Formally real fields from a Galois theoretic perspective

Thomas C. Craven\textsuperscript{a}, Tara L. Smith\textsuperscript{b,}\textsuperscript{*}

\textsuperscript{a}Department of Mathematics, University of Hawaii, Honolulu, HI 96822, USA
\textsuperscript{b}Department of Mathematics, University of Cincinnati, Cincinnati, OH 45221, USA

Communicated by M.-F. Roy; received 21 October 1996; received in revised form 13 January 1998

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 equivalence classes of anisotropic quadratic forms over $F$. There is a close connection between (nontrivial) involutions in $\mathcal{G}_F$ and orderings on $F$. The purpose of this paper is to investigate how the lattice of orderings and preorderings on $F$ is determined by $\mathcal{G}_F$, and to provide a Galois-theoretic version of reduced Witt rings. © 2000 Elsevier Science B.V. All rights reserved.

MSC: 11E81; 12D15

1. Introduction and notation

The W-groups $\mathcal{G}_F$ and their properties have been studied in [9–12]. The connections with involutions have been presented in [11]. We shall show that this can be generalized to provide a realization in $\mathcal{G}_F$ of preorderings on $F$, given by subgroups which can be generated by involutions. Section 2 develops the properties of these special subgroups of the W-group and Section 3 shows the correspondence with preorderings of the field $F$. In Section 4 we apply the results to special types of preorderings, namely fans and SAP preorderings. Section 5 looks at a particular numerical invariant of finite spaces of orderings obtained from the corresponding subgroup, and the final section looks at the topology when the spaces of orderings are infinite.

Many of the ideas applied here to subgroups of W-groups generated by involutions are special cases of ideas which apply more generally to arbitrary subgroups of

\textsuperscript{*}Corresponding author. Tel.: 1 513 5564048; fax: 1 513 5563417
E-mail address: tsmith@math.uc.edu (T.L. Smith)

0022-4049/00/$-$ see front matter © 2000 Elsevier Science B.V. All rights reserved.
PII: S0022-4049(98)00068-1
W-groups. These more general results, and in particular the connections between subgroups of W-groups and additive properties of subgroups of the square class group of the base field, are explored in [4].

Given a set of elements \( g_i \in G, i \) in some index set \( I \), we write \( \langle g_i \mid i \in I \rangle \) for the subgroup of \( G \) topologically generated by the set \( \{g_i \mid i \in I\} \); viz. the closed subgroup of \( G \) generated by the set of elements \( g_i \). Whenever we speak of a subgroup being generated by a set of elements, it should be understood that we mean topologically generated, i.e. one takes the closure of the subgroup generated by the given set of elements.

The W-group \( \mathcal{G}_F \) of a field \( F \) is the Galois group over \( F \) of the field \( F^{(3)} \), which is defined to be the compositum over \( F \) of all cyclic of order 2, cyclic of order 4, and dihedral of order 8 extensions of \( F \). The field \( F^{(3)} \) can also be viewed as being constructed in a two-tiered process of taking multiquadratic extensions of \( F \) as follows. Let \( F^{(2)} \) denote the compositum over \( F \) of all quadratic extensions of \( F \). Then \( F^{(3)} \) is the compositum over \( F^{(2)} \) of all quadratic extensions of \( F^{(2)} \) which are Galois over \( F \). In the case where \( F \) is formally real, \( \mathcal{G}_F \) determines \( W(F) \) and conversely. The details of this relationship are given in the next section. These groups all lie in the category \( \mathcal{G} \), the full subcategory of the category of pro-2-groups whose objects are those pro-2-groups \( G \) satisfying \( g^4 = 1 \) and \( g^2 \in Z(G) \) for all \( g \in G \). The Frattini subgroup of such a group \( G \), denoted \( \Phi(G) \), is (topologically) generated by squares and commutators (cf. [10, Proposition 1.3]). Indeed, for \( G \) in \( \mathcal{G} \), \( \Phi(G) = [G,G]G^2 = G^2 \). (The reader is referred to [14, Ch.3, Section 3] for more details on the structure of pro-\( p \)-groups.)

We define an essential subgroup of a group \( G \in \mathcal{G} \) to be a closed subgroup \( H \) satisfying \( H \cap \Phi(G) = \Phi(H) \). An essential subgroup is characterized by the fact that a minimal set of topological generators for \( H \) extends to a minimal set for \( G \).

We will need a number of results on orderings and W-groups, which are proved in [11]. In particular, letting \( \Phi = \Phi(\mathcal{G}_F) \), we have \( \mathcal{G}_F/\Phi \cong \text{Gal}(F^{(2)}/F) \) and the nonidentity cosets of \( \Phi \) in \( \mathcal{G}_F \) which are represented by involutions are in 1-1 correspondence with the elements of \( X_F \), the set of all orderings on \( F \). Recall that an ordering \( P \) on a field \( F \) is a subset \( P \subseteq F \) satisfying

1. \( P + P \subseteq P \),
2. \( P \cdot P \subseteq P \),
3. \( P \cap -P = \emptyset \), and
4. \( P \cup -P = \hat{F} \).

An involution \( \sigma \) not in \( \Phi \) (a ‘nontrivial’ involution) determines an ordering \( P_\sigma = \{a \in F \mid \sqrt{a} = \sigma(\sqrt{a})\} = (F^{(3)}_\sigma)^3 \cap \hat{F} \), where \( F^{(3)}_\sigma \) is the fixed field of \( \sigma \) in \( F^{(3)} \). In particular, if \( \sigma^2 = 1 \), \( \sigma \notin \Phi \), then \( \sigma(\sqrt{\text{I}}) = -\sqrt{\text{I}} \). Any two involutions in the same coset of \( \Phi \) determine the same ordering on \( F \), since their actions on \( F^{(2)} \) are the same. A nontrivial involution is called real if its fixed field \( F^{(3)}_\sigma \) is a relative real closure of \( F \) in \( F^{(3)} \); every nonidentity coset of \( \Phi \) which is represented by an involution is represented by a real involution. All real involutions in a given coset are conjugates. Conversely, if \( P \) is any ordering on \( F \), then there exists a nontrivial involution \( \sigma \) in \( \mathcal{G}_F \) such that \( P = (F^{(3)}_\sigma)^3 \cap \hat{F} \). This \( \sigma \) is uniquely determined by \( P \) up to multiplication by elements of \( \Phi \), that is, \( P \) determines a unique coset \( \sigma \Phi \), where \( \sigma \) is an involution in \( \mathcal{G}_F \).
Finally, we will need the concept of a preorder on the field \( F \). The principal facts about preorderings are nicely presented in [3]. A subset \( T \subseteq \hat{F} \) is a preorder on \( F \) if it satisfies

1. \( \hat{F}^2 \subseteq T \),
2. \( T + T \subseteq T \), and
3. \( T \cdot T \subseteq T \).

With these three conditions, the condition that \( T \) is a proper subset of \( \hat{F} \) is equivalent to requiring \(-1 \notin T\). Every ordering is a preorder, and every preorder on \( F \) is the intersection of the orderings on \( F \) which contain it.

2. Involution subgroups

The Galois-theoretic manifestation of a preorder on \( F \) is an essential subgroup of \( \mathscr{G}_F \) which is generated by involutions. This turns out to be a direct generalization of the correspondence between orderings on \( F \) and nontrivial involutions in \( \mathscr{G}_F \), as such involutions determine an essential subgroup isomorphic to \( \mathbb{Z}/2\mathbb{Z} \). As in the case with orderings, distinct preorderings correspond to subgroups which are distinct \( \mod \Phi(\mathscr{G}_F) \). The relevant subgroups of \( \mathscr{G}_F \) will be seen (in the next section) to be those given by the following definition.

**Definition.** An involution subgroup of a group \( G \) in \( \mathfrak{cat} \) is an essential subgroup of \( G \) generated (topologically) by involutions.

**Theorem 2.1.** Let \( G \in \mathfrak{cat} \) and write \( \Phi = \Phi(G) \).

1. Any closed subgroup \( H \subseteq G \) can be written as
   \[ H \cong \mathcal{E}_H \times (H \cap \Phi)/\Phi(H), \]
   where \( \mathcal{E}_H \) is an essential subgroup.

2. \( \mathcal{E}_H \) is a maximal essential subgroup of \( G \) in \( H \).

3. The group \( \mathcal{E}_H \) is determined up to isomorphism.

4. If \( H' \) is any other closed subgroup of \( G \) with \( H\Phi = H'\Phi \), then \( \mathcal{E}_H \cong \mathcal{E}_{H'} \).

**Proof.** (1) If \( H \cap \Phi = \Phi(H) \), we are done. Assume that \( \Phi(H) \subseteq H \cap \Phi \). Since \( H/(H \cap \Phi) \) is an elementary 2-group, we may choose a set of elements \( \{ h_i \in H \mid i \in I \} \) such that \( \{ \tilde{h}_i = h_i(H \cap \Phi) \mid i \in I \} \) is a \( \mathbb{Z}/2\mathbb{Z} \)-basis for \( H/(H \cap \Phi) \). Extend this to a set of elements \( \{ h_i, t_j \in H \mid i \in I, j \in J \} \) such that the images \( \{ h_i \Phi(H), t_j \Phi(H) \mid i \in I, j \in J \} \) form a basis of \( H/\Phi(H) \). Then \( \{ h_i, t_j \mid i \in I, j \in J \} \) is a minimal set of generators for \( H \). By our choice of \( \{ t_j \} \), we have \( \langle t_j \Phi(H) \mid j \in J \rangle \cong (H \cap \Phi)/\Phi(H) \). Furthermore \( \langle t_j \mid j \in J \rangle \triangleleft H \) and \( \langle t_j \mid j \in J \rangle \cap \langle h_i \mid i \in I \rangle = 1 \). Since the generators \( t_j \), being in \( H \cap \Phi \), are central, we also have \( \langle h_i \mid i \in I \rangle \triangleleft H \), so that \( H \cong \langle h_i \mid i \in I \rangle \times \langle t_j \mid j \in J \rangle \).

Set \( \mathcal{E}_H = \langle h_i \mid i \in I \rangle \). We must show that \( \mathcal{E}_H \) is an essential subgroup; i.e. \( \Phi(\langle h_i \mid i \in I \rangle) = \langle h_i \mid i \in I \rangle \cap \Phi \). Let \( h = \prod_{i=1}^n h'_i \in \Phi \), where \( h'_i \in \{ h_i \mid i \in I \} \). Then \( \prod h'_i \rightarrow 1 \) in \( H \cap \Phi \) and so, as \( h_i \) is a basis of \( \mathcal{E}_H \) must appear in pairs. Reordering
the factors gives \( h \) as a product of \( h_i^2 \) and commutators of the form \([h'_i, h'_j]\), whence \( h \in \Phi(\mathcal{H}). \)

(2) Let \( \mathcal{E}' \supseteq \mathcal{E}_H \) be a subgroup of \( H \). We claim that \( \mathcal{E}' \) is not an essential subgroup of \( G \). By (1), we can write \( H \cong \mathcal{E}_H \times K \), where \( K \) is an elementary 2-group. Thus we have \( \Phi(H) \cong \Phi(\mathcal{E}_H \times K) = \Phi(\mathcal{E}_H) \times \Phi(K) \cong \Phi(\mathcal{E}_H) \). Therefore, since \( \mathcal{E}_H \subseteq \mathcal{E}' \subseteq H \), we have \( \Phi(\mathcal{E}') = \Phi(H) = \Phi(\mathcal{E}_H) \). Since \( \mathcal{E}' \) properly contains \( \mathcal{E}_H \), we can properly extend the minimal set of generators \( \{h_i\} \) of \( \mathcal{E}_H \) to a minimal set \( \{h_i', h_j'\} \) of \( \mathcal{E}' \). Then \( \{h_i, h_j'\} \) forms a basis for \( \mathcal{E}' / \Phi(\mathcal{E}') \) and \( \{h_i\} \) forms a basis of \( \mathcal{E}_H / \Phi(\mathcal{E}_H) \). By construction of \( \mathcal{E}_H \), the set \( \{h_i\} \) is a basis for \( H/(H \cap \Phi) \) and therefore contains a basis for \( \mathcal{E}'/(H \cap \Phi) \cong \mathcal{E}' / (\mathcal{E}' \cap \Phi) \). Comparing \( \mathcal{E}' / \Phi(\mathcal{E}') \) with \( \mathcal{E}' / (\mathcal{E}' \cap \Phi) \), we see that \( \mathcal{E}' \cap \Phi \cong \Phi(\mathcal{E}') \).

(3) Let \( \mathcal{E}, \mathcal{E}' \) be maximal essential subgroups of \( H \). Let \( \{\tilde{h}_i\} \) be any basis for \( H/H \cap \Phi \). Then there exist liftings to \( H \), \( \{h_i\} \) and \( \{h'_i\} \), which are minimal sets of (topological) generators for \( \mathcal{E} \) and \( \mathcal{E}' \), respectively. We have \( h_i(H \cap \Phi) = h'_i(H \cap \Phi) \) for each \( i \). Define a map \( \theta : \mathcal{E} \to \mathcal{E}' \) by extending \( h_i \to h'_i \) multiplicatively. We must check that \( \theta \) is well-defined, i.e., if \( \prod [h_i = 1] \) in \( \mathcal{E} \), we must have \( \prod [h'_i = 1] \) in \( \mathcal{E}' \). Note that for each \( i \), there exists an element \( \phi_i \in \Phi \) with \( h'_i = h_i \phi_i \). We know that since \( \{h_i\} \) is a minimal set of generators for \( \mathcal{E} \), a product \( \prod [h_i = 1] \in \Phi(\mathcal{E}) \) can always be written in the form \( \prod [h_i = 1] \prod [h'_i = 1] \prod [h_i h_m] \). But then, since all \( \phi_i \) are central elements of order at most two, we obtain

\[
\theta\left(\prod [h_i]\right) = \prod \left(\theta(h_k)\right)^2 \prod [\theta(h_i), \theta(h_m)] = \prod \left(h_k \phi_k\right)^2 \prod [h_i h_m] = 1.
\]

Thus we have a well-defined surjective homomorphism which is clearly invertible.

(4) Since \( H \Phi = H' \Phi \), we have \( \mathcal{E}_H \Phi \cong \mathcal{E}_H \Phi \) by (3). Thus, it will suffice to show that \( \mathcal{E}_H \Phi \cong \mathcal{E}_H \), i.e. that \( \mathcal{E}_H \) is a maximal essential subgroup of \( H \Phi \). Assume that \( \mathcal{E} \supseteq \mathcal{E}_H \) is a subgroup of \( H \Phi \). Then we have

\[
\mathcal{E}_H / \Phi(\mathcal{E}_H) = \mathcal{E}_H / (\mathcal{E}_H \cap \Phi) \cong \mathcal{E}_H \Phi / \Phi \subseteq \mathcal{E} \Phi / \Phi \subseteq H \Phi / \Phi \cong H(H \cap \Phi).
\]

But by (1), we have \( \mathcal{E}_H / (\mathcal{E}_H \cap \Phi) = H(H \cap \Phi) \). Thus all groups in (2.1) are isomorphic. If \( \mathcal{E} \) is an essential subgroup, then \( \mathcal{E} \Phi / \Phi \cong \mathcal{E} / (\mathcal{E} \cap \Phi) = \mathcal{E} / \Phi(\mathcal{E}) \), so (2.1) implies that \( \mathcal{E} \) and \( \mathcal{E}_H \) have the same minimal set of generators and hence are equal.

**Corollary 2.2.** (1) Any subgroup \( H \subseteq G \subseteq \mathcal{E} \) at topologically generated by involutions can be written as

\[
H \cong \mathcal{E}_H \times (H \cap \Phi) / \Phi(H),
\]

where \( \mathcal{E}_H \) is an involution subgroup.

(2) \( \mathcal{E}_H \) is a maximal involution subgroup of \( G \) in \( H \).

(3) The group \( \mathcal{E}_H \) is determined up to isomorphism.

(4) If \( H' \) is any other subgroup topologically generated by involutions with \( H \Phi = H' \Phi \), then \( \mathcal{E}_H \cong \mathcal{E}_H' \).
Proof. The proof is analogous to the proof of Theorem 2.1. Since \( H \) is generated by involutions, the elements \( \{ h_i, t_j \in H \mid i \in I, j \in J \} \) can be chosen to be involutions. Then \( \mathcal{H} = \mathcal{E}_H \) in the proof of Theorem 2.1. □

The involution subgroups of a W-group \( \mathcal{G} \) satisfy additional properties not shared by general elements of \( \mathcal{G} \). For example, no such group can have \( \mathbb{Z}/2\mathbb{Z} \) as a direct factor. Indeed, we have the following result obtained in [8]. In order to prove it, we will need to understand precisely how the relations on \( W(F) \) determine \( \mathcal{G}_F \) and conversely. This is described carefully in [9, 10] and [12]. We give a brief explanation here.

Let \( G = \hat{F}/\hat{F}^2 \) 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 \( B = \{ b_i \mid i \in I \} \) 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 \( \text{Br}(F) \) of \( F \) generated by the classes of quaternion algebras over \( F \) (see [2] or [5]). Let \( \mathcal{F} \) be the free group in the category \( \mathcal{G} \) at 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 \( \{ z_i^2, [z_i, z_j] : i, j \in I, j > i \} \). 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 \( \langle \cdot, \cdot \rangle : \Phi(\mathcal{F}) \times P \to \mathbb{Z}/2\mathbb{Z} \), obtained by letting \( \{ z_i^2, [z_i, z_j] : i, j \in I, j > i \} \) and \( \{ t_i^2, t_it_j, i, j \in I, j > i \} \) be dual bases. We have a group homomorphism \( \theta : P \to Q \) given by \( \theta(t_i^2) = (b_i, b_i), \theta(t_it_j) = (b_i, b_j) \).

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 \( Q \). It can then be shown that the W-group \( \mathcal{G} \) and the group \( \mathcal{F}/\mathcal{R} \) are isomorphic to 2-groups.

This description of the relations on the W-group allows one to define an abstract W-group associated with any abstract Witt ring \( W \) (in the sense of [5]). To do this, one just replaces \( (\hat{F}/\hat{F}^2, Q) \) in the description above with the associated “quaternionic structure” \( (G_W, Q_W) \) for the Witt ring \( W \) [15].

Proposition 2.3. Any two nontrivial involutions of \( \mathcal{G} = \mathcal{G}_F \) which are not in the same coset of \( \Phi(\mathcal{G}_F) \) do not commute with each other. In other words, \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \) is not an essential subgroup of \( \mathcal{G} \).

Proof. Assume \( H = \langle \sigma, \tau \mid \sigma^2 = \tau^2 = [\sigma, \tau] = 1 \rangle \subseteq \mathcal{G} \), and assume \( \sigma, \tau, \sigma \tau \notin \Phi = \Phi(\mathcal{G}_F) \). Then \( -1 \notin \hat{F}^2 \), for if \( -1 \in \hat{F}^2 \), we would have \( (a, a) = 1 \) in \( \text{Br}_2(F) \) for all \( a \in \hat{F} \). This means, in the relations for \( \mathcal{G} \), no “squared terms” appear. But if \( H \) is a subgroup of \( \mathcal{G} \), then \( \sigma^2 \) and \( \tau^2 \) both appear.

Let \( L/F \) be a dihedral extension of order 8 containing \( F(\sqrt{a}, \sqrt{-a}) \), where \( \text{Gal}(L/F(\sqrt{-1})) \cong \mathbb{Z}_4 \), and where \( \sqrt{a} \) is not fixed by \( \sigma \). (We can do this because \( \sigma \notin \Phi \).) Such an extension is referred to as a \( D^{n \times a} \)-extension of \( F \); it exists since the quaternion algebra \( (a, -a) \) is split over \( F \).) Consider \( \langle \sigma, \tau \rangle \), the image of \( H \) in \( \text{Gal}(L/F) \). We have \( \hat{\sigma}^2 = 1 \), so the fixed field of \( \hat{\sigma} \) is of index 2 in \( L \) and does not contain \( \sqrt{a} \). This means it cannot contain \( \sqrt{-1} \) either, but must be one of the two extensions of \( F \) of degree 4 sitting over \( F(\sqrt{-a}) \), so \( (\sqrt{-1})^a = -\sqrt{-1} \). Now choose
an element \( b \in \bar{F} \setminus \bar{F}^2 \) for which \( \sqrt{b^\sigma} = \sqrt{b} \) and \( \sqrt{b^\tau} = -\sqrt{b} \). Such a \( b \) exists since \( \sigma, \tau, \sigma \tau \not \in \Phi \). Consider the image \( \langle \bar{\sigma}, \bar{\tau} \rangle \) of \( H \) inside the Galois group \( G \) of a \( D_{\infty, b} \_b \_b \) extension \( K \) of \( F \). The fixed field \( K_\sigma \) of \( \bar{\sigma} \) cannot contain \( \sqrt{b} \), so it must be one of the two subfields of index 2 in \( K \) not containing \( \sqrt{b} \). On the other hand, the fixed field \( K_\tau \) of \( \tau \) cannot contain \( \sqrt{b} \), so considering the subfield lattice, we see the intersection \( K_\sigma \cap K_\tau = F \). Thus, the image of \( H \) in \( G \) generates \( G \), which means \( \sigma \) and \( \tau \) cannot commute. This is a contradiction, so \( H \) cannot exist as an essential subgroup of \( \Phi \). □

**Remark.** It can be shown [4] that the only essential subgroups of \( \Phi_F \) that are generated by two generators (independent mod \( \Phi(\Phi_F) \)) are isomorphic to \( \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \) \( \cong \) \( \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \) or \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \) where \( \times \) denotes the free product in the category \( \mathcal{G} \_at \). Of these five groups, only the last two have any nontrivial involutions, and only the last is an involution subgroup.

3. **Connections with preorderings**

For any group \( G \in \mathcal{G} \_at \), we define an equivalence relation on the closed subgroups of \( G \) by \( H \sim H' \) if \( H\Phi(G) = H'\Phi(G) \). This restricts to an equivalence relation on the subgroups of \( G \) topologically generated by involutions. In Theorem 2.1 we showed that the isomorphism type of a maximal essential subgroup of any group in an equivalence class is an invariant of the equivalence class. Thus, we can identify any equivalence class by \( [\mathcal{E}] \) where \( \mathcal{E} \) is an essential subgroup of \( G \) in the equivalence class. We define a partial ordering on the set of equivalence classes by \( [\mathcal{E}_1] \leq [\mathcal{E}_2] \) if \( \mathcal{E}_1 \Phi(G) \subseteq \mathcal{E}_2 \Phi(G) \); this restricts to a partial ordering on the set of equivalence classes of subgroups topologically generated by involutions, where again we can identify any equivalence class by \( [\mathcal{F}] \) where \( \mathcal{F} \) is an involution subgroup of \( G \).

Now let \( G = \Phi_F \) be the W-group of a field \( F \). To any closed subgroup \( H \subseteq G \) we can associate a subgroup \( T_H \) of \( \bar{F} \) by defining \( T_H = \{ a \in \bar{F} \mid \sigma(\sqrt{a}) = \sqrt{a} \ \forall \sigma \in H \} \). Notice that since \( \Phi(G) \) fixes \( \sqrt{F} = \{ \sqrt{a} \mid a \in \bar{F} \} \), the subgroup \( T_H \) is an invariant of the equivalence class \( [H] \) of \( H \).

**Proposition 3.1.** Let \( H \) range over the closed subgroups of \( \Phi_F \) with \( H \not \in \Phi(\Phi_F) \). There is a bijective inclusion-reversing correspondence between equivalence classes \( [H] \) and subgroups \( T \) of \( \bar{F} \) containing \( \bar{F}^2 \). Furthermore, \( H \) is generated by involutions if and only if \( T_H \) is a preordering on \( F \).

**Proof.** Again let \( \Phi \) denote the Frattini subgroup \( \Phi(\Phi_F) \). Suppose that \( T_{[\mathcal{E}]} = T_{[\mathcal{E}']}. \) Let \( \{ \sigma_i \mid i \in I \} \) be a minimal set of topological generators for \( \mathcal{E} \), and \( \{ \sigma'_i \mid i \in I' \} \) be a minimal set of topological generators for \( \mathcal{E}' \). Then we may write the sets as \( T_{[\mathcal{E}]} = \cap_{i \in I} T_{\sigma_i} \) and \( T_{[\mathcal{E}']} = \cap_{i \in I'} T_{\sigma'_i} \), where \( T_\sigma = T(\sigma) \). We need to show that \( \{ \sigma_i \mid i \in I \} \times \{ \sigma'_i \mid i \in I' \} \). In fact, it clearly suffices to show that \( \bigcap T_{\sigma_i} \subseteq T_\sigma \) implies \( \sigma \in \langle \sigma_i \mid i \in I \rangle \Phi \). Suppose that \( \sigma \not \in \langle \sigma_i \mid i \in I \rangle \Phi \), and let \( L \) be the fixed field of \( \langle \sigma_i \mid i \in I \rangle \Phi \). Then we
have \( a \in \bigcap T_\alpha \iff \sigma(\sqrt{a}) = \sqrt{a} \) for all \( i \iff \sqrt{a} \in L \). But \( \sigma \notin \langle \sigma_i \mid i \in I \rangle \Phi \) implies that the fixed field of \( \langle \sigma, \sigma_i \mid i \in I \rangle \Phi \) is properly contained in \( L \). Since \( L \) is a subfield of \( F^{(2)} \), there exists some \( a \in \bigcap T_\alpha \), with \( \sigma(\sqrt{a}) \neq \sqrt{a} \). But then \( a \notin T_\alpha \), a contradiction. This shows injectivity.

To show surjectivity, let \( T \) be any subgroup of \( F^2 \) containing \( F^2 \). Observe that every subgroup \( S \) of \( F \) containing \( F^2 \) and of index 2 in \( F \) can be written as \( S = T_\alpha \) for some \( \sigma \in \mathcal{G}_F \). Then \( T \) can be written as \( T = \bigcap_{\alpha \supseteq T} T_\alpha = T_{\langle \sigma \rangle} \), where \( \mathcal{S} \sim \langle \sigma \mid T_\alpha \supseteq T \rangle \). Thus, we have a one-to-one correspondence; it is clearly inclusion-reversing.

By [11], there is a one-to-one correspondence between cosets \( \sigma \Phi, \langle \sigma \rangle \) an involution subgroup, and orderings on \( F \), where the ordering corresponding to \( \sigma \Phi \) is \( P_\sigma = \{ a \in F \mid \sigma(\sqrt{a}) = \sqrt{a} \} \). If \( \{ \sigma_i \mid i \in I \} \) is a minimal set of topological generators for \( H \), all of which are involutions, then \( T_H = \bigcap_{\alpha \in I} P_\alpha \), so we see that \( T_H \) is a preordering.

Conversely, let \( H \) be any closed subgroup of \( \mathcal{G}_F \) not contained in \( \Phi \), such that \( T_H \) is a preordering. By Theorem 2.1, \( H \) is generated by involutions if and only if \( H \) is also generated by involutions. By Theorem 2.1, \( H \) is a subfield of \( \mathcal{F} \). Now \( \mathcal{F} \) is generated by involutions, namely \( F(\{ \sqrt{a} \mid a \in T_H \}) \). Thus \( \mathcal{F} \Phi \cong \delta_H \Phi \), so \( \delta_H \) is also generated by involutions, and hence so is \( H \). \( \square \)

Note that by [11] we have a one-to-one correspondence between orderings and equivalence classes \( [\mathcal{S}] \) of involution subgroups of \( \mathcal{G}_F \) for which \( |\mathcal{S} / \Phi(\mathcal{S})| = 2 \). The following corollary generalizes this result to preorderings.

**Corollary 3.2.** Let \( F \) be a formally real field. Then there is a bijective inclusion-reversing correspondence between preorderings of \( F \) and equivalence classes \( [\mathcal{S}] \) of involution subgroups of \( \mathcal{G}_F \).

**Proof.** In the proof of the theorem above, restrict the subgroups \( T \) of \( F \) to those which are preorderings, and the equivalence classes \( [H] \) to those which are represented by involution subgroups. \( \square \)

**Remark.** The correspondence of the preceding corollary gives a quantitative result when the sets are finite: namely \( |\mathcal{S} / \Phi(\mathcal{S})| = |F/T_{[\mathcal{S}]}| \). The first number is 2 raised to the power of the minimal number of generating involutions of \( \mathcal{S} \), while the second is 2 raised to the minimal number of orderings whose intersection gives \( T_{[\mathcal{S}]} \).

**Theorem 3.3.** Let \( F \) be a formally real field. The isomorphism type of an involution subgroup \( \mathcal{S} \) of \( \mathcal{G}_F \) determines \( W_{T_{[\mathcal{S}]}}, \) the reduced Witt ring of the preordering \( T_{[\mathcal{S}]} \).

**Proof.** Write \( T \) for the preordering \( T_{[\mathcal{S}]} \). Recall that for any element \( b \in F \), we have \( \sqrt{b} \) in the fixed field of \( \mathcal{S} \) if and only if \( b \in T \). Choose a minimal set of generators \( \{ \sigma_i \mid i \in I \} \) for \( \mathcal{S} \) and extend it to a minimal set of generators \( \{ \sigma_i, \tau_j \mid i \in I, j \in J \} \) for \( \mathcal{G}_F \). Now \( \mathcal{G}_F / \Phi(\mathcal{G}_F) \cong \text{Gal}(F^{(2)}/F) \) is dual to the square class group \( F/F^2 \), so we can choose
a set of generators \( \{a_i, b_j \mid i \in I, j \in J\} \) for \( F/F^2 \) such that \( \sigma_i \) fixes all \( \sqrt{a_i}, \sqrt{b_i} \) except \( \sigma_i(\sqrt{a_i}) = -\sqrt{a_i} \) and similarly \( \tau_j \) fixes all \( \sqrt{b_j}, \sqrt{a_j} \) except \( \tau_j(\sqrt{b_j}) = -\sqrt{b_j} \). Thus, \( b_j \in T \) for all \( j \). Now consider the (abstract) reduced Witt ring \( W_T \) and its associated quaternionic structure \((G_T, Q_T)\). We need to show that \( \mathcal{I} \) is the \( W \)-group affiliated with the quaternionic structure \((G_T, Q_T)\). Let \((G, Q)\) be the quaternionic structure for \( F \). Then \( G \cong F/F^2 \) and \( G \rightarrow G_T \) by sending \( b_j \mapsto 1 \) for all \( j \). Thus \( G_T \) has \( \{a_i \mid i \in I\} \) as a basis and \( \mathcal{J}/\Phi(\mathcal{J}) \) is dual to \( G_T \) just as \( \mathcal{G}_F/\Phi(\mathcal{G}_F) \) was dual to \( G \). The relations on \( \mathcal{G}_F \) are as described in Section 2. The relations on \( \mathcal{J} \) are precisely the subset of the relations on \( \mathcal{G}_F \) which can be expressed solely in terms of the generators \( \sigma_i \) of \( \mathcal{J} \), i.e., the relators \( \mathcal{J} = \mathcal{G}_F \) \( \mathcal{I} \) is a subring of \( \mathcal{J} \) dual to the kernel of the map to \( \mathcal{G}_F \[6, Section 3\]. By [1, Theorem 2.1] there then exists a pythagorean field \( K \) with Witt ring \( W(K) \cong \mathcal{W}_T(F) \), hence \( \mathcal{J} \cong \mathcal{G}_K \). \( \square \)

With finiteness conditions on \( X_T \) we can generally say more; this will be pursued further in the next section. Here we actually need a weaker condition than that the set \( X_T \) be finite, namely that \( T \) have finite chain length. The formal definition is given in the next section in (4.1).

**Corollary 3.4.** Let \( F \) be a formally real field. Any involution subgroup \( \mathcal{J} \) of the \( W \)-group \( \mathcal{G}_F \) can itself be realized as the \( W \)-group associated to some abstract Witt ring \( W \). If the preordering \( T \) associated to \( \mathcal{J} \) has finite chain length, then \( \mathcal{J} \) can be realized as the \( W \)-group of some field \( K \).

**Proof.** The reduced Witt ring of \( F \) with respect to \( T \) is an abstract Witt ring in the sense of Marshall [5, Ch. 4, Section 7, Ch. 6, Section 3], and \( \mathcal{J} \) will then be the abstract \( W \)-group associated to this Witt ring. If \( T \) has finite chain length, then there are only finitely many places from \( F \) to \( \mathbb{R} \) compatible with \( T \) [6, Section 3]. By [1, Theorem 2.1] there then exists a pythagorean field \( K \) with Witt ring \( W(K) \cong \mathcal{W}_T(F) \), hence \( \mathcal{J} \cong \mathcal{G}_K \). \( \square \)

This leads to the general question of whether every essential subgroup of \( \mathcal{G}_F \) is in fact realizable as the \( W \)-group of some abstract Witt ring or field. There is at least some evidence to this effect. For example, the proof of Proposition 2.3 shows that \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \) is not essential, and since no assumption was made on the order of \( \tau \) in that proof, it also shows that \( \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \) cannot be essential. Thus, the only abelian essential subgroups other than \( \mathbb{Z}/2\mathbb{Z} \) are of the form \( \prod \mathbb{Z}/4\mathbb{Z} \). On the other hand, it is known that these are precisely the abelian \( W \)-groups [12]. Additional results of this nature are given in [4]. All groups that are currently known not to be realizable as \( W \)-groups are also known not to be realizable as essential subgroups of \( W \)-groups.
It is natural to ask about the fixed fields of the groups corresponding to preorderings of the field $F$. As noted in the introduction, these may not be formally real, even when the preordering is a single ordering. The issue of when a single involution is real is carefully considered in [11]. In particular, every ordering is shown to have a corresponding real involution $\sigma$. Any other real involution inducing the same ordering is conjugate to $\sigma$, and all the involutions inducing the same ordering are the elements of $\sigma\Phi$ [11, Proposition 2.9].

**Proposition 3.5.** Let $T$ be a preordering of the field $F$. For each ordering $P \in X_T$, choose a single real involution $\sigma_P$ determining $P$. Let $\mathcal{I}$ be the subgroup generated by $\{\sigma_P \mid P \in X_T\}$ and let $K$ be the fixed field of $\mathcal{I}$. Then the orderings of $F$ which extend to $K$ are precisely those in $X_T$.

**Proof.** First assume that $P \notin X_T$. Since $P \notin T$, there exists an element $b \in T$ with $-b \in P$. Every element of $\mathcal{I}$ fixes $\sqrt{b}$, so it lies in $K$ and $P$ cannot extend. On the other hand, if $P \in X_T$, then $P$ extends to the fixed field of the generator $\sigma_P$ of $\mathcal{I}$, hence it must extend to the subfield $K$. 

4. Special preorderings and their groups

Let $T$ be a preordering of a formally real field $F$. Let $\mathcal{I}_T$ be an involution subgroup of $\mathcal{G}_T$ in the equivalence class corresponding to $T$ given by Corollary 3.2. By Corollary 2.2 $\mathcal{I}_T$ is determined up to isomorphism (only). We next look at the isomorphism types of involution subgroups which correspond to special types of preorderings.

**Proposition 4.1.** (1) A preordering $T$ is a fan if and only if $\mathcal{I}_T \cong \bigoplus_{\mu \in J_7} \mathbb{Z}/4\mathbb{Z}$ with nontrivial $\mathbb{Z}/2\mathbb{Z}$-action on each of the $\mathbb{Z}/4\mathbb{Z}$ factors. If $|F/T| = 2^n$, then the product has $n-1$ factors of $\mathbb{Z}/4\mathbb{Z}$. We shall refer to such a group as a fan group.

(2) A preordering $T$ is SAP if and only if $\mathcal{I}_T$ contains no subgroup isomorphic to $(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z}$, that is, no fan subgroup of order 32. If $|F/T| = 2^n$, $T$ is SAP if and only if $\mathcal{I}_T \cong \bigoplus_{\mu \in J_7} \mathbb{Z}/2\mathbb{Z}$ where $|J_T| = n$.

**Proof.** The preordering $T$ is a fan if and only if the Witt ring $W_T(F)$ is isomorphic to an integral group ring $\mathbb{Z}[A]$ [3, Theorems 5.9, 5.10]. Furthermore, $|F/T| = 2^n$ if and only if $|A| = 2^{n-1}$. Minac and Smith [10] show that the associated W-group must be $\bigoplus_{\mu \in J_7} \mathbb{Z}/4\mathbb{Z}$ with action as claimed.

The preordering $T$ is SAP if and only if $T$ is not contained in any fan of index 8 in $F$. Since the preorderings containing $T$ precisely correspond to the involution subgroups of $\mathcal{I}_T$, the first statement in (2) follows from (1). If $|F/T| = 2^n$, the preordering $T$ is SAP if and only if $W_T(F) \cong \bigoplus_{\mu \in J_7} \mathbb{Z}/n\mathbb{Z}$, with the product being in the category of abstract Witt rings. In this case, Minac and Smith [10] show that the associated W-group must be $\bigoplus_{\mu \in J_7} \mathbb{Z}/2\mathbb{Z}$. 

\[\square\]
In the case where \(|F/T| = 2^n\) is finite, the involution groups associated to fans and to SAP preorderings represent the extremes as far as orders of involution subgroups are concerned. That is, \(T\) is a fan if and only if \(|\mathcal{F}_T|\) is as small as possible for a preordering of index \(2^n\), and \(T\) is SAP if and only if \(|\mathcal{F}_T|\) is as large as possible for a preordering of index \(2^n\). Since necessarily \(|\mathcal{F}_T/\Phi(\mathcal{F}_T)| = 2^n\), this is equivalent to saying that \(\Phi(\mathcal{F}_T)\) is as small as possible for fan groups, and as large as possible for SAP groups. Specifically, for a fan group \(\mathcal{F}\) with \(|\mathcal{F}/\Phi(\mathcal{F})| = 2^n\), we have \(|\mathcal{F}| = 2^{2n-1}\), and consequently \(|\Phi(\mathcal{F})| = 2^{n-1}\), while for a SAP group we have \(|\mathcal{F}| = 2^{n(n+1)/2}\) and \(|\Phi(\mathcal{F})| = 2^{n(n-1)/2}\).

The fans and the SAP preorderings are also the extreme cases involved in determining the numbers associated with any preordering: chain length and (reduced) stability index. To discuss these, we again assume that the group \(\hat{F}/T\) is finite. This is, in fact, equivalent to both of the numbers, chain length and stability index, being finite [3, Theorem 13.9]. The clopen sets of the Harrison subbasis for the topology of \(X_T\) are of the form \(H_T(a) = \{P \in X_T | a \in P\}\). We recall from [3, Section 8] that the chain length of a preordering \(T\), denoted \(\text{cl}(T)\), is the maximum length \(n\) of a chain

\[
\emptyset = H_T(-1) \subseteq H_T(a_1) \subseteq H_T(a_2) \subseteq \cdots \subseteq H_T(a_n) = T.
\] (4.1)

Relating this to the group \(\mathcal{F}_T\), one has \(H_T(a_1) \subseteq H_T(a_2)\) if and only if for all \(P \in X_T\), \(a_1 \in P \Rightarrow a_2 \in P\), if and only if for all \(\sigma \in \mathcal{F}_T\), \(\sigma(\sqrt{a_1}) = \sqrt{a_1} \Rightarrow \sigma(\sqrt{a_2}) = \sqrt{a_2}\). For a SAP preordering with \(|X_T| = n\), the chain length is \(n\). In general, to read this number off of the group (as in Proposition 4.1(2)) requires that the group be written in a canonical form. It is complicated further by the fact that the chain length of a fan may be 1 or 2 (1 when \(|X_T| = 1\) and 2 otherwise) and the fan group when \(|X_T| = 2\) may be written either as \(\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}\) as in Proposition 4.1(1), or as \(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\) as in Proposition 4.1(2). The canonical form we will choose is based on a recursive construction of the associated Witt rings \(W_T(F)\).

The stability index is determined by the largest index in \(\hat{F}\) of a fan \(T' \supseteq T\) and is denoted \(\text{st}(T)\); it is \(n\) when \(|\hat{F}:T'| = 2^{n+1}\), or equivalently, when \(|X_T| = 2^n\) [3, Theorem 13.7]. In particular, a SAP field (or preordering) with more than one ordering has stability index 1.

Since we can associate a W-group to an abstract Witt ring, we can define an (abstract) involution group in this more general context. An involution group is the W-group associated to an abstract reduced Witt ring, as described in [15]. In this context we will not have a specific field in mind (though one always exists when \(X\) is finite), so we shall write \(\text{st}(X)\) and \(\text{cl}(X)\) for \(\text{st}(T)\) and \(\text{cl}(T)\), where \(X\) is the corresponding abstract space of orderings.

The Witt rings associated with involution groups are torsion-free (cf. [11, Theorem 2.11]). These (reduced) Witt rings, when finitely generated, can be constructed recursively via products and group ring extensions in the category of Witt rings [1, 5]. And, of course, the associated W-groups can also be constructed recursively; see [10] for details. For our purposes, we need only note that any finite involution group is built up recursively by a finite number of operations, beginning with \(\mathbb{Z}/2\mathbb{Z}\) and at
each step either forming the semidirect product $\mathbb{Z}/4\mathbb{Z} \rtimes \mathcal{I}$ (with the action given in [10, Section 3]) or forming the free product $\mathcal{I}_1 * \mathcal{I}_2$ in $\mathcal{I}$, where $\mathcal{I}, \mathcal{I}_1$ and $\mathcal{I}_2$ were previously constructed by the process. Translating the computation of chain length and stability index into $W$-groups then gives a means of immediately reading off the values from the structure of a given involution group.

Proposition 4.2. Let $\mathcal{I}, \mathcal{I}_1$ and $\mathcal{I}_2$ be finite involution groups with associated spaces of orderings $(X, G)$, $(X_1, G_1)$ and $(X_2, G_2)$. The chain length of the space of orderings associated with $\mathcal{I}_1 * \mathcal{I}_2$ is $\text{cl}(X_1) + \text{cl}(X_2)$. Its stability index is $\max(\text{st}(X_1), \text{st}(X_2))$ unless $\mathcal{I}_1 = \mathcal{I}_2 = \mathbb{Z}/2\mathbb{Z}$, in which case it is 1. The chain length of the space of orderings associated with $\mathbb{Z}/4\mathbb{Z} \rtimes \mathcal{I}$ is $\text{cl}(X)$ unless $\mathcal{I} = \mathbb{Z}/2\mathbb{Z}$ in which case it is 2. Its stability index is $\text{st}(X) + 1$.

Proof. The group $\mathcal{I}_1 * \mathcal{I}_2$ has associated set of orderings $X_1 \cup X_2$ with Harrison sub-basic sets of the form $H_{X_1}(a) \cup H_{X_2}(b)$, $a \in G_1$, $b \in G_2$, so the first chain length claim follows immediately from the defining expression (4.1). For the same reason, one sees that the stability index is $\max(\text{st}(X_1), \text{st}(X_2))$, with the single exception of the case where each space $X_i$ has only one ordering so that they have stability index zero while the space with two orderings has index one.

The space of orderings associated with the group $\mathbb{Z}/4\mathbb{Z} \rtimes \mathcal{I}$ is homeomorphic to $\{(P,k) \mid P \in X, k \in \{0, 1\}\}$ with Harrison subbasis generated (under the operation of symmetric difference) by the two copies of $X$ and the sets of the form $\{H_X(a) \times \{0\} \cup H_X(a) \times \{1\} \mid a \in G\}$. Thus, the set of orderings associated with a fan is doubled in size, whence the stability index increases by 1, and the chain length is unchanged except in the special case of going from one to two orderings. □

We would now like to examine properties of fan subgroups more closely. The following several results give group theoretic analogues to a number of the results in [3, Ch. 5].

Proposition 4.3. An involution subgroup $\mathcal{I}$ of $\mathcal{G}_F$ is a fan group if and only if, for every $\sigma \in \mathcal{I}$ such that $\sigma(\sqrt{-1}) = -\sqrt{-1}$, we have $\sigma^2 = 1$.

Proof. Suppose $\mathcal{I}$ is a fan group, and let $\sigma \in \mathcal{I}$ be such that $\sigma(\sqrt{-1}) = -\sqrt{-1}$. Then $T_{[\sigma]}$ is a subgroup of index 2 in $F$, which contains $T$ and which does not contain $\sqrt{-1}$. Since $T$ is a fan, we have $T_{[\sigma]}$ is an ordering, and $\sigma^2 = 1$.

Conversely, let $\mathcal{I} = \mathcal{I}_{[T]}$, and suppose that for all $\sigma \in \mathcal{I}$, if $\sigma(\sqrt{-1}) = -\sqrt{-1}$, then $\sigma^2 = 1$. Let $S \supseteq T$ be a subgroup of $F$ of index 2, with $-1 \notin S$. We need to see that $S = T_{[\sigma]}$ for some $\sigma \in \mathcal{I}$, for then $S$ will be an ordering, since such a $\sigma$ will not fix $\sqrt{-1}$. Let $\tau \in \mathcal{G}_F$ be such that the fixed field of $\langle \tau \rangle \Phi$ is $F(\sqrt{S})$. Then $\tau \Phi \subseteq \mathcal{I} \Phi$ because $T \subseteq S$, so there exists an $\sigma \in \mathcal{I}$ such that $\sigma \Phi = \tau \Phi$, and $T_{[\sigma]} = S$. □

Remark. By [10, Proposition 3.3], every $W$-group $\mathcal{G}_F$ of a formally real field $F$ has a fan group $(\prod_{i \in I} \mathbb{Z}/4\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$ as a homomorphic image, where $\{-1, a_i \mid i \in I\}$ forms a basis for $F/F^2$. The field is superpythagorean (that is, $F$ is pythagorean, so $F^2$ is a
preordering, and moreover $F^2$ is a fan) precisely when this “homomorphic image” is in fact the group itself.

**Corollary 4.4.** If $\mathcal{I}$ is a fan group, then any involution subgroup of $\mathcal{I}$ is also a fan group.

**Proof.** If $\sigma \in \mathcal{I}'$, where $\mathcal{I}'$ is an involution subgroup of $\mathcal{I}$, and if $\sigma(\sqrt{\tau}) = -\sqrt{\tau}$, then $\sigma^2 = 1$, since $\mathcal{I}$ is a fan group. Thus $\mathcal{I}'$ must also be a fan group. $\square$

**Proposition 4.5.** Any involution subgroup $G$ of $\mathbb{G}_F$ which can be generated by two elements is a fan group.

**Proof.** If $G$ can be generated by a single element, then $G \cong \mathbb{Z}/2\mathbb{Z}$, which is the “trivial” fan group. Let $G \in \mathbb{G}$ be generated by two involutions. Then $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. However, as shown in Proposition 2.3, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is not an essential subgroup of $\mathbb{G}_F$. Thus, any such subgroup of $\mathbb{G}_F$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, which is a fan group. $\square$

**Theorem 4.6.** For any involution subgroup $\mathcal{I}$ of $\mathbb{G}_F$, the following are equivalent.

1. $\mathcal{I}$ is a fan group.
2. Any subgroup $H$ of $\mathcal{I}$ such that $\sqrt{\tau}$ is not in the fixed field of $H$ is generated by involutions.
3. Every three-generator involution subgroup of $\mathcal{I}$ is a fan group.

**Proof.** First assume $\mathcal{I}$ is a fan subgroup of $\mathbb{G}_F$. Then we may choose generators $\{\sigma_i, i \in I; \tau\}$ for $\mathcal{I}$ where $\prod_{i \in I}/(\sigma_i) \cong \prod_{i \in I} \mathbb{Z}/4\mathbb{Z}$ and $\tau^2 = 1$, with $\tau \sigma_i \tau = \sigma_i^{-1}$ for all $i \in I$. Notice that every element in $\mathcal{I}$ can be “factored” in the form $\tau^e \prod_{i \in I} \sigma_i^{e_i}$, $e, e_i \in \{0, 1\}$ times some element of the commutator subgroup of $\mathcal{I}$. The involutions of $\mathcal{I}$ are precisely those elements which have $\tau$ in their “factorization”, and these are also, by Proposition 4.3, precisely the elements which do not fix $\sqrt{\tau}$. Any two elements of exponent four commute with each other. Now let $H$ be any subgroup of $\mathcal{I}$ such that $\sqrt{\tau}$ is not in the fixed field of $H$. Then among the generators of $H$ is at least one which contains $\tau$ in its factorization, again by Proposition 4.3. Call this generator $\tau'$. Then if $\rho$ is any generator of $H$ which is of exponent 4, we may replace it by $\rho \tau'$, which will be an involution. Thus, $H$ can be generated by involutions. This shows (1) implies (2). That (1) implies (3) follows directly from Corollary 4.4.

Now assume that (2) holds. Let $\sigma \in \mathcal{I}$ be such that $\sigma(\sqrt{\tau}) = -\sqrt{\tau}$. Then $\langle \sigma \rangle$ is generated by involutions, so $\sigma^2 = 1$, and by Proposition 4.3, $\mathcal{I}$ is a fan group. Thus (2) implies (1).

Finally, assume that every involution subgroup $H$ of the involution subgroup $\mathcal{I}$ of $\mathbb{G}_F$ generated by three elements is a fan group. Thus, if $\sigma \in H$ has the property that $\sigma(\sqrt{\tau}) = -\sqrt{\tau}$, then $\sigma^2 = 1$. Now suppose $\sigma \in \mathcal{I}$ is such that $\sigma(\sqrt{\tau}) = -\sqrt{\tau}$. If we can show that $\sigma^2 = 1$, then by Proposition 4.3, we will have that $\mathcal{I}$ is a fan group.
group. Since \( \sigma \) lies in an involution group, it can be written as a product of generating involutions \( \sigma = \tau_1 \tau_2 \cdots \tau_m \). Each of the generators carries \( \sqrt{-1} \) to \( -\sqrt{-1} \), so \( m \) must be odd. If \( m = 1 \), \( \sigma \) is an involution and we are done. If \( m = 3 \), then \( \sigma \) lies in the subgroup generated by the three involutions \( \tau_1, \tau_2, \tau_3 \) which is a fan group by hypothesis, so again \( \sigma^2 = 1 \). If \( m > 3 \), we use the same argument inductively: the element \( \sigma_0 = \tau_{m-2} \tau_{m-1} \tau_m \) lies in a three generator involution subgroup, hence is a fan group and thus \( \sigma_0 \) is an involution. Now \( \sigma = \tau_1 \tau_2 \cdots \tau_{m-3} \sigma_0 \) has shorter length and we are done by induction. Thus (3) implies (1). \( \square \)

5. \( |\Phi(\mathcal{J}_T)| \) as an invariant

In this section we take a look at \( |\Phi(\mathcal{J}_T)| \) as a useful numerical invariant for studying the (categorically equivalent) structure of finite spaces of orderings, finitely generated reduced Witt rings and finite involution groups. We have seen in the previous section that \( |\Phi(\mathcal{J}_T)| \) is minimal for fan groups and maximal for SAP groups. This suggests using \( \log_2 |\Phi(\mathcal{J}_T)| \) as a measure of the degree to which orderings can be separated by the elements of the Harrison subbasis. Let \( T \) be a given preordering of a formally real field \( F, X \) its corresponding set of orderings. The numbers commonly studied in describing the structure of the Witt ring \( W_T(F) \) are \( \|X\|, \|F/T\|, \text{cl}(X), \) and \( \text{st}(X) \). We shall see that \( |\Phi(\mathcal{J}_T)| \) is independent of these four numbers, thus providing additional information in distinguishing Witt rings.

We begin by mentioning two examples which indicate what \( |\Phi(\mathcal{J}_T)| \) can and cannot do. Our first example is the smallest value of \( \|F/T\| \) for which this number and \( |\Phi(\mathcal{J}_T)| \) do not completely determine the involution group \( \mathcal{J}_T \).

Example 5.1. Taking \( |\mathcal{J}/\Phi(\mathcal{J})| = \|F/T\| = 2^2 \), we consider the groups \( \mathcal{J}_1 = \mathbb{Z}/4\mathbb{Z} \succ (\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}) \) and \( \mathcal{J}_2 = \mathbb{Z}/4\mathbb{Z} \succ ((\mathbb{Z}/4\mathbb{Z} * \mathbb{Z}/4\mathbb{Z} * \mathbb{Z}/4\mathbb{Z}) \succ \mathbb{Z}/2\mathbb{Z}) \), corresponding to spaces of orderings \( X_i, i = 1, 2 \). For each of these groups, \( |\Phi(\mathcal{J}_i)| = 2^7 \), \( i = 1, 2 \). On the other hand, all three of the other invariants are different: \( |X_1| = 8, |X_2| = 9, \text{cl}(X_1) = 4, \text{st}(X_1) = 2 \) and \( \text{cl}(X_2) = 3 = \text{st}(X_2) \).

The next example shows that \( |\Phi(\mathcal{J})| \) is truly independent of the other four invariants, in that \( |\Phi(\mathcal{J}_i)| \) can distinguish two Witt rings for which all the other invariants are equal.

Example 5.2. Now we use the groups \( \mathcal{J}_1 = \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z} * (\mathbb{Z}/4\mathbb{Z} * \mathbb{Z}/4\mathbb{Z} * \mathbb{Z}/4\mathbb{Z}) \) and \( \mathcal{J}_2 = \mathbb{Z}/4\mathbb{Z} \succ ((\mathbb{Z}/4\mathbb{Z} \succ \mathbb{Z}/2\mathbb{Z}) \succ \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}) \). Here we have \( |\Phi(\mathcal{J}_1)| = 2^{16} \) and \( |\Phi(\mathcal{J}_2)| = 2^{15} \). But \( |X_i| = 14, |\mathcal{J}_i/\Phi(\mathcal{J}_i)| = 2^7, \text{cl}(X_i) = 5 \) and \( \text{st}(X_i) = 3 \), for \( i = 1, 2 \).

We next establish a few simple results regarding the computation of \( \Phi(\mathcal{J}) \). Using the recursive construction of finite involution groups described in the previous section and
the fact that \( \Phi(\mathbb{Z}/2\mathbb{Z}) = \{0\} \), the following proposition suffices for all computations. Note that it extends the SAP and fan examples following Proposition 4.1.

**Proposition 5.3.** Let \( \mathcal{F}_1 \) and \( \mathcal{F}_2 \) be involution groups with \( |\mathcal{F}_1/\Phi(\mathcal{F}_1)| = 2^m \), \( |\mathcal{F}_1| = 2^n \) and \( |\Phi(\mathcal{F}_2)| = 2^r \). Then

\[
|\mathcal{F}_1 \ast \mathcal{F}_2| / \Phi(\mathcal{F}_1 \ast \mathcal{F}_2) = 2^{m+n}, \quad |\Phi(\mathcal{F}_1 \ast \mathcal{F}_2)| = 2^{r+s+mn}
\]

and

\[
|\mathcal{Z}/4\mathcal{Z} \ast \mathcal{F}_1| / \Phi(\mathcal{Z}/4\mathcal{Z} \ast \mathcal{F}_1) = 2^{m+1}, \quad |\Phi(\mathcal{Z}/4\mathcal{Z} \ast \mathcal{F}_1)| = 2^{r+1}
\]

**Proof.** By [10, Section 2], for any finite groups \( G_1, G_2 \) in \( \mathcal{Cat} \),

\[
|G_1 \ast G_2| = |G_1||G_2|2^{\log_2 |G_1/\Phi(G_1)| \log_2 |G_2/\Phi(G_2)|},
\]

and \( (G_1 \ast G_2)/\Phi(G_1 \ast G_2) \cong G_1/\Phi(G_1) \times G_2/\Phi(G_2) \). Here \( |\mathcal{F}_1 \ast \mathcal{F}_2| = 2^{r+m+n+s+mn} \) and

\[
|(\mathcal{F}_1 \ast \mathcal{F}_2)/\Phi(\mathcal{F}_1 \ast \mathcal{F}_2)| = |\mathcal{F}_1/\Phi(\mathcal{F}_1)| \cdot |\mathcal{F}_2/\Phi(\mathcal{F}_2)| = 2^{m+n},
\]

so \( |\Phi(\mathcal{F}_1 \ast \mathcal{F}_2)| = 2^{r+s+mn} \).

By the way semidirect products work we know \( |\mathcal{Z}/4\mathcal{Z} \ast \mathcal{F}_1| = 4 \cdot |\mathcal{F}_1| = 2^{m+r+2} \), and since for \( G \in \mathcal{Cat} \), \( \log_2 |G/\Phi(G)| \) is the minimum number of generators for \( G \), clearly \( |(\mathcal{Z}/4\mathcal{Z} \ast \mathcal{F}_1)/\Phi(\mathcal{Z}/4\mathcal{Z} \ast \mathcal{F}_1)| = 2^{m+1} \) and thus also \( |\Phi(\mathcal{Z}/4\mathcal{Z} \ast \mathcal{F}_1)| = 2^{r+1} \).

The situation of Example 5.2 cannot happen for lower stability index. Indeed, when the stability index is at most 2, the value of \( |\Phi(\mathcal{F})| \) is completely determined by the number of orderings and the size of the Harrison subbasis, though the chain length may vary for such spaces of orderings.

**Theorem 5.4.** Assume that \( \mathcal{F} \) is an finite involution group with space of orderings \( X \) having stability index at most 2. Set \( 2^q = |\mathcal{F}| / \Phi(\mathcal{F})| \). Then

\[
\log_2 |\Phi(\mathcal{F})| = \frac{q^2 + q - 2|X|}{2} = \left(\frac{q + 1}{2}\right)^2 - |X|.
\]

**Proof.** Following the methods pioneered in [1], we prove the theorem using the recursive construction of \( \mathcal{F} \). Since the stability index is at most 2, Proposition 4.2 shows there are only three cases to consider: (1) a SAP group \( \mathcal{F} \), (2) a semidirect product \( \mathcal{Z}/4\mathcal{Z} \ast \mathcal{F} \) where \( \mathcal{F} \) is a SAP group, and (3) free products of groups of the first two types. For a SAP group, \( |X| = q \), so our earlier computation of \( |\Phi(\mathcal{F})| \) shows that Eq. (5.1) holds in this case. For case (2), we may assume (5.1) for \( \mathcal{F} \). The space of orderings for \( \mathcal{Z}/4\mathcal{Z} \ast \mathcal{F} \) has cardinality \( 2|X| = 2q \) and \( |\mathcal{Z}/4\mathcal{Z} \ast \mathcal{F}/\Phi(\mathcal{Z}/4\mathcal{Z} \ast \mathcal{F})| = 2^{r+1} \), so Proposition 5.3 yields

\[
\log_2 |\Phi(\mathcal{Z}/4\mathcal{Z} \ast \mathcal{F})| = \frac{q^2 + q - 2|X|}{2} + 1 = \frac{(q + 1)^2 + (q + 1) - 2(2|X|)}{2}
\]
as desired. Finally, for case (3) we may assume that (5.1) holds for two groups \( \mathcal{I}_1 \) and \( \mathcal{I}_2 \) with spaces of orderings \( X_i \) and quotients \( |\mathcal{I}_i/\Phi(\mathcal{I}_i)| = 2^{q_i} \), \( i=1,2 \). Applying Proposition 5.3 again, we obtain

\[
\log_2 |\Phi(\mathcal{I}_1 \ast \mathcal{I}_2)| = \frac{q_1^2 + q_1 - 2|X_1|}{2} + \frac{q_2^2 + q_2 - 2|X_2|}{2} + q_1q_2
\]

\[
= \frac{(q_1 + q_2)^2 + (q_1 + q_2) - 2(|X_1| + |X_2|)}{2}.
\]

This completes the proof since the space of orderings for the free product is the union of the two spaces of orderings \( X_1 \cup X_2 \) and the group of square classes (corresponding to \( \mathcal{I}_1 \ast \mathcal{I}_2/\Phi(\mathcal{I}_1 \ast \mathcal{I}_2) \)) is, in a natural way, the product of the two groups, and so has cardinality \( 2^{m+q} \) (cf. [1] or [5]). \( \square \)

Let \( F \) be a pythagorean field with finite space of orderings \( X \). Let \( P(t) = \sum h_q t^q \) be the polynomial where \( h_q \) is the dimension of the cohomology group \( H^q(Gal(F(2)/F), \mathbb{Z}/2\mathbb{Z}) \) over \( \mathbb{Z}/2\mathbb{Z} \). These polynomials have been studied by Mináč in [7], where they are called Poincaré polynomials. Some of the major invariants can be immediately read from this polynomial, as \( \deg P(t) = \text{st}(X) \), \( |X| = P(1) = \sum h_q \) and \( \log_2 |\hat{F}/\hat{F}^2| = 1 + P'(0) \) [7, Theorem 5.2.1]. In particular, we note that \( h_1 = \log_2 |\hat{F}/\hat{F}^2| - 1 \).

**Theorem 5.5.** For any finite space of orderings \( X \) with associated polynomial \( P \) and involution group \( \mathcal{F} \) we have

\[
\log_2 |\Phi(\mathcal{F})| = \left(\frac{m}{2}\right) - h_2,
\]

where \( m = \log_2 |\Phi(\mathcal{F})| \) (i.e., \( m = \log_2 |\hat{F}/\hat{F}^2| \) where \( F \) is a pythagorean field with \( \mathcal{F}_F = \mathcal{F} \)).

**Proof.** We prove the theorem using the recursive construction of the spaces of orderings (or equivalently, of reduced Witt rings or involution groups). If \( |X| = 1 \), then \( \mathcal{F} \cong \mathbb{Z}/2\mathbb{Z} \), \( m = 1 \), \( |\Phi(\mathcal{F})| = 1 \) and \( P(t) = 1 \) so the claim holds: \( 0 = 0 + 0 \). From [7, p. 173], we need the following two facts:

1. For a direct sum of spaces of orderings (corresponding to the free product of involution groups), \( P_{X_1 \oplus X_2}(t) = P_{X_1}(t) + P_{X_2}(t) + t - 1 \).

2. For a group extension \( X' \) of a space of orderings \( X \) (corresponding to the semi-direct product with \( \mathbb{Z}/4\mathbb{Z} \)), \( P_{X'} = (t + 1)P_{X}(t) \).

For the case of \( X_1 \oplus X_2 \), we assume inductively that we have two spaces \( X_1, X_2 \) satisfying Eq. (5.2): \( \log_2 |\Phi(\mathcal{I}_i)| = \left(\frac{m_i}{2}\right) - a_i \), \( i=1,2 \), where \( a_i \) is the coefficient of \( t^2 \) in \( P_i(t) \). From Proposition 5.3 and the induction hypothesis, we have

\[
\log_2 |\Phi(\mathcal{I}_1 \ast \mathcal{I}_2)| = \log_2 |\Phi(\mathcal{I}_1)| + \log_2 |\Phi(\mathcal{I}_2)| + m_1m_2
\]

\[
= \left(\frac{m_1}{2}\right) - a_1 + \left(\frac{m_2}{2}\right) - a_2 + m_1m_2
\]

\[
= \left(\frac{m_1 + m_2}{2}\right) - (a_1 + a_2)
\]
as desired, since $a_1 + a_2$ is the coefficient of $t^2$ in the Poincaré polynomial $P_{X_1 \oplus X_2}(t)$. Next we consider the group extension case $\mathbb{Z}/4\mathbb{Z} \times \mathcal{J}$ where we assume (5.2) holds for $\mathcal{J}$: $\log_2 (|\Phi(\mathcal{J})|) = \binom{n}{2} - a$, where $a$ denotes the coefficient of $t^2$ in $P(t)$. Again using Proposition 5.3 and the induction hypothesis, we obtain

$$\log_2 |\Phi(\mathbb{Z}/4\mathbb{Z} \times \mathcal{J})| = \log_2 |\Phi(\mathcal{J})| + 1 = \binom{m}{2} - a + 1 = \binom{m+1}{2} - (a + m - 1)$$

as desired, because the coefficient of $t^2$ in $(1 + t)P(t)$ is $a + m - 1$, since the coefficient of $t$ in $P(t)$ is $m - 1$ as noted above. \(\square\)

Note that Theorem 5.4 is a special case of Theorem 5.5 since $|X| = q$ if the space is 1-stable and $|X| = P(1) = 1 + (q - 1) + h_2$ for stability 2 [7, Theorem 5.2.1]. A proof of Theorem 5.5 can also be given in the general context of abstract W-groups, using the relations on $G_F$, as in [15].

Looking at examples, one discovers that $P(t)$ is determined by $h_1$, $|X|$ and $|\Phi|$ for all small spaces of orderings. In fact, the smallest example where this does not happen requires $|X| = 34$, in which case we have polynomials $P_1(t) = 1 + 10t + 14t^2 + 7t^3 + 2t^4 = (1 + t)1 + 9t + 5t^2 + 2t^3$ and $P_2(t) = 1 + 10t + 14t^2 + 8t^3 + t^4$ for which $\log_2 |\Phi| = 41$. Finding such examples is accomplished by using the Mináč characterization of Poincaré polynomials [7, Theorem 5.2.3].

6. Topology

The space of orderings of a field and the W-group of a field each have a natural topology. For Galois groups, this is an inverse limit topology of finite groups. For the space of orderings $X_T$ over a preordering $T$, the topology makes it a Boolean space (compact, Hausdorff, and totally disconnected); in particular, the topology is also the inverse limit topology of finite (discrete) quotient spaces. For this reason, one naturally asks whether there is a relationship between the topologies since orderings correspond to involutions in an involution subgroup.

Let $T$ be a preordering of a field $F$ and let $\mathcal{J}$ be an involution subgroup corresponding to $T$ by Theorem 3.2. For each ordering $P$ in $X_T = \{ P \in X_F \mid P \supset T \}$, choose a corresponding involution $\sigma_P \in \mathcal{J}$. Of course, the involution $\sigma_P$ is only determined up to being an element of the coset $\sigma_P \Phi(\mathcal{J})$, but it has the property that, for $a \in \hat{F}$, $a \in P \Leftrightarrow \sigma_P(\sqrt{a}) = \sqrt{a}$. As noted earlier, the clopen sets of the Harrison subbasis for the topology of $X_T$ are of the form $H(a) = \{ P \in X_T \mid a \in P \}$. If we embed $X_T$ in $\mathcal{J}$ via $P \mapsto \sigma_P$, the subbasic set $H(a)$ gets mapped to $\{ \sigma_P \mid a \in P \}$, which is the intersection of the image of $X_T$ with the set $\{ \sigma \in \mathcal{J} \mid \sigma(\sqrt{a}) = \sqrt{a} \}$. The latter set is one of the defining basic open sets of the inverse limit topology on $\mathcal{J}$, so the image of $H(a)$ is open in the induced topology.
Lemma 6.1. Let $X$ and $Y$ be compact Hausdorff topological spaces. Assume there is an injection $f : X \to Y$ which is an open mapping and assume also that the image of $X$ is closed in $Y$. Then $f$ gives a homeomorphism of $X$ onto its image in $Y$.

Proof. We only need to show that $f$ is continuous. Let $U \subset Y$ be open. Its complement $U^c$, being a closed subset of a Hausdorff space, is compact. We claim that $f^{-1}(U^c)$ is also compact. To see this, let $\{V_i\}$ be any open cover of $f^{-1}(U^c)$. Since $f$ is an open mapping, each set $f(V_i)$ is open, hence the collection $\{f(V_i)\}$ is an open cover of $U^c \cap f(X)$. This latter set is closed in the compact space $Y$, and hence is itself compact, so there is a finite subcover $\{f(V_i)\}$. Then the sets $V_i$ cover $f^{-1}(U^c)$, and it is seen to be compact, hence closed in the Hausdorff space $X$. Therefore $f^{-1}(U)$ is open and the mapping is continuous.

Proposition 6.2. The injection of $X_T$ into $\mathcal{J}$ defined by $P \mapsto \sigma_P$ as above is a homeomorphism onto its image. That is, the induced topology on the image is identical to the Harrison topology.

Proof. We must compare the topology on the image of $X_T$ induced by the topology of $\mathcal{J}$ as a profinite 2-group, with the Harrison topology on the space of orderings. To work with an arbitrary preordering $T$ rather than $X_T$, it is convenient to consider the spaces and groups abstractly. Write $G = \mathbb{F}/T$ for the group associated with $X_T$ as an abstract space of orderings. We begin by considering the composition $X_T \to \mathcal{J} \to \mathcal{J}/\Phi(\mathcal{J})$. We have a natural isomorphism $\mathcal{J}/\Phi(\mathcal{J}) \cong \text{Hom}(G, \{\pm 1\})$. Now $\text{Hom}(G, \{\pm 1\})$ sits inside $\{\pm 1\}^G$ and has its topology induced by this inclusion, where the latter set has the product topology. The induced topology on the image of $X_T$ under this composition is thus the same as the usual one used to induce the Harrison subbasis topology [13, Section 6]. It follows that the composition $X_T \to \mathcal{J} \to \mathcal{J}/\Phi(\mathcal{J})$ is a continuous injection. The continuous image of the compact set $X_T$ is closed in (the Hausdorff space) $\mathcal{J}/\Phi(\mathcal{J})$. Since $\mathcal{J}/\Phi(\mathcal{J})$ has the quotient topology from $\mathcal{J}$, we see that the image of $X_T$ in $\mathcal{J}$ is also closed. As noted prior to Lemma 6.1, the mapping $X_T \to \mathcal{J}$ is open, so the result now follows from Lemma 6.1.

References