THE m–ORDERED REAL FREE GROUP

Antonio José Engler

RELATÓRIO TÉCNICO Nº 50/87

ABSTRACT. During the last years the study of the formally real fields has been a source of new interesting research. One of the most attractive aspects of these studies has been to find out the characteristics of the total Galois group of these fields attached to properties concerning the fact of being real.

Among the profinite groups the free profinite groups have appeared very frequently as the total Galois group of some fields ([BNW] , [D]). Haran and Jarden [HJ1] established the "real" analogue of the notion of a free profinite group. The aim of the present not is to examine closely a particular case of the real profinite groups; those having finitely many classes of involutions. Of course they are in connexion with fields having finitely many orderings. Of particular interest will be the pro–2–groups, as one can expect working on formally real fields.

The results of this paper have been announced at the Conference on Quadratic Forms and Real Algebraic Geometry, Corvallis, July 1986.

Universidade Estadual de Campinas
Instituto de Matemática, Estatística e Ciência da Computação
IMECC – UNICAMP
Caixa Postal 6065
13.081 - Campinas, SP
BRASIL

O conteúdo do presente Relatório Técnico é de única responsabilidade do autor.

Novembro – 1987

THE m-ORDERED REAL FREE GROUP

Antonio José Engler
IMECC - UNICAMP
Caixa Postal 6065
13.081 - Campinas, SP., Brasil

INTRODUCTION.

During the last years the study of the formally real fields has been a source of new interesting research. One of the most attractive aspects of these studies has been to find out the characteristics of the total Galois group of these fields attached to properties concerning the fact of being real.

Among the profinite groups the free profinite groups have appeared very frequently as the total Galois group of some fields ([BNW],[D]). Haran and Jarden [HJ1] established the "real" analogue of the notion of a free profinite group . The aim to the present note is to examine closely a particular case of the real profinite groups; those having finitely many classes of involutions. Of course they are in connexion with fields having finitely many orderings. Of particular interest will be the pro-2-groups, as one can expect working on formally real fields.

Notations.

Throughout this paper we assume that $\mathcal{C}$ is a class of finite groups that contains the subgroups and the quotients of groups in $\mathcal{C}$, and that is closed under extensions. We also assume that $\mathcal{C}$ contains the cyclic group of order 2. A pro-$\mathcal{C}$-group is a projective limit of groups in $\mathcal{C}$. As usual, if $\mathcal{C}$ is the class of groups having order a power of the prime number 2 we say pro-2-group instead of pro-$\mathcal{C}$-group.

All homomorphisms between pro-$\mathcal{C}$-groups are assumed to the continuos, and all subgroups are assumed to be closed. If S is a subset of a pro-$\mathcal{C}$-group G, $\langle S \rangle$ will denote the closed subgroup generated by S. For general facts about profinite groups, see [R].

Let B be a set, $F(B)$ will denote the free pro-$\mathcal{C}$-group on B, in the restricted sense (cf. [R]). Let $A_1,\dots,A_m$

be pro-$\mathcal{C}$-groups ; $\coprod_{i=1}^{m} A_i$ will always denote their free pro-$\mathcal{C}$-product (cf. [BNW]). For a field K, G(K) denotes its absolute Galois group.

Our definition of real free pro-$\mathcal{C}$-group is a particular case of [HJ1] (Definition 1.1).

DEFINITION: A pro-$\mathcal{C}$-group G is said to be m-ordered real free on a set B if the following conditions are satisfied:

(1) There is a subset C of G containing m involutions (i.e. every element of C has order 2).

(2) B is a subset of G, disjoint from C, convergent to 1. (i.e. every open normal subgroup of G contains all but finitely many elements of B).

(3) Every map I from $C \cup B$ into a pro-$\mathcal{C}$-group G', convergent to 1, such that $I(c)^2 = 1$ for every $c \in C$, can be extended to a unique homomorphism of G into G'.

1. THE REAL FREE m-ORDERED GROUP.

The existence and uniqueness of a real free m-ordered group is stated in [HJ1] (Lemma 1.3). First we will give two different characterizations of these groups. Actually we construct the real free m-ordered group.

THEOREM 1.1: Let G be a pro-$\mathcal{C}$-group, $m > 0$ a natural number and B be a subset of G. The following conditions are equivalent:

(A) G is a m-ordered real free group on B.

(B) There are $c_1,\dots,c_m$ distinct involutions of G such that $G \simeq \langle c_1\rangle \rtimes F(X)$, where $X = \{c_1c_2,\dots,c_1c_m\} \cup B \cup c_1Bc_1$. ($c_1Bc_1 = \{c_1Bc_1 \mid b \in B\}$, if $B \neq \emptyset$).

(c) $G \simeq \coprod_{i=1}^{m+1} A_i$, where $A_i = \langle c_i\rangle$ for $i = i,\dots,m$ and $A_{m+1} = F(B)$.

PROOF: To prove that (A) $\Longrightarrow$(B) it is enough to show that the group $\langle c_1\rangle \rtimes F(X)$ is a real free m-ordered group on B. Let $C = \{c_1,\dots,c_m\}$ and consider two new sets of simbols $\{c_1c_2,\dots,c_1c_{m+1}\}$ and $c_1Bc_1 = \{c_1bc_1 \mid b \in B\}$, in case of B be a non-void set. Now let F(X) be the usual free pro-$\mathcal{C}$-group on $X = \{c_1c_2,\dots,c_1c_m\} \cup B \cup c_1Bc_1$. Call φ the unique automorphism of F(X) such that $\varphi(c_1c_j) = (c_1c_j)^{-1}$, $j = 2,\dots,m$ and $\varphi(b) = c_1bc_1$, $\varphi(c_1bc_1) = b$, for every $b \in B$, if $B \neq \emptyset$. Clearly $\varphi^2 = 1$ and we will denote $\varphi(x) = c_1xc_1$, for every $x \in F(X)$. Let RF be the group $\{c_1^{\varepsilon}x \mid \varepsilon = 0,1;\ x \in F(X)\}$ where the operation is given in the obvious way. Clearly $RF = \langle c_1\rangle \rtimes F(X)$.

We claim that RF is the m-ordered real free pro-$\mathcal{C}$-group on B.

Let G' be a pro-$\mathcal{C}$-group and $I : C \cup B \longrightarrow G'$ be a map convergent to 1 such that $I(c)^2 = 1$ for every $c \in C$. We extend I to X setting $I(c_1c_j) = I(c_1)I(c_j)$, $j = 2,\dots,m$; $I(c_1bc_1) = I(c_1)\ I(b)\ I(c_1)$ for every $b \in B$, if $B \neq \emptyset$. This extension is convergent to 1 too . Let $f: F(X) \longrightarrow G'$ be the unique homomorphism extending I to $F(X)$. Since $f(c_1xc_1) = f(c_1)f(x)f(c_1)$ for every $x \in X$, by construction, it follows that $f(c_1xc_1) = f(c_1)f(x)f(c_1)$ for every $x \in F(X)$ too, since $f\circ$(conjugation by c_1) and (conjugation by $f(c_1)$)$\circ f$ must be equal by the uniqueness of the extension. Then we can extend f to a homomorphism from RF to G' by $f(c_1^{\varepsilon}x) = f(c_1^{\varepsilon})\,f(x)$ for $\varepsilon = 0,1$ and $x \in F(X)$. This homomorphisms is clearly the unique extension of I.

(A) $\Longrightarrow$ (C) For $j = 1,\dots,m$ let e_j be a generator of A_j and define $f_j : A_j \longrightarrow G$ by $f(e_j) = c_j$, where $C = \{c_1,\dots,c_m\}$. Let f_{m+1} be the unique homomorphism extending the identical map of B.

Let $G' = \coprod_{j=1}^{m+1} A_j$ and call $\psi_j : A_j \longrightarrow G'$ the natural maps of the product. By the universal property of G' there exists a unique homomorphism $g : G' \longrightarrow G$ such that $g\circ\psi_j = f_j$ for $j = 1,\dots,m+1$. On the other side there exists a unique homomorphism $h : G \longrightarrow G'$ such that $h(c_j) = \psi_j(e_j)$, $j = 1,\dots,m$ and $h(b) = \psi_{m+1}(b)$ for $b \in B$. A straightforward verification shows that h is an isomorphism.

(C) $\Longrightarrow$ (A) It is an imediate consequence of the universal property of the free product.

REMARKS: 1.2 By Corollary 3.2 of [HJ1] or by Theorem A' of [HR] the set C (according to the definition) is a complete system of representatives of the conjugacy classes of involutions in a real free pro-$\mathcal{C}$-group G. Hence G has exactly m conjugacy classes of involutions and that is the motivation of the expression "m-ordered" in our definition.

1.3 The m-ordered real free pro-$\mathcal{C}$-group on B will be denoted by RF(m,B). Of course RF(m,B) is the usual (restricted) free pro-$\mathcal{C}$-group if $m = 0$. We will constantly use the semidirect product representation $\mathrm{RF}(m,B) \simeq \simeq \langle c \rangle \rtimes F(m,B)$, where $c \in C$ and F(m,B) is the free pro-$\mathcal{C}$-group on the set X described in the Theorem 1.1.

1.4 Let F be the usual free pro-$\mathcal{C}$-group on a set X. If X is a finite set and $m < \#X$ is a natural number such that $\#X - m+1$ is even, then we construct a real free group RF(m,B) such that $F(m,B) = F$ (up to isomorphism). It is enough to consider a set B containing $1/2(\#X-m+1)$ elements and C a set of m involutions. For a non-finite set X we do not need any restriction on m to get RF(m,B) such that $F(m,B) = F$. We just consider X as the union of appropriate sets.

1.5 The notion of real free profinite groups has some importance in the theory of Pseudo Real Closed Fields. Haran and Jarden [HJ2] proved that the absolute Galois group of a Pseudo Real Closed Field is real projective and conversely, a real projective group is the absolute Galois group of some pseudo real closed field. ([HJ2], Theorem 10.4). On the other hand, every real free group is a real projective group ([HJ1], Corollary 3.3).

We combine these results in the following statements:

(A) The real free profinite group $RF(m,B)$ is real projective.

(B) There exists a field K such that $G(K)$ is isomorphic to $RF(m,B)$.

Observe that K is a formally real field whenever $m > 0$.

1.6 Let K be a field, G be a real projective profinite group and $f: G(K) \to G$ be an epimorphism such that for every involution $c \in G$ there is an involution $e \in G(K)$ such that $f(e) = c$ then the homomorphism f splits and there are closed subgroups of $G(K)$ isomorphic to G. Hence there are algebraic extensions L of K such that $G(L) \simeq G$.

2. THE SUBGROUPS AND THE QUOTIENTS OF $RF(m,B)$.

As in many other cases ([BNW], [LVDD]) we will prove that the open subgroups of a real free group are also real free.

PROPOSITION 2.1: (A) An open subgroup H of $RF(m,B)$ is isomorphic to $RF(m',B')$ for some m' and B'. If in addition, B is a non-finite set, then $B' = B$ could be chosen.

For index two subgroups we have the following more precise formulation:

(B) For every finite subset $B_o \subset B$ and $\{c_{i_1},\ldots,c_{i_r}\} \subset C$, $r \leq m$ there exists a unique open index 2 subgroup H of $RF(m,B)$ such that $B_o = \{b \in B \mid b \notin H\}$, $\{c_{i_1},\ldots,c_{i_r}\} = \{c \in C \mid c \notin H\}$ and $H \simeq RF(2(m-r),B_1)$, where $\#B_1 = \#B$ if B is a non-finite set and $\#B_1 = 2\#B + r$ in the finite case.

In the case of $r = m$, or equivalentely $H \cap C = \emptyset$, we have that $H \simeq F(m,B)$.

PROOF: The statement (A) follows directly from Kurosh's Theorem in [BNW] and (B) is a consequence of the universal property of the real free group and from the Theorem.

COROLLARY 2.2: Let K be a field such that $G(K)$ is isomorphic to $RF(m,B)$. Then K has exactly m distint orders and $G(K(i)) \simeq F(m,B)$ is a free profinite group.

(i is the square root of -1).

In the next result we consider a more general situation where a pro-$\mathcal{C}$-group G satisfies the following separation hypothesis:

Let G be a pro-$\mathcal{C}$-group that has exactly m classes of conjugacy of involutions. Let $I(G)$ be the set of the involutions of G, that we assume to be a closed subset of G, and let $c_1,\dots,c_m$ be a complete system of representatives of the classes of $I(G)$.

(SH) For every $c_{i_1},\dots,c_{i_r}, c_{i_{r+1}},\dots,c_{i_{r+s}}$ there is in index 2 subgroup H of G such that $c_{i_1},\dots,c_{i_r} \in H$ and $c_{i_{r+1}},\dots,c_{i_{r+s}} \notin H$.

PROPOSITION 2.3: Keeping the notations and the hypothesis just introduced above the following statements are true:

(A) Let $S_j = \langle \{c_j g c_j g^{-1} \mid g \in G\}\rangle$ and $T_j = \langle \{g c_j g^{-1} \mid g \in G\}\rangle$.

Then: (A1) S_j and T_j are normal subgroups of G and $T_j = \langle c_j\rangle \rtimes S_j$.

(A2) $S_j \subset H$ for every index 2 subgroup of G.

(A3) Let H be an index 2 subgroup of G such that $c_j \notin H$. If H' is a normal subgroup of H such that $S_j \subset H'$, then $\langle c_j\rangle \rtimes H'$ is a normal subgroup of G. If in addition $(H:H') = 2$ the converse is true.

(A4) $G/T_j \simeq H/S_j$ for every index 2 subgroup H of G and such that $c_j \notin H$.

(B) Let $S = \langle\{cc' \mid c, c' \in I(G)\}\rangle$ and $T = \langle\{c \mid c \in I(G)\}\rangle$. Then: (B1) S and T are normal subgroups of G and $S = \langle c\rangle \rtimes T$ for every $c \in I(G)$.

(B2) Let H be an index 2 subgroup of G such that $H \cap I(G) = \emptyset$. If H' is a normal subgroup of H such that $S \subset H'$, then $\langle c\rangle \rtimes H'$ is a normal subgroup of G. If in addition $(H:H') = 2$ the converse is true.

(B3) $G/T \simeq H/S$ for every index two subgroup H of G such that $H \cap I(G) = \emptyset$.

(C) Let $S(I) = S_1 S_2 \ldots S_m$. Then $T = \langle c_1\rangle \rtimes (\ldots(\langle c_m\rangle \rtimes S(I))\ldots)$, $T/S(I) \simeq (\mathbb{Z}/2\mathbb{Z})^m$ and $T/S(I) \subset Z(G/S(I))$ = the center of $G/S(I)$.

PROOF: It is a simple verification.

By Proposition 2.1 the real free group $RF(m,B)$ satisfies the hypothesis (HS) and we can improve the last result for this group.

PROPOSITION 2.4: With the same notations of the Proposition 2.3 we have:

(A) $RF(m,B)/T_j \simeq F(m,B)/S_j \simeq RF(m-1,B)$.

(B) $RF(m,B)/T \simeq F(m,B)/S \simeq F(B)$.

(C) $RF(m,B)/S(I) \simeq (\mathbb{Z}/2\mathbb{Z})^m \times F(B)$.

PROOF: Let $\pi: RF(m,B) \longrightarrow RF(m,B)/T$ be the canonical surjection. Observe that for $x,y \in C \cup B$, $x \neq y$, and either $x \notin C$ or $y \notin C$, there is an index two subgroup H of $HF(m,B)$ such that $c_j \in H$, $x \notin H$ and $y \in H$, by Proposition 2.1. Hence $xy^{-1} \notin H$, $T_j \subset H$ and then $xy^{-1} \notin$ $\notin T_j$. Thus the restriction of π to $(C-\{c_j\}) \cup B$ is injective. Let $\lambda: \pi(C-\{c_j\}) \cup B \longrightarrow G$ be a map convergent to 1 such that $\lambda(\pi(x))^2 = 1$ for every $x \in C-\{c_j\}$. Then, there exists a homomorphism $f: RF(m,B) \longrightarrow G$ whose restriction to $C \cup B$ is $\lambda \circ \pi$. Since $f(c_j) = 1$ it follows that $T_j \subset$ kernel (f). Let $\bar{f}: RF(m,B)/T_j \longrightarrow G$ be the morphism gived by $\bar{f}(gT_j) = f(g)$ for every $g \in RF(m,B)$. This morphism extends λ to $RF(m,B)/T_j$ and since f is unique and π is a surjection, $\bar{f}$ is also unique.

Statement B follows in the same way and the last one is a consequence of 2.3.

Next we introduce some notations: Let K be a formally real field and $c \in I(G(K))$ be an involution. Call $K(c)$ the intersection of those real closed fields that are conjugated to $Fix(c)$ = the fixed field of $\{1,c\}$. Let K^* be the Galois order closure of K, that is , the intersection of all real closures of K inside a fixed algebraic closure of K. Observe that $K^* = \cap K(c)$, for every $c \in$ $\in I(G(K))$. Finally, $K_1(c)$ denote the quadratic extension of $K(c)$ gived by the square root of -1. Observe that $K(c)$, $K_1(c)$ and K^* are Galois extensions of K. For every Galois extension $N|K$, $G(N,K)$ denotes its Galois group.

COROLLARY 2.5: For a field K such that $G(K) \simeq RF(m,B)$ let $C = \{c_1,\dots,c_m\}$ be a system of representatives of the conjugacy classes of involutions. Then:

(A) $G(K(c_j),K) \simeq RF(m-1,B)$ for every $j = i,\dots,m$.

(B) $G(K^*,K) \simeq F(B)$.

(C) $G(K_1(c_1) \cap K_1(c_2) \cap \dots \cap K_1(c_m), K) \simeq (\mathbb{Z}/2\mathbb{Z})^m \times F(B)$.

PROOF: The result follows from $G(K(c_j)) = T_j$, $G(K_1(c_j)) = S_j$, $G(K^*) = T$ and $G(K_1(c_1) \cap \dots \cap K_1(c_m)) \simeq S(I)$.

As a consequence of (B) we get:

COROLLARY 2.6: If $G(K) \simeq RF(m,B)$ then the direct product $(\hat{\mathbb{Z}})^B$ is a quotient of $G(K^*,K)$.

Now, fix a natural number $m > 0$ and a set B. Denote by $RF_2(m,B)$ the m-ordered real free pro-2-group, by $RF(p)$ the maximal pro-p-quotient of $RF(m,B)$ and by $F_p(B)$ the free pro-p-group on B.

PROPOSITION 2.7: For every prime number p we have:

(A) For $p \neq 2$, $RF(p) \simeq F_p(B)$.

(B) For $p = 2$, $RF(2) \simeq RF_2(m,B)$.

These isomorphisms are canonically defined.

PROOF: First we prove that $RF(2) \simeq RF_2(m,B)$. Let $g: RF(m,B) \longrightarrow RF(2)$ be the canonical projection and $f: RF(m,B) \longrightarrow RF_2(m,B)$ be the unique morphism induced by the identical map of $C \cup B$. Since $RF_2(m,B)$ is a pro-2-group we have that $\text{kernel}(g) \subset \text{kernel}(f)$. Let $\varphi: RF_2(m,B) \longrightarrow RF(2)$ be the unique morphism induced by the map $\varphi(x) = g(x)$, $x \in C \cup B$. Since $(\varphi \circ f)(x) = g(x)$ for every $x \in C \cup B$ it follows that $\varphi \circ f = g$. Hence $\text{kernel}(f) \subset \text{kernel}(g)$. Thus $\text{kernel}(f) = \text{kernel}(g)$ and φ is an isomorphism.

In the proof of $RF(p) \simeq F_p(B)$ we need to take care of the involutions. This is made by setting $f(c) = 1$ for every $c \in C$ in the above definition of f. We finish the proof as above.

In the Corollary 2.8 we established the "real" analogue of a well known fact about free profinite groups ([R], Proposition 3.2, pg. 225).

For a field K we denote by $K(p)$ its maximal p-extension.

COROLLARY 2.8: Let K be a field such that $G(K) \simeq RF(m,B)$. Then:

(A) For $p \neq 2$, $G(K(p),K) \simeq F_p(B)$.

(B) For $p = 2$, $G(K(2),K) \simeq RF_2(m,B)$.

COROLLARY 2.9: $RF_2(m,B)$ is a real projective profinite group.

PROOF: Let N be a normal subgroup of $RF(m,B)$ such that $RF(m,B)/N = RF_2(m,B)$ and let P be a 2-Sylow subgroup of $RF(m,B)$. We have that $(RF(m,B):N) = (RF(m,B):NP)(NP:N)$ and $(RF(m,B):P) = (RF(m,B):NP)(NP:P)$. Since $(RF(m,B):N)$ is a 2-power and $(RF(m,B):P)$ is an odd supernatural number it follows that $(RF(m,B):NP) = 1$ and $NP = RF(m,B)$. Hence $RF_2(m,B) = NP/P \simeq P/(N \cap P)$. Let f be the epimorphism $f: P \longrightarrow RF_2(m,B)$ and s a continuous section, $s: RF_2(m,B) \longrightarrow P$. ([R] Proposition 3.5 pg 31)

Let $C = \{c_1,\dots,c_m\}$ be the set of involutions such that $C \cup B$ is the set of generators of $RF_2(m,B)$. For every $i = 1,\dots,m$ let $e_i \in P$ be an involution such that $f(e_i) = c_i$. Hence, there exists a unique map $g: RF_2(m,B) \longrightarrow P$ such that $g(c_i) = e_i$ for $i = 1,\dots,m$ and $g(b) = s(b)$ for every $\in B$. By the universal property of $RF_2(m,B)$ we have that $fg = id$ and g is an injection. Hence $RF_2(m,B)$ is a closed subgroup of $RF(m,B)$ and then is a real projective group by ([HJ1], Theorem 3.6).

Clearly we can adapt the definition of real projective profinite group ([HJ2], pg 38) with respect to the class of pro-2-groups in the obvious way. Of course a pro-2-group that is a real projective profinite group is a real projective pro-2-group too. In the Corollary 3.5 we will see the converse.

3. THE REAL FREE PRO-2-GROUP.

In this section we will characterize the fields K for which $G(K(2),K) \simeq RF_2(m,B)$.

We will use the same notations we have introduced just before the Corollary 2.5, but now $K(c)$ will be a relative real closure of K in $K(2)$ and K^* is the pythagorean closure of K. (See [B])

PROPOSITION 3.1: Let K be a formally real field such that $G(K(2),K) = RF_2(m,B)$. Choose a system $C = \{c_1,\ldots,c_m\}$ of representatives of the involutions of $G(K(2),K)$. Then:

(A) $G(K(c_j),K) \simeq RF_2(m-1,B)$ for every $j = 1,\ldots,m$.

(B) $G(K^*,K) \simeq F_2(B)$.

(C) $G(K_1(c_1) \cap \ldots \cap K_1(c_m),K) \simeq (\mathbb{Z}/2\mathbb{Z})^m \times F_2(B)$.

PROOF: It follows from Corollary 2.5.

The first conclusion of the Corollary was independently proved by Ershov ([E2], Theorem 4) and Ware ([W2], Corollary 3.5).

The item (B) has a kind of converse. Let K, K^2, and Q(K) be the multiplicative groups of the non-zero elements, squares, and sums of squares, respectively.

We will denote by $\mathbb{F}_2$ the prime field of characteristic 2, by #B the cardinal number of a set B. Let $\tilde{u}(K)$ be the Hasse number of a field K. ($\tilde{u}(K) = \max\{\dim q\}$, where q ranges over all anisotropic forms which becomes isotropic over all (if any) real closures of K.) As usual $H^2(G) = H^2(G,\mathbb{Z}/2\mathbb{Z})$ for any pro-2-group G.

THEOREM 3.2: Let K be a formally real field having m orderings and let B be a set such that $\#B = \dim_{\mathbb{F}_2} Q(K)/K^2$. Then the following conditions are equivalent:

(A) $G(K(2),K) \simeq RF_2(m,B)$.

(B) $G(K^*,K) \simeq F_2(B)$ and $H^2(G(K(2),K)) \simeq (\mathbb{Z}/2\mathbb{Z})^m$.

(C) $\tilde{u}(K) \leq 2$.

(D) G(K(2),K(i)) is a free pro-2-group.

PROOF: (A) $\Longrightarrow$ (B) We have already seen that $G(K^*,K) \simeq F_2(B)$. On the other side by Theorem 1.1 and ([N], Satz (4.1)) $H^2(G(K(2),K)) = \prod_{j=1}^{m+1} H^2(A_j)$ and the resunt follows from the fact that $A_j = \mathbb{Z}/2\mathbb{Z}$ for $j = 1,\dots,m$ and A_{m+1} is a free pro-2-group.

In the proof of $(B) \Longrightarrow (A)$ we need the lemma.

LEMMA 3.3: If K is a formally real field such that $G(K^*,K)$ is a free pro-2-group then every element of $Q(K)-K^2$ is a sum of 2 squares.

PROOF: Let $a \in Q(K) - K^2$ and $H = G(K^*,K(\sqrt{a}))$. Setting $G(K^*,K) = F_2(B)$ and $B_o = \{b \in B \mid b \notin H\}$, then B_o is a finite subset of B and $H = \text{kernel}(f)$, where $f\colon F_2(B) \longrightarrow \mathbb{Z}/2\mathbb{Z}$ is the unique homomorphism such that $f(b) = 1$ for every $b \in B_o$ and $f(b) = 0$ for every $b \in B$, $b \notin B_o$.

Let $g\colon F_2(B) \longrightarrow \mathbb{Z}/4\mathbb{Z}$ be the unique homomorphism such that $g(b) = 1$ for every $b \in B_o$ and $g(b) = 0$ for every $b \in B$, $b \notin B_o$. Observe that g is a surjection such that $\ell \circ g = f$, where $\ell\colon Z/4Z \longrightarrow \mathbb{Z}/2\mathbb{Z}$ is the homomorphism given by $\ell(1+4\mathbb{Z}) = 1+2\mathbb{Z}$. Hence $\text{kernel}(g) \subset \text{kernel}(f)$ and the fixed field E of $\text{kernel}(g)$ is a cyclic extension of K that contains $K(\sqrt{a})$. By [DD], $E = K(\sqrt{x+y\sqrt{d}})$ where d is a sum of 2 squares. Hence $K(\sqrt{a}) = K(\sqrt{d})$ and then there exists $b \in K$ such that $a = db^2$ and a is a sum of 2 squares.

To continue the proof recall that the Arf's map $\theta\colon \dot{K}/K^2 + K^2 \longrightarrow B(K(2),K) \simeq H^2(G(K(2),K))$, that is given by $\theta(\bar{c}) = [(-1,c)]$ = the class of the quaternion algebra, is an injection, ([L], Chapter 3, Theorem 2.7 and Corollary 2.11).

Now we go back to the proof of (B) $\Longrightarrow$ (A) in Theorem 3.2.

Since K has m orderings we have that $|\dot{K}/Q(K)| \geq 2^m$. Since the Arf's map is injective and $|H^2(G(K(2),K))| = 2^m$ it follows that $|\dot{K}/Q(K)| = 2^m$, θ is an isomorphism and K is a SAP field.

Let $P_1,\dots,P_m$ be the positive cones of the orderings of K, $R_1,\dots,R_m$ be, respectively, the real closures of K in $K(2)$ with respect to $P_1,\dots,P_m$ and $A_i = G(K(2),R_i)$, $i = 1,\dots,m$ (See [B] Chapter II).

For every i, $i = 1,\dots,m$, take $a_i \in \dot{K}$ such that $a_i \notin P_i$ but $a_i \in P_j$ for every $j \neq i$. Observe that the set of classes $\{a_iQ(K) \mid i = 1,\dots,m\}$ is a $\mathbb{F}_2$-base of $\dot{K}/Q(K)$ and $K(\sqrt{a_1},\dots,\sqrt{a_m}) \cap K^* = K$. Hence $G = G(K(2),K) = HT$, where $H = G(K(2),K(\sqrt{a_1},\dots,\sqrt{a_m}))$ and T was given in Proposition 2.3. By the hypothesis $F_2(B) = G(K^*,K) = G/T = HT/T = H/(H \cap T)$. Since $F_2(B)$ is a free pro-2-group the exact sequence $1 \longrightarrow H \cap T \longrightarrow H \longrightarrow F_2(B) \longrightarrow 1$ splits and so there exists a closed subgroup A_{m+1} of H isomorphic to $F_2(B)$. Call R_{m+1} the fixed field of A_{m+1}. Since $H = A_{m+1}(H \cap T)$ and $G = HT$ we have that $G = A_{m+1}T$ and so $K^* \cap R_{m+1} = K$.

We claim that $G = \coprod_{j=1}^{m+1} A_j$. We will prove this using the cohomological criterion due to Neukirch ([N], Satz 4.3). So we will show that Res: $H^g(G) \longrightarrow \prod_{j=1}^{m+1} H^2(A_j)$ is bijective for $q = 1,2$.

For $q = 1$, from Kummer's theory we obtain a commutative diagram

$$\begin{tikzcd}
H^1(G) \arrow[r, phantom, "\simeq"] \arrow[d] & \dot{K}/K^2 \arrow[d, "\varphi"] \\
\prod_{j=1}^{m+1} H^1(A_j) \arrow[r, phantom, "\simeq"] & \prod_{j=1}^{m+1} \dot{R}_j/R_j^2
\end{tikzcd}$$

where φ is given canonically. It is enough to prove that φ is an isomorphism. Let $\{a_b \mid b \in B\}$ be a set of elements of $\dot{K}$ such that the set of classes $\{a_b K^2 \mid b \in B\}$ is a $\mathbb{F}_2$-base of $\dot{Q}(K)/K^2$. Observe that the indexes b ranges over B because of $G(K^*,K) \simeq F_2(B)$. Clearly $\{a_1,\dots,a_m\} \cup \{a_b \mid b \in B\}$ is a representative set of a $\mathbb{F}_2$-base of $\dot{K}/K^2$. By the choice of A_{m+1} we get that $\{a_b R_{m+1}^2 \mid b \in B\}$ is a $\mathbb{F}_2$-base of $\dot{R}_{m+1}/R_{m+1}^2$.

Let $c \in \dot{K}$, there are $\varepsilon_1,\dots,\varepsilon_m$, $\varepsilon_b \in \{0,1\}$, $b \in B$, almost all of then null and $d \in \dot{K}$ such that $c = (\prod_{j=1}^{m} a_j^{\varepsilon_b})(\prod_{b\in B} a_b^{\varepsilon_b})d^2$. Hence φ is the isomorphism $\varphi(cK^2) = (a_1^{\varepsilon_1} R_1^2,\dots,a_m^{\varepsilon_m} R_m^2, a_{m+1} R_{m+1}^2)$, where $a_{m+1} = \prod_{b\in B} a_b^{\varepsilon_b} R_{m+1}^2$.

Let $q = 2$. Since we have the following commutative diagram

$$\begin{tikzcd}
H^2(G) \arrow[r, phantom, "\simeq"] \arrow[d, "\mathrm{Res}"'] & B(K(2),K) \arrow[d, "\mathrm{Res}"'] \\
\prod_{j=1}^{m+1} H^2(A_j) \arrow[r, phantom, "\simeq"] & \prod_{j=1}^{m+1} B(K(2),R_j)
\end{tikzcd}$$

it remains to show that the right map is injective.

As we have seen, each element of $B(K(2),K)$ is of the form $[(-1,c)]$, $c \in K$. Let $c = a_1^{\varepsilon_1} \ldots a_m^{\varepsilon_m} a_{m+1}^{\varepsilon_{m+1}} d^2$, where $\varepsilon_1, \ldots, \varepsilon_{m+1} \in \{0,1\}$, $a_{m+1} \in Q(K)$ and $d \in K$. Hence $[(-1,c)] = \prod_{j=1}^{m+1} [(-1,a_j)]^{\varepsilon_j}$. But $[(-1,a_{m+1})] = 0$ since a_{m+1} is a sum of 2 squares by Lemma 3.3 and $B(K(2),R_{m+1}) = 0$ by [W1] Proposition 3.1 . To finish the proof observe that $B(K(2),R_j) = \{0, [(-1,a_j)]\}$ for $j = 1,\ldots,m$.

(A) $\Longrightarrow$ (C) By [W1] Proposition 3.2.

(C) $\Longleftrightarrow$ (D) is Proposition 3.2 of [W1].

To prove (C) $\Longrightarrow$ (B) we need a lemma.

LEMMA 3.4: Let K be a field and IK be the ideal consisting of all even-dimensional quadratic forms over K. The following statements are equivalent:

(A) $(IK)^2 = 2IK$.

(B) The Arf's map θ is an isomorphism.

PROOF: (A) $\Longrightarrow$ (B). Since $B(K(2),K)$ is generated by quaternions algebras, by Merkuryev's Theorem [M], we need only to prove that for every quaternion algebra (a,b), $a,b \in \dot{K}$, there is $c \in \dot{K}$ such that $[(a,b)] = [(-1,c)]$. But this is a consequence of $\langle 1,-a,-b,ab\rangle \simeq \langle 1,1,-c,-c\rangle = 2\langle 1,-c\rangle$, by Corollary 3.3 in [L], which follows from $(IK)^2 = 2IK$ by Theorem 2.1 in [EL].

(B)$\Longrightarrow$(A) Let $\langle 1,a,b,ab\rangle$, $a,b \in \dot{K}$ be a 2-fold Pfister form. By the hypothesis there exists $c \in \dot{K}$ such $[(-a,-b)] = [(-1,c)]$. Hence $\langle 1,a,b,ab\rangle \simeq 2\langle 1,-c\rangle \in 2IK$ what finish the proof.

COROLLARY 3.5: If K is a pythagorean field the above conditions are equivalent to

(B') The classes of quaternions algebras form a subgroup in $B(K(2),K)$.

PROOF: See [EL], Theorem 5.3.

Now we go back to the proof of (C)$\Longrightarrow$(B) in Theorem 3.2. By [ELP] Theorem F, we have that $(IK)^2 = 2IK$ and K is a SAP field. Hence $H^2(G(K(2),K)) \simeq \dot{K}/Q(K) \simeq (\mathbb{Z}/2\mathbb{Z})^m$ by the Lemma. On the other hand, by [W2], Corollary 3.5 we have that $G(K^*,K)$ is a free pro-2-group since $G(K(2), K(\sqrt{-1}))$ is also a free pro-2-group by [ELP] Theorem F.

The last theorem adds precision to Proposition 3.2 of Ware [W1]. We got the free generators of $G(K(2),$

$K(\sqrt{-1})$) and the action of an involution on these generators, as well as the arithmetical meaning of the generators.

Ershov ([E2], Theorem 4) proved that $\tilde{u}(K) \leq 2$ implies that $G(K(2),K)$ is isomorphic to a free pro-2-product $\prod_{i=1}^{m+1} A_i$, where A_i is isomorphic to $(\mathbb{Z}/2\mathbb{Z})$ for $i = 1,\dots,m$ and $A_{m+1} = F_2(B)$, whenever K has m orders. Our theorem provides a connexion between these two results.

In the next corollary we find the analogue of the Theorem 6.5 of [R].

COROLLARY 3.6: Let G be a group with exactly $m > 0$ conjugation classes of involutions. The following conditions are equivalent:

(A) G is a real projective pro-2-group.

(B) G is a pro-2-group that is a real projective profinite group.

(C) There exists a set B such that $G \simeq RF_2(m,B)$.

PROOF: (A) $\Longrightarrow$ (B) Choose a set X for which there exists a surjection $f: RF_2(m,B) \longrightarrow G$ such that $f(c_j) = e_i$, $i = 1,\dots,m$, where $\{c_1,\dots,c_m\}$ and $\{e_1,\dots,e_m\}$ are representatives sets of the classes of involutions of $RF_2(m,B)$

and G respectively. Clearly f has the lift property with respect to involutions. Hence there is $g: G \longrightarrow RF_2(m,B)$ such that $fg = 1$. Hence G is a closed subgroup of $RF_2(m,B)$. Since $RF_2(m,B)$ is a real projective group by Corollary 2.9 so is G by ([HJ2], Corollary 10.5).

$(B) \Longrightarrow (C)$ By [HJ2], Theorem 10.4 there exists a field K such that $G(K) \simeq G$. Since G is a pro-2-group $G(K) \simeq G(K(2),K)$. Since $G(K(i)) \subset G(K)$ is a pro-2-group and is a projective group as a subgroup of a projective group $G(K(i))$ is a free profinite group by ([R], Chapter IV, Theorem 6.5). Thus $G \simeq G(K) \simeq RF_2(m,B)$ by Theorem 3.2.

$(C) \Longrightarrow (A)$ is trivial.

4. EXAMPLES:

4.1. Let k be a formally real field, $a \in \dot{k} - k^2$ such that a is a sum of 2 squares and let R be a real closure of k. (For instance, $k = \mathbb{Q}$, $a = 2$.) Let K be an intermediate field between k and R not containing $\sqrt{a}$ and maximal with respect to the property of exclusion of $\sqrt{a}$ in R. Then by [EV2], Proposition 3 and [EV1] Proposition 9 we have that $G(K) = RF_2(1,\{b\})$.

4.2. Let k be a formally real Hilbetian field and $c_1,\dots,c_m$ be involutions in $G(k)$. Geyer ([G], Theorem 4.3) proves that for almost all $(g_1,\ldots,g_m) \in G(k)^m$ (in the sense of Haar measure of $G(k)$), the subgroup $\langle g_1c_1g_1^{-1},\ldots,g_mc_mg_m^{-1}\rangle$ is isomorphic to the free product $\prod_{i=1}^{m}\langle g_ic_ig_i^{-1}\rangle$. Hence by Theorem 1.1 $\langle g_1c_1g_1^{-1},\ldots,g_mc_mg_m^{-1}\rangle \simeq RF(m,\emptyset)$.

4.3. Let k be an algebraic number field that has m orderings such that $k(i)$ contains all 2-power roots of the unity. Then by [R], Theorem 8.8, pg 302 and Corollary 3.2, pg 255 it follows that $G(k(2),k(i))$ is a free pro-2-group. Hence by Theorem 3.2 $G(k(2),k) = RF_2(m,B)$, for some set B. By Corollary 2.9 and Remark 1.6 there exists an algebraic extension L over k such that $G(L) \simeq RF_2(m,B)$.

4.4. The famous "Tsen's Theorem" provides another family of fields that satisfy the conditions of Theorem 3.2. It is enough to consider a m-ordered algebraic extension of the rational function field $R(X)$ where R is a real closed field.

4.5. Let $K = R(t)$, (the rational function field), where R is the real number field and let A be the set of all prime divisors of $R(t)|R$. For each finite subset S of A, let $K_S|K$ be the maximal normal extension of K unramified at the elements of $A-S$. As is shown in ([KN], Satz 2) or ([HJ1], Lemma 4.2) $G(K_S,K) \simeq RF(m,B)$, where S contains m real primes of degree 1 and finite at t and

#B complex primes of degree 2.

Now, fix $S_o \subset A$, a set of m real primes of degree 1 and finite at t and call B the set of all complex primes of degree 2. Let $K(S_o)$ be the maximal normal extension of K unramified at the elements of $A-(S_o \cup B)$. Clearly $K(S_o) = \cup K_S$, where $S = S_o \cup S_1$ and S_1 ranges over the set of finite subset of B. An easy verification shows that $G(K(S_o),K) \simeq RF(m,B)$. Finally, by Remark 1.6 there are algebraic extensions L of $R(t)$ such that $G(L) \simeq RF(m,B)$.

REFERENCES

[B] BECKER, E. Hereditarily-Pythagorean Fields and Orderings of Higher Level, Monografias de Matemática nº 29, IMPA, Rio de Janeiro, 1978.

[BNW] BINZ, E., NEUKIRCH, J. and WENZEL, G.H. A Subgroup Theorem for Free Products of Profinite Groups. J. Algebra 19 (1971), 104-109.

[D] Douady, A. Determination d'un groupe de Galois. C. R. Acad. Sci. Paris 258 (1964), 5305-5308.

[DD] DILLER, J., DRESS, A. Zur Galoistheorie pythagoraischer Korper, Arch. der Math. 16 (1965), 148-152.

[E1] ERSHOV, Yu. L. Profinite Groups. English Transl. in Math. Notes (1981) 357-366.

[E2] ERSHOV, Yu. L. Galois Groups of Maximal 2-Extensions. English Transl. in Math . Notes 36 (1984), 956-961.

[EL] ELMAN, R. , LAM, T.Y. Quadratic Forms Over formally Real Fields and Pythagorean Fields. Amer. J. Math. 94 (1972), 1155-1194.

[ELP] ELMAN, R. , LAM, T.Y. and PRESTEL, A. On Some Hasse Principles over Formally Real Fields. Math. Z. 134 (1973), 291-301.

[EV1] ENGLER, A.J. , VISWANATHAN, T.M. Digging Holes in Algebraic Closures A La Artin-II. Contemporary Math. 8 (1982), 351-360.

[EV2] ENGLER, A.J. , VISWANATHAN, T.M. Formally Real Fields with a Simple Description of the Absolute Galois Group. Manuscripta Math. 56 (1986), 71-87.

[G] GEYER, W.D. Galois Groups of Intersections of Local Fields. Israel J. Math. 30 (1978), 382-396.

[Gr1] GRIFFIN, M. The Pythagorean Closure of fields. Math. Sc. 38 (1967), 177-191.

[Gr2] GRIFFIN, M. Galois Theory and Ordered Fields. Queen's University Preprint 18 (1972).

[HJ1] HARAN, D. and JARDEN, M. Real Free Groups and the Absolute Galois Group of R(t). J. Pure and Appl. Algebra 37 (1985), 155-165.

[HJ2] HARAN, D. and JARDEN, M. The Absolute Galois Group of a Pseudo Real Closed Field. Ph.D. Thesis Tel-Aviv.

[HR] HERFORT, W. and RIBES, L. Torsion elements and centralizers in free products of profinite groups. J. reine angew. Math. 358 (1985), 155-161.

[KN] KRULL, W. and NEUKIRCH, J. Die Struktur der absoluten Galoisgruppe uber dem Korper R(t). Math. Ann. 193 (1971), 197-209.

[L1] LAM, T.Y. The Algebraic Theory of Quadratic Forms. Benjamin, New York, 1973.

[L2] LAM, T.Y. Orderings, Valuations and Quadratic Forms. CBMS, n. 52 AMS, 1983.

[LVDD] LUBOTZKY, A. and VAN DEN DRIES, L. Subgroups of Free Profinite Groups and Large Subfields of Q. Israel J. Math. 39 (1981), 25-45.

[M] MERKURYEV, A.S. On the Norm Residue Symbol of degree 2. Soviet. Mat. Doklady 24 (1981), 546-551.

[N] NEUKIRCH, J. Freie Produkte pro-endlicher Gruppen und ihre Kohomologie. Arch. Math. 22 (1971), 337-357.

[O] OLTIKAR, B.C. Ph. D. Thesis, Carleton.

[P] PRESTEL, A. Remarks on the Pythagoras and Hasse Number of Real Fields. J. reine angew. Math. 303/304 (1978), 284-294.

[R] RIBES, L. Introduction of Profinite Groups and Galois Cohomology. Queen's Papers in Pure and applied Math. 24 (1970).

[W1] WARE, R. Quadratic Forms and Profinite 2-groups. J. Algebra 58 (1979), 227-237.

[W2] WARE, R. Quadratic Forms and Profinite 2-groups II: The Galois Group of the Pythagorean Closure of a Formally Real Field. J. Pure and Appl. Algebra 30 (1983), 95-107.