The Derived Length of \( p \)-Groups

Avinoam Mann

Einstein Institute of Mathematics, The Hebrew University of Jerusalem, Jerusalem, Israel 91904

Communicated by Alexander Lubotzky

Received April 27, 1999

In this note we prove two results concerned with the derived length of \( p \)-groups. First, we improve a little a lower bound of P. Hall for the order of a group of a given derived length. Next, we improve a bound for the derived length of a product of two \( p \)-groups.

1. ORDERS

Let \( G \) be a group of order \( p^n \) and derived length \( k + 1 \). It was shown by Hall [H, III.7.11] that \( n \geq 2^k + k \). We provide a small improvement.

**Theorem 1.** Let \( G \) have order \( p^n \) and derived length \( k + 1 \). Then \( n \geq 2^k + 2k - 2 \).

**Corollary 2.** A \( p \)-group of derived length 4 has order at least \( p^{13} \).

It is well known that the least possible order of a non-abelian group is \( p^3 \). The least order of a group of length 3 is \( p^7 \) for \( p = 2, 3 \), and \( p^9 \) in general (see [B1]). For groups of length 4, the bound of the corollary is not yet the best possible, as it is known that for \( p \) odd, a group of length 4 has order at least \( p^{14} \) (theses of Blackburn and Evans-Riley). For primes at least 5, groups of length \( k \) and order \( p^{2k-2} \) were constructed by Evans *et al.* [ERNS], improving previous examples of Hall, which have, for all primes, order \( p^{2k-1} \) (see [H, III.17.7] for odd primes, and there exist easy matrix...

---

1 The author is indebted to N. Blackburn, S. Evans-Riley, M. Morigi, and M. F. Newman for communicating their results prior to publication, for acquainting him with several of the references of this note, and for helpful comments generally.
examples for \( p = 2 \). Thus for \( p \geq 5 \) the minimal order of a group of length 4 is \( p^{14} \), and for \( p = 2, 3 \) the minimal order is \( p^{13}, p^{14}, \) or \( p^{15} \).

**Proof of Theorem 1.** Hall’s proof depends on the following lemma [H, III.7.10].

**Lemma 3.** Let \( N \) be a non-abelian normal subgroup of \( G \) contained in \( \gamma(G) \). Then \( |N| \geq p^{i+2} \). In particular, if \( G^{(i+1)} \neq 1 \), then \( |G^{(i)} : G^{(i+1)}| \geq p^{2i+1} \).

Summing the last inequality over all \( i < k \), we get \( |G : G^{(k)}| \geq p^{2k+1} \), so \( |G| \geq p^{2k+1} \). Theorem 1 will be proved by showing that equality, \( |G^{(i)} : G^{(i+1)}| = p^{2i+1} \), is possible for two values of \( i \) at most. So suppose that this equality holds for some \( i \), and let this \( i \) be the smallest one for which it holds. Assume for the moment that \( G^{(i+1)} = p \) and \( |G^{(i)}| = p^{2i+2} \). If \( G^{(i)} \) contains two normal subgroups of \( G \) of order \( p^2 \), their product is a subgroup \( M \leq Z_2(G) \) which is either maximal or equal to \( G^{(i)} \). In either case \( G^{(i+1)} = [G^{(i)}, M] = 1 \), a contradiction. Therefore \( G^{(i)} \) contains a unique subgroup, say \( N \), which has order \( p^2 \) and is normal in \( G \). Omitting the assumption that \( |G^{(i+1)}| = p \), this means that \( G^{(i)} \) contains a unique subgroup, still called \( N \), which has index \( p^2 \) and is normal in \( G \).

Consider \( K = [G^{(i)}, G] \). If \( |G^{(i)} : K| \geq p^2 \), then \( K \leq N \). But any subgroup between \( G^{(i)} \) and \( K \) is normal in \( G \); therefore the uniqueness of \( N \) shows that \( G^{(i)}/K \) has a unique subgroup of index \( p^2 \), so either \( K = N \) or \( G^{(i)}/K \) is cyclic. The latter is also the case, of course, if \( |G^{(i)} : K| = p \). But if \( G^{(i)}/K \) is cyclic, then \( G^{(i+1)} = [G^{(i)}, K] \leq [\gamma_2(G), \gamma_2+1(G)] \leq \gamma_2+1+1(G) \). Then for any \( i < j < k \) we obtain that \( G^{(j)} \leq \gamma_2+1(G) \), so Lemma 3 applied to \( N = G^{(j)} \) shows that \( |G^{(j)} : G^{(j+1)}| \geq p^{2j+2} \).

There remains the possibility that \( K = N \). We then consider \( L := [N, G^{(i)}] \). Since \( N/L \leq Z(G^{(i)}/L) \), the group \( G^{(i)}/L \) has a centre of index \( p^2 \), hence a commutator subgroup of order \( p \), i.e., \( |G^{(i+1)}/L| = p \). Now we see that

\[
G^{(i+1)} = [L, G^{(i+1)}] = [N, G^{(i)}, G^{(i+1)}] = [G, G^{(i)}, G^{(i)}, G^{(i+1)}] \leq \gamma_2+2+1(G)
\]

and the argument continues as before.

Note that the proof shows that equality in Theorem 1 is possible only if the two values of \( i \) for which \( |G^{(i)} : G^{(i+1)}| = p^{2i+1} \) holds are \( k - 1 \) and \( k - 2 \).

**Proof of Corollary 2.** Let \( G \) have derived length 4. Theorem 1 and the last remark show that \( |G| \geq p^{12} \), and equality is possible only if \( |G^{(i)} : G^{(i+1)}| = p^{2i+1} \) for \( i = 1, 2 \). But \( |G : G^2| \geq p^4 \), by [B2].
2. PRODUCTS

Let $G = AB$ be a product of two subgroups. It was proved by Ito [AFG, 2.1.1] that if $A$ and $B$ are abelian, then $G$ is metabelian. The Wielandt-Kegel theorem states that if $G$ is finite and $A$ and $B$ are nilpotent, then $G$ is soluble [AFG, 2.4.3]. But it is still not known if in that situation $dl(G)$ is bounded by a function of $cl(A)$ and $cl(B)$. Here $dl(X)$ and $cl(X)$ denote the derived length and class of the group $X$, respectively. By [P], to provide such a bound it suffices to do so when $G$ is a $p$-group. The even stronger conjecture that $dl(G) \leq cl(A) + cl(B)$, which holds when $A$ and $B$ have relatively prime orders [AFG, 2.5.4], was recently disproved in [CS], even when $G$ is a $p$-group.

We now assume again that $G$ is a $p$-group. Write $A \mathbb{Z} p^m; B \mathbb{Z} p^n$. A bound in terms of the classes obviously implies one in terms of $m$ and $n$. A result of the latter type was obtained by Kazarin [K], namely $dl(G) \leq 2m + n + 2$. In [M] Morigi improved that to $dl(G) \leq 2m + n + 2$. The main effort in [M] is in the case that $A$ is abelian ($m = 0$). In this case the bound is $n + 2$, and examples given in [M] and [CS] show that we may have $n = 1$ and $dl(G) = 3$, or $n = 2$ and $dl(G) = 4$. But for large $n$ the bound can be improved significantly. This is stated in Corollary 5, which follows immediately from the next result, proved by the method of [M].

**Theorem 4.** Let the $p$-group $G = AB$ be a product of an abelian group $A$ and a group $B$ satisfying $B \mathbb{Z} p^n$. Then $cl([A, B]) \leq 2n + 1$.

**Corollary 5.** Let $G$ be as in the theorem. Then $dl(G) < 2 \log_2 (n + 2) + 3$.

Note that if in the aforementioned examples of Hall we write $G \mathbb{Z} p^n$, then $dl(G)$ is about $log_2 n$, so taking $B = G$ and $A = 1$ we see that our bound is of the right order of magnitude. However, we do not know if a similar bound obtains without the assumption that $A$ is abelian. For the general case we have

**Corollary 6.** Given $\varepsilon > 0$ there exists $C = C(\varepsilon)$ such that if $G = AB$ is a $p$-group and $|A'| = p^n, |B'| = p^n$, then $dl(G) \leq (m + 1)C + en$.

For the proof of Theorem 4 we need two lemmas from [M]. First, it is pointed out in Lemma 2 of [M] that Ito’s proof for the case of two abelian factors establishes a more general result. For completeness, we state here an even more general result, though we need only the same special case as in [M]. The proof is still the same as Ito’s.


Lemma 8. Let $G$ be as in the theorem, with $B$ not abelian. Then there exists a subgroup $W \leq Z(B)$ such that $AW = WA$ and $AW \cap B' \neq 1$.

This is proved in the course of the proof of Theorem 1 of [M].

Proof of Theorem 4. The proof is given by induction on $n$, the case $n = 0$ being the result of Ito mentioned above. So we assume now that $B$ is not abelian.

Case I ($A \cap B' \neq 1$). Write $T = A \cap B'$. Then $T^G = T^{AB} = T^B \leq B'$.

Let $N \leq T^G$ be normal in $G$ and of order $p$. Then $N \leq Z(G)$, and $|(B/N)| = p^{n-1}$, so by induction $cl([A, B]N/N) \leq 2(n - 1) + 1$, and $cl([A, B]) \leq 2n$.

Case II (The General Case). Write $Z = Z([A, B])$, and consider $G/Z = AWZ/Z邹BZ/Z$, where $W$ is the subgroup guaranteed by Lemma 8. Still following [M], we note that taking $V = A$ in Lemma 7 shows that $[A, W] \leq Z$. Therefore $AWZ/Z$ is abelian. We note also that $AW Z \cap (BZ) \geq AW \cap B'$.

Subcase IIa ($AW \cap B' \leq Z$). Then $|(BZ/Z)| < |B'|$, so by induction $cl([A, B]/Z) \leq 2(n - 1) + 1$, and $cl([A, B]) \leq 2n$.

Subcase IIb ($AW \cap B' \leq Z$). Then the factorisation $G/Z = AWZ/Z邹BZ/Z$ satisfies the assumption of Case I, so by that case $cl([A, B]/Z) \leq 2n$, and $cl([A, B]) \leq 2n + 1$.

Proof of Corollary 6. We choose $C$ so that $2\log_2(k + 2) + 3 \leq ek + C$ holds for all $k$. If $A$ is abelian the result follows from Corollary 5. For non-abelian $A$ we repeat Kazarin's construction. Let $H = \langle A', B \rangle$. Then $H = A_1B, A_1 = H \cap A$. Here $A_1 \geq A'$, so $A_1 \triangleleft A$, and $N = A_1G = A_1H$, so $N = A_1B_1, B_1 = N \cap B$. Let $|(B/B_1)| = p^k$. Suppose first that $A_1' \neq A'$. Then by induction $dl(N) \leq mC + \epsilon(n - k)$, while $dl(G/N) \leq ek + C$ by Corollary 5 and the choice of $C$, so our claim follows. Finally, if $A_1' = A'$ then $H = \langle A', B \rangle = \langle H', B \rangle = B$, so $A' \leq B$ and $A'G = A'B \leq B$, so writing now $|(B/A')| = p^k$ we have $dl(G) \leq \log_2(n - k + 2) + ek + C \leq \epsilon n + 2C \leq \epsilon n + (m + 1)C$, by the choice of $C$ and the assumption $m \geq 1$.

References


