t_a) \in Q_1(x)\}$$

are both subgroups of G_2'. By the above, their union is G_2', so one of them is all of G_2'.

Claim 4. There exists $t \in G_2 \backslash G_2'$ with $q(b, t) \in Q_1(x) \ \forall\, b \in G_2'$ (i.e., with $Q_2(t) \subseteq Q_1(x)$). First note the parenthetical remark follows from

https://doi.org/10.4153/CJM-1982-089-1 Published online by Cambridge University Press

the main statement since $q(b, t) = q(e_2tb, t)$ holds for every $b \in G_2$. First suppose $q(a, b) \in Q_1(x)$ holds for every $a, b \in G_2'$. In this case take t arbitrary in $G_2 \backslash G_2'$. Then for $b \in G_2'$, $t_b = ta$ for some $a \in G_2'$, so

$$q(b, t) = q(b, t_b) * q(b, a) \in Q_1(x)$$

by the assumption and the definition of t_b. On the other hand, if we are not in this case, then by claim 3, there exists $a \in G_2'$ with

$$q(e_2at_a, b) \in Q_1(x) \ \forall\ b \in G_2'.$$

In this case, take $t = e_2at_a$. This proves the claim.

Now choose t as in claim 4. Thus $Q_2(t) \subseteq Q_1(x)$. Since $t \in G_2 \backslash G_2'$, e_2t is rigid in G_2, so by [**13**, p. 93],

$$Q_2(t) \cong G_2/\{1, e_2t\}.$$

Since $|G_2| \geqq 8$, this implies $|Q_2(t)| \geqq 4$. Thus $|Q_1(x)| \geqq 4$, so $|Q_1| \geqq 4$. Thus R_1 is also an indecomposible group ring and $|G_1| \geqq 8$. Choose a subgroup G_1' of index 2 in G_1 and containing the basic part of G_1. We can play exactly the same game with G_1 that we have been playing with G_2. Let $b \in G_2'$, $b \neq 1$. Then by claim 4,

$$q(b, t) \in Q_1(x) \subseteq Q_1.$$

Also $q(b, t) \neq 0$ since $t \in G_2 \backslash G_2'$ and $b \neq 1$. Thus

$$Q_2(b) \cap Q_1 \neq 0,$$

so using b as x in claim 4 and reversing the roles of G_1 and G_2, there exists $u \in G_1 \backslash G_1'$ with $Q_1(u) \subseteq Q_2(b)$. This certainly implies $Q_1(u) \cap Q_2 \neq 0$, so again by claim 4, but using u instead of x, there exists $t' \in G_2 \backslash G_2'$ with $Q_2(t') \subseteq Q_1(u)$. Thus $Q_2(t') \subseteq Q_2(b)$. On the other hand, $|G_2| \geqq 8$, so $|G_2'| \geqq 4$. Thus there exists $a \in G_2'$, $a \neq 1, b$. Then $q(a, t') \in Q_2(t')$, but since the elements of $G_2 \backslash G_2'$ are all rigid in G_2, $q(a, t') \in Q_2(b)$ is impossible. This contradiction proves the theorem.

(3.8) COROLLARY. *Suppose the decomposition $G_1 \perp \ldots \perp G_k$ of G has the properties:*

(i) *For all $i = 1, \ldots, k$, either $|Q_i| \leqq 2$ or R_i is an indecomposible group ring, and*

(ii) *The sets Q_i with $|Q_i| = 2$ are all distinct. Then*

$$\phi: R_1 \cap \ldots \cap R_k \rightarrow R$$

is an isomorphism.

Proof. By condition (ii) and Theorem 3.4, $Q_i \cap Q_j = 0$ holds for all $i, j \in \{1, \ldots, k\}$, $i \neq j$. The result follows from this and Theorem 3.1.

(3.9) *Remark.* Condition (ii) of Corollary 3.8 is not really restrictive. For suppose a decomposition $G = G_1 \perp \ldots \perp G_k$ has been found satisfying condition (i) of Corollary 3.8. Consider the subset J of $\{1, \ldots, k\}$ consisting of those i with $|Q_i| = 2$. Put an equivalence relation $\sim$ on J by defining $i \sim j$ to mean $Q_i = Q_j$. Then by grouping together those factors G_i, $i \in J$ which are equivalent via $\sim$, one obtains a coarser decomposition of G which is still orthogonal and satisfies both conditions of Corollary 3.8. This same method is used in the proof of [**13**, Theorem 5.14].

We now give a result extending Corollary 2.9 in case char $(R) = 2$. Although the hypothesis is very special, it is suspected that this is just one of a class of similar results involving Witt rings R which have the property that there exists $a \in G$ with $|D\langle 1, a\rangle| < \infty$.

(3.10) THEOREM. *Suppose* char $(R) = 2$. *Then there exists* $a \in G$ *with* $|D\langle 1, a\rangle| \leqq 4$ *if and only if* R *is* $\mathbf{Z}/2\mathbf{Z}$, *a group ring, or a product of two group rings.*

Proof. $(\Leftarrow)$ is clear. To prove $(\Rightarrow)$ suppose char $(R) = 2$ (i.e., that $-1 = 1$) and that there exists $a \in G$ with $|D\langle 1, a\rangle| \leqq 4$. If $|D\langle 1, a\rangle| \leqq 2$, the result follows from Corollary 2.9. Thus we can assume $|D\langle 1, a\rangle| = 4$ and that

$$|D\langle 1, c\rangle| \geqq 4 \;\forall\; c \in G.$$

If $a = 1$ then $|G| = 4$. Examining the Witt rings of this type (e.g. see the list in [**13**, p. 177]) we see

$$R \cong \mathbf{Z}/2\mathbf{Z}[\Delta_2] \sqcap \mathbf{Z}/2\mathbf{Z}[\Delta_2].$$

This leaves the case that $a \neq 1$. In this case the four elements of $D\langle 1, a\rangle$ are $1, a, b, ab$ for some $b \in G$. Note that $D\langle 1, a\rangle \subseteq D\langle 1, b\rangle$ and similarly $D\langle 1, a\rangle \subseteq D\langle 1, ab\rangle$, so

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

Before getting into the main part of the proof we need to eliminate one more easy case. Suppose one of $D\langle 1, b\rangle$, $D\langle 1, ab\rangle$ is equal to G, say $D\langle 1, b\rangle = G$. Let H be a subgroup of index 2 in G with $a \in H$, $b \notin H$. Thus $G = \{1, b\} \perp H$ and, by Theorem 3.1,

$$R \cong \mathbf{Z}/2\mathbf{Z}[\Delta_2] \sqcap S$$

where S is the Witt ring associated to the restriction of q to H. Since

$$D\langle 1, a\rangle \cap H = \{1, a\},$$

a is rigid in H, so S is a group ring by Corollary 2.9. Thus we are left with the case where $D\langle 1, b\rangle$ and $D\langle 1, ab\rangle$ are proper subgroups of G.

Fix an element $t \in G$. Later we will assume

$$t \notin D\langle 1, b\rangle \cup D\langle 1, ab\rangle,$$

but we don't need this for the first claim.

Claim 1.

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

One inclusion is clear. To prove the other, suppose

$$u \in D\langle 1, t\rangle \cap D\langle 1, a\rangle D\langle 1, bt\rangle.$$

We wish to show that u or $tu \in D\langle 1, b\rangle$. By assumption there exists $v \in D\langle 1, a\rangle$ with $q(uv, bt) = 0$. Thus $q(u, bt) = q(v, bt)$, i.e., $q(u, b) = q(v, t)$, and hence

$$q(ut, b) = q(u, b) * q(t, b) = q(v, t) * q(t, b) = q(vb, t).$$

Thus, replacing u by ut if necessary, we can assume $v = 1$ or a. Suppose $v = 1$. Then $q(u, b) = 0$, so $u \in D\langle 1, b\rangle$. Suppose $v = a$. Then $q(u, b) = q(a, t)$ so by linkage there exists $w \in D\langle 1, a\rangle$ with $q(u, b) = q(wt, b)$. Thus $q(tuw, b) = 0$. Since $q(w, b) = 0$ (recall, $D\langle 1, a\rangle \subseteq D\langle 1, b\rangle$), this yields $q(tu, b) = 0$, i.e., $tu \in D\langle 1, b\rangle$. This proves the claim.

Now suppose $t \notin D\langle 1, b\rangle \cup D\langle 1, ab\rangle$. Note this hypothesis is equivalent to $D\langle 1, a\rangle \cap D\langle 1, t\rangle = 1$. Note also that

$$ut \notin D\langle 1, b\rangle \cup D\langle 1, ab\rangle$$

holds for every $u \in D\langle 1, a\rangle$.

Claim 2. $D\langle 1, t\rangle \cap D\langle 1, a\rangle D\langle 1, at\rangle = \{1, t\}$ or $\{1, t, u, tu\}$ with $u \in D\langle 1, b\rangle$, $tu \in D\langle 1, ab\rangle$. For let

$$u \in D\langle 1, t\rangle \cap D\langle 1, a\rangle D\langle 1, at\rangle.$$

Thus there exists $v \in D\langle 1, a\rangle$ with $q(uv, at) = 0$, so $q(u, a) = q(v, t)$. If $v = a$, this yields $q(ut, a) = 0$, so

$$ut \in D\langle 1, a\rangle \cap D\langle 1, t\rangle = 1,$$

i.e., $u = t$. Otherwise, by linkage, there exists $w \in D\langle 1, a\rangle$ with

$$q(v, t) = q(v, uw) = q(a, uw),$$

so $q(av, uw) = 0$. Since $av \in D\langle 1, a\rangle$, $q(av, w) = 0$, so $q(av, u) = 0$. Since $av \neq 1$, $av = a, b$, or ab. Therefore

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

This proves

$$(3.11) \quad D\langle 1, t\rangle \cap D\langle 1, a\rangle D\langle 1, at\rangle \subseteq \{t\} \cup D\langle 1, b\rangle \cup D\langle 1, ab\rangle.$$

Suppose

$$D\langle 1, t\rangle \cap D\langle 1, a\rangle D\langle 1, at\rangle \neq \{1, t\}.$$

Then there exists u in this intersection, $u \neq 1$, and $u \in D\langle 1, b\rangle$ (say). tu is also in this intersection, and since $t \notin D\langle 1, b\rangle$, it follows from (3.11) that $tu \in D\langle 1, ab\rangle$. Now suppose x lies in this intersection and in $D\langle 1, b\rangle$, $x \neq 1, u$. Then $u, x, ux \in D\langle 1, b\rangle$ so, as above, $tu, tx, tux \in D\langle 1, ab\rangle$. Thus

$$t = (tu)(tx)(tux) \in D\langle 1, ab\rangle.$$

This is a contradiction, proving the claim.

It follows that

$$D\langle 1, a\rangle D\langle 1, t\rangle \cap D\langle 1, a\rangle D\langle 1, at\rangle$$
$$= D\langle 1, a\rangle (D\langle 1, t\rangle \cap D\langle 1, a\rangle D\langle 1, at\rangle)$$

is either $D\langle 1, a\rangle\{1, t\}$ or $D\langle 1, a\rangle\{1, t, u, tu\}$ with u as in claim 2. Note

$$t = b(bt) \in D\langle 1, a\rangle D\langle 1, bt\rangle$$

and also (if we are in the second case)

$$u \in D\langle 1, t\rangle \cap D\langle 1, b\rangle \subseteq D\langle 1, bt\rangle \subseteq D\langle 1, b\rangle D\langle 1, bt\rangle.$$

Thus

$$D\langle 1, a\rangle D\langle 1, t\rangle \cap D\langle 1, a\rangle D\langle 1, at\rangle \subseteq D\langle 1, a\rangle D\langle 1, bt\rangle,$$

and similarly,

$$D\langle 1, a\rangle D\langle 1, t\rangle \cap D\langle 1, a\rangle D\langle 1, at\rangle \subseteq D\langle 1, a\rangle D\langle 1, abt\rangle.$$

Note also, by symmetry, claim 2 holds with bt replacing t, so this yields

$$D\langle 1, a\rangle D\langle 1, t\rangle \cap D\langle 1, a\rangle D\langle 1, at\rangle$$
$$= D\langle 1, a\rangle D\langle 1, bt\rangle \cap D\langle 1, a\rangle D\langle 1, abt\rangle.$$

Call this group T. Consider also the 2-fold Pfister form $p = \langle 1, a\rangle \otimes \langle 1, t\rangle$. By [**13**, Proposition 2.10],

$$D(p) = \cup \{D\langle 1, a\rangle D\langle 1, xt\rangle | x \in D\langle 1, a\rangle\}.$$

Claim 3. One of the groups $D\langle 1, a\rangle\ \langle D1, xt\rangle$, $x \in D\langle 1, a\rangle$, is equal to T. For consider the group $H = D(p)/T$ and the subgroups

$$H_{xt} = D\langle 1, a\rangle D\langle 1, xt\rangle / T.$$

Thus

$$H = \cup \{H_{xt} | x \in D\langle 1, a\rangle\},$$

$$H_t \cap H_{at} = 1 \quad \text{and} \quad H_{bt} \cap H_{abt} = 1.$$

If $H_{xt} \cap H_{yt} = 1\ \forall\ x, y \in D\langle 1, a\rangle, x \neq y$, then as in the proof of Theorem 2.4, there exists $x \in D\langle 1, a\rangle$ with $H_{xt} = 1$. Thus we may assume there exists $x, y \in D\langle 1, a\rangle$, $x \neq y$, with $H_{xt} \cap H_{yt} \neq 1$. Replacing t by xt and

b by ab if necessary, we can assume $H_t \cap H_{bt} \neq 1$. Pick $\alpha \in H_t \cap H_{bt}$, $\alpha \neq 1$. We can assume $H_t \cup H_{bt} \neq H$. (Otherwise, one of H_t, H_{bt} is H, so, since $H_t \cap H_{at} = 1$, $H_{bt} \cap H_{abt} = 1$, one of H_{at}, H_{abt} is 1.) Therefore, there exists $\beta \in H \backslash (H_t \cup H_{bt})$. Replacing t by bt if necessary, we can assume $\beta \in H_{at}$. Thus $\alpha\beta \notin H_t \cup H_{bt}$ and $\alpha\beta \notin H_{at}$ (otherwise $\alpha \in H_t \cap H_{at} = 1$) so $\alpha\beta \in H_{abt}$.

Now pick $c, d \in D(p)$ representing the cosets α, β. Using claim 1 we can assume $c \in D\langle 1, t\rangle \cap D\langle 1, b\rangle$. We can also assume $d \in D\langle 1, at\rangle$ and that there exists $e \in D\langle 1, a\rangle$ with $cde \in D\langle 1, abt\rangle$. Thus $q(cde, abt) = 0$ so

$$(3.12) \quad q(c, a) * q(d, b) * q(e, t) = 0$$

and hence also

$$(3.13) \quad q(c, a) * q(dt, b) * q(eb, t) = 0.$$

Case 1. $e = 1$ or b. Then by (3.12) or (3.13), $q(c, a) = q(d', b)$ where $d' = d$ or dt. By linkage there exists $x \in D\langle 1, a\rangle$ with

$$q(c, a) = q(cx, a) = q(cx, b).$$

But $q(cx, b) = 0$. Thus $q(c, a) = 0$, so $c \in D\langle 1, a\rangle$, a contradiction to $c \notin T$.

Case 2. $e = a$ or ab. Then by (3.12) or (3.13) $q(ct, a) = q(d', b)$ where $d' = d$ or dt. By linkage, there exists $x \in D\langle 1, a\rangle$ with

$$q(ct, a) = q(ctx, a) = q(ctx, b).$$

Since $q(ctx, b) = q(t, b)$, this yields $q(ct, a) = q(t, b)$, i.e., $q(c, a) = q(t, ab)$. Again by linkage, there exists $y \in D\langle 1, a\rangle$ with $q(t, ab) = q(cy, ab)$ so

$$q(ab, cty) = q(ab, ct) = 0.$$

Thus ct lies in

$$D\langle 1, abt\rangle \cap D\langle 1, a\rangle D\langle 1, bt\rangle \subseteq T,$$

so $c \in T$, a contradiction. This proves the claim.

Claim 4. There exists $x \in D\langle 1, a\rangle$ such that $|D\langle 1, xt\rangle| = 4$, and for any such x,

$$D\langle 1, xt\rangle = \{1, xt, u, xtu\}$$

with $u \in D\langle 1, b\rangle$ and $xtu \in D\langle 1, ab\rangle$. Also

$$D\langle 1, b\rangle D\langle 1, ab\rangle = G.$$

For by claim 3, there exists $x \in D\langle 1, a\rangle$ with

$$D\langle 1, a\rangle D\langle 1, xt\rangle = T.$$

Since T has index at most 4 over $D\langle 1, a\rangle$ and

$$D\langle 1, xt\rangle \cap D\langle 1, a\rangle = 1,$$

this implies $|D\langle 1, xt\rangle| \leqq 4$. Thus $|D\langle 1, xt\rangle| = 4$, and T has exact index 4 over $D\langle 1, a\rangle$. Now suppose only that $x \in D\langle 1, a\rangle$, $|D\langle 1, xt\rangle| = 4$. Since

$$T \subseteq D\langle 1, a\rangle D\langle 1, xt\rangle,$$

this implies $T = D\langle 1, a\rangle D\langle 1, xt\rangle$, so

$$D\langle 1, xt\rangle \subseteq T \subseteq D\langle 1, a\rangle D\langle 1, axt\rangle.$$

Thus by claim 2 (applied to xt instead of t)

$$D\langle 1, xt\rangle = \{1, xt, u, xtu\}$$

with $u \in D\langle 1, b\rangle$, $xtu \in D\langle 1, ab\rangle$. In particular,

$$t = (u)(x)(xtu) \in D\langle 1, b\rangle D\langle 1, ab\rangle.$$

Since t is arbitrary not in $D\langle 1, b\rangle \cup D\langle 1, ab\rangle$, this proves $G = D\langle 1, b\rangle D\langle 1, ab\rangle$ and completes the proof of claim 4.

Now choose a basis $\{u_i | i \in I\}$ of $D\langle 1, b\rangle$ modulo $D\langle 1, a\rangle$ and a basis $\{v_k | k \in K\}$ of $D\langle 1, ab\rangle$ modulo $D\langle 1, a\rangle$. For $i \in I$, $k \in K$,

$$u_i v_k \notin D\langle 1, b\rangle \cup D\langle 1, ab\rangle$$

so modifying $u_i v_k$ by a suitable element of $D\langle 1, a\rangle$ and using claim 4, there exists $u_{ik} \in D\langle 1, b\rangle$ and $v_{ik} \in D\langle 1, ab\rangle$ such that

$$D\langle 1, u_{ik} v_{ik}\rangle = \{1, u_{ik}, v_{ik}, u_{ik} v_{ik}\}$$

with

$$u_{ik} v_{ik} \equiv u_i v_k (\text{mod } D\langle 1, a\rangle).$$

This implies

$$u_{ik} \equiv u_i (\text{mod } D\langle 1, a\rangle) \quad \text{and} \quad v_{ik} \equiv v_k (\text{mod } D\langle 1, a\rangle).$$

Claim 5. Suppose $i, j \in I$, $k, l \in K$. Then

$$u_{ik} \equiv u_{il} (\text{mod } \{1, ab\}) \quad \text{and} \quad v_{ik} \equiv v_{jk} (\text{mod } \{1, b\}).$$

By symmetry, it is enough to verify the first of these. For simplicity of notation, let $u = u_{ik}$, $u' = u_{il}$, $v = v_{ik}$, and $v' = v_{il}$. Also assume, contrary to the claim, that $uu' \in \{a, b\}$. The hypotheses imply

$$D\langle 1, u'v'\rangle \cap D\langle 1, uv\rangle = 1.$$

Thus, we are in a position to apply claim 4, but with uv replacing a and $u'v'$ replacing t. This implies that either $u' \in D\langle 1, u\rangle$ and $v' \in D\langle 1, v\rangle$ or $u' \in D\langle 1, v\rangle$ and $v' \in D\langle 1, u\rangle$. In the latter case

$$q(v, uu') = q(v, u) = 0.$$

Since $uu' \in \{a, b\}$ and $q(v, ab) = 0$, this yields $q(v, a) = 0$ contradicting $v \notin D\langle 1, a\rangle$. Thus we are in the former case.

Note $q(v', ab) = 0$ so $q(v', a) = q(v', b)$. Since $uu' \in \{a, b\}$ this yields

$$q(v', a) = q(v', uu') = q(v', u) = q(vv', u)$$

so by linkage there exists $x \in D\langle 1, a\rangle$ with

$$q(vv', u) = q(vv', xv'),$$

i.e.,

$$q(v', u) = q(vv', x).$$

Since $q(v, ab) = 0, q(v', ab) = 0$, we may, replacing x by xab if necessary, assume $x \in \{1, a\}$. Suppose $x = 1$. Thus $q(v', u) = 0$. Since $q(v', u') = 0$ this implies $q(v', uu') = 0$, i.e., either $q(v', a) = 0$, or $q(v', b) = 0$. Since $q(v', ab) = 0$, this yields $q(v', a) = 0$ in any case. This contradicts $v' \notin D\langle 1, a\rangle$. Next, suppose $x = a$. Then

$$q(v', u) = q(vv', a),$$

i.e.,

$$q(v, a) = q(v', ua).$$

Since $uu' \in \{a, b\}$, $uu'a \in \{1, ab\}$. Since $q(v', ab) = 0$, this implies

$$q(v', uu'a) = 0,$$

i.e.

$$q(v', ua) = q(v', u') = 0.$$

Thus $q(v, a) = 0$. This contradicts $v \notin D\langle 1, a\rangle$ and proves the claim.

Now let H_1 be the span of

$$\{u_{ik}|i \in I, k \in K\} \cup \{ab\},$$

and let H_2 be the span of

$$\{v_{ik}|i \in I, k \in K\} \cup \{b\}.$$

Since $G = D\langle 1, b\rangle D\langle 1, ab\rangle$, it follows that $G = H_1H_2$. Moreover, by claim 5,

$$q(u_{ik}, v_{jl}) = q(u_{ik}, v_{il}) = q(u_{il}, v_{il}) = 0 \,\forall\, i, j \in I \text{ and } \forall\, k, l \in K.$$

Thus $G = H_1 \perp H_2$. Also ab is rigid in H_1 and b is rigid in H_2. (After all, $D\langle 1, b\rangle = H_1\{1, b\}$, so $D\langle 1, b\rangle \cap H_2 = \{1, b\}$, and similarly, $D\langle 1, ab\rangle \cap H_1 = \{1, ab\}$.) Thus, by Corollary 2.9, the Witt ring R_i associated to the restriction of q to H_i is a group ring, $i = 1, 2$. By Theorem 3.4, this implies $R \cong R_1 \triangle R_2$, a product of two group rings.

4. The elementary types. All known Witt rings R with $|G| < \infty$ are built up by forming products and group rings from the following list:

(4.1) $\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/4\mathbf{Z}$, and $\mathbf{L}_{2k-1}$, $\mathbf{L}_{2k,0}$, and $\mathbf{L}_{2k,1}$, $k \geqq 2$.

(Recall the notation of [**13**, p. 95].) Any Witt ring R with $|G| < \infty$ which is built up in this way is said to be of *elementary type*. The following result is well known:

(4.2) THEOREM. *Every Witt ring of elementary type is realized as the Witt ring of a field of characteristic* $\neq 2$.

Proof. Of the Witt rings in the list (4.1), the first three are realized, for example, as the Witt rings of the real field, the complex field, and the field with three elements, respectively. The rest are realized as Witt rings of suitable extensions of the 2-adic completion of the rationals. If R is realized as the Witt ring of a field F, char $(F) \neq 2$, and Δ is a group of exponent 2 with $|\Delta| = 2^n$, then $R[\Delta]$ is realized as the Witt ring of the iterated power series field $F((t_1)) \ldots ((t_n))$. Finally, if R_i is realized as the Witt ring of a field of characteristic $\neq 2$ for $i = 1, \ldots, k$, then the same is true for $R_1 \triangle \ldots \triangle R_k$ by [**10**, Theorem 3.3].

We note in passing that the Witt rings in the list (4.1) have characteristic 0, 2, 4, or 8 ($\mathbf{L}_{2k,0}$, $\mathbf{L}_{2k,1}$, and $\mathbf{L}_{2k-1}$ have characteristic 2, 4 and 8 respectively). Thus the same is true for the elementary types. It is an open problem whether Witt rings R exist with $|G| < \infty$ and char $(R) \geqq 16$.

We now use Corollary 3.8 to develop another characterization of the elementary types. First we need a definition. We will say that the Witt ring R is a *weak product* of Witt rings $R_1, \ldots, R_k$ if G has an orthogonal decomposition $G_1 \perp \ldots \perp G_k$ with R_i being the Witt ring associated to the restriction of q to G_i for $i = 1, \ldots, k$. Note that, in general, there will be several ways of forming a weak product from given Witt rings $R_1, \ldots, R_k$. Note also that the usual product $R_1 \triangle \ldots \triangle R_k$ is one of these.

(4.3) COROLLARY. *Suppose the Witt ring R is a weak product of Witt rings of elementary type. Then R is also of elementary type.*

Proof. By assumption $G = G_1 \perp \ldots \perp G_k$ and the Witt ring R_i associated to G_i is of elementary type for $i = 1, \ldots, k$. Thus, R_i can be expressed as a product of indecomposibles of elementary type. Thus, replacing $G_1 \perp \ldots \perp G_k$ by a finer decomposition, we can assume each R_i is itself indecomposible. Being of elementary type, this implies each R_i is either a group ring or $|Q_i| \leqq 2$. Now using Remark 3.9, we can form a coarser decomposition where the factors are still of elementary type, but now satisfy both conditions of Corollary 3.8. Then, by Corollary 3.8, R is a product of Witt rings of elementary type, and is hence itself of elementary type.

(4.4) COROLLARY. *A Witt ring R with $|G| < \infty$ is of elementary type if and only if it can be built up from* $\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z}$, *and* $\mathbf{Z}/4\mathbf{Z}$ *by forming weak products and group rings.*

Proof. ($\Leftarrow$) follows from Corollary 4.3. ($\Rightarrow$) follows from the fact that the Witt rings $\mathbf{L}_{2k-1}$, $\mathbf{L}_{2k,0}$, and $\mathbf{L}_{2k,1}$, $k \geqq 2$ are all expressible as weak products of Witt rings from the set $\{\mathbf{Z}, \mathbf{Z}/4\mathbf{Z}[\Delta_2], \mathbf{Z}/2\mathbf{Z}[\Delta_2 \times \Delta_2]\}$.

We conclude this section by computing $e(n)$: = the number of Witt rings R of elementary type with $|G| = 2^n$. First we compute $e'(n)$: = the number of elementary types with $|G| = 2^n$ and char $(R) = 2$. Let $s'(n)$ denote the number of indecomposible elementary types with $|G| = 2^n$, char $(R) = 2$. Thus $s'(1) = 1$, $s'(2) = 1$, and for $n \geqq 3$, $s'(n)$ is either $e'(n-1)$ or $e'(n-1) + 1$ depending on whether n is odd or even. The term $e'(n-1)$ gives the number of group rings of this type. The extra 1 is required when n is even, $n \geqq 3$, since in this case there is one more elementary indecomposible, namely $\mathbf{L}_{n,0}$, which is not a group ring.

By a *partition* of n is meant an n-tuple $m = (m_1, \ldots, m_n)$ of non-negative integers satisfying

$$\sum_{i=1}^{n} i m_i = n.$$

Each Witt ring R with $|G| = 2^n$ gives rise to a partition of n. Namely, let $R = R_1 \triangle \ldots \triangle R_k$ be the normalized decomposition of R, and let m_i denote the number of factors R_j with $|G_{R_j}| = 2^i$. For $u \geqq 1$, $v \geqq 0$, let $\phi(u, v)$ denote the number of ways of choosing v objects from a set of u objects, repetitions allowed. Thus

$$\phi(u, v) = (u + v - 1)!/v!(u - 1)!.$$

Then the number of elementary types with $|G| = 2^n$, char $(R) = 2$, having the associated partition m is

$$P_m' = \prod_{i=1}^{n} \phi(s'(i), m_i).$$

Thus $e'(n) = \sum_m P_m'$, the sum running over all partitions of n.

Next we compute the number of elementary types with $|G| = 2^n$ which have no factor $\mathbf{Z}/2\mathbf{Z}[\Delta_2]$ in their normalized decomposition. Let us denote this number by $e''(n)$. Define $s(1) = 2$, $s(2) = 2$, and for $n \geqq 3$ define $s(n)$ to be either $e(n-1) + 1$ or $e(n-1) + 2$ depending on whether n is odd or even. For $n \geqq 2$, $s(n)$ is just the number of indecomposibles of elementary type with $|G| = 2^n$. For $n = 1$, it is one less than this number, corresponding to the fact that we are avoiding $\mathbf{Z}/2\mathbf{Z}[\Delta_2]$. As before, for $n \geqq 3$, the term $e(n-1)$ comes from the group rings, and the extra term (1 or 2) comes from the fact that $\mathbf{L}_n$ is an additional elementary indecomposible if n is odd, and $\mathbf{L}_{n,0}$, $\mathbf{L}_{n,1}$ are additional elementary inde-

https://doi.org/10.4153/CJM-1982-089-1 Published online by Cambridge University Press

composibles if n is even. Then, as above, $e''(n) = \sum_m P_m''$, where for each partition m,

$$P_m'' = \prod_{i=1}^{n} \phi(s(i), m_i).$$

Finally, to get $e(n)$ from $e''(n)$ we need to add on the number of elementary types with $|G| = 2^n$ and with $\mathbf{Z}/2\mathbf{Z}[\Delta_2]$ appearing in the normalized decomposition. Any such R is necessarily of the form

$$R = \mathbf{Z}/2\mathbf{Z}[\Delta_2] \sqcap S$$

where S is of elementary type with char $(S) = 2$ and $|G_S| = 2^{n-1}$. Thus

$$e(n) = e''(n) + e'(n-1).$$

Thus, in summary, we have proved the following theorem:

(4.5) THEOREM. $e(0) = 1, e(1) = 3$. *For* $n \geqq 2$,

$$e(n) = e''(n) + e'(n-1)$$

where

$$e'(n) = \sum_m \prod_{i=1}^{n} \phi(s'(i), m_i),$$

$$e''(n) = \sum_m \prod_{i=1}^{n} \phi(s(i), m_i),$$

the sums running over all partitions $m = (m_1, \ldots, m_n)$ *of* n. *Here*

$$s'(n) = \begin{cases} 1, & \text{if } n = 1 \text{ or } 2 \\ e'(n-1), & \text{if } n \geqq 3,\ n \text{ odd} \\ e'(n-1) + 1, & \text{if } n \geqq 3,\ n \text{ even} \end{cases} \quad \text{and}$$

$$s(n) = \begin{cases} 2, & \text{if } n = 1 \text{ or } 2 \\ e(n-1) + 1, & \text{if } n \geqq 3,\ n \text{ odd} \\ e(n-1) + 2, & \text{if } n \geqq 3,\ n \text{ even.} \end{cases}$$

(4.6) COROLLARY. *For* $n \leqq 20$, *we have the table on the following page.*

Proof. This follows from Theorem 4.5 by direct computation.

(4.7) *Remark.* In computing $e(n)$ we are identifying those elementary types which are isomorphic as Witt rings. However, using [**6**, p. 21] or [**13**, Proposition 4.6] we see that two elementary types are isomorphic as Witt rings if and only if they are isomorphic as rings. Thus, the distinction between ring isomorphism and Witt ring isomorphism is not crucial here.

n	$e'(n)$	$e(n)$
0	1	1
1	1	3
2	2	6
3	4	17
4	10	51
5	22	155
6	54	492
7	130	1600
8	328	5340
9	832	18150
10	2156	62711
11	5638	219480
12	14937	776907
13	39886	2775942
14	107425	10000288
15	291229	36280937
16	794458	132447126
17	2178595	486161754
18	6003100	1793218752
19	16611406	6643162316
20	46143648	24706819426

5. The case $|G| \leqq 32$. In this section an algorithm is described for computing all non-isomorphic quaternionic schemes over G, where $|G| = 2^n$ and $n \leqq 5$. For each such n, it turns out that the number of isomorphism classes is $e(n)$ (terminology as in Section 4), thus proving that only elementary types occur. This extends results in [**2**, **11**, and **15**].

In this section, let $0 \leqq n \leqq 5$ be arbitrary, $m = 2^n$, and let $x_1, \ldots, x_m$ denote the elements of G. We assume, without loss of generality, that:

(i) x_1 is the identity in G,

(ii) $-1 = x_1$ or $-1 = x_2$,

(iii) $B = \{b_i | 1 \leqq i \leqq n\}$ is a basis for G as a vector space over $\mathbf{Z}/2\mathbf{Z}$, where $b_i = x_{2^{i-1}+1}$, and

(iv) $x_i x_j = x_{i+j-1}$, where $1 \leqq i < j < m$ and $x_j \in B$.

In view of (iii), the automorphisms of G which fix -1 correspond to the maps f: $B \rightarrow G$ such that $|f(B)| = |B|$, $f(B)$ is linearly independent, and, if $-1 = x_2, f(x_2) = x_2$.

Let $<$ denote the order on G defined by $x_i < x_j$ if and only if $i < j$.

The set $\mathcal{G}$ of all subgroups of G can be linearly ordered as follows, where S and $T \in \mathcal{G}$:

(i) If $|S| > |T|$, then $S < T$, and

(ii) If $|S| = |T|$, then the order is determined lexicographically, using the order on G.

Let $G_1, \ldots, G_\alpha$ denote the elements of $\mathcal{G}$, written in increasing order.

Our algorithm will be applied separately for each choice of $\langle G, -1 \rangle$, where $n \leqq 5$. Since the algorithm builds quaternionic schemes in stages, we require the following terminology:

(5.1) *Definition.* A *scheme segment* (over G) of length $k \leqq m$ is a function $V: \{x_1, \ldots, x_k\} \to \mathcal{G}$ such that

(i) $-x_i \in V(x_i)$, whenever $x_1 \leqq x_i \leqq x_k$,

(ii) $x_i \in V(x_j) \Leftrightarrow x_j \in V(x_i)$,

whenever $x_1 \leqq x_i \leqq x_k$ and $x_1 \leqq x_j \leqq x_k$, and

(iii) $V(x_1) = G$.

Clearly a scheme segment of length m is just a quadratic form scheme on G in the sense that it is a function $V: G \to \mathcal{G}$ which satisfies $-a \in V(a)$ and

$$a \in V(b) \Leftrightarrow b \in V(a) \ \forall\, a, b \in G.$$

(Note however, that our terminology differs from that in [**2**, **10**, **15**, and **16**]. In the latter terminology it is the mapping $x \mapsto V(-x)$ which is the quadratic form scheme, not $x \mapsto V(x)$.) A quadratic form scheme V on G is a quaternionic scheme if it satisfies.

$$(5.2) \qquad bV(a) \cap V(ac) \cap dV(c) \neq \emptyset \Rightarrow aV(b) \cap V(bd) \cap cV(d) \neq \emptyset,$$

for all a, b, c, and $d \in G$.

The set S of all scheme segments over G has a linear order, $<$, which is defined as follows:

(i) If length $(V) <$ length (W), then $V < W$, and

(ii) If length $(V) =$ length (W), then the order is determined lexicographically by the order on $\mathcal{G}$.

(5.3) *Definition.* Suppose that V and W are scheme segments and that length $(W) = j \leqq k =$ length (V). Then

(i) V is an *extension* of W (denoted $W \prec V$ or $V \succ W$) if and only if $V(x_i) = W(x_i)$, whenever $1 \leqq i \leqq j$.

(ii) $W \subseteq V$ if and only if $W(x_i) \subseteq V(x_i)$, whenever $1 \leqq i \leqq j$.

(5.4) *Definition.* For each scheme segment V, let $F(V)$ be the least (with respect to $\subseteq$) quadratic form scheme such that $V \subseteq F(V)$.

It is easy to see that $F(V)$ exists, is unique, and can be determined with a simple algorithm.

Note that if $F(V)$ is not an extension of V, then no quadratic form scheme is an extension of V.

(5.5) *Definition.* Two scheme segments of length k, V and W, are *isomorphic* ($V \cong W$ or $V \cong_\phi W$) if there is a group automorphism ϕ on G such that:

(i) $\phi(-1) = -1$,

(ii) $\phi(\{x_1, \ldots, x_k\}) = \{x_1, \ldots, x_k\}$, and

(iii) $\phi(V(x_i)) = W(\phi(x_i))$, whenever $1 \leqq i \leqq k$.

Clearly, two scheme segments of length m are isomorphic if and only if they are isomorphic as quadratic form schemes.

Since an automorphism ϕ of G is determined by $\phi|_B$, a backtracking algorithm can efficiently determine whether or not two scheme segments are isomorphic.

Our algorithm will use a proposition $C(-)$, to be specified later, to generate a list $\mathscr{L} = \{L_1, \ldots, L_p\}$ of scheme segments over G such that:

(i) length $(L_1) = 1$, and

(ii) L_{k+1} is the least element, with respect to $<$, in $\{V \in S | C(V)$, V is isomorphic to no member of $\{L_1, \ldots, L_k\}$, and V is an extension of some L_j, $1 \leqq j \leqq k$, such that length $(L_j) + 1 =$ length $(V)\}$.

It follows that $1 \leqq i < j \leqq p$ implies that $L_i < L_j$.

The key to the algorithm lies in choosing a condition C such that:

(i) there is an efficient algorithm for determining when C holds,

(ii) each scheme segment of length m in $\mathscr{L}$ is a quaternionic scheme over G, and

(iii) each quaternionic scheme over G is isomorphic to some member of $\mathscr{L}$.

Ideally, C should reject any scheme segment which can not be extended to a quaternionic scheme, rather than later having to reject many of its extensions. If C is chosen such that

$$C(V) \Rightarrow (F(V)) \succ V)$$

then we are assured that every element of $\mathscr{L}$ can at least be extended to some quadratic form scheme. However we are unable to find an efficient C which also determines whether or not a scheme segment can be extended to a quaternionic scheme. The difficulty is that given a scheme segment L, we are unable to construct a quaternionic scheme $Q(L)$ such that, for any quaternionic scheme $Q \supseteq L$, $L \subseteq Q(L) \subseteq Q$. Thus, we are often unable to determine whether or not a scheme segment has any extensions which are quaternionic schemes, until after many of them have been generated and checked.

To reduce this difficulty we shall define, for each scheme segment, V, a function

$$P(V): G \rightarrow \text{the power set of } \{1, \ldots, \alpha\}$$

such that $Q(x_i) = G_\beta$, for some $\beta \in P(V)(x_i)$, whenever $Q \succ V$ is a quaternionic scheme and length $(V) < i \leqq m$.

(5.6) *Definition*. Suppose that $V \neq L_1$ is a scheme segment of length k and that $W = V|_{\{x_1, \ldots, x_{k-1}\}}$.

Then:

(i) For all $x \in G$ let

$$P(L_1)(x) = \{\beta | G_\beta \supseteq F(L_1)(x)\} \quad \text{and}$$
$$P'(V)(x) = \{\beta | G_\beta \supseteq F(V)(x)\} \cap P(W)(x),$$

(ii) If $x_k \in B$, then

(a) Whenever $y < x_k$, let

$$P(V)(x_ky) = \{\beta | y_1V(x_k) \cap G_\beta \cap y_2V(y) \neq \phi$$

whenever $y_1, y_2 \in G$ satisfy

$$x_kF(V)(y_1) \cap F(V)(y_1y_2) \cap yF(V)(y_2) \neq \phi\} \cap P'(V)(x_ky),$$

and

(b) If $z \neq x_ky$ for any y such that $x_1 \leqq y < x_k$, then let

$$P(V)(z) = P'(V)(z), \quad \text{and}$$

(iii) If $x_k \notin B$, then let $P(V) = P'(V)$.

(5.7) *Definition*. Suppose that V is a scheme segment of length k. Then $C(V)$ holds if and only if

(i) $V \prec F(V)$,

(ii) If $(k > 1)$ then $V(x_k) = G_\beta$, for some

$$\beta \in P(V|_{\{x_1,\dots,x_{k-1}\}})(x_k),$$

(iii) $P(V)(y) \neq \emptyset$, whenever $x_k < y \leqq x_m$,

(iv) If $(x_k \notin B)$ then

$$y_1V(x_k) \cap V(x_ky) \cap y_2V(y) \neq \emptyset,$$

whenever $y_1, y_2, y \in G$ and $y, x_ky \leqq x_k$, and

$$x_kF(V)(y_1) \cap F(V)(y_1y_2) \cap yF(V)(y_2) \neq \emptyset, \quad \text{and}$$

(v) If $k = m$, then V is a quaternionic scheme.

As each computation of $P(V)$ involving (ii)a is extremely time consuming, that calculation was only made when $x_k \in B$. To partially compensate for the resultant lowering of the effectiveness of P, condition (iv) was incorporated into the definition of C.

Note that if V is a quaternionic scheme such that $V \cong W$ implies that $V < W$, then $V \in \mathscr{L}$. To see this, suppose that it fails for some V and choose the largest i such that $V|_{\{x_1,\dots,x_i\}}$ is in $\mathscr{L}$. Then, by the construction of $\mathscr{L}$, there is a scheme segment $W \in \mathscr{L}$ of length $i + 1$ such that

$$W < V|_{\{x_1,\dots,x_{i+1}\}} \quad \text{and}$$
$$V|_{\{x_1,\dots,x_{i+1}\}} \cong_\phi W,$$

for some automorphism ϕ of G. Clearly, ϕ induces an extension U of W such that $V \cong_\phi U$ and $U < V$. This contradicts our choice of V.

(5.8) *Remark*. In order to generate the quaternionic schemes within a reasonable time, when $n = 5$, the above algorithm was modified to utilize the following facts, where V is a scheme segment of length $k > 1$.

(i) If $\{x_1, \dots, x_k\}$ is a group (i.e., $k = 2^i$ for some i) containing a nonrigid element and satisfying $V(y) \subseteq \{x_1, \dots, x_k\}$ whenever $x_1 < y \leqq x_k$,

https://doi.org/10.4153/CJM-1982-089-1 Published online by Cambridge University Press

then V can be extended to at most one quaternionic scheme W. Further, $W(y) = \{1, -y\}$, whenever $x_k < y \leqq x_m$.

(ii) If $k \geqq m/2$, then $F(V)$ is the only scheme extending V, and

(iii) If $-1 = x_2$ and $V(x_2) = \{x_1\}$, then $-x \in V(y)$ implies that $V(x) \subseteq V(y)$,

To justify the use of these we note that (ii) is elementary, (iii) is a well-known property of reduced quaternionic schemes (which are already classified in any case), and (i) follows from Corollary 2.7.

(5.9) *Remark.* An earlier version of this algorithm was implemented in Pascal and run on a Decsystem 2060. Computation times, when $n = 3, 4$, and 5 respectively, were $1\frac{1}{2}$ seconds, $1\frac{1}{2}$ minutes, and $4\frac{1}{2}$ hours.

(5.10) *Remark.* A variation of this algorithm was used to compute all non-isomorphic quadratic form schemes on G satisfying the extra axiom in [**15**, **16**]. It turns out that for $n = 5$, this extra axiom is equivalent to (1.2). This was already known for $n \leqq 4$ by the computation in [**15**].

References

1. L. Berman, C. Cordes and R. Ware, *Quadratic forms, rigid elements, and formal power series fields*, J. of Alg. *66* (1980), 123–133.

2. C. Cordes, *Quadratic forms over non-formally real fields with a finite number of quaternion algebras*, Pac. J. Math. *63* (1976), 357–365.

3. C. Cordes and J. Ramsey Jr., *Quadratic forms over fields with* $u = q/2 < +\infty$, Fund. Math. *99* (1978), 1–10.

4. T. Craven, *Characterizing reduced Witt rings of fields*, J. of Alg. *53* (1978), 68–77.

5. ——— *Witt rings and orderings of skew fields*, preprint.

6. D. Harrison, *Witt rings*, notes by J. Cunningham, Univ. of Kentucky (1970).

7. B. Kirkwood and B. McDonald, in preparation.

8. J. Kleinstein and A. Rosenberg, *Succinct and representational Witt rings*, Pac. J. Math. *86* (1980), 99–137.

9. M. Knebusch, *On the local theory of signatures and reduced quadratic forms*, preprint.

10. M. Kula, *Fields with prescribed quadratic form schemes*, Math. Zeit. *167* (1979), 201–212.

11. M. Kula, L. Szczepanik and K. Szymiczek, *Quadratic forms over formally real fields with eight square classes*, Manuscripta Math. *29* (1979), 295–303.

12. M. Marshall, *Spaces of orderings IV*, Can. J. Math. *32* (1980), 603–627.

13. ——— *Abstract Witt rings*, Queen's papers in pure and applied Math. *57*, Queen's Univ. (1980).

14. M. Marshall and J. Yucas, *Linked quaternionic mappings and their associated Witt rings*, Pac. J. Math. *95* (1981).

15. L. Szczepanik, *Fields and quadratic form schemes with the index of the radical not exceeding* 16, preprint.

16. ——— *Quadratic form schemes with non trivial radical*, preprint.

17. E. Witt, *Theorie der Quadratischen Formen in beliebigen Körpern*, J. reine angew. Math. *176* (1937), 31–44.

18. J. Yucas, *A note on quadratic forms, rigid elements, and orderings of fields*, preprint.

University of Saskatchewan,
Saskatoon, Saskatchewan