ISRAEL JOURNAL OF MATHEMATICS 85 (1994), 85–101

THE ABSOLUTE GALOIS GROUP OF A HILBERTIAN PRC FIELD*

BY

MICHAEL D. FRIED**

Department of Mathematics, UC Irvine
Irvine, CA. 92717, USA, e-mail: mfried@math.uci.edu

AND

HELMUT VÖLKLEIN***

Department of Mathematics, University of Florida
Gainesville, FL 32611, USA. e-mail: helmut@math.ufl.edu

ABSTRACT

We determine the absolute Galois group of a countable Hilbertian P(seudo) R(eal) C(losed) field P of characteristic 0. This group turns out to be real-free, determined up to isomorphism by the topological space of orderings of P. Examples of such fields P are the proper finite extensions of the field of all totally real numbers.

Introduction

All fields occurring in this paper are assumed to have characteristic 0. A field P is called P(seudo)A(lgebraically)C(losed) if every (non-empty) absolutely irreducible variety V defined over P has a P-rational point. In [FV2] it was shown that over a Hilbertian PAC-field, all finite embedding problems are solvable. Thus, the absolute Galois group of a countable Hilbertian PAC-field is the free profinite group of countably infinite rank. Now we generalize this result to the

* Part of this work was done while the authors were fellows of the Institute for Advanced Studies in Jerusalem
** Supported by NSA grant MDA 14776 and BSF grant 87-00038
*** Supported by NSA grant MDA 904-89-H-2028
Received June 23, 1992 and in revised form July 16, 1993

larger class of P(seudo)R(eal)C(losed) fields P. These are defined by the property that every non-singular absolutely irreducible variety V defined over P has a P-rational point if it has a point over each real closure of P. Our main result says that all restricted finite embedding problems over a Hilbertian PRC-field (of characteristic 0) are solvable. This is the main step in proving that the absolute Galois group of such a field is real-free (in the sense of [HJ2]), determined up to isomorphism by the topological space of orderings of the field (see Corollary 1).

Pop [P] has recently shown that the field $\mathbb{Q}_{re}$ of all totally real algebraic numbers is PRC. Then any finite extension K of $\mathbb{Q}_{re}$ is PRC [Pr, Th. (3.1)]. Since $\mathbb{Q}_{re}$ is a Galois extension of $\mathbb{Q}$, any finite proper extension K of $\mathbb{Q}_{re}$ is also Hilbertian (by Weissauer's theorem [Ws] or [FrJ], Cor. 12.15]). Thus, $G(\bar{\mathbb{Q}}/K)$ is real-free by the results of this paper. Actually, there are exactly two possible isomorphism types for these groups $G(\bar{\mathbb{Q}}/K)$ (Corollary 2). The latter is an observation of M. Jarden.

ACKNOWLEDGEMENT: We thank D. Haran and M. Jarden for helpful discussions.

Comments on PRC fields: PRC-fields were introduced by Prestel [Pr]. The absolute Galois group of a PRC-field is real-projective in the sense of [HJ1]. Conversely, each real-projective profinite group is the absolute Galois group of a PRC-field by [HJ1]. On the other hand, for any real closed field R, $R(x)$ has real-projective (even real-free) absolute Galois group, but it is not PRC. ∎

Notations: As above, we assume all occurring fields to have characteristic 0. Denote the algebraic closure of a field k by $\bar{k}$. The absolute Galois group $G(\bar{k}/k)$ of k is denoted by G_k. The semi-direct product of groups A and B is written as $A \times^s B$ (where A is normal). The normalizer (resp., centralizer) of A in B is denoted $N_B(A)$ (resp., $C_B(A)$). An involution is an element of order 2. Other notations as introduced above. ∎

1. Real points on Hurwitz spaces

We recall the set-up of [FV1, §1]. Let G be a finite group, let $\mathrm{Aut}(G)$ be its automorphism group and let $\mathrm{Inn}(G)$ be the group of inner automorphisms.

1.1 THE HURWITZ MONODROMY GROUP. Fix an integer $r \geq 3$. We let $\mathcal{U}_r$ be the space of all subsets of cardinality r of the Riemann sphere $\mathbb{P}^1 = \mathbb{C} \cup \{\infty\}$.

We choose a base point $\mathbf{b} = \{b_1, \ldots, b_r\} \in \mathcal{U}_r$, where $b_\nu = 1 + (r - 2\nu + 1)i$ (and $i^2 = -1$). The important property is that the complex conjugate of b_ν is $b_{r-\nu+1}$ for $1 \leq \nu \leq r/2$.

The space $\mathcal{U}_r$ has a natural structure of algebraic variety defined over $\mathbb{Q}$ [FV1, §1.1]. So, the above base point $\mathbf{b}$ is rational over $\mathbb{Q}$. For the moment, we view $\mathcal{U}_r$ only as a complex manifold. Its fundamental group $\pi_1(\mathcal{U}_r, \mathbf{b})$, based at $\mathbf{b}$, is the Hurwitz monodromy group H_r, which has classical **elementary braid** generators $Q_1, \ldots, Q_{r-1}$ [FV1,§1.3].

1.2 Moduli spaces for covers of the Riemann sphere. Consider covers $\chi\colon X \to \mathbb{P}^1$ of compact (connected) Riemann surfaces. Two covers $\chi\colon X \to \mathbb{P}^1$ and $\chi'\colon X' \to \mathbb{P}^1$ are **equivalent** if there exists an isomorphism $\epsilon\colon X \to X'$ with $\chi'\epsilon = \chi$. Let $\mathrm{Aut}(X/\mathbb{P}^1)$ be the group of automorphisms ϵ of X with $\chi\epsilon = \chi$. We call χ a Galois cover if $\mathrm{Aut}(X/\mathbb{P}^1)$ is transitive on the fibers of χ. From now on χ will be a Galois cover. All but finitely many points of $\mathbb{P}^1$ have the same number of inverse images under χ. These exceptional points are the **branch points** of χ.

Let $\mathcal{H}_r^{\text{ab}}(G)$ be the set of equivalence classes $|\chi|$ of all Galois covers $\chi\colon X \to \mathbb{P}^1$ with r branch points and with $\mathrm{Aut}(X/\mathbb{P}^1) \cong G$. Let $\mathcal{H}_r^{\text{in}}(G)$ be the set of equivalence classes of pairs (χ, h) where $\chi\colon X \to \mathbb{P}^1$ is a Galois cover with r branch points, and $h\colon \mathrm{Aut}(X/\mathbb{P}^1) \to G$ is an isomorphism. Two such pairs (χ, h) and $(\chi'\colon X' \to \mathbb{P}^1, h')$ are called **equivalent** iff there is an isomorphism $\delta\colon X \to X'$ with $\chi'\delta = \chi$ and $h'c_\delta = h$. Here $c_\delta\colon \mathrm{Aut}(X/\mathbb{P}^1) \to \mathrm{Aut}(X'/\mathbb{P}^1)$ is the isomorphism induced by δ (i.e., $c_\delta(A) = \delta A \delta^{-1}$). Let $|\chi, h|$ denote the equivalence class of the pair (χ, h). Let $\Lambda\colon \mathcal{H}_r^{\text{in}}(G) \to \mathcal{H}_r^{\text{ab}}(G)$ be the map sending $|\chi, h|$ to $|\chi|$.

Define the maps $\Psi\colon \mathcal{H}_r^{\text{ab}}(G) \to \mathcal{U}_r$ and $\Psi'\colon \mathcal{H}_r^{\text{in}}(G) \to \mathcal{U}_r$ by sending $|\chi|$ and $|\chi, h|$, respectively, to the set of branch points of χ. The sets $\mathcal{H}_r^{\text{ab}}(G)$ and $\mathcal{H}_r^{\text{in}}(G)$ carry a natural topology [FV1, §1.2] such that Ψ and Ψ' are (unramified) coverings. Then also $\Lambda\colon \mathcal{H}_r^{\text{in}}(G) \to \mathcal{H}_r^{\text{ab}}(G)$ is a covering, and $\Psi \circ \Lambda = \Psi'$. Note that through these coverings the spaces $\mathcal{H}_r^{\text{ab}}(G)$ and $\mathcal{H}_r^{\text{in}}(G)$ inherit a structure of complex manifold from $\mathcal{U}_r$.

To determine the equivalence class of the covering Ψ, we need to identify the natural permutation representation of $H_r = \pi_1(\mathcal{U}_r, \mathbf{b})$ on the fiber $\Psi^{-1}(\mathbf{b})$. (Here $\mathbf{b}$ is our fixed base point in $\mathcal{U}_r$.) Recall that this action is defined as follows: Each closed path ω in $\mathcal{U}_r$ based at $\mathbf{b}$ sends a point $\boldsymbol{p} \in \Psi^{-1}(\mathbf{b})$ to the endpoint of the unique lift of ω with initial point $\boldsymbol{p}$. Similarly for $\mathcal{H}_r^{\rm in}(G)$.

This depends on the choice of generators $\gamma_1, \dots, \gamma_r$ for the fundamental group $\Gamma = \pi_1(\mathbb{P}^1 \setminus \mathbf{b}, 0)$. (By abuse, we identify the paths γ_j and their homotopy classes.) Let γ_j be a path that goes on a straight line (in the complex plane) from 0 towards b_j, then travels on a small circle in clockwise direction around b_j, and returns on the straight line to 0. (The small circles must be disjoint). Then Γ is a free group on generators $\gamma_1, \dots, \gamma_{r-1}$, and $\gamma_1 \cdots \gamma_r = 1$. We can arrange things such that the complex conjugate of γ_j is γ_{r-j+1}^{-1} for $j = 1, \dots, r/2$ (since the corresponding relation holds for the b_j's).

Now let χ: $X \to \mathbb{P}^1$ be a (Galois) cover of $\mathbb{P}^1$ with $|\chi| \in \Psi^{-1}(\mathbf{b})$. This means $\text{Aut}(X/\mathbb{P}^1) \cong G$, and $b_1, \dots, b_r$ are the branch points of χ. Thus χ restricts to an unramified cover of the punctured sphere $\mathbb{P}^1 \setminus \mathbf{b}$. By the theory of covering spaces, the latter corresponds to a normal subgroup U_χ of $\Gamma = \pi_1(\mathbb{P}^1 \setminus \mathbf{b}, 0)$, and Γ/U_χ is isomorphic to $\text{Aut}(X/\mathbb{P}^1)$. Thus there is a surjection f: $\Gamma \to G$ with kernel U_χ. The surjection f is determined by the r-tuple $(\sigma_1, \dots, \sigma_r) = (f(\gamma_1), \dots, f(\gamma_r))$. This r-tuple $(\sigma_1, \dots, \sigma_r)$ has the following properties: $\sigma_1 \cdots \sigma_r = 1$, the group G is generated by $\sigma_1, \dots, \sigma_r$, and $\sigma_j \neq 1$ for all j. The last condition means that the cover χ is actually ramified over each b_j [FV1, §1.3]. Let $\mathcal{E}_r$ denote the set of these r-tuples $(\sigma_1, \dots, \sigma_r)$.

Each tuple $(\sigma_1, \dots, \sigma_r) \in \mathcal{E}_r$ occurs for some χ. Another choice of f (for the same or equivalent χ) results in an r-tuple conjugate to $(\sigma_1, \dots, \sigma_r)$ under an element of $\text{Aut}(G)$. Since f determines $U_\chi = \ker(f)$, hence $|\chi|$ uniquely, we get the following. The above gives a bijection between the points $|\chi|$ in the fiber $\Psi^{-1}(\mathbf{b})$ and the set $\mathcal{E}_r^{\rm ab} \stackrel{\rm def}{=} \mathcal{E}_r/\text{Aut}(G)$ of $\text{Aut}(G)$-classes of the tuples $(\sigma_1, \dots, \sigma_r)$. Via this bijection, $H_r = \pi_1(\mathcal{U}_r, \mathbf{b}) = \langle Q_1, \dots, Q_{r-1} \rangle$ acts on $\mathcal{E}_r^{\rm ab}$. For a suitable choice of the generators $Q_1, \dots, Q_{r-1}$ this action is given by the following rule [FV1, §1.4]: The element Q_j sends the class of $(\sigma_1, \dots, \sigma_r)$ to the class of

$$(1) \qquad (\sigma_1, \dots, \sigma_{j+1}, \sigma_{j+1}^{-1}\sigma_j\sigma_{j+1}, \dots, \sigma_r)$$

(This observation goes back to Clebsch and Hurwitz).

Similarly, we get a bijection between the points $|\chi, h|$ in the fiber $(\Psi')^{-1}(\mathbf{b})$ and the set $\mathcal{E}_r^{\rm in} \stackrel{\rm def}{=} \mathcal{E}_r/\text{Inn}(G)$. Here one has to observe additionally that if χ: $X \to \mathbb{P}^1$ is a Galois cover with branch points $b_1, \dots, b_r$ as above, then there is a surjection ι: $\Gamma \to \text{Aut}(X/\mathbb{P}^1)$ with kernel U_χ that is *canonical up to composition with inner automorphisms*: Fix a point $y_0 \in \chi^{-1}(0)$. For each path γ representing an element of Γ, let y be the endpoint of the unique lift of γ to $X \setminus \chi^{-1}(\mathbf{b})$ with initial point y_0. Then, ι sends γ to the unique element ϵ of $\mathrm{Aut}(X/\mathbb{P}^1)$ with $\epsilon(y) = y_0$. Varying y_0 over $\chi^{-1}(0)$ means composing ι with inner automorphisms of $\mathrm{Aut}(X/\mathbb{P}^1)$. Now set $f = h\iota$, and associate to $|\chi, h|$ the $\mathrm{Inn}(G)$-class of the tuple $(\sigma_1, \ldots, \sigma_r) = (f(\gamma_1), \ldots, f(\gamma_r))$. This yields the desired bijection between $(\Psi')^{-1}(\mathbf{b})$ and $\mathcal{E}_r^{\mathrm{in}}$. The resulting action of H_r on $\mathcal{E}_r^{\mathrm{in}}$ is again given by formula (1) [FV1, §1.4].

1.3 THE ALGEBRAIC STRUCTURE OF THE MODULI SPACES. Consider a cover $\chi\colon X \to \mathbb{P}^1$ as above. The space X has a unique structure of algebraic variety defined over $\mathbb{C}$ (compatible with its analytic structure) such that χ becomes an algebraic morphism (Riemann's existence theorem). Thus, for each (not necessarily continuous) automorphism β of $\mathbb{C}$, we can consider the cover $\chi^\beta\colon X^\beta \to \mathbb{P}^1$ obtained from $\chi\colon X \to \mathbb{P}^1$ through base change with β.

By the main result of [FV1], the spaces $\mathcal{H}_r^{\mathrm{ab}}(G)$ and $\mathcal{H}_r^{\mathrm{in}}(G)$ have a structure of (reducible) algebraic variety defined over $\mathbb{Q}$ (compatible with their natural analytic structure) such that Ψ, Ψ' and Λ are morphisms defined over $\mathbb{Q}$. Also, each automorphism β of $\mathbb{C}$ sends the point $|\chi| \in \mathcal{H}_r^{\mathrm{ab}}(G)$ to $|\chi^\beta|$. Further, β sends the point $|\chi, h| \in \mathcal{H}_r^{\mathrm{in}}(G)$ to $|\chi^\beta, h \circ \beta^{-1}|$, where $\chi\colon X \to \mathbb{P}^1$ and $h\colon \mathrm{Aut}(X/\mathbb{P}^1) \to G$ as usual, and $h \circ \beta^{-1}\colon \mathrm{Aut}(X^\beta/\mathbb{P}^1) \to G$ is the isomorphism that maps a^β to $h(a)$ for every $a \in \mathrm{Aut}(X/\mathbb{P}^1)$. With these conditions the $\mathbb{Q}$-structures on these spaces are unique.

In particular, we get an action of the absolute Galois group $G_{\mathbb{Q}}$ on the fibers $\Psi^{-1}(\mathbf{b})$ and $(\Psi')^{-1}(\mathbf{b})$. Via the above bijections, this gives an action on $\mathcal{E}_r^{\mathrm{ab}}$ and on $\mathcal{E}_r^{\mathrm{in}}$. We need the following fact.

(2) Complex conjugation c acts on $\mathcal{E}_r^{\mathrm{ab}}$ and on $\mathcal{E}_r^{\mathrm{in}}$ by sending the class of $(\sigma_1, \ldots, \sigma_r)$ to the class of $(\sigma_r^{-1}, \ldots, \sigma_1^{-1})$.

It suffices to prove the following statement. If $|\chi, h| \in (\Psi')^{-1}(\mathbf{b})$ corresponds to the class of $(\sigma_1, \ldots, \sigma_r)$ in $\mathcal{E}_r^{\mathrm{in}}$, then $|\chi^c, h \circ c|$ corresponds to the class of $(\sigma_r^{-1}, \ldots, \sigma_1^{-1})$. This is a straightforward consequence of the definitions, and of the formula $c(\gamma_j) = \gamma_{r-j+1}^{-1}$ $(j = 1, \ldots, r/2)$ from §1.2 (cf. [DeFr, Lemma 2.1]).

1.4 CHOOSING SUITABLE COMPONENTS OF THE MODULI SPACES. Fix an integer $s \geq 4$ divisible by 4. Let r be the product of s with the number of conjugacy classes $\neq \{1\}$ of G. Let $\mathcal{E}^{(s)}$ be the set of all r-tuples $(\sigma_1, \ldots, \sigma_r) \in \mathcal{E}_r$ satisfying this: For each conjugacy class $C \neq \{1\}$ of G there are exactly s indices j such that $\sigma_j \in C$. Further, let $\mathcal{E}^{(s)}_{ab}$ (resp., $\mathcal{E}^{(s)}_{in}$) be the image of $\mathcal{E}^{(s)}$ in $\mathcal{E}^{ab}_r$ (resp., $\mathcal{E}^{in}_r$).

The sets $\mathcal{E}^{(s)}_{ab}$ and $\mathcal{E}^{(s)}_{in}$ are invariant under the action of the Hurwitz group H_r (via formula (1)). For the rest of §1, assume the *Schur multiplier* of G is generated by commutators [FV1, §2.4]. By a theorem of Conway and Parker [FV1, Appendix], this implies that H_r acts transitively on $\mathcal{E}^{(s)}_{ab}$ and $\mathcal{E}^{(s)}_{in}$ for suitably large s. From now on we assume s has been chosen such that this holds.

By the theory of covering spaces, the connected components of $\mathcal{H}^{ab}_r(G)$ (resp., $\mathcal{H}^{in}_r(G)$) are in 1-1 correspondence with the orbits of H_r on the fiber $\Psi^{-1}(\mathbf{b})$ (resp., $(\Psi')^{-1}(\mathbf{b})$). The set $\mathcal{E}^{(s)}_{ab}$ (resp., $\mathcal{E}^{(s)}_{in}$) yields such an orbit (through the identifications in §1.3). Let $\mathcal{H}$ (resp., $\mathcal{H}'$) denote the corresponding component of $\mathcal{H}^{ab}_r(G)$ (resp., $\mathcal{H}^{in}_r(G)$). We call these spaces **Hurwitz spaces**. By [FV1, Thm. 1], $\mathcal{H}$ and $\mathcal{H}'$ are absolutely irreducible components, defined over $\mathbb{Q}$, of $\mathcal{H}^{ab}_r(G)$ and $\mathcal{H}^{in}_r(G)$, respectively. From now on we work only with $\mathcal{H}$ and $\mathcal{H}'$.

Let $\Psi\colon \mathcal{H} \to \mathcal{U}_r$ and $\Psi'\colon \mathcal{H}' \to \mathcal{U}_r$ denote the restriction of the original maps. Thus $\Psi\colon \mathcal{H} \to \mathcal{U}_r$ is a connected covering, and the fiber $\Psi^{-1}(\mathbf{b})$ is identified with the set $\mathcal{E}^{(s)}_{ab}$. A similar statement holds for $\mathcal{H}'$. We get the sequence of coverings

$$\mathcal{H}' \xrightarrow{\Lambda} \mathcal{H} \xrightarrow{\Psi} \mathcal{U}_r$$

where Λ restricts to the natural map $\mathcal{E}^{(s)}_{in} \to \mathcal{E}^{(s)}_{ab}$ on the fibers over $\mathbf{b}$.

For $A \in \mathrm{Aut}(G)$, let $\delta_A\colon \mathcal{H}' \to \mathcal{H}'$ send the point $|\chi, h|$ to $|\chi, A \circ h|$. Then δ_A is an automorphism of the covering $\Lambda\colon \mathcal{H}' \to \mathcal{H}$. It depends only on the class of A modulo $\mathrm{Inn}(G)$. In fact, Λ is a Galois covering, and $A \mapsto \delta_A$ induces an isomorphism from $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ to $\mathrm{Aut}(\mathcal{H}'/\mathcal{H})$ [FV1, §6.1]. Furthermore, δ_A is a morphism defined over $\mathbb{Q}$ [FV1, §6.2].

Identify the fiber $(\Psi')^{-1}(\mathbf{b})$ with $\mathcal{E}^{in}_r$ as above. This yields an action of the maps δ_A on $\mathcal{E}^{in}_r$. Thereby, δ_A sends the class of $(\sigma_1, \ldots, \sigma_r)$ to the class of $(A(\sigma_1), \ldots, A(\sigma_r))$. (Clear from the definitions).

1.5 MORE ABOUT COMPLEX CONJUGATION c. The following observation is crucial in the proof of the main theorem.

(3) For each $A \in \mathrm{Aut}(G)$ with $A^2 = 1$ there is $\bar{Q}$-rational point $\boldsymbol{q} \in \mathcal{H}'$ lying over $\mathbf{b}$ such that $c(\boldsymbol{q}) = \delta_A(\boldsymbol{q})$.

Recall the choice of r and s from §1.4. Choose $\sigma_1, \ldots, \sigma_{r/2}$ such that for each conjugacy class $C \neq \{1\}$ of G there are exactly $s/2$ indices $j \in \{1, \ldots, r/2\}$ with $\sigma_j \in C$. Arrange additionally that $\sigma_1 \cdots \sigma_{r/2} = 1$: take $\sigma_2 = \sigma_1^{-1}$, $\sigma_4 = \sigma_3^{-1}$

etc. This is possible since s is divisible by 4. Then set $\sigma_{r-j+1} = A(\sigma_j^{-1})$ for $j = 1, \ldots, r/2$. This yields an r-tuple $(\sigma_1, \ldots, \sigma_r)$ in $\mathcal{E}^{(s)}$ such that $(\sigma_r^{-1}, \ldots, \sigma_1^{-1})$ is the A-conjugate of $(\sigma_1, \ldots, \sigma_r)$. By (2) and the action of δ_A on $\mathcal{E}_r^{\text{in}}$ (§1.4), we can take $\boldsymbol{q}$ to be the point corresponding to $(\sigma_1, \ldots, \sigma_r)$.

Remark: Serre [Se2, p. 92] uses the same construction of the tuple $(\sigma_1, \ldots, \sigma_r)$ for $A = 1$ to obtain regular extensions of $\mathbb{R}(t)$. We adopted the choice of the b_js from there. ∎

2. The embedding problem over a Hilbertian PRC-field

We proceed similarly as in our paper on PAC-fields [FV2, section 1]. Here, however, there are places that require additional arguments.

LEMMA 1: *Let $\mathcal{H}' \to \mathcal{H}$ be an unramified Galois covering of absolutely irreducible, non-singular varieties defined over a PRC-field P of characteristic 0. Assume all automorphisms of the cover are defined over P. Let $\beta\colon G_P \to \mathrm{Aut}(\mathcal{H}'/\mathcal{H})$ be a homomorphism such that for each involution $I \in G_P$ there is a $\bar{P}$-point $\boldsymbol{q} \in \mathcal{H}'$ with $I(\boldsymbol{q}) = \beta(I)(\boldsymbol{q})$. Then there exists a P-rational point $\boldsymbol{p}$ of $\mathcal{H}$ and a point $\boldsymbol{p}' \in \mathcal{H}'$ lying over $\boldsymbol{p}$ with the following property: $P(\boldsymbol{p}')$ is the fixed field of $\ker(\beta)$, and the G_P-orbit of $\boldsymbol{p}'$ coincides with the $\beta(G_P)$-orbit of $\boldsymbol{p}'$.*

Proof: We modify the proof of [FV2, Lemma 1]. View β as a 1-cocycle of G_P in $\mathrm{Aut}(\mathcal{H}')$. Such a cocycle defines a twisted form $\mathcal{H}''$ of $\mathcal{H}'$ over P (via Galois cohomology, see [Se1, Ch.III, Prop.5]). Identify the $\bar{P}$-points of $\mathcal{H}''$ and of the original variety $\mathcal{H}'$. Then the twisted form defines a new action of G_P on these $\bar{P}$-points $\boldsymbol{p}'$. If the old action of $g \in G_P$ sends $\boldsymbol{p}'$ to $g\boldsymbol{p}'$, then the new action sends $\boldsymbol{p}'$ to $g\beta(g)\boldsymbol{p}'$.

Consider an involution I in G_P. The fixed field R in $\bar{P}$ of I is a real closure of P. The point $\boldsymbol{q}$ with $I(\boldsymbol{q}) = \beta(I)(\boldsymbol{q})$ is an R-rational point of $\mathcal{H}''$ (since $G(\bar{P}/R) = \langle I \rangle$). Thus $\mathcal{H}''$ has a point over each real closure of P. Since P is PRC (and $\mathcal{H}''$ is non-singular), $\mathcal{H}''$ has a P-rational point $\boldsymbol{p}'$. The remainder of the proof is as in [FV2, Lemma 1]: The fact that $\boldsymbol{p}'$ is a P-rational point of $\mathcal{H}''$ means that $g\boldsymbol{p}' = \beta(g)^{-1}\boldsymbol{p}'$ for all $g \in G_P$. Since $\beta(g) \in \mathrm{Aut}(\mathcal{H}'/\mathcal{H})$, the image $\boldsymbol{p}$ of $\boldsymbol{p}'$ in $\mathcal{H}$ is rational over P. The rest of the claim is clear. ∎

The following group-theoretic Lemma overcomes some complications in the PRC-case. We thank D. Haran for supplying the present version of this Lemma (improved from the original version).

LEMMA 2: *Let H be a finite group, and G a normal subgroup. Then there exists a surjection $f\colon \hat{H} \to H$ of finite groups such that for $\hat{G} = f^{-1}(G)$ the following holds: $C_{\hat{H}}(\hat{G}) = 1$, and the Schur multiplier of $\hat{G}$ is generated by commutators. Further, each involution in $H \setminus G$ lifts to an involution in $\hat{H}$.*

Proof: Choose a presentation $1 \to \mathcal{R} \to \mathcal{F} \to H \to 1$, where $\mathcal{F}$ is the free product of a free group of finite rank with finitely many groups of order 2, say $\langle\delta_1\rangle, \dots, \langle\delta_e\rangle$, such that $\delta_1, \dots, \delta_e$ map onto the involutions in $H \setminus G$. The inverse image $\mathcal{F}_1$ of G in $\mathcal{F}$ contains no conjugates of $\delta_1, \dots, \delta_e$. Hence, by the Kurosh Subgroup Theorem it is a free group of finite rank. Let $\mathcal{N} = [\mathcal{F}_1, \mathcal{R}]$ be the group generated by commutators $[f, r]$ with $f \in \mathcal{F}_1, r \in \mathcal{R}$. Set $F = \mathcal{F}/\mathcal{N}$, $F_1 = \mathcal{F}_1/\mathcal{N}$, and $R = \mathcal{R}/\mathcal{N}$. Then $1 \to R \to F_1 \to G \to 1$ is a central extension.

By the general theory of the Schur multiplier [Hu, Kap.5, §23], R is the direct product of the Schur multiplier $M(G) = R \cap (F_1)'$ and a free abelian group A. Let A_0 be the intersection of all the F-conjugates of A. Then $A_0 \triangleleft F$. Since $[R : A] = |M(G)| < \infty$, also $[F : A_0] < \infty$. Set $\tilde{H} = F/A_0$, $\tilde{G} = F_1/A_0$, and $S = R/A_0$. Clearly, each involution in $H \setminus G$ lifts to an involution in $\tilde{H}$. Note that S is the direct product of $S \cap (\tilde{G})' \cong M(G)$ and A/A_0.

STEP 1: *The Schur multiplier $M = M(\tilde{G})$ is generated by commutators..*

This is similar to the proof of [FV1, Lemma 1]. Let D be a representation group of $\tilde{G}$. Then there is a central extension

$$1 \to M \to D \to \tilde{G} \to 1$$

such that M lies in the commutator subgroup D' of D. Let L be the subgroup of M generated by commutators from D that fall into M. Set $\bar{M} = M/L$, $\bar{D} = D/L$. Then we have the central extension

$$1 \to \bar{M} \to \bar{D} \to \tilde{G} \to 1$$

where $\bar{M} \leq (\bar{D})'$. Furthermore, $\bar{M}$ contains no non-trivial commutators from $\bar{D}$. Let T be the inverse image of S in $\bar{D}$ under the map $\bar{D} \to \tilde{G}$. Since S is central in $\tilde{G}$, we have $[T, \bar{D}] \leq \bar{M}$. Hence $[T, \bar{D}] = 1$. Thus the sequence

$$1 \to T \to D \to G \to 1$$

is also a central extension. This implies that $|T \cap (\bar{D})'| \leq |M(G)|$ (see the proof of [Hu, Kap.3, Satz 23.5]).

On the other hand, $T \cap (\bar{D})'$ contains the inverse image in $\bar{D}$ of $S \cap (\tilde{G})' \cong M(G)$ (since $\bar{M} \subset (\bar{D})'$); thus $|T \cap (\bar{D})'| \geq |M(G)| \cdot |\bar{M}|$. Hence $\bar{M} = 1$, and so $M(\tilde{G}) = M = L$ is generated by commutators. This completes Step 1.

STEP 2: *Let T be a non-abelian finite simple group with trivial Schur multiplier. (For example, $T = \mathrm{SL}_2(8)$ [Hu, Satz 25.7].) Form the regular wreath product $\hat{H}$ of $\tilde{H}$ with T [Hu, Def. 15.6]. Thus $\hat{H} = T^j \times^s \tilde{H}$, with $j = |\tilde{H}|$, and $\tilde{H}$ acts on T^j by permuting the factors in its regular representation. Define $f\colon \hat{H} \to H$ as the composition of projection $\hat{H} \to \tilde{H}$ followed by the natural map $\tilde{H} \to H$. Then the properties required in the Lemma hold.*

We have T^j contained in $\hat{G} = f^{-1}(G)$. Clearly, $C_{\hat{H}}(T^j) = 1$, hence also $C_{\hat{H}}(\hat{G}) = 1$. It is also clear that each involution in $H \smallsetminus G$ lifts to an involution in $\hat{H}$ (because this is true for $\tilde{H}$).

Any central extension of T splits because T is perfect and $M(T) = 1$. Thus every central extension of T^j splits. This implies that every representation group of $\hat{G}$ has a normal subgroup isomorphic to T^j such that the quotient by this subgroup is a representation group of $\tilde{G}$. Therefore, $M(\hat{G}) \cong M(\tilde{G})$ is generated by commutators. ∎

PROPOSITION 1: *Let P be a PRC-field (of characteristic 0). Let H be a finite group and G a normal subgroup. Suppose $\beta\colon G_P \to H/G$ is a surjection such that for every involution $I \in G_P$ there exists an element in H of order ≤ 2 whose image in H/G equals $\beta(I)$. Let P' be the fixed field of $\ker(\beta)$. Then we have:*
(a) There exists a Galois extension L of $P(x)$ containing P' and regular over P', such that there is an isomorphism $G(L/P(x)) \to H$ sending $G(L/P'(x))$ to G.
(b) If P is Hilbertian, then there exists a Galois extension P''/P containing P' such that there is an isomorphism $G(P''/P) \to H$ sending $G(P''/P')$ to G.

Proof: Claim (b) follows from (a): If P is Hilbertian, we obtain the desired extension P''/P by specializing the extension $L/P(x)$. It remains to prove (a).

PART 1: *Reduction to the case that $C_H(G) = 1$ and $M(G)$ is generated by commutators.* Let $f : \hat{H} \to H$ and $\hat{G} = f^{-1}(G)$ be as in Lemma 2. Then $\hat{H}/\hat{G} \cong H/G$ canonically. Suppose the conclusion of the Proposition holds for $\hat{H}$ in place of H and $\hat{G}$ in place of G. Then we can embed P' into a Galois extension $K/P(x)$ with an isomorphism $G(K/P(x)) \to \hat{H}$ sending $G(K/P'(x))$ to $\hat{G}$. The subfield of K corresponding to the kernel of $f : \hat{H} \to H$ is the desired

L. This completes the reduction to the special case that $C_H(G) = 1$ and $M(G)$ is generated by commutators. Assume from now on that these conditions hold.

PART 2: *Application of [FV1].* Now we use the results of §1.4. There we constructed the unramified Galois cover Λ: $\mathcal{H}' \to \mathcal{H}$ of absolutely irreducible nonsingular varieties defined over $\mathbb{Q}$. Recall that all automorphisms of this cover are defined over $\mathbb{Q}$, and are of the form δ_A, $A \in \text{Aut}(G)$.

Proposition 3 of [FV1] yields the following facts. For each point $\boldsymbol{p} \in \mathcal{H}$, rational over some field k, and for each point $\boldsymbol{p}' \in \mathcal{H}'$ lying over $\boldsymbol{p}$, there is a Galois extension $L/k'(x)$, regular over $k' = k(\boldsymbol{p}')$, with the following properties: L is Galois over $k(x)$, and there is an isomorphism h from $G(L/k(x))$ to the group Δ of all $A \in \text{Aut}(G)$ for which $\delta_A(\boldsymbol{p}')$ is conjugate to $\boldsymbol{p}'$ under $G(k'/k)$. Furthermore, h restricts to an isomorphism between $G(L/k'(x))$ and $\text{Inn}(G)$. (Note: k'/k is Galois because all automorphisms of the Galois covering Λ are defined over $\mathbb{Q}$).

Now assume $k = P$ is a PRC-field. Consider the given Galois extension P'/P with group isomorphic to G/H. Since $C_H(G) = 1$, we can view H as a subgroup of $\text{Aut}(G)$ (via conjugation action). Then H/G is a subgroup of $\text{Out}(G)$. Hence it is isomorphic to a subgroup F of $\text{Aut}(\mathcal{H}'/\mathcal{H})$, via the map $A \mapsto \delta_A$. The composition of the given map β: $G_P \to H/G$ with the map $H/G \cong F$ yields a homomorphism $\tilde{\beta}$: $G_P \to \text{Aut}(\mathcal{H}'/\mathcal{H})$. Part 3 below shows that the hypothesis on the $\tilde{\beta}(I)$ from Lemma 1 holds. Thus we can choose $\boldsymbol{p}$ and $\boldsymbol{p}'$ so that $P(\boldsymbol{p}') = P'$, and the G_P-orbit of $\boldsymbol{p}'$ equals the F-orbit of $\boldsymbol{p}'$.

For the associated Galois extension $L/P(x)$, it follows that $G(L/P(x))$ is isomorphic to the group Δ of all $A \in \text{Aut}(G)$ for which $\delta_A(\boldsymbol{p}')$ is conjugate to $\boldsymbol{p}'$ under $G(P'/P)$. Since $G_P \cdot \boldsymbol{p}' = F \cdot \boldsymbol{p}'$, we get

$$\Delta = \{A \in \text{Aut}(G) \colon \delta_A(\boldsymbol{p}') \in F \cdot \boldsymbol{p}'\} = \{A \in \text{Aut}(G) \colon \delta_A \in F\} = H.$$

Thus $G(L/P(x))$ is isomorphic to H, under an isomorphism that maps the subgroup $G(L/P'(x))$ onto G ($\cong \text{Inn}(G)$).

PART 3: *Verifying the hypothesis of Lemma 1.* It remains to show that for each involution I of G_P there exists a $\bar{P}$-point $\boldsymbol{q} \in \mathcal{H}'$ with $I(\boldsymbol{q}) = \tilde{\beta}(I)(\boldsymbol{q})$. We have $\tilde{\beta}(I) = \delta_A$ where $A \in H$ has image in H/G equal to $\beta(I)$. By the hypothesis on lifting of involutions, we can choose A such that $A^2 = 1$. By §1.5 there exists a $\bar{\mathbb{Q}}$-point $\boldsymbol{q}' \in \mathcal{H}'$ such that $c(\boldsymbol{q}') = \delta_A(\boldsymbol{q}')$.

Note that $\sqrt{-1}$ does not lie in the real closed field fixed by I. Therefore, the restriction I_0 of I to an element of $G_{\mathbb{Q}}$ is not trivial. Since all involutions in $G_{\mathbb{Q}}$

are conjugate, there is $\alpha \in G_{\mathbb{Q}}$ such that $\alpha^{-1} I_0 \alpha$ equals the restriction of c to $\bar{\mathbb{Q}}$. Set $\boldsymbol{q} = \alpha(\boldsymbol{q}')$. Since δ_A is defined over $\mathbb{Q}$ we have

$$I(\boldsymbol{q}) = I_0(\boldsymbol{q}) = I_0\alpha(\boldsymbol{q}') = \alpha c(\boldsymbol{q}') = \alpha\delta_A(\boldsymbol{q}') = \delta_A\alpha(\boldsymbol{q}') = \delta_A(\boldsymbol{q}) = \tilde{\beta}(I)(\boldsymbol{q}),$$

as desired. ∎

We thank M. Jarden and D. Haran for their contributions to the following lemma.

LEMMA 3: *Let f: $E \to C$ be a surjection of finite groups. Let Z be a set of involutions of C such that every $z \in Z$ lifts to an involution of E. Then there exists a surjection g: $A \to E$ of finite groups with the following properties: Every automorphism γ of C with $\gamma(Z) = Z$ lifts to an automorphism α of A (i.e., $f \circ g \circ \alpha = \gamma \circ f \circ g$). Further, every $z \in Z$ lifts to an involution in A.*

Proof: Let $\mathcal{F}_0$ be a free group with a system of generators that are in 1-1 correspondence with the elements of E, and let $\mathcal{F}_0 \to E$ be the extension of the given map on the generators. Let $\mathcal{F}$ be the free product of $\mathcal{F}_0$ and a number of groups $\langle y_i \rangle$ of order 2, one for each element of Z. Extend the above map to a map $\mathcal{F} \to E$ sending the y_i to involutions of E that lie over the corresponding elements of Z.

Let $\mathcal{N}$ be the intersection of all normal subgroups N of $\mathcal{F}$ with $\mathcal{F}/N \cong E$. Then $A \stackrel{\text{def}}{=} \mathcal{F}/\mathcal{N}$ is a finite group, and the map $\mathcal{F} \to E$ induces a surjection g: $A \to E$. Every automorphism γ of C with $\gamma(Z) = Z$ is induced from an automorphism of $\mathcal{F}$ (permuting the generators). This automorphism fixes $\mathcal{N}$, hence induces an automorphism α of A. Clearly α lifts γ. Also, since every $z \in Z$ lifts to an involution of $\mathcal{F}$, it lifts to an involution of A. ∎

THEOREM: *Let P be a PRC-field of characteristic 0. Let h: $H \to C$ be a surjection of finite groups, and let β: $G_P \to C$ be a surjection such that for every involution I of G_P the element $\beta(I)$ lifts to an element of H of order ≤ 2. Then:*
(a) There exists a surjection ϵ_0: $G_{P(x)} \to H$ with $h\epsilon_0 = \beta_0$, where β_0: $G_{P(x)} \to C$ is the composition of β with restriction $G_{P(x)} \to G_P$.
(b) If P is Hilbertian there exists a surjection ϵ: $G_P \to H$ with $h\epsilon = \beta$.

Proof: We prove (b). The same proof works for (a) if we replace β by β_0, G_P by $G_{P(x)}$ and use part (a) of Proposition 1 instead of part (b).

Let Z be the set of involutions of C that lift to involutions of G_P. By [HJ1, Cor. 6.2] there is a surjection $\lambda\colon \tilde{C} \to C$ of finite groups such that the involutions of $\tilde{C} \smallsetminus \ker(\lambda)$ are mapped onto Z by λ. Set

$$E = \{(a,b) \in H \times \tilde{C}\colon\ h(a) = \lambda(b)\}$$

(the fiber product of H and $\tilde{C}$ over C). Let $\pi\colon E \to H$, $\tilde{\pi}\colon E \to \tilde{C}$ be the projections. Consider the surjection $f = h \circ \pi = \lambda \circ \tilde{\pi}\colon E \to C$. Clearly, each $z \in Z$ lifts to an involution of E. Thus we can choose a surjection $g\colon A \to E$ with the properties from Lemma 3.

Now suppose P is Hilbertian. It follows from Proposition 1(b) that there is a surjection $\theta\colon G_P \to A$ with $\ker(f \circ g \circ \theta) = \ker(\beta)$. Thus $\gamma \circ f \circ g \circ \theta = \beta$ for some automorphism γ of C. Now fix some $z \in Z$. There is an involution $\nu \in G_P$ with $z = \beta(\nu)$. Since $\beta = \gamma \circ f \circ g \circ \theta$, we have $z = \gamma(z')$, where $z' = f \circ g \circ \theta(\nu)$. Now

$$z' = f \circ g \circ \theta(\nu) = \lambda \circ \tilde{\pi} \circ g \circ \theta(\nu) = \lambda(\tilde{z})$$

where $\tilde{z} = \tilde{\pi} \circ g \circ \theta(\nu)$ is an involution of $\tilde{C} \smallsetminus \ker(\lambda)$ (since $z' \neq 1$). Thus $z' = \lambda(\tilde{z}) \in Z$ by the choice of λ. We have shown that $z' = \gamma^{-1}(z)$ lies in Z for every $z \in Z$. Thus $\gamma(Z) = Z$.

By choice of A, we can lift γ to an automorphism α of A. Then $\epsilon \overset{\text{def}}{=} \pi \circ g \circ \alpha \circ \theta$ is a surjection $G_P \to H$ with $h\epsilon = h \circ \pi \circ g \circ \alpha \circ \theta = f \circ g \circ \alpha \circ \theta = \gamma \circ f \circ g \circ \theta = \beta$, as desired. ∎

The theorem suggests the following definition. Let $\mathcal{G}$ be a profinite group. We say that all **restricted finite embedding problems** for $\mathcal{G}$ are solvable if the following holds: For each surjection $h\colon H \to C$ of finite groups, and for each surjection $\beta\colon \mathcal{G} \to C$ such that for every involution I of $\mathcal{G}$ the element $\beta(I)$ lifts to an element of H of order ≤ 2 there exists a surjection $\epsilon\colon \mathcal{G} \to H$ with $h\epsilon = \beta$.

Now we show that among groups of countable rank, this condition characterizes the real-free groups $\mathcal{G}$ (in the sense of [HJ2]). This generalizes Iwasawa's result: Solvability of *all* finite embedding problems for a profinite group of countable rank forces the group to be free. More precisely, the group is isomorphic to the free profinite group $\hat{F}_\omega$ of countably infinite rank [FrJ, Cor. 24.2].

For each profinite group $\mathcal{G}$, let $\Delta(\mathcal{G})$ be the set of conjugacy classes of elements of $\mathcal{G}$ of order ≤ 2. Endow $\Delta(\mathcal{G})$ with the topology as a quotient of the (closed) set of elements of order ≤ 2. We view $\Delta(G)$ as a *pointed topological space*, where the trivial class $\{1\}$ is the distinguished element.

PROPOSITION 2: *Suppose $\mathcal{G}$ and $\mathcal{H}$ are profinite groups of countable rank for which all restricted finite embedding problems are solvable. If $\Delta(\mathcal{G})$ and $\Delta(\mathcal{H})$ are homeomorphic as pointed topological spaces, then $\mathcal{G}$ and $\mathcal{H}$ are isomorphic.*

Proof: Fix a homeomorphism between $\Delta(\mathcal{G})$ and $\Delta(\mathcal{H})$ under which the trivial class of $\Delta(\mathcal{G})$ corresponds to that of $\Delta(\mathcal{H})$. Use this homeomorphism to identify the two spaces. Set $\Delta = \Delta(\mathcal{G}) = \Delta(\mathcal{H})$.

The condition of countable rank yields sequences of open normal subgroups of $\mathcal{G}$ and $\mathcal{H}$, respectively,

$$\mathcal{G} = \mathcal{N}^{(0)} > \mathcal{N}^{(1)} > \mathcal{N}^{(2)} > \cdots$$

$$\mathcal{H} = \mathcal{M}^{(0)} > \mathcal{M}^{(1)} > \mathcal{M}^{(2)} > \cdots$$

with trivial intersection.

We now construct further such sequences

$$\mathcal{G} = \mathcal{N}_0 > \mathcal{N}_1 > N_2 > \cdots$$

$$\mathcal{H} = \mathcal{M}_0 > \mathcal{M}_1 > \mathcal{M}_2 > \cdots$$

with the following additional properties.

(1) There are isomorphisms κ_i: $\mathcal{G}/\mathcal{N}_i \to \mathcal{H}/\mathcal{M}_i$, compatible in the sense that κ_i composed with the natural map $\mathcal{H}/\mathcal{M}_i \to \mathcal{H}/\mathcal{M}_{i-1}$ is the same as the composition of $\mathcal{G}/\mathcal{N}_i \to \mathcal{G}/\mathcal{N}_{i-1}$ with κ_{i-1}.

(2) For each $\delta \in \Delta$, the images of δ in $\Delta(\mathcal{G}/\mathcal{N}_i)$ and in $\Delta(\mathcal{H}/\mathcal{M}_i)$ correspond under κ_i.

We construct the κ_i inductively, starting with the trivial case $i = 0$. Now assume $i > 0$, and everything has been constructed up to the index $i-1$, satisfying (1) and (2). If i is even, proceed as follows; if i is odd, interchange the roles of $\mathcal{G}$ and $\mathcal{H}$. (This is the usual trick in showing that free profinite groups are characterized by the solvability of embedding problems, cf. [FrJ, Lemma 24.1]).

Choose $\mathcal{M}_i$ to be any open normal subgroup of $\mathcal{H}$ contained in $\mathcal{M}^{(i)}$ and in $\mathcal{M}_{i-1}$. Since the open normal subgroups $\mathcal{N}$ of $\mathcal{G}$ form a basis for the neighborhoods of 1, one can choose $\mathcal{N} \subset \mathcal{N}_{i-1}$ such that any two elements of Δ that have the same image in $\Delta(\mathcal{G}/\mathcal{N})$ also have the same image in $\Delta(\mathcal{H}/\mathcal{M}_i)$. Set $\bar{\mathcal{G}} = \mathcal{G}/\mathcal{N}$ and $\bar{\mathcal{H}} = \mathcal{H}/\mathcal{M}_i$.

Now consider the fiber product

$$F = \{(g\mathcal{N}, h\mathcal{M}_i) \in \bar{\mathcal{G}} \times \bar{\mathcal{H}}\colon\ \kappa_{i-1}(g\mathcal{N}_{i-1}) = h\mathcal{M}_{i-1}\}$$

Let $\pi_1\colon F \to \bar{\mathcal{G}}$ and $\pi_2\colon F \to \bar{\mathcal{H}}$ be the projections. By [HJ1, Cor. 6.2] there exists a finite group E and a surjection $\lambda\colon E \to F$ such that the involutions of $E \setminus \ker(\lambda)$ are mapped onto those involutions $(g\mathcal{N}, h\mathcal{M}_i)$ of F for which $g \in \mathcal{G}$ and $h \in \mathcal{H}$ correspond to the same element of Δ.

The canonical map $\mathcal{G} \to \bar{\mathcal{G}}$ and the map $\pi_1\lambda\colon E \to \bar{\mathcal{G}}$ make a restricted embedding problem for $\mathcal{G}$. Namely, by (2), for each involution g of $\mathcal{G}$ there is an involution $h \in \mathcal{H}$ with $\kappa_{i-1}(g\mathcal{N}_{i-1}) = h\mathcal{M}_{i-1}$, such that g and h correspond to the same element of Δ. Thus if $g\mathcal{N} \neq 1$ then $g\mathcal{N}$ lifts to the involution $(g\mathcal{N}, h\mathcal{M}_i)$ of F, and this involution lifts to an involution of E (by the choice of E). The condition of a *restricted* embedding problem is fulfilled. Let $\chi\colon \mathcal{G} \to E$ be a solution of this embedding problem (i.e., $\pi_1\lambda\chi$ is the canonical map $\mathcal{G} \to \bar{\mathcal{G}}$).

Finally let $\mathcal{N}_i$ be the kernel of the surjection $\pi_2\lambda\chi\colon \mathcal{G} \to \bar{\mathcal{H}}$. Let $\kappa_i : \mathcal{G}/\mathcal{N}_i \to \bar{\mathcal{H}} = \mathcal{H}/\mathcal{M}_i$ be the induced isomorphism. The validity of (1) is then clear by construction. For (2), consider $\delta \in \Delta$, represented by the involution $g \in \mathcal{G}$.

If $\lambda\chi(g) \neq 1$, then $\chi(g)$ is an involution of $E \setminus \ker(\lambda)$. Hence $\lambda\chi(g)$ is of the form $(g'\mathcal{N}, h\mathcal{M}_i)$ where $g' \in \mathcal{G}$ and $h \in \mathcal{H}$ correspond to the same element δ' of Δ. Since $\pi_1\lambda\chi$ is the canonical map $\mathcal{G} \to \bar{\mathcal{G}}$, we have $g'\mathcal{N} = g\mathcal{N}$. This implies that δ and δ' have the same image in $\Delta(\mathcal{H}/\mathcal{M}_i)$ (by the choice of $\mathcal{N}$). We have $\kappa_i(g\mathcal{N}_i) = h\mathcal{M}_i$. Hence the image of δ in $\Delta(\mathcal{G}/\mathcal{N}_i)$ corresponds under κ_i to the image of δ' in $\Delta(\mathcal{H}/\mathcal{M}_i)$. The latter equals the image of δ in $\Delta(\mathcal{H}/\mathcal{M}_i)$ (by the above). This proves (2) in the case $\lambda\chi(g) \neq 1$.

Now assume $\lambda\chi(g) = 1$. Then $\kappa_i(g\mathcal{N}_i) = \pi_2\lambda\chi(g) = 1$, and $g\mathcal{N} = \pi_1\lambda\chi(g) = 1$. The former means that δ has trivial image in $\Delta(\mathcal{G}/\mathcal{N}_i)$, and the latter means that δ has trivial image in $\Delta(\mathcal{G}/\mathcal{N})$. Then it also has trivial image in $\Delta(\mathcal{H}/\mathcal{M}_i)$ (by the choice of $\mathcal{N}$). Thus (2) also holds in the present case. Now we have verified conditions (1) and (2).

If one alternates the roles of $\mathcal{G}$ and $\mathcal{H}$ in each step of the construction, then it is clear that the sequences $(\mathcal{N}_i)$ and $(\mathcal{M}_i)$ both have trivial intersection. (This is because we have required that $\mathcal{M}_i \leq \mathcal{M}^{(i)}$; in the next step one gets $\mathcal{N}_{i+1} \leq \mathcal{N}^{(i+1)}$ etc.). It follows from (1) that the isomorphisms κ_i glue together to an isomorphism from $\mathcal{G}$ to $\mathcal{H}$. This completes the proof of the Proposition. ∎

Remark: Compare the above Proposition with Lemma 3.4 of [HJ3], which considers *proper* real embedding problems (as opposed to our *restricted* embedding problems). ∎

From now on we consider only profinite groups $\mathcal{G}$ whose involutions form a closed subset. The absolute Galois group G_K of each field K has this property. (The subgroup of G_K fixing $\sqrt{-1}$ is a neighborhood of the identity that contains no involutions). Let $\Delta_0(\mathcal{G}) \overset{\text{def}}{=} \Delta(\mathcal{G}) \smallsetminus \{1\}$ be the set of conjugacy classes of involutions of $\mathcal{G}$. Since the involutions form a closed set, $\Delta(\mathcal{G})$ has the topology of a disjoint union of $\Delta_0(\mathcal{G})$ and the distinguished point.

Proposition 2 says that for each topological space Δ_0 there is — up to isomorphism — at most one profinite group $\mathcal{G}$ of countable rank with the following properties: $\Delta_0(\mathcal{G}) \cong \Delta_0$, all finite restricted embedding problems for $\mathcal{G}$ are solvable, and the set of involutions of $\mathcal{G}$ is closed. If such $\mathcal{G}$ exists then Δ_0 is a boolean space with countable basis.

Conversely, for each such Δ_0 there is actually a group $\mathcal{G} = \mathcal{G}(\Delta_0)$ with the above properties. This is a *real-free* group in the sense of [HJ2]. It can be constructed as follows (see [HJ2]): Take a group freely generated (in the category of profinite groups) by a set of involutions homeomorphic to Δ_0. Form the free product of this group with $\hat{F}_\omega$ (see above). This yields the group $\mathcal{G}(\Delta_0)$.

For a field P, let $Y(P)$ be the set of orderings of P. The *Harrison topology* on $Y(P)$ has a subbasis of clopen sets of the form H_a, $a \in P^*$, where H_a is the set of all orderings for which a is positive. The spaces $Y(P)$ and $\Delta_0(G_P)$ are naturally homeomorphic, via the map that associates with a class of involutions $I \in G_P$ the ordering of P induced by the unique ordering of the fixed field of I [H, p. 399].

If P is countable, its absolute Galois group has countable rank [FJ, Ex. 15.13]. Combine this with the above remarks, with Proposition 2 and our main theorem to obtain the following.

COROLLARY 1: *If P is a countable Hilbertian PRC-field, then the absolute Galois group G_P is isomorphic to the real-free group $\mathcal{G}(Y(P))$. Here $Y(P)$ is the topological space of orderings of P. Thus G_P is isomorphic to the free product (in the category of profinite groups) of $\hat{F}_\omega$ with a group that is freely generated by a set of involutions homeomorphic to $Y(P)$.*

COROLLARY 2: *Let P be a finite proper extension of the field $\mathbb{Q}_{re}$ of all totally* *real algebraic numbers. Then the absolute Galois group G_P is real-free. If P has no ordering then G_P is isomorphic to $\hat{F}_\omega$. Otherwise G_P is isomorphic to $\mathcal{G}(X_\omega)$, with X_ω the Cantor set. Thus only two isomorphism types occur among the G_P.*

Proof: By the Introduction, P is countable, Hilbertian and PRC. Thus $G_P \cong \mathcal{G}(Y(P))$ by Corollary 1. If P has no ordering then $Y(P)$ is empty, hence $G_P \cong \hat{F}_\omega$. It remains to show that $Y(P) \cong X_\omega$ in all other cases. This is done in the following Remark, which is due to M. Jarden. ∎

Remark — M. Jarden: Proper real extensions of $\mathbb{Q}_{re}$. Let P be a finite proper extension of $\mathbb{Q}_{re}$ that has at least one ordering. There is a number field L with $L\mathbb{Q}_{re} = P$. Let $K = L \cap \mathbb{Q}_{re}$. Then L has a finite positive number of orderings. Let L_1 be a finite extension of L contained in P, and let $K_1 = L_1 \cap \mathbb{Q}_{re}$. Then L is linearly disjoint from K_1 over K. As K_1 is totally real, each embedding of K into the reals extends to $[K_1 : K]$ embeddings of K_1 into the reals. Therefore, each ordering of K extends to $[K_1 : K]$ orderings of K_1. Since L is linearly disjoint from K_1 over K, each pair of orderings of L and of K_1 which coincide on K has a unique extension to L_1 [Ja; p. 241]. Since the space of orderings of P is the projective limit of the space of orderings of all those L_1's, it is isomorphic to the Cantor set X_ω (see [HJ3]). ∎

References

[DeFr] P. Debes and M. Fried, *Rigidity and real residue class fields,* Acta Arithmetica **56** (1990), 13–45.

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

[FV1] M. Fried and H. Völklein, *The inverse Galois problem and rational points on moduli spaces,* Math. Annalen **290** (1991), 771–800.

[FV2] M. Fried and H. Völklein, *The embedding problem over a Hilbertian PAC-field,* Annals of Mathematics **135** (1992), 469–481.

[H] D. Haran, *Closed subgroups of $G(\mathbb{Q})$ with involutions,* Journal of Algebra **129** (1990), 393–411.

[HJ1] D. Haran and M. Jarden, *The absolute Galois group of a pseudo-real-closed field,* Ann. Scuola Norm. Sup. Pisa **12** (1985), 449–489.

[HJ2] D. Haran and M. Jarden, *Real-free groups and the absolute Galois group of $\mathbb{R}(t)$,* Journal of Pure and Applied Mathematics **37** (1986), 155–165.

[HJ3] D. Haran and M. Jarden, *The absolute Galois group of a pseudo real closed algebraic field*, Pacific J. Math. **123** (1986), 55–69.

[Hu] B. Huppert, *Endliche Gruppen I*, Die Grundlehren der mathematischen Wissenschaften **134**, Springer, Berlin, 1967.

[Iw] K. Iwasawa, *On solvable extensions of algebraic number fields*, Annals of Math. **58** (1953), 548–572.

[Ja] M. Jarden, *The elementary theory of large e-fold ordered fields*, Acta Math. **149** (1982), 239–260.

[P] F. Pop, *Fields of totally* Σ*-adic numbers*, preprint 1991.

[Pr] A. Prestel, *Pseudo real closed fields*, in *Set Theory and Model Theory*, Lecture Notes in Mathematics **872**, Springer, Berlin, 1981.

[Se1] J.-P. Serre, *Cohomologie Galoisienne*, Lecure Notes in Mathematics **5**, Springer, Berlin, 1964.

[Se2] J.-P. Serre, *Topics in Galois Theory*, Jones and Bartlett, Boston, 1992.

[Ws] R. Weissauer, *Der Hilbertsche Irreduzibilitätssatz*, Journal für die reine und angewandte Mathematik **334** (1982), 203–220.