ON FREE PROFINITE GROUPS OF UNCOUNTABLE RANK*

by

Moshe Jarden, Tel Aviv University

Contemporary Mathematics **186** (1995), 371–383

* This research was supported by THE ISRAEL SCIENCE FOUNDATION administered by THE ISRAEL ACADEMY OF SCIENCES AND HUMANITIES

Introduction

Let C be an algebraically closed field, consider a transcendental element t over C, and let $K = C(t)$. Douady [Dou] applies Riemann Existence theorem and a descent lemma of Grothendieck to prove that if $\mathrm{char}(C) = 0$, then $G(K)$ is the free profinite group $\hat{F}_m$, of rank $m = \mathrm{card}(C)$. In the case $\mathrm{char}(C) = p > 0$, results of Grothendieck imply that the maximal prime-to-p quotient of $G(K)$ is isomorphic to the maximal prime to p quotient of the free profinite group of $\hat{F}_m$. Since K is Hilbertian and $G(K)$ is projective each finite embedding problem over K with an abelian kernel is solvable [FrJ, Thm. 24.50]. Hence, if in addition K is countable, and we denote the compositum of all solvable extensions of K by K_{solv}, then $\mathcal{G}(K_{\mathrm{solv}}/K)$ is isomorphic to the free prosolvable group of rank $\aleph_0$. Harbater [Ha1, Cor. 1.5] proves that each finite group occurs as a Galois group over K. Finally, Harbater [Ha2] and Pop [Po2] prove that each finite embedding problem over K is solvable (we then say that both K and $G(K)$ are ω-**free**). By Iwasawa's criterion, this implies that $G(K) \cong \hat{F}_\omega$.

If m is uncountable, then the solvability of each embedding problem over K does not suffice for $G(K)$ to be free. Indeed, by Corollary 3.6, there exists a projective nonfree ω-free group G *. In order to prove that $G(K) \cong \hat{F}_m$ one can either solve each finite embedding problem m times (Lemma 2.1) or to solve each embedding problem once in a regular way (Proposition 2.3). Harbater [Ha2, Thm. 3.6] verifies the former condition and concludes that $G(K) \cong \hat{F}_m$ [Ha2, Thm. 4.4].

A theorem of Fried, Völklein [FrV] and Pop [Po1], says that if M is PAC and Hilbertian, then M is ω-free. Example 3.2 translates Example 3.1 into fields and constructs a Hilbertian PAC field M such that $G(M)$ is not free. So, we may say that the theorem is in a certain sense sharp.

One knows that if M is PAC, then $G(M)$ is projective. So, Fried and Völklein [FrV] conjecture that if M is a countable Hilbertian field with $G(M)$ projective, then M is ω-free. Thus would mean that if M is an arbitrary Hilbertian field with $G(M)$ projective, then M is ω-free (Observation 4.1).

The most prominent field to which this conjecture applies is the maximal cyclo-

* This answers a question of Harbater in a private communication.

tomic extension of $\mathbb{Q}$. This special case of the conjecture is due to Shafarevich. We pay attention to another case, namely to an algebraic extension M of $C(t)$ which is Hilbertian. In this case $G(M)$ is automatically projective. We prove that if M is Galois over $C(t)$ and Hilbertian, then M is ω-free.

ACKNOWLEDGEMENT: The author is indebted to Dan Haran, Katherine Stevenson, and to Helmut Völklein for useful comments to previous versions of this note.

1. The absolute Galois group of $\mathbb{C}(T)$

1.1 RANK OF A PROFINITE GROUP. A subset X of a profinite group G is said to **converge to** 1 if each open subgroup of X contains all but finitely many elements of X. We say that X **generates** G if G is the smallest closed subgroup of itself which contains X. A theorem of Douady [FrJ, Prop. 15.11] states that each profinite group G has a set of generators that converges to 1. The smallest cardinality of such a set is the **rank** of G. If $\mathrm{rank}(G)$ is infinite, then it is equal to the cardinality of the set of all open normal subgroups of G [FrJ, Suppl. 15.12]. In the latter case, if H is an open subgroup of G, then each open normal subgroup of H contains an open normal subgroup of G and vice versa. Hence $\mathrm{rank}(H) = \mathrm{rank}(G)$.

1.2 FREE PROFINITE GROUPS. A profinite group F is **free** if it has a subset X with the following two properties:

(1a) X converges to 1;

(1b) Every map α_0 of X into a profinite group G such that $\alpha_0(X)$ converges to 1 uniquely extends to a homomorphism (by which we also mean continuous) $\alpha\colon F \to G$.

The set X is a **basis** of F. Its cardinality is equal to $\mathrm{rank}(F)$ [FrJ, Lemma 15.18]. For each cardinal number m there exists a unique (up to an isomorphism) free profinite group of rank m [FrJ, Prop. 15.17]. We denote it by $\hat{F}_m$. For example, $\hat{F}_\omega$ is the free profinite group on countably many generators.

1.3 PROJECTIVE GROUPS. An **embedding problem** for a profinite group G is a pair

$$(\varphi\colon G \to A,\ \alpha\colon B \to A) \tag{2}$$

of epimorphisms of profinite groups. It is **finite** if B is finite. A **solution** (**weak solution**) to the embedding problem is an epimorphism (homomorphism) $\gamma\colon G \to B$ such that $\alpha \circ \gamma = \varphi$. The group G is **projective** if each finite embedding problem is weakly solvable. In this case each embedding problem is weakly solvable (Gruenberg [FrJ, Lemma 20.8]). It follows that a profinite group G is projective if and only if it is isomorphic to a closed subgroup of a free profinite group [FrJ, Cor. 20.14]. Another necessary and sufficient condition for G to be projective is that its cohomological dimension, $\mathrm{cd}(G)$, is at most 1.

1.4 ω-FREE GROUPS. We say that G has the **embedding property** if each finite embedding problem (2) is solvable, provided B is a quotient of G. If in addition, each finite group is a quotient of G, we say that G is ω**-free**. Thus G is ω-free, if every finite embedding problem for G is solvable.

1.5 THE GROUP $\hat{F}_e$. A profinite group F of rank $\le e$ (e finite) is isomorphic to $\hat{F}_e$ if and only if each finite group of rank at most e is a quotient of F [FrJ, Lemma 15.29].

1.6 IWASAWA'S CRITERION. Iwasawa [FrJ, Cor. 24.2] characterizes $\hat{F}_\omega$ as a profinite group of rank $\aleph_0$ which is ω-free. Example 3.1 below shows that this characterization is false for groups of uncountable ranks.

1.7 PRESENTATION OF A FREE PROFINITE GROUP OF ARBITRARY RANK AS AN INVERSE LIMIT OF FREE PROFINITE GROUPS OF FINITE RANK. One way to construct a free profinite group of arbitrary rank is to start with a set X. For each finite subset S of X consider the free profinite group $\hat{F}_S$ with basis S. If S' is another finite subset of X which contains S, then the map $S' \to \hat{F}_S$ which sends each $s \in S$ onto itself and each $s' \in S' \smallsetminus S$ onto 1 uniquely extends to an epimorphism $\alpha_{S'S}\colon \hat{F}_{S'} \to \hat{F}_S$. The inverse limit of the groups $\hat{F}_S$ and the maps $\alpha_{S'S}$ is isomorphic to the free profinite group $\hat{F}_X$ with basis X. Moreover, for each S, the map $\alpha_{XS}\colon \hat{F}_X \to \hat{F}_S$ is an epimorphism whose kernel is the smallest closed normal subgroup of $\hat{F}_X$ which contains $X \smallsetminus S$ [Rib, Props. 7.4 and 7.5 of Chap. 1].

Using compactness, it is possible to relax the above rigid condition on the maps $\alpha_{S'S}$. Suppose that $G = \varprojlim G_S$, where S ranges over all finite subsets of X. Assume that for each S the group G_S is isomorphic to $\hat{F}_S$, and if $S' \supseteq S$, then the associated homomorphism $\rho_{S'S}\colon G_{S'} \to G_S$ is surjective. Consider also the compact space $(G_S)^S$ of all functions from S into G_S. Let Φ_S be a closed subset of $(G_S)^S$. Suppose that each $\varphi \in \Phi_S$ satisfies $\langle \varphi(s) \mid s \in S\rangle = G_S$. Suppose also that if $S' \supseteq S$ and $\varphi' \in \Phi_{S'}$, then $\varphi = \rho_{S'S} \circ \varphi'|_S \in \Phi_S$ and $\rho_{S'S}(\varphi_{S'}(s')) = 1$ for each $s' \in S' \smallsetminus S$. Then φ (resp., φ') uniquely extends to an isomorphism $\varphi\colon \hat{F}_S \to G_S$ (resp., $\varphi'\colon \hat{F}_{S'} \to G_S$) such that $\rho_{S'S} \circ \varphi_{S'} = \varphi_S \circ \alpha_{S'S}$. It follows that $\Phi = \varprojlim \Phi_S$ is nonempty and each $\varphi \in \Phi$ gives an isomorphism of $\hat{F}_X$ onto G. In particular, $\varphi(X)$ is a basis of G and for each S we have $\rho_S \circ \varphi|_S \in \Phi_S$ (see also the proof of [Rib, Chap. 1, Prop. 8.2]).

1.8 Douady's theorem. Let C be an algebraically closed field of characteristic zero. Douady [Dou] applies the criterion of 1.7 to prove that the absolute Galois group of $K = C(t)$ is free of rank equal to the cardinality of C. Consider first a finite subset S of C of r elements. Let K_S be the maximal extension of K in which at most the points of $S \cup \{\infty\}$ are ramified. It is a Galois extension of K. Let $G_S = \mathcal{G}(K_S/K)$. The inertia group of each $s \in S$ in K_S is a procyclic group (actually isomorphic to $\hat{\mathbb{Z}}$), which is determined up to conjugacy. Let Φ_S be the set of all functions $\varphi\colon S \to G_S$ such that $\varphi(s)$ generates an inertia group of s and $\langle \varphi(s) \mid s \in S\rangle = G_S$. It is a closed subset of $(G_S)^S$ and if $S' \supseteq S$, then the restriction map res: $G_{S'} \to G_S$ maps $\Phi_{S'}$ into Φ_S as in 1.7.

Consider now an algebraically closed field C' that contains C. Let $K' = C'(t)$, K'_S, G'_S, and Φ'_S be the fields, the Galois group, and the set defined for C' as K, K_S, G_S, Φ_S are defined for C. Using transcendental descent methods or by the model completeness of the theory of algebraically closed fields, one proves that $K'_S = C'K_S$. Hence, res: $G'_S \to G_S$ is an isomorphism. Moreover, restriction maps Φ'_S onto Φ_S.

This reduces the problem of determining the groups G_S to the case $C = \mathbb{C}$. In this case one uses algebraic topology and proves for $C = \mathbb{C}$ that Φ_S is nonempty. Application of the Riemann existence theorem guarantees that each finite group of rank at most r is a quotient of G_S [Mat. p. 21]. It follows from 1.5 that $G_S \cong \hat{F}_S$.

By 1.7, the absolute Galois group $G(K)$ of K is isomorphic to $\hat{F}_C$. Moreover, there is an injective map $\varphi\colon C \to G(K)$ such that $\varphi(C)$ is a basis for $G(K)$ and for each finite subset S of C and for each $s \in S$ the restriction of $\varphi(s)$ to K_S generates an inertia group of s in K_S.

2. Alternative criterion for freeness

The application of algebraic topology and the Riemann existence theorem restrict Douady's proof to characteristic zero. In order to prove that $G(C(t))$ is free if C is an algebraically closed field of arbitrary characteristic one needs other criteria for freeness.

LEMMA 2.1 (Chatzidakis): *Let m be an infinite cardinal. A necessary and sufficient condition for a profinite group F to be isomorphic to $\hat{F}_m$ is that each finite embedding problem for F with a nontrivial kernel has exactly m solutions.*

Proof: Lemma 24.14 of [FrJ] says that the condition is necessary.

Conversely, suppose that each finite embedding problem for F with a nontrivial kernel has exactly m solutions. Hence, in order to prove that $F \cong \hat{F}_m$, it suffices to prove that $\mathrm{rank}(F) = m$ [FrJ, 24.18]. Indeed, each embedding problem $(F \to 1,\ G \to 1)$ with G finite and nontrivial has exactly m solutions. Hence, F has exactly m open normal subgroups. By [FrJ, Suppl. 15.12], $\mathrm{rank}(F) = m$. ∎

If a field C is not separably closed, then $\mathrm{cd}(G(C)) \geq 1$ [Rib, p. 208], hence $\mathrm{cd}(G(C(t))) \geq 2$ [Rib, p. 272]. In other words, $G(C(t))$ is not projective and in particular $G(C(t))$ is not free. So, in order to prove freeness for $G(C(t))$ we have to assume that C is separably closed. In general we denote the separable closure of a field K by K_s and its algebraic closure by $\tilde{K}$. Observe that $K_s(t)_s \cap \tilde{K}(t) = K_s(t)$ and $K_s(t)_s\tilde{K}(t) = \tilde{K}(t)_s$. Hence $G(K_s(t)) \cong G(\tilde{K}(t))$. So, we may assume that C is algebraically closed.

Let again $K = C(t)$. Lemma 2.1 states that in order to prove that $G(K)$ is free of rank $m = \mathrm{card}(C)$ we have to prove that each finite embedding problem for $G(K)$ with a nontrivial kernel has exactly m solutions. Since K has at most m finite algebraic extensions, it suffices to solve each such embedding problem at least m times.

Now, a finite embedding problem for $G(K)$ can be represented as an epimorphism

$$\alpha\colon B \to \mathcal{G}(L/K), \tag{1}$$

where L/K is a finite Galois extension and B is a finite group. A **solution** to this problem is a Galois extension N of K which contains L and an isomorphism $\theta\colon \mathcal{G}(N/K) \to B$ such that $\alpha \circ \theta = \mathrm{res}_L$. One way to insure that two solutions θ_1 and θ_2 with solution fields N_1 and N_2 are distinct is to construct them such that the sets of branch points of K in N_1 and N_2 do not coincide. Another way is to solve the embedding problem (1) in a **regular** way. This means, to construct a Galois extension F of $K(u)$ (with u transcendental over K) which is regular over L and an isomorphism $\theta\colon \mathcal{G}(F/K(u)) \to B$ such that $\alpha \circ \theta = \mathrm{res}_L$. Since K is a Hilbertian field, it is possible to specialize u to an element of K and to extend the specialization to a place of F into $\tilde{K} \cup \{\infty\}$ such that the residue field of F will solve the embedding problem (1). Due to the special nature of the Hilbert sets of K, we can do it in m distinct ways. This depends on the following result.

Lemma 2.2: *Let $K = C(t)$ be the field of rational functions of an arbitrary field C of cardinality m. Suppose that L' is the compositum of less than m finite separable algebraic extensions of K. Then each separable Hilbert subset of L' contains elements of K. In particular, L' is separably Hilbertian.*

Proof: Consider a separable Hilbert subset H of L'. By [FrJ, Lemma 11.12], there exists an irreducible polynomial $f \in L'[T,X]$ which is separable in X such that $H = H_{L'}(f) = \{a \in L' \| f(a,X) \text{ is irreducible in } L'[X]\}$. By assumption $L' = \bigcup_{\kappa<k} L_\kappa$, where k is a smaller cardinal than m and L_κ is a finite separable extension of K, which we may assume to contain the coefficients of f. Then $\bigcap_{\kappa<k} H_{L_\kappa}(f) \subseteq H_{L'}(f)$.

Each H_{L_κ} contains a separable Hilbert subset of K [FrJ, Cor. 11.7]. Hence, by [FrJ, Thm. 12.9], there exists a nonempty Zariski open subset U_κ of $\mathbb{A}^2$ such that

$$\{(a+bt\|(a,b) \in U_\kappa(K)\} \subseteq H_{L_\kappa}. \tag{2}$$

Since $k < m$, the intersection of all $U_\kappa(K)$ is nonempty. Combined with the preceding paragraph, this concludes the proof of the lemma.

To be on the safe side, let us prove the claim about the intersection. To this end observe that the complement C_κ of U_κ is a union of finitely many curves and points.

As such, C_κ contains only finitely many lines. As $k < m$, there exists a line Λ which is defined over K and is not contained in any of the sets C_κ. Hence $\Lambda(K) \cap C_\kappa(K)$ is a finite set for each $\kappa < k$. Since the cardinality of $\Lambda(K)$ is m, this implies that $\Lambda(K) \not\subseteq \bigcup_{\kappa<k} C_\kappa(K)$. Conclude that $\Lambda(K)$ contains points (indeed m points) that belong to each U_κ. ∎

PROPOSITION 2.3: *Let $K = C(t)$ be the field of rational functions of an arbitrary field C and let $m = \mathrm{card}(C)$. If an embedding problem (1) has a regular solution, then it has m solutions, which are linearly disjoint over L.*

In particular, if each finite embedding problem over K has a regular solution, then $G(K)$ is free of rank m.

Proof: Let $\lambda < m$ be an ordinal and suppose by infinite induction that for each $\kappa < \lambda$ we have already constructed a solution field L_κ to (1) such that the fields L_κ with $\kappa < \lambda$ are linearly disjoint over L. Denote the compositum of all these L_κ by L'. Recall that m, as a cardinal number, is the smallest ordinal with cardinality at least m. Thus, the cardinality λ is less than m.

Write the regular solution field F of (1) as $K(u,x)$ with x integral over $K[u]$. Then $\mathrm{irr}(x, K(u))$ is an irreducible Galois polynomial $f(u,X)$ and $\mathrm{irr}(x, L(u))$ is an absolutely irreducible polynomial $g(u,X)$. In particular $g(u,X)$ is irreducible over L'. Now use Lemma 2.2 to specialize u to an element a of K such that the Galois group of $f(a,X)$ over K is isomorphic to that of $f(u,X)$ over $K(u)$ and $g(a,X)$ is irreducible over L'. The splitting field of $f(a,X)$ over K is a new solution of (1), which we may take as L_λ. It is linearly disjoint from L' over L. This concludes the transfinite induction.

The second part of the Proposition follows from Lemma 2.1. ∎

Applications 2.4: Let C be an algebraically closed field of cardinality m and let $K = C(t)$. Harbater [Ha2, Thm. 3.6] solves each finite embedding problem with a nontrivial kernel m times by varying the branch points that enter in the solutions. He concludes from Lemma 2.1 that $G(K) \cong \hat{F}_m$ [Ha2, Thm. 4.4]. ∎

Remark 2.5: Recall that each open subgroup of $\hat{F}_m$ is isomorphic to $\hat{F}_m$ [FrJ, Prop. 15.27]. Hence, once one proves that $G(C(t))$ is free of rank m, then so is $G(L)$ for each finite extension L of $C(t)$. ∎

PROBLEM 2.6: *Let C be an algebraically closed field and let $K = C(t)$. Does every finite embedding problem over K have a regular solution?*

3. Nonfree ω-free groups

The next example proves that Iwasawa's criterion for $\hat{F}_\omega$ is not valid for profinite groups of uncountable rank.

EXAMPLE 3.1: *Let m be an uncountable cardinal. Then there exists a nonfree closed normal subgroup G of $\hat{F}_m$ for which each finite embedding problem is solvable.*

Proof: We recall several definitions and results of Melnikov [Me1] which hold for each infinite cardinal m. Consider a profinite group G and a finite simple group S. Denote the intersection of all open normal subgroup M of G such that $G/M \cong S$ by $M_S(G)$. Then $G/M_S(G) \cong S^I$ for some set I whose cardinality we denote by $r_G(S)$ (Melnikov denotes it by $r_S(G)$). We call r_G the **rank function** of G. Let $X(m)$ be the set of all functions f from the set of finite simple groups to the set of cardinal numbers $\leq m$ such that for each prime p the value $f(\mathbb{Z}/p\mathbb{Z})$ is either 0 or m. Melnikov proves:

(1a) The set of all rank functions of normal subgroups of $\hat{F}_m$ coincides with $X(m)$ [Me1, Thm. 3.2].

(1b) If two closed normal subgroups of $\hat{F}_m$ have the same rank function, they are isomorphic [Me1, Thm. 3.1].

(1c) A closed normal subgroup G of $\hat{F}_m$ is isomorphic to $\hat{F}_m$ if and only if $r_G(S) = m$ for each finite simple group S [Me1, Cor. 3.1].

We adjust the proof of [Me1, Prop. 3.1] to prove:

(1d) Let G be a closed normal subgroup of $\hat{F}_m$ such that $r_G(S) = \infty$ for each S. Then, each finite embedding problem ($\varphi\colon G \to A$, $\alpha\colon B \to A$) for G is solvable.

Indeed, let $C = \mathrm{Ker}(\alpha)$. By induction on the order of B we may assume that C is a minimal normal closed subgroup of B. Hence $C \cong S^k$ for some finite simple group S and a positive integer k. Extend φ to an epimorphism φ' of an open subgroup F of $\hat{F}_m$ onto A. Then F is free of rank m ([FrJ, Prop. 15.27] and §1.1). It follows that there exists an epimorphism $\psi\colon F \to B$ such that $\alpha \circ \psi = \varphi'$. Then $\psi(G)$ is a normal subgroup of B and $C\psi(G) = B$. By the minimality of C there are two possibilities. Either $C \le \psi(G)$ or $C \cap \psi(G) = 1$. In the former case $\psi(G) = B$ and $\psi|_G$ solves the embedding problem. In the latter case, $B \cong C \times \psi(G)$ and therefore $\psi(G) \cong A$. Since C is a minimal normal subgroup of B, this implies that $k = 1$. That is, $C \cong S$. So, $B = S \times A$. As $r_G(S) = \infty$, there exists a closed normal subgroup N of G such that $G/N \cong S$ and $\mathrm{Ker}(\varphi) \not\le N$. Hence $G \to G/(\mathrm{Ker}(\varphi) \cap N) \cong S \times A = B$ gives the desired solution.

Assume again that m is uncountable. To construct the desired group define $f(S) = \aleph_0$ if S is simple nonabelian and $f(\mathbb{Z}/p\mathbb{Z}) = m$ for all p. By (1a), $\hat{F}_m$ has a closed normal subgroup G such that $r_G = f$. By (1d), each finite embedding problem for G is solvable. By (1c), G is not free, as desired. ∎

Recall that a field K is **PAC** if each absolutely irreducible variety defined over K has a K-rational point. A field K is **ω-free** if $G(K)$ is ω-free, i.e., if every finite embedding problem over K is solvable. If in addition K is countable, then, by Iwasawa's criterion, $G(K) \cong \hat{F}_\omega$.

Open problem 7 of [FrJ] asks whether every PAC Hilbertian field is ω-free. Fried and Völklein [FrV, Thm. A] solve the problem in characteristic 0. Pop [Po1, Thm. 1] does it in the general case.

We translate Example 3.1 into an example of fields which shows that in some sense, the result of Fried-Völklein and Pop is sharp.

EXAMPLE 3.2: *Every field K_0 has an extension K which is perfect, PAC, and separably Hilbertian but $G(K)$ is not free.*

Proof: Choose an uncountable cardinal m. Let G be the closed normal subgroup of $\hat{F}_m$ which Example 3.1 supplies. As G is projective, [FrJ, Cor. 20.16] supplies an extension K of K_0 which is perfect, PAC and $G(K) \cong G$. In particular, K is ω-free. By a theorem of Roquette [FrJ, Cor. 24.38], K is separably Hilbertian. Finally, note that by the choice of G, the group $G(K)$ is not free. ∎

Remark 3.3: Dominating embedding problems. Let G be a profinite group. Let $\alpha\colon \hat{A} \to A$ be an epimorphism of profinite groups. We say that an embedding problem $(\hat{\varphi}\colon \hat{G} \to \hat{A},\ \hat{\pi}\colon \hat{B} \to \hat{A})$ **dominates** the embedding problem $(\varphi\colon G \to A,\ \pi\colon B \to A)$ **over** α, if $\varphi = \alpha \circ \hat{\varphi}$ and there exists an epimorphism $\beta\colon \hat{B} \to B$ such that $\pi \circ \beta = \alpha \circ \hat{\pi}$. If in this case $\hat{\gamma}$ is a solution to the former embedding problem, then $\gamma = \beta \circ \hat{\gamma}$ is a solution to the latter embedding problem.

Let $(\varphi_i\colon G \to A_i,\ \pi_i\colon B_i \to A_i)$, $i = 1, 2$ be finite embedding problems of a profinite group G. Let $\alpha\colon A_2 \to A_1$ be a homomorphism such that $\alpha \circ \varphi_2 = \varphi_1$.

Let $B = B_1 \times_{A_1} B_2$ be the fibred product of B_1 and B_2 over A_1 [FrJ, Sect. 20.2]. Denote the projection of B onto B_i by ρ_i, $i = 1, 2$. Then the embedding problem $(\varphi_2\colon G \to A_2,\ \pi_2 \circ \rho_2\colon B \to A_2)$ dominates each of the given embedding problems. ∎

LEMMA 3.4: *Every ω-free profinite group G is isomorphic to an inverse limit $G \cong \varprojlim_{i \in I} G_i$ where $G_i \cong \hat{F}_\omega$ for each $i \in I$ and* $\mathrm{card}(I) = \mathrm{rank}(G)$.

Proof: Let $\mathcal{N}$ be the collection of all closed normal subgroups N of G such that $G/N \cong \hat{F}_\omega$. We construct a subfamily $\mathcal{N}_\omega$ of $\mathcal{N}$ of cardinality $\mathrm{rank}(G)$ such that each open normal subgroup K of G contains a group N which belongs to $\mathcal{N}_\omega$. Hence, the intersection of all $N \in \mathcal{N}_\omega$ is 1. Moreover, for all $N_1, N_2 \in \mathcal{N}_\omega$ there exists $N \in \mathcal{N}_\omega$ with $N \le N_1 \cap N_2$. So, the quotients G/N with $N \in \mathcal{N}_\omega$ build an inverse system and $G \cong \varprojlim G/N$.

The construction applies two claims.

CLAIM A: *Let $K_1 \ge K2 \ge K_3 \ge \cdots$ be open normal subgroups of G. Then G has a closed normal subgroup $K_\omega \in \mathcal{N}$ which is contained in each K_i.* The proof of Claim A follows that of [Jar, Lemma 6.6]. By induction we construct a descending sequence $G \ge N_1 \ge N_2 \ge N_3 \ge \cdots$ of open normal subgroups of G such that $N_n \le K_n$, $n = 1, 2, 3, \ldots$, and for each i we order the finite embedding problems of the form $(G \to G/N_i,\ \pi\colon B \to G/N_i)$ in a sequence

(2) $$(G \to G/N_i,\ \pi_{ij}\colon B_{ij} \to G/N_i)$$

$j = 1, 2, 3, \ldots$, such that for each n and for each $i, j \le n$, embedding problem (2) has a solution which factors through G/N_{n+1}.

Indeed, suppose that N_i, B_{ij}, and π_{ij} have already been constructed for $i \le n$ and for each j. Choose by Remark 3.3 a finite embedding problem $(G \to G/N_n, : \ \pi\colon B \to G/N_n)$ which dominates (2) for each $i, j \le n$. Since G is ω-free, this problem has a solution γ. Then $N_{n+1} = \mathrm{Ker}(\gamma) \cap K_{n+1}$ satisfies the requirements of the induction.

Let $K_\omega = \bigcap_{n=1}^{\infty} N_n$. To prove that G/K_ω is ω-free, consider a finite embedding problem $(\varphi\colon G/K_\omega \to A,\ \pi\colon B \to A)$. Since the kernel of φ contains N_i/K_ω for some i, we may take the corresponding fibred product as in Remark 3.3 and assume that $A = G/N_i$ and that φ is the canonical map. Hence, in the above notation, $B = B_{ij}$ and $\pi = \pi_{ij}$ for some j. Let $n = \max\{i, j\}$. By construction, there is a solution γ to that problem which factors through G/N_{n+1} and therefore also through G/K_ω. Conclude that G/K_ω is ω-free.

Claim B: *Let K_ω and L_ω be closed normal subgroups of G such that* $\mathrm{rank}(G/K_\omega)$ *and* $\mathrm{rank}(G/L_\omega)$ *are at most* $\aleph_0$. *Then G has a closed normal subgroup $N \in \mathcal{N}$ which is contained in both K_ω and L_ω.* Indeed, there exists a descending sequence of open normals subgroup N_i whose intersection is contained in both K_ω and L_ω. By Claim A, there exists a normal subgroup $N \in \mathcal{N}$ of G which is contained in each N_i. It satisfies $N \le K_\omega \cap L_\omega$.

Part C: *Construction.* Since G is ω-free, its rank is infinite. Hence, the cardinality of the collection of all open subgroups of G is $\mathrm{rank}(G)$ [FrJ, Supplement 15.12]. For each open normal subgroup K of G choose $N \in \mathcal{N}$ contianed in K (Claim A). Denote the subcollection of $\mathcal{N}$ obtained in this way by $\mathcal{N}_0$. Then $\mathrm{card}(\mathcal{N}_0) = \mathrm{rank}(G)$.

Now use induction to construct an ascending sequence $\mathcal{N}_0 \subseteq \mathcal{N}_1 \subseteq \mathcal{N}_2 \subseteq \cdots$ of subcollections of $\mathcal{N}$, each of cardinality $\mathrm{card}(G)$, such that for each i and for all $K, L \in \mathcal{N}_i$ there exists $N \in \mathcal{N}_{i+1}$ which is contained in both K and L. Indeed, having constructed $\mathcal{N}_i$, we use Claim B to choose for each pair $(K, L) \in \mathcal{N}_i^2$ exactly one $N \in \mathcal{N}$ such that $N \le K \cap L$ and let $\mathcal{N}_{i+1}$ be the collection of all those N.

The union $\mathcal{N}_\omega = \bigcup_{i=0}^{\infty} \mathcal{N}_i$ has the desired properties. ∎

The following example has slightly different properties than Example 3.1, but serves the same goal as Example 3.1.

EXAMPLE 3.5 (Melnikov [Me2, Example]): *Let m be an uncountable cardinal. Then there exists a nonfree ω-free profinite group G for which each finite embedding problem is solvable. In particular G is projective. Moreover, no open subgroup of G is isomorphic to a closed normal subgroup of a free profinite group.*

Proof: We break the proof into several parts and start with a general (well known) statement:

PART A: *Let P be a projective group and let F be an ω-free profinite group. Then the free product $G = P * F$ is also ω-free.*

Indeed, let $(\varphi\colon G \to A,\ \alpha\colon B \to A)$ be a finite embedding problem for G. Then there exists a homomorphism $\gamma_1\colon P \to B$ such that $\alpha \circ \gamma_1 = \varphi|_P$. Also, there exists an epimorphism $\gamma_2\colon F \to B$ such that $\alpha \circ \gamma_2 = \varphi|_F$. Combine γ_1 and γ_2 to an epimorphism $\gamma\colon G \to B$. Then $\alpha \circ \gamma = \varphi$ and therefore γ is a solution of the embedding problem. Conclude that G is ω-free.

PART B: *The example.* Let P be a free pro-p group of rank m and let $F = \hat{F}_\omega$. Then $G = P * F$ has the properties stated in the example

Indeed, the proof of Lemma 3.4 works in the category of pro-p groups as it works in the category of all profinite groups. In particular we may present P as an inverse limit $P = \varprojlim P_i$ of free pro-p groups of rank $\aleph_0$. In particular, each P_i is projective. Hence, by Part A, $G_i = P_i * F$ is ω-free. Since $\mathrm{rank}(G_i) = \aleph_0$, Iwaswa's criterion 1.6 implies that $G_i \cong \hat{F}_\omega$. Now note that $G = \varprojlim G_i$.

PART C: *No open subgroup H of G is isomorphic to a closed normal subgroup of a free group.*

Let H be an open subgroup of G. Consider the double class decompositions of G: $G = \dot\bigcup_{i\in I} Px_iH$ and $G = \dot\bigcup_{j\in J} Fy_jH$. By a theorem of Binz, Neukirch, and Wenzel [BNW, p. 105] H is a free product: $H \cong \prod^*_{i\in I}(P^{x_i} \cap H) * \prod^*_{j\in J}(P^{y_j} \cap H) * E$, where E is a free profinite group of finite rank. In particular, in the notation of Example 3.1,

$r_H(\mathbb{Z}/p\mathbb{Z}) = m$ and $r_H(\mathbb{Z}/q\mathbb{Z}) = \aleph_0$ for each prime $q \neq p$. Conclude from (1d), that H is isomorphic to no closed normal subgroup of a free profinite group.

PART C: *Remark.* At the end of the Melnikov's example he asks about the existence of a nonfree inverse limit of free profinite groups of finite rank. This is however already included in the present example. Indeed, each G_i is the inverse limit of free profinite groups of finite rank. Hence, so is G. ∎

Combine Example 3.1 (or Example 3.5) with Lemma 3.4:

COROLLARY 3.6: *There exists a nonfree inverse limit* $G = \varprojlim_{i \in I} G_i$ *of free profinite groups, such that* $\mathrm{card}(I) = \mathrm{rank}(G)$.

Remark 3.7: On a proof of Pop. Pop [Po2, end of Sect. 2] considers an algebraically closed field C, lets $K = C(t)$ (in our notation), and proves that $G(K)$ is free. To that end he writes C as a union of countable algebraically closed fields C_i, lets $K_i = C_i(t)$, and states that "$G(K)$ is the inverse limit of $G(K_i)$ in a *canonical way*". He then proves that $G(K_i) \cong \hat{F}_\omega$ and concludes that $G(K)$ is free.

In light of Corollary 3.6, Pop's proof appear to be incomplete. ∎

4. On a conjecture of Fried and Völklein

Recall that the absolute Galois group of a PAC field is projective. So, in an attempt to generalize their theorem "Hilbertian, PAC, and characteristic 0 imply ω-free", Fried and Völklein [FrV, p. 270] conjecture that the absolute Galois group of each countable Hilbertian field with a projective absolute Galois group is ω-free. Since the maximal cyclotomic extension $\mathbb{Q}_{\mathrm{cycl}}$ ($= \mathbb{Q}_{\mathrm{ab}}$) of $\mathbb{Q}$ is both Hilbertian (Kuyk [FrJ, Thm. 15.6]) and with a projective absolute Galois group (a consequence of [Rib, Thm. 8.8 on page 302]), this conjecture generalizes a conjecture the Shafarevich that $G(\mathbb{Q}_{\mathrm{cycl}})$ is free. Note that $\mathbb{Q}_{\mathrm{cycl}}$ is not PAC (Frey [FrJ, Cor. 10.15]). So Shafarevich's conjecture does not follow from the theorem of Fried and Völklein. If one replaces $\mathbb{Q}$ by a function field K of one variable over a finite field of characteristic p, then K_{cycl} becomes a finite extension of $\tilde{\mathbb{F}}_p(t)$. By the theorem of Harbater and Pop $G(\tilde{\mathbb{F}}_p(t)) \cong \hat{F}_\omega$. So, $G(K_{\mathrm{cycl}})$, as an open subgroup of $\hat{F}_\omega$, is isomorphic to $\hat{F}_\omega$. In particular K_{cycl} is ω-free.

Observation 4.1: *If each countable separably Hilbertian field with a projective absolute Galois group is ω-free, then so is each arbitrary separably Hilbertian field with a projective absolute Galois group.*

Proof: To say that a polynomial with coefficients in a field K is irreducible is an elementary statement on K [FrJ, p. 77]. Hence, to say that K is Hilbertian, is a conjunction of countably many elementary statements on K.

Similarly, the solvability of each finite embedding problem over K is an elementary statement on K [FrJ, Remark on p. 315]. Hence, to say that K is ω-free is also a conjunction of countably many elementary statements on K.

Finally, an embedding problem (2) of Section 1 with $G = G(K)$ is weakly solvable if at least one of the embedding problems (φ: $G(K) \to A$, α: $B_0 \to A$) in which B_0 is a subgroup of B such that $\alpha(B_0) = A$ is solvable. So, this is also an elementary statement on K. Thus, to say that $G(K)$ is projective is equivalent to a conjunction of countably many elementary statements on K.

Suppose now that K is a separably Hilbertian field with $G(K)$ projective. By Skolem-Löwenheim's theorem [FrJ, Prop. 6.4], K has a countable elementary subfield K_0. By the first and the third paragraphs of this proof, K_0 is separably Hilbertian and $G(K_0)$ is projective. By assumption, K_0 is ω-free. It follows that K is also ω-free. ∎

We have already mentioned (Remark 2.4) that each open subgroup of a free profinite group is free. We use the technique of the proof of Observation 4.1 to prove the analog of this results for ω-free groups.

Lemma 4.2: *Let G be an ω-free profinite group. Then each open subgroup of G is ω-free and each closed normal subgroup of G has the embedding property.*

Proof: Let (φ: $H \to A$, α: $B \to A$) be a finite embedding problem for H. As in the proof of Lemma 3.3, find a closed normal subgroup N of G, which is contained in $\mathrm{Ker}(\varphi)$ such that $G/N \cong \hat{F}_\omega$. Since H/N is open in G/N, it is isomorphic to $\hat{F}_\omega$. As φ factors through H/N, the embedding problem is solvable.

In particular, each open normal subgroup of G has the embedding property. Hence, by [FrJ, Lemma 24.3], so does each closed normal subgroup of G. ∎

As mentioned in Section 2, if C is algebraically closed, then each closed subgroup of $G(C(t))$ is projective. We may therefore rephrase a special case of the conjecture of Fried and Völklein:

CONJECTURE 4.3: *Let C be an algebraically closed field and let M be an algebraic extension of $C(t)$ which is separably Hilbertian. Then M is ω-free.*

Here is a special case in which Conjecture 4.3 holds.

PROPOSITION 4.4: *Let C be an algebraically closed field and let N be a Galois extension of $K = C(t)$ which is separably Hilbertian. Then N is ω-free.*

Proof: By Douady's theorem in characteristic 0 and by the theorem of Harbater-Pop, $G(K)$ is ω-free. Hence, by Lemma 4.2, $G(N)$ has the embedding property.

Let u be a transcendental element over K. and let G be a finite group. Then $C(u)$ has a Galois extension L with $\mathcal{G}(L/C(u)) \cong G$. Observe that L is linearly disjoint from N over C. Hence, also $\mathcal{G}(NL/N(u)) \cong G$. Since N is Hilbertian, G occurs as a Galois group over N. Combine this with the preceding paragraph to conclude that $G(N)$ is ω-free. ∎

Remark 4.5: GA realization. Let S be a finite group with a trivial center and let K be a field. We say that S is **GA** over K if the following condition holds:

(GA) $K(t)$ has a subfield E and an extension F such that F/K is regular, F/E is Galois and there exists an isomorphism of $\mathcal{G}(F/E)$ onto $\mathrm{Aut}(S)$ which maps $\mathcal{G}(F/K(t))$ onto $\mathrm{Inn}(S) \cong S$.

It follows that S is also GA over every extension of K.

Matzat [Mat, Satz 2 and Bemerkung 5] proves that if K is Hilbertian, $\mathrm{char}(K) = 0$ (the proof works for $\mathrm{char}(K) \neq 2$), $G(K)$ is projective, and every finite nonabelian simple group is GA over K, then K is ω-free. In an attempt to solve Shafarevich's conjecture, he then gives a long list of finite simple groups which are GA over $\mathbb{Q}_{\mathrm{cycl}}$. For example all A_n's with $n \geq 5$ and all sporadic groups are on that list.

Let now C be an algebraically closed field* of $\mathrm{char}(K) \neq 2$ and let M be a separable algebraic extension of $K = C(t)$ which is Hilbertian. If $\mathrm{char}(C) = 0$, then all

* The author is indebted to Helmut Völklein for the following argument.

groups on Matzat's list are GA over M. In general, consider the group $\mathrm{Out}(S)$ of outer automorphisms and suppose that

(2) $\mathrm{Out}(S)$ is a subgroup of $\mathrm{PGL}(2, C) = \mathrm{Aut}(C(t)/C)$.

Let E be the fixed field of $\mathrm{Out}(S)$ in $C(t)$. By Luroth's theorem, $E = C(u)$ for some transcendental element u over C. Since $G(C(u))$ is free, we can solve the embedding problem $1 \to S \to \mathrm{Aut}(S) \to \mathcal{G}(C(t)/C(u)) \to 1$ over $C(u)$. Hence S is GA over C. For example, condition (2) holds if $\mathrm{Out}(S) \cong \mathbb{Z}/n\mathbb{Z}$ with n relatively prime to $\mathrm{char}(C)$. Note that $\mathrm{Out}(S)$ is cyclic for all alternating and sporadic simple groups. Moreover, 6 families of the 16 families of simple groups of Lie type satisfy the condition '$\mathrm{Out}(S)$ is cyclic'. Some more satisfy the weaker condition (2). However, there are finite simple group which do not satisfy (2). So, it is not clear that this method will lead to the solution of Conjecture 4.3. ∎

References

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

[Dou] A. Douady, *Détermination d'un groupe de Galois,* C. R. Acad. Sc. Paris **258** (1964), 5305–5308.

[FrJ] M.D. Fried and M. Jarden, *Field Arithmetic,* Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 1986.

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

[Ha1] D. Harbater, *Mock covers and Galois extensions,* Journal of Algebra **91** (1984), 281–293.

[Ha2] D. Harbater, *Fundamental groups and embedding problems in characteristic p,* preprint, Philadelphiya, 1993 (See also these proceedings).

[Jar] M. Jarden, *Algebraic realization of p-adically projective groups,* Compositio Mathematica **79** (1991), 21–62.

[Mat] B. H. Matzat, *Zum Einbettungsproblem der algebraischen Zahlentheorie mit nicht abelschem Kern,* Inventiones mathematicae **80** (1985), 365–374.

[Me1] O. V. Melnikov, *Normal subgroups of free profinite groups,* Math. USSR Izvestija **12** (1978), 1–20.

[Me2] O. V. Melnikov, *Projective limits of free profinite grous (russian),* Doklady Akademii Nauk BSSR **26** (1980), 968–970.

[Po1] F. Pop, *Hilbertian fields with a universal local global principle,* preprint, Heidelberg, 1993.

[Po2] F. Pop, *The geometric case of a conjecture of Shafarevich, — $G_{\tilde{\kappa}(t)}$ is profinite free —*, preprint, Heidelberg, 1993.

[Rib] L. Ribes, *Introduction to Profinite Groups and Galois Cohomology,* Queen's papers in Pure and Applied Mathematics **24**, Queen's University, Kingston, 1970.