Maximal abelian subgroups of free profinite groups

BY DAN HARAN AND ALEXANDER LUBOTZKY

Mathematisches Institut, Universität Erlangen, West Germany, and Institute of Mathematics, The Hebrew University, Jersualem, Israel

(*Received* 14 *May* 1984)

The aim of this note is to answer in the negative a question of W.-D. Geyer, asked at the 1983 Group Theory Meeting in Oberwolfach: Is a maximal abelian subgroup A of a free profinite group F necessarily isomorphic to $\hat{\mathbb{Z}}$, the profinite completion of $\mathbb{Z}$?

Of course, A is the direct product $\Pi_p A_p$ of its Sylow-p subgroups, and

$$\mathrm{cd}\,(A_p) \leqslant \mathrm{cd}\,(F) \leqslant 1$$

(where cd stands for cohomological dimension) for every p ([8], corollary 3·3). Thus A_p is a free pro-p-group ([8], theorem 6·5). As A_p is also abelian, it easily follows that either $A_p = 1$ or $A_p \cong \mathbb{Z}_p$, the free pro-p-group on one generator. Thus $A \cong \Pi_{p\in\pi}\mathbb{Z}_p$, where π is a set of primes. If π is the set of all primes then $\Pi_{p\in\pi}\mathbb{Z}_p \cong \hat{\mathbb{Z}}$.

We prove by way of converse the following result:

THEOREM. *Let F be the free profinite group on a set X, where $|X| \geqslant 2$, and let π be a non-empty set of primes. Then F has a maximal abelian subgroup isomorphic to $\Pi_{p\in\pi}\mathbb{Z}_p$.*

The idea of the proof is the following: we show that $A = \Pi_{p\in\pi}\mathbb{Z}_p$ is a free factor of $\hat{F}_\omega$, i.e. $\hat{F}_\omega \cong A * B$ for some profinite group B. To conclude from this that A is a maximal abelian subgroup of $\hat{F}_\omega$ (the general case then follows from this one), we show that

$$C_{A*B}(a) = C_A(a) \qquad (*)$$

for every $1 \neq a \in A$. To this end we embed $\hat{F}_\omega$ in the absolute Galois group of a certain algebraic field and then use some facts about the henselizations of this field. Thus our proof uses field theory in an essential way. We leave open the question whether (*) holds for arbitrary profinite groups A and B.

In this note $A * B$ always denotes the free product in the category of profinite groups of A and B. For basic information about this notion see [6].

We begin by proving some more properties:

Definition [7]. A discrete group Γ is called locally extended residually finite (LERF) if every finitely generated subgroup of Γ is an intersection of subgroups of finite index in Γ.

LEMMA 1. *The discrete free product of two finite groups is LERF.*

Proof. Let Γ be the discrete free product of finite groups A and B. The kernel K of the natural map $\Gamma \to A \times B$ is a free subgroup of Γ (by the Kurosh subgroup theorem [5], theorem 1·10, p. 178) of finite index in Γ. By a result of Hall ([7], theorem 2·2), K is LERF. Hence Γ is LERF by [7], lemma 1·1.

LEMMA 2. *Let Δ be a finitely generated subgroup of a LERF group Γ. Then the canonical* *map* $\hat{\imath}: \hat{\Delta} \to \hat{\Gamma}$ *extending the inclusion* $i: \Delta \to \Gamma$ *is injective.* (*Here* $\hat{\Gamma}$, $\hat{\Delta}$ *denote the profinite completions of* Γ, Δ, *respectively.*)

Proof. The Lemma asserts that the closure of Δ in $\hat{\Gamma}$ is isomorphic to $\hat{\Delta}$, i.e. the profinite topology of Γ induces the profinite topology of Δ. Thus we have to prove that if Δ_1 is a normal subgroup of finite index in Δ then there exists a normal subgroup of finite index Γ_1 in Γ such that $\Gamma_1 \cap \Delta \subseteq \Delta_1$.

Now Δ_1 is finitely generated, since Δ is finitely generated and $(\Delta:\Delta_1) < \infty$. But Γ is LERF, hence $\Delta_1 = \bigcap_{\alpha\in I}\Gamma_\alpha$, where $\{\Gamma_\alpha|\alpha\in I\}$ is the family of subgroups of finite index in Γ containing Δ_1. In particular $\Delta_1 = \bigcap_{\alpha\in I}(\Gamma_\alpha \cap \Delta)$. As $(\Delta:\Delta_1) < \infty$, there exists a finite subset J of I such that $\Delta_1 = \bigcap_{\alpha\in J}(\Gamma_\alpha \cap \Delta)$. Define $\Gamma_0 = \bigcap_{\alpha\in J}\Gamma_\alpha$ and $\Gamma_1 = \bigcap_{\gamma\in\Gamma}\Gamma_0^\gamma$. Clearly $(\Gamma:\Gamma_0) < \infty$; hence Γ_1 is a normal subgroup of finite index in Γ, and

$$\Gamma_1 \cap \Delta \subseteq \Gamma_0 \cap \Delta = \Delta_1.$$

LEMMA 3. *Let* $\{A_\alpha|\alpha\in I\}$ *and* $\{B_\beta|\beta\in J\}$ *be two inverse systems of profinite groups and put*

$$A = \varprojlim_{\alpha\in I} A_\alpha, \quad B = \varprojlim_{\beta\in J} B_\beta.$$

Then

$$A * B = \varprojlim_{(\alpha,\beta)\in I\times J} A_\alpha * B_\beta.$$

(*Here* $I\times J$ *is the inverse system for which* $(\alpha',\beta') \geqslant (\alpha,\beta)$ *iff* $\alpha' \geqslant \alpha$ *and* $\beta' \geqslant \beta$; *the maps are the obvious ones.*)

Proof. The group $A * B$ contains A and B as closed subgroups and satisfies the following universal property: Every pair of homomorphisms $\phi_1: A\to G$, $\phi_2: B\to G$ into a finite group G extends to a unique homomorphism $\phi: A*B\to G$. Clearly there exists $\alpha\in I$, $\beta\in J$ such that ϕ_1 factors through A_α and ϕ_2 through B_β. Therefore

$$\varprojlim_{(\alpha,\beta)\in I\times J} A_\alpha * B_\beta$$

has the above universal property.

PROPOSITION 4. *Let* A *and* B *be two profinite groups and* $A' \leqslant A$, $B' \leqslant B$ *closed subgroups. Then the map* $A' * B' \to A * B$ *induced by the inclusions* $A'\to A$, $B'\to B$, *is injective*, i.e. *the smallest closed subgroup* K *of* $A*B$ *containing* A' *and* B' *is isomorphic to* $A' * B'$. *Moreover,* $K\cap A = A'$.

Proof. To prove the first assertion of the Proposition we may assume that A and B are finite. Indeed, let $\{N_\alpha\}$ (resp. $\{M_\beta\}$) be the family of open normal subgroups of A (resp. B). Then

$$A' = \varprojlim_{\alpha} A'N_\alpha/N_\alpha \quad\text{and}\quad B' = \varprojlim_{\beta} B'M_\beta/M_\beta.$$

By Lemma 3,

$$A*B = \varprojlim_{(\alpha,\beta)} A/N_\alpha * B/M_\beta \quad\text{and}\quad A'*B' = \varprojlim_{(\alpha,\beta)} A'N_\alpha/N_\alpha * B'M_\beta/M_\beta.$$

But the map $A'*B'\to A*B$ is induced by the maps

$$A'N_\alpha/N_\alpha * B'M_\beta/M_\beta \to A/N_\alpha * B/M_\beta,$$

therefore it suffices to show that the latter is injective for every (α,β).

Let Γ (resp. Δ) be the discrete free product of the finite groups A and B (resp. A' and B'). Then $\hat{\Gamma} \cong A * B$, $\hat{\Delta} \cong A' * B'$, and the inclusions $A' \to A$ and $B' \to B$ induce the inclusion $i: \Delta \to \Gamma$. We have to show that $\hat{\imath}: \hat{\Delta} \to \hat{\Gamma}$ is also an inclusion. But Γ is LERF by Lemma 1, hence the assertion follows by Lemma 2.

Clearly $K \cap A \geqslant A'$. Conversely, let $a \in K \cap A$ and consider the map $\alpha: A * B \to A$ induced by the identity $A \to A$ and by the trivial map $B \to \{1\} \subseteq A$. It suffices to show that $\alpha(a) \in A'$, since α is injective on A. But $\alpha(K) = \alpha \circ \hat{\imath}(A' * B')$, and $\alpha \circ \hat{\imath}$ is induced by the inclusion $A' \to A$ and by the map $B' \to \{1\} \subseteq A$; hence $\alpha(K) = A'$. Thus $\alpha(a) \in A'$.

Let us fix a prime p and let v be the p-adic valuation of the rationals $\mathbb{Q}$. Let $(\mathbb{Q}_p, v_p)$ be the henselization of $(\mathbb{Q}, v)$, i.e. $\mathbb{Q}_p$ is the intersection of the field of p-adic numbers $\tilde{\mathbb{Q}}_p$ with the algebraic closure $\tilde{\mathbb{Q}}$ of $\mathbb{Q}$, and v_p extends v. Let $\tilde{v}$ be the unique extension of v_p to a valuation of the algebraic closure $\tilde{\mathbb{Q}}$ of $\mathbb{Q}$ (cf. [1], proposition 11). For a field F denote by $G(F) = \mathfrak{g}(\tilde{F}/F)$ its absolute Galois group.

LEMMA 5. *If* $\sigma \in G(\mathbb{Q})$ *then either* $\sigma \in G(\mathbb{Q}_p)$ *or* $\mathbb{Q}_p \mathbb{Q}_p^\sigma = \tilde{\mathbb{Q}}$.

Proof. Assume $\mathbb{Q}_p^\sigma = \mathbb{Q}_p$. Then the restriction $\bar{\sigma}$ of σ to $\mathbb{Q}_p$ is an automorphism of $\mathbb{Q}_p$, hence its fixed field K is henselian with respect to v_p (cf. [2], satz 1·7). But $\mathbb{Q}_p$ is a henselization of $\mathbb{Q}$, hence $K = \mathbb{Q}_p$, whence $\bar{\sigma} = 1$. Thus $\sigma \in G(\mathbb{Q}_p)$.

Assume $\mathbb{Q}_p^\sigma \neq \mathbb{Q}_p$. As $\mathbb{Q}_p$ (resp. $\mathbb{Q}_p^\sigma$) is the decomposition field of $\tilde{v}$ (resp. $\sigma\tilde{v}$) we have that $\tilde{v} \neq \sigma\tilde{v}$. This implies that the restrictions of $\tilde{v}$ and $\sigma\tilde{v}$ to $\mathbb{Q}_p \mathbb{Q}_p^\sigma$ are also distinct, since $\mathbb{Q}_p \mathbb{Q}_p^\sigma$ is henselian with respect to both of these valuations. Thus by a result of F.K. Schmidt ([2], Satz 1·5) $\mathbb{Q}_p \mathbb{Q}_p^\sigma = \tilde{\mathbb{Q}}$.

LEMMA 6. (*a*) $\hat{\mathbb{Z}}$ *is isomorphic to a subgroup of* $G(\mathbb{Q}_p)$.

(*b*) $\hat{F}_\omega$ *is isomorphic to a subgroup of* $G(\mathbb{Q}_p) * G(\mathbb{Q}_p)$.

(*c*) *Let* $G = \mathfrak{g}_1 * \dots * \mathfrak{g}_n$, *qhere* $\mathfrak{g}_i \cong G(\mathbb{Q}_p)$ *for* $i = 1, \dots, n$. *Then for every* $1 \neq a \in \mathfrak{g}_1$ *the centralizer* $C_G(a)$ *of* a *in* G *is contained in* $\mathfrak{g}_1$.

Proof. (*a*) The Galois group of the maximal unramified extension of $\mathbb{Q}_p$ over $\mathbb{Q}_p$ is $\hat{\mathbb{Z}}$ (cf. [2], p. 353). Thus there exists an epimorphism $r: G(\mathbb{Q}_p) \to \hat{\mathbb{Z}}$. But $\hat{\mathbb{Z}}$ is free, hence r has a section, i.e. an embedding $\hat{\mathbb{Z}} \to G(\mathbb{Q}_p)$.

(*b*) By (*a*) and by Proposition 4 there exists an embedding

$$\hat{F}_2 \cong \hat{\mathbb{Z}} * \hat{\mathbb{Z}} \to G(\mathbb{Q}_p) * G(\mathbb{Q}_p).$$

But $\hat{F}_\omega$ is isomorphic to a subgroup of $\hat{F}_2$, by [4], corollary 3·9, hence (*b*) follows.

(*c*) By [3], theorem 4·1, there exist $\tau_1, \dots, \tau_n \in G(\mathbb{Q})$ such that

$$G(\textstyle\bigcap_{i=1}^n \mathbb{Q}_p^{\tau_i}) = G(\mathbb{Q}_p^{\tau_i}) * \dots * G(\mathbb{Q}_p^{\tau_n}).$$

Without loss of generality $\tau_1 = 1$. Since $G(\mathbb{Q}_p^{\tau_i}) \cong G(\mathbb{Q}_p)$, we may assume that

$$G = G(\textstyle\bigcap_{i=1}^n \mathbb{Q}_p^{\tau_i});$$

in particular, G is a subgroup of $G(\mathbb{Q})$ and its subgroup $\mathfrak{g}_1$ is $G(\mathbb{Q}_p)$. Now if $\sigma \in C_G(a)$ then

$$1 \neq a = a^\sigma \in \mathfrak{g}_1 \cap \mathfrak{g}_1^\sigma = G(\mathbb{Q}_p) \cap G(\mathbb{Q}_p^\sigma) = G(\mathbb{Q}_p \mathbb{Q}_p^\sigma),$$

so $\mathbb{Q}_p \mathbb{Q}_p^\sigma \neq \tilde{\mathbb{Q}}$. Thus $\sigma \in G(\mathbb{Q}_p) = \mathfrak{g}_1$, by Lemma 5.

COROLLARY 7. *Let $P \neq 1$ be a subgroup of $\hat{\mathbb{Z}}$, and let $H = P * \hat{F}_\omega$. If $1 \neq a \in P$ then $C_H(a) = P$. In particular, P is a maximal abelian subgroup of H.*

Proof. Let $G = \mathfrak{g}_1 * \mathfrak{g}_2 * \mathfrak{g}_3$, where $\mathfrak{g}_i \cong G(\mathbb{Q}_p)$ for $i = 1, 2, 3$.

By Lemma 6 (*a*), (*b*) we may assume that P is a subgroup of $\mathfrak{g}_1$ and $\hat{F}_\omega$ is a subgroup of $\mathfrak{g}_2 * \mathfrak{g}_3$. Thus H is a subgroup of G, by Proposition 4, and $H \cap \mathfrak{g}_1 = P$. It follows by Lemma 6 (*c*) that

$$C_H(a) = C_G(a) \cap H = (C_G(a) \cap \mathfrak{g}_1) \cap H = C_G(a) \cap P = C_P(a)$$

and $C_P(a) = P$, since P is abelian. Thus $C_H(a) = P$.

LEMMA 8. *Let P be a countably generated projective profinite group and let F be a free profinite group of infinite rank. Then $P * F \cong F$.*

Proof. Assume first that $F = \hat{F}_\omega$. By Iwasawa's criterion ([**8**], theorem 9·3) we have to show the following: Let $\alpha: B \to A$ be an epimorphism of finite groups and

$$\phi: P * \hat{F}_\omega \to A$$

an epimorphism. Then there exists an epimorphism $\psi: P * \hat{F}_\omega \to B$ such that $\alpha \circ \psi = \phi$.

Denote $A_1 = \phi(P)$, $A_2 = \phi(\hat{F}_\omega)$, $B_1 = \alpha^{-1}(A_1)$, $B_2 = \alpha^{-1}(A_2)$. By the projectivity of P there exists $\psi_1: P \to B_1$ such that $\alpha \circ \psi_1 = \mathrm{res}_P\, \phi$; by Iwasawa's criterion there exists an epimorphism $\psi_2: \hat{F}_\omega \to B_2$ such that $\alpha \circ \psi_2 = \mathrm{res}_{\hat{F}_\omega} \phi$. The maps ψ_1, ψ_2 define a map $\psi: P * \hat{F}_\omega \to B$ such that $\alpha \circ \psi = \phi$. But

$$\alpha(\psi(P * \hat{F}_\omega)) = A \quad \text{and} \quad \psi(P * \hat{F}_\omega) \supseteq \psi_2(\hat{F}_\omega) = B_2 \supseteq \mathrm{Ker}\,\alpha;$$

thus ψ is an epimorphism. This establishes the case $F = F_\omega$.

In the general case $F \cong \hat{F}_\omega * F$, hence $P * F \cong P * \hat{F}_\omega * F \cong \hat{F}_\omega * F \cong F$.

Remarks. (*a*) One can also deduce the Lemma from [**6**], satz 3·7, p. 347.

(*b*) We do not know whether a finitely generated free profinite group can be written as a free product of two profinite groups, not both of them free. If the Grushko–Neumann theorem ([**5**], corollary 1·9, p. 178) is true for profinite groups, then one can prove that such a decomposition is impossible.

We are now in a position to prove the Theorem: Let π be a nonempty set of primes. The group $P = \Pi_{p \in \pi} \mathbb{Z}_p$ is a subgroup of the free group $\hat{\mathbb{Z}}$, hence P is projective (cf. [**4**], proposition 4·8). Thus for $F = \hat{F}_\omega$ the result follows from Corollary 7 and Lemma 8.

If $|X| > \aleph_0$ then

$$F = \varprojlim_{\alpha \in I} F_\alpha,$$

where the F_α are finitely generated free profinite groups. But $F \cong A * \hat{F}_\omega * F$ by Lemma 8, hence

$$F = \varprojlim_{\alpha \in I} A * \hat{F}_\omega * F_\alpha$$

in such a way that the maps of this inverse system are the identity on A. As

$$\hat{F}_\omega * F_\alpha \cong \hat{F}_\omega,$$

the centralizer of A in $A * \hat{F}_\omega * F_\alpha$ is A for every $\alpha \in I$, hence A is equal to its own centralizer in the inverse limit F.

If $|X| < \aleph_0$, fix $p \in \pi$ and an epimorphism $\phi: F \to \mathbb{Z}_p$, and denote $N = \operatorname{Ker} \phi$. By [4], corollary 3·9, $N \cong \hat{F}_\omega$; hence A can be embedded as a maximal abelian subgroup of N. Therefore $C_F(A) \cap N = C_N(A) = A$.

It remains to show that no $x \in F \backslash N$ centralizes A. Indeed, otherwise the p-Sylow subgroup B_p of the closed procyclic group B generated by x centralizes the p-Sylow subgroup A_p of A. Both A_p and B_p are non-trivial by the way we chose p and ϕ. Thus $\mathbb{Z}_p \times \mathbb{Z}_p \cong A_p \times B_p$ is a subgroup of F, a contradiction, since $\mathbb{Z}_p \times \mathbb{Z}_p$ is not projective.

Problem. What are the isomorphism classes of maximal abelian subgroups of $G(\mathbb{Q})$?

Added in proof. Since this paper was submitted, we have learned that W. Herfort and L. Ribes (Torsion elements and centralizers in free products of profinite groups) have shown that the relation (*) holds for arbitrary profinite groups A and B.

REFERENCES

[1] J. Ax. A metamathematical approach to some problems in number theory. *Proc. of Symposia in Pure Math.* vol. 20 (1971), 161–190. American Mathematical Society.

[2] W.-D. Geyer. Unendliche algebraische Zahlkörper, über denen jede Gleichung auflösbar von beschränkter Stufe ist. *J. Number Theory* **1** (1969), 346–374.

[3] W.-D. Geyer. Galois groups of intersections of local fields. *Israel J. Math.* **30** (1978), 382–396.

[4] A. Lubotzky and L. van den Dries. Subgroups of free pro-finite groups and large subfields of $\tilde{\mathbb{Q}}$. *Israel J. Math.* **39** (1981), 25–45.

[5] R. C. Lyndon and P. E. Schupp. *Combinatorial Group Theory.* Ergebnisse der Mathematik und ihrer Grenzgebiete 89 (Springer-Verlag, 1977).

[6] J. Neukirch. Freie Produkte proendlicher Gruppen und ihre Kohomologie. *Arch. Math.* **22** (1971), 337–357.

[7] P. Scott. Subgroups of surface groups are almost geometric. *J. London Math. Soc.* **17** (1978), 555–565.

[8] L. Ribes. Introduction to profinite groups and Galois cohomology. Queens Papers in Pure and Applied Mathematics, vol. 24 (Kingston).