Additive structure of multiplicative subgroups of fields and Galois theory

Louis Mahé, Ján Mináč *†, and Tara L. Smith ‡

Abstract. One of the fundamental questions in current field theory, related to Grothendieck's conjecture of birational anabelian geometry, is the investigation of the precise relationship between the Galois theory of fields and the structure of the fields themselves. In this paper we initiate the classification of additive properties of multiplicative subgroups of fields containing all squares, using pro-2-Galois groups of nilpotency class at most 2, and of exponent at most 4. This work extends some powerful methods and techniques from formally real fields to general fields of characteristic not 2.

Contents

§1. Introduction

Let F be a field of characteristic not 2 and T be a multiplicative subgroup of $\dot{F} = F \setminus \{0\}$ containing the squares. By the additive structure of T, we mean a description of the T-cosets forming $T + aT$. The purpose of this article is to relate the additive structure of such a group T, to some Galois pro-2-group H associated with T. In the case when T is a usual ordering, the group H is a group of order 2. In the general case, H is a pro-2-group

1991 *Mathematics Subject Classification.* Primary 11E81; Secondary 12D15.

The two first authors were supported by the Volkswagen-Stiftung (RIP-Program at Oberwolfach)

* Research supported in part by the Natural Sciences and Engineering Research Council of Canada and by the special Dean of Science Fund at the University of Western Ontario.

† Supported by the Mathematical Sciences Research Institute, Berkeley

‡ Research supported in part by the Taft Memorial Fund of the University of Cincinnati

of nilpotency class at most 2, and of exponent at most 4. Therefore the structure of H is relatively simple, and this is one of the attractive features of this investigation.

One of our main motivations is to extend Artin-Schreier theory to this general situation. In classical Artin-Schreier theory as modified by Becker, one studies euclidean closures and their relationship with Galois theory [ArSch1, ArSch2, Be1]. Recall that such a closure is a maximal 2-extension of an ordered field to which the given ordering extends. (See [Be1].)

It came as a surprise to us that for a good number of isomorphism types of groups H as above, we could provide a complete algebraic characterization of the multiplicative subgroups of $\dot{F}/\dot{F}^2$ associated with H, entirely analogous to the classical algebraic description of orderings of fields. We thus obtain a fascinating direct link between Galois theory and additive properties of multiplicative subgroups of fields.

We obtain in particular a Galois-theoretic characterization of rigidity conditions (Proposition 3.4 and Proposition 3.5) and a full classification of rigid groups T (§7). We also know how to make closures (as defined below) with respect to these rigid "orderings" (§8).

In §9 we refine the notion of H-orderings of fields. We show that under natural conditions, we can control the behaviour of the additive structure of these orderings under quadratic extensions. It is worthwhile to point out that each finite Galois 2-extension can be obtained by successive quadratic extensions. Therefore, it is sufficient to investigate quadratic extensions.

We have in §2 a nice illustration of what a W-group can or cannot be. Since the W-group of the field F, together with its level, determines the Witt ring $W(F)$, it is clear that every result about the W-group of F and its subgroups will provide information on $W(F)$.

This fits together with one of the main ideas behind this work (see §10): obtaining new Local-Global Principles for quadratic forms, with respect to these new "orderings". This will be the subject of a subsequent article.

We now enter into more detail, fix some notation, and present a more technical outline of the structure of the paper.

Notation 1.1. All fields in this paper are assumed to be of characteristic not 2, with any exceptions clearly pointed out. Occasionally we denote a field extension K/F as $F \longrightarrow K$. The compositum of two fields K and L contained in a larger field is denoted as KL. Recall that the *level* of a field F is the smallest natural number $n > 0$ such that -1 is a sum of n squares in F or ∞ if no such n exists. Given a field F, we denote by $F(\sqrt{\dot{F}})$ the compositum of all quadratic extensions of F, and by $F^{(3)}$ the compositum of all quadratic extensions of $F(\sqrt{\dot{F}})$ which are Galois over F. (The field $F(\sqrt{\dot{F}})$ was denoted by $F^{(2)}$ in previous papers (e.g. [MiSm2]), and this explains the notation $F^{(3)}$.) The W-group of the field F is then defined as $\mathcal{G}_F = \mathrm{Gal}(F^{(3)}/F)$. This W-group is the Galois-theoretic analogue of the Witt ring, in that if two fields have isomorphic Witt rings, then their W-groups are also isomorphic. Conversely, if two fields have isomorphic W-groups, then their Witt rings are also isomorphic (provided that the fields have the same level when the quadratic form $\langle 1, 1\rangle$ is universal over one of the fields (See [MiSp2, Theorem 3.8])).

We denote by $\Phi(\mathcal{G}_F)$ the Frattini subgroup of $\mathcal{G}_F$. The Frattini subgroup is by definition the intersection of the maximal proper subgroups H of $\mathcal{G}_F$. (This means that H is a maximal subgroup of $\mathcal{G}_F$ among the family of all closed subgroups of $\mathcal{G}_F$ not equal to $\mathcal{G}_F$. It is a basic fact in the theory of pro-2-groups that each such subgroup of $\mathcal{G}_F$ is a closed subgroup of $\mathcal{G}_F$ of index two.) Notice that $\mathrm{Gal}(F^{(3)}/F(\sqrt{\dot{F}})) = \Phi(\mathcal{G}_F)$. In the case of a pro-2-group G, the Frattini subgroup is exactly the closure of the group generated by squares. Observe that for each closed subgroup H of $\mathcal{G}_F$ we have $\Phi(H) \subseteq \Phi(\mathcal{G}_F) \cap H$. We say that a closed subgroup $H \subseteq \mathcal{G}_F$ satisfying $\Phi(H) = H \cap \Phi(\mathcal{G}_F)$ is an *essential* subgroup of $\mathcal{G}_F$. Two essential subgroups H_1, H_2 are *equivalent* if $H_1\Phi(\mathcal{G}_F) = H_2\Phi(\mathcal{G}_F)$. In general, for a closed subgroup H of $\mathcal{G}_F$, we have $H = \mathcal{E} \times \prod_i (\mathbb{Z}/2\mathbb{Z})_i$ where $\mathcal{E}$ is essential: $\Phi(H) = \Phi(\mathcal{E})$ and $\Phi(\mathcal{G}_F) \cap H \cong \Phi(\mathcal{E}) \times \prod_i (\mathbb{Z}/2\mathbb{Z})_i$. The equivalence class of $\mathcal{E}$ is that of H, and equivalent essential subgroups are always isomorphic. (See [CrSm, Theorem 2.1].)

Remark. For typographical reasons we are using two different notations for the action of a Galois element σ on a field element x: the exponential notation x^σ and the functional notation $\sigma(x)$. This should not cause confusion, as in any given instance the order in which the elements enter the products will be clear or is irrelevant.

We now give the field-theoretic interpretation of the notion of an essential subgroup of $\mathcal{G}_F$. Let H be any closed subgroup of $\mathcal{G}_F$ and let L be the fixed field of H. Let N and M be the fixed fields of $\Phi(H)$ and $\Phi(\mathcal{G}_F) \cap H$ respectively. Because $\Phi(H) \subseteq \Phi(\mathcal{G}_F) \cap H$, we see that $M \subseteq N$ and equality holds for one of the inclusions if it holds for the other. Finally observe that M is the compositum of $F(\sqrt{\dot{F}})$ and L, and that N is the compositum of all quadratic extensions of L contained in $F^{(3)}$. Summarizing the discussion above we obtain:

Proposition 1.2. *Let H be a closed subgroup of $\mathcal{G}_F$ and L be the fixed field of H. Then H is an essential subgroup of $\mathcal{G}_F$ if and only if the maximal multiquadratic extension of L contained in $F^{(3)}$ is equal to the compositum of L and $F(\sqrt{\dot{F}})$.*

Kummer theory and Burnside's Basis Theorem allow us to prove the following:

Proposition 1.3. *For H a closed subgroup of $\mathcal{G}_F$, the assignment*

$$H \mapsto u(H) = P_H := \{a \in \dot{F} \mid (\sqrt{a})^\sigma = \sqrt{a}, \quad \forall \sigma \in H\}$$

induces a $1-1$ correspondence between equivalence classes of essential subgroups of $\mathcal{G}_F$ and multiplicative subgroups of $\dot{F}/\dot{F}^2$.

Proof. Recall from Kummer theory that $\mathrm{Gal}(F(\sqrt{\dot{F}})/F)$ is the Pontrjagin dual of the discrete group $\dot{F}/\dot{F}^2$ under the pairing $(g, [f]) = g(\sqrt{f})/\sqrt{f}$ of $\mathrm{Gal}(F(\sqrt{\dot{F}})/F)$ with $\dot{F}/\dot{F}^2$, with values in $\mathbb{Z}/2\mathbb{Z} \cong \{\pm 1\}$. (See [ArTa, Chapter 6].)

Assume that H_1 and H_2 are two essential subgroups of $\mathcal{G}_F$ such that $P_{H_1} = P_{H_2} =: P$. This means $\frac{H_1\Phi(\mathcal{G}_F)}{\Phi(\mathcal{G}_F)} = \frac{H_2\Phi(\mathcal{G}_F)}{\Phi(\mathcal{G}_F)}$ because they are both the annihilator of P under the pairing above. (See [Mo, Chapter 5].)

Therefore, by considering the natural map $\mathcal{G}_F \longrightarrow \mathrm{Gal}(F(\sqrt{\dot{F}})/F)$ and the inverse image of $\frac{H_1\Phi(\mathcal{G}_F)}{\Phi(\mathcal{G}_F)} = \frac{H_2\Phi(\mathcal{G}_F)}{\Phi(\mathcal{G}_F)}$ in $\mathcal{G}_F$, we can conclude that $H_1\Phi(\mathcal{G}_F) = H_2\Phi(\mathcal{G}_F)$. This proves that u is injective on equivalent classes of essential subgroups.

In order to show that it is surjective, consider any subgroup P of $\dot{F}$ containing $\dot{F}^2$. In the $\mathbb{F}_2$-vector space $\dot{F}/\dot{F}^2$, the subspace $P/\dot{F}^2$ may be written as $P = \bigcap_{i\in I} P_i$ where each

P_i is a hyperplane and I is minimal with this property. Then again by Kummer theory and Pontrjagin's duality, there exist elements $\sigma_i \in \mathcal{G}_F, i \in I$ such that $P_{\langle\sigma_i\rangle} = P_i$ for each $i \in I$. (Here $\langle\sigma_i\rangle$ is the group generated by σ_i in $\mathcal{G}_F$.)

Set $H := \langle\sigma_{i|\, i\in I}\rangle$, the closure of the subgroup of $\mathcal{G}_F$ generated by $\sigma_i, i \in I$. Then from Burnside's Basis Theorem for pro-2-groups (see e.g. [Koc, Chapter 6] or [Hal, Chapter 12]), we see that $\{\sigma_i, i \in I\}$ form a minimal set of generators of H and their images modulo $\Phi(H)$ form a topological $\mathbb{F}_2$-basis of $H/\Phi(H)$. From the choice of the σ_i's we have

$$\frac{H}{H \cap \Phi(\mathcal{G}_F)} \cong \frac{H.\Phi(\mathcal{G}_F)}{\Phi(\mathcal{G}_F)} \cong \prod_I \mathbb{Z}/2\mathbb{Z} = \prod_{i\in I}\langle\bar{\sigma_i}\rangle$$

where $\bar{\sigma_i}$ is the image of σ_i in $\frac{H.\Phi(\mathcal{G}_F)}{\Phi(\mathcal{G}_F)}$. On the other hand $\frac{H}{\Phi(H)} \cong \prod_{i\in I}\langle\bar{\sigma_i}\rangle$. Hence, the natural homomorphism $\frac{H}{\Phi(H)} \longrightarrow \frac{H}{\Phi(\mathcal{G}_F)\cap H}$ is an isomorphism and $\Phi(H) = \Phi(\mathcal{G}_F) \cap H$ as desired. This shows that H is essential. Since $P_H = \bigcap_{i\in I} P_i = P$, u is surjective and the proof is complete. $\square$

The motivation for this study of essential subgroups grew out of the observation in [MiSp1] that for $H \cong \mathbb{Z}/2\mathbb{Z}$, if $P_H \neq \dot{F}/\dot{F}^2$ (i.e. if $H \cap \Phi(\mathcal{G}_F) = \{1\}$), then P_H is in fact the positive cone of some ordering on F. The reader is referred to [L2] for further details on orderings and connections to quadratic forms. Some convenient references for basic facts on quadratic forms are [L1] and [Sc].

Since the presence or absence of $\mathbb{Z}/2\mathbb{Z}$ as an essential subgroup of $\mathcal{G}_F$ determines the orderings or lack thereof on F, one wonders whether other subgroups of $\mathcal{G}_F$ also yield interesting information about F. We make the following definition.

Definition 1.4.

(1) Let $\mathcal{C}$ denote the category of pro-2-groups of exponent at most 4, for which squares and commutators are central. (Observe that since each commutator is a product of (three) squares, it is sufficient to assume that all squares are central.) All W-groups are in category $\mathcal{C}$. See [MiSm2] for further details. Note that $\mathcal{C}$ is a full subcategory of the category of pro-2-groups. This allows us to freely use all of the properties of pro-2-groups.

(2) Let H be an isomorphism type of groups. An embedding $\varphi\colon H \longrightarrow \mathcal{G}_F$ is an *essential embedding* if $\varphi(H)$ is an essential subgroup of $\mathcal{G}_F$. Note that if H embeds in $\mathcal{G}_F$, then H has to be in category $\mathcal{C}$.

(3) An *H-ordering* on F is a set $P_{\varphi(H)}$ where φ is an essential embedding of H in $\mathcal{G}_F$.

(4) Let (F,T) be a field with an H-ordering T. We say that (L,S) *extends* (F,T) if L is an extension field of F in the maximal Galois 2-extension $F(2)$ of F, S is a subgroup of $\dot{L}$ containing $\dot{L}^2$, $T = S \cap \dot{F}$, and the induced injection $L/S \longrightarrow \dot{F}/T$ is an isomorphism. We also say (L,S) is a *T-extension* of F. (We will see in Propositions 4.1 and 4.2 that maximal T-extensions always exist, and that a maximal such extension (L,S) in $F(2)$ has $S = \dot{L}^2$.) An extension (L,S) of (F,T) is said to be an *H-extension* if S is an H-ordering of L.

(5) An extension (L,S) of (F,T) is called an *H-closure* if it is a maximal T-extension which is also an H-extension. Note this implies $T = \dot{L}^2$ and $\mathcal{G}_L \cong H$. Note also that we

will not consider maximal H-extensions (K,S), because in general they need not satisfy $S=\dot{K}^2$.

We set the following notation: C_n denotes the cyclic group of order n, D denotes the dihedral group of order 8, Q denotes the quaternion group of order 8.

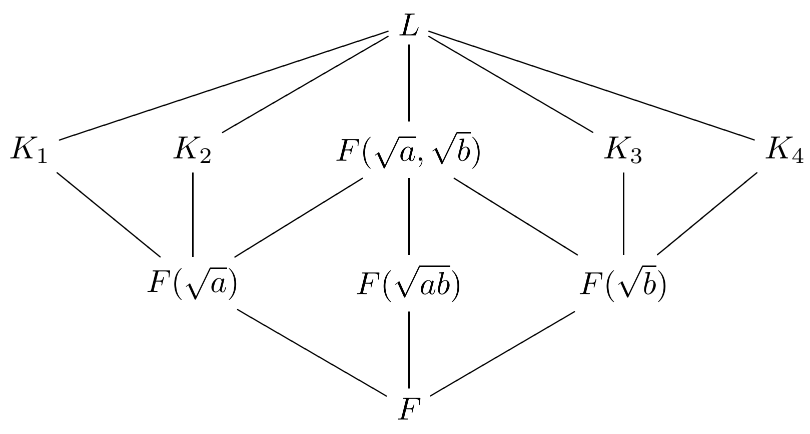
If G_1 and G_2 are in $\mathcal{C}$, we denote by $G_1 * G_2$ the free product (i.e. the coproduct) of the two groups in category $\mathcal{C}$. Then G_1 and G_2 are canonically embedded in $G_1 * G_2$ and the latter can be thought of as $(G_1 \times [G_1,G_2]) \rtimes G_2$ with the obvious action of G_2 on the inner factor. (See [MiSm2].) For example, $D \cong C_2 * C_2$.

Let $a \in \dot{F}\backslash\dot{F}^2$. By a C_4^a-extension of a field F, we mean a cyclic Galois extension K of F of degree 4, with $F(\sqrt{a})$ as its unique quadratic intermediate extension. Let $a,b\in\dot{F}$, independent modulo $\dot{F}^2$. By a $D^{a,b}$-extension of F we mean a dihedral Galois extension L of F of degree 8, containing $F(\sqrt{a},\sqrt{b})$, for which $\mathrm{Gal}(L/F(\sqrt{ab}))\cong C_4$. Observe that any C_4-extension is a C_4^a-extension for an $a\in F$, and that any D-extension is a $D^{a,b}$-extension for suitable $a,b\in\dot{F}$.

The following result is not hard to prove, and is a special case of more general results in [Fr]. (See also [L1, Exercise VII.8].)

Proposition 1.5. *There exists a C_4^a-extension of F if and only if $a\in\dot{F}\setminus F^2$ and the quaternion algebra $\left(\frac{a,a}{F}\right)$ is split. There exists a $D^{a,b}$-extension of F if and only if $a,b\in\dot{F}$ are independent modulo squares and the quaternion algebra $\left(\frac{a,b}{F}\right)$ is split.*

This proposition is actually one of the main tools we use to link the Galois-theoretic properties of an essential subgroup H of $\mathcal{G}_F$ to the algebraic properties of an H-ordering. Since we will need to refer to such extensions often in the sequel, we sketch the subfield lattice of a $D^{a,b}$-extension L/F.



The paper is organized as follows.

In §2, we show that the only abelian groups which can appear as essential subgroups of a W-group are C_2 and $(C_4)^I$ where I is some nonempty set. We also determine the possible nonabelian subgroups generated by two elements. In Theorem 2.7 we provide a strong restriction on possible finite subgroups of a W-group. Some of these results are important in determining the cohomology rings of W-groups.

In §3 we show how properties of an H-ordering T, such as stability under addition or rigidity, may be described in a Galois-theoretic way. The definition and first properties of extensions and closures are given in §4. We illustrate with Proposition 4.9 that even in a very geometric situation, we cannot expect that every H-ordering T admits a closure. We also point out (Proposition 4.10) that this leads to a negative answer to a strong version of the question asked in [Ma]: we produce an example of a field F having no field extension $F \longrightarrow K$ with $W_{red}(K) \cong W(K)$, such that the induced map $W_{red}(F) \longrightarrow W_{red}(K)$ is an isomorphism. (See also [Cr2, Theorem 5.5], from which one can also extract such examples. We address Craven's result in §4.) Later in §8 we are able to provide a similar example of a field F with a subgroup T of $\dot{F}$ such that the associated Witt ring $W_T(F)$ is isomorphic to $W(\mathbb{Q}_p), p \equiv 1(4)$ but again there is no field extension $F \longrightarrow K$ inducing the isomorphism $W_T(K) \cong W(K)$. This example is interesting because $\mid \dot{F}/T \mid$ is finite. (For details see Example 8.14 and the remark following this example.)

In §5 and §6 we study the case of essential subgroups H generated by 1 or 2 elements, and show that they admit closures.

In §7 we give a complete Galois-theoretic, as well as an algebraic classification of rigid orderings, and in §8 we show that they admit closures, provided that in the case of $C(I)$, the associated valuation is not dyadic. (See Theorem 8.15 and Example 8.14.) In Example 6.4 we see that the link between the additive structure of an H-ordering and the Galois-theoretic properties of H is not as tight as we might have expected. This leads us to investigate this question more thoroughly in §9. Actually, with a few natural extra requirements on the Galois groups we are considering, this can be fixed. We are then able to obtain a perfect identification between the two aspects.

As we have already said, application of this theory to local-global principles for quadratic forms will constitute the core of a subsequent paper. In the conclusion we illustrate by an easy example, what we intend to do in this direction.

The authors would like to acknowledge Professors A. Adem, J.-L. Colliot-Thélène, T. Craven, B. Jacob, D. Karagueuzian, J. Koenigsmann, T.-Y. Lam, D. Leep and H. W. Lenstra, Jr. for valuable discussions concerning the results in this paper; and also the hospitality of the Mathematical Sciences Research Institute at Berkeley, the Department of Mathematics at the University of California at Berkeley, and the Mathematisches Forschungsinstitut at Oberwolfach, which the authors were privileged to visit during the preparation of this paper.

§2. Groups not appearing as subgroups of W-groups

In this section we show that no essential subgroup of $\mathcal{G}_F$ can have C_2 as a direct factor (except in the trivial case where the subgroup is C_2), nor can Q appear as a subgroup of $\mathcal{G}_F$. These two facts will then be used to show that the four nonabelian groups $C_2 * C_2 = D, C_2 * C_4, C_4 \rtimes C_4$ and $C_4 * C_4$, together with the abelian group $C_4 \times C_4$, comprise all of the possible two-generator essential subgroups of W-groups. Thus we have a good picture of the minimal realizable and unrealizable subgroups. We further show that every finite subgroup of a W-group is in fact an "S-group" as defined in [Jo]. (We shall call such groups "split groups" here.) The fact that Q is not a subgroup of $\mathcal{G}_F$ is actually a consequence of this last result.

We often use the fact that there is a perfect $\mathbb{F}_2$-vector space duality between the relations among the generators of $\mathcal{G}_F$ and the F-quaternion algebras in $\mathrm{Br}(F)$, the Brauer group of F. (For a detailed exposition of this duality, see [MiSp2, Theorem 2.20].)

Briefly, this duality occurs as follows: let $a_i, i \in I$ form a basis for the $\mathbb{F}_2$-vector space $\dot{F}/\dot{F}^2$, where by abuse of notation we identify an element $a \in \dot{F}$ with its image in $\dot{F}/\dot{F}^2$. We can choose a minimal set of (topological) generators $\sigma_i, i \in I$ for $\mathcal{G}_F$ having the property that $\sigma_i(\sqrt{a_i}) = -\sqrt{a_i}$, and σ_i fixes $\sqrt{a_j}$ for $i \neq j$. Then the quaternion algebra $(\frac{a_i, a_i}{F})$ is viewed as "corresponding to" the square σ_i^2, and the quaternion algebra $(\frac{a_i, a_j}{F}), i \neq j$ is viewed as "corresponding to" the commutator $[\sigma_i, \sigma_j]$. (Because the quaternion algebras $(\frac{a_i, a_j}{F})$ and $(\frac{a_j, a_i}{F})$ are isomorphic and $[\sigma_i, \sigma_j] = [\sigma_j, \sigma_i]$ we see that the order of i and j is irrelevant, and we consider each quaternion algebra and each commutator only one time.)

In order to explain this pairing in a more detailed way, we set $U := \prod_i (C_2)_i \times \prod_{(i,j)} (C_2)_{(i,j)}$ to be a topological group with the product topology, where each $(C_2)_i, i \in I$ is a discrete group of order 2 with a formal generator σ_i^2 and each $(C_2)_{(i,j)}$ is a discrete group of order 2 with a formal generator $[\sigma_i, \sigma_j], i, j \in I, i \neq j$, and with the understanding that $[\sigma_i, \sigma_j] = [\sigma_j, \sigma_i]$ so that $(C_2)_{(i,j)} = (C_2)_{(j,i)}$.

We also set P to be a set of degree 2 homogeneous polynomials in variables $Z_i, i \in I$ over a field $\mathbb{F}_2$.

Then by Pontrjagin's duality we have a perfect pairing $U \times P \longrightarrow \{\pm 1\}$ such that the topological basis $\{\sigma_i^2, [\sigma_i, \sigma_j], i \in I, (i,j)$ is an unordered pair of distinct elements in $I\}$ of U is orthogonal to the vector basis $\{Z_i^2, Z_i Z_j, i \in I, (i,j) \in I \times I, i \neq j\}$. Then we have a homomorphism $\psi \colon P \longrightarrow \mathrm{Br}(F)$ such that $\psi(Z_i^2)$ is the class of $(\frac{a_i, a_i}{F})$ in $\mathrm{Br}(F)$ and $\psi(Z_i, Z_j)$ is the class of $(\frac{a_i, a_j}{F})$ in $\mathrm{Br}(F)$. The kernel Q of ψ may be thought of as the group of relations between the products of quaternion algebras $(\frac{a_i, a_i}{F})$ and $(\frac{a_i, a_j}{F}), i, j \in I, i \notin j$ in $\mathrm{Br}(F)$.

The key fact proved in [MiSp2, Theorem 2.20] tells us that the group of relations ν between the products of σ_i^2 and $[\sigma_i, \sigma_j], i \in I, i, j \in I, i \neq j$ is the annihilator of Q under the pairing above. This allows us to conclude that the pairing between U and P induces Pontrjagin's duality between ν and the group of quaternion algebras in $\mathrm{Br}(F)$. (See [MiSp2, Corollary 2.21].)

Using this Pontrjagin duality, we can say informally that the relations among the generators of $\mathcal{G}_F$ which may all be expressed as products of squares and commutators of elements $\sigma_i, i \in I$, are "dual" to the corresponding product of quaternion algebras in $\mathrm{Br}(F)$. In particular, this means that if σ_i, σ_j correspond to linearly independent elements a_i, a_j in $\dot{F}/\dot{F}^2$ over $\mathbb{F}_2$, respectively, under this dual relation, then if $(\frac{a_i, a_i}{F}) = 1 \in \mathrm{Br}(F)$, σ_i^2 will not appear in any of the relations for $\mathcal{G}_F$, and if $(\frac{a_i, a_j}{F}) = 1 \in Br(F), i \neq j$, then $[\sigma_i, \sigma_j]$ will not appear in any of the relations for $\mathcal{G}_F$.

Lemma 2.1. [Mi1], [CrSm] *The groups $C_2 \times C_2$ and $C_4 \times C_2$ cannot be realized as essential subgroups of $\mathcal{G}_F$ for any field F.*

Proof. Assume $H = \langle \sigma, \tau \mid \sigma^2 = \tau^2 = [\sigma, \tau] = 1 \rangle \subseteq \mathcal{G}_F$ or $H = \langle \sigma, \tau \mid \sigma^2 = [\sigma, \tau] = 1, \tau^4 = 1 \rangle$, and assume $\sigma, \tau, \sigma\tau \notin \Phi(\mathcal{G}_F)$. Then $-1 \notin \dot{F}^2$, for if $-1 \in \dot{F}^2$, we would have

$(\frac{a,a}{F}) = 1 \in Br(F)$ for all $a \in \dot{F}$. This means, in the relations for $\mathcal{G}_F$, no "squared terms" appear. But if H is a subgroup of $\mathcal{G}_F$, then σ^2 appears as a relation in $\mathcal{G}_F$.

Now consider a $D^{a,-a}$-extension L/F, where $\sqrt{a}$ is not fixed by σ. Such an extension exists since $\sigma \notin \Phi(\mathcal{G}_F)$, $|\dot{F}/\dot{F}^2| \geq 4$, and $-1 \notin \dot{F}^2$. Consider $\langle \bar{\sigma}, \bar{\tau} \rangle$, the image of H in $\mathrm{Gal}(L/F)$. We have $\bar{\sigma}^2 = 1$, so the fixed field of $\bar{\sigma}$ is of index 2 in L and does not contain $\sqrt{a}$. This means it cannot contain $\sqrt{-1}$ either, but must be one of the two extensions of F of degree 4 sitting over $F(\sqrt{-a})$, so $(\sqrt{-1})^{\sigma} = -\sqrt{-1}$. Now choose an element $b \in \dot{F} \backslash \dot{F}^2$ for which $\sqrt{b}^{\sigma} = \sqrt{b}$ and $\sqrt{b}^{\tau} = -\sqrt{b}$. Such an element b exists since $\sigma, \tau, \sigma\tau \notin \Phi(\mathcal{G}_F)$. Consider the image $\langle \bar{\sigma}, \bar{\tau} \rangle$ of H inside the Galois group G of a $D^{b,-b}$-extension K of F. (Because $(\sqrt{-1})^{\sigma} = -\sqrt{-1}$ we see that $-b$ is not a square in F, and we can conclude that the elements b and $-b$ are linearly independent when they are considered as elements in $\dot{F}/\dot{F}^2$.) The fixed field K_σ of $\bar{\sigma}$ cannot contain $\sqrt{-b}$, so it must be one of the two subfields of index 2 in K not containing $\sqrt{-b}$. On the other hand, the fixed field K_τ of τ cannot contain $\sqrt{b}$, so considering the subfield lattice, we see that $K_\sigma \cap K_\tau = F$. Then the image of H in G generates G, which means σ and τ cannot commute. This is a contradiction, so H cannot exist as an essential subgroup of $\mathcal{G}_F$. □

From the lemma above we immediately obtain the following result, which is used in [AKMi] to investigate those fields F for which the cohomology ring $H^*(\mathcal{G}_F)$ is Cohen-Macaulay.

Corollary 2.2. *Let σ be any involution in $\mathcal{G}_F \backslash \Phi(\mathcal{G}_F)$ and set $E_\sigma = \Phi(\mathcal{G}_F) \times \langle \sigma \rangle$. Then the centralizer $Z(E_\sigma)$ of E_σ in $\mathcal{G}_F$ is E_σ itself.*

Proof. If $\tau \in Z(E_\sigma) \setminus E_\sigma$ then $[\tau, \sigma] = 1$ and $\langle \tau, \sigma \rangle = C_2 \times C_2$ or $C_4 \times C_2$, where $\langle \tau, \sigma \rangle$ is an essential subgroup of $\mathcal{G}_F$. From Lemma 2.1, this is a contradiction, and we see $\tau \in E_\sigma$ as desired. □

Corollary 2.3. *No essential subgroup of $\mathcal{G}_F$ can have C_2 as a direct factor (except in the trivial case where the subgroup is C_2).*

Proof. Since $\Phi(H \times C_2) = \Phi(H)$, if $H \times C_2$ is a subgroup with $\Phi(H \times C_2) = (H \times C_2) \cap \Phi(\mathcal{G}_F)$, then the C_2-factor is not in $\Phi(\mathcal{G}_F)$. Take any single element $\sigma \in H \backslash \Phi(H)$. Then $\langle \sigma \rangle \times C_2 \cong C_2 \times C_2$ or $C_4 \times C_2$, which cannot be an essential subgroup. Therefore neither can $H \times C_2$. □

Proposition 2.4. *The quaternion group Q cannot appear as a subgroup of $\mathcal{G}_F$.*

Proof. Suppose $Q = \langle \sigma, \tau | \sigma^2 = \tau^2 = [\sigma, \tau] \rangle \subseteq \mathcal{G}_F$. Then as in the lemma above, $-1 \notin \dot{F}^2$, since we have $\sigma^2\tau^2, \sigma^2[\sigma, \tau], \tau^2[\sigma, \tau]$ in the relations for $\mathcal{G}_F$. Consider the image of Q in any dihedral extension of F of order 8. Since Q is not isomorphic to D, this image must be a proper quotient of Q, and therefore is elementary abelian. Then the same argument as in the lemma above shows that $(\sqrt{-1})^{\sigma} = -\sqrt{-1}$. Indeed we see again that there exists a $D^{a,-a}$-extension L/F, where $\sqrt{a}$ is not fixed by σ. As we have just observed, the image $\bar{\sigma}$ of σ in $\mathrm{Gal}(L/F)$ has order at most 2, and the order must be 2 because $\sigma(\sqrt{a}) = -\sqrt{a}$. Therefore we can again conclude that $\sigma(\sqrt{-a}) = \sqrt{-a}$ and consequently $\sigma(\sqrt{-1}) = -\sqrt{-1}$. Choosing an element $b \in \dot{F} \backslash \dot{F}^2$ for which $\sqrt{b}^{\sigma} = \sqrt{b}$ and $\sqrt{b}^{\tau} = -\sqrt{b}$ as before, we can again take a $D^{b,-b}$-extension of F, and observe that the image of Q in the Galois group of this extension must generate the entire group, which is a contradiction. □

Theorem 2.5. *The only groups generated by two elements which can arise as essential subgroups of $\mathcal{G}_F$ are the five groups $C_2 * C_2$, $C_2 * C_4$, $C_4 * C_4$, $C_4 \times C_4$, and $C_4 \rtimes C_4$.*

Proof. Let H be generated by x, y. We have an exact sequence

$$1 \to \Phi(H) \to H \to C_2 \times C_2 \to 1,$$

where $\Phi(H) \cong (C_2)^k$ is generated by $x^2, y^2, [x,y]$, so $k \leq 3$. Then $|H| = 2^{k+2}$, so $|H| \leq 32$, and $|H| = 32$ if and only if $|\Phi(H)| = 8$, if and only if $H \cong C_4 * C_4$. Otherwise $|H| = 8$ or 16, and there are only a few groups to consider. If $|H| = 8$, necessarily $H \cong C_2 * C_2$, as all other groups of order 8 and exponent at most 4 either have C_2 as a direct factor or are isomorphic to Q.

There are fourteen groups of order 16; among these, five are abelian, and by Lemma 2.1 only $C_4 \times C_4$ among these can be an essential subgroup of $\mathcal{G}_F$. Among the nine nonabelian groups, two have C_2 as a direct factor, and four more have exponent 8. The remaining three are the groups $C_2 * C_4$, $C_4 \rtimes C_4$, and DC, the central product of D and C_4 amalgamating the unique central subgroup of order 2 in each group. This group, however, has Q as a subgroup (see [LaSm]), so cannot be an essential subgroup of $\mathcal{G}_F$. □

That the group Q cannot appear as a subgroup of any W-group is a special case of a more general description of the kinds of groups which can appear as essential subgroups of W-groups. All finite subgroups must in fact be "split groups", which we define next. These are the same as "S-groups" as defined in [Jo]. The quaternion group Q is not such a group.

Definition 2.6. Let G be a nontrivial finite group and $X = \{x_1, x_2, \ldots, x_n\}$ be an ordered minimal set of generators for G. We say that G satisfies the *split condition with respect to X* if $\langle x_1 \rangle \cap [G,G]\langle x_2, \ldots, x_n \rangle = \{1\}$. The group G is called a *split group* if it has a minimal generating set with respect to which it satisifies the split condition. We also take the trivial group to be a split group.

Theorem 2.7. *Let $\mathcal{G}_F$ be a W-group, and let G be any finite subgroup of $\mathcal{G}_F$. Then G is a split group.*

Proof. Each finite subgroup H of $\mathcal{G}_F$ can be written as $H = G \times \prod_1^m C_2$ for some $m \in \mathbb{N} \cup \{0\}$, where G is an essential subgroup of $\mathcal{G}_F$ [CrSm]. Thus it is enough to prove the theorem for G a finite essential subgroup of $\mathcal{G}_F$.

Then let G be such a group and let P_G be the associated G-ordering. Let $\dot{F}/P_G = \langle a_1 P_G, \ldots, a_n P_G \rangle$ so that the cosets $a_i P_G$ give a minimal generating set for $\dot{F}/P_G$. Further set $\{\sigma_1, \ldots, \sigma_n\}$ to be a minimal generating set for G such that $\sigma_i(\sqrt{a_j}) = (-1)^{\delta_{ij}}\sqrt{a_j}$ where δ_{ij} is the Kronecker delta. (This is possible because G is an essential subgroup of $\mathcal{G}_F$, so that a minimal set of generators for G can be extended to a minimal (topological) generating set of $\mathcal{G}_F$.)

Assume first that we can choose the representatives a_i in such a way that $a_1 t_1 + a_1 t_2 = f^2 \in \dot{F}^2$ for some $t_1, t_2 \in P_G$. (Note that this is equivalent to saying that $a_1 \in P_G + P_G$.) In this instance, there are two cases to consider.

First, suppose that t_1, t_2 are congruent mod $\dot{F}^2$. Then there exists $g \in \dot{F}$ such that $a_1t_1 + a_1t_1g^2 = f^2$, and so $a_1t_1f^2 = (a_1t_1)^2 + (a_1t_1g)^2$, and a_1t_1 is a sum of two squares in F which is not itself a square. Thus we have a $C_4^{a_1t_1}$-extension L of F. We claim that G satisfies the split condition with respect to $\{\sigma_1, \dots, \sigma_n\}$. Checking this condition is equivalent to showing $\sigma_1^2 \notin [G,G]\langle\sigma_2, \dots, \sigma_n\rangle$. Suppose it is not true. Then we have an identity $\sigma_1^2 \prod_{1\le i<j\le n}[\sigma_i, \sigma_j]^{\epsilon_{ij}} \prod_{k=2}^n \sigma_k^{2\epsilon_k} = 1$ in G, where $\epsilon_{ij}, \epsilon_k \in \{0,1\}$. Restricting to L we see that $\sigma_1^2|_L = 1$. This cannot be the case as σ_1 does not fix $\sqrt{a_1t_1}$. Thus in this case G is a split group.

Next suppose that $t_1\dot{F}^2 \neq t_2\dot{F}^2$. In this case we can find a $D^{a_1t_1, a_1t_2}$-extension L/F. Assuming again that G does not satisfy the split condition with respect to $\{\sigma_1, \dots, \sigma_n\}$, we again have an identity $\sigma_1^2 \prod_{1\le i<j\le n}[\sigma_i, \sigma_j]^{\epsilon_{ij}} \prod_{k=2}^n \sigma_k^{2\epsilon_k} = 1$ in G, where $\epsilon_{ij}, \epsilon_k \in \{0,1\}$. Since each of the $\sigma_i, i = 2, \dots, n$ acts trivially on $F(\sqrt{a_1t_1}, \sqrt{a_1t_2})$, we see that each $\sigma_i, i > 1$ is central when restricted to L. Thus again $\sigma_1^2|_L = 1$. But $\sigma_1|_L$ generates $\mathrm{Gal}(L/F(\sqrt{a_1t_1} \cdot \sqrt{a_1t_2})) \cong C_4$. Hence G is a split group.

Finally, assume that we cannot choose $a_1 \in P_G + P_G$. Then necessarily $P_G + P_G \subseteq P_G \cup \{0\}$. If $-1 \in P_G$, then $P_G = \dot{F}$ and $G = \{1\}$ which is a split group. Otherwise P_G is a preordering in F, and we may write $P_G = \cap_{i=1}^n P_i$ where each P_i is an ordering, and each $P_i = \{\, f \in \dot{F} \mid \sqrt{f}^{\sigma_i} = \sqrt{f}\,\}$. Then $\{\sigma_1, \dots, \sigma_n\}$ is a minimal generating set for G. Furthermore, each $\sigma_i^2 = 1$. (See [MiSp1] for details. The definition of a preordering in a field F can be found in [L2, Chapter 1], together with the basic properties of preordered rings.) Thus again we see that G is a split group. $\square$

Corollary 2.8. *Each nontrivial finite subgroup G of a W-group $\mathcal{G}_F$ can be obtained inductively from copies of C_2 and C_4 by taking semidirect products at each step. Thus we have $G = G_n \supseteq G_{n-1} \supseteq \cdots \supseteq G_1 \supseteq G_0$ where $G_0 \in \{C_2, C_4\}$, and $G_i = G_{i-1} \rtimes C_2$ or $G_i = G_{i-1} \rtimes C_4$ for each $i = 1, \dots, n$.*

Proof. We proceed by induction on the number of generators of G. The statement clearly holds for any group G generated by a single element. Let G be any (nontrivial) finite subgroup of the W-group $\mathcal{G}_F$. Then we can write $G = H \times \prod_1^m C_2$ where H is essential, and G, if not equal to H, is clearly built up as described from H, where the action in the semidirect product is trivial. We can choose a minimal set of generators $\{\sigma_1, \dots, \sigma_n\}$ for H such that H satisfies the split condition with respect to these generators. Clearly $N := [H,H]\langle\sigma_2, \dots, \sigma_n\rangle$ is a normal subgroup of H, and $H \cong N \rtimes \langle\sigma_1\rangle$, where $\langle\sigma_1\rangle \cong C_2$ or C_4. Since $N \cong \langle\sigma_2, \dots \sigma_n\rangle \times \prod_1^k C_2$ (for some positive integer k), we finish by induction. $\square$

Example 2.9. Consider the W-group $\mathcal{G}_2$ of the 2-adic numbers $\mathbb{Q}_2$. It has the presentation $\langle \sigma, \tau, \rho \mid \sigma^2[\tau, \rho]\rangle$ in the category $\mathcal{C}$ of groups of exponent at most four with squares and commutators central. (See [MiSp2, Example 4.4].) A basis for $\dot{F}/\dot{F}^2$ is given by $\{-1, 2, 5\}$, and σ may be chosen to fix $\sqrt{2}$ and $\sqrt{5}$ but not $\sqrt{-1}$, τ to fix $\sqrt{-1}$ and $\sqrt{5}$ but not $\sqrt{2}$, and ρ to fix $\sqrt{-1}$ and $\sqrt{2}$ but not $\sqrt{5}$. Then $\mathcal{G}_2$ can be constructed inductively from copies of C_4 and C_2 using semidirect products as follows:

$$\begin{aligned}
G_0 &= \langle \rho \rangle \cong C_4 \\
G_1 &= G_0 \times \langle [\sigma,\rho] \rangle \cong G_0 \times C_2 \\
G_2 &= G_1 \rtimes \langle \sigma \rangle \cong G_1 \rtimes C_4 \\
G_3 &= G_2 \times \langle [\sigma,\tau] \rangle \cong G_0 \times C_2 \\
\mathcal{G}_2 &= G_3 \rtimes \langle \tau \rangle \cong G_3 \rtimes C_4
\end{aligned}$$

Thus $\mathcal{G}_2 \cong \{[(C_4 \times C_2) \rtimes C_4] \times C_2\} \rtimes C_4$.

Corollary 2.8 is an interesting generalization of the known structure of W-groups associated with Witt rings of finite elementary type. In fact, all W-groups associated with Witt rings of finite elementary type can easily be seen to be built up from cyclic groups of order 2 or 4, using only semidirect products. First one checks that the groups associated with basic indecomposable groups are such groups. Then the group ring construction for Witt rings corresponds directly to taking a semidirect product with a cyclic group of order 4, while the direct product construction for Witt rings corresponds to taking a free product of W-groups in the appropriate category. But this in turn just involves taking a direct product with an appropriate number of copies of C_2 (representing the necessary commutators) and then taking a semidirect product with the generators of one of the initial W-groups. See [MiSm2] for details.

Corollary 2.8 is quite useful for the investigation of cohomology rings of W-groups. This is important in light of the recent proof of the Milnor Conjecture by Voevodsky [Vo]. In particular, Voevodsky's result shows that the cohomology rings of absolute Galois groups with $\mathbb{F}_2$-coefficients carry no more information about the base field than Milnor's K-theory mod 2. On the other hand, the cohomology rings of W-groups carry substantial additional information. (See [AKMi].)

Using [Jo: Cor, p. 370] and Theorem 2.7 above, we immediately obtain the following.

Corollary 2.10. *Let G be any nontrivial finite subgroup of a W-group $\mathcal{G}_F$. Then the cohomology ring $H^*(G,\mathbb{F}_2)$ contains nonnilpotent elements of degree 2, and hence of every even degree.*

§3. Galois groups and additive structures (1)

In this section we give a simple Galois-theoretic characterization of two important additive properties of H-orderings: stability under addition and rigidity. This generalizes the results on rigidity and on the realizability of certain Galois groups obtained in [MiSm1].

For the rest of this paper, unless otherwise mentioned, subgroups of $\mathcal{G}_F$ will always be *essential.* Throughout this paper we write $T+aT = \{t_1+at_2 \mid t_1,t_2 \in T\cup\{0\}, t_1+at_2 \neq 0\}$, so T and aT are always subsets of $T+aT$, and $T+aT \supseteq \dot{F}^2$. (Here T is any subgroup of $\dot{F}$ containing all squares in $\dot{F}$.)

Proposition 3.1. *Let H be a subgroup of $\mathcal{G}_F$, and T its associated H-ordering. Then H has C_4 as a quotient if and only if $T+T \neq T$.*

Proof. First assume there exists $a \in T+T$ which is not in T. Let K be the fixed field of H in $F^{(3)}$. We construct a C_4^a-extension F_1 of $F_0 = F(\sqrt{T}) = K \cap F^{(2)}$ inside $F^{(3)}$. Then

$L = KF_1$ is a C_4^a-extension of K in $F^{(3)}$, showing H has C_4 as a quotient. We may write $a = t_1+t_2$, so $a^2-at_1 = at_2$. Let $y = a-\sqrt{a}\sqrt{t_1} \in F_0(\sqrt{a})$, so $N_{F_0(\sqrt{a})/F_0}(y) = [a] \in \dot{F}_0/\dot{F}_0^2$. Then $F_1 = F_0(\sqrt{a}, \sqrt{y})$ is a C_4^a-extension of F_0. Since $yy^\sigma = y^2$ or $at_2 \in (\dot{F}_0(\sqrt{a}))^2$ for all $\sigma \in \mathrm{Gal}(F_0(\sqrt{a})/F)$, we see F_1 is Galois over F, and hence is contained in $F^{(3)}$.

Conversely, assume $T + T = T$. If $-1 \in T$, then $T = \dot{F}$ and $H = \{1\}$. If $-1 \notin T$, then T is a preordering, so T is intersection of orderings, and H is generated by involutions. (See [CrSm, Proposition 3.1].) Thus H cannot have C_4 as a quotient. $\square$

Remark. If H has a C_4-quotient, then there exists a C_4^a-extension of F_0 where we may take a to be in F. However, it is not necessarily the case that $a \in T+T$. That is, the quaternion algebra $\left(\frac{a,a}{F(\sqrt{T})}\right)$ is split, so a can be represented as the sum of two squares in $F(\sqrt{T})$, but not necessarily as the sum of two elements in T. This can be seen in Example 6.4.

The following definition generalizes the notion of the rigidity of a field, and introduces the notion of the level of T. (See [Wa, page 1349].)

Definition 3.2. Let T be a subgroup of $\dot{F}/\dot{F}^2$. We say that T has *level* s if -1 is a sum of s elements of T, and not a sum of $s-1$ elements of T. We say that this level is infinite if -1 is not such a sum for any natural number s. We say that the field F is *T-rigid*, or equivalently that T is rigid, if for every $a \notin T \cup -T$, we have $T + aT \subseteq T \cup aT$.

We have the following easy-to-prove but important property of rigid H-orderings:

Proposition 3.3. *Let T be a rigid H-ordering on F. Then*
(1) The level of T is $1, 2$ or infinite.
(2) If the level of T is 2, then $T + T = T \cup -T$.

Proof. Let T be an H-ordering of finite level $s > 1$ and let us write $-1 = a + a_s$ with $a = a_1 + \ldots + a_{s-1}$ and $a_i \in T$ for $i = 1, \ldots, s$. If $a \in T \cup -T$ then since $a \notin -T$ we see $a \in T$ and s must be 2. Thus we may assume $a \notin T \cup -T$. If T is rigid, then $-1 = a + a_s \in T + aT = T \cup aT$. This is a contradiction, proving (1).

Assume the level of T is 2. Then $-1 \in T + T$ and $T \cup -T \subseteq T + T$. Suppose there is $a \in (T + T) \setminus (T \cup -T)$ and let us write $a = s + t, s, t \in T$. Then of course $-a \notin T \cup -T$ and we have $-t = s - a \in T + (-a)T = T \cup -aT$ by rigidity. But $-t \notin T$ because the level is 2, and $-t \notin -aT$ because $a \notin T$. This is again a contradiction, proving (2). $\square$

Proposition 3.4. *Let H be a subgroup of $\mathcal{G}_F$, and let T be an H-ordering. Assume $-1 \in T$. The following are equivalent.*

(1) *F is T-rigid.*
(2) *D is not a quotient of H.*
(3) *H is abelian.*

Proof. We will show (2) $\implies$ (1) $\implies$ (3) $\implies$ (2). For the first implication, we show the contrapositive. Thus assume that F is not T-rigid. Let K be the fixed field of H, and let $F_0 = K \cap F(\sqrt{\dot{F}}) = F(\{\sqrt{t} : t \in T\})$. We will construct a D-extension F_1 of F_0 inside $F^{(3)}$. Then $L = KF_1$ will be a D-extension of K in $F^{(3)}$, showing that H has D as a quotient. Since F is not T-rigid and $-1 \in T$, there exist $a, b \in \dot{F} \setminus T$ such that $b = t_1 - at_2$, where $t_1, t_2 \in T$ but $b \notin T \cup aT$. Let $y = \sqrt{t_1} + \sqrt{a}\sqrt{t_2} \in F_0(\sqrt{a})$, and let $F_1 = F_0(\sqrt{a}, \sqrt{b}, \sqrt{y})$.

Notice that $yy^\sigma \in \{\pm y^2, \pm b\} \subseteq F_0(\sqrt{a}, \sqrt{b})^2$ for all $\sigma \in \mathrm{Gal}(F_0(\sqrt{a}, \sqrt{b})/F)$, so F_1/F is Galois, and $F_1 \subseteq F^{(3)}$. Then the usual argument (see [Sp] or [Ki, Theorem 5]) shows $\mathrm{Gal}(F_1/F_0) \cong D$.

Now assume F is T-rigid. To see that H is abelian, it is sufficient to show that for all $\sigma, \tau \in H$, the restrictions of σ, τ to any D-extension L of F commute. (This is because $F^{(3)}$ is the compositum of all quadratic, C_4- and D-extensions of F. (See [MiSp2, Corollary 2.18].) Thus if σ, τ commute on all D-extensions, they commute in $\mathcal{G}_F$.) Let $D^{a,b}$ be some dihedral quotient of $\mathcal{G}_F$, and let L be the corresponding extension of F. Denote as $\bar{\sigma}, \bar{\tau}$ the images of σ and τ in in $D^{a,b}$ and suppose $[\bar{\sigma}, \bar{\tau}] \neq 1$. Then σ, τ must each move at least one of $\sqrt{a}, \sqrt{b}$, and they cannot both act in the same way on these square roots. That implies $a, b, ab \notin T$. But $(\frac{a,b}{F})$ splits, so $b \in F^2 - aF^2 \subseteq T - aT = T + aT = T \cup aT$ by (1). Since $b \notin T$, we have $b \in aT$, which contradicts the fact that $ab \notin T$. Thus $[\sigma, \tau] = 1$.

The final implication is trivial. □

Proposition 3.5. *Let H be a subgroup of $\mathcal{G}_F$, and let T be an H-ordering. Assume $-1 \notin T$. Let K be the fixed field of H, and let H_0 be the subgroup of H which is the Galois group of $F^{(3)}/K(\sqrt{-1})$. The following are equivalent.*

(1) *F is $(T \cup -T)$-rigid.*
(2) *D is not a quotient of H_0.*
(3) *H_0 is abelian.*
(4) *Every D-extension of K in $F^{(3)}$ contains $K(\sqrt{-1})$.*

Proof. Let $S = T \cup -T$. Then S is clearly an H_0-ordering, and the equivalence of the first three statements follows from the preceding proposition. If there exists a D-extension L of K not containing $K(\sqrt{-1})$, then $L(\sqrt{-1})$ will be a D-extension of $K(\sqrt{-1})$, and H_0 will have D as a quotient. This shows (2) $\implies$ (4). Finally, assume there exist $\sigma, \tau \in H_0$ which do not commute. Then there exists some $D^{a,b}$-extension M of F such that $\mathrm{Gal}(M/F) = \langle \bar{\sigma}, \bar{\tau} \rangle$, where we denote $\bar{\sigma}$ and $\bar{\tau}$ the images of σ and τ in $\mathrm{Gal}(M/F)$. Then σ and τ each move one of a, b and cannot act in the same way on each. Thus $a, b, ab \notin S$, but $(\frac{a,b}{F})$ splits, so $b \in F^2 - aF^2 \subseteq T - aT$. This gives a D-extension MK of K, which, since $a, b, ab \notin S$, does not contain $\sqrt{-1}$. This shows (4) $\implies$ (3). □

§4. Maximal extensions, closures and examples

Given any C_2-ordering P on a field F, one can find a real closure of F with respect to that ordering, i.e. a real closed field L, algebraic over F, with $P = \dot{L}^2 \cap F$. Specifically, set $E = F(\sqrt{P})$. (This means that E is the compositum of all field extensions $F(\sqrt{p}), p \in P$.) Then E is formally real, and a real closure L of F in $\bar{F}$ contains E, $\dot{L} = \dot{L}^2 \cup -\dot{L}^2$, and $\dot{L}^2$ is an ordering of L. ($\bar{F}$ here means an algebraic closure of F.) Then $\mathrm{Gal}(\bar{F}/L)$ is $\langle \tau \rangle \cong C_2$, and we have $P = \{a \in \dot{F} | \sqrt{a}^\tau = \sqrt{a}\}$. Notice that for our purposes nothing is lost by considering a real closure of E inside $F(2)$, i.e. the euclidean closure, rather than a real closure within the algebraic closure $\bar{F}$ of F. (See [Be1].) This observation motivated the definition of H-closure given in Definition 1.4. The following two propositions show that maximal T-extensions always exist, i.e. that given any subgroup T of $\dot{F}$, containing $\dot{F}^2$, we can find a T-extension $(L, \dot{L}^2)$ of (F, T) in $F(2)$. Thus the real problem is in showing that H-closures exist, i.e. in showing that $\mathcal{G}_L \cong H$, or that we can find an H-extension which is a maximal T-extension.

Proposition 4.1. *Let T be a subgroup of $\dot{F}/\dot{F}^2$. Then (F,T) possesses a maximal T-extension.*

Proof. Let $\mathcal{S}$ be the set of T-extensions (L,S) of (F,T) inside $F(2)$, where $\mathcal{S}$ is ordered under inclusion. (See Definition 1.4 (4).) More precisely we may say that $(L_1,S_1) \leq (L_2,S_2)$ if $L_1 \subset L_2$ and $S_2 \cap L_1 = S_1$. Observe that since both (L_1,S_1) and $(L_2,S_2) \in \mathcal{S}$, we automatically have a natural isomorphism $L_1/S_1 \longrightarrow L_2/S_2$. Then $\mathcal{S}$ is nonempty, since $(F,T) \in \mathcal{S}$. Now consider a totally ordered family (F_j,T_j) in $\mathcal{S}$. Let $K = \cup F_j$, $S = \cup T_j$. We will show (K,S) is an upper bound for the family (F_j,T_j) in $\mathcal{S}$. First observe $T = S \cap F$ by definition. Thus $\dot{F}/T \cong \dot{F}_j/T_j \to \dot{K}/S$ is one-to-one. This map is also onto, since if $b \in \dot{K}$, then $b \in F_j$ for some j, and $[b]_S$ is the image of $[b]_{T_j}$. Then by Zorn's Lemma $\mathcal{S}$ contains a maximal element, which is a maximal T-extension of (F,T). $\square$

Proposition 4.2. *Let (K,S) be a maximal T-extension of (F,T). Then $S = \dot{K}^2$.*

Proof. Let $\{a_i : i \in I\}$ be a basis for $\dot{F}/T$ which lifts to a basis for $\dot{K}/S$, which we can do because $S \cap F = T$ and $\dot{K}/S \cong \dot{F}/T$. Assume $S \neq \dot{K}^2$, and choose $c \in S - \dot{K}^2$. Let $L = K(\sqrt{c})$, so $\dot{L}^2 \cap K = \dot{K}^2 \cup c\dot{K}^2 \subseteq S$, and $\{a_i : i \in I\}$ remain independent in $\dot{L}/\dot{L}^2$. Let $\{a_i : i \in I\} \cup \{b_j : j \in J\} \cup \{c\}$ be a basis for $\dot{K}/\dot{K}^2$ such that $\{b_j : j \in J\} \cup \{c\}$ forms a basis for S. Then $\{a_i : i \in I\} \cup \{b_j : j \in J\}$ can be extended to a basis $\{a_i : i \in I\} \cup \{b_j : j \in J\} \cup \{c_{j'} : j' \in J'\}$ for $\dot{L}/\dot{L}^2$. Let S' be the subgroup of $\dot{L}/\dot{L}^2$ generated by $\{b_j : j \in J\} \cup \{c_{j'} : j' \in J'\}$. Then $S' \cap K = S$, so $S' \cap F = T$, and $\dot{L}/S' \cong \dot{K}/S \cong \dot{F}/T$, contradicting the maximality of (K,S). Thus we conclude $S = \dot{K}^2$. $\square$

Corollary 4.3. *An H-ordered field (F,T) is an H-closure if and only if $T = \dot{F}^2$.*

Proof. If (F,T) is an H-closure, then it is also a maximal T-extension, and $T = \dot{F}^2$ by the preceding proposition. Conversely, suppose $T = \dot{F}^2$. Let $L \supset F$ be any proper extension of F in $F(2)$. Then L contains a quadratic extension of F, so $\dot{L}^2 \cap F \supsetneq \dot{F}^2$ and L cannot extend (F,T). This shows that (F,T) is its own maximal T-extension, and as it is an H-ordering, it is an H-closure. $\square$

Thus we see that our main task will be to show that there exists a maximal T-extension $(K,\dot{K}^2)$ for an H-ordered field, which is itself H-ordered, i.e. for which $\mathcal{G}_K \cong H$. The rest of the section is devoted to the study of usual preorderings. We will see in particular that in some important cases, usual preorderings do not admit closures. Although this is in some sense a negative result, we shall see that these examples are very interesting, and that they deserve careful analysis. (See Proposition 4.10 below.)

Suppose F is a formally real field equipped with a preordering T. By [CrSm, Proposition 3.1], T is an H-ordering for an H generated by involutions, and conversely, any H-ordering with H generated by involutions has to be a preordering. Thus, if (L,P) is an H-extension of (F,T), P is a preordering in L. In the same direction we have the following.

Lemma 4.4. *Let (F,T) be an H-ordered field with T a preordering, and assume (K,S) is an H-closure of (F,T). Then for any intermediate extension L/F of K/F, the pair $(L, L\cap S)$ is a T-extension of (F,T) and $L\cap S$ is a preordering of L.*

Proof. Because the composite of the injective maps $\dot F/T \longrightarrow \dot L/(L\cap S) \longrightarrow \dot K/S$ is bijective, each injection is bijective and the intermediate extension is a T-extension. Because T is a preordering, H is generated by involutions and S is also a preordering, forcing $L\cap S$ to be a preordering as well. □

We fix some notation. For any field k let $X(k)$ denote the space of usual orderings of k. Within this section we will sometimes assume that usual orderings contain 0. This will be clear from the context and should not cause confusion. For $U\subseteq k$, let $\hat U$ be the set of orderings of k containing U. When $U=\{g_1,\dots,g_n\}\subset k$, we will denote the Harrison open set $\hat U=\{\beta\in X(k)\mid g_1,\dots,g_n\in\beta\}$ by $D_k(g_1,\dots,g_n)$. A set of the form $D_k(g)$ will be called *principal*. If $F\longrightarrow L$ is an extension, we denote by $\pi\colon X(L)\longrightarrow X(F)$ the restriction map $\beta\mapsto\beta\cap F$.

Let us recall a few basic properties of the real spectrum which will be useful in the sequel. They can be found in [BCR, Chapter 7]. Two other very nice introductions to the real spectrum are given in [Be2] and [L3]. The *real spectrum* $\operatorname{Spec}_{\mathrm r} A$ of a ring A is the set of pairs (p,α) with p a prime ideal of A and α an ordering on the residue field $k(p)$ (the quotient field of A/p). It is equipped with a topology generalizing the Harrison topology, given by the subbasis of sets $D(f):=\{(p,\alpha)\in\operatorname{Spec}_{\mathrm r} A\mid f(\alpha)>0\in k(p)\}$, f being any element of A. When A is a field k, $\operatorname{Spec}_{\mathrm r} A$ is just the space of orderings $X(k)$. Because $p=\alpha\cap-\alpha$ we see that α already determines the prime p, and we will use α instead of (p,α). As in the field case, α may also be thought of as a subset of A, called the "positive cone" of the elements $f\in\alpha$ such that $f(\alpha)>0$ in $k(p)$. Then we may write either $f(\alpha)>0$ or $f\in\alpha$, according to our needs.

When V is an affine algebraic variety over a real closed field R, then the set of R-points $V(R)$ embeds continuously (with respect to the euclidean topology of $V(R)$) as a dense subset in $\operatorname{Spec}_{\mathrm r} R[V]$. This embedding induces a $1-1$ correspondence $C\mapsto\tilde C$ between the semi-algebraic sets of $V(R)$ and the constructible sets of $\operatorname{Spec}_{\mathrm r} R[V]$. (See [BCR, Theorem 7.2.3].)

On the other hand, the map $R[V]\longrightarrow R(V)$ induces an embedding $X(R(V))=\operatorname{Spec}_{\mathrm r} R(V)\longrightarrow\operatorname{Spec}_{\mathrm r} R[V]$ wich has the following properties (See [BCR, §7.6]):

(1) If V is smooth, the embedding is dense.

(2) For every constructible open set $C\subseteq X(R(V))$ there exists a constructible open set $D\subseteq\operatorname{Spec}_{\mathrm r} R[V]$ such that $D\cap X(R(V))=C$.

(3) If D_1,D_2 are constructible sets in $\operatorname{Spec}_{\mathrm r} R[V]$ coinciding on $X(R(V))$, then they coincide on $V(R)$ up to a positive codimensional set.

Lemma 4.5. *Let V be an algebraic variety over a real closed field R and let F denote the function field $R(V)$ of V. Any nonempty open set U of $X(F)$ contains a nonempty principal open set $D_F(u)$.*

Proof. Since we are dealing with the function field F of V, we may always assume V is affine and smooth. As any nonempty open set contains a constructible nonempty open set, we may assume $U \subseteq X(F)$ is constructible. Then we know that there exists a nonempty constructible open set U_1 in $\mathrm{Spec_r}\, R[V]$ such that $U = U_1 \cap X(F)$, and $U_2 := U_1 \cap V(R)$ is not empty. Denote by $(x_1, \dots, x_n)$ the coordinates of the ambient space $\mathbb{R}^n$ of V. Let $a = (a_1, \dots, a_n) \in U_2$. There is a ball of some radius ϵ, centered on a and contained in U_2. If $u = \sum_{i=1}^n (x_i - a_i)^2 - \epsilon$, then the ball $D(-u)$ satisfies $\emptyset \neq D(-u) \subseteq U_1$ in $\mathrm{Spec_r}\, R[V]$ and we also have $D_F(-u) \subseteq U$ in $X(R(V))$. Since the embedding $X(F) \longrightarrow \mathrm{Spec_r}\, R[V]$ is dense, $D_F(-u) \neq \emptyset$. □

Remark 4.6. Note that Lemma 4.5 is not true for a general formally real field. Consider for example the field $F = \mathbb{R}((X))((Y))$ of iterated power series. We have $|X(F)| = 4$ and each singleton is open and does not contain any principal set because it is not principal.

Lemma 4.7. *Let F be the function field of an algebraic R-variety over a real closed field R. Let T be a preordering of F such that $\hat{T}$ is open in $X(F)$, let $s \in T \setminus F^2$ and $L = F(\sqrt{s}) = F[Z]/(Z^2 - s)$.*

(1) For any preordering P on L such that $T = P \cap F$, the restriction map $\pi\colon X(L) \longrightarrow X(F)$ induces a surjection from $\hat{P}$ to $\hat{T}$.

(2) If (L, P) is a T-extension of (F, T), then π induces a bijection between $\hat{P}$ and $\hat{T}$.

Proof. (1) Suppose there exists $\alpha \in \hat{T}$ such that $\pi^{-1}(\alpha) = \{\beta_1, \beta_2\}$ does not intersect $\hat{P}$. Then neither β_1 nor β_2 contains P, and there exist $f_1 \in P \setminus \beta_1, f_2 \in P \setminus \beta_2$. One of the three elements $f \in \{f_1, f_2, f_1 f_2\}$ must satisfy $f \in P \setminus \{\beta_1, \beta_2\}$, so $f(\beta_1) < 0, f(\beta_2) < 0$. This shows that $D_L(-f)$ contains $\{\beta_1, \beta_2\}$ and $D_L(-f) \cap \hat{P} = \emptyset$. Write $f = a + bz, a, b \in F$, and denote by $N(f) = a^2 - b^2 s$ the norm of f from L down to F. Then $D_L(-f) = D_L(N(f), -a) \cup D_L(-N(f), -bz)$. Then $N(f)(\alpha) > 0$ because $-bz$ is positive in exactly one ordering in $\{\beta_1, \beta_2\}$ but $-f \in \beta_1 \cap \beta_2$. Hence we also have $N(f)(\beta_1) > 0, N(f)(\beta_2) > 0$. Thus we have $\{\beta_1, \beta_2\} \subseteq D_L(N(f), -a)$ and also $\alpha \in D_F(N(f), -a)$. By the preceding lemma and because $\hat{T}$ is open, there is a $u \in F$ such that $\emptyset \neq D_F(-u) \subseteq D_F(N(f), -a) \cap \hat{T}$. Hence $D_L(-u) \subset D_L(-f) \subset X(L) \setminus \hat{P}$. Thus $u > 0$ on $\hat{P}$ and $u \in P \cap F = T$. But since $D(-u) \cap \hat{T} \neq \emptyset$, this is a contradiction, which proves (1).

(2) We show that π is also injective. Let $\alpha \in X(F)$. If β_1, β_2 are the two points in $\pi^{-1}\{\alpha\} \subset X(L)$, then z has opposite signs at β_1 and β_2. But we also have $zf \in P$ for some $f \in F$, and if $\beta \in \hat{P}$, then $zf \in \beta$. Since f has the same sign at β_1 and β_2 (given by the sign at α), z would have the same sign at β_1 and β_2 if both were in $\hat{P}$: a contradiction. This shows that only one of the β_i's can be in $\hat{P}$ and that π is injective on $\hat{P}$. □

Remark 4.8. Concerning Lemma 4.7 (2), we should point out that one can construct a field F with a preordering T and a quadratic extension L with a preordering P such that:

(1) $P \cap F = T$,
(2) There is a $1 - 1$ correspondence between C_2-orderings of L containing P and C_2-orderings in F containing T induced by the restriction map,
(3) The natural map $\dot{F}/T \longrightarrow \dot{L}/P$ is not surjective.

One possible example is $F = \mathbb{R}(X, Y)$, T the set of nonzero sums of squares in F and $L = F(\sqrt{s})$, where $s = 1 + X^2$. Then set $\hat{P} = \{\alpha \in X(F) \mid \sqrt{s} \in \alpha\}$, and $P = \bigcap_{\alpha \in \hat{P}} \alpha$. We claim that P satisfies the conditions (1), (2) and (3) above. (1) is valid because for each ordering $\gamma \in X_F$, there is an ordering $\alpha \in X_L$ such that $\alpha \cap F = \gamma$. (2) is also valid because for each ordering $\gamma \in X_F$ there is exactly one ordering $\alpha \in X_L$ such that $\alpha \cap F = \gamma$. Finally using the proof of Proposition 4.10 below (which does not utilize Remark 4.8), we show that (3) is valid as well. Suppose to the contrary that the natural map $\dot{F}/T \longrightarrow \dot{L}/P$ is surjective. Then by (1) it is an isomorphism. In the proof of Proposition 4.10 we show that there is no such P in L. $\square$

Proposition 4.9. *Let F be the function field of an algebraic variety over a real closed field R. Let T be a preordering such that $\hat{T}$ is open. Let $L = F[Z]/(Z^2 - s)$ for $s \in T \setminus F^2$. Then the following conditions are equivalent:*

(1) (F, T) admits a T-extension (L, P) with P a preordering,

(2) There exists an element $f \in \dot{F}$ such that for all $a, b \in F$ there exists $g \in \dot{F}$ for which $[D_F(a^2 - b^2 s, a) \cup D_F(-a^2 + b^2 s, bf)] \cap \hat{T} = D_F(g) \cap \hat{T}$.

Proof. Denote by N the norm from L down to F, by z the class of Z in L and by $\pi\colon X(L) \longrightarrow X(F)$ the restriction map.

Let us prove that condition (1) implies condition (2). Assume (L, P) is a T-extension of (F, T) with P a preordering of L. Then $\dot{F}/T \cong \dot{L}/P$ and for any $h \in \dot{L}$ there is a $g \in \dot{F}$ such that $gh \in P$. Let f be an element of $\dot{F}$ such that $fz \in P$.

We show first that $\pi(D_L(h) \cap \hat{P}) = D_F(g) \cap \hat{T}$. By the preceding lemma we know that π induces a bijection from $\hat{P}$ onto $\hat{T}$. For $\alpha \in \hat{T}$, let β be the unique element of $\hat{P}$ such that $\pi(\beta) = \alpha$. Then we have $\alpha \in D_F(g) \cap \hat{T}$ if and only if $g(\alpha) > 0$ and $\alpha \in \hat{T}$, if and only if $g(\beta) > 0$ and $\beta \in \hat{P}$, because $g \in F \subset L$. Since $gh \in P \subset \beta$, this is also equivalent to $h(\beta) > 0$ and $\beta \in \hat{P}$, i.e. $\beta \in D_L(h) \cap \hat{P}$. Thus we have proved that $\pi(D_L(h) \cap \hat{P}) = D_F(g) \cap \hat{T}$. In particular, if $b \in F$, then $\pi(D_L(bz) \cap \hat{P}) = D_F(bf) \cap \hat{T}$.

On the other hand, for $h = a + bz \in L, a, b \in F$, one has $D_L(h) = D_L(N(h), a) \cup D_L(-N(h), bz)$. Since π is a bijection between $\hat{P}$ and $\hat{T}$, it preserves subset intersections (and of course unions). Then $\pi(D_L(h) \cap \hat{P}) = (\pi(D_L(N(h), a)) \cap \hat{T}) \cup \pi(D_L(-N(h), bz) \cap \hat{P})$. The first set of this union is $D_F(N(h), a) \cap \hat{T}$, and the second is $D_F(-N(h)) \cap \pi(D_L(bz) \cap \hat{P}) = D_F(-N(h), bf) \cap \hat{T}$. This proves (1) implies (2).

Conversely, we show that condition (2) implies condition (1). Suppose there is an f satisfying condition (2). Define $S := D_L(fz) \cap \pi^{-1}(\hat{T})$ and set $P := \bigcap_{\beta \in S} \beta$. We want to show that (L, P) is a T-extension of (F, T). An element $a \in F$ is in P if and only if $a(\beta) > 0$ for $\beta \in S$, if and only if $a(\alpha) > 0$ for $\alpha \in \pi(S)$. Since $\hat{T} \subseteq \pi(D_L(fz))$, we have $P \cap F = T$.

Let $h = a + bz \in \dot{L}$ with $a, b \in F$. By our assumption there exists $g \in \dot{F}$ such that $[D_F(N(h), a) \cup D_F(-N(h), bf)] \cap \hat{T} = D_F(g) \cap \hat{T}$. We claim that $gh \in P$.

For the sake of simplicity write $V = D_F(N(h), a) \cup D_F(-N(h), bf)$. We have $D_L(h) = D_L(N(h), a) \cup D_L(-N(h), bz)$. Hence $D_L(h) \cap S = \pi^{-1}(V) \cap S = (\pi^{-1}(D_F(g) \cap \hat{T})) \cap S = D_L(g) \cap S$. Therefore $gh \in P$ as required. This shows that (L, P) is a T-extension of (F, T), and the proof of the proposition is complete. $\square$

Remark. Observe that in the proof that (2) implies (1) in Proposition 4.9, we did not use all hypotheses in this proposition. In fact we proved:

Let F be a formally real field and T be a preordering of F. Let $L = F(\sqrt{s})$ for $s \in T \backslash F^2$. Suppose that there exists an element $f \in \dot{F}$ such that for all $a, b \in F$ there exists $g \in \dot{F}$ for which $D_F(a^2 - b^2 s, a) \cup D_F(-a^2 + b^2 s, bf) \cap \hat{T} = D_F(g) \cap \hat{T}$. Then (F, T) admits a T-extension (L, P) with P a preordering.

As an application of the material discussed above we have the following illustration.

Proposition 4.10. *Let $F = \mathbb{R}(X, Y)$ and let T be the set of nonzero sums of squares in F. If H is a subgroup of $\mathcal{G}_F$ such that $T = P_H$, then the H-ordered field (F, T) does not admit an H-closure.*

Proof. The hypotheses of Proposition 4.9 are obviously satisfied, because $\hat{T}$ is the whole space. Assume (K, S) is an H-closure of (F, T). Let $s \in T \setminus F^2$, $L = F(\sqrt{s}) = F[Z]/(Z^2 - s)$, and let $P = L \cap \dot{K}^2$. Then by Lemma 4.4, (L, P) is a T-extension of (F, T) with P a preordering of L. By Proposition 4.9, there exists an $f \in F$ such that for every $u, v \in F$ the open sets $D_F(u^2 - v^2 s, u) \cup D_F(-u^2 + v^2 s, vf)$ are principal. We show that this is not true for $s = 1 + X^2$.

Take $h = Y + c + bz \in L$ with $c, b \in \mathbb{R}, b > 0$. Assume that the corresponding set $D_F(N(h), Y + c) \cup D_F(-N(h), f)$ is the principal set $D_F(g)$ for a given square-free polynomial $g \in F$. Note that the equation $N(h) = 0$ in $\mathbb{R}^2$ defines the hyperbola $\mathcal{H}$ of equation $(Y + c)^2 = b^2(1 + X^2)$. Set $A := \{(X, Y) \in \mathbb{R}^2 \mid N(h) > 0, \quad Y + c > 0\}$ (respectively $B := \{(X, Y) \in \mathbb{R}^2 \mid N(h) > 0, \quad Y + c < 0\}$) the open region of the plane above (respectively below) the upper (respectively lower) branch of $\mathcal{H}$. By assumption, we know that $g > 0$ on $\tilde{A} \cap X(F) = D_F(N(h), Y + c)$ and $g < 0$ on $\tilde{B} \cap X(F) = D_F(N(h), -(Y + c))$. This implies that $g \geq 0$ on A and $g \leq 0$ on B (see [BCR], §7.6) and that A and B are separated by a branch (i.e. a 1-dimensional irreducible connected component) of $g = 0$. Moreover, no branch of $g = 0$ can go inside $A \cup B$, or else g would change sign on A or B. (This is due to the fact that g is square free, and thus every branch is a sign-changing branch). Set $C := \mathbb{R}^2 \setminus A \cup B$. Then $\tilde{C} \cap X(F) = D_F(-N(h))$. Since $D_F(g, -N(h)) = D_F(bf, -N(h)) = D_F(f, -N(h))$, we know that f and g have the same sign on C, up to a 0-dimensional set. Thus $f = 0$ must also have a sign-changing branch contained in C, and since f may be chosen square free, any branch of $f = 0$ having a nonempty intersection with the interior of C must be contained in C.

Suppose this is true at the same time for $h = h_1 = Y + z$ and $h = h_2 = Y + 4 + 2z$. Then

(1) no branch of $f = 0$ is allowed to cross a branch of the hyperbolas $\mathcal{H}_i$, $i = 1, 2$, and
(2) there is a branch of $f = 0$ splitting the plane into two connected components, each of them containing one branch of $\mathcal{H}_i$.

As the upper branch of $\mathcal{H}_2$ crosses the two branches of $\mathcal{H}_1$, this is impossible. This provides a contradiction to the existence of an H-closure for T, finishing the proof of Proposition 4.10. □

Remark 4.11. Associated to the group $\dot{F}/T$ of the preceding proposition is the "abstract Witt ring" of T-forms (see [Ma]), which is actually the reduced Witt ring $W_{red}(F)$. (See also [L2, Chapter 1] for the definition of $W_{red}(F)$.) Proposition 4.10 shows there is no extension $F \longrightarrow K$ such that $W_{red}(F)$ becomes isomorphic to $W(K)$.

This can be viewed as a weak version of the "unrealizability" of $W_{red}(F)$ as a "true" Witt ring (See [Ma], as well as [Cr2], and the remarks on Craven's results below). Note that $W_{red}(F)$ might actually be isomorphic to $W(K)$ for some field K not related to F, as shown in Example 8.14. We shall now make these remarks more precise.

Proposition 4.12. *Let $F = \mathbb{R}(X,Y)$. Then there is no field extension $F \longrightarrow K$ with $W(K) \cong W_{red}(K)$ such that the induced map $W_{red}(F) \longrightarrow W_{red}(K) \cong W(K)$ is an isomorphism.*

Proof. Suppose on the contrary that there exists a field extension K/F such that the inclusion $F \longrightarrow K$ induces an isomorphism $W_{red}(F) \cong W_{red}(K) \cong W(K)$.

Because $W_{red}(F)$ is a torsion-free ring and $W_{red}(F) \cong W(K)$ we see that $W(K)$ is torsion-free as well. Thus K is a pythagorean field. (See [L1, Chapter 8].) Observe also that $-1 \notin \dot{K}^2$ because otherwise K would be a quadratically closed field and $W_{red}(F)$ would not be isomorphic to $W(K)$. Hence K^2 is a preordering in K. Set T to be the set of nonzero sums of squares in F. It is well known that the group of units in $W_{red}(F)$ is $\{fT : f \in \dot{F}\} = \dot{F}/T$ and the group of units of $W(K)$ is $\dot{K}/\dot{K}^2$ (because $W(K)$ is reduced). (See [L2, Proposition 1.24].) Therefore the isomorphism $W_{red}(F) \cong W(K)$ induces an isomorphism $\dot{F}/T \cong \dot{K}/\dot{K}^2$.

Now let $F(2)$ be a quadratic closure of F and set $L = K \cap F(2)$. (We assume that both fields K and $F(2)$ lie in some fixed field extension of F.) Let $l_1, l_2 \in L$ and $l_1^2 + l_2^2 \in \dot{L}$. Then because K is a pythagorean field we see that there exists an element $k \in \dot{K}$ such that $k^2 = l_1^2 + l_2^2$. Since k also belongs to $F(2)$ we see that $k \in L$ and L is a pythagorean field. (Observe that in general any intersection of pythagorean fields is a pythagorean field.) We also see that $\dot{L}^2 \cap F = \dot{K}^2 \cap F = T$, because for each $t \in T$, $\sqrt{t} \in F(2)$.

Finally we claim that the natural homomorphism $\varphi : \dot{F}/T \longrightarrow \dot{L}/\dot{L}^2$ is in fact an isomorphism. Because $\dot{L}^2 \cap F = T$, we see that φ is injective. Consider now an element $l \in \dot{L}$. Because the natural map $\dot{F}/T \longrightarrow \dot{K}/\dot{K}^2$ is surjective, we see that there exist elements $f \in \dot{F}$ and $k \in \dot{K}$ such that $lf^{-1} = k^2 \in \dot{K}^2$. Because $lf^{-1} \in \dot{L} \subset F(2)$ we see that $k \in F(2) \cap K = L$. Therefore the map $\dot{F}/T \longrightarrow \dot{L}/\dot{L}^2$ is surjective.

From the proof of Proposition 4.10, we see that there is no field extension L/F, $L \subset F(2)$, such that $\dot{L}^2$ is additively closed, $-1 \notin \dot{L}^2$, and the natural homomorphism $\dot{F}/T \longrightarrow \dot{L}/\dot{L}^2$ is an isomorphism. Thus we have arrived at a contradiction. □

T. Craven kindly called our attention to [Cr2, Theorem 5.5], which can be applied in the construction of formally real fields F such that $W_{red}(F)$ is not isomorphic to $W(K)$ for any field extension under the natural map induced by the inclusion $F \longrightarrow K$. (As observed in the proof of Proposition 4.12 above, if we want $W_{red}(F) \cong W(K)$ then K must be a formally real pythagorean field, and the inclusion $F \longrightarrow K$ induces a natural homomorphism $W_{red}(F) \longrightarrow W_{red}(K) = W(K)$.) The following proposition we attribute to T. Craven, as it is an immediate corollary of [Cr2, Theorem 5.5].

Proposition 4.13 (Craven). *Let $F = L(X)$ where L is a formally real field, which is not a pythagorean field. Then for each pythagorean field extension K/F, the natural homomorphism $W_{red}(F) \longrightarrow W_{red}(K) = W(K)$ induced by the inclusion map $F \longrightarrow K$ is not an isomorphism.*

Proof. Assume that K is a pythagorean field extension of $F = L(X)$, where L is a formally real field which is not pythagorean, and suppose that the field extension $F \longrightarrow K$ induces an isomorphism $W_{red}(F) \longrightarrow W_{red}(K)$.

Because L is not a pythagorean field, there exists an element $l = l_1^2 + l_2^2, l_1, l_2 \in L$ such that $l \notin \dot{L}^2$. Because K is a pythagorean field, there exists an element $k \in \dot{K}$ such that $k^2 = l$. Hence the polynomial $f(X) = X^2 - l$ has a root in K. Then from [Cr2, Theorem 5.5(b)], we see that $f(X)$ has exactly one root in every real closure of L. Of course this is not true, as each real closure of L must contain both roots of $f(X)$. Hence we have arrived at a contradiction, completing the proof. $\square$

Remark. We can say that $W_{red}(F)$ is not realizable as the Witt ring of an extension K/F.

In the other direction we present a case below, where (F,T) admits a maximal preordered T-extension $(\dot{K}, \dot{K}^2)$. We recall that a preordering T in F is SAP (Strong Approximation Property) if and only if for each set of elements $a_1, \dots, a_n \in \dot{F}$ there exists an element $a \in \dot{F}$ such that $D_F(a_1, \dots, a_n) \cap \hat{T} = D_F(a) \cap \hat{T}$. (Here as above, $\hat{T}$ is the set of all orderings $\alpha \in F$ such that $T \subset \alpha$.) If T is SAP and R is a preordering of F containing T, then R is SAP as well. (See [L2, Theorem 17.12 and Corollary 16.8].) The definition of SAP implies that $(D_F(a) \cup D_F(b)) \cap \hat{T} = D_F(c) \cap \hat{T}$ for some $c \in \dot{F}$. Thus condition (2) of Proposition 4.9 holds (and hence also condition (1), by the remark following Proposition 4.9).

Proposition 4.14. *Let F be a formally real field, and let T be a SAP preordering in F. Then (F,T) admits a maximal preordered T-extension $(K, \dot{K}^2)$.*

Proof. Let F be a formally real field and let T be a SAP preordering in F. Using Zorn's lemma we see that there exists a T-extension (L,S) of (F,T) which is maximal among the preordered T-extensions. We claim that S is a SAP preordering in L. In order to show this, pick any elements $a_1, \dots, a_n \in \dot{L}$. Because (L,S) is a T-extension of (F,T) we see that there exist elements $b_1, b_2, \dots, b_n \in \dot{F}$ such that $b_i a_i \in S$ for each $i = 1, 2, \dots, n$. Because T is SAP there exists an element $b \in \dot{F}$ such that $D_F(b_1, \dots, b_n) \cap \hat{T} = D_F(b) \cap \hat{T}$.

We have $D_L(b) \cap \hat{S} = D_L(b_1, \dots, b_n) \cap \hat{S}$. Indeed let $\alpha \in D_L(b) \cap \hat{S}$. Then $b \in \alpha$ and $\alpha \cap F \in \hat{T}$. Therefore $b_1, \dots, b_n \in \alpha$ and $\alpha \in D_L(b_1, \dots, b_n) \cap \hat{S}$. Assume now that $\alpha \in D_L(b_1, \dots, b_n) \cap \hat{S}$. Then $b_1, \dots, b_n \in \alpha$ and $\alpha \cap F \in \hat{T}$. Hence $b \in \alpha$ and $\alpha \in D_L(b) \cap \hat{S}$.

Finally observe that since $b_i a_i \in S$ for all $i = 1, \dots, n$ we have $D_L(b_1, \dots, b_n) = D_L(a_1, \dots, a_n)$. Therefore $D_L(b) \cap \hat{S} = D_L(a_1, \dots, a_n) \cap \hat{S}$ as required.

Now we claim that $S = \dot{L}^2$. Suppose that this is not true. Then there exists an element $s \in S \setminus \dot{L}^2$ and we can set $E = L(\sqrt{s})$. By the remark following Proposition 4.9 we see that one can find a preordering R in E such that (E,R) is a T-extension of (F,T). This is a contradiction with the fact that (L,S) is a maximal T-extension of (F,T) such that S is a preordering in L. Therefore we can set $L = \dot{K}$ and $S = \dot{K}^2$ to complete the proof. $\square$

The preceding proposition will apply in particular when F is a formally real field of transcendence degree 1 over a real closed field, because those fields are known to have stability index 1, which implies Strong Approximation Property ([L2, Corollary 17.11]).

Remark 4.15. Note that SAP is not a necessary condition for the existence of closures for preorderings. If F is pythagorean, then it is its own closure with respect to its minimal preordering. But there are pythagorean fields which are not SAP: for example the field of iterated power series $\mathbb{R}((X))((Y))$. (See also [Cr1] for more examples.)

§5. Cyclic subgroups of W-groups

In this section we consider the subgroups H of $\mathcal{G}_F$ which are the easiest to understand in terms of their associated H-orderings, namely the two cyclic groups C_2 and C_4. As mentioned earlier, C_2 in many ways is the motivating example for this entire theory, and we cite here the results previously given in [MiSp1] for this group, as a means of illustrating the results we are attempting to generalize in this paper. As any single element of $\mathcal{G}_F$ necessarily generates a cyclic subgroup of order 2 or 4, those which generate subgroups of order 4 are precisely those not associated with usual orderings on the field F. These are the so-called half-orders of F, as investigated in [K1]; this concept was first introduced by Sperner [S] in 1949, in a geometrical context.

Definition 5.1. A *nonsimple involution* of $\mathcal{G}_F$ is an element $\sigma \in \mathcal{G}_F$ such that $\sigma^2 = 1$ and $\sigma \notin \Phi(\mathcal{G}_F)$. In other words, a nonsimple involution is an element of $\mathcal{G}_F$ which generates an essential subgroup of order 2.

Theorem 5.2. [MiSp1] *The field F is formally real if and only if $\mathcal{G}_F$ contains a nonsimple involution. There is a one-one correspondence between orderings on F and nontrivial cosets of $\Phi(\mathcal{G}_F)$ which have an involution as a coset representative.*

We have the well-known characterization of those subgroups of $\dot{F}$ that are orderings, which we include here for the sake of completeness.

Proposition 5.3. *A subgroup S of $\dot{F}$ containing $\dot{F}^2$ is a C_2-ordering of F if and only if the following conditions hold.*

(1) $|\dot{F}/S| = 2$ *and*
(2) $1 + s \in S\ \forall s \in S$.

We can now characterize those subgroups S of $\dot{F}$ which are C_4-orderings. They are precisely those subgroups of index 2 which fail to be orderings. We also see that C_4-ordered fields always admit a closure.

Proposition 5.4. *A subgroup S of $\dot{F}$ containing $\dot{F}^2$ is a C_4-ordering of F if and only if the following conditions hold.*

(1) $|\dot{F}/S| = 2$ *and*
(2) $\exists s \in S$ *such that* $1 + s \notin S$.

Proof. We know S is a C_4-ordering of F if and only if there exists $\sigma \in \mathcal{G}_F$ such that $S = \{a \in \dot{F} | \sqrt{a}^\sigma = \sqrt{a}\}$ where $\sigma^2 \neq 1$. Now any subgroup of index 2 in $\dot{F}$ is of the form $\{a \in \dot{F} | \sqrt{a}^\sigma = \sqrt{a}\}$ for some $\sigma \in \mathcal{G}_F$, so we need only guarantee that S is not an ordering, which condition (2) does. $\square$

Remark 5.5.

(1) Note that it is easy to see that condition (2) above can be replaced by (2') $S+S=\dot{F}$.
(2) There are actually two kinds of C_4-orderings, distinguished by whether or not they contain -1. If S is a C_4-ordering such that $-1 \in S$, we say that S has level 1. The prototype is given by $\mathbb{F}_p^2$ when $p \equiv 1 \bmod 4$. If $-1 \notin S$, then necessarily $-1 \in S+S$, and we say that S has level 2. The model is $\mathbb{F}_p^2$ when $p \equiv -1 \bmod 4$. It is clear that every C_4-extension preserves the level.

Proposition 5.6. *Let $(K,\dot{K}^2)$ be a maximal T-extension of a C_4-ordered field (F,T). Then*

(1) *K is characterized by the condition of being maximal in $F(2)$ among fields $L \supseteq F$ such that $\sqrt{a} \notin L$ $\forall a \in \dot{F}\backslash T$.*
(2) *$\mathcal{G}_K \cong C_4$.*
(3) *$\mathrm{Gal}(K(2)/K) \cong \mathbb{Z}_2$, the group of 2-adic integers.*

In particular, every maximal T-extension of a C_4-ordered field (F,T) is a C_4-closure, and thus C_4-closures always exist.

Proof. Let $(K,\dot{K}^2)$ be a maximal T-extension of the C_4-ordered field (F,T). Since $\dot{K}^2 \cap F = T$, we see that for any $a \in \dot{F}\backslash T$, we have $\sqrt{a} \notin K$, while for any $a \in T$, we have $\sqrt{a} \in K$. Now if $L \supsetneq K$ in $F(2)$, then $L \supseteq K(\sqrt{a})$ for some $a \in \dot{K}\backslash\dot{K}^2$. Since the cosets of $\dot{K}^2$ in $\dot{K}$ correspond naturally to the cosets of T in $\dot{F}$, we see that L contains $\sqrt{a'}$ for some $a' \in \dot{F}\setminus T$, and thus K is maximal among such extensions of F in $F(2)$. Conversely, suppose K is maximal in $F(2)$ among fields $L \supseteq F$ such that $\sqrt{a} \notin L$ $\forall a \in \dot{F}\backslash T$. Then we see that $\dot{K}^2 \cap F = T$. We need to see that $|\dot{K}/\dot{K}^2| = 2$. Suppose it is not true. Fix $a \in \dot{F}\backslash T$, so that $a \notin \dot{K}^2$, and suppose there exists some $b \in \dot{K}$ such that a,b are linearly independent in $\dot{K}/\dot{K}^2$. Then certainly $b \notin aT$, and setting $L = K(\sqrt{b})$ contradicts the maximality of K. Thus we have that $(K,\dot{K}^2)$ is a maximal T-extension for (F,T), and this proves (1).

Now observe that $\mathcal{G}_K$ is generated by one generator, since $|\dot{K}/\dot{K}^2| = 2$, so $\mathcal{G}_K \cong C_2$ or C_4. It cannot be C_2, or else T would be an ordering on F. Thus $\mathcal{G}_K \cong C_4$. Finally, $\mathrm{Gal}(K(2)/K)$ is cyclic and cannot be finite, since it is not C_2 (see [Be1]). Thus $\mathrm{Gal}(K(2)/K) \cong \mathbb{Z}_2$. □

§6. Subgroups of W-groups generated by two elements

As we saw in Theorem 2.5, a group generated by two elements appearing as a subgroup of $\mathcal{G}_F$ may only be one in the list $C_2 * C_4, C_4 * C_4, C_2 * C_2, C_4 \times C_4, C_4 \rtimes C_4$. The last two are particular cases of the groups studied in § 7 and § 8, and we will focus in this section on the first three. The third one is better known as the dihedral group D.

We will give an algebraic characterization for the orderings associated with these groups and show that it is always possible to make closures. Portions of the proofs rely on the characterizations of $C_4 \times C_4$- and $C_4 \rtimes C_4$-orderings obtained in § 7; but since the results in § 7 do not rely on those in § 6, we freely use these results where needed.

Lemma 6.1. *Let T be a subgroup of $\dot{F}$ such that $\dot{F}^2 \subseteq T$ and $|\dot{F}/T| = 4$. If $-1 \notin T$, then F is $(T \cup -T)$-rigid.*

Proof. Let $\dot{F}/T = \{1, -1, a, -a\}$. Then $(T \cup -T) + a(T \cup -T) \subseteq (T \cup -T) \cup a(T \cup -T) = \dot{F}$. □

Proposition 6.2. *A subgroup T of $\dot{F}$ is a $C_2 * C_4$-ordering if and only if $\dot{F}^2 \subseteq T$, $|\dot{F}/T| = 4$, and the following two conditions hold.*

(1) *$T + T \neq T$, and*
(2) *$-1 \notin \sum T$, where $\sum T$ denotes the set of all finite sums of elements of T.*

Proof. The conditions $\dot{F}^2 \subseteq T$ and $|\dot{F}/T| = 4$ are necessary and sufficient for T to be a G-ordering for some essential subgroup $G \subseteq \mathcal{G}_F$ generated by two elements σ, τ, independent mod $\Phi(\mathcal{G}_F)$. We next show the necessity of conditions (1) and (2). Let $G \cong C_2 * C_4$ be a subgroup of $\mathcal{G}_F$, where $T = P_G$. We assume G is generated by two noncommuting (hence independent mod $\Phi(\mathcal{G}_F)$) elements σ, τ such that $\sigma^2 = 1, \tau^4 = 1$. If $T + T = T$, then by Proposition 6.14, T would be a D-ordering (this is independent of previous results). Since it is not, we see that (1) holds. Also $-T \not\subseteq \sum T$, since $\sum T \subseteq P_\sigma$, which is an ordering because σ is an involution. Thus P_σ cannot contain $-T$ and condition (2) holds.

We now show the sufficiency of the conditions. Since T is a G-ordering for some essential subgroup with two generators, it must be isomorphic to one of the five groups listed in Theorem 2.5. Since $-1 \notin T$ by (2), it cannot be $C_4 \times C_4$ by Proposition 7.2 in the next section. Also (1) shows that G cannot be isomorphic to $D \cong C_2 * C_2$ by Proposition 6.14, and (2) shows that G cannot be isomorphic to $C_4 \rtimes C_4$ by Proposition 7.6. Finally, from (1) and (2) we can see that $\sum T$ is an ordering on F, since it is clearly a proper subgroup of $\dot{F}$, which properly contains T, so must be of index 2 in $\dot{F}$; it does not contain -1, and it is closed under addition. Then $\sum T = T \cup aT$ for some $a \notin T$, and G is generated by elements σ, τ where the intersection of the fixed field of σ with $F^{(2)}$ is $K(\sqrt{a})$, and the intersection of the fixed field of τ with $F^{(2)}$ is $K(\sqrt{-1})$. Then $P_\sigma = \sum T$ is an ordering, so σ is an involution. This shows G cannot be isomorphic to $C_4 * C_4$. Thus the only remaining possibility is $G \cong C_2 * C_4$. □

Proposition 6.3. *A subgroup T of $\dot{F}$ is a $C_4 * C_4$-ordering if and only if $\dot{F}^2 \subseteq T$, $|\dot{F}/T| = 4$, and one of the following two conditions hold.*

(1) *$-1 \in T$ and F is not T-rigid, or*
(2) *$-1 \notin T$, $-1 \in \sum T$, but $T + T \neq T \cup -T$.*

Proof. If $-1 \in T$, the only possible subgroups H of $\mathcal{G}_F$ with two generators for which T can be an H-ordering are $C_4 \times C_4$ and $C_4 * C_4$. The other three are eliminated by Propositions 6.14, 6.2, and 7.6. Also, if $-1 \in T$, then F is T-rigid if and only if T is a $C_4 \times C_4$-ordering by Proposition 7.2. This leaves $C_4 * C_4$ as the only possibility.

If $-1 \notin T$, there are three possibilities to consider: $-1 \notin \sum T$, $T + T = T \cup -T$, or $-1 \in \sum T$ but $T + T \neq T \cup -T$. The first case occurs if and only if T is either a D-ordering (by Proposition 6.14) or a $C_2 * C_4$-ordering (by Proposition 6.2). The second case occurs if and only if T is a $C_4 \rtimes C_4$-ordering by Proposition 7.6 and Lemma 6.1. Thus, the third case must occur if and only if T is a $C_4 * C_4$-ordering as claimed. □

The following example constructs a $C_4 * C_4$-ordering of $\mathbb{Q}_2$. It is illustrative, in that it shows how even in a relatively "small" setting, the additive structure of T can behave quite differently from the additive structure of $\dot{F}(\sqrt{T})^2$. In particular, it shows that $\langle 1,1\rangle$ may represent elements in $F(\sqrt{T})$ which are not in $T+T$. In this example, $T+T$ is not multiplicatively closed, but of course the form $\langle 1,1\rangle$, being a Pfister form, is multiplicative in $F(\sqrt{T})$.

Example 6.4. In $F=\mathbb{Q}_2$ consider the subgroup $T=\dot{F}^2\cup 5\dot{F}^2$ of the square class group. Using the notation for $\mathcal{G}_2$ as in Example 2.9, we see that the corresponding subgroup of $\mathcal{G}_2$ is $H=\langle\sigma,\tau\rangle\cong C_4 * C_4$. This is a W-group associated with the Witt ring $\mathbb{Z}/4\mathbb{Z}\times_M\mathbb{Z}/4\mathbb{Z}$, where the product "$\times_M$" is taken in the category of Witt rings (see [Ma] and [MiSm2]). The fixed field of H is $K=\mathbb{Q}_2(\sqrt{5})$. The form $\langle 1,1\rangle$ represents -1 over K, and this can be shown as follows. It is well known and easy to show that for any quadratic field extension $F\longrightarrow K=F(\sqrt{a})$, one has $(K^2+K^2)\cap\dot{F}=(F^2+F^2)(F^2+aF^2)$. If $F=\mathbb{Q}_2$ and $a=5$, we have $30=5\times 6\in(K^2+aK^2)$ and $2\in(K^2+K^2)$. Then $15\in K^2+K^2$, and since 15 is congruent to -1 mod 16: it is a negative square in $\mathbb{Q}_2$. This shows that $-1\in K^2+K^2$.

However, when one considers which elements of $\dot{F}/\dot{F}^2$ are in $T+T$, one finds only the six classes represented by $1,2,5,10,-2,-10$. In particular, $-1\notin T+T$, and $T+T$ is not multiplicatively closed (so forms mod T-equivalence do not behave as quadratic forms over a field behave). Nonetheless, it is easy to see that $-1\in T+T+T$, so that $T+T\neq T\cup -T$, but $-1\in\sum T$, consistent with the proposition above.

In §9 we introduce natural conditions for a subgroup H of $\mathcal{G}_F$ in order to keep track of the additive properties of $\dot{F}/T$ under 2-extensions. We shall see in §9 that the group $H\subset\mathcal{G}_F$ above does not possess one of the key properties we require.

Theorem 6.5. *A $(C_2 * C_4)$-ordered field (F,T) admits a closure.*

Proof. Let $\mathcal{S}$ be the set of extensions (L,S) of (F,T) inside $F(2)$ satisfying the additional condition that $-1\notin\sum S$. As in the proof of Proposition 4.1, we see that $\mathcal{S}$ has a maximal element (K,T_0) with $\dot{K}/T_0\cong\dot{F}/T, T=T_0\cap F$, and $-1\notin\sum T_0$. Then (K,T_0) is a $(C_2 * C_4)$-ordered field. To see this we need only show that conditions (1) and (2) of Proposition 6.2 hold, and condition (2) is given by construction of (K,T_0). Condition (1) holds since if $T_0+T_0=T_0$, then $T+T\subseteq(T_0+T_0)\cap F=T_0\cap F=T$, contradicting the fact that T is a $C_2 * C_4$-ordering on F.

To conclude, we must show $T_0=\dot{K}^2$. Notice $\sum T_0$ is an ordering on K, so K is formally real. We may write $\dot{K}/T_0=\{\pm T_0,\pm aT_0\}$, where $a\in T+T$. If $T_0\neq\dot{K}^2$, we can choose $c\in T-\dot{K}^2$, and consider $L=K(\sqrt{c})$. Since $-c\notin\sum T_0$, $\sum T_0$ extends to an ordering S_0 on L. Then $S_0\cup -S_0=\dot{L}$ and $a\in S_0$. Let S be a subgroup of S_0 containing T_0 and maximal with respect to excluding a. Then $\dot{L}/S=\{\pm S,\pm aS\}\cong\dot{K}/T_0\cong\dot{F}/T$. Also $S\cap K\supseteq T_0$ by construction, and if there exists $b\in S\cap K, b\notin T_0$, then $b\in aT_0\cup -T_0\cup -aT_0$, which implies either $a\in S$ or $-1\in S$, which leads to a contradiction in either case. Thus $S\cap K=T_0$, and (L,S) is an extension contradicting the maximality of (K,T_0). We conclude $T_0=\dot{K}^2$. $\square$

Theorem 6.6. *A $(C_4 * C_4)$-ordered field (F,T) admits a $(C_4 * C_4)$-closure $(K,\dot{K}^2)$.*

Proof. Let $(K,\dot{K}^2)$ be a maximal T-extension for (F,T). First assume $-1\in T$. We must show K is not a rigid field. Let $\{1,a,b,ab\}$ be a set of representatives for $\dot{F}/T$ which lifts to a set of representatives for $\dot{K}/\dot{K}^2$. Since F is not T-rigid, we may, without loss of generality, assume $b \in T + aT$. Then $T + aT \subseteq \dot{K}^2 + a\dot{K}^2$, but $b \notin \dot{K}^2 \cup a\dot{K}^2$, so K is not rigid, and $\dot{K}^2$ is a $(C_4 * C_4)$-ordering on K.

Now assume $-1 \notin T = F \cap \dot{K}^2$. Then $-1 \notin \dot{K}^2$, and $-1 \in \sum T \subseteq \sum \dot{K}^2$. Letting $\{1, -1, a, -a\}$ be a set of representatives for $\dot{F}/T$, this again lifts to a set of representatives for $\dot{K}/\dot{K}^2$. Since $T + T \neq T \cup -T$, but clearly also $T + T \neq T$, we may assume $a \in T + T$, so $a \in \dot{K}^2 + \dot{K}^2$ as well. This shows $\dot{K}^2$ is a $(C_4 * C_4)$-ordering on K. $\square$

Remark 6.7. We have defined in Definition 3.2 the level of an H-ordering. It is then easy to see that the level of a $(C_4 * C_4)$-ordering T is at most 4. The level of the closure K (which is the "usual" level) is less than or equal to the level of T. The level of a $(C_4 * C_4)$-closure is either 1 or 2, as any field of finite level with at most four square classes has level at most 2. The level of T is 1 if and only if the level of K is 1, but in the other cases the level may actually decrease: Example 6.4 shows that T has level 3 and that its closure has level 2.

Now we turn our attention to D-orderings. We showed in § 2 that $C_2 \times C_2$ cannot be an essential subgroup of $\mathcal{G}_F$, so if H is an essential subgroup of $\mathcal{G}_F$ generated by two elements of order 2, necessarily $H \cong D$. Recall that according to [Br], a 2-*element fan* in F is a set of two distinct orderings P_1, P_2 on F, and it can be identified with the preordering $T = P_1 \cap P_2$.

Lemma 6.8. *The dihedral group D is a subgroup of $\mathcal{G}_F$ if and only if there is a 2-element fan in F. In this case, $T \subseteq \dot{F}$ is a D-ordering if and only if T is a 2-element fan in F.*

Proof. Let $H = \langle \sigma, \tau | \sigma^2 = \tau^2 = [\sigma, \tau]^2 = 1 \rangle \cong D$ be a subgroup of $\mathcal{G}_F$. Then P_σ and P_τ are positive cones of two distinct orderings on F, and $P_H = P_\sigma \cap P_\tau$. Conversely, if P_1, P_2 are positive cones corresponding to distinct orderings on F, then there exist nontrivial involutions $\sigma, \tau \in \mathcal{G}_F$, in distinct cosets of $\Phi(\mathcal{G}_F)$, such that $P_1 = P_\sigma$ and $P_2 = P_\tau$. Then $H = \langle \sigma, \tau \rangle$ is an essential subgroup of $\mathcal{G}_F$, and $H \cong D$. $\square$

In [BEK], a field F with two orderings P_1, P_2 is defined to be maximal with respect to P_1, P_2 if for any algebraic extension K of F, at least one of the two orderings cannot be extended to K. Since we prefer to work inside $F(2)$, we modify this as follows.

Definition 6.9. A field F with two orderings P_1, P_2 is *maximal with respect to* P_1, P_2 if for any 2-extension K of F, at least one of the orderings does not extend to K.

Proposition 6.10. *(F, P_1, P_2) is maximal if and only if (F, T_F) is a D-ordered field, where $T_F = P_1 \cap P_2$, and there exists no proper D-ordered extension field $(L, T_L) \subseteq F(2)$ with $T_L \cap F = T_F$.*

Proof. Suppose that the field (F, P_1, P_2) is maximal. Let σ_1, σ_2 be involutions in $\mathcal{G}_F$ such that $P_i = \{a \in \dot{F} | \sqrt{a}^{\sigma_i} = \sqrt{a}\}, i = 1, 2$. Then the subgroup $\langle \sigma_1, \sigma_2 \rangle \subseteq \mathcal{G}_F$ is isomorphic to D, as we have seen, and (F, T_F) is a D-ordered field as claimed.

Now suppose that L is a D-ordered field containing F inside $F(2)$, such that $T_L \cap F = T_F$. Then $\mathcal{G}_L$ contains a subgroup isomorphic to D, which we can take to be generated by two involutions τ_1, τ_2 such that $T_L = Q_1 \cap Q_2$, where $Q_i = \{a \in \dot{L} | \sqrt{a}^{\tau_i} = \sqrt{a}\}, i = 1, 2$ are distinct orderings of L. Now $Q_i \cap F \supseteq T_L \cap F = T_F$, so $Q_i \cap F$ is an ordering of F

which contains $T_F, i = 1, 2$. Thus $\{Q_1 \cap F, Q_2 \cap F\} = \{P_1, P_2\}$. Then by maximality of (F, P_1, P_2), we see $L = F$.

Conversely, suppose that F is a D-ordered field contained in no proper D-ordered extension field as described. Then F has at least two distinct orderings P_1 and P_2 corresponding to the two involutions generating the subgroup D of $\mathcal{G}_F$, and since there is no proper D-ordered extension field, we see that it is not possible for both orderings to extend to any extension of F. Thus (F, P_1, P_2) is maximal, as claimed. □

By Zorn's Lemma we immediately see the following.

Proposition 6.11. [BEK, Prop.3] *Given a field F with two orderings P_1, P_2, there always exists an algebraic extension $\tilde{F}$ of F which is maximal with respect to $\tilde{P}_1, \tilde{P}_2$, where $\tilde{P}_1, \tilde{P}_2$ are extensions of P_1, P_2 to $\tilde{F}$.*

Theorem 6.12. *A field (F, P_1, P_2) is maximal if and only if*

(1) *there exist exactly two orderings on F and*
(2) *F is pythagorean, i.e. any sum of squares is a square in F.*

Proof. [BEK] Suppose three different orderings P_1, P_2, P_3 are possible in F. Let $x \in \dot{F}$ be such that x is positive with respect to the first two orderings, and negative with respect to P_3. Then $\sqrt{x} \notin F$, so $F(\sqrt{x})$ is a proper algebraic extension of F, and since x is positive with respect to P_1 and P_2, they extend to $F(\sqrt{x})$, and (F, P_1, P_2) cannot be maximal. Similarly, if α, β are elements of F such that $\sqrt{\alpha^2 + \beta^2} \notin F$, then P_1, P_2 can be extended to the proper extension $F(\sqrt{\alpha^2 + \beta^2})$ of F, again contradicting maximality. Thus conditions (1) and (2) are necessary.

Conversely, one can show that any field F satisfying conditions (1) and (2) has $\dot{F}/\dot{F}^2 = \{1, -1, a, -a\}$ for some $a \in \dot{F}$. Now let F be such a field and let P_1, P_2 be the two unique orderings in F, so that a is positive with respect to P_1 and negative with respect to P_2. Suppose (F, P_1, P_2) were not maximal, and let $K = F(\sqrt{b})$ be a proper quadratic extension of F such that both P_1 and P_2 extend to K. Since K is an ordered proper extension of F, $b \neq 1, -1 \in \dot{F}/\dot{F}^2$, so $b = a$ or $-a$. Then either $\sqrt{a} \in K$ or $\sqrt{-a} \in K$, so that not both P_1 and P_2 extend to K. This is a contradiction. □

Corollary 6.13. *The D-ordered field (F, T) is a maximal D-ordered field if and only if $\mathcal{G}_F \cong D$. Thus any D-ordered field admits a D-closure.*

Proof. By the preceding theorem, if F is maximal, it has exactly two orderings, so $\mathcal{G}_F$ has exactly two involutions which are independent mod $\Phi(\mathcal{G}_F)$. Also F is pythagorean, so by [MiSp1] $\mathcal{G}_F$ is generated by involutions. Thus $\mathcal{G}_F$ is generated by two elements of order 2, and since $\mathcal{G}_F$ is necessarily an essential subgroup of itself, we see that $\mathcal{G}_F \cong D$.

Conversely, if $\mathcal{G}_F \cong D$, then F is a D-ordered field, and since orderings on F correspond to independent involutions in $\mathcal{G}_F$, we see that F has precisely two distinct orderings. Also, since $\mathcal{G}_F$ is generated by these involutions, we see that F is pythagorean. Thus, by the preceding theorem, F is a maximal D-ordered field. Then we see that for any D-ordered field (L, P_H), a maximal D-ordered extension $(F, \dot{F}^2)$ containing (L, P_H) will be a closure for (L, P_H). □

Proposition 6.14. *A subgroup S of $\dot{F}$ containing $\dot{F}^2$ is a D-ordering of F if and only if $|\dot{F}/S| = 4$ and $1 + s \in S$ whenever $s \in S$.*

Proof. All that is necessary for S to be a D-ordering of F is that it be a 2-element fan in F. In other words, S must be a preordering of index 4 in F. A subgroup S of $\dot{F}$ is such a preordering if and only if the conditions in the statement of the proposition are met. □

§7. Classification of rigid orderings

This section will provide a full Galois-theoretic and algebraic characterization of all possible rigid orderings. We start with the following definition.

Definition 7.1. Let I be a possibly empty index set. We call G a $C(I)$-group if G is isomorphic to $(C_4)^I \times C_4$, an $S(I)$-group if G is isomorphic to $(C_4)^I \rtimes C_4$, and a $D(I)$-group if G is isomorphic to $(C_4)^I \rtimes C_2$, the semidirect product being defined with the nontrivial action of C_4 or C_2 on each inner factor in the last two cases, when I is nonempty. A G-ordering on F is called a $C(I)$- (respectively $S(I)$-, $D(I)$-) ordering if G is a $C(I)$- (respectively $S(I)$-, $D(I)$-) group. When $I = \emptyset$ the $C(I)$- and $S(I)$-orderings are the C_4-orderings, and the $D(I)$-orderings are the C_2-orderings, that is the usual orderings. Observe that $C(\emptyset)$- and $S(\emptyset)$-orderings both correspond to the same group C_4. The difference between them is that a $C(\emptyset)$-ordering has level 1, while an $S(\emptyset)$-ordering has level 2. (See Remark 5.5 for comparison.) When $|I| = 1$, we obtain the groups generated by two elements which are respectively $(C_4) \times C_4$, $(C_4) \rtimes C_4$ and D.

In this section we will characterize $C(I)$-orderings, $S(I)$-orderings and $D(I)$-orderings in terms of their algebraic properties as subgroups of $\dot{F}$. We will see in particular that they are all rigid, and that they constitute the whole class of rigid orderings. The group $\coprod_{i\in I} G_i$ will denote the direct sum of the groups $G_i, i \in I$.

Proposition 7.2. *A subgroup T of $\dot{F}$ containing $\dot{F}^2$ is a $C(I)$-ordering if and only if the following three conditions hold.*

(1) $-1 \in T$,
(2) *F is T-rigid, and*
(3) $\dot{F}/T \cong \coprod_{i\in I\cup\{x\}} (C_2)_i$.

In other words, the $C(I)$-orderings are exactly the rigid orderings of level 1.

Proof. If $I = \emptyset$, the result follows from Proposition 5.4 and Remark 5.5, so we shall assume $I \neq \emptyset$. We begin by showing that the three conditions above are necessary. Let $G \cong C(I)$ and let T be a G-ordering. Suppose $-1 \notin T$. Let $\{\sigma_i, i \in I; \sigma_x\}$ generate G. Then $T = \cap_{i\in I\cup\{x\}} P_{\sigma_i}$ and $|\dot{F}/T| \geq 4$. Thus there are at least four classes mod T, which we can represent as $1, -1, a, -a$ for some $a \in \dot{F}$, and there exists a $D^{a,-a}$-extension L of F. Hence there exist elements $\sigma, \tau \in G$ such that $a \in P_\sigma \backslash P_\tau$ and $-a \in P_\tau \backslash P_\sigma$. It then follows that the restriction of $\sigma\tau$ to L has order 4, so that $\sigma|_L, \tau|_L$ generate $\mathrm{Gal}(L/F) \cong D$, and hence cannot commute. Yet $\sigma, \tau \in G$, which is an abelian group. This is a contradiction, so $-1 \in T$, and (1) holds.

Since $-1 \in T$, we have $T \cup -T = T$. Suppose we have a nonrigid element $c \in \dot{F}\backslash T$, so that we have $t_1, t_2 \in T$ with $t_1 + ct_2 \notin T \cup cT$. Then $b = 1 + ct_2/t_1 \notin T \cup cT$. Let

$a = -ct_2/t_1 \notin T$. Then $a + b = 1$, so $(\frac{a,b}{F})$ splits. Since $b \notin T \cup cT = T \cup aT$, a and b are independent mod T and thus mod $\dot{F}^2$. Hence we have a $D^{a,b}$-extension L of F, and by the same argument as above, we find $\sigma, \tau \in G$ which do not commute, leading to a contradiction. Thus F is T-rigid and (2) holds. Finally, by Kummer theory we know that $\dot{F}/T$ is isomorphic to the dual $(G/\Phi(G))^* \cong \coprod_{i \in I \cup \{x\}} (C_2)_i$, giving (3).

We now show that the three conditions are sufficient for T to be a $C(I)$-ordering. By (3) we see that $T = \cap_{i \in I \cup \{x\}} P_i$ where P_i is the kernel of the projection $\dot{F} \to \dot{F}/T \cong \coprod_{i \in I \cup \{x\}} (C_2)_i \to (C_2)_i$. Further, for each P_i we have a $\sigma_i \in \mathcal{G}_F$ such that $P_i = P_{\sigma_i}$. Let G be the closed subgroup of $\mathcal{G}_F$ generated by $\{\sigma_i | i \in I \cup \{x\}\}$. Then $G \subseteq \{\sigma | P_\sigma \supseteq T\}$ because every element of G must fix every $\sqrt{a}$ left fixed by the σ_i. So we also have $T = \cap_{\sigma \in G} P_\sigma$, and T is a G-ordering. It remains to show that G is a $C(I)$-group.

Since $-1 \in T \subseteq P_{\sigma_i}$, none of the P_{σ_i} can be usual orderings on F, so each σ_i must have exponent 4 in G. Since $-1 \in T$ and F is T-rigid, we see by Proposition 3.4 that G is abelian. Then G is a compact abelian group of exponent 4, and $(G/\Phi(G))^* \cong \coprod_{i \in I \cup \{x\}} (C_2)_i$ is a discrete group of exponent 2. Then $((G/\Phi(G))^*)^* \cong G/\Phi(G) \cong \prod_{i \in I \cup \{x\}} (C_2)_i$, and $G \cong \prod_{i \in I \cup \{x\}} (C_4)_i$, so G is a $C(I)$-group as claimed. $\square$

In order to characterize the subgroups of $\dot{F}$ which are $S(I)$-orderings, we will first prove three lemmas. Let G be an $S(I)$-group. It will be helpful to fix the following notation: write $G = G_1 \rtimes G_2$ where $G_1 \cong \prod_{i \in I} (C_4)_i$ and $G_2 \cong C_4$. Let τ be a generator of G_2 and $P_\tau = \{a \in \dot{F} | \sqrt{a}^\tau = \sqrt{a}\}$.

Lemma 7.3. *Let T be a G-ordering. Then T has index 2 in P_{G_1}.*

Proof. If $P_{G_1} \subseteq P_\tau$, we would have $T = P_{G_1} \cap P_\tau = P_{G_1} = P_G$. But by Kummer theory and the Burnside Basis Theorem, that would imply $G = G_1$. Thus $P_{G_1} \nsubseteq P_\tau$, $T \subsetneq P_{G_1}$, and $|P_{G_1}/T| \geq 2$. On the other hand, since $T = P_{G_1} \cap P_\tau$, we have $|P_{G_1}/T| \leq 2$, and so $|P_{G_1}/T| = 2$. $\square$

Lemma 7.4. *For any group homomorphism $\theta : G \to C_4 = \langle \sigma \rangle$, we have $\theta(G_1) \subseteq \langle \sigma^2 \rangle$.*

Proof. If $a \in G_1$, writing multiplicatively, we have

$$\theta(a^{-1}) = \theta(\tau a \tau^{-1}) = \theta(\tau)\theta(a)\theta(\tau)^{-1} = \theta(a),$$

so $\theta(a)^2 = 1$. $\square$

Lemma 7.5. *We have $T + T \subseteq P_{G_1}$.*

Proof. Let $a \in T + T, a \notin T$, and consider the following three cases.

Case 1: $a = x^2 + y^2$. Then there exists a C_4^a-extension L of F, and we have a map $\theta : G \to \mathrm{Gal}(L/F) \cong C_4$, and by Lemma 7.4 $\theta(G_1)$ has order at most 2. Thus $\theta(G_1)$ fixes $\sqrt{a}$ and $a \in P_{G_1}$.

Case 2: $a = x^2 + t, t \in T \setminus \dot{F}^2$. We have $a^2 = ax^2 + at$, and a, at are independent modulo $\dot{F}^2$. Thus there exists a $D^{a,at}$-extension L of F, and $\mathrm{Gal}(L/F(\sqrt{t})) \cong C_4$. Since $t \in T$, we have $\sqrt{t}^\sigma = \sqrt{t}$ for $\sigma \in G$, which means we have a homomorphism $\theta : G \to \mathrm{Gal}(L/F(\sqrt{t})) \cong C_4$. Again applying Lemma 7.4, $\theta(G_1)$ has order at most 2, so G_1 must fix $\sqrt{a}$ and $a \in P_{G_1}$.

Case 3: $a = s + t$, $s, t \in T \backslash \dot{F}^2$. We can write $as^{-1} = 1 + ts^{-1}$, and then we are in one of the previous two cases. Hence $as^{-1} \in P_{G_1}$, and it follows that $a \in P_{G_1}$. $\square$

Proposition 7.6. *A subgroup T of $\dot{F}$ containing $\dot{F}^2$ is an $S(I)$-ordering if and only if the following four conditions hold.*

(1) $-1 \notin T$,
(2) *F is $(T \cup -T)$-rigid,*
(3) $T + T = T \cup -T$, *and*
(4) $\dot{F}/T \cong \coprod_{i \in I \cup \{x\}} (C_2)_i$.

Proof. When $I = \emptyset$ the result follows from Proposition 5.4 and Remark 5.5. Thus we may assume that $I \neq \emptyset$. We begin by showing the conditions above are necessary. Condition (4) follows from Kummer theory. Condition (1) follows from Lemma 7.5 above, for if $-1 \in T$, we would have $\dot{F} \subseteq \dot{F}^2 - \dot{F}^2 \subseteq T - T = T + T \subseteq P_{G_1}$, but as $|I| \geq 1$, we cannot have P_{G_1} being all of $\dot{F}$.

To show the necessity of condition (3), first observe that $-1 \in P_{G_1}$, $-1 \notin T$, and $|P_{G_1}/T| = 2$, so $P_{G_1} = T \cup -T$, and thus $T + T \subseteq T \cup -T$. To show equality, we need to show that some element of $-T$ is in $T + T$. In this case, that amounts to showing that T is not additively closed. Suppose that T were additively closed. Then T would be a preordering, so contained in some ordering P_σ for some $\sigma \in \mathcal{G}_F$. Further, σ is an involution not contained in $\Phi(\mathcal{G}_F)$, and $\sigma \in G = G_1 \rtimes G_2$. In particular, σ is not a square in G, and $\sigma \neq \tau$. Thus $\sigma = \sigma_1 \tau$ for some $\sigma_1 \in G_1$ and

$$\sigma^2 = \sigma_1 \tau \sigma_1 \tau = \sigma_1 \tau \sigma_1 \tau^{-1} \tau^2 = \sigma_1 \sigma_1^{-1} \tau^2 = \tau^2 \neq 1.$$

Thus σ is not an involution, which is a contradiction, and so $-1 \in T + T$. Finally, since F is P_{G_1}-rigid and $T \cup -T = P_{G_1}$, we see that (2) holds.

Now we must show that conditions (1) - (4) are sufficient for T to be an $S(I)$-ordering. Letting $S = T \cup -T$, we see that S satisfies the condition for being a G_1-ordering, with $G_1 \cong \prod_{i \in I} (C_4)_i$, as given in Proposition 7.2. Let Q be a subgroup of index 2 in $\dot{F}$ such that $T = S \cap Q$, and let $\tau \in \mathcal{G}_F$ such that $Q = P_\tau$. Let G be the subgroup of $\mathcal{G}_F$ generated by G_1 and τ. We need to see that $G = G_1 \rtimes G_2$ where G_2 is the subgroup of $\mathcal{G}_F$ generated by τ. Specifically, we need to show that $G_1 \cap G_2 = \{1\}$ and that $[\sigma, \tau]\sigma^2 = 1 \ \forall \sigma \in G_1$.

Since G_1 fixes $\sqrt{-1}$ and τ does not, we cannot have τ or τ^{-1} in G_1. Suppose $\tau^2 \in G_1$. Then it has order 2 in G_1 and hence must be a square. Let $\sigma \in G_1$ such that $\sigma^2 = \tau^2$. Since $P_\sigma \neq P_\tau$, there exists $a \in P_\tau \backslash P_\sigma$, and neither a nor $-a$ can be a square, since neither is in P_σ. Since also $-1 \notin \dot{F}^2$, we have a $D^{a,-a}$-extension L of F, and $\sigma|_L$ has order 4 in $\mathrm{Gal}(L/F)$. However, since τ fixes $\sqrt{a}$, $\tau|_L \in \mathrm{Gal}(L/F(\sqrt{a})) \cong C_2 \times C_2$, and so $\sigma^2 \neq \tau^2$, contradicting the assumption. Thus $G_1 \cap G_2 = \{1\}$.

To prove $[\sigma, \tau]\sigma^2 = 1 \ \forall \sigma \in G_1$, it is sufficient to show that this condition holds for the restriction of σ, τ to each C_4- and D-extension of F. Suppose L is a C_4^a-extension of F. Then a is a sum of two squares, so $a \in T + T = T \cup -T = P_{G_1}$ and $[\sigma, \tau]\sigma^2|_L = \sigma^2|_L$. Since $\sigma \in G_1$, $\sigma \in \mathrm{Gal}(L/F(\sqrt{a}))$ and $\sigma^2|_L = 1$.

Now suppose L is a $D^{a,b}$-extension of F. We may assume $\sigma \notin Z(\mathrm{Gal}(L/F))$ (the centralizer), since otherwise clearly $[\sigma, \tau]\sigma^2|_L = 1$. Without loss of generality, we may assume $\sqrt{a}^\sigma = -\sqrt{a}$. Then $a \notin T \cup -T$, and since $1 = ax^2 + by^2$, we have $b \in T - aT$, and by rigidity, $b \in T \cup -aT \cup -T \cup aT$. However, if b were in $-T$ or aT, then we would obtain $a \in T + T = T \cup -T$, a contradiction. Thus $b \in T \cup -aT$.

If $b \in T$, then σ and τ both fix $\sqrt{b}$ and both have order 2. If τ does not fix $\sqrt{a}$, then σ, τ act the same on $\sqrt{a}$ and $\sqrt{b}$ and hence commute. If τ fixes $\sqrt{a}$ then $\tau \in Z(\mathrm{Gal}(L/F))$ so in either case $[\sigma, \tau]\sigma^2 = \sigma^2 = 1$.

If $b \in -aT$, then σ fixes neither $\sqrt{a}$ nor $\sqrt{-a}$, so has order 4. Since τ acts differently on $\sqrt{a}$ and $\sqrt{b}$, it must fix one of them and be of order 2, and the same holds for $\sigma\tau$. Then $[\sigma, \tau]\sigma^2 = \sigma\tau\sigma^{-1}\tau^{-1}\sigma^2 = \tau^{-1}\sigma^{-2}\tau^{-1}\sigma^2 = 1$ since $\sigma^2 \in Z(\mathrm{Gal}(L/F))$. □

We have another convenient formulation of Proposition 7.6 as follows:

Corollary 7.7. *A subgroup T of $\dot{F}$ containing $\dot{F}^2$ is an $S(I)$-ordering if and only if the following three conditions hold.*

(a) T has level 2,

(b) F is T-rigid, and

(c) $\dot{F}/T \cong \coprod_{i \in I \cup \{x\}} (C_2)_i$.

In other words the $S(I)$-orderings are exactly the rigid orderings of level 2.

Proof. If $I = \emptyset$, the result follows from Definition 7.1, so we shall assume that $I \neq \emptyset$. Assume that T satisfies (1), (2) and (3) of Proposition 7.6. We show it is rigid. Let $a \in \dot{F} \setminus (T \cup -T)$. Then $T + aT \subset (T \cup -T) + a(T \cup -T) = T \cup -T \cup aT \cup -aT$. Take $s+at \in T+aT$ and suppose it is not in $T \cup aT$. Then it is in $-T \cup -aT$. If $s+at = -u \in -T$ then $-a = t(u+s) \in T + T = T \cup -T$, a contradiction. If $s + at = -au \in -aT$ then $-a = s/(u+t) \in T + T = T \cup -T$, a contradiction. Thus T is rigid.

By Proposition 3.3, a rigid ordering of finite level greater than 1 is exactly a rigid ordering of level 2. This proves (a) and (b).

Conversely, if T satisfies (a) and (b), then it satisfies (1) and (3) by Proposition 3.3. Let us show we also have (2). Let $a \in \dot{F} \setminus \pm(T \cup -T) = T \cup -T$. Then $(T \cup -T) + a(T \cup -T) = \pm(T + aT) \cup \pm(T - aT) \subseteq \pm(T \cup aT) \cup \pm(T \cup -aT) = (T \cup -T) \cup a(T \cup -T)$. Since we always have $S \cup aS \subseteq S + aS$ for any subgroup S, we see that F is $T \cup -T$-rigid. □

Example 7.8. It is well-known that if $K \longrightarrow L$ is a field extension and if T is a usual ordering of L, then $S = K \cap T$ is a usual ordering of K. This need not hold for $C(\emptyset)$-orderings nor for $S(\emptyset)$-orderings. Consider for example $L = K(\sqrt{\dot{K}})$ and assume that L is equipped with some $C_\emptyset$-ordering T. Since $\dot{L}^2 \cap K = \dot{K}$ and $\dot{L}^2 \subseteq T$, we also have $T \cap K = \dot{K}$: the $C_\emptyset$-ordering T "vanishes" under the restriction. This happens in particular if K is the finite field $\mathbb{F}_q$ with an odd number q of elements. With $L = \mathbb{F}_{q^2}$, $\dot{L}^2$ is a $C_\emptyset$-ordering. Observe that this cannot happen when T is an $S(\emptyset)$-ordering in an extension L of K: since -1 is not in T, it cannot be in $S = T \cap K$, and S cannot be the trivial index 1 subgroup. But $S(\emptyset)$-orderings are subject to another pathology of their own: it may happen that the restriction of an $S(\emptyset)$-ordering is a C_2-ordering. (Observe that this cannot happen with $C(\emptyset)$-orderings.) Take for example $K = \mathbb{Q}, L = K(\sqrt{10})$, and denote by N the norm map from L down to K. Let α be the ordering of L containing $\sqrt{10}$. Let v be the discrete rank 1 valuation on $\mathbb{Q}$ associated to the prime 3. Define $T := \{h \in \dot{L} \mid (-1)^{v(N(h))} h \in \alpha\}$. Then $-1 \notin T$ and T is a subgroup containing $\dot{K}^2$, of index 2 in $\dot{K}$ (if $x \notin T, -x \in T$) . It is not a usual ordering, since $-4-\sqrt{10}$ is negative at the two orderings of L but belongs to T, as its norm 6 has an odd 3-valuation. Thus it must be an $S(\emptyset)$-ordering. Since $N(f)=f^2$ has an even valuation when $f\in K$, we see that $S:=T\cap K$ is the usual ordering of $\mathbb{Q}$.

Proposition 7.9. *A subgroup T of $\dot F$ containing $\dot F^2$ is a $D(I)$-ordering if and only if the following three conditions hold.*

(1) $-1\notin T$,
(2) $T+T=T$,
(3) F *is* T*-rigid, and*
(4) $\dot F/T\cong\coprod_{i\in I\cup\{x\}}(C_2)_i$.

In other words, $D(I)$-orderings are exactly the rigid orderings of infinite level.

Proof. It is known that conditions (1), (2), (3) are one of the characterizations of fans [BK], and by [CrSm, Proposition 4.1], fans are exactly $D(I)$-orderings for some index set I (possibly empty if we think of usual orderings as 1-element fans). By Proposition 3.3, we immediately see that they are the rigid orderings of infinite level. □

To conclude the section we may summarize the results with the following

Theorem 7.10. *Rigid orderings are exactly $C(I)-,S(I)-$ or $D(I)$-orderings for some (possibly empty) index set I.*

Proof. This is a straightforward application of Proposition 3.3, Proposition 7.2, Corollary 7.7 and Proposition 7.9. □

§8. Construction of closures for rigid orderings

In this section we employ valuation-theoretic techniques to construct closures for $C(I)$-, $S(I)$- and $D(I)$-orderings. From the preceding section, we know that both $C(I)$- and $S(I)$-orderings are T-rigid. Then for such an ordering we will be able to use results of Arason, Elman, Jacob [AEJ], Efrat [Ef] and Ware [Wa] to associate a valuation to T. For $D(I)$-orderings, it is the "Fan Trivialization Theorem" of Bröcker [Br, Theorem 2.7] that will be used. Since it is well known (see [Ri]) that for each algebraic extension K/F we can extend any valuation v on F to a valuation w on K, we can then use this to extend $S(I)$- or $D(I)$-orderings, and in most cases also $C(I)$-orderings, from F to $F(\sqrt{t})$, $t\in T$. This will allow us to prove the existence of $S(I)$- and $D(I)$-closures, and in most cases also $C(I)$-closures.

For the reader's convenience we define here some of the valuation-theoretic notation we will be using below. For more detailed information, we refer the reader to [End] and [Ri] as well as [AEJ], [Wa] and [Br].

Let $v:F\to\Gamma\cup\{\infty\}$ be a valuation on the field F, where Γ is some linearly ordered abelian group. Then we set A_v to be the valuation subring of F, M_v to be the unique maximal ideal of A_v (consisting of those elements $f\in F$ such that $v(f)>0$), and U_v to be the group of invertible elements of A_v. We say T is *compatible* with v (or A_v) if $1+M_v\subseteq T$. We denote the residue field A_v/M_v by F_v, and we set $\pi_v:A_v\to F_v$ to denote the canonical epimorphism from A_v onto F_v.

The strategy of the proof is as follows: It is easy to reduce the problem of constructing H-closures to the problem of extending a given H-ordering T of a field F to an H-ordering T' of any quadratic extension $L = F(\sqrt{t}), t \in T$, such that $T' \cap F = T$. (Here $H \cong C(I), S(I)$, or $D(I)$.) In order to extend T in this manner, we first find a suitable T-compatible valuation v on F and then extend v to a valuation w on L. We then extend the induced ordering $\bar{T}$ of the residue field F_v to $\hat{T}$ on the residue field L_w of L with respect to the valuation w. Finally we lift the ordering $\hat{T}$ from the residue field L_w to an ordering $\tilde{T}$ on L, and then show that $\tilde{T}$ is the desired extension of T from F to L.

Suppose first that we are given some $S(I)$-ordering T of F. In this case, T is "not exceptional" in the sense of [AEJ, Definition 2.15]. Thus we can apply [AEJ, Theorem 2.16] to obtain the following.

Proposition 8.1. *Let T be any $S(I)$-ordering of F. Then there exists a T-compatible nondyadic valuation v of F such that $U_vT = T \cup -T$. The set $\bar{T} := \pi_v(T \cap U_v)$ is an $S(\emptyset)$-ordering of F_v.*

Proof. By [AEJ, Theorem 2.16], we have a T-compatible valuation v such that $U_vT = T \cup -T$. The last statement of the proposition follows from this. Indeed we have

$$\frac{U_v}{U_v \cap T} \cong \frac{U_vT}{T} \cong \frac{T \cup -T}{T}.$$

Since $-1 \notin T$ we see that $F_v = \bar{T} \cup -\bar{T}$ and $-1 \notin \bar{T}$. Therefore $\bar{T}$ has index 2 in $\dot{F}_v$.

Since T is an $S(I)$-ordering on F, we see that there exist elements $t_1, t_2, t_3 \in T$ such that $t_1 + t_2 + t_3 = 0$. Dividing through by that element t_i whose value $v(t_i)$ is minimal among the three elements considered (say t_1), we may assume we have

$$-1 = t_2 + t_3, v(t_2), v(t_3) \geq 0$$

Passing to the residue field we obtain $\bar{t_1} + \bar{t_2} = -\bar{1}$ in F_v. Since $-1 \notin \bar{T}$ we see that $\bar{t_i} \neq 0, i = 2, 3$. Thus $-1 \in \bar{T} + \bar{T} \setminus \bar{T}$, and $\bar{T}$ is a $S(\emptyset)$-ordering of F_v, as claimed.

Observe also that $-1 \notin \bar{T}$ implies $-1 \neq 1$ and $\operatorname{char} F_v \neq 2$. Thus v is nondyadic. $\square$

Next suppose we have a $C(I)$-ordering T of F. Then we may apply [Ef, Propositions 2.1 and 2.3 and Theorem 4.1], to yield the following result.

Proposition 8.2. *Let T be any $C(I)$-ordering of F. Then there exists a T-compatible valuation ring A_v of F such that $[U_vT : T] \leq 2$ and $\dim_{\mathbb{F}_2} \Gamma/2\Gamma \geq |I|$, where Γ is the associated value group. The set $\bar{T} := \pi_v(T \cap U_v)$ is either $\dot{F}_v$ itself or a $C(\emptyset)$-ordering of F_v.*

Proof. Observe again that the last statement claiming that $\bar{T} := \pi_v(T \cap U_v)$ is either $\dot{F}_v$ itself or a $C(\emptyset)$-ordering, and also the statement $\dim_{\mathbb{F}_2} \Gamma/2\Gamma \geq |I|$, are consequences of the first part of the proposition. We have $\frac{U_vT}{T} \cong \frac{U_v}{U_v \cap T}$, so $[U_v : U_v \cap T] \leq 2$; hence $U_v = U_vT$ or $[U_v : U_v \cap T] = 2$. In the latter case, we see that $\bar{T} = \pi_v(T \cap U_v)$ is a $C(\emptyset)$-ordering as $-\bar{1} \in \bar{T}$. Also observe that we have $|I| + 1 = \dim_{\mathbb{F}_2} \frac{\dot{F}}{T} = \dim_{\mathbb{F}_2} \frac{\dot{F}}{U_vT} + \dim_{\mathbb{F}_2} \frac{U_vT}{T}$. From the hypothesis $[U_vT : T] \leq 2$ we see that $\dim_{\mathbb{F}_2} \frac{U_vT}{T} \leq 1$. Hence $\dim_{\mathbb{F}_2} \frac{\dot{F}}{U_vT} \geq |I|$. Therefore $\dim_{\mathbb{F}_2} \Gamma_v \geq \dim_{\mathbb{F}_2} \frac{\dot{F}}{U_vT} \geq |I|$ as claimed. $\square$

Proposition 8.3. (Fan Trivialization Theorem [Br, Theorem 2.7]) *Let T be any $D(I)$-ordering of F. Then there exists a T-compatible valuation ring A_v of F such that the set $\bar{T} := \pi_v(T \cap U_v)$ is either an ordering of F_v or a D-ordering of F_v. (When $\bar{T}$ is an ordering, T is called a valuation fan.) Moreover, the valuation v may be chosen such that $v(T)$ contains no convex subgroups of $v(F)$.*

Now suppose that we have an $S(I)$-ordering (respectively $C(I)$-, $D(I)$-ordering) T together with a T-compatible valuation v on F. Assume $t \in T$, and let $K = F(\sqrt{t})$. Our goal is to find an $S(I)$-ordering (respectively $C(I)$-, $D(I)$-ordering) T' of K such that $T' \cap F = T$ and $\dot{F}/T \cong \dot{K}/T'$ is the isomorphism of multiplicative groups induced by the inclusion $F \hookrightarrow K$. Note that if $T' \cap F = T$, then the map $\dot{F}/T \to \dot{K}/T'$ is injective, so we need only worry about surjectivity. Then recall the well-known Krull's Theorem ([Ri, Theorem 5]):

Theorem 8.4. (Krull) *Let F be a field and $\tilde{F}$ any overfield of F. Any valuation v in F can be extended to a valuation $\tilde{v}$ in $\tilde{F}$.*

Thus we see that there exists a valuation w on K which extends v. In order to proceed we make the following convenient reduction.

Lemma 8.5. *Assume that $T_1 \subseteq T_2$ are respectively $S(I_1)$- and $S(I_2)$-orderings of F, and let $t \in T_1 \setminus \dot{F}^2$. Let $K = F(\sqrt{t})$. Suppose T_1' is an extension of T_1 to an $S(I_1)$-ordering of K. Then $T_2' := T_1'T_2$ is an $S(I_2)$-ordering of K extending T_2.*

Proof. We first show that $T_2' \cap F = T_2$. By definition, $T_2 \subseteq T_2' \cap F$, and if $f \in T_2' \cap F$ then there exists $t_1' \in T_1', t_2 \in T_2$ such that $f = t_1't_2$. This implies $t_1' \in F \cap T_1' = T_1 \subseteq T_2$, and $f \in T_2$. Thus $T_2' \cap F = T_2$.

Consider the natural homomorphism $\varphi_2 : \dot{F}/T_2 \to \dot{K}/T_2'$ induced by the inclusion map $F \hookrightarrow K$. Because $T_2' \cap F = T_2$ we see that φ_2 is injective. Consider the following diagram:

$$\begin{array}{ccc} \dot{F}/T_1 & \xrightarrow{\varphi_1} & \dot{K}/T_1' \\ \downarrow & & \downarrow \\ \dot{F}/T_2 & \xrightarrow{\varphi_2} & \dot{K}/T_2' \end{array}$$

Since we know that $\varphi_1 : \dot{F}/T_1 \to \dot{K}/T_1'$ is bijective, and since $T_1' \subseteq T_2'$, we see that φ_2 is also surjective.

Finally we shall show that T_2' is an $S(I_2)$-ordering by checking that conditions (a),(b),(c) of Corollary 7.7 hold. Since $T_2' \cap F = T_2$, we see that $-1 \notin T_2'$. As $-1 \in T_1' + T_1' \subseteq T_2' + T_2'$, we see that T_2' satisfies condition (a).

Suppose $s = u + av \in K$ with $u, v \in T_2'$ and $a \notin (T_2' \cup -T_2')$. By definition of T_2', u, v can be written $u = u_1'u_2, v = v_1'v_2$ with $u_1', v_1' \in (T_1' \cup -T_1')$, $u_2, v_2 \in T_2$. Then $su_2^{-1} = u_1' + (av_2u_2^{-1})v_1'$. Because $av_2u_2^{-1} \notin (T_1' \cup -T_1')$, the T_1'-rigidity of K implies $su_2^{-1} \in T_1' \cup (av_2u_2^{-1})T_1'$, and thus $s \in T_2' \cup aT_2'$, giving condition (b).

Finally, to check condition (c), observe that $\dot{K}/T_2' \cong \dot{F}/T_2 \cong \coprod_{i \in I_2 \cup \{x\}} (C_2)_i$. Thus T_2' is an $S(I_2)$-ordering which extends T_2. $\square$

Lemma 8.6. *Assume that $T_1 \subseteq T_2$ are respectively $C(I_1)$- and $C(I_2)$-orderings of F, and let $t \in T_1 \setminus \dot{F}^2$. Let $K = F(\sqrt{t})$. Suppose T_1' is an extension of T_1 to a $C(I_1)$-ordering of K. Then $T_2' := T_1'T_2$ is a $C(I_2)$-ordering of K extending T_2.*

Proof. The proof is identical to that of Lemma 8.5, except that one must now check that $-1 \in T_2'$. Since $T_2' \cap F = T_2$, we see $-1 \in T_2'$. □

Lemma 8.7. *Assume that $T_1 \subseteq T_2$ are respectively $D(I_1)$- and $D(I_2)$-orderings of F, and let $t \in T_1 \setminus \dot{F}^2$. Let $K = F(\sqrt{t})$. Suppose T_1' is an extension of T_1 to a $D(I_1)$-ordering of K. Then $T_2' := T_1'T_2$ is a $D(I_2)$-ordering of K extending T_2.*

Proof. Again the proof takes the same arguments as in the proof of Lemma 8.5 to show that T_2' extends T_2, that $-1 \notin T_2'$ and that K is T_2'-rigid. Let us prove $T_2' + T_2' = T_2'$. Consider $u, v \in T_2'$ and write them as above, $u = u_1'u_2, v = v_1'v_2$, with $u_1', v_1' \in T_1'$ and $u_2, v_2 \in T_2$. Then $u+v = u_2(u_1' + (v_2u_2^{-1})v_1')$. We know that $-1 \notin T_2'$, and this implies that $v_2u_2^{-1} \notin -T_1'$. If $v_2u_2^{-1} \in T_1'$, then $(u+v)u_2^{-1} \in T_1' + T_1' = T_1'$ and $u+v \in T_2'$. The remaining possibility is $v_2u_2^{-1} \notin T_1' \cup -T_1'$, and by T_1'-rigidity of K, we have $(u+v)u_2^{-1} \in T_1' \cup (v_2u_2^{-1})T_1'$ and $u+v \in T_2'$. Hence condition (2) holds. □

We consider the following situation. Assume that $v : F \to \Gamma_v \cup \{\infty\}$ is a valuation on the field F, with valuation ring A_v and maximal ideal M_v. Let $F_v = A_v/M_v$ be the residue field, and denote by π_v the canonical homomorphism of A_v onto its quotient ring F_v.

Lemma 8.8. *Assume that v is a valuation on the field F and that T_0 is an $S(I_0)$-ordering of $\dot{F}_v$ for some (possibly empty) set I_0. Set $T_1 = \pi_v^{-1}(T_0)$. Then the group $T = T_1\dot{F}^2$ is an $S(I)$-ordering of F with $|I| = dim_{\mathbb{F}_2}(\frac{\dot{F}}{T \cup -T})$.*

Proof. What is needed is to check that the conditions in Corollary 7.7 hold for T. First, suppose that $-1 \in T$. Then $-1 = t_0 f^2$ for some $t_0 \in T_1, f \in \dot{F}$. Hence $f^2 = (-t_0)^{-1} \in -T_1 \subseteq U_v$, and so $f \in U_v$ as well. Passing to the residue field F_v and knowing $\dot{F_v}^2 \subseteq T_0$ we see $-1 = \bar{t}_0\bar{f}^2 \in T_0$, which is a contradiction. Thus we must have $-1 \notin T$. Since $-1 \in T_0 + T_0$, we have $-1 + m \in T_1 + T_1$ for some m in the maximal ideal of the valuation, and $-1 + m \in -T_1 \subset T$. This shows that the level of T is 2.

To see that F is T-rigid, let $a \in \dot{F} \setminus (T \cup -T), t_1, t_2 \in T$, and consider $b := t_1 + t_2a$. We consider various possibilities for $v(t_1)$ relative to $v(t_2a)$. First suppose that $v(t_1) = v(t_2a)$. Then $b = t_1(1 + t_1^{-1}t_2a)$, with $u := t_1^{-1}t_2a \in U_v$. Since $a \notin T \cup -T$, we see that $\pi_v(u) = \bar{u} \notin T_0 \cup -T_0$. (Otherwise $u \in \pi_v^{-1}(T_0) = T_1 \subseteq T$ or $u \in -\pi_v^{-1}(T_0) = -T_1 \subseteq -T$ and hence $a \in T \cup -T$, a contradiction.) Since we are assuming F_v is T_0-rigid, we see that $1 + \bar{u} \in T_0 \cup \bar{u}T_0$. Hence $1 + u \in \pi_v^{-1}(T_0 \cup \bar{u}T_0) = T_1 \cup uT_1$. Thus, rewriting $u = t_1^{-1}t_2a$ and multiplying through by t_1, we see

$$b = t_1 + t_2a \in T_1 \cup aT_1 \subseteq T \cup aT$$

as required. Now assume that $v(t_1) \neq v(t_2a)$. If $v(t_1) < v(t_2a)$, then again let $b = t_1(1+u)$, where $u = t_1^{-1}t_2a$. Now, however, $v(u) > 0$, so $1 + u \in 1 + M_v \subseteq T_1 = \pi_v^{-1}(T_0)$, and thus $b \in T$. If $v(t_1) > v(t_2a)$, set $b = at_2(1 + t_1t_2^{-1}a^{-1})$. We see $v(t_1t_2^{-1}a^{-1}) > 0$, and therefore $b \in aT$. In each case $b = t_1 + at_2 \in T \cup aT$ as desired.

It remains to see that $\dot{F}/T \cong \coprod_{i\in I\cup\{x\}}(C_2)_i$. This condition follows from the fact that $\dot{F}/T$ is an $\mathbb{F}_2$-vector space and that $dim_{\mathbb{F}_2}\dot{F}/T$ is $1+|I|$. $\square$

We have the analogue to Lemma 8.8 for the case of $C(I)$-orderings.

Lemma 8.9. *Assume that v is a valuation on the field F such that $[\Gamma_v : 2\Gamma_v] \geq 2$. Let T_0 be $\dot{F}_v$ or a $C(I_0)$-ordering of F_v for some (possibly empty) set I_0. Set $T_1 = \pi_v^{-1}(T_0)$. Then the group $T = T_1\dot{F}^2$ is a $C(I)$-ordering of F with $|I| = dim_{\mathbb{F}_2}(\frac{\dot{F}}{T}) - 1$.*

Proof. We must check that the conditions of Proposition 7.2 hold for T. Clearly if $-1 \in T_0$, then $-1 \in T_1 \subseteq T$. To see that F is T-rigid, one applies the same argument as in Lemma 8.8. As in the case for $S(I)$-orderings, $\dot{F}/T$ is clearly an $\mathbb{F}_2$-vector space. Since $[\Gamma_v\colon 2\Gamma_v] \geq 2$, its dimension is strictly positive and thus may be written $dim_{\mathbb{F}_2}(\dot{F}/T) = 1+|I|$. $\square$

Again, we also have the analogue to Lemma 8.8 for the case of $D(I)$-orderings.

Lemma 8.10. ([Br]) *Assume that v is a valuation on the field F. Let T_0 be a fan of $\dot{F}_v$. Set $T_1 = \pi_v^{-1}(T_0)$. Then the group $T = T_1\dot{F}^2$ is a fan (i.e. a $D(I)$-ordering) of F.*

We now formulate the key results in this section.

Theorem 8.11. *Let T be any $S(I)$-ordering of F and let $L = F(\sqrt{t}), t \in T$. Then there exists an $S(I)$-ordering T' on L such that (L, T') is an $S(I)$-extension of (F, T).*

Proof. From Proposition 8.1, we see that there exists a nondyadic T-compatible valuation ring A_v in F such that $U_vT = T \cup -T$ and that $\bar{T} := \pi_v(U_v \cap T)$ is an $S(\emptyset)$-ordering of F_v. As $\pi_v^{-1}(\bar{T}) = (U_v \cap T)(1+M_v)$ and because $(1+M_v) \subseteq T$, one has $T_1 := \pi_v^{-1}(\bar{T})\dot{F}^2 \subseteq T$. By Lemma 8.8, we see that T_1 is an $S(J)$-ordering in F for a suitable set J.

Let w be any valuation of L which extends v. Let L_w denote its residue field, and Γ_v, Γ_w denote the valuation groups of v and w. We may assume $\Gamma_v \subseteq \Gamma_w$, and we set $e = [\Gamma_w : \Gamma_v]$, the ramification degree of w with respect to v, and $f = [L_w : F_v]$, the residue class degree of w with respect to v. It is well known that $ef \leq [L : F] = 2$ and in particular we have $f = [L_w : F_v] \leq 2$. More precisely, one has $L_w = F_v(\sqrt{\pi_v(u_0)})$ with $u_0 = 1$ if $f = 1$, and $u_0/t \in \dot{F}^2$ if $f = 2$. By Proposition 5.6 and Remark 5.5, C_4-orderings are known to admit C_4-closures of the same level, and as $\pi_v(u_0) \in \bar{T}$, the $S(\emptyset)$-ordering $\bar{T}$ admits an $S(\emptyset)$-extension $\tilde{T}$ to $F_v(\sqrt{\pi_v(u_0)}) = L_w$. Calling $T_2 = \pi_w^{-1}(\tilde{T})L^2$, Lemma 8.8 implies that T_2 is an $S(K)$-ordering of L for a suitable set K.

Let us first show that $T_1 = T_2 \cap F$. By definition of T_1, an element $s \in T_1$ has the same square class as an element $u \in U_v$ such that $\pi_v(u) \in \bar{T} \subseteq \tilde{T}$. This implies that $\pi_w(u) \in \tilde{T}$, and thus u and s are in T_2. This shows $T_1 \subseteq T_2 \cap F$.

For the reverse inclusion, we state the following claim:

Claim. *With notation as above, one has $\dot{L} = U_w\dot{F} \cap \sqrt{t}U_w\dot{F}$.*

Proof. We know that $e \leq 2$. If $e = 1$, then $\dot{L} = \dot{F}U_w$ and we are done. If $e = 2$, then $f = 1$ and we may show that $w(\sqrt{t}) \notin \Gamma_v$. Otherwise $\sqrt{t} = xu$ with $x \in F$ and $u \in U_w$, and denoting by σ the nontrivial element of the Galois group $\mathrm{Gal}(L/F)$, we know that $\frac{\sigma(\sqrt{t})}{\sqrt{t}} = -1$ and thus $\pi_w(\frac{\sigma(\sqrt{t})}{\sqrt{t}}) = \pi_w(\frac{\sigma(u)}{u}) = -1$. Since $f = 1$, $L_w = F_v$, and so $\pi_w(\frac{\sigma(u)}{u})$

must also be 1. Since the valuation v is not dyadic, this would be a contradiction. Thus we see that since $\Gamma_w \cong \dot{L}/U_w, \Gamma_v \cong \dot{F}/U_v$, and $[\Gamma_w : \Gamma_v] = 2$, the factor group $\dot{L}/U_w\dot{F}$ is $\{1,\sqrt{t}\}$, and we can write $\dot{L} = U_w\dot{F} \cup \sqrt{t}U_w\dot{F}$. □

We now finish the proof of the theorem. If $\alpha \in T_2 \cap F$, we may write $\alpha = u\lambda^2$ with $u \in \pi_w^{-1}(\tilde{T}), \lambda \in \dot{L}$, and writing $\lambda = \sqrt{t}^{\eta}u_1 g$ with $u_1 \in U_w, g \in \dot{F}, \eta = 0$ or 1, this yields $\alpha = uu_1^2 t^{\eta} g^2$. Since $t^{\eta}g^2 \in T_1$, we may assume $\alpha = uu_1^2$. Then $\pi_v(\alpha) = \pi_w(\alpha) \in \tilde{T} \cap F_v = \bar{T}$ and $\alpha \in T_1$. This proves $T_1 = T_2 \cap F$.

We define a new subgroup T_2' of $\dot{L}$ as follows.

(1) If $\sqrt{t} \in (T_2 \cup -T_2)$, set $T_2' = T_2$.
(2) If $\sqrt{t} \notin (T_2 \cup -T_2)$ and $[\Gamma_w : \Gamma_v] = 1$, again set $T_2' = T_2$.
(3) If $\sqrt{t} \notin (T_2 \cup -T_2)$ and $[\Gamma_w : \Gamma_v] = 2$, set $T_2' = T_2 \cup \sqrt{t}T_2$.

Then again $T_1 = T_2' \cap F$, the only thing to prove being that in the third case, $\sqrt{t}T_2 \cap F \subseteq T_1$. But if $\alpha \in \sqrt{t}T_2 \cap F$ we have $\alpha = \sqrt{t}ug^2$ with $u \in U_w, g \in \dot{F}$ and this implies $w(\sqrt{t}) \in \Gamma_v$, contradicting $[\Gamma_w : \Gamma_v] = 2$. This shows that $\sqrt{t}T_2 \cap F = \emptyset$ in the third case.

Since T_2 is an $S(K)$-ordering, it is easy to check that conditions (1)-(3) of Proposition 7.6 hold for T_2' and to see that T_2' is also an $S(K')$-ordering for a suitable set K'.

We want to show that the injection $\dot{F}/T_1 \longrightarrow \dot{L}/T_2'$ is also surjective, which reduces to showing that $\dot{L} = T_2'\dot{F}$. We already know $\dot{L} = U_w\dot{F} \cup \sqrt{t}U_w\dot{F}$, and by Lemma 8.1, $U_w \subseteq T_2 \cup -T_2$. This gives us $U_w\dot{F} \subseteq T_2\dot{F} \subseteq T_2'\dot{F}$. In cases (1) and (3), one has $\sqrt{t} \in T_2' \cup -T_2'$, and so $\dot{L} \subseteq T_2'\dot{F}$. In case (2), there exists $x_0 \in \dot{F}$ such that $\sqrt{t}x_0 \in U_w \subseteq T_2\dot{F}$. So $\sqrt{t} \in T_2\dot{F}$, finishing the proof that $\dot{F}/T_1 \longrightarrow \dot{L}/T_2'$ is an isomorphism.

We have proved so far that (L, T_2') is an $S(J)$-extension of (F, T_1), and that T_1 is contained in the $S(I)$-ordering T. We may then apply Lemma 8.5 to show that (L, T_1T_2') is an $S(I)$-extension of (F, T), and the theorem is proved. □

Corollary 8.12. *An $S(I)$-ordered field (F, T) admits an $S(I)$-closure.*

Proof. Let $\mathcal{S}$ be the set of extensions (L, S) of (F, T) inside $F(2)$ such that S is an $S(I)$-ordering on L. Then by a Zorn's Lemma argument $\mathcal{S}$ has a maximal element (K, T_0) with $\dot{K}/T_0 \cong \dot{F}/T, T = T_0 \cap F$, and T_0 is an $S(I)$-ordering on K. We are done by Corollary 4.3 if we can show $T_0 = \dot{K}^2$. If not, choose $t \in T_0 \backslash \dot{K}^2$. Then by Theorem 8.11 we can extend T_0 to an $S(I)$-ordering on $K(\sqrt{t})$, contradicting the maximality of (K, T_0). □

Corollary 8.12 can be reformulated in the language of Galois theory as in the following corollary, which tells us that a certain family of subgroups of $G_F := \mathrm{Gal}(F(2)/F)$ occurs whenever G_F contains certain subquotients of G_F. Observe that in Corollary 8.13 we do not specify the action of the outer factor $\mathbb{Z}_2$ on the normal subgroup $(\mathbb{Z}_2)^I$ as this action depends upon a subtler analysis of the roots of unity belonging to the fields under consideration.

Corollary 8.13. *Let F be a field of characteristic $\neq 2$. Suppose that we have a tower of field extensions $F \subset N_1 \subset N_2 \subset N_1^{(3)} \subset F(2)$, where $N_1^{(3)}/N_2$ is a Galois extension and $\mathrm{Gal}(N_1^{(3)}/N_2) \cong (C_4)^I \rtimes C_4$ for I some nonempty set. Then $G_F = \mathrm{Gal}(F(2)/F)$ contains the closed subgroup $(\mathbb{Z}_2)^I \rtimes \mathbb{Z}_2$.*

Proof. Let $F \subset N_1 \subset N_2 \subset N_1^{(3)} \subset F(2)$ be a tower of field extensions, where $N_1^{(3)}/N_2$ is a Galois extension and $\mathrm{Gal}(\frac{N_1^{(3)}}{N_2}) \cong (C_4)^I \rtimes C_4$ for I some nonempty set. Set $T = \{t \in \dot{N}_1 \mid (\sqrt{t})^\sigma = \sqrt{t}$ for each $\sigma \in \mathrm{Gal}(N_1^{(3)}/N_2)\}$. From Definition 7.1 we see that T is an $S(I)$-ordering of N_1. From Corollary 8.12 it follows that there exists a field extension N of N_1 such that $\dot{N}^2$ is an $S(I)$-ordering of N and $\dot{N}^2 \cap N_1 = T$. Then Proposition 8.1 implies the existence of an $\dot{N}^2$-compatible valuation ring A_v of N such that $U_v\dot{N}^2 = \dot{N}^2 \cup -\dot{N}^2$.

It is well known that an $\dot{N}^2$-compatible valuation v on N is 2-henselian. Moreover N is a rigid field (and is $S(I)$-closed). In Proposition 8.1 we observed that v is a nondyadic valuation (i.e., char $F_v \neq 2$) and in this case it follows from basic valuation theory (see e.g. [End, §20]) that we have a split short exact sequence

$$1 \longrightarrow I_v \longrightarrow G_N(2) \longrightarrow G_{N_v}(2) \longrightarrow 1,$$

where I_v is the inertia subgroup of $G_N(2) := \mathrm{Gal}(N(2)/N) = \mathrm{Gal}(F(2)/N)$ and N_v is the residue field of v. Moreover it is well known that I_v is an abelian group. (See e.g. [EnKo].)

Because $\dot{N}^2$ is an $S(I)$-ordering of N we see that $s(N) = 2$. In particular N is not a formally real field, and so $G_N(2)$ is a torsion-free group. (See [Be].) Therefore using Pontrjagin's duality and the well-known structure of abelian divisible groups, we see that $I_v \cong (\mathbb{Z}_2)^J$ for some set J. (See e.g. [RZ, §4.3, Theorem 4.3.3].)

Because $\dot{N}^2$ is compatible with v and

$$\frac{U_v}{U_v \cap \dot{N}^2} \cong \frac{\dot{N}^2 \cup -\dot{N}^2}{\dot{N}^2},$$

we see that $\mid \dot{N}_v/\dot{N}_v^2 \mid = 2$. Hence $G_{N_v}(2) \cong \mathbb{Z}_2$. Since $\dot{N}^2$ is an $S(I)$-ordering of N, it follows that the cardinality of I is the same as the cardinality of J. Hence $I_v \cong (\mathbb{Z}_2)^I$. Since the Galois group $G_N(2) = I_v \rtimes \mathbb{Z}_2$ is a closed subgroup of G_F, the proof is completed. $\square$

In the case of $C(I)$-orderings, we cannot always find a closure. The problem arises from the fact that the valuation whose existence is guaranteed by Proposition 8.2 may be dyadic, and thus the appropriate modification of Theorem 8.11 will not go through. For $S(I)$- and $D(I)$-orderings we do not have this problem, as the valuation in question will be nondyadic. Example 8.14 below constructs a $C(1)$-ordered field which we show in Proposition 8.15 does not admit a $C(1)$-closure.

Example 8.14. Recall that a field K of characteristic 2 is called *perfect* if $K^2 = K$. S. MacLane has shown that for any field K of characteristic 2, there exists a field F of characteristic 0 with a valuation $v : F \to \mathbb{Z} \cup \{\infty\}$ such that $F_v \cong K$ ([Mac, Theorem 2]. For some more general theorems on valued fields with prescribed residue fields, see [Ri, Chapter I]). Then let F be such a field where $F_v = K$ is a field of characteristic 2 which is not perfect. Let T_0 be a multiplicative subgroup of $\dot{K}$ of index 2 in $\dot{K}$ such that $\dot{K}^2 \subsetneq T_0 \subsetneq \dot{K}$. Let $T = \dot{F}^2\pi_v^{-1}(T_0)$, a subgroup of $\dot{F}$. Here π_v is the residue map $U_v \longrightarrow \dot{K}$. Then $\mid \dot{F}/T \mid = 4$, and one can choose as representatives of the factor group $\dot{F}/T$ the elements $1, u, \rho, \rho u$ where $v(\rho) = 1, u \in U_v$, and $\pi_v(u) \notin T_0$.

We claim that F is T-rigid. Since any element in ρT or in ρuT lies outside of U_vT, we see that all elements of $\rho T \cup \rho uT$ are T-rigid. (See [AEJ, Proposition 1.5.]) Consider an element $\alpha = t_1 + t_2 u \in T + uT$, with $t_1, t_2 \in \dot{F}$. Then $\alpha = t_2(t_1 t_2^{-1} + u)$, so it is enough to show $t_1 t_2^{-1} + u \in T \cup uT$. Thus we may restrict our attention to elements which can be written as $tf^2 + u$, where $t \in \pi_v^{-1}(T_0)$, $f \in \dot{F}$. If $v(f) = 0$, then $tf^2 + u \in U_v \subseteq T \cup uT$. If $v(f) > 0$, then $tf^2 + u = u(1 + tf^2 u^{-1}) \in uT$. Finally, if $v(f) < 0$, then $tf^2 + u = tf^2(1 + uf^{-2}t^{-1}) \in T$. Thus F is T-rigid.

Since $-1 \in T_0$, we have $-1 \in T$, and T is a $C(1)$-ordering of F. Observe that $T \neq \dot{F}^2$ and (F, T) is not $C(1)$-closed.

Proposition 8.15. *The $C(1)$-ordered field (F, T) does not admit a $C(1)$-closure.*

Proof. Recall that a valuation ν on a field L is said to be T-*coarse* if $\nu(T)$ contains no nontrivial convex subgroups of the valuation group Γ_ν of ν. Suppose that $F \subsetneq N \subsetneq F(2)$, $\dot{N}^2 \cap F = T$, and $\dot{N}^2$ is a $C(1)$-ordering of N. Then applying [AEJ, Corollary 2.1.7] or [Wa, Theorem 2.16], we see that there exists a $\dot{N}^2$-compatible valuation w on N such that $[U_w \dot{N}^2 : \dot{N}^2] \leq 2$. This means that $\mid U_w / U_w \cap \dot{N}^2 \mid \leq 2$. We may further choose w to be the unique finest N^2-coarse N^2-compatible valuation on N (see [AEJ, Theorem 3.8]). Consider $z :=$ the restriction of the valuation w to F. First observe that z is a T-compatible valuation on F. Indeed, from $M_w \cap F = M_z$ we get $(1 + M_w) \cap F = 1 + M_z$. Thus we have

$$1 + M_z = (1 + M_w) \cap F \subseteq \dot{N}^2 \cap F = T.$$

Let Δ be the maximal convex subgroup of Γ_z contained in $z(T)$. Then set y to be the composite valuation

$$y : \dot{F} \xrightarrow{z} \Gamma_z \xrightarrow{\rho} \Gamma_z/\Delta,$$

where the last map $\rho : \Gamma_z \to \Gamma_z/\Delta$ is the natural projection. Then, following the notation of [AEJ, Definition 2.2], the valuation ring $A_y = O_F(U_z T, T)$, and $y(T)$ contains no nontrivial convex subgroups of the value group $\Gamma_y = \Gamma_z/\Delta$ ([AEJ, Lemma 3.1 and Proposition 3.2]), so y is T-coarse. Observe that y is also T-compatible. However, since $\Gamma_v = \mathbb{Z}$ and $v(T) = 2\mathbb{Z} \neq \mathbb{Z}$, the valuation v is also T-coarse. Hence, by [AEJ, Corollary 3.7], we see that the valuations v and y are comparable. Since A_v is a maximal proper subring of F (because $\Gamma_v = \mathbb{Z}$), we see that $A_v \supseteq A_y \supseteq A_z$. However, since $M_z \supseteq M_y \supseteq M_v$ and $2 \in M_v$, we see that both valuations y and z are dyadic. Since $F_z \subseteq F_w$, it follows that w is also dyadic. But from [AEJ, Theorem 3.8 and Lemma 4.4], it follows that w cannot be a dyadic valuation. Indeed, $[D_N\langle 1, -n^2\rangle \dot{N}^2 : \dot{N}^2] = 4 > 2$ for all $n \in \dot{N}$. Thus we have a contradiction, and there can be no $C(1)$-closure of (F, T). $\square$

Remark 8.16. Example 8.14 is analogous to Proposition 4.10. What makes this example striking when compared to Proposition 4.10 is that here we have $\mid \dot{F}/T \mid = 4 < \infty$, but in Proposition 4.10 $\mid \dot{F}/T \mid = \infty$. Although this example is a relatively simple consequence of the work in [AEJ], it seems to be the first example where the Witt ring of a field with finitely many square classes is realizable as a "Witt ring of T-forms over some field F", but it is not realizable as an actual Witt ring of any field extension K of F. We make this last comment more precise.

First observe that, analogous to the definition of reduced Witt rings of fields, one may define $W_T(F)$ for any subgroup T of $\dot{F}$ which contains all nonzero squares in F. One possible definition is as follows: (See also [La2, Corollary 1.27] and [Sc, Chapter 2, § 9].)

Let $\mathbb{Z}[\dot{F}/T]$ be the group ring of $\dot{F}/T$ with coefficients in $\mathbb{Z}$. Let J be the ideal of $\mathbb{Z}[\dot{F}/T]$ generated by

(1) $[T]+[-T]$,
(2) $[aT]+[bT]-[(a+b)T]-[ab(a+b)T], (a,b,a+b\in\dot{F})$,
(3) $[aT][bT]-[abT], (a,b\in\dot{F})$.

Then we set $W_T(F)=\mathbb{Z}[\dot{F}/T]\big/J$.

A systematic study of $W_T(F)$ for H-orderings T of F is very desirable, but it is not pursued in this particular paper. Here we just point out that if T is any $C(1)$-ordering of F then $W_T(F)\cong W(\mathbb{Q}_p)$, where p is any prime such that $p\equiv 1 \pmod 4$, and $\mathbb{Q}_p$ is the field of p-adic numbers.

Since T is a $C(1)$-ordering in $\dot{F}$ and $\dot{\mathbb{Q}}_p^2$ is a $C(1)$-ordering in $\mathbb{Q}_p$ (see Proposition 7.2 and [L1, Chapter 6]), we see that there exists a group homomorphism $\varphi\colon \dot{F}/T\longrightarrow \dot{\mathbb{Q}}_p/\dot{\mathbb{Q}}_p^2$ such that φ takes any relation in the form (1), (2) or (3) above again to a relation of the same type. Using the same argument for φ^{-1} rather than φ, we see that φ indeed induces an isomorphism $\tilde{\varphi}\colon W_T(F)\cong W(\mathbb{Q}_p)$.

Similar to Proposition 4.12, we have the following proposition.

Proposition 8.17. *Let (F,T) be the field F with $C(1)$-ordering T constructed in Example 8.14 above. Then there is no field extension K/F with $C(1)$-ordering $\dot{K}^2$ which is a T-extension of (F,T). (Equivalently, $W_T(F)$ cannot be realized as $W(K)$ for any field extension K of F.)*

Proof. Suppose to the contrary that there exists a field extension K/F such that $\dot{K}^2$ is a $C(1)$-ordering of K and $(\dot{K},\dot{K}^2)$ is a T-extension of (F,T). Assume that both K and a quadratic closure $F(2)$ of F are contained in some common overfield so that we can consider the field $L=K\cap F(2)$. The natural isomorphism $\psi\colon \dot{F}/T\longrightarrow \dot{K}/\dot{K}^2$ factors through $\theta\colon \dot{F}/T\longrightarrow \dot{L}/(\dot{K}^2\cap L)$. Because ψ is injective, so is θ. Observe that θ is also surjective. Indeed since ψ is surjective, we see that for each $l\in\dot{L}$ there exists an element $f\in\dot{F}$ such that $lf^{-1}\in\dot{K}^2\cap L$. Thus we see that $(L,\dot{K}^2\cap L)$ is a T-extension of (F,T).

We claim that $(\dot{L},\dot{K}^2\cap L)$ is a $C(1)$-closure of $(F,\dot{T})$. Observe that $\dot{K}^2\cap L=\dot{L}^2$. Indeed if $k^2\in L, k\in\dot{K}$ then $k\in\dot{K}\cap F(2)=\dot{L}$. Since $\dot{L}^2\subset\dot{K}^2\cap L$ is obvious, we see that $\dot{K}^2\cap L=\dot{L}^2$. In order to conclude the proof, it is enough to show that $\dot{L}^2$ is a $C(1)$-ordering in $\dot{L}$. Because $\sqrt{-1}\in\dot{K}$ we see that $\sqrt{-1}\in\dot{L}$ as well, and $-1\in\dot{L}^2$. From the isomorphism $\theta\colon\dot{F}/T\longrightarrow\dot{L}/\dot{L}^2$ we see that $\dot{L}/\dot{L}^2=C_2\oplus C_2$. By Proposition 7.2 it remains only to show that L is $\dot{L}^2$-rigid. Consider an element $a\in\dot{L}\diagdown\dot{L}^2$. For any $l\in\dot{L}$ we have $l^2+a\in\dot{K}^2\cup a\dot{K}^2$ because $\dot{K}$ is $\dot{K}^2$-rigid and $\dot{L}^2=\dot{K}^2\cap L$. Hence $l^2+a\in(\dot{K}^2\cap L)\cup(a\dot{K}^2\cap L)$. Finally since $\dot{K}^2\cap L=\dot{L}^2$ and $a\dot{K}^2\cap L=a\dot{L}^2$ we see that $\dot{L}$ is $\dot{L}^2$-rigid. $\square$

Theorem 8.18. *A $C(I)$-ordered field (F,T) possessing a nondyadic T-compatible valuation ring A_v as in Proposition 8.2 admits a $C(I)$-closure.*

Proof. The proof is essentially the same as the proof of Theorem 8.11 and Corollary 8.12, and we will follow the same plan and the same notation. Applying Proposition 8.2, we find a valuation v on F such that $\bar{T} := \pi_v(U_v \cap T)$ is either $\dot{F_v}$ or a C-ordering. By assumption here this valuation is nondyadic. By Lemma 8.9, T_1 is a $C(J)$-ordering contained in T. Taking any valuation w on $L = F(\sqrt{t})$ extending v, we extend $\bar{T}$ to $\tilde{T}$ in L_w. We obtain, by Lemma 8.9, a $C(K)$-ordering T_2 in L. We enlarge it to a $C(K')$-ordering T_2', according to the three cases (1), (2), (3), replacing $T_2 \cup -T_2$ by T_2. The only serious change is in proving that $\dot{L} = T_2'\dot{F}$. For this it is enough to show that $U_w \subseteq T_2\dot{F}$, which can be done as follows. If the index $[U_vT : T] = [\dot{F_v} : \bar{T}]$ is 1, then $[\dot{L_w} : \tilde{T}] = [U_wT_2 : T_2] = 1$ and $U_w \subseteq T_2$. If this index is 2, there exists $a \in U_v$ such that $U_w \subseteq T_2 \cup aT_2 \subseteq T_2\dot{F}$. This shows that (L, T_2') is a $C(J)$-extension of (F, T_1), and we apply Lemma 8.5 to show that (L, T_1T_2') is a $C(I)$-extension of (F,T). We finish by applying the same argument as in Corollary 8.12. □

The following observation about valuations when F contains a real-closed field was pointed out to us by J.-L. Colliot-Thélène.

Corollary 8.19. *Let v be a T-compatible valuation with value group Γ, and denote by U_v the units of the valuation ring. Suppose there exists an integer $n > 1$ such that any n-divisible subgroup of Γ is trivial. Assume that F contains a real-closed field R. Then R is contained in U_v, and in particular the valuation is nondyadic.*

Proof. Assume F contains a real-closed field R. If $a \in R$ is positive, for the given integer n there exists $b \in R$ such that $a = b^n$, and thus $v(a) = nv(b)$. Thus $v(a)$, being divisible by any power of n, must be 0, and the elements of R must be units. This implies that the residue field F_v contains R, and the valuation v cannot be dyadic. In particular, the T-compatible valuation which is known to exist, cannot be dyadic, and (F,T) admits a closure by Theorem 8.18. □

Theorem 8.20. *A $D(I)$-ordered field (F,T) admits a $D(I)$-closure.*

Proof. We have already proved that D-orderings admit closures, and thus we may assume that $|I| > 1$. It has also already been shown in [Sch] that valuation fans admit closures. Here is a more general situation and a different proof, that consists again in transpositions of the proofs of Theorem 8.11 and Corollary 8.12. As in Theorem 8.11, if $t \in T$ and $L = F(\sqrt{t})$, applying Proposition 8.3, we find a valuation v on F such that $\bar{T} := \pi_v(U_v \cap T)$ is either an ordering or a D-ordering. By Lemma 8.10, T_1 is a $D(J)$-ordering contained in T. Taking any valuation w on $L = F(\sqrt{t})$ extending v, we extend $\bar{T}$ to $\tilde{T}$ in L_w. By Lemma 8.10 we obtain a $D(K)$-ordering T_2 in L. We enlarge it to a $D(K')$-ordering T_2', according to the three cases (1), (2), (3), replacing $T_2 \cup -T_2$ by T_2. As in the case for $C(I)$-ordered fields, the only serious change is in proving that $\dot{L} = T_2'\dot{F}$, and the proof is identical to that for $C(I)$-ordered fields. □

§9. Galois groups and additive structures (2)

Throughout this paper, we have considered a number of subgroups H of $\mathcal{G}_F$ which behave pretty well, in that we have a certain control over the additive structure of the associated orderings, and we are able to make closures. Actually some of these groups H have an additional property which helped us in a subtle but important way. Let us introduce the following definition and notation.

Definition and Notation 9.1.

(1) We say that an essential subgroup H of $\mathcal{G}_F$ is *liftable* if we can write $\mathcal{G}_F = G \rtimes H$ for some normal subgroup G of $\mathcal{G}_F$. This means that H is not only a subgroup of $\mathcal{G}_F$, but also a quotient $\mathcal{G}_F \longrightarrow H$ such that $H \longrightarrow \mathcal{G}_F \longrightarrow H$ is the identity map. The H-ordering P_H is called a *liftable* ordering. (The name *liftable* was chosen because such an H corresponds, as a quotient of $\mathcal{G}_F$, to a Galois extension of F inside $F^{(3)}$, of group H, which can be lifted as a Galois subextension of $F^{(3)}$ of same group H.)

(2) If we want to realize some subgroup H of $\mathcal{G}_F$ as a $\mathcal{G}_K$ for some field K, we certainly need to use an H which satisfies known properties of W-groups. In particular, if $H \neq \{1\}, C_2$, then by Corollary 2.18 of [MiSp2], we see that H can be embedded in a suitable product $\prod_I D \times \prod_J C_4$, where each factor is a quotient of H. According to the use in universal algebra, see e.g. [Gr, p. 123], we refer to this as the *subdirect product* condition.

(3) We say that an essential subgroup H of $\mathcal{G}_F$ is a *fair* subgroup if it is liftable and if it is either $\{1\}$ or C_2 or a subdirect product of some $\prod_I D \times \prod_J C_4$. The H-ordering P_H will be called a *fair* ordering if H is a fair subgroup of $\mathcal{G}_F$.

Remark 9.2. We observed in Example 6.4 that the subgroup $H = \langle \sigma, \tau \rangle \cong C_4 * C_4$ in $\mathcal{G}_{\mathbb{Q}_2}$ has associated H-ordering $T = \dot{F}^2 \cup 5\dot{F}^2, F = \mathbb{Q}_2$, such that $T + T$ is not multiplicatively closed. We now use the description of $\mathcal{G}_F = \mathbb{G}_2$ as in Example 2.9, to show that H is <u>*not*</u> a liftable subgroup of $\mathcal{G}_F$. Suppose instead that H is a liftable subgroup of $\mathcal{G}_F$. Then there exists a subgroup G of $\mathcal{G}_F$ such that $\mathcal{G}_F = G \rtimes H$. Then G must contain some element of the form $\alpha = \rho \times h \times \phi$ where ρ is an element of $\mathcal{G}_F$ such that ρ, σ, τ generate $\mathcal{G}_F$ and $\sigma^2[\rho, \tau] = 1, h \in H$ and ϕ is some element in $\Phi(\mathcal{G}_F)$. Because G is a normal subgroup of $\mathcal{G}_F$ we see that $\alpha \in G$ implies $\alpha^{-1}(\tau^{-1}\alpha\tau) = [\alpha, \tau] \in G$ as well. Hence $[\alpha, \tau] = [\rho h \phi, \tau] = [\rho, \tau][h, \tau] \in G$. On the other hand $[\rho, \tau][h, \tau] = \sigma^2[h, \tau] \in H$. Because $\mathcal{G}_F = G \rtimes H$ we see $G \cap H = \{1\}$ and thus $\sigma^2[h, \tau] = 1$. This equality is impossible as H is a free group in category $\mathcal{C}$. Therefore H is not liftable.

Observe that it is sometimes fairly easy to establish the "fairness" of a given subgroup. For example if $H = \langle \sigma \rangle$ is an essential subgroup of $\mathcal{G}_F$ of order 2, then for $f \notin P_H$ the restriction $H \longrightarrow \mathrm{Gal}(F(\sqrt{f})/F)$ induces an isomorphism. Since the subdirect product condition is empty, H is fair. We can also readily check the following:

Proposition 9.3. *Let $\varphi\colon D(I) \longrightarrow \mathcal{G}_F$ be an essential embedding. Then $\varphi(D(I))$ is a liftable subgroup of $\mathcal{G}_F$. As the subdirect product condition is also trivially satisfied, it is a fair subgroup of $\mathcal{G}_F$.*

Proof. Consider a $D(I)$-ordering T of F for some $\mid I \mid \geq 1$. Pick a basis for $\dot{F}/T$ of the form $\{[-1]\} \cup \{[a_i], i \in I\}$. (As usual $[f]$ means the class represented by f in the factor group $\dot{F}/T$.) Set $K/F = F(\sqrt{-1}, \sqrt[4]{a_i}\colon i \in I)$. Then $\mathrm{Gal}(K/F) \cong (\prod_I C_4) \rtimes C_2$, where we can choose generators $\bar{\tau}_i$, $i \in I$ for factors in the inner product and $\bar{\sigma}$ for the outer factor such that $\bar{\sigma}(\sqrt{-1}) = -\sqrt{-1}$, $\bar{\sigma}(\sqrt[4]{a_i}) = \sqrt[4]{a_i}$, $\bar{\tau}_i(\sqrt{-1}) = \sqrt{-1}$ and $\bar{\tau}_i(\sqrt[4]{a_i}) = \sqrt{-1}\,\sqrt[4]{a_i}$, $\bar{\tau}_i(\sqrt[4]{a_j}) = \sqrt[4]{a_j}$ for $j \neq i$. Moreover the action of $\bar{\sigma}$ on $\prod_I C_4$ is described as $\bar{\sigma}^{-1}\ \bar{\tau}_i\ \bar{\sigma} = \bar{\tau}_i^3$ for each $i \in I$. (Or equivalently $\bar{\sigma}^{-1}\ \bar{\tau}\ \bar{\sigma} = \bar{\tau}^{-1}$ for each $\bar{\tau} \in \prod_I C_4$.)

Pick any elements σ, τ_i, $i \in I \in H := \varphi(D(I))$ such that their homomorphic image from H to $\mathrm{Gal}(K/F)$ are elements $\bar{\sigma}$, $\bar{\tau}_i$, $i \in I$. This is possible as H surjects on $\mathrm{Gal}(K/F)$. Then the essential subgroup H of $\mathcal{G}_F$ is generated by the minimal set of generators $\{\sigma, \tau_i, i \in I\}$. Moreover the natural restriction map $r\colon H \longrightarrow \mathrm{Gal}(K/F)$ is an isomorphism, as r takes the generators of H to the generators of $\mathrm{Gal}(K/F)$ and both sets of generators satisfy the same relations. $\square$

Now we consider C_4-orderings and determine when they are fair orderings. Observe that a C_4-ordering is automatically fair provided it is liftable, so it is enough to decide when a C_4-ordering T is liftable.

Proposition 9.4. *Let T be a C_4-ordering of F. Then T is liftable if and only if there exists an element $f \in (F^2 + F^2) \setminus (T \cup \{0\})$.*

Proof. Suppose that T is a C_4-ordering of $F, T = P_H$ for $H \cong C_4$, and H is essentially embedded in $\mathcal{G}_F$. Suppose also that $f \in (F^2 + F^2) \setminus (T \cup \{0\})$. Then since $f \notin T$ and $T \supset \dot{F}^2$, we see that $f \notin F^2$ and a C_4^f-extension K of F exists. Because $f \in \dot{F} \setminus T$, an element $h \in H$ exists such that $h(\sqrt{f}) = -\sqrt{f}$. Then the image of h in $\mathrm{Gal}(K/F)$ under the natural homomorphism $H \longrightarrow \mathrm{Gal}(K/F)$ is a generator of $\mathrm{Gal}(K/F)$. Therefore the homomorphism is in fact an isomorphism, and H is liftable as asserted. Assume now that $H \cong C_4$ is a liftable subgroup of $\mathcal{G}_F$. Then a surjective homomorphism $\varphi\colon \mathcal{G}_F \longrightarrow C_4$ exists, which induces an isomorphism $\psi\colon H \longrightarrow C_4$. Let K be the fixed field of the kernel of φ. Then K/F is a Galois extension on $\mathrm{Gal}(K/F) \cong C_4$. Let $F(\sqrt{f})$ be a unique quadratic extension of F contained in K. Also let $T = P_H$. Then H acts nontrivially on f and $f \in (F^2 + F^2) \setminus \{0\}$. Hence $f \in (F^2 + F^2) \setminus (T \cup \{0\})$ as claimed. $\square$

Example 9.5. The following simple example shows that we cannot drop the condition $\exists\, f \in (F^2 + F^2) \setminus (T \cup \{0\})$ from the proposition above, and that unfair C_4-orderings exist in nature. Consider again $F = \mathbb{Q}_2$ and set $T = (F^2 + F^2) \setminus \{0\}$. Then T is a subgroup of $\dot{F}$ of index 2. Because $\mathbb{Q}_2$ is not a formally real field, $\mathbb{Q}_2$ does not admit any usual ordering, and T is a C_4-ordering of F. However T contains all sums of two squares, and therefore T is not liftable.

On the bright side, we wish to point out that for each C_4-ordering there exists a quadratic extension of the base field, and an extension of the original C_4-ordering on this quadratic extension where this extended ordering become a fair ordering. In other words an unfair ordering may become fair in some algebraic extension. More precisely we have the following proposition, in which we use Definition 1.4(4) of an H-extension

Proposition 9.6. *Let T be a C_4-ordering in F. If T is not fair, there exists $t \in T$ and a C_4-extension $(F(\sqrt{t}), V)$ of (F, T) such that V is a fair ordering in $F(\sqrt{t})$.*

Proof. Suppose that T is a C_4-ordering in F. Then by Proposition 5.4 there must exist an element $t \in T$ such that $1 + t \notin T$. If T is not a fair ordering, we know from the characterization of fair orderings in Proposition 9.4 that $t \notin \dot{F}^2$. Hence $K = F(\sqrt{t})$ is a quadratic extension of F and $[K\colon F] = 2$. From the proof of Proposition 4.2, we know that there exists some subgroup V in K such that $\mid \dot{K}/V \mid = 2$ and $V \cap \dot{F} = T$. Then V is a C_4-ordering of K, and V is fair as $1 + (\sqrt{t})^2 \notin V$. □

In this section we merely give a few examples of fair orderings and are not pursuing a systematic check of which orderings considered in this paper are fair and which will become fair after extension to a suitable 2-extension of the base field. The development of a theory of fair orderings of fields is planned for a subsequent paper.

We complete our family of examples of orderings by considering $H = \mathcal{F}(I)$, where I is some nonempty index set and $\mathcal{F}(I)$ is the free pro-2-group in the category $\mathcal{C}$, on a minimal set $\{\sigma_i \mid i \in I\}$ of generators I. (We assume as usual that each open subgroup V of $\mathcal{F}(I)$ contains all but finitely many $\sigma_i, i \in I$. See [Koc, Chapter 4].)

Proposition 9.7. *Let K/F be a Galois extension such that* $\mathrm{Gal}(K/F) \cong \mathcal{F}(I) = \langle \sigma_i \mid i \in I \rangle$ *where $\{\sigma_i, i \in I\}$ is a family of minimal generators of the free pro-2-group $\mathcal{F}(I)$. Then there exists a fair $\mathcal{F}(I)$-ordering in F.*

Proof. We first embed the group $\mathcal{F}(I)$ essentially in $\mathcal{G}_F$. Since $F^{(3)}$ is the maximal Galois subextension of a quadratic closure F_q of F such that $\mathrm{Gal}(F^{(3)}/F)$ belongs to the category $\mathcal{C}$, and since $\mathcal{F}(I)$ also belongs to $\mathcal{C}$, we see that $K \subset F^{(3)}$. Therefore there exists a surjective natural homomorphism $\pi\colon \mathcal{G}_F \longrightarrow \mathrm{Gal}(K/F)$.

It is well known that there exists a continuous map $s\colon \mathrm{Gal}(K/F) \longrightarrow \mathcal{G}_F$ such that $\pi \circ s$ is the identity map on $\mathrm{Gal}(K/F)$ (See [Koc, 1.3]). (Here we use only the fact that both groups $\mathrm{Gal}(K/F)$ and $\mathcal{G}_F$ are profinite groups.) Set $s(\sigma_i) = \omega_i$ for each $i \in I$. Then for each open subgroup V of $\mathcal{G}_F$ the set $s^{-1}(V)$ is an open subset of $\mathrm{Gal}(K/F)$, and because open subgroups of $\mathrm{Gal}(K/F)$ form a basis for the topology of $\mathrm{Gal}(K/F)$ we see that all but finitely many $\sigma_i, i \in I$, are in $\sigma^{-1}(V)$. Hence all but finitely many ω_i are in V.

Because $\mathcal{F}(I)$ is a free object of $\mathcal{C}$ on the set of generators $(\sigma_i), i \in I$ we see that there exists a continuous homomorphism $p\colon \mathrm{Gal}(K/F) \longrightarrow \mathcal{G}_F$ such that $p(\sigma_i) = \omega_i$ for each $i \in I$. Set $H = p(\mathrm{Gal}(K/F))$. Then we have $\pi \circ p = 1$ and $\mathcal{G}_F \cong \ker \pi \rtimes H$. Moreover, π restricted to H induces an isomorphism $\varphi\colon H \longrightarrow \mathrm{Gal}(K/F)$. Observe that $\varphi(\omega_i) = \sigma_i$ for each $i \in I$. Because $\sigma_i \mod \phi(\mathrm{Gal}(K/F))$ are topologically independent, we see that ω_i must be topologically independent $\mod \phi(\mathcal{G}_F)$. This means that $\{\omega_i, i \in I\}$ generates the essential subgroup H of $\mathcal{G}_F$.

One can check that $\mathcal{F}(I)$ is a subdirect product of its dihedral and C_4 quotients directly from the structure of $\mathcal{F}(I)$, but it is also possible simply to observe that $\mathcal{F}(I)$ is the W-group of a suitable field A and all W-groups have this property. That each $\mathcal{F}(I)$ is the W-group of a suitable field A follows from the fact that for each index set $I \neq \phi$ we can find a field A such that the Galois group of its quadratic closure is a free pro-2-group (see e.g., [GM, page 98]), and therefore its W-group is $\mathcal{F}(I)$. □

The following corollary applies, for example, in the case of $F = \mathbb{Q}_p(t)$.

Corollary 9.8. *Let F be the quotient field of a complete local integral domain properly contained in F. Let $\mathcal{F}(I)$ be any free object of category $\mathcal{C}$ on generators I, where I is a nonempty finite set. Then F admits a fair $\mathcal{F}(I)$-ordering.*

Proof. From Proposition 9.7 we see that it is sufficient to show that each group $\mathcal{F}(I), I$ finite and nonempty, occurs as a Galois group over F. Harbater's well-known result [Har, p. 186] says that each finite group is realizable over F. (For a very nice and rather elementary proof of this result see [HaVöl, Theorem 4.4].) □

Let us fix the following notation.

Notation 9.9. Let $i\colon F_1 \longrightarrow F_2$ be a quadratic extension and let $i^\star\colon \mathcal{G}_{F_2} \longrightarrow \mathcal{G}_{F_1}$ be the associated restriction map. (See e.g. [MiSm3] for the existence of this map.) Let H_2 be a subgroup of $\mathcal{G}_{F_2}$ and let $H_1 = i^\star(H_2)$. Assume H_1 is essential in $\mathcal{G}_{F_1}$. Observe that this property is not automatically satisfied since the image of an essential group under the restriction map $i^\star$ need not be essential. (See Remark 7.8 for an example exhibiting such a case.) When this is the case, we say that the extension $(F_1, H_1) \longrightarrow (F_2, H_2)$ is essential. Put $T_1 = P_{H_1}, T_2 = P_{H_2}$. Then it follows that $T_1 = T_2 \cap F_1$.

If we are working with fair groups H as above, then we can show that for an essential quadratic extension $(F_1, H_1) \longrightarrow (F_2, H_2)$, the additive structure of the associated orderings is preserved if and only if $i^\star$ induces an isomorphism between H_2 and H_1.

Theorem 9.10. *Assume the hypotheses in Notation 9.9 hold and that H_1, H_2 are fair subgroups of $\mathcal{G}_{F_1}, \mathcal{G}_{F_2}$ respectively. Then the restriction $i^\star$ induces an isomorphism between H_2 and H_1 if and only if $\dot F_1/T_1 \cong \dot F_2/T_2$ and for each $a \in F_1, T_1 + aT_1 = (T_2 + aT_2) \cap F_1$.*

Since the proof is a bit long and since the two directions are not using the same assumptions on H_1, H_2, we split the theorem in two parts, Proposition 9.11 and Proposition 9.12

Proposition 9.11. *Assume that H_1 is liftable. Following Notation 9.9, if the restriction $i^\star$ induces an isomorphism between H_2 and H_1, then $\dot F_1/T_1 \cong \dot F_2/T_2$ and for each $a \in F_1, \quad T_1 + aT_1 = (T_2 + aT_2) \cap F_1$.*

Proof. We know that $\dot F_i/T_i$ is the Pontrjagin dual of $H_i/\Phi(H_i)$ for $i = 1, 2$. Thus the natural isomorphism $H_2 \longrightarrow H_1$ yields an isomorphism $\dot F_1/T_1 \cong \dot F_2/T_2$. In order to show that for each $a \in F_1$ we have $T_1 + aT_1 = (T_2 + aT_2) \cap F_1$, it is enough to show that for every $b, c \in \dot F_1 \setminus T_1$, if there exists $s_2, t_2 \in T_2$ such that $bs_2 + ct_2 = 1$, then there exists $s_1, t_1 \in T_1$ such that $bs_1 + ct_1 = 1$. Indeed, assume that the latter condition involving $b, c \in \dot F_1 \setminus T_1$ is valid. Consider any $a \in \dot F_1$ and any relation $u_2 + av_2 = d$, where $u_2, v_2 \in T_2 \cup \{0\}$ and $d \in \dot F_1$. We want to show that there exist elements $u_1, v_1 \in T_1 \cup \{0\}$ such that $u_1 + av_1 = d$. If $u_2 = 0$ then $v_2 \in \dot F_1 \cap T_2 = T_1$, and we are done. If $v_2 = 0$ then $u_2 = d \in \dot F_1 \cap T_2 = T_1$, and again we are done. Then assume $u_2, v_2 \in T_2$. If $-a \in T_1$, let us write $d = s^2 - t^2$ for some elements $s, t \in \dot F_1$. We then have $d = s^2 + a(-at^2/a^2) \in T_1 + aT_1$. Hence we may assume that $-a \notin T_1$. Finally we also assume that $d \notin T_1$. From the equation $u_2 + av_2 = d$ we obtain $u_2 = d - av_2$, and since $u_2, v_2 \in T_2$ we can rewrite this equation as $1 = ds_2 - at_2$ where $d, -a \in \dot F_1 \setminus T_1$. Using our hypothesis we see that there exist elements $s_1, t_1 \in T_1$ such that $1 = ds_1 - at_1$. Hence $d \in T_1 + aT_1$ as required.

Now take $b, c \in \dot F_1 \setminus T_1$ and assume that $bs_2 + ct_2 = 1$ for some $s_2, t_2 \in T_2$. Then the quaternion algebra $\left(\frac{bs_2, ct_2}{F_2}\right)$ splits. We consider the following cases.

(1) Suppose bs_2, ct_2 are linearly independent in $\dot{F}_2/T_2$. Then they are also independent modulo $\dot{F}_2^2$, and by Proposition 1.5 we have a dihedral extension L_2/F_2 such that $F_2(\sqrt{bs_2}, \sqrt{ct_2}) \subset L_2$ and $\mathrm{Gal}(L_2/F_2(\sqrt{bcs_2t_2})) \cong C_4$. In particular we have an exact sequence

$$1 \longrightarrow C_2 \longrightarrow \mathrm{Gal}(L_2/F_2) \cong D \longrightarrow \mathrm{Gal}(F_2(\sqrt{bs_2}, \sqrt{ct_2})/F_2) \cong C_2 \times C_2 \longrightarrow 1.$$

Let θ denote the restriction map from H_2 to $\mathrm{Gal}(F_2(\sqrt{bs_2}, \sqrt{ct_2})/F_2)$. We show it is surjective. Denote by u_1, u_2 the two generators of $\mathrm{Gal}(F_2(\sqrt{bs_2}, \sqrt{ct_2})/F_2)$ defined by $u_1(\sqrt{bs_2})/\sqrt{bs_2} = -1, u_1(\sqrt{ct_2})/\sqrt{ct_2} = 1, u_2(\sqrt{bs_2})/\sqrt{bs_2} = 1, u_2(\sqrt{ct_2})/\sqrt{ct_2} = -1$. We may look at u_1, u_2 as linear functions on the $\mathbb{F}_2$-vector subspace of $\dot{F}_2/\dot{F}_2^2$ spanned by bs_2, ct_2, which are assumed to be independent, and since $bT_2 \cap cT_2 = \emptyset$, we may extend them to linear functions v_1, v_2 defined on the subspace generated by bT_2, cT_2, by putting $v_i(x) = u_i(b)$ if $x \in bT_2$ and $v_i(x) = u_i(c)$ if $x \in cT_2$. Then v_i may be viewed as a function on the $\mathbb{F}_2$-vector subspace generated by the cosets bT_2, cT_2 in $\dot{F}_2/T_2$. Again, these functions v_i's may be extended to w_i defined on the whole vector space $\dot{F}_2/T_2$. By duality, one has $(\dot{F}_2/T_2)^\star \cong H_2/\Phi(H_2)$, and the w_i's yield to elements in $H_2/\Phi(H_2)$ which may be lifted as elements $h_1, h_2 \in H_2$. Since the duality is precisely given by the pairing $H_2/\Phi(H_2) \times \dot{F}_2/T_2 \longrightarrow \{\pm 1\}$ defined by $(h, f) \mapsto h(\sqrt{f})/\sqrt{f}$, it is immediate that h_i goes to u_i under the restriction map $\theta\colon H_2 \longrightarrow \mathrm{Gal}(F_2(\sqrt{bs_2}, \sqrt{ct_2})/F_2)$. This shows the surjectivity of θ. Since θ factors through $\psi\colon H_2 \longrightarrow \mathrm{Gal}(L_2/F_2) \cong D$ and since the kernel of $\mathrm{Gal}(L_2/F_2) \longrightarrow \mathrm{Gal}(F_2(\sqrt{bs_2}, \sqrt{ct_2})/F_2)$ is the Frattini subgroup of $\mathrm{Gal}(L_2/F_2)$, we see that ψ is also surjective. This means that D may be viewed as a quotient of H_2 and that we have inclusion maps ${F_2^{(3)}}^{H_2} \longrightarrow L_2' \longrightarrow F_2^{(3)}$ such that $\mathrm{Gal}(L_2'/{F_2^{(3)}}^{H_2}) \cong D$. Since $i^\star(H_2) = H_1$, applying $i^\star$ to this diagram gives us another diagram ${F_1^{(3)}}^{H_1} \longrightarrow L_1' \longrightarrow F_1^{(3)}$ with $\mathrm{Gal}(L_1'/{F_1^{(3)}}^{H_1}) \cong D$.

Since H_1 is liftable, we know that there exists an H_1-extension K/F_1 inside $F_1^{(3)}$ containing a D-extension L_1/F_1. This extension is a $D^{u,v}$-extension for suitable $u, v \in F_1$ by Proposition 1.5. We claim that we have $u = bs_1, v = ct_1$ for suitable $s_1, t_1 \in T_1$. Consider the surjective homomorphism

$$\theta\colon H_2 \longrightarrow \mathrm{Gal}(F_2(\sqrt{bs_2}, \sqrt{ct_2})/F_2)$$

defined above. This homomorphism factors through the surjective homomorphism $\psi\colon H_2 \longrightarrow \mathrm{Gal}(L_2/F_2) \cong D$. Using the isomorphism $\beta\colon H_2 \longrightarrow H_1$ induced by $i^\star$ and our construction of L_1/F_1, we see that the homomorphism $\psi\colon H_2 \longrightarrow \mathrm{Gal}(L_2/F_2)$ is compatible, via identification of H_2 with H_1 using $i^\star$, with the restriction homomorphism $\tilde{\psi}\colon H_1 \longrightarrow \mathrm{Gal}(L_1/F_1)$. Passing to the quotients $\mathrm{Gal}(F_2(\sqrt{bs_2}, \sqrt{ct_2})/F_2)$ and $\mathrm{Gal}(F_1(\sqrt{u}, \sqrt{v})/F_1)$ of $\mathrm{Gal}(L_2/F_2)$ and $\mathrm{Gal}(L_1/F_1)$ respectively, we see that we can identify the homomorphism $\theta\colon H_2 \longrightarrow \mathrm{Gal}(F_2(\sqrt{bs_2}, \sqrt{ct_2})/F_2)$ with the restriction homomorphism $\tilde{\theta}\colon H_1 \longrightarrow \mathrm{Gal}(F_1(\sqrt{u}, \sqrt{v})/F_1)$ via the isomorphism $i^\star\colon H_2 \longrightarrow H_1$. Finally from the natural isomorphism $\dot{F}_1/T_1 \cong \dot{F}_2/T_2$ we may assume that $u = bs_1$ and $v = ct_1$ for suitable elements $s_1, t_1 \in T_1$. By Proposition 1.5, this implies that the quaternion algebra $\left(\frac{bs_1, ct_1}{F_1}\right)$ splits, and that there exist $\tilde{s_1}, \tilde{t_1} \in T_1$ such that $b\tilde{s_1} + c\tilde{t_1} = 1$.

Suppose now that bs_2, ct_2 are linearly dependent in $\dot{F}_2/T_2$. Then b and c are equal modulo T_2 and we may assume $b = c$. There are still two more cases to consider.

(2) Suppose we have $cs_2 + ct_2 = 1$ with $s_2 = t_2 \bmod \dot{F}_2^2$. By Proposition 1.5, there exists a $C_4^{cs_2}$-extension L_2/F_2 with $F_2(\sqrt{cs_2}) \subset L_2$. Using arguments similar to those in (1), we show that the restriction $\psi: H_2 \longrightarrow \mathrm{Gal}(L_2/F_2)$ is onto, and we find $s_1 \in T_1$ such that $\left(\frac{cs_1, cs_1}{F_1}\right)$ splits. This implies that there exist $\tilde{s_1}, \tilde{t_1} \in T_1$ such that $c\tilde{s_1} + c\tilde{t_1} = 1$.

(3) Suppose we have $cs_2 + ct_2 = 1$ with $s_2 \neq t_2 \bmod \dot{F}_2^2$. As in (1) we find L_2 with $\mathrm{Gal}(L_2/F_2) \cong D$ and we have a tower of fields $F_2 \longrightarrow F_2(\sqrt{s_2t_2}) \longrightarrow F_2(\sqrt{cs_2}, \sqrt{ct_2}) \longrightarrow L_2$. Since H_2 fixes $F_2(\sqrt{s_2t_2})$, the restriction map $\psi: H_2 \longrightarrow \mathrm{Gal}(L_2/F_2)$ induces a surjective homomorphism $\psi': H_2 \longrightarrow \mathrm{Gal}(L_2/F_2(\sqrt{s_2t_2})) \cong C_4$. We finish with arguments as in (2) and replacing F_2 by $F_2(\sqrt{s_2t_2})$, we find $\tilde{s_1}, \tilde{t_1} \in T_1$ such that $c\tilde{s_1} + c\tilde{t_1} = 1$. $\square$

We now prove the result in the other direction.

Proposition 9.12. *Let H_1, H_2 be as in Notation 9.9 and assume they are fair subgroups. If the inclusion $i: F_1 \longrightarrow F_2$ induces an isomorphism $\dot{F}_1/T_1 \longrightarrow \dot{F}_2/T_2$ and if $(T_2 + aT_2) \cap \dot{F} = T_1 + aT_1$ for any $a \in F_1$, then $i^\star$ induces an isomorphism between H_2 and H_1.*

Proof. If $H_2 = \{1\}$ then $H_1 = \{1\}$ as well. If $H_2 = C_2$ then $i^\star(H_2) \neq \{1\}$ because T_2 is a usual ordering in $\dot{F}_2$, and it cannot contain $\dot{F}_1$. However if H_1 were $\{1\}$ then $T_1 = \dot{F}_1$. Therefore $i^\star$ induces an isomorphism between H_2 and H_1.

For the rest of our proof we assume that $H_2 \neq \{1\}, C_2$. Call $\beta: H_2 \longrightarrow H_1$ the restriction of $i^\star$ to H_2. Because $i^\star$ is a group homomorphism from $\mathcal{G}_{F_2}$ into $\mathcal{G}_{F_1}$, we have $i^\star(\Phi(\mathcal{G}_{F_2})) \subset \Phi(\mathcal{G}_{F_1})$. Also we have $\beta(\Phi(H_2)) \subset \Phi(H_1)$. Then the map β induces $\hat{\beta}: H_2/\Phi(H_2) \longrightarrow H_1/\Phi(H_1)$, which is an isomorphism because its dual map $\dot{F}_1/T_1 \longrightarrow \dot{F}_2/T_2$ is an isomorphism. By definition β is onto. We want to show that β is injective. From the fact that $\hat{\beta}$ is an isomorphism, we see that $\ker\beta \subseteq \Phi(H_2)$. Take a fixed set of minimal (topological) generators $(\sigma_i)_{i\in I}$ for H_2. Then $\gamma \in \Phi(H_2)$ has a unique description, up to a permutation, as $\gamma = \prod_{i\in I} \sigma_i^2 \times \prod_{(u,v)\in K} [\sigma_u, \sigma_v]$ for some possibly infinite sets I, K.

To complete the proof we use the following lemma.

Lemma 9.13. *Assume that H_1, H_2, T_1, T_2 are as in Proposition 9.12, and let δ be σ_i^2 or $[\sigma_u, \sigma_v]$. Suppose that we have a surjective map $\varphi: H_2 \longrightarrow G$ where $G = D$ or C_4. Then there exists a group $\tilde{G}$ which is again either D or C_4 and a homomorphism $\psi: H_1 \longrightarrow \tilde{G}$ such that $\psi(\beta(\delta)) \neq 1 \in \tilde{G}$ if and only if $\varphi(\delta) \neq 1 \in G$. Moreover $\tilde{G}$ and the homomorphism ψ depend only on G and on the fields F_1 and F_2, but not on δ.*

Proof. (1) Assume first that $G = C_4$. Since H_2 is liftable, there exist an H_2-extension K_2/F_2 and a C_4^u-extension L_2 of F_2 with $F_2 \longrightarrow F_2(\sqrt{u}) \longrightarrow L_2 \longrightarrow K_2$. Since $\dot{F}_1/T_1 \cong \dot{F}_2/T_2$, there exist $a \in \dot{F}_1, s_2 \in T_2$ such that $u = as_2$. Let $\delta = \sigma^2$, which is the only case to be considered when $G = C_4$. Then $\varphi(\sigma^2) \neq 1 \in \mathrm{Gal}(L_2/F_2)$ if and only if $\varphi(\sigma)$ has order 4. Thus $\varphi(\sigma^2) \neq 1$ if and only if $\varphi(\sigma)$ generates $\mathrm{Gal}(L_2/F_2)$. This happens precisely when $\varphi(\sigma)(\sqrt{as_2}) = -\sqrt{as_2}$. Since H_2, and thus $\varphi(\sigma)$, fixes $\sqrt{s_2}$, this is equivalent to $\varphi(\sigma)(\sqrt{a}) = -\sqrt{a}$. On the other hand, we know by Proposition 1.5 that the quaternion algebra $\left(\frac{as_2, as_2}{F_2}\right)$ splits, and this implies the existence of $s_2', t_2' \in T_2$ such that $as_2' + at_2' = 1$.

From the assumption on the additive structure, this implies the existence of $s_1, t_1 \in T_1$ such that $as_1 + at_1 = 1$. Two cases are to be considered.
(1.1) If $s_1 = t_1 \bmod \dot{F}_1^2$, then there is a $C_4^{as_1}$-extension L_1 of F_1 with $F_1 \longrightarrow F_1(\sqrt{as_1}) \longrightarrow L_1$. Denoting by $\psi\colon H_1 \longrightarrow \mathrm{Gal}(L_1/F_1)$ the restriction, because H_1 fixes $\sqrt{T_1}$ we have $\psi(\beta(\sigma))(\sqrt{as_1})/\sqrt{as_1} = \psi(\beta(\sigma))(\sqrt{a})/\sqrt{a} = \varphi(\sigma)(\sqrt{a})/\sqrt{a} = -1$, showing $\psi(\beta(\delta)) \neq 1 \in C_4 = \tilde{G}$.
(1.2) If $s_1 \neq t_1 \bmod \dot{F}_1^2$, then there is a D^{as_1,at_1}-extension L_1 of F_1 with $F_1 \longrightarrow F_1(\sqrt{s_1t_1}) \longrightarrow L_1$. Here $L_1/F_1(\sqrt{s_1t_1})$ is a C_4-extension. Since $\beta(\sigma) \in H_1$ fixes $F_1(\sqrt{s_1t_1})$, $\psi(\beta(\sigma))$ is in the Galois group of the latter extension, which is again a C_4-extension. We then use the same argument as in (1.1) to conclude that $\psi(\beta(\delta)) \neq 1 \in \tilde{G} = C_4$.

(2) Assume $G = D$. Again there is an H_2-extension K_2 *of* F_2 and a D^{as_2,bs_2}-extension L_2 of F_2 with $F_2 \longrightarrow F_2(\sqrt{abs_2t_2}) \longrightarrow L_2 \longrightarrow K_2$. Since φ is surjective, there is an element $\tau \in H_2$ such that $\tau(\sqrt{abs_2t_2})/\sqrt{abs_2t_2} = -1$, or else $\varphi(H_2)$ would fix $F_2(\sqrt{abs_2t_2})$ and would be contained in a proper subgroup of $\mathrm{Gal}(L_2/F_2) \cong D$. This implies $ab \notin T_2$. Since there exist $s_2', t_2' \in T_2$ such that $as_2' + bt_2' = 1$, we also have, by the assumption on the additive structures, $as_1 + bt_1 = 1$ for some $s_1, t_1 \in T_1$. Since $ab \notin T_1$, we see that as_1, bt_1 are independent modulo $\dot{F}_1^2$, and there is a D^{as_1,bt_1}-extension L_1 of F_1 with $F_1 \longrightarrow F_1(\sqrt{abs_1t_1}) \longrightarrow L_1$. Denote by $\psi\colon H_1 \longrightarrow \mathrm{Gal}(L_1/F_1) \cong D$ the restriction map.
(2.1) Suppose $\delta = \sigma^2$ and $\varphi(\delta) \neq 1$. Then $\varphi(\sigma)$ has order 4 and must fix the quadratic extension $F_2(\sqrt{abs_2t_2})$. Then it belongs to $\mathrm{Gal}(L_2/F_2(\sqrt{abs_2t_2})) \cong C_4$. With the same arguments as in (1), we show that $\psi(\beta(\delta)) \neq 1$.
(2.2) Suppose $\delta = [\sigma_u, \sigma_v]$ and $\varphi(\delta) \neq 1$. Then none of $\varphi(\sigma_u), \varphi(\sigma_v)$ is in $\Phi(D)$ (i.e. they do not fix the biquadratic extension $F_2(\sqrt{as_2}, \sqrt{bt_2})$), and they act differently on this biquadratic extension. Since $\varphi(\sigma_u)$ (respectively $\varphi(\sigma_v)$) acts the same way on elements in $\sqrt{\dot{F}}$ as $\psi(\beta(\sigma_u))$ (respectively $\psi(\beta(\sigma_v))$, we see that $\psi(\beta(\delta)) \neq 1 \in G$.

To conclude the proof, we point out that in all cases above, we first associated $\tilde{G}$ with the given homomorphism $\varphi\colon H_2 \longrightarrow G$ and only then checked that $\varphi(\delta) \neq 1 \in G$ is equivalent to $\psi(\beta(\delta)) \neq 1 \in \tilde{G}$. $\square$

We can now finish the proof of Proposition 9.12. Suppose $\gamma \neq 1 \in \Phi(H_2)$. Since H_2 satisfies the subdirect product condition, there exists a surjective map $\varphi\colon H_2 \longrightarrow G$ with $G \cong D$ or C_4 and with $\varphi(\gamma) \neq 1 \in G$. Recall that the minimal set of generators $(\sigma_i)_{i\in I}$ may be chosen in such a way that for any open set U of H_2 there are at most finitely many σ_i's outside U. (See for example [Koc, Chapter 4].) Since $\ker\varphi$ is open, we may thus assume, when working with a given φ, that $\gamma = \gamma_0 \times \gamma_1$, with $\gamma_0 = \prod_{i\in I_0} \sigma_i^2 \times \prod_{(u,v)\in K_0} [\sigma_u, \sigma_v]$, $\gamma_1 = \prod_{i\in I_1} \sigma_i^2 \times \prod_{(u,v)\in K_1} [\sigma_u, \sigma_v]$, with the following properties. The sets I_0, K_0 are finite. Any individual factor $\sigma_i^2, [\sigma_u, \sigma_v]$ of γ_0 is not in $\ker\varphi$, while any individual factor of γ_1 is in $\ker\varphi$. We may assume that $\gamma = \gamma_0$, and in particular we have only a finite number n of terms δ_i's with $\delta_i = \sigma_i^2$ or $[\sigma_u, \sigma_v]$. The Frattini group $\Phi(G) \cong C_2$ may be written $\{1, \epsilon\}$, and each $\varphi(\delta_i)$ must be ϵ, since it is not 1 by assumption. Since $\varphi(\gamma) = \epsilon^n \neq 1$, n must be odd. By Lemma 9.13, we know that there exists a group $\tilde{G}$ which is again D or C_4 and a homomorphism $\psi\colon H_1 \longrightarrow \tilde{G}$, such that $\varphi(\delta_i) = \epsilon \neq 1$ is equivalent to $\psi(\beta(\delta_i)) = \epsilon \neq 1$. Because n is odd, this shows that $\psi(\beta(\gamma)) \neq 1$, and therefore $\beta(\gamma) \neq 1$. This shows the injectivity of β and finishes the proof of Proposition 9.12. $\square$

§10. Concluding Remarks

In this article we have considered all $C(I)$- and $S(I)$-orderings. These groups correspond to W-groups for p-adic fields, for odd primes p. In particular, the W-group $\mathcal{G}_p$ of $\mathbb{Q}_p$ is $C_4 \times C_4$ for $p \equiv 1(4)$ and is $C_4 \rtimes C_4$ for $p \equiv 3(4)$. It is then natural to look for a characterization of $\mathcal{G}_2$-orderings, i.e. those orderings corresponding to subgroups isomorphic to the W-group of $\mathbb{Q}_2$. This is currently under investigation [MiSm4].

For the field $\mathbb{Q}$, there is a unique C_2-ordering, which is the unique ordering on $\mathbb{Q}$. In addition there is a one-to-one correspondence between $C_4 \times C_4$-orderings on $\mathbb{Q}$ and primes $p \equiv 1(4)$, and a one-to-one correspondence between $C_4 \rtimes C_4$-orderings on $\mathbb{Q}$ and primes $p \equiv 3(4)$. In each case the correspondence is given by $T_p = \dot{\mathbb{Q}}_p^2 \cap \mathbb{Q}$. It is not hard to see that each such intersection gives rise to an H-ordering of the appropriate type. To see that every such orderings may be obtained in this way, one shows that each such ordering corresponds to a certain valuation on $\mathbb{Q}$, and the valuations on $\mathbb{Q}$ are well-known to be classified by the primes. (See e.g. [End, Theorem 1.16].)

This observation then lends itself to an alternative perspective on the Hasse-Minkowski Theorem, which states that a quadratic form defined over $\mathbb{Q}$ is isotropic over $\mathbb{Q}$ if and only if it is isotropic over each $\mathbb{Q}_p$, including $\mathbb{Q}_\infty$, the real numbers. Using Hilbert's reciprocity law, one can prove that a ternary quadratic form is isotropic over $\mathbb{Q}$ if and only if it is isotropic over all but one of these fields. Thus we see that a ternary quadratic form over $\mathbb{Q}$ is isotropic if and only if it is isotropic with respect to all C_2-, $(C_4 \times C_4)$-, and $(C_4 \rtimes C_4)$-orderings on $\mathbb{Q}$.

We point out that the case of a ternary quadratic form over $\mathbb{Q}$, together with the clever use of Dirichlet's theorem on the existence of an infinite number of primes in an arithmetic progression, where first term and increment are relatively prime, are the main ingredients of a proof of the full Hasse-Minkowski theorem over $\mathbb{Q}$. For a very nice exposition of the Hasse-Minkowski theorem over $\mathbb{Q}$, see [BS]. See also [L1, Chapter 6, Exercise 22].

It is not difficult however, to find a quaternary quadratic form φ over $\mathbb{Q}$ such that φ is isotropic over all $\mathbb{Q}_p$, p is an odd prime, and $\mathbb{Q}_\infty = \mathbb{R}$ but φ is anisotropic over $\mathbb{Q}_2$. Because we were unable to locate an explicit example of such a form in the literature, we write down one explicit example here:

$$\varphi = X_1^2 + X_2^2 - 7X_3^2 - 31X_4^2$$

Because $-7 \equiv 1(\mod 8)$ and $-31 \equiv 1(\mod 8)$, we see that φ is equivalent to $\psi = X_1^2 + X_2^2 + X_3^2 + X_4^2$ over $\mathbb{Q}_2$. Because the level of $\mathbb{Q}_2$ is 4, we see that ψ is anisotropic over $\mathbb{Q}_2$. On the other hand using the well-known Springer theorem for local fields ([L1, Chapter 6, Proposition 1.9]), and the fact that each ternary quadratic form over any finite field is isotropic, we see that φ is isotropic over each $\mathbb{Q}_p$, p an odd prime. Since φ is an indefinite quadratic form, φ is isotropic over $\mathbb{Q}_\infty$ as well.

In a subsequent paper we will present several applications of this theory to different kinds of local-global principles for quadratic forms. In order to get a sense of what can be done in this direction, we show below an example of a simple situation in which our theory applies.

Consider a field F. Recall that a $C(\emptyset)$-ordering T on F is an index 2 multiplicative subgroup of $\dot{F}/\dot{F}^2$ containing -1. Additively speaking, it is a hyperplane containing -1

in the $\mathbb{F}_2$-vector space $\dot{F}/\dot{F}^2$. If $f \in \dot{F} \setminus (\dot{F}^2 \cup -\dot{F}^2)$ and if V is any subspace of $\dot{F}/\dot{F}^2$ such that $\dot{F}/\dot{F}^2 = \mathrm{Span}\{f, -1\} \oplus V$, then $T := \mathrm{Span}\{-1\} + V$ is a $C(\emptyset)$-ordering not containing f. Then the next lemma follows immediately.

Lemma 10.1. *Let $C_0(F)$ denote the set of $C(\emptyset)$-orderings of F. Then $C_0(F) = \emptyset$ if and only if $\dot{F} = \dot{F}^2 \cup -\dot{F}^2$, and in general,*

$$\bigcap_{T \in C_0(F)} T = \dot{F}^2 \cup -\dot{F}^2.$$

To every $C(\emptyset)$-ordering T we associate a fixed closure F_T of F in the quadratic closure of F. Denote by $\langle\langle a_1, \dots, a_n \rangle\rangle$ the Pfister form $\langle 1, -a_1 \rangle \otimes \dots \otimes \langle 1, -a_n \rangle$. (For the basic theory of Pfister forms see e.g. [L1, Chapter 10] or [Sc, Chapter 4]. Observe that both Lam and Scharlau denote by $\langle\langle a_1, \dots, a_n \rangle\rangle$ the Pfister form $\langle 1, a_1 \rangle \otimes \dots \otimes \langle 1, a_n \rangle$.) Then we have the following.

Proposition 10.2. *Assume $C_0(F) \neq \emptyset$ and denote by φ the map $W(F) \longrightarrow \prod_{T \in C_0(F)} W(F_T)$ induced by the inclusions $F \longrightarrow F_T$. Then $\operatorname{Ker} \varphi = I^2F + 2W(F)$ where IF denotes the fundamental ideal of $W(F)$.*

Proof. For $T \in C_0(F)$ we have $\dot{F}/T = \{\bar{1}, \bar{f}\}$ for a certain $f \in \dot{F}$, and it is easy to see that $W(F_T) \cong C_2[\epsilon]/\epsilon^2$ and that the isomorphism, say π, is defined by $\pi(\langle \bar{1} \rangle) = 1, \pi(\langle \bar{f} \rangle) = 1+\epsilon$. If $a, b \in \dot{F}$ then the possibilities for $\bar{a}, \bar{b}$ are (1) $\bar{a} = 1$ or $\bar{b} = 1$, or (2) $\bar{a} = \bar{b} = \bar{f}$. In any case the image in $W(F_T)$ of the 2-fold Pfister form $\langle\langle a, b \rangle\rangle$ is in $2W(F_T) = 0$, and we have shown the inclusion $I^2F + 2W(F) \subseteq \operatorname{Ker} \varphi$.

Take $q \in \operatorname{Ker} \varphi$. Then $q \in IF$, because any odd-dimensional form is nonzero in $W(F_T)$. But it is known ([Pf, p. 122, Kor. to Satz 13]) that any element q of IF may be written $q = \langle\langle u \rangle\rangle + q_1$, with $q_1 \in I^2F$. Since $q \in \operatorname{Ker} \varphi$, and $I^2F \subset \operatorname{Ker} \varphi$, we deduce $\langle\langle u \rangle\rangle \in \operatorname{Ker} \varphi$. The latter is equivalent to $u \in T$ for every T, meaning $u \in \dot{F}^2 \cup -\dot{F}^2$, or in other words $\langle\langle u \rangle\rangle = 0$ or 2 in $W(F)$. □

Recall that a field F is said to have virtual cohomological dimension n, denoted $\mathrm{vcd}(F) = n$, if $H^d(\mathrm{Gal}(F(2))/F(\sqrt{-1})), \mu_2) = 0$ for $d > n$, and $H^n(\mathrm{Gal}(F(2))/F\ (\sqrt{-1})), \mu_2) \neq 0$. (If we also considered the case of $\mathbb{F}_p, p$ an odd prime, as coefficients of the cohomology groups of absolute Galois groups, it would be more appropriate to say that F as above has virtual 2-cohomological dimension equal to n.) If $\mathrm{vcd}(F) \leq 1$, then I^2F is torsion-free. To see this, observe first that $\mathrm{vcd}(F) \leq 1$ implies each binary quadratic form over $F(\sqrt{-1})$ is universal. Then use [L1, Chapter 11, Theorem 1.8 and Exercise 20] to conclude that I^2F is torsion free. An example of a formally real field F with $vcd(F) = 1$ is $F = \mathbb{R}(X)$. We have the following local-global principle:

Theorem 10.3. *Let F be a field with* $\mathrm{vcd}(F) \leq 1$. *Let $D_0(F)$ (resp. $C_0(F)$, $S_0(F)$) denote the set of usual orderings $X(F)$ (resp. $C(\emptyset)$-orderings, $S(\emptyset)$-orderings) of F. Then*

$$\Lambda \colon W(F) \longrightarrow \prod_{T \in D_0(F) \cup C_0(F) \cup S_0(F)} W(F_T)$$

is injective. If F is formally real, we may drop $S_0(F)$. (If not, we may of course drop $D_0(F)$.)

Proof. It is clear that a form $q \in \operatorname{Ker}\Lambda$ is in IF, and thus can be written $q = \langle\langle a\rangle\rangle + q_2$ with $q_2 \in I^2F$. By Pfister's Local-Global Principle [L1, Chapter 8, §4], q is torsion and it is therefore the case for $\langle\langle a\rangle\rangle$ and q_2. (It is trivial when $D_0(F) = \emptyset$, and if not, we use the fact that the signature $\hat{q}$ of q is 0 and that $\hat{q_2} \equiv 0(\mathrm{mod}4)$.)

Since I^2F is torsion-free, one has $q_2 = 0$, and $q = \langle\langle a\rangle\rangle$. Since q vanishes on $C_0(F)$, by Proposition 10.2 we have $a \in \dot{F}^2 \cup -\dot{F}^2$. (If $C_0(F) = \emptyset$, this condition is trivially satisfied.) If the level $s(F)$ is 1, we are finished, and otherwise $D_0(F) \cup S_0(F) \neq \emptyset$, showing that $q \neq \langle\langle -1\rangle\rangle$. Thus $q = \langle\langle 1\rangle\rangle = 0$. □

Remark 10.4. In this case we even have a strong Hasse Principle, that is a local-global principle for detecting whether a quadratic form is anisotropic rather than just hyperbolic. Indeed, the fact that each ternary form over $F(\sqrt{-1})$ is isotropic and [ELP, Theorem F] give us the strong Hasse Principle for forms of rank greater than or equal to 3. Then the use of $C_0(F), S_0(F)$ and $D_0(F)$ provides the result for rank 2 forms.

Finally let us point out that our results are closely related to some ideas in birational anabelian Grothendieck geometry. In particular there is a close connection between ideas explored in this paper and the work of Bogomolov, Tschinkel and Pop ([Bo], [BoT], [Po1], and [Po2]; see also Koenigsmann's thesis [K1] and paper [K2]). Roughly speaking, they establish that for certain fields K the isomorphy type of K, modulo purely inseparable extensions of K, is functorially encoded in the pro-p-quotient of the absolute Galois group $\tilde{G} := \operatorname{Gal}(\bar{K}/K), \operatorname{char} K \neq p$. In fact Bogomolov in [Bo] and also Pop in lectures at MSRI in the fall of 1999, considered smaller Galois groups than the Galois group defined above, namely the maximal pro-p-quotient of the group $\tilde{G}/[[\tilde{G},\tilde{G}],\tilde{G}]$. In this paper we consider $p = 2$, because of the connections with quadratic forms. It is expected however that a substantial part of our results can be extended to any prime p provided that the base field F contains a primitive pth root of unity. We allow F to be any field with $\operatorname{char} F \neq 2$, and we are concerned with even smaller Galois groups than were considered by Bogomolov and Pop. Of course in this more general setting we cannot obtain as precise results as Bogomolov and Pop, but we do get some interesting information about the additive properties of multiplicative subgroups of fields. It would be very interesting to investigate further relationships between our work and the quoted work of Bogomolov, Pop and Tschinkel.

References

[AKMi] A. Adem, D. Karagueuzian and J. Mináč, *On the cohomology of Galois groups determined by Witt rings*, Adv. Math. **148** (1999), 105–160.

[ArTa] E. Artin and J. Tate, *Class field theory*, Benjamin, 1967.

[AEJ] J. Arason, R. Elman and B. Jacob, *Rigid elements, valuations, and realization of Witt rings*, J. Algebra **110** (1987), 449–467.

[ArSch1] E. Artin and O. Schreier, *Algebraische Konstruktion reeller Körper*, Abh. Math. Sem. Univ. Hamburg **5** (1927), 85–99.

[ArSch2] E. Artin and O. Schreier, *Eine Kennzeichnung der reell abgeschlossenen Körper*, Abh. Math. Sem. Univ. Hamburg **5** (1927), 225–231.

[Be1] E. Becker, *Euklidische Körper und euklidische Hüllen von Körpern*, J. reine angew. Math. **268/269** (1974), 41–52.

[Be2] ______, *On the real spectrum of a ring and its applications to semialgebraic geometry*, Bull. AMS **15** (1986), 19–60.

[BK] E. Becker, E. Köpping, *Reduzierte quadratische Formen und Semiordnungen reeller Körper*, Abh. Math. Sem. Univ. Hamburg **46** (1977), 143–177.

[BCR] J. Bochnak, M. Coste, M. -F. Roy, *Real Algebraic Geometry*, Ergeb. Math., vol. 36, Springer-Verlag, Berlin, Heidelberg, 1998.

[Bo] F. A. Bogomolov, *On two conjectures in birational algebraic geometry*, Algebraic Geometry and Analytic Geometry (A. Fujiki et. al., eds.), ICM-90 Satellige Conference Proceedings, Springer-Verlag, Tokyo, 1991.

[BoT] F. A. Bogomolov and Y. Tschinkel, *Commuting elements in Galois groups of function fields*, preprint in Ar. Xiv: Math. AG/0012245, http://xxx.lanl.gov/ (2000).

[BS] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, Inc., 1966.

[BEK] Bredikhin, Ershov, and Kal'nei, *Fields with two linear orderings*, Translated from Mat. Zametki Vol. 7 (1970), 525–536, Math Notes, Institute of Mathematics, Siberian Branch, Academy of Sciences of hte USSR (1970), 319–325.

[Br] L. Bröcker, *Zur Theorie der quadratischen Formen über formal reellen Körpern*, Math. Ann. **210** (1974), 233–256.

[Cr1] T. Craven, *Characterizing reduced Witt rings of fields*, J. Algebra **53** (1978), 68–77.

[Cr2] ______, *Fields maximal with respect to a set of orderings*, J. Algebra **115** (1988), 200–218.

[CrSm] T. Craven and T. Smith, *Formally real fields from a Galois theoretic perspective*, J. Pure Appl. Alg. **145** (2000), 19–36.

[Ef] I. Efrat, *Construction of valuations from K - theory*, Mathematical Research Letters **6** (1999), 335–343.

[ELP] R. Elman, T.-Y. Lam and A. Prestel, *On some Hasse Principles over formally real fields*, Math. Z. **134** (1973), 291–301.

[End] O. Endler, *Valuation theory*, Springer-Verlag, New York, 1972.

[EnKo] A. J. Engler and J. Koenigsmann, *Abelian subgroups of pro-p Galois groups*, Trans. A.M.S. **350** (1998), 2473–2485.

[Fr] A. Fröhlich, *Orthogonal representations of Galois groups, Stiefel-Whitney classes and Hasse-Witt invariants*, J. Reine Angew. Math. **360** (1985), 84–123.

[GM] W. Gao and J. Mináč, *Milnor conjecture and Galois theory I*, Fields Institute Communications **16** (1997), 95–110.

[Gr] G. Grätzer, *Universal Algebra*, Second Edition, Springer-Verlag, 1979.

[Hal] M. Hall,Jr, *The theory of groups*, The Macmillan Company, New York, 1959.

[Har] D. Harbater, *Galois coverings of the arithmetic line*, Number Theory, New York 1984-1985, Lecture Notes in Mathematics **1240** (1987), Springer-Verlag, New York, 165–195.

[HaVöl] D. Haran and H. Völklein, *Galois groups over complete valued fields*, Israel Journal of Mathematics **93** (1996), 9–27.

[Jo] D. L. Johnson, *Non-nilpotent elements of cohomology rings*, Math. Zeit. **112** (1969), 364–374.

[Ki] I. Kiming, *Explicit classifications of some 2-extensions of a field of characteristic different from* 2, Can. J. of Math. **42** (1990), 825–855.

[Koc] H. Koch, *Galoische Theorie der p-Erweiterungen*, Springer-Verlag, New York, 1970.

[K1] J. Koenigsmann, *Half-ordered fields*, Dissertation Thesis, Universität Konstanz, Konstanz, 1993.

[K2] ______, *From p-rigid elements to valuations (with a Galois characterization of p-adic fields)*, with appendix by F. Pop, J. Reine Angew. Math. **465** (1995), 165–182.

[L1] T. Y. Lam, *The algebraic theory of quadratic forms*, Benjamin/Cummings Publishing Co., Reading, Mass., 1980.

[L2] ______, *Orderings, valuations and quadratic forms*, Conference Board of the Mathematical Sciences No. 52, Amer. Math. Soc., Providence, RI, 1983.

[L3] ______, *An introduction to real algebra*, Rocky Mountain J. Math. **14** (1984), 767–814.

[LaSm] T. Y. Lam and T. Smith, *On the Clifford-Littlewood-Eckmann groups: A new look at periodicity mod 8*, Rocky Mtn. J. Math. **19** (1989), 749–786.

[Mac] S. MacLane, *Subfields and automorphism groups of p-adic fields*, Ann. of Math. **40** (1939), 423–442.

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

[Me] A. Merkurjev, *On the norm residue symbol of degree two*, English translation: Soviet Math. Dokladi **24** (1981), 546-551, Dokladi Akad. Nauk. SSSR **261** (1981), 542-547.

[Mi1] J. Mináč, *Elementary 2-abelian subgroups of W-groups,*, unpublished manuscript (1987).

[MiSm1] J. Mináč and T. Smith, *A characterization of C-fields via Galois groups*, J. Algebra **137** (1991), 1–11.

[MiSm2] ———, *Decomposition of Witt rings and Galois groups*, Canad. J. Math **47** (1995), 1274–1289.

[MiSm3] ———, *W-Groups under quadratic extensions of fields*, Canad. J. Math. **52** (2000), 833–848.

[MiSm4] ———, *Formally dyadic fields*, in preparation.

[MiSp1] J. Mináč and M. Spira, *Formally real fields, pythagorean fields, C-fields and W-groups*, Math. Z. **205** (1990), 519–530.

[MiSp2] ———, *Witt rings and Galois groups*, Ann. of Math. **144** (1996), 35–60.

[Mo] S. Morris, *Pontryagin duality and the structure of locally compact abelian groups*, London Mathematical Society Lecture Note Series, vol. 29, Cambridge University Press, Cambridge, 1980.

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

[Po1] F. Pop, *On Grothendieck's conjecture of birational anabelian geometry*, Ann. Math. **139** (1994), 145–182.

[Po2] ———, *Glimpses of Grothendieck's anabelian geometry*, Geometric Galois Action 1: Around Grothendieck's Esquisse d'un Programme (L. Schneps and P. Lochak, eds.), Lecture Notes in Mathematics, vol. 242, Springer-Verlag, Berlin, 1997, pp. 113–126.

[Ri] P. Ribenboim, *Théorie des Valuations*, Université de Montreal, Les Presses de l'Université Montreal, 1965.

[RZ] L. Ribes and P. Zalesskii, *Profinite Groups*, Springer-Verlag, Berlin, 2000.

[Sc] W. Scharlau, *Quadratic and Hermitian Forms*, Springer-Verlag, 1985.

[Sch] N. Schwartz, *Signatures and Real Closures of Fields*, Publications de l'Université Paris VII **32** (1990), 65–78.

[S] E. Sperner, *Die Ordnungsfunktionen einer Geometrie*, Math. Ann. **121** (1949), 107–130.

[Sp] M. Spira, *Witt rings and Galois groups*, Ph.D. Thesis, University of California, Berkeley, California, 1987.

[Vo] V. Voevodsky, On 2-torsion in motivic cohomology, http:/www.math.uiuc.edu/K-theory/0502/index.html (2001).

[Wa] R. Ware, *Valuation rings and rigid elements in fields*, Canad. J. Math. **33** (1981), 1338–1355.

IRMAR, Campus de Beaulieu, F-35042 Rennes-Cedex France
E-mail address: `Louis.Mahe@univ-rennes1.fr`

Dept. of Mathematics, Univ. of Western Ontario, London, Ontario N6A 5B7 Canada
E-mail address: `minac@uwo.ca`

Dept. of Mathematical Sciences, Univ. of Cincinnati, Cincinnati, Ohio 45221-0025 U.S.A.
E-mail address: `tsmith@math.uc.edu`