DERIVED SUBGROUPS AND CENTERS OF CAPABLE GROUPS

I. M. ISAACS

(Communicated by Stephen D. Smith)

Abstract. A group $G$ is said to be capable if it is isomorphic to the central factor group $H/\mathbf{Z}(H)$ for some group $H$. It is shown in this paper that if $G$ is finite and capable, then the index of the center $\mathbf{Z}(G)$ in $G$ is bounded above by some function of the order of the derived subgroup $G'$. If $G'$ is cyclic and its elements of order 4 are central, then, in fact, $|G: \mathbf{Z}(G)| \leq |G'|^2$.

1. Introduction

Recall that a group $G$ is said to be capable if there exists some group $H$ such that $H/\mathbf{Z}(H)$ is isomorphic to $G$. Of course, there are groups that are not capable (nontrivial cyclic groups, for example), and so the condition that a group is capable imposes certain restrictions on its structure. It is known, for example, that if $G$ is a finite capable $p$-group with $|G'| = p$, then $|G: \mathbf{Z}(G)| = p^2$. (I would like to thank A. Mann for informing me of this result, a special case of which appears in [1].)

As extraspecial $p$-groups show, there is no general upper bound on the index of the center of a finite group in terms of the order of its derived subgroup. In this paper, we prove that there is such a bound for all capable groups.

Theorem A. There exists a function $B(n)$ defined on the natural numbers such that if $G$ is finite and capable, then $|G: \mathbf{Z}(G)| \leq B(|G'|)$.

As an immediate consequence, we have the following general result. (Recall that the second center of a group $G$ is the preimage in $G$ of $\mathbf{Z}(G/\mathbf{Z}(G))$.)

Corollary B. Let $G$ be an arbitrary finite group. Then the index of the second center of $G$ is bounded above by some function of $|G'|$.

Proof. The group $G/\mathbf{Z}(G)$ is capable, and $|(G/\mathbf{Z}(G))'| \leq |G'|$. The result follows by applying Theorem A to $G/\mathbf{Z}(G)$. \qed

We shall not attempt to find the optimal function $B(n)$ in Theorem A, but in the special case where $G'$ is cyclic and all elements of order 4 in $G'$ are central, we obtain the best possible bound.

Received by the editors December 20, 1999 and, in revised form, February 22, 2000.

2000 Mathematics Subject Classification. Primary 20D99.

This paper was written with the partial support of the U.S. National Security Agency.

©2001 American Mathematical Society

2853
Theorem C. Let $G$ be finite and capable, and suppose that $G'$ is cyclic and that all elements of order 4 in $G'$ are central in $G$. Then $|G : Z(G)| \leq |G'|^2$, and equality holds if $G$ is nilpotent.

Unfortunately, we have been unable to decide whether or not the assumption about elements of order 4 in Theorem C is really necessary.

We mention that we are aware of two other related papers in the literature. In [3], H. Heineken considers capable groups $G$ for which $G'$ is central and elementary abelian of order $p^n$, where $p$ is a prime number. In Proposition 3, he shows that if $n = 2$, then $|G : Z(G)| \leq p^5$. Heineken also asserts that for arbitrary $n$, if $p > 2$, then there exist examples where $|G : Z(G)| = p^m$, where $m = 2n + \binom{n}{2}$. In [4], Heineken and D. Nikolova show that under certain very restrictive additional conditions, the index $|G : Z(G)|$ cannot exceed $p^m$, where $m = 2n + \binom{n}{2}$. (In order to obtain this bound, the authors assume that $G$ has exponent $p$ and that $G' = Z(G)$.)

I would like to thank A. Moreto for informing me of the existence of the papers [2] and [3], and for a number of helpful conversations on the subject of this paper. It was the referee who told me about [4], and I thank him too.

2. The general case

In this section, we work toward a proof of Theorem A. We begin with a couple of preliminary lemmas, which must surely be known. We thank D. S. Passman for helping us to find a proof of the first of these results.

(2.1) Lemma. Let $G$ be a finite capable group. Then there is a finite group $H$ such that $H/Z(H) \cong G$.

Proof. Since $G$ is capable, there is by definition a possibly infinite group $H$ such that $H/Z \cong G$, where $Z = Z(H)$. By choosing one element in each of the finitely many cosets of $Z$ in $H$, we can produce a finitely generated subgroup $K$ of $H$ such that $H = ZK$. Then $Z(K) \subseteq Z(H) = Z$, and so $Z(K) = K \cap Z$. It follows that $K/Z(K) = K/(K \cap Z) \cong ZK/Z = H/Z \cong G$, and we can therefore replace $H$ by $K$ and assume that $H$ is finitely generated.

Now $|H : Z| < \infty$, and hence by Schreier’s theorem, the abelian group $Z$ is finitely generated, and thus we can write $Z = T \times F$, where $T$ is finite and $F$ is torsion free. Certainly $Z/F \subseteq Z(H/F)$, and we claim that equality holds here. To see this, let $h \in H$ be central modulo $F$, so that $[H, h] \subseteq F$, and in particular $[H, h]$ is central in $H$. It follows that the map $x \mapsto [x, h]$ defines a homomorphism from $H$ into $F$. Since $Z$ is in the kernel of this homomorphism and $H/Z$ is finite, we see that $[H, h]$ is a finite subgroup of $F$. But $F$ is torsion free, and thus $[H, h] = 1$ and $h \in Z$.

Now $H/F$ is a finite group, and we have $(H/F)/Z(H/F) = (H/F)/(Z/F) \cong H/Z \cong G$. This completes the proof.

(2.2) Lemma. Let $A \subseteq G$, where $A$ is abelian, and suppose that $|G : A| = m < \infty$ and that $|G'| = n < \infty$. Then

$$|G : Z(G)| \leq m^{1+\log(n)},$$

where the logarithm is to the base 2.
Proof. First, we argue that we can choose a subset $X \subseteq G$ such that $G = \langle X, A \rangle$ and $|X| \leq \log(m)$. To prove this, write $A_0 = A$ and recursively construct subgroups $A_i$ such that $A_i = \langle A_{i-1}, x_i \rangle$, where $x_i$ is chosen arbitrarily in $G - A_{i-1}$ as long as $A_{i-1} < G$. We thus have $A = A_0 < A_1 < \cdots < A_r = G$ for some integer $r \leq \log(|G : A|) = \log(m)$. The set $X = \{x_i \mid 1 \leq i \leq r\}$ has the desired properties.

Each conjugacy class of $G$ is contained in some coset of $G'$ in $G$, and thus each of the classes of $G$ has cardinality no larger than $|G'|$. It follows that $|G : C_G(x)| \leq |G'|$ for each element $x \in G$, and thus $|G : C_G(X)| \leq |G'|^{|X|}$. Since $A$ is abelian and $G = \langle A, X \rangle$, we see that $A \cap C_G(X) \subseteq Z(G)$, and thus

$$ |G : Z(G)| \leq |G : A||A : A \cap C_G(X)| \leq |G : A||G : C_G(X)| \leq |G : A||G'|^{1+|X|} \leq mn^{\log(m)} = mn^{\log(n)}, $$

and the result follows. \hfill \Box

Of course, if we know the smallest prime divisor $p$ of $m = |G : A|$ in the situation of Lemma 2.2, we can work with logarithms to the base $p$, and thereby obtain a better bound.

Every group with trivial center is clearly capable, and our next result establishes Theorem A for such groups.

(2.3) Theorem. There is a function $F(n)$ defined on the natural numbers such that if $Z(G) = 1$ and $|G'| = n < \infty$, then $|G| \leq F(n)$.

Proof. Let $C = C_G(G')$, and write $m = |G : C|$, so that $m$ is bounded above by some function of $n$. (For example, since $G/C$ is isomorphically embedded in $\text{Aut}(G')$, it follows that $m \leq n!$.) We have $|G : C| \leq G'$, and thus $|G, C, C| = 1$. We conclude by the three subgroups lemma that $C'$ centralizes $G$, and since we are assuming that $Z(G) = 1$, we see that $C' = 1$ and $C$ is abelian.

We can now apply Lemma 2.2 to the abelian subgroup $C \subseteq G$ of index $m$, and we conclude that $|G| = |G : Z(G)| \leq m^{1+\log(n)}$. The result follows since $m$ is bounded in terms of $n$. \hfill \Box

We mention that a bound significantly better than the inequality $m \leq n!$ is available in the situation of Theorem 2.3. If we argue as in the proof of Lemma 2.2, we can find a generating set $X$ for $G'$ with $|X| \leq \log(n)$, where $n = |G'|$. Then $C = C_G(G') = C_G(X)$, and it follows that $m = |G : C| \leq |G'|^{1+|X|} \leq n^{\log(n)}$. (A version of this easy argument goes back at least as far as 1939, where it appears in the proof of statement (35) of the paper [3], by H. Wielandt.)

Before we begin the proof of Theorem A, we recursively define the relevant function $B(n)$. We start by setting $B(1) = 1$, and we assume that we have fixed some particular bounding function $F(n)$ as in Theorem 2.3. (We assume, as we may, that $F(1) = 1$ and that $F$ is monotonically increasing.) If $n > 1$, we let $M$ be the maximum of the quantities $B(n/q)$, where $q$ runs over prime divisors of $n$, and we set

$$ B(n) = \max\{F(n), (nM)^{1+\log(n)}\}. $$

It is easy to see that with this definition, we have $B(m) \leq B(n)$ whenever $m$ divides $n$, and of course, $F(n) \leq B(n)$ for all $n$. 

---

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
Proof of Theorem A. We are given a finite capable group \( G = H/Z \), where \( Z = \mathbb{Z}(H) \). Write \( U = H'Z \) and let \( n = |G'| = |U/Z| \). By Lemma 2.1, we can assume that \( H \) is finite, and we show that \( |G : \mathbb{Z}(G)| \leq B(n) \) by induction on \( |H| \). (Note that if \( H = 1 \), then \( G = 1 \) and the inequality is trivially true.)

If \( Z = 1 \), then \( H = G \), and by Lemma 2.3, we have \( |G : \mathbb{Z}(G)| = |G| \leq B(n) \). There is nothing further to prove in this case, and so we assume that \( Z > 1 \), and we choose a subgroup \( T \subseteq Z \) of prime order \( p \). Let \( Y/T = \mathbb{Z}(H/T) \), and note that \( Y \supseteq Z \) and \( H/Y \cong (H/T)/\mathbb{Z}(H/T) \) is capable.

Suppose first that \( Y \cap U = Z \). Let \( A/Y = \mathbb{Z}(H/Y) \) and note that \( UY/Y = (H/Y)' \), and this subgroup has order \( n \). Since \( |H/T| < |H| \), we can apply the inductive hypothesis to deduce that \( |H : A| \leq B(n) \). But \( [H, A] \subseteq Y \cap H' \subseteq Y \cap U = Z \), and thus \( A/Z \subseteq \mathbb{Z}(H/Z) \). This shows that \( |G : \mathbb{Z}(G)| \leq |H : A| \leq B(n) \), as desired.

We can now assume that \( Y \cap U > Z \). Let \( y \) be an element of \( Y \cap U \) that does not lie in \( Z \) and set \( C = C_H(y) < H \). We have \( [H, Y] \subseteq T \subseteq Z \), and thus the map \( h \mapsto [h, y] \) defines a homomorphism from \( H \) into \( T \) with kernel \( C \), and we see that \( C \triangleleft H \) and \( [H : C] \) divides \( |T| = p \). It follows that \( [H : C] = p \) and also, since \( H/C \) is abelian, we have \( U \subseteq C \). Because \( [H, Y] \subseteq Z \), we also have \( 1 = [h, y]^p = [h, y]^p \) for all elements \( h \in H \). We deduce that \( y^p \in Z \), and thus \( y \) has order \( p \) modulo \( Z \).

Let \( X = \mathbb{Z}(C) \) and observe that \( y \in X \cap U \), and hence \( |X \cap U : Z| \) is divisible by \( p \) and \( [U : X \cap U] \) is a divisor of \( |U : Z| = n/p \). Now \( (H/X)' = UX/X \cong U/(X \cap U) \), and thus \( |(H/X)'| \) divides \( n/p \). It follows that \( C/X \) is a capable group whose derived subgroup has order dividing \( |(H/X)'| \), which in turn divides \( n/p \).

Write \( V/X = \mathbb{Z}(C/X) \). Since \( C < H \), the inductive hypothesis applies, and we conclude that \( |C : V| \leq B(|(C/X)'|) \leq B(n/p) \). Now let \( h \in H - C \) and write \( S/X = C_{V/X}(h) \). Since \( H/C \) has prime order, we see that \( h \) generates \( H \) modulo \( C \), and thus \( S/X \subseteq \mathbb{Z}(H/X) \). But \( |(H/X)'| \leq n/p \), and thus \( |(H/X) : C_{H/X}(h)| \leq n/p \), and we have \( |V : S| \leq n/p \). Now \( |H : C| = p \) and \( |C : V| \leq B(n/p) \), and so we see that \( |H : S| \leq nB(n/p) \). In particular, \( |H : S| \leq nM \), since \( M \) is the maximum value of \( B(n/q) \), as \( q \) runs over all prime divisors of \( n \).

Since \( S/X \subseteq \mathbb{Z}(H/X) \), we have \( [H, S] \subseteq X \). But \( S \subseteq C \) and \( X = \mathbb{Z}(C) \), and so \( [H, S, S] \subseteq [X, C] = 1 \), and thus we see by the three subgroups lemma that \( S' \) centralizes \( H \). We conclude that \( S' \subseteq Z \), and thus \( S/Z \) is abelian. Since \( |H : S| \leq nM \) and \( |(H/Z)'| = n \), Lemma 2.2 yields that \( |G : \mathbb{Z}(G)| = |(H/Z) : \mathbb{Z}(H/Z)| \leq (nM)^{1 + \log(n)} \). In particular, \( |G : \mathbb{Z}(G)| \leq B(n) \), as required.

3. Cyclic derived subgroups

We begin toward a proof of Theorem C by studying groups that are not necessarily capable, but which have a cyclic derived subgroup.

(3.1) Lemma. Let \( G \) be finite and assume that \( G' \) is a cyclic \( p \)-group for some prime \( p \). If \( G' \cap \mathbb{Z}(G) \) is nontrivial, then \( G \) has a normal \( p \)-complement.

Proof. Let \( P \in \text{Syl}_p(G) \). Then \( G' \subseteq P \), and so \( P \triangleleft G \) and \( G \) has a \( p \)-complement \( H \). By Fitting’s lemma, we can write \( G' = C_{G'}(H) \times [G', H] \), and we observe that the first factor is nontrivial since we are assuming that \( G' \cap \mathbb{Z}(G) > 1 \). Since the cyclic \( p \)-group \( G' \) is indecomposable, we conclude that \( [G', H] = 1 \), and thus \( [P, H] = [P, H, H] = 1 \), where the first equality follows because \( |[H], [P]| = 1 \). We conclude that \( P \) normalizes \( H \), and thus \( H \triangleleft G \), as required.
(3.2) Theorem. Let $G$ be finite and assume that $G'$ is cyclic. Let $\pi$ be the set of prime divisors of $|G' \cap Z(G)|$ and let $b$ be the $\pi'$-part of $|G'|$. Then:

(a) $G$ has a normal $\pi$-complement $M$ and $G/M$ is nilpotent.
(b) $|M : M \cap Z(G)|$ divides $\varphi(b)$, where $\varphi$ is Euler’s function.
(c) $|G : Z(G)|$ divides $\varphi(b)|G : V|$, where $V/M = Z(G/M)$.

Proof. Let $p \in \pi$ and note that since $G'$ is cyclic, the derived subgroup of $G/O_{p'}(G)$ is a cyclic $p$-group. Also, since $G' \cap Z(G) \not\subseteq O_{p'}(G)$ by the definition of the set $\pi$, we conclude that the group $G/O_{p'}(G)$ satisfies the hypotheses of Lemma 3.1, and hence it has a normal $p$-complement. It follows that $G$ has a normal $p$-complement, and since this is true for every prime $p \in \pi$, we see that $G$ has a normal $\pi$-complement $M$ and that $G/M$ is nilpotent. This proves (a).

Now let $B = M \triangleleft G'$ and write $C = C_M(B)$. Since $B$ is cyclic of order $b$ and $B \triangleleft G$, we see that $|M : C|$ divides $\varphi(b)$, and thus to prove (b), it suffices to show that $|C : C \cap Z(G)|$ divides $b$.

Since $C \triangleleft G$, we have $[G, C] \subseteq C \cap G' \subseteq M \cap G' = B$, and thus $[G, C, C] \subseteq [B, C] = 1$. By the three subgroups lemma, it follows that $[C', G] = 1$, and thus $C' \subseteq G' \cap Z(G)$. But $C$ is a $\pi'$-group, and by the definition of $\pi$ it follows that no prime divisor of $|C|$ divides the order of $G' \cap Z(G)$. We conclude that $C' = 1$ and $C$ is abelian.

Now let $Q \in \text{Syl}_p(C)$, where $p$ is an arbitrary prime in $\pi'$, and note that $Q \triangleleft G$ since $C$ is abelian and $C \triangleleft G$. Since $q \in \pi'$ is arbitrary, we see that to establish that $|C : C \cap Z(G)|$ divides $b$, as claimed, it suffices to show that the $q$-part of this index divides $b$, or equivalently, that $|Q : Q \cap Z(G)|$ divides $b$.

Now, $[G, M] \subseteq B \subseteq C$, and thus $M/C \subseteq Z(G/C)$. Since $G/M$ is nilpotent, it follows that $G/C$ is nilpotent, and we let $K/C$ be the normal $q$-complement of $G/C$. Now $K$ acts on $Q$, and we prove next that $C_Q(K) \subseteq Z(G)$. To this end, we let $L = [C_Q(K), G]$ and we note that $L \subseteq G'$ and also $L \subseteq C_Q(K)$ since $C_Q(K) \triangleleft G$. Since $K$ centralizes $L$ and $L \triangleleft G$, we see that the $q$-group $G/K$ acts on the $q$-group $L$, and thus if $L > 1$, we have $1 < C_L(G) \subseteq G' \cap Z(G)$. This is a contradiction since $q \not\in \pi$, and it follows that $L = 1$, and thus $C_Q(K) \subseteq Z(G)$, as claimed, and thus, in fact, $C_Q(K) = Q \cap Z(G)$.

Since $Q \subseteq C$ and $C$ is abelian, the $q'$-group $K/C$ acts on $Q$, and hence we have $Q = [Q, K] \times C_Q(K)$ by Fitting’s lemma. We have established that $C_Q(K) = Q \cap Z(G)$, and therefore $|Q : Q \cap Z(G)| = |Q, K|$, and this divides $b$ since $[Q, K] \subseteq B$. This shows that $|C : C \cap Z(G)|$ divides $b$, as claimed, and the proof of (b) is complete.

Finally, to prove (c), we let $V/M = Z(G/M)$ and $W = C_V(B)$. (Note that $Z(G) \subseteq W$ and that $W \cap M = C$.) Since $B$ is cyclic of order $b$, we see that $|V : W|$ divides $\varphi(b)$, and thus $|G : W|$ divides $|G : V|\varphi(b)$. It suffices, therefore, to show that $|W : Z(G)|$ divides $b$.

First, we prove that a Hall $\pi$-subgroup $H$ of $W$ is central in $G$ by showing separately that $H$ centralizes the Hall $\pi'$-subgroup $M$ of $G$ and that it centralizes a Hall $\pi$-subgroup $S$ of $G$, where $S$ is chosen to contain $H$. We have $[M, H] \subseteq M \cap G' = B$, and thus $[M, H] = [M, H, H] \subseteq [B, H] = 1$, as desired, where the last equality follows since $H \subseteq W = C_V(B)$. Also, $[H, G] \subseteq M$ since $H \subseteq V$, and thus since $H \subseteq S$, we have $[H, S] \subseteq M \cap S = 1$. This shows that $H \subseteq Z(G)$, as claimed, and thus $|W : Z(G)|$ is a $\pi'$-number. We now have $W = (W \cap M)Z(G) = CZ(G)$,
and thus \( |W : Z(G)| = |C : C \cap Z(G)| \), which, as we have seen, is a divisor of \( b \). This completes the proof.

Next, we quote a known result.

(3.3) Lemma. Let \( \sigma \in \text{Aut}(G) \) and assume that \( \sigma \) fixes all elements of prime order and of order 4 in \( [G, \sigma] \). Then \( [G, \sigma] \) has exponent dividing the order \( o(\sigma) \).

Proof. This is Theorem A(c) of [5].

Somewhat surprisingly, we need the following result, which establishes a lower bound on the index of the center of our group. We remark that if \( G \) is a \( p \)-group and \( G' \) is cyclic, then a generator of \( G' \) must actually be a commutator in \( G \). The same conclusion therefore holds for finite nilpotent groups with cyclic derived subgroups. (One can work with one Sylow subgroup at a time.)

(3.4) Lemma. Let \( G \) be nilpotent and assume that \( G' \) is cyclic and that all elements of order 4 in \( G' \) are central in \( G \). Then \( |G : Z(G)| \geq |G'|^2 \).

Proof. As we remarked, some generator of \( G' \) must be a commutator, and thus we can choose elements \( a \) and \( b \) in \( G \) such that \( \langle a, b \rangle = G' \), and we see that \( X' = G' \), where \( X = \langle a, b \rangle \). Since \( |X : Z(X)| \leq |G : Z(G)| \), it is no loss to assume that \( G = X \), and thus we have \( G = \langle a, b \rangle \). Write \( Z = Z(G) \) and let \( A = \langle Z, a \rangle \) and \( B = \langle Z, b \rangle \). Then both \( A \) and \( B \) are abelian, and since \( G = \langle A, B \rangle \), we see that \( A \cap B = Z \).

Consider the inner automorphism \( \sigma \) of \( G \) induced by \( a \), and note that the order of \( \sigma \) is exactly \( |\langle a \rangle : \langle a \rangle \cap Z| = |A : Z| \). Since \( [G, \sigma] = G' \) is cyclic, every subgroup of prime order in \( [G, \sigma] \) is normal, and hence is central in \( G \) since \( G \) is nilpotent. Thus \( \sigma \) fixes all elements of prime order in \( [G, \sigma] \) and also, by hypothesis, \( \sigma \) fixes all elements of order 4 in \( [G, \sigma] \). Thus Lemma 3.3 applies, and so \( |A : Z| = o(\sigma) \) is a multiple of the exponent of \( [G, \sigma] \). Since \( [G, \sigma] = G' \) is cyclic, its exponent is equal to its order, and we have \( |A : Z| \geq |G'| \). Similarly, \( |B : Z| \geq |G'| \), and thus \( |G : Z| \geq |AB|/|Z| = |A : Z||B : Z| \geq |G'|^2 \), as desired.

The following result is very closely related to Theorem 1 of [2].

(3.5) Lemma. Let \( G \) be nilpotent and assume that \( G' \) is cyclic and that all elements of order 4 in \( G' \) are central in \( G \). Then there exist subgroups \( X \) and \( Y \) of \( G \) such that \( XY = G \), \( X' = G' \), \( [X, Y] = 1 \) and \( |G : Y| = |G'|^2 \).

Proof. Since \( G \) is nilpotent, we can find (as in the previous proof) a two-generator subgroup \( X = \langle a, b \rangle \) of \( G \) such that \( X' = G' \). Let \( Y = C_G(X) \). By Lemma 3.4, we see that \( |G : Y| \geq |X : X \cap Y| = |X : Z(X)| \geq |X'|^2 = |G'|^2 \). But \( Y = C_G(a) \cap C_G(b) \), and so \( |G : Y| \leq |G : C_G(a)||G : C_G(b)| = |\text{cl}(a)||\text{cl}(b)| \leq |G'|^2 \). It follows that we have equality throughout, and thus in particular, we see that \( |G'|^2 = |G : Y| = |X : X \cap Y| \), and it follows that \( XY = G \), as required.

Proof of Theorem C. It suffices to prove the inequality in the statement of the theorem; the fact that equality must hold if \( G \) is nilpotent will then follow via Lemma 3.4.

Since \( G \) is capable, we can assume that \( G = H/Z \), where \( H \) is some finite group and \( Z = Z(H) \). We wish to apply Theorem 3.2 to \( G \), and so as in that theorem, we let \( \pi \) be the set of prime divisors of \( |G' \cap Z(G)| \). Then \( H/Z \) has a normal \( \pi \)-complement \( M/Z \), and we let \( V/M = Z(H/M) \). By Theorem 3.2(c), we know that
\[ G : \mathbb{Z}(G) \] divides \( b_\varphi(b) | H : V, \) where \( b \) is the \( \pi' \)-part of \( |G'|. \) Since \( b_\varphi(b) \leq b^2, \) we see that it suffices to show that \( |H : V| \) is at most equal to the \( \pi' \)-part of \( |G'|^2. \)

Let \( K/Z \) be a Hall \( \pi \)-subgroup of \( H/Z. \) Then \( K/Z \cong H/M \) and it suffices to prove that \( |K/Z : Z(K/Z)| \leq |(K/Z)|^2. \) By Theorem 3.2(a), we know that \( K/Z \) is nilpotent, and thus by Lemma 3.5, there exist subgroups \( X \) and \( Y \) of \( K, \) each of them containing \( Z, \) and such that \( XY = K \) and \( [X,Y] \subseteq Z. \) Also \( (X/Z)' = (K/Z)' \) and \( |K : Y| = |(K/Z)'|^2. \)

If \( Y/Z \) is abelian, then since \( Y/Z \) centralizes \( X/Z, \) we see that \( Y/Z \subseteq Z(K/Z), \) and thus \( |K/Z : Z(K/Z)| \leq |K : Y| = |(K/Z)'|^2, \) as required. It suffices to show, therefore, that \( Y' \subseteq Z. \)

Since \( [X,Y] \subseteq Z, \) we have \( [X,Y,X] = 1, \) and thus by the three subgroups lemma, \( X' \) centralizes \( Y, \) and similarly \( Y' \) centralizes \( X. \) Since \( (X/Z)' = (K/Z)' \), we see that \( X'Z = K'Z, \) and it follows that \( K' \) centralizes \( Y. \) But \( Y' \subseteq K', \) and thus \( Y' \) centralizes both \( X \) and \( Y, \) and thus \( Y' \subseteq Z(K) \) since \( K = XY. \)

Recall that our goal is to show that \( Y' \subseteq Z. \) Since we now know that \( Y' \) centralizes \( K, \) it suffices to show that \( Y' \) also centralizes \( M. \) Now \( Y'Z/Z \subseteq (H/Z)', \) which is cyclic, and thus \( Y'Z \triangleleft H \) and of course, \( Y'Z/Z \) is a \( \pi \)-subgroup of \( H/Z. \) Thus \( Y'Z/Z \) and \( M/Z \) are normal subgroups of coprime orders in \( H/Z, \) and it follows that \( [M,Y'Z] \subseteq Z. \) If \( m \in M, \) it follows that the map \( y \mapsto [m,y] \) is a homomorphism from \( Y'Z \) into \( Z, \) and \( Z \) is contained in the kernel of this map. Therefore \( |M,Y'Z| \) divides \( |Y'Z/Z|, \) and it follows that \( |M,Y'Z| \) is a \( \pi \)-group.

Also, we can interchange the roles of \( M \) and \( Y'Z \) in this argument, and we deduce that \( [M,Y'Z] \) is a \( \pi' \)-group. It follows that \( |M,Y'| = 1, \) and thus \( Y' \subseteq Z(MK) = Z(H) = Z, \) as desired. This completes the proof. \( \square \)

References


Department of Mathematics, University of Wisconsin, 480 Lincoln Drive, Madison, Wisconsin 53706

E-mail address: isaacs@math.wisc.edu