Annals of Math. 135 (1992), 469–481

THE EMBEDDING PROBLEM OVER A HILBERTIAN PAC-FIELD

Michael D. Fried, UC Irvine*

*Helmut Völklein***, U of Florida and Universität Erlangen*

Abstract: We show that the absolute Galois group of a countable Hilbertian P(seudo)-A(lgebraically)C(losed) field of characteristic 0 is a free profinite group of countably infinite rank (Theorem A). As a consequence, $G(\bar{Q}/Q)$ is the extension of groups with a fairly simple structure (e.g., $\prod_{n=2}^{\infty} S_n$) by a countably free group. In addition, we characterize those PAC fields over which every finite group is a Galois group as those with the *RG-Hilbertian* property (Theorem B).

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 absolutely irreducible variety defined over P has a P-rational point. We use the methods of [FrVo]—to which this paper is a sequel—to prove a long-standing conjecture on *Hilbertian PAC-fields P*: Every finite embedding problem over P is solvable (Theorem A). For countable P this, combined with a result of Iwasawa, implies that the absolute Galois group of P is ω-free; that is, $G(\bar{P}/P)$ is a free profinite group of countably infinite rank, denoted $\hat{F}_\omega$.

By a result of [FrJ; 2], every countable Hilbertian field k has a Galois extension P/k with P Hilbertian and PAC, and $G(P/k) \cong \prod_{n=2}^{\infty} S_n$ (where S_n is the symmetric group of degree n). From the above, $G(\bar{k}/P) = G(\bar{P}/P) \cong \hat{F}_\omega$, and we get the exact sequence

$$1 \to \hat{F}_\omega \to G(\bar{k}/k) \to \prod_{n=2}^{\infty} S_n \to 1.$$

*Supported by NSA grant MDA 904-91-H-0057. and BSF grant #87-00038

**Supported by NSA grant MDA 904-89-H-2028

This holds in particular for k the rational field Q (or any algebraic number field). In this case it can be seen as a counterpart to Shafarevich's conjecture, which says that the abelian closure of k has an ω-free absolute Galois group: This would imply that $G(\bar{k}/k)$ is the extension of an abelian group by $\hat{F}_\omega$.

Now suppose that the countable Hilbertian field k has in addition projective absolute Galois group. (This holds, for example, for the abelian closure of a number field.) Then $G(\bar{k}/k)$ is the semi-direct product of an ω-free normal subgroup and a subgroup isomorphic to the *universal frattini cover* of the group $\prod_{n=2}^{\infty} S_n$ (Corollary 2).

In [FrVo] it was proved that each PAC-field P of characteristic 0 has the following property: Every finite group is the Galois group of a regular extension $L/P(x)$, where x is transcendental over P, and "regular" means —following common abuse—that P is algebraically closed in L. In order to conclude that each finite group is a Galois group over P, it suffices to know that Hilbert's irreducibility theorem holds for regular Galois extensions of $P(x)$. This led to the concept of *RG-Hilbertian*: We define a field P to be RG-Hilbertian if Hilbert's irreducibility theorem holds for regular Galois extensions of $P(x)$. We prove that a PAC-field P of characteristic 0 is RG-Hilbertian if and only if every finite group is a Galois group over P (Theorem B)—a parallel to our Theorem A, which says that a PAC-field P of characteristic 0 is Hilbertian if and only if all finite embedding problems over P are solvable. By example we demonstrate that the RG-Hilbertian property is actually weaker than the full Hilbertian property: the field P can be chosen such that every finite group is a Galois group over P, but not every finite embedding problem over P is solvable.

The main theme of the paper [FrVo] is to show that for a fixed finite group G with trivial center, G is the Galois group of a regular extension of $k(x)$, for some field k, if and only if there exist k-rational points on certain algebraic varieties. Here we use an extension of this, namely that also the solvability of certain embedding problems over k is implied by the existence of k-rational points on certain varieties.

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

Keywords: Embedding problems; Galois groups; PAC-fields; Hilbertian fields; ω-free profinite groups; $G(\bar{Q}/Q)$ as an extension.

Comments on PAC fields: PAC-fields first appeared in [Ax]. They have been studied since then by many authors (cf. [FrJ]). PAC fields have projective absolute Galois group—a result of Ax [FrJ; Theorem 10.17]. Conversely, if H is a projective profinite group, then there exists a PAC field P such that H is the absolute Galois group of P—an observation of Lubotzky and van den Dries [LD]. New examples of Hilbertian PAC-fields (besides those constructed in [FrJ,2]) have recently been found by F. Pop. For example, one obtains such a field when adjoining $\sqrt{-1}$ to the field Q_{re} of all totally real algebraic numbers. Then our Theorem A implies:

$$G(\bar{Q}/\ Q_{re}(\sqrt{-1})) \;\cong\; \hat{F}_\omega$$

On the other hand, the abelian closure of any number field has projective absolute Galois group, and it is Hilbertian [FrJ; Theorem 15.6]. But Frey noted that such a field isn't PAC ([Fy] or [FrJ; Corollary 10.15]). Shafarevich conjectured that the abelian closure of a number field has an ω-free absolute Galois group. We know of no counterexample to the following:

Conjecture: *If the absolute Galois group of a countable Hilbertian field is projective, then it is already ω-free.*

Our proof of the corresponding result for PAC-fields would also prove this conjecture if one could show that each finite group G satisfying the hypothesis of Lemma 2 has this property: One of the infinitely many absolutely irreducible Q-varieties associated to G in [FrVo, Prop. 1] has a nonempty Q-subvariety that is unirational over $\bar{Q}$ (and therefore has a point over each field with projective absolute Galois group).

We remark that the following consequence of the above conjecture holds [FrJ; Thm. 24.50]: If k is countable Hilbertian with projective absolute Galois group, then $G(k_{\text{sol}}/k)$ is the free pro-solvable group of countably infinite rank, where k_{sol} denotes the solvable closure of k. (Originally proved by Iwasawa [Iw] for k the abelian closure of a number field.)

Notations: As above, all occurring fields are assumed to have characteristic 0. The algebraic closure of a field k is denoted by $\bar{k}$. The absolute Galois group $G(\bar{k}/k)$ of k is denoted by G_k. In expressions like $k(x)$ or $P(x)$ always x denotes an indeterminate, transcendental over the fields k and P. 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., $C_B(A)$). Finally, $\text{Aut}(A)$ (resp., $\text{Inn}(A)$) is the automorphism group of A (resp., the group of inner automorphisms of A). Other notations as introduced above.

1. THE EMBEDDING PROBLEM OVER A HILBERTIAN PAC- FIELD

We are going to show that all finite embedding problems over a Hilbertian PAC-field P are solvable (Theorem A). Our first lemma is a geometric form of the "field crossing argument" from [FrJ; §23.1]; the same idea occurs also in [Se, 2.1].

Lemma 1: *Let $\mathcal{H}' \to \mathcal{H}$ be an unramified Galois cover of absolutely irreducible varieties defined over a PAC-field P of characteristic 0. Assume all automorphisms of the cover are defined over P. If P'/P is any Galois extension (inside a fixed algebraic closure of P) with Galois group isomorphic to a subgroup F of* $\mathrm{Aut}(\mathcal{H}'/\mathcal{H})$*, 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: $P(\boldsymbol{p}') = P'$, and the G_P-orbit of $\boldsymbol{p}'$ coincides with the F-orbit of $\boldsymbol{p}'$.*

Proof: By hypothesis there is a homomorphism $\beta : G_P \to \mathrm{Aut}(\mathcal{H}'/\mathcal{H})$ with kernel $G(\bar{P}/P')$ and with image F. Since G_P acts trivially on $\mathrm{Aut}(\mathcal{H}'/\mathcal{H})$, we can view β as a 1-cocycle of G_P with values in $\mathrm{Aut}(\mathcal{H}')$. By Weil's cocycle criterion [W], such a cocycle corresponds to a twisted form of $\mathcal{H}'$ over P. We identify the $\bar{P}$-points of the twisted form 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 we denote the old action of $g \in G_P$ by $\boldsymbol{p}' \mapsto g\boldsymbol{p}'$, then the new action of g sends $\boldsymbol{p}'$ to $g\beta(g)\boldsymbol{p}'$.

As P is PAC, there is a point $\boldsymbol{p}' \in \mathcal{H}'$ that is rational over P with respect to the twisted form. This means that $\beta(g)\boldsymbol{p}' = g^{-1}\boldsymbol{p}'$ for each $g \in G_P$. Thus $\ker(\beta)$ is the stabilizer of $\boldsymbol{p}'$ in G_P. Hence $P(\boldsymbol{p}') = P'$. Furthermore, the G_P-orbit of $\boldsymbol{p}'$ equals the F-orbit of $\boldsymbol{p}'$. ▫

In Lemma 2 and 3 we assume P is a Hilbertian PAC-field (of characteristic 0). Lemma 2 invokes the main results of [FrVo]; this is the heart of the proof of Theorem A. The hypothesis on the Schur multiplier comes in because our application of [FrVo] is based on the Conway-Parker theorem (cf. [FrVo, §2.2]) which requires this hypothesis.

Lemma 2: *Let H be a finite group and G a normal subgroup of H, such that $C_H(G) = \{1\}$. Assume the Schur multiplier of G is trivial. Then each Galois extension P'/P with Galois group isomorphic to H/G can be embedded in a Galois extension P''/P for which there is an isomorphism $G(P''/P) \to H$ sending $G(P''/P')$ to G.*

Proof: By [FrVo, Proposition 3], under the given hypotheses on G there exists an unramified Galois cover $\mathcal{H}' \to \mathcal{H}$ of absolutely irreducible varieties defined over Q, and an identification of the automorphism group $\mathrm{Aut}(\mathcal{H}'/\mathcal{H})$ of this cover with the group $\mathrm{Out}(G) = \mathrm{Aut}(G)/\,\mathrm{Inn}(G)$, such that the following hold. First: all automorphisms of the cover $\mathcal{H}' \to \mathcal{H}$ are defined over Q. Furthermore, 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 regular extension $L/k'(x)$, where $k' = k(\boldsymbol{p}')$, with the following properties: L is Galois over $k(x)$, and the group $G(L/k(x))$ is isomorphic to the group of all $g \in \mathrm{Aut}(G)$ for which the image of g in $\mathrm{Out}(G) = \mathrm{Aut}(\mathcal{H}'/\mathcal{H})$ maps $\boldsymbol{p}'$ to a $G(k'/k)$-conjugate of $\boldsymbol{p}'$. Under this isomorphism, the subgroup $G(L/k'(x))$ is mapped onto $\mathrm{Inn}(G)$.

Now assume $k = P$ is a Hilbertian PAC-field, and consider the given Galois extension P'/P with $G(P'/P) \cong H/G$. Since $C_H(G) = \{1\}$, the conjugation action of H on G induces an isomorphism from H to a subgroup $\bar{H}$ of $\mathrm{Aut}(G)$. Hence $G(P'/P) \cong H/G \cong \bar{H}/\,\mathrm{Inn}(G)$, and $F \overset{\mathrm{def}}{=} \bar{H}/\,\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Out}(G)$= $\mathrm{Aut}(\mathcal{H}'/\mathcal{H})$. Thus by Lemma 1 we may choose $\boldsymbol{p}$ and $\boldsymbol{p}'$ so that $P(\boldsymbol{p}') = P'$, and the $G(P'/P)$-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 of all $g \in \mathrm{Aut}(G)$ for which the image of g in $\mathrm{Out}(G)$ lies in F. But this group is just $\bar{H}$. Thus $G(L/P(x))$ is isomorphic to $\bar{H}$, under an isomorphism that identifies $G(L/P'(x))$ with $\mathrm{Inn}(G)$. Hence $G(L/P(x))$ is isomorphic to H, under an isomorphism that maps $G(L/P'(x))$ to 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, and this isomorphism identifies $G(P''/P')$ with G (cf. [FrJ, Lemma 12.12]).

□

Now we are ready to tackle the general embedding problem over P. The projectivity of G_P allows us to reduce to the case of split embedding problems, and these are reduced group-theoretically to the special case of Lemma 2. Only then does the PAC-assumption on P come into play.

Lemma 3: *Let A be any finite group, and B a normal subgroup. Then each Galois extension P'/P with Galois group isomorphic to A/B can be embedded in a Galois extension P''/P for which there is an isomorphism $G(P''/P) \to A$ sending $G(P''/P')$ to B.*

Proof: By induction on the order of B we may assume that B is a minimal normal subgroup of A. Thus $B \cong S^m$, the direct product of m copies of a simple group S. The remainder of the proof falls into two parts. The first observes that we may assume that A splits over B (a version of "Jarden's Lemma" from [Ma, p. 231]).

Part 1: *Application of the projectivity of G_P.* Since G_P is projective there exists $\alpha : G_P \to A$ such that the composition of α with the natural map from A to A/B has kernel $G_{P'}$ (see [FrJ, Th. 10.17]). This composition is surjective, so the image C_1 of α satisfies $A = BC_1$. Then 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. Suppose that the lemma holds with A_1 in place of A and for the fixed field P_1' of $\ker(\alpha)$ in place of P' (but for the same B). Then we may embed P_1' in an extension P_1'' 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''. This shows that it suffices to consider split extensions with kernel B.

Part 2: *Reduction to the special case of Lemma 2.* From now on assume $A = B \times^s C$, for some C. Every finite split embedding problem with abelian kernel over a Hilbertian field is solvable ([Ma; Folg. 1, p. 231] or [FrJ; Thm. 24.50]). Thus we may further assume that S is non-abelian (simple). Then $B = S^m$ is perfect, and so it has a *universal* central extension $\tilde{B}$. Furthermore, $\tilde{B}$ has trivial Schur multiplier (see [Ka; p. 152–153]). By the universal property of the universal central extension, the action of C on B lifts uniquely to an action of C on $\tilde{B}$. Form accordingly the semi-direct product $\hat{A} = \tilde{B} \times^s C$.

Let T be a non-abelian finite simple group with trivial Schur multiplier (e.g., $T = \mathrm{SL}_2(8)$ [Hu, Satz 25.7]). Consider the regular wreath product H of $\hat{A}$ with T (e.g., [Hu, Def. 15.6]). Thus $H = T^j \times^s \hat{A}$, with $j = |\hat{A}|$, and $\hat{A}$ acts on T^j by permuting the factors in its regular permutation representation. Then $H = (T^j \times^s \tilde{B}) \times^s C = G \times^s C$, with $G = T^j \times^s \tilde{B}$. Clearly, $C_H(T^j) = \{1\}$, hence also $C_H(G) = \{1\}$.

Since T and $\tilde{B}$ are perfect groups with trivial Schur multiplier, every central extension of these groups splits. From this one concludes easily that also every central extension of $G = T^j \times^s \tilde{B}$ splits. Thus also G has trivial Schur multiplier.

We have now shown that G and H satisfy the hypotheses of Lemma 2. It follows that the given Galois extension P'/P with group isomorphic to $A/B \cong H/G$ can be embedded in an extension K/P with $G(K/P) \cong H$, such that $G(K/P')$ corresponds to G. Then the fixed field in K of the kernel of the natural map from H onto A (which sends G onto B) is the desired P''. ◻

Lemma 4: *For every surjection $h : E \to C$ of finite groups there exists a surjection $g : A \to E$ of finite groups such that every automorphism γ of C lifts to an automorphism α of A: $h \circ g \circ \alpha = \gamma \circ h \circ g$.*

Proof: Let H be the semi-direct product of C with its automorphism group $\mathrm{Aut}(C)$. Choose a surjection $\mathcal{F} \to H$ with $\mathcal{F}$ a free group (of finite rank), and let $\mathcal{F}_0$ be the inverse image of C in $\mathcal{F}$. Then $\mathcal{F}_0$ is again a free group, of rank greater or equal to that of $\mathcal{F}$ (by Schreier's subgroup formula; e.g. [FrJ; Prop. 15.25]). Thus by choosing $\mathcal{F}$ of suitably large rank we can assure that the map $\mathcal{F}_0 \to C$ can be factored as $h \circ f$ for some surjection $f : \mathcal{F}_0 \to E$. Let $\mathcal{R}_0$ be the intersection of all $\mathcal{F}$-conjugates of the kernel of f.

Every automorphism γ of C is induced from an inner automorphism of H, hence from an inner automorphism of $\mathcal{F}$, and thus from an inner automorphism of the finite group $\mathcal{F}/\mathcal{R}_0$. This inner automorphism restricts to an automorphism of $A = \mathcal{F}_0/\mathcal{R}_0$ that still induces γ. By construction, the natural map $A \to C$ factors as $h \circ g$ for some surjection $g : A \to E$. ◻

One says that all finite embedding problems over a field P are solvable if for every surjection $h : E \to C$ of finite groups and for every surjection $\lambda : G_P \to C$ there exists a surjection $\epsilon : G_P \to E$ with $h \circ \epsilon = \lambda$. Recall that a profinite group is called ω-free if it is isomorphic to the free profinite group $\hat{F}_\omega$ of countably infinite rank [FrJ, §15.5].

Theorem A: *A PAC-field P of characteristic 0 is Hilbertian if and only if all finite embedding problems over P are solvable. In particular, a countable PAC-field of characteristic 0 is Hilbertian if and only if its absolute Galois group is ω-free.*

Proof: By a result of Iwasawa [Iw, p. 567] (see [FrJ; Cor. 24.2 and Ex. 15.13(b)]), it suffices to prove the first assertion. The "if" part is a result of Roquette [FrJ; Cor. 24.38]; we give a new proof in Lemma 5 below, using the methods of this paper.

Now assume P is Hilbertian. We have to show that all finite embedding problems over P are solvable. So suppose we have a surjection $h : E \to C$ of finite groups and a surjection $\lambda : G_P \to C$. Let $g : A \to E$ be as in Lemma 4. It follows from Lemma 3 that there is a surjection $\theta : G_P \to A$ with $\ker(h \circ g \circ \theta) = \ker(\lambda)$. Thus $\gamma \circ h \circ g \circ \theta = \lambda$ for some automorphism γ of C. By choice of A, we can lift γ to an automorphism α of A. Then $\epsilon \overset{\text{def}}{=} g \circ \alpha \circ \theta$ is a surjection $G_P \to E$ with $h\epsilon = h \circ g \circ \alpha \circ \theta = \gamma \circ h \circ g \circ \theta = \lambda$, as desired. ▫

By a result of [FrJ, 2] (c.f. [FrJ; Th. 16.46]), every countable Hilbertian field k has a Galois extension P/k with P Hilbertian and PAC, and $G(P/k) \cong \prod_{i=1}^{\infty} S_{n_i}$. In the above references, there are certain special conditions on the sequence (n_i), but the construction can easily be modified to yield $n_i = i$. For the convenience of the reader, we sketch the argument in Remark 1 below. From the Theorem we get $G_P \cong \hat{F}_\omega$.

Corollary 1: *Suppose k is a countable Hilbertian field of characteristic 0. Then there is an exact sequence*

$$1 \to \hat{F}_\omega \to G_k \to \prod_{n=2}^{\infty} S_n \to 1$$

The field P with $G(P/k) \cong \prod_{n=2}^{\infty} S_n$ has the nice property that it is a rather small extension of k with ω-free absolute Galois group G_P. Its construction, however, is not canonical (see Remark 1 below). In particular, G_P is not necessarily a characteristic subgroup of G_k. To have a more canonical example, consider the composite of *all* S_n- extensions of k, for all n. This yields an analog to the consideration of Q_{ab} (the composite of all abelian extensions of Q) in Shafarevich's conjecture (Introduction). Actually, not much is changed if one excludes any finite number of values of n in the above. For simplicity, we consider the composite K of all S_n- extensions of k with $n \geq 5$. Remark 1 shows that K is PAC. In the next paragraph we show that K is also Hilbertian. Therefore, from Theorem A, G_K is ω-free.

By definition of K, the group $\Gamma = G(K/k)$ embeds as a subgroup of the product of (countably many) symmetric groups S_{n_i}, and projection from Γ to any one of the factors is surjective (i.e., Γ is a subdirect product of the S_{n_i}). Thus the closure Γ' of the commutator subgroup of Γ is a subdirect product of the alternating groups A_{n_i}. As $n_i \geq 5$ these groups A_{n_i} are simple. Hence $\Gamma' \cong \prod A_{m_j}$ for some subsequence (m_j) of (n_i) (see [M; Lemma 1.3]; in fact Γ' is the product of countably many copies of $\prod_{n=5}^{\infty} A_n$). The fixed field of Γ' in K is Hilbertian since it is an abelian extension of the Hilbertian field k [FrJ; Thm. 15.6]. Thus K is Hilbertian by Weissauer's theorem (see Remark 2 below) because Γ' has non-trivial finite normal subgroups.

Question: Is the composite of all A_n-extensions of k also PAC?

Remark 1: *Construction of Hilbertian PAC-fields, after [FrJ, 2].* Let k be countable and Hilbertian. An algebraic extension P of k is PAC if every absolutely irreducible projective curve defined over k has infinitely many P-rational points [FrJ; Th. 10.4]. By a result of Lefschetz (see [FrJ, 2]) one can restrict to plane curves having only singularities of multiplicity 2. There are only countably many pairs (C, M) where C is an absolutely irreducible projective plane curve defined over k that has only singularities of multiplicity 2, and M is a finite set of $\bar{k}$-points of C. Enumerate these pairs as $(C_1, M_1), (C_2, M_2), (C_3, M_3), \ldots$. We are going to construct a Galois extension P of k such that each C_i has a P-rational point not in M_i. Then C_i has infinitely many P-rational points, and P is PAC by the above.

For each C_i there exists a point O in the plane such that projection from O to a suitable line yields a cover $\varphi_i : C_i \to \mathcal{P}^1$ (where $\mathcal{P}^1$ is the projective line) with the following properties: φ_i is defined over k, and the Galois closure of the corresponding function field extension $k(C_i)/k(x)$ has Galois group S_{n_i}, where n_i is the degree of the plane curve C_i [FrJ, 2]. Since k is Hilbertian, there exist infinitely many points $c \in C_i$ such that the Galois closure of the extension $k(c)/k$ also has group S_{n_i}; additionally, one can require that this Galois closure is linearly disjoint from any given finite extension of k (see e.g., [Se, Prop. 4.10]).

Now we define recursively a sequence (k_i) of linearly disjoint Galois extensions of k and a strictly increasing sequence (m_i) of integers with $G(k_i/k) \cong S_{m_i}$, such that C_i has a k_i- rational point not in M_i. Set $k_0 = k,\ m_0 = 1$. To construct k_i and m_i for $i \geq 1$ choose an integer n such that $m_i \stackrel{\text{def}}{=} nn_i > m_{i-1}$ (where again n_i is the degree of C_i). A "sufficiently general" substitution of degree n (with coefficients from k) in the equation defining C_i yields a curve $\bar{C}_i$ of degree $m_i = nn_i$ that is again among the curves $C_1, C_2, \ldots$. By the preceding paragraph, there exists $c \in \bar{C}_i$ such that the natural map $\bar{C}_i \to C_i$ is defined at c and does not map c into M_i, the Galois closure k_i of the extension $k(c)/k$ has group S_{m_i} and k_i is linearly disjoint from the composite $k_0 \cdots k_{i-1}$. This concludes the construction of the above sequence (k_i). Finally, using [FrJ; Lemma 15.8] one can "fill in" more fields during this inductive construction to get a sequence (K_j) with $k_i = K_{m_i}$ and $G(K_j/k) \cong S_j$, such that for all j, the field K_j is linearly disjoint from $K_1 \cdots K_{j-1}$. Then the composite P of all K_j satisfies $G(P/k) \cong \prod_{j=2}^{\infty} S_j$. Further, P is PAC because every curve C_i has a P-rational point, and P is Hilbertian by Weissauer's theorem (see Remark 2 below) because $G(P/k)$ has non-trivial finite normal subgroups. $\square$

The above shows that the composite P_N of the fields K_j with $j \geq N$ is still PAC and Hilbertian. Since the intersection of all these fields P_N is just k, it follows that G_k is the closure of an ascending union of ω-free normal subgroups.

Now we return to the set-up of Corollary 1. Assume additionally that G_k is projective. This implies that the epimorphism $\varphi : G_k \to \prod_{n=2}^{\infty} S_n$ lifts to a homomorphism $\psi : G_k \to \mathcal{E}$, where $\mathcal{E}$ is the *universal frattini cover* of $\prod_{n=2}^{\infty} S_n$: This is the minimal projective cover of $\prod_{n=2}^{\infty} S_n$, and the map $\mathcal{E} \to \prod_{n=2}^{\infty} S_n$ has pro-nilpotent kernel $\mathcal{N}$ (see [FrJ; Lemma 20.2, Prop. 20.33]). The map ψ is surjective by the defining property of a frattini cover [FrJ; §20.6]. Further, $\ker(\psi)$ is normal in $\ker(\varphi) \cong \hat{F}_\omega$, and the quotient is isomorphic to the pro-nilpotent group $\mathcal{N}$. Hence also $\ker(\psi)$ is ω-free (by Corollary 3 below). Finally, the map ψ is a splitting extension since $\mathcal{E}$ is projective. Thus we have proved:

Corollary 2: *Suppose k is a countable Hilbertian field of characteristic 0, and G_k is projective. Then G_k is the semi-direct product of an ω-free normal subgroup and a subgroup isomorphic to the universal frattini cover of $\prod_{n=2}^{\infty} S_n$.*

We recall that according to our conjecture from the Introduction, the group G_k should itself be ω-free in the situation of Corollary 2. Furthermore, as a consequence of the (folklore) conjecture that every finite group is the Galois group of a regular extension of $Q(x)$, every finite group should be a quotient of G_k in the situation of Corollary 1.

Remark 2: *Hilbertian fields versus subgroups of $\hat{F}_\omega$.* Theorem A implies a "transfer theorem" that turns results about algebraic extensions of Hilbertian fields into results about subgroups of $\hat{F}_\omega$ (as noted by Jarden and Lubotzky [JaLu]). Namely, consider a countable Hilbertian PAC-field P (as above). Then $G_P \cong \hat{F}_\omega$ by Theorem A.

Now take a result saying that certain algebraic extensions of a Hilbertian field are again Hilbertian; e.g., Weissauer's theorem says that any non-trivial finite extension of a Galois extension of a Hilbertian field is again Hilbertian (see [Ws] for a non-standard proof and [Fr] for a standard proof). Theorem A then implies that certain analogously defined subgroups of an ω-free group are again ω-free. For example, Weissauer's theorem translates into the result that any proper closed subgroup U_1 of finite index in a normal subgroup U of $\hat{F}_\omega$ is again ω-free (a direct proof of this was given by Lubotzky-Melnikov-v. d. Dries; see [FrJ; Theorem 24.7]). Namely, the fixed field P_1 in $\bar{P}$ of U_1 is Hilbertian by Weissauer's theorem. Since every algebraic extension of a PAC-field is again PAC [FrJ; Cor. 10.7], it follows from Theorem A that $U_1 = G_{P_1}$ is ω-free.

There are several results about extensions of Hilbertian fields similar to Weissauer's (see [JaLu]). For most of them, the corresponding result about subgroups of $\hat{F}_\omega$ has been proved directly. However, this is not true for the result of Uchida [U] on pro-nilpotent extensions of Hilbertian fields, which translates into a new result:

Corollary 3: *If N is a normal subgroup of $\hat{F}_\omega$ such that $\hat{F}_\omega/N$ is pro-nilpotent, and U is a subgroup of $\hat{F}_\omega$ containing N, then U is again ω-free provided the index $[\hat{F}_\omega : U]$ is divisible by at least two distinct primes (in the sense of super-natural numbers).* □

A slightly different proof of this corollary is given in [JaLu], using [FrVo, Th. 2] instead of Theorem A.

2. THE RG-HILBERTIAN PROPERTY

The Hilbertian property can be rephrased as follows in terms of Galois extensions: A field P is Hilbertian if and only if every finite Galois extension of $P(x)$ can be specialized to a Galois extension of P with the same Galois group. In most applications (e.g., to the Inverse Galois Problem) it isn't the full Hilbertian property for P that is used, but rather a weaker version: if G is the Galois group of a *regular* extension of $P(x)$, then G is also a Galois group over P. We formalize this.

Definition: We say a field P is *R(egular)G(alois)- Hilbertian* if every regular (finite) Galois extension of $P(x)$ can be specialized to a Galois extension of P with the same Galois group.

If P is a PAC-field of characteristic 0, then every finite group is the Galois group of a regular extension of $P(x)$, by [FrVo, Theorem 2]. Thus if P is also RG-Hilbertian, then each finite group is a Galois group over P. The converse is also true:

Theorem B: *A PAC-field P of characteristic 0 is RG-Hilbertian if and only if every finite group is a Galois group over P.*

It remains to prove the "if" part of Theorem B. This is a simple application of Lemma 1. We refine the argument a little to simultaneously give a new proof of the "if" part of Theorem A (originally due to Roquette).

Lemma 5: *Let P be a PAC-field, and let $L/P(x)$ be a finite Galois extension. Assume that either:*

(A) all finite embedding problems over P are solvable; or

(B) P is algebraically closed in L and each finite group is a Galois group over P.

Then the extension $L/P(x)$ can be specialized to a Galois extension of P with the same Galois group.

Proof: There is a non-singular curve Γ defined and irreducible over P with function field L. The extension $L/P(x)$ corresponds to a cover $\varphi : \Gamma \to \mathcal{P}^1$ defined over P. We identify the group $H = G(L/P(x))$ canonically with the automorphism group of this cover. The absolutely irreducible components $\Gamma_1, \ldots, \Gamma_s$ of Γ are defined over the algebraic closure P_1 of P in L, and $G = G(L/P_1(x))$ is the subgroup of H stabilizing $\Gamma_1, \ldots, \Gamma_s$. The group H/G permutes $\Gamma_1, \ldots, \Gamma_s$ sharply transitively.

Both H and G_P act naturally on the $\bar{P}$-points of Γ. Since the automorphisms from H are defined over P, the group G_P centralizes H. The groups H/G and $G_P/G_{P_1} \cong G(P_1/P)$ act sharply transitively on $\Gamma_1, \ldots, \Gamma_s$, and they centralize each other. Thus there exists an isomorphism $\bar{\alpha} : G_P/G_{P_1} \to H/G$ such that $\bar{g}\bar{\alpha}(\bar{g})$ fixes Γ_1 for each $\bar{g} \in G_P/G_{P_1}$. This yields a surjection $\alpha : G_P \to H/G$ such that $g\alpha(g)$ fixes Γ_1 for each $g \in G_P$.

Now let $\beta : G_P \to H$ be a surjection such that β composed with the natural map $H \to H/G$ equals α. Such β exists in case (A) by the definition of an embedding problem, and it exists in case (B) because there $H = G$, and H is a quotient of G_P.

As in the proof of Lemma 1 we view β as a 1-cocycle of G_P in $\mathrm{Aut}(\Gamma)$. Hence β defines a twisted form of Γ, such that each $g \in G_P$ acts via this twisted form as $g\beta(g)$ on the $\bar{P}$-points of Γ (cf. the proof of Lemma 1). Since $g\beta(g)$ fixes Γ_1 (because of the corresponding property of α), it follows that Γ_1 is defined over P in the twisted form. By the PAC property, Γ_1 has a P-rational point c relative to the twisted form that does not lie over a branch point of φ. Now, as in Lemma 1, $\varphi(c)$ is a P-rational point of $\mathcal{P}^1$ which yields the desired specialization $P(c)/P$ of the extension $L/P(x)$ with the same Galois group H. ▫

Remark 3: By Theorems A and B, for a PAC-field P the RG-Hilbertian and Hilbertian properties are equivalent to purely group-theoretic properties of the absolute Galois group G_P: P is RG-Hilbertian if and only if each finite group is a quotient of G_P; and P is Hilbertian if and only if each finite embedding problem for G_P is solvable. ▫

We conclude with an example showing that the RG-Hilbertian property is actually weaker than the full Hilbertian property.

Example: *A PAC-field that is RG-Hilbertian but not Hilbertian.* Let $G_1, G_2, G_3, \dots$ be a listing that includes each nontrivial finite group just once (up to isomorphism), and suppose $|G_1| = 2$. The profinite group $H = \prod_{i=1}^{\infty} G_i$ has countably infinite rank [FrJ, Ex. 15.13]. Hence H is a quotient of $\hat{F}_\omega$ [FrJ, Cor. 15.20]. As in the proof of Corollary 2 it follows that the universal frattini cover $\tilde{H}$ of H is also a quotient of $\hat{F}_\omega$. Since $\tilde{H}$ is projective, it embeds as a subgroup of $\hat{F}_\omega$.

Let again be P a countable Hilbertian PAC-field. Then $\tilde{H}$ embeds into $G_P \cong \hat{F}_\omega$. Let K be the fixed field of $\tilde{H}$ in $\bar{P}$. Then K is PAC (since it is an algebraic extension of the PAC-field P) and every finite group is a Galois group over K. Hence K is RG-Hilbertian by Theorem B. We now show that K is not Hilbertian.

Let $\lambda : \tilde{H} \to H$ be the natural map. Then $\lambda^{-1}(G_1)$ is an extension of the group G_1 (of order 2) by the kernel of λ, which is pro-nilpotent [FrJ, Lemma 20.2]. Hence each surjection from $\tilde{H}$ to the symmetric group S_5 maps $\lambda^{-1}(G_1)$ to a solvable normal subgroup of S_5, which must be trivial. Thus the map $\tilde{H} \to G_1$ that is the composition of λ with projection to G_1 does *not* factor through a surjection $\tilde{H} \to S_5$. This means that not all finite embedding problems over K are solvable. Hence K is not Hilbertian (by Theorem A). □

Bibliography

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

[Fr] M. Fried, On the Sprindžuk-Weissauer approach to universal Hilbert subsets, *Israel J. Math* **51** (1985), 347–363.

[FrJ] M. Fried and M. Jarden, Field Arithmetic, *Springer–Ergebnisse der Math. und ihrer Grenz.* **11** (1986).

[FrJ, 2] M. Fried and M. Jarden, Diophantine properties of subfields of $\bar{Q}$, *Amer. J. Math.* **100** (1978), 653–666.

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

[Fy] G. Frey, Pseudo algebraically closed fields with non-archimedean real valuations, *J. of Algebra* **26** (1973), 202–207.

[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.

[JaLu] M. Jarden and A. Lubotzky, A transfer principle between the Hilbertian and the ω-free properties, *J. London Math. Soc.*, to appear.

[Ka] G. Karpilovsky, Projective representations of finite groups, *M. Dekker, New York and Basel 1985.*

[LD] A. Lubotzky and L. v. d. Dries, Subgroups of free profinite groups and large subfields of $\bar{Q}$, *Israel J. Math.* **39** (1981), 25–45.

[Ma] H. Matzat, Konstruktive Galoistheorie, *Lecture Notes in Math, Springer–Verlag* **1284** (1986).

[M] O.V. Mel'nikov, Normal subgroups of free profinite groups, *Math. USSR Izvestija* **12** (1978), 1–20.

[P F. Pop, The theory of totally Σ-adic numbers, preprint 1990.

[Se] J.-P. Serre, Topics in Galois Theory, *Research Notes in Mathematics, Jones and Barlett* **1** (1992).

[U] K. Uchida, Separably Hilbertian fields, *Kodai Math. Journal* **3** (1980), 83–95.

[W] A. Weil, The field of definition of a variety, *Amer. J. Math* **78** (1956), 509–524.

[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