ISRAEL JOURNAL OF MATHEMATICS 85 (1994), 57–78

ON GALOIS GROUPS OVER PYTHAGOREAN AND SEMI-REAL CLOSED FIELDS*

BY

IDO EFRAT

The Institute for Advanced Studies
The Hebrew University of Jerusalem
Givat Ram 91904, Jerusalem, Israel
e-mail: efrat@coma.huji.ac.il

AND

DAN HARAN

School of Mathematical Sciences
Raymond and Beverly Sackler Faculty of Exact Sciences
Tel-Aviv University, Ramat Aviv, Tel-Aviv 69978, Israel
e-mail: haran@math.tau.ac.il

ABSTRACT

We call a field K semi-real closed if it is algebraically maximal with respect to a semi-ordering. It is proved that (as in the case of real closed fields) this is a Galois-theoretic property. We give a recursive description of all absolute Galois groups of semi-real closed fields of finite rank.

Introduction

By a well-known theorem of Artin and Schreier [AS], being a real closed field is a Galois-theoretic property. More specifically, a field K is real closed if and only if its absolute Galois group $G(K)$ is of order two. This enables one to reflect many arithmetical properties of orderings on K as group-theoretic properties of $G(K)$. However, in studying the structure of formally real fields, the collection of all orderings is in many respects too small. For many uses one needs to consider the

* Research carried out at the Institute for Advanced Studies of the Hebrew University of Jerusalem.
Received March 2, 1992 and in revised form August 19, 1993

broader collection of the semi-orderings (also called q-orderings) on K. These arithmetical objects, introduced by A. Prestel and studied mainly by him [P], by L. Bröcker [Br1] and by Becker and Köpping [BK], are defined as follows: A **semi-ordering** on K is a subset $S \subset K$ such that $1 \in S$, $K = S \cup -S$, $S \cap -S = \{0\}$, $S + S = S$ and $K^2 S = S$ (here K^2 denotes the set of all squares in K). Thus, an ordering is a semi-ordering closed under multiplication.

In the present paper we study the absolute Galois groups of the **semi-real closed** fields, that is, fields K that admit a semi-ordering which does not extend to any proper algebraic extension of K. Their importance can be realized, e.g., from the following local-global principle for isotropy, essentially due to Prestel [P, Th. 2.9]: Assume that K is pythagorean (i.e., K is formally real and every sum of squares in K is a square in K) and let φ be a quadratic form over K. Then φ is isotropic in K if and only if it is isotropic in every semi-real closed algebraic extension of K.

Inspired by Artin-Schreier's theorem, we first prove that being semi-real closed is a Galois-theoretic property. In other words, if K and L are fields with $G(K) \cong G(L)$ and if K is semi-real closed then so is L (Theorem 5.1(c)). However, unlike in the case of real closed fields, there are infinitely many profinite groups that appear as absolute Galois groups of semi-real closed fields. In section 5, we give a recursive description of all such finitely generated groups. For example, the groups of rank ≤ 4 in this class are $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}_2^2 \rtimes \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}_2^3 \rtimes \mathbb{Z}/2\mathbb{Z}$. Here $\mathbb{Z}_2$ is the additive group of the dyadic integers (written multiplicatively) and the involution in $\mathbb{Z}/2\mathbb{Z}$ acts by inversion.

ACKNOWLEDGEMENT: This research has begun while both authors were staying at the Heidelberg University in summer 1991, supported by the Deutsche Forschungsgemeinschaft (Efrat) and the Alexander-von-Humboldt Foundation (Haran). We wish to thank Moshe Jarden for several helpful remarks.

1. Realization of certain group-theoretic constructions

In [JW] Jacob and Ware show that the class of all maximal pro-2 Galois groups of fields is closed with respect to free pro-2 products and certain constructions of semi-direct products. In this section we strengthen a few of their methods in order to realize such constructions as the absolute Galois groups of fields (see also [Br3, §4], [JWd, §6] and [K, §3].)

To achieve more generality, we fix a prime number p. Recall that a valued field (K, v) is **p-henselian** if Hensel's lemma holds in it for polynomials that split completely in the maximal pro-p Galois extension $K(p)$ of K. Equivalently, (K, v) is p-henselian if v extends uniquely to $K(p)$ [Br2, Lemma 1.2]. A **p-henselization** of a valued field (K, v) is a p-henselian separable immediate pro-p extension of it. It is the decomposition field of an extension of v to $K(p)$ [Br2, p. 151]. We denote the residue field of a valued field (K, v) by $\bar{K}_v$ and its value group by Γ_v. The Galois group of a Galois extension L/K is denoted by $\mathcal{G}(L/K)$ and the algebraic closure of K is denoted by $\tilde{K}$. The following lemma is well-known and is brought here for convenience.

LEMMA 1.1: *Let (F, v) be a p-henselian valued field that contains the pth roots of unity. Suppose that* $\mathrm{char}\, \bar{F}_v \neq p$. *Then there is a natural split exact sequence*

$$1 \to \mathbb{Z}_p^m \to \mathcal{G}(F(p)/F) \to \mathcal{G}(\bar{F}_v(p)/\bar{F}_v) \to 1 \ , \tag{1}$$

with $m = \dim_{\mathbb{F}_p} \Gamma_v / p\Gamma_v$.

Proof: Let $v(p)$ be the unique extension of v to $F(p)$. Since $\mathrm{char}\, F \neq p$ and F contains the pth roots of unity, every finite Galois subextension F' of $F(p)/F$ is obtained as a finite tower $F = F_0 \subset F_1 \subset \cdots \subset F_n = F'$ with $F_{i+1} = F_i(\sqrt[p]{\alpha_i})$, $\alpha_i \in F_i$, by [La, Ch. VIII, Th. 10]. It follows that $\overline{F(p)}_{v(p)}/\bar{F}_v$ is a p-extension. Since $\mathrm{char}\, \bar{F}_v \neq p$ and by [En, Th. 14.5], this extension is Galois. Furthermore, $F(p)$ is closed under taking pth roots, hence so is $\overline{F(p)}_{v(p)}$. Since the latter field contains the pth root of unity, it has no proper Galois p-extensions, by [La, Ch. VIII, Th. 10] again. Therefore $\overline{F(p)}_{v(p)} = \bar{F}_v(p)$. Since (F, v) is p-henselian, $\mathcal{G}(F(p)/F)$ is the decomposition group of $v(p)/v$. As $\mathrm{char}\, \bar{F}_v \neq p$, the ramification group of $v(p)/v$ is trivial [En, 20.18]. Let G^T be the inertia group and F^T the inertia field of $v(p)/v$. The value group of $v(p)$ is $\Delta = \varinjlim \frac{1}{p^n}\Gamma$. [En, Th. 20.12] yields a natural isomorphism $G^T \cong \mathrm{Hom}(\Delta/\Gamma, \Omega^\times)$, where Ω is the algebraic closure of $\bar{F}_v$. Since $\mathrm{char}\, \Omega \neq p$ and Δ/Γ is p-primary, $G^T \cong \mathrm{Hom}(\Delta/\Gamma, \mathbb{Q}/\mathbb{Z})$ naturally. Therefore

$$G^T \cong \varprojlim \mathrm{Hom}(\frac{1}{p^n}\Gamma/\Gamma, \mathbb{Q}/\mathbb{Z}) \cong \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^m \cong \mathbb{Z}_p^m \quad .$$

Now use the natural isomorphism $\mathcal{G}(F^T/F) \cong \mathcal{G}(\bar{F}_v(p)/\bar{F}_v)$ [En, 19.8(b)] to obtain the exact sequence (1).

To show that (1) splits choose $T \subseteq F^\times$ such that the values $v(t)$, $t \in T$, represent a linear basis of $\Gamma_v/p\Gamma_v$ over $\mathbb{F}_p$. Then $L = F(t^{1/p^n} \mid t \in T,\ n \in \mathbb{N})$ is a totally ramified extension of F in $F(p)$, and its value group is p-divisible. The previous argument (with F replaced by L) shows that the map Res : $\mathcal{G}(F(p)/L) \to \mathcal{G}(\bar{F}_v(p)/\bar{F})$ is an isomorphism. Its inverse is the desired section. ∎

LEMMA 1.2: *Let E be a field of characteristic $\neq p$ that contains the pth roots of unity and such that $G(E)$ is pro-p, and let m be a cardinal number.*

(a) *There exists a field F extending E such that* $\mathrm{tr.deg}(F/E) = m$ *and for which there is a split exact sequence* $1 \to \mathbb{Z}_p^m \to G(F) \xrightarrow{\mathrm{Res}} G(E) \to 1$;

(b) *There exists a field F extending E such that* $\mathrm{tr.deg}(F/E) = m$ *and the map* Res: $G(F) \to G(E)$ *is an isomorphism.*

Proof: (a) Let $\mathbb{Z}_{(p)}$ be the localization of $\mathbb{Z}$ at the ideal $p\mathbb{Z}$, let I be a well-ordered set of cardinality m and let Γ be the direct sum of m copies of $\mathbb{Z}_{(p)}$ indexed by I. Then $m = \dim_{\mathbb{F}_p} \Gamma/p\Gamma$. Order Γ lexicographically with respect to the natural ordering of $\mathbb{Z}_{(p)}$ induced from $\mathbb{Q}$. Let $L = E((\Gamma))$ be the field of formal power series $\sum_{\gamma\in\Gamma} a_\gamma t^\gamma$ with $a_\gamma \in E$ and $\{\gamma \in \Gamma \mid a_\gamma \neq 0\}$ well-ordered. The natural valuation v on L is henselian and has residue field E and value group Γ [P, p. 89]. The unique extension v_p of v to a p-Sylow extension L_p of L is also henselian. Since all separable algebraic extensions of E are pro-p and since Γ is q-divisible for all primes $q \neq p$, the extension v_p/v is immediate. For each $i \in I$ define $\gamma_i \in \Gamma$ by $(\gamma_i)_i = 1$ and $(\gamma_i)_j = 0$ whenever $i \neq j \in I$. Denote the relative algebraic closure of $E(t^{\gamma_i} \mid i \in I)$ in L_p by F. The restriction of v_p to F is again henselian with residue field E and value group Γ. Therefore Lemma 1.1 yields the split exact sequence (1). Observe that the elements t^{γ_i}, $i \in I$, form a transcendence base of F/E of cardinality m.

(b) In the exact sequence of (a), the image of the section has a fixed field with the desired properties. Alternatively, one can argue as in (a), with $\mathbb{Z}_{(p)}$ replaced by $\mathbb{Q}$. ∎

PROPOSITION 1.3: *Let $K_1, \ldots, K_m$ be fields of equal characteristic such that $G(K_1), \ldots, G(K_m)$ are pro-p groups. Then there exists a field K of the same characteristic such that $G(K) \cong G(K_1) *_p \cdots *_p G(K_m)$ (free pro-p product) and* $\mathrm{tr.deg}K \le \max_{1\le i\le m} \mathrm{tr.deg}K_i + 1$.

Proof: If $\mathrm{char}\, K_1 = \cdots = \mathrm{char}\, K_m = p$ then $G(K_1), \ldots, G(K_m)$ are free pro-p groups [R, Ch. V, Cor. 3.4], and therefore so is $G = G(K_1) *_p \cdots *_p G(K_m)$.

If this group is finitely generated then it can be realized as the absolute Galois group of an algebraic extension K of the Hilbertian field $\mathbb{F}_p(t)$ [FJ, Th. 20.22 and Th. 12.10]. If G is not finitely generated then $G \cong G(K_i)$ for some i, so we can take $K = K_i$.

We may therefore assume that $\operatorname{char} K_1 = \cdots = \operatorname{char} K_m \neq p$. Since K_i and its perfect closure have isomorphic absolute Galois groups, we may assume without loss of generality that K_i is perfect, $i = 1, \ldots, m$. In light of Lemma 1.2(b), we may also assume that $\text{tr.deg} K_1 = \cdots = \text{tr.deg} K_m$. By identifying transcendence bases of $K_1, \ldots, K_m$ over the prime field, we may assume that they are all algebraic over a certain perfect field K_0. Using Sylow's theorem, we may assume that $G(K_0)$ is a pro-p group. In particular, K_0 is infinite. Finally, let ζ_p be a primitive root of unity of order p; since $p \nmid [K_0(\zeta_p) : K_0]$, we have $\zeta_p \in K_0$.

Next, let x be a transcendental element over K_0 and choose $a_1, \ldots, a_m \in K_0$ distinct. Let $v_1, \ldots, v_m$ be the valuations on $E = K_0(x)$ that correspond to the primes $(x - a_1), \ldots, (x - a_m)$. Zorn's lemma yields a maximal extension $(E', v_1', \ldots, v_m')$ of $(E, v_1, \ldots, v_m)$ contained in $E(p)$ such that for each $1 \leq i \leq m$, v_i' is unramified over v_i and the residue field of v_i' is contained in K_i. By Krull's Existenzsatz [En, Th. 27.6] this residue field must in fact coincide with K_i. Denoting $y = (x - a_1) \cdots (x - a_m)$, we have that $v_i'(y)$ is a generator of $v_i'((E')^\times)$ for each $1 \leq i \leq m$. Next let $E'' = E'(y^{1/p^n} \mid n \in \mathbb{N})$ and for each $1 \leq i \leq m$ let v_i'' be the unique extension of v_i' to E''. Then the value group of v_i'' is p-divisible and its residue field remains K_i. Let (H_i, u_i) be a henselization (hence an immediate extension) of (E'', v_i''). Also, let L_i be a p-Sylow extension of H_i and let w_i be the unique extension of u_i to L_i. Let F be a p-Sylow extension of E''. Replacing L_i and H_i, $i = 1, \ldots, m$, by appropriate isomorphic copies over E'', we may assume without loss of generality that $L_1, \ldots, L_m$ contain F. We show that the assertion holds with $K = L_1 \cap \cdots \cap L_m$. Since $v_1, \ldots, v_m$ are distinct discrete valuations, they are independent, and therefore so are their extensions $\operatorname{Res}_K w_1, \ldots, \operatorname{Res}_K w_m$ (since K/E is algebraic). The value group of w_i is p-divisible (in fact divisible). By Ostrowski's formula [Ri, p. 236, Th. 2] and since all algebraic extensions of K_i are pro-p, the residue field of w_i must still be K_i. Hence, by [JWd, Th. 4.3], $G(K) = G(L_1) *_p \cdots *_p G(L_m)$. But by Lemma 1.1, Res: $G(L_i) \to G(K_i)$ is an isomorphism, whence the assertion. ∎

We denote, as customary, $K_q = K(2)$. The following result is implicit in [JW,

§2]. It shows that (with a few exceptions) valuations can be recognized inside the maximal pro-2 Galois group.

PROPOSITION 1.4: *Let K be a field of characteristic $\neq 2$, let A be a free abelian pro-2 group (i.e., $A \cong \mathbb{Z}_2^m$ for some cardinal m) and let $\bar{G} \not\cong \mathbb{Z}/2\mathbb{Z}, 1$ be a pro-2 group. Then the following conditions are equivalent:*

(a) $\mathcal{G}(K_q/K) \cong A \rtimes \bar{G}$;

(b) $\mathcal{G}(K_q/K) \cong A \rtimes \bar{G}$ *and the involutions in* $\bar{G}$ *act on* A *by inversion;*

(c) K *is 2-henselian with respect to a valuation* v *such that* $\dim_{\mathbb{F}_2} \Gamma_v/2\Gamma_v = \operatorname{rank}(A)$ *and such that* $\mathcal{G}((\bar{K}_v)_q/\bar{K}_v) \cong \bar{G}$ *and* $\operatorname{char} \bar{K}_v \neq 2$.

If $\bar{G} \cong \mathbb{Z}/2\mathbb{Z}$ *then (c) implies (a) and (b).*

Proof: (a)$\Rightarrow$(b): Let ε be an involution ($\neq 1$) in $\mathcal{G}(K_q/K)$. By [B, Satz 8, Kor. 3], $\operatorname{char} K = 0$ and the restriction of ε to $\mathcal{G}(\mathbb{Q}_q/\mathbb{Q})$ is conjugate to the complex conjugation. Therefore it acts on the 2^nth roots of unity by inversion. It follows from [JW, Th. 2.2(iii)] that ε acts on A by inversion.

(b)$\Rightarrow$(a): Trivial.

(a)$\Rightarrow$(c): This is contained in [JW, Th. 2.5] (and its proof).

(c)$\Rightarrow$(a): Apply Lemma 1.1 with $p = 2$. ∎

Remark: A complete description of the action of $\bar{G}$ on A is given in [JW, Th. 2.3]. This, however, will not be needed in the present work. ∎

Convention: In light of Proposition 1.4, whenever we consider in the sequel semi-direct products of groups, we assume that the action of the involutions is by inversion. ∎

2. The chain length of a group

Denote the set of all involutions ($\neq 1$) of a profinite group G by $\operatorname{Inv}(G)$. We define the **chain length** $\operatorname{cl}(G)$ of a profinite group G to be the supremum of all $n \in \mathbb{N}$ for which there exist open subgroups $G_0, \ldots, G_n$ of G of index ≤ 2 satisfying $\operatorname{Inv}(G_0) \subset \cdots \subset \operatorname{Inv}(G_n)$. Also recall that the **chain length** $\operatorname{cl}(K)$ of a field K is the supremum of all $n \in \mathbb{N}$ for which there exist $a_0, \ldots, a_n \in K$ such that $H(a_0) \subset \cdots \subset H(a_n)$ (where $H(a)$ is the set of all orderings on K containing a.) In the special case where G is a maximal pro-2 Galois group of a field, parts (a), (b), (c) and (d) of the following lemma essentially correspond to [L, Prop. 8.6(1), Th. 8.28, Th. 8.27 and Prop. 8.6(2)], respectively.

LEMMA 2.1: *Let G be a pro-2 group containing an open subgroup G' of index ≤ 2 such that* $\mathrm{Inv}(G') = \emptyset$.

(a) *If G is generated by involutions and* $\mathrm{cl}(G) = 1$ *then* $G \cong \mathbb{Z}/2\mathbb{Z}$;

(b) *If* $G = \Gamma_1 *_2 \cdots *_2 \Gamma_m$ *then* $\mathrm{cl}(G) = \sum_{i=1}^m \mathrm{cl}(\Gamma_i)$;

(c) *If $G = A \rtimes H$ where A is a free abelian pro-2 group and* $\mathrm{cl}(H) \geq 2$ *then* $\mathrm{cl}(G) = \mathrm{cl}(H)$;

(d) *If $G = A \rtimes \mathbb{Z}/2\mathbb{Z}$ where A is a non-trivial free abelian pro-2 group then* $\mathrm{cl}(G) = 2$;

(e) $\mathrm{cl}(G) \leq \mathrm{rank}(G)$;

(f) *If K is a field then* $\mathrm{cl}(K) = \mathrm{cl}(G(K)) = \mathrm{cl}(\mathcal{G}(K_q/K))$.

Proof: (a) Let $\Phi(G)$ be the Frattini subgroup of G [FJ, §20.1] and let $\rho: G \to \bar{G} = G/\Phi(G)$ be the natural epimorphism. If $G \not\cong \mathbb{Z}/2\mathbb{Z}$ is generated by involutions then $\mathrm{rank}(\bar{G}) = \mathrm{rank}(G) \geq 2$ by [FJ, Lemma 20.36]. Since $\bar{G}$ is generated by $\rho(\mathrm{Inv}(G))$, there exist $\varepsilon_1, \varepsilon_2 \in \mathrm{Inv}(G)$ such that $\rho(\varepsilon_1) \neq \rho(\varepsilon_2)$. But $\Phi(G)$ is the intersection of all open subgroups of G of index 2. Hence there exists such a subgroup G_1 that contains just one of $\varepsilon_1, \varepsilon_2$. Then $\emptyset = \mathrm{Inv}(G') \subset \mathrm{Inv}(G_1) \subset \mathrm{Inv}(G)$, so $\mathrm{cl}(G) \geq 2$.

(b) Denote the set of all open subgroups of G of index ≤ 2 by $Q(G)$. By the universal property of G, the map $H \mapsto (H \cap \Gamma_1, \ldots, H \cap \Gamma_m)$ is a bijection between $Q(G)$ and $Q(\Gamma_1) \times \cdots \times Q(\Gamma_m)$. Partially order $Q(G)$ by the relation $\mathrm{Inv}(H) \subseteq \mathrm{Inv}(H')$ for $H, H' \in Q(G)$, and similarly for $Q(\Gamma_i)$, $i = 1, \ldots, m$. Also equip $Q(\Gamma_1) \times \cdots \times Q(\Gamma_m)$ with the product partial order. Clearly $\mathrm{Inv}(H) \subseteq \mathrm{Inv}(H')$ implies that $\mathrm{Inv}(H \cap \Gamma_i) \subseteq \mathrm{Inv}(H' \cap \Gamma_i)$, $i = 1, \ldots, m$. The converse also holds since $\mathrm{Inv}(G) = \bigcup_{i=1}^m \bigcup_{g \in G} \mathrm{Inv}(\Gamma_i)^g$ by [HR1, Th. A'] and since H, H' are normal in G. Therefore the above bijection is an isomorphism of partially ordered sets, whence our assertion.

(c) Let $\pi: G \to H$ be a splitting epimorphism with $\mathrm{Ker}(\pi) = A$. Identify H with a closed subgroup of G via a section of π. We have $\mathrm{Inv}(G) = A\mathrm{Inv}(H)$. If $H_0, \ldots, H_n$ are open subgroups of H of index ≤ 2 such that $\mathrm{Inv}(H_0) \subset \cdots \subset \mathrm{Inv}(H_n)$ then $G_i = AH_i$, $i = 0, \ldots, n$, are subgroups of G of index ≤ 2 satisfying $\mathrm{Inv}(G_0) \subset \cdots \subset \mathrm{Inv}(G_n)$. Consequently $\mathrm{cl}(H) \leq \mathrm{cl}(G)$. If $\mathrm{cl}(G) \leq 2$ then we are done. So assume that $\mathrm{cl}(G) \geq 3$.

To prove that $\mathrm{cl}(H) \geq \mathrm{cl}(G)$, let $G_0, \ldots, G_n$, $n \geq 3$, be open subgroups of G of index ≤ 2 such that $\mathrm{Inv}(G_0) \subset \cdots \subset \mathrm{Inv}(G_n)$. It suffices to show that $A \subseteq G_i$ for all i, since then $\mathrm{Inv}(G_i) = A\mathrm{Inv}(\pi(G_i))$, and hence $\mathrm{Inv}(\pi(G_0)) \subset$

$\cdots \subset \mathrm{Inv}(\pi(G_n))$.

Consider first the case when $i \le 1$. If $A \not\subseteq G_i$ we choose $a \in A \smallsetminus G_i$, $\varepsilon \in \mathrm{Inv}(G_{i-1}) \smallsetminus G_i$ and $\delta \in \mathrm{Inv}(G_{i+2}) \smallsetminus G_{i+1}$. Then $a\varepsilon \in \mathrm{Inv}(G_i) \subseteq G_{i+1}$, so $a \in G_{i+1}$. Since $\delta \notin G_i$ we have $a\delta \in \mathrm{Inv}(G_i) \subseteq G_{i+1}$. This yields the contradiction $\delta \in G_{i+1}$. Thus $A \subseteq G_0, G_1$.

Next let $2 \le i \le n$. Fix $\varepsilon \in \mathrm{Inv}(G_1)$ ($\subseteq G_i$) to obtain from what we have just proved that $A\varepsilon \subseteq \mathrm{Inv}(G_1)$. Therefore $A = (A\varepsilon)\varepsilon \subseteq \mathrm{Inv}(G_1)\varepsilon \subseteq G_i$, as required.

(d) Write $A = B \times \mathbb{Z}_2$ with B a free abelian pro-2 group. Then

$$A \rtimes \mathbb{Z}/2\mathbb{Z} = (B \times \mathbb{Z}_2) \rtimes \mathbb{Z}/2\mathbb{Z} \cong B \rtimes (\mathbb{Z}_2 \rtimes \mathbb{Z}/2\mathbb{Z}) \cong B \rtimes (\mathbb{Z}/2\mathbb{Z} *_2 \mathbb{Z}/2\mathbb{Z}),$$

so the assertion follows from (b) and (c).

(e) Let $\Phi(G)$, $\bar{G}$ and ρ be as in the proof of (a). We have $\bar{G} \cong (\mathbb{Z}/2\mathbb{Z})^I$ for a set I with $|I| = \mathrm{rank}(G)$ [FJ, Lemma 20.36]. Since $\Phi(G) \le G'$, the involutions in G are mapped by ρ to involutions ($\neq 1$) in $\bar{G}$. Now let G_1, G_2 be open subgroups of G of index ≤ 2 such that $\mathrm{Inv}(G_1) \subset \mathrm{Inv}(G_2)$. Then $\Phi(G) \le G_1$, so taking $\varepsilon \in \mathrm{Inv}(G_2) \smallsetminus G_1$ we have $\rho(\varepsilon) \notin \rho(G_1)$. Hence $\langle \rho(\mathrm{Inv}(G_1)) \rangle \subset \langle \rho(\mathrm{Inv}(G_2)) \rangle$. Conclude that $\mathrm{cl}(G) \le \dim_{\mathbb{F}_2} \bar{G} = \mathrm{rank}(G)$.

(f) This follows from Artin-Schreier's theory and its relative pro-2 version [B, §4]. ∎

Remark 2.2: If $G = \mathcal{G}(K_q/K)$ for a field K then $G' = \mathcal{G}(K_q/K(\sqrt{-1}))$ has index ≤ 2 in G and $\mathrm{Inv}(G') = \emptyset$, by [B, Satz 8, Kor. 3]. Therefore Lemma 2.1 applies to G. Also, recall that K is pythagorean if and only if G is generated by involutions [B, §3, Kor. 2 and §2, Satz 6]. Therefore, in this case G' can be intrinsically defined as the closed subgroup of G generated by all products of two involutions. Equivalently, G' is the unique open subgroup of G of index 2 for which $\mathrm{Inv}(G') = \emptyset$. ∎

3. Galois groups of pythagorean fields

Pythagorean fields of finite chain length have been extensively studied by Marshall [M], Jacob [J], Mináč [Mi], Craven [C], and others and their structure is well understood. Specifically, let $\mathcal{C}$ be the minimal collection of isomorphism types of pro-2 groups such that

(i) $\mathbb{Z}/2\mathbb{Z} \in \mathcal{C}$;

(ii) If $G_1, \ldots, G_m \in \mathcal{C}$ then $G_1 *_2 \cdots *_2 G_m \in \mathcal{C}$;

(iii) If $H \in \mathcal{C}$ and if A is a free abelian pro-2 group then $A \rtimes H \in \mathcal{C}$.

The following result is of fundamental importance:

THEOREM 3.1: *The following conditions on a pro-2 group G are equivalent:*

(a) $G \cong G(K)$ *for some pythagorean field K of finite chain length;*

(b) $G \cong \mathcal{G}(K_q/K)$ *for some pythagorean field K of finite chain length;*

(c) $G \in \mathcal{C}$.

Proof: The implication (a)⇒(b) is trivial, while the implication (b)⇒(c) is proved by Mináč [Mi]. To prove that (c)⇒(a), let $\mathcal{D}$ be the collection of all groups that satisfy (a). Clearly, $\mathbb{Z}/2\mathbb{Z} = G(\mathbb{R}) \in \mathcal{D}$. Also, if $G_1, \ldots, G_m$ are pro-2 groups generated by involutions then so is $G_1 *_2 \cdots *_2 G_m$. It follows from Proposition 1.3 and Lemma 2.1(b)(f) that $\mathcal{D}$ is closed under taking free pro-2 products. Finally, if $H \in \mathcal{D}$ and if A is a free abelian pro-2 group then the products $a\varepsilon$, where $a \in A$ and $\varepsilon \in \mathrm{Inv}(H)$, are involutions that generate $A \rtimes G$. Use this together with Lemma 1.2(a) and Lemma 2.1(c)(d) to obtain that $A \rtimes H \in \mathcal{D}$. Conclude that $\mathcal{C} \subseteq \mathcal{D}$, as asserted. ∎

Unfortunately, the above recursive presentation of $G \in \mathcal{C}$ is not unique: one can of course permute $G_1, \ldots, G_m$ in (ii), or use the isomorphisms $\mathbb{Z}_2 \rtimes \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} *_2 \mathbb{Z}/2\mathbb{Z}$ and $A \rtimes (B \rtimes H) \cong (A \times B) \rtimes H$ for free abelian pro-2 groups A and B and for a pro-2 group H. However, as our next result shows, apart from that the construction is unique.

Call a pro-2 group $H \neq 1$ **decomposable** if it can be written as $H_1 *_2 H_2$, with $H_1, H_2 \neq 1$ pro-2 groups. Otherwise call it **indecomposable.** Let $Z(H)$ denote the center of H. For every $G \in \mathcal{C}$ let G' be the unique open subgroup of G such that $(G : G') = 2$ and $\mathrm{Inv}(G') = \emptyset$ (Remark 2.2).

PROPOSITION 3.2: *Let $\mathbb{Z}/2\mathbb{Z} \ncong G \in \mathcal{C}$.*

(a) *There exists a free abelian pro-2 group A together with indecomposable groups $H_1, \ldots, H_m \in \mathcal{C}$, $2 \leq m < \infty$, such that $G \cong A \rtimes (H_1 *_2 \cdots *_2 H_m)$ and $\mathrm{cl}(H_1), \ldots, \mathrm{cl}(H_m) < \mathrm{cl}(G)$.*

(b) *This presentation of G is unique up to a permutation of $H_1, \ldots, H_m$.*

(c) *G is indecomposable if and only if $A \neq 1$ in the presentation in (a).*

For the proof we need a few lemmas.

LEMMA 3.3: *Suppose that $G = A \rtimes H$, where A is a free abelian pro-2 group, $H = H_1 *_2 \cdots *_2 H_m$ and $H_1, \ldots, H_m \neq 1$. If G is the maximal pro-2 Galois group of a pythagorean field then so are H, $H_1, \ldots, H_m$.*

Proof: Since H, $H_1, \ldots, H_m$ are closed subgroups of G they are also maximal pro-2 Galois groups of fields. On the other hand, since H, $H_1, \ldots, H_m$ are quotients of G, they are generated by involutions. Hence the above fields are pythagorean. ∎

LEMMA 3.4: *Suppose that $G = A \rtimes H \in \mathcal{C}$, where A is a free abelian pro-2 group, $H = H_1 *_2 \cdots *_2 H_m$, $H_1, \ldots, H_m \neq 1$ and $2 \leq m < \infty$. Then:*

(a) *$H, H_1, \ldots, H_m \in \mathcal{C}$ and $\mathrm{cl}(H_1), \ldots, \mathrm{cl}(H_m) < \mathrm{cl}(G)$;*
(b) *$Z(G') = A \times Z(H')$;*
(c) *If $Z(H') \neq 1$ then $m = 2$ and $H_1 \cong H_2 \cong \mathbb{Z}/2\mathbb{Z}$;*
(d) *If $m = 2$ and $H_1 \cong H_2 \cong \mathbb{Z}/2\mathbb{Z}$, then $Z(H') = H' \cong \mathbb{Z}_2$ and $G/Z(G') \cong \mathbb{Z}/2\mathbb{Z}$;*

Proof: (a) By Lemma 2.1(b)(c), $\mathrm{cl}(H_1), \ldots, \mathrm{cl}(H_m) < \mathrm{cl}(G) < \infty$. Together with Lemma 3.3 this gives that $H, H_1, \ldots, H_m \in \mathcal{C}$.
(b) As $(G : AH') = 2$ and AH' contains no involutions, $G' = AH'$. Furthermore, H' is generated by products of two involutions. Hence it acts trivially on A, whence $G' = A \times H'$. Thus $Z(G') = A \times Z(H')$.
(c), (d) Use Kurosh subgroup theorem for open subgroups of free pro-2 products [BiNW] to decompose H' as a free pro-2 product

$$H' = \textstyle\coprod^{(2)}_{1 \leq i \leq m} \coprod^{(2)}_{\sigma \in \Sigma(i)} (H' \cap H_i^\sigma) *_2 \hat{F} \ ,$$

where for each $1 \leq i \leq m$, $\Sigma(i) \subseteq H$, $H = \bigcup_{\sigma \in \Sigma(i)} H_i \sigma H'$, and where $\hat{F}$ is a free pro-2 group of rank $\sum_{i=1}^m [(H : H') - |\Sigma(i)|] - (H : H') + 1$. Since $(H : H') = 2$ and $H_i \not\subseteq H'$, we have $H_i \sigma H' = H_i H' \sigma = H\sigma = H$, whence $|\Sigma(i)| = 1$ for all i. It follows that H' decomposes as $(H' \cap H_1)^{\sigma_1} *_2 \cdots *_2 (H' \cap H_m)^{\sigma_m} *_2 \hat{F}$, where $\sigma_1, \ldots, \sigma_m \in H$ and $\mathrm{rank}(\hat{F}) = m - 1 \geq 1$. We can further decompose $\hat{F}$ as the free pro-2 product of $m - 1$ copies of $\mathbb{Z}_2$.

Now suppose that $Z(H') \neq 1$. Then, by [HR1, Th. A'], just one free factor in this decomposition of H' is non-trivial. Therefore $H' \cap H_1 = \cdots = H' \cap H_m = 1$ and $m = 2$, whence (c).

To prove (d), suppose that $m = 2$ and $H_1 \cong H_2 \cong \mathbb{Z}/2\mathbb{Z}$. Then $H' = \hat{F} \cong \mathbb{Z}_2$. Therefore, (b) implies that $G/Z(G') \cong H/Z(H') = H/H' \cong \mathbb{Z}/2\mathbb{Z}$. ∎

Proof of Proposition 3.2(a): Every group $H \in \mathcal{C}$ can be constructed in a finite number of steps of the form (i)–(iii). Denote the minimal number of steps required by $n(H)$. We first prove that $G \cong A \rtimes H$ for some free abelian pro-2 group A and for some group $H \in \mathcal{C}$ which is either of order 2 or is decomposable. If G itself is decomposable, then we take $A = 1$ and $G = H$. So suppose that G is indecomposable. Since $G \not\cong \mathbb{Z}/2\mathbb{Z}$, the last of $n(G)$ steps in a construction of G cannot be of the form (i) or (ii). Hence $G \cong A \rtimes H$, where $A \neq 1$ is a free abelian pro-2 group, $H \in \mathcal{C}$ and $n(H) = n(G) - 1$. Assume by contradiction that H is not of order 2 and is indecomposable. The same argument shows that $H \cong \bar{A} \rtimes \bar{H}$ for a free abelian pro-2 group $\bar{A}$ and a group $\bar{H} \in \mathcal{C}$ such that $n(\bar{H}) = n(H) - 1$. Then $G \cong (A \times \bar{A}) \rtimes \bar{H}$ is a presentation of G which requires only $n(\bar{H}) + 1 = n(G) - 1$ steps. This contradiction shows that H is indeed either of order 2 or is decomposable.

In the first case $A \neq 1$, because $G \not\cong \mathbb{Z}/2\mathbb{Z}$. Hence we get as in the proof of Lemma 2.1(d) that $G \cong B \rtimes (\mathbb{Z}/2\mathbb{Z} *_2 \mathbb{Z}/2\mathbb{Z})$ for some free abelian pro-2 group B. In the second case we use Lemma 2.1(b) to write $H = H_1 *_2 \cdots *_2 H_m$, with $H_1, \ldots, H_m$ indecomposable and $2 \leq m < \infty$. By Lemma 3.4(a), $H_1, \ldots, H_m \in \mathcal{C}$ and $\mathrm{cl}(H_1), \ldots, \mathrm{cl}(H_m) < \mathrm{cl}(G)$.

Proof of Proposition 3.2(c): Suppose that $A \neq 1$ and $G = G_1 *_2 G_2$ with $G_1, G_2 \neq 1$. Apply Lemma 3.4 with respect to the decomposition $G = 1 \rtimes (G_1 *_2 G_2)$ to obtain that either $Z(G') = 1$ or both $Z(G') \cong \mathbb{Z}_2$ and $G/Z(G') \cong \mathbb{Z}/2\mathbb{Z}$. On the other hand, apply Lemma 3.4 with respect to the decomposition $G \cong A \rtimes (H_1 *_2 \cdots *_2 H_m)$, to obtain that either $Z(G') = A$ or $Z(G') \cong A \times \mathbb{Z}_2$. However $Z(G') = A$ is impossible, since it implies that both $Z(G') \neq 1$ and $G/Z(G') \cong H_1 *_2 \cdots *_2 H_m \not\cong \mathbb{Z}/2\mathbb{Z}$. Conclude that $Z(G') \cong A \times \mathbb{Z}_2$, and therefore $A = 1$ contrary to the assumption. The converse implication is trivial.

LEMMA 3.5: *Let $G \in \mathcal{C}$ be indecomposable. There exists a direct system G_λ, $\lambda \in \Lambda$, ordered by inclusion, of finitely generated indecomposable groups in $\mathcal{C}$ such that $G = \langle G_\lambda \mid \lambda \in \Lambda \rangle$.*

Proof: We use induction on $\mathrm{cl}(G)$. If $\mathrm{cl}(G) = 1$ then $G \cong \mathbb{Z}/2\mathbb{Z}$ by Lemma 2.1(a), so the assertion is clear. Otherwise $G \not\cong \mathbb{Z}/2\mathbb{Z}$, and therefore G is presented as in Proposition 3.2(a), with $A \neq 1$. In light of Lemma 3.4(a) we may assume that systems $H_{i,\lambda(i)}$, $\lambda(i) \in \Lambda(i)$, have already been constructed for H_i, $1 \leq i \leq m$. Take G_λ, $\lambda \in \Lambda$, to be the collection of all closed subgroups

$A_0\langle H_{1,\lambda(1)},\ldots,H_{m,\lambda(m)}\rangle \cong A_0\rtimes(H_{1,\lambda(1)} *_2 \cdots *_2 H_{m,\lambda(m)})$ (cf. [HR3, Cor. 5.4]) of G with $A_0 \neq 1$ a finitely generated subgroup of A. These groups are indecomposable by Proposition 3.2(c) and generate G. ∎

LEMMA 3.6: *Assume that $G = G_1 *_2 \cdots *_2 G_n = H_1 *_2 \cdots *_2 H_m$, with $G_1,\ldots,G_n$, $H_1,\ldots,H_m \in \mathcal{C}$ indecomposable. Then $n = m$ and for some permutation π of $\{1,\ldots,n\}$, G_i is conjugate to $H_{\pi(i)}$, $i = 1,\ldots,n$.*

Proof: Use Lemma 3.5 to construct for all $1 \le i \le n$ and all $1 \le j \le m$ direct systems $G_{i,\lambda}$, $\lambda \in \Lambda(i)$ and $H_{j,\mu}$, $\mu \in M(j)$, of finitely generated indecomposable groups in $\mathcal{C}$ such that $G_i = \langle G_{i,\lambda} |\ \lambda \in \Lambda(i)\rangle$ and $H_j = \langle H_{j,\mu} |\ \mu \in M(j)\rangle$.

Fix $1 \le i \le n$ and $\lambda \in \Lambda(i)$. By Kurosh subgroup theorem for finitely generated closed subgroups of free pro-2 products ([H, Th. 9.7], [HR2, Th. 4.4], [Me]),

$$G_{i,\lambda} = \textstyle\coprod^{(2)}_{1\le j\le m} \coprod^{(2)}_{\sigma\in\Sigma(i,j,\lambda)} (G_{i,\lambda} \cap H_j^\sigma) *_2 \hat{F}_{i,\lambda}\ ,$$

where $\hat{F}_{i,\lambda}$ is a free pro-2 group and $G = \dot{\bigcup}_{\sigma\in\Sigma(i,j,\lambda)} H_j\sigma G_{i,\lambda}$ for all $1 \le j \le m$. Since $G_{i,\lambda}$ is generated by involutions, so is its quotient $\hat{F}_{i,\lambda}$, hence $\hat{F}_{i,\lambda} = 1$. As $G_{i,\lambda}$ is indecomposable, there is precisely one pair $1 \le j = j(i,\lambda) \le m$, $\sigma = \sigma(i,\lambda) \in \Sigma(i,j,\lambda)$ for which $G_{i,\lambda} \cap H_j^\sigma \neq 1$, and in fact $G_{i,\lambda} \le H_{j(i,\lambda)}^{\sigma(i,\lambda)}$. But the $G_{i,\lambda}$, $\lambda \in \Lambda$, form a direct system and any two distinct conjugates of $H_1,\ldots,H_m$ have trivial intersection [HR1, Th. B']. Hence $j(i,\lambda)$ and $H_{j(i,\lambda)}^{\sigma(i,\lambda)}$ do not depend on λ. We may therefore write $j(i) = j(i,\lambda)$ and $\sigma(i) = \sigma(i,\lambda)$. Then $G_i = \langle G_{i,\lambda} |\ \lambda \in \Lambda(i)\rangle \le H_{j(i)}^{\sigma(i)}$.

Conversely, for each $1 \le j \le m$ the same argument yields $1 \le i = i(j) \le n$ and $\tau(j) \in G$ such that $H_j \le G_{i(j)}^{\tau(j)}$. We have $G_i \le H_{j(i)}^{\sigma(i)} \le G_{i(j(i))}^{\tau(j(i))\sigma(i)}$. Projecting into the direct product $G_1 \times \cdots \times G_m$, we get that $i = i(j(i))$ for all $1 \le i \le n$. Similarly, $j = j(i(j))$ for all $1 \le j \le m$. It follows that $n = m$. Without loss of generality, $j(i) = i$ and $i(j) = j$ for all $1 \le i,j \le n$. In particular, $G_i \le H_i^{\sigma(i)} \le G_i^{\tau(i)\sigma(i)}$ for all $1 \le i \le n$. By [HR1, Th. B'] again, we must have here equalities, so G_i and H_i are conjugate. ∎

Proof of Proposition 3.2(b): If $G/Z(G') \cong \mathbb{Z}/2\mathbb{Z}$ then certainly $Z(G') \neq A$. By Lemma 3.4, $m = 2$ and $H_1 \cong H_2 \cong \mathbb{Z}/2\mathbb{Z}$. Also, the isomorphism type of A is uniquely determined by $Z(G') \cong A \times \mathbb{Z}_2$. If on the other hand, $G/Z(G') \not\cong \mathbb{Z}/2\mathbb{Z}$ then by Lemma 3.4, $Z(G') = A$. Thus, in this case as well, G determines A, and hence also $H \cong G/A$. By Lemma 3.6, the groups $H_1,\ldots,H_m$ are determined inside H up to a permutation and conjugacy. ∎

4. Covers of fields by semi-orderings

We say that a semi-ordered field (K, S) is **quadratically semi-real closed** if it has no proper pro-2 extension to which S extends. By [Br1, Folg. 2.18] or [P, Th. 1.26], a semi-ordering S on a field K always extends to a 2-Sylow extension of K. We therefore have:

LEMMA 4.1: *A semi-ordered field (K, S) is semi-real closed if and only if it is quadratically semi-real closed and $G(K)$ is pro-2.*

LEMMA 4.2: *A subset S of a field K is a semi-ordering if and only if the following conditions hold:*

(i) $1 \in S$;
(ii) $K^2 S = S$;
(iii) $S \cap -S = \{0\}$;
(iv) $K = S \cup -S$;
(v) *Every (non-empty) sum of finitely many non-zero elements of S is non-zero.*

Moreover, (K, S) is quadratically semi-real closed if and only if in addition it satisfies:

(vi) $K^2 = \{x \in K \mid xS = S\}$.

Proof: The first assertion is straightforward. Also, a semi-ordered field (K, S) is quadratically semi-real closed exactly when S extends to an extension $K(\sqrt{x})$, $x \in K$, if and only if $x \in K^2$. By [Br1, Folg. 2.18], this is equivalent to (vi). ∎

4.3 Remarks: (a) Let (K, S) be a semi-ordered field. It is straightforward to check that (vi) holds if and only if $K \smallsetminus K^2 = -S \cdot S$.

(b) It follows from Lemma 4.1 and Lemma 4.2 that the classes of semi-ordered fields, quadratically semi-real closed fields and semi-real closed fields are elementary in the first-order language of rings augmented by a unary relation symbol S which is interpreted as a semi-ordering. ∎

From [Br1, Folg. 2.19d] we get:

COROLLARY 4.4: *A quadratically semi-real closed field is pythagorean.*

Now let S_i, $i \in I$, be a collection of semi-orderings on a field K. It is straightforward to check that $T = \bigcap_{i \in I} \{x \in K \mid xS_i = S_i\}$ is a preordering on K [L, Def. 1.1]. In this case we say that S_i, $i \in I$, form a **cover** of T. When $T = \sum K^2$

is the set of all sums of squares in K we say that S_i, $i \in I$, **cover** K. For example, if T is an arbitrary preordering on the field K, then the collection S_i, $i \in I$, of all orderings of K that contain T form a cover of T. Indeed, $T = \bigcap_{i\in I} S_i$ [L, Th. 1.6] and $S_i = \{x \in K \mid xS_i = S_i\}$ for all $i \in I$.

Definition: The **covering number** $\mathrm{cn}(T)$ of a preordering T on a field K is the minimal size (possibly ∞) of a cover of T. For a field K we set $\mathrm{cn}(K) = \mathrm{cn}(\sum K^2)$ and call it the **covering number of** K. ∎

4.5 Remarks: (a) Let K be a pythagorean field. Then $\mathrm{cn}(K) = 1$ if and only if K is quadratically semi-real closed (Lemma 4.2).

(b) For every semi-ordered field (K, S), Zorn's lemma yields a maximal extension $(\bar{K}, \bar{S})$, $\bar{K} \subseteq K_q$, such that $\bar{S} \cap K = S$. Use this fact together with [Br1, Folg. 2.18] to conclude that a collection S_i, $i \in I$, of semi-orderings on a pythagorean field K forms a cover if and only if $K = \bigcap_{i\in I} \bar{K}_i$ for every collection $(\bar{K}_i, \bar{S}_i)$, $i \in I$, of quadratically semi-real closed subextensions of K_q/K such that $\bar{S}_i \cap K = S_i$ for all $i \in I$.

(c) Suppose that the collection S_i, $i \in I$, is cover of K but that no proper subcollection of it is a cover. Then $S_{i_1} \neq aS_{i_2}$ whenever $i_1, i_2 \in I$, $i_1 \neq i_2$, and $a \in K$. Otherwise, $\{x \in K \mid xS_{i_1} = S_{i_1}\} = \{x \in K \mid xS_{i_2} = S_{i_2}\}$, hence S_i, $i \in I \smallsetminus \{i_2\}$, is also a cover of K. ∎

5. The main results

We first show that being semi-real closed is a Galois-theoretic property.

THEOREM 5.1: *Let K and L be fields.*

(a) *If $\mathcal{G}(K_q/K) \cong \mathcal{G}(L_q/L)$ with K pythagorean then $\mathrm{cn}(K) = \mathrm{cn}(L)$;*

(b) *If $\mathcal{G}(K_q/K) \cong \mathcal{G}(L_q/L)$ and K is quadratically semi-real closed then so is L;*

(c) *If $G(K) \cong G(L)$ and K is semi-real closed then so is L.*

Proof: For an arbitrary field K Kummer theory gives

$$K^\times/(K^\times)^2 \cong H^1(G(K)) \cong H^1(\mathcal{G}(K_q/K)) = \mathrm{Hom}(\mathcal{G}(K_q/K), \mathbb{Z}/2\mathbb{Z})$$

canonically (the cohomology groups taken with respect to the module $\mathbb{Z}/2\mathbb{Z}$ and the trivial actions and the homomorphisms being continuous.) Let ψ be the image of the square class of -1 in $H^1(\mathcal{G}(K_q/K))$ under this isomorphism. We express the fact that K has a cover S_i, $i \in I$, in terms of $H^1(\mathcal{G}(K_q/K))$ and ψ as follows: For each $i \in I$ let A_i be the subset of $H^1(\mathcal{G}(K_q/K))$ corresponding to the set of square classes in S_i. Then conditions (i)–(iv) of Lemma 4.2 say that $0 \in A_i$ and $H^1(\mathcal{G}(K_q/K)) = A_i \cup (\psi + A_i)$. To express in this way condition (v), we use the canonical cohomological representation of the Witt-Grothendieck ring by means of generators and relations [S, Satz 1.2.1] $\widehat{W}(K) \cong \mathbb{Z}[H^1(\mathcal{G}(K_q/K))]/J$, where J is the ideal generated by all formal sums (in the group ring) $\alpha + \beta - \gamma - \delta$ such that $\alpha, \beta, \gamma, \delta \in H^1(\mathcal{G}(K_q/K))$, $\alpha + \beta = \gamma + \delta$ in $H^1(\mathcal{G}(K_q/K))$ and $\alpha \cup \beta = \gamma \cup \delta$ in $H^2(\mathcal{G}(K_q/K))$. By Witt's decomposition theorem [P, Th. 10.4], condition (v) for S_i is thus equivalent to the following statement: For any $\alpha_1, \ldots, \alpha_n \in A_i$, the formal sum $\alpha_1 + \cdots + \alpha_n$ in $\mathbb{Z}[H^1(\mathcal{G}(K_q/K))]$ is not congruent to any formal sum $\beta_1 + \cdots + \beta_{n-2} + 0 + \psi$ modulo J. Also, in the above notation, S_i, $i \in I$, cover K if and only if $\bigcap_{i \in I} \{\alpha \in H^1(\mathcal{G}(K_q/K) \mid \alpha + A_i = A_i\} = \{0\}$.

Now if $\mathcal{G}(K_q/K)$ is generated by involutions then by [B, §2, Satz 6], one can recognize ψ as the only continuous homomorphism in $H^1(\mathcal{G}(K_q/K))$ with torsion-free kernel. Therefore for pythagorean fields the above information can be expressed in terms of $\mathcal{G}(K_q/K)$ alone. This proves (a).

(b) follows from (a), by Corollary 4.4 and Remark 4.5(a); (c) follows from (b) by Lemma 4.1. ∎

Let $G \cong \mathcal{G}(K_q/K)$ with K a pythagorean field. We define $\mathrm{cn}(G) = \mathrm{cn}(K)$, and call it the **covering number of** G. By Theorem 5.1(a) this definition is independent of the choice of K. From Theorem 3.1, Lemma 4.1, Corollary 4.4 and Remark 4.5(a) we obtain (with $\mathcal{C}$ as in §3):

Corollary 5.2: *The following conditions on a pro-2 group G are equivalent:*

(a) *G is the absolute Galois group of a semi-real closed field of finite chain length;*

(b) *G is the maximal pro-2 Galois group of a quadratically semi-real closed field of finite chain length;*

(c) *$G \in \mathcal{C}$ and $\mathrm{cn}(G) = 1$.*

To make this characterization effective, we now develop a method for the computation of $\mathrm{cn}(G)$, where $G \in \mathcal{C}$ is presented as in Proposition 3.2(a). This is accomplished in Proposition 5.6 and Proposition 5.7 below.

The following result is contained in [E, Cor. 4.4].

LEMMA 5.3: *Let $\bar{K}_1, \dots, \bar{K}_m$ be extensions of a field K of characteristic $\neq 2$ which are contained in K_q and assume that $\mathcal{G}(K_q/K) = \mathcal{G}(K_q/\bar{K}_1) *_2 \cdots *_2 \mathcal{G}(K_q/\bar{K}_m)$. Then:*

(a) $K^\times/(K^\times)^2 \cong \bar{K}_1^\times/(\bar{K}_1^\times)^2 \times \cdots \times \bar{K}_m^\times/(\bar{K}_m^\times)^2$ *canonically;*

(b) *A K-quadratic form that is $\bar{K}_i$-isotropic for all $1 \leq i \leq m$ is K-isotropic.*

LEMMA 5.4: *Let $\bar{K}_1, \dots, \bar{K}_m$ be extensions of a field K contained in K_q and assume that $\mathcal{G}(K_q/K) = \mathcal{G}(K_q/\bar{K}_1) *_2 \cdots *_2 \mathcal{G}(K_q/\bar{K}_m)$. Let S be a semi-ordering on K. Then S extends to a unique $\bar{K}_i$, $1 \leq i \leq m$.*

Proof: To prove the existence of such an extension it suffices by [P, Lemma 1.24] to find $1 \leq i \leq m$ such that every quadratic form with coefficients in S is $\bar{K}_i$-anisotropic. Assume that for each $1 \leq i \leq m$ there exists a $\bar{K}_i$-isotropic quadratic form φ_i with coefficients in S. Then the sum $\varphi_1 \perp \ldots \perp \varphi_m$ is $\bar{K}_i$-isotropic for all $1 \leq i \leq m$. By Lemma 5.3(b) it is K-isotropic (notice that since K admits a semi-ordering, char $K = 0$). This contradicts condition (v) of Lemma 4.2.

To prove the uniqueness, assume that $\bar{S}, \bar{S}'$ are semi-orderings on $\bar{K}_i, \bar{K}_{i'}$, respectively, where $1 \leq i, i' \leq m$, $i \neq i'$. We show that $\bar{S} \cap K \neq \bar{S}' \cap K$. Use Lemma 5.3(a) to obtain $a \in K^\times$ such that $a \equiv 1 \bmod (\bar{K}_i^\times)^2$ and $a \equiv -1 \bmod (\bar{K}_{i'}^\times)^2$. Then $a \in \bar{S}$ and $a \notin \bar{S}'$, as required. ∎

5.5 Remarks: (a) If S is an ordering then Lemma 5.4 asserts that every involution in $\mathcal{G}(K_q/K)$ is conjugate to an involution in a unique $\mathcal{G}(K_q/\bar{K}_i)$, $i = 1, \dots, m$ [B, Satz 8, Kor. 3]. This is proved by purely group-theoretic methods in [HR1, Th. A'].

(b) Suppose that $G \cong A \rtimes H$, where A is a free abelian pro-2 group, $H = H_1 *_2 \cdots *_2 H_m$ and $H_1, \dots, H_m \neq 1$. If G is a maximal pro-2 Galois group of a pythagorean field then so are $H, H_1, \dots, H_m$ (Lemma 3.3), hence $\mathrm{cn}(H)$, $\mathrm{cn}(H_1), \dots, \mathrm{cn}(H_m)$ are well-defined. Therefore the statements of the following two propositions make sense. ∎

PROPOSITION 5.6: *Let G be a maximal pro-2 Galois group of a pythagorean field, and suppose that $G = G_1 *_2 \cdots *_2 G_m$ for some pro-2 groups $G_1, \dots, G_m$. Then $\mathrm{cn}(G) = \mathrm{cn}(G_1) + \cdots + \mathrm{cn}(G_m)$.*

Proof: Let K be a pythagorean field with $G \cong \mathcal{G}(K_q/K)$ and let $\bar{K}_1, \dots, \bar{K}_m$ be the fixed fields in K_q of $G_1, \dots, G_m$, respectively. Since $G_1, \dots, G_m$ are quotients of G and K is pythagorean, so are $\bar{K}_1, \dots, \bar{K}_m$. The pythagoreanity of K also implies that $\operatorname{char} K = 0$. We need to show that $\operatorname{cn}(K) = \operatorname{cn}(\bar{K}_1) + \cdots + \operatorname{cn}(\bar{K}_m)$.

Take a cover S_i, $i \in I$, of K. For each $i \in I$ there exists a unique $1 \le \theta(i) \le m$ and a semi-ordering $\bar{S}_i$ on $\bar{K}_{\theta(i)}$ such that $S_i = K \cap \bar{S}_i$ (Lemma 5.4). We claim that for each $1 \le j \le m$, the semi-orderings $\bar{S}_i$, $i \in \theta^{-1}(j)$, form a cover of $\bar{K}_j$. Indeed, take $x \in \bar{K}_j^\times$ such that $x\bar{S}_i = \bar{S}_i$ for all $i \in \theta^{-1}(j)$. We need to show that $x \in \bar{K}_j^2$. By Lemma 5.3(a) we may assume that $x \in K^\times$ and that $x \in \bar{K}_l^2$ whenever $l \ne j$, $1 \le l \le m$. Then $x\bar{S}_i = \bar{S}_i$, hence $xS_i = S_i$, for all $i \in I$. Conclude that $x \in K^2$, as claimed. It follows that $\operatorname{cn}(K) \ge \operatorname{cn}(\bar{K}_1) + \cdots + \operatorname{cn}(\bar{K}_m)$.

To prove the converse inequality, take for each $1 \le j \le m$ a cover $\bar{S}_i$, $i \in I_j$, of $\bar{K}_j$ having $\operatorname{cn}(\bar{K}_j)$ elements. We show that the $\operatorname{cn}(\bar{K}_1) + \cdots + \operatorname{cn}(\bar{K}_m)$ semi-orderings $S_i = \bar{S}_i \cap K$, $i \in I = I_1 \mathbin{\dot\cup} \cdots \mathbin{\dot\cup} I_m$, cover K. Indeed take $x \in K$ such that $x(\bar{S}_i \cap K) = \bar{S}_i \cap K$ for every $i \in I$. Use Lemma 5.3(a) to obtain that $x\bar{S}_i = \bar{S}_i$ for every $i \in I$. Then $x \in \bar{K}_j^2$ for each $1 \le j \le m$. By Lemma 5.3(a) again, $x \in K^2$, as desired. ∎

For $x \in \mathbb{R}$, let $\lceil x \rceil$ be the smallest integer $\ge x$.

PROPOSITION 5.7: *Let G be a maximal pro-2 Galois group of a pythagorean field and suppose that $G = A \rtimes H$, with A a free abelian pro-2 group and $\operatorname{cn}(H) < \infty$. Then*

$$\operatorname{cn}(G) = \begin{cases} \lceil \operatorname{cn}(H)/2^{\operatorname{rank}(A)} \rceil & \operatorname{rank}(A) < \infty,\ (A, H) \ne (\mathbb{Z}_2, \mathbb{Z}/2\mathbb{Z}) \\ 2 & A \cong \mathbb{Z}_2,\ H \cong \mathbb{Z}/2\mathbb{Z} \\ 1 & \operatorname{rank}(A) = \infty\ . \end{cases}$$

Proof: CASE (I): $\operatorname{rank}(A) < \infty$ and $H \not\cong \mathbb{Z}/2\mathbb{Z}$. Let K be a pythagorean field with $G \cong \mathcal{G}(K_q/K)$. By Proposition 1.4, K is 2-henselian with respect to a valuation v such that $\dim_{\mathbb{F}_2} v(K^\times)/2v(K^\times) = \operatorname{rank}(A)$ and $\mathcal{G}((\bar{K}_v)_q/\bar{K}_v) \cong H$. We denote for simplicity $k = \bar{K}_v$ and observe that k is pythagorean. Choose $T \subset K^\times$ such that $1 \in T$ and such that the elements $v(t)$, $t \in T$, form a representatives system for $v(K^\times) \bmod 2v(K^\times)$. Then $|T| = 2^{\operatorname{rank}(A)}$. Also let U be the set of all units of K with respect to v and let $\bar{a}$ denote the residue of $a \in U$ in k. Note that any element of K can be written as ax^2t with $a \in U$, $x \in K$ and $t \in T$. By Hensel's lemma and since $\operatorname{char} k = 0$, the 1-units of K with respect to v are in K^2.

Now let S_i, $i \in I$, be a cover of K with $|I| = \mathrm{cn}(K) = \mathrm{cn}(G)$. For each $i \in I$ and $t \in T$, put $\varepsilon_{i,t} = 1$ if $t \in S_i$ and $\varepsilon_{i,t} = -1$ otherwise. The set $s(i,t) = \{\varepsilon_{i,t}\bar{a} |\ a \in U,\ at \in S_i\}$ is a semi-ordering on k by Springer's theorem [L, Th. 4.6]. We show that $s(i,t)$, $i \in I$, $t \in T$, cover k. Indeed, take $a \in U$ such that $\bar{a}s(i,t) = s(i,t)$ for all $i \in I$ and $t \in T$. If $b \in U$, $x \in K^\times$ and $t \in T$ satisfy $bx^2t \in S_i$, then $\varepsilon_{i,t}\bar{b} \in s(i,t)$, so $\varepsilon_{i,t}\overline{ab} \in s(i,t)$. Thus $abx^2t \in S_i$, proving that $aS_i = S_i$. It follows that $a \in K^2$, hence $\bar{a} \in k^2$, as desired. Conclude that $\mathrm{cn}(G) \times 2^{\mathrm{rank}(A)} = |I \times T| \geq \mathrm{cn}(k) = \mathrm{cn}(H)$ and therefore $\mathrm{cn}(G) \geq \lceil \mathrm{cn}(H)/2^{\mathrm{rank}(A)} \rceil$.

To complete the proof in this case, we construct a cover of K which consists of $n = \lceil \mathrm{cn}(H)/2^{\mathrm{rank}(A)} \rceil = \lceil \mathrm{cn}(k)/|T| \rceil$ elements. Let I be a set of cardinality n and fix $i_0 \in I$. Choose a subset T_0 of T containing 1 such that $\mathrm{cn}(k) = (n-1)|T| + |T_0|$. Let R be the set of all pairs $(i,t) \in I \times T$ such that either $i \neq i_0$ or both $i = i_0$ and $t \in T_0$. By assumption, k has a cover $s(i,t)$, $(i,t) \in R$. For $t \in T \smallsetminus T_0$ define $s(i_0,t)$ to be an ordering on k that is different from $s(i_0,1)$ (note that since $\mathcal{G}(k_q/k) \not\cong \mathbb{Z}/2\mathbb{Z}$, the pythagorean field k is not uniquely ordered, by [B, Satz 3]). In particular, $\bar{a}s(i_0,1) \neq s(i_0,t)$ for all $\bar{a} \in k$. By Remark 4.5(c) and since $\mathrm{cn}(k) < \infty$, this inequality in fact holds for all $1 \neq t \in T$.

For $i \in I$ denote

$$S_i = \{ax^2t |\ a \in U,\ x \in K,\ t \in T,\ \bar{a} \in s(i,t)\} \ .$$

Use again Springer's theorem to verify that S_i is a semi-ordering on K. We prove that S_i, $i \in I$, form a cover of K. To this end we take $b \in U$, $x \in K$ and $t \in T$ such that $bx^2tS_i = S_i$ for all $i \in I$, and show that $b \in K^2$ and $t = 1$. Indeed, for $a \in U$ we have under this condition that $\bar{a} \in s(i_0,1)$ if and only if $abt \in btS_{i_0} = S_{i_0}$. Therefore $\bar{b}s(i_0,1) = s(i_0,t)$, which can happen only when $t = 1$. Thus $bS_i = S_i$, so $\bar{b}s(i,t') = s(i,t')$ for all $i \in I$ and $t' \in T$. As $s(i,t')$, $(i,t') \in R$, cover k, this implies that $\bar{b} \in k^2$. By Hensel's lemma $b \in K^2$, as required.

Case (II): $\mathrm{rank}(A) = \infty$ and $H \not\cong \mathbb{Z}/2\mathbb{Z}$. As in the third paragraph of the proof of Case (I) (with $n = 1$ and $I = \{i_0\}$) one shows that $\mathrm{cn}(G) = 1$.

Case (III): $A \neq 1$ and $H \cong \mathbb{Z}/2\mathbb{Z}$. Write $A = B \times \mathbb{Z}_2$ with B free abelian pro-2. Then $A \rtimes H \cong B \rtimes (\mathbb{Z}_2 \rtimes \mathbb{Z}/2\mathbb{Z}) \cong B \rtimes (\mathbb{Z}/2\mathbb{Z} *_2 \mathbb{Z}/2\mathbb{Z})$. The group $\mathbb{Z}/2\mathbb{Z} *_2 \mathbb{Z}/2\mathbb{Z}$ can be realized as a maximal pro-2 Galois group of a pythagorean field (Theorem 3.1), and therefore Proposition 5.6 yields $\mathrm{cn}(\mathbb{Z}/2\mathbb{Z} *_2 \mathbb{Z}/2\mathbb{Z}) = 2$. We also have

$\mathrm{rank}(A) = \mathrm{rank}(B) + 1$. The preceding two cases (with A and H replaced by B and $\mathbb{Z}/2\mathbb{Z} *_2 \mathbb{Z}/2\mathbb{Z}$, respectively) give us that $\mathrm{cn}(G) = \lceil 2/2^{\mathrm{rank}(B)} \rceil = 1$ if $2 \leq \mathrm{rank}(A) < \infty$ and also $\mathrm{cn}(G) = 1$ if $\mathrm{rank}(A) = \infty$. Finally, if $A \cong \mathbb{Z}_2$ then $B = 1$ so $\mathrm{cn}(G) = 2$.

CASE (IV): $A = 1$, $H \cong \mathbb{Z}/2\mathbb{Z}$. Trivial. ∎

COROLLARY 5.8: *Let G be a maximal pro-2 Galois group of a pythagorean field. Then* $\mathrm{cn}(G) \leq \mathrm{cl}(G)$.

Proof: This is trivial when $\mathrm{cl}(G) = \infty$. If $\mathrm{cl}(G) < \infty$ then we may proceed by induction on the structure of $G \in \mathcal{C}$. For $G \cong \mathbb{Z}/2\mathbb{Z}$ one has $\mathrm{cn}(G) = \mathrm{cl}(G) = 1$. If $G = G_1 *_2 \cdots *_2 G_m$ and $\mathrm{cn}(G_i) \leq \mathrm{cl}(G_i)$, $i = 1, \ldots, m$ (see Remark 5.5(b)), then by Lemma 2.1(b) and by Proposition 5.6, $\mathrm{cn}(G) = \mathrm{cn}(G_1) + \cdots + \mathrm{cn}(G_m) \leq \mathrm{cl}(G_1) + \cdots + \mathrm{cl}(G_m) = \mathrm{cl}(G)$. Suppose next that $G \cong A \rtimes H$, where A is a free abelian pro-2 group, and that $\mathrm{cn}(H) \leq \mathrm{cl}(H)$ (again, $\mathrm{cn}(H)$ is well-defined by Remark 5.5(b)). Then $\mathrm{cn}(H) \leq \mathrm{cl}(G) < \infty$ by Lemma 2.1(c)(d). Hence we may apply Proposition 5.7. If $\mathrm{rank}(A) < \infty$ and $(A, H) \neq (\mathbb{Z}_2, \mathbb{Z}/2\mathbb{Z})$ then it gives $\mathrm{cn}(G) = \lceil \mathrm{cn}(H)/2^{\mathrm{rank}(A)} \rceil \leq \mathrm{cn}(H) \leq \mathrm{cl}(G)$. If $A \cong \mathbb{Z}_2$ and $H \cong \mathbb{Z}/2\mathbb{Z}$ then $\mathrm{cn}(G) = \mathrm{cl}(G) = 2$. Finally, if $\mathrm{rank}(A) = \infty$ then $\mathrm{cn}(K) = 1 \leq \mathrm{cl}(K)$. ∎

Conclusion: Let $G \in \mathcal{C}$. Then $\mathrm{cn}(G)$ can be recursively computed using Propositions 5.6 and 5.7. Applying Corollary 5.2, one can thus effectively determine whether G is the absolute Galois group of a semi-real closed field of finite chain length (i.e., whether $\mathrm{cn}(G) = 1$). Likewise one can list the finitely generated absolute Galois groups of semi-real closed fields according to increasing rank. The following table gives the 34 maximal pro-2 Galois groups of pythagorean fields of rank ≤ 6 and the associated covering numbers. Note that by Proposition 3.2(b) these groups are non-isomorphic. Out of them 11 correspond to semi-real closed fields. We denote here the free pro-2 product of e copies of $\mathbb{Z}/2\mathbb{Z}$ by D_e. ∎

$G = \mathcal{G}(K_q/K)$	$\mathrm{rank}(G)$	$\mathrm{cn}(K)$
D_1	1	1
D_2	2	2

$G = \mathcal{G}(K_q/K)$	rank(G)	cn(K)
$\mathbb{Z}_2 \rtimes D_2$	3	1
D_3	3	3
$\mathbb{Z}_2^2 \rtimes D_2$	4	1
$(\mathbb{Z}_2 \rtimes D_2) *_2 D_1$	4	2
$\mathbb{Z}_2 \rtimes D_3$	4	2
D_4	4	4
$\mathbb{Z}_2^2 \rtimes D_3$	5	1
$\mathbb{Z}_2^3 \rtimes D_2$	5	1
$\mathbb{Z}_2 \rtimes ((\mathbb{Z}_2 \rtimes D_2) *_2 D_1)$	5	1
$\mathbb{Z}_2 \rtimes D_4$	5	2
$(\mathbb{Z}_2^2 \rtimes D_2) *_2 D_1$	5	2
$(\mathbb{Z}_2 \rtimes D_2) *_2 D_2$	5	3
$(\mathbb{Z}_2 \rtimes D_3) *_2 D_1$	5	3
D_5	5	5
$\mathbb{Z}_2^2 \rtimes D_4$	6	1
$\mathbb{Z}_2^3 \rtimes D_3$	6	1
$\mathbb{Z}_2^4 \rtimes D_2$	6	1
$\mathbb{Z}_2 \rtimes ((\mathbb{Z}_2^2 \rtimes D_2) *_2 D_1)$	6	1
$\mathbb{Z}_2^2 \rtimes ((\mathbb{Z}_2 \rtimes D_2) *_2 D_1)$	6	1
$(\mathbb{Z}_2 \rtimes D_2) *_2 (\mathbb{Z}_2 \rtimes D_2)$	6	2
$(\mathbb{Z}_2^3 \rtimes D_2) *_2 D_1$	6	2
$(\mathbb{Z}_2 \rtimes ((\mathbb{Z}_2 \rtimes D_2) *_2 D_1)) *_2 D_1$	6	2
$(\mathbb{Z}_2^2 \rtimes D_3) *_2 D_1$	6	2
$(\mathbb{Z}_2^3 \rtimes D_2) *_2 D_1$	6	2
$\mathbb{Z}_2 \rtimes ((\mathbb{Z}_2 \rtimes D_2) *_2 D_2)$	6	2
$\mathbb{Z}_2 \rtimes ((\mathbb{Z}_2 \rtimes D_3) * D_1)$	6	2
$(\mathbb{Z}_2 \rtimes D_4) *_2 D_1$	6	3
$\mathbb{Z}_2 \rtimes D_5$	6	3
$(\mathbb{Z}_2^2 \rtimes D_2) *_2 D_2$	6	3
$(\mathbb{Z}_2 \rtimes D_2) *_2 D_3$	6	4
$(\mathbb{Z}_2 \rtimes D_3) *_2 D_2$	6	4
D_6	6	6

References

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

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

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

[BiNW] E. Binz, J. Neukirch and G.H. Wenzel, *A subgroup theorem for free products of pro-finite groups*, J. Algebra **19** (1971), 104–109.

[Br1] L. Bröcker, *Zur Theorie der quadratischen Formen über formal reellen Körpern*, Math. Ann. **210** (1974), 233–256.

[Br2] L. Bröcker, *Characterization of fans and hereditarily pythagorean fields*, Math. Z. **151** (1976), 149–163.

[Br3] L. Bröcker, *Über die Anzahl der Ordnungen eines kommutativen Körpers*, Arch. Math. **29** (1977), 458–464.

[C] T. Craven, *Characterizing Reduced Witt rings of Fields*, J. Algebra **53** (1978), 68–77.

[E] I. Efrat, *Local-global principles for Witt rings*, J. Pure Appl. Math., to appear.

[En] O. Endler, *Valuation Theory*, Springer, 1972.

[FJ] M. Fried and M. Jarden, *Field Arithmetic*, Ergebnisse der Mathematik III **11**, Springer, 1986.

[H] D. Haran, *On closed subgroups of free products of profinite groups*, Proc. London Math. Soc. (3) **55** (1987), 266–298.

[HR1] W.N. Herfort and L. Ribes, *Torsion elements and centralizers in free products of profinite groups*, J. reine angew. Math. **358** (1985), 155–161.

[HR2] W.N. Herfort and L. Ribes, *Subgroups of free pro-p products*, Math. Proc. Camb. Phil. Soc. **101** (1987), 197–206.

[HR3] W.N. Herfort and L. Ribes, *Frobenius subgroups of free products of prosolvable groups*, Monatshefte Math. **108** (1989), 165–182.

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

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

[JWd] B. Jacob and A. Wadsworth, *A new construction of noncrossed product algebras,* Trans. Amer. Math. Soc. **293** (1986), 693–721.

[K] M. Kula, *Fields with prescribed quadratic forms schemes,* Math. Z. **167** (1979), 201–212.

[L] T.Y. Lam, *Orderings, valuations and quadratic forms,* Conf. Board of the Mathematical Sciences AMS **52**, 1983.

[La] S. Lang, *Algebra,* Addison-Wesley, 1965.

[M] M. Marshall, *Spaces of orderings IV,* Canad. J. Math. **32** (1980), 603–627.

[Me] O.V. Melnikov, *Subgroups and homologies of free products of profinite groups,* Izvestiya Akad. Nauk SSSR, Ser. Mat. **53** (1989), 97–120 (Russian); Math. USSR Izvestiya **34** (1990), 97–119 (English translation).

[Mi] J. Mináč, *Galois groups of some 2-extensions of ordered fields,* C.R. Math. Rep. Acad. Sci. Canada **8** (1986), 103–108.

[P] A. Prestel, *Lectures on Formally Real Fields,* Lect. Notes Math. **1093**, Springer, 1984.

[R] L. Ribes, *Introduction to Profinite Groups and Galois Cohomology,* Queen's University, 1970.

[Ri] P. Ribenboim, *Théorie des valuations,* Les Presses de l'Université de Montréal, 1968.

[S] W. Scharlau, *Quadratische Formen und Galois Cohomologie,* Invent. math. **4** (1967), 238–264.