TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 345, Number 2, October 1994

ON POWER SUBGROUPS OF PROFINITE GROUPS

CONSUELO MARTÍNEZ

ABSTRACT. In this paper we prove that if G is a finitely generated pro-(finite nilpotent) group, then every subgroup G^n, generated by nth powers of elements of G, is closed in G. It is also obtained, as a consequence of the above proof, that if G is a nilpotent group generated by m elements $x_1, \dots, x_m$, then there is a function $f(m, n)$ such that if every word in $x_i^{\pm 1}$ of length $\leq f(m, n)$ has order n, then G is a group of exponent n. This question had been formulated by Ol'shansky in the general case and, in this paper, is proved in the solvable case and the problem is reduced to the existence of such function for finite simple groups.

A group G is called residually finite if it has a family of normal subgroups $\{N_i\}_{i\in I}$ such that G/N is a finite group and $\bigcap_{i\in I} N = 1$. The set of normal subgroups may be taken as basis of a topology over G. So a profinite group is a residually finite group that is complete with respect to the above topology, that is, an inverse limit of finite groups.

The main well-known facts that we will use about a profinite group G are the following:

(i) A profinite group G is compact.

(ii) A profinite group G is (topologically) finitely generated by elements $g_1, \dots, g_m$ if $H = \langle g_1, \dots, g_m \rangle$ is a dense subgroup of G.

For definition and basic properties of profinite groups see [1, 4 and 6].

Let G be a (topologically) finitely generated profinite group. By G^n, $n \geq 1$, we denote the subgroups of G generated by all nth powers a^n, $a \in G$.

A. Shalev conjectured that for any n the subgroup G^n is closed in G. This is the same as saying that for arbitrary integers $m \geq 1$, $n \geq 1$ there exists an integer $N = N(m, n)$ such that in an arbitrary m-generated finite group G every product of nth powers of elements of G can be represented in the form $a_1^n \cdots a_N^n$, where $a_i \in G$, $1 \leq i \leq N$.

Let us show, for example, that the existence of a function $N(m, n)$ implies that G^n is closed.

The subset $M = \{a_1^n \cdots a_N^n : a_1, \dots, a_N \in G\}$ of G is closed as the image of the compact $G \times \cdots \times G$ under the continuous map $(a_1, \dots, a_N) \to a_1^n \cdots a_N^n$. Now we can consider the finite nilpotent group G/H, where H is an arbitrary open subgroup of G and so we have $G^n H = MH$, which implies that G^n lies in the closure of M. Hence $G^n = M$.

In this paper we prove Shalev's Conjecture when G is a pro-(finite nilpotent)

Received by the editors February 8, 1994.
1991 *Mathematics Subject Classification.* Primary 20E18; Secondary 20F05.

group. A group is said to be pro-(finite nilpotent) if it is an inverse limit of finite nilpotent groups. In particular, every pro-p group is pro-(finite nilpotent).

Theorem. *Let G be a finitely generated pro-(finite nilpotent) group. Then the subgroup G^n is closed in G.*

In view of what was said above, actually we will prove that for arbitrary integers $m \geq 1$, $n \geq 1$ there exists an integer $N = N(m, n)$ such that in an arbitrary m-generated nilpotent group G every product of nth powers of elements of G can be represented in the form $a_1^n \cdots a_N^n$, where $a_i \in G$, $1 \leq i \leq N$.

Lemma 1. *Let G be an arbitrary group generated by m elements $x_1, \ldots, x_m$. Let H be a normal subgroup of G of index $\leq d$. Then we can choose a system of coset representatives of the subgroup H in G among words $x_{i_1}^{\pm 1} \cdots x_{i_k}^{\pm 1}$, $k \leq d$.*

Proof. We have to prove that an arbitrary element $g = x_{j_1}^{\pm 1} \cdots x_{j_s}^{\pm 1}$ is comparable modulo H to some word of length $\leq d$. Let us suppose that $s > d$. Consider the following $d+1$ words: $x_{j_1}^{\pm 1}, x_{j_1}^{\pm 1} x_{j_2}^{\pm 1}, \ldots, x_{j_1}^{\pm 1} x_{j_2}^{\pm 1} \cdots x_{j_{d+1}}^{\pm 1}$. Since $|G : H| \leq d$ at least two of these words are comparable modulo H. Thus there exist two subwords v' and v'' of g such that v' is a beginning of v'' and $v'H = v''H$. Hence the subword $v'^{-1}v''$ of g lies in H. Cancelling this subword out we get $gH = g_1 H$, where g_1 is a word in $x_i^{\pm 1}$ of length $< s$. This proves the lemma.

Lemma 2. *Let G be an arbitrary group generated by m elements $x_1, \ldots, x_m$. Let H be a normal subgroup of G of index $\leq d$. Then we can choose a system of generators of the subgroup H among words $x_{i_1}^{\pm 1} x_{i_2}^{\pm 1} \cdots x_{i_k}^{\pm 1}$, $k \leq 2d + 1$.*

Proof. By Lemma 1 there exists a complete system of representatives of cosets of the subgroup H in G, $g_1, g_2, \ldots$ such that every representative g_i is a word of length $\leq d$ in $x_j^{\pm 1}$. For an arbitrary element $g \in G$, let $\overline{g}$ denote the representative g_i such that $gH = g_i H$. It is known (see [3, Lemma 7.2.2]) that the subgroup H is generated by all elements $g_i x_h \overline{g_i x_h}^{-1}$. Every such element is a word of length $\leq 2d + 1$. The lemma is proved.

Lemma 3. *There exists a function $f(m, n)$ such that in an arbitrary nilpotent group G generated by m elements $x_1, \ldots, x_m$ the subgroup G^n is generated by elements v^n, where $v = x_{i_1}^{\pm 1} x_{i_2}^{\pm 1} x_{i_k}^{\pm 1}$, $k \leq f(m, n)$.*

Proof. Let $\Phi(G^n)$ be the Frattini subgroup of the group G^n. It is known that the quotient group of a nilpotent group modulo its Frattini subgroup is abelian (see [3]). It is also known that any system of generators of the group G^n modulo $\Phi(G^n)$ generates G^n. Hence, without loss of generality we will factor $\Phi(G^n)$ out and assume that the group G^n is abelian.

The positive solution of the restricted Burnside problem (see [7, 8, 9]) implies that there exists a function $h(m, n)$ such that for any m-generated nilpotent group G we have $|G : G^n| \leq h(m, n)$.

By Lemmas 1 and 2 we can find a system of coset representatives $\{g_i\}$ of the subgroup G^n in G and a system $\{h_j\}$ of generators of the subgroup G^n such that every representative g_i is a word of length $\leq h(m, n)$ and every generator h_j is a word of length $\leq 2h(m, n) + 1$.

For an arbitrary representative g_i and an arbitrary element $h \in G^n$ we have

$$(g_i h)^n = g_i^n h^{g_i^{n-1}} h^{g_i^{n-2}} \cdots h^{g_i} h$$

where $x^y = y^{-1}xy$. Since the group G^n is abelian, the expression $F(g_i, h) = h^{g_i^{n-1}} h^{g_i^{n-2}} \cdots h^{g_i h}$, where g_i is fixed is additive with respect to h, that is,

$$F(g_i, h_1 h_2) = F(g_i, h_1)F(g_i, h_2)$$

Hence the subgroup G^n is generated by g_i^n and $F(g_i, h_j) = g_i^{-n}(g_i h_j)^n$. Now it remains to let $f(m, n) = 3h(m, n) + 1$. The lemma is proved

Lemma 4 (see [1, p. 33]). *If H is a nilpotent group generated by elements $a_1, \ldots, a_d$, then every element of the commutator subgroup (H, H) to a product of the form $(g_1, a_1) \cdots (g_d, a_d)$ with $g_1, \ldots, g_d \in H$.*

Proof of the theorem. Let G be a nilpotent group generated by $x_1, \ldots, x_m$. Let $v_1, \ldots, v_s$ be all words in $x_i^{\pm 1}$ of length $\leq f(m, n)$, $s \leq (2m)^{f(m,n)+1}$. By Lemma 3, the subgroup G^n is generated by elements $v_1^n, \ldots, v_s^n$. An arbitrary element $a \in G^n$ can be represented in the form $a = (v_1^n)^{k_1} \cdots (v_s^n)^{k_s} b$, where $k \geq 0$, $1 \leq i \leq s$ and $b \in (G^n, G^n)$.

Now, from Lemma 4 it follows that there exist elements $g_1, \ldots, g_s \in G^n$ such that

$$\begin{aligned} \mathbf{a} &= (v_1^n)^{k_1} \cdots (v_s^n)^{k_s} (g_1, v_1^n) \cdots (g_s, v_s^n) \\ &= (v_1^{k_1})^n \cdots (v_s^{k_s})^n ((v_1^{-1})^{g_1})^n v_1^n \cdots ((v_s^{-1})^{g_s})^n v_s^n. \end{aligned}$$

Thus $\mathbf{a}$ is a product of $\leq 3s$ element and each of them is an nth power. We let $N(m, n) = 3(2m)^{f(m,n)+1}$. The theorem is proved.

Lemma 3 has the following corollary.

Corollary. *Let G be a nilpotent group generated by m elements $x_1, \ldots, x_m$. If every word in $x_i^{\pm 1}$ of length $\leq f(m, n)$ has order n, then G is a group of exponent n.*

This assertion can be extended to all solvable groups.

In [5] A. Y. Ol'shansky formulated the following question: Is it true that there exists a function $N(m, n)$ such that if G is a finite group generated by m elements $x_1, \ldots, x_m$ and all words in $x_i^{\pm 1}$ of length $\leq N(m, n)$ have order n then G is a group of exponent n?

Ol'shansky noted that the existence of such functions for sufficiently large n would imply the existence of a nonresidually finite hyperbolic group (the well-known problem of M. Gromov [2]).

In fact, Adian and Lysenok proved that if $F = F\langle x_1, \ldots, x_m\rangle$ denotes the free group in a finite set of free generators, $v_1, \ldots, v_r$ is a finite number of words and p is a sufficient big prime number, then the group $G = \langle x_1, \ldots, x_m | v_1^p = 1, \ldots, v_r^p = 1\rangle$ is an hyperbolic group. If the existence of the function $N(m, p)$ in the question posed by Ol'shansky was known, the above group, where $v_1, \ldots, v_r$ are the set of words in $x_i^{\pm 1}$ of length $\leq N(m, p)$, can be proved not to be residually finite considering the following steps:

1. If $H \triangleleft G$ has finite index, then G/H is a finite group generated by m elements $a_1, \ldots, a_m$ $(a_i = x_i H)$ and satisfying that every word of length $\leq N(m, p)$ has order p. So G/H has exponent p and the existence of a function

$f(m, p)$ bounding its order ($|G/H| \leq f(m, p)$) is known by the solution to the restricted Burnside problem

2. There are only finitely many normal subgroups of a given index r. So there are only finitely many subgroups of G of bounded index.

3. If G were residually finite, then it would be finite, which is known not to be the case when $m \geq 2$.

In what follows we will show that Ol'shansky's problem can be reduced to the case when G is a finite simple group, which is, however, the most difficult part of it.

Proposition 1. *Suppose that there exists a function $N_{si}(m, n)$ such that if G is a finite simple group generated by m elements $x_1, \ldots, x_m$ and all words in $x_i^{\pm 1}$ of length $\leq N_{si}(m, n)$ have order n then G is a group of exponent n. Let*

$$N(m, n) = \max(h(m, n^2), N_{si}(m^{2h(m,n)+2}, n)(2h(m, n) + 1)).$$

Then for an arbitrary finite group G generated by m elements $x_1, \ldots, x_m$ such that every word in $x_i^{\pm 1}$ of length $\leq N(m, n)$ has order n, the group G has exponent n.

Proof. Let us show first that $G^n = (G^n)^n$. The quotient $G/(G^n)^n$ is a group of exponent n^2. Hence, $|G/(G^n)^n| \leq h(m, n^2)$.

Since $N(m, n) \geq h(m, n^2)$ it follows that the group $G/(G^n)^n$ has exponent n, so $G^n = (G^n)^n$.

Suppose that $G^n \neq (1)$ and let M be a maximal normal subgroup of the group G^n such that $M \neq G^n$. Then either G^n/M is a cyclic group of prime order or G^n/M is a simple group. By Lemma 2 the subgroup G^n has a system of generators $\{g_j\}$ such that every g_j is a word in $x_i^{\pm 1}$ of length $\leq 2h(m, n) + 1$. There are not more than $m^{2h(m,n)+2}$ distinct words of this length. Because of the choice of the function $N(m, n)$ every word in $g_j^{\pm 1}$ of length $\leq N_{si}(m^{h(m,n)+2}, n)$ has order n. Hence, by our assumption, the quotient group G^n/M has exponent n. Thus, $(G)^n \subset M$, the contradiction. The proposition is proved.

This proof implies the following

Corollary. *Let G be a solvable group generated by m elements $x_1, \ldots, x_m$. If every word in $x_i^{\pm 1}$ of length $\leq \max(h(m, n^2), 2h(m, n))$ has order n, then G is a group of exponent n.*

Acknowledgments

I want to thank Professor E. Zelmanov for bringing this problem to my attention and for his continuous help and comments during the elaboration of this paper.

References

1. J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal, *Analytic pro-p groups*, London Math. Society Lecture Notes 157, Cambridge Univ. Press, 1991.
2. M. Gromov, *Hyperbolic groups*, Essays in Group Theory, MSRI Ser., vol. 8, Springer-Verlag, 1987, pp. 75–263.

3. M. Hall, *The theory of groups*, Chelsea, New York, 1976.
4. H. Koch, *Galoissche Theory der p-Erweiterungen*, VEB Deutscher Verlag der Wissenschaften, Berlin, 1970.
5. Kourovka Note-Book, *Unsolved problems in group theory*, Novosibirsk, 1993.
6. J. P. Serre, *Cohomologie galoisienne*, Springer-Verlag, 1964.
7. M. Vaughan-Lee, *The restricted Burnside problem*, 2nd ed., Clarendon Press, Oxford, 1993.
8. E. Zelmanov, *The solution of the restricted Burnside problem for groups of odd exponent*, Izv. Math.-USSR **36** (1991), 41–60.
9. ———, *The solution of the restricted Burnside problem for 2-groups*, Mat. Sb. **182** (1991), 568–592.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF OVIEDO, 33.007-OVIEDO, SPAIN
E-mail address: chelo@pinon.ccu.uniovi.es