Available online at www.sciencedirect.com

ScienceDirect

Journal of Algebra 318 (2007) 953–956

JOURNAL OF Algebra

www.elsevier.com/locate/jalgebra

The power structure of p-groups II

Avinoam Mann

Einstein Institute of Mathematics, Hebrew University, Jerusalem, Israel

Received 20 February 2007

Available online 28 June 2007

Communicated by Aner Shalev

Abstract

We derive inequalities for the index $|G : G^p|$ in a p-group G.
2007 Published by Elsevier Inc.

Keywords: p-Groups; Power structure

Let G be a finite p-group, and let G^p and $\Omega_1(G)$ denote the subgroups of G generated by all pth powers, and by all elements of order p, respectively. Let us quote [BE] "although these subgroups are the objects of the study of the power structure of p-groups, very little is known about them in general." In that paper, N. Blackburn and A. Espuelas derive, under some assumptions, inequalities involving the orders and indices of the above subgroups. Here we prove inequalities of the same type, which hold in all p-groups. Though these inequalities follow quickly from known results and proofs, especially from results of T.J. Laffey, they seem not to have been noted before.[1]

We let $d(G)$ denote the minimal number of generators of G. Logarithms are taken to base 2.

Theorem 1. *Let G be a finite p-group, p odd, and let p^k be the maximal order of an exponent p subgroup of G. Then $|G : G^p| \leqslant p^{k(\log k+2)}$. In particular, this inequality holds if $|\Omega_1(G)| = p^k$.*

Theorem 2. *Let G be as in Theorem 1, and let E be a maximal normal elementary abelian subgroup of G. If $|E| = p^r$, then $|G : G^p| \leqslant p^{\binom{r}{2}+r}$.*

E-mail address: mann@math.huji.ac.il.

[1] This note is independent of a previous one with a similar title [M2]. I am grateful to Yakov Berkovich and to the referee for constructive remarks regarding the contents and presentation of this note. In particular, the referee pointed out that one can apply Proposition 4 to improve our original Theorem 2.

0021-8693/2007 Published by Elsevier Inc.
doi:10.1016/j.jalgebra.2007.06.022

Theorem 3. *Let G be a 2-group, and let E be a maximal normal elementary abelian subgroup of G. If $|E| = 2^s$, then $|G : G^2| \leqslant 2^{s(3s+1)/2}$. Equality holds only if G is dihedral (not of order 8), generalized quaternion, or semi-dihedral.*

We also state two inequalities for special classes of p-groups.

Definition. A p-group G is *p-central*, if either p is odd and $\Omega_1(G) \leqslant Z(G)$, or $p = 2$ and all elements of order 2 or 4 lie in $Z(G)$.

Proposition 4. *In a p-central group we have $|G : G^p| \leqslant |\Omega_1(G)|$.*

Proposition 5. *If G and k are as in Theorem 1, with $p = 3$, then $|G : G^3| \leqslant 3^{2k}$.*

For the proofs, we state first some known results.

Lemma A. *(See T.J. Laffey [L1, Corollary 1].) Let G be a p-group, p odd. Then G contains a subgroup S of class 2 and exponent p, such that $d(G) \leqslant d(S)$.*

Corollary. *Let G and k be as in Theorem 1. Then each subgroup of G can be generated by k elements.*

Lemma B. *(See J.L. Alperin [H, III.12.1].) Let G be a p-group, and let A be maximal among the normal abelian subgroups of G of exponent q, where $q \neq 2$ is a power of p. Then A contains all elements of order dividing q in $C_G(A)$.*

Lemma C. *Let G be p-central, and write $N = \Omega_1(G)$. Then G/N is also p-central, and $|\Omega_1(G/N)| \leqslant |N|$. If $|N| = p^k$, each subgroup of G can be generated by k elements.*

For the proof, see [H, III.12.2] (statement and proof) for odd p, and [M1] for $p = 2$. The second part for odd p is a special case of the Corollary to Lemma A.

Lemma D. *(See M. Bianchi–A. Gillio Berta Mauri–L. Verardi [BGV, Proposition 4(a)].) Let G be p-central, p odd, and let $x, y \in G$. Then $x^p = y^p$ iff $x\Omega_1(G) = y\Omega_1(G)$.*

Proof of Theorem 1. By Lemma A, $d(G) \leqslant k$. Moreover, if $H \leqslant G$, then $d(H) \leqslant k$ as well. Write $K = G/G^p$, and let A be a maximal normal abelian subgroup of K. By the above, $|A| \leqslant p^k$. Since $C_K(A) = A$, we can consider $L := K/C_K(A)$ as a subgroup of $\mathrm{Aut}(A)$, which in turn is isomorphic to a subgroup of $\mathbf{GL}(k, p)$. Therefore L has derived length at most $\log k + 1$. Since the factors in the derived series of L are elementary abelian and can be generated by k elements, we have $|L| \leqslant p^{k(\log k+1)}$. $\square$

Proof of Proposition 5. By [H, III.6.6 and III.6.5], groups of exponent 3 are metabelian. Hence if $p = 3$, then $H := G/G^p$ is metabelian, and, as in the preceding proof, both H/H' and H' can be generated by k elements, hence have order at most 3^k. $\square$

Proof of Proposition 4. For $p = 2$, this is a part of Lemma C, because $|G : G^2| = p^{d(G)}$. For odd p, Lemma D shows that the number of pth powers is $|G : \Omega_1(G)|$, hence $|G^p| \geqslant |G : \Omega_1(G)|$, which is our claim.

For completeness, we offer here another proof, independent of [BGV]. It proceeds by induction on $|G|$. Write $N = \Omega_1(G)$. First, assume that $N \leqslant G^p$. Then $|G : G^p| = |G/N : (G/N)^p| \leqslant |\Omega_1(G/N)| \leqslant |N|$, where the first inequality follows from the inductive hypothesis. Next, let $N \nleqslant G^p$, and write $N = (N \cap G^p) \times A$, for some subgroup $A \lhd G$ (recall that N is central and elementary abelian). Suppose that $x \in G$ and $x^p \in A$. Then $x^p \in A \cap G^p = 1$. Thus $x \in N \leqslant Z(G)$. It follows that $\Omega_1(G/A) = N/A \leqslant Z(G/A)$, i.e. G/A is also p-central. Now the induction hypothesis implies $|G : G^p| \leqslant |A||G/A : (G/A)^p| \leqslant |A||\Omega_1(G/A)| = |A||N/A| = |N|$. □

Proof of Theorem 2. Write $C = C_G(E)$. Then G/C is a p-subgroup of $Aut(E) \cong \mathbf{GL}(r, p)$, and therefore $|G : C| \leqslant p^{\binom{r}{2}}$. By Lemma B, $E = \Omega_1(C)$, and thus $\Omega_1(C) \leqslant C$, and, by Proposition 4, $|G : G^p| \leqslant |G : C^p| = |G : C||C : C^p| \leqslant p^{\binom{r}{2}+r}$. □

Proof of Theorem 3. Let A be a maximal normal abelian subgroup of G of exponent 4 containing E, and let $C = C_G(A)$. Then A is the direct product of s cyclic subgroups of order 2 or 4, $|A| \leqslant 2^{2s}$, and $|G : C| \leqslant 2^{s^2+\binom{s}{2}}$. By Lemma B, all elements of order dividing 4 in C lie in A, i.e. in $Z(C)$. By [M1, Theorem 1], $d(C) \leqslant s$, and therefore $|C : C^2| \leqslant 2^s$ and $|G : G^2| \leqslant |G : C^2| \leqslant 2^{s^2+\binom{s}{2}+s}$. Suppose that equality holds. Then, first, $|A| = 2^{2s}$ and $|G : C| = 2^{s^2+\binom{s}{2}}$, and, second, $G^2 = C^2$, hence G/C is elementary abelian. But A is the direct product of s cyclic subgroups of order 4, and G/C is isomorphic to the Sylow 2-subgroup of $\mathrm{Aut}(A)$, which is elementary abelian only if $s = 1$. That implies $|G : C| = |C : C^2| = 2$, and thus C is a cyclic maximal subgroup of G, and among the groups containing such a subgroup, only the ones listed in the theorem have a maximal normal elementary abelian subgroup of order 2. □

Let us remark, that given data as in the above results, and also the exponent of G, one can bound the order of G. This follows from the solution of the Restricted Burnside Problem [VL], since we bound the number of generators of G. A much better bound, and an elementary proof, is given in [L2].

It is natural to inquire to what extent the above bounds can be improved. There are two types of questions here. First, we can ask for improvements in the general case. Is, say, the logarithmic factor really necessary? Or we can ask what happens for specific values of k (or of r or s). E.g. if in Theorem 1 we have $k < p - 1$, then G is regular [H, III.10.14], and $|G : G^p| = |\Omega_1(G)| = p^k$. If $k = p - 1$, then G is either regular or of maximal class [B, Theorem 1.1], and in the latter case we have $|G : G^p| = p^p$ [H, III.14.16]. Thus the first open case is $k = p$, more specifically, we can ask for the structure of groups in which $|\Omega_1(G)| = p^p$ (that question, raised by Y.Berkovich, prompted the investigations in this note). As for Theorem 2, the split extension of an elementary abelian group E of order p^r by the Sylow p-subgroup of $Aut(E)$ has order $p^{\binom{r}{2}+r}$, and is of exponent p if p is large relative to r. Hence the bound in Theorem 2 is best possible in general, but can be improved for small values of r. Finally, Y. Berkovich has pointed out that if $s = 2$ in Theorem 3, then it can be shown that $|G : G^2| \leqslant 2^4$.

There is no converse of the above theorems. To see this, let F be a non-abelian free group of rank d, let H be a normal subgroup of finite p-power index, let H/N be the largest finite factor group of H of exponent p, and take $G = F/N$. Since $d(H) = |F : H|(d - 1) + 1$, the order of H/N, and with it of $\Omega_1(G)$, can be made arbitrarily large, by choosing H of large enough index, but the order of G/G^p is bounded by the largest order of a finite d-generator group of exponent p. A more elementary example is exhibited by groups of maximal class and order at least p^{p+1}. As we remarked already, in these groups $|G : G^p| = p^p$. But there exist groups of maximal class of any order $\geqslant p^{p+1}$ such that $\Omega_1(G) = G$ (by [H, III.14.13(b)], if G is of maximal class, then $\Omega_1(G/Z(G)) = G/Z(G)$). However, the largest order of a subgroup of exponent p in these groups is p^p, while in the previous examples we can find elementary abelian subgroups of arbitrarily large order.

If $|G/G^p| \leqslant p^{p-1}$, then G is regular [H, III.10.13], and $|\Omega_1(G)| = |G : G^p|$. What if $|G/G^p| = p^p$? The 2-groups such that $|G : G^2| = 4$ are just the 2-generator groups, and they can contain arbitrarily large elementary abelian subgroups. For $p = 3$, taking F above to be of rank 2 yields 3-groups containing arbitrarily large elementary abelian subgroups with $|G/G^3| = 3^3$. Other examples, valid for all odd primes, are provided by the so-called *Nottingham Group*. This is an infinite pro-p group, in which $|G : G^p| = p^p$, and it has finite quotients (which are p-groups) containing normal elementary abelian subgroups of arbitrarily large order. For the proofs, see [C, Theorem 6 and Remark 3(i) following it; take $q = p$] (these examples were pointed out by the referee).

References

[BGV] M. Bianchi, A. Gillio Berta Mauri, L. Verardi, Groups in which elements with the same p-power permute, Matematiche (Catania) 51 (Suppl.) (1996) 53–61 (1997).

[B] N. Blackburn, Generalizations of certain elementary theorems on p-groups, Proc. London Math. Soc. (3) 11 (1961) 1–22.

[BE] N. Blackburn, A. Espuelas, The power structure of metabelian p-groups, Proc. Amer. Math. Soc. 92 (1984) 478–484.

[C] R. Camina, The Nottingham group, in: M.P.F. du Sautoy, D. Segal, A. Shalev (Eds.), New Horizons in pro-p Groups, Birkhäuser, Boston, 2000.

[H] B. Huppert, Endliche Gruppen I, Springer-Verlag, Berlin, 1967.

[L1] T.J. Laffey, The minimum number of generators of a finite p-group, Bull. London Math. Soc. 5 (1973) 288–290.

[L2] T.J. Laffey, Bounding the order of a finite p-group, Proc. R. Ir. Acad. 80A (1980) 131–134.

[M1] A. Mann, Generators of 2-groups, Israel J. Math. 10 (1971) 158–159.

[M2] A. Mann, The power structure of p-groups I, J. Algebra 42 (1976) 121–135.

[VL] M.R. Vaughan-Lee, The Restricted Burnside Problem, 2nd ed., Oxford University Press, Oxford, 1993.