ISRAEL JOURNAL OF MATHEMATICS **122** (2001), 149–156

GROUPS WITH MULTIPLICATIVE SUBGROUP GROWTH

BY

JAN-CHRISTOPH PUCHTA

Albert-Ludwigs-Universität Freiburg, Mathematisches Institut
Eckerstr. 1, 79104 Freiburg, Germany
e-mail: jcp@arcade.mathematik.uni-freiburg.de

ABSTRACT

The subgroup growth and the normal growth of a pronilpotent group is multiplicative. We show the converse for the normal growth and under the additional condition of prosolvability for subgroup growth. On the other hand, we show that the normal growth of any profinite group has some weak multiplicativity properties. These allow one to determine all groups with monotonic normal growth.

1. Introduction and results

Let G be a finitely generated profinite group, and denote by $a_n(G)$ the number of open subgroups of index n. An overview of recent results concerning the behaviour of $a_n(G)$ for various classes of groups was given by Lubotzky [4]. Since a profinite pronilpotent group is the direct product of its Sylow subgroups, $a_n(G)$ is multiplicative whenever G is pronilpotent. Thus the study of the subgroup growth of pronilpotent groups reduces to the study of pro-p-groups, which was initiated by Grunewald, Segal and Smith [1]. In this note we will consider the question, to what extent multiplicativity of $a_n(G)$ determines the structure of G. The question, whether multiplicativity of a_n implies pronilpotence of G, seems to be difficult unless we assume prosolvability. Things become easier if we consider $a_n^{\triangleleft}(G)$, the number of normal subgroups of index n. More generally, for every $A \leq \mathrm{Aut}(G)$ define $a_n^A(G)$ to be the number of A-invariant subgroups of index n.

Received October 25, 1999

THEOREM 1: *Let G be a finitely generated profinite group. Then the following statements are equivalent:*

1. *G is pronilpotent.*
2. *For any A, $a_n^A(G)$ is multiplicative.*
3. *There is some A with* $\mathrm{Inn}(G) \leq A \leq \mathrm{Aut}(G)$, *such that $a_n^A(G)$ is submultiplicative.*
4. *G is prosolvable, and there is some A which fixes all p'-Hall groups of G, such that* $\mathrm{Inn}(G) \leq N_{\mathrm{Aut}(G)}(A)$ *and $a_n^A(G)$ is multiplicative*

THEOREM 2: *Let G be a finitely generated profinite group. Assume that every even n with at least 3 distinct prime factors can be written as $n = d \cdot t$ with $(d,t) = 1$ and $d > 1, t > 1$, such that $a_n^{\triangleleft}(G) = a_d^{\triangleleft}(G) \cdot a_t^{\triangleleft}(G)$. Then G is prosolvable.*

On the other hand, for every group we have some weak multiplicativity, thus we cannot hope to give a simple combinatorial description of $a_n^{\triangleleft}(G)$, e.g., for free groups G, whereas $a_n(G)$ can be computed easily.

THEOREM 3: *Let G be a finitely generated profinite group.*

1. *Let $n = \prod p_i^{e_i}$ be the prime factorization of n. Assume that for every $i \neq j$ we have*
$$p_i \not| (p_j^{e_j} - 1)(p_j^{e_j-1} - 1) \cdots (p_j - 1).$$
Then we have
$$a_n^{\triangleleft}(G) = \prod a_{p_i^{e_i}}^{\triangleleft}(G).$$
2. *If G is prosolvable, then 1. is true with $a_n(G)$ instead of $a_n^{\triangleleft}(G)$.*
3. *Let p be a prime, n an integer, such that $(n, p(p-1)) = 1$ and n has no divisor $d \equiv 1 \pmod{p}$. Then we have*
$$a_{pn}^{\triangleleft}(G) = a_p^{\triangleleft}(G) \cdot a_n^{\triangleleft}(G).$$

As an application we determine all groups with monotonic growth.

THEOREM 4: *Let G be a finitely generated profinite group. Assume that $a_n^{\triangleleft}(G)$ is monotonic. Then G is trivial, cyclic of order 2 or infinite procyclic.*

The proof of Theorem 4 depends on the following result from elementary number theory.

THEOREM 5: *Let f be a monotonic real valued function. Assume that there is some Q such that for any n, relatively prime to Q, and any $\epsilon > 0$ there is some m_0 such that, for $m > m_0$, there is some m' with $|m - m'| < \epsilon m$ which solves the equation $f(nm') = f(n)f(m')$. Then there is some constant c such that we have $f(n) = n^c$ for every n relatively prime to Q.*

Theorem 5 was proven by P. Erdős under the assumption that f is monotonic and multiplicative. In the sequel monotony was replaced by several other regularity properties (see, e.g., [3] for an overview); however, the assumption of multiplicativity has never been weakened.

ACKNOWLEDGEMENT: This paper is part of the author's diploma thesis written under the supervision of T. Weigel. I would like to thank him for his help and advice.

2. Notations and preparations

In the sequel G will always denote a finitely generated profinite group. Let A be some group of automorphisms. We will call A harmless, if it fixes all p'-Hallgroups of G and if $\mathrm{Inn}(G) \leq N_{\mathrm{Aut}(G)}(A)$.

LEMMA 6: *Assume that A is harmless, $U < G$ A-invariant, $g \in G$. Then U^g is A-invariant, too.*

Proof: Assume $\alpha \in A$. Then we have

$$(U^g)^\alpha = U^{g\alpha g^{-1} g} = U^{\alpha^g g} = U^{\beta g} = U^g$$

where $\beta \in A$, since A is normalized by $\mathrm{Inn}(G)$. Note that we identified $g \in G$ with its canonical image in $\mathrm{Inn}(G)$. ∎

We define $b_n(G)$ by

$$b_n^A(G) = \sum_{\substack{[G:U]=n \\ \alpha \in A \Rightarrow U^\alpha = U}} \frac{1}{[G : N_G(U)]}.$$

The main reason to introduce b is the following property.

LEMMA 7: *Assume that G is prosolvable and that A is harmless. Then $b_n^A(G)$ is multiplicative.*

Proof: Fix an integer k. The intersection of all subgroups of index $\leq n$ is a characteristic subgroup N. Consider the natural action of A on the quotient. Since the Hall subgroups of G are exactly the projective limits of the Hall subgroups of the finite quotients of G, A acts harmless on G/N. Now $b_n^A(G/N) = b_n^A(G)$ for $n \leq k$, thus it suffices to prove that $b_n^A(G/N)$ is multiplicative. Hence we may assume that G is a finite solvable group.

Let U be an A-invariant subgroup of G, $[G : U] = n$. Let $S_{p'}$ be a p'-Hallgroup of G. In a solvable group all Sylow systems are conjugated, and for every subgroup U there is a Sylow system $\{S_p\}$ such that $U \cap S_p$ is a p-Sylow subgroup of U for all p (see, e.g., [2], VI.2.4 and VI.2.5). Hence there is some $g \in G$ such that $U^g = \bigcap_{p|n} U^g S_{p'}$ and U^g is unique. Furthermore, $U^g S_{p'}$ is A-invariant, since U^g is A-invariant by Lemma 6, and $S_{p'}$ is A-invariant by assumption. Now write $n = \prod p_i^{e_i}$, and choose for every p_i a subgroup V_i of G containing $S_{p_i'}$ of index $p_i^{e_i}$ in G. Then $\bigcap V_i$ is an A-invariant subgroup of index n, thus there is a bijection between the set of conjugacy classes of A-invariant subgroups of index n and tuples of A-invariant subgroups containing S_{p_i} of index $p_i^{e_i}$. The number of the latter is clearly multiplicative, whereas the number of the former equals $b_n^A(G)$. Thus $b_n^A(G)$ is multiplicative. ∎

Lemma 8: *Let G be prosolvable, A harmless, and $a_n^A(G)$ be multiplicative. Define $B = \langle A, \mathrm{Inn}(G)\rangle$. Then $a_n^B(G)$ is multiplicative, too.*

Proof: For every subgroup U of finite index set $\delta(U) = [G : N_G(U)]$. If U, V are A-invariant subgroups with coprime finite index, we have $\delta(U)\delta(V) \geq \delta(U \cap V)$, since $N_G(U) \cap N_G(V) \leq N_G(U \cap V)$. By Lemma 7, $b_n^A(G)$ is multiplicative, thus we have

$$b_n^A(G) = \prod_{i=1}^{k} b_{p_i^{e_i}}^A(G)$$

and

$$\sum_{\substack{[G:U]=n \\ U^A=U}} \delta(U)^{-1} = \prod_{i=1}^{k} \sum_{\substack{[G:U]=p_i^{e_i} \\ U^A=U}} \delta(U)^{-1}.$$

As in the proof of Lemma 7, for every U with $[G : U] = n$ we can find some k-tuple of subgroups U_i of index $p_i^{e_i}$, and since $a_n^A(G)$ is multiplicative, this is a bijection. Thus on both sides of the second equality above there is the same number of terms, and every single term on the right hand side is at most equal to the corresponding term on the left hand side. Thus every term on the right hand side equals the corresponding term on the left hand side, i.e., for every U we have $\delta(U) = \delta(US_{p_1'}) \cdots \delta(US_{p_k'})$. Especially, if N is an A-invariant normal subgroup, we have $\delta(US_{p_1'}) \cdots \delta(US_{p_k'}) = 1$, thus $\delta(US_{p_i'}) = 1$ for every i, hence

$US_{p_i'}$ is normal. Thus there is a bijection between k-tuples of A-invariant normal subgroups of index $p_i^{e_i}$ and A-invariant normal subgroups of index n. The latter number equals $a_n^B(G)$, whereas the first is multiplicative. ∎

3. Proof of Theorems 1–4 and 6

We begin with Theorem 1. The implication 2. ⇒ 3. is trivial, and since the p-Sylow subgroups of a pronilpotent group are characteristic, 1. implies all other statements. By Lemma 8, 4. implies 3., thus it suffices to show that 3. implies 1.

Thus assume that $a_n^A(G)$ is submultiplicative. Let N be an A-invariant, thus normal subgroup of index n, $n = \prod p_i^{e_i}$. If there exist A-invariant subgroups N_i with $[G : N_i] = p_i^{e_i}$, $\bigcap N_i = N$, then G/N is nilpotent, thus the N_i are uniquely determined. On the other hand, the intersection of A-invariant subgroups is A-invariant, thus if $\tilde{a}_n^A(G)$ denotes the number of A-invariant subgroups which are intersections of A-invariant subgroups of coprime prime power indices, we have

$$a_n^A(G) \geq \tilde{a}_n^A(G) = \prod_{i=1}^{k} \tilde{a}_{p_i^{e_i}}^A(G) = \prod_{i=1}^{k} a_{p_i^{e_i}}^A(G) \geq a_n^A(G),$$

where the last inequality reflects the assumption that $a_n^A(G)$ is submultiplicative. Thus equality holds everywhere, i.e., every A-invariant subgroup is a unique intersection of A-invariant subgroups of coprime prime power indices.

Let N be a normal subgroup of finite index. Then N contains a characteristic subgroup of finite index; so to prove that G/N is nilpotent for all N, it suffices to show that G/N is nilpotent for all characteristic N. Especially, we may assume that N is A-invariant. We know that N is the intersection of A-invariant subgroups of coprime prime power indices, thus G/N has normal p'-Hall groups for any p, thus G/N is nilpotent. Since this is true for any N, we obtain that G is pronilpotent. ∎

To prove Theorem 2, choose an open normal subgroup N. We have to show that G/N is solvable. If $[G : N]$ is odd, or has at most two different prime factors, this is true by the odd order theorem resp. Burnsides theorem. If N and M are normal subgroups of coprime index, such that G/N and G/M are solvable, $G/(N\cap M)$ is solvable. Since $N/(N\cap M)$ and $M/(N\cap M)$ are normal Hall groups, they are uniquely determined; thus if n and m are coprime, the number of normal subgroups N of index nm, which can be written as the intersection of normal subgroups of index n and m, such that G/N is solvable, equals the number of pairs (N_1, N_2) of normal subgroups of index n and m respectively, such that both G/N_1 and G/N_2 are solvable. Now let n be an integer, such that for all normal subgroups N of index $< n$, G/N is solvable. We have to show that G/N is solvable for all normal subgroups of index n. By assumption there are coprime numbers $dt = n$, $d, t > 1$, such that $a_n^{\triangleleft}(G) = a_d^{\triangleleft}(G)a_t^{\triangleleft}(G)$. There are $a_d^{\triangleleft}(G)a_t^{\triangleleft}(G)$ pairs of normal subgroups (N_1, N_2), such that $[G : N_1] = d, [G : N_2] = t$ and $G/N_1, G/N_2$ are solvable. Each such pair defines a normal subgroup N of index n with G/N solvable, hence there are at least $a_d^{\triangleleft}(G)a_t^{\triangleleft}(G)$ normal subgroups of index n with solvable quotient. But by multiplicativity this is already the total number of normal subgroups of index n, thus for all normal N with index n, G/N is solvable. ∎

To prove Theorem 3, assume that n is a natural number fulfilling the condition of 1. Every group of order n is nilpotent [5]. For let H be a minimal counterexample. Then H is minimal non-nilpotent, since the divisibility properties of n hold for any divisor of n, too. Thus $|H| = p^a q^b$. Suppose that the q-Sylow subgroups are not normal. Then their number is $\equiv 1 \pmod{q}$, and at the same time a divisor of p^a, thus there is some $j \leq a$ such that $q|p^j - 1$; by assumption $j = 0$. Thus there is only one q-Sylow subgroup, which therefore is normal. In the same way we see that the p-Sylow subgroup is normal, hence H is nilpotent.

Now assume that N is a normal subgroup of index n. Then G/N is nilpotent, thus there are uniquely determined normal subgroups N_i of index $p_i^{e_i}$ such that $N = \bigcap N_i$. Thus there is a bijection between normal subgroups of index n and tuples of normal subgroups of index $p_i^{e_i}$, which yields the desired multiplicativity.

If G is prosolvable, then $b_n(G)$ is multiplicative, and the same reasoning as in Theorem 1 gives the multiplicativity of $a_n(G)$.

Finally, if p is prime, and n has no divisor $d \equiv 1 \pmod{p}$, the p-Sylow subgroup P of any group of order np is normal. Since $(n, p(p-1)) = 1$, G/P acts trivial on P, thus P has a normal complement. If N is a normal subgroup of index pn, it can be uniquely written as the intersection of a normal subgroup of index p and a normal subgroup of index n. Thus $a_p^{\triangleleft}(G)a_n^{\triangleleft}(G) = a_{pn}^{\triangleleft}(G)$.

Finally we will show how Theorem 4 can be deduced from Theorem 3 and Theorem 5. We may assume that $a_n^{\triangleleft}(G)$ is monotonically increasing, since otherwise G is finite; and since there is exactly one subgroup of index 1 and $|G|$, we conclude that there is one subgroup of index $|G| - 1$, thus $|G| - 1 \Big| |G|$. This is impossible unless $|G| = 1, 2$. Thus we may assume that $a_n^{\triangleleft}(G)$ is nondecreasing.

We show that the assumptions of Theorem 5 are satisfied. Set $Q = 2$. If n is odd, and $p \equiv 2 \pmod{n}$ is some prime, then $(n, p(p-1)) = 1$. By Theorem 3 we get $a_p^{\triangleleft}(G)a_n^{\triangleleft}(G) = a_{pn}^{\triangleleft}(G)$ for these p. If m is sufficiently large, by the prime number theorem for arithmetic progressions (see, e.g., [6], IV.7.5) there is always a prime $p \equiv 2 \pmod{n}$ in the interval $[m, (1+\epsilon)m]$, thus the assumptions of Theorem 5 hold. We conclude that there is some constant c such that $a_n^{\triangleleft}(G) = n^c$ for all odd n. Since $a_n^{\triangleleft}(G)$ is an integer, c has to be a nonnegative integer. Since the number of subgroups of prime index p is $\equiv 1 \pmod{p}$, we conclude $c = 0$. By monotony we get $a_n^{\triangleleft}(G) = 1$ for all n. Thus G is pronilpotent. If S_p is a p-Sylow subgroup of G, we find that S_p is procyclic, thus G itself is procyclic.

4. Proof of Theorem 5

Without loss we assume that f is monotonic increasing, otherwise we consider f^{-1}. Choose $\epsilon > 0$ and an integer n which is coprime to Q. For $m > m_0 = m_0(n, \epsilon)$ we have some m' with $m/n \leq m' \leq (1+\epsilon)m/n$ such that $f(m'n) = f(m')f(n)$. Since f is monotonic, we get

$$f(m) \leq f(m'n) = f(m')f(n) \leq f\Big(\Big[(1+\epsilon)\frac{m}{n}\Big]\Big)f(n).$$

If m/n is still greater than m_0, we can apply this inequality with m replaced by $(1+\epsilon)\frac{m}{n}$ to obtain the estimate

$$f(m) \leq f\Big(\Big[(1+\epsilon)^2\frac{m}{n^2}\Big]\Big)f(n)^2.$$

By induction we obtain the bound

$$f(m) \leq f\Big(\Big[(1+\epsilon)^k\frac{m}{n^k}\Big]\Big)f(n)^k,$$

valid for any integer $k > 0$ such that

$$(1+\epsilon)^{k-1}\frac{m}{n^{k-1}} > m_0.$$

Choosing

$$k = \Big[\frac{\log m - \log m_0}{\log n - \log(1+\epsilon)} + 1\Big]$$

yields

$$f(m) \leq f(n)^{[\frac{\log m - \log m_0}{\log n - \log(1+\epsilon)} + 1]} f(m_0).$$

In the same way, we can give a lower bound for f by comparing $f(m')$ with $f([(1-\epsilon)m])$:

$$f(m) \geq f(n)^{[\frac{\log m - \log m_0}{\log n - \log(1-\epsilon)}]} f(m_0).$$

Taking the logarithm and dividing by $\log m$, we obtain

$$\frac{\log f(m)}{\log m} = \frac{\log f(n)}{\log n}(1 + O(\epsilon)) + O_\epsilon\Big(\frac{1}{\log m}\Big),$$

where the second error term depends on ϵ, since m_0 depends on ϵ. Fixing ϵ and choosing m sufficiently large, we get

$$\left|\frac{\log f(m)}{\log m} - \frac{\log f(n)}{\log n}\right| < \epsilon.$$

We may conclude that

$$\frac{\log f(m)}{\log m} \to \frac{\log f(n)}{\log n}.$$

The limit of the left hand side does not depend on n, thus $\log f(q)/\log q = c$ for any other integer q which is coprime to Q. Thus $f(n) = n^c$ for every n with $(n, Q) = 1$.

References

[1] F. J. Grunewald, D. Segal and G. C. Smith, *Subgroups of finite index in nilpotent groups*, Inventiones Mathematicae **93** (1988), 185–223.

[2] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin, Heidelberg, New York, 1967.

[3] I. Kátai, *Characterization of* $\log n$, in *Studies in Pure Mathematics to the Memory of Paul Turan* (P. Erdős, ed.), Akademia Kiado, Budapest, 1983, pp. 415–421.

[4] A. Lubotzky, *Counting finite index subgroups*, in *Groups '93 Galway/St. Andrews'* (C. M. Campbell et al., eds.), Cambridge University Press, Cambridge, 1995, pp. 368–404.

[5] G. Pazderski, *Die Ordnungen, zu denen nur Gruppen mit gegebener Eigenschaft gehoeren*, Archiv der Mathematik **10** (1959), 331–343.

[6] K. Prachar, *Primzahlverteilung*, Springer-Verlag, Berlin, Heidelberg, New York, 1978.