ISRAEL JOURNAL OF MATHEMATICS, Vol. 39, Nos. 1-2, 1981

SUBGROUPS OF FREE PROFINITE GROUPS AND LARGE SUBFIELDS OF $\tilde{\mathbf{Q}}$

BY

A. LUBOTZKY[†] AND L. VAN DEN DRIES

ABSTRACT

We prove that many subgroups of free profinite groups are free, and use this to give new examples of pseudo-algebraically closed subfields of $\tilde{\mathbf{Q}}$ satisfying Hilbert's Irreducibility Theorem, and to solve problems posed by M. Jarden and A. Macintyre. We also find a subfield of $\tilde{\mathbf{Q}}$ which does not satisfy Hilbert's Irreducibility Theorem, but all of whose proper finite extensions do.

Introduction

A classical theorem of Nielsen and Schreier states that subgroups of free groups are free. This can for instance be proved by the method of coset representatives of combinatorial group theory. Using Galois cohomology, Tate proved the pro-p analogue of the Nielsen–Schreier theorem: closed subgroups of free pro-p groups are free pro-p groups, see [5], [8], [19]. Neither combinatorial methods nor Galois cohomology seem to give similar results for closed subgroups of free profinite groups. (Such groups occur frequently as Galois groups, see section 4.) In fact, some restrictions on the closed subgroups are needed to obtain an analogue, even for *normal* closed subgroups: the kernel of the natural map of a free profinite group F onto its maximal pro-solvable quotient is not a free profinite group if F is of rank >1, see also the introduction of §3. (The rank 1 or procyclic case is not interesting for the questions we consider.)

Our main result (3.1) gives a very general sufficient condition for a closed *normal* subgroup N of $\hat{F}_e$, the free profinite group on e generators, $e \in \mathbf{N}$, to be free as a profinite group. This condition (which is not necessary as (3.15) shows) states that $\hat{F}_e/N$ is *not e-freely indexed.* For instance, if $\mathrm{rk}(\hat{F}_e/N) < e$, the condition is obviously satisfied, "rk" denoting the minimal number of (topological) generators.

[†] The first author was supported by NSF grant MCS76-11625.

Received April 26, 1980

This notion of "e-freely indexed profinite group", which is fundamental for our purpose, seems to be new, and is defined and studied in section 2. Roughly, this notion, combined with a theorem of Iwasawa, (1.7), allows us to reduce the problem of freeness of closed normal subgroups of $\hat{F}_e$ to that of the solvability of certain lifting problems for *open* subgroups of $\hat{F}_e$. But properties of open subgroups of $\hat{F}_e$ are readily derived from properties of subgroups of finite index in $\hat{F}_e$, the (discrete) free group on e generators, as we show in section 1.

One surprising consequence of our main result is that, although a closed normal subgroup N of $\hat{F}_e$, $e \geqq 2$, need not be free, all *proper* open subgroups of N are free (on $\aleph_0$ generators if the index $[\hat{F}_e : N]$ is infinite), see (3.10). Other corollaries are analogous to well known results for discrete free groups: the closed commutator subgroup of $\hat{F}_e$, $e \geqq 2$, is free, (3.9), and a closed normal subgroup of $\hat{F}_e$, $e \geqq 2$, is (topologically) finitely generated if and only if its index in $\hat{F}_e$ is finite.

We also prove similar theorems for subgroups of $\hat{F}_\omega$, the free profinite group on $\aleph_0$ generators. Moreover, all results described above are in fact proved in the more general context of pro-$\mathscr{C}$ groups, where $\mathscr{C}$ is any class of finite groups closed under subgroups, homomorphic images and extensions.

In the last section, §4, we apply our results to fields, mainly to so-called pseudo-algebraically closed fields (PAC-fields), introduced by J. Ax in [2]. Interesting examples of such fields have been discovered by M. Jarden. In particular he found many algebraic PAC-extensions K of $\mathbf{Q}$ such that $G(K) \simeq \hat{F}_e$, $e \in \mathbf{N}$, and even some with $G(K) \simeq \hat{F}_\omega$, where $G(K) = \mathrm{Gal}(\tilde{\mathbf{Q}}/K)$. In fact, our research was motivated by a question posed by A. Macintyre: which profinite groups can occur as absolute Galois groups of PAC-fields? In (4.8) we observe that these profinite groups are exactly the closed subgroups of free profinite groups.

Applying results of section 3 to the algebraic PAC-extensions of $\mathbf{Q}$ discovered by Jarden, we obtain:

(1) examples of hilbertian fields of a new type; they are surprisingly close to their algebraic closure $\tilde{\mathbf{Q}}$, see (4.5);

(2) an example of a non-hilbertian, non-algebraically closed field all of whose proper finite extensions are hilbertian, see (4.6);

(3) a solution to a problem posed by Jarden in [12], see (4.7).

Finally, our results have also applications related to the congruence subgroup problem. For this, see [15].

Section 1 is mainly included to make this paper self-contained. For other proofs of Propositions (1.4) and (1.10), see [3].

After this paper was written L. Ribes called our attention to D. V. Mel'nikov's paper, *Normal subgroups of free profinite groups* (Math. USSR-Izvestiya, Vol. 12, No. 1 (1978)), where most of the consequences in Section 3 of our main theorem (3.1) are derived in another way and in somewhat greater generality. As our methods are different and more elementary, it seemed still worthwhile not to omit those parts of Section 3.

Some conventions and terminology

Unless we indicate otherwise, we suppose subgroups of profinite groups to be closed and morphisms between profinite groups to be continuous. If (sub) groups in the ordinary sense are intended, we call them discrete, if there is any possibility of misunderstanding. Further "$\lhd$, $\leqq$" are used for "normal subgroup of, subgroup of"; 1 denotes the group identity as well as the trivial group. Most other terminology is standard, see chapter I of [19]; in particular, free profinite groups are, what some authors call, free in the restricted sense: their free generating set converges to 1. In (3.9) we also use the derived series $G^{(n)}$, and the lower central series $G_{(n)}$ of a profinite group G: $G^{(1)} = G_{(1)} =$ closure of $[G, G]$, $G^{(n+1)} = (G^{(n)})^{(1)}$, $G_{(n+1)} =$ closure of $[G_{(n)}, G]$. The Frattini subgroup $\Phi(G)$ of a profinite group G is the intersection of its maximal proper open subgroups, see (3.12). Finally, $\mathbf{N} = \{0, 1, 2, \cdots\}$, and we use e, f, n for elements of $\mathbf{N}$.

§1. Open subgroups of free pro-$\mathscr{C}$ groups

We recall first some notions and facts on profinite groups which will be constantly used in the following. If we give no reference or proof, the reader may consult chapter I of [19] for details.

(1.1) *From now on in this paper $\mathscr{C}$ will denote a class of finite groups which is closed under formation of subgroups, homomorphic images, finite products, and which contains at least one non-trivial group.* Pro-$\mathscr{C}$ groups are profinite groups whose finite quotients are in $\mathscr{C}$. So the pro-$\mathscr{C}$ groups are closed under formation of subgroups, homomorphic images and (infinite) products.

The class $\mathscr{C}$ is called *full* if $\mathscr{C}$ is also closed under extension of groups. So the classes of finite abelian groups and finite nilpotent groups are not full, while the classes of (finite) p-groups, finite solvable groups and all finite groups are full. If $\mathscr{C}$ is full, then the pro-$\mathscr{C}$ groups are closed under extension of profinite groups: if N is a normal subgroup of the profinite group G, and N and G/N are pro-$\mathscr{C}$ groups, then G is a pro-$\mathscr{C}$ group. If $\mathscr{C}$ is full, $S \in \mathscr{C}$ and $p \mid \# S$, where p is

prime, then $\mathscr{C}$ contains a cyclic group of order p; as every p-group has a normal series with cyclic factors of order p, $\mathscr{C}$ contains all p-groups, and hence all pro-p-groups are pro-$\mathscr{C}$ groups.

Let G be any group. Then the family $NS(G,\mathscr{C}) \overset{\text{def.}}{=} \{N \mid N \lhd G,\ G/N \in \mathscr{C}\}$ serves as basis of neighborhoods of the identity for a topology on G making G a topological group. This topology will be called the pro-$\mathscr{C}$ topology of G, and the pro-$\mathscr{C}$ group

$$\hat{G}(\mathscr{C}) \overset{\text{def.}}{=} \varprojlim_{N \in NS(G,\mathscr{C})} G/N$$

together with the canonical continuous morphism $\tau : G \to \hat{G}(\mathscr{C})$, is called the pro-$\mathscr{C}$ completion of G.

Let further $S(G,\mathscr{C})$ be the set of all subgroups of G which contain an $N \in NS(G,\mathscr{C})$. With these notations we have:

(1.2) PROPOSITION. (a) *$\tau(G)$ is dense in $G(\mathscr{C})$.*

(b) *$S(G,\mathscr{C}) =$ set of open subgroups of G.*

(c) *Each group morphism $\phi : G \to H$ is continuous, if G and H are both endowed with their pro-$\mathscr{C}$ topology, and there is a unique continuous morphism $\hat{\phi}(\mathscr{C}) : \hat{G}(\mathscr{C}) \to \hat{H}(\mathscr{C})$ making the diagram*

$$\begin{array}{ccc} G & \longrightarrow & H \\ \downarrow & & \downarrow \\ \hat{G}(\mathscr{C}) & \longrightarrow & \hat{H}(\mathscr{C}) \end{array}$$

commutative.

(d) *The functor $\hat{}(\mathscr{C})$ is right exact.*

Suppose moreover that $\mathscr{C}$ is full and let G be a group. Then one has:

(e) *Let $H \in S(G,\mathscr{C})$. Then the pro-$\mathscr{C}$ topology of G induces on H the pro-$\mathscr{C}$ topology of H; the induced morphism $\hat{H}(\mathscr{C}) \to \hat{G}(\mathscr{C})$ is a (topological) isomorphism of $\hat{H}(\mathscr{C})$ onto the open subgroup $\overline{\tau H}$ of $\hat{G}(\mathscr{C})$, where $\tau : G \to \hat{G}(\mathscr{C})$ is the canonical map. Moreover $\tau^{-1}(\overline{\tau H}) = H$, $[G:H] = [\hat{G}(\mathscr{C}) : \overline{\tau H}]$, and G/H is canonically isomorphic with $\hat{G}(\mathscr{C})/\overline{\tau H}$ if $H \lhd G$.*

(f) *$H \mapsto \overline{\tau H}$ is a bijection of $S(G,\mathscr{C})$ onto the set of open subgroups of $\hat{G}(\mathscr{C})$, and maps $NS(G,\mathscr{C})$ onto the set of open normal subgroups of $\hat{G}(\mathscr{C})$.*

PROOF. We leave (a) and (b) to the reader. As for (c), we only indicate how $\hat{\phi}(\mathscr{C})$ is defined: let $g = (g_M \cdot M) \in \varprojlim G/M$, M ranging over $NS(G,\mathscr{C})$; then $\hat{\phi}(\mathscr{C})(g) = (\phi(g_{\phi^{-1}N}) \cdot N)$, N ranging over $NS(H,\mathscr{C})$.

(d) If $\phi: G \to H$ is surjective, then by (a) and (c), $\hat{\phi}(\mathscr{C})(\hat{G}(\mathscr{C}))$ is dense in $\hat{H}(\mathscr{C})$ and is compact, so coincides with $\hat{H}(\mathscr{C})$. Similarly, one checks $\mathrm{Ker}(\hat{\phi}(\mathscr{C}))$.

(e) We suppose first that $H \lhd G$, i.e. $H \in NS(G, \mathscr{C})$, and show that $NS(H, \mathscr{C}) \subset S(G, \mathscr{C})$. Let $N \in NS(H, \mathscr{C})$ and write $G = \tau_1 H \cup \cdots \cup \tau_n H$. Then $M = N^{\tau_1} \cap \cdots \cap N^{\tau_n}$ is a normal subgroup of G and H/M is embedded in $H/N^{\tau_1} \times \cdots \times H/N^{\tau_n} \in \mathscr{C}$, so $H/M \in \mathscr{C}$. Because also $G/H \in \mathscr{C}$, we get $G/M \in \mathscr{C}$, so $N \supset M \in NS(G, \mathscr{C})$, resulting in $N \in S(G, \mathscr{C})$.

If H is an arbitrary element of $S(G, \mathscr{C})$, then H contains an $H' \in NS(G, \mathscr{C})$, and the inclusion $NS(H', \mathscr{C}) \subset S(G, \mathscr{C})$ easily implies that $NS(H, \mathscr{C}) \subset S(G, \mathscr{C})$, from which we get that the pro-$\mathscr{C}$ topology of H is induced by the pro-$\mathscr{C}$ topology of G. The remaining assertions in (e) and (f) are now routine. □

(1.3) For a finitely generated group G, henceforth f.g. group G, the rank of G, $\mathrm{rk}(G)$, is its minimal number of generators. This notion is extended to profinite groups as follows: a subset X of a profinite group G is said to generate G if the (discrete) subgroup generated by X is dense in G; we call G finitely generated, f.g. for short, if G has a finite subset which generates G, and in that case we let $\mathrm{rk}(G)$ be the minimal number of elements of such a subset. If G is a group generated by a finite subset X, then $\tau(X)$ generates the profinite group $\hat{G}(\mathscr{C})$, so $\mathrm{rk}(\hat{G}(\mathscr{C})) \leqq \mathrm{rk}(G)$.

In particular, let F_e be the free group on e generators, $e \in \mathbf{N}$. Then its pro-$\mathscr{C}$ completion $\hat{F}_e(\mathscr{C})$ is also the free pro-$\mathscr{C}$ group on a set of e elements, see [19, pp. 61–62], and $\mathrm{rk}\,\hat{F}_e(\mathscr{C}) \leqq e$. But $\mathscr{C}$ contains the group $(\mathbf{Z}/p\mathbf{Z})^e$ of rank e, for some prime p, so $\hat{F}_e(\mathscr{C})$ has a finite group of rank e as homomorphic image, so actually

$$\mathrm{rk}(\hat{F}_e(\mathscr{C})) = e = \mathrm{rk}(F_e).$$

It is convenient to define $E(G) = \mathrm{rk}(G) - 1$ for f.g. (profinite) groups G. It is well known that for subgroups H of finite index in F_e the following holds: H is free and $E(H) = [F_e : H](e-1) = [F_e : H] \cdot E(F_e)$, cf. [17, p. 16]. We have the following profinite analogue.

(1.4) PROPOSITION. *Let $\mathscr{C}$ be a full class, $e \in \mathbf{N}$. Then each open subgroup H of $\hat{F}_e(\mathscr{C})$ is a free pro-$\mathscr{C}$ group on a set of $1 + [\hat{F}_e(\mathscr{C}) : H] \cdot (e-1)$ elements, so again*

$$(*) \qquad E(H) = [\hat{F}_e(\mathscr{C}) : H] \cdot E(\hat{F}_e(\mathscr{C})).$$

PROOF. This follows immediately from (1.2), (e) and (f), and the remark above on free discrete groups.

(1.5) The condition on $\mathscr{C}$ to be full is essential: let $\mathscr{N}$ be the class of finite nilpotent groups. As every pro-nilpotent group is the product of its p-Sylow subgroups, we have:

$$\hat{F}_e(\mathscr{N}) \simeq \prod_p \hat{F}_e(p),$$

where p runs over all primes and $\hat{F}_e(p)$ is the free pro-p-group on e generators. Suppose $e \geqq 2$, and let U_2, U_3 be open subgroups of $\hat{F}_e(2)$, $\hat{F}_e(3)$ of index 2, 3 respectively. Then $\mathrm{rk}(U_2) = 1 + 2(e-1) = 2e-1$ and $\mathrm{rk}(U_3) = 1 + 3(e-1) = 3e-2$. The open subgroup $U = U_2 \times U_3 \times \Pi_{p \neq 2,3} \hat{F}_e(p)$ of $\hat{F}_e(\boldsymbol{N})$ is of index 6 and $\mathrm{rk}(U) = \max\{2e-1, 3e-2, e\} = 3e-2 > e$, so U is neither free as a pro-nilpotent group, nor is formula (*) of (1.4) satisfied for $H = U$ and $\mathscr{C} = \mathscr{N}$.

(1.6) By abuse of language we let $\hat{F}_\omega(\mathscr{C})$ denote the free pro-$\mathscr{C}$ group on a set of $\aleph_0$ elements, cf. [19, p. 61], so $\hat{F}_\omega(\mathscr{C})$ is here *not* intended as the pro-$\mathscr{C}$ completion of the free (discrete) group F_ω on $\aleph_0$ generators. In fact, $\hat{F}_\omega(\mathscr{C}) = \varprojlim F_\omega/N$, N ranging over the normal subgroups with $F_\omega/N \in \mathscr{C}$ which contain almost all the generators (from a fixed set of free generators of F_ω).

Our proofs that many subgroups of $\hat{F}_e(\mathscr{C})$ are isomorphic with $\hat{F}_\omega(\mathscr{C})$ use in an essential way a characterization of $\hat{F}_\omega(\mathscr{C})$ in terms of lifting problems. More precisely:

DEFINITION. A $\mathscr{C}$-lifting problem for a pro-$\mathscr{C}$ group G is a diagram

(**)
$$\begin{array}{ccc} & & A \\ & & \downarrow \\ G & \longrightarrow & B \end{array}$$

of two surjective morphisms between pro-$\mathscr{C}$ groups G, A, B. It is called finite if A and B are finite, i.e. in $\mathscr{C}$. A solution of a $\mathscr{C}$-lifting problem (**) for G is a surjective morphism $G \to A$ such that

$$\begin{array}{ccc} & \nearrow & A \\ & & \downarrow \\ G & \longrightarrow & B \end{array}$$ commutes.

(1.7) PROPOSITION (Iwasawa, see [19, p. 84]). *Let G be a pro-$\mathscr{C}$ group with a countable system of neighborhoods of* 1. *Then $G \simeq \hat{F}_\omega(\mathscr{C})$ if and only if each finite $\mathscr{C}$-lifting problem for G has a solution.*

(1.8) Jarden noted, [11, 1.1] (and it follows easily from (3.2)), that every finite $\mathscr{C}$-lifting problem

$$\begin{array}{ccc} & & B \\ & & \downarrow \\ \hat{F}_e(\mathscr{C}) & \longrightarrow & A \end{array}$$

with $\mathrm{rk}(B) \leqq e$, is solvable.

A consequence of this fact and Iwasawa's theorem (1.7) is that, in case $\mathscr{C}$ is full, every open subgroup of $\hat{F}_\omega(\mathscr{C})$ is isomorphic to $\hat{F}_\omega(\mathscr{C})$. To prove this, we establish some notation.

(1.9) Let $\hat{F}_\omega(\mathscr{C})$ be free as a pro-$\mathscr{C}$ group on $(x_n)_{n\geqq 1}$. Then we may identify $\hat{F}_e(\mathscr{C})$ with the (closed) subgroup of $\hat{F}_\omega(\mathscr{C})$ generated by $x_1, \cdots, x_e$. For $e \leqq f$ we define morphisms

$$\phi_{ef} : F_f(\mathscr{C}) \to F_e(\mathscr{C}) \qquad \text{by} \qquad \begin{aligned} \phi_{ef}(x_i) &= x_i \quad \text{if } 1 \leqq i \leqq e, \\ \phi_{ef}(x_i) &= 1 \quad \text{if } e < i \leqq f, \end{aligned}$$

and

$$\phi_e : F_\omega(\mathscr{C}) \to F_e(\mathscr{C}) \qquad \text{by} \qquad \begin{aligned} \phi_e(x_i) &= x_i \quad \text{if } 1 \leqq i \leqq e, \\ \phi_e(x_i) &= 1 \quad \text{if } i > e. \end{aligned}$$

Because $\phi_{ef} \cdot \phi_f = \phi_e$, the maps ϕ_e induce a morphism of $\hat{F}_\omega(\mathscr{C})$ into the inverse limit $\varprojlim \hat{F}_e(\mathscr{C})$ of the system $(\hat{F}_e(\mathscr{C}), \phi_{ef})$, which is in fact an isomorphism of profinite groups.

(1.10) PROPOSITION. *Let $\mathscr{C}$ be a full class. Then each open subgroup of $\hat{F}_\omega(\mathscr{C})$ is isomorphic to $\hat{F}_\omega(\mathscr{C})$.*

PROOF. Let G be an open subgroup of $\hat{F}_\omega(\mathscr{C})$ and let

$$\begin{array}{ccc} & & B \\ & & \downarrow \theta \\ G & \xrightarrow[\psi]{} & A \end{array}$$

be a finite $\mathscr{C}$-embedding problem. Put $G_1 = \ker(\psi)$. Then the isomorphism $\hat{F}_\omega(\mathscr{C}) \simeq \varprojlim \hat{F}_e(\mathscr{C})$, indicated above, restricts to isomorphisms $G \simeq \varprojlim \phi_e(G)$ and $G_1 \simeq \varprojlim \phi_e(G_1)$, giving rise to an isomorphism $G/G_1 \simeq \varprojlim \phi_e(G)/\phi_e(G_1)$. Now G/G_1 is finite, so for all sufficiently large e we have in fact a natural

isomorphism $G/G_1 \simeq \phi_e(G)/\phi_e(G_1)$. Take an $e \geqq \mathrm{rk}(B)$ for which such an isomorphism holds. Then, by (1.4), the open subgroup $\phi_e(G)$ of $\hat{F}_e(\mathscr{C})$ is a free pro-$\mathscr{C}$ group of rank $\geqq \mathrm{rk}(B)$, so by (1.8) there is a solution $\rho : \phi_e(G) \to B$ of the lifting problem

$$\begin{array}{ccccccc} & & & & & & B \\ & & & & & & \downarrow \theta \\ \phi_e(G) & \longrightarrow & \phi_e(G)/\phi_e(G_1) & \longrightarrow & G/G_1 & \longrightarrow & A \end{array}$$

Hence the composition map $G \to \phi_e(G) \xrightarrow{\rho} B$ is a solution of the lifting problem we started with. □

§2. Freely indexed groups

NOTATION. Let $T(e, r) = 1 + r(e-1)$ for $e, r \in \mathbf{N}$.

(2.1) Recall from (1.3) that if H is a subgroup of index r in the free group F_e, then $H \simeq F_{T(e,r)}$. From this and its profinite analogue we obtain: if G is any f.g. (profinite) group with $\mathrm{rk}(G) \leqq e$ and H a subgroup of index r in G, then H is also finitely generated and $\mathrm{rk}(H) \leqq T(e, r)$.

The following formula will be often used:

(2.2) $$T(T(e, r), k) = T(e, rk) \qquad \text{for } e, r, k \in \mathbf{N}.$$

(2.3) DEFINITION. A f.g. (profinite) group G is called *freely indexed*, if

$$\mathrm{rk}(H) = T(\mathrm{rk}(G), [G : H])$$

for each subgroup H of finite index in G.

If $\mathrm{rk}(G) = e$ and G is freely indexed, we say also that G is e-freely indexed.

Note that our definition says that $E(H) = [G : H] \cdot E(G)$ for freely indexed (profinite) G and $H \leqq G$ of finite index. So E is an Euler characteristic, in the sense of [4], for the class of freely indexed (profinite) groups.

Clearly the free group F_e is e-freely indexed, and every f.g. infinite simple group is freely indexed (for such a group does not have any proper subgroup of finite index).

(2.4) LEMMA. *Let G be a (profinite) group with $\mathrm{rk}(G) \leqq e$, and let H be a subgroup of index r in G. Then G is e-freely indexed iff H is $T(e, r)$-freely indexed.*

PROOF. Assume that G is e-freely indexed, and let K be a subgroup of index k in H. Then

$$[G:K] = rk, \qquad \text{so } \mathrm{rk}(K) = T(e, rk) = T(T(e,r), k).$$

This proves that H is $T(e,r)$-freely indexed.

Assume now that H is $T(e,r)$-freely indexed, and let L be a subgroup of G of index l. We have to show that $\mathrm{rk}(L) = T(e,l)$.

As $\mathrm{rk}(G) \leqq e$, we know that $\mathrm{rk}(L) \leqq T(e,l)$. Now, if $\mathrm{rk}(L) < T(e,l)$, then

$$\mathrm{rk}(L \cap H) \leqq T(\mathrm{rk}\, L, [L : L \cap H]) < T(T(e,l), [L : L \cap H])$$

$$= T(e, l \cdot [L : L \cap H]) = T(e, [G:L] \cdot [L : L \cap H]) = T(e, [G : L \cap H]);$$

but using the assumption that H is $T(e,r)$-freely indexed, we get:

$$\mathrm{rk}(H \cap L) = T(T(e,r), [H : H \cap L]) = T(e, r \cdot [H : H \cap L])$$

$$= T(e, [G:H] \cdot [H : H \cap L]) = T(e, [G : H \cap L]),$$

which contradicts the previous inequality. Hence $\mathrm{rk}(L) = T(e,l)$. □

(2.5) LEMMA. *Let G be a* f.g. *profinite group with* $\mathrm{rk}(G) \leqq e$.

(i) *If $K \leqq L$ are open subgroups of G and* $\mathrm{rk}(K) = T(e, [G:K])$, *then* $\mathrm{rk}(L) = T(e, [G:L])$.

(ii) *If $(K_\alpha)_{\alpha \in A}$ is a system of neighborhoods of $1 \in G$ consisting of open subgroups of G and* $\mathrm{rk}(K_\alpha) = T(e, [G:K_\alpha])$ *for all $\alpha \in A$, then G is e-freely indexed.*

(iii) *Suppose G is infinite and not e-freely indexed. Then there is for each natural number n an open subgroup L_n of G such that $T(e, [G:K]) \geqq \mathrm{rk}(K) + n$, for all open subgroups K of L_n.*

PROOF. For (i) the argument is the same as in the proof of (2.4). (ii) is an immediate consequence of (i) and the definition of e-freely indexed. (iii) is proved by induction on n: For L_1 we can take any open subgroup of G with $T(e, [G:L_1]) > \mathrm{rk}(L_1)$. Suppose $n \geqq 1$ and L_n is an open subgroup of G satisfying the inequality of (iii). Then we have for every *proper* open subgroup L_{n+1} of L_n:

$$T(e, [G:L_{n+1}]) = T(T(e, [G:L_n]), [L_n : L_{n+1}]) \geqq T(\mathrm{rk}(L_n) + n, [L_n : L_{n+1}])$$

$$= T(\mathrm{rk}(L_n), [L_n : L_{n+1}]) + n \cdot [L_n : L_{n+1}] \geqq \mathrm{rk}(L_{n+1}) + (n+1). \qquad \square$$

(2.6) EXAMPLES. (A) Every infinite procyclic group is 1-freely indexed, [19, p. 58].

(B) Let $\mathscr{C}$ be a full class of finite groups. Then $\hat{F}_e(\mathscr{C})$ is e-freely indexed, by (1.4).

If $\mathscr{C}$ is the non-full class of finite nilpotent groups and $e \geqq 2$, then (1.5) shows that $\hat{F}_e(\mathscr{C})$ is not freely indexed. A similar argument shows that for $\mathscr{C}$ the class of finite abelian groups and $e \geqq 2$, $\hat{F}_e(\mathscr{C})$ is not freely indexed.

(C) Let $\mathscr{C}$ and $\mathscr{C}'$ be full classes, with $\mathscr{C}' \subsetneqq \mathscr{C}$, and suppose N is a normal subgroup of $\hat{F}_e(\mathscr{C})$ of finite index. Define K as the normal subgroup of N such that N/K is the maximal pro-$\mathscr{C}'$ quotient of N; so K is a (topologically) characteristic subgroup of N, hence a normal subgroup of $\hat{F}_e$.

We claim: $F_e(\mathscr{C})/K$ is e-freely indexed. Indeed, its subgroup N/K is isomorphic with $\hat{F}_k(\mathscr{C}')$, where $k = T(e, [\hat{F}_e(\mathscr{C}) : N])$, so the claim follows from (2.4).

(D) Let $S = \{p_1, p_2, \cdots\}$ be an infinite set of prime numbers, $p_1 < p_2 < \cdots$, and let $F = \hat{F}_e$, $e \geqq 2$. We define by induction a descending sequence $(N_i)_{i \geq 1}$ of normal open subgroups of F as follows: $N_1 = F$. If N_i is already defined, then $N_i \simeq \hat{F}_{r_i}$, where $r_i = T(e, [F : N_i])$, so N_i has a unique open normal subgroup H such that

$$N_i/H \simeq (\mathbf{Z}/p_i\mathbf{Z})^{r_i}. \qquad \text{Put } N_{i+1} = H.$$

Note that N_{i+1} is in fact a (topologically) characteristic subgroup of N_i, so by induction on i, of F as well. Finally put $N = \bigcap_{i=1}^{\infty} N_i$. We claim that the profinite group $G = F/N$ is e-freely indexed.

By (2.5) (ii) it suffices to show that $\mathrm{rk}(N_i/N) = T(e, [F : N_i]) = r_i$. It is clear that $\mathrm{rk}(N_i/N) \leqq \mathrm{rk}(N_i) = T(e, [F : N_i]) = r_i$. On the other hand, $(\mathbf{Z}/p_i\mathbf{Z})^{r_i}$, which has rank r_i, is a quotient of N_i/N, so $\mathrm{rk}(N_i/N) = r_i$.

G is clearly a pro-solvable group, but far from being free pro-solvable. In fact, its supernatural order $\# G$ is the product $\prod p_i^{r_i}$, so is a product of *finite* powers of primes.

REMARK. Such behavior of being freely indexed without being free, as indicated in Example (D), is impossible for pro-p-groups. In fact, it is proved in [16] that each e-freely indexed pro-p-group is isomorphic to $\hat{F}_e(p)$.

QUESTIONS. (1) Is there an e-freely indexed profinite group, $e \geqq 2$, whose supernatural order is $\prod_p p^{\alpha_p}$, where $\alpha_p \leqq M$ for some $M \in \mathbf{N}$ and all primes p?

(2) Is a residually finite freely indexed discrete group necessarily free?

§3. Subgroups of $\hat{F}_e(\mathscr{C})$ and $\hat{F}_\omega(\mathscr{C})$

Let $\mathscr{C}$ in this section be a full class of finite groups. We want to find conditions on a subgroup N of $\hat{F}_e(\mathscr{C})$ which imply that N is a free pro-$\mathscr{C}$ group (on finitely many or on $\aleph_0$ generators). If N is of finite index in $\hat{F}_e(\mathscr{C})$ this is the case, by

(1.4). It is also well known that each subgroup of a free pro-p-group is a free pro-p-group. On the other hand, suppose that $\mathscr{C}$ contains, besides all p-groups for some prime p, also a non p-group. Then, for $e \geqq 1$, the p-Sylow subgroups of $\hat{F}_e(\mathscr{C})$ are certainly not free pro-$\mathscr{C}$ groups. However, if $e \geqq 2$, they are not normal in $\hat{F}_e(\mathscr{C})$. But, under the same assumption on $\mathscr{C}$, even normal subgroups are not always free pro-$\mathscr{C}$ groups: let N be the kernel of the canonical map $\hat{F}_e(\mathscr{C}) \to \hat{F}_e(p)$, $e \geqq 1$. Then N does not have $\mathbf{Z}/p\mathbf{Z}$ as a quotient, so N is not a free pro-$\mathscr{C}$ group.

Nevertheless, our theorem (3.10) states that all subgroups of $\hat{F}_e(\mathscr{C})$ which are *proper* subgroups of finite index in a *normal* subgroup of $\hat{F}_e(\mathscr{C})$ are free pro-$\mathscr{C}$ groups. This is one of the many corollaries of our main result, which now follows.

(3.1) THEOREM. *Let N be a normal subgroup of $\hat{F}_e(\mathscr{C})$ of infinite index, $e \geqq 2$, such that $\hat{F}_e(\mathscr{C})/N$ is not e-freely indexed. Then $N \simeq \hat{F}_\omega(\mathscr{C})$.*

For the proof we need the following lemma, proved by Gaschütz for finite groups, and extended by Jarden and Kiehne in [14] to f.g. profinite groups.

(3.2) LEMMA. *Let $\phi : H \to K$ be a surjective morphism of profinite groups with* $\mathrm{rk}(H) = e$.

Then for each system of generators $y_1, \cdots, y_e$ of K there exists a system of generators $x_1, \cdots, x_e$ of H with

$$\phi(x_i) = y_i, \qquad i = 1, \cdots, e.$$

(3.3) We also want to have available the notion of *cartesian square*: this is defined as an inclusion diagram of subgroups of a group G

$$\begin{array}{ccc} G_1 & \hookrightarrow & G \\ \uparrow & & \uparrow \\ G_0 & \hookrightarrow & G_2 \end{array}$$

satisfying the following equivalent conditions:

(a) $G = G_1 \cdot G_2$ and $G_1 \cap G_2 = G_0$.

(b) The natural (coset space) map $G_1/G_0 \to G/G_2$ is bijective.

(b′) The natural map $G_2/G_0 \to G/G_1$ is bijective.

Note that it makes no difference whether we read the left coset version of (b) and (b′), or the right coset version; moreover, in the case of a cartesian diagram as above, we have: if $G_0 \lhd G_1$ and $G_0 \lhd G_2$, then $G_0 \lhd G$; if $G_2 \lhd G$ (resp. $G_1 \lhd G$), then $G_0 \lhd G_1$ (resp. $G_0 \lhd G_2$), and the map (b) (resp. (b′)) is an isomorphism of groups.

(3.4) PROOF OF THEOREM (3.1). By Iwasawa's characterization of $\hat{F}_\omega(\mathscr{C})$, (1.7), it suffices to find a solution to a given finite $\mathscr{C}$-lifting problem:

(3.5)
$$\begin{array}{ccc} & & B \\ & & \downarrow \theta \\ N & \xrightarrow{\psi} & A \end{array}$$

Let $N_1 = \ker(\psi)$. There is an open subgroup L_1 of $\hat{F}_e(\mathscr{C})$ with $L_1 \cap N = N_1$, so putting $L = L_1 \cdot N$ we have a cartesian square

(3.6)
$$\begin{array}{ccc} L & & \\ | & \searrow & \\ L_1 & & N \\ | & \searrow & | \\ N_1 & & \end{array}$$

As $\hat{F}_e(\mathscr{C})/N$ is infinite, of rank $\leqq e$, but not e-freely indexed, it follows from Lemma (2.5) that L has an open subgroup $L' \supset N$ such that $\mathrm{rk}(L') - \mathrm{rk}(L'/N)$ is arbitrarily large. Putting $L_1' = L_1 \cap L'$ we obtain

$$[N : N_1] \leqq [L' : L_1'] \leqq [L : L_1] = [N : N_1], \quad \text{i.e. } [N : N_1] = [L' : L_1'].$$

Moreover, for suitably "small" L', its subgroup L_1' will be normal in L'.

So replacing, if necessary, L and L_1 by L' and L_1', we may assume that in the cartesian square (3.6) L_1 is normal in L and $\mathrm{rk}(L) - \mathrm{rk}(L/N) \geqq \mathrm{rk}(B)$. Put $l = \mathrm{rk}(L)$, $l_1 = \mathrm{rk}(L_1/N_1) = \mathrm{rk}(L/N)$ and $b = \mathrm{rk}(B)$. So $l \geqq b + l_1$. Let $y_1, \cdots, y_b$ generate B and denote by $\bar{y}_1, \cdots, \bar{y}_b$ their images in L/L_1 under the map $B \xrightarrow{\theta} A \simeq N/N_1 \simeq L/L_1$. Choose further $y_{b+1}, \cdots, y_{b+l_1}$ in L_1 such that under the map $L_1 \to L_1/N_1 \simeq L/N$ their images $\bar{y}_{b+1}, \cdots, \bar{y}_{b+l_1}$ generate L/N. Hence, by (3.2), there are generators $z_1, \cdots, z_l$ of L such that under the canonical map $L \to L/L_1 \times L/N$ (which is surjective because $L_1 \cdot N = L$) the image of z_i is $(\bar{y}_i, 1)$ for $i = 1, \cdots, b$, is equal to $(1, \bar{y}_i)$ for $i = b+1, \cdots, b+l_1$, and equals $(1, 1)$ if $b + l_1 < i \leqq l$.

Because the pro-$\mathscr{C}$ group L is necessarily free on $z_1, \cdots, z_l$, cf. [19, p. 68], we can define a morphism $\phi : L \to B$ by $\phi(z_i) = y_i$ for $i = 1, \cdots, b$; $\phi(z_i) = 1$ for $b < i \leqq l$.

It is now routine to check that the two subdiagrams of the diagram

$$\begin{array}{ccccc} L & & \xrightarrow{\phi} & & B \\ & \searrow & \downarrow & & \downarrow \theta \\ & & L/L_1 & & \\ & & \downarrow & & \\ N & \longrightarrow & N/N_1 & \xrightarrow{\sim} & A \end{array}$$

commute, so $N \hookrightarrow L \xrightarrow{\phi} B$ is the required solution to the lifting problem (3.5), provided this map is surjective. Because ϕ is surjective, we only have to show that $N \cdot \mathrm{Ker}(\phi) = L$, which clearly is a consequence of $N_1 \cdot \mathrm{Ker}(\phi) \supset L_1$. As for this last inclusion: we have $y_i z_i^{-1} \in \mathrm{Ker}(L \to L/L_1 \simeq L/N) = N_1$ and $z_i \in \mathrm{Ker}(\phi)$ for $i = b+1, \cdots, b+l_1$, so $y_i \in N_1 \cdot \mathrm{Ker}(\phi)$ for such i. Now the y_i's for $i = b+1, \cdots, b+l_1$ generate L_1 modulo N_1, so $L_1 \subset N_1 \cdot \mathrm{Ker}(\phi)$. This concludes the proof of (3.1). □

As a first corollary we derive an analogue of our main result (3.1) for $\hat{F}_\omega(\mathscr{C})$. We use the notations introduced in (1.9).

(3.7) COROLLARY. *Let N be a normal subgroup of $\hat{F}_\omega(\mathscr{C})$ such that $\hat{F}_e(\mathscr{C})/\phi_e(N)$ is not e-freely indexed for infinitely many e. Then $N \simeq \hat{F}_\omega(\mathscr{C})$.*

PROOF Let, as before, a finite $\mathscr{C}$-lifting problem

$$\begin{array}{ccc} & & B \\ & & \downarrow \theta \\ N & \xrightarrow{\psi} & A \end{array}$$

be given and put $N_1 = \mathrm{Ker}(\psi)$. Then, exactly as in the proof of (1.10), we have for each sufficiently large e a natural isomorphism $N/N_1 \simeq \phi_e(N)/\phi_e(N_1)$. Take an $e \geqq \mathrm{rk}(B)$ for which such an isomorphism holds and such that $\hat{F}_e(\mathscr{C})/\phi_e(N)$ is not e-freely indexed. Then (3.1), or (1.8) in case $\hat{F}_e(\mathscr{C})/\phi_e(N)$ is finite, implies that there is a solution $\rho : \phi_e(N) \to B$ of the lifting problem

$$\begin{array}{ccccccc} & & & & & & B \\ & & & & & & \downarrow \theta \\ \phi_e(N) & \longrightarrow & \phi_e(N)/\phi_e(N_1) & \xrightarrow{\sim} & N/N_1 & \xrightarrow{\sim} & A \end{array}$$

Hence the composition map $N \to \phi_e(N) \xrightarrow{\rho} B$ is a solution of the lifting problem we started with.

(3.8) COROLLARY. (i) *If N is a normal subgroup of infinite index of $\hat{F}_e(\mathscr{C})$, $e \geqq 2$, with $\mathrm{rk}(\hat{F}_e(\mathscr{C})/N) < e$, then $N \simeq \hat{F}_\omega(\mathscr{C})$.*

(ii) *If N is a normal subgroup of $\hat{F}_\omega(\mathscr{C})$ such that $\hat{F}_\omega(\mathscr{C})/N$ is* f.g., *then $N \simeq \hat{F}_\omega(\mathscr{C})$.*

This is immediate from (3.1), respectively (3.7). In case (i) $\hat{F}_e(\mathscr{C})/N$ is clearly not e-freely indexed, but it may be freely indexed: take N to be the (topological) normal closure of x_1 in $\hat{F}_e = \langle x_1, \cdots, x_e \rangle$, $e \geqq 2$, i.e. the smallest (closed) normal

subgroup of $\hat{F}_e$ containing x_1. Then $\hat{F}_e/N \simeq \hat{F}_{e-1}$, so $\hat{F}_e/N$ is not e-freely indexed, but it is $e-1$ freely indexed. So $N \simeq \hat{F}_\omega$. See also [7, p. 246] for another structure theorem describing the normal closure of x_1 in $\hat{F}_2$.

(3.9) COROLLARY. *Let $G = \hat{F}_e(\mathscr{C})$, $e \geqq 2$, or $G = \hat{F}_\omega(\mathscr{C})$.*

(i) *If N is a normal subgroup of infinite index in G such that G/N is abelian, then $N \simeq \hat{F}_\omega(\mathscr{C})$.*

(ii) *For all $n \geqq 1$, $G^{(n)} \simeq \hat{F}_\omega(\mathscr{C})$ and $G_{(n)} \simeq \hat{F}_\omega(\mathscr{C})$.*

PROOF. If A is an abelian profinite group of rank $e \geqq 2$, then for some prime p, $1 < [A : A^p] < \infty$, but $\mathrm{rk}(A^p) \leqq \mathrm{rk}(A) = e$, so A cannot be e-freely indexed. This fact implies (i).

(ii) follows from (i) by induction on n. □

We come now to the most unexpected result of this section.

(3.10) THEOREM. *Let $G = \hat{F}_e(\mathscr{C})$, $e \geqq 2$, or $G = \hat{F}_\omega(\mathscr{C})$. Then each proper open subgroup of a normal subgroup of infinite index in G is isomorphic to $\hat{F}_\omega(\mathscr{C})$.*

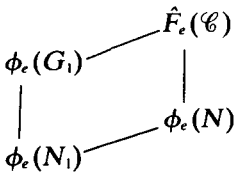
PROOF. Let N_1 be a proper open subgroup of the normal subgroup N of infinite index in G, say $[N : N_1] = r > 1$. Let G_1 be an open subgroup of G with $G_1 \cap N = N_1$. Replacing G_1 if necessary, by $G_1 \cdot N$, we may assume without loss of generality that we have a cartesian square

Consider first the case that $G = \hat{F}_e(\mathscr{C})$. Then $\mathrm{rk}(G_1/N_1) = \mathrm{rk}(G/N) \leqq \mathrm{rk}(G) < \mathrm{rk}(G_1)$, so by (3.8)(i) we get $N_1 \simeq \hat{F}_\omega(\mathscr{C})$.

We now consider the case $G = \hat{F}_\omega(\mathscr{C})$. The finiteness of N/N_1 and condition (b′) of (3.3) imply easily that for all sufficiently large e, say for $e \geqq M$:

$$\phi_e(N)/\phi_e(N_1) \simeq N/N_1 \simeq G/G_1 \simeq \hat{F}_e(\mathscr{C})/\phi_e(G_1).$$

So for $e \geqq M$ we have a cartesian square



Then, as before, $\mathrm{rk}(\phi_e(G_1)/\phi_e(N_1)) < \mathrm{rk}(\phi_e(G_1))$ and $\phi_e(G_1) \simeq \hat{F}_{T(e,r)}(\mathscr{C})$, so $\phi_e(G_1)/\phi_e(N_1)$ is not $T(e,r)$-freely indexed, for all $e \geqq M$. Because $G_1 \simeq \varprojlim \phi_e(G_1)$ (canonically), the same reasoning as in the proof of (3.7) shows that then $N_1 \simeq \hat{F}_\omega(\mathscr{C})$. □

REMARK. If we take for N the kernel of the natural map $\hat{F}_2 \to \hat{F}_2(p)$, p a prime, then N is a normal subgroup of infinite index in $\hat{F}_2$, but N is not free (it does not have $\mathbf{Z}/(p)$ as a quotient). But the preceding theorem says that all its proper open subgroups are free (isomorphic with $\hat{F}_\omega$). Moreover N is torsion free (as a subgroup of the torsion free group $\hat{F}_2$, see [10, 16.2]). This is in contrast with the pro-p case: Serre proved in [20] that a torsion free pro-p-group with an open subgroup which is a free pro-p-group, is itself a free pro-p-group.

The following corollary extends a result by Anderson, [1, p. 235].

(3.11) COROLLARY. *$\hat{F}_e(\mathscr{C})$, for $e \geqq 2$, and $\hat{F}_\omega(\mathscr{C})$ have trivial center.*

PROOF. The center is a normal subgroup but it cannot have proper open subgroups because these would not be abelian, by (3.10) or (1.10). So the center is trivial. □

Next we generalize a theorem in [18].

(3.12) COROLLARY. *Suppose the (full) class $\mathscr{C}$ contains the cyclic groups $\mathbf{Z}/p\mathbf{Z}$ and $\mathbf{Z}/q\mathbf{Z}$ for two different primes p and q. Let $G = \hat{F}_e(\mathscr{C})$ for $e \geqq 2$, or $G = \hat{F}_\omega(\mathscr{C})$. Then the Frattini subgroup $\Phi(G)$ of G is trivial.*

PROOF. For every profinite group G, $\Phi(G)$ is pro-nilpotent, since this is true for every finite group G. If in our case $\Phi(G)$ would not be trivial, then it had a proper open subgroup which, by (3.10) or (1.10), would be a free pro-$\mathscr{C}$ group on at least two generators, but such a profinite group cannot be pro-nilpotent. □

There are of course many similar applications, for instance, for $e \geqq 2$, $\hat{F}_e$ does not have any non-trivial pro-solvable normal subgroup, etc.

More substantial is the following. Call a subgroup H of a profinite group G *subnormal* (in G) if there is a finite series of subgroups $H = H_0 \lhd H_1 \lhd \cdots \lhd H_k = G$.

We can now generalize (3.10) to subnormal subgroups.

(3.13) THEOREM. *Let $G = \hat{F}_e(\mathscr{C})$, $e \geqq 2$, or $G = \hat{F}_\omega(\mathscr{C})$. Then each proper open subgroup of a subnormal subgroup of infinite index in G is isomorphic to $\hat{F}_\omega(\mathscr{C})$.*

PROOF. Let H be a subnormal subgroup of infinite index in G, say $H =$

$H_0 \lhd H_1 \lhd \cdots \lhd H_k = G$ for subgroups H_i of G. We use induction on k. For $k = 1$, we can apply (3.10). Suppose $k > 1$. If H_0 is of finite index in H_1, then each proper open subgroup of H_0 is also a proper open subgroup of H_1, and we can apply the induction hypothesis. So let H_0 be of infinite index in H_1. Then $H = H_0$ is a normal subgroup of infinite index in a proper open subgroup G' of H_1. But then $G' \simeq \hat{F}_{e'}(\mathscr{C})$ for some $e' \geqq 2$, or $G' \simeq \hat{F}_\omega(\mathscr{C})$, by the induction hypothesis. Now we can again apply (3.10) to show that every proper open subgroup of H is isomorphic to $\hat{F}_\omega(\mathscr{C})$. □

A consequence is a profinite analogue of a well-known result of L. Greenberg for discrete free groups, cf. [17, p. 18].

(3.14) COROLLARY. *If $e \geqq 2$, then a non-trivial subnormal subgroup H of $\hat{F}_e(\mathscr{C})$ is finitely generated if and only if H is of finite index in $\hat{F}_e(\mathscr{C})$.*

PROOF. If H is of infinite index, then each of its proper open subgroups (which do exist) is not finitely generated by (3.13), so H cannot be finitely generated, see (2.1). □

Now we give a result which shows that the sufficient condition of Theorem (3.1) for N to be a free pro-$\mathscr{C}$ group, is not a necessary condition. Namely, in (2.6) (D) we indicated a normal subgroup N of $\hat{F}_e$, $e \geqq 2$, such that $\hat{F}_e/N$ is e-freely indexed. Nevertheless, in this particular case one still has $N \simeq \hat{F}_\omega$, as the following result implies. Note that in this proposition we do not suppose the subgroup to be normal.

(3.15) PROPOSITION. *Let N be a subgroup of infinite index in $\hat{F}_e(\mathscr{C})$, $e \geqq 2$, such that $[\hat{F}_e(\mathscr{C}) : N] = \prod p^{\alpha(p)}$ (p ranging over the primes) with all $\alpha(p)$ finite.*
Then $N \simeq \hat{F}_\omega(\mathscr{C})$.

PROOF. We follow the proof of Theorem (3.1) and use notations introduced there. Our assumption guarantees that we can obtain a cartesian square (3.6) such that $[L : N]$ is prime to $\#(B)$ (and hence to $\#(A)$), and $l = \mathrm{rk}(L) \geqq \mathrm{rk}(B) = b$. Because $L \simeq \hat{F}_l(\mathscr{C})$, there is by (1.8) a solution $\phi : L \to B$ of the $\mathscr{C}$-lifting problem

$$\begin{array}{ccccccc} & & & & & & B \\ & & & & & & \downarrow \theta \\ L & \longrightarrow & L/L_1 & \xrightarrow{\sim} & N/N_1 & \xrightarrow{\sim} & A. \end{array}$$

Now $[L : N \cdot \mathrm{Ker}\,\phi]$ divides the two supernatural numbers $[L : N]$ and $[L : \mathrm{Ker}(\phi)] = \#B$, which are relatively prime. So $L = N \cdot \mathrm{Ker}\,\phi$, from which it

follows that the map $N \hookrightarrow L \xrightarrow{\varphi} B$ is surjective, hence it solves the $\mathscr{C}$-lifting problem we started with.

(3.16) We conclude with remarking that Example (2.6)(C) can now be generalized to the case that N is of infinite index in $\hat{F}_e(\mathscr{C})$, but using otherwise the same assumptions and notations:

$$\hat{F}_e(\mathscr{C})/K \text{ is } e\text{-freely indexed}, \qquad \text{for } e \geqq 2.$$

This follows from (3.1), because K cannot be isomorphic with $\hat{F}_\omega(\mathscr{C})$: it does not have any non-trivial $\mathscr{C}'$-quotient.

§4. Applications to fields

(4.1) The most immediate applications of the results in §3 are to certain infinite extensions of function fields in one variable. As an example, let K be a function field in one variable over a countable algebraically closed field C of characteristic 0, i.e. K is a finite extension of $C(t)$, t transcendental over C. Then the absolute Galois group $G(K) = \mathrm{Gal}(\tilde{K} \mid K)$ is isomorphic to $\hat{F}_\omega$, cf. [3, p. 109]. Now let K_{ab} be the maximal abelian extension of K (within the algebraic closure $\tilde{K}$ of K). Then, by (3.9), we get:

$$G(K_{ab}) \simeq \hat{F}_\omega.$$

Similarly, let L be an infinite normal extension of K, $L \neq \tilde{K}$; then for each proper finite extension M of L we have: $G(M) \simeq \hat{F}_\omega$ (by (3.10)).

The groups $\hat{F}_e$ also occur naturally as Galois groups over function fields: let $S \subset \mathbf{C}$, $\# S = e$, and let K be the maximal algebraic extension of $\mathbf{C}(t)$, within a fixed algebraic closure of $\mathbf{C}(t)$, which is unramified at all points of $\mathbf{C} \backslash S$. Then $K \mid \mathbf{C}(t)$ is normal and $\mathrm{Gal}(K \mid \mathbf{C}(t)) \simeq \hat{F}_e$. (This is a consequence of Riemann's Existence Theorem, cf. [19, p. 79].) So many results of §3 can be applied to subextensions $L \mid \mathbf{C}(t)$ of $K \mid \mathbf{C}(t)$, to give results on $\mathrm{Gal}(K \mid L)$.

(4.2) A more recent source of free profinite groups as Galois groups comes from M. Jarden's work, [9, 10]. He starts, in some sense, from the other end:

Let $G = G(\mathbf{Q}) = \mathrm{Gal}(\tilde{\mathbf{Q}} \mid \mathbf{Q})$, and $e \in \mathbf{N}$. Then for almost all $(\sigma_1, \cdots, \sigma_e) \in G^e$ — in the sense of the product measure on G^e, induced by the Haar measure on the compact group G — one has:

(a) the closed subgroup $\langle \sigma_1, \cdots, \sigma_e \rangle$ of G generated by $\{\sigma_1, \cdots, \sigma_e\}$ is free, as a profinite group, on $\sigma_1, \cdots, \sigma_e$;

(b) its fixed field $\mathrm{Fix}\langle \sigma_1, \cdots, \sigma_e \rangle$ is pseudo-algebraically closed.

(Note that

$$\mathrm{Fix}(\sigma_1, \cdots, \sigma_e) = \{x \in \tilde{\mathbf{Q}} \mid \sigma_1(x) = \cdots = \sigma_e(x) = x\} = \mathrm{Fix}(\langle \sigma_1, \cdots, \sigma_e \rangle).)$$

Here a field K is called pseudo-algebraically closed (PAC for short) if each nonvoid absolutely irreducible affine variety defined over K has K-rational points.

(4.3) REMARK. For simplicity, we state all of Jarden's results only for algebraic extensions of $\mathbf{Q}$, but in most cases $\mathbf{Q}$ can be replaced by any countable *hilbertian* field K (and $\tilde{\mathbf{Q}}$ by the algebraic closure of K). Because the notion of "hilbertian field" is used further on, let us give a definition.

A field K is called hilbertian if Hilbert's Irreducibility Theorem — proved by Hilbert for $\mathbf{Q}$ — holds for it, i.e.: for each irreducible $f(T, X) \in K(T)[X]$ there are infinitely many $t \in K$ such that $f(t, x)$ is defined and irreducible in $K[X]$.

(4.4) Fields K such that $G(K) \simeq \hat{F}_e$, resp. $G(K) \simeq \hat{F}_\omega$, are called e-free, resp. ω-free. Generalizing Ax results on the elementary theory of finite fields in [2], Jarden and Kiehne proved, cf. [14], that for each $e \in \mathbf{N}$ the elementary theory of perfect e-free PAC-fields is decidable.

Jarden proved analogues for ω-free PAC-fields in [11], but for some time it remained an open problem whether algebraic extensions of $\mathbf{Q}$ could be ω-free and PAC. See however [13] for a construction of such a field, and [6] for another construction which gives even a decidable model. Our results of §3 make it clear that such fields occur in great abundance. For instance, let $(\sigma_1, \sigma_2) \in G^2$, $G = \mathrm{Gal}(\tilde{\mathbf{Q}} \mid \mathbf{Q})$, such that its fixed field K is a 2-free PAC-field (which is the case for almost all $(\sigma_1, \sigma_2) \in G^2$).

Then, by (3.9), its maximal abelian extension K_{ab} is an ω-free PAC-field (the PAC-property is preserved under separable algebraic extensions). Also, if L is any infinite normal extension of K, $L \neq \tilde{\mathbf{Q}}$, then each proper finite extension L' of L is an ω-free PAC-field.

(4.5) Now Roquette has noted that ω-free PAC-fields of characteristic 0 are always hilbertian (a proof is given in [13], and a quite different one in [6]).

This means that we now have rather surprising examples of hilbertian fields. Hilbertian extensions of $\mathbf{Q}$ were thought of as not too large, i.e. rather "far" from their algebraic closure $\tilde{\mathbf{Q}}$. One way to make this precise is to call an algebraic extension $L \mid \mathbf{Q}$ *large*, if L contains a field K such that $G(K)$ is finitely generated. In fact, it is well known that fields K whose absolute Galois group $G(K)$ is finitely generated, cannot be hilbertian. But the ω-free PAC-fields we

described in (4.4) are hilbertian, and at the same time large as well (because they contain a 2-free field).

We can also obtain in this way a hilbertian field which is a finite extension of a non-hilbertian field. In fact we have a stronger result:

(4.6) PROPOSITION. *There exists a non-hilbertian proper subfield L of $\tilde{\mathbf{Q}}$ all of whose proper finite extensions are hilbertian.*

PROOF. Let K be a 2-free PAC-subfield of $\tilde{\mathbf{Q}}$ and let L be its maximal solvable extension, i.e. the compositum of all its finite solvable extensions. Then L has clearly no proper solvable extension, so L is certainly not hilbertian. (Consider the irreducible polynomial $X^2 - T \in L(T)[X]$.) Now $G(L)$ is a normal subgroup of $G(K) \simeq \hat{F}_2$ of infinite index, so all proper subgroups of $G(L)$ of finite index are isomorphic to $\hat{F}_\omega$, by (3.10). In other words, each proper finite extension of L is ω-free and PAC, hence hilbertian. □

REMARK. If we take K in the above proof such that it contains a primitive pth root of unity, p a prime, then we can take for L also the maximal p-extension of K. L will then not have any cyclic extension of degree p, so L is not hilbertian, but L has for each prime $q \neq p$ a cyclic extension of degree q (which is hilbertian).

(4.7) Let us now present the solution of a problem posed by Jarden in [12]. In this paper he gave another method to obtain e-free PAC-fields:

Let $e \in \mathbf{N}$. Then for almost all $\sigma \in G = \mathrm{Gal}(\tilde{\mathbf{Q}} \mid \mathbf{Q})$ and almost all $(\tau_1, \cdots, \tau_e) \in G^e$, the field $\mathrm{Fix}(\sigma^{\tau_1}, \cdots, \sigma^{\tau_e})$ is e-free and PAC (here we write σ^τ for the conjugate $\tau^{-1}\sigma\tau$ of σ).

This raised the following problem, cf. [12, problem 2]: does there exist for almost all $\sigma \in G$ a sequence $\tau_1, \tau_2, \tau_3, \cdots$ in G such that the (closed) subgroup of G generated by $\sigma^{\tau_1}, \sigma^{\tau_2}, \sigma^{\tau_3}, \cdots$ is isomorphic to $\hat{F}_\omega$?

PROPOSITION. *For almost all σ and τ in G the closed subgroup of G generated by the conjugates σ^{τ^n} $(n \in \mathbf{Z})$ of σ is isomorphic to $\hat{F}_\omega$.*

An immediate field theoretic consequence of its proof is the following.

COROLLARY. *For almost all σ and τ in G, the intersection of the conjugate fields $\tau^n(K)$, $n \in \mathbf{Z}$, where $K = \mathrm{Fix}(\sigma)$, is an ω-free* PAC*-field, in particular a hilbertian field.*

PROOF OF THE PROPOSITION. If $\sigma, \tau \in G$ then the (closed) subgroup of G generated by the σ^{τ^n}, $n \in \mathbf{Z}$, is exactly the normal closure of σ in $\langle \sigma, \tau \rangle$. As we

noted in connection with Corollary (3.8) this normal closure is isomorphic with $\hat{F}_\omega$ if the profinite group $\langle \sigma, \tau \rangle$ is free on σ, τ. But this is the case for almost all $(\sigma, \tau) \in G^2$, see (4.2). □

(4.8) We conclude with indicating which profinite groups occur as absolute Galois groups of PAC-fields. This was initially the motivating question for our work. As it turned out, the answer we give here is easily obtained by combining some results scattered in the literature.

PROPOSITION. *The following are equivalent for a profinite group G.*

(1) *G is isomorphic with a subgroup of a free profinite group.*

(2) $\mathrm{cd}(G) \leqq 1$.

(3) *G is projective (in the category of profinite groups).*

(4) $G \simeq G(K)$ *for some* PAC*-field K.*

PROOF. (1) $\Rightarrow$ (2) is well known and due to Tate. (2) $\Rightarrow$ (3) is proved by Gruenberg in [8]. (3) $\Rightarrow$ (1) follows because every profinite group, in particular G, is the homomorphic image of a free profinite group, a (non-obvious) fact proved by Douady in [5].

We have now shown the equivalence of (1), (2) and (3). (4) $\Rightarrow$ (2) is due to Ax, [2]; see also lemma 2.1 of [9] for the non-perfect case. (1) $\Rightarrow$ (4): clearly we have only to show that for each cardinal κ there is a PAC-field K such that $G(K) \simeq \hat{F}_\kappa$, $\hat{F}_\kappa$ being the free profinite group on a set of cardinality κ. For $\kappa \leqq \aleph_0$, see (4.2) and (4.4).

Suppose $\kappa > \aleph_0$. Now Jarden's lemma (2.3) in [11] easily implies that there is a perfect PAC-field K and a Galois extension $L \mid K$ such that $\mathrm{Gal}(L \mid K) \simeq \hat{F}_\kappa$. So $\hat{F}_\kappa$ is a homomorphic image of $G(K)$. Because $\hat{F}_\kappa$ is projective, this implies that $\hat{F}_\kappa$ is also isomorphic with a subgroup of $G(K)$, hence $\hat{F}_\kappa \simeq G(K')$ for some separable algebraic extension K' of K. Then K' is a PAC-field as required. □

Note added in proof. Ralph Strebel answered Question 2 in §2 in the affirmative.

ACKNOWLEDGEMENTS

The authors would like to thank Angus Macintyre for many stimulating discussions.

This work was partially done while the first author was visiting Yale University, which he wants to thank for its invitation and its warm hospitality.

REFERENCES

1. M. P. Anderson, *Exactness properties of profinite completion functors*, Topology **13** (1974), 229–239.

2. J. Ax, *The elementary theory of finite fields*, Ann. of Math. **88** (1968), 239–271.

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

4. I. M. Chiswell, *Euler characteristics of groups*, Math. Z. **147** (1976), 1–11.

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

6. L. van den Dries, *Decidable PAC-fields of algebraic numbers*, in preparation.

7. D. Gildenhuys and C. Lim, *Free pro-$\mathscr{C}$-groups*, Math. Z. **125** (1972), 233–254.

8. K. W. Gruenberg, *Projective profinite groups*, J. London Math. Soc. **42** (1967), 155–165.

9. M. Jarden, *Elementary statements over large algebraic fields*, Trans. Amer. Math. Soc. **164** (1972), 67–91.

10. M. Jarden, *Algebraic extensions of finite corank of hilbertian fields*, Israel J. Math. **18** (1974), 279–307.

11. M. Jarden, *The elementary theory of ω-free Ax fields*, Invent. Math. **38** (1976), 187–206.

12. M. Jarden, *Intersections of conjugate fields of finite corank over hilbertian fields*, J. London Math. Soc. **53** (1978), 393–396.

13. M. Jarden, *An analogue of Cebotarev density theorem for fields of finite corank*, preprint.

14. M. Jarden and U. Kiehne, *The elementary theory of algebraic fields of finite corank*, Invent. Math. **30** (1975), 275–294.

15. A. Lubotzky, *On the non-congruence structure of* SL_2, in preparation.

16. A. Lubotzky, *Combinatorial group theory for pro-p-groups*, in preparation.

17. R. C. Lyndon and P. E. Schupp, *Combinatorial Group Theory*, Springer-Verlag, Berlin–Heidelberg–New York, 1977.

18. R. C. Oltikar and L. Ribes, *On the Frattini subgroup of free products of profinite groups*, Comm. Algebra **7** (3) (1979), 313–325.

19. L. Ribes, *Introduction of profinite groups and Galois cohomology*, Queens papers in pure and applied mathematics, no. 24 (1970).

20. J.-P. Serre, *Sur la dimension cohomologique des groupes profinis*, Topology **3** (1975), 413–420.

DEPARTMENT OF MATHEMATICS
BAR-ILAN UNIVERSITY
RAMAT GAN, ISRAEL

DEPARTMENT OF MATHEMATICS
YALE UNIVERSITY
NEW HAVEN, CT 06520 USA