THE ABSOLUTE GALOIS GROUP OF A PSEUDO REAL CLOSED ALGEBRAIC FIELD

DAN HARAN AND MOSHE JARDEN

The absolute Galois group of a PRC (= pseudo real closed) field is characterized as a real projective group. Specifically, it is known that if E is a PRC field, then its absolute Galois group $G(E)$ is real projective. Conversely, if G is a real projective group, then there exists a PRC field E such that $G(E) \cong G$. The construction of E makes it of infinite transcendence degree over Q. However, if a field E is algebraic over Q, then rank $G(E) \leq \aleph_0$. Therefore it is natural to ask whether for a given real projective group G of rank $\leq \aleph_0$ we may choose E to be algebraic over Q.

There are two reasons for asking this question. First of all, the corresponding question for projective groups and PAC fields is known to have an affirmative answer, since there exist algebraic PAC fields E such that $G(E) \cong \hat{F}_\omega$ = the free profinite group of ranks $\aleph_0$ and since every projective group G of rank $\leq \aleph_0$ is isomorphic to a closed subgroup of $\hat{F}_\omega$. A generalization of this fact to real projective groups and PRC fields will be a contribution to the desired description of the closed subgroups of $G(\mathbf{Q})$. Secondly, an affirmative answer to this question will give us a necessary tool to the study of the elementary theory of all PRC fields which are algebraic over Q.

The main goal of this work is indeed to give the desired affirmative answer:

THEOREM. *If K is a countable formally real Hilbertian field and G is a real projective group of* rank $\leq \aleph_0$, *then there exists a PRC algebraic extension E of K such that $G(K) \cong G$.*

In order to make this introduction self-contained we repeat the basic definitions involved in the Theorem.

A field E is said to be PRC (= pseudo real closed), if every absolutely irreducible variety V defined over K, which has a simple $\overline{K}$-rational point in every real closed field $\overline{K}$ containing K, has a K-rational point.

A diagram

$$\begin{array}{ccc} & & G \\ & & \downarrow \varphi \\ B & \xrightarrow[\alpha]{} & A \end{array} \tag{1}$$

of epimorphisms of profinite groups is said to be a *real embedding problem for* G if for every involution (i.e. element of order 2) g of G such that $\varphi(g) \neq 1$ there exists an involution b of B such that $\alpha(b) = \varphi(g)$. The problem is *finite* if B is a finite group.

A profinite group is said to be *real projective* if the subset Inv G of all involutions of G is closed and every finite real embedding problem (1) for G is solvable, i.e., there exists a homomorphism $\gamma\colon G \to B$ such that $\alpha \circ \gamma = \varphi$.

We sketch here the basic ideas involved in the proof of the Theorem. We choose a closed system X of representatives for the conjugacy classes of Inv G and choose a sequence S of generators for G that converges to 1. Let $\hat{D} = D(X, S)$ be the real free group in the sense of [**6**] with the basis (X, S). Then the obvious surjection $\hat{D} \to G$ induces a cover of the corresponding Artin-Schreier structures [**5**]. Hence it has a section, and consequently G is isomorphic to a closed subgroup of $\hat{D}$.

Secondly, we show that the Boolean space $X_\omega = \{\pm 1\}^{\mathbf{N}}$ together with a discrete sequence form a basis for a universal real free group $\hat{D}_\omega$ of countable rank, which, among other properties, contains all real free groups of rank $\leq \aleph_0$ as closed subgroups.

Using a theorem of Binz-Neukirch-Wenzel about open subgroups of free product of profinite groups and a method of Lubotzky-v.d. Dries, we embed $\hat{D}_\omega$ as a closed normal subgroup of the free real group $\hat{D}_{e,f}$, where $e \geq 1$ and $f \geq 2$.

Now it is well known that K has an algebraic PRC extension K_σ such that $G(K_\sigma) \cong \hat{D}_{e,f}$ [**5**]. By what has been said above K_σ has an algebraic extension E such that $G(E) \cong G$. By the Prestel extension theorem E is also PRC.

1. Boolean spaces of countable weight. A topological space X is a *Boolean space* if it is an inverse limit of finite discrete spaces. Two other equivalent definitions are:

(a) X is a compact totally disconnected Hausdorff space;

(b) X is compact and every $x \in X$ has a basis of closed-open neighbourhoods, whose intersection is $\{x\}$.

The following lemma characterizes a subclass of Boolean spaces. Here an inverse limit of topological spaces $X = \varprojlim X_i$, where i ranges over $\mathbf{N} = \{1, 2, \dots\}$ with its usual order, is said to be the inverse limit of a *sequence* of spaces. We leave the proof of the lemma to the reader. Our suggestion is to prove the implications (a) $\Rightarrow$ (b) $\Rightarrow$ (c) $\Rightarrow$ (d) $\Rightarrow$ (a) and (c) $\Rightarrow$ (e) $\Rightarrow$ (f) $\Rightarrow$ (b).

LEMMA 1.1. *The following conditions on a Boolean space X are equivalent*:

(a) *X has a countable basis for its topology*;

(b) *the family of closed-open subsets of X is countable*;

(c) *X is the inverse limit of a sequence of finite discrete spaces*;

(d) *X is homeomorphic to a closed subset of the product space $\{\pm 1\}^{\mathbf{N}}$*;

(e) *given two continuous surjections $\varphi\colon \{\pm 1\}^{\mathbf{N}} \to X_0$ and $\alpha\colon X \to X_0$ onto a finite discrete space X_0, there exists a continuous surjection $\gamma\colon \{\pm 1\}^{\mathbf{N}} \to X$ such that $\alpha \circ \gamma = \varphi$*;

(f) *either $X = \emptyset$ or X is a quotient space of $\{\pm 1\}^{\mathbf{N}}$, i.e., there exists a continuous surjection $\{\pm 1\}^{\mathbf{N}} \to X$.*

A Boolean space satisfying either of the conditions of Lemma 1.1 is said to be of *weight* $\leq \aleph_0$ [**6**, §2].

We now focus our attention on one of these spaces. The equivalence of (a) and (b) in the following lemma follows from [**7**, Corollary 2–98 and Corollary 2–59], that of (b) and (c) from [**4**, IV.4.1]. We leave the implications (a) $\Leftrightarrow$ (d). (c) & (d) $\Rightarrow$ (e), (e) $\Rightarrow$ (a), (c) $\Rightarrow$ (f) and (f) $\Rightarrow$ (a) to the reader.

LEMMA 1.2. *The following conditions on a nonempty Boolean space X_ω of weight $\leq \aleph_0$ are equivalent.*

(a) *X_ω is perfect, i.e., has no isolated points.*

(b) *X_ω is homeomorphic to the Cantor 'middle thirds' set.*

(c) *X_ω is homeomorphic to $\{\pm 1\}^{\mathbf{N}}$.*

(d) *$|X_\omega| > 1$ and every nonempty closed-open subset of X_ω is homeomorphic to X_ω.*

(e) *Let X be a Boolean space of weight $\leq \aleph_0$, let X_0 be a finite discrete space and let $\varphi\colon X_\omega \to X_0$ and $\alpha\colon X \to X_0$ be continuous maps. If $\alpha(X) \subseteq \varphi(X_\omega)$, then there exists a continuous injection $\gamma\colon X \to X_\omega$ such that $\varphi \circ \gamma = \alpha$.*

(f) *Let $\varphi\colon X_\omega \to X_0$ and $\alpha\colon X \to X_0$ be as in* (e). *If $\alpha(X) = \varphi(X_\omega)$, then there exists a continuous surjection $\gamma\colon X_\omega \to X$ such that $\alpha \circ \gamma = \emptyset$.*

DEFINITION 1.3. The Boolean space X_ω satisfying one, and hence all, of the conditions of Lemma 1.2 is called the *universal Boolean space of weight* $\aleph_0$.

2. The group $\hat{D}_\omega$. Real free groups have been introduced in [**6**]. In this work we are interested in real free groups of countable rank. Among them there is a universal one denoted $\hat{D}_\omega$. In the notation of [**6**, §1] it is

defined as

$$\hat{D}_\omega = \hat{D}(X_\omega, S_\omega) = \hat{D}(X_\omega, X_\omega, 1),$$

where X_ω is the universal Boolean space of weight $\aleph_0$ and Y_ω is the one point compactification of a countable discrete space S_ω (and 1 is the compactification point of Y_ω). In other words $\hat{D}_\omega$ contains the spaces X_ω and Y_ω as disjoint closed subspaces, the elements of X_ω are involutions of $\hat{D}_\omega$ (i.e. of order 2) and the following universal property is satisfied.

(1) Every continuous map φ from $X_\omega \cup Y_\omega$ into a profinite group G, such that $\varphi(x)^2 = 1$ for every $x \in X_\omega$ and $\varphi(1) = 1$; uniquely extends to a homomorphism $\varphi\colon \hat{D}_\omega \to G$.

The following properties of $\hat{D}_\omega$ follow from the study of real free groups in [**6**].

(2) $\operatorname{rank}(\hat{D}_\omega) = \aleph_0$ (since both X_ω and Y_ω are of weight $\aleph_0$, by [**6**, Lemma 2.2]).

(3) $\operatorname{Inv}\hat{D}_\omega$ is closed in $\hat{D}_\omega$, and X_ω is a closed system of representatives of the distinct conjugacy classes of $\operatorname{Inv}\hat{D}_\omega$ [**6**, Corollaries 3.2 and 3.3].

(4) $\hat{D}_\omega$ is real projective, i.e., if $\alpha\colon B \to A$ is an epimorphism of finite groups and $\varphi\colon \hat{D}_\omega \to A$ is a homomorphism and if for every $\varepsilon \in \operatorname{Inv}\hat{D}_\omega$ such that $\varphi(\varepsilon) \neq 1$ there exists a $b \in \operatorname{Inv}B$ such that $\alpha(b) = \varphi(\varepsilon)$, then there exists a homomorphism $\gamma\colon \hat{D}_\omega \to B$ such that $\alpha \circ \gamma = \varphi$ [**6**, Corollary 3.3].

(5) The subsets Y_ω and S_ω of $\hat{D}_\omega$ converge to 1, i.e., for every open subgroup N of $\hat{D}_\omega$ the set $Y_\omega - N = S_\omega - N$ is finite (since it is closed in Y_ω, hence compact, and discrete).

(6) Every closed subgroup of $\hat{D}_\omega$ is a real projective group of rank $\leq \aleph_0$ (by (2) and [**5**, Corollary 10.5]).

(7) the following characterization of $\hat{D}_\omega$ makes it especially attractive:

PROPOSITION 2.1. *Let R be a countable real closed field and let $F = R(t)$ be the field of rational functions in one variable over R. Then $G(F) \cong \hat{D}_\omega$.*

Proof. By [**6**, Proposition 4.1], $G(F) \cong \hat{D}(X(F), H)$ where $X(F)$ is the space of orderings of F and $H = \{a + b\sqrt{-1} \mid a, b \in R \text{ and } b > 0\}$. By [**2**, Theorem 11], $X(F) \cong X_\omega$; also $|H| = \aleph_0 = |S_\omega|$. Hence $\hat{D}(X(F), H) \cong \hat{D}(X_\omega, S_\omega) = \hat{D}_\omega$.

We shall see that the converse of the property (6) above is also true. But first we need a lemma, which is an easy corollary of some of the deeper theorems of [**5**]. It appears as Lemma 3.5 of [**6**].

LEMMA 2.2. *Let P and G be real projective groups.*

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

(b) *Let $\alpha\colon P \to G$ be a continuous epimorphism and let X be a system of representatives of the conjugacy classes of* $\mathrm{Inv}(P)$. *If α maps X bijectively onto a system of representatives of the conjugacy classes of* $\mathrm{Inv}(G)$, *then there exists a continuous monomorphism $\gamma\colon G \to P$ such that $\alpha \circ \gamma = \mathrm{id}_G$.*

PROPOSITION 2.3. *Let $\varphi\colon \hat{D}_\omega \to H$ be an epimorphism onto a finite group H and let G be a real projective group of* $\mathrm{rank} \leq \aleph_0$. *If $\pi\colon G \to H$ is an epimorphism such that $\pi(\mathrm{Inv}\, G) \subseteq \varphi(\mathrm{Inv}\, \hat{D}_\omega)$ then there exists an embedding $\gamma\colon G \to \hat{D}_\omega$ such that $\varphi \circ \gamma = \pi$.*

Proof. Note that the existence of a *homomorphism* $\gamma\colon G \to \hat{D}_\omega$ such that $\varphi \circ \gamma = \pi$ is already guaranteed by the definition of real projective groups. Our task is to use the assumption on the weight of G and to show how to choose γ to be injective. Our proof breaks into parts.

Part A: Choosing a more convenient basis for $\hat{D}_\omega$.

By Lemma 2.2(a), there exists a closed system X of representatives of the conjugacy classes of $\mathrm{Inv}\, G$.

Claim. With no loss we may assume that $\pi(X) \subseteq \varphi(X_\omega)$ and $H = \varphi\langle Y_\omega\rangle$.

Indeed, for each $h \in \pi(X)$ we may choose a $g = g(h) \in G$ such that $h^{\pi(g)} \in \varphi(X_\omega)$, since $\pi(X) \subseteq \pi(\mathrm{Inv}\, G) \subseteq \varphi(\mathrm{Inv}\, \hat{D}_\omega)$ and X_ω is a system of representatives of the conjugacy classes of $\hat{D}_\omega$, by (3). We replace then X by

$$\tilde{X} = \bigcup_{h \in \pi(X)} \left\{ x^{g(h)} \middle| x \in X,\ \pi(x) = h \right\},$$

which is also a closed system of representatives of the conjugacy classes of $\mathrm{Inv}\, G$ and satisfies

$$\pi(\tilde{X}) = \left\{ h^{\pi(g(h))} \middle| h \in \pi(X) \right\} \subseteq \varphi(X_\omega).$$

Let $x_1, \ldots, x_n \in X_\omega$ such that $\varphi(X_\omega) = \{\varphi(x_1), \ldots, \varphi(x_n)\}$. By (5), $Y_\omega \cap \mathrm{Ker}(\varphi)$ is infinite, hence we can choose n elements $y_1, \ldots, y_n \in (Y_\omega \cap \mathrm{Ker}\, \varphi) - \{1\}$. Let $Y_0 = Y_\omega - \{y_1, \ldots, y_n\}$ and $Y_1 = \{x_1 y_1, \ldots, x_n y_n\}$. Then

$$\begin{aligned} H &= \langle \varphi(X_\omega), \varphi(Y_\omega)\rangle = \langle \varphi(x_1), \ldots, \varphi(x_n), \varphi(Y_0)\rangle \\ &= \langle \varphi(x_1 y_1), \ldots, \varphi(x_n y_n), \varphi(Y_0)\rangle = \varphi\langle Y_0 \cup Y_1\rangle. \end{aligned}$$

Define ρ: $X_\omega \cup Y_\omega \to \hat{D}_\omega$ by

$$\rho(x) = x \qquad \text{for } x \in X_\omega$$
$$\rho(y) = y \qquad \text{for } y \in Y_0, \text{ and}$$
$$\rho(y_i) = x_i y_i \quad \text{for } i = 1, \ldots, n.$$

Then ρ extends to a homomorphism ρ: $\hat{D}_\omega \to \hat{D}_\omega$. But $\rho^2(z) = z$ for all $z \in X_\omega \cup Y_\omega$, hence ρ^2, and therefore also ρ, is an isomorphism. It follows that $(X_\omega, Y_0 \cup Y_1)$ is also a basis for $\hat{D}_\omega$. Thus we may replace Y_ω by $Y_0 \cup Y_1$ and attain the required property. This proves the Claim.

Part B: Constructing γ.

By Lemma 1.2(e) there exists a continuous embedding β: $X \to X_\omega$ such that $\varphi \circ \beta(x) = \pi(x)$ for each $x \in X$. Let $X' = \beta(X)$ and let α: $X' \to X$ be the inverse of β; then $\pi \circ \alpha(x) = \varphi(x')$ for each $x' \in X'$.

By [**6**, Proposition 3.4] (or by a direct check), the group $\langle Y_\omega \rangle$ is real free with the basis (φ, Y_ω), i.e., $\langle Y_\omega \rangle \cong \hat{F}_\omega$ is the free profinite group of rank $\aleph_0$. Since $\varphi\langle Y_\omega \rangle = H$, by the Iwasawa theorem ([**12**, p. 84]), there exists a continuous epimorphism $\hat{\alpha}$: $\langle Y_\omega \rangle \to G$ such that $\pi \circ \hat{\alpha}(y) = \varphi(y)$ for every $y \in \langle Y_\omega \rangle$. Denote by α its restriction to Y_ω.

Let $Z = X' \cup Y_\omega$. We have constructed a continuous map α: $Z \to G$ such that $\pi \circ \alpha = \varphi$ on Z. Let $\hat{D} = \langle Z \rangle$. By [**6**, Proposition 3.4], $\hat{D}$ is a real free group and (X', Y_ω) is its basis, hence α extends to a homomorphism α: $\hat{D} \to G$ such that $\pi \circ \alpha = \varphi$, on $\hat{D}$. Clearly the restriction of α to $\langle Y_\omega \rangle$ is $\hat{\alpha}$, hence α is an epimorphism. By [**6**, corollary 3.2], X' is a closed system of representatives of the conjugacy classes of $\operatorname{Inv}\hat{D}$ and it maps bijectively onto X by α. Therefore by Lemma 2.2(b), there exists an embedding γ: $G \to \hat{D}$ such that $\alpha \circ \gamma = \mathrm{id}_G$. Clearly $\pi = \varphi \circ \gamma$. □

3. Characterization of $\hat{D}_\omega$ by embedding problems. A *proper real embedding problem* for a profinite group G is a diagram

$$\begin{array}{ccc} & & G \\ & & \downarrow \varphi \\ B & \underset{\pi}{\to} & A \end{array} \tag{1}$$

and a closed involution domain I (i.e., a closed subset $I \subseteq \operatorname{Inv} B$ closed under conjugation) of B such that π and φ are epimorphisms of profinite groups and $\pi(I) = \varphi(\operatorname{Inv} G)$.

A *solution* to the problem is an epimorphism γ: $G \to B$ such that $\pi \circ \gamma = \varphi$ and $\gamma(\operatorname{Inv} G) = I$.

Problem (1) is said to be *finite* if B is a finite group.

REMARK 3.1. If every finite proper real embedding problem for a profinite group G is solvable, then $\operatorname{Inv} G \neq \varnothing$ and G has an open subgroup G' of index 2 such that $G' \cap \operatorname{Inv}(G) = \varnothing$. In particular $\operatorname{Inv} G$ is closed in G.

Indeed, consider the diagram

$$\begin{array}{c} G \\ \downarrow \\ \{\pm 1\} \to \{1\} \end{array} \tag{1}$$

and the involution domain $\{-1\}$ of $\{\pm 1\}$. By assumption there exists an epimorphism $\gamma\colon G \to \{\pm 1\}$ such that $\gamma(\operatorname{Inv} G) = \{-1\}$. Then $G' = \operatorname{Ker}\gamma$ has the required properties.

LEMMA 3.2. *Every finite proper real embedding problem for $\hat{D}_\omega$ is solvable.*

Proof. Let diagram (1) with an involution domain $I \subseteq B$ be a finite problem for $G = \hat{D}_\omega$. Denote $I_0 = \{b \in I \mid \pi(b) \in \varphi(X_\omega)\}$; then every element of I is conjugate to an element of I_0, since every element of $\operatorname{Inv}\hat{D}_\omega$ is conjugate to an element of X_ω and $\pi(I) = \varphi(\operatorname{Inv}\hat{D}_\omega)$. The set $Y_1 = Y_\omega - \operatorname{Ker}(\varphi)$ is finite. Choose a subset $Y_2 \subseteq Y_\omega - (Y_1 \cup \{1\})$ of exactly $|\operatorname{Ker}\pi|$ elements and denote $Y_3 = Y_\omega - (Y_1 \cup Y_2)$.

By Lemma 1.2(f), there exists a continuous surjection $\gamma_0\colon X_\omega \to I_0$ such that $\pi \circ \gamma_0 = \varphi$ on X_ω. Define $\gamma_1\colon Y_1 \to B$ such that $\pi \circ \gamma_1 = \varphi$ on Y_1 and let $\gamma_2\colon Y_2 \to \operatorname{Ker}\pi$ be a bijection. Finally define $\gamma_3\colon Y_3 \to B$ by $\gamma_3(Y_3) = 1$. The map $\gamma\colon X_\omega \cup Y_\omega \to B$ that extends these four maps is continous and $\pi \circ \gamma = \varphi$ on $X_\omega \cup Y_\omega$. Therefore the unique homomorphism $\gamma\colon \hat{D}_\omega \to B$ that extends it satisfies $\pi \circ \gamma = \varphi$. Moreover, $\operatorname{Ker}\pi \subseteq \gamma(\hat{D}_\omega)$ and $\varphi(\hat{D}_\omega) = \pi(B) = A$, hence γ is an epimorphism. This also implies that $\gamma(\operatorname{Inv}\hat{D})$ is the smallest involution domain that contains $\gamma(X_\omega) = I_0$, hence $\gamma(\operatorname{Inv}\hat{D}) = I$. □

We strengthen Lemma 3.2 by going to a countable inverse limit.

COROLLARY 3.3. *Consider the following diagram*

$$\begin{array}{c} \hat{D}_\omega \\ \downarrow \varphi \\ B \xrightarrow[\pi]{} A \end{array} \tag{1}$$

in which A is a finite group, B is a profinite group of rank $\leq \aleph_0$, *and φ and π are epimorphisms. Let I be a closed involution domain in B such that $\pi(I) = \varphi(\mathrm{Inv}\hat{D}_\omega)$. Then there exists an epimorphism $\gamma\colon \hat{D}_\omega \to B$ such that $\pi \circ \gamma = \varphi$ and $\gamma(\mathrm{Inv}\hat{D}_\omega) = I$.*

Proof. Let $\mathrm{Ker}\,\pi \geq N_1 \geq N_2 \geq N_3 \geq \cdots$ be a descending sequence of open normal subgroups with a trivial intersection. Let $\pi_n\colon B/N_n \to A$ be the epimorphism induced by π, then $I_n = I/N_n$ is an involution domain of B/N_n and $\pi_n(I_n) = \varphi(\mathrm{Inv}\hat{D}_\omega)$. Assume by induction, that there exists an epimorphism $\gamma_n\colon \hat{D}_\omega \to B/N_n$ such that $\pi_n \circ \gamma_n = \varphi$ and $\gamma_n(\mathrm{Inv}\hat{D}_\omega) = I_n$. Let $\beta_n\colon B/N_{n+1} \to B/N_n$ be the canonical epimorphism. Then, by Lemma 3.2, there exists an epimorphism $\gamma_{n+1}\colon \hat{D}_\omega \to B/N_{n+1}$ such that $\beta_n \circ \gamma_{n+1} = \gamma_n$ and $\gamma_{n+1}(\mathrm{Inv}\hat{D}_\omega) = I_{n+1}$, hence $\pi_{n+1} \circ \gamma_{n+1} = \varphi$.

The epimorphisms γ_n define an epimorphism $\gamma\colon \hat{D}_\omega \to B$ such that $\pi \circ \gamma = \varphi$ and $\varphi(\mathrm{Inv}\hat{D}_\omega) = I$, since $I = \varprojlim I_n$. □

The converse of Lemma 3.2 is also true:

LEMMA 3.4. *Let G be a profinite group of* rank $\leq \aleph_0$. *If every finite proper real embedding problem for G is solvable then $G \cong \hat{D}_\omega$.*

Proof. Both G and $\hat{D}_\omega$ have descending sequences of open normal subgroups whose intersections are 1, say $G = N_1' \geq N_2' \geq \cdots$ and $\hat{D}_\omega = M_1' \geq M_2' \geq \cdots$. Let $n \geq 0$ and assume by induction that we have already constructed

(a) two sequences of open normal subgroups $G = N_0 \geq N_1 \geq N_2 \geq \cdots \geq N_n$ and $\hat{D}_\omega = M_0 \geq M_1 \geq M_2 \geq \cdots \geq M_n$ such that $N_i \leq N_i'$ and $M_i \leq M_i'$ for $i = 1, \ldots, n$, and

(b) isomorphisms $\varphi_i\colon G/N_i \to \hat{D}_\omega/M_i$ such that $\varphi_i((\mathrm{Inv}G)/N_i) = (\mathrm{Inv}\hat{D}_\omega)/M_i$ for $i = 0, 1, \ldots, n$ and the following diagrams commute

$$\begin{array}{ccc} G/N_i & \xrightarrow{\varphi_i} & \hat{D}_\omega/M_i \\ \downarrow & & \downarrow \\ G/N_{i-1} & \xrightarrow{\varphi_{i-1}} & \hat{D}_\omega/M_{i-1} \end{array} \tag{2}$$

for $i = 1, \ldots, n$ (where the vertical maps are the canonical epimorphisms). Note that the trivial map $\varphi_0\colon G/N_0 \to \hat{D}_\omega/M_0$ satisfies (b), since $\mathrm{Inv}G$ and $\mathrm{Inv}\hat{D}_\omega$ are not empty, by Remark 3.1.

Let $K = N'_{n+1} \cap N_n$. By Lemma 3.2 there exists an epimorphism γ': $\hat{D}_\omega \to G/K$ such that

$$\begin{array}{ccc} & & \hat{D}_\omega \\ & \gamma' \swarrow & \downarrow \\ G/K \to G/N_n & \xrightarrow{\varphi_n} & \hat{D}_\omega/M_n \end{array} \tag{3}$$

commutes and $\gamma'(\mathrm{Inv}\,\hat{D}_\omega) = (\mathrm{Inv}\,G)/K$. Let $M_{n+1} = N'_{n+1} \cap (\mathrm{Ker}\,\gamma')$ and let γ: $\hat{D}_\omega/M_{n+1} \to G/K$ be the epimorphism induced by γ'. Then $M_{n+1} \leq M_n \cap M'_{n+1}$,

$$\begin{array}{ccc} G/K & \xleftarrow{\gamma} & \hat{D}_\omega/M_{n+1} \\ \downarrow & & \downarrow \\ G/N_n & \xrightarrow{\varphi_n} & \hat{D}_\omega/M_n \end{array} \tag{4}$$

commutes and $\gamma((\mathrm{Inv}\,\hat{D}_\omega)/M_{n+1}) = (\mathrm{Inv}\,G)/K$. By assumption there exists an epimorphism φ': $G \to \hat{D}_\omega/M_{n+1}$ such that $\varphi'(\mathrm{Inv}\,G) = (\mathrm{Inv}\,\hat{D}_\omega)/M_{n+1}$ and

$$\begin{array}{ccc} & & G \\ & & \downarrow \quad \searrow \varphi' \\ G/K & \xleftarrow{\gamma} & \hat{D}_\omega/M_{n+1} \end{array} \tag{5}$$

commutes. Let $N_{n+1} = \mathrm{Ker}\,\varphi'$ and let φ_{n+1}: $G/N_{n+1} \to \hat{D}/M_{n+1}$ be the isomorphism induced by φ'. Then $N_{n+1} \leq N'_{n+1} \cap N_n$, diagram (2) commutes for $i = n+1$ and $\varphi_{n+1}((\mathrm{Inv}\,G)/N_{n+1}) = (\mathrm{Inv}\,\hat{D}_\omega)/M_{n+1}$.

The compatible sequence $\varphi_0, \varphi_1, \varphi_2, \ldots$ of isomorphisms defines an isomorphism φ: $G \to \hat{D}_\omega$. □

4. Embedding of $\hat{D}_\omega$ in $\hat{D}_{e,f}$. The aim of this section is to identify $\hat{D}_\omega$ as a closed normal subgroup of a finitely generated real free group $\hat{D}_{e,f}$, where $e, f \geq 0$. Recall [**6**, §1] that $\hat{D}_{e,f} = \hat{D}(X, S)$, where X and S are the discrete spaces of e and f elements, respectively. In other words, there are $\varepsilon_1, \ldots, \varepsilon_e, \sigma_1, \ldots, \sigma_f \in \hat{D}_{e,f}$ such that

(1) $\hat{D}_{e,f} = \langle \varepsilon_1, \ldots, \varepsilon_e, \sigma_1, \ldots, \sigma_f \rangle$, $\varepsilon_1^2 = \cdots = \varepsilon_e^2 = 1$; and

(2) every map ϑ from $\{\varepsilon_1, \ldots, \varepsilon_e, \sigma_1, \ldots, \sigma_f\}$ into a profinite group G such that $\vartheta(\varepsilon_1)^2 = \cdots = \vartheta(\varepsilon_e)^2 = 1$, uniquely extends to a homomorphism ϑ: $\hat{D}_{e,f} \to G$.

LEMMA 4.1. *Let* $\varepsilon_1, \ldots, \varepsilon_e, \sigma_1, \ldots, \sigma_f \in \hat{D}_{e,f}$ *satisfy* (1). *Then*:

(a) *the property* (2) *is also satisfied.*

(b) *for every* $\varepsilon \in \operatorname{Inv} \hat{D}_{e,f}$ *there exists a unique* $1 \leq i \leq e$ *such that* ε *is conjugate to* ε_i; *moreover*, $\{\sigma \in \hat{D}_{e,f} | \varepsilon^\sigma = \varepsilon\} = \{1, \varepsilon\}$.

(c) $\hat{D}_{e,f} = \hat{D}_e * \hat{F}_f$, *where* $\hat{D}_e = \langle \varepsilon_1, \ldots, \varepsilon_e \rangle$ *is the free (profinite) product of* e *copies of* $\mathbf{Z}/2\mathbf{Z}$ *and* $\hat{F}_f = \langle \sigma_1, \ldots, \sigma_f \rangle$ *is the free profinite group of rank* f.

Proof. (a) see [**5**, the remark preceding Lemma 5.4].

(b) see [**5**, Proposition 6.1].

(c) follows from (2). □

The following assertion is used in the sequel. Its proof is left to the reader.

LEMMA 4.2. *Let* $\varphi: G \to H$ *be an epimorphism of profinite groups and let* S *be a subset of* G. *If* G_0 *is the smallest closed normal subgroup of* G *containing* S, *then* $\varphi(G_0)$ *is the smallest closed normal subgroup of* H *containing* $\varphi(S)$.

The key to the Lubotzky-v.d. Dries method [**10**] of recognizing certain closed subgroups of $\hat{F}_m$ as isomorphic to $\hat{F}_\omega$ is the Nielsen-Schreier formula for the rank of open subgroups of $\hat{F}_m$. The same role is played in our context by the following special case of the Binz-Neukirch-Wenzel theorem [**1**, p. 105].

LEMMA 4.3. *Let* $G = \coprod_{i \in I} G_i$ *be the free product of the profinite groups* G_i, *where* I *is a finite set. Let* H *be an open subgroup of* G. *For every* $i \in I$ *we consider the double class decomposition of* G:

$$G = \bigcup_{j \in J(i)} G_i x(i,j) H.$$

Then

$$H \cong \coprod_i \prod_{j \in J(i)} \left(G_i^{x(i,j)} \cap H\right) * \hat{F}_m,$$

where

$$m = \sum_{i \in I} \left[(G:H) - |J(i)|\right] - (G:H) + 1.$$

COROLLARY 4.4. *Suppose that* $G = D * F$, *where* $D \cong \hat{D}_e$ *and* $F \cong \hat{F}_f$. *If* H *is an open normal subgroup of* G *of index* n *which contains* D, *then* $H \cong \hat{D}_{en, 1+n(f-1)}$.

Proof. For $z \in G$ we have $DzH = DHz = Hz$, hence if $G = \bigcup_{i=1}^{n} Hz(i)$, then $G = \bigcup_{i=1}^{n} Dz(i)H$. Moreover, $D^{z(i)} \cap H = D^{z(i)} \cong \hat{D}_e$, since $H \triangleleft G$. Secondly, $FzH = FHz = G$ and $(F: F \cap H) = (G: H) = n$, hence, by the Nielsen-Schreier formula, [**1**, p. 108] $F \cap H \cong \hat{F}_{1+n(f-1)}$. Thus, in the notation of Lemma 4.2

$$m = [(G: H) - n] + [(G: H) - 1] - (G: H) + 1 = 0$$

and

$$H \cong (D^{z(1)} \cap H) * (D^{z(2)} \cap H) * \cdots * (D^{z(n)} \cap H) * (F \cap H)$$
$$= D^{z(1)} * D^{z(2)} * \cdots * D^{z(n)} * (F \cap H) \cong \hat{D}_{en} * \hat{F}_{1+n(f-1)}. \qquad \square$$

PROPOSITION 4.5. *Let $G = \hat{D}_{e,f}$, where $e \geq 1$ and $f \geq 2$, and let K be an open subgroup of G. Then there exists a closed normal subgroup H of G such that $H \cong \hat{D}_\omega$, $G = KH$ and*

$$\text{Inv}H = \text{Inv}G. \tag{3}$$

Proof. We break the proof into parts.

Part A. Construction of H.

By Lemma 4.1(c), $G = D * F$, where $D \cong \hat{D}_e$ and $F \cong \hat{F}_f$ are closed subgroups of G. Let p be a prime which does not divide $(G: K)$. Fix an epimorphism $\rho: G \to \mathbf{Z}_p$ such that $\rho(D) = 1$ and let $H = \text{Ker}\rho$. The lattice $G = G_0 > G_1 > G_2 > \cdots$ of open subgroups of G containing H is isomorphic to the lattice of open subgroups of $\mathbf{Z}_p$, hence G_i is the only normal subgroup of G of index p^i containing H, for each $i \geq 0$, and $H = \bigcap_{i=0}^{\infty} G_i$. In particular $(G: KH) = p^i$ for some $i \geq 0$, but $(G: KH) | (G: K)$, hence $i = 0$, whence $G = KH$. By Lemma 4.1(b), every involution of $G = D * F$ is conjugate to an involution of D; but $D \leq H$, hence (3) holds.

Part B. Embedding problem.

We employ Lemma 3.4 to show that $H \cong \hat{D}_\omega$. Let

$$\begin{array}{ccc} & & H \\ & & \downarrow \varphi \\ B & \underset{\pi}{\to} & A \end{array} \tag{4}$$

together with an involution domain $I \subseteq \text{Inv}B$ such that $\pi(I) = \varphi(\text{Inv}H)$ be a finite proper embedding problem for H. Then $\text{Ker}\varphi$ is open in H, hence there exists an open $N \triangleleft G$ such that $N \cap H = \text{Ker}\varphi$. Now $H \leq NH \triangleleft G$, hence there is an $i \geq 0$ such that $NH = G_i$. It follows that φ can be extended to an epimorphism $\varphi: G_i \to A$, with kernel N.

Let $n = p|B| + i$. With no loss we may assume that $i = 0$, i.e., φ can be extended to G, and, moreover, that

$$f > 2n \tag{5}$$

and

(6) for every conjugacy class $C \subseteq \varphi(\mathrm{Inv}H)$ there are at least n conjugacy classes in $\mathrm{Inv}G$ mapped by φ onto C (in particular $e \geq n$, by Lemma 4.1(b)).

Indeed, otherwise replace G by its open normal subgroup G_n(and G_j by G_{j+n} for every $j \geq 0$ and N by $G_n \cap N$) and restrict φ from G_i to G_n. By Corollary 4.4, $G_n \cong \hat{D}_{e',f'}$, where

$$f' = 1 + p^n(f-1) > 2^n \geq 2n.$$

Also, $\rho(G_n) \cong \mathbf{Z}_p$ and $\mathrm{Inv}G_n \subseteq H$, by (3). To check (6) we consider an $\varepsilon \in \mathrm{Inv}H$ which satisfies $\varphi(\varepsilon) \in C$, and let $\sigma(1), \ldots, \sigma(n) \in G$ belong to distinct cosets modulo G_n. Then $\varepsilon^{\sigma(1)}, \ldots, \varepsilon^{\sigma(n)} \in \varphi^{-1}(C)$ represent distinct conjugacy classes in G_n. Indeed, if $\varepsilon^{\sigma(j)} = \varepsilon^{\sigma(k)\tau}$, where $1 \leq j, k \leq n$ and $\tau \in G_n$, then $\sigma(k)\tau\sigma(j)^{-1} = 1$ or $\sigma(k)\tau\sigma(j)^{-1} = \varepsilon$, by Lemma 4.1(b). In both cases $\sigma(k)\tau\sigma(j)^{-1} \in G_n$, whence $\sigma(k)G_n = \sigma(j)G_n$, i.e., $k = j$.

In particular, $G = NH$, which implies that

$$G = NG_1. \tag{7}$$

Part C. Generators for G.

Let H_0, A_0 and B_0 be the smallest closed normal subgroups of G, A and B containing $\mathrm{Inv}G = \mathrm{Inv}H$, $\varphi(\mathrm{Inv}H) = \pi(I)$ and I, respectively. By Lemma 4.3 we have

$$\varphi(H_0) = A_0 = \pi(B_0). \tag{8}$$

Also $D \leq H_0 \leq H$, since D is generated by involutions. Let us show that

$$(F \cap H_0N) - G_1 \neq \varnothing. \tag{9}$$

Indeed, $G_1 \neq G$, hence $N \not\leq G_1$, by (7). Also, $G = H_0F$, since $G = \langle D, F\rangle$, by Lemma 4.1(c) and $D \leq H_0$. Thus there exists a $\sigma \in N - G_1$, and there exists an $\varepsilon \in H_0$ such that $\varepsilon\sigma \in F$. Clearly $\varepsilon\sigma \notin G_1$, hence $\varepsilon\sigma \in (F \cap H_0N) - G_1$.

We use (9) to find generators for F. Let $\sigma \mapsto \bar{\sigma}$ denote the canonical map $G \to \bar{G}$, where $\bar{G} = G/N \cap G_1$. By (7)

$$\bar{G} \cong G/N \times G/G_1 \cong A \times \mathbf{Z}/p\mathbf{Z},$$

hence $|\bar{G}| = p|A| \leq n$. Choose generators $\bar{\sigma}_1, \ldots, \bar{\sigma}_n$ of the subgroup $\bar{F}$ of $\bar{G}$. With no loss $\bar{\sigma}_1 \in \overline{(F \cap H_0N) - G_1}$, by (9). Put $\bar{\sigma}_{n+1} = \cdots = \bar{\sigma}_f = 1$. By the Gaschütz Lemma [**9**, Lemma 4.2], $\bar{\sigma}_1, \ldots, \bar{\sigma}_f$ lift to generators

$\sigma_1, \ldots, \sigma_f$ of F. Observe that

$$\sigma_1 \notin G_1 \tag{10}$$

and $\varphi(\sigma_1) \in \varphi(H_0 N) = \varphi(H_0)$, hence by (8)

$$\varphi(\sigma_1) \in \pi(B_0) \tag{11}$$

also

$$\varphi(\sigma_{n+1}) = \cdots = \varphi(\sigma_f) = 1. \tag{12}$$

Fix $\varepsilon_1, \ldots, \varepsilon_e \in \operatorname{Inv} G$ that generate D. Then $G = \langle \varepsilon_1, \ldots, \varepsilon_e, \sigma_1, \ldots, \sigma_f \rangle$, by Lemma 4.1(c).

Part D. Solution by the embedding problem.

Define γ: $\{\varepsilon_1, \ldots, \varepsilon_e, \sigma_1, \ldots, \sigma_f\} \to B$ as follows. First choose $\gamma(\sigma_1), \ldots, \gamma(\sigma_n) \in B$ such that $\pi(\gamma(\sigma_j)) = \varphi(\sigma_j)$, $j = 1, \ldots, n$, and

$$\gamma(\sigma_1) \in B_0 \tag{13}$$

(this is possible by (11)). Next let $\gamma(\sigma_{n+1}), \ldots, \gamma(\sigma_f)$ be a set of generators of $\operatorname{Ker}\pi$ (by (5), $|\operatorname{Ker}\pi| \leq n < n - f$). Finally let $b_1, \ldots, b_m$ be representatives of the conjugacy classes of I, with $m \leq n$. By Lemma 4.1(b) every $a \in \varphi(\operatorname{Inv} G) = \pi(I)$ is conjugate to one of the $\varphi(\varepsilon_1), \ldots, \varphi(\varepsilon_e)$; moreover, by (6), a is conjugate to at least n elements of this e-tuple. Thus, reordering $\varepsilon_1, \ldots, \varepsilon_e$ if necessary, we may assume that $\pi(b_i)$ is conjugate to $\varphi(\varepsilon_i)$, for $i = 1, \ldots, m$. Therefore with no loss $\pi(b_i) = \varphi(\varepsilon_i)$, for $i = 1, \ldots, m$. Choose $b_{m+1}, \ldots, b_e \in I$ such that $\pi(b_i) = \varphi(\varepsilon_i)$, for $i = m + 1, \ldots, e$ and define $\gamma(\varepsilon_i) = b_i$, for $i = 1, \ldots, e$.

The map γ uniquely extends to a homomorphism γ: $G \to B$ such that $\pi \circ \gamma = \varphi$. But $\operatorname{Ker}\pi \subseteq \gamma(G)$ and $\varphi(G) = \pi(B) = A$, hence $\gamma(G) = B$. Also $\gamma(\varepsilon_1), \ldots, \gamma(\varepsilon_0) \in I$, hence $\gamma(\operatorname{Inv} G) \subseteq I$ by Lemma 4.1(b). On the other hand $b_1, \ldots, b_m \in \gamma(\operatorname{Inv} G)$, hence $I \subseteq \gamma(\operatorname{Inv} G)$. Therefore, by (3)

$$\gamma(\operatorname{Inv} G) = \gamma(\operatorname{Inv} H) = I. \tag{14}$$

Finally, $\langle \sigma_1 \rangle H$ is an open subgroup of G containing H, hence $\langle \sigma_1 \rangle H = G_i$ for some $i \geq 0$. But $\langle \sigma_1 \rangle \not\leq G_1$ by (10), hence $\langle \sigma_1 \rangle H = G_0 = G$. By Lemma 4.2 and (14), $\gamma(H_0) = B_0$, in particular $\gamma(\sigma_1) \in \gamma(H_0) \subseteq \gamma(H)$, by (13). Therefore $\gamma(G) = \gamma(\langle \sigma_1 \rangle H) = \gamma(H)$. Thus the restriction of γ to H solves the problem (4). □

5. Algebraic realization of real projective groups of rank $\leq \aleph_0$. We are now in a position to apply the information about real projective groups of rank $\leq \aleph_0$ gathered so far to realize them as the absolute Galois groups of algebraic PRC fields. Thus is our main result.

THEOREM 5.1. *Let K be a countable formally real Hilbertian field and let K' be a finite Galois extension of K. If G is a real projective group of* rank $\leq \aleph_0$ *and* $\pi\colon G \to \mathcal{G}(K'/K)$ *is an epimorphism such that* $\pi(\mathrm{Inv}\, G) \subseteq \mathrm{res}_{K'}(\mathrm{Inv}\, G(K))$, *then there exists a* PRC *algebraic extension E of K and an isomorphism γ such that the following diagram is commutative.*

$$\begin{array}{ccc} G & \xrightarrow{\gamma} & G(E) \\ & \searrow \quad \swarrow & \\ & \mathcal{G}(K'/K) & \end{array} \tag{1}$$

Proof. Let $\{\bar{\delta}_1, \ldots, \bar{\delta}_e\} = \mathrm{res}_{K'}(\mathrm{Inv}\, G(K))$ and Let $\bar{\sigma}_{e+1}, \ldots, \bar{\sigma}_{e+f}$ be a set of generators for $\mathcal{G}(K'/K)$ such that $f \geq 2$. Let $\delta_1, \ldots, \delta_e \in \mathrm{Inv}\, G(K)$ extend $\bar{\delta}_1, \ldots, \bar{\delta}_e$, respectively. The set S of all $(e+f)$-tuples $(\sigma_1, \ldots, \sigma_{e+f}) \in G(K)^{e+f}$ such that $\mathrm{res}_{K'}\sigma_i = 1$ for $i = 1, \ldots, e$ and $\mathrm{res}_{K'}\sigma_i = \bar{\sigma}_i$ for $i = e+1, \ldots, e+f$ is of positive measure (with respect to the normalized Haar measure of $G(K)^{e+f}$). Therefore by [**5**, Proposition 5.6], there exists an $(e+f)$-tuple $(\sigma_1, \ldots, \sigma_{e+f}) \in S$ such that, denoting $\varepsilon_i = \delta_i^{\sigma_i}$ for $i = 1, \ldots, e$, we have: $K_\sigma = \tilde{K}(\varepsilon_1, \ldots, \varepsilon_e, \sigma_{e+1}, \ldots, \sigma_{e+f})$ is a PRC field and

$$G(K_\sigma) = \langle \varepsilon_1, \ldots, \varepsilon_e, \sigma_{e+1}, \ldots, \sigma_{e+f} \rangle \cong \hat{D}_{e,f}.$$

In particular, $\mathrm{res}_{K'}(G(K_\sigma)) = \mathcal{G}(K'/K)$ and $\varepsilon_1, \ldots, \varepsilon_e$ represent the conjugacy classes of $\mathrm{Inv}\, G(K_\sigma)$, by Lemma 4.1(b). Hence

$$\mathrm{res}_{K'}(\mathrm{Inv}\, G(K_\sigma)) = \{\bar{\delta}_1, \ldots, \bar{\delta}_e\} = \mathrm{res}_{K'}(\mathrm{Inv}\, G(K)) \supseteq \pi(\mathrm{Inv}\, G).$$

By Lemma 4.5, K_σ has a Galois extension N such that $K'K_\sigma \cap N = K_\sigma$, $G(N) \cong \hat{D}_\omega$ and $\mathrm{Inv}\, G(N) = \mathrm{Inv}\, G(K_\sigma)$. In particular $\mathrm{res}_{K'}(G(N)) = \mathcal{G}(K'/K)$ and $\pi(\mathrm{Inv}\, G) \subseteq \mathrm{res}_{K'}(\mathrm{Inv}\, G(N))$. It follows from Proposition 2.3 that there exists an embedding $\gamma\colon G \to G(N)$ such that $\mathrm{res}_{K'} \circ \gamma = \pi$. The field $E = \tilde{K}(\gamma(G))$ is an algebraic extension of a PRC field K_σ, hence [**11**, Theorem 3.1] E is PRC. Now $\gamma\colon G \to G(E)$ is an isomorphism and (1) commutes. □

REFERENCES

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

[2] T. Craven, *The topological space of orderings of a rational function field*, Duke Math. J., **41** (1974), 339–347.

[3] A. Douady, *Cohomologie des groupes compacts totalement discontinus*, Séminaire Bourbaki 1959–1960, exposé 189.

[4] J. Dugundji, *Topology*, Allyn and Bacon, Inc., Boston 1976.

[5] D. Haran and M. Jarden, *The absolute Galois group of a pseudo real closed field*, to appear in Annali della Scuola Normale Superiore di Pisa.
[6] ———, *Real free groups*, to appear in J. Pure Appl. Algebra.
[7] J. Hocking and G. Young, *Topology*, Reading, Mass., Addison-Wesley, 1961.
[8] M. Jarden, *An analogue of Čebotarev density theorem for fields of finite corank*, J. Math., Kyoto University, **20** (1980), 141–147.
[9] M. Jarden and U. Kiehne, *The elementary theory of algebraic fields of finite corank*, Inventiones Math., **30** (1975), 275–294.
[10] A. Lubotzky and L. van den Dries, *Subgroups of free profinite groups and large subfields of* $\tilde{\mathbf{Q}}$, Israel J. Math., **39** (1980), 25–45.
[11] A. Prestel, *Pseudo real closed fields*, in: *Set theory and model theory*, 127–156, Lecture Notes in Mathematics 782, Springer, Berlin, 1981.
[12] L. Ribes, *Introduction to profinite groups and Galois cohomology*, Queen's University, Kingston, 1970.

Received December 11, 1984. The first author was supported by Alexander von Humboldt Foundation. The second author was partially supported by the fund for Basic Research administered by the Israel Academy of Sciences and Humanities.

DEPARTMENT OF MATHEMATICS
RUTGERS UNIVERSITY
NEW BRUNSWICK, NJ 08903
USA

AND

SCHOOL OF MATHEMATICAL SCIENCES
THE RAYMOND AND BEVERLY SACKLER
FACULTY OF EXACT SCIENCES
TEL AVIV UNIVERSITY
RAMAT AVIV TEL AVIV 69978
ISRAEL