May 2014

Classification of W-groups of Pythagorean formally real fields

Fatemeh Bagherzadeh Golmakani
The University of Western Ontario

Supervisor
Jan Minac
The University of Western Ontario

Graduate Program in Mathematics

A thesis submitted in partial fulfillment of the requirements for the degree in Doctor of Philosophy

Classification of W-groups of Pythagorean Formally Real fields

(Thesis format: Monograph)

by

Fatemeh Bagherzadeh Golmakani

Department of Mathematics

A thesis submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy

The School of Graduate and Postdoctoral Studies
Western University
London, Ontario, Canada

Abstract

In this work we consider the Galois point of view in determining the structure of a space of orderings of fields via considering small Galois quotients of absolute Galois groups G_F of Pythagorean formally real fields. Galois theoretic, group theoretic and combinatorial arguments are used to reduce the structure of W-groups. When X_F, the space of orderings of the Pythagorean formally real field F, is a connected space, then the structure of $\mathcal{G}_F$ is reduced to the structure of $\mathcal{G}_{\bar{F}}$, the W-group of the residue field of F. In the disconnected case the structure of $\mathcal{G}_F$ is the free product of groups $\mathcal{G}_{F_i}$ where the $\mathcal{G}_{F_i}$ are W-groups corresponding to the connected components X_i of X_F. Then we show that a simple invariant (n, a) of the space of orderings of the field F, where $|\dot{F}/\dot{F}^2| = 2^n$ and $|X_F| = a$ can completely determine the structure of X_F and $\mathcal{G}_F$ in some cases.

Keywords: W-groups of Pythagorean formally real fields, formally real fields, the space of orderings of field F,

To my parents

Assadollah and Ashraf

and my sister

Parisa.

Acknowledgements

I would like to thank my research advisor Professor Ján Mináč for teaching me about math research and for his encouragement throughout my PhD years at Western. I could not do this work without his guidance.

It is my pleasure to also thank Dr. Andrew Schultz, Dr. Robert Mercer, Dr. Nicole Lemire and Dr. Graham Denham for carefully reading my thesis and offering detailed comments and suggestions on every chapter.

I also want to gratefully acknowledge Dr. Rasul Shafikov, my research co-supervisor Dr. Matthias Franz, and my friends Leslie Hallock and Michael Rogelstad for reading my thesis line by line and helping me revise it.

Also, I would like to thank the Chair of Mathematics Department at Western University Dr. André Boivin, and the Associate Chair (Graduate Program) Dr. Rasul Shafikov, for all their support during my PhD program.

I also want to acknowledge all of my teachers in Iran. This thesis is a result of their effort to teach me mathematics during my undergrad years at University of Shahid Bahonar of Kerman.

Finally, it is my pleasure to thank my parents. I am deeply indebted to them for everything I have now. I dedicate this thesis to them.

Fatemeh Bagherzadeh Golmakani. London, Ontario, February 2014.

Contents

Introduction

It was in 1900 that David Hilbert formed a list of twenty-three problems in mathematics at the Paris conference of the International Congress of Mathematicians. Then in 1927 the theory of formally real fields led Artin to solve Hilbert's seventeenth problem. Hilbert's seventeenth problem concerns the expression of definite rational functions as sums of quotients of squares.

The theory of formally real fields originally comes from a basic algebraic property of a field of real numbers which is that the only relations of the form $\sum \alpha_i^2 = 0$ are the trivial ones $0^2 + 0^2 + ... + 0^2 = 0$. Artin and Schreier called any field having this property $formally\ real$. In 1927 Emil Artin and Otto Schreier developed the theory of orderings on fields. Emil Artin and Otto Schreier characterized formally real fields as fields admitting orderings. Actually Artin proved a theorem which was used as one of the main tools in his solution of Hilbert's 17th problem.

The problem of determining absolute Galois groups, and even their canonical non-trivial quotients, is an extremely difficult problem. On the other hand, our determination of the structure of W-groups of formally real Pythagorean fields with finitely many orderings represents a significant advance in Galois theory. In this work we make progress in determining certain canonical finite 2-quotients of absolute

Galois groups of Pythagorean formally real fields.

We use mainly Galois theoretic, group theoretic and combinatorial arguments. We will show that in some cases a simple invariant of the order space of Pythagorean field F determines this order space and consequently the W-group completely.

Throughout this thesis, F is a field with char$F = 0$. We use the notation $|S|$ to denote the cardinality number of a set S, and we denote the group of nonzero elements of the field F by $\dot{F}$. $\sum F^2$ is the set of all finite sums of squares of elements of F, and $\dot{F}/\dot{F}^2$ is the square class group which is an $\mathbb{F}_2$-vector space. Here $\mathbb{F}_2$ means a field with two elements. One can show that $\sum \dot{F}^2$ is a subgroup of $\dot{F}$.
A Pythagorean field is a field in which every sum of two squares is a square.The two obvious examples of Pythagorean fields are $\mathbb{R}$ and $\mathbb{C}$. Actually there are many other non trivial examples.

By an *ordering* on a field F we mean a subset $P \subsetneq F$ such that $P + P \subseteq P$, $P.P \subseteq P$ and $P \cup (-P) = F$. It is easy to check that $\dot{P} = P - \{0\}$ is a subgroup of $\dot{F}$, P contains $\sum \dot{F}^2$ and $-1 \notin P$. A *preordering* in a field F is a proper subset $T \subsetneq F$ such that $\dot{F}^2 \subseteq T$, $T + T \subseteq T$ and $T.T \subseteq T$. One can show that F is $formally\ real$ if it has at least one ordering.

Example 1.

Consider field $F = \mathbb{R}((x))$ of all formal Laurent series over $\mathbb{R}$. A formal Laurent series is power series in one variable like

$$f = \sum_{k=n}^{\infty} a_k x^k, n \in Z.$$

So the square class group is $\dot{F}/\dot{F}^2 = \{[1], [-1], [x], [-x]\}$. Actually this field has two

orderings P_1 and P_2. Here P_1 is an ordering such that x is an element of P_1 and it contains all formal Laurent series $f = \sum_n^\infty a_n x^n, n \in Z$ such that if $a_n \neq 0$ then $a_n > 0$. The other ordering P_2 does not contain x. It contains all formal Laurent series $f = \sum_n^\infty a_n x^n, n \in Z$ such that, if $a_n \neq 0$, then $a_n(-1)^n > 0$. We explain this example with more details in Chapter 2.

Now for a Pythagorean formally real field F, define $F^{(2)} = F(\sqrt{a} : a \in \dot{F})$ as the compositum of all quadratic extensions of F. Thus $F^{(2)}$ is the smallest field that contains all square roots $\sqrt{a}$, for all $a \in \dot{F}$. Then define $F^{(3)} = F^{(2)}(\sqrt{y} : y \in F^{(2)}$ such that $F^{(2)}(\sqrt{y})/F$ is Galois). Thus $F^{(3)}$ is a compositum of all quadratic extensions K of $F^{(2)}$ such that K/F is Galois.

Definition 1. *For any Pythagorean formally real field F such that the number of elements of the group $\dot{F}/\dot{F}^2$ is finite, the W-group of field F is $\mathcal{G}_F = Gal(F^{(3)}/F)$.*

We show that all W-groups are objects of category $\mathcal{C}$, where $\mathcal{C}$ 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) For all $g \in G$, $g^2 \in Z(G)$ the center of G.

Suppose F is a Pythagorean formally real field. Our goal is to determine the structure of the W-group of F. First recall that the Frattini subgroup $\Phi(G)$ of a group G is the intersection of all maximal subgroups of G. Let p be a prime number. A group G is called a finite p-group if the number of elements of G is a power of p. One can show that if G is a finite p-group, then $\Phi(G) = G^p[G, G]$.

This is the map of the technique we used in this work.

Step 1. We use Corollary 2.10, [MS] to relate the ordering space X_F to the set of non simple involutions $\{\sigma \in \mathcal{G}_F | \, \sigma^2 = 1, \, \sigma \notin \Phi(F)\}$. Then we prove the basic Lemma 3.5 about the space of orderings of a Pythagorean formally real field F, which corresponds to the main lemma that M. Marshall proved about general space of orderings, Lemma 1.3, [M1]. But our proof is completely based on Galois theory.

Step 2. In this step connected concept for the space of orderings help us to classify $\mathcal{G}_F$. By using Lemma 3.5 we show that in the case that the space of orderings X_F of a Pythagorean formally real field F is connected, the translation group of $\mathcal{G}_F$ is nontrivial. This is the key point that M. Marshall used for classifying the usual space of orderings. We prove it here by a Galois theoretical argument.

Step 3. We show that if X_F, the space of orderings of a Pythagorean formally real field F, is a connected space, then the structure of $\mathcal{G}_F$ is reduced to the structure of $\mathcal{G}_{\bar{F}}$, the W-group of the residue field of F (Theorem 3.16). In the disconnected case we can reduce the structure of $\mathcal{G}_F$ to the free product of $\mathcal{G}_{F_i}$ such that $\mathcal{G}_{F_i}$ are W-groups corresponding to the connected components X_i of X_F (Theorem 3.18). Then we show that in interesting cases a simple invariant (n, a), where $\dot{F}/\dot{F}^2 = 2^n$ and $|X_F| = a$, can completely determine the structure of X_F and $\mathcal{G}_F$ (Theorems 3.22, 3.27, 3.30). A sufficient condition for uniqueness of the structure of $\mathcal{G}_F$ based on the binary representation of a giving by Theorem 3.35. In the end the relation between W-groups and Coxeter groups will be discussed.

Thesis Organization

Chapter 1: This chapter contains the basic definitions and concepts of W-groups. We recall some theorems and lemmas about the structure of W-groups which help us in their description. Most theorems in Chapter 1 come from the joint works of Ján Mináč and Michel Spira [MS1] or Ján Mináč and Tara Smith [MS].

The main theorem that we will use is a theorem which makes a correspondence between the set of orderings of F and the set of non-simple involutions of $Gal(F^{(3)}/F)$. With this correspondence we are able to use the theorems that M. Marshall proved about spaces of orderings [M1].

Chapter 2: In this chapter we recall the main concepts of space of orderings and its related theorems from [M1]. Two examples of a field F: one with infinite number of ordering and one with finite number of ordering is discussed.

Chapter 3: This is the most important chapter. In Section 3.1 we prove the main lemma for the space of orderings X_F of a Pythagorean formally real field F. Then we use this lemma to show that the translation group is nontrivial in the case X_F is a connected space. Then the structure of the W-group $\mathcal{G}_F$ is determined.

In Section 3.2 we will prove some theorems that in some cases a simple invariant (n, a) of the space of orderings determines the structure of $\mathcal{G}_F$. As an example we compute $\mathcal{G}_F$ of field F, where $\dot{F}/\dot{F}^2 = 2^4$.

Finally in Section 3.3 the relation between W-groups and Coxeter groups is discussed and we find a condition determining W-groups are Coxeter groups.

Chapter 1

W-groups

The characterization of Witt rings in the category of all rings is a very difficult problem. Until now we have information just about finitely generated Witt rings. But for each field F of characteristic not 2 there exists a certain Galois group which carries the same information as the Witt ring $W(F)$ of F. We denote this group by $\mathcal{G}_F$ and call it the W-group of F. We hope that determining the structure of the W-groups helps us to do more than just characterize Witt rings.

A Pythagorean field is a field in which every sum of two squares is a square. The two obvious examples of Pythagorean fields are $\mathbb{R}$ and $\mathbb{C}$. The field of rational numbers is not a Pythagorean field. Actually, there are many other non trivial examples of Pythagorean fields. Indeed any quadratically closed field is Pythagorean, but the converse is not true. The field of real numbers $\mathbb{R}$, is Pythagorean but its quadratic closure is $\mathbb{C}$.

In this work we are interested in the W-groups of Pythagorean fields for which $-1 \notin \sum F^2$. ($\sum F^2$ is the set of all finite sums of squares of elements of F). E.

Artin and O. Schreier called any field with the property $-1 \notin \sum F^2$ a formally real field. They characterized formally real fields as fields admitting orderings (Theorem 1.5, [La2]).

Definition 1.1. *By an ordering on a field F we mean a subset $P \subsetneqq F$ such that $P + P \subseteq P$, $P.P \subseteq P$ and $P \cup (-P) = \dot{F}$.*

It is easy to check that $\dot{P} = P - \{0\}$ is a multiplicative subgroup of $\dot{F}$, P contains $\sum \dot{F}^2$ and $-1 \notin P$.

Definition 1.2. *A quadratic form over field F is a homogeneous quadratic polynomial with coefficients in a F. In the case of two variable, it is called a binary form and has the following form: $q(x, y) = ax^2 + bxy + cy^2$ where $a, b, c \in F$.*

Every quadratic form q in n variables over a field of characteristic not equal to 2 is equivalent to a diagonal form $q(x) = a_1x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2$, (Corollary 2.4, [La3]). Such a diagonal form is often denoted by $\langle a_1, \ldots, a_n \rangle$.

We say that the form $f = \langle d_1, ..., d_n \rangle$ represent $e \in \dot{F}$ if and only if there exist $x_1, ...x_n \in F$ such that $e = a_1x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2$. Let D_f denotes the set of all elements of F that can be represented by the form f. Two forms $q = \langle a_1, ..., a_n \rangle$ and $q' = \langle b_1, ..., b_m \rangle$ are equivalent if and only if $d(q) = d(q')$ and q, q' represent a common element $e \in \dot{F}$. For two forms $f = \langle a_1, ..., a_n \rangle$ and $g = \langle b_1, ..., b_m \rangle$, define their sum and product by

$$f \oplus g = \langle a_1, ..., a_n, b_1, ..., b_m \rangle$$

$$f \otimes g = \langle a_1b_1, ..., a_1b_m, ..., a_nb_1, ..., a_nb_m \rangle.$$

Classification of all quadratic forms up to equivalence can be reduced to the case of diagonal forms.

Definition 1.3. *The Witt ring $W(F)$ is the set of equivalence classes of non-degenerate quadratic forms, with the group operation corresponding to the orthogonal direct sum of forms and the tensor product of two forms as the ring product. With these operations, $W(F)$ has a commutative ring structure.*

J. Mináč and T. Smith show in [MS] that the direct product of Witt rings corresponds to the free product of W-groups in the proper category. They also show the group ring construction of Witt rings corresponds to the semidirect product of W-groups. The W-group and their structure is defined as follows:

For a Pythagorean formally real field F, define $F^{(2)} = F(\sqrt{a} : a \in \dot{F})$ to be the compositum of all quadratic extensions of F. Thus $F^{(2)}$ is the smallest field that contains all square roots $\sqrt{a}$, for all $a \in \dot{F}$. Then define $F^{(3)} = F^{(2)}(\sqrt{y} : y \in F^{(2)}$ such that $F^{(2)}(\sqrt{y})/F$ is Galois). Thus $F^{(3)}$ is the compositum of all quadratic extensions K of $F^{(2)}$ such that K/F is Galois.

Definition 1.4. *Let F be a Pythagorean formally real field F such that the number of elements of the group $\dot{F}/\dot{F}^2$ is finite. Then the W-group of F is $\mathcal{G}_F = Gal(F^{(3)}/F)$.*

Two elements $a, b \in \dot{F}$ are called independent modulo squares if and only if $a\dot{F}^2 \neq b\dot{F}^2$ in the square class group $\dot{F}/\dot{F}^2$.

For a Pythagorean formally real field F such that $|\dot{F}/\dot{F}^2| = 2^n$, consider the W-group $\mathcal{G}_F = Gal(F^{(3)}/F)$, and let X_F be the set of all orderings of F. We want to classify the W-groups $\mathcal{G}_F = Gal(F^{(3)}/F)$ of the Pythagorean formally real fields F. Two extreme cases for F have been studied in the literature:

1. The SAP case, in which $|\dot{F}/\dot{F}^2| = 2^n$ and $|X_F| = n$. The "SAP" case refers to a preordering of field F satisfying the "Strong approximation property" (see

page 126 [La2]).

2. The fan case which is defined as follows.

Definition 1.5. *A preordering in a field F is a proper subset $T \subsetneqq F$ such that $\dot{F}^2 \subseteq T$, $T + T \subseteq T$ and $T.T \subseteq T$.*

For Pythagorean formally real fields it is easy to check that $\sum F^2 = F^2$, and $\dot{F}^2$ is a subgroup of $\dot{F}$. One can show that F^2 is a preordering of F.

Definition 1.6. *A preordering $T \subseteq F$ is called a fan if for any set $S \supseteq T$ the following holds. If $-1 \notin S$ and $\dot{S} = S\backslash\{0\}$ is a subgroup of index 2 in $\dot{F}$ then S is an ordering.*

We know F^2 is a preordering of F. If $|\dot{F}/\dot{F}^2| = 2^n$, then there are exactly 2^{n-1} sets $S \supseteq F^2$ such that $-1 \notin S$ and $\dot{S} = S\backslash\{0\}$ is a subgroup of index 2 in $\dot{F}$. For F^2 to be a fan (we say F is a fan),in this case each such S must be an ordering. Therefore we can conclude the fan case is the case that the number of orderings of our field is maximal. So in the fan case, if $|\dot{F}/\dot{F}^2| = 2^n$, then $|X_F| = 2^{n-1}$ (Chapter 5, [La2]).

We recall a very useful theorem about the structure of $F^{(3)}$ that J. Mináč and T. Smith proved in [MS].

Theorem 1.7. *$F^{(3)}$ is the composition of all extensions K of F such that $Gal(K/F)$ is one of the $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ and D_4.*

Here D_4 denotes the usual dihedral group of order 8. This is a very important theorem as it says that for checking a relation among generators in W-groups of

fields it is enough to check this relation by restricting to each dihedral, $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$-extension.[1]

Definition 1.8. *(1.2, [MS1]) A Galois extension L of F is called a D_4-extension of F if $Gal(L/F) \cong D_4$. If $a, b \in \dot{F}$ are independent modulo squares, then by a $D_4^{a,b}$-extension of F we mean a D_4-extension K of F such that $K \supseteq F(\sqrt{a}, \sqrt{b})$ and $Gal(K/F(\sqrt{ab})) \cong \mathbb{Z}/4\mathbb{Z}$.*

Definition 1.9. *Let $a, b \in \dot{F},$. Then we define the quaternion algebra $A = (\frac{a,b}{F})$ to be the F-algebra on two generators i, j with the defining relations $i^2 = a$, $j^2 = b$, $ij = -ji$. Let $k := ij$, so $k^2 = -ab$, $ik = -ki = aj$ and $kj = -jk = bi$.*

We say a quaternion algebra $A = (\frac{a,b}{F})$ is split over F and (denoted by $A = (\frac{a,b}{F}) = 1$), if $ax^2 + by^2 = 1$ is solvable in F or, equivalently, if the binary form $\langle a, b\rangle$ represents 1 (Theorem 2.7, [La3]).

Theorem 1.10. *(1.4, [MS1]) Let $a, b \in F$ be independent modulo squares. Then there exist a $D_4^{a,b}$-extension of F if and only if quaternion algebra $(\frac{a,b}{F})$ is split.*

Proof: See Theorem 4 in [MS].

The Frattini subgroup $\Phi(G)$ of a group G is the intersection of all maximal subgroups of G. Let p be a prime number. A group G is called a p-group if the number of elements of G is a power of p. One can show that if G is a finite p-group, then $\Phi(G) = G^p[G, G]$. For a W-group $\mathcal{G}_F$, let Φ_F denotes the Frattini subgroup group $\Phi(\mathcal{G}_F)$, which is a normal subgroup of $\mathcal{G}_F$. It was shown in [MS] that all W-groups are 2-groups, so Φ_F is generated by commutators and the squares of elements of $\mathcal{G}_F$. Following page 521 [MS], we define:

[1] This result was recently extended in [EM1], although we shall not use the extension in this thesis, it suggests that we may extend some of our results to a larger family of fields.

Definition 1.11. *An involution σ of $\mathcal{G}_F$ is simple if $\sigma \in \Phi_F$. Also σ is real if it is not simple and if the fixed field $F_\sigma^{(3)} \subseteq F^{(3)}$ of σ is formally real.*

Two involutions σ_1 and σ_2 are independent mod Φ_F if they are in different classes of $\mathcal{G}_F/\Phi_F$. By abuse of language we say σ is nonreal if σ is not simple and not real.

J. Mináč and M. Spira related the generators of $\mathcal{G}_F$ to the set of orderings of field F, also see [MS1].

Theorem 1.12. *(2.7, [MS1]) Let F is a field. Then*

1. If F is a formally real, then $\mathcal{G}_F$ contains a real involution.

2. If $\mathcal{G}_F$ contain a nonsimple involution[2], then F is formally real.

Proof: See Theorem 2.7 in [MS1].

If σ is a nonsimple involution in $\mathcal{G}_F$, and b is any element of $\dot{F}$ such that $\sigma(\sqrt{b}) = -\sqrt{b}$. Then notice that:

1. b is not a sum of two squares.

2. If $(\frac{b,c}{F}) = 1$, then $\sigma(\sqrt{c}) = \sqrt{c}$.

3. $\sigma(\sqrt{-1}) = -\sqrt{-1}$.

For the proof see Theorem 2.7 in [MS1].

Definition 1.13. *For a nonsimple involution σ in $\mathcal{G}_F$ define*

$$P_\sigma := \{a \in \dot{F} : \sigma(\sqrt{a}) = \sqrt{a}\}.$$

It is easy to check that P_σ is an ordering of the field F (see [MS1], page 522). For each $P \in X_F$ there exists a real involution $\sigma \in \mathcal{G}_F$ such that $P = (F_\sigma^{(3)})^2 \cap \dot{F}$. Following Definition 2.8 and Proposition 2.9 in [MS1], suppose σ and τ are nonsimple involutions in $\mathcal{G}_F$. Then $P_\sigma = P_\tau$ if and only if $\sigma\Phi_F = \tau\Phi_F$. So one can say $\sigma = \sigma_P$ mod Φ_F.

[2]This is an involution which is not simple.

Theorem 1.14. *(2.10, [MS1]) Let F be a Pythagorean formally real field. Then there exists a bijection between the set of orderings of the field F and the set of nontrivial cosets $\sigma\Phi_F$ of $\mathcal{G}_F$ such that σ is an involution. This is the bijection*

$$\sigma\Phi_F \longleftrightarrow P_\sigma.$$

Proof: See Corollary 2.10 [MS1].

The following theorem of [MS1] is another important theorem which gives us nice information about the generators of $\mathcal{G}_F$ when F is Pythagorean field.

Theorem 1.15. *(2.11, [MS1]) Let F be a formally real field. Then the following conditions are equivalent:*

1. F is Pythagorean.

2. $\mathcal{G}_F$ is generated by involutions.

3. $\Phi_F = [\mathcal{G}_F, \mathcal{G}_F]$.

Proof: See Theorem 2.11 in [MS1].

Remark: Note that $\mathcal{G}_F$ is generated by the non- simple involutions in this case since Frattini is in the center of $\mathcal{G}_F$ and is the commutator group, the commutator group is generated by non-simple involutions.

Definition 1.16. *For any field F, an element $a \in \dot{F}$ is called rigid if $D\langle 1, a\rangle = \dot{F}^2 \cup a\dot{F}^2$. $a \in \dot{F}$ is called double-rigid if both a and $-a$ are rigid.*

Definition 1.17. *Let F be a field. Define Bas$(F) = \{a \in \dot{F} | a$ is not double-rigid$\} \cup \dot{F}^2 \cup -\dot{F}^2$, which is a subgroup of $\dot{F}$.*

If $|\dot{F}/\dot{F}^2| > 2$, then Bas $(F) = \{a \in \dot{F} | a$ is not double-rigid$\}$, because -1 is not rigid.

Assume F is a Pythagorean formally real field. We will now mention some strong theorems which help us to characterize $\mathcal{G}_F$. These theorems are based on the Bas(F) and the elements of $\mathcal{G}_F$ which fix field $F(\sqrt{-1})$.

Following [MS] page 1280, we define:

$$H = \{\sigma \in \mathcal{G}_F | \sigma(\sqrt{-1}) = \sqrt{-1}\},$$

Choose a basis $\{-1, a_i | i \in I\}$ for $\dot{F}/\dot{F}^2$, such that $\{-1, a_i | i \in I'\}$ is the basis for the basic part $\text{Bas}(F)/\dot{F}^2$ of $\dot{F}/\dot{F}^2$, $I' \subset I$. Let $J = I \backslash I'$, so $\{a_j | j \in J\}$ are all double-rigid elements of this basis. Let $\{\sigma_{-1}, \sigma_i | i \in I\}$ be a dual set corresponding to the basis $\{-1, a_i | i \in I\}$, (This means $\sigma_i(\sqrt{a_j}) = (-1)^{\delta^{i,j}}\sqrt{a_j}$, such that $\delta^{i,j} = 1$, if $i = j = 1$, and $\delta^{i,j} = 0$ otherwise) and let Δ_J denotes the subgroup of $\mathcal{G}_F$ generated by $\{\sigma_j | j \in J\}$. Then

$$Z(H) = \{\sigma \in \mathcal{G}_F | \sigma(\sqrt{b}) = \sqrt{b}\ \forall b \in \text{Bas}(F)\} = \Delta_J.$$

One can show that any $\sigma_j \in \mathcal{G}_F$, with $j \in J$, has order 4, and that $\Delta_J \cong \prod_J \mathbb{Z}/4\mathbb{Z}$. (Corollary 3.3, [MS]).

Theorem 1.18. *Suppose $\sigma \in \mathcal{G}_F$. Then $\sigma(\sqrt{b}) = \sqrt{b}$ for all $b \in$ Bas(F) if and only if $\sigma \in Z(H)$.*

Proof: See Theorem 4.2 in [MS].

J. Mináč and T. Smith proved the next theorem which is important for determining the structure of $\mathcal{G}_F$. In the next theorem $\mathcal{G}_K$ is the W-group of some appropriate field K. This theorem was proved in the general, but if F is a Pythagorean formally real field, then K is the residue field of some 2-Henselian valuation on F. Their work is based on [M2], [Wr], [JWr] and [AEJ]. First, we recall the theorem in the general case, and then in Theorem 1.25 the specific case.

Theorem 1.19. *With the above notations,* $\mathcal{G}_F \cong \Delta_J \rtimes \mathcal{G}_K = (\prod_J \mathbb{Z}/4\mathbb{Z}) \rtimes \mathcal{G}_K$*, where* $\mathcal{G}_K$ *is generated by* $\{\sigma_i \mid i \in I \setminus J\} \cup \sigma_{-1}$ *and* $\mathcal{G}_K$ *acts on* Δ_J *by these equations:*

$$\sigma_i^{-1}\tau\sigma_i = \tau \quad \forall \tau \in \Delta_J,\, i \in I$$

$$\sigma_{-1}^{-1}\tau\sigma_{-1} = \tau^3 \quad \forall \tau \in \Delta_J.$$

Proof: See Theorem 3.5 in [MS].

We recall the concept of valuation and some useful theorems from [La2].

Definition 1.20. *Let* F *be a field. A valuation ring on* F *is a subring* A *of* F *such that for every* $x \in \dot{F}$ *at least one of* x *or* x^{-1} *is in* A*. We denote by* $\dot{A}$ *the group of all* $x \in \dot{F}$ *such that both* x, x^{-1} *are in* A*, and we call* $\dot{A}$ *the group of units of* A*.*

Definition 1.21. *A valuation* ν *on the field* F *is a group homomorphism from* $\dot{F}$ *into an ordered abelian group* $(\Gamma, \leqslant)$ *such that for any* $x, y \in \dot{F},\ x \neq -y$*:*

$$\nu(x+y) \geqslant min\{\nu(x), \nu(y)\}.$$

For a valuation $\nu : \dot{F} \to \Gamma$ on F, let

$$A_\nu = \{x \in F | x = 0 \,\text{or}\, \nu(x) \geqslant 0\}$$

$$\mathfrak{m} := \{x \in F | x = 0 \,\text{or}\, \nu(x) > 0\}.$$

Here, A_ν is a valuation ring on F , $\mathfrak{m}$ is called the maximal ideal of ν and Γ is called the value group of ν. $\bar{F} := A/\mathfrak{m}$ is the residue field of ν. In the literature a valuation ν is denoted sometimes by $(\nu, \mathfrak{m}, \bar{F})$.

Definition 1.22. *A valuation* ν *is called a Henselian valuation if, for any algebraic extension* $K \supseteq F$*, we can extend uniquely the valuation* ν *to a valuation* $\nu' : \dot{K} \to \Gamma$*.*

A valuation ν is called a 2- Henselian valuation if, for any quadratic extension $K \supseteq F$, there is a unique extension of ν to a valuation $\nu' : \dot{K} \to \Gamma$ (Page 27 [La2]). So if ν is Henselian, then it is also 2-Henselian.

Lemma 1.23. *(3.14 in [La2]) Let $(\nu, \mathfrak{m}, \bar{F})$ be a valuation on F such that $char\bar{F} \neq 2$. Then the valuation ν on F is 2-Henselian if and only if $1 + \mathfrak{m} \subseteq F^2$.*

Proof: See Lemma 3.14 in [La2].

Theorem 1.24. *(3.16, [La2]) If a field F has a 2-Henselian valuation ν, then:*

1. F is formally real iff the residue field $\bar{F}$ is formally real.

2. F is Pythagorean iff $\bar{F}$ is Pythagorean.

Proof: See Theorem 3.16 in [La2].

Theorem 1.25. *For a Pythagorean formally real field F,*

$$\mathcal{G}_F \cong (\prod_J \mathbb{Z}/4\mathbb{Z}) \rtimes \mathcal{G}_{\bar{F}}$$

where $\mathcal{G}_{\bar{F}}$ acts on $\prod_J \mathbb{Z}/4\mathbb{Z}$ by:
There exists a family of minimal set of generators σ_i, $i \in I$, σ_{-1} such that

$$\sigma_i^{-1}\tau\sigma_i = \tau \quad \forall \tau \in \prod_J \mathbb{Z}/4\mathbb{Z},\ \sigma_i \in \mathcal{G}_{\bar{F}}$$

$$\sigma_{-1}^{-1}\tau\sigma_{-1} = \tau^3 \quad \forall \tau \in \prod_J \mathbb{Z}/4\mathbb{Z}.$$

Here $\bar{F}$ is the residue field of some 2-Henselian valuation on F.

Proof: See ([MS], proof of Theorem 3.5 and page 1282).

We now turn to group theoretical characterizations of W-groups from a categorical point of view.

Definition 1.26. *A profinite group is a topological group which is Hausdorff, compact and totally disconnected.*

Definition 1.27. *A pro-p-group (for some prime number p) is a profinite group G such that for any open normal subgroup $N \triangleleft G$, the quotient group G/N is a p-group.*

J. Mináč and T. Smith show in [MS] that the group $\mathcal{G}_F$ is a topological group with the usual pro-2-group topology and it is in the category $\mathcal{C}$ which is defined as follows: If G is a pro-2-group, define the descending central sequence of G by :

$$G^{(1)} = G \qquad G^{(i+1)} = (G^{(i)})^2[G^{(i)}, G] \qquad i = 1, 2, ...$$

Then $\mathcal{C}$ is the full category of all pro-2-groups G with $G^{(3)} = \{1\}$. We can now conclude the following useful lemma.

Lemma 1.28. *(1.1, [MS]) The category $\mathcal{C}$ 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) $g^2 \in Z(G)$ where $Z(G)$ is the center of G. $\forall g \in G$.

Proof: By the definition of category $\mathcal{C}$, for any group G in the category $\mathcal{C}$ we have

$$G^{(3)} = (G^2[G, G])^2[G^2[G, G], G] = \langle 1 \rangle$$

The proof of $g^4 = 1$ and $g^2 \in Z(G) \, \forall g \in G$ is an easy exercise.□

Also, for any x, y in any group we have $[x, y] = x^{-2}(xy^{-1})^2y^2$. So for the group $\mathcal{G}_F$ which is in the category $\mathcal{C}$, the commutators are in the center of $\mathcal{G}_F$. By Theorem 1.15, $[\mathcal{G}_F, \mathcal{G}_F] = \Phi_F$. So the Frattini subgroup Φ_F of Pythagorean formally real field F is topologically generated by the squares of elements of $\mathcal{G}_F$.

In the category $\mathcal{C}$, the free product is actually a coproduct, defined as follows. First we need to define the free commutator subgroup. Since in this work we concerned with finite W-groups, We have the following based Definition 2.1 in [MS] one can define:

Definition 1.29. *Suppose $\mathcal{G}_1$ and $\mathcal{G}_2$ are two objects in category $\mathcal{C}$. Define the free commutator subgroup $\langle \mathcal{G}_1, \mathcal{G}_2 \rangle$ to be*

$$\mathcal{G}_1/\Phi(\mathcal{G}_1) \otimes_{\mathbb{F}_2} \mathcal{G}_2/\Phi(\mathcal{G}_2).$$

Following [MS] page 1277, let $\mathcal{G}_1, \mathcal{G}_2 \in \mathcal{C}$, and let the group $\mathcal{G}$ is the free product of $\mathcal{G}_1$ and $\mathcal{G}_2$ in the category $\mathcal{C}$. As a topological space, $\mathcal{G}$ is $\mathcal{G}_1 \times \mathcal{G}_2 \times \langle \mathcal{G}_1, \mathcal{G}_2 \rangle$ equipped with the product topology. Any element of the form $\langle \gamma_1, \gamma_2 \rangle$ of $\langle \mathcal{G}_1, \mathcal{G}_2 \rangle$ is actually the commutator of elements γ_1 and γ_2 in $\mathcal{G}$. One can define multiplication in $\mathcal{G}$ by the following properties:
(1) $\mathcal{G}_1$, $\mathcal{G}_2$ and $\langle \mathcal{G}_1, \mathcal{G}_2 \rangle$ are subspaces of $\mathcal{G}$. They 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 $\gamma_2 \in \mathcal{G}_2$ define

$$(\gamma_1, 1, 1)(1, \gamma_2, 1) = (\gamma_1, \gamma_2, 1)$$

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

$\mathcal{G}_2$ acts on $\mathcal{G}_1 \times \langle \mathcal{G}_1, \mathcal{G}_2 \rangle$ by $\gamma_1^{-1}\gamma_2\gamma_1 = \gamma_2\langle \gamma_1, \gamma_2 \rangle$ $\gamma_1 \in \mathcal{G}_1$ and $\gamma_2 \in \mathcal{G}_2$. Also note that the subgroup $\langle \mathcal{G}_1, \mathcal{G}_2 \rangle$ is in the center of $\mathcal{G}$. Now we can conclude $\mathcal{G}$ is isomorphic to the semidirect products

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

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

Theorem 1.30. *(2.2, [MS]) Let $\mathcal{G}_1 * \mathcal{G}_2$ denote the free product of the groups $\mathcal{G}_1$ and $\mathcal{G}_2$ in the category $\mathcal{C}$. Then*

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

Proof: See Theorem 2.2 in [MS].

By Theorem 1.24 if F is a Pythagorean formally real field, the residue field $\bar{F}$ is also a Pythagorean formally real field. So in Theorem 1.25, the residue field $\bar{F}$ is also a Pythagorean formally real field. Now one can apply Theorem 1.25 to $\bar{F}$. In Chapter 3, we continue to reduce the structure of the W-group $\mathcal{G}_{\bar{F}}$ of the residue field $\bar{F}$ and prove stronger theorems about the structure of $\mathcal{G}_F$. To achieve this goal we need some theorems about the space of orderings which will be discussed in Chapter 2.

Chapter 2

Spaces of orderings

In this chapter we recall the definition and some theorems about the space of orderings from [M1].

Definition 2.1. *A space of orderings is a pair (X, G) consisting of an elementary 2-group G with a distinguished element $-1 \in G$ and a subset X of the character group $\chi(G) = Hom(G, \{1, -1\})$ which satisfying the following properties:*
1. X is a closed subset of $\chi(G)$.
2. $\forall \sigma \in X, \sigma(-1) = -1$.
3. $X^{\perp} = \{a \in G \,|\, \sigma a = 1 \text{ for all } \sigma \in X\} = 1$.
4. If f and g are two forms over G and $x \in D_{f \oplus g}$, then there exist $y \in D_f$ and $z \in D_g$ such that $x \in D_{\langle y,z \rangle}$.

Following ([M1], page 320) we say a space of orderings is finite if X is finite (or equivalently G is finite). Also $f = \langle a_1, ..., a_n \rangle$ where $a_1, ..., a_n \in G$ denote form f of dimension n over G. We can define the signature of a form f at $\sigma \in X$ by $\sigma f = \sum_n^1 \sigma(a_i)$. Two forms f, g are called congruent, denoted by
$f \equiv g \,(\mathrm{mod}\, X)$, if they have the same dimension and the same signature at each $\sigma \in X$. A form f represents $x \in G$ if there exist $x_2, ..., x_n \in G$ such that $f \equiv$

$\langle x, x_2, ..., x_n\rangle$. Denoted D_f the set of all elements of G which are represented by f. For two forms $f = \langle a_1, ..., a_n\rangle$ and $g = \langle b_1, ..., b_m\rangle$, their sum and product are defined by:

$$f \oplus g = \langle a_1, ..., a_n, b_1, ..., b_m\rangle,$$

$$f \otimes g = \langle a_1b_1, ..., a_1b_m, ..., a_nb_1, ..., a_nb_m\rangle.$$

If $a \in G$, then $af = \langle a\rangle \otimes f$. Suppose S is a subset of G, let $S^{\perp}$ denotes the group of elements σ of $\chi(G)$ such that $\sigma(a) = 1$ for all $a \in S$. And if $T \subseteq \chi(G)$, then define

$$T^{\perp} = \{a \in G \,|\, \sigma(a) = 1 \,\text{for all}\, \sigma \in T\}.$$

Example 2.2.

If F is a formally real field, then let X_F be the set of all orderings of F, and $G = \dot{F}/\sum \dot{F}^2$. We will prove in Chapter 3 that (X_F, G_F) is a space of orderings.

To determine the space of orderings X_F of a Pythagorean formally real field F, we need some theorems and concepts that Murray Marshall proved about general space of orderings in [M1].

Example 2.3.

In the trivial case. Let $G = \{1\}$, then $X = \emptyset$, so $(X, G) \sim (X_F, G_F)$, where F is any field satisfying $F^2 = F$.

Let (X, G) be a finite space of orderings and $\sigma_1, ..., \sigma_m \in X$. Consider all linear combinations $\sigma = {\sigma_1}^{\epsilon_1}...{\sigma_m}^{\epsilon_m}$ such that $\epsilon_1...\epsilon_m \in \{0, 1\}$ in $\chi(G)$.

Definition 2.4. *Let $\sigma_1, ..., \sigma_m \in X$ be given. Define*

$$Y = \{\sigma \in X \,|\, \sigma \textit{ is a linear combination of} \sigma_1, ..., \sigma_m\},$$

$$\Delta = \{a \in G | \sigma_i(a) = 1 \, for \; all \; i = 1...m\}.$$

Y and Δ will satisfy the duality condition:

$$\Delta = Y^{\perp}, \qquad Y = \Delta^{\perp} \cap X.$$

We say that $(Y, G/\Delta)$ is the subspace of (X, G) generated by $\sigma_1, ..., \sigma_m$.

Note that in above definition σ should be a product of odd number of orderings σ_i such that $\sigma_i \in \{\sigma_1, ..., \sigma_m\}$.

Suppose $a_1, ..., a_m \in G$. Following ([M1] page 322) we denote by f the Pfister form $\langle 1, a_1 \rangle \otimes ... \otimes \langle 1, a_m \rangle$, and $X(a_1, ..., a_m)$ denotes the Harrison Basic set:

$$\{\sigma \in X | \sigma(a_i) = 1 \, \text{for all} \, i = 1, 2, ..., m\}.$$

Lemma 2.5. *(2.1, [M1]) Suppose $Y = X(a_1, ..., a_m)$ as above and $f = \langle 1, a_1 \rangle \otimes ... \otimes \langle 1, a_m \rangle$. Then Y and $\Delta = D_f$ satisfy the duality condition.*

Proof: (Lemma 2.1, [M1]).

Theorem 2.6. *The subspace $(Y, G/\Delta)$ of (X, G) defined above is also a space of orderings.*

Proof: See Lemma 2.2 in [M1].

Following the ([M1], page 323), two orderings $\sigma, \sigma' \in X$ are called simply connected in X, denoted $\sigma \backsim_s \sigma'$, if there exist orderings $\tau, \tau' \in X, \{\sigma, \sigma'\} \neq \{\tau, \tau'\}$, such that $\sigma\sigma' = \tau\tau'$. Two orderings $\sigma, \sigma' \in X$ are connected in X, denoted $\sigma \backsim \sigma'$, if either $\sigma = \sigma'$ or there exists a sequence of orderings

$$\sigma = \sigma_0, \, \sigma_1, ..., \sigma_k = \sigma' \in X \, \text{such that} \, \sigma_{i-1} \backsim_s \sigma_i \, \text{for} \, i = 1, ..., k.$$

Let $X = X_1 \cup ... \cup X_k$ denote the decomposition of X determined by the above equivalence relation $\sim$. Following M. Marshall we call X_i, $i = 1, ..., k$, as the connected components of X. The ordering space X is connected if it has only one connected component.

By property 3 of the definition of the ordering space (X, G), we can find a basis $\sigma_1, ..., \sigma_n$ of $\chi(G)$ consisting of elements of X. We refer this as a basis for X, and call n the rank (or dimension) of X. Notice that by property 2, if $\sigma_1, ..., \sigma_n$ is a basis of X, then any element of X should be a product of an odd number of $\{\sigma_1, ..., \sigma_n\}$.

Lemma 2.7. *(Basic lemma, [M1]) Suppose X consists of n independent orderings (n is odd, $n \geq 5$) together with their product $\sigma_1\sigma_2...\sigma_n$ and some (possibly empty) subset of*
$\sigma_1\sigma_3\sigma_4, \sigma_1\sigma_3\sigma_5, \sigma_2\sigma_3\sigma_4, \sigma_2\sigma_3\sigma_5$. *Then X is not a space of orderings.*

Proof: See the basic lemma in [M1].
This lemma will be used frequently in the future, especially in Chapter 3. We will prove the analogue of this lemma for X_F, the space of orderings of a Pythagorean formally real field F.

Theorem 2.8. *(Decomposition Theorem, [M1]) Suppose $X_1, ..., X_k$ are the connected components of X. Then X_i is subspace of X for any i, and*

$$rank\, X = \sum_{1}^{k} rank\, X_i.$$

Proof: See decomposition theorem in [M1].

Now let $G_i = G/\Delta_i$, where $\Delta_i = {X_i}^{\perp}$, $i = 1, ..., k$. By Theorem 2.0.38, each (X_i, G_i) is a subspaces of (X, G). We identify G with $G_1 \times ... \times G_k$. Then one can

write

$$(X, G) = \bigoplus_{i=1}^{k} (X_i, G_i).$$

The space (X, G) is called the direct sum of the spaces (X_i, G_i), $1 \leq i \leq k$.

Lemma 2.7 and Theorem 2.8 will help us to reduce the ordering space (X, G) to a smaller connected ordering space. Therefore it is enough to study the structure of finite connected spaces of orderings.

Definition 2.9. *The translation group T for an ordering space X is the set of all $\alpha \in \chi(G)$ such that $\alpha X = X$.*

M. Marshall proved in [M1] that if X_F is a connected space, then the translation group T is a nonempty subgroup of $\chi(G)$. By using this he reduced even the connected ordering space to the ordering spaces with the smaller rank. We recall this method here. We will use it in the next chapter to prove that if the set of orderings of a Pythagorean formally real field F is connected, then the W-group of F has a nontrivial translation group modulo the Frattini subgroup.

Theorem 2.10. *(4.2, [M1]) Suppose that $\sigma_1, ..., \sigma_n \in X$ is a basis of X, that $\alpha \in \chi(G)$, and that $\alpha\sigma_1, ..., \alpha\sigma_n \in X$. Then $\alpha X = X$.*

Proof: See Lemma 4.2 in [M1].

For $\alpha \in \chi(G)$ let X_α be the set $\{\sigma \in X \,|\, \sigma\alpha \in X\} = \alpha X \cap X$. It is easy to show that X_α is the maximal subset of X which satisfies $\alpha X_\alpha = X_\alpha$. By Lemma 4.3, [M1] X_α is a subspace of X. Consider the family $\mathcal{M} = \{X_\alpha \,|\, \alpha \in \chi(G)\}$. M. Marshall proved some interesting propositions about this family in [M1]. We recall them briefly:

1. Suppose $\sigma_1, \sigma_1\alpha, \sigma_1\beta, \sigma_1\alpha\beta \in X_F$. Then either $X_\alpha \subseteq X_\beta$ or $X_\beta \subseteq X_\alpha$.
2. Let $\alpha \neq 1, \beta \neq 1$, $X_\alpha \cap X_\beta \neq \emptyset$ such that rank $X_\alpha \geq 3$ and rank $X_\beta \geq 3$. Then there exists $\gamma \in \chi(G), \gamma \neq 1$ such that $X_\alpha, X_\beta \subseteq X_\gamma$.

Theorem 2.11. *(4.7, [M1]) Let X be a connected space with rank $X \neq 1$. Then there exists $\alpha \in \chi(G), \alpha \neq 1$, such that $\alpha X = X$.*

Proof: See Theorem 4.7 in [M1].

Now assume X is a connected space. If the rank $X \neq 1$, then by the last theorem the translation group T is nonempty. Let $G' = T^\perp$ and X' denote the set of all restrictions $\sigma|_{G'}$ such that $\sigma \in X$. Following [M1], page 328, the new ordering space X' is a disconnected space. Thus rank $X' = 1$, or X' would be a disconnected space of rank ≥ 3, so X' has strictly lower rank than X. Thus one can determine the structure of (X, G) inductively. The next two theorems have the main role in this process.

Remark: Note that any element of X can be written uniquely as $x = tx'$ where $t \in T$ and $x' \in X'$.

Theorem 2.12. *(4.8, [M1]) Let X be a connected space, and let X' and G' be defined as above. Then (X', G') is a space of orderings.*

Proof: See Theorem 4.8 in [M1].

Theorem 2.13. *(4.10, [M1]) Let (X, G) be a finite space of orderings. Then there exists a Pythagorean formally real field F such that $(X, G) \backsim (X_F, G_F)$.*

Proof: See Theorem 4.10 in [M1].

To continue we determine the space of orderings for some fields. Consider the field $\mathbb{R}(x) = \{\frac{p(x)}{q(x)} \mid (p(x), q(x)) = 1\}$.

Theorem 2.14. *There is a one-to-one correspondence between the set of orderings of* $\mathbb{R}(x)$ *and* $\mathbb{R} \cup \{\infty\}$.

$$P \longrightarrow \varphi(P) = a = \sup\{\alpha \mid (x - \alpha) \in P\},$$

$$P_a \longleftarrow a.$$

We need some propositions to prove this theorem.

Assume $p(x) = x^n + a_1 x^{n-1} + ... + a_n$ is a polynomial with coefficients in the real field $\mathbb{R}$. By the result in algebra:

$$p(x) = \prod_{i=1}^{l}(x - \bar{\beta}_i)(x - \beta_i) \prod_{j=1}^{s}(x - \alpha_j) \text{ such that } 2l + s = n, \ \ \beta_i \in \mathbb{C}.$$

We call $Q = \prod_{i=1}^{l}(x - \bar{\beta}_i)(x - \beta_i)$ the quadratic part of $p(x)$, and $\prod_{j=1}^{s}(x - \alpha_j)$ the real part of $p(x)$.

Lemma 2.15. *The quadratic part of* $p(x)$ *is an element of* P *where* P *is any ordering of* $\mathbb{R}(x)$.

Proof: By the definition of an ordering P of a field F, any square and any positive real number are elements of ordering P. For all i, we have

$$\begin{aligned}
(x - \bar{\beta}_i)(x - \beta_i) &= x^2 - x(\beta_i + \bar{\beta}_i) + \beta_i\bar{\beta}_i \\
\beta_i\bar{\beta}_i &= (a + ib)(a - ib) = a^2 + b^2 \in \mathbb{R} \\
\beta_i + \bar{\beta}_i &= (a + ib + a - ib) = 2a \in \mathbb{R} \\
\Longrightarrow (x - \bar{\beta}_i)(x - \beta_i) &= x^2 - x(\beta_i + \bar{\beta}_i) + \beta_i\bar{\beta}_i \\
&= x^2 - xb + c \\
&= (x - \frac{b}{2})^2 - \frac{b^2 - 4c}{4}
\end{aligned}$$

But $b^2 - 4c < 0$, so $(x - \bar{\beta_i})(x - \beta_i) = \underbrace{(x - \frac{b}{2})^2}_{\in P} + d$ such that $d \in \mathbb{R}^+$. Therefore $(x - \bar{\beta_i})(x - \beta_i) \in P$.□

Lemma 2.16. *For any ordering P and positive number a, if $b < a$ and $x - a \in P$, then $x - b \in P$.*

Proof: If $x - b \notin P$, then $b - x \in P$. Therefore, $b - x + x - a \in P$, $b - a \in P$. On the other hand, $0 < a - b \in P$, so $b - a \in P \cap -P$, which is a contradiction. Therefore, $x - b \in P \ \forall b < a$.□

Assume P is an arbitrary ordering of $\mathbb{R}(x)$, and let $a = \sup\{\alpha \in \mathbb{R} | (x - \alpha) \in P\}$. There are two possibilities:

1. a is finite number.
2. a is infinity.

Consider an ordering P of $\mathbb{R}(x)$. If a is finite, then one can prove the following lemma.

Lemma 2.17. *Let $a = \sup\{\alpha \,|(x - \alpha) \in P\}$. Let P_a be the set*

$$P_a := \{f(x) = \frac{p(x)}{q(x)} \in \mathbb{R}(x) \,|\, f(a) \geq 0\}.$$

Then P_a is an ordering of $\mathbb{R}(x)$.

Proof: If $f(x)$ and $g(x) \in P_a$, then $f(a) \geq 0$ and $g(a) \geq 0$. Thus $fg(a) \geq 0$ and $(f + g)(a) \geq 0$. Therefore $P_a \cdot P_a \subseteq P_a$ and $P_a + P_a \subseteq P_a$. It is easy to check that $P_a \cup -P_a = \mathbb{R}(x)$, so P_a is an ordering of $\mathbb{R}(x)$.□

Theorem 2.18. *Let P be an ordering and $a = \sup\{\alpha \in \mathbb{R} | (x - \alpha) \in P\}$ and P_a is a subset of $\mathbb{R}(x)$ which is defined in last theorem. Then $P = P_a$.*

Proof: If we fix $a \in \mathbb{R}$ then for any $f(x) \in \mathbb{R}(x)$ we can write:

$$f(x) = \frac{p(x)}{q(x)} = \frac{Q\prod_{j=1}^{s}(x-\alpha_j)\prod_{i=1}^{k}(x-\lambda_i)}{Q'\prod_{j=1}^{s'}(x-\alpha'_j)\prod_{i=1}^{k'}(x-\lambda'_i)},$$

such that λ_i, $\lambda'_i \leq a$, α_j, $\alpha'_j > a$ and Q, Q' are the quadratic part of p and q respectively. Suppose $f(x) \in P_a$. Since $f(a) \geq 0$ then $s + s'$ should be even.

Because for any j, $\alpha_j, \alpha'_j > a$, by definition of a we can conclude $(x - \alpha_j)$ and $(x - \alpha'_j)$ are not in P, so $-(x - \alpha_j)$, $-(x - \alpha'_j)$ are elements of P.

$$f(x) = \frac{p(x)}{q(x)} = \frac{Q(-1)^{s+s'}\prod_{j=1}^{s}(x-\alpha_j)\prod_{i=1}^{k}(x-\lambda_i)}{Q'\prod_{j=1}^{s'}(x-\alpha'_j)\prod_{i=1}^{k'}(x-\lambda'_i)}$$

$$= \frac{Q(-1)^{s}\prod_{j=1}^{s}(x-\alpha_j)\prod_{i=1}^{k}(x-\lambda_i)}{Q'(-1)^{s'}\prod_{j=1}^{s'}(x-\alpha'_j)\prod_{i'=1}^{k'}(x-\lambda'_i)}.$$

So $f(x) \in P$.

Conversely suppose:

$$f(x) = \frac{p(x)}{q(x)} = \frac{Q\prod_{j=1}^{s}(x-\alpha_j)\prod_{i=1}^{k}(x-\lambda_i)}{Q'\prod_{j'=1}^{s'}(x-\alpha_{j'})\prod_{i'=1}^{k'}(x-\lambda_{i'})} \in P$$

But $x - \alpha_j \notin P$ so for all j, $-(x - \alpha_j) \in P$, then $(-1)^{s+s'}f(x) \in P$. Since $P \cap -P = \{0\}$, then $(-1)^{s+s'} = 1$ and $s + s'$ is even. Then $f(a) \geq 0$ and $f(x) \in P_a$.□

Proof of Theorem 2.15:
The ordering P_a was characterized in Lemma 2.17, so we need just to prove φ is a one-to-one correspondence.

If P_1 and P_2 are two orderings such that $P_1 \neq P_2$, then $\varphi(P_1) \neq \varphi(P_2)$. If $P_1 \neq P_2$ and $\varphi(P_1) = \varphi(P_2) = a$, then P_{1_a} and P_{2_a} contain $\{(x - \alpha_i) | \, \alpha_i \leq a\}$, but

we characterized P_{1_a} and P_{2_a} in Lemma 2.17, so $P_1 = P_2$.

Conversely, for any $a \in \mathbb{R}$, let P be an ordering of F such that $a = \sup\{\alpha_i \,|(x - \alpha_i) \in P\}$. We proved in Lemma 2.0.49 that P containes $\{(x - \alpha)\,|\alpha \leq a\}$. Thus by the definition of a, for any $b > a$ such that $a \neq b$, one can conclude that $P_a \neq P_b$.□

As we showed in Theorem 2.15, the field $\mathbb{R}(x) = \{\frac{p(x)}{q(x)}|(p(x), q(x)) = 1\}$ of rational functions is an example of a field with an infinite number of orderings. We finish this chapter with the example of a field which has just two orderings.

Example 2.19.

Consider the field $F = \mathbb{R}((x))$ of all formal Laurent series over $\mathbb{R}$. A formal Laurent series is power series in one variable of the form

$$f = \sum_{k=n}^{\infty} a_k x^k, n \in \mathbb{Z}.$$

The square class group is $\dot{F}/\dot{F}^2 = \{[1], [-1], [x], [-x]\}$. We show that this field has two orderings which we call P_1 and P_2. There are two cases for arbitrary ordering P of F.

Case 1: The ordering P contains x. We show that P is unique and it contains all formal Laurent series $f = \sum_n^{\infty} a_n x^n, n \in \mathbb{Z}$, such that if $a_n \neq 0$ then $a_n > 0$. In this case we name it P_1. First we claim that any element like of the form

$$g = a_0 + a_1 x + a_2 x^2 + ...$$

is an element in $\mathbb{R}((x))^2$ if $a_0 > 0$. For $F = \mathbb{R}((x))$ we can define a valuation

$$\nu : \mathbb{R}((x)) \longrightarrow \mathbb{R}$$

$$f = \sum_{n=m}^{\infty} a_n x^n \in \mathbb{R}(x) \text{ if } a_m \neq 0 \qquad \nu(f) = m.$$

Now we see that $A_\nu = \mathbb{R}[[x]]$, so $\bar{F} = \mathbb{R}$. We use [La1], Lemma VI.1.1 which says any element $u \in F$ such that $\nu(u) = 0$ is a square in F if and only if $\bar{u}$ is a square in $\bar{F}$. Hence $g = a_0 + a_1 x + a_2 x^2 + ...$ is a square in $F = \mathbb{R}((x))$ if $a_0 > 0$. We can conclude that for any ordering P of F, g is an element of P. Suppose $f = \sum_n^\infty a_n x^n, n \in \mathbb{Z}$ and $f \in P_1$. We see that

$$f = \sum_{n=m}^{\infty} a_n x^n = x^m(a_m + a_{m+1}x + ...).$$

But $x^m \in P_1$ (Because $x \in P_1$), $f \in P_1$, so $a_m > 0$. Conversely if

$$P_1 = \{f \in \mathbb{R}((x)) \mid f = \sum_{n=m}^{\infty} a_n x^n, \text{ for } a_m \neq 0 \ a_m > 0\},$$

then it is easy to show that P_1 is an ordering.

Case 2: The ordering P does not contain x. We named it P_2. Then P_2 contains $-x$ and also $(-1)^n x^n$. Again suppose $f = \sum_{n=m}^\infty a_n x^n, m \in \mathbb{Z}$, then

$$f = \sum_{n=m}^{\infty} a_n x^n = x^m(a_m + a_{m+1}x + ...).$$

If $f \in P_2$ if and only if $a_n(-1)^n > 0$, as $(-1)^n x^n \in P_2$.

Now consider $(X_F, \dot{F}/\dot{F}^2)$ where $F = \mathbb{R}((x))$. As we have shown $X_F = \{P_1, P_2\}$.

Even in this simple example where X_F has a very simple structure, it is not obvious how to compute $\mathcal{G}_F = Gal(F^{(3)}/F)$. We prove some theorems in Chapter 3 which makes much easier to determine of W-groups. Then one can show that $\mathcal{G}_F = C_2 * C_2$.

Chapter 3

Classification of finite W-groups

In this chapter we obtain the fundamental results on the structure of the W-group of a formally real Pythagorean field with finitely many orderings. The SAP case is quite easy and therefore usually we assume that our field is not SAP. This means that $|\dot{F}/\dot{F}^2| = 2^n$ and $|X_F| = a$, $a \neq n$. If X_F is a connected space, we reduce the structure of $\mathcal{G}_F$ to the structure of $\mathcal{G}_{\bar{F}}$, the W-group of the residue field $\bar{F}$.

If the space X_F is disconnected, the structure of $\mathcal{G}_F$ is reduced to the free product of $\mathcal{G}_{F_i}$ such that $\mathcal{G}_{F_i}$ are W-groups of Pythagorean fields F_i; here F_i is a Pythagorean formally real field for which X_{F_i} is equal to the connected components X_i of X_F . We use M. Marshall's method, (see [M1]) for classification, but everything will be proved from a Galois point of view. An essential ingredient is the theorem relating the ordering space X_F to $\{\sigma \in Gal(F^{(3)}/F) | \, \sigma^2 = 1, \, \sigma \notin \Phi_F\}$, the set of non simple involutions, (see [MS1]).

In the next step we will use L. Brocker's formula about the set $O(n)$, the possible number of orderings of field F in which $|\dot{F}/\dot{F}^2| = 2^n$ (see [Mz]). Then we are able to

give further classification for $\mathcal{G}_F$ such that $|\dot{F}/\dot{F}^2| = 2^n$ and $|X_F| = a$. According to the work in the PhD thesis of J. Mináč, and also J.L. Merzel's work in [Mz], we find the sufficient condition for uniqueness of the structure of $\mathcal{G}_F$ based on the number of elements of space of orderings X_F. In the end we discuss just a little about the relation of W-groups with Coxeter groups.

3.1 Space of orderings X_F of a Pythagorean formally real field F

Following [M1], we recall the definition of a space of orderings is a pair (X, G) consisting of an elementary 2-group G with a distinguished element $-1 \in G$ and a subset X of the character group $\chi(G) = Hom(G, \{1, -1\})$ which satisfying the following properties:

1. X is a closed subset of $\chi(G)$.
2. For all $\sigma \in X, \sigma(-1) = -1$.
3. $X^{\perp} = \{a \in G \,|\, \sigma a = 1 \text{ for all } \sigma \in X\} = 1$.
4. If f and g are two forms over G and $x \in D_{f \oplus g}$, then there exist $y \in D_f$ and $z \in D_g$ such that $x \in D_{\langle y,z \rangle}$.

Now for any Pythagorean formally real field F, let X_F be the set of all orderings of F, and $G = \dot{F}/\dot{F}^2$. We will show in the following that (X_F, G_F) is the space of orderings.

Assume F is a Pythagorean formally real field, and let $\mathcal{G}_F$ be its W-group. Let $\mathcal{X}_F = \{\sigma\Phi_F \,|\, \sigma^2 = 1, \sigma \notin \Phi_F\}$ be the set of classes of non simple involutions of $\mathcal{G}_F$ modulo the Frattini subgroup of $\mathcal{G}_F$, and also let X_F be the space of orderings of F. For any $\sigma \in \mathcal{X}_F$ consider $P_\sigma = \{a \in \dot{F} \,|\, \sigma(\sqrt{a}) = \sqrt{a}\}$. Recall Theorem 1.0.16 say that there exists a bijection between the set of orderings of F and the set of nontrivial cosets $\sigma\Phi_F$, where σ is an involution in $\mathcal{G}_F$. From now on, we identify $\mathcal{X}_F$ with X_F. We claim $(X_F, \dot{F}/\dot{F}^2)$ is a space of orderings, so X_F should have the following properties.

1. X_F is a closed subset of the set of involutions of $\mathcal{G}_F$.

2. $\sigma(\sqrt{-1}) = -\sqrt{-1}$.

3. $X_F^{\perp} = \{a \in \dot{F}/\dot{F}^2, \sigma(\sqrt{a}) = \sqrt{a} \text{ for any } \sigma \in X\}$ is the trivial preordering $\sum \dot{F}^2 = \dot{F}^2$.

4. If f and g are two forms over $\dot{F}/\dot{F}^2$ and if $x \in D_{f\oplus g}$, then there exist $y \in D_f$ and $z \in D_g$ such that $x \in D_{\langle y,z\rangle}$.

To illustrate property 4, first we need to recall Corollary 2.4 in [La3] which says the following:
For any quadratic space (V, B) over F, there exist scalars $d_1, d_2, ..., d_n \in F$ such that the n-ary quadratic form V is equivalent to the diagonal form, $d_1X_1^2 + ... + d_nX_n^2$, which is denoted by $\langle d_1, ..., d_n\rangle$. If $f = \langle d_1, ..., d_n\rangle$, then we define $d(f) = d_1...d_n.\dot{F}^2$. Two forms $q = \langle a_1, ..., a_n\rangle$ and $q' = \langle b_1, ..., b_n\rangle$ are equivalent if and only if $d(q) = d(q')$ and q, q' represent a common element $e \in \dot{F}$.

Before proving these properties we define the signature of an involution $\sigma \in \mathcal{G}_F$. For any $b \in \dot{F}/\dot{F}^2$, $(\text{sig}\,\sigma)(b) = \sigma(\sqrt{b})/\sqrt{b} \in \{\pm 1\}$. By the definition of P_σ in [MS2]:

$$P_\sigma := \{a \in \dot{F}/\dot{F}^2 \mid \sigma(\sqrt{a}) = \sqrt{a}\}$$

we see that $(\text{sig}\,\sigma)(b) = (\text{sig}P_\sigma)(b)$ for any $b \in \dot{F}/\dot{F}^2$ where $(\text{sig } P_\sigma)$ is the classical signature function

$$(\text{sig}P_\sigma)(b) = \begin{cases} 1 & \text{if } b \in P_\sigma, \\ -1 & \text{if } b \notin P_\sigma. \end{cases}$$

Here as usual we think about $b \in \dot{F}/\dot{F}^2$ as an element of the quotient group of the multiplicative group $\dot{F}$ of F modulo its squares $\dot{F}^2$. On the other hand any element $\gamma \in \chi(\dot{F}/\dot{F}^2)$ induces $\bar{\gamma} : F^{(2)} \longrightarrow F^{(2)}$ which fixes F, and $\bar{\gamma}$ is an involution in

$Gal(F^{(2)}/F)$. We can extend $\bar{\gamma}$ to an involution in $Gal(F^{(3)}/F)$.

Proof of 1. Assume that K/F is any Galois extension which may be possibly infinite. Let us recall the Krull topology on the $Gal(K/F)$. The Krull topology on $Gal(K/F)$ is defined via a neighborhood basis $\mathcal{U}(K/F)$ at the unit element:

$$\mathcal{U}(K/F) = \{Gal(K/N) \,|\, N \in \mathcal{N}\}$$

where $\mathcal{N}$ is the set of all subfields N of K which contain F and are finite and Galois over F.
We shall apply this for $K = F^{(3)}$. Observe first that $\Phi(Gal(F^{(3)}/F))$, the Frattini subgroup of $Gal(F^{(3)}/F)$, is a closed subgroup of $Gal(F^{(3)}/F)$. Indeed $\Phi(Gal(F^{(3)}/F))$ contains all $\tau \in Gal(F^{(3)}/F)$ which fix $F^{(2)}$. By definition of Frattini subgroup $\Phi(Gal(F^{(3)}/F)) = \bigcap H_i$ for all maximal subgroup H_i of $\mathcal{G}_F$. If $\tau \in \Phi(Gal(F^{(3)}/F))$, and $\tau \notin Gal(F^{(3)}/F^{(2)})$, so there exist $b \in \dot{F}$ such that $\tau(\sqrt{b}) = -\sqrt{b}$. Hence $\tau \notin Gal(F^{(3)}/F(\sqrt{b}))$ but $Gal(F^{(3)}/F(\sqrt{b}))$ has index 2 in $\mathcal{G}_F$, so it is a maximal subgroup $\mathcal{G}_F$ and this is contradiction.

Therefore if $\gamma \notin \Phi(Gal(F^{(3)}/F))$ then there exists $a \in \dot{F}$ such that $\gamma(\sqrt{a}) = -\sqrt{a}$. But then for all $\sigma \in \gamma Gal(F^{(3)}/F(\sqrt{a}))$ we also have that

$$\sigma(\sqrt{a}) = -\sqrt{a}.$$

Because $\gamma Gal(F^{(3)}/F(\sqrt{a}))$ is an open neighborhood of γ, we see that $\Phi(Gal(F^{(3)}/F))$ is a closed subgroup of $Gal(F^{(3)}/F)$. Therefore we can consider the quotient topology on $W := Gal(F^{(3)}/F)/\Phi(Gal(F^{(3)}/F))$. We consider X_F to be a subset of W and we claim that X_F is a closed subset of W.

Suppose that $[\alpha] \in W \setminus X_F$. Let $[\alpha] = \alpha.\Phi(Gal(F^{(3)}/F))$. Then either $\alpha \in \Phi(Gal(F^{(3)}/F))$ or α is not an involution in $Gal(F^{(3)}/F)$. If $\alpha \in \Phi(Gal(F^{(3)}/F))$

then $\alpha(\sqrt{-1}) = \sqrt{-1}$ and $\alpha.Gal(F^{(3)}/F(\sqrt{-1}))$ has image in W disjoint with X_F. If α is not involution, then

$$P_\alpha := \{a \in \dot{F}/\dot{F}^2 \mid \alpha(\sqrt{a}) = \sqrt{a}\}$$

is not an ordering of F. This follows from Corollary 2.10 in [MS1]. Indeed by Kummer theory P_α determines $\alpha.\Phi(Gal(F^{(3)}/F))$ and if P_α is an ordering then $\alpha.\Phi(Gal(F^{(3)}/F))$ consists of involutions, but α is not an involution. Because P_α is not an ordering we see that P_α is not additively closed. This means that there exists $h, q \in P_\alpha$ such that $h + q \notin P_\alpha$.

Consider $H := Gal(F^{(3)}/K)$, where $K = F(\sqrt{h}, \sqrt{q}, \sqrt{h+q})$. Then the action of all elements $\alpha.H$ on K is the same as the action of α on K. This means that for all $\beta \in \alpha.H$,

$$P_\beta := \{a \in \dot{F}/\dot{F}^2 \mid \beta(\sqrt{a}) = \sqrt{a}\}$$

is not an ordering in F. Hence the image of the open neighborhood $\alpha.H$ of α in W has empty intersection with X_F. This proves that X_F is a closed subset of W.□

Proof of 2. See claim 3, Theorem 2.7 in [MS1].

Proof of 3. Let $X = \{\sigma_1\Phi_F, \sigma_2\Phi_F, ..., \sigma_n\Phi_F\}$. Then any $\sigma_i\Phi_F$ corresponds to the ordering P_i of F (see [MS1]). Now use Artin's theorem (Theorem 1.6 [La2]) about preorderings, so $X^\perp = \bigcap_{P_i \in X_F} P_i = \dot{F}^2$.□

Proof of 4. Let $f = \langle a_1, ..., a_m\rangle$ and $g = \langle b_1, ..., b_n\rangle$ be two forms on F. Suppose there exist $f_1, ..., f_{m+n} \in F$ such that $x = a_1f_1^2 + ... + b_nf_{m+n}^2$. Now let:

$$y = a_1f_1^2 + ... + a_mf_m^2 \text{ and } z = b_1f_{1+n}^2 + ... + b_mf_{m+n}^2.$$

So we found $y \in D_f$, $z \in D_g$ such that $x \in D_{\langle y,z\rangle}$.$\square$

Let $\{P_{\sigma_1}, P_{\sigma_2}, ..., P_{\sigma_m}\}$ be an arbitrary subset of X_F, $Y = \{P \in X_F \,|\, P = P_{\sigma_{i_1}} \cdots P_{\sigma_{i_k}}\}$ and $T = \bigcap P_{\sigma_i}$ $i = 1, ..., m$. Then $(Y, \dot{F}/\dot{T})$ is a subspace of the ordering space $(X_F, \dot{F}/\dot{F}^2)$ if Y, T satisfy the duality condition:

$$T = \bigcap P_\sigma \text{ such that } P_\sigma \in Y, \quad Y = \{P \in X_F \,|\, T \subseteq P\}.$$

Therefore with these definitions, any $(Y, \dot{F}/\dot{T})$ where T is a preordering of F, is a subspace of $(X_F, \dot{F}/\dot{F}^2)$. One can show that any subspace $(Y, \dot{F}/\dot{T})$ is an ordering space and then by (Theorem 4.10 [M1]) there is a Pythagorean formally real field E such that Y corresponds to X_E.

Consider the Pfister form $f = \langle 1, a_1\rangle \otimes ... \otimes \langle 1, a_m\rangle = \langle 1, a_1, .., a_m, a_1a_2, ..., a_1a_2...a_m\rangle$ on F and $X(a_1, ..., a_m) = \{P \in X_F \,|\, a_i \in P,\ i = 1, ..., m\}$. It is easy to show that $T = \bigcap_{P \in X(a_1,...,a_m)} P$ is a preordering of field F.

Theorem 3.1. *Let $(Y, \dot{F}/\dot{T})$ be any subspace of $(X_F, \dot{F}/\dot{F}^2)$. Then $(Y, \dot{F}/\dot{T})$ is also a space of orderings.*

Proof: This is a consequence of Theorem 2.6.

Definition 3.2. *Any subgroup $G \subseteq \mathcal{G}_F$ such that $G \cong (\prod_1^n \mathbb{Z}/4\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$ is called a Galois fan.*

Example 3.3. *Consider a Pythagorean field F and its W-group $\mathcal{G}_F$. Let G be a subgroup of $\mathcal{G}_F$, where $G = \langle \sigma_1, \sigma_2, \sigma_3\rangle$ such that $\sigma_1, \sigma_1, \sigma_3$ are independent involutions mod Φ_F. Then the generators of G satisfy $([\sigma_1, \sigma_2][\sigma_2, \sigma_3][\sigma_3, \sigma_1]) = 1$ if and only if $G \cong (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$.*

Proof: Suppose $G \cong (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$, τ_1 and τ_2 are generators of $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and σ_1 is the generator of $\mathbb{Z}/2\mathbb{Z}$. Let $\sigma_1\sigma_2 = \tau_1$ and $\sigma_1\sigma_3 = \tau_2$. Due to the structure of G, the generator σ_1 acts on τ_i with this action

$$\sigma_1^{-1}\tau_i\sigma_1 = \tau_i^{-1}, \;\; i = 1, 2 \text{ then } \sigma_1\tau_i\sigma_1 = \tau_i^3 \quad (I)$$

Also $[\sigma_1, \sigma_2] = [\sigma_1, \sigma_1\tau_1] = \sigma_1^{-1}(\sigma_1\tau_1)^{-1}\sigma_1\sigma_1\tau_1 = \sigma_1\tau_1^3\sigma_1\sigma_1\sigma_1\tau_1 = \tau_1\sigma_1\sigma_1\tau_1 = \tau_1^2$

In the same way

$$[\sigma_3, \sigma_1] = [\sigma_1\tau_2, \sigma_2] = \tau_2^2,$$

$$[\sigma_2, \sigma_3] = [\tau_1\sigma_1, \tau_2\sigma_1] = \sigma_1\tau_1^3\sigma_1\tau_2^3\tau_1\sigma_1\tau_2\sigma_1 = \tau_1\sigma_1\sigma_1\tau_2^3\tau_1\sigma_1\tau_2\sigma_1 = \tau_1\tau_2^3\tau_1\tau_2^3$$

So

$$([\sigma_1, \sigma_2][\sigma_2, \sigma_3][\sigma_3, \sigma_1]) = \tau_1^2\tau_1\tau_2^3\tau_1\tau_2^3\tau_2^2 = \tau_1^3\tau_2^3\tau_1\tau_2$$

τ_1 and τ_2 are the generators of $(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z})$, so

$$([\sigma_1, \sigma_2], [\sigma_2, \sigma_3], [\sigma_3, \sigma_1]) = 1$$

Conversely, let F is a Pythagorean field and $\sigma_1, \sigma_2, \sigma_3$ are involutions which are independent mod Φ_F and satisfy this relation:

$$([\sigma_1, \sigma_2][\sigma_2, \sigma_3][\sigma_3, \sigma_1]) = 1 \quad (II).$$

Suppose $\tau_1 = \sigma_1\sigma_2$ and $\tau_2 = \sigma_1\sigma_3$. We will show that τ_1 and τ_2 have order 4. Since $\Phi_F = [\mathcal{G}_F, \mathcal{G}_F]$ and any element in Φ_F has order 2,

$$\tau_1^4 = \sigma_1\sigma_2\sigma_1\sigma_2\sigma_1\sigma_2\sigma_1\sigma_2 = [\sigma_1, \sigma_2][\sigma_1, \sigma_2] = ([\sigma_1, \sigma_2])^2 = 1.$$

In the same way $\tau_2^4 = 1$. But $\tau_1^2 \neq 1$ because if $\tau_1^2 = (\sigma_1\sigma_2)^2 = 1$, σ_1, σ_2 are independent so $\sigma_1\sigma_2 \notin \Phi_F$. By (Theorem 2.7, [MS]) $(\sigma_1\sigma_2)(\sqrt{-1}) = -\sqrt{-1}$ but since

σ_1 and σ_2 are non simple involutions then $\sigma_1\sigma_2(\sqrt{-1}) = \sqrt{-1}$, so this is contradiction. Therefore $\tau_1^2 = (\sigma_1\sigma_2)^2 \neq 1$ and the order of τ_1 is 4. In the same way τ_2 has order 4.

Now consider $H = \langle\tau_1\rangle \times \langle\tau_2\rangle$ and $K = \langle\sigma_1\rangle$. Since

$$\sigma_1^{-1}\tau_1\sigma_1 = \sigma_1(\sigma_1\sigma_2)\sigma_1 = \sigma_2\sigma_1 = (\sigma_1\sigma_2)^{-1} = \tau_1^{-1} = \tau_1^3$$

$$\sigma_1^{-1}\tau_2\sigma_1 = \sigma_1(\sigma_1\sigma_3)\sigma_1 = \sigma_3\sigma_1 = (\sigma_1\sigma_3)^{-1} = \tau_2^{-1} = \tau_2^3$$

K acts on H by $\sigma_1^{-1}\tau_i\sigma_1 = \tau_i^{-1} = \tau_i^3$. So this action makes the set

$$\{(h,k) \,|\, h \in (\langle\tau_1\rangle \times \langle\tau_2\rangle),\, k \in \langle\sigma_1\rangle\}$$

into a semidirect product group $(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$.

On the other hand $(\langle\tau_1\rangle \times \langle\tau_2\rangle) \cap \langle\sigma_1\rangle = 1$ and $(\langle\tau_1\rangle \times \langle\tau_2\rangle)$ is normal subgroup. Then $G \cong (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$. □

Example 3.4.

There is a one-to-one correspondence between Galois fans G of $\mathcal{G}_F$ generated by three elements and classical fans of the space of orderings with four elements.

Proof: If G is a subgroup of $\mathcal{G}_F$ such that $G = \langle\sigma_1, \sigma_2, \sigma_3\rangle$ and $\sigma_1, \sigma_1, \sigma_3$ are independent involutions mod Φ_F and satisfy

$[\sigma_1, \sigma_2][\sigma_2, \sigma_3][\sigma_3, \sigma_1] = 1$, then:

$$[\sigma_1, \sigma_2][\sigma_2, \sigma_3][\sigma_3, \sigma_1] = \sigma_1\sigma_2\sigma_1\sigma_2\sigma_2\sigma_3\sigma_2\sigma_3\sigma_3\sigma_1\sigma_3\sigma_1 = 1$$

$$\sigma_1\sigma_2\sigma_1\sigma_2\sigma_2\sigma_3\sigma_2\sigma_3\sigma_3\sigma_1\sigma_3 = \sigma_1$$

$$\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1\sigma_3 = \sigma_1\sigma_1 = 1 \Longrightarrow (\sigma_2\sigma_1\sigma_3)^2 = 1$$

So $\sigma_2\sigma_1\sigma_3$ is an involution. But we know by assumption that $\sigma_2\sigma_1\sigma_3 \notin \Phi_F$ since $\sigma_1, \sigma_1, \sigma_3$ are independent involution mod Φ_F, so $\sigma_2\sigma_1\sigma_3$ is an element of X_F .
On the other hand by Theorem 1.0.16 any $\sigma_i \in X_F$ corresponds to the ordering P_{σ_i} of F. So we have three ordering $P_{\sigma_1}, P_{\sigma_2}, P_{\sigma_3}$ and ordering P_4 which corresponds to non-simple involution $\sigma_1\sigma_2\sigma_3$. So by this correspondence

$$\sigma_1 \longrightarrow P_1$$

$$\sigma_2 \longrightarrow P_2$$

$$\sigma_3 \longrightarrow P_3$$

$$\sigma_1\sigma_2\sigma_3 \longrightarrow P_4,$$

the subgroup G corresponds to the classical fan with four elements.□

As shown in the last example, if F is a fan with four elements, then the W-group is $\mathcal{G}_F = \langle \sigma_1, \sigma_2, \sigma_3 \mid (\sigma_1\sigma_2\sigma_3)^2 = 1 \rangle \cong (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$. In the same way we can show that if $|\dot{F}/\dot{F}^2| = 2^n$ and $|X_F| = 2^{n-1}$, i.e the fan case with 2^{n-1} elements, then $\mathcal{G}_F \cong (\prod_1^{n-1} \mathbb{Z}/4\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$.

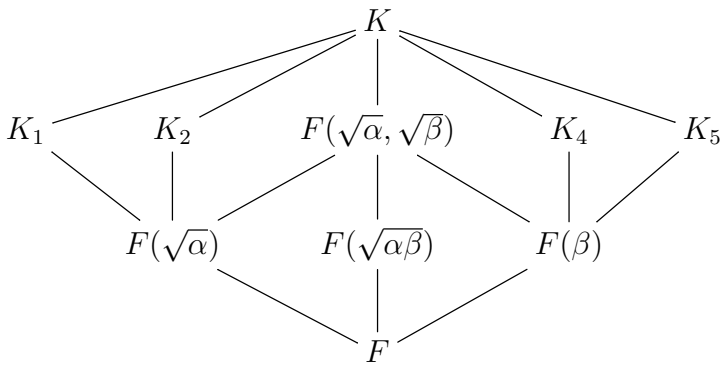
Now we are ready to prove the main lemma for the space of ordering X_F from the Galois point of view (which corresponds to Lemma 1.3 in [M]).

First recall Definition 1.8 and Theorem 1.10. A Galois extension L of F is called a D_4-extension of F if $G(L/F) \cong D_4$. If $a, b \in \dot{F}$ are independent modulo squares, then by a $D_4^{a,b}$-extension of F we mean a D_4-extension K of F such that $K \supset F(\sqrt{a}, \sqrt{b})$ and $G(K/F(\sqrt{ab})) \cong \mathbb{Z}/4\mathbb{Z}$. Let $a, b \in F$ be independent modulo squares. Then there exists a $D_4^{a,b}$-extension of F if and only if $(\frac{a,b}{F}) = 1$

Lemma 3.5. *There does not exist any Pythagorean formally real field F such that $\mathcal{G}_F = \langle \sigma_1, ..., \sigma_5 \,|\, (\sigma_i)^2 = (\sigma_1 \cdots \sigma_5)^2 = 1,\ i = 1, .., 5 \rangle$ and $\sigma_1, ..., \sigma_5$ are independent involutions mod Φ_F*

Proof: Since $\sigma_1, ..., \sigma_5$ are independent modulo Φ_F, there exists a dual basis $\{a_1, ..., a_5\}$ such that $\sigma_i(\sqrt{a_j}) = (-1)^{\delta_{i,j}}(\sqrt{a_j})$.

Claim 1: If there exists a $D_4^{\frac{a_i a_j}{c}, \frac{1}{c}}$-extension K of F, then c equals 1 or $a_i a_j$.
Proof: Consider the following diagram of a $D_4^{\frac{a_i a_j}{c}, \frac{1}{c}}$-extension K of F. Without loss generality, let $\frac{a_i a_j}{c} = \alpha$, $\frac{1}{c} = \beta$.



We can write $c = a_1^{\epsilon_1} ... a_5^{\epsilon_5}$. We will show that $\epsilon_t = 0$ for $t \neq i, j$. If $\epsilon_t = 1$ let $\bar{\sigma}_t$ be the restriction of σ_t to the $D_4^{\alpha,\beta}$-extension K of F, and let K_{σ_t} be the fixed field of $\bar{\sigma}_t$. Now we have

$$\bar{\sigma}_t(\sqrt{\beta}) = -\sqrt{\beta} \quad , \quad \bar{\sigma}_t(\sqrt{\alpha}) = -\sqrt{\alpha}$$

So $\sqrt{\alpha},\ \sqrt{\beta} \notin K_{\sigma_t}$
All five intermediate fields of index 2 in the above diagram contain $\sqrt{\alpha}$ or $\sqrt{\beta}$. So K_{σ_t} can not be any of the five intermediate fields of index 2 in this diagram. Thus, it should be $F(\sqrt{\alpha\beta})$. On the other hand $Gal(K/F(\sqrt{\alpha\beta})) \cong C_4$. But $\langle \sigma_t \rangle \cong C_2$, and this is a contradiction.

Now we show $\epsilon_i, \epsilon_j = 1$. If $\epsilon_i = 1$, $\epsilon_j = 0$, let $\tau = \overline{\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5}$ be the restriction of $\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5$ to the field K. We have

$$\tau(\sqrt{\alpha}) = -\sqrt{\alpha} \quad , \quad \tau(\sqrt{\beta}) = -\sqrt{\beta}.$$

Let K_τ be the fixed field of τ. Then $\sqrt{\alpha}\,, \sqrt{\beta} \notin K_\tau$, so K_τ can not be any of the five intermediate fields of index 2 in diagram, since $\tau^2 = (\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5)^2 \cong C_2$, which would create a contradiction. In the same way if $\epsilon_i = 0, \epsilon_j = 1$ we will also get a contradiction, so c should be a_ia_j or 1.□

Proof of Lemma 3.5: Now let $a_1a_2a_3a_4a_5 = a$. Consider two forms $f = \langle 1, aa_5, aa_4\rangle$ and $g = \langle aa_3, a_1a_3, a_2a_3\rangle$. We have

$$\sigma_1(f) = \sigma_1(1) + \sigma_1(aa_5) + \sigma_1(aa_4) = -1$$
$$\sigma_1(g) = \sigma_1(aa_3) + \sigma_1(a_1a_3) + \sigma_1(a_2a_3) = -1$$
$$\Longrightarrow \sigma_1(f) = \sigma_1(g).$$

It is easy to check that $\forall\sigma \in X_F\ \sigma(f) = \sigma(g)$ therefore $sig(f) = sig(g)$, so $f \cong g$. Then $aa_3 \in D_f$. We can conclude that:

$$\exists W, Y, Z \in F \text{ such that } W^2 + aa_5Y^2 + aa_4Z^2 = aa_3$$
$$W^2 + \underbrace{(aa_5\frac{Y^2}{Z^2} + aa_4)}_{b} Z^2 = aa_3$$

So we have these relations:

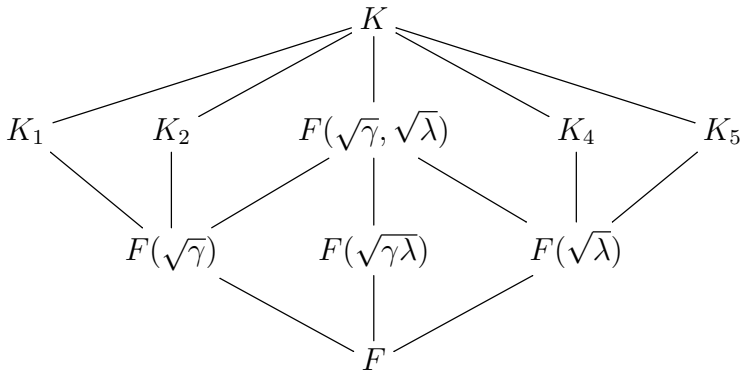
$$bZ^2 + W^2 = aa_3 \tag{3.1}$$

$$aa_5\frac{Y^2}{Z^2} + aa_4 = b \tag{3.2}$$

$$\frac{aa_5}{b}\frac{Y^2}{Z^2} + \frac{aa_4}{b} = 1 \tag{3.3}$$

Let $\gamma = \frac{aa_5}{b}, \lambda = \frac{aa_4}{b}$. By Theorem 1.10 there exists a $D_4^{\gamma,\lambda}$-extension K of F. Consider the following diagram and compare this diagram with the diagram in claim 1 (take $a_i = a_4, a_j = a_5$ in that diagram). If we consider

$$\gamma = \frac{aa_4}{b} = 1/c \text{ then } \lambda = \frac{aa_5}{b} = \frac{aa_4 \times a_4a_5}{b} = \frac{a_4a_5}{c} \mod F^2$$



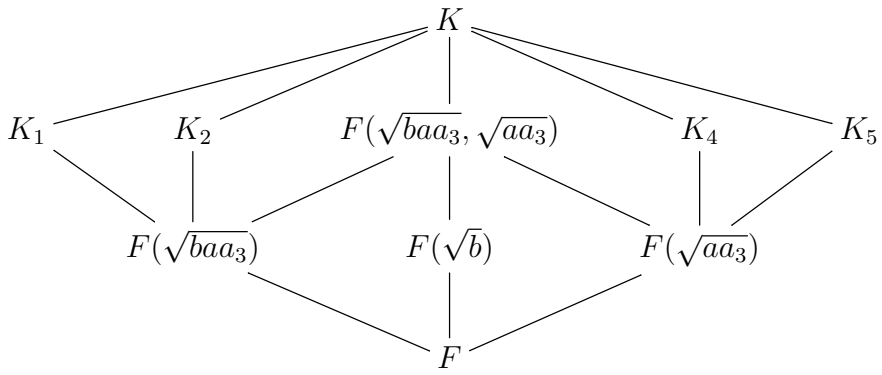
But in the above claim we proved $c = 1$ or $c = a_4a_5$. Then

$$c = 1 \Longrightarrow \frac{aa_4}{b} = 1 \text{ then } b = aa_4$$
$$c = a_4a_5 \Longrightarrow \frac{aa_5}{b} = 1 \text{ then } b = aa_5.$$

Now consider the $D_4^{baa_3,aa_3}$-extension K of F. This extension exists since by relation (3.1):

$$bZ^2 + W^2 = aa_3 \Longrightarrow \frac{b}{aa_3}Z^2 + \frac{1}{aa_3}W^2 = 1.$$

Consider the following diagram of this extension:



If $b = aa_5$, let $\bar{\sigma_5}$ be the restriction of σ_5 to the extension K, and K_{σ_5} be the fixed field of $\bar{\sigma_5}$:

$$\bar{\sigma_5}(\sqrt{baa_3}) = \bar{\sigma_5}(\sqrt{a_3a_5}) = -\sqrt{a_3a_5} \quad , \quad \bar{\sigma_5}(\sqrt{aa_3}) = -\sqrt{aa_3}$$

$$\Longrightarrow \sqrt{baa_3}, \quad \sqrt{aa_3} \notin K_{\sigma_5}.$$

Therefore, K_{σ_5} cannot be any of the five intermediate fields of index 2 in this diagram. Then it should be $F(\sqrt{b})$. But we know $Gal(K/F(\sqrt{b})) \cong C_4$ in the last dihedral diagram, whereas $\langle \sigma_5 \rangle \cong C_2$. This is a contradiction. In the case of $b = aa_4$, take σ_4 in a similar way we will also get contradiction. So the group

$$\langle \sigma_1, ..., \sigma_5 | (\sigma_i)^2 = (\sigma_1 \cdots \sigma_5)^2 = 1 \ i = 1, ..., 5 \rangle$$

cannot be a W-group of any Pythagorean formally real field F.$\square$

We will use the last theorem to show that the translation group $T = Z(Gal(F^{(3)}/F(\sqrt{-1}))/\Phi_F$ is a nontrivial set. The translation group T is exactly the set of all elements α of $Gal(F^{(3)}/F(\sqrt{-1})) =< \sigma_i\sigma_j | \sigma_i, \sigma_j \in X_F >$ which have the property $\alpha X_F = X_F$. First we need to prove some lemmas leading to Theorem 3.1.15.

In the next lemma we call an extension L/F quadratic if the degree of L over F is at most 2.

Lemma 3.6. *The set of all quadratic extensions $F(\sqrt{a})$ of field F where $a \in \dot{F}/\dot{F}^2$ form a vector space over $\mathbb{F}_2$.*

Proof: By Kummer theory there is a one-to-one correspondence between the set of all quadratic extensions $F(\sqrt{a})$ of F and group $\dot{F}/\dot{F}^2$ such that $F(\sqrt{a}) \longleftrightarrow [a]$. We can define addition of two elements $F(\sqrt{a_1})$ and $F(\sqrt{a_2})$ of this vector space: $F(\sqrt{a_1}) \oplus F(\sqrt{a_2}) = F(\sqrt{a_1 a_2})$.$\square$

Recall that $F^{(2)}$ is the compositum of all quadratic extensions of F. We use Kummer theory, see ([AT], Chapter 6, Section 2). We see that there is a one-to-one correspondence between the finite dimensional vector subspaces $A \subset \dot{F}/\dot{F}^2$ and finite extensions K/F, $F \subset K \subset F^{(2)}$ where $[K : F] = 2^s < \infty$. The correspondence is :

$$A \longrightarrow F(\sqrt{A}),$$

here $F(\sqrt{A})$ means the compositum of all quadratic extensions $F(\sqrt{a})$, $a \in A$.

Theorem 3.7. *Suppose σ is an element of $\mathcal{G}_F$, $\sigma \neq 1$ which satisfies this property:*

$$\textit{if } \sigma(\sqrt{a}) = \sqrt{a} \quad \textit{then } \sigma(\sqrt{1+a}) = \sqrt{1+a}).$$

Then $\sigma \in X_F$.

Proof: Let $P_\sigma = \{a \in \dot{F}/\dot{F}^2 : \sigma(\sqrt{a}) = \sqrt{a}\}$. Since $\sigma(\sqrt{1}) = \sqrt{1}$, for any a, b in P_σ, $\sigma(\sqrt{1/a}) = \sqrt{1/a}$ and $\sigma(\sqrt{b/a}) = \sqrt{b/a}$, so $\sigma(\sqrt{1+b/a}) = \sqrt{1+b/a}$. Therefore

$$\sigma(\sqrt{a+b}) = \sigma(\sqrt{a(1+b/a)}) = \sigma(\sqrt{a})\sigma(\sqrt{1+b/a}) = \sqrt{a}\sqrt{1+b/a} = \sqrt{a+b}.$$

So $P_\sigma + P_\sigma \subseteq P_\sigma$, and it is easy to check the other conditions of an ordering. But by Theorem 1.0.16, any ordering P_σ of field F corresponds to the non-simple involution σ of $\mathcal{G}_F$, therefore $\sigma \in X_F$.$\square$

Now we apply Lemma 4.2 in [M1] for the space of ordering X_F. We have:

Lemma 3.8. *Suppose* $\{\sigma_1, ..., \sigma_n\}$ *is a basis for* X_F*, and* $\alpha \in \mathcal{G}_F$ *such that* $\sigma_i\alpha \in X_F$ *for* $i = 1...n$*. Then* $\alpha X_F = X_F$*.*

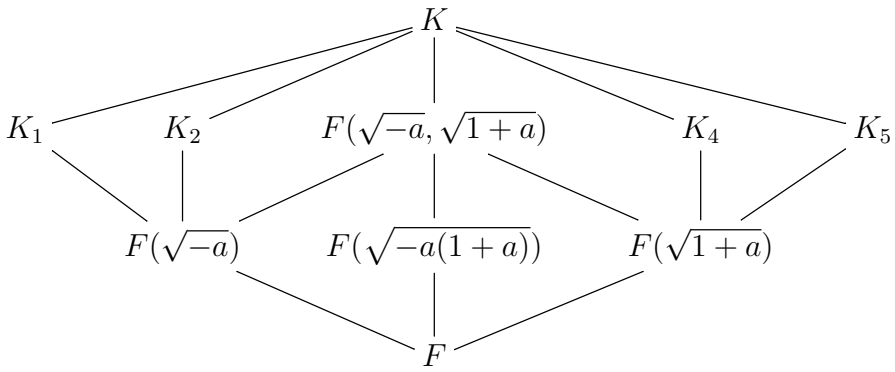
Proof: We will follow here the main idea of the proof of Lemma 4.2 of [M1], but we do it from a Galois point of view. Since $\sigma_1, \sigma_1\alpha \in X_F$, $\sigma_1(\sqrt{-1}) = \sigma_1\alpha(\sqrt{-1}) = -\sqrt{-1}$, so $\alpha(\sqrt{-1}) = \sqrt{-1}$. We wish to show that if $\sigma \in X_F$, then $\sigma\alpha \in X_F$. By the last theorem if $\sigma \in \mathcal{G}_F/\Phi_F$ satisfies this condition:

$$\sigma(\sqrt{a}) = \sqrt{a} \text{ then } \sigma(\sqrt{1+a}) = \sqrt{1+a}$$

then $\sigma \in X_F$.Therefore it is enough to show that $\sigma\alpha(\sqrt{a}) = \sqrt{a}$ implies $\sigma\alpha(\sqrt{1+a}) = \sqrt{1+a}$.

We assume $a+1$ and a are independent modulo squares, since otherwise we are done.

Claim: We show that if $\sigma \in X_F$ and $\sigma(\sqrt{a}) = \sqrt{a}$, then $\sigma(\sqrt{1+a}) = \sqrt{1+a}$.
Consider the $D_4^{-a,1+a}$-extension, K/F, (This extension exists since $-a, 1+a$ are independent modulo squares, and $\langle -a, 1+a\rangle = 1$). Consider dihedral diagram



Let K_σ be the fixed field of restriction σ to K. If

$$\sigma(\sqrt{1+a}) \neq \sqrt{1+a}, \text{ then } \sqrt{1+a} \notin K_\sigma \text{ and } \sigma(\sqrt{-a}) = -\sqrt{-a} \text{ then } \sqrt{-a} \notin K_\sigma.$$

So K_σ is not any of the five intermediate fields of index 2 in the diagram of the $D_4^{-a,1+a}$-extension K of F. Therefore, it is equal to $F(\sqrt{-a(1+a)})$. But

$$Gal(K/F(\sqrt{-a(1+a)})) = C_4 \text{ and } \langle\sigma\rangle = C_2.$$

This is a contradiction. Then $\sigma(\sqrt{1+a}) = \sqrt{1+a}$.

There are three cases to consider:

Case 1. $\alpha(\sqrt{a}) = -\sqrt{a}$. For each σ_i we have $\sigma_i\alpha(\sqrt{a}) = \sigma_i(-\sqrt{a}) = -\sigma_i(\sqrt{a})$. Define for any $\tau \in Gal(F^{(2)}/F)$, K_τ the fixed field of τ, and denote for any $\tau \in \mathcal{G}_F$ its restriction to $F^{(2)}$ by $\bar{\tau}$. Because of $\sigma_i\alpha(\sqrt{a}) = \sigma_i(-\sqrt{a}) = -\sigma_i(\sqrt{a})$ we see that: $\sqrt{a} \in K_{\sigma_i}$ or $K_{\sigma_i\alpha}$. This means for each $i = 1, ..., n$ we can choose $\varepsilon_i \in \{0, 1\}$ such that $\sqrt{a} \in K_{\sigma_i\alpha^{\varepsilon_i}}$. Consider now the set $W := \{\sigma_1\alpha^{\varepsilon_1}, ..., \sigma_n\alpha^{\varepsilon_n}\}$ as a subset of $Gal(F^{(2)}/F) = \prod_1^n C_2$. Let V be the smallest vector space over $\mathbb{F}_2$ containing W. We claim that $\dim_{\mathbb{F}_2} V \leq n-1$. Indeed $V \cup \{\alpha\}$ spans $Gal(F^{(2)}/F) = \prod_{i=1}^n \langle\sigma_i\rangle$ and $\dim_{\mathbb{F}_2} Gal(F^{(2)}/F) = n$.

Consider now the field Ł := $\bigcap K_{\sigma_i\alpha^{\varepsilon_i}}$, $i = 1, ..., n$. Then $Gal(F^{(2)}/L) = V$. Indeed since each $\sigma_i\alpha^{\epsilon_i}$, $i = 1, ..., n$ fixes L we see that $V \subset Gal(F^{(2)}/L)$. Therefore the fixed field of V is exactly L as each element $k \in F^{(2)}$ which is fixed by V is fixed by all $\sigma_i\alpha^{\epsilon_i}$, $i = 1, ..., n$ and hence $k \in L$. We have:

$$2^n = [F^{(2)} : F] = [F^{(2)} : L][L : F].$$

By Galois theory $[F^{(2)} : L] = |V|$. But $|V| \leq 2^{n-1}$ and we can conclude that $[L : F] \leq 2$. Now use our assumption that $\sigma_i\alpha \in X_F$, $i = 1, ..., n$. By the last claim we see that $\sqrt{1+a} \in K^{\sigma_i\alpha^{\epsilon_i}}$ for each $i = 1, ..., n$. Hence we see that $\sqrt{a}$ and $\sqrt{1+a} \in L$. Because $\alpha(\sqrt{a}) = -\sqrt{a}$ we see that $\sqrt{a} \notin F$ and hence $L = F(\sqrt{a})$. Now by Lemma 3.6 we see that:

$$[1 + a] = 1 \text{ or } [1 + a] = [a], \text{ in } \dot{F}/\dot{F}^2.$$

But we assumed $\sigma\alpha(\sqrt{a}) = \sqrt{a}$, so $\sigma\alpha(\sqrt{1+a}) = \sqrt{1+a}$. Now by Theorem 3.7 $\sigma\alpha \in X_F$.

Case 2. Suppose $\alpha(\sqrt{1+a}) = -\sqrt{1+a}$ and $\alpha(\sqrt{-1}) = \sqrt{-1}$. Then $\alpha(\sqrt{-(1+a)} = -\sqrt{-(1+a)}$. Let $-(1+a) = t$, so $\alpha(\sqrt{t}) = -\sqrt{t}$. Apply the argument of case (1) here. Then in vector space $\dot{F}/\dot{F}^2$, $[1 + t] = 1$ or $[1 + t] = [t]$. Thus

$$[-a] = [1] \text{ or } [-a] = [-(1 + a)].$$

But $\sigma\alpha(\sqrt{a}) = \sqrt{a}$ and $\sigma\alpha(\sqrt{-1}) = -\sqrt{-1}$, so $[-a] \neq [1]$. Therefore $[a] = [1 + a]$, so $\sigma\alpha(\sqrt{1+a}) = \sqrt{1+a}$. Again by theorem 3.7, $\sigma\alpha \in X_F$.

Case 3. Suppose $\alpha(\sqrt{a}) = \sqrt{a}$ and $\alpha(\sqrt{1+a}) = \sqrt{1+a}$. If $\sigma\alpha(\sqrt{a}) = \sqrt{a}$ then $\sigma(\sqrt{a}) = \sqrt{a}$. But we show in claim 1 that $\sigma(\sqrt{1+a}) = \sqrt{1+a}$. On the other hand we assumed $\alpha(\sqrt{1+a}) = \sqrt{1+a}$, so $\sigma\alpha(\sqrt{1+a}) = \sqrt{1+a}$, and therefore by the

last theorem $\sigma\alpha \in X_F$.$\square$

Now we are going to prove that if X_F is connected, then the translation group $T = Gal(F^{(3)}/F(\sqrt{-1}))$ is a nontrivial set modulo Φ_F. For any $\alpha \in \mathcal{G}_F$, let $X_\alpha = \{\sigma \in X_F \,|\, \sigma\alpha \in X_F\} = X_F \cap \alpha X$. It is easy to show that $\alpha X_\alpha = X_\alpha$. Then we can show that the partially ordered set $\mathcal{X} = \{X_\alpha \subset X_F | \alpha \in \mathcal{G}_F\}$ has a maximal element which is $X_\tau = X_F$ for some τ. Then $\tau X_F = X_F$, and $\tau \in T$ as we claimed.

Lemma 3.9. *(4.4, [M1]) Suppose $\{\sigma_1, ..., \sigma_n\}$ is a basis of X_F, and $\sigma_1, \sigma_1\alpha, \sigma_1\beta, \sigma_1\alpha\beta$ are four different elements of X_F. Then $X_\alpha \subseteq X_\beta$ or $X_\beta \subseteq X_\alpha$.*

Proof: M. Marshal proved this lemma for general spaces of orderings. We recall his proof (Lemma 4.4 in [M1]) for X_F instead of a general space of orderings.

First of all α and β should be the product of even number of elements of basis. If they are the product of odd number of σ_i, $i = 1, ..., n$, then $\sigma_1\alpha$ and $\sigma_1\beta$ are product of even orderings and they cannot be in X_F. Also we assumed σ_1, $\sigma_1\alpha$, $\sigma_1\beta$ and $\sigma_1\alpha\beta$ are different elements of X_F, so α, β and $\alpha\beta$ are not in Φ_F.

Suppose $X_\alpha \nsubseteq X_\beta$ and $X_\beta \nsubseteq X_\alpha$. Then there are two elements σ_2, σ_3 such that $\sigma_2 \in X_\alpha - X_\beta$, $\sigma_3 \in X_\beta - X_\alpha$. So $\sigma_2\alpha$ and $\sigma_3\beta$ are in X_F
Consider these elements of $\mathcal{G}_F$:

$$\begin{array}{cccc} \sigma_1 & \sigma_2 & \sigma_3 & \sigma_1\sigma_2\sigma_3 \\ \sigma_1\alpha & \sigma_2\alpha & \sigma_3\alpha & \sigma_1\sigma_2\sigma_3\alpha \\ \sigma_1\beta & \sigma_2\beta & \sigma_3\beta & \sigma_1\sigma_2\sigma_3\beta \\ \sigma_1\alpha\beta & \sigma_2\alpha\beta & \sigma_3\alpha\beta & \sigma_1\sigma_2\sigma_3\alpha\beta \end{array}$$

As we assumed, all the elements in the first column are in X_F. By assumption, σ_2, $\sigma_2\alpha \in X_F$ and $\sigma_2\beta \notin X_F$. If $\sigma_2\alpha\beta \in X_F$, then let $\gamma = \sigma_1\sigma_2\alpha \in \mathcal{G}_F$. We can write

$$\sigma_1\gamma = \sigma_2\alpha, \quad \sigma_2\gamma = \sigma_2\sigma_1\sigma_2\alpha = [\sigma_2, \sigma_1]\sigma_1\alpha \quad \sigma_1\alpha\gamma = \sigma_2 \quad \sigma_1\beta\gamma = \sigma_2\alpha\beta$$

But as we mentioned in the beginning of this chapter $X_F = \{\sigma\Phi_F | \sigma^2 = 1, \sigma \notin \Phi_F\}$, so we work modulo the Frattini subgroup Φ_F. Thus $\sigma_2\gamma = \sigma_2\sigma_1\sigma_2\alpha = [\sigma_2, \sigma_1]\sigma_1\alpha = \sigma_1\alpha$ to mod Φ_F. By an assumption $\sigma_1\alpha \in X_F$, until now the product of four elements σ_1, $\sigma_2, \sigma_1\alpha$, $\sigma_1\beta$ in γ, are elements of X_F. Apply Lemma 3.8 to the subspace of X_F which is generated by four elements σ_1, $\sigma_2, \sigma_1\alpha$, $\sigma_1\beta$, so the product of γ to any ordering which is generated by this four elements should be in X_F. Hence $(\sigma_1\alpha\beta)\gamma = \sigma_2\beta \in X_F$; this is a contradiction with a assumption on σ_2. Thus $\sigma_2\alpha\beta \notin X_F$, and by the same argument we can show that $\sigma_3\alpha\beta$, $\sigma_1\sigma_2\sigma_3\alpha$, $\sigma_1\sigma_2\sigma_3\beta \notin X_F$.

Now consider these elements of X_F: $\sigma_1\alpha$, $\sigma_1\beta$, σ_2, $\sigma_2\alpha$, σ_3. First we show that these elements are independent mod Φ_F. By the assumption we see that the set $A = \{\sigma_1, \sigma_1\alpha, \sigma_1\beta, \sigma_1\alpha\beta\}$ is generated by three independent elements σ_1, α, β mod Φ_F. All elements in A are in $X_\alpha \cap X_\beta$, but $\sigma_2, \sigma_3 \notin X_\alpha \cap X_\beta$, so the space of orderings generated by $A \cup \{\sigma_2\}$ has dimension 4. By the definition of σ_2 these elements $\sigma_2, \sigma_2\alpha, \sigma_2\beta, \sigma_2\alpha\beta$ are in X_α, but $\sigma_3 \notin X_\alpha$ so the dimension of space of orderings generated by $A \cup \{\sigma_2\} \cup \sigma_3$ is 5. Consider the set $B = \langle\sigma_1\alpha, \sigma_1\beta, \sigma_2, \sigma_2\alpha, \sigma_3\rangle$. Since $\sigma_1 = (\sigma_1\alpha)(\sigma_2\alpha)\sigma_2$, we have $B = \langle\sigma_1, \sigma_2, \alpha, \beta, \sigma_3\rangle = A \cup \{\sigma_2\} \cup \sigma_3$. Hence the five elements $\sigma_1\alpha$, $\sigma_1\beta$, σ_2, $\sigma_2\alpha$, σ_3 are independent. But

$$\begin{aligned}(\sigma_1\alpha)(\sigma_1\beta)(\sigma_2)(\sigma_2\alpha)(\sigma_3) &= \sigma_1\alpha\sigma_1\beta\alpha\sigma_3 \\ &= [\sigma_1, \alpha][\alpha, \beta]\beta^{-1}\sigma_3 = \beta\sigma_3.\end{aligned}$$

Therefore $(\sigma_1\alpha)(\sigma_1\beta)(\sigma_2)(\sigma_2\alpha)(\sigma_3) = \beta\sigma_3$ mod Φ_F. But we supposed $\sigma_3 \in X_\beta$. So

$\beta\sigma_3 \in X_F$. Now we have five involution elements, whose product is again an involution.

As we proved in Lemma 3.5 $\langle \sigma_1\alpha,\ \sigma_1\beta, \sigma_2, \sigma_2\alpha, \sigma_3, (\sigma_1\alpha\sigma_1\beta\sigma_2\sigma_2\alpha\sigma_3)\rangle$ cannot be a space of orderings of any Pythagorean formally real field. This is a contradiction. Then $X_\alpha \subseteq X_\beta$ or $X_\beta \subseteq X_\alpha$.□

Lemma 3.10. *(4.5 [M1]) Suppose rank X_α and rank $X_\beta \geqslant 3$. Then either $X_\alpha \cap X_\beta = \emptyset$ or $|X_\alpha \cap X_\beta| \geqslant 2$.*

Proof: We recall the proof of Theorem 4.5 in [M1]. Suppose our claim is false i.e $X_\alpha \cap X_\beta \neq \emptyset$ and $X_\alpha \cap X_\beta = \{\sigma_1\}$, so $\sigma_1\alpha, \sigma_1\beta \in X_F$. Then $X_\alpha \nsubseteq X_\beta$ and $X_\beta \nsubseteq X_\alpha$ otherwise $|X_\alpha \cap X_\beta| \geqslant 2$, so there exist $\sigma_2 \in X_\alpha - X_\beta$ such that $\sigma_2 \neq \sigma_1\alpha$. If $\sigma_1\alpha$ is the only element of $X_\alpha - X_\beta$ then X_α would have a basis in X_β, and then by Lemma 3.9 $X_\alpha \subset X_\beta$, this is a contradiction. With the same argument we show that there exist $\sigma_3 \in X_\beta - X_\alpha$ such that $\sigma_3 \neq \sigma_1\beta$

Again consider the set of elements of $\mathcal{G}_F$ in the last lemma, $\sigma_1, \sigma_1\alpha, \sigma_1\beta \in X_F$. If $\sigma_1\alpha\beta \in X_F$, then $X_\alpha \subset X_\beta$ or $X_\beta \subset X_\alpha$ so $\sigma_1\alpha\beta \notin X_F$. Also $\sigma_2, \sigma_2\alpha \in X_F$. If $\sigma_2\alpha\beta \in X_F$, then $\sigma_2\alpha \in X_\alpha \cap X_\beta, \sigma_2\alpha \neq \sigma_1$, but this is a contradiction with $X_\alpha \cap X_\beta = \{\sigma_1\}$, so $\sigma_2\alpha\beta \notin X_F$. With the same argument used in the last lemma we can show that the group generated by these five elements $\sigma_1\alpha, \sigma_1\beta, \sigma_2, \sigma_2\alpha, \sigma_3$ and their product cannot be a subgroup of $\mathcal{G}_F$. Therefore our assumption is wrong , so $|X_\alpha \cap X_\beta| \geqslant 2$.□

If we apply Lemma 4.6 in [M1] for the space of orderings X_F. Then we have:

Lemma 3.11. *Suppose $\alpha, \beta \neq 1$, $X_\alpha \cap X_\beta \neq \emptyset$ and rank X_α and rank $X_\beta \geq 3$. Then there exist $\gamma \in Gal(F^{(3)}/F(\sqrt{-1}))$ such that $X_\alpha, X_\beta \subseteq X_\gamma$.*

Proof: Recall the proof Lemma 4.6 in [M1]. If $X_\alpha \subseteq X_\beta$ or $X_\beta \subseteq X_\alpha$, then there is nothing to prove. If $X_\alpha \nsubseteq X_\beta$ and $X_\beta \nsubseteq X_\alpha$ then by the last lemma $|X_\alpha \cap X_\beta| \geq 2$. Therefore there exist $\sigma_1, \sigma_2 \in X_\alpha \cap X_\beta$ such that $\sigma_1 \neq \sigma_2$. Let $\gamma = \sigma_1\sigma_2$ and consider these four elements of X_F:

$$\sigma_1,\ \sigma_1\alpha,\ \sigma_1\gamma = \sigma_1\sigma_1\sigma_2 = \sigma_2, \quad \sigma_1\gamma\alpha = \sigma_1\sigma_1\sigma_2\alpha = \sigma_2\alpha.$$

Now by Lemma 3.1.9 $X_\alpha \subseteq X_\gamma$ or $X_\gamma \subseteq X_\alpha$ (I) . But

$$\sigma_1\beta\gamma = \sigma_1\beta\sigma_1\sigma_2 = \underbrace{\sigma_1\beta\sigma_1\beta}_{1}\beta^{-1}\sigma_2 = \beta^{-1}\sigma_2 = (\sigma_2\beta)^{-1}. \quad \text{(II)}$$

We know from the assumption $\sigma_2\beta \in X_F$ that $\sigma_2\beta$ is an involution. Then $\sigma_2\beta = (\sigma_2\beta)^{-1} \in X_F$. Therefore by equation (II), $\sigma_1\beta \in X_\gamma$.

On the other hand $\sigma_1\beta\alpha \notin X_F$. If $\sigma_1\beta\alpha \in X_F$, by assumption we know that σ_1 , $\sigma_1\alpha$, $\sigma_1\beta \in X_F$, and then by Lemma 3.1.9 $X_\alpha \subseteq X_\beta$ or $X_\beta \subseteq X_\alpha$ so we are done. Therefore $\sigma_1\beta\alpha \notin X_F$, so $\sigma_1\beta \notin X_\alpha$. Now by (I) we can conclude that $X_\alpha \subseteq X_\gamma$. In the same way we can show that $X_\beta \subseteq X_\gamma$.□

Following [M1] page 323, we define the connected relation:

Definition 3.12. *Two orderings σ and σ' are simply connected in X_F (denoted $\sigma \sim_s \sigma'$) if there exist orderings $\tau, \tau' \in X_F$, $\{\sigma, \sigma'\} \neq \{\tau, \tau'\}$ such that $\sigma\sigma' = \tau\tau'$. Two orderings σ, σ' are connected in X_F (denoted $\sigma \sim \sigma'$) if either $\sigma = \sigma'$ or there exists a sequence of orderings $\sigma = \sigma_0, \sigma_1, ..., \sigma_k = \sigma'$ in X_F such that $\sigma_{i-1} \sim_s \sigma_i$ for $i = 1, ..., k$.*

Let $X_F = X_1 \cup ... \cup X_k$ denote the decomposition of X_F determined by the above equivalence relation. According to M. Marshal we call X_i, $i = 1, ..., k$, the connected components of X_F. For any formally real field F the space of orderings X_F is connected if it has just one connected component. As we see, if the nontrivial

ordering space X_F is connected, then the minimum number of orderings should be 4. Let $X_F = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ is connected space, without loss generality we can assume $\sigma_1\sigma_2\sigma_3 = \sigma_4$. Therefore X_F has three independent orderings and $|\dot{F}/\dot{F}^2| = 2^3$, $|X_F| = 4$. Hence F is a fan case. So by abuse of the language we can say the smallest connected ordering space is a fan case with 4 elements.

Now apply decomposition theorem in [M1] for X_F.

Theorem 3.13. *Suppose $X_1, ..., X_k$ are the connected components of X_F. Then each X_i is a subspace of X_F and rank $X_F = \sum_1^k$ rank X_i.*

Proof: See proof of decomposition theorem in [M1].
We can conclude by Theorem 4.10 in [M1] that for any ordering space X_i there exists a Pythagorean formally real field F_i such that space of ordering X_{F_i} of F corresponds to X_i.

Theorem 3.14. *If X_F is connected space of Pythagorean formally real field F and rank $X_F \neq 1$ then there exists $\alpha \in Gal(F^{(3)}/F(\sqrt{-1}))$, $\alpha \neq 1$ such that $\alpha X_F = X_F$.*

Proof: We recall the proof of Theorem 4.7 in [M1] for X_F. We assumed rank $X_F \neq 1$, so there exist $\sigma_1, \sigma_2 \in X_F$ such that $\sigma_1 \neq \sigma_2$. Because $\alpha = \sigma_1\sigma_2$ would fix $F(\sqrt{-1})$, so $\alpha = \sigma_1\sigma_2 \in Gal(F^{(3)}/F(\sqrt{-1}))$. Now

$$\sigma_1\alpha = \sigma_1\sigma_1\sigma_2 = \sigma_2 \in X_F \Longrightarrow \sigma_1 \in X_\alpha$$

$$\sigma_2\alpha^{-1} = \sigma_2(\sigma_1\sigma_2)^{-1} = \sigma_1 \in X_F \qquad (\alpha\sigma_2)^{-1} = \sigma_2\alpha \in X_F \bmod \Phi_F.$$

So $\sigma_2 \in X_\alpha$. X_F is connected so there are two other involutions, σ_3, σ_4 such that $\sigma_1\sigma_2\sigma_3 = \sigma_4$. Then $\alpha\sigma_3 = \sigma_4 \in X_F$, so $\sigma_3 \in X_\alpha$, and rank $X_\alpha \geq 3$. Consider one such X_α, which is maximal in the set $\{X_\alpha \,|\, \alpha \in Gal(F^{(3)}/F(\sqrt{-1}))\}$. If $X_\alpha = X_F$,

we are done. If $X_\alpha \neq X_F$ then we can find $\sigma_i, \sigma_j \in X_F$ such that $\sigma_i \in X_\alpha, \sigma_j \notin X_\alpha$. Now let $\beta = \sigma_i\sigma_j$

$$\sigma_i \in X_\alpha \,,\, \sigma_i\beta = \sigma_i\sigma_i\sigma_j = \sigma_j \in X_F \Longrightarrow \sigma_i \in X_\beta \Longrightarrow \sigma_i \in X_\alpha \cap X_\beta. \tag{3.4}$$

X_F is connected, so there are two other involutions σ_n, σ_m such that $\sigma_i, \sigma_j, \sigma_n, \sigma_m \in X_F$ and $\sigma_m\sigma_i\sigma_j = \sigma_n$ so $\sigma_m \in X_\beta$. On the other hand:

$$\sigma_j\beta = \sigma_j\sigma_i\sigma_j = \sigma_i[\sigma_i, \sigma_j] = \sigma_i \bmod \Phi_F.$$

So $\sigma_j\beta \in X_F$, then $\sigma_j \in X_\beta$, rank $X_\beta \geq 3$. By relation (3.4), $X_\alpha \cap X_\beta \neq \emptyset$. Therefore by the Lemma 3.1.11, there exists an element $\gamma \in Gal(F^{(3)}/F(\sqrt{-1}))$ such that $X_\alpha, X_\beta \subseteq X_\gamma$. But $\sigma_j \notin X_\alpha$ and $\sigma_j \in X_\beta \subseteq X_\gamma$, so X_γ can not be equal to X_α, hence it contains X_α properly, but this is a contradiction, because X_α was maximal. Therefore $X_\alpha = X_F$, so $\alpha X_F = X_F$.□

The following theorem can be detected from section 6, [EM2] in a very different way.

Theorem 3.15. *If X_F is a connected space of a Pythagorean formally real field F, then $Gal(F^{(3)}/F(\sqrt{-1}))$ has nontrivial center modulo Frattini subgroup.*

Proof: Let $|X_F| = n$. By the last theorem there exists an element $\tau = \sigma_1\sigma_2 \in Gal(F^{(3)}/F(\sqrt{-1}))$ such that $\tau X_F = X_F$. Therefore for any $\sigma_i \in X_F, \tau\sigma_i = \sigma_{k(i)}$, $k(i) \in \{1, ..., n\}$. Let:

$$\begin{aligned} \tau\sigma_i = \sigma_m \quad , \quad \tau\sigma_j = \sigma_n \qquad\qquad (I) \\ \Longrightarrow \sigma_1\sigma_2\sigma_i = \sigma_m \Longrightarrow \sigma_i = \sigma_i^{-1} = \sigma_2\sigma_1\sigma_m \\ \sigma_1\sigma_2\sigma_j = \sigma_n \Longrightarrow \sigma_j = \sigma_j^{-1} = \sigma_2\sigma_1\sigma_n. \end{aligned}$$

Now for any element $\gamma = \sigma_i\sigma_j \in Gal(F^{(3)}/F(\sqrt{-1}))$

$$\begin{aligned}
\tau\sigma_i\sigma_j\tau^{-1}\sigma_j\sigma_i &= \sigma_m\sigma_n \underbrace{\sigma_j}_{\sigma_2\sigma_1\sigma_n}\underbrace{\sigma_i}_{\sigma_2\sigma_1\sigma_m} \quad by\,(I)\\
&= \sigma_m\sigma_n\sigma_2\sigma_1\sigma_n\sigma_2\sigma_1\sigma_m\\
&= \sigma_m\sigma_n[\sigma_1,\sigma_n][\sigma_2,\sigma_n][\sigma_2,\sigma_1]\sigma_n\sigma_m\\
&= \sigma_m\sigma_n\sigma_n\sigma_m[\sigma_1,\sigma_n][\sigma_2,\sigma_n][\sigma_2,\sigma_1]\\
&= [\sigma_1,\sigma_n][\sigma_2,\sigma_n][\sigma_2,\sigma_1]\\
(\sigma_j = \sigma_2\sigma_1\sigma_n)^2 = 1 &\Longrightarrow [\sigma_1,\sigma_n][\sigma_2,\sigma_n][\sigma_2,\sigma_1] = 1\\
\Longrightarrow \tau\sigma_i\sigma_j &= \sigma_i\sigma_j\tau.
\end{aligned}$$

The last part is a conclusion of Example 3.3. Then τ is in the center of $Gal(F^{(3)}/F(\sqrt{-1}))$.□

Following [MS] page 1279, we recall an element $a \in \dot{F}$ is rigid if $D\langle 1, a\rangle = \dot{F}^2 \cup a\dot{F}^2$, or form $\langle 1, a\rangle$ represents as few element as possible. An element $a \in \dot{F}$ is called double-rigid if both a and $-a$ are rigid. In the case $|\dot{F}/\dot{F}^2| > 2$, $\mathrm{Bas}(F) = \{a \in \dot{F} \mid a \text{ is not double-rigid}\}$, so $\mathrm{Bas}(F)$ is a subgroup of $\dot{F}$. But since $\mathrm{Bas}(F)$ contains $\dot{F}^2$, we can consider $\mathrm{Bas}(F)$ as a subgroup of $\dot{F}/\dot{F}^2$. The next theorem is a generalization of Theorem 3.5 in [MS].

Theorem 3.16. *For any Pythagorean formally real field F consider X_F. If X_F is a connected ordering space of F, then $\mathcal{G}_F \cong \prod C_4 \rtimes \mathcal{G}_{\bar{F}}$, where $\bar{F}$ is the residue field of some 2-Henselian valuation on F. $\bar{F}$ is also a Pythagorean formally real field with a smaller number of orderings and the set of orderings $X_{\bar{F}}$ is disconnected. For a suitable set of generators σ_i, σ_{-1}, $\mathcal{G}_{\bar{F}}$ acts on $\prod C_4$ by:*

$$\sigma_i^{-1}\tau\sigma_i = \tau \quad \textit{(Here } \tau \textit{ is any element of the inner product of copies of } C_4\textit{)}$$

$$\sigma_{-1}^{-1}\tau\sigma_{-1} = \tau^3.$$

Proof. X_F is connected, so by the last theorem $Gal(F^{(3)}/F(\sqrt{-1}))$ has nontrivial center. We show that any element $\gamma = \sigma_i\sigma_j \in Gal(F^{(3)}/F(\sqrt{-1}))$ such that σ_i, σ_j are elements of the basis $\{\sigma_1, ..., \sigma_n\}$ has order 4. σ_i, σ_j are independent involutions mod Φ_F, so $\sigma_i\sigma_j \notin \Phi_F$. But if $(\sigma_i\sigma_j)^2 = 1$, then $\sigma_i\sigma_j$ is a non simple involution. So $\sigma_i\sigma_j(\sqrt{-1}) = -\sqrt{-1}$ but $\sigma_i\sigma_j(\sqrt{-1}) = \sigma_i(\sigma_j\sqrt{-1}) = \sigma_i(-\sqrt{-1}) = \sqrt{-1}$ which is a contradiction. So $\gamma = \sigma_i\sigma_j$ has order 4. Therefore the center of $Gal(F^{(3)}/F(\sqrt{-1}))$ is isomorphic to $\prod_1^m C_4$.

Let

$$H = \{\sigma \in \mathcal{G}_F \,|\, \sigma(\sqrt{-1}) = \sqrt{-1}\}.$$

Recall Theorem 1.18:

$$\sigma(\sqrt{b}) = \sqrt{b}\ \forall b \in Bas(F) \iff \sigma \in Z(H).$$

So

$$Z(H) = \{\sigma \in \mathcal{G}_F \,|\, \sigma(\sqrt{b}) = \sqrt{b}\ \forall b \in \mathrm{Bas}(F)\}.$$

Use the notation of Theorem 1.18. Then

$$Z(H) = \{\sigma \in \mathcal{G}_F \,|\, \sigma(\sqrt{b}) = \sqrt{b}\ \forall b \in \mathrm{Bas}(F)\} = \Delta_J.$$

On the other hand $H = Gal(F^{(3)}/F(\sqrt{-1}))$, so the center of $Gal(F^{(3)}/F(\sqrt{-1}))$ that was nontrivial and isomorphic to a product of copies of C_4 is equal to the set

$$\{\sigma \in \mathcal{G}_F \,|\, \sigma(\sqrt{b}) = \sqrt{b}\ \forall b \in \mathrm{Bas}(F)\} = \Delta_J.$$

Now let $E = F(\sqrt{a_i} \,|\, a_i \in Bas(F))$ be the fixed field of $Z(H)$. Consider $X' = \{\sigma|_E, \sigma \in X_F\}$. Any nontrivial element of X' would not fix Bas (F), so $X' = \{\sigma_{-1}, \sigma_i \,|\, i \in I'\}$. By Theorem 2.13 there exists a Pythagorean formally real field K

such that $(X', \frac{E}{E^2}) \sim (X_K, \dot{K}/\dot{K}^2)$. Because $\mathcal{G}_K$ is the W-group of the Pythagorean real field K, it is generated by $X_K = X'$. On the other hand by Theorem 1.0.27, $\mathcal{G}_F \cong \Delta_J \rtimes \mathcal{G}_K$ where K is the residue field of some 2-Henselian valuation on F. Therefore, $\mathcal{G}_F \cong \Delta_J \rtimes \mathcal{G}_{\bar{F}} \cong \prod C_4 \rtimes \mathcal{G}_{\bar{F}}$. Since F is Pythagorean formally real field then by Theorem 1.24 the residue field $\bar{F}$ of some 2-Henselian valuation on F is also Pythagorean formally real field.

We proved in the last theorem that $Z(H)$ is nontrivial, thus there exists at least one element $\gamma \in Z(H)$. $H = Gal(F^{(3)}/F(\sqrt{-1}))$, so $H = \langle \sigma_i\sigma_j \,|\, \sigma_i, \sigma_j \in X_F \rangle$. Hence $Z(H)$ is generated by this kind of pair $\gamma = \sigma_i\sigma_j$ where $\sigma_i, \sigma_j \in X_F$. If E is the fixed field of $Z(H)$, since $Z(H)$ has at least one element $\gamma = \sigma_i\sigma_j$, then $\sigma_i|_E = \sigma_j|_E$. Then the rank of $X_{\bar{F}}$ is less than the rank of X_F and X_F is a disconnected space (Remark 1, [M1]).□

Note that in this case, any $\sigma \in X_F$ can be written uniquely as a product $t\sigma'$ where $t \in T$, $\sigma' \in X_{\bar{F}}$. Then $|X_F| = |T||X_{\bar{F}}|$ and $|T| = 2^m$ where m is the dimension of T as F_2 vector space.

In Theorem 3.18 we will show that if the space of orderings X_F is disconnected space, then $\mathcal{G}_F$ is equal to the free product of $\mathcal{G}_{F_i}$ in the category $\mathcal{C}$, where $\mathcal{G}_{F_i}$ is the W-group of some Pythagorean field F_i. Then we can use Theorem 3.16 which has the main role in determining the structure of W-group of Pythagorean formally real field F. As we proved in this theorem $\bar{F}$ is again a Pythagorean formally real field and $X_{\bar{F}}$ is a disconnected space. So one can apply Theorem 3.18 to $\bar{F}$, and then apply Theorem 3.16 for any Pythagorean formally real field F_i which has connected ordering space X_{F_i}. In this way one can determine the structure of W-groups inductively. We will show directly in Example 3.20 and Example 3.23 how this process will work.

Lemma 3.17. *Let F be a Pythagorean formally real field, and a be an element of F which is not a square in F. Then*

$$D_F < 1, -a >= F^2 - aF^2 = \bigcap_{-a \in P} P.$$

Proof: Consider the trivial preordering $F^2 - a \notin -F^2$, so by (Lemma 1.2, [La2]) $F^2[-a]$ is preordering. Now use Artin's theorem (Theorem 1.6, [La2]). Therefore $F^2[-a] = \bigcap_{P \supseteq F^2[-a]} P$. But

$$F^2[-a] = F^2 - aF^2 = \{X^2 - aY^2 | X, Y \in F\} = D_F < 1, -a > .$$

For any ordering $P, F^2 \subseteq P$, so if $P \supseteq F^2[-a]$ then $-a \in P$ and therefore,

$$F^2[-a] = F^2 - aF^2 = \bigcap_{-a \in P} P. \square$$

Theorem 3.18. *Let $X_F = \{\sigma_1, ..., \sigma_n \,|\, \sigma_i^2 = 1,\ \sigma_i \notin \Phi_F\}$ and $X_F = \bigcup_{i=1}^{k} (X_i, \dot{F}/\dot{F}^2)$ where X_i are the connected components of X_F and $\mathcal{G}_{F_i}$ are the W-groups corresponding to the field F_i. Then*

$$\mathcal{G}_F \cong \mathcal{G}_{F_1} * ... * \mathcal{G}_{F_k}$$

Proof: First of all by Theorem 2.0.46, for any finite space of orderings X_i there exists a Pythagorean field F_i such that X_i is equivalent to space of orderings of F_i. So $X_F = X_{F_1} \oplus X_{F_2} \oplus ... \oplus X_{F_k}$. Recall ([MI1], theorem in page 105) that says;
If $X_F = X_1 \oplus X_2 \oplus ... \oplus X_k$ where X_i are the connected components of X_F then $G_F = G_{F_1} * ... * G_{F_k}$, where $G_F = Gal(F(2)/F)$. (Recall that $F(2)$ is the maximal 2-extension of F in some fixed separable closure of F.)

Now consider the quotient of G_F by the third 2-descending central sequence, (see page 16). By observing that free products in category of pro-2-groups are mapped to free products in the category $\mathcal{C}$ of the corresponding factors divided by third 2-descending central sequence we obtain our desired claim.$\square$

Example 3.19.

We can determine the structure of $\mathcal{G}_F = \langle \sigma_1, ..., \sigma_6 \,|\, (\sigma_1\sigma_2\sigma_3)^2 = 1\,,\ (\sigma_4\sigma_5\sigma_6)^2 = 1\rangle$ and the Frattini subgroup Φ_F.

To determine the structure of $X_F = \{\sigma_1, ..., \sigma_6 \,|\, (\sigma_1\sigma_2\sigma_3)^2 = 1\,,\ (\sigma_4\sigma_5\sigma_6)^2 = 1\}$ we show that it has two connected components $X_1 = \{\sigma_1, \sigma_2, \sigma_3, \sigma_1\sigma_2\sigma_3\}$ and $X_2 = \{\sigma_4, \sigma_5, \sigma_6, \sigma_4\sigma_5\sigma_6\}$. Let $\mathcal{G}_{F_1}$ and $\mathcal{G}_{F_2}$ are the two W-groups corresponding to X_{F_1} and X_{F_2} respectively. Therefore $\mathcal{G}_{F_1} = \langle \sigma_1, \sigma_2, \sigma_3 \,|\, (\sigma_1\sigma_2\sigma_3)^2 = 1\rangle$ and $\mathcal{G}_{F_2} = \langle \sigma_4, \sigma_5, \sigma_6 \,|\, (\sigma_4\sigma_5\sigma_6)^2 = 1\rangle$.

But $\mathcal{G}_{F_1}$ and $\mathcal{G}_{F_2}$ are Galois fans with four elements. As we showed in Example 3.1.3, $\mathcal{G}_{F_1}$ and $\mathcal{G}_{F_2}$ are isomorphic to the group $(C_4 \times C_4) \rtimes C_2$. Now use the last theorem and Theorem 1.0.32 about the free product of two pro-2-groups, so

$$\mathcal{G}_F \cong \mathcal{G}_{F_1} * \mathcal{G}_{F_2} \cong (\mathcal{G}_{F_1} \times \langle \mathcal{G}_{F_1}, \mathcal{G}_{F_2}\rangle) \rtimes \mathcal{G}_{F_2}.$$

Therefore,

$$\mathcal{G}_F \cong ((\prod_2 C_4 \rtimes C_2) \times \langle \mathcal{G}_{F_1}, \mathcal{G}_{F_2}\rangle) \rtimes (\prod_2 C_4 \rtimes C_2).$$

On the other hand,

$$\langle \mathcal{G}_{F_1}, \mathcal{G}_{F_2}\rangle = \langle [a_i, a_j] \,|\, a_i \in \mathcal{G}_{F_1},\ a_j \in \mathcal{G}_{F_2}\rangle.$$

Because $\mathcal{G}_{F_1} = \langle \sigma_1, \sigma_2, \sigma_3\rangle$ and $\mathcal{G}_{F_2} = \langle \sigma_4, \sigma_5, \sigma_6\rangle$, then

$$\langle \mathcal{G}_{F_1}, \mathcal{G}_{F_2}\rangle = \langle [\sigma_i, \sigma_j] \,|\, i = 1, 2, 3, \quad j = 4, 5, 6\rangle.$$

There are 9 such commutators, since any of $[\sigma_i, \sigma_j]$ has order two so

$$\langle \mathcal{G}_{F_1}, \mathcal{G}_{F_2}\rangle \cong \prod_9 C_2$$

$$\mathcal{G}_F \cong \mathcal{G}_{F_1} * \mathcal{G}_{F_2} \cong ((\prod_2 C_4 \rtimes C_2) \times \prod_9 C_2) \rtimes (\prod_2 C_4 \rtimes C_2).$$

Therefore, this is a group of order 2^{19}.

We know from Theorem 1.0.17 that $\Phi_F = [\mathcal{G}_F, \mathcal{G}_F]$. There are two cases for elements in $[\mathcal{G}_F, \mathcal{G}_F]$.

First case: if g_1, g_2 are in different components, as we mentioned there are 9 such kind of commutators.
Second case: if g_1, g_2 are in the same component, there are 4 commutators. Two $[\sigma_1, \sigma_2], [\sigma_1, \sigma_3]$ of X_1 and and two commutators $[\sigma_4, \sigma_5], [\sigma_4, \sigma_6]$ of X_2.
As we assumed $(\sigma_1\sigma_2\sigma_3)^2 = 1$ and $(\sigma_4\sigma_5\sigma_6)^2 = 1$, then $[\sigma_2, \sigma_3]$ and $[\sigma_5, \sigma_6]$ will be generated by these four commutators. Therefore we have 13 commutators and any of them has order 2. So $\Phi_F \cong \prod_{13} C_2$.□

Example 3.20.

If the W-group $\mathcal{G}_F$ of a Pythagorean formally real field F is isomorphic to $\prod_2 C_4 \rtimes \mathcal{G}_K$ such that $\mathcal{G}_K$ is the W-group in the last example, we can compute the Frattini subgroup Φ_F.
Apply Theorem 3.18 for $\mathcal{G}_F$, so $\mathcal{G}_F = \prod_2 C_4 \rtimes \mathcal{G}_K = \prod_2 C_4 \rtimes (\mathcal{G}_{F_1} * \mathcal{G}_{F_2})$. In the last example we showed that $\Phi_K \cong \prod_{13} C_2$. Therefore $\mathcal{G}_K$ has 13 commutators. Assume γ_1, γ_2 are the generators of $\prod_2 C_4$, so they have order 4. Any element of Φ_F has the form $\gamma_1^{\epsilon_1}\gamma_2^{\epsilon_2}h$ where h is a commutator of $\mathcal{G}_K$ and $\epsilon_1, \epsilon_2 = 0, 1$. Then $|\Phi_F| = 2^{15}$.

3.2 Classifying the structure of W-groups

In this chapter we will try to classify the structure of $\mathcal{G}_F$ by the number of orderings of the field F and $|\dot{F}/\dot{F}^2|$. These results are based on J. Mináč's work in [MI2], J.L. Merzel's work in [Mz], and Theorems 3.16 and 3.18. But the approach to prove results here is mostly combinatorial.

L.Brocker and L.Berman found nice results about the set of possible numbers of X_F. They denoted O the function from the set of positive integers to the power set of $\mathbb{N}$. The set $O(n)$ gives us all the possible numbers for $|X_F|$. In the case $|\dot{F}/\dot{F}^2| = 2^n$, L. Brocker and L.Berman proved for $n \geq 2$, $O(n) = 2O(n-1) \cup (1 + O(n-1))$ see ([Mz] page 188) and [Be]. Thus for small space of orderings we have:

$$|\dot{F}/\dot{F}^2| = 2^1 \text{ then } O(1) = \{1\}$$

$$|\dot{F}/\dot{F}^2| = 2^2 \text{ then } O(2) = 2O(1) \cup (1 + O(1)) = \{2\}$$

$$|\dot{F}/\dot{F}^2| = 2^3 \text{ then } O(3) = 2O(2) \cup (1 + O(2)) = \{3, 4\}$$

When we say F, (or X_F) has type $(2^n, a)$, we mean a is the number of orderings of F and $|\dot{F}/\dot{F}^2| = 2^n$ or equivalent that ($X_F = \langle \sigma_1, ..., \sigma_n \rangle$ and $|X_F| = a$).

Definition 3.21. *(2.4, [Mz]) $k \in O(n)$ is called decomposable if there exist $a, b, r, s \in \mathbb{N}$ such that $n = a + b$, $k = r + s$, $r \in O(a)$ and $s \in O(b)$, $k \in O(n)$. It is indecomposable otherwise.*

Theorem 3.22. *If field F is of type $(2^n, n)$, then $\mathcal{G}_F \cong \underbrace{C_2 * ... * C_2}_{n}$.*

Proof: In this case the number of generators of X_F and the number of orderings are equal, all the orderings of field F are independent. Therefore if any two orderings σ_i, σ_j are in the same connected component, then there exist α , $\beta \in X_F$ such that

$\sigma_i\sigma_j = \alpha\beta$, so $\sigma_i\sigma_j\alpha\beta = 1$. This means σ_i, σ_j, α and β are dependent mod Φ_F; this is a contradiction. So all the orderings are in separate connected components. Therefore $X_F = \bigcup_{i=1}^{n} X_i$ where all X_i are trivial spaces of type $(2^1, 1)$. We know that $\mathcal{G}_F$ corresponding to the trivial space X_i is C_2. Then by the Theorem 3.18 we have $\mathcal{G}_F \cong \underbrace{C_2 * ... * C_2}_{n}$.$\square$

Example 3.23.

If X_F is of type $(2^4, 6)$, then the structure of $\mathcal{G}_F$ will be determined completely. First of all since F has 4 independent orderings, and any connected component has at least one element, the number of connected components of X_F is at most 4. Because there are 6 orderings, one of the components should be nontrivial. We mentioned before that, the smallest connected ordering space is of type $(2^3, 4)$ (which corresponds to the four element fan), thus either X_F has one or two components.

If X_F has two components let X_1 be of type $(2^3, 4)$ and X_2 be the trivial ordering space. Then the number of orderings together is 5, this is a contradiction. Consequently X_F is a connected space.

Assume $X_F = \{\sigma_1, ..., \sigma_6\}$ is connected ordering space. Then $\sigma_1 \sim \sigma_2$. Without loss of generality assume $\sigma_1\sigma_2 = \sigma_4\sigma_3$. On the other hand $\sigma_5 \sim \sigma_6$ are connected, so assume $\sigma_5\sigma_6 = \sigma_1\sigma_4$. Then $\sigma_1\sigma_4\sigma_5 = \sigma_6$ therefore $\sigma_2\sigma_3\sigma_5 = \sigma_6$.

Now we can rewrite $X_F = \{\sigma_1, \sigma_2, \sigma_3, \sigma_1\sigma_2\sigma_3, \sigma_5, \sigma_2\sigma_3\sigma_5\}$. It is easy to check that just $\alpha = \sigma_2\sigma_3 \in Z(Gal(F^{(3)}/F(\sqrt{-1})))/\Phi_F$ satisfies this condition: for any $\sigma \in X_F$, $\alpha\sigma \in X_F$. Therefore $Z(Gal(F^{(3)}/F(\sqrt{-1})))/\Phi_F = \langle\alpha\rangle$. Now let $X'_F = \{\sigma_i|_E \text{ for all } \sigma_i \in X_F\}$ where E is fixed field of $Z(Gal(F^{(3)}/F(\sqrt{-1})))/\Phi_F = \langle\alpha\rangle$, so

$$\sigma_2|_E = \sigma_3|_E \qquad \sigma_1\sigma_2\sigma_3|_E = \sigma_1|_E \qquad \sigma_2\sigma_3\sigma_5|_E = \sigma_5|_E.$$

Now $X'_F = \{\sigma_1, \sigma_2, \sigma_5\}$, since X'_F has 3 orderings and as we mentioned before the smallest connected space has 4 elements, so X'_F is a disconnected space. This is a space of type $(2^3, 3)$, so by the Theorem 3.22 $\mathcal{G}_{F'} = C_2 * C_2 * C_2$. Then apply Theorem 3.16, so

$$\mathcal{G}_F = (C_4 \rtimes (C_2 * C_2 * C_2)).$$

Example 3.24.

If $|\dot{F}/\dot{F}^2| = 4$, then X_F is generated by four orderings. In this case we can classify all the possible W-groups $\mathcal{G}_F$. If $|\dot{F}/\dot{F}^2| = 2^4$, then

$$O(4) = 2O(3) \cup (1 + O(3)) = \{4, 5, 6, 8\}.$$

First case: X_F is of type $(2^4, 5)$. By Example 3.25 X_F is disconnected space. Since $a > n$ one of the connected components should be nontrivial. But the smallest connected space is of type $(2^3, 4)$, so there are just 2 components: X_1, X_2. Let X_1 be of type $(2^3, 4)$, X_2 be trivial, and $\mathcal{G}_{F_1}$, $\mathcal{G}_{F_2}$ be the W-groups corresponding to X_1, X_2. But X_1 is a space of orderings of a fan with four elements, so $\mathcal{G}_{F_1} = (C_4 \times C_4) \rtimes C_2$. On the other hand $\mathcal{G}_{F_2} = C_2$. Therefore by Theorem 3.18,

$$\mathcal{G}_F = \mathcal{G}_{F_1} * \mathcal{G}_{F_2} = ((C_4 \times C_4) \rtimes C_2) * C_2.$$

Second case: X_F is of type $(2^4, 8)$. X_F is a fan with 8 elements, so it corresponds to the Galois fan

$$\mathcal{G}_F = (\prod_{i=1}^{3} C_4) \rtimes C_2$$

see Example 3.4 and note after that. As we proved in the last theorem if X_F is of type $(2^4, 4)$, then

$$\mathcal{G}_F = C_2 * C_2 * C_2 * C_2.$$

Now use the last example, then we know completely the structure of $\mathcal{G}_F$ for Pythagorean formally real field F where $|\dot{F}/\dot{F}^2| = 4$.

$$\begin{aligned}
&X_F \quad \textit{of type} \quad (2^4, 4) \Longrightarrow \mathcal{G}_F = C_2 * C_2 * C_2 * C_2 \\
&X_F \quad \textit{of type} \quad (2^4, 5) \Longrightarrow \mathcal{G}_F = ((C_4 \times C_4) \rtimes C_2) * C_2 \\
&X_F \quad \textit{of type} \quad (2^4, 6) \Longrightarrow \mathcal{G}_F = C_4 \rtimes (C_2 * C_2 * C_2) \\
&X_F \quad \textit{of type} \quad (2^4, 8) \Longrightarrow \mathcal{G}_F = (\prod_{i=1}^{3} C_4) \rtimes C_2.
\end{aligned}$$

In all cases $C_2 = \langle\sigma\rangle$ acts on $C_4 = \langle\tau\rangle$, by $\sigma\tau\sigma^{-1} = \tau^3$.

Theorem 3.25. *If X_F of type $(2^n, a)$ is a connected space, then $a \geqslant 2(n-1)$.*

Proof: Again we use the method of counting orderings. We proved in Theorem 3.14 that if X_F is a connected space, then there exists $\alpha \in Z(Gal(F^{(3)}/F(\sqrt{-1})))/\Phi_F$ such that $\alpha = \sigma_1 ... \sigma_{2t}$ and $\alpha X_F = X_F$. We claim if σ_i is an element of the basis of X_F, then $\alpha\sigma_i$ is an ordering which is in the basis.

We can write $\alpha = \sigma_1^{\epsilon_1} \cdots \sigma_n^{\epsilon_n}$, $\epsilon_k \in \{0, 1\}$, such that the number of ϵ_k, which $\epsilon_k = 1$ is even. Assume for this time that α is a product of more than two of the σ_i's. Consider $\alpha\sigma_i$, where $i = 1, ..., n$. If for $k = i$, $\epsilon_i = 0$, then $\alpha\sigma_i = \sigma_1^{\epsilon_1} \cdots \sigma_n^{\epsilon_n}\sigma_i$ which is not equal to any element in the basis. If for $k = i$, $\epsilon_i = 1$, we can move σ_i to the left side, then we have

$$\sigma_1^{\epsilon_1} ... \sigma_n^{\epsilon_n}\sigma_i = \sigma_1^{\epsilon_1} ... \underbrace{\sigma_i\sigma_i}_{1} ... \sigma_n^{\epsilon_n} \prod_l [\sigma_i, \sigma_l]$$

which is not equal to an element of the basis. Therefore when i changes from 1 to n, $\alpha\sigma_i$ gives us n new orderings which are not equal to the elements of basis. So the number of orderings is bigger than $2n$.

Note that in the expression of α, if α is product of two elements of the basis, (without loss of generality assume $\alpha = \sigma_1\sigma_2$) then in the product, $\alpha\sigma_i = \sigma_1\sigma_2\sigma_i$ for

$i = 1$, $\alpha\sigma_1 = \sigma_1\sigma_2\sigma_1 = \sigma_2 \bmod \Phi_F$, and $i = 1$, $\alpha\sigma_2 = \sigma_1\sigma_2\sigma_1 = \sigma_1$. So just for $i = 3, ..., n$ the product $\alpha\sigma_i$ gives us $n-2$ new orderings, so $a \geqslant n+n-2 = 2(n-1)$.□ Since we have shown that if σ is the product of 2 generators, we have $a \geqslant 2(n-1)$ and if σ is the product of an even number of generators greater than 2, we have $a \geqslant 2n$, we have in general that $a \geqslant 2(n-1)$.

Example 3.26.

Assume X_F is the space of orderings of type $(2^5, 6)$. First of all by the last theorem X_F is a disconnected space. But it can not have 6 components , since there are just five generators for X_F. We know the smallest connected component has type $(2^3, 4)$ which corresponds to the four element fan. Therefore, if $X_F = X_1 \cup ... \cup X_i$, because all the X_i can not be trivial components, at least there exists i such that $|X_i| \geqslant 4$. Therefore $i \leqslant 3$. Now there are two cases to check.

Case 1: Assume $X_F = X_1 \cup X_2$. Then X_1 should be trivial connected component and X_2 would be of type $(2^4, 5)$. But $5 < 2(4-1)$, so by the last theorem X_2 is not connected and this is a contradiction.

Case 2 : Assume $X_F = X_1 \cup X_2 \cup X_3$. As we discussed, one of X_i should be nontrivial. Therefore the only case is X_1, X_2 are trivial and X_3 is of type $(2^3, 4)$. W-groups that correspond to X_1, X_2, X_3 are C_2, C_2 and $(C_4 \times C_4) \rtimes C_2$ respectively. Then by Theorem 3.18

$$\mathcal{G}_F = C_2 * C_2 * ((C_4 \times C_4) \rtimes C_2).$$

Now we generalize this example to the general case $(2^n, n+1)$, for all Pythagorean formally real fields which they have just one dependent ordering. The structure of W-group of this kind of fields will be determined in the following theorem.

Theorem 3.27. *Let F be a Pythagorean formally real field. If the ordering space X_F has type $(2^n, n+1)$, $n > 3$, then $X_F = X_1 \cup ... \cup X_{n-2}$ and the W-group corresponding to X_F has this unique structure*

$$\mathcal{G}_F = \underbrace{C_2 *, ..., * C_2}_{n-3} * ((C_4 \times C_4) \rtimes C_2).$$

Proof: $n > 3$, so $n + 1 < 2(n - 1)$. Thus by Theorem 3.25 X_F, is a disconnected space. As the smallest connected space has type $(2^3, 4)$ and we have n generators, the number of connected components is $n - 2$; $n - 3$ trivial components and one connected component of type $(2^3, 4)$. Using Theorem 3.18, the structure of X_F gives us the W-group $\mathcal{G}_F$ that we mentioned. Therefore it is enough to show that this is the only structure for X_F. Then the structure of $\mathcal{G}_F$ will be unique.

Let $X_F = X_1 \cup ... \cup X_i$ and $X_1, ..., X_i$ are of type $(2^{n_1}, a_1), ..., (2^{n_i}, a_i)$ respectively. Using Theorem 3.25, except for a fan with 4 elements which corresponds to a connected ordering space of type $(2^3, 4)$, for any connected component of type $(2^{n_i}, a_i)$, since $a_i \geqslant 2(n_i - 1)$, $a_i - n_i \geqslant n_i - 2$. Hence for $n_i \geqslant 4$, $a_i - n_i \geqslant 2$.

Now $n_1 + n_2 ... + n_i = n$ and $a_1 + a_2 ... + a_i = n + 1$, and any X_i has at least $a_i = n_i$ orderings. So for only one of the X_i, a_i can be equal to $n_i + 1$. Since the only space of type $(2^n, n + 1)$ which is connected is the space of type $(2^3, 4)$, so X_i has type $(2^3, 4)$ and all the other components are trivial. But this is the structure we found first. Consequently the structure of W-group $\mathcal{G}_F$ is unique as we claimed.□

Example 3.28.

We can determine the structure of the W-group $\mathcal{G}_F$ for any Pythagorean formally real field F such that X_F is of type $(2^5, 7)$.
Since $7 < 2(5 - 1)$, then by the last lemma X_F is disconnected space. Because the

number of generators and the number of orderings are not equal, X_F cannot have 7 connected components . If $X_F = X_1 \cup ... \cup X_i$, all components can not be trivial, so at least one X_i is a nontrivial connected space. As we mentioned before the smallest nontrivial connected space is a fan of type $(2^3, 4)$, so $i \leqslant 3$.

X_F can not have three components, one nontrivial (fan with four elements) and 2 trivial because the number of orderings will be 6 and again it is a contradiction with type of X_F.

The only case is $X_F = X_1 \cup X_2$ with both X_1 trivial and X_2 non trivial. We cannot have have both X_1 and X_2 nontrivial since the minimum number of orderings in a nontrivial component is four, so with two nontrivial components the number of orderings is eight and this is a contradiction. Therefore X_1 is trivial and X_2 should be of type $(2^4, 6)$. By Example 3.23 the W-group corresponding to X_2 is $C_4 \rtimes (C_2 * C_2 * C_2)$ and the W-group of the trivial space is C_2, so:

$$\mathcal{G}_F \simeq (C_4 \rtimes (C_2 * C_2 * C_2)) * C_2$$

Example 3.29.

We show that, the space of ordering X_F of type $(2^5, 8)$ is a connected space.

By the same argument in the last example if $X_F = X_1 \cup ... \cup X_i$, then $i \leqslant 3$. The only case with 3 components is when X_1 is a fan with four elements and X_2, X_3 are trivial components, so in this case we have six orderings. But the number of orderings of X_F is eight, so $X_F = X_1 \cup X_2$ or X_F is connected. Suppose $X_F = X_1 \cup X_2$. X_F has just five generators, so one of X_i should have four generators. By Example 3.2.4 the only connected spaces with four generators are the spaces of type $(2^4, 6)$ and $(2^4, 8)$ and in both cases taking the union with the trivial space $(2^1, 1)$ the number of orderings is not 8. Therefore X_F is a connected space.

We point out that in the case the type of field is $(2^n, 2^{n-1})$, where $n \geq 3$ then the space of orderings is necessarily fan and therefore its space of orderings is connected. This was already observed in ([MI2], Chapter 1. Theorem 1.2)

Theorem 3.30. *If X_F is of type $(2^n, 2^{n-2}+1)$, then the type of X_F completely classifies the structure of X_F, and $X_F = X_1 \cup X_2$ such that X_1 is a trivial space and X_2 is a fan with 2^{n-2} elements . Then $\mathcal{G}_F = C_2 * ((\prod_{i=1}^{n-2} C_4) \rtimes C_2)$.*

Proof: Let $X_F = X_1 \cup X_2$ such that X_1 is trivial space and X_2 is a fan with 2^{n-2} elements. Then by Theorem 3.18, $\mathcal{G}_F = C_2 * ((\prod_{i=1}^{n-2} C_4) \rtimes C_2)$. This is one of the possible structures for $\mathcal{G}_F$. Now we prove, this is only structure for X_F.

First assume that X_F is a disconnected space with two components, $X_F = X_1 \cup X_2$ such that X_1 and X_2 are of type $(2^m, a_1), (2^k, a_2)$ respectively. Therefore $n = m + k$, $2^{n-2} + 1 = a_1 + a_2$. We will show for any choice of X_1, X_2 if $m, k \neq 1$, then $a_1 + a_2 < 2^{n-2} + 1$.

If $|\dot{F}/\dot{F}^2| = 2^n$ and F is a fan case, then the number of orderings of F is maximum, so $|X_F| = 2^{n-1}$. So if X_1 , X_2 are not fan, then $a_1 + a_2 < 2^{m-1} + 2^{k-1}$.

$$a = 2^{n-2} + 1 = 2^{m-1} \times 2^{k-1} + 1$$

$$2^{m-1} + 2^{k-1} < 2^{m-1}2^{k-1} + 1 \Longleftrightarrow 2^{m-1}2^{k-1} - 2^{m-1} - 2^{k-1} + 1 > 0$$
$$\Longleftrightarrow 2^{m-1}2^{k-1} - 2^{m-1} - 2^{k-1} + 1 = (2^{m-1} - 1)(2^{k-1} - 1) > 0$$

this is true if $m, k \neq 1$. But $a_1 + a_2 < 2^{m-1} + 2^{k-1}$, so for $m, k \neq 1$, $a_1 + a_2 < 2^{n-2} + 1 = a$. Therefore X_F cannot have two components unless one of them be trivial. This is the first case we mentioned. In the same way we can check that X_F does not have more than two components. So it's enough to show that X_F is not a

connected space.

If X_F is a connected space, then

$$\exists \gamma \in Z(Gal(F^{(3)}/F(\sqrt{-1}))/\Phi_F \quad \text{such that} \quad \gamma X_F = X_F,$$

so the number of orderings should be even. But we assumed $|X_F| = 2^{n-2}+1$, so X_F cannot be a connected space. Therefore the only structure is $X_F = X_1 \cup X_2$ where X_1 is a trivial space and X_2 is a fan with 2^{n-2} elements. This is the structure we mentioned first. But $\mathcal{G}_{F_1} = C_2$ and $\mathcal{G}_{F_2} = (\prod_{i=1}^{n-2} C_4) \rtimes C_2$, now by Theorem 3.18

$$\mathcal{G}_F = C_2 * ((\prod_{i=1}^{n-2} C_4) \rtimes C_2)).\square$$

Theorem 3.31. *If X_F is of type $(2^n, a)$ such that $a \geq 2^{n-2}+2$, then X_F is a connected ordering space.*

Proof: Assume X_F is a disconnected space with two components $X_F = X_1 \cup X_2$ such that X_1 and X_2 are of type $(2^m, a_1), (2^k, a_2)$ respectively, so $n = m + k$ and $a = a_1 + a_2$. We claim that $a_1 + a_2 < 2^{n-2} + 2 < a$ for any choice of X_1, X_2. But we proved in the last Theorem that if X_1 and X_2 are not fan, then $a_1 + a_2 < 2^{n-2} + 1$, except for $k = 1$ or $m = 1$. If $k = 1$, then $m = n - 1$, X_2 has type $(2^1, 1)$ and $a_1 = a - 1$. Therefore X_1 has type $(2^{n-1}, a - 1)$.

Since $a > 2^{n-2} + 2$, so $a - 1 > 2^{n-2} + 1$. But the maximum number of orderings for F such that $|\dot{F}/\dot{F}^2| = 2^{n-1}$ is 2^{n-2} (this is the case of one fan with 2^{n-2} elements). Then $a_1 > 2^{n-2} + 1$ cannot be number of elements of X_1, and this a contradiction. Therefore X_F cannot have 2 components. In the same way we can prove X_F does not have more than two components, so it is a connected space.$\square$

To continue we consider the binary representation of the invariant $|X_F| = a$ depending on the invariant n where $|\dot{F}/\dot{F}^2| = 2^n$ which is appeared in [Mz] and [MI3]. Based on the work in [MI3] we will show that: for a field F of type $(2^n, a)$, if a has a binary representation of the form

$$a = 2^{n-k} + 2^{i_1} + 2^{i_2} + ... + 2^{i_{k-1}}, \quad 0 \leq i_1 < i_2 < ... < i_{k-1} < n - k,$$

then the structure of W-group of F is completely determined. The key point is that for fixed n this representation is unique. One example of an invariant $|X_F| = a$ has this kind of representation is a field F of type $(2^7, 15)$, since one can write $15 = 2^{7-4} + 2^0 + 2^1 + 2^2, \leq 0 < 1 < 2 < 7 - 4$.

There are of course some numbers which does not have this specific representation. One example of $a \in O(n)$ which does not have such a representation will be discussed in the following example.

Example 3.32.

A field F of type $(2^6, 21)$ is an example such that $a = |X_F|$ does not have such a binary form. If there exist a binary representation

$$21 = 2^{6-k} + 2^{i_1} + 2^{i_2} + ... + 2^{i_{k-1}}, \quad 0 \leq i_1 < i_2 < ... < i_{k-1} < 6 - k,$$

then $6 - k \leq 4$. If $6 - k = 4$, $k = 2$ but there does not exist any i such that $21 = 2^4 + 2^i$. For $6 - k = 3$, we can see that there does not exist $i_1 < i_2 < 3$ such that $21 = 2^3 + 2^{i_1} + 2^{i_2}$. This true about $6 - k = 2$ and $6 - k = 1$. Therefore $a = 21$ does not have a binary representation depend on $n = 6$.

Lemma 3.33. *If X_F is an ordering space of type $(2^n, a)$ such that*

$$a = 2^{n-k} + 2^{i_1} + 2^{i_2} + ... + 2^{i_{k-1}}, \quad 0 \leq i_1 < i_2 < ... < i_{k-1} < n - k,$$

then this representation of a is unique.

Proof: This uniqueness is the immediate consequence of uniqueness of expanding natural numbers in dyadic expansion.□

Lemma 3.34. *If X_F is an ordering space of type $(2^n, a)$ such that*

$$a = 2^{n-k} + 2^{i_1} + 2^{i_2} + ... + 2^{i_{k-1}}, \quad 1 \leqslant i_1 < i_2 < ... < i_{k-1} < n-k,$$

then X_F is a connected space.

Proof: This is the obvious corollary of (Corollary 2, [MI3]).

Theorem 3.35. *Suppose the ordering space X_F is of type:*

$$(2^n, 2^{n-k} + 2^{i_1} + 2^{i_2} + ... + 2^{i_{k-1}}) \text{ such that } 0 \leqslant i_1 < ... < i_{k-1} < n-k.$$

Then

$$\mathcal{G}_F = C_2 * (\prod_1^{i_2} C_4 \rtimes (C_2 * (\prod_1^{i_3 - i_2} C_4 \rtimes ...(C_2 * (\prod_1^{n-k-i_2...-i_l} C_4) \rtimes C_2)...), \ \ i_1 = 0,$$

such that $n - k - i_2... - i_l \geqslant 0$,

$$\mathcal{G}_F = \prod_1^{i_1} C_4 \rtimes (C_2 * (\prod_1^{i_2 - i_1} C_4 \rtimes ...(C_2 * (\prod_1^{n-k-i_1-i_2...-i_l} C_4) \rtimes C_2)...), \ \ i_1 \neq 0,$$

such that $n - k - i_1 - i_2... - i_l \geqslant 0$.

Proof: We use induction. By Theorem 3.34 all the elements $a = 2^{n-k} + 2^{i_1} + ... + 2^{i_{k-1}} \in O(n), n > 2$ such that $1 \leq i_1 < ... < i_{k-1} < n-k$ are indecomposable elements of the set $O(n)$. This means that X_F of type $(2^n, a)$ is a connected space.

For $n = 3, 4$, we proved in the first of this section that the structure of $\mathcal{G}_F$ for any $a \in O(3)$ and $O(4)$ is unique. Now assume for any $j < n$ our claim is true . Therefore

by induction for X_F of type $(2^j, a)$ such that $a = 2^{j-k} + 2^{i_1} + ... + 2^{i_{k-1}} \in O(n), n > 2$ and $0 \leqslant i_1 < ... < i_{k-1} < j - k$, we have:

$$\mathcal{G}_F = \prod_1^{i_1} C_4 \rtimes (C_2 * (\prod_1^{i_2 - i_1} C_4 \rtimes ...(C_2 * (\prod_1^{n-k-i_1-i_2,...-i_l} C_4) \rtimes C_2)...), \;\; i_1 \neq 0$$

$$\mathcal{G}_F = C_2 * (\prod_1^{i_2} C_4 \rtimes (C_2 * (\prod_1^{i_3 - i_2} C_4 \rtimes ...(C_2 * (\prod_1^{n-k-i_2...-i_l} C_4) \rtimes C_2)...), \;\; i_1 = 0.$$

Now if $a \in O(n)$ and $a = 2^{n-k} + 2^{i_1} + ... + 2^{i_{k-1}}$ such that $1 \leqslant i_1 < ... < i_{k-1} < n - k$, then by Lemma 3.33 this representation is unique. X_F is a connected space, so T, the translation group of $\mathcal{G}_F$, is nonempty. Therefore there exists $\gamma \in T$ such that for all σ in X_F, $\gamma\sigma \in X_F$.

As we said before any $\sigma \in X_F$ can be written uniquely as a product $t\sigma'$ where $t \in T$, $\sigma' \in X_{\bar{F}}$. Then $|X_F| = |T||X_{\bar{F}}|$ and $|T| = 2^m$ where m is the dimension of T as F_2 vector space. Then $a = |T| \times a'$, $a' \in N$, but we proved before $|X'_F| = a'$ where X'_F is the space of restriction of elements of X_F to the fixed field of T(see the proof of Theorem 3.16). Let t_1 be the F_2 dimension of T, so

$$a = 2^{n-k} + 2^{i_1} + 2^{i_2} + ... + 2^{i_{k-1}} = 2^{t_1}.a' = 2^{t_1} \times |X'_F|.$$

If

$$t_1 < i_1 \Longrightarrow a = 2^{n-k} + 2^{i_1} + ... + 2^{i_{k-1}} = 2^{t_1} \underbrace{(2^{n-k-t_1} + 2^{i_1 - t_1} + ... + 2^{i_{k-1-t_1}})}_{|X'_F|}.$$

Let $n - t_1 = n'$ and apply the last lemma for $2^{n'-k} + 2^{i_1} + ... + 2^{i_{k-1}-t_1}$. Then X'_F is a connected space. But it is mentioned in Theorem 3.16 that X'_F is a disconnected space, this is a contradiction. Therefore $t_1 \geqslant i_1$. Since $a = 2^{t_1}.a'$, so $t_1 = i_1$. Now by Theorem 3.16, $\mathcal{G}_F = (\prod_1^{t_1 = i_1} C_4) \rtimes (\mathcal{G}_{F'})$ where $\mathcal{G}_{F'}$ is the W-group corresponding

to X'_F.

But $|X'_F| = 2^{n-k-t_1} + 2^{i_1-t_1} + ... + 2^{i_{k-1}-t_1}$, $i_1 - t_1 = 0$ and $n - t < n$, so by the induction assumption

$$\mathcal{G}_{F'} = C_2 * (\prod_1^{i_2-i_1} C_4 \rtimes (C_2 * (\prod_1^{i_3-i_2-i_1} C_4 \rtimes ...(C_2 * (\prod_1^{n-k-i_2...-i_l} C_4) \rtimes C_2)...).$$

Then

$$\mathcal{G}_F = \prod_1^{t_1=i_1} C_4 \rtimes (\mathcal{G}'_F) = \prod_1^{t_1=i_1} C_4 \rtimes \Big(C_2 * (\prod_1^{i_2-i_1} C_4 \rtimes ...(C_2 * (\prod_1^{n-k-i_2...-i_l} C_4) \rtimes C_2)...\Big)$$

as we claimed.

If a is odd number, then one of the possible structures for X_F is $X_F = X_1 \cup X_2$ such that X_1 is a trivial space and X_2 is a connected space of type $(2^{n-1}, 2^{n-k} + 2^{i_2} + ... + 2^{i_{k-1}})$. We will show that this is the only structure for X_F.

Assume $X_F = X_1 \cup ... \cup X_k$ such that $X_1, ..., X_k$ are of type $(2^{n_1}, a_1), ..., (2^{n_k}, a_k)$ respectively. But the type of X_F was $(2^n, 2^{n-k} + 2^{i_1} + ... + 2^{i_{k-1}})$, $0 = i_1 < i_2 < ... < i_{k-1} < n - k$. Since a is an odd number and any nontrivial connected space X_i has even number of elements, so at least one of the X_i say X_1 should be a trivial connected space of type $(2^1, 1)$.

Now $X_2 \cup ... \cup X_k$ is a space of type $(2^{n-1}, 2^{n-k} + 2^{i_2} + ... + 2^{i_{k-1}})$. By Lemma 3.34 this space is a connected space, and this is a contradiction. Therefore the only structure for X_F is $X_F = X_1 \cup X_2$ such that X_1 is a trivial space and X_2 is of type $(2^{n-1}, 2^{n-k} + 2^{i_2} + ... + 2^{i_{k-1}})$. This is the structure we mentioned before. Now by

the induction assumption, $\mathcal{G}_{F_2}$ corresponding to X_2 is

$$\mathcal{G}_{F_2} = \prod_{1}^{i_2} C_4 \rtimes (C_2 * (\prod_{1}^{i_3-i_2} C_4 \times ...(C_2 * (\prod_{1}^{n-k-i_2...-i_l} C_4) \rtimes C_2)...) \rtimes C_2$$

and obviously since X_1 is trivial space, $\mathcal{G}_{F_1}$ is C_2. Therefore, by Theorem 3.18

$$\mathcal{G}_F = \mathcal{G}_{F_1} * \mathcal{G}_{F_2} = C_2 * \Big(\prod_{1}^{i_2} C_4 \rtimes (C_2 * (\prod_{1}^{i_3-i_2} C_4 \rtimes ...(C_2 * (\prod_{1}^{n-k-i_2...-i_l} C_4) \rtimes C_2)...\Big)$$

as we claimed.□

The last theorem gave us a very good sufficient condition on the number of orderings of field F to be sure that the structure of the W-group $\mathcal{G}_F$ is unique. Now we show with an example that this condition is not a necessary condition.

Example 3.36.

If X_F is an ordering space of type $(2^6, 7)$, then by Theorem 3.27 the ordering space X_F and $\mathcal{G}_F$ have unique structure. But $a = 7$ has this binary representation

$$7 = 2^2 + 2^1 + 2^0$$

which is not in the form we want. Since the binary representation is unique, then

$|X_F|$ cannot have a representation such as the one in last theorem, although the structure of it's W-group is unique.

3.3 W-groups as Coxeter Groups

Definition 3.37. *We define a Coxeter group W as a group generated by $S \subset W$ such that*

$$W = \langle s_i \in S \,|\, (s_i)^2 = (s_i s_j)^{m_{i,j}} = 1 \rangle \text{ where } m_{i,j} \in \{2, 3, ...\} \cup \{\infty\}.$$

A pair (W, S) is called a Coxeter system. A Coxeter system (W, S) is reducible if $W = W_1 \times W_2$ and $S = S_1 \sqcup S_2$ where $\emptyset \neq S_1 \subset W_1, \emptyset \neq S_2 \subset W_2$ and $(W_1, S_1), (W_2, S_2)$ are Coxeter systems. Otherwise a Coxeter system is said to be irreducible. One can find the complete classification of finite Coxeter systems in [Ka].

Theorem 3.38. *The only finite W-group which is a Coxeter group is D_4.*

Proof: By the classification theorem (Theorem A, section 8.1, [Ka]), with the exception of the graph that has two vertexes and one edge of order 4, all the other Coxeter graphs of a Coxeter system have at least one edge of order 3. We know from the definition of a Coxeter graph that an edge of order 3 represents an element of order 3 in the Coxeter group.

On the other hand any element in a W-groups has order 2 or 4. Therefore the only Coxeter group that can be a W-group is a group with two generators s_1, s_2 such that $(s_1 s_2)^4 = 1$. A W-group which is generated by two involutions σ_1, σ_2 is $C_2 * C_2$, which is isomorphic to the group D_4.□

Definition 3.39. *For the Coxeter group $W = \langle s_i \subset S \,|\, (s_i)^2 = (s_i s_j)^{m_{i,j}} = 1 \rangle$, the descending q-central sequence of W is defined inductively by*

$$W^{(1,q)} = W \ , \ W^{(i+1,q)} = (W^{(i,q)})^q [W^{(i,q)}, W] \qquad i = 1, 2....$$

$$\text{If } q = 2, \quad \text{then } W^{(1,2)} = W, \quad W^{(2,2)} = W^2[W, W]$$

$$W^{(3,2)} = (W^2[W, W])^2[W^2[W, W], W].$$

Now define the Coxeter quotient group to be $W/W^{(3,2)} = W/W^{(3)}$.

Lemma 3.40. *Let W be any Coxeter group. If $H := (W^2[W, W])^2[W^2[W, W], W]$, then*

$$[xy, z] = [x, z][[x, z], y][y, z] \qquad (a)$$

$$[x, yz] = [x, z][x, y][[x, y], z] \qquad (b)$$

Proof: (a) and (b) are just direct computation. □

On the other hand,

$$[[W, W], W] \subset (W^2[W, W])^2[W^2[W, W], W].$$

So (a) and (b) will be reduced to

$$[xy, z] = [x, z][y, z] \qquad \text{mod } H$$

$$[x, yz] = [x, z][x, y] \qquad \text{mod } H$$

Lemma 3.41. *Consider H in the last lemma. If $\sigma_i, \sigma_j, \sigma_k \in W$, then*

$$\sigma_i[\sigma_j, \sigma_k] = [\sigma_j, \sigma_k]\sigma_i \quad \textit{mod } H$$

Proof:

$$\sigma_i[\sigma_j, \sigma_k]\sigma_i^{-1}[\sigma_j, \sigma_k]^{-1} = [\sigma_i, [\sigma_j, \sigma_k]] \in H$$

$$\sigma_i[\sigma_j, \sigma_k]\sigma_i[\sigma_j, \sigma_k] = 1 \quad \text{mod } H$$

$$\Longrightarrow \sigma_i[\sigma_j, \sigma_k] = [\sigma_j, \sigma_k]\sigma_i \quad \text{mod } H.\square$$

Therefore, in the Coxeter Quotient group $W/W^{(3)}$ all commutators commute with any element.

Theorem 3.42. *For a formally real Pythagorean field F, the W-group $\mathcal{G}_F$ is a Coxeter quotient if and only if F is a SAP case in which case $\mathcal{G}_F = C_2 * ... * C_2$.*

Proof : We know that the Coxeter group $W = \langle s_i \,|\, (s_i)^2 = (s_i s_j)^{m_{i,j}} = 1 \rangle$ and $\mathcal{G}_F = \langle \sigma_i \,|\, \sigma_i^2 = 1\,,\, \sigma_i \notin |\Phi_F \rangle$.

Assume $\mathcal{G}_F \cong W/W^{(3)}$ for some Coxeter quotient group, then there exists

$$\varphi : W/W^{(3)} \to \mathcal{G}_F \text{ such that } \varphi(\overline{s_i}) = \sigma_i.$$

But by the last lemma for any $s_i, s_j, s_k \in W,\ s_i[s_j, s_k] \equiv [s_j, s_k]s_i \bmod W^{(3)}$. Then all generators of $W/W^{(3)}$ have order 2 and all commutators of $W/W^{(3)}$ are central. We claim there are no cancellation relations between commutators of $\mathcal{G}_F$. To see this, suppose $\prod[\sigma_i, \sigma_j]^{\epsilon_{i,j}} = 1$. Because φ is an isomorphism, there exist

$$s_i, s_j \in W \text{ such that } \prod_{1 \leqslant i,j \leqslant n} [\varphi(s_i), \varphi(s_j)]^{\epsilon_{i,j}} = \prod [\sigma_i, \sigma_j]^{\epsilon_{i,j}} = 1.$$

But φ is injective, so

$$\varphi(\prod_{1 \leqslant i,j \leqslant n} [s_i, s_j]^{\epsilon_{i,j}}) = \prod_{1 \leqslant i,j \leqslant n} [\varphi(s_i), \varphi(s_j)]^{\epsilon_{i,j}} = 1$$
$$\implies \prod_{1 \leqslant i,j \leqslant n} [s_i, s_j]^{\epsilon_{i,j}} = 1.$$

This is a contradiction since there are no cancellation relations between commutators in W/W^3. Therefore in this case, $\mathcal{G}_F = C_2 * ... * C_2$, meaning F is SAP. It is easy to check that if $\mathcal{G}_F = C_2 * ... * C_2$, then $\varphi : W/W^{(3)} \to \mathcal{G}_F$ such that $\varphi(\overline{s_i}) = \sigma_i$ is an isomorphism.$\square$

3.4 Conclusion

A person who speaks several languages may obtain insights which a person who speaks one language, may not be able to reach.

Galois theory contains at least two languages: Field theory and group theory. Their appearance and music are very different, yet remarkably there is a translation. After suitable translations of some problems which may have appeared impossible in field theory for example, these same problems were able to be solved in group theory.

Murray Marshall's classification of finite spaces of orderings is a remarkable achievement in the theory of formally real fields. This classification is beautiful and nontrivial. The proofs are sometimes rather mysterious and puzzling.

The first goal of this thesis was to unveil some of this mystery by translating M. Marshall's work to Galois theory. This was possible because of the work of J. Mináč and M. Spira, who detected orderings of fields using small pro-2-quotients of absolute Galois groups. They built on the previous classical work of E. Artin, O. Schreier and E. Becker.

In this thesis we showed that some of the proofs in Marshall's work have become transparent, and related to some nice group theoretical properties of Galois groups. Further, remarkably, this led to a direct, interesting classification of some canonical quotients of absolute Galois groups of Pythagorean formally real fields with finitely many square classes.

Some consequences of detecting the entire structure of some of these Galois

groups using only very simple invariants, are fascinating. The main open problem is to extend this classification to all Pythagorean formally real fields.

Can one generalize these techniques also for nonformally real fields?

The world which has opened up to us is a very rich, multilingual world. One should speak in the language of Galois theory, orderings, valuations, K-theory, cohomology, Steenrod operations, and Massey products. If one is fluent in all of these languages, then one may hope to appreciate the beauty, mystery, and possibly the solutions of some of the burning key questions in current Galois theory and arithmetic algebraic geometry.

Bibliography

[AEJ] J. Arason, R. Elman and B. Jacob, The Graded Witt Ring and Galois Cohomology,CNS Conf.Proc.2(1984),17-50

[AT] E. Artin, J. Tate, Class Field Theory, AMS Chelsea Publishing, 2009.

[Be] L. Berman, The Kaplansky Radical and Values of Binary Quadratic Forms over Fields,PhD. Thesis University of California, Berkely, California, 1978.

[EM1] I. Efrat, J. Mináč, On the descending central sequence of absolute Galois groups. Amer. J. Math. 133 (2011), no. 6, 1503-1532.

[EM2] I. Efrat, J. Mináč, Small Galois Groups that Encode Valuations, Acta Arithmetica 156 (2012), 7-17.

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

[Ka] R. Kane, Reflection Groups and Invariant theory, CMS books in mathematics 5, 2001.

[La1] T.Y. Lam, The Algebraic Theory of Quadratic Forms, mathematics lecture note series, (1973) .

[La2] T.Y. Lam, Orderings Valuations and Quadratic forms, CBMS Regional Conference, AMS, No 52. (1983) .

[La3] T.Y. Lam, Introduction to Quadratic forms over fields,Graduate studies in Mathematics, Vol 67, 2005.

[M1] M. Marshall, Classification Of Finite Spaces Of Orderings Can J, Math, Vol XXXI, No 2,1979 pp 320-330.

[M2] M. Marshall, Abstract Witt Rings,Queen's Papers in Pure and Appl.Math.57, Queen's University, Kingston, Ontario, Canada, 1980.

[MI1] J. Mináč, Galois Groups of some 2-extensions of Ordered Fields, C.R.Math.Rep.Acad.Sci.Canada, Vol.8,1986 (103-108).

[MI2] J. Mináč, Galois Groups, Order Space and Valuations, PhD Thesis, Queen's University, (1986).

[MI3] J. Mináč, Remark about the sets $O(n)$ in the theory of ordered fields C.R Math.Acad.Sci.Canada-Vol.XI,No. 2, (1987), 125-129.

[MS] J. Mináč, T. Smith, Decomposition of Witt rings and Galois group Can.J.Math. Vol. 47(6), 1995 pp. 1274-1289.

[MS1] J. Mináč , M. Spira, Formally real field, Pythagorean fields,C-fields and W-group,Math.Z 205(1990), 519-530.

[MS2] J. Mináč, M. Spira, Witt Rings and Galois Groups, Annals of Mathematics, Vol. 144, 1996, pp. 35-60.

[Mz] J.L. Merzel, Quadratic forms over fields with finitely many orderings,Contemporary Mathematics, AMS, Vol 8, (1982), pp. 185-229.

[Wr] R. Ware, Valuation Rings and Rigid Elements in Fields, Canad, J. Math 33(1981), 1338-1355.

Curriculum Vitae

Fatemeh Bagherzadeh Golmakani

Last Updated September 2013

Department of Mathematics, University of Western Ontario
London, Ontario Canada

EDUCATION

- **PhD student in Pure Mathematics ,** University of Western Ontario,London, Canada
  (Supervisor: Professor Ján Mináč)
- **M.Sc. in Mathematics,** Shahid Bahonar University of Kerman, Kerman, Iran 2001-2003
- **B.Sc. in Mathematics,** Shahid Bahonar University of Kerman, Kerman, Iran, 1997-2001

FIELDS OF INTEREST

Galois groups of maximal p-extensions,Valuation Theory and Quadratic Forms, Field Theory

AWARDS

- **The first rank graduate's award**, M.Sc. Shahid Bahonar University, Iran, 2003
- **Fifth place,** The 24th National Competition of Mathematics Students, Tehran, Iran, 2000,

ATTENDED WORKSHOPS AND SCHOOLS

- **First conference in algebraic topology and Geometry**, Amirkabir University, Tehran ,Iran, January 2001
- **Second conference in algebraic topology and Geometry**, Tabriz , Tehran ,Iran, summer 2003
- **Conference on Homotopy theory and derived algebraic geometry** Fields Institute, Toronto, Canada, September , 2010
- **Conference on K-theory and Motives, on the occasion of the 60th birth- day of Andrei Suslin**, Los Angeles (CA),March 2011

TEACHING EXPERIENCE

- **Instructor**
  - Fall 2005
    - General mathematics I(Calculus I), Shahid Bahonar University of Kerman, Kerman, Iran
  - Winter 2006
    - General mathematics II(Advanced Calculus), Shahid Bahonar University of Kerman, Iran
    - Discrete mathematics, Shahid Bahonar University of Kerman, Iran
  - Summer 2006
    - General mathematics I(Calculus I), Shahid Bahonar University of Kerman, Iran
  - Summer, Fall 2007
    - Preparing class for Mathematics Olympiad for high school student, Mathematics Home, Kerma, Iran.
    - Elementary Calculus, Azad University, Bardsir, Kerman, Iran.
- **Teaching Assistant**, Department of Mathematics University of Western Ontario, 2009-2013:
  - Elementary Calculus, Advanced Calculus, linear Algerbra, Finite Math, Intermediate calculus, Galois Theory, Algebraic number theory.

COMPUTER SKILLS

- Microsoft Office, Latex,

REFERENCES

- Ján Mináč, Professor, Department of Mathematics, University of Western Ontario, London, Ontario , Canada

- Masoud Khalkhali, Professor, Department of Mathematics, University of Western Ontario, London, Ontario, Canada