339

ASTÉRISQUE

2011

SÉMINAIRE BOURBAKI
VOLUME 2009/2010
EXPOSÉS 1012-1026

(1026) *Finite index subgroups and verbal subgroups in profinite groups*

John S. WILSON

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
Publié avec le concours du CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Séminaire BOURBAKI Juin 2010
62e année, 2009-2010, n° 1026, p. 387 à 408

FINITE INDEX SUBGROUPS AND VERBAL SUBGROUPS IN PROFINITE GROUPS

by **John S. WILSON**

In the 1970s J-P. Serre proved that if H is a subgroup of finite index in a finitely generated pro-p-group G then H is necessarily an open subgroup of G, and he commented that he did not know whether the same conclusion holds for arbitrary finitely generated profinite groups G. This was finally shown to be the case by Nikolov and Segal in 2003. The result depends on important properties of values of group words in finite groups, which are likely to have other applications. We shall discuss the background to these results, aspects of the proof, related results, and some ways in which the results have already been used.

1. INTRODUCTION TO PROFINITE GROUPS

A profinite group is by definition an inverse limit of finite groups. The profinite groups can be characterized among topological groups as the compact Hausdorff totally disconnected groups.

Among the profinite groups, pro-p-groups—inverse limits of finite p-groups, where p is a fixed prime—play a distinguished role, like the role of finite p-groups among finite groups. They are precisely the compact Hausdorff totally disconnected groups such that $x^{p^n} \to 1$ as $n \to \infty$ for all elements x.

Profinite groups arise naturally in many parts of mathematics: in analysis and the general theory of topological groups as the quotients of compact groups modulo the connected component of the identity; in algebraic number theory as Galois groups, etc.; and in combinatorics and model theory as automorphism groups of structures (in connection for example with the small index property). They arise in finite group theory as objects encoding information about infinite families of groups and allowing concise statements of asymptotic results, and in infinite group theory as examples, and as completions, etc.

Since profinite groups are compact and Hausdorff, their subgroups of principal interest, those that are again profinite, are just the closed subgroups. Therefore, for example, we shall say that a subset S *topologically* generates a profinite group G if the closure of the abstract subgroup generated by S is G. A profinite group is called (*topologically*) *finitely generated* if it is topologically generated by some finite set.

Consideration of coset decompositions shows that a subgroup of finite index in a profinite group is open if and only if it is closed, and, since profinite groups are compact, that open subgroups have finite index. It is natural to ask under what circumstances the converse holds, i.e. when all subgroups of finite index are open. Since profinite groups can also be described as the topological groups (topologically) isomorphic to closed subgroups of Cartesian products of finite groups with the product topology, useful insight can be gained by considering the special case of Cartesian products.

2. CARTESIAN PRODUCTS AND THEIR IMAGES

We write $C = \prod_{i\in I} G_i$ for the Cartesian product of a family of sets $(G_i)_{i\in I}$. Its elements are the vectors $(g_i)_{i\in I}$, with entries $g_i \in G_i$ for each $i \in I$. For each i write $\pi_i : C \to G_i$ for the projection map.

If each G_i is a group, then so is C with componentwise multiplication. If each G_i is a topological space, then so is C, with subbase of open sets

$$\{\pi_i^{-1}(U) \mid i \in I,\ U \text{ open in } G_i\}.$$

If each G_i is a topological group, then so is C.

Tychonoff's theorem asserts that if each G_i is a compact topological space, then so is C. Hence if each G_i is a compact Hausdorff topological group, then so is each closed subgroup of C.

In particular, we may take each G_i to be a finite group with the discrete topology. All profinite groups are (topologically) isomorphic to closed subgroups of such products; and the countably based (i.e. separable) profinite groups are precisely the (groups isomorphic to) closed subgroups of $\prod_{n\in\mathbb{N}} \mathrm{Sym}(n)$.

In general, not all subgroups of finite index in a profinite group are open. Consider, for example, the product $C = \prod_{i\in\mathbb{N}} G_i$ with each G_i a non-trivial finite group. The definition of the product topology shows that C has $\aleph_0$ open normal subgroups. However it can be proved that if for some non-trivial finite group F we have $G_i \cong F$ for all i, then C has $2^{2^{\aleph_0}}$ subgroups of index $|F|$. In the case when $F \cong \mathbb{Z}/p\mathbb{Z}$ this is clear, for then $\dim_{\mathbb{F}_p} C = 2^{\aleph_0}$, and the dual of a vector space of infinite dimension d

has dimension 2^d. To see where non-open subgroups come from when F is non-abelian, we consider ultraproducts.

Let I be an infinite index set. We recall that an *ultrafilter* on I is a family $\mathscr{U}$ of subsets of I such that

(i) $\varnothing \notin \mathscr{U}$;
(ii) if $X_1, X_2 \in \mathscr{U}$ then $X_1 \cap X_2 \in \mathscr{U}$;
(iii) for each $X \subseteq I$, either $X \in \mathscr{U}$ or $I \setminus X \in \mathscr{U}$.

From this it follows that if $X_1 \in \mathscr{U}$ and $X_1 \subseteq X_2$ then $X_2 \in \mathscr{U}$. For $i \in I$ the family $\mathscr{U}_i = \{X \subseteq I \mid i \in X\}$ is an ultrafilter. An ultrafilter that is not of the form $\mathscr{U}_i$ must evidently contain all subsets of I with finite complements, and the existence of such *non-principal ultrafilters* follows from Zorn's lemma. We fix a non-principal ultrafilter $\mathscr{U}$.

Let $(G_i)_{i\in I}$ be a family of groups. Write $C = \prod G_i$ and let $K_{\mathscr{U}}$ be the normal subgroup $\{(g_i) \in C \mid \{i \mid g_i = 1\} \in \mathscr{U}\}$ of C. The *ultraproduct* $\prod G_i/\mathscr{U}$ is defined to be the quotient group $C/K_{\mathscr{U}}$.

Now take all groups G_i to be equal to a non-trivial finite group F. If $(g_i) \in C$ then $\{i \in I \mid g_i = f\}$ belongs to $\mathscr{U}$ for just one $f \in F$, and it follows easily that $C/K_{\mathscr{U}} = \prod G_i/\mathscr{U}$ is isomorphic to F. Clearly $K_{\mathscr{U}}$ is not open.

This method for obtaining non-open subgroups of finite index in Cartesian powers is of course non-constructive. This is necessarily the case, since it is consistent with (ZF and) the principle of dependent choice that all subgroups of finite index in all countably based profinite groups are open, as observed by Lascar [**8**].

The above argument gives the implication (i) $\Rightarrow$ (ii) in the following result:

THEOREM 2.1 (Saxl and Wilson [**20**]; Martínez and Zel'manov [**11**])
Let $C = \prod_{i\in\mathbb{N}} S_i$ with each S_i a non-abelian finite simple group. Then the following are equivalent:

(i) *all subgroups of finite index are open in C*;
(ii) *there are only finitely many groups S_i of each isomorphism type.*

It is reasonable to ask what restrictions there are on abstract images of profinite groups. They can be countably infinite: for example this holds trivially for $C = \prod G_i$ with all groups G_i cyclic of order p, and it holds for $\mathbb{Z}_p$, as shown by considering the composite of the inclusion from $\mathbb{Z}_p$ to its field of fractions $\mathbb{Q}_p$ and a surjective $\mathbb{Q}$-linear map from $\mathbb{Q}_p$ to $\mathbb{Q}$.

If $(S_i)_{i\in\mathbb{N}}$ is a family of Chevalley groups ${}^{\varepsilon}X_r(F_i)$ of the same (twisted or untwisted) type ${}^{\varepsilon}X_r$, then for any ultrafilter $\mathscr{U}$ on $\mathbb{N}$ we have $\prod_i S_i/\mathscr{U} \cong {}^{\varepsilon}X_r(\prod F_i/\mathscr{U})$ by a result of Point [**18**]; in particular this group is simple. These Chevalley groups are the

only completely explicit examples of infinite simple images of profinite groups known to the author.

Now let $\mathscr{U}$ be an ultrafilter on $\mathbb{N}$. The *ultralimit* $\lim_{\mathscr{U}} r_i$ of a bounded sequence $(r_i)_{i\in\mathbb{N}}$ of real numbers is the unique $\alpha \in \mathbb{R}$ such that for any $\varepsilon > 0$ the set $\{i \in \mathbb{N} \mid |r_i - \alpha| < \varepsilon\}$ is in $\mathscr{U}$. Again let $C = \prod_{i\in\mathbb{N}} S_i$ with each S_i a non-abelian finite simple group. Define $h = h_{\mathscr{U}} : C \to [0,1]$ by

$$h(a) = \lim_{\mathscr{U}} \frac{\log |a_i^{S_i}|}{\log |S_i|} \quad \text{for } a = (a_i) \in C;$$

here, $a_i^{S_i}$ denotes the conjugacy class of a_i in S_i. Clearly we have $h(b^{-1}ab) = h(a)$ and $h(ab) \leqslant h(a) + h(b)$ for all $a, b \in C$, and so $L_{\mathscr{U}} = \{g \in C \mid h(g) = 0\}$ is a normal subgroup of C.

Nikolov [**12**] has proved the following result.

THEOREM 2.2. — *With the above notation, the simple quotients of C are exactly the groups $C/L_{\mathscr{U}}$ for some ultrafilter $\mathscr{U}$ on $\mathbb{N}$; the infinite simple quotients all have cardinality $2^{\aleph_0}$.*

In [**4**], Holt constructed a sequence $(K_i)_{i\in\mathbb{N}}$ of finite groups with no non-trivial abelian images and with $(\log |K_i|)/(\log |\{x^2 \mid x \in K_i\}|)$ unbounded. These two properties imply that $\prod K_i$ is a profinite group with no non-trivial abelian continuous homomorphic image but with an abstract subgroup of index 2.

The implication (ii) $\Rightarrow$ (i) in Theorem 2.1 is a consequence of assertion (a) of the following result, and the proof of Theorem 2.2 depends on assertion (c). These results in turn depend on the classification of the finite simple groups (CFSG).

THEOREM 2.3. — (a) (Saxl and Wilson [**20**]; Martínez and Zel'manov [**11**]) *For each integer $q > 0$, there is a number $n(q)$ such that in every non-abelian finite simple group S either each element of S is a product of $n(q)$ q-th powers or all q-th powers equal the identity element.*

(b) (Wilson [**24**]) *There is a constant c such that every element of every non-abelian finite simple group S is a product of c commutators.*

(c) (Liebeck and Shalev [**10**]) *There is a constant d such that if S is a non-abelian finite simple group and $1 \neq h \in S$ then every element of S is a product of at most n conjugates of h, where $n = \lfloor d \log |S| / \log |h^S| \rfloor$.*

It is now known that the constant c above can be taken to be 1: thus every element of a non-abelian finite simple group is a commutator. This was established in [**9**], completing the work of many mathematicians over many years.