Linear and Multilinear Algebra, 1976, Vol. 3, pp. 307–312

Printed in Great Britain

How Abelian is a Finite Group?

Dedicated to Olga Taussky

P. ERDÖS and E. G. STRAUS

University of California at Los Angeles

(*Received October 7, 1975*)

INTRODUCTION

A well known theorem of G. A. Miller [4] (see also [2]) shows that a p-group of order p^n where $n > v(v-1)/2$ contains an Abelian subgroup of order p^v. It is clear that this theorem together with Sylow's Theorem implies that any finite group of large order contains an Abelian p-group of large order. In this note we use simple number theoretic considerations to make this implication more precise. In Section 1 we show that a group of finite order n contains an Abelian p-group whose order is greater than $\log n - o(\log n)$. We also give arguments to indicate that the correct answer is probably considerably larger.

In the opposite direction it is now known as a result of the work of Adjan and Novikov [1] that Burnside groups with more than one generator whose degree is, say, a sufficiently large prime contain no noncyclic finite or Abelian subgroups. Thus no analogous results about large Abelian subgroups hold for infinite groups.

About the upper bounds on the orders of Abelian subgroups of finite groups, it was shown by J. L. Alperin that there exist p-groups of order p^{3n+2} without Abelian subgroups of order greater than p^{n+2}. The symmetric group S_{3n} contains no Abelian subgroup of order greater than $3^n < N^{c/\log\log N}$ where $N = (3n)! = |S_{3n}|$. Thus for any $\varepsilon > 0$ there are finite groups G whose largest Abelian subgroup has order $o(|G|^\varepsilon)$.

In Section 2 we obtain lower bounds for the number of (ordered) k-tuples of elements of a group G which have pairwise commuting elements. For $k = 2$ this question was answered by Erdös and Turan [3]. And the general

question was raised by Linnik at a conference in Balaton-Füred 1969. As in that paper, the answer is intimately related to the number $c(G)$ of conjugacy classes of G. The growth rate of

$$c(n) = \min_{n \leqslant |G| < \infty} c(G)$$

is very imperfectly understood. The best general result is still the one of Landau [3]

$$c(n) > \log_2 \log_2 n.$$

The correct growth rate of $c(n)$ is probably much larger. Perhaps $c(n!) = p(n)$, the number of partitions of n, which is the value attained for the symmetric group S_n. Any improvement on the estimate of $c(n)$ would give corresponding improvements of the estimates in Section 2.

1. LOWER BOUNDS FOR THE ORDER OF ABELIAN p-GROUPS IN A GROUP OF ORDER n

Assume that G is a group of order n and every Abelian p-group $A < G$ has order $|A| \leqslant f(n)$ then by Miller's theorem it follows that for every primary divisor p^ν of n we have $p \leqslant f(n)$ and, if $p \leqslant \sqrt{f(n)}$, then

$$p^{\sqrt{2\nu}-\frac{1}{2}} < f(n), \quad \text{or} \quad \nu < \frac{1}{2}\left(\frac{\log f(n)}{\log p} + \frac{1}{2}\right)^2 < \left(\frac{\log f(n)}{\log p}\right)^2.$$

Thus for

$$n = \prod_{p_i \leqslant f(n)} p_i^{\nu_i}$$

we have

$$\log n = \sum_{p_i \leqslant f(n)} \nu_i \log p_i < \sum_{p_i \leqslant f(n)} \log p_i + \log^2 f(n) \sum_{p_i \leqslant \sqrt{f(n)}} \frac{1}{\log p_i} < f(n) + o(f(n))$$

we have thus proved:

THEOREM 1.1. *A group G of order n contains an Abelian p-group, A, with*

$$|A| > \log n - o(\log n). \tag{1.2}$$

The lower bound in Theorem 1.1 could only be approximated under very unlikely circumstances. Say we assume that $|A| < (1 + \delta) \log n$ for all Abelian subgroups $A < G$ where $|G| = n$. Then we have seen that n must be nearly the product of all primes $\leqslant \log n$ with the omission of a small number of primes and the inclusion of some primes p, $\log n < p < (1 + \delta) \log n$ and higher powers of some primes $< \sqrt{(1 + \delta) \log n}$. For each prime p $p \geqslant (1 + \delta)/2 \log n$ which divides n. The Sylow p-group, S_p, must be self-centralizing for otherwise there would be a cyclic subgroup of order $pq \geqslant 2p \geqslant (1 + \delta) \log n$.

Thus the normalizer $N(S_p)$ must have order pd_p where $d_p \mid (p-1)$ and the number of conjugate Sylow p-groups is

$$\frac{n}{pd_p} \equiv 1 (\mathrm{mod}\ p).$$

In other words, for each $p \geqslant (1+\delta)/2 \log n$ which divides n we have

$$\frac{n}{p} \equiv d_p (\mathrm{mod}\ p) \tag{1.3}$$

where d_p is a divisor of $p-1$. Similar results could be obtained for primes $p \geqslant (1+\delta)/3 \log n$ etc. Since the number of conjugacy classes of elements of order p is $(p-1)/d_p$ most of the values d_p in (1.3) must be "large" divisors $(>cp/\log p)$ of $p-1$. In any case the existence of large n which satisfy a large system of simultaneous congruences (1.3) appears improbable.

2. ON THE NUMBER OF COMMUTING k-TUPLES IN A GROUP OF ORDER n

In this section we wish to obtain inequalities for the numbers $A_k(n)$ of ordered k-tuples $(a_1, a_2, \ldots, a_k)$ of elements a_i in a group G of order n so that $a_i a_j = a_j a_i$ for all $1 \leqslant i, j \leqslant k$. For $k = 2$ Erdös and Turan [3] proved the following.

THEOREM 2.1 *The number of commuting pairs (a_1, a_2) of elements of a group G is*

$$A_2(G) = |G| c(G) \tag{2.2}$$

where $c(G)$ is the number of conjugacy classes of G. Since $c(G)$ goes to infinity with $|G|$ it follows from (2.2) *that, for example*

$$A_2(n) > n \log_2 \log_2 n. \tag{2.3}$$

For the sake of completeness we include the simple proof.

Each $a \in G$ commutes with the elements of its centralizer $Z(a)$. So the number of commuting ordered pairs (a, b) is $|Z(a)|$. This number clearly remains unchanged if a is replaced by a conjugate element. Thus the number of commuting ordered pairs (a', b') with $a' \sim a$ is $|C(a)|\,|Z(a)| = |G|$, where $C(a)$ is the conjugacy class of a. Summing over the $c(G)$ conjugacy classes gives us $|G|c(G)$ commuting ordered pairs.

We now first consider the number of $A_3(G)$ of commuting triples in G and wish to show that for large $|G|$ that number is large compared to $A_2(G)$. For this purpose we observe that the number of conjugacy classes whose elements have centralizers of order $< \frac{1}{2}c(G)$ is certainly itself less than $\frac{1}{2}c(G)$ since each such class contains more than $2|G|/c(G)$ elements.

Restricting attention to those $a \in G$ with $|Z(a)| \geqslant \frac{1}{2}c(G)$ we see that each such a belongs to $|Z(a)|c(Z(a))$ ordered commuting triples (a, b, c) since (b, c) can be any of the $|Z(a)|c(Z(a))$ commuting pairs in $Z(a)$.

Thus the number of ordered commuting triples (a', b, c) with $a' \equiv a$ is

$$|C(a)|\,|Z(a)|c(Z(a)) = |G|c(Z(a)).$$

Summing over the conjugacy classes with centralizers of order $\geqslant \frac{1}{2}c(G)$ we get at least

$$\tfrac{1}{2}|G|c(G)c(Z(a)) > c_2 A_2(G) \log\log c(G)$$

ordered commuting triples.

THEOREM 2.4 *Let $c(n)$ denote the minimal number of conjugacy classes in a group of order $\geqslant n$. Then the number of commuting ordered triples of elements of G is*

$$A_3(G) > \tfrac{1}{2}|G|c(G)c(\tfrac{1}{2}c(G)).$$

We can now iterate this process to obtain lower bounds for ordered commuting k-tuples of elements of a group G.

THEOREM 2.5 *Let $c_l(n)$ be defined by $c_1(n) = c(n)$ and $c_{l+1}(n) = c(\frac{1}{2}c_l(n))$. Then the number of commuting ordered k-tuples in a group G satisfies*

$$A_k(G) > \frac{1}{2^{k-2}}|G|c(G)c_2(|G|)\ldots c_{k-1}(|G|) \tag{2.6}$$

for all sufficiently large $|G|$. In particular if $A_k(n)$ is the minimal number of commuting ordered k-tuples in any group of order $\geqslant n$ we have

$$A_k(n) \geqslant \frac{1}{2^{k-2}}nc_1(n)c_2(n)\ldots c_{k-1}(n). \tag{2.7}$$

Further we have

$$A_k(G)/A_{k-1}(G) \to \infty \quad as \quad |G| \to \infty. \tag{2.8}$$

Proof By induction on k. We already know (2.6) for $k = 2$. Now assume that (2.6) holds for k and that $|G|$ is so large that it holds for all groups of order $\geqslant \frac{1}{2}c(G)$. Then each a with centralizer $Z(a)$ of order $|Z(a)| \geqslant \frac{1}{2}c(G)$ is the first element of $A_k(Z(a))$ commuting ordered $(k+1)$-tuples. The same holds for all the conjugates of a and hence the number of commuting ordered $(k+1)$-tuples whose first element is conjugate to a is

$$|C(a)|A_k(Z(a)) \geqslant |C(a)|\frac{1}{2^{k-2}}|Z(a)|c(Z(a))\ldots c_{k-1}(|Z(a)|) \tag{2.9}$$

$$\geqslant \frac{1}{2^{k-2}}|G|c_2(|G|)\ldots c_k(|G|).$$

Summing (2.9) over those conjugacy classes whose elements have centralizers of order $\geqslant \frac{1}{2}c(G)$ we get

$$A_{k+1}(G) \geqslant \frac{1}{2^{k-1}} |G| c(G) c_2(|G|) \dots c_k(|G|). \tag{2.10}$$

To prove (2.8) we again proceed by induction on k. From Theorem 2.4 we know that $A_3(G)/A_2(G) \to \infty$ as $|G| \to \infty$. Now assume that for each $M > 0$ there is an $N(M)$ so that for all $|G| \geqslant N$ we have $A_{k+1}(G)/A_k(G) > M$. Now pick $|G|$ so large that $c(G) > N(2M)^k$ and write

$$\frac{A_{k+2}(G)}{A_{k+1}(G)} = \frac{\sum |C(a)| A_{k+1}(Z(a))}{\sum |C(a)| A_k(Z(a))} \tag{2.11}$$

where the summation extends over the conjugacy classes of G. There are at most $c(G)^{1/k}$ conjugacy classes $C(a)$ for which $|Z(a)| < N(2M)$. Thus we get

$$\begin{aligned} A_{k+2}(G) &\geqslant \sum_{|Z(a)| \geqslant N(2M)} |C(a)| A_{k+1}(Z(a)) \\ &\geqslant 2M \sum_{|Z(a)| \geqslant N(2M)} |C(a)| A_k(Z(a)) \\ &= 2M(A_{k+1}(G) - \sum_{|Z(a)| < c(G)^{1/k}} |C(a)| A_k(Z(a) \\ &> 2M(A_{k+1}(G) - \sum_{|Z(a)| < c(G)^{1/k}} |C(a)| c(G)) \\ &> 2M(A_{k+1}(G) - A_2(G)) \\ &> M A_{k+1}(G). \end{aligned}$$

3. COMMENTS AND PROBLEMS

A companion question to the one discussed in Section 2 would be the consideration of a maximal set $\{a_1, \dots, a_k\}$ of elements in a group G so that no two elements commute. The dihedral group D_n of order $2n$ gives an example for the existence of groups where k is more than half the order of the group.

QUESTION 3.1* *Is it true that in a group G of order n there are at most* $[n/2] + 1$ *elements no two of which commute?*

A companion question to 3.1 would be that of covering a group by subgroups. Clearly the answer to Question 3.1 deals with a lower bound.

QUESTION 3.2 *Can a group G or order n be expressed as the union of no more than* $[n/2] + 1$ *Abelian subgroups?*

M. Isaacs has shown that there exist relations between the maximal number, M, of elements in a group G no two of which commute and the minimal covering, m, of a group by Abelian subgroups. He found inequalities of the form $m \leqslant (M!)^2$ and exhibited finite groups for which $m \geqslant 2^{M/2}$.

* Added in proof: This question was answered in the affirmative by David R. Mason.

References

[1] S. Adjan and P. S. Novikov, Infinite periodic groups I, II, III, *Izv. Akad. Nauk SSR Ser. Mat.* **32** (1968), 212–244, 251–524, 709–731.
[2] W. Burnside, On some properties of groups whose orders are powers of primes, *Proc. London Math. Soc.* **11** (1913), 225–245.
[3] P. Erdös and P. Turan, On some problems of a statistical group-theory IV, *Acta Math. Hungaricae*, **19** (1968), 413–435.
[4] G. A. Miller, H. F. Blichfeldt and L. E. Dickson, *Theory and Applications of Finite Groups*, Dover (1961), p. 120.