Can. J. Math. Vol. **47** (6), 1995 pp. 1274–1289

DECOMPOSITION OF WITT RINGS AND GALOIS GROUPS

JÁN MINÁČ AND TARA L. SMITH

ABSTRACT. To each field F of characteristic not 2, one can associate a certain Galois group $\mathcal{G}_F$, the so-called W-group of F, which carries essentially the same information as the Witt ring $W(F)$ of F. In this paper we show that direct products of Witt rings correspond to free products of these Galois groups (in the appropriate category), group ring construction of Witt rings corresponds to semidirect products of W-groups, and the basic part of $W(F)$ is related to the center of $\mathcal{G}_F$. In an appendix we provide a complete list of Witt rings and corresponding W-groups for fields F with $|\dot{F}/\dot{F}^2| \leq 16$.

1. **Introduction.** The intriguing relation between the theory of quadratic forms and Galois theory has been of interest for a long time. (See for example [Wi:1936], [Wr:1979], [Wr:1983], [Wr:1985], [JWr:1989], [AEJ:1984], among others.) However, recently the connection between the Witt ring structure for a field F (of characteristic not 2) and its Galois groups was made quite precise. If L is a Galois field extension of F, with $\mathrm{Gal}(L/F) \cong G$, we call L a G-extension of F. Given a field F, with $\mathrm{char}\, F \neq 2$, one can consider the field extension $F^{(3)}/F$ which is the compositum over F of all $\mathbb{Z}/2\mathbb{Z}$-, $\mathbb{Z}/4\mathbb{Z}$-, and D_4-extensions of F. (Here D_4 denotes the dihedral group of order 8.) One can then show that the Galois group $\mathcal{G}_F$ of $F^{(3)}$ over F, hereafter referred to as the W-group of F, is determined by $W(F)$, and that $\mathcal{G}_F$ determines $W(F)$ except in the case when the level $s(F)$ of F is ≤ 2 and the form $\langle 1, 1\rangle$ is universal. (In this paper basic knowledge of quadratic form theory and profinite groups will be assumed. See [La:1973] or [Sc:1985] for the former and [N:1971] and [Se:1965] for the latter. Throughout we will assume all fields to be of characteristic not 2.) In other words, knowledge of $\mathcal{G}_F$ is essentially equivalent to knowledge of $W(F)$. (See [MiSm:1993], [MiSp:1990], [MiSp:1995], [Sm:1988], [Sp:1987].) This relationship between a specific Galois group of F and $W(F)$ opened a new way of attacking some questions in quadratic from theory and posed other new questions. In particular, it allows one to use the techniques of inverse Galois theory to study some classical problems in the theory of Witt rings.

One of the most outstanding problems is the characterization of Witt rings in the category of all rings. In spite of many efforts, very little is known. Indeed, we know only a very few finitely generated Witt rings (*i.e.* Witt rings of fields with finitely many square classes), namely those which are Witt rings of the real numbers, the complex numbers, finite fields, or a local field, and those rings which can be obtained from them using group

The first author was supported in part by the Natural Sciences and Engineering Research Council of Canada.
The second author was supported in part by NSF Grant DMS-9196244 and by the National Security Agency.
Received by the editors April 22, 1994.
AMS subject classification: 11E81.

ring construction and direct product formation in the category of Witt rings. These are the so-called "elementary type" Witt rings. A complete list of Witt rings for fields F with $|\dot{F}/\dot{F}^2| \leq 32$ has been published, and all of these are of elementary type. However it remains an open question whether all finitely generated Witt rings are of elementary type. (See [CMa:1982], [Ma:1980], [La:1973], [Sc:1985], [Pf:1966].)

Realizability of the elementary type Witt rings described above implies realizability of certain groups as W-groups $\mathcal{G}_F$. In this paper we will answer the question, which ones? In particular we will determine the group-theoretic analogues for W-groups to the group ring and direct product constructions for Witt rings. We want to emphasize that here we do not make any assumption on the finiteness of $|\dot{F}/\dot{F}^2|$. (Similar results on the analogues to group ring and direct product constructions for absolute 2-Galois groups are obtained in [JWr:1989].) Berman [Be:1978] introduced the very useful and fundamental notion of the basic part Bas(F) of a field F. (See also [Ma:1980].) In this paper we show that Bas(F) is closely related to the center $Z(\mathcal{G}_F)$ of the W-group of F. In fact, if $-1 \in \dot{F}^2$, then $Z(\mathcal{G}_F)$ modulo the Frattini subgroup of $\mathcal{G}_F$ is dual to $\dot{F}/\text{Bas}(F)$. We conclude by considering some possible areas for further exploration, and providing a complete list of W-groups for fields with small square class groups.

Throughout this article we will be viewing the groups that arise as being in a subcategory of the category of groups. We describe this category here.

DEFINITION 1.1. The category C is the full subcategory of the category of pro-2-groups whose objects are those pro-2-groups G satisfying

(1) $g^4 = 1\ \forall g \in G$,

(2) $g^2 \in Z(G)$, the center of G, $\forall g \in G$.

LEMMA 1.2. *Objects of the category C are precisely central extensions of elementary abelian 2-groups by elementary abelian 2-groups.*

Here, by elementary abelian 2-group we mean $\prod_I \mathbb{Z}/2\mathbb{Z}$ with I possibly infinite, and possibly empty. This product carries the usual product topology.

PROOF. Suppose first that G is a central extension of $A = \prod_I \mathbb{Z}/2\mathbb{Z}$ by $B = \prod_J \mathbb{Z}/2\mathbb{Z}$, and for each $g \in G$, let $\bar{g}$ denote the image of g in B. Then we have $\bar{g}^2 = 1$, so $g^2 \in A$, so $g^4 = (g^2)^2 = 1$ and $g^2 \in Z(G)$. On the other hand, assume that G is a pro-2-group satisfying conditions (1) and (2) above. Let A be the closed subgroup of G generated by squares. Then $A \subseteq Z(G)$, and $B := G/A$ is 2-elementary abelian. Since $g^2 \in Z(G)$ $\forall g \in G$, we see that for each element $a \in A$ we have $a^2 = 1$. Thus A is 2-elementary abelian as well. (Here we are using the fact that a compact topological group A with the property $a^2 = 1\ \forall a \in A$ is 2-elementary. This is an easy consequence of Pontrjagin's duality theorem [Pn:1966].) ∎

Critical to our understanding of the connections between decomposition of Witt rings and the structure of W-groups is the relationship between the construction of the W-group and the Witt ring. We explain this now; for details see [MiSm:1993], [MiSp:1995], and [Sm:1988].

Let $W(F)$ be a Witt ring of a field F, and let $G = \dot{F}/\dot{F}^2$ be the group of square classes of F. Then G has a natural structure as a vector space over the field $\mathbb{Z}/2\mathbb{Z}$, and we can choose a basis $B = \{b_i : i \in I\}$ for G as a $\mathbb{Z}/2\mathbb{Z}$-vector space, where I is some linearly ordered index set. Let Q be the subgroup of the Brauer group $\mathrm{Br}(F)$ of F generated by the classes of quaternion algebras over F. (See [La:1973] or [Ma:1980].) Together G and Q provide us with a quaternionic structure (G, Q, q) following [Ma:1980], where q is the map $q: G \times G \to Q$ defined by sending $(a, b) \in G \times G$ to the class of the quaternion algebra $(\frac{a,b}{F})$ in $Q \subset \mathrm{Br}(F)$. By abuse of notation we write (a, b) to denote the image $q(a, b)$ of (a, b) in Q. The close relation between quaternionic structures and Witt rings was exploited in [Ma:1980], where both were defined abstractly using only a few axioms and not relying on any underlying field. It is shown in Theorem 4.5 of [Ma:1980] that the category of Witt rings and the category of quaternionic structures are naturally equivalent. This relationship is used in [MiSp:1995], and consequently in this article. Roughly speaking, quaternionic structures form the bridge between Witt rings and Galois theory. We can now explain how to construct $\mathcal{G}_F$, the W-group of F, using the quaternionic structure (G, Q, q) above.

Let $\mathcal{F}$ be the free group in the category C on the symbols $\{z_i : i \in I\}$. Then $\Phi(\mathcal{F})$, the Frattini subgroup of $\mathcal{F}$, is a $\mathbb{Z}/2\mathbb{Z}$-vector space with basis $\langle z_i^2, [z_i, z_j] : i, j \in I, i \leq j\rangle$. Let P be the set of homogeneous polynomials of degree 2 in the variables $t_i, i \in I$, with coefficients in $\mathbb{Z}/2\mathbb{Z}$. Thus P is also a $\mathbb{Z}/2\mathbb{Z}$-vector space. We then have a natural pairing $\langle\ ,\ \rangle: \Phi(\mathcal{F}) \times P \to \mathbb{Z}/2\mathbb{Z}$, obtained by letting $\{z_i^2, [z_i, z_j] : i, j \in I, j > i\}$ and $\{t_i^2, t_i t_j\ ; i, j \in I, j > i\}$ be dual bases.

We have a group homomorphism $\theta: P \to Q$ given by $\theta(t_i^2) = (b_i, b_i), \theta(t_i t_j) = (b_i, b_j)$. Let $\mathcal{R} = (\ker\theta)^{\perp} = \{s \in \Phi(\mathcal{F}) : \langle s, p\rangle = 0\ \forall p \in \ker\theta\}$. Then $\mathcal{R}$ can be viewed as the dual Q^* of Q. The major result needed in our paper is the following.

PROPOSITION 1.3. *The W-group $\mathcal{G}$ and the group $\mathcal{F}/\mathcal{R}$ are isomorphic pro-2-groups.*

REMARK. It is in fact possible to associate an abstract W-group to any abstract Witt ring (in the sense of [Ma:1980]) by using the approach in the proposition above. In the case that the abstract Witt ring is in fact the Witt ring of a field F, then the abstract W-group constructed in this manner will be isomorphic to the W-group of F. See [Sm:1988] for details.

2. **Direct products and free products.** The concept of direct products of Witt rings was introduced in [Ma:1980]. In this section we shall show that this notion corresponds to the free product of W-groups in the category C. (See also [MiSm:1993] and [Sm:1988].)

In order to describe the free product of two groups $\mathcal{G}_1$ and $\mathcal{G}_2$ in C, it is convenient to make the following definition.

DEFINITION 2.1. Suppose $\mathcal{G}_1, \mathcal{G}_2 \in C$. Let $\mathcal{G}_1/\Phi(\mathcal{G}_1) = \varprojlim_{j\in J} G_j$, $\mathcal{G}_2/\Phi(\mathcal{G}_2) = \varprojlim_{k\in K} H_k$, where G_j and H_k are finite 2-elementary groups and $\Phi(\mathcal{G}_i)$ denotes the Frattini

subgroup of $\mathcal{G}_i$, $i = 1,2$. Then we define the free commutator subgroup $\langle \mathcal{G}_1 ; \mathcal{G}_2 \rangle$ to be $\lim_{\leftarrow j\times k\in J\times K} G_j \otimes_{\mathbb{Z}/2\mathbb{Z}} H_k$, where G_j and H_k are viewed as vector spaces over the field $\mathbb{Z}/2\mathbb{Z}$.

One checks easily that the groups $G_j \otimes_{\mathbb{Z}/2\mathbb{Z}} H_k$ indeed form a projective system, and that this definition of the free commutator subgroup is independent of the particular choice of G_j and H_k used in the representation of $\mathcal{G}_i/\Phi(\mathcal{G}_i)$ as a projective limit. Moreover, we observe that we have a natural map $\mathcal{G}_1 \times \mathcal{G}_2 \to \langle \mathcal{G}_1 ; \mathcal{G}_2 \rangle$. For $\gamma_i \in \mathcal{G}_i$, we denote the image of (γ_1, γ_2) as $\langle \gamma_1, \gamma_2 \rangle$.

We can now describe the group $\mathcal{G}$ which will turn out to be the free product of $\mathcal{G}_1$ and $\mathcal{G}_2$ in the category C. As a topological space $\mathcal{G}$ is just $\mathcal{G}_1 \times \mathcal{G}_2 \times \langle \mathcal{G}_1 ; \mathcal{G}_2 \rangle$, with the product topology. Multiplication in $\mathcal{G}$ is determined by the following properties:

(1) $\mathcal{G}_1$, $\mathcal{G}_2$, and $\langle \mathcal{G}_1 ; \mathcal{G}_2 \rangle$ considered as subspaces of $\mathcal{G}$ are also subgroups of $\mathcal{G}$ with their original multiplications.

(2) $\langle \mathcal{G}_1 ; \mathcal{G}_2 \rangle$ is in the center of $\mathcal{G}$.

(3) For each $\gamma_1 \in \mathcal{G}_1$ and $\gamma_2 \in \mathcal{G}_2$, we define the product $\gamma_1 \cdot \gamma_2$ inside $\mathcal{G}$ as $(\gamma_1, \gamma_2, 1)$, and the product $\gamma_2 \cdot \gamma_1$ as $(\gamma_1, \gamma_2, \langle \gamma_1, \gamma_2 \rangle)$. More precisely we have:

$$(\gamma_1, 1, 1) \cdot (1, \gamma_2, 1) = (\gamma_1, \gamma_2, 1) ;$$
$$(1, \gamma_2, 1) \cdot (\gamma_1, 1, 1) = (\gamma_1, \gamma_2, \langle \gamma_1, \gamma_2 \rangle).$$

REMARKS. Observe that $\mathcal{G}$ can be expressed as the semidirect products

$$\mathcal{G} \cong (\mathcal{G}_1 \times \langle \mathcal{G}_1, \mathcal{G}_2 \rangle) \rtimes \mathcal{G}_2$$
$$\cong (\mathcal{G}_2 \times \langle \mathcal{G}_1, \mathcal{G}_2 \rangle) \rtimes \mathcal{G}_1.$$

Here the action of $\mathcal{G}_2$ on $\mathcal{G}_1 \times \langle \mathcal{G}_1, \mathcal{G}_2 \rangle$ is defined by the fact that $\langle \mathcal{G}_1, \mathcal{G}_2 \rangle$ is central in $\mathcal{G}$, and by the rule $\gamma_1^{-1}\gamma_2\gamma_1 = \gamma_2\langle \gamma_1, \gamma_2 \rangle$ $\forall \gamma_1 \in \mathcal{G}_1, \gamma_2 \in \mathcal{G}_2$. The element $\langle \gamma_1, \gamma_2 \rangle$ is actually the commutator of the elements γ_1 and γ_2 in $\mathcal{G}$. One can check quite easily that $\mathcal{G}$ is indeed an element of C.

Let $\mathcal{G}$ be as defined above, and let $\mathcal{G}_1 * \mathcal{G}_2$ denote the free product of the groups $\mathcal{G}_1$ and $\mathcal{G}_2$ in the category C. Then we have the following.

THEOREM 2.2. $\mathcal{G} \cong \mathcal{G}_1 * \mathcal{G}_2$.

PROOF. Consider $\mathcal{G}$ as $\mathcal{G}_1 \times \mathcal{G}_2 \times \langle \mathcal{G}_1, \mathcal{G}_2 \rangle$, so that elements of of $\mathcal{G}$ are triples $(\gamma_1, \gamma_2, \gamma_3)$, with $\gamma_1 \in \mathcal{G}_1, \gamma_2 \in \mathcal{G}_2$, and $\gamma_3 \in \langle \mathcal{G}_1, \mathcal{G}_2 \rangle$. Let j_i denote the natural injections of $\mathcal{G}_i$ into $\mathcal{G}$, $i = 1,2$. Suppose also that we are given an element $G \in C$ and continuous homomorphisms $\varphi_i \colon \mathcal{G}_i \to G$, $i = 1,2$ (in the category C). We would like to show that there exists a unique homomorphism $\varphi \colon \mathcal{G} \to G$ in C such that the diagrams

$$\begin{array}{ccc} \mathcal{G}_i & \xrightarrow{j_i} & \mathcal{G} \\ {\scriptstyle \varphi_i}\downarrow & \swarrow{\scriptstyle \varphi} & \\ G & & \end{array}$$

https://doi.org/10.4153/CJM-1995-065-0 Published online by Cambridge University Press

are commutative, $i = 1, 2$. Since $\mathcal{G}$ is generated by $\mathcal{G}_1, \mathcal{G}_2$, there can exist at most one homomorphism φ as above, which is determined by

$$\varphi\big(j_i(\gamma_i)\big) = \varphi_i(\gamma_i) \quad \gamma_i \in \mathcal{G}_i.$$

To show that such a φ exists, first observe that we have a well-defined homomorphism in C, namely $\psi\colon \langle \mathcal{G}_1, \mathcal{G}_2\rangle \to G$ given by $\psi(\langle \gamma_1, \gamma_2\rangle) = [\varphi_1(\gamma_1), \varphi_2(\gamma_2)]$, $\gamma_1 \in \mathcal{G}_1, \gamma_2 \in \mathcal{G}_2$. Then for each $(\gamma_1, \gamma_2, \gamma_3) \in \mathcal{G}$, define

$$\varphi\big((\gamma_1, \gamma_2, \gamma_3)\big) = \varphi_1(\gamma_1)\varphi_2(\gamma_2)\psi(\gamma_3).$$

The map φ is clearly continuous, so we need only check that φ is a homomorphism. But it is straightforward to check that for any $(\gamma_1, \gamma_2, \gamma_3)$ and $(\gamma_1', \gamma_2', \gamma_3') \in \mathcal{G}$,

$$\begin{aligned}\varphi\big((\gamma_1, \gamma_2, \gamma_3)(\gamma_1', \gamma_2', \gamma_3')\big) &= \varphi_1(\gamma_1\gamma_1')\varphi_2(\gamma_2\gamma_2')\psi(\langle \gamma_1', \gamma_2\rangle\gamma_3\gamma_3') \\ &= \varphi\big((\gamma_1, \gamma_2, \gamma_3)\big)\varphi\big((\gamma_1', \gamma_2', \gamma_3')\big).\end{aligned}$$

Thus we see $\mathcal{G} \cong \mathcal{G}_1 * \mathcal{G}_2$ as claimed. ∎

Of course, one can characterize free products $\mathcal{G}_1 * \mathcal{G}_2$ using generators and relations. In order to formulate this result, assume that $\mathcal{G} \cong \mathcal{F}/\mathcal{R}$, $\mathcal{G}_1 \cong \mathcal{F}_1/\mathcal{R}_1$, and $\mathcal{G}_2 \cong \mathcal{F}_2/\mathcal{R}_2$, where $\mathcal{G} \cong \mathcal{G}_1 * \mathcal{G}_2$, and $\mathcal{F}$, $\mathcal{F}_1$, and $\mathcal{F}_2$ are free objects in C. Moreover assume that $\mathcal{F}_i$ has the set $\mathcal{A}_i$ as a minimal set of generators, and that $\mathcal{G}_i \subset \mathcal{G}$, $i = 1, 2$. Then we have the following very simple characterization of the set of relations $\mathcal{R}$ in the category C.

PROPOSITION 2.3. *Keep the notation above. Then the set $\mathcal{A} := \mathcal{A}_1 \cup \mathcal{A}_2$ generates $\mathcal{F}$, and $\mathcal{R} = \mathcal{R}_1 \times \mathcal{R}_2$.*

PROOF. From the previous theorem we know that $\mathcal{G} \cong \mathcal{G}_1 \times \mathcal{G}_2 \times \langle \mathcal{G}_1, \mathcal{G}_2\rangle$ as a topological group under the multiplication described above. Therefore $\mathcal{G}/\Phi(\mathcal{G}) \cong \mathcal{G}_1/\Phi(\mathcal{G}_1) \times \mathcal{G}_2/\Phi(\mathcal{G}_2)$. Since the image of the sets $\mathcal{A}_1 \cup \mathcal{A}_2 = \mathcal{A}$ in $\mathcal{G}/\Phi(\mathcal{G})$ is a minimal set of generators of $\mathcal{G}/\Phi(\mathcal{G})$, we see that $\mathcal{A}_1 \cup \mathcal{A}_2$ is a minimal set of generators of $\mathcal{G}$ as well. (See [Se:1965].) Thus what remains to show is that $\mathcal{R}$ = the closed normal subgroup generated by $\mathcal{R}_1 \cup \mathcal{R}_2 \cong \mathcal{R}_1 \times \mathcal{R}_2$. From the relation $\mathcal{F}/\Phi(\mathcal{F}) \cong \mathcal{G}_1/\Phi(\mathcal{G}_1) \times \mathcal{G}_2/\Phi(\mathcal{G}_2)$ we deduce that $\mathcal{R} \subseteq \Phi(\mathcal{F})$. But $\Phi(\mathcal{F})$ is 2-elementary, *i.e.* $\Phi(\mathcal{F}) = \prod_{j\in J} \mathbb{Z}/2\mathbb{Z}$ for some index set J. Since $\mathcal{R}_1 \cap \mathcal{R}_2 = \{1\}$, we see that $\mathcal{R}_1 \cup \mathcal{R}_2$ generates the subgroup $\mathcal{R}_1 \times \mathcal{R}_2$ in $\mathcal{F}$. Moreover, it is in fact a subgroup of $\Phi(\mathcal{F})$, and thus is normal in $\mathcal{F}$. Finally from $\mathcal{F}/\mathcal{R}_1 \times \mathcal{R}_2 \cong \mathcal{G}_1 \times \mathcal{G}_2 \times \langle \mathcal{G}_1, \mathcal{G}_2\rangle$ we conclude $\mathcal{R} \cong \mathcal{R}_1 \times \mathcal{R}_2$. ∎

Our main theorem in this section follows easily from the above analysis and the following result from the theory of abstract Witt rings.

PROPOSITION 2.4 [MA:1980; PP. 100–102]. *Suppose that S_1 and S_2 are two Witt rings, and let S be their direct product in the category of Witt rings. Let (G_1, Q_1, q_1) and (G_2, Q_2, q_2) be the quaternionic structures corresponding to the Witt rings S_1 and S_2, respectively. Then the quaternionic structure corresponding to S is $(G_1 \times G_2, Q_1 \times Q_2,$*

$q_1 \times q_2$). Conversely, suppose that S is a Witt ring with quaternionic structure (G, Q, q), and suppose that G_1 and G_2 are subgroups of G such that $G = G_1 \times G_2$ and such that $\forall a, b \in G$, $q(a,b) = 0 \Leftrightarrow q_i(a_i, b_i) = 0$, $i = 1,2$, where x_i denotes the component of $x \in G$ in G_i and q_i is obtained by the restriction of q to G_i, $i = 1,2$. Then there exist Witt rings S_1 and S_2 with corresponding quaternionic structures (G_1, Q_1, q_1) and (G_2, Q_2, q_2), such that $S = S_1 \times S_2$ in the category of Witt rings.

THEOREM 2.5. *Suppose that S_1 and S_2 are two Witt rings, and let S be their direct product in the category of Witt rings. Let $\mathcal{G}_1$ and $\mathcal{G}_2$ be the W-groups corresponding to the Witt rings S_1 and S_2, respectively. Then the W-group $\mathcal{G}$ corresponding to S is isomorphic to $\mathcal{G}_1 * \mathcal{G}_2$. Conversely, if $\mathcal{G}$ is the W-group of a Witt ring S, and if $\mathcal{G} \cong \mathcal{G}_1 * \mathcal{G}_2$ in the category C, then there exist Witt rings S_1 and S_2 such that $\mathcal{G}_i$ is the W-group associated to S_i, $i = 1,2$, and $S \cong S_1 \times S_2$.*

PROOF. Let Q_1, Q_2, and $Q_1 \times Q_2$ be the quaternionic structures corresponding to S_1, S_2, and S, as above. Then $\mathcal{R}_1 = Q_1^*$, $\mathcal{R}_2 = Q_2^*$, and $\mathcal{R} = (Q_1 \times Q_2)^*$, with respect to the pairings described in Section 1. Since $(Q_1 \times Q_2)^* \cong Q_1^* \times Q_2^*$ as topological groups, we conclude that $\mathcal{R} \cong \mathcal{R}_1 \times \mathcal{R}_2$. Thus we have $\mathcal{G} \cong \mathcal{G}_1 * \mathcal{G}_2$ as claimed.

To prove the converse, let $\mathcal{G} \cong \mathcal{G}_1 * \mathcal{G}_2$ be the W-group of some Witt ring S, with quaternionic structure (G, Q, q). Then $[\mathcal{G}/\Phi(\mathcal{G})]^* \cong G$. Set $G_i \cong [\mathcal{G}_i/\Phi(\mathcal{G}_i)]^*$, $i = 1,2$. Then clearly $G \cong G_1 \times G_2$. Set $Q_i, i = 1,2$ to be the subgroup of Q generated by those elements with both slots in G_i. Then under the pairing $\langle\ ,\ \rangle$ defined in the proposition in Section 1, we find that the dual to Q_i is precisely the relations $\mathcal{R}_i$ defining the group G_i, $i = 1,2$. (This follows immediately from the observations that $\mathcal{R} \cong \mathcal{R}_1 \times \mathcal{R}_2$, because $\mathcal{G} \cong \mathcal{G}_1 * \mathcal{G}_2$, that $\mathcal{R}_i$ is orthogonal to $Q_j, j \neq i$, and that $\mathcal{R}$ is dual to Q.) Set $q_i: G_i \times G_i \to Q_i$, $i = 1,2$ to be the restriction of q to G_i. Let a, b be any two elements of G, and again let x_i denote the component of $x \in G$ in G_i. Then $q(a,b) = 0 \Leftrightarrow (a,b)$ is orthogonal to $\mathcal{R} \Leftrightarrow (a_i, b_i)$ is orthogonal to $\mathcal{R}_i$, $i = 1,2, \Leftrightarrow q_i(a_i, b_i) = 0$. Thus we conclude that $S \cong S_1 \times S_2$, where S_i is the (abstract) Witt ring with associated quaternionic pairing (G_i, Q_i, q_i) and associated W-group $\mathcal{G}_i$, $i = 1,2$. ∎

3. **Group rings and semidirect products.** In this section we show that the group ring construction for Witt rings corresponds in a natural way to a semidirect product construction for W-groups. Moreover, in the case when $s(F) = 1$, it is in fact a direct product. Since the group ring formation for Witt rings determines which elements in $\dot{F}$ are "basic", we begin by recalling definitions related to this concept, and then setting up convenient notation for $\mathcal{G}_F$ to allow us to keep track of which elements are basic.

Recall that an element $a \in \dot{F}$ is rigid if $D(\langle 1, a\rangle) = \dot{F}^2 \cup a\dot{F}^2$, in other words, if $\langle 1, a\rangle$ represents as few elements as possible. An element $a \in \dot{F}$ is called *double-rigid* if both a and $-a$ are rigid. Now $\mathrm{Bas}(F) = \{a \in \dot{F} \mid a \text{ is not double-rigid}\} \cup \dot{F}^2 \cup -\dot{F}^2$ is a subgroup of $\dot{F}$ (see [Be:1978] and [Wr:1981]). This is the so-called basic part of F. Observe that if $|\dot{F}/\dot{F}^2| > 2$, then $\mathrm{Bas}(F) = \{a \in \dot{F} \mid a \text{ is not double-rigid}\}$, because then certainly -1 is not rigid.

We introduce the following notation: Let $\mathcal{H} = \{\sigma \in \mathcal{G}_F \mid \sigma(\sqrt{-1}) = \sqrt{-1}\}$, *i.e.* the set of elements in $\mathcal{G}_F$ fixing $\sqrt{-1}$, so $\mathcal{H} = \mathcal{G}_F$ if $s(F) = 1$. Choose a basis $\{-1, a_i \mid i \in I\}$ for $\dot{F}/\dot{F}^2$, or $\{a_i \mid i \in I\}$ if $s(F) = 1$, such that $\{-1, a_i \mid i \in I'\}$ (respectively $\{a_i \mid i \in I'\}$) forms a basis for the basic part $\mathrm{Bas}(F)$ of F, for some subset I' of I (which we can do since $\mathrm{Bas}(F)$ is a subgroup of $\dot{F}$, containing $\dot{F}^2$). Let $J = I \setminus I'$, so $\{a_j \mid j \in J\}$ are all double-rigid elements. Let $\{\sigma_{-1}, \sigma_i \mid i \in I\}$ if $-1 \notin \dot{F}^2$, or $\{\sigma_i \mid i \in I\}$ if $-1 \in \dot{F}^2$, be a corresponding "dual" set of generators for $\mathcal{G}_F$. Assume that the basis has been chosen so that $\{\sigma_i \mid i \in I\} \subseteq \mathcal{H}$.

LEMMA 3.1. *Retain the notation above. Then for any $i \in I, j \in J$, $i \neq j$, $[\sigma_i, \sigma_j] = 1$.*

PROOF. Since $F^{(3)}$ is generated by $\mathbb{Z}/2\mathbb{Z}$-, $\mathbb{Z}/4\mathbb{Z}$-, and D_4-extensions of F, it suffices to show that σ_j and σ_i commute when restricted to any $\mathbb{Z}/2\mathbb{Z}$-, $\mathbb{Z}/4\mathbb{Z}$-, or D_4-extension of F. Since $\mathbb{Z}/2\mathbb{Z}$- and $\mathbb{Z}/4\mathbb{Z}$-extensions are abelian, it is enough to check that for each extension L/F with $\mathrm{Gal}(L/F) \cong D_4$, we have $[\sigma_i, \sigma_j]|_L = 1$. Let $F(\sqrt{a}, \sqrt{b})$ be the fixed field of the center $Z\big(\mathrm{Gal}(L/F)\big)$ of $\mathrm{Gal}(L/F)$, and assume that $\mathrm{Gal}\big(L/F(\sqrt{ab})\big) \cong \mathbb{Z}/4\mathbb{Z}$. Suppose, contradictory to our claim, that $[\sigma_i, \sigma_j]|_L \neq 1$. Then neither σ_j nor σ_i are in $Z\big(\mathrm{Gal}(L/F)\big)$. Thus σ_j fails to fix either $\sqrt{a}$ or $\sqrt{b}$. Say $\sigma_j(\sqrt{a}) = -\sqrt{a}$. Then by the duality of the generators for $\mathcal{G}_F$ and the basis for $\dot{F}/\dot{F}^2$, we see that a_j must appear as a factor in the decomposition of a as a product of basis elements in $\dot{F}/\dot{F}^2$, and therefore $a \notin \mathrm{Bas}(F)$, so a is double-rigid. On the other hand, since $\mathrm{Gal}(L/F) \cong D_4$, $\mathrm{Gal}\big(L/F(\sqrt{ab})\big) \cong \mathbb{Z}/4\mathbb{Z}$, and $L \supseteq F(\sqrt{a}, \sqrt{b})$, we see that the quaternion algebra (a, b) splits over F. (See [Sp:1987] for a proof.) Thus $b \in D_F(\langle 1, -a\rangle)$, so $b = -a \in \dot{F}/\dot{F}^2$. Now by assumption, both σ_j and σ_i fix $\sqrt{-1}$, so $\sigma_j(\sqrt{a}) = -\sqrt{a}$, $\sigma_j(\sqrt{b}) = -\sqrt{b}$, $\sigma_i(\sqrt{a}) = -\sqrt{a}$, and $\sigma_i(\sqrt{b}) = -\sqrt{b}$. Then $\sigma_i\sigma_j^{-1}$ fixes both $\sqrt{a}$ and $\sqrt{b}$, so $\sigma_i\sigma_j^{-1}|_L \in Z\big(\mathrm{Gal}(L/F)\big)$, and $[\sigma_j, \sigma_i]|_L = 1$, contrary to assumption. Thus in fact σ_j and σ_i commute as claimed. ∎

LEMMA 3.2. *For any $j \in J$, σ_j has order 4 in $\mathcal{G}_F$.*

PROOF. We consider two cases. First suppose $s(F) = 1$. Then the F-quaternion algebra (a, a) is split for any $a \in \dot{F}$, so in particular (a_j, a_j) is split. Thus (see [La:1973]) there exists a Galois extension K/F, with $K \supseteq F(\sqrt{a_j})$ and $\mathrm{Gal}(K/F) \cong \mathbb{Z}/4\mathbb{Z}$. Since $\sigma_j(\sqrt{a_j}) = -\sqrt{a_j}$ by assumption, we see that σ_j generates $\mathrm{Gal}(K/F)$, and thus has order a multiple of 4 in $\mathcal{G}_F$. The result follows by observing that $\mathcal{G}_F$ has exponent 4.

Now consider the case $-1 \notin \dot{F}^2$. The splitting of the quaternion algebra $(a_j, -a_j)$ implies the existence of a D_4-extension L/F, with $L \supseteq F(\sqrt{a_j}, \sqrt{-1})$ and $\mathrm{Gal}\big(L/F(\sqrt{-1})\big) \cong \mathbb{Z}/4\mathbb{Z}$. (One can take, for example, $L = F(\sqrt{-1}, \sqrt[4]{a_j})$.) Look at σ_j restricted to L. Since σ_j fixes $\sqrt{-1}$ by assumption, $\sigma_j|_L \in \mathrm{Gal}\big(L/F(\sqrt{-1})\big)$. On the other hand, the unique quadratic extension of $F(\sqrt{-1})$ in L is $F(\sqrt{-1}, \sqrt{a_j})$, and $\sqrt{a_j}$ is not fixed by σ_j. Thus $\sigma_j|_L$ generates $\mathrm{Gal}\big(L/F(\sqrt{-1})\big)$, and again the order of σ_j in $\mathcal{G}_F$ must be (a multiple of) 4. ∎

REMARK. One could also prove this lemma quite easily from the description of the relations in $\mathcal{G}_F$ given in the proposition in Section 1. Following the notation there we

have, in the first case, that $t_j^2 \in \ker(\theta)$, but $\langle z_j^2, t_j^2\rangle \neq 0$, so $\sigma_j^2 \neq 1$, and in the second case, that $t_j^2 + t_{-1}t_j \in \ker(\theta)$, but $\langle z_j^2, t_j^2 + t_{-1}t_j\rangle \neq 0$, so again $\sigma_j^2 \neq 1$.

COROLLARY 3.3. *Let Δ_J denote the closed subgroup of $\mathcal{G}_F$ generated by σ_j, $j \in J$. Then $\Delta_J \cong \prod_J \mathbb{Z}/4\mathbb{Z}$ in the category of pro-2-groups.*

PROOF. (Sketch) Δ_J is an abelian pro-2-group of exponent 4. The result follows from Pontrjagin duality ([Pn:1966]). The dual $(\Delta_J)^*$ to Δ_J is a discrete abelian group of exponent 4, generated by x_j, $j \in J$, such that $x_j(\sigma_j) = \sqrt{-1} \in \mathbb{C}$, and $x_j(\sigma_k) = 1$ if $j \neq k$. One checks easily that $(\Delta_J)^*$ is isomorphic to $\oplus_J \mathbb{Z}/4\mathbb{Z}$. We have a natural isomorphism $\theta\colon \Delta_J \longrightarrow (\Delta_J^*)^* \cong \prod_J \mathbb{Z}/4\mathbb{Z}$ given by $\theta(\sigma)(x) = x(\sigma)$. ∎

THEOREM 3.4. *Let J' be any subset of J, and let $\Delta_{J'}$ denote the closed subgroup of $\mathcal{G}_F$ generated by σ_j, $j \in J'$. Then the group Δ_J' is a normal subgroup of $\mathcal{G}_F$.*

PROOF. If $\sqrt{-1} \in \dot{F}$, then the theorem follows from the fact that $[\sigma_j, \sigma_i] = 1$ for all $i \in I$, which we proved at the beginning of this section. If $\sqrt{-1} \notin \dot{F}$, then for each $j \in J' \subseteq J$ we have $\sigma_j^2[\sigma_j, \sigma_{-1}] = \sigma_j(\sigma_{-1}^{-1}\sigma_j\sigma_{-1}) = 1$. There are a number of ways to see this. From our "generator-relation" description of $\mathcal{G}_F$, this is equivalent to the fact that any product of quaternion algebras in $\mathrm{Br}_2(F)$ which is equal to 1 includes either both (a_j, a_j) and $(a_j, -1)$ or neither of them. This in turn follows from the existence of a nondyadic 2-Henselian valuation of F such that the value group Γ satisfies $\Gamma/2\Gamma \cong \langle [a_j] \mid j \in J\rangle \subseteq \dot{F}/\dot{F}^2$. Alternatively one can observe that since any $a_j, j \in J$ is double-rigid, the only $x \in \dot{F}/\dot{F}^2$ with $(a_j, x) = 1$ is $x = 1$ or $x = -a_j$. Perhaps most enlightening is the following explicit proof.

To see that $\tau = \sigma_j^2[\sigma_j, \sigma_{-1}] = 1$, it is enough to show that restriction of τ to any L/F with L/F Galois and $\mathrm{Gal}(L/F) \cong \mathbb{Z}/4\mathbb{Z}$ or D_4 is the identity. Assume first that $\mathrm{Gal}(L/F) \cong \mathbb{Z}/4\mathbb{Z}$. Let $F(\sqrt{b})$ be the unique quadratic subextension of L. Then b is a sum of 2 squares and hence is basic. This means that a_j does not appear in the expression for b as a product of our chosen basis elements, and thus that σ_j^2 restricted to L is the identity. Since $\mathrm{Gal}(L/F)$ is abelian, $[\sigma_j, \sigma_{-1}]|_L$ is also the identity, and hence $\tau|_L = 1$.

Next assume that $\mathrm{Gal}(L/F) \cong D_4$, and let $F(\sqrt{b}, \sqrt{c})$ be the unique biquadratic subextension of L, with $\mathrm{Gal}\big(L/F(\sqrt{bc})\big) \cong \mathbb{Z}/4\mathbb{Z}$. Then $(b, c) = 1 \in \mathrm{Br}(F)$. If one of b, c, say b, is double rigid, then in fact $b = -c \in \dot{F}/\dot{F}^2$. Assume first that a_j is a factor in the decomposition of b as a product of basis elements. Then $\sigma_j(\sqrt{b}) = -\sqrt{b}$ and $\sigma_j(\sqrt{c}) = -\sqrt{c}$. Thus σ_j generates $\mathrm{Gal}\big(L/F(\sqrt{-1})\big)$, so $\sigma_j^2 \neq 1 \in \mathrm{Gal}(L/F)$. On the other hand, since $\sigma_{-1}(\sqrt{-1}) = -\sqrt{-1}$, σ_{-1} cannot fix both $\sqrt{b}$ and $\sqrt{c}$, so $[\sigma_j, \sigma_{-1}] \neq 1 \in \mathrm{Gal}(L/F)$. From the structure of D_4 it then follows that $\tau|_L = 1$. Assume next that a_j is not a factor of b. Then $\sigma_j|_{F(\sqrt{b},\sqrt{c})} = 1$ and $\sigma_j^2|_L = 1 = [\sigma_j, \sigma_{-1}]|_L$. Finally, assume both b and c are basic. Then a_j is not a factor of either b or c, and as above $\sigma_j|_{F(\sqrt{b},\sqrt{c})} = 1$ and $\sigma_j^2|_L = 1 = [\sigma_j, \sigma_{-1}]|_L$.

Summarizing the results above we see that for all $j \in J' \subseteq J$, $\sigma_i^{-1}\sigma_j\sigma_i = \sigma_j\ \forall i \in I$, and $\sigma_{-1}^{-1}\sigma_j\sigma_{-1} = \sigma_j^3$. Thus $\Delta_{J'}$ is a normal subgroup of $\mathcal{G}_F$. ∎

Recall that for $\Lambda_{J'} = \langle a_j \mid j \in J' \rangle \subseteq \dot{F}/\dot{F}^2$, $J' \subseteq J$ as above, we have $W(F) = S[\Lambda_{J'}]$ where S is again a Witt ring of a field. In fact, if $J' = J$ one can actually identify S with a Witt ring of a residue field of some 2-Henselian valuation on F. (See [Ma:1980], [Wr:1981], [JWr:1989], [J:1981], [AEJ:1987].) Then let $S = W(K)$ for some appropriate field K. The main result of this section is that the W-group $\mathcal{G}_F$ of F is a semi-direct product of $\Delta_{J'}$ with the W-group $\mathcal{G}_K$ of K.

THEOREM 3.5. *Keep the notation above. Then*

$$\mathcal{G}_F \cong \Delta_{J'} \rtimes \mathcal{G}_K \cong \left(\prod_{J'} \mathbb{Z}/4\mathbb{Z}\right) \rtimes \mathcal{G}_K$$

where $\mathcal{G}_K$ is generated by $\{\sigma_i \mid i \in I \setminus J'\} \cup \sigma_{-1}$ if $-1 \notin \dot{F}^2$ and by $\{\sigma_i \mid i \in I \setminus J'\}$ if $-1 \in \dot{F}^2$. The action of $\mathcal{G}_K$ on $\Delta_{J'}$ is given by the equations

$$\sigma_i^{-1}\tau\sigma_i = \tau \quad \forall \tau \in \Delta_{J'},$$
$$\sigma_{-1}^{-1}\tau\sigma_{-1} = \tau^3 \quad \forall \tau \in \Delta_{J'} \text{ (if } -1 \notin \dot{F}^2\text{)}.$$

PROOF. Let G be the closed subgroup of $\mathcal{G}_F$ generated by $\{\sigma_i \mid i \in I \setminus J'\} \cup \sigma_{-1}$ if $-1 \notin \dot{F}^2$ and by $\{\sigma_i \mid i \in I \setminus J'\}$ if $-1 \in \dot{F}^2$. We will show $\Delta_{J'} \rtimes G \cong \mathcal{G}_F$, where the action of G on $\Delta_{J'}$ is as described in the theorem, and $G \cong \mathcal{G}_K$. Assume first that $\sqrt{-1} \in \dot{F}$. Since $\Delta_{J'}$ and G generate $\mathcal{G}_F$ and $\Delta_{J'}$ is a normal subgroup of $\mathcal{G}_F$, we will have $\mathcal{G}_F$ as a semidirect product of these two subgroups if we can show $\Delta_{J'} \cap G = \{1\}$. Since $\{\sigma_i \mid i \in I \setminus J'\} \cap \{\sigma_j \mid j \in J'\} = \emptyset$ by definition, it suffices to show that $\Phi(\Delta_{J'}) \cap \Phi(G) = 1$. In other words, we must exclude the possibility that for some nonempty subset C of J' and some element $h \in \Phi(G)$, we have $(\prod_{c \in C} \sigma_c^2)h = 1$. Let C be any nonempty subset of J', and let $j \in C$. Then for $L = F(\sqrt[4]{a_j})$, $\mathrm{Gal}(L/F) \cong \mathbb{Z}/4\mathbb{Z}$, and the unique quadratic subextension of L is $F(\sqrt{a_j})$. Hence $\sigma_j|_L$ generates $\mathrm{Gal}(L/F)$, but $\sigma_c^2|_L = 1$ for all $c \neq j$, $c \in C$, $h|_L = 1$, and thus $(\prod_{c \in C} \sigma_c^2)h = \sigma_j^2 \neq 1$. That the action is as claimed follows from the preceding theorem. To see that $G \cong \mathcal{G}_K$, observe first that $\mathcal{G}_K$ and G have the same minimal set of generators, namely $\{\sigma_i \mid i \in I \setminus J'\}$. Thus it suffices to check that they satisfy the same relations. This follows from the fact that the relations among F-quaternion algebras whose entries consist of "dual elements of $\dot{F}$ to the elements of G" are precisely the same as those satisfied by the "corresponding" quaternion algebras over K. (See [Ma:1980], [JWr:1989], [J:1981], [Wr:1981].) The case $\sqrt{-1} \notin \dot{F}$ is handled in the same way as the case $\sqrt{-1} \in \dot{F}$, the only difference being that σ_{-1} has nontrivial action on $\Delta_{J'}$. The details are left to the reader. ∎

As a converse to this result we have the following.

THEOREM 3.6. *Assume that F and K are fields with associated W-groups $\mathcal{G}_F$ and $\mathcal{G}_K$, such that $s(F) \geq 4$ or $s(F) = s(K)$, and that $\mathcal{G}_F \cong \Delta_{J'} \rtimes \mathcal{G}_K \cong (\prod_{J'} \mathbb{Z}/4\mathbb{Z}) \rtimes \mathcal{G}_K$, where the action of $\mathcal{G}_K$ on $\Delta_{J'}$ is given as follows: Set $\mathcal{H} = \{\sigma \in \mathcal{G}_K \mid \sigma(\sqrt{-1}) = \sqrt{-1}\}$.*

https://doi.org/10.4153/CJM-1995-065-0 Published online by Cambridge University Press

Then $\sigma^{-1}\tau\sigma = \tau\ \forall \sigma \in \mathcal{H}, \tau \in \Delta_{J'}$ *and* $\sigma^{-1}\tau\sigma = \tau^3\ \forall \sigma \in \mathcal{G}_K \setminus \mathcal{H}, \tau \in \Delta_{J'}$. *Under these assumptions we have* $W(F) \cong W(K)[\sum_{J'} \mathbb{Z}/2\mathbb{Z}]$.

PROOF. From the Remark in [Ma:1980; p. 114] we see that there exists a field extension M/K such that $W(M) \cong W(K)[\sum_{J'} \mathbb{Z}/2\mathbb{Z}]$. From the previous theorem we then conclude $\mathcal{G}_M \cong \Delta_{J'} \rtimes \mathcal{G}_K \cong \mathcal{G}_F$. Since we assume $s(F) \geq 4$ or $s(F) = s(K) = s(M)$, we see ([MiSp:1995]) that $W(K)[\sum_{J'} \mathbb{Z}/2\mathbb{Z}] \cong W(M) \cong W(F)$. ∎

4. $\mathcal{G}_F$ **and the basic part of** $W(F)$**.** The connection between $\mathrm{Bas}(F)$ and $\mathcal{G}_F$ again divides into two cases, $\sqrt{-1} \in F$ and $\sqrt{-1} \notin F$. The answer is the following: Let $\mathcal{H}$ be the subgroup of $\mathcal{G}_F$ generated by those elements in $\mathcal{G}_F$ which fix $\sqrt{-1}$, and let $\mathcal{L}$ be the subgroup of $\mathcal{G}_F$ generated by those elements of $\mathcal{G}_F$ fixing $\{\sqrt{a} \mid a \in D_F(\langle 1, 1\rangle)\}$ pointwise. Then $\dot{F}/\mathrm{Bas}(F)$ can be viewed as the $\mathbb{Z}/2\mathbb{Z}$-dual to the subgroup of $\mathcal{G}_F/\Phi(\mathcal{G}_F)$ consisting of the images of $Z(\mathcal{H}) \cap \mathcal{L}$, in case $-1 \notin \dot{F}^2$, and as the $\mathbb{Z}/2\mathbb{Z}$-dual to $Z(\mathcal{G}_F)/\Phi(\mathcal{G}_F)$ in case $-1 \in \dot{F}^2$.Thus in the level 1 case, the basic part of the field corresponds to the center of the W-group. Because of the simpler description in this case, and to avoid having to account for the different behavior of -1 in each proof, we will examine the two cases separately. We begin with the case $\sqrt{-1} \in \dot{F}$.

THEOREM 4.1. *Let* $\Phi = \Phi(\mathcal{G}_F)$ *denote the Frattini subgroup of the W-group* $\mathcal{G}_F$ *of the field F, and let* $\mathcal{Z}$ *denote its center.*

(1) If $|\dot{F}/\dot{F}^2| \leq 2$, *then* $\mathcal{Z} = \mathcal{G}_F$.

(2) If $|\dot{F}/\dot{F}^2| \geq 4$ *and* $\sqrt{-1} \notin F$, *then* $\mathcal{Z} = \Phi$.

(3) If $\sqrt{-1} \in F$, *then* $\mathcal{Z}/\Phi$ *is the annihilator of the* $\mathbb{Z}/2\mathbb{Z}$*-vector space* $\mathrm{Bas}(F)/\dot{F}^2$ *under the pairing* $\langle\ ,\ \rangle : \dot{F}/\dot{F}^2 \times \mathcal{G}_F/\Phi \longrightarrow \mathbb{Z}/2\mathbb{Z}$ *given by* $\langle a, \sigma\rangle = \frac{\sigma(\sqrt{a})}{\sqrt{a}} \in \{1, -1\} \cong \mathbb{Z}/2\mathbb{Z}$.

PROOF. For (1), observe that this means $\mathcal{G}_F$ is a cyclic group, and hence must be abelian. For (2), let $\sigma \in \mathcal{G}_F \setminus \Phi$. Then there exists an element $a \in \dot{F}$ such that $a \notin \pm\dot{F}^2$, and $\sigma(\sqrt{a}) = -\sqrt{a}$. Since the quaternion algebra $(a, -a) = 1 \in \mathrm{Br}(F)$, there is a D_4-extension K/F, $K \subseteq F^{(3)}$, with $K \supseteq F(\sqrt{a}, \sqrt{-a})$, and such that $\mathrm{Gal}\big(K/F(\sqrt{-1})\big) \cong \mathbb{Z}/4\mathbb{Z}$. Since $Z\big(\mathrm{Gal}(K/F)\big) = \mathrm{Gal}\big(K/F(\sqrt{a}, \sqrt{-a})\big)$, we see $\sigma \notin Z\big(\mathrm{Gal}(K/F)\big)$, and hence $\sigma \notin \mathcal{Z}$. Thus $\mathcal{Z} = \Phi$ as claimed. (We will refer hereafter to an extension $K \supseteq F(\sqrt{a}, \sqrt{b}) \supseteq F$, with $\mathrm{Gal}(K/F) \cong D_4$ and $\mathrm{Gal}\big(K/F(\sqrt{ab})\big) \cong \mathbb{Z}/4\mathbb{Z}$ as a $D_4^{(a,b)}$-extension of F.)

Now suppose $\sqrt{-1} \in F$. We have a natural pairing $\langle\ ,\ \rangle : \dot{F}/\dot{F}^2 \times \mathcal{G}_F/\Phi \longrightarrow \mathbb{Z}/2\mathbb{Z}$ given by $\langle a, \sigma\rangle = \frac{\sigma(\sqrt{a})}{\sqrt{a}} \in \{1, -1\} \cong \mathbb{Z}/2\mathbb{Z}$, where by abuse of notation we have used a to denote both an element of $\dot{F}$ and its square class in $\dot{F}/\dot{F}^2$, and σ to denote both an element in $\mathcal{G}_F$ and its image in $\mathcal{G}_F/\Phi$. Suppose that $a \in \mathrm{Bas}(F)$ and $\sigma \in \mathcal{Z}$. We claim that $\sigma(\sqrt{a}) = \sqrt{a}$. If not, then $\sigma(\sqrt{a}) = -\sqrt{a}$. Since $a \in \mathrm{Bas}(F)$, $\exists b \in \dot{F}$, $b \notin \dot{F}^2 \cup a\dot{F}^2$, such that $(a, b) = 1 \in \mathrm{Br}(F)$, so that there exists a $D_4^{(a,b)}$-extension K of F. Let $\bar{\sigma}$ denote the image of σ in $\mathrm{Gal}(K/F)$. Then it is clear that $\bar{\sigma} \notin Z\big(\mathrm{Gal}(K/F)\big)$, and so also $\sigma \notin \mathcal{Z}$. This is a contradiction, so the claim is proved. Thus in the pairing $\langle\ ,\ \rangle$, $\mathcal{Z}/\Phi$ and $\mathrm{Bas}(F)$

are orthogonal to each other. To complete the proof, we must show that if $\sigma \in \mathcal{G}_F$ has the property $\sigma(\sqrt{b}) = \sqrt{b}\ \forall b \in \mathrm{Bas}(F)$, then $\sigma \in \mathcal{Z}$. Now since $F^{(3)}$ is the compositum over F of all cyclic of order 4 and dihedral of order 8 extensions of F, it follows that $\sigma \in \mathcal{Z} \Leftrightarrow \bar{\sigma} \in Z\big(\mathrm{Gal}(K/F)\big)$ $\forall D_4$-extensions K/F. Let K be a $D_4^{(a,b)}$-extension. Then $(a,b) = 1 \in \mathrm{Br}(F)$, so neither a nor b is rigid. Then both $\sqrt{a}$ and $\sqrt{b}$ are fixed by σ by assumption, so $\bar{\sigma} \in Z\big(\mathrm{Gal}(K/F)\big)$, completing our proof. ∎

Now we turn our attention to the case when $\sqrt{-1} \notin F$. Set $\mathcal{H} = \{\sigma \in \mathcal{G}_F \mid \sigma(\sqrt{-1}) = \sqrt{-1}\}$, and set $\mathcal{L} = \{\sigma \in \mathcal{G}_F \mid \sigma(\sqrt{a}) = \sqrt{a}\ \forall a \in D_F(\langle 1,1\rangle)\}$.

THEOREM 4.2. $\sigma(\sqrt{b}) = \sqrt{b}\ \forall b \in \mathrm{Bas}(F) \Leftrightarrow \sigma \in Z(\mathcal{H}) \cap \mathcal{L}$. *In other words,* $\big(Z(\mathcal{H}) \cap \mathcal{L}\big)/\Phi$ *is the annihilator of* $\mathrm{Bas}(F)$ *under the pairing* $\langle\ ,\ \rangle : \dot{F}/\dot{F}^2 \times \mathcal{G}_F/\Phi \to \mathbb{Z}/2\mathbb{Z}$ *given by* $\langle a, \sigma\rangle = \frac{\sigma(\sqrt{a})}{\sqrt{a}} \in \{1,-1\} \cong \mathbb{Z}/2\mathbb{Z}$.

PROOF. Suppose first that $\sigma \in \mathcal{F} := \{\sigma \in \mathcal{G}_F \mid \sigma(\sqrt{b}) = \sqrt{b}\ \forall b \in \mathrm{Bas}(F)\}$. Then, as in the preceding proof, we see that $\sigma \in Z(\mathcal{H})$. Now let $a \in D(\langle 1,1\rangle)$. If $a \in \pm\dot{F}^2$, then $\pm a \in \mathrm{Bas}(F)$ and $\sqrt{a}$ and $\sqrt{-a}$ are both fixed by all $\sigma \in \mathcal{F}$. Then if $a \in D(\langle 1,1\rangle)$, $a \notin \pm\dot{F}^2$, we see $a \in D(\langle 1,-a\rangle)$, so $\pm a \in \mathrm{Bas}(F)$ and again $\sigma \in \mathcal{F}$ fixes $\sqrt{a}$ and $\sqrt{-a}$. Thus $\mathcal{F} \subseteq Z(\mathcal{H}) \cap \mathcal{L}$.

To finish the proof, we must prove the opposite inclusion, $\mathcal{L} \cap Z(\mathcal{H}) \subseteq \mathcal{F}$. Then let $\sigma \in \mathcal{L} \cap Z(\mathcal{H})$ and $b \in \mathrm{Bas}(F)$. We must show $\sigma(\sqrt{b}) = \sqrt{b}$. This is clearly true if $\pm b \in D_F(\langle 1,1\rangle)$, so we shall assume this is not the case. Since $b \in \mathrm{Bas}(F)$, either b or $-b$ is not rigid. Say $-b$ is not rigid. Then there exists $c \in D_F(\langle 1,-b\rangle)$ with b, c, -1 independent mod $\dot{F}^2$. It follows that we can find $\tau \in \mathcal{G}_F$ fixing $\sqrt{-1}$ (so $\tau \in \mathcal{H}$), which also fixes $\sqrt{b}$, but such that $\tau(\sqrt{c}) = -\sqrt{c}$. Then consider any $D_4^{b,c}$-extension L/F. Suppose $\sigma(\sqrt{b}) = -\sqrt{b}$). Then $[\sigma,\tau]|_L \neq 1|_L$, and we see $\sigma \notin Z(\mathcal{H})$, a contradiction. Hence σ fixes $\sqrt{b}$. Next suppose that $-b$ is rigid. Then necessarily b is not rigid, and by the argument we have just given we see σ fixes $\sqrt{-b}$. Since by assumption $\sigma \in \mathcal{H}$, σ fixes $\sqrt{-1}$ as well, and hence must fix $\sqrt{b}$. ∎

REMARK. -1 is not in general explicitly determined just by knowledge of $\mathcal{G}_F$. So it could be argued that $\mathcal{H}$ is not a purely group-theoretical notion. However, the "negative" of the Kaplansky radical, $-KR := \{a \in \dot{F} \mid D_F(\langle 1,a\rangle) = \dot{F}\}$, is determined by $\mathcal{G}_F$ ([MiSm:1993]), and this is all that is necessary for the determination of $\mathrm{Bas}(F)$. Specifically, if $-KR$ is "trivial", then $-KR = \{-1\}$, and -1 is determined. If $-KR$, or the Kaplansky radical, is nontrivial, then in fact $\mathrm{Bas}(F) = \dot{F}$. This follows from the observation that for any $b \in \dot{F} \setminus KR$, we have $D_F(\langle 1,b\rangle) \supseteq (KR \cup bKR)$, so $|D_F(\langle 1,b\rangle)| \geq 2|KR| \geq 4$, and b is not rigid. Thus if b is rigid then $b \in KR$. Then $D_F(\langle 1,-b\rangle) = \dot{F}$, so $-b$ is rigid if and only if $|\dot{F}/\dot{F}^2| \leq 2$. Since we are concerned with $\mathcal{H}$ only in the case $-1 \notin \dot{F}^2$, we see that $\dot{F}/\dot{F}^2 = \{1,-1\}$ in this case, and again $\mathrm{Bas}(F) = \dot{F}$.

5. **Concluding remarks.** Our results in Section 1–Section 3 compare with those in [JWr:1989] as follows: In going from Witt rings to Galois groups, we are considering quotients of $\mathrm{Gal}\big(F(2)/F\big)$, so our results give less information on which pro-2-Galois groups arise over a field, given its Witt ring. In going from Galois groups to Witt rings, we are effectively starting with a weaker hypothesis (information only on a quotient of the absolute pro-2-Galois group, rather than the whole group), so the results can be considered as stronger. Also it is important to note that we do not make the assumption that $|\dot{F}/\dot{F}^2| < \infty$, so again our results are more general.

In Section 4 we have shown that the center of $\mathcal{G}_F$ corresponds to $\dot{F}/\operatorname{Bas}(F)$, in the case when $\sqrt{-1} \in \dot{F}$. One may ask whether it is possible to refine this result in some way. For example, since the center of a group consists of the intersection of the centralizers of individual group elements, one may try to determine what the centralizer of a given element should correspond to, either in $\dot{F}$ or in $W(F)$. Is there a correspondence between $C_{\mathcal{G}_F}(\sigma)$ and some quotient $\dot{F}/\operatorname{Bas}_\sigma(F)$, where $\operatorname{Bas}_\sigma(F)$ is a "local basic" part of F with respect to σ, sitting inside $\operatorname{Bas}(F)$?

This is one aspect of a much larger question concerning connections between subgroups and quotients of $\mathcal{G}_F$ and the corresponding parts of $\dot{F}/\dot{F}^2$ or $W(F)$. One may ask such questions as when and how a W-group for a field K occurs as a subgroup or quotient group of the W-group of a field F. The authors will investigate such questions in future work ([MiSm:pre]).

The approach taken in this paper clarifies the relationship between Witt rings and Galois groups. It illustrates how one can translate Galois group properties into Witt ring properties and vice versa, using elementary duality principles.

6. **Appendix: W-groups for fields F with $|\dot{F}/\dot{F}^2| \leq 16$.** We present below a complete list of the W-groups that occur for fields with square class group of order less than or equal to 16, in conjunction with their corresponding Witt rings. This gives a concrete illustration of how the results in this article can be used to generate all "elementary type" W-groups. It also makes clear the inability of the W-group to distinguish the level of the field in the case $\langle 1, 1\rangle$ is universal. The number before the decimal point in each case indicates the order of $\dot{F}/\dot{F}^2$. In all cases the $*$ is to be interpreted as the free product in the category C described in Section 2, and the action of the semi-direct product is that described in Section 3. Recall also that for Witt rings, $\mathbb{Z} \times \mathbb{Z} \cong \mathbb{Z}[x]$, and if $2 \neq 0 \in R$, $R \times \mathbb{Z}/2\mathbb{Z}[x] \cong R \times \mathbb{Z}/4\mathbb{Z}$. See [Ma:1980] for further description of notation, particularly for the descriptions of the Witt rings $\mathbb{L}_{2k-1}$, $\mathbb{L}_{2k,0}$, and $\mathbb{L}_{2k,1}$ which arise as Witt rings of the reals, the p-adic fields $\mathbb{Q}_p$ and finite extensions of $\mathbb{Q}_2$. We denote the corresponding W-groups as $\mathbb{G}_{2k-1}$, $\mathbb{G}_{2k,0}$ and $\mathbb{G}_{2k,1}$ respectively. We give explicit descriptions of $\mathbb{G}_3$, $\mathbb{G}_{4,0}$ and $\mathbb{G}_{4,1}$, as well as their corresponding Witt rings $\mathbb{L}_3$, $\mathbb{L}_{4,0}$, and $\mathbb{L}_{4,1}$ at the end of the table below.

	$W(F)$	$\lvert\mathcal{G}_F\rvert$	$\mathcal{G}_F$
1.1	$\mathbb{Z}/2\mathbb{Z}$	1	1
2.1	$\mathbb{Z}$	2	$\mathbb{Z}/2\mathbb{Z}$
2.2	$\mathbb{Z}/4\mathbb{Z}$	4	$\mathbb{Z}/4\mathbb{Z}$
2.3	$\mathbb{Z}/2\mathbb{Z}[x]$	4	$\mathbb{Z}/4\mathbb{Z}$
4.1	$\mathbb{Z}[x]$	8	$\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$
4.2	$\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	16	$\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/4\mathbb{Z}$
4.3	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	32	$\mathbb{Z}/4\mathbb{Z} * \mathbb{Z}/4\mathbb{Z}$
4.4	$\mathbb{Z}/2\mathbb{Z}[x] \times \mathbb{Z}/2\mathbb{Z}[y]$	32	$\mathbb{Z}/4\mathbb{Z} * \mathbb{Z}/4\mathbb{Z}$
4.5	$\mathbb{Z}/4\mathbb{Z}[x]$	16	$\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$
4.6	$\mathbb{Z}/2\mathbb{Z}[x,y]$	16	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
8.1	$\mathbb{Z} \times \mathbb{Z}[x]$	64	$\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$
8.2	$\mathbb{Z}[x] \times \mathbb{Z}/4\mathbb{Z}$	128	$\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/4\mathbb{Z}$
8.3	$\mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z})^2$	256	$\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/4\mathbb{Z} * \mathbb{Z}/4\mathbb{Z}$
8.4	$\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}[x]$	128	$\mathbb{Z}/2\mathbb{Z} * (\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z})$
8.5	$\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}[x,y]$	128	$\mathbb{Z}/2\mathbb{Z} * (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z})$
8.6	$(\mathbb{Z}/4\mathbb{Z})^3$	512	$\mathbb{Z}/4\mathbb{Z} * \mathbb{Z}/4\mathbb{Z} * \mathbb{Z}/4\mathbb{Z}$
8.7	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}[x]$	256	$\mathbb{Z}/4\mathbb{Z} * (\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z})$
8.8	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}[x,y]$	256	$\mathbb{Z}/4\mathbb{Z} * (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z})$
8.9	$(\mathbb{Z}/2\mathbb{Z}[x])^3$	512	$\mathbb{Z}/4\mathbb{Z} * \mathbb{Z}/4\mathbb{Z} * \mathbb{Z}/4\mathbb{Z}$
8.10	$\mathbb{Z}/2\mathbb{Z}[x] \times \mathbb{Z}/2\mathbb{Z}[y,z]$	256	$\mathbb{Z}/4\mathbb{Z} * (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z})$
8.11	$\mathbb{Z}[x,y]$	32	$\mathbb{Z}/4\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z})$
8.12	$(\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z})[x]$	64	$\mathbb{Z}/4\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/4\mathbb{Z})$
8.13	$(\mathbb{Z}/4\mathbb{Z})^2[x]$	128	$\mathbb{Z}/4\mathbb{Z} \rtimes (\mathbb{Z}/4\mathbb{Z} * \mathbb{Z}/4\mathbb{Z})$
8.14	$(\mathbb{Z}/2\mathbb{Z}[x] \times \mathbb{Z}/2\mathbb{Z}[y])[z]$	64	$\mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z} * \mathbb{Z}/4\mathbb{Z})$
8.15	$\mathbb{Z}/4\mathbb{Z}[x,y]$	64	$\mathbb{Z}/4\mathbb{Z} \rtimes (\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z})$
8.16	$\mathbb{Z}/2\mathbb{Z}[x,y,z]$	64	$(\mathbb{Z}/4\mathbb{Z})^3$
8.17	$\mathbb{L}_3$	256	$\mathbb{G}_3$
16.1	$\mathbb{Z}[x] \times \mathbb{Z}[y]$	2^{10}	$\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$
16.2	$\mathbb{Z} \times \mathbb{Z}[x] \times \mathbb{Z}/4\mathbb{Z}$	2^{11}	$\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/4\mathbb{Z}$
16.3	$\mathbb{Z}[x] \times (\mathbb{Z}/4\mathbb{Z})^2$	2^{12}	$\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/4\mathbb{Z} * \mathbb{Z}/4\mathbb{Z}$
16.4	$\mathbb{Z}[x] \times \mathbb{Z}/4\mathbb{Z}[y]$	2^{11}	$\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z} * (\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z})$
16.5	$\mathbb{Z}[x] \times \mathbb{Z}/2\mathbb{Z}[y,z]$	2^{11}	$\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z} * (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z})$
16.6	$\mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z})^3$	2^{13}	$\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/4\mathbb{Z} * \mathbb{Z}/4\mathbb{Z} * \mathbb{Z}/4\mathbb{Z}$
16.7	$\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}[x]$	2^{12}	$\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/4\mathbb{Z} * (\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z})$
16.8	$\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}[x,y]$	2^{12}	$\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/4\mathbb{Z} * (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z})$
16.9	$\mathbb{Z} \times \mathbb{Z}[x,y]$	2^9	$\mathbb{Z}/2\mathbb{Z} * \big(\mathbb{Z}/4\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z})\big)$
16.10	$\mathbb{Z} \times (\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z})[x]$	2^{10}	$\mathbb{Z}/2\mathbb{Z} * \big(\mathbb{Z}/4\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/4\mathbb{Z})\big)$
16.11	$\mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z})^2[x]$	2^{11}	$\mathbb{Z}/2\mathbb{Z} * \big(\mathbb{Z}/4\mathbb{Z} \rtimes (\mathbb{Z}/4\mathbb{Z} * \mathbb{Z}/4\mathbb{Z})\big)$
16.12	$\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z}[x] \times \mathbb{Z}/2\mathbb{Z}[y])[z]$	2^{11}	$\mathbb{Z}/2\mathbb{Z} * \big(\mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z} * \mathbb{Z}/4\mathbb{Z})\big)$
16.13	$\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}[x,y]$	2^{10}	$\mathbb{Z}/2\mathbb{Z} * \big(\mathbb{Z}/4\mathbb{Z} \rtimes (\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z})\big)$

https://doi.org/10.4153/CJM-1995-065-0 Published online by Cambridge University Press

	$W(F)$	$\lvert\mathcal{G}_F\rvert$	$\mathcal{G}_F$
16.14	$\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}[x,y,z]$	2^{10}	$\mathbb{Z}/2\mathbb{Z}*(\mathbb{Z}/4\mathbb{Z})^3$
16.15	$\mathbb{Z}\times\mathbb{L}_3$	2^{12}	$\mathbb{Z}/2\mathbb{Z}*\mathbb{G}_3$
16.16	$(\mathbb{Z}/4\mathbb{Z})^4$	2^{14}	$\mathbb{Z}/4\mathbb{Z}*\mathbb{Z}/4\mathbb{Z}*\mathbb{Z}/4\mathbb{Z}*\mathbb{Z}/4\mathbb{Z}$
16.17	$(\mathbb{Z}/4\mathbb{Z})^2\times\mathbb{Z}/4\mathbb{Z}[x]$	2^{13}	$\mathbb{Z}/4\mathbb{Z}*\mathbb{Z}/4\mathbb{Z}*(\mathbb{Z}/4\mathbb{Z}\rtimes\mathbb{Z}/4\mathbb{Z})$
16.18	$(\mathbb{Z}/4\mathbb{Z})^2\times\mathbb{Z}/2\mathbb{Z}[x,y]$	2^{13}	$\mathbb{Z}/4\mathbb{Z}*\mathbb{Z}/4\mathbb{Z}*(\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z})$
16.19	$\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}[x,y]$	2^{10}	$\mathbb{Z}/4\mathbb{Z}*\big(\mathbb{Z}/4\mathbb{Z}\rtimes(\mathbb{Z}/2\mathbb{Z}*\mathbb{Z}/2\mathbb{Z})\big)$
16.20	$\mathbb{Z}/4\mathbb{Z}\times(\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z})[x]$	2^{11}	$\mathbb{Z}/4\mathbb{Z}*\big(\mathbb{Z}/4\mathbb{Z}\rtimes(\mathbb{Z}/4\mathbb{Z}*\mathbb{Z}/2\mathbb{Z})\big)$
16.21	$\mathbb{Z}/4\mathbb{Z}\times(\mathbb{Z}/4\mathbb{Z})^2[x]$	2^{12}	$\mathbb{Z}/4\mathbb{Z}*\big(\mathbb{Z}/4\mathbb{Z}\rtimes(\mathbb{Z}/4\mathbb{Z}*\mathbb{Z}/4\mathbb{Z})\big)$
16.22	$\mathbb{Z}/4\mathbb{Z}\times(\mathbb{Z}/2\mathbb{Z}[x]\times\mathbb{Z}/2\mathbb{Z}[y])[z]$	2^{12}	$\mathbb{Z}/4\mathbb{Z}*\big(\mathbb{Z}/4\mathbb{Z}\times(\mathbb{Z}/4\mathbb{Z}*\mathbb{Z}/4\mathbb{Z})\big)$
16.23	$\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}[x,y]$	2^{11}	$\mathbb{Z}/4\mathbb{Z}*\big(\mathbb{Z}/4\mathbb{Z}\rtimes(\mathbb{Z}/4\mathbb{Z}\rtimes\mathbb{Z}/4\mathbb{Z})\big)$
16.24	$\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}[x,y,z]$	2^{11}	$\mathbb{Z}/4\mathbb{Z}*(\mathbb{Z}/4\mathbb{Z})^3$
16.25	$\mathbb{Z}/4\mathbb{Z}\times\mathbb{L}_3$	2^{13}	$\mathbb{Z}/4\mathbb{Z}*\mathbb{G}_3$
16.26	$(\mathbb{Z}/2\mathbb{Z}[x])^4$	2^{14}	$\mathbb{Z}/4\mathbb{Z}*\mathbb{Z}/4\mathbb{Z}*\mathbb{Z}/4\mathbb{Z}*\mathbb{Z}/4\mathbb{Z}$
16.27	$\mathbb{Z}/2\mathbb{Z}[x]\times\mathbb{Z}/2\mathbb{Z}[y]\times\mathbb{Z}/2\mathbb{Z}[z,w]$	2^{13}	$\mathbb{Z}/4\mathbb{Z}*\mathbb{Z}/4\mathbb{Z}*(\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z})$
16.28	$\mathbb{Z}/2\mathbb{Z}[x]\times(\mathbb{Z}/2\mathbb{Z}[y]\times\mathbb{Z}/2\mathbb{Z}[z])[w]$	2^{12}	$\mathbb{Z}/4\mathbb{Z}*\big(\mathbb{Z}/4\mathbb{Z}\times(\mathbb{Z}/4\mathbb{Z}*\mathbb{Z}/4\mathbb{Z})\big)$
16.29	$\mathbb{Z}/2\mathbb{Z}[x]\times\mathbb{Z}/2\mathbb{Z}[y,z,w]$	2^{11}	$\mathbb{Z}/4\mathbb{Z}*(\mathbb{Z}/4\mathbb{Z})^3$
16.30	$\mathbb{Z}/4\mathbb{Z}[x]\times\mathbb{Z}/4\mathbb{Z}[y]$	2^{12}	$(\mathbb{Z}/4\mathbb{Z}\rtimes\mathbb{Z}/4\mathbb{Z})*(\mathbb{Z}/4\mathbb{Z}\rtimes\mathbb{Z}/4\mathbb{Z})$
16.31	$\mathbb{Z}/4\mathbb{Z}[x]\times\mathbb{Z}/2\mathbb{Z}[y,z]$	2^{12}	$(\mathbb{Z}/4\mathbb{Z}\rtimes\mathbb{Z}/4\mathbb{Z})*(\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z})$
16.32	$\mathbb{Z}/2\mathbb{Z}[x,y]\times\mathbb{Z}/2\mathbb{Z}[z,w]$	2^{12}	$(\mathbb{Z}/4\mathbb{Z})^2*(\mathbb{Z}/4\mathbb{Z})^2$
16.33	$(\mathbb{Z})^3[x]$	2^8	$\mathbb{Z}/4\mathbb{Z}\rtimes(\mathbb{Z}/2\mathbb{Z}*\mathbb{Z}/2\mathbb{Z}*\mathbb{Z}/2\mathbb{Z})$
16.34	$(\mathbb{Z}^2\times\mathbb{Z}/4\mathbb{Z})[x]$	2^9	$\mathbb{Z}/4\mathbb{Z}\rtimes(\mathbb{Z}/4\mathbb{Z}*\mathbb{Z}/2\mathbb{Z}*\mathbb{Z}/2\mathbb{Z})$
16.35	$(\mathbb{Z}\times(\mathbb{Z}/4\mathbb{Z})^2)[x]$	2^{10}	$\mathbb{Z}/4\mathbb{Z}\rtimes(\mathbb{Z}/2\mathbb{Z}*\mathbb{Z}/4\mathbb{Z}*\mathbb{Z}/4\mathbb{Z})$
16.36	$(\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}[x])[y]$	2^9	$\mathbb{Z}/4\mathbb{Z}\rtimes\big(\mathbb{Z}/2\mathbb{Z}*(\mathbb{Z}/4\mathbb{Z}\rtimes\mathbb{Z}/4\mathbb{Z})\big)$
16.37	$(\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}[x,y])[z]$	2^9	$\mathbb{Z}/4\mathbb{Z}\rtimes\big(\mathbb{Z}/2\mathbb{Z}*(\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z})\big)$
16.38	$(\mathbb{Z}/4\mathbb{Z})^3[x]$	2^{11}	$\mathbb{Z}/4\mathbb{Z}\rtimes(\mathbb{Z}/4\mathbb{Z}*\mathbb{Z}/4\mathbb{Z}*\mathbb{Z}/4\mathbb{Z})$
16.39	$(\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}[x])[y]$	2^{10}	$\mathbb{Z}/4\mathbb{Z}\rtimes\big(\mathbb{Z}/4\mathbb{Z}*(\mathbb{Z}/4\mathbb{Z}\rtimes\mathbb{Z}/4\mathbb{Z})\big)$
16.40	$(\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}[x,y])[z]$	2^{10}	$\mathbb{Z}/4\mathbb{Z}\rtimes\big(\mathbb{Z}/4\mathbb{Z}*(\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z})\big)$
16.41	$(\mathbb{Z}/2\mathbb{Z}[x])^3[y]$	2^{11}	$\mathbb{Z}/4\mathbb{Z}\times(\mathbb{Z}/4\mathbb{Z}*\mathbb{Z}/4\mathbb{Z}*\mathbb{Z}/4\mathbb{Z})$
16.42	$(\mathbb{Z}/2\mathbb{Z}[x]\times\mathbb{Z}/2\mathbb{Z}[y,z])[w]$	2^{10}	$\mathbb{Z}/4\mathbb{Z}\times\big(\mathbb{Z}/4\mathbb{Z}*(\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z})\big)$
16.43	$\mathbb{Z}[x,y,z]$	2^8	$\mathbb{Z}/4\mathbb{Z}\rtimes\big(\mathbb{Z}/4\mathbb{Z}\rtimes(\mathbb{Z}/4\mathbb{Z}\rtimes\mathbb{Z}/4\mathbb{Z})\big)$
16.44	$(\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z})[x,y]$	2^8	$\mathbb{Z}/4\mathbb{Z}\rtimes\big(\mathbb{Z}/4\mathbb{Z}\rtimes(\mathbb{Z}/4\mathbb{Z}*\mathbb{Z}/2\mathbb{Z})\big)$
16.45	$(\mathbb{Z}/4\mathbb{Z})^2[x,y]$	2^9	$\mathbb{Z}/4\mathbb{Z}\rtimes\big(\mathbb{Z}/4\mathbb{Z}\rtimes(\mathbb{Z}/4\mathbb{Z}*\mathbb{Z}/4\mathbb{Z})\big)$
16.46	$(\mathbb{Z}/2\mathbb{Z}[x]\times\mathbb{Z}/2\mathbb{Z}[y])[z,w]$	2^9	$\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}\times(\mathbb{Z}/4\mathbb{Z}*\mathbb{Z}/4\mathbb{Z})$
16.47	$\mathbb{Z}/4\mathbb{Z}[x,y,z]$	2^8	$\mathbb{Z}/4\mathbb{Z}\rtimes\big(\mathbb{Z}/4\mathbb{Z}\rtimes(\mathbb{Z}/4\mathbb{Z}\rtimes\mathbb{Z}/4\mathbb{Z})\big)$
16.48	$\mathbb{Z}/2\mathbb{Z}[x,y,z,w]$	2^8	$(\mathbb{Z}/4\mathbb{Z})^4$
16.49	$\mathbb{L}_3[x]$	2^{10}	$\mathbb{Z}/4\mathbb{Z}\rtimes\mathbb{G}_3$
16.50	$\mathbb{L}_{4,0}$	2^{12}	$\mathbb{G}_{4,0}$
16.51	$\mathbb{L}_{4,1}$	2^{12}	$\mathbb{G}_{4,1}$

The groups $\mathbb{G}_3, \mathbb{G}_{4,0}$, and $\mathbb{G}_{4,1}$ have the following presentations, all given in category

https://doi.org/10.4153/CJM-1995-065-0 Published online by Cambridge University Press

C, *i.e.* the groups have exponent 4, with commutators and squares central of order 2:

$$\mathbb{G}_3 \cong \langle x, y, z \mid x^2 = [y, z] \rangle$$
$$\mathbb{G}_{4,0} \cong \langle x, y, z, w \mid [x, y] = [z, w] \rangle$$
$$\mathbb{G}_{4,1} \cong \langle x, y, z, w \mid [x, y][z, w] = x^2 \rangle$$

The corresponding Witt rings have the following structure:

$\mathbb{L}_3 = \mathbb{Z}/8\mathbb{Z} \cdot 1 \oplus \mathbb{Z}/2\mathbb{Z} \cdot (1 - x) \oplus \mathbb{Z}/2\mathbb{Z} \cdot (1 - y)$ with multiplication defined by $(1 - x)(1 - y) = 4$

$\mathbb{L}_{4,0} = \mathbb{Z}/2\mathbb{Z} \cdot 1 \oplus \mathbb{Z}/2\mathbb{Z} \cdot p \oplus \sum_{i=1}^{2} \big(\mathbb{Z}/2\mathbb{Z} \cdot (1 - x_i) \oplus \mathbb{Z}/2\mathbb{Z} \cdot (1 - y_i)\big)$ with multiplication defined by $(1 - x_i)(1 - y_j) = \delta_{ij} p$, $(1 - x_i)p = (1 - y_i)p = 0$

$\mathbb{L}_{4,1} = \mathbb{Z}/4\mathbb{Z} \cdot 1 \oplus \mathbb{Z}/4\mathbb{Z} \cdot (1 - z) \oplus \mathbb{Z}/2\mathbb{Z} \cdot (1 - x) \oplus \mathbb{Z}/2\mathbb{Z} \cdot (1 - y)$ with multiplication defined by $(1 - x)(1 - y) = 2(1 - z)$, $(1 - z)(1 - x) = (1 - z)(1 - y) = 0$

REFERENCES

[AEJ:1984] J. Arason, R. Elman and B. Jacob, *The graded Witt ring and Galois cohomology,* CMS Conf. Proc. **4**(1984), 17–50.

[AEJ:1987] ———, *Rigid elements, valuations, and realization of Witt rings,* J. Algebra **110**(1987), 449–467.

[Be:1978] L. Berman, *The Kaplansky Radical and Values of Binary Quadratic Forms over Fields,* Ph.D. Thesis, University of California, Berkeley, California, 1978.

[CMa:1982] A. Carson and M. Marshall, *Decomposition of Witt rings,* Canad. J. Math **34**(1982), 1276–1302.

[J:1981] B. Jacob, *On the structure of Pythagorean fields,* J. Algebra **68**(1981), 247–267.

[JWr:1989] B. Jacob and R. Ware, *A recursive description of the maximal pro-2-Galois group via Witt rings,* Math. Z. **200**(1989), 379–396.

[La:1973] T. Y. Lam, *The Algebraic Theory of Quadratic Forms,* W. A. Benjamin, Reading, Massachusetts, 1973, Second printing with revisions, 1980.

[Ma:1980] M. Marshall, *Abstract Witt Rings,* Queen's Papers in Pure and Appl. Math. **57**, Queen's University, Kingston, Ontario, Canada, 1980.

[MiSm:1993] J. Mináč and T. L. Smith, *W-groups and values of binary forms,* J. Pure Appl. Algebra **87**(1993), 61–78.

[MiSm:pre] ———, *Quotients and subgroups of W-groups,* preprint .

[MiSp:1990] J. Mináč and M. Spira, *Formally real fields, pythagorean fields, C-fields, and W-groups,* Math. Z. **205**(1990), 519–530.

[MiSp:1995] ———, *Witt rings and Galois groups,* Annals of Math., to appear.

[N:1971] J. Neukirch, *Freie Produkte proendlicher Gruppen und ihre Kohomologie,* Arch. Math **22**(1971), 337–357.

[Pf:1966] A. Pfister, *Quadratische Formen in beliebigen Körpern,* Invent. Math. **1**(1966), 116–132.

[Pn:1966] L. Pontrjagin, *Topological Groups,* Gordon and Breach, 1966.

[Sc:1985] W. Scharlau, *Quadratic and Hermitian Forms,* Grundlehren Math. Wiss. **270**, Springer-Verlag, Berlin, 1985.

[Se:1965] J.-P. Serre, *Cohomologie Galoisienne,* Lecture Notes in Math. **5**, Springer-Verlag, New York, Berlin, 1965, Cinquième édition, réviseé et complétée, 1994.

[Sm:1988] T. L. Smith, *Some 2-Groups Arising in Quadratic Form Theory and Their Generalizations,* Ph.D. Thesis, University of California, Berkeley, California, 1988.

[Sp:1987] M. Spira, *Witt Rings and Galois Groups,* Ph.D. Thesis, University of California, Berkeley, California, 1987.

[Wr:1979] R. Ware, *Quadratic forms and pro-finite 2-groups,* J. Algebra **58**(1979), 227–237.

[Wr:1981] ———, *Valuation rings and rigid elements in fields,* Canad. J. Math **33**(1981), 1338–1355.

[Wr:1983] ———, *Quadratic forms and pro-2-groups II: The galois group of the pythagorean closure of a formally real field,* J. Pure Appl. Algebra **30**(1983), 95–107.

[Wr:1985] ———, *Quadratic forms and pro-2-groups III,* Comm. Algebra **13**(1985), 1713–1736.
[Wi:1936] E. Witt, *Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der ordnung p^f,* J. Reine Angew. Math. **174**(1936), 237–245.

Department of Mathematics
University of Western Ontario
London, Ontario
N6A 5B7

Department of Mathematical Sciences
University of Cincinnati
Cincinnati, Ohio 45221-0025
U.S.A.