FROBENIUS SUBGROUPS OF FREE PROFINITE PRODUCTS

ROBERT M. GURALNICK AND DAN HARAN

Abstract. We solve an open problem of Herfort and Ribes: Profinite Frobenius groups of certain type do occur as closed subgroups of free profinite products of two profinite groups. This also solves a question of Pop about prosolvable subgroups of free profinite products.

1. Introduction

Herfort and Ribes show in [10, Theorem 3.2] that a closed solvable subgroup of the free product of a family of profinite groups $\{A_x\}_{x \in X}$ must be one of the following:

(1) a conjugate of a subgroup of one of the free factors A_x;
(2) isomorphic to $\hat{\mathbb{Z}}_\sigma \rtimes \hat{\mathbb{Z}}_{\sigma'}$, where σ and σ' are disjoint sets of prime numbers;
(3) free pro-$\mathcal{C}$ product of two copies of the group of order 2, for some full class $\mathcal{C}$ of finite groups;
(4) a profinite Frobenius group of the form $\hat{\mathbb{Z}}_\sigma \rtimes C$ with Frobenius kernel $\hat{\mathbb{Z}}_\sigma$, where C is a finite cyclic group.

In [10, Section 4] they show that each group of one of the first three types does occur as a closed subgroup of a free profinite product, namely, of two finite groups. As for the Frobenius groups, Herfort and Ribes state in [10] and show in [11] that they occur as closed subgroups of free *prosolvable* products of two finite groups. They (implicitly) leave open the question whether the above Frobenius groups occur as closed subgroups of free profinite products of, say, two finite groups.

This problem has been explicitly posed in [14] (see [14, Open Question 9.5.5]).

The main result of this paper is an affirmative answer to this question.

The proof uses the classification of finite simple groups (by analyzing automorphisms of simple groups and subgroups stabilized by them). If C has prime power order, the proof is much simpler and does not require the

---

2000 *Mathematics Subject Classification.* primary 20E18; secondary 20D45, 20D05.

Key words and phrases. profinite group, free profinite product, Frobenius group, intravariant subgroup, finite simple group, automorphism.

The first author was partially supported by NSF grant DMS 0653873. The second author was partially supported by the Israel Science Foundation (Grant No. 343/07) and the Minerva Minkowski Center for Geometry at Tel Aviv University.

classification (Sylow's theorem is the main tool in that case). This had been essentially done by the authors several years ago in an unpublished work. See Remark 4.7. A. Zalesski and P. Zalesskii also found an independent proof in this case.

We thank P. Zalesskii for reminding us that our result also answers a question of Pop [12]. That paper characterizes closed prosolvable groups of free profinite products of profinite groups and the question is the following. Is there a free profinite product $G = \coprod_{i\in I} G_i$ and a closed prosolvable subgroup H of G such that

(1) there is no prime ℓ such that $H \cap G_i^\sigma$ is a pro-ℓ group for all $i \in I$ and all $\sigma \in G$;
(2) $H \leq G_i^\sigma$ for no $i \in I$ and no $\sigma \in G$?

A Frobenius subgroup of a free product of certain two finite groups provides such an example (Example 5.3).

We are grateful to W. Herfort for useful remarks to an earlier version of this paper.

2. Finite and profinite Frobenius Subgroups

Recall that the notions of order and index extend from finite groups to profinite groups; instead of natural numbers these are supernatural numbers ([14, Section 2.3] or [4, Section 22.8]). In particular, a profinite group has Sylow p-subgroups for each prime p ([14, Corollary 2.3.6] or [4, Section 22.9]).

A profinite group F is a *Frobenius group* if it is a semidirect product $F = C \ltimes K$ of nontrivial profinite groups C, K of co-prime orders, where C acts on K so that $[c, k] \neq 1$ for every $1 \neq c \in C, 1 \neq k \in K$. One then calls K the *Frobenius kernel* and C a *Frobenius complement* of F.

Since we deal only with a special type of Frobenius groups, we adopt the following notation. Let C be a finite cyclic group. A *C-group* is a profinite group with a distinguished subgroup isomorphic to C; we identify this subgroup with C. A *C-homomorphism* of C-groups $G \to H$ is a continuous homomorphism $G \to H$ that maps the copy of C in G identically onto the copy of C in H. If $A \triangleleft G$ then G/A is a C-group if and only if $A \cap C = 1$ (we identify C with CA/A); in this case $G \to G/A$ is a C-epimorphism.

We call a profinite C-group F a *C-Frobenius group* if F is a Frobenius group with complement C and procyclic kernel. The following properties are easy to verify:

Lemma 2.1. *Let $C \neq 1$ be a finite cyclic group acting on a procyclic group $K \neq 1$. Then $F = C \ltimes K$ is a C-Frobenius group if and only if for each prime p dividing the order of K, the order of C divides $p - 1$ and C acts faithfully on the p-primary part of K. If F is a C-Frobenius group then:*

(a) *Every prime divisor of $|C|$ is strictly smaller than any prime divisor of $|K|$.*
(b) *K is of odd order.*

(c) *Any quotient group $\overline{F}$ of F is either a quotient of C or a $\overline{C}$-Frobenius group, where $\overline{C}$ is the image of C in $\overline{F}$.*
(d) *Let $\hat{K} \to K$ be an epimorphism of procyclic groups of orders divisible by the same primes. Suppose that C acts on $\hat{K}$ such that $\hat{K} \to K$ is C-equivariant. Then $C \ltimes \hat{K}$ is also a C-Frobenius group.*
(e) *Every subgroup of F is a conjugate of C_1K_1, where $C_1 \leq C$ and $K_1 \leq K$.*
(f) *A subgroup of F is normal if and only if it is either a subgroup of K or of the form C_1K, where $C_1 \leq C$. In particular, a minimal normal subgroup of F is a minimal subgroup of K.*
(g) *Let $C_1 \leq C$, $K_1 \leq K$, and $f \in F$. Then*

$$C_1^f K_1 \cap K = K_1 \qquad \textit{and} \qquad C_1^f K_1 \cap C = \begin{cases} C_1 & \textit{if } f \in CK_1 \\ 1 & \textit{if } f \notin CK_1. \end{cases}$$

Lemma 2.2. *Let $F = CK$ be a finite C-Frobenius group (with Frobenius kernel K). Suppose F acts transitively on a set Δ. Then*
(a) *There is $L \in \Delta$ such that its F-stabilizer is C_1K_1 with $C_1 \leq C$ and $K_1 \leq K$. Fix such L. Then*
(b) *C_1 is the C-stabilizer of L, and hence also of every L^c, with $c \in C$.*
(c) *Every point of $\Delta \smallsetminus \{L^c | c \in C\}$ has a trivial C-stabilizer.*

Proof. (a) Let $L \in \Delta$. Its F-stabilizer F_1 is, by Lemma 2.1(e), a conjugate of C_1K_1 for some $C_1 \leq C$ and $K_1 \leq K$. Replacing L by a conjugate we may assume that $F_1 = C_1K_1$.

(b),(c) By Lemma 2.1(g)

$$(L^f)^c = L^f \iff c \in (C_1K_1)^f \iff c \in C_1^f K_1 \cap C = \begin{cases} C_1 & \text{if } f \in CK_1 \\ 1 & \text{if } f \notin CK_1 \end{cases}$$

and $L^{CK_1} = L^{K_1C} = L^C$. □

3. Intravariant Subgroups

Definition 3.1. Let $H \leq G$ be groups and let A be a group acting on G from the right. We say that H is *A-intravariant in G* if for every $x \in A$ there is $g \in G$ such that $H^x = H^g$. We say that H is *an intravariant subgroup of G* if it is $\mathrm{Aut}(G)$-intravariant in G.

We point out that Sylow subgroups and their normalizers are intravariant subgroups. In the rest of this section we exhibit further families of intravariant subgroups of finite simple groups.

Recall that an *almost simple group* is a group G with a unique minimal normal subgroup S which is a nonabelian simple group. Thus, $S \triangleleft G \leq \mathrm{Aut}(S)$. We refer the reader to [1, 3, 6, 7] for the basic facts about automorphisms of finite simple groups.

We recall some facts about automorphisms of the finite simple groups and most especially about Chevalley groups. The most complicated cases to deal with are PSL and PSU.

Our first result is [9, 3.22].

Lemma 3.2. *Let S be a finite nonsolvable group. Let $x \in \mathrm{Aut}(S)$. Then $C_S(x) \neq 1$.*

The next result is the Borel-Tits Theorem [7, Theorem 3.1.3].

Lemma 3.3. *Let S be a simple Chevalley group and U a nontrivial unipotent subgroup. Let $A = \mathrm{Aut}(S)$. Then there exists a proper parabolic subgroup P of S such that U is contained in the unipotent radical of P and $N_A(P) \geq N_A(U)$.*

We remark that P is proper, since the unipotent radical of P is normal in P, while S is simple.

We also require:

Lemma 3.4. *Let $S \lhd G$ be finite groups. Let R be an r-subgroup of G for some prime r.*

(1) *If r divides $|S|$, then R normalizes some Sylow r-subgroup of S.*
(2) *If r does not divide $|S|$ but another prime p does divide $|S|$, then R normalizes a Sylow p-subgroup of S.*

Proof. Let Q be a Sylow r-subgroup of G containing R. Then R normalizes $Q \cap S$, which gives (1).

To prove (2), let P be a Sylow p-subgroup of S. By Sylow's theorem, $G = SN_G(P)$. Since r does not divide $|S|$, $N_G(P)$ contains a Sylow r-subgroup of G, say, Q^g, with $g \in G$. Then $R \leq Q \leq N_G(P^{g^{-1}})$, that is, R normalizes $P^{g^{-1}}$. □

We now examine PSL and PSU more closely. Let $S = \mathrm{PSL}(d, p^e)$, where p is a prime and S is simple. Let σ be the Frobenius automorphism and τ the graph automorphism (which we may view as the inverse transpose map) of S. Then

$$\Omega = \mathrm{PGL}(d, p^e) \cup \{\sigma, \tau\}$$

generates $A = \mathrm{Aut}(S)$. Moreover, $\mathrm{PGL}(d, p^e)\langle\sigma\rangle$ is of index 2 in A.

We will use the following elementary result from linear algebra.

Lemma 3.5. *Let F be a finite field. Let $B \in \mathrm{M}_d(F)$ be semisimple. Let $a \in F$. Then there is $B' \in \mathrm{M}_d(F)$ such that $BB' = B'B$ and $\det(B') = a$.*

Proof. First assume that the minimal polynomial g of B is of degree d and irreducible. Then $K := F[B] \cong F[X]/(g)$ is a finite field extension of F. Hence the norm $N_F^K\colon K \to F$ is surjective. Let $B' \in K$ such that $N_F^K(B') = a$. View B' as a matrix (since $F[B] \subseteq \mathrm{M}_d(F)$). Then B' commutes with B and $a = N_F^K(B') = \det(B')$ [2, Chapter III, §9.4, Proposition 6].

In the general case we may assume that B is in rational canonical form. Thus $B = \mathrm{diag}(B_1, \dots, B_r)$, where each $B_i \in \mathrm{M}_{d_i}(F)$ has minimal polynomial irreducible of degree d_i. By the previous case there is $B_i' \in \mathrm{M}_{d_i}(F)$ that commutes with B_i and $\det(B_1') = a$ and $\det(B_i') = 1$ for $i > 1$. Then $B = \mathrm{diag}(B_1', \dots, B_r')$ commutes with B and $\det(B') = a$. $\square$

Lemma 3.6. *Let $S = \mathrm{PSL}(d, p^e)$ and $H = \mathrm{PGL}(d, p^e)$. Put $A = \mathrm{Aut}(S)$.*

(1) *Any parabolic subgroup P of S whose normalizer contains an element outside of $H\langle\sigma\rangle$ is intravariant.*
(2) *If $h \in H$ is a semisimple element (i.e. has order prime to p), then $\langle h\rangle$ is A-intravariant in H.*
(3) *If $h \in H$ is semisimple, then $C_S(h)$ and $N_S(\langle h\rangle)$ are intravariant subgroups of S.*

Proof. (1) We may conjugate P in S and thus assume that P contains the standard Borel subgroup of S that consists of upper triangular matrices of determinant 1. Clearly, diagonal matrices and σ normalize P. Hence P is an intravariant subgroup of S if and only if $N_A(P)$ contains an element outside of $H\langle\sigma\rangle$.

(2) Let $x \in A$. We have to show that there is $s \in H$ such that $\langle h\rangle^x = \langle h\rangle^s$. We may assume that $x \in \Omega$. If $x \in H$, the assertion is trivial. So assume that either $x = \sigma$ or $x = \tau$. Put $F = \mathbb{F}_{p^e}$. Lift h to a semisimple element of $\mathrm{GL}(d, F)$. It suffices to show that there is $m \in \mathbb{Z}$ such that h^x, h^m are conjugate in $\mathrm{GL}(d, F)$, i.e., similar over F.

Since every square matrix is similar over F to its transpose, h^τ is similar to h^{-1}. On the other hand, h^σ is similar over F to h^p. Indeed, consider $\mathrm{GL}(d, F)$ as a subgroup of $\mathrm{GL}(d, \overline{F})$ and extend σ to the Frobenius automorphism of $\mathrm{GL}(d, \overline{F})$. There is $z \in \mathrm{GL}(d, \overline{F})$ such that $h^z \in \mathrm{GL}(d, \overline{F})$ is diagonal. Then clearly $(h^z)^\sigma = (h^z)^p$. Therefore $(h^\sigma)^{z^\sigma} = (h^z)^\sigma = (h^z)^p = (h^p)^z$. Hence h^σ, h^p are similar over $\overline{F}$. Therefore they are similar over F.

(3) Let $x \in A$. By (2) there is $s \in H$ such that $\langle h\rangle^x = \langle h\rangle^s$. By Lemma 3.5 there is $z \in H$ such that $zh = hz$ and $\det(z) \equiv \det(s) \pmod{(F^\times)^d}$. Replace s by $z^{-1}s$ to get that $s \in S$. As $C_S(h) = S \cap C_H(h)$, $N_S(h) = S \cap N_H(h)$, and $S^x = S = S^s$, we get $C_S(h)^x = C_S(h)^s$ and $N_S(h)^x = N_S(h)^s$. $\square$

Proposition 3.7. *Let $S = \mathrm{PSL}(n, p^e)$ be simple. Then every $x \in \mathrm{Aut}(S)$ normalizes a nontrivial proper intravariant subgroup of S.*

Proof. Let $H = \mathrm{PGL}(n, p^e)$. If $C_H(x)$ is not a p-group, we may choose $1 \neq h \in C_H(x)$ of order prime to p. Thus, h is semisimple and $C_S(h)^x = C_S(h^x) = C_S(h)$. By Lemma 3.6(3), $C_S(h)$ is an intravariant subgroup of S. By Lemma 3.2, $C_S(h) \neq 1$; clearly $C_S(h) \neq S$. So we may assume that $C_H(x)$ is a p-group (i.e. consists of unipotent elements). In particular, $C_H(x) \leq S$, whence $C_S(x) = C_H(x)$.

If $x \in \mathrm{Aut}(S) \smallsetminus H\langle\sigma\rangle$, then, by Lemma 3.3, x normalizes some proper parabolic subgroup of S which is intravariant by Lemma 3.6(1).

If x is in H, then $x \in C_H(x) \leq S$, so x is contained in some Sylow p-subgroup of S, which is intravariant.

So we may assume that $x \in H\langle\sigma\rangle \smallsetminus H$. Write $x = yz = zy$, where $y \in \langle x\rangle$ has order prime to p and $z \in \langle x\rangle$ has order a power of p. The restriction to $\langle y\rangle$ of the projection $H\langle\sigma\rangle \to \langle\sigma\rangle$ is injective, because its kernel $H \cap \langle y\rangle$ is contained in the p-group $C_H(x)$. Thus, writing y as $\sigma^j h$, with some $h \in H$, we see that y and σ^j have the same order. By Shintani descent [6, p. 81] they are conjugate by an element of H. Since $C_H(\sigma^j)$ contains the Jordan matrix $J_n(1)$, it follows that $C_H(y)$ contains a regular unipotent element (a conjugate of $J_n(1)$).

As z commutes with y, it normalizes $C_H(y)$. Its order is a power of p, and so z normalizes some Sylow p-subgroup T of $C_H(y)$. But y centralizes T and so $x = yz$ normalizes T. Since T contains a regular unipotent element, T is contained in a unique Sylow p-subgroup P of H. As $T = T^x \leq P^x$, we have $P^x = P$. Thus x normalizes this intravariant subgroup. □

The same result holds for $S = \mathrm{PSU}(d, p^e)$.

Lemma 3.8. *Let $S = \mathrm{PSU}(d, p^e)$ be simple. If $x \in \mathrm{Aut}(S)$, then x normalizes a nontrivial proper intravariant subgroup of S.*

Proof. In this case $\mathrm{Aut}(S) = H\langle\sigma\rangle$, where $H = \mathrm{PGU}(d, p^e)$ and σ is the Frobenius automorphism of order $2e$. Let $x \in \mathrm{Aut}(S)$. If $C_H(x)$ contains a nontrivial semisimple element h, then $C_S(h)$ is an intravariant subgroup normalized by x. Otherwise, $C_H(x)$ is unipotent and by Lemma 3.3, x normalizes some (proper) parabolic subgroup of S. In this case, all parabolics are intravariant, whence the result. □

The analogous result is true for almost all of the families of simple groups. However, it is not true for $S = \Omega^+(8, q)$. Take $x \in S$ of order $(q^4 - 1)/\gcd(2, q-1)$. It is not difficult to see that x is contained in no maximal subgroup of $\mathrm{Aut}(S)$ not containing S, whence it cannot normalize any nontrivial intravariant subgroup of S. If we only consider cyclic groups of automorphisms of simple groups which do not contain any inner automorphisms, then the result is true. We will revisit this topic in a future paper. It is not required for the results of this paper.

The outer automorphism groups of the other simple groups are less complicated. It is convenient to use the notation $\mathrm{PSL}^\epsilon(d, q)$ with $\epsilon = \pm$—here PSL^+ means PSL and PSL^- means PSU.

Lemma 3.9. *Let G be an almost simple finite group with socle S. Suppose that G/S is a Frobenius group with a cyclic Frobenius kernel K and a cyclic Frobenius complement C. If $|C| > 3$, then $S \cong \mathrm{PSL}^\epsilon(d, q)$ and the Frobenius kernel is contained in the subgroup of diagonal automorphisms of* $\mathrm{Out}(S)$. *Moreover, $d \geq 5$ and $q > 5$.*

Proof. We have $G/S \leq \mathrm{Out}(S)$. If S is an alternating or sporadic group, then $\mathrm{Out}(S)$ and hence also G/S has exponent 2, a contradiction to G/S being Frobenius. So S is a Chevalley group.

Let r be a prime dividing $|K|$. By Lemma 2.1, $|C|$ divides $r-1$. As $|C|>3$, we have $r\geq 5$. As K is cyclic, C normalizes its Sylow r-subgroup. If S is not $\mathrm{PSL}^{\epsilon}(d,q)$, then the Sylow r-subgroup of K consists of field automorphisms. However, the normalizer in $\mathrm{Out}(S)$ of a field automorphism is its centralizer. Thus, C centralizes a nontrivial subgroup of K, a contradiction to $G/S=C\ltimes K$ being Frobenius. This proves that $S\cong\mathrm{PSL}^{\epsilon}(d,q)$. Arguing similarly, it follows that K consists of diagonal automorphisms and so $r|\gcd(d,q-\epsilon 1)$, whence $d\geq 5$ and $q>5$. □

We can now show:

Corollary 3.10. *Let G be an almost simple finite group with socle S. Suppose that G/S is a Frobenius group with cyclic Frobenius kernel K and cyclic Frobenius complement C. Let D be any cyclic subgroup of G with $DS/S=C$. If C has prime power order, assume the same is true of D. Then D normalizes a proper nontrivial intravariant subgroup H of S.*

Proof. If $|C|$, and hence also $|D|$, is a prime power, then D normalizes a nontrivial Sylow subgroup of S by Lemma 3.4. Otherwise, $|C|>3$, and hence by Lemma 3.9, S is either PSL or PSU. Now apply Proposition 3.7 and Lemma 3.8. □

4. Lifting Frobenius Groups

To show our main result we need some preparations.

Lemma 4.1. *Let $\rho_1\colon F_1\to F_3$ and $\rho_2\colon F_2\to F_3$ be C-epimorphisms of C-Frobenius groups. Then $F_1\times_{F_3}F_2$ contains a C-Frobenius group mapped onto F_1.*

Proof. Let K_i be the Frobenius kernel of F_i, and $K_i^{(p)}$ its Sylow p-subgroup, respectively, for $i=1,2,3$ and for each prime p. Put $F=F_1\times_{F_3}F_2$. We identify C with $C\times_{F_3}C$ and thus F is a C-group and the coordinate projections $F\to F_1$, $F\to F_2$ are C-epimorphisms. Clearly every $1\neq c\in C$ acts fixed-point-freely on the abelian subgroup $K=K_1\times_{F_3}K_2$ of F. For each prime p we find below a cyclic p-subgroup $\langle k_p\rangle$ of K normalized by C and mapped by $F\to F_1$ onto $K_1^{(p)}$. Then $C\big(\prod_p\langle k_p\rangle\big)$ is a C-Frobenius group mapped onto F_1.

Fix a generator k_1 of $K_1^{(p)}$ and put $k_3=\rho_1(k_1)$. By Sylow's theorem, $\rho_1(K_1^{(p)})=K_3^{(p)}=\rho_2(K_2^{(p)})$. So there is $k_2\in K_2^{(p)}$ such that $k_3=\rho_2(k_2)$. If $k_3=1$, take $k_2=1$; otherwise k_2 generates $K_2^{(p)}$. Then $k=(k_1,k_2)\in F$ and $\langle k\rangle\leq F$ is normalized by C, that is, $(k_1^c,k_2^c)\in\langle k\rangle$, where c is a generator of C.

Indeed, if $k_2=1$, the assertion is clear. So assume that $k_2\neq 1$ and hence $k_3\neq 1$.

Let $i=1,2,3$. Writing $K_i^{(p)}$ additively, it is a quotient of $\mathbb{Z}_p$ so that k_i is the class of the generator 1 of $\mathbb{Z}_p$ and $\rho_1\colon K_1^{(p)}\to K_3^{(p)}$, $\rho_2\colon K_2^{(p)}\to K_3^{(p)}$

are the quotient maps. As the order of c is prime to p, there is a unique $m_i \in (\mathbb{Z}_p)^\times$ such that c acts on $K_i^{(p)}$ by multiplication by the image of m_i. But ρ_1, ρ_2 are C-equivariant, hence $m_1 = m_3 = m_2$. Thus $(k_1^c, k_2^c) = (m_1 k_1, m_2 k_2) = m_1 k \in \langle k \rangle$, □

We show that in one case we can lift arbitrary finite Frobenius groups.

Lemma 4.2. *Let G be a finite group and A a minimal normal subgroup of G. Assume that A is an elementary abelian p-group and G/A is a Frobenius group. Let C be a subgroup of G such that $G \to G/A$ maps C isomorphically onto a Frobenius complement of G/A. Assume that the Frobenius kernel of G/A does not centralize A. Then $G = HA$ with $C \le H$ and $A \cap H = 1$.*

Proof. We write every subgroup of G/A as N/A, where $A \le N \le G$. Let M/A be the Frobenius kernel of G/A.

We first claim that if $L \le M$ acts nontrivially on A and $LA \triangleleft G$ then $C_A(L) = C_A(LA) = 1$. Indeed, $C_A(L) \le C_A(LA) \triangleleft G$ and $C_A(LA) \lneqq A$. So the claim follows by the minimality of A.

Since M acts nontrivially on A, so does some Sylow r-subgroup R of M. By Thompson's theorem M/A is nilpotent, hence its Sylow r-subgroup RA/A is normal in G/A. By the above claim, $C_A(R) = 1$. Also, $A \cap Z(RA) = C_A(RA) = 1$, whence $r \neq p$. By Sylow's theorem, $G = N_G(R)RA = N_G(R)A$. Note that $N_A(R) = C_A(R)$, hence $N_G(R) \cap A = N_A(R) = 1$. Thus $H := N_G(R)$ is a complement of A in G (an alternative way to see that A has a complement is to observe that $H^i(G/A, A) = 0$ for all $i \ge 0$), whence $H \cong G/A$.

Let D be the preimage of C/A in H. Then $AC = AD$. So it suffices to show that $H^1(D, A) = 0$, whence C and D are conjugate and the result follows by replacing H with a conjugate that contains C.

Let $R_0 = C_R(A)$. By the choice of R, the r-group R/R_0 is not trivial. Let R_1/R_0 be its center. Then $R_1/R_0 \neq 1$. Let $B = A \otimes_{\mathbb{F}_p} k$ where k is the algebraic closure of $\mathbb{F}_p$. Then R_1 acts as an abelian group on B. Write $B = \oplus B_i$, where B_i are the eigenspaces of R_1 on B, corresponding to linear characters of R_1/R_0. Note that $R_1 A \triangleleft G$ and R_1 acts nontrivially on A. Hence by the claim above $C_A(R_1) = 1$, whence R_1 has no fixed points on B. Thus each B_i has a nontrivial character. Since $(R_1/R_0)D$ is also a Frobenius group, D freely permutes the nontrivial linear characters of R_1, whence D freely permutes the B_i. Thus, B (and so also A) is a free D-module (see also [8, Lemma 2.1(3)]). In particular, $H^1(D, A) = 0$ as required. □

In the general case, we cannot always lift a Frobenius group: E.g., consider $G = \mathrm{SL}(2, 3)$ with $|A| = 2$). However, in the case we need, we have:

Lemma 4.3. *Let G be a finite C-group and A a minimal normal subgroup of G. Assume that A is an elementary abelian p-group and G/A is a C-Frobenius group. Then G contains a C-Frobenius group H such that $G = HA$.*

Proof. We have $A \cap C = 1$. Put $F = G/A$ and let K be the Frobenius kernel of F. Let $A \leq M \triangleleft G$ such that $K = M/A$. So $G = C \ltimes M$. For each prime r let K_r be the Sylow r-subgroup of K and let M_r be a Sylow r-subgroup of M such that $M_r A/A = K_r$. As A acts trivially on itself, F acts on A, and A is an irreducible F-module.

If K acts nontrivially on A, the result follows by the previous lemma. So assume that K does act trivially on A. As K is cyclic, M is abelian. It suffices to find, for each prime r dividing $|K|$, a cyclic r-subgroup L_r of M, normalized by C, such that $L_r A/A = K_r$. Indeed, then $H = (\prod_r L_r)C$ is a C-Frobenius group mapped onto F.

Since M is abelian, M_r is normalized by C. So if M_r is cyclic, take $L_r = M_r$. This is certainly the case if $r \neq p$, since then $M_r \cong K_r$. So let $r = p$ with M_p not cyclic and $K_p \neq 1$. Thus, $|C|$ divides $p - 1$. Hence every vector space over $\mathbb{Z}/p\mathbb{Z}$ on which C acts is the direct sum of 1-dimensional C-modules. Since C acts irreducibly on A, this implies that $|A| = p$.

As K_p and A are cyclic and M_p is not, M_p is of rank 2, whence its Frattini quotient $\overline{M_p}$ is of dimension 2. In particular, the image $\overline{A}$ of A in $\overline{M_p}$ is of dimension 1. Thus, by complete reducibility, $\overline{M_p} = \overline{A} \oplus \overline{B}$ for some 1-dimensional C-module $\overline{B}$. Choose a cyclic subgroup L_p of M_p such that its image in $\overline{M_p}$ is $\overline{B}$. Then, L_p is normalized by C and $M_p = L_p A$, whence $L_p A/A = K_p$. □

Lemma 4.4. *Let G be a finite group and let $A \triangleleft G$. Assume that $A = \prod_{i=1}^t Q_i$ and the conjugation in G transitively permutes the Q_i. Let $G_1 = N_G(Q_1)$ and for each right coset Z of G_1 in G let $\widehat{Z} \in Z$. Let U_1 be a G_1-intravariant subgroup in Q_1. Then $U := \prod_Z U_1^{\widehat{Z}} \leq A$ is G-intravariant in A. Moreover, if U_1 is not normal in Q_1 then U is not normal in A.*

Proof. We have $\{Q_i\}_{i=1}^t = \{Q_1^{\widehat{Z}}\}_{Z \in G/G_1}$. Thus $A = \prod_{Z \in G/G_1} Q_1^{\widehat{Z}}$ and hence $U \leq A$.

To show the intravariance, let $g \in G$. For each $Z \in G/G_1$ we have $Q_1^{\widehat{Z} g \widehat{Zg}^{-1}} = Q_1$, hence $\widehat{Z} g \widehat{Zg}^{-1} \in G_1$. Thus there is $b_Z \in Q_1$ such that $U_1^{\widehat{Z} g \widehat{Zg}^{-1}} = U_1^{b_Z}$. Put $a_Z = \widehat{Zg}^{-1} b_Z \widehat{Zg}$, then $a_Z \in Q_1^{\widehat{Zg}}$ and $U_1^{\widehat{Z} g} = (U_1^{\widehat{Zg}})^{a_Z}$. Thus $a := \prod_{Z \in G/G_1} a_Z \in A$ and $U^g = U^a$.

The last assertion is clear. □

Lemma 4.5. *Assume, in the situation of the preceding lemma, that G is a C-group such that G/A is a C-Frobenius group. Let $C_1 = N_C(Q_1) = C \cap G_1$ and assume that $G_1/A = C_1 K_1$ for some subgroup K_1 of the Frobenius kernel of G/A. Assume that U_1 is C_1-invariant. Then we may choose the $\widehat{Z} \in Z$ so that U is C-invariant.*

Proof. It suffices to choose the representatives $\widehat{Z}$ so that

$$U_1^{\widehat{Zc}} = U_1^{\widehat{Z}c} \text{ for every } c \in C. \tag{1}$$

But to achieve (1), it suffices to achieve it only for a representative Z of each C-orbit in G/G_1 (when G and $C \le G$ act on G/G_1 by multiplication from the right). Let C_Z be the C-stabilizer of Z and let R_Z be a set of representatives of C/C_Z in C. Suppose we have found $\widehat{Z} \in Z$ such that C_Z normalizes $U_1^{\widehat{Z}}$. Then put $\widehat{Zcr} = \widehat{Z}r$ for all $c \in C_Z$ and $r \in R_Z$ to get (1).

As G acts transitively on G/G_1 with A acting trivially, this induces a transitive action of $F = G/A$ on G/G_1 and the F-stabilizer of G_1 is C_1K_1. By Lemma 2.2 either $Z = G_1c$ for some $c \in C$ and $C_Z = C_1$ or $C_Z = 1$. In the former case we may take $\widehat{Z} = c$ to make C_Z normalize $U_1^{\widehat{Z}}$. In the latter case we may choose $\widehat{Z}$ arbitrarily. $\square$

We now prove the main step:

Theorem 4.6. *Let G be a finite group with a normal subgroup A and a cyclic subgroup C such that $C \cap A = 1$ and G/A is a C-Frobenius group. Then G contains a C-Frobenius group H such that $G = HA$.*

Proof. Put $F = G/A$ and let K be its Frobenius kernel. We identify CA/A with C.

We prove the result by induction on the order of A. We may assume that $A \ne 1$. We divide the proof into several parts.

Part A *We may assume that A is a minimal normal subgroup of G.* Let B be a minimal normal subgroup G contained in A. By induction, G/B satisfies the theorem with $A/B \triangleleft G/B$. Thus there is a subgroup H_0 of G containing B and C such that $H_0A = G$ and H_0/B is a C-Frobenius group. If $B \ne A$, apply the induction to H_0 with $B \triangleleft H_0$ to get a C-Frobenius subgroup H of H_0 such that $H_0 = HB$. Then $HA = H_0A = G$. So we may assume that $B = A$.

Part B Thus A is the direct product of copies of a finite simple group. If A is an elementary abelian p-group with p prime, then we are done by Lemma 4.3. So we may assume that $A = Q_1 \times \ldots \times Q_t$ where $Q_i = Q$ is a nonabelian simple group.

Part C *We may assume that G acts faithfully on A, that is, $G \to \mathrm{Aut}(A)$ is an embedding.* Indeed, otherwise let B be a minimal normal subgroup of G contained in the kernel of this map. Then $A \cap B = 1$, and hence B is isomorphic to a subgroup of G/A. In particular, B is solvable. Moreover, the image of B in G/A is a minimal normal subgroup, and hence is contained in K by Lemma 2.1(f). Thus, $AB \cap C = 1$. This allows us to identify C with CAB/AB.

The quotient G/AB of G/A either equals to C (that is, $G = ABC$) or is a C-Frobenius group with $|G/AB| < |G/A|$. In both cases there is a solvable subgroup G_0 of G containing C and B, such that $G_0A/B = G/B$: In the first case take $G_0 = CB$. In the second case proceed by subinduction on $|G/A|$; by the hypothesis, there is a subgroup G_0 of G containing C and B, such that $G_0A/B = G/B$ and G_0/B is CB/B-Frobenius. In particular, G_0/B is solvable, hence so is G_0. In both cases, as $G_0A = G$, we may replace

G by G_0 and A by $A \cap G_0$. As G_0 is solvable but A not, $|A \cap G_0| < |A|$. So the existence of H follows by induction.

Part D *Reduction to intravariance.* Our aim is to construct a subgroup U of A such that U is A-intravariant in G, C normalizes U, and A does not normalize U. Then $N_G(U)A = G$ and $N_G(U) \cap A$ is a proper subgroup of A. Hence by induction hypothesis $N_G(U)$ contains a C-Frobenius subgroup H with $HA = G$.

Part E *Division into three cases.* So let $G_1 = N_G(Q_1)$. Then $A \leq G_1$; put $F_1 = G_1/A \leq F$. Note that $F = G/A$ acts transitively on the set $\Delta := \{Q_1, \ldots, Q_t\}$, and F_1 is the stabilizer of Q_1. By Lemma 2.1(e) we may replace Q_1 by some conjugate Q_i to assume that $F_1 = C_1K_1$, where $C_1 \leq C$ and $K_1 \leq K$. We divide the rest of the proof into three cases.

Case I: C_1 centralizes Q_1. In this case let $U_1 \neq 1$ be a Sylow subgroup of Q_1. Then U_1 is C_1-invariant, intravariant in Q_1, and not normal in Q_1. By Lemma 4.4 and Lemma 4.5 there is a C-invariant G-intravariant subgroup U of A which is not normal in A. (Notice that case $C_1 = 1$ is included here.)

Case II: $C_1, K_1 \neq 1$. In this case F_1 is a C_1-Frobenius group. Let $\phi\colon G_1 \to \mathrm{Aut}(Q_1)$ be the map induced by the action of G_1 on Q_1 and let $\overline{G}_1 = \phi(G_1)$. Then $\phi(A) = \phi(Q_1) = Q_1$, hence ϕ induces a surjection $\overline{\phi}\colon F_1 = \overline{G}_1/A \to \overline{G}_1/Q_1 \leq \mathrm{Out}(Q_1)$. We first claim that $\overline{\phi}$ is an isomorphism, that is, $F_1 \to \mathrm{Out}(Q_1)$ is injective.

It suffices to show that $K_1 \to \mathrm{Out}(Q_1)$ is injective, since the kernel of $F_1 \to \mathrm{Out}(Q_1)$ is a normal subgroup of the Frobenius group F_1, which does not intersect its Frobenius kernel K_1 and hence is trivial by Lemma 2.1(f).

So let $g \in G$ with image in K_1 act on Q_1 as an inner automorphism. As $F = G/A$ is a Frobenius group, for every $\sigma \in G$ we have $\sigma g \sigma^{-1} = g^m a$ for some $m \in \mathbb{N}$ and $a \in A$. It follows that g acts as an inner automorphism, namely $(g^\sigma)^m a^\sigma$, on Q_1^σ. Thus g acts as an inner automorphism on A. As G acts faithfully on A, this means that $g \in A$. Therefore the image of g in K_1 is trivial. This proves the claim.

Thus $\overline{G}_1/Q_1 \cong F_1$ is a C_1-Frobenius group. By Corollary 3.10, C_1 normalizes some nontrivial intravariant proper subgroup U_1 of Q_1. So again we are done by Lemma 4.4 and Lemma 4.5.

Case III: $K_1 = 1$ and C_1 does not centralize Q_1. In particular, C does not centralize Q_1. Notice that $G_1 = C_1A \leq CA$. For each $g \in G$ let $\Delta_g = \{Q_1^{\sigma g} | \sigma \in CA\} \subseteq \Delta$. Then $\Delta_{g_1} \cap \Delta_{g_2} \neq \emptyset \implies CAg_1 = CAg_2 \implies \Delta_{g_1} = \Delta_{g_2}$. Thus Δ is the disjoint union of the distinct Δ_g. Therefore if we define $\tilde{Q}_g = \langle Q_1^{\sigma g} | \sigma \in CA\rangle$, then A is the direct product of the distinct $\tilde{Q}_g$. The conjugation in G permutes the Δ_g and hence also the $\tilde{Q}_g$. Put $\tilde{G}_1 = N_G(\tilde{Q}_1)$; then $\tilde{G}_1 = CA$. Thus $\tilde{C}_1 = C \cap \tilde{G}_1 = C$.

We define $U_1 = C_{\tilde{Q}_1}(\tilde{C}_1)$; thus U_1 is a $\tilde{C}_1$-invariant subgroup of $\tilde{Q}_1$. By our assumption, $U_1 \neq \tilde{Q}_1$. By Lemma 3.2, $U_1 \neq 1$. As $\tilde{G}_1 = \tilde{C}_1 A = \tilde{C}_1(\tilde{Q}_1 \times \prod_{\tilde{Q}_g \neq \tilde{Q}_1} \tilde{Q}_g)$ and U_1 is $\tilde{C}_1$-invariant, U_1 is $\tilde{G}_1$-intravariant in $\tilde{Q}_1$.

Now apply again Lemma 4.4 and Lemma 4.5 with $\{\tilde{Q}_g | g \in G\}$ instead of Δ and with $\tilde{Q}_1, \tilde{G}_1, \tilde{C}_1$ instead of Q_1, G_1, C_1.

□

Remark 4.7. If C is an r-group for some prime r, we may considerably simplify the proof of Theorem 4.6, leaving out the classification of finite simple groups. Mainly, omit Part C and replace Part E by the following:

Let M be the normal subgroup of G such that $M/A = K$. By Lemma 3.4, C normalizes some nontrivial Sylow subgroup U of M. By Frattini argument, U is intravariant in G.

5. Profinite Groups

Theorem 5.1. *Let G be a C-group and let $G \to F$ be a C-epimorphism onto a C-Frobenius group F. Then G contains a C-Frobenius subgroup H that maps onto F. Moreover, we may assume that F and H have precisely the same prime divisors.*

Proof. The last assertion of the theorem follows immediately from the rest, because we may drop from the Frobenius kernel of H its p-primary components for those primes p that do not divide the order of the Frobenius kernel of F.

If necessary, replace G by a closed subgroup to assume that G is finitely generated. Then there is a sequence $N_0 \geq N_1 \geq N_2 \geq \dots$ of open normal subgroups of G such that $\bigcap_i N_i = \{1\}$. Let $A = \ker(G \to F)$. Since $\bigcap_i N_i A = A$, without loss of generality $C \cap N_i A = \{1\}$ for every i.

Put $M_i = N_i \cap A$ for every i. Then $F = G/M_0$ and $G = \varprojlim_i G/M_i$. For each i we have the following cartesian diagram of epimorphisms of C-groups

$$\begin{tikzcd}
G/M_{i+1} \arrow[r] \arrow[d] & G/N_{i+1} \arrow[d] \\
G/M_i \arrow[r] & G/M_i N_{i+1}
\end{tikzcd}$$

in which the groups on the right handed side are finite. By induction hypothesis G/M_i contains a C-Frobenius subgroup F_i that maps onto F. Its image in $G/M_i N_{i+1}$ is a C-Frobenius subgroup. By Theorem 4.6 it lifts to a C-Frobenius subgroup of G/N_{i+1}. Hence by Lemma 4.1 F_i lifts to a C-Frobenius subgroup F_{i+1} of G/N_{i+1}. Thus $H = \varprojlim_i F_i$ is a C-Frobenius subgroup of G that maps onto F. □

Corollary 5.2. *Let $\beta\colon B \to C$ be an epimorphism of a finite group B onto a finite nontrivial cyclic group C and let F be a C-Frobenius group with Frobenius kernel $K \cong \hat{\mathbb{Z}}_\pi$ for some set π of primes. Then there is a C-embedding $F \to B \coprod C$.*

Proof. By Theorem 5.1 it suffices to construct a C-epimorphism $B \coprod C \to F$. Let k be a generator of K. The epimorphism $B \to C$ given by $b \mapsto \beta(b)^k$ together with the identity map $C \to C$ define a C-homomorphism $B \coprod C \to F$. Its image $\langle C, C^k \rangle$ contains C and $(c^k)^{-1}c = k^{-1}k^c \in K$, where c is a generator of C. Since $F = CK$, it suffices to show that $k^{-1}k^c$ generates K.

If this assertion holds for each Sylow subgroup of K (and its generator instead of k) then it holds for K. Thus we may assume that $K \cong \mathbb{Z}_p$ for some prime p. Finally, we may replace K by its Frattini quotient. $\overline{K} \cong \mathbb{Z}/p\mathbb{Z}$.

As $c \neq 1$, we have $k^{-1}k^c \neq 1$ and hence $k^{-1}k^c$ generates K. □

Example 5.3. Let $K = \mathbb{Z}_7$. Then $C = \mathbb{Z}/6\mathbb{Z}$ acts fixed-point freely on K and hence the semidirect product $F = CK$ is a C-Frobenius group. By the corollary there is an embedding $\lambda\colon F \to G_1 \coprod G_2$, where $G_1 = G_2 = C$, such that $\lambda(C) = G_2$. Let $H = \lambda(F)$. Then H is prosolvable, but

(1) $H \cap G_2 = G_2$ is of order 6, and hence is not an ℓ-group for some prime ℓ;
(2) H is infinite, and hence $H \leq G_i^\sigma$ for no $i \in I$ and no $\sigma \in G$.

This answers the question of Pop mentioned in the introduction.

References

[1] M. Aschbacher and G. Seitz, Involutions in Chevalley groups over fields of even order, Nagoya Math. J. 63 (1976); Correction, Nagoya Math. J. 72 (1978), 135–136.
[2] N. Bourbaki, Elements of Mathematics, Algebra I, Springer-Verlag, Berlin Heidelberg New York, 1989.
[3] R. Carter, Simple groups of Lie type, Wiley Classics Library, John Wiley & Sons, Inc, New York, 1989.
[4] M. D. Fried and M. Jarden, Field Arithmetic, Third Edition, revised by Moshe Jarden, Ergebnisse der Mathematik (3) 11, Springer-Verlag, Heidelberg, 2008.
[5] M. Fried, R. Guralnick and J. Saxl, Schur covers and Carlitz's conjecture, Israel J. Math. 82 (1993), 157–225.
[6] D. Gorenstein and R. Lyons, The local structure of finite groups of characteristic 2-type, Memoirs Amer. Math. Soc. 42 (1983), Number 276.
[7] D. Gorenstein, R. Lyons and R. Solomon, The Classification of Finite Simple Groups, Number 3, Mathematics Surveys and Monographs 40, Amer. Math. Soc., Providence, RI, 1998.
[8] R. Guralnick, Frobenius groups as monodromy groups, J. Aust. Math. Soc. 85 (2008), 191–196.
[9] R. Guralnick, P. Müller and J. Saxl, The rational function analogue of a question of Schur and exceptionality of permutation representations, Mem. Amer. Math. Soc. 162 (2003), no. 773.
[10] W. Herfort and L. Ribes, Solvable subgroups of free products of profinite groups, Group theory (Singapore, 1987), 391–403, de Gruyter, Berlin, 1989.
[11] W. Herfort and L. Ribes, Frobenius subgroups of free products of prosolvable groups, Monatsh. Math. 108 (1989), 165–182.
[12] F. Pop, On prosolvable subgroups of profinite free products and some applications, Manuscripta Math. 86 (1995), no. 1, 125–135.
[13] T. Shintani, Two remarks on irreducible characters of finite general linear groups, J. Math. Soc. Japan 28 (1976), 396–414.

[14] L. Ribes and P. Zalesskii, Profinite groups. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) 40, Springer-Verlag, Berlin, 2000.

Department of Mathematics, University of Southern California, Los Angeles, CA 90089–2532, USA

E-mail address: guralnic@usc.edu

Sackler School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, ISRAEL

E-mail address: haran@post.tau.ac.il