Available online at www.sciencedirect.com
SCIENCE DIRECT®
C. R. Acad. Sci. Paris, Ser. I 337 (2003) 303–308
COMPTES RENDUS MATHEMATIQUE

Group Theory

Finite index subgroups in profinite groups

Nikolay Nikolov [a], Dan Segal [b]

[a] *Einstein Institute of Mathematics, The Hebrew University of Jerusalem, Jerusalem 91904, Israel*
[b] *All Souls College, Oxford, Oxfordshire OX1 4AL, UK*

Received 23 June 2003; accepted 4 July 2003

Presented by Jean-Pierre Serre

Abstract

We prove that *every subgroup of finite index in a* (*topologically*) *finitely generated profinite group is open*. This implies that the topology in such a group is uniquely determined by the group structure. The result follows from a 'uniformity theorem' about finite groups: given a group word w that defines a locally finite variety and a natural number d, there exists $f = f_w(d)$ such that in every finite d-generator group G, each element of the verbal subgroup $w(G)$ is a product of f w-values. Similar methods show that in a finite d-generator group, each element of the derived group is a product of $g(d)$ commutators; this implies that the (abstract) derived group in any finitely generated profinite group is closed. ***To cite this article: N. Nikolov, D. Segal, C. R. Acad. Sci. Paris, Ser. I 337 (2003).***

Résumé

Sous-groupes d'indice fini des groupes profinis. Le résultat principal est que tout sous-groupe d'indice fini dans un groupe profini de type fini est ouvert. Par conséquent, la topologie d'un tel groupe est uniquement déterminée par la structure de groupe sous-jacente. Ce résultat se déduit d'un « théorème d'uniformité » pour les groupes finis : soit w un mot tel que la variété de groupes associée est localement finie, et soit d un entier. Si G est un groupe fini ayant d générateurs, alors chaque élément du sous-groupe verbal $w(G)$ est produit de $f_w(d)$ valeurs de w dans G. On obtient des résultats analogues pour le sous-groupe dérivé. ***Pour citer cet article : N. Nikolov, D. Segal, C. R. Acad. Sci. Paris, Ser. I 337 (2003).***

Version française abrégée

Un groupe profini G est dit de *type fini* s'il y a un ensemble fini S d'éléments de G tel que le sous-groupe engendré par S est dense en G. Notre principal résultat est

Théorème 0.1. *Dans un groupe profini de type fini, tout sous-groupe d'indice fini est ouvert.*

Cela entraîne que la topologie d'un tel groupe est déterminée par la structure de groupe sous-jacente.

E-mail addresses: nikinbg@abv.bg (N. Nikolov), dan.segal@all-souls.ox.ac.uk (D. Segal).

1631-073X/$ – see front matter
doi:10.1016/S1631-073X(03)00349-2

La démonstration s'appuie sur les propriétés de certains *sous-groupes verbaux*. Soit $w = w(x_1, \dots, x_k)$ un mot (dans le langage des groupes), et G un groupe (abstrait). On note

$$w(G) = \langle w(g_1, \dots, g_k) \mid g_1, \dots, g_k \in G \rangle,$$

le sous-groupe engendré par les *valeurs de w en G*. Le mot w est dit *localement fini* si tout groupe H de type fini avec $w(H) = 1$ est fini. Un théorème de Oates et Powell [6] entraîne l'existence, pour tout groupe fini H, d'un mot $w = w_H$ localement fini tel que $w(H) = 1$.

Théorème 0.2. *Soit w un mot localement fini, et soit G un groupe profini de type fini. Alors le sous-groupe (abstrait) verbal $w(G)$ est ouvert.*

On en déduit le Théorème 0.1 en prenant $w = w_{G/N}$, N un sous-groupe normal quelconque d'indice fini en G.

Pour montrer que $w(G)$ est ouvert, il suffit (quand w est localement fini) d'établir qu'il est *fermé*. Un argument simple et bien connu montre maintenant que Théorème 0.2 équivaut au résultat suivant, qui concerne les groupes finis :

Théorème 0.3. *Soit w un mot localement fini et soit $d > 0$ un entier. Il existe un entier $f = f_w(d)$ tel que : si G est un groupe fini engendré par d éléments, alors chaque élément de $w(G)$ peut s'écrire comme produit de f valeurs de w en G.*

Il y a aussi un résultat analogue pour le mot $[x, y] = x^{-1}y^{-1}xy$, qui n'est pas localement fini :

Théorème 0.4. *Soit $d > 0$ un entier. Il existe un entier $g = g(d)$ tel que : si G est un groupe fini engendré par d éléments et $H \lhd G$ un sous-groupe normal quelconque, alors chaque élément du sous-groupe $[H, G]$ peut s'écrire comme produit de g commutateurs $[u, v]$ $(u \in H,\ v \in G)$.*

Il s'ensuit que le *sous-groupe dérivé* $[G, G]$ *est fermé pour tout groupe profini G de type fini*.

Les deux derniers théorèmes se déduisent d'un résultat général, concernant un groupe fini $G = \langle g_1, \dots, g_d \rangle$ et un sous-groupe normal $H = [H, G]$. Il affirme que, sous des conditions convenables, tout élément de H peut s'écrire comme produit d'un nombre borné de commutateurs $[h, g_i]$ et de puissances h^q $(h \in H)$ (respectivement de commutateurs $[h, h']$ $(h, h' \in H)$). La démonstration de ce théorème, qui est longue, ressemble à une forme non-commutative du lemme de Hensel ; elle utilise la classification des groupes simples finis.

1. Strong completeness of profinite groups

A profinite group G is said to be finitely generated if it is finitely generated as a topological group, i.e., G contains a dense finitely generated subgroup. G is called *strongly complete* if it satisfies the following equivalent conditions: (a) G is its own profinite completion, (b) every group homomorphism from G to any profinite group is continuous, (c) every subgroup of finite index in G is open.

In the 1970s Serre proved that all finitely generated pro-p groups are strongly complete, and there have been several attempts in the intervening period to extend Serre's result; see [8], §4.2. Our main result is

Theorem 1.1. *Every finitely generated profinite group is strongly complete.*

This implies that the topology in such groups is uniquely determined by the underlying abstract group structure.

The proof depends on properties of certain *verbal subgroups*. If $w = w(x_1, \dots, x_k)$ is a group word, the corresponding verbal subgroup in a group G is

$$w(G) = \langle w(g_1, \dots, g_k) \mid g_1, \dots, g_k \in G \rangle,$$

the subgroup generated (*algebraically*, if G happens to be a topological group) by all w-values in G; for example, if $w = [x_1, x_2]$ then $w(G) = G'$ is the (algebraic) derived group, and if $w = x^q$ then $w(G) = G^q$. We call the word w *locally finite* if $w(G)$ has finite index in G for every finitely generated (abstract) group G. Neither $[x_1, x_2]$ nor (if q is large) x^q are locally finite, while $[x_1, x_2]x_3^q$ is locally finite for every $q > 0$.

Now let G be a d-generator profinite group and N a normal subgroup of finite index. A theorem of Oates and Powell ([6]; [3], Theorem 52.11) shows that *the laws of the finite group G/N have a finite basis*: it follows that there exists a group word w such that (a) $w(G/N) = 1$ and (b) every group H satisfying $w(H) = 1$ is isomorphic to a section of some Cartesian power of G/N; this is an application of Birkhoff's well-known characterization of group varieties, and it implies that the word w is locally finite.

Since N contains $w(G)$, Theorem 1.1 will follow from

Theorem 1.2. *Let w be a locally finite group word and let G be a finitely generated profinite group. Then the (algebraic) verbal subgroup $w(G)$ is open in G.*

Though not necessary for the main theorem, the following variation is also of interest:

Theorem 1.3. *Let G be a finitely generated profinite group and H a closed normal subgroup of G. Then the subgroup $[H, G]$ generated (algebraically) by all commutators $[h, g] = h^{-1}g^{-1}hg$ $(h \in H,\ g \in G)$ is closed in G.*

This shows in particular that *the (algebraic) derived group G' is closed*, and (by an obvious induction) that *every term of the (algebraic) lower central series of G is also closed.*

Thus $w(G)$ is closed if (a) w is a locally finite word or (b) w is one of the words $[x_1, \dots, x_n]$ with $n \geqslant 2$. This does *not* hold for arbitrary words, however: Romankov [7] has shown that it fails (even in pro-p groups) for the "2nd derived word" $w = [[x_1, x_2], [x_3, x_4]]$. On the other hand, it seems likely (though at this stage by no means certain) that it does hold for the "Burnside words" $w = x^q$; indeed, we can prove that the verbal subgroup G^q is closed in a finitely generated profinite group G provided G does not involve all finite groups as open sections.

2. Uniform bounds for finite groups

If the word w is locally finite and G is a finitely generated profinite group, then $w(G)$ is open if and only if it is closed. A simple compactness argument then shows that Theorem 1.2 is equivalent to the following result about finite groups:

Theorem 2.1. *Let w be a locally finite group word and d a natural number. Then there exists $f = f_w(d)$ such that if G is any d-generator finite group, then every element of $w(G)$ is equal to a product of f w-values.*

(By *w-values* here we mean elements of the form $w(g_1, \dots, g_k)^{\pm 1}$.)

Similarly, Theorem 1.3 follows from

Theorem 2.2. *Let d be a natural number. Then there exists $g = g(d)$ such that if G is any d-generator finite group and H is any normal subgroup of G, then every element of $[H, G]$ is equal to a product of g commutators $[u, v]$ with $u \in H$ and $v \in G$.*

In particular, every element of the derived group is a product of $g(d)$ commutators. The proof actually gives $g(d) = 12d^3 + \mathrm{O}(d^2)$. (The restriction of this theorem to *soluble* groups was the main result of [9], with the explicit function $g(d) = 72d^2 + 46d$.)

These theorems are applications of our main technical result, which is as follows. Before stating it let us introduce some notation. For any subset S of a group G and natural number n,

$$S^{*n} = \{s_1 s_2 \dots s_n \mid s_1, \dots, s_n \in S\}.$$

For $g \in G$ and $S, T \subseteq G$,

$$[S, g] = \big\{[s, g] \mid s \in S\big\}, \qquad \mathfrak{c}(S, T) = \big\{[s, t] \mid s \in S,\ t \in T\big\}.$$

For an integer q we write $G^{\{q\}} = \{g^q \mid g \in G\}$.

Key Theorem. *There exist numerical functions h_1, h_2 and z and an absolute constant D with the following property. Let $G = \langle g_1, \dots, g_d \rangle$ be a finite group and H a subgroup such that* (i) $H = [H, G]$, (ii) *if $H \geqslant N > Z$, where N and Z are normal subgroups of G and N/Z is non-Abelian, then N/Z is neither simple nor the direct product of two isomorphic simple groups. Then*

$$\text{(A):} \quad H = \big([H, g_1] \cdots [H, g_d]\big)^{*h_1(d,q)} \cdot \big(H^{\{q\}}\big)^{*z(q)}$$

for each $q \in \mathbb{N}$, and

$$\text{(B):} \quad H = \big([H, g_1] \cdots [H, g_d]\big)^{*h_2(d)} \cdot \mathfrak{c}(H, H)^{*D}.$$

The deduction of Theorem 2.1 is not quite direct. One applies the Key Theorem not to G itself but to the group $w(G)$, which is generated by a bounded number of w-values $g_1, \dots, g_{d'}$. We take $q = |F_1/w(F_1)|$, where F_1 is the infinite cyclic group, and choose a suitable characteristic subgroup H of $w(G)$: the pair $(w(G), H)$ must satisfy the hypotheses of the Key Theorem, while on the other hand Theorem 2.1 is already known for the quotient group G/H. The result then follows from (A) on noting that each element $[h, g_i]$ is a product of two w-values and each element h^q is a w-value.

Theorem 2.2 is deduced in a similar way from Key Theorem (B), applied to the pair (G, H_1) where H_1 is a suitably chosen subgroup of H.

3. Equations in finite simple groups

The Key Theorem depends ultimately on properties of the finite simple groups. The required results are far-reaching generalizations of a theorem of Wilson [10] about products of commutators in simple groups; they are proved by a delicate analysis of the internal structure of the groups, known from the classification, together with some results of Liebeck, Pyber and Shalev [1,2].

Let α, β be automorphisms of a group G. For $x, y \in G$, we define the "twisted commutator"

$$T_{\alpha,\beta}(x, y) = x^{-1} y^{-1} x^{\alpha} y^{\beta}.$$

Recall that a group S is said to be *quasisimple* if $S = [S, S]$ and $S/\mathrm{Z}(S)$ is simple (here $\mathrm{Z}(S)$ denotes the centre of S).

Theorem 3.1. *There is an absolute constant D such that if S is a finite quasisimple group and α_i, β_i $(i = 1, \dots, D)$ are any automorphisms of S then*

$$S = T_{\alpha_1,\beta_1}(S, S) \cdots T_{\alpha_D,\beta_D}(S, S).$$

Theorem 3.2. *Let q be a natural number. There exist natural numbers $C = C(q)$ and $M = M(q)$ such that if S is a finite quasisimple group with $|S| > C$, β_i $(i = 1, \dots, M)$ are any automorphisms of S, and q_i $(i = 1, \dots, M)$ are any divisors of q, then there exist inner automorphisms α_i of S such that*

$$S = \big[S, (\beta_1\alpha_1)^{q_1}\big] \cdots \big[S, (\beta_M\alpha_M)^{q_M}\big].$$

4. Proof of the Key Theorem

This is too long and elaborate to explain in detail; here is a rough sketch of the general form of argument, basically that of Hensel's lemma. Let $(g_1, \dots, g_m)$ be the sequence $(g_1, \dots, g_d)$ repeated a large number of times. To prove (A), fix $h \in H$ and consider the equation

$$h = \prod_{i=1}^{3}\prod_{j=1}^{m}[u_{ij}, g_j] \cdot \prod_{j=1}^{z} v_j^q = \Phi(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)\Psi(\mathbf{v}). \tag{1}$$

We are required to solve this equation with the u_{ij} and the v_j elements of H. We pick certain small normal subgroups $K \leqslant N$ of G, contained in H, and assume inductively that (1) can be solved modulo K. Thus

$$\Phi(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)\Psi(\mathbf{v}) = \kappa^{-1}h$$

for some $\kappa \in K$. The aim is to lift $(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3, \mathbf{v})$ to a solution of (1) by replacing u_{ij} with $a_{ij}u_{ij}$ and v_j with b_jv_j, where the a_{ij} and b_j are taken from N. This is equivalent to solving the equation

$$\Phi'_{\mathbf{u}}(\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3) \cdot \big(\Psi'_{\mathbf{v}}(\mathbf{b})\big)^{\Phi(\mathbf{u})^{-1}} = \kappa \tag{2}$$

with $\mathbf{a}_i \in N^{(m)}$ and $\mathbf{b} \in N^{(z)}$, where

$$\Phi(\mathbf{a} \cdot \mathbf{u}) = \Phi'_{\mathbf{u}}(\mathbf{a})\Phi(\mathbf{u}), \qquad \Psi(\mathbf{b} \cdot \mathbf{v}) = \Psi'_{\mathbf{v}}(\mathbf{b})\Psi(\mathbf{v})$$

in an obvious notation. Now $\Phi'_{\mathbf{u}}(\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3)$ is a product of commutators of the form $[a_{ij}, g_j]^{\gamma_{ij}}$ where the $\gamma_{ij} = \gamma_{ij}(\mathbf{u})$ depend on $\mathbf{u}_1$, $\mathbf{u}_2$, $\mathbf{u}_3$. The analogue of the non-singularity hypothesis in Hensel's lemma is the following condition, which we make part of our inductive hypothesis:

$$K\big\langle g_j^{\gamma_{ij}(\mathbf{u})} \mid j = 1, \dots, m\big\rangle = G \quad (i = 1, 2, 3); \tag{3}$$

assuming this, we then have to solve (2) subject to the additional constraint

$$\big\langle g_j^{\gamma_{ij}(\mathbf{a}\cdot\mathbf{u})} \mid j = 1, \dots, m\big\rangle = G \quad (i = 1, 2, 3). \tag{4}$$

When N is a soluble group, one proves, independently, (i) that $\Phi'_{\mathbf{u}}(\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3) = \kappa$ has many solutions, and (ii) that (4) holds for many triples $(\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3) \in N^{(3m)}$; this uses methods developed in [9]. Together, (i) and (ii) imply that (2) and (4) can be simultaneously satisfied, taking $b_j = 1$ for all j.

When N is not soluble, it is essentially a direct power of some quasisimple group S. In this case, we can show (i) that (4) is satisfied for *some* choice of $(\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3)$, and (ii) if $|S|$ is small then it is satisfied by *many* such choices.

Generalizing methods introduced in [4] and [5], and using Theorems 3.1 and 3.2, one proves (iii) that the equation $\Phi'_{\mathbf{u}}(\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3) = \kappa$ has many solutions, and (iv) provided $|S| > C(q)$, the equation $\Psi'_{\mathbf{v}}(\mathbf{b}) = \kappa'$ has at least one solution for any $\kappa' \in K$.

If S is small, (ii) and (iii) imply that we may again simultaneously satisfy (2) and (4), taking $b_j = 1$ for all j. Otherwise, by (i) and (iv) we may first pick $\mathbf{a}_1$, $\mathbf{a}_2$, $\mathbf{a}_3$ to satisfy (4), put

$$\kappa' = \big(\Phi'_{\mathbf{u}}(\mathbf{a})^{-1}\kappa\big)^{\Phi(\mathbf{u})},$$

and then solve $\Psi'_{\mathbf{v}}(\mathbf{b}) = \kappa'$.

Part (B) is proved in a similar way, using

$$\Psi(\mathbf{v}_1, \mathbf{v}_2) = \prod_{j=1}^{D} [v_{1j}, v_{2j}].$$

References

[1] M.W. Liebeck, L. Pyber, Finite linear groups and bounded generation, Duke Math. J. 107 (2001) 159–171.
[2] M.W. Liebeck, A. Shalev, Diameters of finite simple groups: sharp bounds and applications, Ann. of Math. 154 (2001) 383–406.
[3] H. Neumann, Varieties of Groups, in: Ergeb. Math., Vol. 37, Springer-Verlag, Berlin, 1967.
[4] N. Nikolov, Power subgroups of profinite groups. D.Phil. thesis, University of Oxford, 2002.
[5] N. Nikolov, On the commutator width of perfect groups, Bull. London Math. Soc., in press.
[6] S. Oates, M.B. Powell, Identical relations in finite groups, J. Algebra 1 (1964) 11–39.
[7] V.A. Roman'kov, Width of verbal subgroups in solvable groups, Algebra i Logika 21 (1982) 60–72 (in Russian). English translation: Algebra and Logic 21 (1982) 41–49.
[8] L. Ribes, P.A. Zalesskii, Profinite Groups, in: Ergeb. Math. (3), Vol. 40, Springer, Berlin, 2000.
[9] D. Segal, Closed subgroups of profinite groups, Proc. London Math. Soc. (3) 81 (2000) 29–54.
[10] J.S. Wilson, On simple pseudofinite groups, J. London Math. Soc. (2) 51 (1995) 471–490.