JOURNAL OF ALGEBRA 129, 393–411 (1990)

Closed Subgroups of $G(\mathbb{Q})$ with Involutions

DAN HARAN

School of Mathematical Sciences, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv 69978, Israel

Communicated by A. Fröhlich

Received November 20, 1987

INTRODUCTION

The aim of this note is to determine certain closed subgroups of the absolute Galois group $G(\mathbb{Q})$ of $\mathbb{Q}$, in particular subgroups generated by involutions (=elements of order 2).

Geyer [3, 4.1] has shown, in a far more general set-up, that subgroups generated by finitely many involutions are *almost always* free profinite products of copies of $\mathbb{Z}/2\mathbb{Z}$. To be precise, fix an involution $\varepsilon \in G(\mathbb{Q})$; for almost all (in the sense of the Haar measure) e-tuples $(\sigma_1, ..., \sigma_e)$ in $G(\mathbb{Q})^e = G(\mathbb{Q}) \times \cdots \times G(\mathbb{Q})$ (e copies) we have

$$\langle \varepsilon^{\sigma_1}, ..., \varepsilon^{\sigma_e} \rangle = \langle \varepsilon^{\sigma_1} \rangle * \cdots * \langle \varepsilon^{\sigma_e} \rangle \cong \hat{D}_e = \mathbb{Z}/2\mathbb{Z} * \cdots * \mathbb{Z}/2\mathbb{Z} \ (e\text{- times}).$$

The above measure-theoretic restriction is necessary, since any closed subgroup of $\hat{D}_e$ generated by finitely many involutions also appears as a closed subgroup of $G(\mathbb{Q})$. However, the following characterization of virtually projective closed subgroups of $G(\mathbb{Q})$ shows that nothing worse can happen. (Recall that a profinite group G is *virtually projective* if it contains an open subgroup that is projective.)

THEOREM. *Let G be a profinite group. The following conditions are equivalent*:

(a) *G is isomorphic to the absolute Galois group of an algebraic extension of $\mathbb{Q}$ and G is virtually projective*;

(b) *G is a closed subgroup of $\hat{D}_e$, where $3 \leqslant e \leqslant \omega$*;

(c) *G is real projective* (*Definition* 1.1) *and countably generated.*

Moreover, if G is generated by involutions (*but not necessarily by a*

0021-8693/90 \$3.00

finite number of them!) then (b), (c), *and the following condition* (a′) *are equivalent.*

(a′) *G is isomorphic to the absolute Galois group of an algebraic extension of* $\mathbb{Q}$.

The essential ingredients of the proof are the Local–Global Principle for Brauer groups and the Strong Approximation Property for algebraic number fields on one hand and some new group-theoretic results about real projective groups on the other hand. In particular, we succeed in characterizing real projective groups essentially by their Sylow subgroups.

1. Real Projective and Real Free Groups

In this section we explain the equivalence (b) $\Rightarrow$ (c) of the main theorem and fix the notation.

Definition 1.1 (cf. [5, p. 472] and [4, Definition 4.1]). Let G be a profinite group for which the set $\mathrm{Inv}(G)$ of involutions in G is a closed subset of G.

(1) An *embedding problem* for G consists of a continuous epimorphism $\alpha\colon B \to A$ of profinite groups and a continuous homomorphism $\varphi\colon G \to A$. It is *finite* if B and A are finite groups. It is said to be *real* if $1 \notin \varphi(\mathrm{Inv}(G))$ and for every involution $x \in G$ there exists an involution $b \in B$ such that $\alpha(b) = \varphi(x)$. A *solution* of the embedding problem is a continuous homomorphism $\gamma\colon G \to B$ such that $\alpha \circ \gamma = \varphi$.

(2) G is *projective* if every finite embedding problem for G is solvable.

(3) G is *real projective* if every finite real embedding problem for G is solvable.

(4) A *finite* $\mathrm{Inv}(G)$*-embedding problem* (φ, α, C) for G consists of an epimorphism $\alpha\colon B \to A$ of finite groups, a continuous homomorphism $\varphi\colon G \to A$ such that $1 \notin \varphi(\mathrm{Inv}(G))$, and a set C of involutions in B closed under the conjugation in B such that $\varphi(\mathrm{Inv}(G)) \subseteq \alpha(C)$. Its *kernel* is $\mathrm{Ker}\,\alpha$. A *solution* of such a problem is a continuous homomorphism $\gamma\colon G \to B$ such that $\gamma(\mathrm{Inv}(G)) \subseteq C$ and $\alpha \circ \gamma = \varphi$.

Remark 1.2. (a) Let G be real projective and let $\varphi\colon G \to A$, $\alpha\colon B \to A$ be a finite embedding problem for G such that for every involution $x \in G$ with $\varphi(x) \neq 1$ there exists an involution $b \in B$ such that $\alpha(b) = \varphi(x)$. Then (φ, α) is solvable. Indeed, since $\mathrm{Inv}(G)$ is closed (that is, 1 is not in its closure), there exists an open normal subgroup N of G disjoint to $\mathrm{Inv}(G)$. Therefore φ factors into $\hat{\varphi}\colon G \to \hat{A} = G/N$ and $\varphi_0\colon \hat{A} \to A$. Put $\hat{B} = B \times_A \hat{A}$

and let $\hat{\alpha}: \hat{B} \to \hat{A}$ and $\hat{\varphi}_0: \hat{B} \to B$ be the coordinate projections, so that $\varphi_0 \circ \hat{\alpha} = \alpha \circ \hat{\varphi}_0$. It is easy to see that $(\hat{\varphi}, \hat{\alpha})$ is a finite real embedding problem for G. A solution $\hat{\gamma}$ of $(\hat{\varphi}, \hat{\alpha})$ gives a solution $\gamma = \hat{\varphi}_0 \circ \hat{\gamma}$ of (φ, α).

This shows that our definition of real projective groups is the same as the one given in [5].

(b) A group G (with $\mathrm{Inv}(G)$ closed in G) is projective relative to the family X of all subgroups of order 2 of G (in the sense of [4, Definition 4.1]) if and only if every finite $\mathrm{Inv}(G)$-embedding problem for G is solvable.

Indeed, $\mathrm{Inv}(G)$ is closed, so it is a Boolean space. If $\varepsilon_1, \varepsilon_2 \in \mathrm{Inv}(G)$ are not equal then there exists a clopen subset U of $\mathrm{Inv}(G)$ such that $\varepsilon_1 \in U, \varepsilon_2 \notin U$. As both U and $\mathrm{Inv}(G) \setminus U$ are closed in G, the subsets $\bigcup_{\varepsilon \in U} \langle \varepsilon \rangle$ and $\bigcup_{\varepsilon \notin U} \langle \varepsilon \rangle$ of G are closed; thus X is *separated* [4, Definition 3.1]. Furthermore, as in (a), it is enough to consider only those finite X-embedding problems $(\varphi, \alpha, \mathrm{Con}(B))$ for G that satisfy $1 \notin \varphi(\mathrm{Inv}(G))$. Thus our assertion easily follows from the identification of a subgroup of order 2 in X with its generator in $\mathrm{Inv}(G)$.

We shall use without mention the fact that a closed subgroup of a real projective group is real projective (see [5, Corollary 10.5]) and that a real projective group with no involution is projective (clear from the definition).

As an example of real projective groups we consider real free groups:

DEFINITION 1.3 (cf. [6, Definition 1.1]). Let $\mathscr{C}$ be a full family of finite groups, let X be a Boolean space, and S a set. A pro-$\mathscr{C}$ group $\hat{D} = \hat{D}_{\mathscr{C}}(X, S)$ is *real free on* (X, S) if it contains X and S as disjoint subsets such that X is closed in $\mathrm{Inv}(\hat{D})$, S converges to 1, and

(*) every map φ from $X \cup S$ into a pro-$\mathscr{C}$ group G, continuous on X, such that $\varphi(x)^2 = 1$ for every $x \in X$ and $\varphi(S)$ converges to 1, extends to a unique homomorphism of $\hat{D}$ into G.

(The group $\hat{D}_{\mathscr{C}}(X, S)$ is, in fact, the free pro-$\mathscr{C}$ product of the free pro-$\mathscr{C}$ group of rank $|S|$ with the free pro-$\mathscr{C}$ product of copies of $\mathbb{Z}/2\mathbb{Z}$ over the space X.)

If $\mathscr{C}$ is the family of all finite groups, denote $\hat{D}_{e,f} = \hat{D}_{\mathscr{C}}(X, S)$, where $|X| = e$ and $|S| = f$; if $f = 0$ write $\hat{D}_e$ for $\hat{D}_{e,f}$. If X_ω is the Cantor "middle thirds" set (cf. [7, Lemma 1.2]) and $|S| = \aleph_0$ write $\hat{D}_\omega$ for $\hat{D}_{\mathscr{C}}(X_\omega, S)$ (cf. [7, Section 2]). If $\mathscr{C}$ is the family of all 2-groups, write $\hat{D}_2(X, S)$ for $\hat{D}_{\mathscr{C}}(X, S)$.

We note that the set X is a complete system of representatives of the conjugacy classes of involutions in $\hat{D}(X, S)$ (see [6, Corollary 3.2]).

PROPOSITION 1.4. *Every closed subgroup of* $\hat{D}_{e,f}$ *is real projective.*

Conversely, every countably generated real projective group can be embedded in $\hat{D}_\omega$, in $\hat{D}_e$ with $e \geqslant 3$, and in $\hat{D}_{e,f}$ with $e \geqslant 1$ and $f \geqslant 1$.

Proof. The first assertion follows from [6, Theorem 3.6]. By [7, Proposition 2.3] (take $H = 1$ there) every countably generated real projective group can be embedded in $\hat{D}_\omega$, and hence, by [7, Corollary 4.4], also in $\hat{D}_{e,f}$, where $e \geqslant 1$ and $f \geqslant 2$. If $e \geqslant 3$ then $\hat{D}_e \cong \hat{D}_{e-2} * \hat{D}_2$, and $\hat{\mathbb{Z}}$ is a closed subgroup of $\hat{D}_2$ (see Lemma 1.5), hence [9, Proposition 4] $\hat{D}_{1,1} \cong \mathbb{Z}/2\mathbb{Z} * \hat{\mathbb{Z}}$ can be embedded in $\hat{D}_e$; clearly $\hat{D}_{1,1}$ can also be embedded in $\hat{D}_{e,f}$ with $e \geqslant 1$ and $f \geqslant 1$. Thus it suffices to show that $\hat{D}_{1,1}$ contains $\hat{D}_{1,2}$. But, by [7, Lemma 4.3], $\hat{D}_{1,1}$ contains $\hat{D}_{e,1}$ for some $e \geqslant 3$, and $\hat{D}_{e,1} \cong \hat{D}_{e-2,1} * \hat{D}_2$ contains $\hat{D}_{1,1} * \hat{\mathbb{Z}} \cong \hat{D}_{1,2}$. ∎

The restrictions posed on e and f in the Proposition are the least possible. Indeed, $\hat{D}_{0,f}$ contains no involutions, the group $\hat{D}_1 = \mathbb{Z}/2\mathbb{Z}$ is finite and the closed subgroups of $\hat{D}_2$ containing involutions are dihedral groups.

We call a profinite group G *dihedral* if it is generated by two elements ε and τ such that $\varepsilon^2 = 1$ and $\tau^\varepsilon = \tau^{-1}$ (according to this definition cyclic groups are not excluded). Note that G is the semi-direct product of $\langle \varepsilon \rangle$ with $\langle \tau \rangle$. The following (well known) property relates them to our subject:

LEMMA 1.5. (a) *A profinite group is dihedral if and only if it is generated by two elements of order $\leqslant 2$.*

(b) *An infinite profinite group containing involutions is dihedral if and only if it is a subgroup of $\hat{D}_2$.*

Proof. (a) If $G = \langle \varepsilon, \tau \rangle$, and $\varepsilon^2 = 1$, $\tau^\varepsilon = \tau^{-1}$, then $G = \langle \varepsilon, \varepsilon\tau \rangle$ and $(\varepsilon\tau)^2 = (\tau^\varepsilon)\tau = 1$. Conversely, if $G = \langle \varepsilon_1, \varepsilon_2 \rangle$ and $\varepsilon_1^2 = \varepsilon_2^2 = 1$, then $G = \langle \varepsilon_1, \varepsilon_1\varepsilon_2 \rangle$ and $(\varepsilon_1\varepsilon_2)^{\varepsilon_1} = \varepsilon_2\varepsilon_1 = (\varepsilon_1\varepsilon_2)^{-1}$.

(b) Let $D = \langle \delta, \sigma \rangle$, where $\langle \delta \rangle \cong \mathbb{Z}/2\mathbb{Z}$, $\langle \sigma \rangle \cong \hat{\mathbb{Z}}$, and $\sigma^\delta = \sigma^{-1}$. Clearly every dihedral group $G = \langle \varepsilon, \tau \rangle$ is an epimorphic image of D (by $\delta \mapsto \varepsilon$, $\sigma \mapsto \tau$), hence by (a) and [2, Proposition 15.4] we have $D \cong \hat{D}_2$.

Note that D is the disjoint union of $\langle \sigma \rangle$ and $\langle \sigma \rangle \delta$, and all $\sigma_0 \in \langle \sigma \rangle$ and $\varepsilon_0 \in \langle \sigma \rangle \delta$ satisfy $\varepsilon_0^2 = 1$, $\sigma_0^{\varepsilon_0} = \sigma_0^{-1}$. Thus if G is a subgroup of D containing involutions, and τ_0 is a generator of $G_0 = G \cap \langle \sigma \rangle$, then $G = G_0 \langle \varepsilon_0 \rangle$, where $\varepsilon_0 \in G \cap \langle \sigma \rangle \delta$, so $G = \langle \varepsilon_0, \tau_0 \rangle$ is dihedral. Conversely, if $G = \langle \varepsilon, \tau \rangle$ is an infinite dihedral group with $\varepsilon^2 = 1$, $\tau^\varepsilon = \tau^{-1}$, there exist embeddings $\langle \tau \rangle \to \langle \sigma \rangle$, $\langle \varepsilon \rangle \to \langle \delta \rangle$; these give rise to an embedding $G \to D$. ∎

2. REAL EMBEDDING PROBLEMS

Our aim is to find simpler conditions for a group to be real projective. We begin with some results on finite groups.

DEFINITION 2.1. Let $C_1, ..., C_e$ be e distinct conjugacy classes of involutions in a finite group G. Let $G^* = G^*(C_1, ..., C_e)$ be the intersection of all groups in

$$\mathbf{M} = \{M \mid M \text{ is a maximal subgroup of } G \text{ and } M \cap C_i \neq \varnothing \text{ for } i = 1, ..., e\}.$$

(If $e = 0$ then G^* is nothing but the Frattini subgroup of G.)

PROPOSITION 2.2. *Let $K \neq 1$ be a minimal normal subgroup of a finite group G contained in G^*. Then K is an elementary abelian p-group. If G is a p-group then $K \cong \mathbb{Z}/p\mathbb{Z}$ and K is contained in the center of G.*

Proof. We first show that K is a p-group for some prime p.

Let p be a prime that divides the order $|K|$ of K, such that $p = 2$ if $|K|$ is even. Let $P \leqslant K$ be a Sylow p-subgroup of K (whence $P \neq 1$) and let $\Pi = \{P^g \mid g \in G\} = \{P^k \mid k \in K\}$ be the family of all Sylow p-subgroups of K. Then $|\Pi| = (K:N_K(P))$ divides $(K:P)$ and therefore is odd. Thus the action of an involution $\varepsilon \in G$ on Π by conjugation must have a fixed point, i.e., $P^{g\varepsilon} = P^g$ for some $g \in G$, whence $g\varepsilon g^{-1} \in N_G(P)$.

We deduce that every maximal subgroup M of G containing $N_G(P)$ is in $\mathbf{M}$, and so $KN_G(P) \leqslant G^*N_G(P) \leqslant M$. But since $KN_G(P) = G$ (the Frattini argument), there is no such group M. Thus $N_G(P) = G$, whence P is a normal subgroup of G. By the minimality of K we get that $K = P$, so that K is a p-group.

Using the minimality again we note that K equals its center, hence K is abelian. Finally, K equals $\{\sigma \in K \mid \sigma^p = 1\}$, whence K is an elementary abelian p-group. (Cf. [2, Lemma 20.9].) If G is a p-group then the G-conjugacy classes of $K \smallsetminus \{1\}$ have p-power orders, hence at least one of them is of order 1, say $\{\sigma\}$; thus σ is in the center of G and $K = \langle \sigma \rangle$ by the minimality of K. ∎

PROPOSITION 2.3. *Let G be a profinite group and assume that* $\mathrm{Inv}(G)$ *is closed in G. The following conditions are equivalent:*

(a) *G is real projective.*

(b) *Every finite* $\mathrm{Inv}(G)$*-embedding problem for G is solvable.*

(c) *Every finite* $\mathrm{Inv}(G)$*-embedding problem for G with minimal normal elementary abelian p-subgroup as kernel is solvable.*

Proof. (b) $\Rightarrow$ (a) and (b) $\Rightarrow$ (c) are clear.

(a) $\Rightarrow$ (b) follows from [5, Corollary 6.2]: Given a finite $\mathrm{Inv}(G)$-embedding problem $(\phi, \alpha\colon B \to A, C)$ for G, there exist a finite group B' and an epimorphism $\theta\colon B' \to B$ which maps the involutions of $B' \smallsetminus \mathrm{Ker}\,\theta$ onto

C. Thus $(\varphi, \alpha \circ \theta)$ is a finite real embedding problem for G; its solution $\gamma: G \to B'$ produces the solution $\theta \circ \gamma$ of our $\mathrm{Inv}(G)$-embedding problem.

(c) $\Rightarrow$ (b): It suffices to solve every finite $\mathrm{Inv}(G)$-embedding problem $(\varphi, \alpha: B \to A, C)$ for G in which the kernel $\mathrm{Ker}\,\alpha$ is a minimal normal subgroup of B. Indeed, otherwise let $1 \neq K \leqslant \mathrm{Ker}\,\alpha$ be a minimal normal subgroup of B; let $\pi: B \to \bar{B} = B/K$ be the canonical epimorphism, $\bar{C} = \pi(C)$; and let $\bar{\alpha}: \bar{B} \to A$ be the map induced by α. Then $(\varphi, \bar{\alpha}, \bar{C})$ is a finite $\mathrm{Inv}(G)$-embedding problem for G. Suppose, by induction on the order of B, that it has a solution $\bar{\gamma}: G \to \bar{B}$; in particular $\bar{\gamma}(\mathrm{Inv}(G) \subseteq \bar{C}$. Then $(\bar{\gamma}, \pi, C)$ is a finite $\mathrm{Inv}(G)$-embedding problem with kernel K for G; its solution also solves (φ, α, C).

Assume therefore, that the kernel K is a minimal normal subgroup of B. Let $C_1, ..., C_e$ be the distinct conjugacy classes in C. If $K \not\subseteq B^*(C_1, ..., C_e)$ then there is a maximal subgroup M of B such that $M \cap C_i \neq \varnothing$ for $i = 1, ..., e$, and $K \not\subseteq M$, whence $\alpha(M) = \alpha(MK) = \alpha(G) = A$. Thus $(\varphi, \mathrm{res}_M\, \alpha, C \cap M)$ is a finite $\mathrm{Inv}(G)$-embedding problem for G; its solution also solves (φ, α, C). If $K \subseteq B^*(C_1, ..., C_e)$ then K is an elementary abelian p-group by Proposition 2.2, so the problem is solvable by assumption. ∎

Remark 2.4. Let G be a pro-p-group with $\mathrm{Inv}(G)$ closed in G. It easily follows from the Sylow theory that G is real projective iff G is real projective in the category of pro-p-groups (i.e., every finite embedding problem for G consisting of pro-p-groups is solvable). Carrying the proof of Proposition 2.3 in the category of pro-p-groups we obtain that the following are equivalent:

(a) G is real projective.

(b) Every finite $\mathrm{Inv}(G)$-embedding problem $(\varphi, \alpha: B \to A, C)$ for G, in which B is a p-group, is solvable.

(c) Every finite $\mathrm{Inv}(G)$-embedding problem $(\varphi, \alpha: B \to A, C)$ for G, in which B is a p-group and $\mathrm{Ker}\,\alpha \cong \mathbb{Z}/p\mathbb{Z}$ lies in the center of B, is solvable.

3. Fields with Real Projective Absolute Galois Group

In this section we present some field-theoretic properties of a field whose absolute Galois group is real projective.

DEFINITION 3.1. Let G be a profinite group such that $\mathrm{Inv}(G)$ is closed in G. We say that G has the *Strong Approximation Property* (SAP) if for every proper clopen subset Z of $\mathrm{Inv}(G)$ closed under the conjugation in G

there exists an open normal subgroup N of G such that $(G:N)=2$ and $Z=\mathrm{Inv}(G)\cap N$. The motivation for this definition is explained below.

Remark 3.2. The absolute Galois group G of a field K has the SAP if and only if K satisfies the following *Strong Approximation Property* for fields:

> For all $a, b \in K^\times$ there exists $c \in K^\times$ such that in every ordering P on K, a, b are positive if and only if c is positive.

Indeed, the set $X(K)$ of all orderings on K is a Boolean space in the topology given by the subbase of clopen sets of the form

$$H(a)=\{Q\in X(K) \mid a \text{ is positive in } Q\}, \text{ where } a\in K^\times$$

(see [12, Section 6]). In this notation the SAP can be written as For all $a, b\in K^\times$ there exists $c\in K^\times$ such that $H(a)\cap H(b)=H(c)$. The clopen subsets of $X(K)$ are the Boolean combinations of the subbasic sets. It is an easy exercise in the theory of Boolean spaces to see that K has the SAP if and only if every clopen subset of $X(K)$ is in the subbase.

To every involution ε in G there corresponds the ordering $P(\varepsilon)$ of K that extends to the unique ordering of the (real closed) fixed field of ε in $\tilde{K}$, the algebraic closure of K. The map P: $\mathrm{Inv}(G)\to X(K)$ is surjective and $P(\varepsilon_1)=P(\varepsilon_2)$ iff ε_1 is conjugate to ε_2 (see [10, Chapter XI, Section 2, Theorems 4 and 3]). Moreover, P is clearly continuous, hence a closed map, but it is also open (if U is open in $\mathrm{Inv}(G)$ then $U'=\bigcup_{\sigma\in G}U^\sigma$ is also open, so $X(K)\smallsetminus P(U)=X(K)\smallsetminus P(U')=P(\mathrm{Inv}(G)\smallsetminus U')$ is closed), so it induces a bijection between the clopen subsets of $\mathrm{Inv}(G)$ closed under the conjugation in G and the clopen subsets of $X(K)$. Thus the SAP for K is equivalent to:

If Z is a clopen subset of $\mathrm{Inv}(G)$ closed under the conjugation then there exists $c\in K^\times$ such that $Z=P^{-1}(H(c))$, i.e., all $\varepsilon\in\mathrm{Inv}(G)$ satisfy

$$\varepsilon(\sqrt{c})=\sqrt{c} \qquad \text{iff} \qquad \varepsilon\in Z$$

This is obviously equivalent to SAP for G.

PROPOSITION 3.3. *A real projective group G has the* SAP.

Proof. If G is real free, say $G=\hat{D}(X,S)$, and Z is a proper clopen subset of $\mathrm{Inv}(G)$ then the map $\varphi: X\cup S\to \mathbb{Z}/2\mathbb{Z}$ defined by $\varphi(S)=\varphi(X\cap Z)=1$, $\varphi(X\smallsetminus Z)\neq 1$, induces a homomorphism $\varphi: G\to\mathbb{Z}/2\mathbb{Z}$. Its kernel N has the required property.

In the general case let X_0 be a closed system of representives of the conjugacy classes of $\mathrm{Inv}(G)$, and let X be a homeomorphic copy of X_0.

For a suitable set S we have an epimorphism $\alpha\colon \hat{D}(X, S) \to G$ extending the given homeomorphism $X \to X_0$. Thus α maps nonconjugate involutions of $D = \hat{D}(X, S)$ into nonconjugate involutions in G; therefore a right inverse $\gamma\colon G \to D$ of α (see [6, Lemma 3.5]) maps nonconjugate involutions into nonconjugate involutions. Put $Z' = \bigcup_{d \in D} \gamma(Z)^d$; then Z' is a proper closed subset of D and $\gamma^{-1}(Z') = Z$. Let N be an open subgroup of D of index 2 such that $N \cap \mathrm{Inv}(D) = Z'$; then $\gamma^{-1}(N) \cap \mathrm{Inv}(G) = \gamma^{-1}(Z') = Z$. ∎

LEMMA 3.4. *Let K be a field, denote $G = G(K)$, and let $\{R_i\}_{i \in I}$ be a set of real closed extensions of K inducing the orderings on K (one for each ordering on K). The following conditions are equivalent:*

(a) *Every finite real embedding problem ($\varphi\colon G \to A$, $\alpha\colon B \to A$) with* $\mathrm{Ker}\,\alpha \cong \mathbb{Z}/2\mathbb{Z}$ *contained in the center of B is solvable.*

(b) *Every central extension of profinite groups*

$$0 \to \mathbb{Z}/2\mathbb{Z} \to E \xrightarrow[\beta]{} G \to 1$$

splits if $\mathrm{Inv}(G) \subseteq \beta(\mathrm{Inv}(E))$.

(c) *The natural map*

$$H^2(G, \mathbb{Z}/2\mathbb{Z}) \to \prod_{i \in I} H^2(G(R_i), \mathbb{Z}/2\mathbb{Z}),$$

where the groups act trivially on $\mathbb{Z}/2\mathbb{Z}$, is injective.

(d) *The natural map*

$$H^2(G, \tilde{K}^\times)_2 = \{a \in H^2(G, \tilde{K}^\times) \mid 2a = 0\} \to \prod_{i \in I} H^2(G(R_i), \tilde{R}_i^\times)$$

is injective.

Moreover, if K is formally real and $G(K(\sqrt{-1}))$ is projective then (a)–(d) *are also equivalent to*

(e) *The natural map*

$$H^2(\mathcal{G}(K(\sqrt{-1})/K), K(\sqrt{-1})^\times) \to \prod_{i \in I} H^2(G(R_i), \tilde{R}_i^\times)$$

is injective.

(f) *Every totally positive element of K is a sum of two squares in K.*

Proof. (a) ⇒ (b): Choose an open normal subgroup N of E such that $N \cap \mathrm{Ker}\,\beta = 1$ and $\beta(N) \cap \mathrm{Inv}(G) \neq \varnothing$. Put $B = E/N$ and $A = G/\beta(N)$. We obtain the following commutative diagram with a cartesian square:

$$\begin{tikzcd} & & & G \arrow[d, equal] & \\ 0 \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & E \arrow[r, "\beta"] \arrow[d, "p"] & G \arrow[r] \arrow[d, "\varphi"] & 1 \\ & & B \arrow[r, "\alpha"] & A & \end{tikzcd}$$

and $(\varphi: G \to A,\ \alpha: B \to A)$ is a finite real embedding problem with $\operatorname{Ker} \alpha \cong \mathbb{Z}/2\mathbb{Z}$ contained in the center of B. Its solution $\gamma: G \to B$, together with the identity $G \to G$, induces a right inverse $\theta: G \to E$ of β (such that $p \circ \theta = \gamma$).

(b) $\Rightarrow$ (a): Let $E = B \times_A G$ and let $p: E \to B$ and $\beta: E \to G$ be the coordinate projections. Check that $\operatorname{Ker} \beta$ lies in the center of E. By asumption $0 \to \mathbb{Z}/2\mathbb{Z} \to E \to_\beta G \to 1$ splits via some $\theta: G \to E$; then $p \circ \theta$ solves $(\varphi: G \to A,\ \alpha: B \to A)$.

(b) $\Leftrightarrow$ (c): This follows from the correspondence of $H^2(G, \mathbb{Z}/2\mathbb{Z})$ with the isomorphy classes of central extensions of G by $\mathbb{Z}/2\mathbb{Z}$ (see [13, p. 100]). An extension $0 \to \mathbb{Z}/2\mathbb{Z} \to E \to G \to 1$ corresponds to 0 iff it splits, and its restriction to $G(R_i)$ corresponds to 0 in $H^2(G(R_i), \mathbb{Z}/2\mathbb{Z})$ iff the restriction splits, i.e., $\operatorname{res}_{\tilde{K}} \varepsilon_i$, where ε_i is the generator of $G(R_i)$, is the image of an involution in E. Recall also that $\{\operatorname{res}_{\tilde{K}} \varepsilon_i\}_{i \in I}$ represents the conjugacy classes of involutions in G; therefore the condition "$\operatorname{Inv}(G) \subseteq \beta(\operatorname{Inv}(E))$" in (b) is equivalent to "$\{\operatorname{res}_{\tilde{K}} \varepsilon_i\}_{i \in I} \subseteq \beta(\operatorname{Inv}(E))$".

(c) $\Leftrightarrow$ (d): The short exact sequence of G-modules

$$1 \to \{\pm 1\} \to \tilde{K}^\times \underset{\mu}{\to} \tilde{K}^\times \to 1,$$

where $\mu(a) = a^2$, and Hilbert's Theorem 90 induce the exact sequence $0 \to H^2(G, \mathbb{Z}/2\mathbb{Z}) \to H^2(G, \tilde{K}^\times) \to_\mu \tilde{H}^2(G, \tilde{K}^\times)$, which yields the isomorphism $H^2(G, \mathbb{Z}/2\mathbb{Z}) \cong H^2(G, \tilde{K}^\times)_2$.

Analogously $H^2(G(R_i), \mathbb{Z}/2\mathbb{Z}) \cong H^2(G(R_i), \tilde{R}_i^\times)_2 = H^2(G(R_i), \tilde{R}_i^\times)$ for every $i \in I$ (the last group is annihilated by 2 by [13, p. 138]).

(d) $\Leftrightarrow$ (e): Assume that $G(K(\sqrt{-1}))$ is projective. Then $B(K(\sqrt{-1})) = H^2(G(K(\sqrt{-1})), \tilde{K}^\times) = 0$ (see [13, p. 263]), hence the inflation $H^2(\mathcal{G}(K(\sqrt{-1})/K), K(\sqrt{-1})^\times) \to H^2(G, \tilde{K}^\times)$ is an isomorphism (see [13, p. 249]). In particular, the elements of $H^2(G, \tilde{K}^\times)$ are of order $\leqslant 2$, whence $H^2(\mathcal{G}K(\sqrt{-1})/K), K(\sqrt{-1})^\times) \cong H^2(G, \tilde{K}^\times)_2$.

(e) $\Leftrightarrow$ (f): There is a natural isomorphism

$$H^2(\mathcal{G}(K(\sqrt{-1})/K),\ K(\sqrt{-1})^\times) \cong K^\times / N_{K(\sqrt{-1})/K} K(\sqrt{-1})^\times$$

(if $\mathcal{G}(K(\sqrt{-1})/K) = \langle \varepsilon \rangle$ then this isomorphism is induced by the homomorphism $a \mapsto x_a$ from $K^\times$ to $Z^2(\langle \varepsilon \rangle, K(\sqrt{-1})^\times)$ given by

$x_a(1, 1) = x_a(\varepsilon, 1) = x_a(1, \varepsilon) = 0, x_a(\varepsilon, \varepsilon) = a$) and analogously $H^2(G(R_i), \tilde{R}_i^\times) \cong \tilde{R}_i^\times / N_{\tilde{R}_i/R_i} \tilde{R}_i^\times$ for every $i \in I$. Note that $a \in R_i^\times$ is in $N_{\tilde{R}_i/R_i} \tilde{R}_i^\times$ iff it is positive in the unique ordering on R_i. Thus the map in (e) is injective iff every totally positive element $a \in K^\times$ is in $N_{K(\sqrt{-1})/K} K(\sqrt{-1})^\times$, i.e., $a \in K^\times$ is a sum of two squares in K. ▮

Corollary 3.5. *Let K be a field such that $G(K)$ is real projective and let L be a formally real algebraic extension of K. Then L has the* SAP, *$G(L(\sqrt{-1}))$ is projective and every totally positive element of L is a sum of two squares.*

Proof. The subgroup $(G(L)$ of $G(K)$ is real projective. Apply Proposition 3.3 and Lemma 3.4. ▮

4. Real Projective Pro-2-Groups

For a profinite group with no involutions the notions of projectivity and real projectivity coincide, by definition; likewise freeness and real freeness coincide. Thus if G is a pro-p-group for an odd prime p then G is real free if and only if G is real projective (cf. [2, Proposition 20.37]). We now extend this result to pro-2-groups.

Proposition 4.1. *Let G be a real projective* pro-2-group, *and let X be a closed system of representatives of the conjugacy classes of involutions in G. Then there exists a subset S of G converging to* 1 *such that G is the free* pro-2-group $\hat{D}_2(X, S)$.

Proof. This is essentially proved in [4], in a more general setting, though only for countably generated groups. We give here a simplified proof for our case.

Let $\pi_G \colon G \to \bar{G}$ denote the Frattini map (= the quotient map modulo the Frattini subgroup) of G, and denote $\bar{X} = \pi_G(X)$. Note that $1 \notin \bar{X}$, since there is an open subgroup of G of index $\leqslant 2$ not meeting $\mathrm{Inv}(G)$ (see [5, Proposition 7.7]). There is a closed subgroup $\bar{F}$ of $\bar{G}$ such that $\bar{G} = \langle \bar{X} \rangle \times \bar{F}$ (see [4, Lemma 9.2]). Let F be a minimal closed subgroup of G mapped by π_G onto $\bar{F}$. Then the restriction of π_G to F is a Frattini cover $F \to \bar{F}$. (Cf. [2, Section 20.6] for the notion of Frattini cover.) Moreover, $\bar{F}$ is the Frattini quotient of F, since the Frattini subgroup of $\bar{F}$ is trivial. Now F is projective, since it is contained in the real projective group G and has no involutions (the involutions of G are mapped by π_G onto $\bar{X}$, and $\bar{X} \cap \bar{F} = \varnothing$). Therefore F is a free pro-2-group of the same rank as $\bar{F}$, say m. Fix a free set S of generators of F converging to 1.

Fix a space X', a set S', a homeomorphism $\xi \colon X' \to X$, and a bijection

$\sigma: S' \to S$ and denote $D = \hat{D}_2(X', S')$. Recall that D is the free pro-2 product $\langle X' \rangle * \langle S' \rangle$, where $\langle X' \rangle$ is the free pro-2-product of copies of C_2 over X', and $F' = \langle S' \rangle$ is the restricted free pro-2-group of rank m. Let $\delta: D \to G$ denote the unique homomorphism extending ξ and σ. Note that δ maps F' isomorphically onto F. We claim that δ is an isomorphism.

Indeed, δ is onto, since $\pi_G \circ \delta$ is clearly surjective and π_G is a Frattini cover (cf. [2, Lemma 20.27(b)]). By [6, Lemma 3.5] we know that δ has a right inverse $\gamma: G \to D$. Thus it suffices to show that $\gamma(G) = D$.

For this purpose we consider the Frattini quotient map $\pi_D: D \to \bar{D}$ and show that the homomorphism $\bar{\delta}: \bar{D} \to \bar{G}$ induced by δ is an isomorphism. It then follows that the right inverse $\bar{\gamma}: \bar{G} \to \bar{D}$ of $\bar{\delta}$, which is induced by γ, is necessarily surjective, hence $\pi_D \circ \gamma = \bar{\gamma} \circ \pi_G$ is surjective, whence γ is onto, since π_D is a Frattini cover.

Put $\bar{X}' = \pi_D(X')$ and $\bar{F}' = \pi_D(F')$; then (see [4, Lemma 9.3]) $\bar{D} = \langle \bar{X}' \rangle \times \bar{F}'$. Clearly $\bar{\delta}(\bar{X}') = \bar{X}$, and $\bar{\delta}$ maps $\bar{F}'$ isomorphically onto $\bar{F}$. But δ extends ξ, hence it maps nonconjugate involutions in D onto nonconjugate involutions in G. Thus if $x \in X'$ then $\gamma(\delta(x))$ and x are conjugate in D, whence their images in $\bar{D}$ are equal. Therefore $\bar{\gamma}: \bar{X} \to \bar{X}'$ is the inverse of $\bar{\delta}: \bar{X}' \to \bar{X}$, which implies that $\bar{\delta}: \langle \bar{X}' \rangle \to \langle \bar{X} \rangle$ is an isomorphism. But $\bar{\delta}$ maps $\bar{F}'$ isomorphically onto $\bar{F}$. Therefore $\bar{\delta}: \bar{D} = \langle \bar{X}' \rangle \times \bar{F}' \to \bar{G} = \langle \bar{X} \rangle \times \bar{F}$ is an isomorphism. ∎

PROPOSITION 4.2. *Let G be a* pro-2-group *and assume that* Inv(G) *is closed in G. The following conditions are eqivalent*:

(a) *G is real free in the category of* pro-2-groups.

(b) *G is real projective.*

(c) 1. *Every finite real embedding problem $(\varphi: G \to A,\ \alpha: B \to A)$ with* $\operatorname{Ker} \alpha \cong \mathbb{Z}/2\mathbb{Z}$ *contained in the center of B is solvable, and*

2. *G has the* SAP.

Proof. (a) ⇒ (b): The pro-2 analogue of [6, Corollary 3.3] shows that G is real projective in the category of pro-2-groups, whence G is real projective (Remark 2.4).

(b) ⇒ (a): This implication is Proposition 4.1.

(b) ⇒ (d): This is clear from the definition of a real projective group and from Proposition 3.3.

(c) ⇒ (b): It suffices to solve elvery finite Inv(G)-embedding problem $(\varphi, \alpha: B \to A, C)$ for G in which B is a 2-group and $K = \operatorname{Ker} \alpha \cong \mathbb{Z}/2\mathbb{Z}$ lies in the center of B. By assumption there exists $\psi: G \to B$ such that $\alpha \circ \psi = \varphi$. We shall modify ψ to ensure that it maps Inv(G) into C.

$\mathrm{Inv}(G) \cap \psi^{-1}(\bar{X}_i)$, for $i = 1, ..., n$. The sets $X_1, ..., X_n$ are clopen in $\mathrm{Inv}(G)$, closed under the conjugation in G, and $\mathrm{Inv}(G)$ is their disjoint union. Let $1 \leqslant i \leqslant n$. As G has the SAP, there is a continuous homomorphism $\rho_i: G \to K \cong \mathbb{Z}/2\mathbb{Z}$ such that $\rho_i(X_i)$ is the generator, say ε, of K, and $\rho_i(X_j) = 1$ for $j \neq i$. Let $m_i = 0$ if $\bar{X}_i \subseteq C$, and let $m_i = 1$ if $\bar{X}_i \nsubseteq C$ (in which case $\bar{X}_i \varepsilon \subseteq C$, since $(\varphi, \alpha: B \to A, C)$ is an $\mathrm{Inv}(G)$-embedding problem). Define $\psi': G \to B$ by $\psi'(g) = \psi(g)\, \rho_1(g)^{m_1} \cdots \rho_n(g)^{m_n}$. Since K is in the center of B, it is easy to see that ψ' is a continuous homomorphism such that $\alpha \circ \psi = \varphi$ and $\psi'(X_i) \subseteq C$ for $1 \leqslant i \leqslant n$. Thus ψ' solves $(\varphi, \alpha: B \to A, C)$. ▮

COROLLARY 4.3. *Let K be a formally real field such that $G(K)$ is a* pro-2-group. *Then $G(K)$ is a real free* pro-2-group *iff K has the* SAP, *$G(K(\sqrt{-1}))$ is a free* pro-2-group, *and every totally positive element of K is a sum of two squares. (The last condition can be replaced by any of the equivalent conditions of Lemma* 3.4.)

Proof. The conditions are necessary by Corollary 3.5. Conversely, if the conditions hold, then $G(K)$ has the SAP (Remark 3.2) and every finite real embedding problem $(\varphi: G \to A,\ \alpha: B \to A)$ with $\mathrm{Ker}\, \alpha \cong \mathbb{Z}/2\mathbb{Z}$ contained in the center of B is solvable (Lemma 3.4). Thus $G(K)$ is a real free pro-2-group. ▮

THEOREM 4.4. *Let K be an algebraic extension of $\mathbb{Q}$ such that $G(K)$ is a* pro-p-group. *If $G(K(\sqrt{-1}))$ is a free* pro-p-group *then $G(K)$ is a real free* pro-p-group.

Proof. If K is not formally real then $G(K)$ is torsion free, and hence a free pro-p-group, by a theorem of Serre ([14, Corollaire 2]). Assume that K is formally real, whence $G(K)$ is a pro-2-group. For each valuation v on K let K_v be the completion of K with respect to v. Then $H^2(G(K), \tilde{K}^\times) \to \prod_v H^2(G(K_v), \tilde{K}_v^\times)$ is injective ([11, Satz II]).

The group $G(K_v)$ may be identified with a subgroup of $G(K)$, so its subgroup $G(K_v(\sqrt{-1}))$ is a subgroup of $G(K(\sqrt{-1}))$, and hence real free. Thus if K_v is not formally real then again by Serre's theorem $G(K_v)$ (and hence also every closed subgroup of it) is projective; in particular, $B(K_v) = H^2(G(K_v), \tilde{K}_v^\times) = 0$ in this case (cf. [13, p. 263]). But if K_v is formally real then $K_v \cong_K \mathbb{R}$ is a real closed extension of K, it induces an ordering on K via the embedding $K \to \mathbb{R}$, and nonequivalent valuations induce distinct orderings on K. Therefore condition (d) in Lemma 3.4 is satisfied. As K has the SAP ([12, Corollary 9.2]), our assertion follows from Corollary 4.3. ▮

5. Characterization of Real Projective Groups by Their Sylow Subgroups

A profinite group is projective iff its Sylow p-subgroup is a free pro-p-group for every p ([2, Proposition 20.47]). The straightforward analog of this is not valid for real projective groups. E.g., the direct product of $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}_3$ is not real projective, although $\mathbb{Z}/2\mathbb{Z}$ is a real free pro-2-group and $\mathbb{Z}_3$ is a (real) free pro-3-groups. However, the correct statement (Proposition 5.5) is not very far from this.

Lemma 5.1. *Let A be an abelian normal subgroup of a finite group G and let H be a subgroup of G containing A such that $(G:H)$ is prime to $^{\#}A$. Suppose that A has a complement K in H. Then A has a complement L in G with the followng property: If δ is an involution in G such that*

$$\delta^g \in H \Rightarrow \delta^g \in \bigcup_{h \in H} K^h, \qquad \textit{for every} \quad g \in G \tag{1}$$

then δ has a conjugate in L.

Proof (after Brandis [1, Section 2]). For $x, y \in G$ such that $xy^{-1} \in H$ let $k(x, y)$ denote the unique element of K that satisfies $k(x, y)A = xy^{-1}A$. Fix a system Φ of representatives of the right cosets of G modulo H. Then the set

$$L = \{g \in G \mid \prod (r_1 g)^{-1} k(r_1 g, r_2) r_2 = 1\},$$

where the product ranges over pairs $(r_1, r_2) \in \Phi \times \Phi$ with $r_1 g r_2^{-1} \in H$, is a complement of A in G [1, Satz 2.6].

Let $\delta \in \mathrm{Inv}(K)$ satisfy (1). If we replace Φ in the above definition by another system Φ' of representatives of the right cosets of G modulo H then the resulting complement L' is a conjugate of L in G [1, Lemma 2.7]. Using (1) we may choose Φ' so that for all $r \in \Phi'$ we have

$$Hr\delta \neq Hr \Rightarrow r, r\delta \in \Phi',$$

$$Hr\delta = Hr \Rightarrow r\delta r^{-1} \in K.$$

(Indeed, the condition $Hr\delta = Hr$ implies that $r\delta r^{-1} \in H$, hence $r\delta r^{-1} \in K^h$ for some $h \in H$, by (1); replace r by hr to obtain $r\delta r^{-1} \in K$.)

If $r_1, r_2 \in \Phi'$ and $Hr_1\delta = Hr_2$ then either $Hr_1\delta \neq Hr_1$ or $Hr_1\delta = Hr_1$. In the first case $r_1\delta \in \Phi'$, and $Hr_1\delta = Hr_2$, so $r_1\delta = r_2$. Thus $k(r_1\delta, r_2) = 1$, whence $[(r_1\delta)^{-1} k(r_1\delta, r_2) r_2] = (r_1\delta)^{-1} r_2 = 1$. In the second case $Hr_1 = Hr_2$, so $r_1 = r_2$. In particular $Hr_1\delta = Hr_1$, hence by the choice of Φ' we have $r_1\delta r_1^{-1} \in K$. Thus $k(r_1\delta, r_1) = r_1\delta r_1^{-1}$, whence $(r_1\delta)^{-1} k(r_1\delta, r_1) r_1 = 1$. It follows that $\delta \in L'$, whence a conjugate of δ is in L. ∎

We shall need a slight generalization of [8, Lemma 2.4]. The set $\mathrm{Subg}(G)$ of closed subgroups of a profinite group G is a Boolean space: it is the inverse limit of the finite sets $\mathrm{Subg}(G/N)$, where N runs through the open normal subgroups of G. Let G continuously act on a Boolean space X. Denoting by $D(x)$ the stabilizer of $x \in X$ we get a map $D: X \to \mathrm{Subg}(G)$. Note that if $N \lhd G$ then G/N acts on X/N, and $D(xN) = D(x)N$ for every $x \in X$.

LEMMA 5.2. *Let G be a profinite group continuously acting on a Boolean space X. If the map $D: X \to \mathrm{Subg}(G)$ is continuous then there exists a closed system X_0 of representatives of the G-orbits in X.*

Proof. Assume first that G is finite, whence D is locally constant. (This case is due to M. Jarden.) Then for every $x \in X$ there exists a clopen neighbourhood $U \subseteq X$ such that

(i) $D(y) = D(x)$ for every $y \in U$ and

(ii) $x^\sigma \notin U$ for each $\sigma \notin D(x)$.

Replace U by $U \smallsetminus \bigcup_{\sigma \notin D(x)} U^\sigma$, if necessary, to assume that $U^\sigma \cap U = \varnothing$ for all $\sigma \notin D(x)$.

From this point one may proceed as in the proof of [8, Lemma 2.4]. ∎

LEMMA 5.3. *Let G be a profinite group such that* $\mathrm{Inv}(G)$ *is closed in G and*

$$\{\sigma \in G \mid \varepsilon^\sigma = \varepsilon\} = \{\varepsilon, 1\} \qquad \textit{for every} \quad \varepsilon \in \mathrm{Inv}(G). \tag{2}$$

(a) *There exists a closed system X of representatives of the conjugacy classes of* $\mathrm{Inv}(G)$.

(b) *Let G_2 be a closed subgroup of G. If X is as in* (a) *and Φ is a closed system of representatives of the left cosets of G_2 in G then*

$$X_2 = \{x^r \mid x \in X \;\&\; r \in \Phi\} \cap G_2 \tag{3}$$

is a closed system of representatives of the conjugacy classes of involutions in G_2. Moreover, if $r, s \in \Phi$ and $x, y \in X$ such that $x^r = y^s \in X_2$ then $x = y$ and $r = s$.

Proof. (a) G acts on $\mathrm{Inv}(G)$ by conjugation, and the map $D: \mathrm{Inv}(G) \to \mathrm{Subg}(G)$, given by $D(x) = \{1, x\}$, is obviously continuous. Apply Lemma 5.2.

(b) For the existence of Φ see [13, p. 31].

Clearly X_2 is a closed set. If $\varepsilon \in \mathrm{Inv}(G_2)$, there are $x \in X$ and $g \in G$ such that $\varepsilon = x^g$. Write g as $r\gamma$, where $r \in \Phi$ and $\gamma \in G_2$; then ε is conjugate in G_2 to $x^r \in X_2$. If $r, s \in \Phi$ and $x, y \in X$ such that $y^s \in X_2$ and x^r is conjugate in

G_2 to y^s, then x and y are conjugate in G, hence $x=y$. Thus $x^s=x^{r\gamma}$ for some $\gamma\in G_2$. By assumption, $r\gamma s^{-1}\in\langle x\rangle$, whence $r\gamma\in s\langle x^s\rangle$. But $x^s=y^s\in X_2\subseteq G_2$. Therefore $rG_2=sG_2$, whence $r=s$. ▮

For the next lemma let G, G_2, X, Φ, X_2 be as in Lemma 5.2. Furthermore assume that G_2 is a Sylow 2-subgroup of G and that G_2 is a real free pro-2-group. Fix a subset S of G_2 converging to 1 such that $G_2=\hat{D}_2(X_2, S)$; it exists by Proposition 4.1. Consider a finite $\mathrm{Inv}(G)$-embedding problem $(\varphi, \alpha\colon B\to A, C)$ for G such that $\varphi(G)=A$; then $A_2=\varphi(G_2)$ is a Sylow 2-subgroup of A. Assume that $B_2=\alpha^{-1}(A_2)$ is a Sylow 2-subgroup of B, i.e., $\operatorname{Ker}\alpha$ is a 2-group.

LEMMA 5.4. (a) *There exist continuous maps* $\psi_X\colon X\to C$, $\psi_S\colon S\to B_2$, *and* $\rho\colon\Phi\to B$ *such that* $\alpha\circ\psi_X=\mathrm{res}_X\,\varphi$, $\alpha\circ\psi_S=\mathrm{res}_S\,\varphi$ *and* $\alpha\circ\rho=\mathrm{res}_\Phi\,\varphi$.

Let ψ_X, ψ_S, *and* ρ *be maps as in* (a).

(b) *There exists a unique continuous homomorphism* $\psi_2\colon G_2\to B_2$ *extending* ψ_S *and satisfying*

$$\psi_2(x^r)=\psi_X(x)^{\rho(r)},\qquad \text{for all}\quad x\in X \text{ and } r\in\Phi \text{ such that } x^r\in G_2. \tag{4}$$

(c) *We have* $\alpha\circ\psi_2=\mathrm{res}_{G_2}\,\varphi$.

(d) *Let* $N=\varphi^{-1}(A_2)$. *For every* $y\in\mathrm{Inv}(N)$ *there is* $g\in N$ *such that* $y^g\in G_2$.

(e) *Let* $x_2\in X_2$ *and* $b\in B$. *If* $\psi_2(x_2)^b\in B_2$ *then* $\psi_2(x_2)^b\in\bigcup_{b'\in B_2}\psi_2(G_2)^{b'}$.

(f) *Let* L *be a subgroup of* B *mapped by* α *isomorphically onto* A, *and let* $b\in L$. *If there is* $c\in C$ *such that* $\alpha(b)=\alpha(c)$ *and* c *has a conjugate in* L *then* $b\in C$.

Proof. (a) We have $\varphi(X)\subseteq\alpha(C)$. Let $\lambda\colon A\to B$ be a set-theoretic right inverse of $\alpha\colon B\to A$ such that $\lambda(\varphi(x))\in C$ for every $x\in X$. Then $\lambda\circ\varphi(G_2)\subseteq B_2$, and the respective restrictions of $\lambda\circ\varphi$ to X, S, and Φ satisfy the requirements.

(b) By Lemma 5.3 there is a unique continuous map $\psi_2\colon X_2\to B$ that satisfies (4). A fortiori $\psi_2(X_2)\subseteq B_2$; indeed, if $x\in X$, $r\in\Phi$ such that $x^r\in X_2$, then

$$\alpha\circ\psi_2(x^r)=\alpha[\psi_X(x)^{\rho(r)}]=\varphi(x)^{\varphi(r)}=\varphi(x^r)\in\varphi(G_2)=A_2.$$

Thus ψ_2 together with ψ_S extend to a unique homomorphism $\psi_2\colon G_2=\hat{D}_2(X_2, S)\to B_2$.

(c) Clearly $\alpha\circ\mathrm{res}_{X_2}\psi_2=\mathrm{res}_{X_2}\varphi$; also, $\alpha\circ\mathrm{res}_S\,\psi=\alpha\circ\psi_S=\mathrm{res}_S\,\varphi$. Therefore $\alpha\circ\psi_2=\mathrm{res}_{G_2}\,\varphi$.

(d) Consider the left cosets space $G_2\backslash N$. The supernatural number $(N{:}G_2)$ is odd, since $(N{:}G_2)$ divides $(G{:}G_2)$. But $gG_2 \to ygG_2$ is a permutation of $G_2\backslash N$ of order $\leqslant 2$. Therefore it has a fixed point, say gG_2, with $g \in N$; clearly $y^g \in G_2$.

(e) Write x_2 as x^s, where $x \in X$ and $s \in \Phi$, and put $a = \varphi(s)\,\alpha(b) \in A$. It suffices to find $r \in G$ such that $\varphi(r)\,A_2 = aA_2$ and $x^r \in G_2$. Indeed, then without loss of generality $r \in \Phi$, and $\rho(r)\,B_2 = \rho(s)\,bB_2$, since $B_2 = \alpha^{-1}(A_2)$. Let $b' \in B_2$ such that $\rho(r)b' = \rho(s)b$; then

$$\psi_2(x_2)^b = \psi_X(x)^{\rho(s)b} = \psi_X(x)^{\rho(r)b'} = \psi_2(x^r)^{b'} \in \psi_2(G_2)^{b'},$$

as claimed.

Choose $g_0 \in G$ such that $\varphi(g_0) = a$ and let $y = x^{g_0}$. Then

$$\begin{aligned}\varphi(y) &= \varphi(x)^a = (\alpha \circ \psi_X(x))^{\varphi(s)\alpha(b)}\\ &= \alpha(\psi_X(x)^{\rho(s)b}) = \alpha(\psi_2(x_2)^b) \in \alpha(B_2) = A_2,\end{aligned}$$

so by (d) there is $g \in N$ such that $\varphi(g) \in A_2$ and $y^g \in G_2$. Thus $r = g_0 g$ has the required property.

(f) There is a conjugate $c' \in L$ of c; a fortiori $c' \in C$. Thus $\alpha(b)$ and $\alpha(c')$ are conjugate in A, hence b and c' are conjugate in L, and therefore also in B, whence $b \in C$. ∎

PROPOSITION 5.5. *A profinite group G is real projective if and only if*:

(a) *For every prime p the Sylow p-subgroup G_p of G is a real free* pro-p-group; *and*

(b) *For every $\varepsilon \in \mathrm{Inv}(G)$ we have $\{\sigma \in G \mid \varepsilon^\sigma = \varepsilon\} = \{\varepsilon, 1\}$.*

Proof. If G is real projective then G_p is real projective for every p. For (b) see [6, Corollary 3.2 and Theorem 3.6].

Conversely, assume (a) and (b). Then $\mathrm{Inv}(G)$ is closed in G, since it is the image of the compact $\mathrm{Inv}(G_2) \times G$ under the continuous map $(\varepsilon, \sigma) \to \varepsilon^\sigma$. By Proposition 2.3(c) it suffices to solve every finite $\mathrm{Inv}(G)$-embedding problem $(\varphi, \alpha{:}\ B \to A, C)$ for G in which $\mathrm{Ker}\,\alpha$ is an elementary abelian p-group. Without loss of generality $\varphi(G) = A$. Fix a Sylow p-subgroup G_p of G; then $A_p = \varphi(G_p)$ and $B_p = \alpha^{-1}(A_p)$ are Sylow p-subgroups of A and B, respectively. Choose (Lemma 5.3(a)) a closed system X of representatives of the conjugacy classes of involutions in G.

If $p = 2$, let Φ be a closed system of representatives of the left cosets of G_2 in G containing 1 and define X_2 by (3). Also choose $\psi_X{:}\ X \to C$, $\psi_S{:}\ S \to B_2$, and $\rho{:}\ \Phi \to B$ satisfying Lemma 5.4(a). Let $\psi_2{:}\ G_2 \to B_2$ satisfy Lemma 5.4(b); then $\alpha \circ \psi_2 = \mathrm{res}_{G_2}\,\varphi$. If $p \neq 2$, there exists $\psi_p{:}\ G_p \to B_p$ such that $\alpha \circ \psi_p = \mathrm{res}_{G_2}\,\varphi$, since G_p is real projective. In both cases $K = \psi_p(G_p)$ is mapped via α onto A_p. We first make the following

Assumption. α is injective on K, that is a complement to $\operatorname{Ker}\alpha$ in B.

Note that $(B:B_p)$ is prime to p, hence to $|\operatorname{Ker}\alpha|$. By Lemma 5.1, $\operatorname{Ker}\alpha$ has a complement L in B such that if $p=2$ and $\delta\in K$ is an involution and

$$\delta^b\in B_2 \Rightarrow \delta^b\in \bigcup_{b'\in B_2} K^{b'}, \qquad \text{for every} \quad b\in B \tag{5}$$

then δ has a conjugate in L. Let $\alpha'\colon A\to L$ be the inverse of $\operatorname{res}_L\alpha\colon L\to A$. Then $\psi=\alpha'\circ\varphi\colon G\to B$ satisfies $\alpha\circ\psi=\varphi$. To complete the proof it is enough to show that $\psi(x)\in C$ for every $x\in X$.

Case I. p is odd. By assumption there is $c\in C$ such that $\alpha\circ\psi(x)=\varphi(x)=\alpha(c)$. As $(B:L)=|\operatorname{Ker}\alpha|$ is odd, L contains a Sylow 2-subgroup of B, whence c has a conjugate in L. Thus $\psi(x)\in C$ by Lemma 5.4(f).

Case II. $p=2$. There is $r\in G$ such that $x^r\in G_2$; without loss of generality $r\in\Phi$. Then $x^r\in X_2$, so $\delta=\psi_2(x^r)=\psi_X(x)^{\rho(r)}\in C$, since $\psi_X(X)\subseteq C$. By Lemma 5.4(e), δ satisfies (5), therefore δ has a conjugate in L. But $\alpha(\delta)=\alpha\circ\psi_2(x^r)=\varphi(x^r)=\alpha\circ\psi(x^r)$, hence $\psi(x)^r=\psi(x^r)\in C$ by Lemma 5.4(f). Thus $\psi(x)\in C$.

To eliminate the above made assumption, let N be an open normal subgroup of G such that $N\cap G_p\subseteq\operatorname{Ker}\psi_p$. Define $\hat A=G/N$, $\hat B=B\times_A\hat A$, let $\hat\alpha\colon\hat B\to\hat A$ and $\pi\colon\hat B\to B$ be the projection maps, and put $\hat C=\{\delta\in\operatorname{Inv}(\hat B)\mid\pi(\delta)\in C\}$. We obtain the diagram

$$\begin{tikzcd}
 & G \arrow[d, "\hat\varphi"] \arrow[dd, bend left, "\varphi"] \\
\hat B \arrow[r, "\hat\alpha"] \arrow[d, "\pi"] & \hat A \arrow[d, "\varphi_0"] \\
B \arrow[r, "\alpha"] & A
\end{tikzcd}$$

Clearly $(\hat\varphi, \alpha\colon\hat B\to\hat A, \hat C)$ is a finite $\operatorname{Inv}(G)$-embedding problem for G with kernel isomorphic to $\operatorname{Ker}\alpha$, and a solution $\hat\psi\colon G\to\hat B$ of it gives a solution $\pi\circ\hat\psi$ of the original problem. Now let $\hat A_p=\hat\varphi(G_p)$, $\hat B_p=\hat\alpha^{-1}(\hat A_p)$. Let $\hat\psi_p\colon G_p\to\hat B$, $\hat\psi_X\colon X\to\hat B$, $\hat\psi_S\colon S\to\hat B$, and $\hat\rho\colon\Phi\to\hat B$ be the unique maps that satisfy

$$\begin{aligned}
\hat\alpha\circ\hat\psi_p&=\operatorname{res}_{G_p}\hat\varphi &&\text{and} && \pi\circ\hat\psi_p=\psi_p,\\
\hat\alpha\circ\hat\psi_X&=\operatorname{res}_X\hat\varphi &&\text{and} && \pi\circ\hat\psi_X=\psi_X,\\
\hat\alpha\circ\hat\psi_S&=\operatorname{res}_S\hat\varphi &&\text{and} && \pi\circ\hat\psi_S=\psi_S,\\
\hat\alpha\circ\hat\rho&=\operatorname{res}_\Phi\hat\varphi &&\text{and} && \pi\circ\hat\rho=\rho.
\end{aligned}$$

Then $\hat{\psi}_p(G) \subseteq \hat{B}_p$, $\hat{\psi}_X(X) \subseteq \hat{C}$, and $\hat{\psi}_S(S) \subseteq \hat{B}_p$, and $\hat{\psi}_p$ is the unique map defined by $\hat{\psi}_X$, $\hat{\psi}_S$, and $\hat{\rho}$ in Lemma 5.4(a). But $\hat{\alpha}$ is injective on $\hat{K} = \hat{\psi}_p(G_p)$: if $\hat{\alpha} \circ \hat{\psi}_p(g) = 1$ then $\hat{\varphi}(g) = 1$, hence $g \in N$, whence also $\pi \circ \hat{\psi}_p(g) = 1$; therefore $\hat{\psi}_p(g) \in (\mathrm{Ker}\,\hat{\alpha}) \cap (\mathrm{Ker}\,\pi) = 1$. Thus replacing $\alpha\colon B \to A$, φ, C, K by $\alpha\colon \hat{B} \to \hat{A}$, $\hat{\varphi}$, $\hat{C}$, $\hat{K}$ we obtain the desired property. ∎

6. Real Projective Subgroups of $G(\mathbb{Q})$

THEOREM 6.1. *Let K be an algebraic extension of $\mathbb{Q}$. The following conditions are equivalent*:

(a) *$G(K)$ is real projective*;

(b) *$G(K)$ is virtually projective*;

(c) *$G(K(\sqrt{-1}))$ is projective.*

Proof. If $G(K)$ is real projective then its subgroup $G(K(\sqrt{-1}))$ is real projective, but has no involutions, and hence is projective. If $G(K)$ is virtually projective then, obviously, so is $G(K(\sqrt{-1}))$; but the latter is torsion free, hence $G(K(\sqrt{-1}))$ is projective ([2, Proposition 20.47] and [14, Corollaire 2]). Thus only (c) $\Rightarrow$ (a) remains to be shown.

Assume that $G(K(\sqrt{-1}))$ is projective. By the Artin-Schreier theory we know that $\{\sigma \in G(K) \mid \varepsilon^\sigma = \varepsilon\} = \{\varepsilon, 1\}$ for every $\varepsilon \in \mathrm{Inv}(G)$. Thus by Proposition 5.5 we may replace $G(K)$ by its Sylow p-subgroup, and hence assume that $G(K(\sqrt{-1}))$ is a free pro-p-group. The assertion now folows from Theorem 4.4. ∎

COROLLARY 6.2. *Let K be an algebraic extension of $\mathbb{Q}$. If $K(\sqrt{-1})$ contains the maximal abelian extension $\mathbb{Q}^{ab}$ of $\mathbb{Q}$ then $G(K)$ is real projective.*

Proof. One can deduce from [13, p. 303] that $cd_l(G(\mathbb{Q}^{ab})) = 1$ for every l, i.e., $G(\mathbb{Q}^{ab})$ is projective. ∎

COROLLARY 6.3. *Let G be a closed subgroup of $G(\mathbb{Q})$ generated by involutions. Then G is real projective.*

Proof. All involutions in $G(\mathbb{Q})$ are conjugate, therefore their restrictions to $\mathbb{Q}^{ab}$ are equal. Let $\varepsilon \in G(\mathbb{Q}^{ab}/\mathbb{Q})$ be this restriction and let $K_0 \subseteq \mathbb{Q}^{ab}$ be its fixed field; then $\varepsilon^2 = 1$ and $\varepsilon(\sqrt{-1}) = -\sqrt{-1}$, hence $K_0(\sqrt{-1}) = \mathbb{Q}^{ab}$. Let K be the fixed field of G in $G(\mathbb{Q})$. Then $K \cap \mathbb{Q}^{ab} = K_0$, hence $\mathbb{Q}^{ab}(\varepsilon) \subseteq K$, whence $\mathbb{Q}^{ab} \subseteq K(\sqrt{-1})$. Thus $G = G(K)$ is real projective by Corollary 6.2. ∎

We conclude with an open problem. Note that though we have necessary and sufficient conditions for the absolute Galois group of a field K to be real projective, we do not know to what extent these conditions are essential. In particular we may even ask:

Problem 6.4. Let K be a field of characteristic 0 such that $G(K(\sqrt{-1}))$ is projective. Is $G(K)$ real projective?

REFERENCES

1. A. BRANDIS, Verschränkte Homomorphismen endlicher Gruppen, *Math. Z.* **162** (1978), 205–217.
2. M. FRIED AND M. JARDEN, "Field Arithmetic," Ergebnisse der Mathematik und ihrer Grenzgebiete (3), Vol. II, Springer-Verlag, Berlin/New York, 1987.
3. W.-D. GEYER, Galois groups of intersections of local fields, *Israel J. Math.* **30** (1978), 382–396.
4. D. HARAN, On closed subgroups of free products of profinite groups, *Proc. London Math. Soc.* (3) **55** (1987), 266–298.
5. D. HARAN AND M. JARDEN, The absolute Galois group of a pseudo real closed field, *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* (4) **12** (1985), 449–489.
6. D. HARAN AND M. JARDEN, Real free groups and the absolute Galois group of $\mathbb{R}(t)$, *J. Pure Appl. Algebra* **37** (1985), 155–165.
7. D. HARAN AND M. JARDEN, The absolute Galois group of a pseudo real closed algebraic field, *Pacific J. Math.* **123** (1986), 55–69.
8. D. HARAN AND M. JARDEN, The absolute Galois group of a pseudo p-adically closed algebraic field, *J. Reine Angew. Math.* **383** (1988), 147–206.
9. D. HARAN AND A. LUBOTZKY, Maximal abelian subgroups of free profinite groups, *Math. Proc. Cambridge Philos. Soc.* **97** (1985), 51–55.
10. S. LANG, "Algebra" (2nd edition), Addison–Wesley, Reading, MA, 1964.
11. J. NEUKIRCH, Über eine algebraische Kennzeichnung der Henselkörper, *J. Reine Angew. Math.* **231** (1968), 75–81.
12. A. PRESTEL, "Lectures on Formally Real Fields," IMPA, Rio de Janeiro, 1975, and Lecture Notes in Mathematics, Vol. 1093, Springer-Verlag, Berlin/New York, 1984.
13. L. RIBES, "Introduction to Profinite Groups and Galois Cohomology," Queen's Papers in Pure and Applied Mathematics, Vol. 24, Queen's Univ., Kingston, Ontario, 1970.
14. J.-P. SERRE, Sur la dimension cohomologique des groupes profinis, *Topology* **3** (1965), 413–420.