RANDOM NORMAL SUBGROUPS OF FREE PROFINITE GROUPS

by

Moshe Jarden*, Tel Aviv University

and

Alexander Lubotzky, The Hebrew University in Jerusalem

e-mail: jarden@math.tau.ac.il and alexlub@math.huji.ac.il

Dedicated to Avinoam Mann
on the occasion of his 60th birthday

26 February, 1998

* Partially supported by the Hermann Minkowski Center for Geometry.

Introduction

Theorem 16.13 of [FrJ] states that for a Hilbertian field K, for a positive integer e, and for almost all $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in G(K)^e$ (with respect to the Haar measure), the closed subgroup $\langle \boldsymbol{\sigma} \rangle$ of $G(K)^e$ generated by $\sigma_1, \ldots, \sigma_e$ is isomorphic to $\hat{F}_e$. Here $G(K)$ is the absolute Galois group of K, and $\hat{F}_e$ is the free profinite group on e generators.

The closed normal subgroup $[\boldsymbol{\sigma}]$ of $G(K)$ generated by $\sigma_1, \ldots, \sigma_e$ is expected to be much larger than $\langle \boldsymbol{\sigma} \rangle$. Indeed, for K Hilbertian and countable, [Jar, Thm. 2.7] states that for almost all $\boldsymbol{\sigma} \in G(K)^e$, $[\boldsymbol{\sigma}]$ is isomorphic to the free profinite group $\hat{F}_\omega$ on countably many generators. Since $\hat{F}_\omega$ itself occurs as $G(K)$ for some countable Hilbertian field K, the same conclusions hold for $\hat{F}_\omega$ rather than $G(K)$ [Jar, Cor. 3.1].

One may therefore choose a fixed positive integer n, let $F = \hat{F}_n$ and ask about the groups $\langle \boldsymbol{\sigma} \rangle$ and $[\boldsymbol{\sigma}]$ for a random e-tuple $\boldsymbol{\sigma} \in F^e$.

If $n = 1$, then $F = \hat{\mathbb{Z}}$. In this case F is abelian and therefore $[\boldsymbol{\sigma}] = \langle \boldsymbol{\sigma} \rangle$. By [FrJ, Lemma 16.15], $\langle \boldsymbol{\sigma} \rangle \cong \hat{\mathbb{Z}}$. In addition $\langle \boldsymbol{\sigma} \rangle$ has an infinite index in $\hat{\mathbb{Z}}$ if $e = 1$ and a finite index if $e \geq 2$. [KaL, Prop. 12] generalizes the latter result to the group $A = \hat{\mathbb{Z}}^n$ where now n is an arbitrary positive integer. It says that for almost all $\boldsymbol{\sigma} \in A^e$, $(A : \langle \boldsymbol{\sigma} \rangle) = \infty$ if $e \leq n$ but $(A : \langle \boldsymbol{\sigma} \rangle) < \infty$ if $e > n$. We complete this result and prove that for almost all $\boldsymbol{\sigma} \in A^e$, $\langle \boldsymbol{\sigma} \rangle \cong \hat{\mathbb{Z}}^e$ if $e \leq n$ and $\langle \boldsymbol{\sigma} \rangle \cong \hat{\mathbb{Z}}^n$ if $e \geq n$ (Theorem 3.1).

Let us now fix $n \geq 2$, write again $F = \hat{F}$, and choose a random e-tuple $\boldsymbol{\sigma}$ in F^e. Then $\langle \boldsymbol{\sigma} \rangle \cong \hat{F}_e$ and $(F : \langle \boldsymbol{\sigma} \rangle) = \infty$ [Lub, Thm. 1 and Kal, Prop. 11].

For an extensive study of related questioned about $\langle \boldsymbol{\sigma} \rangle$ when $\hat{F}$ is replaced by other finitely generated profinite groups see [Man] and the references therein.

The main goal of this work is the study the closed normal group $[\boldsymbol{\sigma}]$ for $\boldsymbol{\sigma} \in F^e$. We expect that $[\boldsymbol{\sigma}]$ is much larger than $\langle \boldsymbol{\sigma} \rangle$ and therefore ask whether

$$[\boldsymbol{\sigma}] \cong \hat{F}_\omega. \tag{1}$$

Since open subgroups of F are finitely generated, (1) is certainly false if $[\boldsymbol{\sigma}]$ has finite index. However, we prove that under the condition

$$(F : [\boldsymbol{\sigma}]) = \infty, \tag{2}$$

(1) holds with probability 1 (Theorem 2.7).

In section 1, we study Condition (2). We prove that it holds for each $\boldsymbol{\sigma} \in G(K)^e$ if $e < n$, it holds for almost all (but not for all) $\boldsymbol{\sigma} \in G(K)^e$ if $e = n$, and it holds with probability strictly between 0 and 1 if $e > n$. The result that (2) holds with probability less than 1 depends on the classification of finite simple groups.

It follows that if $e \leq n$, then (1) holds for almost all $\boldsymbol{\sigma} \in F^e$. If $e > n$, then (1) holds for a set of $\boldsymbol{\sigma}$'s of measure strictly between 0 and 1.

Since every open subgroup of F is free, it follows that for each $e \geq 1$, and for almost all $\boldsymbol{\sigma} \in F^e$, $[\boldsymbol{\sigma}]$ is a free profinite group. This is a certain analog to Schreier's subgroup theorem of free discrete groups and to Tate's subgroup theorem for free pro-p groups. Both theorems assert that subgroups of a free group in the corresponding category are free. In our case, this theorem is false, even for normal closed subgroups. But our results say that in a certain sense it holds for the majority of closed normal subgroups.

An essential ingredient in the proofs is the method of "non-commutative localization": If S is a finite simple group, a **pro-S-group** is a profinite group whose composition factors are all isomorphic to S. When $S \cong \mathbb{Z}/p\mathbb{Z}$, these are just the familiar pro-p groups. In our work we replace F by its maximal pro-S quotient, which is a free pro-S group. When S is non-abelian, some new phenomena appear (see §2) which make the latter group substantially different from the free pro-p groups. This calls for a systematic study of the free pro-S groups, for non-abelian simple groups S.

1. On the index of normal subgroups generated by random elements

Let $n \geq 2$ and consider the free profinite group $F = \hat{F}_n$ on n generators. Let e be a positive integer and let μ be the normalized Haar measure of the direct product F^e of e copies of F. For each $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in F^e$ let $\langle \boldsymbol{\sigma} \rangle$ be the closed subgroup of F generated by $\sigma_1, \ldots, \sigma_e$. Also, let $[\boldsymbol{\sigma}] = [\boldsymbol{\sigma}]_F$ be the closed normal subgroup of F generated by $\sigma_1, \ldots, \sigma_e$. In other words, $[\boldsymbol{\sigma}]$ is the intersection of all closed normal subgroups of F that contain $\langle \boldsymbol{\sigma} \rangle$. Note that if E is a normal subgroup of F and $\boldsymbol{\sigma} \in E^e$, then $[\boldsymbol{\sigma}]_E \leq [\boldsymbol{\sigma}]_F \leq E$ but it may happen that $[\boldsymbol{\sigma}]_E < [\boldsymbol{\sigma}]_F$.

The purpose of this section is to study the index of $[\boldsymbol{\sigma}]$ in F.

Remark 1.1: The function $d_n(S)$. Let S be a finite nonabelian simple group. Denote the set of all n-tuples of elements of S that generate S by $D_n(S)$. In particular, $|D_n(S)| \leq |S|^n$. If $\sigma_1, \ldots, \sigma_r$ generate S and $r \leq n$, then S is generated by each n-tuple $(\sigma_1, \ldots, \sigma_r, \ldots, \sigma_n)$. It follows that $|D_n(S)| \geq |S|^{n-r}$ and $|\mathrm{Aut}(S)| \leq |S|^r$.

Denote the maximal number m such that S^m is a quotient of F (recall: $F = \hat{F}_n$), by $d_n(S)$. It is also the number of open normal subgroups of F such that $F/N \cong S$. A theorem of P. Hall [Lub, Lemma 2] states that

$$d_n(S) = \frac{|D_n(S)|}{|\mathrm{Aut}(S)|}. \tag{1}$$

Since S is embedded in $\mathrm{Aut}(S)$, we have $|\mathrm{Aut}(S)| \geq |S|$. Hence, by (1),

$$|S|^{n-2r} \leq \frac{|S|^{n-r}}{|\mathrm{Aut}(S)|} \leq d_n(S) \leq |S|^{n-1}. \tag{2}$$

One of the consequences of the classification of finite groups is that S is generated by two elements [AsG, Thm. B]. Hence, the lower bound of (2) improves to $d_n(S) \geq |S|^{n-4}$.

∎

For a profinite group G and a closed normal subgroup H we set:

$$B_e(H, G) = \{\boldsymbol{\sigma} \in G^e \mid [\boldsymbol{\sigma}]_G = H\}, \qquad B_e(G) = B_e(G, G)$$
$$C_e(G) = \{\boldsymbol{\sigma} \in G^e \mid (G : [\boldsymbol{\sigma}]) = \infty\}$$

LEMMA 1.2: *Let G be a profinite group and let H be a closed normal subgroup.*

(a) *$B_e(H,G)$ is closed subset of G^e.*

(b) *$C_e(G)$ is a measurable subset of G^e.*

Proof of (a): For each open normal subgroup N of G, $\{\boldsymbol{\sigma} \in G^e \mid [\boldsymbol{\sigma}]_G N = HN\}$ is an open closed subset of G. The intersection of all these sets is $B_e(H,G)$. Hence, $B_e(H,G)$ is closed.

Proof of (b): We have $C_e(G) = G^e \smallsetminus \bigcup_E B_e(E,G)$, where E ranges over all open normal subgroup of G. By (a), each $B_e(E,G)$ is closed. Hence, C_e is measurable. ∎

LEMMA 1.3: *Let P be the free pro-p-group of rank $n \geq 2$ and let e be a positive integer. Then, $\mu(C_e(P)) > 0$.*

*Proof**: Assume that $\mu(C_e(P)) = 0$. Take an open normal subgroup Q of P of index r such that

$$er \leq \frac{1}{4}(r(n-1)+1)^2. \tag{3}$$

Then the Frattini subgroup $\Phi(Q)$ of Q is an open subgroup of P. In particular $\Phi(Q)^e$ has a positive measure. We may therefore choose $\boldsymbol{\sigma} \in \Phi(Q)^e \smallsetminus C_e(P)$. Thus $N = [\boldsymbol{\sigma}]$ is an open normal subgroup of P and therefore also of Q. Hence $G = Q/N$ is a finite p-group.

By Nielsen-Schreier formula [FrJ, Prop. 15.27], $\mathrm{rank}(Q) = r(n-1)+1$. Since $N \leq \Phi(Q)$, we have $\Phi(G) = \Phi(Q)/N$ and $\mathrm{rank}(G) = \mathrm{rank}(G/\Phi(G)) = \mathrm{rank}(Q/\Phi(Q)) = \mathrm{rank}(Q) = r(n-1)+1$.

On the other hand, let $\tau_1, \ldots, \tau_r$ be representatives for the left cosets of P modulo Q. Then $N = [\sigma_i^{\tau_j} \mid i = 1, \ldots, e,\ j = 1, \ldots, r]_Q$, (i.e., N is the closed normal subgroup of Q generated by $\sigma_1, \ldots, \sigma_e$). In other words, relation.rank$(G) \leq er$. By the Golod-Shafarevich inequality, relation.rank$(G) > \frac{1}{4}\mathrm{rank}(G)^2$ (e.g., Roquette in [CaF, p. 237, Thm. 10]). Hence, $er > \frac{1}{4}(r(n-1)+1)^2$. This contradiction to (3) proves that $\mu(C_e(P)) > 0$. ∎

* The authors are indebted to the referee for suggesting to replace a former proof which used a sharpened form of the Golod-Shafarevich inequality by the original simpler inequality.

THEOREM 1.4: *Let F be the free profinite group on $n \geq 2$ generators.*

(a1) *If $e \leq n$, then $\mu(B_e(F)) = 0$. In fact, if $e < n$, then $B_e(F) = \emptyset$ while if $e = n$, then $B_e(F) \neq \emptyset$.*

(a2) *If $e > n$, then $0 < \mu(B_e(F)) < 1$.*

(b1) *If $e \leq n$, then $\mu(C_e(F)) = 1$. In fact, if $e < n$, then $C_e(F) = F^e$ while if $e = n$, then $C_e(F) \neq F^e$.*

(b2) *If $e > n$, then $0 < \mu(C_e(F)) < 1$.*

The proof naturally breaks up into several parts.

PART A: *In each case $\mu(C_e(F)) > 0$.* Choose a prime number p, and let $P = \hat{F}_n(p)$ be the free pro-p group on n generators. Let $\pi\colon F \to P$ be an epimorphism. If $\boldsymbol{\sigma} \in F^e$, then $\pi([\boldsymbol{\sigma}]) = [\pi(\boldsymbol{\sigma})]$. Hence, if $[\pi(\boldsymbol{\sigma})]$ has infinite index in P, then $[\boldsymbol{\sigma}]$ has infinite index in F. By Lemma 1.3, $\mu(C_e(P)) > 0$. Also, $\pi^{-1}(C_e(P)) \subseteq C_e(F)$. Hence, $\mu(C_e(F)) > 0$.

PART B: *If $e < n$, then $(F : [\boldsymbol{\sigma}]) = \infty$ for each $\boldsymbol{\sigma} \in F^e$.* Again, choose a prime number p. Let $\boldsymbol{\sigma}$ be an arbitrary e-tuple of F. Let $\varphi\colon F \to \mathbb{Z}_p^n$ be an epimorphism. Each open subgroup of $\mathbb{Z}_p^n$ is isomorphic to $\mathbb{Z}_p^n$ and therefore can not be generated by less than n elements. Since $\varphi([\boldsymbol{\sigma}]) = [\varphi(\boldsymbol{\sigma})] = \langle \varphi(\boldsymbol{\sigma}) \rangle$, this implies that the index of $\varphi([\boldsymbol{\sigma}])$ in $\mathbb{Z}_p^n$ is infinite. It follows that $(F : [\boldsymbol{\sigma}]) = \infty$.

PART C: *If $e = n$, then $\mu(C_e(F)) = 1$.* Consider an epimorphism $\varphi\colon F \to \hat{\mathbb{Z}}^n$. By [KaL, Prop. 12(ii)], $[\boldsymbol{\sigma}] = \langle \boldsymbol{\sigma} \rangle$ has an infinite index in $\hat{\mathbb{Z}}^n$ for almost all $\boldsymbol{\sigma} \in (\hat{\mathbb{Z}}^n)^n$. Hence $[F : [\boldsymbol{\sigma}]) = \infty$ for almost all $\boldsymbol{\sigma} \in F^n$.

PART D: *If $e > n$, then $\mu(B_e(F)) > 0$.* Let $C = B_e(F)$. We have to prove that $\mu(F^e \smallsetminus C) < 1$. To this end note that

$$F^e \smallsetminus C = \bigcup_p \bigcup_{F/N \cong \mathbb{Z}/p\mathbb{Z}} N^e \cup \bigcup_{S \in \mathrm{SNA}} \bigcup_{F/N \cong S} N^e.$$

Here SNA is the set of all non-abelian finite simple groups.

Recall that if A and B are independent subsets of a probability space, then $1 - \mu(A \cup B) = (1 - \mu(A))(1 - \mu(B))$. Also, if B is a union of a sequence $B_1, B_2, B_3, \ldots$ of

independent sets, then $1-\mu(B)=\prod_{i=1}^{\infty}(1-\mu(B_i))$. Hence $\mu(A\cup B)<1$ if and only if $1-\mu(A)>0$ and $\sum_{i=1}^{\infty}\mu(B_i)<\infty$.

Let in our case $A=\bigcup_p\bigcup_{F/N=\mathbb{Z}/p\mathbb{Z}}N^e$ and let B_j range over all N^e with $F/N\in SNA$. Then $A,B_1,B_2,B_3,\ldots$ are indeed independent. Moreover, $\mu(A)$ is equal to the measure of all $\boldsymbol{\sigma}\in(\hat{\mathbb{Z}}^n)^e$ which are contained in a maximal subgroup of prime index. The latter measure is equal to the measure of all $\boldsymbol{\sigma}\in(\hat{\mathbb{Z}}^n)^e$ which do not generate $\hat{\mathbb{Z}}^n$. Thus, by [KaL, Prop. 12(i)], $1-\mu(A)=\prod_{e-n<i\le e}\zeta(i)^{-1}>0$, where ζ is the Riemann zeta function.

To prove the condition on the B_j's, let $S\in SNA$ and use the inequality $d_n(S)\le|D_n(S)|\le|S|^n$. Note that any sequence $N_1,N_2,N_3,\ldots$ of distinct open normal subgroups of F with coquotient in SNA is independent. By (2),

$$(4)\qquad \sum_{S\in\mathrm{SNA}}\sum_{F/N\cong S}\mu(N^e)=\sum_{S\in\mathrm{SNA}}\frac{d_n(S)}{|S|^e}\le\sum_{S\in\mathrm{SNA}}\frac{1}{|S|^{e+1-n}}\le\sum_{S\in\mathrm{SNA}}\frac{1}{|S|^2}<\infty.$$

The last inequality holds because for each positive integer n there are at most 2 simple groups of order n ([KLS, Thm. 5.1] proves this result by using the classification of finite simple groups). Conclude that $\mu(C)>0$.

PART E: *Conclusion of the proof.* Let $C=B_e(F)$. If $e<n$, then F is not generated by e elements (e.g., because $(\mathbb{Z}/p\mathbb{Z})^n$, which is a quotient of F, is not generated by e elements.) and therefore $C=\emptyset$. If $e=n$, then F is generated by e elements and therefore $C\neq\emptyset$. However, since $C\subseteq F^e\smallsetminus C_e(F)$, Part C implies that $\mu(C)=0$. This concludes the proof of (a1).

Part D of the proof takes care of the first inequality of (a2). In order to prove also the second one take a proper open normal subgroup E of F. Then $E^e\subseteq F^e\smallsetminus B_e(F)$ and $\mu(E^e)>0$. Conclude that $\mu(B_0(F,F))<1$.

Parts B and C give (b1).

Finally, if $e>n$, then, by Part D, $\mu(F^e\smallsetminus C_e(F))\ge\mu(B_e(F))>0$. Together with Part A we get $0<\mu(C_e(F))<1$. ∎

Remark 1.5: Note that the only application of the classification of simple groups in the proof of Theorem 1.4 occurs in the proof of Part D, and therefore in the proof of the inequalities $\mu(B_e(F))>0$ and $\mu(C_e(F))<1$. ∎

If $e > n$, then $[\boldsymbol{\sigma}]$ is, with a positive probability, of infinite index. The next result supplies some information about the quotient $F/[\boldsymbol{\sigma}]$.

PROPOSITION 1.6: *Let $e > n$. Then almost all $\boldsymbol{\sigma} \in F^e$ have the following properties:*

(a) *The maximal abelian quotient of $F/[\boldsymbol{\sigma}]$ is finite.*

(b) *There are only finitely many open maximal normal subgroups N of F which contain $[\boldsymbol{\sigma}]$ such that F/N is simple and nonabelian.*

Proof of (a): Let A be the set of all $\sigma \in (\hat{\mathbb{Z}}^n)^e$ such that $(\mathbb{Z}^n : \langle \boldsymbol{\sigma} \rangle) < \infty$. By [KaL, Prop. 12(ii)], the measure of A in $(\hat{\mathbb{Z}}^n)^e$ is 1. Choose an epimorphism $\psi\colon F \to \hat{\mathbb{Z}}^n$ and let $K = \mathrm{Ker}(\psi)$. Then $\mu(\psi^{-1}(A)) = 1$. For each $\sigma \in F^n$ the maximal abelian quotient of $F/[\boldsymbol{\sigma}]$ is $F/[\boldsymbol{\sigma}]K$. Moreover $[\boldsymbol{\sigma}]K = \psi^{-1}\langle \boldsymbol{\sigma} \rangle$. Hence, $(F : [\boldsymbol{\sigma}]K) = (\mathbb{Z}^n : \langle \boldsymbol{\sigma} \rangle)$. Conclude that if $\sigma \in \psi^{-1}(A)$, then the maximal abelian extension of $F/[\boldsymbol{\sigma}]$ is finite.

Proof of (b): By (4) and by a lemma of Borel-Cantelli [FrJ, Lemma 16.7(a)], almost all $\sigma \in F^e$ belong to only finitely many open normal subgroups S such that $S/N \in \mathrm{SNA}$. This proves (b). ∎

2. Normal subgroups generated by random elements are free

As in Section 1, we fix an integer $n \geq 2$, let $F = \hat{F}_n$, and let e be a positive integer. We wish to prove that $[\boldsymbol{\sigma}]$ is a free profinite group for almost all $\boldsymbol{\sigma} \in F^e$. The case where the index if finite is well known. So, we prove that $[\boldsymbol{\sigma}] \cong \hat{F}_\omega$ for almost all $\boldsymbol{\sigma} \in F^e$ which satisfy $(F : [\boldsymbol{\sigma}]) = \infty$. A basic tool is the following criterion of Melnikov:

LEMMA 2.1: *Let N be a normal closed subgroup of F such that*

(1a) *for each prime number p, the group $\mathbb{Z}/p\mathbb{Z}$ is a quotient of N.*

(1b) *for each finite simple nonabelian group S and for each positive integer q, the group S^q is a quotient of N; and*

Then $N \cong \hat{F}_\omega$.

Proof: Since each open subgroup of F is finitely generated, (1b) and the right hand side of (2) of §1 imply that $(F : N) = \infty$. By [Mel, Prop. 3.1], each finite embedding problem for N is solvable. Hence, by Iwasawa's criterion [FrJ, Cor. 24.2], $N \cong \hat{F}_\omega$. ∎

LEMMA 2.2: *For almost all $\boldsymbol{\sigma} \in F^e$, and for each prime number p, the group $\mathbb{Z}/p\mathbb{Z}$ is a quotient of $[\boldsymbol{\sigma}]$.*

Proof: For each p let N_p be the smallest closed normal subgroup N of F such that F/N is a pro-p-group. Then N_p has an infinite index.

Otherwise, N_p would be open and therefore a free profinite group [FrJ, Prop. 15.27] of rank at least 2. Hence, N_p would have an open normal subgroup M such that $N_p/M \cong \mathbb{Z}/p\mathbb{Z}$. Let M_0 be the intersection of all conjugates of M in F. Then M_0 is an open normal subgroup of F and F/M_0 is an p-group. This contradicts the choice of N_p.

It follows that the union $U = \bigcup N_p^e$, where p ranges over all prime numbers is a zero subset of F^e. If $\boldsymbol{\sigma} \notin U$, then for each p, the quotient $[\boldsymbol{\sigma}] \cdot N_p/N_p$ is a nontrivial pro-p-group. As such it has $\mathbb{Z}/p\mathbb{Z}$ as a quotient. Conclude that $\mathbb{Z}/p\mathbb{Z}$ is a quotient of $[\boldsymbol{\sigma}]$. ∎

Lemma 2.2 settles condition (1a) of Melnikov's criterion. To handle also condition (1b), we study the notion of S-rank of a profinite group. This depends on two Lemmas:

LEMMA 2.3: *Let H be a closed subgroup of a profinite group G. Let $\mathcal{N}$ be a nonempty family of closed normal subgroups of G which is closed under finite intersections and such that $HN = G$ for each $N \in \mathcal{N}$. Let N_0 be the intersection of all $N \in \mathcal{N}$. Then $HN_0 = G$.*

Proof: Let $g \in G$. For each $N \in \mathcal{N}$ there exist $h \in H$ and $n \in N$ such that $hn = g$. Hence, the closed subset $H \cap gN$ of G is nonempty. Since $\mathcal{N}$ is closed under finite intersections, so is the family $\{H \cap gN \mid N \in \mathcal{N}\}$. By compactness, $H \cap gN_0 = \bigcap_{N \in \mathcal{N}} (H \cap gN) \neq \emptyset$. Thus, there exists $n_0 \in N_0$ and $h_0 \in H$ such that $h_0 n_0 = g$. ∎

To give an example where the assumptions of Lemma 2.3 are satisfied we consider a profinite group G and a closed subgroup H of G. Denote the family of all closed normal subgroups M of G such that $HM = G$ by $\mathcal{N}(G, H)$. Denote the intersection of all $M \in \mathcal{N}(G, H)$ by $\mathbf{N}(G, H)$.

In the proof of Lemma 2.5 and elsewhere we will use Rule 2.4 below.

RULE 2.4: *Let G be a profinite group, H an open subgroup of G, and M and N closed normal subgroups of G such that $M \leq N$. Then $HM = G$ if and only if $HN = M$ and $(H \cap N)M = N$.*

LEMMA 2.5: *Let S be a simple nonabelian group and let G be a profinite group. Consider a positive integer k and an open normal subgroup H of G such that $G/H \cong S^k$. Then $\mathcal{N}(G, H)$ is closed under finite intersections. Hence, by Lemma 2.3, $H \cdot \mathbf{N}(G, H) = G$.*

Proof: It suffices to prove that if M and N are open normal subgroups of G such that $HM = HN = G$, then $H(M \cap N) = G$. We prove this statement by induction on k and starts with the case $k = 1$.

By assumption, $HM/H = G/H \cong S$ is a nonabelian simple group. Hence, there exist $m, m' \in M$ such that $[m, m'] \notin H$. Since $HN = G$ there exist $h \in H$ and $n \in N$ such that $m' = hn$. Use the identity $[m, m'] = [m, hn] = [m, n][m, h]^n$ and the relation $[m, h]^n \in H$ to conclude that $[m, n] \notin H$. Since $[m, n] \in M \cap N$, it follows that $M \cap N \not\leq H$. Finally, since $G/H \cong S$ is simple, we have $H(M \cap N) = G$.

Suppose now that $k > 1$ and that the statement is true for $k-1$. Then G has an open normal subgroup E which contains H such that $G/E \cong S$ and $E/H \cong S^{k-1}$. It satisfies, $EM = EN = G$. By rule 2.4, $H(E \cap M) = E$ and $H(E \cap N) = E$. By the induction hypothesis applied to E instead of to G we have $H \cdot (E \cap M \cap N) = E$. By the case $k = 1$, $E(M \cap N) = G$. Hence, by Rule 2.4, $H(M \cap N) = G$. ∎

Let $\mathcal{D}$ be a family of finite simple groups. A finite **$\mathcal{D}$-group** is a finite group whose composition factors belong to $\mathcal{D}$. An inverse limit of $\mathcal{D}$-groups is a **pro-$\mathcal{D}$ group**. If $\mathcal{D}$ consists of one group S only, then we speak of an **S-group** and a **pro-$\mathcal{S}$-group**.

For each profinite group G we denote the intersection of all open normal subgroups N such that $G/N \cong S$ by $M_S(G)$. Then $G/M_S(G) \cong S^I$ for some set I. We denote the cardinality of I by $r_S(G)$ and call it the **S-rank** of G.

In the notation of Remark 1.1, $r_S(F) = d_n(S)$. Also, if $\bar{F}$ is the free pro-S-group of rank n, then $r_S(\bar{F}) = r_S(F)$. Let N be a nontrivial closed subgroup of $\bar{F}$ of infinite index. If $S = \mathbb{Z}/p\mathbb{Z}$, then $\mathrm{rank}(N) = \infty$ [FrJ, Cor. 24.8] and therefore also $r_S(N) = \infty$. It is quite surprising that for nonabelian S there exists N such that $r_S(N) < \infty$. This will follow from Lemma 2.6(a). Nevertheless, there are only countably many such N (Lemma 2.6(d)).

Recall that the **rank** of a profinite group G is the cardinality of a minimal set of generators of F.

LEMMA 2.6: *Let G be a profinite group, let S be a simple nonabelian group, and let k be a nonnegative integer.*

(a) *Let $H' \leq G'$ be open normal subgroups of G such that $G'/H' \cong S^k$. Then $\mathbf{N}(G', H') \triangleleft G$ and $r_S(\mathbf{N}(G', H')) = k$.*

(b) *Suppose that N is a closed normal subgroup of G such that $r_S(N) = k$. Then there exist open normal subgroups $H' \leq G'$ of G such that $G'/H' \cong S^k$, $H'N = G'$ and $H' \cap N = M_S(N)$.*

(c) *Suppose that G is a pro-S-group. Let N be a closed normal subgroup of G such that $r_S(N) = k$. Then there exists open normal subgroups $H' \leq G'$ of G such that $N = \mathbf{N}(G', H')$ and $G'/H' \cong S^k$.*

(d) *Suppose that G is a pro-S-group. The number of closed normal subgroups of G such that $r_S(N) < \infty$ is bounded by* $\max\{\aleph_0, \mathrm{rank}(G)\}$. *In particular, if* $\mathrm{rank}(G) \leq \aleph_0$, *then there are at most countably many closed normal subgroups N of G such that $r_S(N) < \infty$.*

Proof of (a): Let $N = \mathbf{N}(G', H')$ and $M = H' \cap N$. Observe that the family $\mathcal{N}(G', H')$ is closed under conjugation by elements of G. Hence, $N \triangleleft G$.

By Lemma 2.5, $H'N = G'$. Hence, $N/M \cong G'/H' \cong S^k$ and therefore $r_S(N) \geq k$. If $r_S(N) > k$, then N would have an open normal subgroup N_0 such that $N/N_0 \cong S$ and $M \not\leq N_0$. Since S is simple, this would imply that $MN_0 = N$. The group N_0 need not be normal in G'. So, consider $N_1 = \mathbf{N}(N, M)$. Then $N_1 \leq N_0$. By the preceding paragraph, $N_1 \triangleleft G'$. By Lemma 2.5, $MN_1 = N$ and therefore $H'N_1 = G'$. By the definition of N, this would imply that $N \leq N_1 \leq N_0 < N$. This is a contradiction. Conclude that $r_S(N) = k$.

Proof of (b): Since $N \triangleleft G$, the set of all open $N' \triangleleft N$ such that $N/N' \cong S$ is closed under conjugation by elements of G. Hence, $M_S(N) \triangleleft G$. This implies the existence of G' and H' as in (b).

Proof of (c): Let $M = M_S(N)$. By assumption, $N/M \cong S^k$. Let G' and H' be as in (b). Then, $N \in \mathcal{N}(G', H')$. Hence, $N_0 = N(G', H') \leq N$. In particular, by Lemma 2.5, N_0 is a closed normal subgroup of N which satisfies $H'N_0 = G'$ and therefore $MN_0 = N$. Since G is a pro-S group, so is N/N_0. Hence, if $N_0 < N$, then N would contain an open normal subgroup N_1 which contains N_0 such that $N/N_1 \cong S$. In particular, $MN_1 = N$. On the other hand, by the definition of M, we would have $M \leq N_1$ and therefore $N_1 = N$. This contradiction implies that $N_0 = N$.

Proof of (d): The cardinality of the set of all open normal subgroups of G is at most $\max\{\aleph_0, \mathrm{rank}(G)\}$ [FrJ, Supplement 15.12]. Now use (c). ∎

THEOREM 2.7: $[\boldsymbol{\sigma}] \cong \hat{F}_\omega$ *for almost all* $\boldsymbol{\sigma} \in C_e(F)$.

Proof: By Lemmas 2.1 and 2.2 it suffices to consider a nonabelian simple group S and to prove that $r_S([\boldsymbol{\sigma}]) = \infty$ for almost all $\boldsymbol{\sigma} \in C_e(F)$.

To this end denote the set of all open normal subgroups of F by $\mathcal{E}$. Each $E \in \mathcal{E}$ is a free profinite group and $\mathrm{rank}(E) = 1 + (F : E)(n-1)$ [FrJ, Prop. 15.27]. So, there is an epimorphism h_E of E onto the free pro-S-group with $\mathrm{rank}(E)$ generators. Denote the latter group by $\bar{E}$. If $\boldsymbol{\sigma} \in E$, then $[\boldsymbol{\sigma}] = [\boldsymbol{\sigma}]_F$ is a normal subgroup of E. Hence, $h_E([\boldsymbol{\sigma}])$ is a normal subgroup of $\bar{E}$. (Nevertheless, since $[\boldsymbol{\sigma}]$ may properly contain $[\boldsymbol{\sigma}]_E$, we may have that $[h_E(\boldsymbol{\sigma})]_{\bar{E}} < h_E([\boldsymbol{\sigma}])$.) Let

$$C_e(F,E) = \{\boldsymbol{\sigma} \in C_e(F) \cap E^e \mid (\bar{E} : h_E[\boldsymbol{\sigma}]) = \infty\} \qquad C = \bigcup_{E \in \mathcal{E}} C_e(F,E),$$

Suppose first that $\boldsymbol{\sigma} \in C_e(F) \smallsetminus C$. Then, $(F : [\boldsymbol{\sigma}]) = \infty$ and for each open normal subgroup E of F that contains $[\boldsymbol{\sigma}]$, $h_E([\boldsymbol{\sigma}])$ is an open normal subgroup of $\bar{E}$. By [Mel, Prop. 2.1], $h_E([\boldsymbol{\sigma}])$ is a free pro-S-group. Moreover, $\bar{r} = \mathrm{rank}(h_E([\boldsymbol{\sigma}])) \geq \mathrm{rank}(\bar{E}) = \mathrm{rank}(E) = 1 + (F : E)(n-1)$. Let $m = \mathrm{rank}(S)$. By the remarks preceding Lemma 2.6 and by (2) of §1, $r_S([\boldsymbol{\sigma}]) \geq r_S(h_E([\boldsymbol{\sigma}])) = d_{\bar{r}}(S) \geq \frac{|S|^{\bar{r}-m}}{|\mathrm{Aut}(S)|}$. As $(F : E)$ is unbounded and $n > 1$, and since $\bar{r}$ tends to infinity with $(F : E)$, we find that $r_S([\boldsymbol{\sigma}]) = \infty$.

Next, for each $E \in \mathcal{E}$ let $\mathcal{B}(\bar{E})$ be the set of all pairs (G', H') such that $H' \leq G'$ are open normal subgroups of $\bar{E}$ and $(\bar{E} : \mathbf{N}(G', H')) = \infty$. Let $B(\bar{E})$ be the union of all the sets $\mathbf{N}(G', H')^e$ with $(G', H') \in \mathcal{B}(\bar{E})$. By the index assumption, each set $\mathbf{N}(G', H')^e$ with $(G', H') \in \mathcal{B}(\bar{E})$ has measure zero. Since $\mathcal{B}(\bar{E})$ is countable, $B(\bar{E})$ is a zero set in $\bar{E}^e$. It follows that $B = \bigcup_{E \in \mathcal{E}} h_E^{-1}(B(\bar{E}))$ is a zero set in F^e.

If $\boldsymbol{\sigma} \in C \smallsetminus B$, then there exists $E \in \mathcal{E}$ such that $\boldsymbol{\sigma} \in C_e(F,E)$ and $h_E(\boldsymbol{\sigma}) \notin B(\bar{E})$. In particular, $h_E([\boldsymbol{\sigma}])$ is a closed normal subgroup of $\bar{E}$ of an infinite index. If $r_S(h_E([\boldsymbol{\sigma}])) < \infty$, there would exist $(G', H') \in \mathcal{B}(\bar{E})$ such that $h_E([\boldsymbol{\sigma}]) = \mathbf{N}(G', H')$ (Lemma 2.6(c)). Since $h_E(\boldsymbol{\sigma}) \in h_E([\boldsymbol{\sigma}])^e$, we would have that $\boldsymbol{\sigma} \in B(\bar{E})$. This contradiction proves that $r_S([\boldsymbol{\sigma}]) \geq r_S(h_E([\boldsymbol{\sigma}])) = \infty$.

Conclude that for all $\boldsymbol{\sigma} \in C_e(F) \smallsetminus B$, we have $r_S([\boldsymbol{\sigma}]) = \infty$, as desired. ∎

Corollary 2.8:

(a) *If $e \leq n$ then $[\boldsymbol{\sigma}] \cong \hat{F}_\omega$ for almost all $\boldsymbol{\sigma} \in F^e$.*

(b) *If $e > n$, then $[\boldsymbol{\sigma}] \cong \hat{F}_\omega$ for a set of $\boldsymbol{\sigma} \in F^e$ of a positive measure (but less than 1).*

Proof: By Theorem 1.4, $\mu(C_e(F)) = 1$ (resp., $\mu(C_e(F)) > 0$) if $e \leq n$ (resp., if $e > n$). Now apply Theorem 2.7 . ∎

COROLLARY 2.9: *For each $e \geq 1$ and for almost all $\boldsymbol{\sigma} \in F^e$, $[\boldsymbol{\sigma}]$ is a free profinite group.*

Proof: If $\boldsymbol{\sigma} \in F^e \smallsetminus C_e(F)$, then $[\boldsymbol{\sigma}]$ is open in F and is therefore a free profinite group [FrJ, Prop. 15.27]. By Theorem 2.7, $[\boldsymbol{\sigma}]$ is free for almost all $\boldsymbol{\sigma} \in C_e(F)$. Hence, $[\boldsymbol{\sigma}]$ is free for almost all $\boldsymbol{\sigma} \in F^e$. ∎

Remark 2.10: Exceptional σ. Denote the intersection of all open normal subgroups N of F such that F/N is a solvable group by F^{solv}. The index of F^{solv} in F is infinite. Each open normal subgroup N of F^{solv} is the intersection of F^{solv} with an open normal subgroup of F. In particular, if F/N is simple, it is non-abelian. It follows that $F^{\mathrm{solv}} \neq \hat{F}_\omega$.

Let $\mathcal{N}$ be the set of all open normal subgroups N of F^{solv} such that F^{solv}/N is simple. Denote the intersection of all $N \in \mathcal{N}$ by M. Then F^{solv}/M is the direct product of simple non-abelian groups. Hence, there exists $\sigma \in F^{\mathrm{solv}}$ such that $\sigma \notin N$ for all $N \in \mathcal{N}$. So, $[\sigma] = F^{\mathrm{solv}}$. Thus, the conclusion of Corollary 2.8 does not hold for all $\boldsymbol{\sigma} \in F^e$. ∎

3. Appendix: The group $\hat{\mathbb{Z}}^n$

By [FrJ, Lemma 16.15], $\langle \mathbf{z} \rangle \cong \hat{\mathbb{Z}}$ for almost all $\mathbf{z} \in \hat{\mathbb{Z}}^e$. [KaL] and [Lub] consider the group $A = \hat{\mathbb{Z}}^n$ and compute the index of the subgroup $\langle \mathbf{a} \rangle$ of A generated by a random e-tuple $\mathbf{a} \in A^e$. However, they do not identify that subgroup. So, we fill up this gap here and generalize [FrJ, Lemma 16.15] for an arbitrary $n \geq 1$.

THEOREM 3.1: *For a positive integer n let $A = \hat{\mathbb{Z}}^n$. Then the following statement holds for almost all $\mathbf{a} \in A^e$:*
(a) *If $e \geq n$, then $\langle \mathbf{a} \rangle \cong \hat{\mathbb{Z}}^n$.*
(b) *If $e < n$, then $\langle \mathbf{a} \rangle \cong \hat{\mathbb{Z}}^e$.*

Proof of (a): Suppose first that $e > n$. Then, for almost all $\mathbf{a} \in A^e$ the group $\langle \mathbf{a} \rangle$ is open in A [KaL, Prop. 12]. Hence $\langle \mathbf{a} \rangle$ is the completion of a subgroup of $\mathbb{Z}^n$ of a finite index [FrJ, Lemma 15.4]. The latter is isomorphic to $\mathbb{Z}^n$. Conclude that $\langle \mathbf{a} \rangle \cong \hat{\mathbb{Z}}^n$.

Let therefore $e = n$. For each prime number p consider the quotient group $A_p = \mathbb{Z}_p^n$ of A. By the claim below, almost all $\mathbf{a} \in A^n$ have each abelian group which is generated by n elements as a quotient. Since $\langle \mathbf{a} \rangle$ is generated by n elements, [FrJ, Lemma 15.4] will give that $\langle \mathbf{a} \rangle \cong \hat{\mathbb{Z}}^n$.

CLAIM: *For almost all $\mathbf{a} \in A_p^n$ we have $\langle \mathbf{a} \rangle \cong \mathbb{Z}_p^n$.* Consider each $\mathbf{a} \in A_p^n$ as a column of height n whose ith entry is a row $\mathbf{a}_i = (a_{i1}, a_{i2}, \ldots, a_{in})$ of elements of $\mathbb{Z}_p$. In this way we identify $\mathbf{a}$ with an $n \times n$ matrix with entries in $\mathbb{Z}_p$. Then $\langle \mathbf{a} \rangle$ is a free $\mathbb{Z}_p$-module of rank which is equal to the rank of the matrix $\mathbf{a}$. Thus, $\langle \mathbf{a} \rangle \ncong \hat{\mathbb{Z}}^n$ if and only if $\det(\mathbf{a}) = 0$. But the latter condition is satisfied only for a subset of $M_n(\mathbb{Z}_p)$ of measure 0. Hence, our claim is true.

Proof of (b): Consider now each $\mathbf{a} = (\mathbf{a}_1, \ldots, \mathbf{a}_n) \in A^n$ also as a pair $\mathbf{a} = (\mathbf{b}, \mathbf{c})$, where $\mathbf{b} = (\mathbf{a}_1, \ldots, \mathbf{a}_e) \in A^e$ and $\mathbf{c} = (\mathbf{a}_{e+1}, \ldots, \mathbf{a}_n) \in A^{n-e}$. If

$$\langle \mathbf{a} \rangle \cong \hat{\mathbb{Z}}^n, \tag{1}$$

then for each abelian profinite group B and each $(b'_1, \ldots, b'_e) \in B^e$, we may extend the map $(\mathbf{b}_1, \ldots, \mathbf{b}_e) \mapsto (b'_1, \ldots, b'_e)$ to a map of $\mathbf{a}$ into B (say $\mathbf{a}_i \mapsto 0$, $i = e+1, \ldots, n$) and

therefore to a homomorphism h: $\langle \mathbf{a} \rangle \to B$. The restriction of h to $\langle \mathbf{b} \rangle$ is a homomorphism into B. It follows that $\langle \mathbf{b} \rangle \cong \hat{\mathbb{Z}}^e$.

By (a), (1) holds for almost all $\mathbf{a} \in A^n$. Hence, by Fubini's theorem [Hal, p. 147, Thm. A], for almost all $\mathbf{b} \in A^e$ the set of $\mathbf{c} \in A^{n-e}$ such that (1) holds for $\mathbf{a} = (\mathbf{b}, \mathbf{c})$ has measure 1. In particular, this set is nonempty. It follows from the preceding paragraph, that $\langle \mathbf{b} \rangle \cong \hat{\mathbb{Z}}^e$ for almost all $\mathbf{b} \in A^e$. ∎

References

[AsG] M. Aschbacher and R. Gurlanick, Some applications of the first cohomology group, Journal of Algebra **90** (1984), 446-460.

[CaF] J.W.S. Cassels and A. Fröhlich, *Algebraic Number Theory,* Academic Press, London, 1967.

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

[Hal] P. R. Halmos, *Measure Theory,* D. Van Nostrand Company, Princeton 1968.

[Jar] M. Jarden, *Large normal extensions of Hilbertian fields,* Mathematische Zeitschrift **224** (1997), 555–565.

[KaL] W.M. Kantor and A. Lubotzky, *The probability of generating a finite classical group,* Geometriae Dedicata **36** (1990), 67–87.

[KLS] Kimmerle, Lyons, Sandling, and Teaque, *Composition factors from the group ring and Artin's theorem on the orders of simple groups,* Proceedings of the London Mathematical Society (3) **60** (1990), 89–122.

[Lub] A. Lubotzky, *Random elements of a free profinite group generate a free subgroup,* Illinois Journal of Mathematics **37** (1993), 78–84.

[Man] A. Mann, *Positively finitely generated groups,* Forum Mathematicum **8** (1996), 429–459.

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