HILBERTIAN FIELDS AND FREE PROFINITE GROUPS*

by

Moshe Jarden, Tel Aviv University

and

Alexander Lubotzky, The Hebrew University in Jerusalem

Journal of the London Mathematical Society (2) **46** (1992), 205–227

* Partially supported by grants from the G.I.F., the German–Israeli Foundation for Scientific Research and Development.

Introduction

Readers of Field Arithmetic [FJ], may observe interesting interrelations between two major concepts of the book, the free profinite group $\widehat{F}_\omega$ of rank $\aleph_0$, on one hand, and Hilbertian fields on the other hand. There is an analogy between various results on closed subgroups of $\widehat{F}_\omega$ and algebraic extensions of Hilbertian fields. Results of Melnikov [M1] even extend this analogy to the free profinite group $\widehat{F}_m$ of arbitrary infinite rank m. In this paper we try to make this analogy precise by formulating a "twinning scheme" of pairs of results on closed subgroups of $\widehat{F}_m$ on one hand and algebraic extensions of Hilbertian fields on the other hand. For special class of Hilbertian fields, namely the "ω-free PAC fields of characteristic 0" on one hand and for $\widehat{F}_\omega$ on the other hand the twinning scheme becomes a theorem which we call the "weak twinning principle". In the general case, we prove new results on closed subgroups of free profinite groups which are suggested by known results on Hilbertian fields and fall into the twinning scheme. We also go in the other direction – from groups to fields. The reason for the general phenomenon is still unclear.

Let us explain all these in details. We say that a subset X of a profinite group F **converges to** 1 if each open subgroup of F contains all but finitely many elements of X. In this case, F is the **free profinite group with basis** X, if each map f of X into a profinite group G such that $f(X)$ converges to 1 uniquely extends to a homomorphism of F into G. The cardinality of X is called the **rank** of F. If X is infinite, then $\mathrm{rank}(F)$ is also the cardinality of the family of all open subgroups of F [FJ, Supplement 15.12]. For free F, the rank uniquely determines F up to an isomorphism. In particular, if $\mathrm{rank}(F) = m$, then we denote F by $\widehat{F}_m$. It is the **free profinite group of rank** m. In the special case where $\mathrm{rank}(F) = \aleph_0$, we denote F by $\widehat{F}_\omega$.

A field K is said to be **Hilbertian** if for all irreducible polynomials $f_1, \ldots, f_s \in K[T_1, \ldots, T_r, X]$ and nonzero $g \in K[T_1, \ldots, T_r]$ there exist $a_1, \ldots, a_r \in K$ such that $f_j(a_1, \ldots, a_r, X)$ is irreducible in $K[X]$, $j = 1, \ldots, s$, and $g(a_1, \ldots, a_r) \neq 0$.

The field K is **separably Hilbertian** if the above condition holds only for irreducible polynomials $f_1, \ldots, f_s$ which are separable in X. A field K is Hilbertian if and only if K is separably Hilbertian and, in case $\mathrm{char}(K) > 0$, K is nonperfect [FJ, Prop. 11.16]. As we deal mainly with separable extensions, we formulate our results for Hilbertian fields. However, they also remain valid, possibly with little modifications, for separable Hilbertian fields.

The classical Hilbertian fields are $\mathbb{Q}$ and fields of rational functions over any field [FJ, Chap. 12]. Other basic Hilbertian fields are the fields of formal power series in at least two variables over any field. More Hilbertian fields are obtained from basic Hilbertian fields as suitable algebraic extensions, as stated below.

Denote the absolute Galois group of a field K by $G(K)$. Suppose that PG is a property of closed subgroups of profinite groups. We denote the Galois theoretic counterpart of PG by PF. This means that if L is a algebraic extension of a field K, then L/K has the property PF if the closed subgroup $G(L)$ of $G(K)$ has the property PG. For example, L/K is a Galois extension, if $G(L)$ is a normal subgroup of $G(K)$.

Suppose that m is an infinite cardinal number. Various results on separable algebraic extensions of Hilbertian fields on one hand and on subgroups of $\widehat{F}_m$ on the other hand can be assembled as twinning results in the following manner:

(G) If a closed subgroup H of $\widehat{F}_m$ has the property PG, then $H \cong \widehat{F}_m$.

(F) If a separable algebraic extension L of a Hilbertian field K has property PF, then L is Hilbertian.

Thus, given a (G) statement, you get the corresponding (F) statement as follows: Replace "the subgroup has the property PG" by "the field has the property PF" and "the subgroup is isomorphic to $\widehat{F}_m$" by "the field is Hilbertian", and vica versa from (F) to (G).

We list several statements which fall into this **twinning scheme** and are known to be true.

(G1) Every open subgroup of $\widehat{F}_m$ is isomorphic to $\widehat{F}_m$ [FJ, Prop. 15.27].

(F1) Every finite separable extension of a Hilbertian field is Hilbertian [FJ, Cor. 11.7].

(G2) Every normal subgroup N of $\widehat{F}_m$ such that $\widehat{F}_m/N$ is finitely generated is isomorphic to $\widehat{F}_m$ [M1, Prop. 2.1].

(F2) Every Galois extension N of a Hilbertian field K such that $\mathcal{G}(N/K)$ is finitely generated is Hilbertian [FJ, Prop. 15.5].

(G3) Every proper open (resp., and normal) subgroup of a closed normal subgroup of $\widehat{F}_\omega$ (resp., $\widehat{F}_m$) is isomorphic to $\widehat{F}_\omega$ (resp., $\widehat{F}_m$) [FJ, Prop. 24.7] (resp., [M1, Thm. 3.4]).

(F3) Every proper finite separable extension of a Galois extension of a Hilbertian field is Hilbertian [FJ, Cor. 12.15].

(G4) Every closed normal subgroup N of $\widehat{F}_m$ such that $\widehat{F}_m/N$ is abelian is isomorphic to $\widehat{F}_m$ (a corollary of [M1, Lemma 2.7 and Thm. 3.1]. See also [LD, Cor. 3.9(i)] for the case $m = \aleph_0$.)

(F4) Every abelian extension of a Hilbertian field is Hilbertian [FJ, Thm. 15.6].

Note that Theorem G3 deviates somewhat from the twinning scheme in the uncountable case in that it restricts the open subgroup of the normal closed subgroup of $\widehat{F}_m$ to be normal. In Section 2 we bring G3 into a line with the other (Gn)'s. We prove:

(G3′) Every open proper subgroup of a closed normal subgroup of $\widehat{F}_m$ is isomorphic to $\widehat{F}_m$.

Here are another two interesting field theoretic results:

(F5) The compositum of two Galois extensions of a Hilbertian field K, neither of which contains the other is Hilbertian [HJ].

(F6) If L is an algebraic extension of a Hilbertian field K whose degree is divisible by at least two primes and L is contained in a pronilpotent extension N of K, then L is Hilbertian [U, Thm. 3].

The twinning scheme suggests analogous results about $\widehat{F}_m$ which we indeed prove in Section 1 and Section 4.

(G5) The intersection of any two closed normal subgroups of $\widehat{F}_m$ neither of which contains the other is isomorphic to $\widehat{F}_m$.

(G6) Let M be a closed subgroup of $\widehat{F}_m$ whose index is divisible by at least two distinct primes. If M contains a closed normal subgroup N of $\widehat{F}_m$ such that $\widehat{F}_m/N$ is pronilpotent, then M is isomorphic to $\widehat{F}_m$.

Actually, we prove (G5) and (G6) with the close "is isomorphic to $\widehat{F}_m$" replaced by "is a free profinite group" also for the case where $2 \le m < \aleph_0$. The main tool to handle the case of finite rank is the Nielsen – Schreier formula for the rank of an open subgroup E of F. In the infinite case, in particular in the uncountable case, we replace this formula by an explicit knowledge of a special basis Y for E which is constructed out of a basis X for F in [FJ, Section 15.7]. We also exploit methods and results of Melnikov [M1 and M2].

In the other direction we mention the following group theoretic result:

(G7) Let H be a closed subgroup of $\widehat{F}_m$ with index $(\widehat{F}_m : H) = \prod p^{\alpha(p)}$ where all $\alpha(p)$ are finite. Then H is isomorphic to $\widehat{F}_m$ [LD, 3.15].

A standard argument (Section 5) proves the analogous result which is predicted by the twinning scheme:

(F7) Let L be an algebraic separable extension of a Hilbertian field K of degree $\prod p^{\alpha(p)}$, with all $\alpha(p)$ finite. Then L is Hilbertian.

In addition, we mention in Section 5 some results about subgroups of free profinite groups whose analog for extensions of Hilbertian fields have never been considered. We leave them as open problems.

Although some of the group theoretical ingredients of the proofs of theorems (Gn) enter into the proofs of theorems (Fn), it is difficult to see a real analogy between the proofs of the group theoretic theorems and those of field theory. So, we do not know if the following "twinning principle" is true:

TWINNING PRINCIPLE: *Let m be an infinite cardinal. The following statements are equivalent:*

(G) *If a closed subgroup H of $\widehat{F}_m$ has the property* PG*, then $H \cong \widehat{F}_m$.*

(F) *If a separable algebraic extension L of a Hilbertian field K has the property* PF*, then L is Hilbertian.*

A partial evidence to the correctness of the twinning principle emerges in the countable case. If we restrict statement (G) to the case $m = \aleph_0$ it becomes equivalent to statement (F) on special Hilbertian fields, namely the ω-free PAC fields (Proposition

B). Here a field K is said to be **PAC** if every absolutely irreducible variety V defined over K has a K-rational point. The field K is **ω-free** if each finite embedding problem for $G(K)$ has a solution. That is, given a finite Galois extension L of K and an epimorphism $\alpha\colon B \to \mathcal{G}(L/K)$ from a finite group G there exists an epimorphism $\gamma\colon G(K) \to B$ such that $\alpha \circ \gamma = \mathrm{res}_L$. In case K is countable, it is ω-free if and only if $G(K) \cong \widehat{F}_\omega$ [FJ, Cor. 24.2].

THEOREM (Weak twinning principle): *The following statements are equivalent:*

(G_0) *If a closed subgroup H of $\widehat{F}_\omega$ has the property* PG, *then $H \cong \widehat{F}_\omega$.*

(F_0) *If a separable algebraic extension L of a countable ω-free PAC field K (which is nonperfect if* $\mathrm{char}(K) > 0$*) has the property* PF, *then L is Hilbertian.*

The proof of the Theorem is based on three results:

PROPOSITION A (Ax – Roquette [FJ, Cor. 10.7]): *Every algebraic extension of a PAC field is PAC.*

PROPOSITION B (Roquette [FJ, Cor. 24.38]): *Every ω-free PAC field of characteristic 0 is Hilbertian.*

PROPOSITION C (Fried – Völklein [FV, Thm. A]): *If K is a Hilbertian PAC field of characteristic 0, then K is ω-free.*

Proof of the Theorem: Suppose that G_0 is true. Let L be as in (F_0). In particular L has the property PF and therefore $G(L)$ has the property PG. By (G_0), $G(L) \cong \widehat{F}_\omega$. Also, by Proposition A, L is PAC. Hence, by Proposition B, L is Hilbertian.

Now suppose that (F_0) is true. Let H be a closed subgroup of $\widehat{F}_\omega$ which has property PG. By [FJ, Example 24.39], there exists a countable ω-free PAC field K of characteristic 0. In particular $G(K) = \widehat{F}_\omega$. Let L be the fixed field of H in the algebraic closure $\widetilde{K}$ of K. Then L has property PF. By (F_0), L is Hilbertian. As L is also PAC, Proposition (C) implies that $H \cong \widehat{F}_\omega$, as desired. ∎

The weak twinning principle reduces the group theoretic theorems (G5) and (G6) in the case where $m = \aleph_0$ to the known field theoretic results (F5) and (G6). Note however, that the proof of the twinning principle is based on the deep work of Fried and Völklein (Proposition C). This work uses complex analysis and in particular the Riemann existence theorem. The proofs of (G5) and (G6), which we give below use only group theoretic tools and work for general m.

Acknowledgement: We thank E. Rips for his help in understanding [M2].

1. Intersections of normal subgroups of free profinite groups.

The goal of this section is to prove Theorem G5 of the introduction for $\widehat{F}_m$. We also prove the corresponding theorem in the case where $2 \le m < \aleph_0$. In this case we achieve our goal by using the Nielsen – Schreier formula and tools from [LD] and [FJ]. The case with uncountable rank is more complicated. We have to use the notion of "free pro–Δ–group" developed by Melnikov in [M1] and in particular Theorem 4.1 of [M1]. So, we prove the theorem in the framework of Melnikov's notion of freeness which generalizes the one defined in [FJ] for full families. In order to bring the two notions in line we have changed Melnikov's notation and speak about "free pro–$\mathcal{D}$–group" instead of "free pro–Δ–group":

Let $\mathcal{D}_0$ be a nonempty family of finite simple groups. Denote the family of all finite groups whose composition factors belong to $\mathcal{D}_0$ by $\mathcal{D}$. We call $\mathcal{D}$ a **quasi full family** generated by $\mathcal{D}_0$. Each member of $\mathcal{D}$ is called a $\mathcal{D}$**–group**. An inverse limit of $\mathcal{D}$–groups is a **pro–**$\mathcal{D}$**–group**.

Consider the free discrete group F_0 generated by a set X. Let $\mathcal{N}$ be the collection of all normal subgroups N of F that contain almost all elements of X such that $F/N \in \mathcal{D}$. The profinite completion F of F_0 with respect to $\mathcal{N}$ is the **free pro–**$\mathcal{D}$ **group with basis** X. In particular X converges to 1 and each map f of X into a pro–$\mathcal{D}$–group G for which $f(X)$ also converges to 1 uniquely extends to a homomorphism of F into G [M1, Lemma 2.1]. Thus F is uniquely determined up to isomorphism by the cardinality of X, which is at the same time the rank of F. So, if this rank is m we denote F also by $\widehat{F}_m(\mathcal{D})$.

Note that $\mathcal{D}$ is closed under taking normal subgroups, quotients, and extensions. Conversely, if $\mathcal{C}$ is such a family, and $\mathcal{C}_0$ is the family of all compositions factors of $\mathcal{C}$–groups, then $\mathcal{C}$ is the family of all finite groups whose decomposition factors belong to $\mathcal{C}_0$. In particular this is the case if $\mathcal{C}$ is a **full family**, i.e., $\mathcal{C}$ is closed under taking subgroups, quotients, and extensions [FJ, p. 189]. Thus, some of the results below will be generalizations of results for full families which appear in [FJ] or in [LD].

Throughout this work we fix $\mathcal{D}_0$ and $\mathcal{D}$ as above, reserve the letter m to denote a cardinal number, and let $F = \widehat{F}_m(\mathcal{D})$.

Let G be a profinite group and S a finite simple group. Denote the intersection of all open normal subgroups N of G such that $G/N \cong S$ by $M_S(G)$. By [M1, Lemma 1.3], $G/M_S(G) \cong S^I$ for some set I. We denote the cardinality of I by $r_S(G)$.

Here are some results on F due to Melnikov which are needed in the proof.

Proposition 1.1: *The following statements hold for a nontrivial closed normal subgroup N of F:*

(a) [M1, Prop. 2.1(a)] *If $m = e$ is a positive integer, and $(F : N) = n$, then N is a free pro–$\mathcal{D}$–group of rank $1 + n(e - 1)$.*

(b) [M1, Thm. 3.4] *If $m \geq 2$ and K is a proper open normal subgroup of N, then K is a free pro–$\mathcal{D}$–group. If $(F : K) = \infty$ or m is infinite, then* $\mathrm{rank}(K) = \max\{\aleph_0, m\}$.

(c) [M1, Prop. 3.2] *If $m \geq 2$, then F is not a nontrivial direct product of two profinite groups.*

(d) [M1, Prop. 3.3] *If $m \geq 2$, then the center of F is trivial.*

(e) [M1, Thm. 2.1(b)] *If m is infinite and N is open, then $N \cong F$.*

(f) [M1, Thm. 3.2 and statement at the bottom of page 9] Suppose that m is infinite. For each $S \in \mathcal{D}_0$ we have $r_S(N) \leq r_S(F) = m$.

(g) [M1, Thm. 3.1] If m is infinite and N' is another closed normal subgroup of F such that $r_S(N) = r_S(N')$ for each $S \in \mathcal{D}$, then $N \cong N'$. In particular, if $r_S(N) = m$ for each $S \in \mathcal{D}_0$, then $N \cong F$.

(h) [M1, Thm. 4.1] Suppose that m is infinite. Consider the family $\mathcal{E}_0 = \{S \in \mathcal{D}_0 |\ r_S(N) < m\}$, let $\mathcal{E}$ be the family of all finite groups whose decomposition factors belong to $\mathcal{E}_0$, and let M be the intersection of all open normal subgroups K of F which contain N such that F/K is an $\mathcal{E}$–group. If $\mathcal{E}_0$ is nonempty, then $F/M \cong \widehat{F}_m(\mathcal{E})$.

Recall that a profinite group G has the **embedding property** if for each finite quotient B of G and for each pair of epimorphisms ($\varphi\colon G \to A$, $\alpha\colon B \to A$) there exists an epimorphism $\gamma\colon G \to B$ such that $\alpha \circ \gamma = \varphi$.

LEMMA 1.2: *Let N be a closed normal subgroup of F.*

(a) *N has the embedding property.*

(b) *If $m \le \aleph_0$ and each $\mathcal{D}$–group is a quotient of N, then $N \cong \widehat{F}_\omega(\mathcal{D})$.*

Proof of (a): Suppose first that $N = F$. If m is finite, then the statement follows from the Gaschütz lemma as in [FJ, Prop. 15.31]. If m is infinite, repeat the proof of [FJ, Lemma 23.7].

If N is open, then, by Proposition 1(a,b), N is $\mathcal{D}$–free and therefore has the embedding property.

The general case is now a consequence of [FJ, Lemma 24.3].

Proof of (b): Both N and $\widehat{F}_\omega(\mathcal{D})$ have the embedding property, are of rank at most $\aleph_0$, and have the same finite quotients. By [FJ, Lemma 24.1], $N \cong F_\omega(\mathcal{D})$.

Let G be a profinite group. We say that G **satisfies the eth Nielsen – Schreier formula** if

$$\mathrm{rank}(H) = 1 + (G : H)(e - 1)$$

for each open subgroup H of G. In particular this formula implies for $H = G$ that $\mathrm{rank}(G) = e$.

The following Lemma generalizes Lemma 24.6 of [FJ].

LEMMA 1.3: *Suppose that $m = e \ge 2$ is finite let N be a closed normal subgroup of F of infinite index. If F/N does not satisfy the eth Nielsen – Schreier formula, then $N \cong F$.*

Proof: By Lemma 1.2(b), it suffices to prove that each $\mathcal{D}$–group G is a quotient of N.

By assumption, F has an open subgroup H that contains N such that

$$\mathrm{rank}(H/N) < 1 + (F : H)(e - 1) \tag{1}$$

Also, H has an open normal subgroup E that contains N such that $(H:E) \geq \mathrm{rank}(G)$. By [FJ, Cor. 15.28], $\mathrm{rank}(E/N) \leq 1+(H:E)(\mathrm{rank}(H/N)-1)$. From (1), $\mathrm{rank}(H/N) \leq (F:H)(e-1)$. Hence $\mathrm{rank}(E/N) \leq 1+(F:E)(e-1)-(H:E)$. By Proposition 1.1(a),

$$\mathrm{rank}(E) = 1+(F:E)(e-1) \geq \mathrm{rank}(E/N)+\mathrm{rank}(G) \geq \mathrm{rank}((E/N)\times G).$$

Moreover, In particular, as E is $\mathcal{D}$–free, $(E/N)\times G$ is a quotient of E.

Let $\pi\colon E \to E/N$ be the canonical map. Let $\alpha\colon (E/N)\times G \to E/N$ be the projection on the first factor. By Lemma 1.2(a), there exists an epimorphism $\gamma\colon E \to (E/N)\times G$ such that $\alpha\circ\gamma = \pi$. In particular $\gamma(N) = 1\times G$ and G is therefore a quotient of N, as claimed. ∎

The following Lemma generalizes Cor. 3.9(h) of [LD].

Lemma 1.4: *Suppose that $2 \leq m \leq \aleph_0$. If N is a closed normal subgroup of F of infinite index such that F/N is abelian, then $N \cong \widehat{F}_\omega(\mathcal{D})$.*

Proof: Consider first the case where $m = e$ is finite. Then $A = F/N$ is a finitely generated infinite abelian group. Therefore there exists a prime p such that $1 < (A:A^p) < \infty$. Also, $\mathrm{rank}(A^p) \leq \mathrm{rank}(A) \leq e < 1+(A:A^p)(e-1)$. Hence, A is not e–freely indexed. By Lemma 1.3, $N \cong \widehat{F}_\omega(\mathcal{D})$.

Now consider the case where $m = \aleph_0$. By Lemma 1.2(b) it suffices to prove that each $\mathcal{D}$–group G is a quotient of N. Indeed, take an epimorphism $\varphi\colon F \to \overline{F} = \widehat{F}_e(\mathcal{D})$ with $e \geq \mathrm{rank}(G)$. Then $\overline{F}/\varphi(N)$ is abelian. If $(\overline{F}:\varphi(N))$ is finite, then $\varphi(N)$ is $\mathcal{D}$–free of rank at least e (Prop. 1(a)). If $(\overline{F}:\varphi(N)) = \infty$, then $\varphi(N) \cong \widehat{F}_\omega(\mathcal{D})$, by the preceding paragraph. In both cases G is a quotient of $\varphi(N)$ and therefore also of N. ∎

Lemma 1.5 ([L, Lemma 2.2]): *Let G be a direct product of nontrivial profinite groups M and N. Then G satisfies the eth Nielsen – Schreier formula for no $e > 1$.*

Lemma 1.6: *Let $G = K \times L$ be a direct product of profinite groups K and L, and let $\varphi\colon G \to \overline{G}$ be an epimorphism. Then $A = \varphi(K)\cap\varphi(L)$ lies in the center of $\overline{G}$. In particular A is an abelian group.*

Proof: We have $xy = yx$ for each $x \in K$ and $y \in L$. Hence, each $a \in A$ satisfies $az = za$ for each $z \in \varphi(K)$ and for each $z \in \varphi(L)$ and therefore also for each $z \in \varphi(K)\varphi(L) = \overline{G}$. ∎

The case $m = \aleph_0$ is covered twice in the proof of the following lemma. We have chosen to include the first proof because it uses lighter machinery than the second, which covers the more general case $m \geq \aleph_0$.

LEMMA 1.7: *Suppose that $m \geq 2$. Let K and L be closed normal subgroups of F neither of which contains the other. Suppose that both K and L are isomorphic to F and that $KL = F$. Then $N = K \cap L$ is $\mathcal{D}$–free.*

Proof: Suppose first that $m = e$ is finite. By Lemma 1.5, F/N, which is the direct product of K/N and L/N is not e–freely indexed. Hence, by Proposition 1.1(a) and Lemma 1.3, N is $\mathcal{D}$–free.

Secondly, let $m = \aleph_0$. By Lemma 1.2(b) it suffices to prove that each $\mathcal{D}$–group G is a quotient of N. Indeed, choose an integer $e \geq \max\{2, \mathrm{rank}(G)\}$ and an epimorphism φ: $F \to \overline{F} = \widehat{F}_e(\mathcal{D})$ such that none of the groups $\overline{K} = \varphi(K)$ and $\overline{L} = \varphi(L)$ contains the other. As $\overline{KL} = \overline{F}$, we conclude from the first paragraph that $E = \overline{K} \cap \overline{L}$ is $\mathcal{D}$–free with rank at least e. Let $\overline{N} = \varphi(N)$. By Lemma 1.6, $E/\overline{N}$ is abelian. Hence, by Proposition 1.1(a) and Lemma 1.4, $\overline{N}$ is $\mathcal{D}$–free of rank at least e. In particular G is a quotient of $\overline{N}$ and therefore also a quotient of N, as desired.

Finally suppose that $m \geq \aleph_0$. Consider the family $\mathcal{E}_0 = \{S \in \mathcal{D}_0 |\ r_S(N) < m\}$. If $\mathcal{E}_0$ is empty, then $r_S(N) = m = r_S(F)$ for each $S \in \mathcal{D}$ (Proposition 1.1(f)). Hence, by Proposition 1.1(g), $N \cong F$.

So, assume that $\mathcal{E}_0$ is nonempty and draw a contradiction. To that end, let $\mathcal{E}$ be as in 1.1(h), and let M be the intersection of all open normal subgroups F_0 of F which contain N such that $F/F_0 \in \mathcal{E}$. By Proposition 1.1(h), $\overline{F} = F/M \cong \widehat{F}_m(\mathcal{E})$. Let $\overline{K} = KM/M$ and $\overline{L} = LM/M$. By Lemma 1.6, $\overline{K} \cap \overline{L}$ lies in the center of $\overline{F}$. Hence, by Proposition 1.1(d), $\overline{K} \cap \overline{L} = 1$. As $\overline{KL} = \overline{F}$, this means that $\overline{F} = \overline{K} \times \overline{L}$. But this contradicts Proposition 1.1(c) unless the factorization is trivial. So, say, $\overline{K} = 1$ and therefore $KM = M$. Conclude that $K \leq M$. In particular F/L has no nontrivial quotients which belong to $\mathcal{E}$.

Now choose $S \in \mathcal{E}_0$. Since $K \cong \widehat{F}_m(\mathcal{D})$, we have $K/M_S(K) \cong S^m$, by Proposition 1.1(g). Also, observe that $K/M_S(K)N \cong F/M_S(K)L$ is an $\mathcal{E}$–group. Hence $M_S(K)N = K$. It follows that $N/(M_S(K) \cap N) \cong K/M_S(K)N \cong S^m$ and therefore $r_S(N) \geq m$. This contradicts the choice of S, as desired. ∎

Lemma 1.8: *Let N be a closed nontrivial normal subgroup of F. If $m \geq 2$ and $(F : N) = \infty$, or $m \geq \aleph_0$, then* $\mathrm{rank}(N) = \max\{\aleph_0, m\}$.

Proof: By assumption N has a proper open normal subgroup K. By Proposition 1.1(b), $\mathrm{rank}(N) = \mathrm{rank}(K) = \max\{\aleph_0, m\}$. ∎

Theorem 1.9: *Suppose that $m \geq 2$. Let K and L be closed normal subgroups of $F = \widehat{F}_m(\mathcal{D})$ neither of which contains the other. Then $N = K \cap L$ is $\mathcal{D}$–free. If $(F : K) = \infty$, or $(F : L) = \infty$, or $m \geq \aleph_0$, then* $\mathrm{rank}(N) = \max\{\aleph_0, m\}$, *otherwise* $\mathrm{rank}(N) = 1 + (F : N)(m - 1)$.

Proof: Lemma 1.8 gives the assertion about the ranks. So, all we have to prove is that N is $\mathcal{D}$–free.

If $(F : K) < \infty$, then N is open in L, and therefore, by Proposition 1.1(b), N is $\mathcal{D}$-free. The same consequence holds if $(F : L) < \infty$. So, we may assume that $(F : K) = \infty$ and $(F : L) = \infty$.

By assumption K has a proper open normal subgroup K_1 that contains N and L has a proper open normal subgroup L_1 that contains N. By Proposition 1.1(b), both K_1 and L_1 are $\mathcal{D}$–free. As $F_1 = K_1 L_1$ is a proper open normal subgroup of KL it is $\mathcal{D}$–free. By Lemma 1.8, each of the groups F_1, K_1 and L_1 is isomorphic to $\widehat{F}_\omega(\mathcal{D})$ if $m \leq \aleph_0$ and to F if $m \geq \aleph_0$.

If $K_1 = N$ or $L_1 = N$, then, by Proposition 1.1(b), N is $\mathcal{D}$–free. So, assume that N is a proper subgroup of both K_1 and L_1. Thus, neither of the groups K_1 and L_1 contains the other. Apply Lemma 1.7 to F_1, K_1 and L_1 instead of F, K and L to conclude that N is $\mathcal{D}$–free. ∎

Corollary 1.10: *Suppose that N is a closed normal subgroup of F such that F/N is* *a pronilpotent group whose order is divisible by at least two distinct primes. Then N is $\mathcal{D}$–free.*

Proof: : The group F/N is the direct product of its Sylow subgroups. ∎

Theorem 4.1 generalizes Corollary 1.10 considerably.

2. Open subgroups of closed normal subgroups of free profinite groups.

Theorem G3 of the introduction contains two statements:

(1a) Every proper open subgroup M of a closed normal subgroup N of $\widehat{F}_\omega$ is isomorphic to $\widehat{F}_\omega$, and

(1b) if $m \geq \aleph_0$, then every proper open normal subgroup M of a closed normal subgroup N of $\widehat{F}_m$ is isomorphic to $\widehat{F}_m$.

None of these statements covers the case where $m > \aleph_0$ and M is not necessarily normal in N. The goal of this section is to fill up this gap and to prove that also in this case M is isomorphic to $\widehat{F}_m$. We do this in the more general framework of pro-$\mathcal{D}$-groups where $\mathcal{D}$ is a full family or a quasi full family of finite groups. The main step in the proof is the following result, which has also an independent application in the proof Theorem 4.1.

Proposition 2.1: *Let $\mathcal{D}_0$ be a nonempty family of finite simple groups, $\mathcal{D}$ the quasi full family generated by $\mathcal{D}_0$, m an infinite cardinal, $F = \widehat{F}_m(\mathcal{D})$, and N a closed normal subgroup of F. If $\mathcal{D}$ is a full family, suppose that E is an open proper subgroup of F such that $NE = F$. If $\mathcal{D}$ is only quasi full, assume, in addition, that E is normal. In both cases let $M = N \cap E$. Then, for each $S \in \mathcal{D}_0$, E has a closed normal subgroup D such that $E/D \cong S^m$ and $MD = E$.*

The proof of this Proposition naturally splits into two cases. Lemma 2.3 handles the case where S is nonabelian. Lemma 2.4 takes care of the abelian case. In both cases we use Proposition 15.27 of [FJ] which states that $E \cong \widehat{F}_m(\mathcal{D})$. Moreover, the proof of this proposition construct a basis Y of E with special properties from a basis X of F:

Lemma 2.2: *let X be a basis for F. Then there exists a function ρ: $F \to F$ such that*

(2a) $\rho(1) = 1$,

(2b) *$R = \rho(F)$ is a set of representatives for the left cosets of F modulo E,*

(2c) *the set $\Gamma = \{(r,x) \in R \times X \mid \rho(rx) = rx\}$ is finite,*

(2d) *with $y_{r,x} = rx\rho(rx)^{-1}$ for $(r,x) \in R\times X - \Gamma$, the map $(r,x) \mapsto y_{r,x}$ maps $R\times X-\Gamma$ bijectively onto a basis Y of E, and*

(2e) *if an element $x \in X$ belongs to a normal subgroup N of F which is contained in E, then $y_{r,x} = rxr^{-1}$ for each $r \in R$.*

Proof: Let F_0 be the free discrete subgroup generated by X. Then F is the completion of F_0 with respect to the family of all normal subgroups N of F_0 which contain almost all elements of X. Moreover, the canonical map of F_0 into F identifies F_0 with a dense subgroup of F [M1, Lemma 2.5]. Also, there exists subgroup E_0 of index $(F : E)$ such that E is the closure of E_0 in F [FJ, Lemma 15.14]. Each representative system of F_0/E_0 is also a representative system of F/E. If $\mathcal{D}$ is only quasi full, then E_0 is normal.

By [FJ, Lemmas 15.21] there exists a function ρ_0: $F_0 \to F_0$ such that $\rho_0(1) = 1$, $\rho(f) \in Hf$, and $\rho_0(ef) = \rho(f)$ for each $e \in E_0$ and $f \in F_0$, and finally ρ_0 satisfies condition (5) on page 192 of [FJ]. By [FJ, Lemmas 15.22 and 15.23] the map $(r,x) \mapsto y_{r,x}$ maps $R\times X-\Gamma$ bijectively onto a basis Y of E_0. Moreover, if an element $x \in X$ belongs to a normal subgroup N of F_0 which is contained in E_0, then $y_{r,x} = rxr^{-1}$ for each $r \in R$.

Proposition 15.25 of [FJ] handles only the case where X is finite. However, that part of its proof which states that Γ is finite depends only on the finiteness of R and not on that of X (Note that proof uses the letter N for what we call here Γ.)

The proof of Proposition 15.27 of [FJ] shows that Y is a basis of E in the profinite sense. Note that although that proof is carried out for full families, its proof remains valid also for quasi full families. In the latter case we have to use that $E_0 = F_0 \cap E$ is normal in F_0.

Finally, we may extend ρ_0 to a function ρ: $F \to F$ as follows: For each $f \in F$ we define $\rho(f)$ to be the unique element $r \in R$ such that $r \in Ef$. Then Condition (2) holds. ∎

Lemma 2.3: *Under the assumption of Proposition 2.1, suppose that S is nonabelian.*

Then E has a closed normal subgroup D such that $E/D \cong S^m$ and $MD = E$.

Proof: Let X be a basis for F, and let ρ, R, Γ, $y_{r,x}$, and Y be as in Lemma 2.2. Choose an open normal subgroup E_1 of F which is contained in E. In particular $y_{r,x} = rxr^{-1}$ if $x \in E_1$. Let X_0 be the set of all $x \in X$ for which there exists $r \in R$ such that $(r,x) \in \Gamma$ or $x \notin E_1$. Then X_0 is finite. Let $X_1 = X - X_0$.

Choose a set of epimorphisms $\{\varphi_i\colon F \to S \mid i \in I\}$ with an index set I which contains neither 0 nor 1 such that for each open normal subgroup L of F with $F/L \cong S$ there exists a unique $i \in I$ with $L = \mathrm{Ker}(\varphi_i)$. Then $|I| = m$. For each $i \in I$ denote the restriction of φ_i to E by ψ_i.

For each $i \in I$ let $X_i = X_1 - \mathrm{Ker}(\varphi_i)$. Since X_0 is finite, I has a subset I_1 of cardinality m such that $X_i \subseteq E_1$ for each $i \in I_1$. Indeed, choose a system of generators S_0 for S none of which is 1. There are m subsets A of X_1 with cardinality $|S_0|$. For each such A define an epimorphism of F onto S which maps $X - A$ onto 1 and A onto S_0. The cardinality of the set of kernels of the epimorphisms defined in this way is m. This gives the subset I_1 of I.

Each φ_i is determined by its values on $X_0 \cup X_i$. There are only finitely many possibilities for them. Thus if we define two elements i and j of I_1 to be equivalent if $X_i = X_j$, then each equivalent class is finite. Choose a system of representatives I_2 for the equivalence classes. Then $|I_2| = m$.

For each $i \in I_2$ and each $x \in X_i$ choose an element $s_i(x) \in S$, $s_i(x) \neq 1$, such that $S = \langle s_i(x) \mid x \in X_i \rangle$. Then define an epimorphism $\sigma_i\colon E \to S$ by:

$$\sigma_i(y_{r,x}) = \begin{cases} s_i(x) & \text{if } r = 1 \text{ and } x \in X_i \\ 1 & \text{otherwise} \end{cases}$$

Note that X_i is finite, and therefore σ_i is well defined.

Claim: $\mathrm{Ker}(\sigma_i) \neq \mathrm{Ker}(\sigma_j)$ *for each* $j \in I$. Otherwise $\mathrm{Ker}(\sigma_i) = \mathrm{Ker}(\psi_j)$ for some $j \in I$. Choose $x \in X_i$ and $r \in R$, $r \neq 1$ (Here we use the assumption that E is a proper subgroup of F.) Then $\sigma_i(y_{r,x}) = 1$ and therefore $1 = \psi_j(y_{r,x}) = \varphi_j(r)\varphi_j(x)\varphi_j(r)^{-1}$. Hence $\varphi_j(x) = 1$. It follows that $\psi_j(y_{1,x}) = \varphi_j(x) = 1$. Conclude that $s_i(x) = \sigma_i(y_{1,x}) = 1$. This contradiction to the choice of $s_i(x)$ proves the claim.

If $i, j \in I_2$ and $i \neq j$, then $X_i \neq X_j$. Without loss, we may choose $x \in X_i - X_j$. Then $\sigma_i(y_{1,x}) = s_i(x) \neq 1$ and $\sigma_j(y_{1,x}) = 1$. Conclude that $\mathrm{Ker}(\sigma_i) \neq \mathrm{Ker}(\sigma_j)$.

Let $D = \bigcap_{i \in I_2} \mathrm{Ker}(\sigma_i)$. Since S is nonabelian, $E/D \cong \prod_{i \in I_2} E/\mathrm{Ker}(\sigma_i) \cong S^m$. Moreover, if $MD \neq E$, then there exists $i \in I_2$ such that $\mathrm{Ker}(\sigma_i) \geq MD$. The group $L = N \cdot \mathrm{Ker}(\sigma_i)$ is open and normal in F and $F/L \cong E/\mathrm{Ker}(\sigma_i) \cong S$. Hence, there exists $j \in I$ such that $L = \mathrm{Ker}(\varphi_j)$. Therefore, $\mathrm{Ker}(\sigma_i) = \mathrm{Ker}(\psi_j)$. This contradiction to the claim proves that $MD = E$, as desired. ∎

Before we handle the case where S is abelian, we survey on Pontryagin's duality for vector spaces over $\mathbb{F}_q$ and its application to free profinite groups.

Let q be a prime and let X be a set. Consider the group $V = (\mathbb{Z}/q\mathbb{Z})^X$ which consists of all functions $(v_x)_{x \in X}$ with $v_x \in \mathbb{Z}/q\mathbb{Z}$. Equip V with the product topology and so, consider V as a profinite group. Of course, V is also a vector space over $\mathbb{F}_q$.

Embed X into V by defining $x_x = 1$ and $x_{x'} = 0$ if $x \neq x'$ are in X. In particular, each open neighborhood U of 0 in V contains almost all elements of X. Hence, each continuous homomorphism $\varphi\colon V \to \mathbb{Z}/q\mathbb{Z}$ maps almost all elements of X onto 0. Conversely, each function $\varphi_0\colon X \to \mathbb{Z}/q\mathbb{Z}$ which maps almost all elements of X onto 0 uniquely extends to a continuous homomorphism $\varphi\colon V \to \mathbb{Z}/q\mathbb{Z}$. Indeed, let $X_1 = \{x \in X \mid \varphi_0(x) \neq 0\}$ be the support of φ_0. Define φ at an element $v \in V$ by $\varphi(v) = \sum_{x \in X_1} v_x \varphi_0(x)$. Then φ is a homomorphism and $\mathrm{Ker}(\varphi) \geq \{v \in V \mid \bigwedge_{x \in X_1} v_x = 0\}$ is an open subgroup. We call X a **topological basis** of V. It follows that the dual space to V

$$V^* = \{\varphi\colon V \to \mathbb{Z}/q\mathbb{Z} \mid \varphi \text{ is a continuous homomorphism}\}$$

can be identified with the discrete space

$$\{\varphi\colon X \to \mathbb{Z}/q\mathbb{Z} \mid \text{the support of } \varphi \text{ is finite}\}.$$

The latter has a natural basis $\{\varphi_x \mid x \in X\}$, where $\varphi_x(x') = 1$ if $x' = x$ and $\varphi_x(x') = 0$ if $x' \neq x$.

Pontryagin's duality associates to each subspace W of V^* the closed subspace

$$\mathrm{Ker}(W) = \{v \in V \mid \psi(v) = 0 \text{ for each } \psi \in W\}.$$

If $\mathrm{Ker}(\psi_1) = \mathrm{Ker}(\psi_2)$ for $\psi_1, \psi_2 \in W$, then ψ_1 and ψ_2 differ only by an automorphism of $\mathbb{Z}/q\mathbb{Z}$. Hence, if $|W|$ is infinite, then the cardinality of the set $\{\mathrm{Ker}(\psi) \mid \psi \in W\}$ equals to $|W|$. So $\mathrm{rank}(V/\mathrm{Ker}(W))$, which is the cardinality of the set of all open subgroups of $V/\mathrm{Ker}(W)$ [FJ, p. 188] is equal to that of W.

The map $W \mapsto \mathrm{Ker}(W)$ is bijective and satisfies the relation $\mathrm{Ker}(W_1 \cap W_2) = \mathrm{Ker}(W_1) + \mathrm{Ker}(W_2)$. If $W_1 \cap W_2 = 0$, then $\mathrm{Ker}(W_1) + \mathrm{Ker}(W_2) = V$.

Note that it is much easier to establish Pontryagin's duality for abelian profinite groups than to establish the duality for arbitrary locally compact abelian groups because the former can be reduced to the duality for finite abelian groups:

Let $G = \varprojlim G_i$ be an inverse limit of finite abelian groups. Denote the discrete group of all continuous homomorphisms $\chi\colon G \to \mathbb{C}^*$ by G^*. Then $G^* = \varinjlim G_i^*$ and $G^{**} = \varprojlim G_i^{**}$. The natural isomorphisms $G_i \to G_i^{**}$ induce an isomorphism $G \to G^{**}$. Likewise, all properties of the duality for finite abelian groups are carried over to profinite abelian groups by taking limits.

Consider now the free pro-$\mathcal{D}$-group $F = \widehat{F}_m(\mathcal{D})$ of rank m and let X be a topological basis of F. Denote the intersection of all open normal subgroups L of F with $F/L \cong \mathbb{Z}/q\mathbb{Z}$ by $F^{(q,\mathrm{ab})}$. For each $z \in F$ let $\bar{z}$ be the image of z in the quotient group $V = F/F^{(q,\mathrm{ab})}$. Then the map $x \mapsto \bar{x}$ maps X bijectively onto a topological linear basis of the $\mathbb{F}_q$-vector space V. So we can identify V^* with the discrete space

$$\{\varphi\colon X \to \mathbb{Z}/q\mathbb{Z} \mid \varphi \text{ has a finite support}\}.$$

and also with the space of all continuous homomorphisms $\varphi\colon F \to \mathbb{Z}/q\mathbb{Z}$. Thus, if for $i = 1, 2,$ W_i is a subspace of V^*, then $\mathrm{Ker}(W_i) = \bigcap_{\varphi \in W_i} \mathrm{Ker}(\varphi)$ is a closed subgroup of F which contains $F^{(q,\mathrm{ab})}$. If, in addition, $W_1 \cap W_2 = 0$, then $\mathrm{Ker}(W_1)\mathrm{Ker}(W_2) = F$.

LEMMA 2.4: *Under the assumption of Proposition 2.1, suppose that $S = \mathbb{Z}/q\mathbb{Z}$ for some prime q. Then E has a closed normal subgroup D such that $E/D \cong S^m$ and $MD = E$.*

Proof: For each $x \in X$ let $\varphi_x\colon F \to \mathbb{Z}/q\mathbb{Z}$ be the homomorphism which is defined by $\varphi_x(x) = 1$ and $\varphi_x(x') = 0$ if $x' \neq x$. Then $F^{(q,\mathrm{ab})} = \bigcap_{x \in X} \mathrm{Ker}(\varphi_x)$. Denote the restriction of φ_x to E by ψ_x. Then $E_0 = F^{(q,\mathrm{ab})} \cap E = \bigcap_{x \in X} \mathrm{Ker}(\psi_x)$.

Choose an open normal subgroup E_1 of F which is contained in E. Let $X_0 = X - E_1$ and $X_1 = X \cap E_1$. For each $x \in X_1$ define a homomorphism $\sigma_x\colon E \to \mathbb{Z}/q\mathbb{Z}$ by

$$\sigma_x(y_{r,x'}) = \begin{cases} 1 & \text{if } x' = x \text{ and } r = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Then $D = \bigcap_{x \in X_1} \mathrm{Ker}(\sigma_x)$ satisfies $E/D \cong (\mathbb{Z}/q\mathbb{Z})^m$.

Claim: $E_0 D = E$. By the discussion that precedes the lemma it suffices to prove that the intersection of the vector space generated by the ψ_x's with the vector space generated by the σ_x's is 0. We have to prove that if

$$\sum_{x \in X} a_x \psi_x = \sum_{x \in X_1} b_x \sigma_x \tag{3}$$

with $a_x, b_x \in \mathbb{Z}/q\mathbb{Z}$ and almost all of them are 0, then the right hand side of (3) is 0.

To this end choose $r \in R$, $r \neq 1$, let $x' \in X_1$ and apply (3) on $y_{r,x'}$. Then $\sigma_x(y_{r,x'}) = 0$ and

$$\psi_x(y_{r,x'}) = \varphi_x(rx'r^{-1}) = \varphi_x(r) + \varphi_x(x') - \varphi_x(r) = \begin{cases} 1 & x' = x \\ 0 & x' \neq x. \end{cases} \tag{4}$$

Hence $a_{x'} = 0$. So, (3) reduces to

$$\sum_{x \in X_0} a_x \psi_x = \sum_{x \in X_1} b_x \sigma_x. \tag{5}$$

Now let $x' \in X_1$ and apply (5) to $y_{1,x'}$. By definition $\sigma_x(y_{1,x'}) = 1$ if $x' = x$ and $\sigma_x(y_{1,x'}) = 0$ if $x' \neq x$. Also, if $x \in X_0$, then $x \neq x'$ and therefore, as in (4), $\psi_x(y_{1,x'}) = \varphi_x(x') = 0$. It follows that $b_{x'} = 0$. This completes the proof of the claim.

Finally, if $MD \neq E$, then E has an open normal subgroup K which contains MD such that $E/K \cong \mathbb{Z}/q\mathbb{Z}$. Then $L = NK$ is an open normal subgroup of F such that $F/L \cong \mathbb{Z}/q\mathbb{Z}$. Hence, $K = L \cap E$ contains E_0. Hence, by the claim, $K = KD = E$, a contradiction. Conclude that $MD = E$, as desired. ∎

This concludes the proof of Proposition 2.1.

Theorem 2.5: *Let $\mathcal{D}_0$ be a family of simple groups, $\mathcal{D}$ the quasi full family generated by $\mathcal{D}_0$, m an infinite cardinal, $F = \widehat{F}_m(\mathcal{D})$, and N a closed normal subgroup of F. If $\mathcal{D}$ is a full family, let M be an open proper subgroup of N. If $\mathcal{D}$ is only quasi full, we assume, in addition, that M is normal in N. Then $M \cong \widehat{F}_m(\mathcal{D})$.*

Proof: If $\mathcal{D}$ is a full family, choose an open subgroup H of F such that $N \cap H = M$. If $\mathcal{D}$ is only quasi full, then M is normal in N and therefore we may choose H such that in addition, H is normal in $G = NH$. In both cases H is a proper subgroup of G, N is normal in G and $G \cong \widehat{F}_m(\mathcal{D})$.

By Proposition 2.1, H has for each $S \in \mathcal{D}_0$ a closed normal subgroup D such that $H/D \cong S^m$ and $MD = H$. Hence $M/M \cap D \cong H/D \cong S^m$. So, $r_S(M) \geq m$.

Finally, note that M is normal in H and $H \cong \widehat{F}_m(\mathcal{D})$. By Proposition 1.1(f), $r_S(M) \leq m$. Hence $r_S(M) = m$. Conclude from Proposition 1.1(g) that $M \cong \widehat{F}_m(\mathcal{D})$, as desired. ∎

Note that the case where $\mathcal{D}$ is quasi full is due to Melnikov (see (G3) of the Introduction).

3. Accessible subgroups.

"Accessible subgroups" are the counterpart of "subnormal groups" for profinite groups. The goal of this section is to prove a criterion for an accessible subgroup of a free pro-$\mathcal{D}$-group to be free. Many of the ideas involved in this section are due to Melnikov [M1 and M2].

Recall that a closed subgroup H of a profinite group G is **subnormal** if there exists a finite sequence

$$H = H_n \triangleleft \cdots \triangleleft H_1 \triangleleft H_0 = G$$

with H_i closed, $i = 0, \ldots, n$. We say that H is **accessible** if there exists a transfinite sequence $\{H_\alpha |\ \alpha \leq \gamma\}$ of closed subgroups of G such that $H_0 = G$, $H_\gamma = H$, $H_{\alpha+1} \triangleleft H_\alpha$, for each $\alpha < \gamma$, and $H_\beta = \bigcap_{\alpha<\beta} H_\alpha$ for each limit ordinal $\beta \leq \gamma$.

If G is finite, then H is accessible in G if and only if H is subnormal in G. If H is accessible in G and G_0 is a closed normal subgroup of G which contains H, then H

is accessible in G_0. If φ is an epimorphism of G onto a profinite group $\overline{G}$, then $\varphi(H)$ is accessible in $\overline{G}$.

As Melnikov [M2, Remark 1.5] mentions (without proof), it suffices to consider only countable sequences. To this end we inductively define an ascending sequence of closed subgroups, $N_n(H,G)$, of G which contain H: $N_0(H,G) = G$ and $N_{n+1}(H,G) = \langle H^x |\ x \in N_n(H,G)\rangle$ is the smallest closed normal subgroup of $N_n(H,G)$ which contains H.

Lemma 3.1: *If H is an accessible closed subgroup of a profinite group G, then $H = \bigcap_{n=1}^{\infty} N_n(H,G)$. In particular, if $N_1(H,G) = G$, then $H = G$.*

Proof: Let $N_n = N_n(H,G)$ and $N = \bigcap_{n=1}^{\infty} N_n$. We prove that $N = H$ by proving that $NU = HU$ for each open normal subgroup U of G.

Indeed, $HU = \bigcap_{\alpha\le\gamma} H_\alpha U$. As there are only finitely many subgroups between G and HU, there is a finite sequence of ordinals, $0 = \alpha_0 < \alpha_1 < \cdots < \alpha_r = \gamma$ such that $H_\beta U = H_{\alpha_{i+1}} U$ for each $\alpha_i < \beta \le \alpha_{i+1}$. Then $H_{\alpha_{i+1}} U = H_{\alpha_i+1} U \triangleleft H_{\alpha_i} U$, $i = 0,\ldots,r$. Thus, $HU = H_{\alpha_r} U$ is a subnormal open subgroup of G.

Inductively observe that $N_i \le H_{\alpha_i} U$, $i = 0,\ldots,r$. In particular $N \le N_r \le HU$. Hence, $NU = HU$, as claimed. ∎

Corollary 3.2: *The intersection of closed accessible subgroups of a profinite group G is accessible.*

Proof: Let $H = \bigcap_{j\in J} H_j$ be an intersection of closed accessible subgroups H_j of G. For each nonnegative integer n let $N_n = \bigcap_{j\in J} N_n(H_j,G)$. Then $N_0 = G$, $N_{n+1} \triangleleft N_n$ and $\bigcap_{n=1}^{\infty} N_n = \bigcap_{j\in J}\bigcap_{n=1}^{\infty} N_n(H_j,G) = \bigcap_{j\in J} H_j = H$. Hence H is accessible. ∎

Example 3.3: *Each closed subgroup H of a pronilpotent subgroup G is accessible.* If U is an open normal subgroup of G, then G/U is a finite nilpotent group and therefore HU/U is a subnormal subgroup of G/U [H, p. 308]. Hence, HU is an open subnormal subgroup of G. Conclude from Corollary 3.2 that $H = \bigcap_U HU$ is accessible. ∎

Lemma 3.4: *Let C is a nontrivial minimal closed normal subgroup of a profinite group B. Let H be a closed accessible subgroup of B such that $HC = B$. If $H \cap C \ne 1$, then*

$H = B$. *If* $H \cap C = 1$, *then* $H \triangleleft B$ *and* $B = H \times C$.

Proof: Let $N = N_1(H, B)$ be the smallest closed normal subgroup of B which contains H. If $H \cap C \neq 1$, then $N \cap C \neq 1$. Since $N \cap C$ is normal in B, the minimality of C implies that $N \cap C = C$ and therefore $N \geq C$. As $N \geq H$ we have $N = B$. By Lemma 3.1, $H = B$.

If on the other hand $H \cap C = 1$, then $N \cap C = 1$. Otherwise, by the preceding argument, $H = B$, and therefore $C = 1$, a contradiction. It follows that $B = N \times C$. In particular, the canonical map $\alpha\colon B \to B/C$ maps N bijectively onto B/C. Since $\alpha(H) = B/C$, conclude that $B = N$ and therefore H is normal in B. ∎

We continue to consider the families $\mathcal{D}_0$ and $\mathcal{D}$ of finite groups and the free pro-$\mathcal{D}$-group $F = \widehat{F}_m(\mathcal{D})$ of rank m as in Section 1.

Let G be a pro-$\mathcal{D}$-group. An **embedding problem** for G is a pair

$$(\varphi\colon G \to A,\ \alpha\colon B \to A) \tag{1}$$

of epimorphisms where B is a pro-$\mathcal{D}$-group. A **solution** to (1) is an epimorphism $\gamma\colon G \to B$ such that $\alpha \circ \gamma = \varphi$.

LEMMA 3.5: *Suppose that m is infinite and let G be a pro-$\mathcal{D}$-group with* $\mathrm{rank}(G) = m$. *Each of the following two conditions is necessary and sufficient for G to be isomorphic to $\widehat{F}_m(\mathcal{D})$:*

(2a) *Each embedding problem (1) in which* $\mathrm{rank}(A) < m$ *and* $\mathrm{Ker}(\alpha)$ *is a minimal nontrivial finite normal subgroup of B is solvable.*

(2b) *Each embedding problem (1) in which $B \in \mathcal{D}$ and A nontrivial has m solutions.*

Proof: Suppose first that condition (2a) is satisfied. Use induction on $|\mathrm{Ker}(\alpha)|$ to prove that each embedding problem (1) in which B is a pro-$\mathcal{D}$-group, $\mathrm{rank}(A) < m$ and $\mathrm{Ker}(\alpha) \neq 1$ is solvable. On the other hand the group F also satisfies this condition (with F replacing G) [M1, Lemma 2.2]. Hence $G \cong F$ (The proof of [FJ, Prop. 24.18] which is carried out for the case where D is the family of all finite groups works also for an arbitrary quasi full $\mathcal{D}$.)

Again, the proof of [FJ, Lemma 24.17] applied for pro-$\mathcal{D}$-groups shows that condition (2b) implies condition (2a). Hence, the former also suffices for G to be isomorphic to F. Finally, note that the proof of [FJ, Lemma 24.14] works also for pro-$\mathcal{D}$-groups. So, $\widehat{F}_m(\mathcal{D})$ also satisfies condition (2b). ∎

Let H be a closed subgroup of a profinite group G. The **weight** of the quotient space G/H is the cardinality of the set of open subgroups of G which contain H. In particular, if $(G : H) < \infty$, then $\mathrm{weight}(G/H) < \infty$. If H is normal and G/H is not finitely generated, then $\mathrm{weight}(G/H) = \mathrm{rank}(G/H)$ [FJ, p. 188]. If $(F : H) = \infty$ and $H = \bigcap_{i\in I} H_i$ where each H_i is open, then each open subgroup of G which contains H contains an intersection of finitely many H_i. Hence, $\mathrm{weight}(G/H) = |I|$.

Lemma 3.6: *Let G be a profinite group of infinite rank m and let H is a closed subgroup of G such that* $\mathrm{weight}(G/H) < m$. *Consider a collection $\{G_i |\ i \in I\}$ of open subgroups of G with $|I| = m$. Then for each $i \in I$, $\#\{j \in I |\ H \cap G_j = H \cap G_i\} < m$ and $\#\{H \cap G_i |\ i \in I\} = m$. In particular,* $\mathrm{rank}(H) = m$.

Proof: For each closed subgroup U of G and each $i \in I$ let $J_i(U) = \{j \in I |\ U \cap G_j = U \cap G_i\}$. If U is open, then $U \cap G_i$ is also open and therefore $J_i(U)$ is finite.

Denote the set of all open subgroup of G which contain H by $\mathcal{U}$. If for some $i, j \in I$ we have $H \cap G_j = H \cap G_i$, then there exists a $U \in \mathcal{U}$ such that $U \cap G_j = U \cap G_i$. Indeed, otherwise for each $U \in \mathcal{U}$ the symmetric difference $D(U)$ of $U \cap G_j$ and $U \cap G_i$ will be a nonempty closed subset of G. Intersection of finitely many $D(U)$'s contains a set of this form and therefore it is nonempty. Since G is compact, the intersection of all $D(U)$, which is $D(H)$, is nonempty, a contradiction.

In the above notation this means that $J_i(H) = \bigcup_{U\in\mathcal{U}} J_i(U)$. Hence $|J_i(H)| \leq |\mathcal{U}| \cdot \aleph_0 < m$.

Let I_0 be a system of representatives for the sets $J_i(H)$. Thus, $I = \dot\bigcup_{i\in I_0} J_i(H)$. By the preceding paragraph $\#\{H \cap G_i |\ i \in I\} = |I_0| = m$.

Finally, as each open subgroup of H is the intersection of an open subgroup of G with H, $\mathrm{weight}(H) \leq m$. Hence, by the first statement of the lemma, $\mathrm{rank}(H) = m$. ∎

Lemma 3.7: *Let H be a closed accessible subgroup of a profinite group G. Let H_0 be an open normal subgroup of H. Then G has an open subgroup M_0 such that $H \cap M_0 = H_0$, M_0 is normal in $M = HM_0$, and M is subnormal in G. If $(G : H) = \infty$, then me may choose M_0 such that in addition $(G : M)$ is greater than a given positive integer n.*

Proof: Choose an open subgroup K_0 of G such that $H \cap K_0 = H_0$. If $(G : H) = \infty$ and n is given, choose K_0 such that, in addition, $(G : K_0) > n(H : H_0)$. Let L_0 be the intersection of all K_0^h where h ranges over a system of representatives of H/H_0. Then L_0 is normal in $L = HL_0$. Finally, choose an open normal subgroup N of G which is contained in L. Then $M = HN$ is subnormal and open in G, $M_0 = M \cap L_0$ is open and normal in M and $H \cap M_0 = H_0$, as desired. ∎

Lemma 3.8: *Each open subnormal subgroup H of F is pro-$\mathcal{D}$-free.*

Proof: Choose a normal series $H = H_n \triangleleft \cdots \triangleleft H_1 \triangleleft H_0 = F$ and apply Proposition 1.1(b) inductively on n. ∎

Proposition 3.9: *Suppose that m is infinite. Let H be an accessible closed subgroup of F with* $\mathrm{weight}(F/H) < m$. *then $H \cong F$.*

Proof: Let

$$(\varphi\colon H \to A,\ \alpha\colon B \to A) \tag{3}$$

be an embedding problem such that $B \in \mathcal{D}$ and $C = \mathrm{Ker}(\alpha)$ is a minimal nontrivial subgroup of B. Then $H_0 = \mathrm{Ker}(\varphi)$ is an open normal subgroup of H. Choose an open subgroup G_0 of F such that $H \cap G_0 = H_0$, $G = HG_0$ is subnormal and $G_0 \triangleleft G$ (Lemma 3.7). Then extend φ to an epimorphism $\hat{\varphi}\colon G \to A$ by $\hat{\varphi}(hg_0) = \varphi(h)$ for $h \in H$ and $g_0 \in G_0$. By Lemma 3.8, $G \cong F$. It follows (Lemma 3.5) that the embedding problem $(\hat{\varphi}\colon G \to A,\ \alpha\colon B \to A)$ has m solutions $\hat{\gamma}_i$, $i \in I$. Let $G_i = \mathrm{Ker}(\hat{\gamma}_i)$.

For each $i \in I$, $H_0 \cap G_i = H \cap G_i$. By Lemma 3.6, the cardinality of the set $\{i \in I |\ H_0 \cap G_i = H_0\} = \{i \in I |\ H \cap G_i = H \cap G_0\}$ is less than m. So assume without loss that H_0 is contained in no G_i.

Let γ_i be the restriction of $\hat{\gamma}_i$ to H. Choose $h \in H_0 - G_i$. Then $\gamma_i(h) \neq 1$ and $\alpha(\gamma_i(h)) = \varphi(h) = 1$. Hence, $\gamma_i(h) \in \gamma_i(H) \cap C$ and therefore $\gamma_i(H) \cap C \neq 1$. Also,

$\alpha(\gamma_i(H)) = \varphi(H) = A$, which implies that $\gamma_i(H)C = B$. Since $\hat{\gamma}_i(G) = B$ and H is accessible in G, the group $\gamma_i(H)$ is subnormal in B. By Lemma 3.4, $\gamma_i(H) = B$. So, γ_i is a solution to the embedding problem (3).

Finally note that $H \cap G_i = \mathrm{Ker}(\gamma_i)$. By Lemma 3.6, $\#\{H \cap G_i |\ i \in I\} = m$. Hence, (3) has m solutions. By Lemma 3.5(2b), $H \cong F$. ∎

PROPOSITION 3.10: *Suppose that $m \geq 2$. Let H be an accessible closed subgroup of F of infinite index such that $r_S(H) = \max\{\aleph_0, m\}$ for each $S \in \mathcal{D}_0$. Then $H \cong \widehat{F}_{\max\{\omega,m\}}$.*

Proof: By Lemma 3.5, it suffices to prove that each embedding problem

$$(\varphi \colon H \to A,\ \alpha \colon B \to A) \tag{4}$$

for which B is a pro-$\mathcal{D}$-group, $\mathrm{rank}(A) < \max\{\aleph_0, m\}$, and $C = \mathrm{Ker}(\alpha)$ is a minimal nontrivial finite normal subgroup of B is solvable.

Let $H_0 = \mathrm{Ker}(\varphi)$. If m is finite, then $\mathrm{rank}(B) < \infty$. By Lemma 3.7, there exists an open normal subgroup G_0 of F such that $H \cap G_0 = H_0$, G_0 is normal in $G = HG_0$, G is subnormal in F, and $G \cong \widehat{F}_e(\mathcal{D})$ with $e \geq \mathrm{rank}(B)$.

If m is infinite, H_0 is the intersection of a collection of open normal subgroups K_i of H where i ranges over a set I of cardinality less than m. For each $i \in I$ Lemma 3.7 gives an open subgroup L_i of F such that $H \cap L_i = K_i$, $L_i \triangleleft HL_i$, and HL_i is subnormal in F. Let $G_0 = \bigcap_{i \in I} L_i$ and $G = HG_0 = \bigcap_{i \in I} HL_i$. Then G is an accessible closed subgroup of F (Lemma 3.2), $\mathrm{rank}(F/G) < m$, $G_0 \triangleleft G$, and $H \cap G_0 = H_0$. By Proposition 3.9, $G \cong \widehat{F}_m(\mathcal{D})$.

In each case extend φ to an epimorphism $\hat{\varphi} \colon G \to A$ by $\hat{\varphi}(hg_0) = \varphi(h)$ for $h \in H$ and $g_0 \in G_0$. By [FJ, Prop. 15.3] for finite m and Lemma 3.5 for infinite m there exists an epimorphism $\hat{\gamma} \colon G \to B$ such that $\alpha \circ \hat{\gamma} = \hat{\varphi}$. Let $G_1 = \mathrm{Ker}(\hat{\gamma})$ and let γ be the restriction of $\hat{\gamma}$ to H. Then $\gamma(H)$ is a closed accessible subgroup of B. Also, $\alpha(\gamma(H)) = \varphi(H) = A$. Hence $\gamma(H)C = B$. There are two cases to consider:

CASE A: $\gamma(H) \cap C \neq 1$. By Lemma 3.4, $\gamma(H) = B$. So, γ is a solution to the embedding problem (4).

CASE B: $\gamma(H) \cap C = 1$. By Lemma 3.4, $B = \gamma(H) \times C$. It follows that $B = A \times C$ and α is the projection from on the first factor.

Since C is a minimal nontrivial normal subgroup of B it must be simple. So $C \in \mathcal{D}_0$. By assumption, $r_C(H) = \max\{\aleph_0, m\}$. On the other hand $\mathrm{rank}(H/H_0) = \mathrm{rank}(A) < \max\{\aleph_0, m\}$. Hence, H has an open normal subgroup H_1' such that $H/H_1' \cong C$ and $H_1' \not\geq H_0$. Since C is simple, $H_1'H_0 = H$. Let $H_1 = H_1' \cap H_0$. Then $H/H_1 \cong H_1'/H_1 \times H_0/H_1 \cong A \times C \cong B$. The canonical map $H \to H/H_1$ defines an epimorphism $\gamma\colon H \to B$ such that $\alpha \circ \gamma = \varphi$, as desired. ∎

EXAMPLE 3.11: *The condition on H in Proposition 3.10 to be accessible is indispensable.* Let H_0 be the direct product of all simple finite groups, each taken $\aleph_0$ times. This is a profinite group of rank $\aleph_0$. Since H_0 contains elements of finite order, it is not projective [FJ, Cor. 20.14]. Denote the universal Frattini extension of H_0 by H. It is a projective profinite group of rank $\aleph_0$ [FJ, Prop. 20.33 and Cor. 20.26]. The kernel of the map $\varphi\colon H \to H_0$ is a nontrivial closed normal subgroup of the Frattini subgroup of H. Since the latter subgroup is pronilpotent [FJ, Lemma 20.2], so is the former. It follows that H is not free [FJ, Cor. 24.8(c)]. On the other hand, H as a projective group of rank $\aleph_0$ is isomorphic to a closed subgroup H' of $\widehat{F}_\omega$ [FJ, Cor. 20.14]. By Proposition 3.10, H' is not accessible. ∎

4. Closed subgroups of F which contain $F^{(\mathrm{nil})}$.

The goal of this section is to prove Theorem G6 of the Introduction. The families of finite groups $\mathcal{D}_0$, $\mathcal{D}$ and the free pro-$\mathcal{D}$-group $F = \widehat{F}_m(\mathcal{D})$ of rank m retain the meaning we gave them in Section 1.

We use $F^{(p)}$ to denote the intersection of all open normal subgroups of F such that F/N is a p-group. If $\mathbb{Z}/p\mathbb{Z} \in \mathcal{D}_0$, then $F/F^{(p)}$ is the free pro-p-group of rank m. We also denote the intersection of all open normal subgroups N of F such that F/N is nilpotent by $F^{(\mathrm{nil})}$. Then $F/F^{(\mathrm{nil})}$ is pronilpotent and therefore it is isomorphic to the direct product of its unique p-Sylow groups [FJ, p. 311, Exer. 11].

Theorem 4.1: *Suppose that $m \geq 2$, and $\mathbb{Z}/p\mathbb{Z} \in \mathcal{D}_0$. Let H be a closed subgroup of F of infinite index which contains $F^{(\mathrm{nil})}$. Then H is isomorphic to $\widehat{F}_{\max\{\omega,m\}}(\mathcal{D})$ unless H contains $F^{(p)}$ and* $\mathrm{rank}(H/F^{(p)}) < \max\{\omega, m\}$. *In the latter case H is not pro-$\mathcal{D}$-free unless $\mathcal{D}_0 = \{\mathbb{Z}/p\mathbb{Z}\}$.*

There are three cases to consider:

(1a) *H contains $F^{(p)}$,*

(1b) *$2 \leq m < \infty$ and at least two primes divide $(F : H)$, and*

(1c) *m is infinite and at least two primes divide $(F : H)$.*

We handle these cases in Propositions 4.3, 4.5, and 4.6, respectively. By example 3.3, H is a closed accessible subgroup of F. So, we can apply Proposition 3.10 to H.

Lemma 4.2: *Let H be a closed subgroup of F of infinite index which contains $F^{(\mathrm{nil})}$. Let $S \in \mathcal{D}_0$ be a simple group which is either nonabelian or $S = \mathbb{Z}/q\mathbb{Z}$ where q is a prime which does not divide $(F : H)$. Then $r_S(H) = \max\{\aleph_0, m\}$.*

Proof: There exists a closed normal subgroup N such that $F/N \cong S^m$. The group HN is accessible in F (Example 3.3) and the decomposition factors of F/HN must be equal to S (as factors of F/N) as well as different from S (as factors of F/H). Hence there are none and therefore $HN = F$. It follows that $H/H \cap N \cong F/N \cong S^m$. So, $r_S(H) \geq m$.

If m is finite, then, by assumption, H is contained in an open subgroup E of F of arbitrary large index. By Proposition 1.1(a), E is pro-$\mathcal{D}$-free of arbitrary large rank. Apply the preceding paragraph to E instead of F to conclude in this case that $r_S(H) \geq \aleph_0$.

In each case $\mathrm{rank}(H)$ is infinite. Hence $\mathrm{rank}(H)$ is equal to the cardinality of the set of open subgroups of H [FJ, p. 188]. By [FJ, p. 200, Exer. 9], $\mathrm{rank}(H) \leq \max\{\aleph_0, m\}$. Hence $r_S(H) \leq \mathrm{rank}(H) \leq \max\{\aleph_0, m\}$. Conclude that $r_S(H) = \max\{\aleph_0, m\}$. ∎

Abbreviate $r_{\mathbb{Z}/q\mathbb{Z}}(H)$ by $r_q(H)$.

PROPOSITION 4.3: *Suppose that $m \geq 2$, and $\mathbb{Z}/p\mathbb{Z} \in \mathcal{D}_0$. Let H be a closed subgroup of F which contains $F^{(p)}$. If $\mathrm{rank}(H/F^{(p)}) = \max\{\aleph_0, m\}$, then $H \cong \widehat{F}_{\max\{\omega,m\}}$. Otherwise, H is not a free pro-$\mathcal{D}$-group, unless $\mathcal{D}_0 = \{\mathbb{Z}/p\mathbb{Z}\}$.*

Proof: Suppose that $\mathrm{rank}(H/F^{(p)}) = \max\{\aleph_0, m\}$. The group $H/F^{(p)}$ as a closed subgroup of the free pro-p-group $F/F^{(p)}$ is free [FJ, Cor. 20.38]. Hence $(\mathbb{Z}/p\mathbb{Z})^{\max\{\aleph_0,m\}}$ is a quotient of H and therefore $r_p(H) = \max\{\aleph_0, m\}$. So, by Lemma 4.2, $r_S(H) = \max\{\aleph_0, m\}$ for each $S \in \mathcal{D}_0$. Conclude from Proposition 3.10 that $H \cong \widehat{F}_{\max\{\omega,m\}}$.

Conversely, suppose that $\mathrm{rank}(H/F^{(p)}) < \max\{\aleph_0, m\}$. If $\mathcal{D}_0$ contains a simple group $S \neq \mathbb{Z}/p\mathbb{Z}$, then, by Lemma 4.2, $r_S = \max\{\aleph_0, m\}$. Observe that $H^{(p)} = F^{(p)}$. Hence, if H were a pro-$\mathcal{D}$-group, then, by Proposition 1.1(b),

$$\max\{\aleph_0, m\} > \mathrm{rank}(H/F^{(p)}) = r_p(H) = \mathrm{rank}(H) = r_S(H) = \max\{\aleph_0, m\},$$

a contradiction. So, H is not a free pro-$\mathcal{D}$-group.

Finally, if $\mathcal{D}_0 = \{\mathbb{Z}/p\mathbb{Z}\}$, then, by a theorem of Tate [FJ, Cor. 20.38], H is a free pro-p-group. ∎

LEMMA 4.4: *Let G be a pronilpotent group and let H be a closed subgroup of infinite index of G. Let p be a prime divisor of $(G : H)$ and let n be a positive integer. Then there exist open subgroups D and E of G which contain H such that D is an open normal subgroup of E of index p and $(G : E) \geq n$.*

Proof: The group H as a subgroup of G is also pronilpotent. Let H_p (resp., G_p) be the unique p-Sylow group of H (resp. G). Denote the group generated by all l-Sylow groups of H (resp., G) where l ranges over all primes different from p by $H_{p'}$ (resp.,

$G_{p'}$). Then $H_p = G_p \cap H$, $H_{p'} = G_{p'} \cap H$, $H = H_p \times H_{p'}$ and $G = G_p \times G_{p'}$. Hence $(G : H) = (G_p : H_p)(G_{p'} : H_{p'})$. So, $(G_p : H_p) = \infty$ or $(G_{p'} : H_{p'}) = \infty$. We consider each of these cases separately.

Case A: $(G_p : H_p) = \infty$. Since G_p is a pro-p-group, it has open subgroups D_p and E_p which contain H_p such that D_p is a normal subgroup of E_p of index p and $(G_p : E_p) \geq n$. Let $D = D_p G_{p'}$ and $E = E_p G_{p'}$. Then $H \leq D \triangleleft E$, $(E : D) = (E_p : D_p) = p$, and $(G : E) = (G_p : E_p) \geq n$. In particular both D and E are open in G.

Case B: $(G_{p'} : H_{p'}) = \infty$. Choose an open subgroup C of $G_{p'}$ which contains $H_{p'}$ such that $(G_{p'} : C) \geq n$. Since p divides $(G : H)$, the group H does not contain G_p. Hence H_p is a proper subgroup of G_p, and is therefore contained in a maximal open subgroup M of G_p, which must be of index p. The groups $D = MC$ and $E = G_p C$ have the desired properties. ∎

Proposition 4.5: *Suppose that $m = e \geq 2$ is finite. Let H be a closed subgroup of F of infinite index which contains $F^{(\mathrm{nil})}$. Suppose further that $(F : H)$ is divisible by at least two distinct primes. Then $H \cong \widehat{F}_\omega(\mathcal{D})$.*

Proof: By Lemma 4.2 and Proposition 3.10 we have only to prove that $r_q(H) = \infty$ for each prime q. Indeed, by assumption, there exists a prime $p \neq q$ which divides $(F : H)$. Apply Lemma 4.4 to $F/F^{(\mathrm{nil})}$, $H/F^{(\mathrm{nil})}$ and a positive integer n to find open subgroups D and E and of F which contain H such that D is an open subgroup of E of index p and $(F : E) \geq n$. As D contains $F^{(\mathrm{nil})}$ it is subnormal. Hence, D is a free pro-$\mathcal{D}$-group of rank $1 + (F : D)(e-1)$ [FJ, Prop. 15.27]. Hence

$$r_q(D) = 1 + p(F : E)(e-1). \tag{2}$$

Decompose now the pronilpotent groups $E/F^{(\mathrm{nil})}$ and $D/F^{(\mathrm{nil})}$ as a direct product of their p-Sylow subgroups:

$$E/F^{(\mathrm{nil})} = (E/F^{(\mathrm{nil})})_p \times (E/F^{(\mathrm{nil})})_q \times \prod_{l \neq p,q} (E/F^{(\mathrm{nil})})_l,$$
$$D/F^{(\mathrm{nil})} = (D/F^{(\mathrm{nil})})_p \times (D/F^{(\mathrm{nil})})_q \times \prod_{l \neq p,q} (D/F^{(\mathrm{nil})})_l.$$

Since D is normal in E of index p, $(D/F^{(\mathrm{nil})})_p \le (E/F^{(\mathrm{nil})})_p$ and $(D/F^{(\mathrm{nil})})_l = (E/F^{(\mathrm{nil})})_l$ for each prime $l \ne p$. Hence,

$$r_q(D/F^{(\mathrm{nil})}) = r_q(E/F^{(\mathrm{nil})}) = 1 + (F:E)(e-1). \tag{3}$$

Hence, by (2) and (3),

$$r_q(D) - r_q(D/F^{(\mathrm{nil})}) = (p-1)(F:E)(e-1) \ge (p-1)n(e-1) \ge n. \tag{4}$$

This gives an open normal subgroup D_0 of D such that D/D_0 is an elementary abelian p-group of rank at least n such that $F^{(\mathrm{nil})}D_0 = D$. Hence $HD_0 = D$, and therefore $H/H \cap D_0 \cong D/D_0$. Conclude that $r_q(H) \ge n$. Since n was arbitrary, this implies that $r_q(H) = \infty$. ∎

We may reduce the case where $m = \aleph_0$ to the finite case. The essential point is to prove that $r_q(H) = \aleph_0$ for each prime q. We may achieve this goal by mapping F onto $\widehat{F}_e(\mathcal{D})$ with e large such that H is mapped onto a subgroup whose index is divisible by at least two primes.

The uncountable case is more complicated. If E is an open subgroup of F, then E is a free pro-$\mathcal{D}$-group of the same rank as F. So, we can not use the Nielsen-Schreier formulas as we do in Lemma 4.5. Instead, we use Lemma 2.4.

PROPOSITION 4.6: *Suppose that m is infinite. Let H be a closed subgroup of F which contains $F^{(\mathrm{nil})}$. Suppose further that $(F:H)$ is divisible by two distinct primes. Then $H \cong \widehat{F}_m(\mathcal{D})$.*

Proof: Again we have only to prove that $r_q(H) = m$ for each prime q. By assumption there exists a prime $p \ne q$ which divides $(F:H)$. Since $H \ge F^{(\mathrm{nil})}$ there exist open subgroups $D \triangleleft E$ of F which contain H such that $(E:D) = p$. As E is subnormal in F it is isomorphic to F (Lemma 3.8). As $E^{(\mathrm{nil})} \subseteq F^{(\mathrm{nil})}$ we may assume without loss that $E = F$. Thus $D \triangleleft F$ and $F/D \cong \mathbb{Z}/p\mathbb{Z}$.

The group $D_0 = F^{(q,\mathrm{ab})} \cap D$ contains $F^{(\mathrm{nil})}$. The group D contains the unique closed normal subgroup F_q which contains $F^{(\mathrm{nil})}$ such that $F_q/F^{(\mathrm{nil})}$ is the q-Sylow subgroup of $F/F^{(\mathrm{nil})}$ (since $(DF_q : D)$ divides both p and q). Also, $F^{(q,\mathrm{ab})}F_q = F$.

Hence $F/F^{(q,\mathrm{ab})} \cong D/D_0$ and D_0 is the intersection of all open normal subgroup of D of index q which contain $F^{(\mathrm{nil})}$.

By Lemma 2.4, D has a closed normal subgroup C such that $D/C \cong (\mathbb{Z}/q\mathbb{Z})^m$ and $D_0C = D$. Then $F^{(\mathrm{nil})}C$ is the intersection of a set of normal subgroups of D with coquotients isomorphic to $\mathbb{Z}/q\mathbb{Z}$. Hence $D_0 \le F^{(\mathrm{nil})}C$ and therefore $F^{(\mathrm{nil})}C = D$. It follows that $HC = D$. Hence $H/H \cap C \cong D/C \cong (\mathbb{Z}/q\mathbb{Z})^m$. So, by Proposition 1.1(f), $r_q(H) = m$, as desired. ∎

5. Concluding remarks

In this section we demonstrate the possibility to raise questions about extensions of Hilbertian fields from theorems about free profinite groups. One of these questions is easily answered. Two others remain open.

Here is a generalization of [LD, Prop. 3.15] from free groups of at most countable rank to arbitrary free groups.

PROPOSITION 5.1: *Suppose that $\mathcal{D}$ is a full family and $m \ge 2$. Let H be a closed subgroup of infinite index of $F = \widehat{F}_m(\mathcal{D})$. Suppose that $(F : H) = \prod p^{\alpha(p)}$ with all $\alpha(p)$ finite. Then $H \cong F_{\max\{\omega,m\}}$.*

Proof: Consider an embedding problem

$$(1) \qquad (\varphi\colon H \to A,\ \alpha\colon B \to A)$$

in which $B \in \mathcal{D}$ and A is nontrivial.

To solve (1), let $H_0 = \mathrm{Ker}(\varphi)$. Find an open subgroup G_0 of F such that $H \cap G_0 = H_0$, G_0 is normal in $G = \langle H, G_0\rangle$ and $p^{\alpha(p)}$ divides $(F : G)$ for each p which divides the order of B. In particular $G = HG_0$ and the order of B is relatively prime to $(G : H)$. Extend φ to a homomorphism $\hat{\varphi}\colon G \to A$ by $\hat{\varphi}(hg_0) = \varphi(h)$.

Since G is isomorphic to F there are epimorphisms $\hat{\gamma}_i\colon G \to B$ where i ranges over a set I of cardinality m such that $\alpha \circ \hat{\gamma}_i = \hat{\varphi}$ and $\mathrm{Ker}(\hat{\gamma}_i) \ne \mathrm{Ker}(\hat{\gamma}_j)$ if i, j are distinct elements of I. Denote the restriction of $\hat{\gamma}_i$ to H by γ_i. As the index $(B : \gamma_i(H))$ divides both $(G : H)$ and the order of B it must be 1. Hence $\gamma_i(H) = B$. So, (1) is solvable. If $2 \le m \le \aleph_0$, then $H \cong \widehat{F}_\omega(\mathcal{D})$ [FJ, Cor. 4.2]. If $m > \aleph_0$, then by Lemma 3.6, $\#\{\mathrm{Ker}(\gamma_i) | \ i \in I\} = m$. Conclude that embedding problem (1) has m solutions, as desired. Conclude from Lemma 3.5(b) that $H \cong \widehat{F}_m(\mathcal{D})$. ∎

We prove the field theoretic analog of this theorem.

PROPOSITION 5.2: *Let L be an algebraic separable extension of a Hilbertian field K of degree $\prod p^{\alpha(p)}$, with all $\alpha(p)$ finite. Then L is Hilbertian.*

Proof: Let t be a transcendental element over L. It suffices to prove that if $f \in L[t, X]$ is a polynomial which is irreducible and Galois over $L(t)$, then there are infinitely many $a \in L$ such that $f(a, X)$ is irreducible and Galois over L with the same degree n as $f(t, X)$.

By assumption, K has a finite extension E which is contained in L such that $p^{\alpha(p)} | [E : K]$ for each prime divisor p of n, all the coefficients of f lie in E, and $f(t, X)$ is Galois over $E(t)$. In particular, $[L : E]$ is relatively prime to n. As E is Hilbertian, there are infinitely many elements $a \in E$ such that $f(a, X)$ is irreducible and Galois over E of degree n. Let F be the splitting field of $f(a, X)$ over E. Then $[F : E] = n$ is relatively prime to $[L : E]$. Hence $[LF : L] = n$ and therefore $f(a, X)$ is irreducible and Galois over L of degree n, as desired. ∎

One could attempt to generalize Theorem (G2) of the introduction to nonnormal subgroups: *If $m \ge 2$ and H is a closed subgroup of $F = \widehat{F}_m(\mathcal{D})$ such that $F = \langle H, x_1, \ldots, x_n \rangle$, then H is a free pro-$\mathcal{D}$-group.*

This attempt fails due to a remarkable result of Aschbacher and Guralnik [AG, Thm. A] which uses the classification of simple groups:

PROPOSITION 5.3: *Every finite group is generated by a pair of conjugate solvable subgroups.*

Proposition 5.3 is preserved under taking inverse limits:

COROLLARY 5.4: (a) *Every profinite group is generated by a pair of conjugate prosolvable closed subgroups.*

(b) *Every profinite group is generated by a closed prosolvable subgroup and one more element.*

By Corollary 5.4, F has a closed prosolvable subgroup H and an element x such that $F = \langle H, x\rangle$. If $\mathcal{D}_0$ contains nonabelian simple groups and $m \geq 3$, then $\mathrm{rank}(H) \geq 2$ and hence H is not a free pro-$\mathcal{D}$-group. If $m = 2$ then H could be generated by one element and therefore would be prosolvable. Nevertheless, take an open subgroup E and choose a closed prosolvable subgroup H and an element x_1 in E such that $E = \langle H, x_1\rangle$. Then choose representatives $x_2, \ldots, x_n$ for F/E. We have $F = \langle H, x_1, x_2, \ldots, x_n\rangle$, but H is not free. So, the above conjecture is false.

Likewise, the straight forward generalization of Theorem (F2) of the introduction to the case of a non-Galois extension is false: Each Hilbertian field K has a separable algebraic extension L with $G(L)$ prosolvable and there exists an element $\sigma \in G(K)$ such that $G(K) = \langle G(L), \sigma\rangle$. Since Hilbertian fields admit nonsolvable Galois extensions, L is not Hilbertian.

Proposition 1.1(g) gives rise to the following problem:

PROBLEM 5.5: *Let L be a Galois extension of a Hilbertian field K. Suppose that each finite group is realizable over L as a Galois group. Is L necessarily Hilbertian?*

Melnikov [M1, Lemma 2.7 and Thm. 3.1] (see also [FJ, Prop. 24.10]) proves the following result:

PROPOSITION 5.6: *Suppose that $2 \leq m$. Let X be a basis of F and let N be a closed normal subgroup of F of infinite index. If N contains an element $w \neq 1$ of the discrete group generated by X, then $N \cong \widehat{F}_{\max\{\omega,m\}}$.*

In particular, if N contains the commutator group $[F, F]$ of F, then N is free. The analog of the latter result for Hilbertian fields is true: Every abelian extension of a Hilbertian field is Hilbertian [FJ, Thm. 15.6]. Following the twinning principle, we ask:

PROBLEM 5.7: *Let K be a Hilbertian field. Consider a nonempty set W of words in the variables $X_1, X_2, X_3, \ldots$. Let K_s be the separable closure of K. Denote the fixed* *field in K_s of all automorphisms $w(\sigma_1, \ldots, \sigma_n)$ where $w = w(X_1, \ldots, X_n) \in W$ and $\sigma_1, \ldots, \sigma_n \in G(K)$ by N. Is N Hilbertian?*

Finally, we ask for a generalization of Proposition 3.9:

PROBLEM 5.8: *Suppose that m is uncountable. Let H be a closed subgroup of F such that* $\mathrm{weight}(F/H) < m$. *Is $H \cong F$?*

We conclude this section with a negative answer to Question 1 on page 34 of [LD]. It is related to Proposition 5.1.

THEOREM 5.9: *Let G be a profinite group of order $\prod p^{\alpha(p)}$, where $\alpha(p) \le d$ is bounded. Then G satisfies the eth Nielsen – Schreier formula for no $e \ge 1$.*

Proof: Let G_2 be a 2-Sylow subgroup of G. It is finite of order $2^{\alpha(2)}$. Take an open normal subgroup N of G whose intersection with G_2 is trivial. In particular $2^{\alpha(2)} | (G : N)$ and therefore N has an odd order. By the Feit–Thompson theorem, N is prosolvable.

The order of each closed subgroup of N is $\prod p^{\beta(p)}$ where $\beta(p) \le \alpha(p) \le d$. In particular, the number of generators of each p-Sylow subgroup of an open subgroup H of N is bounded by d. By a theorem of Kovács [Ko], the rank of H is at most $d + 1$ (Using the classification of simple groups, Lucchini [L] has proved the same result for each finite, and hence profinite group.) It follows that N and therefore G satisfy no Nielsen – Schreier formula. ∎

References

[AG] M. Aschbacher and R. Guralnik, *Solvable generation of groups and Sylow subgroups of the lower central series,* Journal of Algebra **77** (1982), 189–201.

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

[FV] M. Fried and H. Völklein, *The embedding problem over a Hilbertian PAC field,* preprint.

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

[HJ] D. Haran and M. Jarden, *Compositum of Galois extensions of Hilbertian fields,* to appear in Annales Sientifiques de l'Ecole Normale Superieure.

[K] W. Kuyk, *Extensions de corps hibertiens,* Journal of Algebra **14** (1970), 112–124.

[Ko] L.G. Kovács, *On finite soluble groups,* Mathematische Zeitschrift **103**, 37–39 (1967).

[L] A. Lubotzky, *Free quotients and the congruence kernel of SL_2,* Journal of Algebra **77** (1982), 411–418.

[LD] A. Lubotzky and L.v.d. Dries, *Subgroups of free profinite groups and large subfields of $\widetilde{\mathbb{Q}}$,* Israel Journal of Mathematics **39** (1981), 25-45.

[Lu] A. Lucchini, *A bound on the number of generators of a finite group,* Archiv der Mathematik **53** (1989), 313–317.

[M1] O.V. Melnikov, *Normal subgroups of free profinite groups,* Mathematical USSR Izvestija **12** (1978), 1–20.

[M2] O.V. Melnikov *Characterization of accessible subgroups of free profinite groups (russian),* Doklady Akademii Nauk BSSR **22** (1978), 677–680.

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

Addresses of the authors:

Moshe Jarden
School of Mathematical Sciences
Raymond and Beverly Sackler Faculty of Exact Sciences
Tel Aviv University
Ramat Aviv, Tel Aviv 69978
ISRAEL
e-mail: jarden@taurus.bitnet

Alexander Lubotzky
Institute of Mathematics
The Hebrew University
Givat Ram, Jerusalem 91904
ISRAEL
alexlub@hujivms.bitnet

9 February, 2007