Math. Z. 168, 71–76 (1979)

Mathematische Zeitschrift

Subgroups of Finite Index in Profinite Groups

Brian Hartley

Department of Mathematics, University of Manchester, Manchester M13 9PL, England

Let $\mathfrak{C}$ be a class of finite groups. By this we understand that $\mathfrak{C}$ is a class in the usual sense, which contains all groups of order 1, and contains, with every group $G \in \mathfrak{C}$, all isomorphic copies of G. By a *pro-*$\mathfrak{C}$ group, we mean a topological group isomorphic to an inverse limit of groups in $\mathfrak{C}$, viewed as a topological group in the usual way. If $\mathfrak{C}$ is closed under taking homomorphic images, this is equivalent to saying that G is a compact totally disconnected Hausdorff topological group such that $G/N \in \mathfrak{C}$ for every open normal subgroup N of G. We write $\mathfrak{C}^*$ for the class of all *pro-*$\mathfrak{C}$ groups.

It seems to be unknown whether every subgroup of finite index in a finitely generated profinite group is open. Here we say that a profinite group is finitely generated, if it has a dense subgroup which is finitely generated in the algebraic sense. The answer is known to be affirmative if $\mathfrak{C}$ is the class $\mathfrak{A}\mathfrak{N}$ of finite abelian-by-nilpotent groups (Anderson [1]) or the class of finite supersoluble groups (Oltikar and Ribes [6]). I am indebted to L. Ribes for bringing these results to my attention, and for several stimulating discussions. We generalize these results as follows. For an integer $l \geqq 1$, let $\mathfrak{N}^l$ denote the class of all finite groups G which have a series

$$1 = G_0 \lhd G_1 \lhd \ldots \lhd G_l = G \qquad (*)$$

with all factors G_{i+1}/G_i nilpotent. The least l for which such a series exists is known as the *nilpotent length* or *Fitting height* of G.

Theorem 1. *If $G \in (\mathfrak{N}^l)^*$ (for some $l \geqq 1$) and G is finitely generated, then every subgroup of finite index in G is open.*

It is easy to see that a profinite group G belongs to $(\mathfrak{N}^l)^*$ if and only if G has a series $(*)$ in which each G_i is closed and each G_{i+1}/G_i is pronilpotent.

As in [1], we prove the theorem by showing that the algebraic derived or commutator group

$$G' = \langle [x, y] : x, y \in G \rangle$$

is closed, whenever $G \in (\mathfrak{N}^l)^*$.

0025-5874/79/0168/0071/$01.20

Lemma 1. *Let G be a compact topological group, S be a closed non-empty subset of G, and let*

$$S^n = \{s_1^{\pm 1} s_2^{\pm 1} \dots s_n^{\pm 1} : s_i \in S\} \qquad (n \geqq 1).$$

Then $G = \langle S \rangle$ if and only if $G = S^n$ for some $n \geqq 1$.

This is no doubt well known. We write $\langle X \rangle$ for the subgroup generated (algebraically) by a subset X of a group.

Proof. Suppose that $G = \langle S \rangle$. We may suppose that S contains 1 and $S = S^{-1}$. By assumption, $G = \bigcup_{n=1}^{\infty} S^n$; also each of the sets S^n is closed. If $S^n < G$ for all n, then Baire's Category Theorem ([4], p. 200) shows that one of the sets S^n is not nowhere dense. Thus S^n contains a non-empty open subset U of G. Clearly $G = \bigcup_{g \in G} U g$, and by compactness we can write $G = \bigcup_{i=1}^{m} U g_i$ $(g_i \in G)$ for some finite m. Since $G = \langle S \rangle$, we can choose $t \geqq 1$ such that $\{g_1, \dots, g_m\} \leqq S^t$. Then clearly $G = S^{n+t}$, as required.

This proves one implication; the other is trivial.

For any group G, let

$$\delta(G) = \{[x, y] : x, y \in G\}$$

denote the *set* of commutators of elements of G.

Lemma 2. *Let $\mathfrak{C}$ be a class of finite groups closed under taking subgroups, homomorphic images, and direct products. Then the following two conditions are equivalent:*

(1) *For every finitely generated $G \in \mathfrak{C}^*$ the derived group G' is closed.*

(2) *There exists an integer-valued function $f(k)$ such that $H' = \delta(H)^{f(k)}$ for every k-generator group $H \in \mathfrak{C}$ $(k \geqq 1)$.*

If these conditions are satisfied, and $\mathfrak{C}$ consists of soluble groups, then every subgroup of finite index in a finitely generated $\mathfrak{C}^*$-group is open.

Proof. (2) $\Rightarrow$ (1). Let G be a k-generator group in $\mathfrak{C}^*$ (that is, G contains a dense subgroup which is generated algebraically by k elements), let $m = f(k)$ and let $x \in G'$. If N is an open normal subgroup of G, then x is congruent modulo N to an element of $\delta(G)^m$, since $G/N \in \mathfrak{C}$. Hence $xN \cap \delta(G)^m \neq \varnothing$. Since $\delta(G)^m$ is compact and each xN is closed, it follows that $\{x\} = \bigcap_N xN$ has non-empty intersection with $\delta(G)^m$, that is, $x \in \delta(G)^m$. So $G' = \delta(G)^m$, which is closed.

Suppose that (1) holds, and let F be the free $\mathfrak{C}^*$-group on k generators, that is, $\varprojlim X/N$, where X is a free abstract group on k generators, and N runs over all normal subgroups of X such that $X/N \in \mathfrak{C}$. By assumption, F' is closed, and so we can use Lemma 1 to conclude that $F' = \delta(F)^m$ for some m. Define $f(k) = m$. Since every k-generator group H in $\mathfrak{C}$ is a homomorphic image of F, we have $H' = \delta(H)^{f(k)}$ for every such H. I am indebted to L. Ribes for this simple argument.

Now suppose the conditions hold. Let G be a finitely generated group in $\mathfrak{C}^*$. We show that every subgroup N of finite index in G is open by induction on the index. It suffices to consider the case $N \lhd G$. By ([1], Proposition 7) G/N is soluble. Unless G/N is of prime order, there is a subgroup $H \lhd G$ with $N<H<G$. By induction, H is open. Then H is also finitely generated, so again by induction, N is open. Hence we may assume that G/N is of prime order p. In that case, $N \geqq G'$, and since G' is closed, we can pass to G/G' and reduce to the case when G is abelian. Also $N \geqq G^p = \{g^p : g \in G\}$, which is also a closed subgroup of G, and passing to G/G^p, we may assume that G has exponent p. Let H be a finitely generated dense subgroup of G. Then H is finite, hence closed, and so $H = G$. Hence G is a finite discrete group, and all its subgroups are open. This proves Lemma 2.

In virtue of Lemma 2, Theorem 1 follows from the following rather surprising result, which has independent interest:

Theorem 2. *If $G \in \mathfrak{N}^l$ and G can be generated by k elements, then $G' = \delta(G)^m$, where $m = k + (2k-1)(l-1)$.*

The proof of this will require some preparatory lemmas. The first of these is based on an argument of Rhemtulla [5].

Lemma 3. *Let $G = \langle x_1, \ldots, x_r \rangle$ and let H be a nilpotent normal subgroup of G. Suppose that $H = \langle y_1^G, \ldots, y_s^G \rangle$ is generated by the conjugacy classes in G of elements $y_1, \ldots, y_s$. Then every element of $[H,G]$ can be expressed in the form $\prod_{i=1}^{r} [h_i, x_i] \prod_{j=1}^{s} [h'_j, y_j]$ $(h_i, h'_j \in H)$, where the product is taken for definiteness in order of increasing suffices.*

Proof. We use induction on the nilpotency class c of H. If $c=1$, then H is abelian. The map $h \mapsto [h, x_i]$ is then an endomorphism of H, and its image is the subgroup $[H, x_i]$. Since x_i normalizes $[H, x_i]$ and operates trivially on $H/[H, x_i]$, every subgroup of H containing $[H, x_i]$ is normalized by x_i. Hence $\prod_{i=1}^{r} [H, x_i] = L$ is normal in G. Clearly G operates trivially on H/L since each of its generators does. Hence $[H,G] \leqq L$, and we must have equality. This deals with the case $c=1$.

Now let $c>1$, let $K = \gamma_{c-1}(H)$, and $L = \gamma_c(H)$, where $\{\gamma_i(H)\}$ is the lower central series of H. By the case $c=1$, we have $[L,G] = \prod_{i=1}^{r} [L, x_i] \lhd G$. Since $[K, y_j] \leqq L$, which is central in H, the usual commutator identities

$$[ab, c] = [a,c]^b [b,c]; \qquad [a, bc] = [a,c][a,b]^c \tag{1}$$

show that the map $k \mapsto [k, y_j]$ $(k \in K)$ is homomorphic; its image is the subgroup $[K, y_j]$. Let $J = \prod_{j=1}^{s} [K, y_j]$, where the order of the factors is immaterial, and let $x \to \bar{x}$ be the natural homomorphism of G onto $\bar{G} = G/[L,G]$. Then $\bar{L}$ is central in $\bar{G}$, so $\bar{J} \lhd \bar{G}$. In the group $\bar{G}/\bar{J}$, the normal subgroup $\bar{K}/\bar{J}$ is centralized by the images of the elements $\bar{y}_1, \ldots, \bar{y}_s$, and hence also by their conjugates. Since $H = \langle y_1^G, \ldots, y_s^G \rangle$, it follows that $\bar{K}/\bar{J}$ is central in $\bar{H}/\bar{J}$, that is, $L = [H,K] \leqq [L,G] J \leqq L$. Hence $L = \prod_{i=1}^{r} [L, x_i] \prod_{j=1}^{s} [K, y_j]$.

Now let $g \in [H, G]$. By induction, we have

$$g \equiv \prod_{i=1}^{r} [h_i, x_i] \prod_{j=1}^{s} [h'_j, y_j] \mod L,$$

where h_i, $h'_j \in H$. Hence, by the previous paragraph, and since L is central in H, we can write

$$\begin{aligned} g &= \prod_{i=1}^{r} [h_i, x_i][l_i, x_i] \prod_{j=1}^{s} [k_j, y_j][h'_j, y_j] \qquad (l_i \in L, k_j \in K) \\ &= \prod_{i=1}^{r} [h_i l_i, x_i] \prod_{j=1}^{s} [k_j h'_j, y_j], \end{aligned}$$

by the identities (1). This gives the result.

A simpler version of the above argument yields the following, which was pointed out to me by P.W. Stroud in 1965:

Lemma 4. *Let $G = \langle x_1, \ldots, x_k \rangle$ be a nilpotent group. Then every element of G' can be expressed in the form $\prod_{i=1}^{k} [g_i, x_i]$, where the product is again taken in order of increasing suffices for definiteness.*

We omit the details.

Before proceeding with the main theorem, we digress to point out some purely group-theoretic consequences of Lemma 3.

Corollary 1. *Suppose that G can be generated by k elements, and G' is nilpotent. Then every element of G' can be written as a product of $\frac{1}{2}k(k+3)-1$ commutators.*

Proof. Let $G = \langle x_1, \ldots, x_k \rangle$ and $G' = H$. Then $H = \langle [x_i, x_j]^G : 1 \leqq i < j \leqq k \rangle$, so H can be generated by the G-conjugacy classes of $\frac{1}{2}k(k-1)$ elements.

By Lemma 3, every element of $[H, G]$ can be expressed as a product of $\frac{1}{2}k(k-1)+k=\frac{1}{2}k(k+1)$ commutators. Since $G/[H, G]$ is nilpotent of class at most two, a straightforward argument shows that every element of G' is congruent modulo $[H, G]$ to a product of $k-1$ commutators, of the form $[g_i, x_i]$ $(g_i \in G, 1 \leqq i \leqq k-1)$ say. From this the result follows.

It would be interesting to know how good these various bounds are.

In the same way as Corollary 1, one can prove

Corollary 2. *Suppose that G can be generated by k elements, and $\gamma_{c+1}(G)$ is nilpotent. Then every element of G' is a product of $k^{c+1}+2k$ commutators.*

The proof uses Lemma 4 and the fact that if $G = \langle x_1, \ldots, x_k \rangle$, then

$$\gamma_{c+1}(G) = \langle [x_{i_1}, \ldots, x_{i_{c+1}}]^G : 1 \leqq i_t \leqq k \rangle.$$

The next lemma is the point where finite group theory comes into play.

Lemma 5. *Let $G = AH$ be a finite group, where $A \lhd G$, $A \cap H = 1$, and A is nilpotent. Suppose that G can be generated by k elements, and $A = [A, G]$. Then A can be generated by $k-1$ conjugacy classes of elements of G.*

Proof. The argument proceeds in steps. Firstly, we may assume that A is a p-group for some prime p. For if $y_1^{(p)}, \ldots, y_{k-1}^{(p)}$ are elements whose G-conjugacy classes generate the Sylow p-subgroup of A, and $y_i = \prod_p y_i^{(p)}$, then $A = \langle y_1^G, \ldots, y_{k-1}^G \rangle$.

We may further assume that A is elementary abelian. For $A/\Phi(A)$ is elementary abelian, where $\Phi(A)$ denotes the Frattini subgroup of A, and any set of elements which generates A modulo $\Phi(A)$, already generates A.

Now we view A as an $\mathbb{F}_p H$-module, with H acting by conjugation. We have to show that A is a $k-1$-generator $\mathbb{F}_p H$-module. If B is the intersection of the maximal submodules of A, then A/B is completely reducible, and no proper submodule C of A can satisfy $A = B + C$. So we may assume that A is completely reducible.

Let V be any irreducible $\mathbb{F}_p H$-module, let $J(\mathbb{F}_p H)$ denote the Jacobson radical of $\mathbb{F}_p H$, and let m_V be the multiplicity with which V occurs in $\mathbb{F}_p H/J(\mathbb{F}_p H)$. Adopting an approach based on methods of Gaschütz, we prove:

(†) *The multiplicity of V in A is at most $m_V(k-1)$.*

From this the result follows, since $\mathbb{F}_p H/J(\mathbb{F}_p H)$ is a direct sum of m_V copies of each irreducible $\mathbb{F}_p H$-module V, and so A is a homomorphic image of a direct sum of $k-1$ copies of the cyclic module $\mathbb{F}_p H/J(\mathbb{F}_p H)$.

To see (†), let A_1 be the largest submodule of A which is a direct sum of copies of V; say $A_1 = V_1 \oplus \ldots \oplus V_t$ $(V_i \cong V, 1 \leqq i \leqq t)$, and let $G_1 = A_1 H$. Since G_1 is a homomorphic image of G, it follows that G_1 can be generated by k elements; say $G_1 = \langle x_1, \ldots, x_k \rangle$. Let $V_1^* = V_2 \oplus \ldots \oplus V_t$. If $\phi \in \mathrm{Hom}_{\mathbb{F}_p H}(V_1^*, V_1)$, then

$$U_\phi = \{v\phi + v : v \in V_1^*\}$$

is a submodule of A complementary to V_1. The number of such submodules U_ϕ is

$$|\mathrm{Hom}_{\mathbb{F}_p H}(V_1^*, V_1)| = |E|^{t-1},$$

where $E = \mathrm{End}_{\mathbb{F}_p H} V$, and in fact these exhaust the submodules complementary to V in A. For each such ϕ, $U_\phi H$ is a subgroup of G_1 complementary to V_1. Since $A = [A, H]$ we have $V_1 = [V_1, H]$ and so $C_{V_1}(U_\phi H) = 0$. Hence $U_\phi H$ has $|V|$ distinct conjugates, each intersecting A in U_ϕ. So the total number of complements to V_1 in G_1 is at least $|E|^{t-1}|V|$.

Now consider the set of all k-tuples $(v_1 x_1, \ldots, v_k x_k)$ $(v_i \in V)$. There are $|V|^k$ such, and each complement to V_1 in G can be generated by exactly one such k-tuple. Since the k-tuple $(x_1, \ldots, x_k)$ lies in no complement, we have $|V|^k > |E|^{t-1} \cdot |V|$. Let $|V| = p^a$, $|E| = p^b$. Then $t < \dfrac{a(k-1)}{b} + 1$. Clearly $a/b = \dim_E V$ and this is well known to be the same as m_V. Hence $t \leqq m_V(k-1)$, as claimed.

A much simpler argument shows that A can be generated by k conjugacy classes under far weaker hypotheses:

Lemma 5′. *Let $G = AH$, $A \lhd G$, $A \cap H = 1$ be a group. If G can be generated by k elements, then A can be generated by k conjugacy classes of G.*

Proof. Let $G=\langle x_1,\ldots,x_k\rangle$. Write $x_i=a_i h_i\,(a_i\in A, h_i\in H)$, and let $N=\langle a_1^G,\ldots,a_k^G\rangle$. Then NH is a subgroup of G containing each x_i. Therefore $NH=G$ and $N=A$.

Now we can conclude the proof of Theorem 2.

Proof of Theorem 2. This is by induction on l. If $l=1$ the theorem follows from Lemma 4. Suppose that $l>1$, and let H be the $\mathfrak{N}^{l-1}$-residual of G, that is, the smallest normal subgroup whose factor group belongs to $\mathfrak{N}^{l-1}$. Then H is nilpotent. By a theorem of Higman ([2] or [3]), G/H' splits over H/H'. Also $H=[H,G]$. By Lemma 5′, there are elements $y_1,\ldots,y_{k-1}\in H$ such that $H=H'\langle y_1^G,\ldots,y_{k-1}^G\rangle$. Since $H'\leqq\Phi(H)$, we have $H=\langle y_1^G,\ldots,y_{k-1}^G\rangle$. By Lemma 3, every element of $H=[H,G]$ can be expressed as a product of $2k-1$ commutators.

Let $u\in G'$. By induction, u can be expressed in the form $u=vw$, where v is a product of $k+(2k-1)(l-2)$ commutators, and $w\in H$. Thus u is a product of $k+(2k-1)(l-1)$ commutators, as required.

Corollary 3. *Let G be a finite group. If G can be generated by k elements, and $G\in\mathfrak{N}^l$, then there exist elements $z_1,\ldots,z_m\in G\,(m=k+(2k-1)(l-1))$ such that every element of G' has the form $\prod_{i=1}^{m}[g_i,z_i]$, where the product is taken in order of increasing i.*

This is a corollary of the proof of Theorem 2 rather than its statement.

References

1. Anderson, M.P.: Subgroups of finite index in profinite groups. Pacific J. Math. **62**, 19–28 (1976)
2. Higman, G.: The complementation of abelian normal subgroups. Publ. Math. Debrecen **4**, 455–458 (1956)
3. Carter, R., Hawkes, T.: The $\mathfrak{F}$-normalizers of a finite soluble group. J. Algebra **5**, 175–202 (1967)
4. Kelley, J.L.: General Topology. Princeton, N.J.: Van Nostrand 1955
5. Rhemtulla, A.H.: Commutators of certain finitely generated soluble groups. Canad. J. Math. **21**, 1160–1164 (1969)
6. Oltikar, B.C., Ribes, L.: On prosupersolvable groups. Pacific J. Math. (to appear)

Received January 12, 1979