THE ABSOLUTE GALOIS GROUP OF A HILBERTIAN PSEUDO-REAL-CLOSED FIELD

Appeared in Israel Journal of Math. **85** (1994), 85–101
Michael D. Fried[*], *UC Irvine*
Helmut Völklein[**], *U of Florida and Universität Erlangen*

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.

---

[*]Supported by NSA grant MDA 14776 and BSF grant 87-00038
[**]Supported by NSA grant MDA 904-89-H-2028
Part of this work was done while the authors were fellows of the Institute for Advanced Studies in Jerusalem

AMS Subject classification: 11G35, 12F10, 14D20, 14E20, 14G05, 20B25, 20C25

Keywords: Embedding problems; Galois groups; PRC-fields; Hilbertian fields; real-free profinite groups

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

Acknowledgement: We thank D. Haran for helpful discussions that led to a proof of Proposition 1.

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 $\mathbf{P}^1 = \mathbf{C} \cup \{\infty\}$. 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 $\mathbf{Q}$ [FV1, §1.1]. So, the above base point $\mathbf{b}$ is rational over $\mathbf{Q}$. 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:** Now we consider covers $\chi : X \to \mathbf{P}^1$ of compact (connected) Riemann surfaces. Two covers $\chi : X \to \mathbf{P}^1$ and $\chi' : X' \to \mathbf{P}^1$ are *equivalent* if there exists an isomorphism $\epsilon : X \to X'$ with $\chi'\epsilon = \chi$. Let $\mathrm{Aut}(X/\mathbf{P}^1)$ be the group of automorphisms ϵ of X with $\chi\epsilon = \chi$. We call χ a Galois cover if $\mathrm{Aut}(X/\mathbf{P}^1)$ is transitive on the fibers of χ. From here on χ will be a Galois cover. All but finitely many points of $\mathbf{P}^1$ have the same number of inverse images under χ. These exceptional points are the *branch points* of χ.

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

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

To determine the equivalence class of the cover Ψ, 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 $\mathcal{U}_r$.) 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 $\gamma_1, \ldots, \gamma_r$ for the fundamental group $\Gamma = \pi_1(\mathbf{P}^1 \backslash \mathbf{b}, 0)$. (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 $\gamma_1, \ldots, \gamma_{r-1}$, 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 $j = 1, \ldots, r/2$ (since the corresponding relation holds for the b_j's).

Now let $\chi : X \to \mathbf{P}^1$ be a (Galois) cover of $\mathbf{P}^1$ with $|\chi| \in \Psi^{-1}(\mathbf{b})$. This means $\mathrm{Aut}(X/\mathbf{P}^1) \cong G$, and $b_1, \ldots, b_r$ are the branch points of χ. Thus χ restricts to an unramified cover of the punctured sphere $\mathbf{P}^1 \backslash \mathbf{b}$. By the theory of covering spaces, the latter corresponds to a normal subgroup U_χ of $\Gamma = \pi_1(\mathbf{P}^1 \backslash \mathbf{b}, 0)$. Then, Γ / U_χ is isomorphic to $\mathrm{Aut}(X/\mathbf{P}^1)$. Thus, there is a surjection $f : \Gamma \to G$ with kernel U_χ. The surjection f is determined by the r-tuple $(\sigma_1, \ldots, \sigma_r) = (f(\gamma_1), \ldots, f(\gamma_r))$. This r-tuple $(\sigma_1, \ldots, \sigma_r)$ has the following properties: $\sigma_1 \cdots \sigma_r = 1$, the group G is generated by $\sigma_1, \ldots, \sigma_r$, 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 $(\sigma_1, \ldots, \sigma_r)$.

Each tuple $(\sigma_1, \ldots, \sigma_r) \in \mathcal{E}_r$ occurs for some χ. Another choice of f (for the same or equivalent χ) results in an r-tuple conjugate to $(\sigma_1, \ldots, \sigma_r)$ under an element of $\mathrm{Aut}(G)$. 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 $\mathcal{E}_r^{\rm ab} \stackrel{\rm def}{=} \mathcal{E}_r / \mathrm{Aut}(G)$ of $\mathrm{Aut}(G)$-classes of the tuples $(\sigma_1, \ldots, \sigma_r)$. Via this bijection, $H_r = \pi_1(\mathcal{U}_r, \mathbf{b}) =< Q_1, \ldots, Q_{r-1} >$ acts on $\mathcal{E}_r^{\rm ab}$. For a suitable generators $Q_1, \ldots, Q_{r-1}$ here is how this action works [FV1, §1.4]. The element Q_j sends the class of $(\sigma_1, \ldots, \sigma_r)$ to the class of

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

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

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

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

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

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

It suffices to show this. If $|\chi, h| \in (\Psi')^{-1}(\mathbf{b})$ corresponds to the class of $(\sigma_1, \dots, \sigma_r)$ in $\mathcal{E}_r^{\text{in}}$, then $|\chi^c, h \circ c|$ corresponds to the class of $(\sigma_r^{-1}, \dots, \sigma_1^{-1})$. This is a straightforward consequence of the definitions, and of the formula $c(\gamma_j) = \gamma_{r-j+1}^{-1}$ $(j = 1, \dots, r/2)$ 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 $\mathcal{E}^{(s)}_{\rm ab}$ (resp., $\mathcal{E}^{(s)}_{\rm in}$) be the image of $\mathcal{E}^{(s)}$ in $\mathcal{E}^{\rm ab}_r$ (resp., $\mathcal{E}^{\rm in}_r$).

The sets $\mathcal{E}^{(s)}_{\rm ab}$ and $\mathcal{E}^{(s)}_{\rm in}$ 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]. From a theorem of Conway and Parker [FV1, Appendix], this implies that H_r acts transitively on $\mathcal{E}^{(s)}_{\rm ab}$ and $\mathcal{E}^{(s)}_{\rm in}$ for suitably large s. From here we assume s has been chosen such that this holds.

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

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

$$\mathcal{H}' \stackrel{\Lambda}{\longrightarrow} \mathcal{H} \stackrel{\Psi}{\longrightarrow} \mathcal{U}_r$$

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

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

Identify the fiber $(\Psi')^{-1}(\mathbf{b})$ with $\mathcal{E}^{\rm in}_r$ as above. This yields an action of the maps δ_A on $\mathcal{E}^{\rm in}_r$. Thereby, δ_A sends the class of $(\sigma_1, \ldots, \sigma_r)$ to the class of $(A(\sigma_1), \ldots, A(\sigma_r))$. (This is 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 $A \in {\rm Aut}(G)$ with $A^2 = 1$ there is a 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 $(\sigma_1, \ldots, \sigma_r)$. From (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 $\mathbf{R}(t)$. We adopted the choice of the b_js from there. □

æ

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 more delicate arguments.

Lemma 1: *Let $\mathcal{H}' \to \mathcal{H}$ be an unramified Galois cover 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 $\beta : G_P \to Aut(\mathcal{H}'/\mathcal{H})$ 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 $\mathrm{Aut}(\mathcal{H}')$. To such a cycle Galois cohomology [Se1, Ch.III, Prop.5], corresponds a twisted form $\mathcal{H}''$ of $\mathcal{H}'$ over P. 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 $\boldsymbol{p}'$. Here is how. 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 [loc. cit.]: $\boldsymbol{p}'$ 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.

Lemma 2: *Let $H = G \times^s C$ be the semi-direct product of finite groups G and C (G is normal). Then, there exists a finite group $\tilde{H} = \tilde{G} \times^s C$ with the following properties. First: There is a surjection $\tilde{H} \to H$ that sends $\tilde{G}$ to G and is the identity on C. Second: The Schur multiplier of $\tilde{G}$ is generated by commutators.*

Proof: Choose a presentation $\mathcal{R} \to \mathcal{F} \to H$, where $\mathcal{F}$ is a free group of finite rank. Then also the inverse image $\mathcal{F}_1$ of G in $\mathcal{F}$ is free of finite rank. Let $[\mathcal{F}_1, \mathcal{R}]$ be the group generated by commutators $[f, r]$ with $f \in \mathcal{F}_1, r \in \mathcal{R}$, and set $F_1 = \mathcal{F}_1/[\mathcal{F}_1, \mathcal{R}]$. The theory of the Schur multiplier [Hu, Kap.5, §23] says the image R of $\mathcal{R}$ in F_1 is the direct product of the Schur multiplier $M(G) = R \cap (F_1)'$ and a free abelian group A. Further, F_1 is a central extension of G with kernel R. In particular, R centralizes F_1. So, the natural action of $\mathcal{F}$ on F_1 factors through $\mathcal{F}/\mathcal{R} \cong H$. Thus, H acts naturally on F_1; the subgroup C of H acts naturally on F_1.

Let A_0 be the intersection of all C-conjugates of A. Then A_0 is a C-invariant subgroup of finite index in R. Thus, C acts naturally on the finite group $\tilde{G} \stackrel{\text{def}}{=} F_1/A_0$. This induces the original action of C on $G \cong \tilde{G}/S$, where S is the image of R in $\tilde{G}$. Note for later use that S is the direct product of $S \cap (\tilde{G})' \cong M(G)$ and A/A_0. Set $\tilde{H} \stackrel{\text{def}}{=} \tilde{G} \times^s C$. It remains to prove the Schur multiplier $M = M(\tilde{G})$ is generated by commutators. The argument we give is similar to the proof of [FV1, Lemma 1].

Let D be a representation group of $\tilde{G}$. Then there is a central extension

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

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

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

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

$$T \to \bar{D} \to G$$

is also a central extension. Conclude $|T \cap (\bar{D})'| \leq |M(G)|$ [Hu, Kap.3, §23].

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

For the remainder of the paper, P is a Hilbertian PRC-field (of characteristic 0). In Lemma 3 we show that all split (finite) embedding problems over P are solvable. This uses the main result of [FV1]. Lemma 2 allows us to adjust the corresponding argument from the PAC-case. In the PRC-case one can't easily do an induction where the kernel of the embedding problem is a minimal normal subgroup.

Lemma 3: *Let $H = G \times^s C$ be the semi-direct product of finite groups G and C. Then, each Galois extension P'/P with Galois group isomorphic to C embeds in a Galois extension P''/P with an isomorphism $G(P''/P) \to H$ sending $G(P''/P')$ to G.*

Proof: We divide the proof into three parts.

Part 1: *Reduction to the case that $C_H(G) = 1$ and $M(G)$ is generated by commutators.* Let $\tilde{H} = \tilde{G} \times^s C$ be as in Lemma 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 $j = |\tilde{H}|$. Here $\tilde{H}$ acts on T^j by permuting the factors in its regular representation. Then $\hat{H} = (T^j \times^s \tilde{G}) \times^s C = \hat{G} \times^s C$, with $\hat{G} = T^j \times^s \tilde{G}$. Now we have, $C_{\hat{H}}(T^j) = 1$ and $C_{\hat{H}}(\hat{G}) = 1$.

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

Suppose the conclusion of the lemma holds for $\hat{H}$ in place of H and $\hat{G}$ in place of G. Then, embed P' into a Galois extension K/P with an isomorphism $G(K/P) \to \hat{H}$ sending $G(K/P')$ to $\hat{G}$. The subfield of K corresponding to the kernel of the natural map $\hat{H} \to H$—sending $\hat{G}$ to G—is the desired P''. 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].* We have reduced to the case that $M(G)$ is generated by commutators. Now use the results of §1.4. There we constructed the unramified Galois cover $\Lambda : \mathcal{H}' \to \mathcal{H}$ of absolutely irreducible non-singular varieties defined over $\mathbf{Q}$. Recall: All automorphisms of this cover are defined over $\mathbf{Q}$. Also, they are of the form δ_A, $A \in \mathrm{Aut}(G)$.

Proposition 3 of [FV1] gives the following. Consider any point $\boldsymbol{p} \in \mathcal{H}$, rational over some field k, and any point $\boldsymbol{p}' \in \mathcal{H}'$ lying over $\boldsymbol{p}$. Let Δ be the group of $A \in \mathrm{Aut}(G)$ for which $\delta_A(\boldsymbol{p}')$ is conjugate to $\boldsymbol{p}'$ under $G(k'/k)$. Here $k' = k(\boldsymbol{p}')$. There is a Galois extension $L/k'(x)$, regular over k', with the following properties: L is Galois over $k(x)$, and there is an isomorphism h from $G(L/k(x))$ to Δ. Furthermore, h restricts to an isomorphism between $G(L/k'(x))$ and $\mathrm{Inn}(G)$. (Note that k'/k is Galois because all automorphisms of the Galois cover Λ are defined over $\mathbf{Q}$.)

Now assume $k = P$ is a Hilbertian PRC-field. Consider the given Galois extension P'/P with group isomorphic to C. Since $C_H(G) = 1$, conjugation by H on G induces an isomorphism from H to a subgroup $\bar{H}$ of $\mathrm{Aut}(G)$. Hence $C \cong H/G \cong \bar{H}/\ \mathrm{Inn}(G)$. The latter subgroup of $\mathrm{Out}(G)$ is isomorphic to a subgroup F of $\mathrm{Aut}(\mathcal{H}'/\mathcal{H})$, via the map $A \mapsto \delta_A$. Restriction $G_P \to G(P'/P) \cong C$ followed by these maps yields a homomorphism $\beta : G_P \to \mathrm{Aut}(\mathcal{H}'/\mathcal{H})$. Part 3 below shows the hypothesis on the $\beta(I)$ 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 $L/P(x)$, $G(L/P(x))$ is isomorphic to the group Δ. Here Δ consists of $A \in \mathrm{Aut}(G)$ with $\delta_A(\boldsymbol{p}')$ conjugate to $\boldsymbol{p}'$ under $G(P'/P)$. Since $G_P \cdot \boldsymbol{p}' = F \cdot \boldsymbol{p}'$, we get

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

Thus,, $G(L/P(x))$ is isomorphic to $\bar{H}$. This isomorphism maps the subgroup $G(L/P'(x))$ onto $\mathrm{Inn}(G)$. Finally, $G(L/P(x))$ is isomorphic to H, by the isomorphism that maps $G(L/P'(x))$ onto G.

Since P is Hilbertian, we can specialize x to get an extension P''/P which is still Galois with Galois group isomorphic to H. This isomorphism identifies $G(P''/P')$ with 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 $I(\boldsymbol{q}) = \beta(I)(\boldsymbol{q})$. We have $\beta(I) = \delta_A$ for some $A \in \mathrm{Aut}(G)$. Since $\bar{H}$ splits over $\mathrm{Inn}(G)$, we can choose A such that $A^2 = 1$. By §1.5 there exists a $\bar{\mathbf{Q}}$-point $\boldsymbol{q}' \in \mathcal{H}'$ such that $c(\boldsymbol{q}') = \delta_A(\boldsymbol{q}')$.

Note: $\sqrt{-1}$ does not lie in the real closed field fixed by I. Therefore, the restriction I_0 of I to an element of $G_{\mathbf{Q}}$ is not trivial. All involutions in $G_{\mathbf{Q}}$ are conjugate. From this there is $\alpha \in G_{\mathbf{Q}}$ such that $\alpha^{-1} I_0 \alpha$ equals the restriction of c to $\bar{\mathbf{Q}}$. Set $\boldsymbol{q} = \alpha(\boldsymbol{q}')$. Since δ_A is defined over $\mathbf{Q}$ we have

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

as desired. □

An observation of Jarden shows each embedding problem over a given field reduces to a split and a frattini embedding problem. Lemma 2 deals with split embeddings. *Restricted* frattini problems over P are solvable because the absolute Galois group of P is real-projective:

Lemma 4: *Let A be a finite group and B a normal subgroup. Suppose $\beta : G_P \to A/B$ is a surjection for which every involution $I \in G_P$ produces an element in A of order ≤ 2 whose image in A/B equals $\beta(I)$. Let P' be the fixed field of $\ker(\beta)$. Then, there exists a Galois extension P''/P containing P' with an isomorphism $G(P''/P) \to A$ sending $G(P''/P')$ to B.*

Proof: Since G_P is real-projective [HJ1] there exists $\alpha : G_P \to A$ with the composition of α and the natural map $A \to A/B$ equal to β. Then the image C_1 of α satisfies $A = BC_1$. Thus A is a homomorphic image of the outer semi-direct product $A_1 = B \times^s C_1$, under the natural map π that sends (b, c) to bc. Let P_1' be the fixed field of $\ker(\alpha)$. Lemma 2 embeds P_1' in an extension P_1''/P with group $G(P_1''/P) \cong A_1$, such that $G(P_1''/P_1')$ corresponds to B. The fixed field of $\ker(\pi)$ in P_1'' is the desired P''. □

M. Jarden suggested the proof of the following lemma. Suppose $h : E \to C$ is a group homomorphism and $x \in C$ an involution. We say x lifts to an involution of E if there is an involution $y \in E$ with $h(y) = x$.

Lemma 5: *Let $h : E \to C$ be a surjection of finite groups. USe X for the involutions of C that lift 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 lifts to an automorphism α of A. (That is, $h \circ g \circ \alpha = \gamma \circ h \circ g$.) Also, every $x \in X$ lifts to an involution in A.*

Proof: Let $\mathcal{F}_0$ be a free group with a system of generators in 1-1 correspondence with the elements of E. Take $\mathcal{F}_0 \to E$ to be the extension of the given map on the generators. Let $\mathcal{F}$ be the free product of $\mathcal{F}_0$ and groups $< y_i >$ of order 2, one for each element of X. Extend this to $\mathcal{F} \to E$ sending the y_i to involutions of E that lie over the elements of X.

Take $\mathcal{N}$ for 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. Also, the map $\mathcal{F} \to E$ induces a surjection $g : A \to E$. Every automorphism γ of C is induced from an automorphism of $\mathcal{F}$ (permuting the generators). This automorphism fixes $\mathcal{N}$. Hence, it induces an automorphism α of A: α lifts γ. Also, every $x \in X$ lifts to an involution of A. □

Theorem: *Let P be a Hilbertian PRC-field of characteristic 0. Consider a surjection $h : E \to C$ of finite groups. Let $\beta : G_P \to C$ be a surjection for which every involution I of G_P has $\beta(I)$ lift to an element of E of order ≤ 2. Then there exists a surjection $\epsilon : G_P \to E$ with $h\epsilon = \beta$.*

Proof: Let $g : A \to E$ be as in Lemma 5. It follows from Lemma 4 there is a surjection $\theta : G_P \to A$ with $\ker(h \circ g \circ \theta) = \ker(\beta)$. Thus $\gamma \circ h \circ g \circ \theta = \beta$ for some automorphism γ of C. By choice of A, we can lift γ to an automorphism α of A. Then $\epsilon \stackrel{\text{def}}{=} g \circ \alpha \circ \theta$ is a surjection $G_P \to E$ with $h\epsilon = h \circ g \circ \alpha \circ \theta = \gamma \circ h \circ g \circ \theta = \beta$. This is what we wanted. □

Rephrase the statement of the Theorem: all restricted finite embedding problems over P (or also, for G_P) are solvable. For countable P we now show this implies G_P is real-free in the sense of [HJ2]. Iwasawa's result says that solvability of *all* finite embedding problems for a profinite group of countable rank forces the group to be free. More precisely, the group is then isomorphic to the free profinite group $\hat{F}_\omega$ of countably infinite rank [FrJ, Cor. 24.2]. What we now prove generalizes this.

Consider a profinite group $\mathcal{G}$. Let $\Delta(\mathcal{G})$ be the conjugacy classes of elements of $\mathcal{G}$ of order ≤ 2. The closed set of elements of at most 2 induces a quotient topology on $\Delta(\mathcal{G})$. View $\Delta(G)$ as a *pointed topological space*: the trivial class $\{1\}$ is the distinguished element.

Proposition 1: *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 countable rank condition yields sequences of open normal subgroups of $\mathcal{G}$ and $\mathcal{H}$, respectively,

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

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

with trivial intersection.

We now construct further such sequences

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

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

with the following additional properties.

(1) There are isomorphisms $\kappa_i : \mathcal{G}/\mathcal{N}_i \to \mathcal{H}/\mathcal{M}_i$, compatible in 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. Start 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 [FrJ, Lemma 24.1]).

Choose any open normal subgroup M_i of $\mathcal{H}$ contained in $\mathcal{M}^{(i)}$ and in $\mathcal{M}_{i-1}$. Open normal subgroups $\mathcal{N}$ of $\mathcal{G}$ form a basis for the neighborhoods of 1. So, 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

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

Let $\pi_1 : F \to \bar{\mathcal{G}}$ and $\pi_2 : F \to \bar{\mathcal{H}}$ be the projections. [HJ1, Cor. 6.2] produces a finite group E and a surjection $\lambda : E \to F$ with this property. 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 $\pi_1\lambda : E \to \bar{\mathcal{G}}$ make a restricted embedding problem for $\mathcal{G}$. Namely, by (2), each involution g of $\mathcal{G}$ corresponds to an involution $h \in \mathcal{M}$ with $\kappa_{i-1}(g\mathcal{N}_{i-1}) = h\mathcal{M}_{i-1}$. Also, 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). We have a *restricted* embedding problem. Let $\chi : \mathcal{G} \to E$ be a solution of this embedding problem. Precisely, $\pi_1\lambda\chi$ is the canonical map $\mathcal{G} \to \bar{\mathcal{G}}$.

Finally let $\mathcal{N}_i$ be the kernel of the surjection $\pi_2\lambda\chi : \mathcal{G} \to \bar{\mathcal{H}}$. Let $\kappa_i : \mathcal{G}/\mathcal{N}_i \to \bar{\mathcal{H}} = \mathcal{H}/\mathcal{M}_i$ be the induced isomorphism. The construction shows (1) holds. For (2), consider an element $\delta \in \Delta$, 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 $\mathcal{G} \to \bar{\mathcal{G}}$, $g'\mathcal{N} = g\mathcal{N}$. Conclude from the choice of $\mathcal{N}$: δ and δ' have the same image in $\Delta(\mathcal{H}/\mathcal{M}_i)$. 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 $\Delta(\mathcal{H}/\mathcal{M}_i)$. Still, from the above, the latter equals the image of δ in $\Delta(\mathcal{H}/\mathcal{M}_i)$. 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 $\Delta(\mathcal{G}/\mathcal{N}_i)$. The latter means δ has trivial image in $\Delta(\mathcal{G}/\mathcal{N})$. Then, by the choice of E, it also has trivial image in $\Delta(\mathcal{H}/\mathcal{M}_i)$. Thus (2) also holds in the present case. We have shown conditions (1) and (2).

Alternates the roles of $\mathcal{G}$ and $\mathcal{H}$ in each step of the construction. Then the sequences $(\mathcal{N}_i)$ and $(\mathcal{M}_i)$ both have trivial intersection. (This is $\mathcal{M}_i \leq \mathcal{M}^{(i)}$; in the next step $\mathcal{N}_{i+1} \leq \mathcal{N}^{(i+1)}$; etc.) From (1), 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]. This considers *proper* real embedding problems (as opposed to our *restricted* embedding problems).

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

Proposition 1 says 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* a group $\mathcal{G} = \mathcal{G}(\Delta_0)$ with the above properties. This is a *real-free* group in the sense of [HJ2]. Construct it as follows [HJ2]. Take a group that is freely generated (in the category of profinite groups) by a set of involutions that is homeomorphic to Δ_0. Then 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 orderings with a positive. The spaces $Y(P)$ and $\Delta_0(G_P)$ are naturally homeomorphic. Indeed, an ordering of P goes to the class of involutions of G_P that correspond to the real closures of P with respect to the given ordering [H, p. 399].

If P is countable, its absolute Galois group has countable rank [FJ, Ex. 15.13]. Combine this with the above remarks, Proposition 1 and our main theorem to get the following. Free product means in the category of profinite groups.

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 of $\hat{F}_\omega$ with a group freely generated by a set of involutions homeomorphic to $Y(P)$.*

Corollary 2: *Let P be a finite proper extension of the field $\mathbf{Q}_{re}$ of all totally real algebraic numbers. Then the absolute Galois group G_P is real-free. If $\sqrt{-1} \in P$ then G_P is isomorphic to $\hat{F}_\omega$. Otherwise G_P is isomorphic to $\mathcal{G}(X_\omega)$. (See Remark below for X_ω.) Thus only two isomorphism types occur among the G_P.*

Proof: As in the Introduction, P is countable, Hilbertian and PRC. From Corollary1, $G_P \cong \mathcal{G}(Y(P))$. If $\sqrt{-1} \in P$ then $Y(P)$ is empty, hence $G_P \cong \hat{F}_\omega$. It remains to show that if $\sqrt{-1} \notin P$ then $Y(P) \cong X_\omega$. The next Remark does this. □

Remark—M. Jarden: *Proper real extensions of* $\mathbf{Q}_{re}$. Let P be a finite proper extension of $\mathbf{Q}_{re}$ that does not contain $\sqrt{1}$. There is a number field L with $L\mathbf{Q}_{re} = P$. Let $K = L \cap \mathbf{Q}_{re}$. Then L has a finite positive number of orderings. Let L_1 be a finite extension of L contained in P, and let $K_1 = L_1 \cap \mathbf{Q}_{re}$. 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, pairs of orderings of L and of K_1 which coincide on K have unique extensions to L_1 [Ja; p. 241].

The space of orderings $X(P)$ of P is the projective limit of the space of orderings of all L_1s. Thus, X_P is isomorphic to the inverse limit of finite sets X_i with the following property. The fiber of each x_i in the map $X_{i+1} \to X_i$ contains at least two elements. Therefore, X_P satisfies property (f) of [HJ3, Lemma 1.2]. This characterizes

$$X_\omega \cong \{\pm 1\}^{\mathbf{N}}.$$

Conclude that X_P is homeomorphic to X_ω. □

Bibliography

[Ax] J. Ax, The elementary theory of finite fields, *Annals of Math.* **88** (1968), 239–271.

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

[FrJ] M. Fried and M. Jarden, Field Arithmetic, *Springer–Ergebnisse* **11** (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 Math* **135** (1992), 1–13.

[H] D. Haran, Closed subgroups of $G(\mathbf{Q})$ with involutions, *J. 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 R(t), *J. Pure and Appl. Math.* **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, *Springer, New York-Heidelberg-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, Springer Lect. Notes* **872** (1981).

[Se1] J.-P. Serre, Cohomologie Galoisienne, *Lect. Notes in Math.* **5**, Springer-Verlag 1964.

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

[Ws] R. Weissauer, Der Hilbertsche Irreduzibilitätssatz, *J. für die reine und angew. Math.* **334** (1982), 203–220.

Mike Fried
Department of Mathematics
UC Irvine
Irvine, California 92717

Helmut Völklein
Department of Mathematics
University of Florida
Gainesville, Fl 32611