J. Austral. Math. Soc. **24** (Series A) (1977), 79–91.

COMMUTATORS AND ABELIAN GROUPS

D. M. RODNEY

(Received 11 December 1975; revised 21 April 1976)

Communicated by M. F. Newman

Abstract

If G is a group, then $\mathbf{K}(G)$ is the set of commutators of elements of G. $\mathbf{C}$ is the class of groups such that $G' = \mathbf{K}(G)$ and $d(G)$ is the minimal cardinality of any generating set of G. We prove:

THEOREM A. *Let G be a nilpotent group of class two such that G' is finite and $d(G') < 4$. Then $G \in \mathbf{C}$.*

THEOREM B. *Let G be a finite group such that G' is elementary abelian of order p^3. Then $G \in \mathbf{C}$.*

THEOREM C. *Let G be a finite group with an elementary abelian Sylow p-subgroup S, of order p^2, such that $S \subseteq G'$. Then $\mathbf{S} \subseteq \mathbf{K}(G)$.*

1. Preliminaries

Macdonald (1963) and the author (1974) have investigated groups with a cyclic derived subgroup in order to determine which elements of the derived subgroup may or may not be commutators. In this paper we extend our interest to metabelian groups and abelian subgroups of the derived subgroup. Here the situation is much more complicated. Consequently the results obtained are very restricted and are mostly concerned with finite groups.

If G is a group, then $\mathbf{K}(G)$ is the set of commutators of elements of G, $\mathbf{C}$ is the class of groups such that $G' = \mathbf{K}(G)$ and $d(G)$ is the minimal cardinality of any generating set of G.

Let $STL(n, p)$ denote the group of all upper unipotent matrices of degree n over the field of p elements. We prove:

THEOREM A. *Let G be a nilpotent group of class two such that G' is finite and $d(G') < 4$. Then $G \in \mathbf{C}$.*

THEOREM B. *Let G be a finite group such that G' is elementary abelian of order p^3. Then $G \in \mathbf{C}$.*

THEOREM C. *Let G be a finite group with an elementary abelian Sylow p-subgroup S, of order p^2, such that $S \subseteq G'$. Then $S \subseteq \mathbf{K}(G)$.*

We will frequently refer to the following results.

THEOREM 1.1 (D. Gorenstein (1968), Theorem 5.2.3). *Let A be a p'-group of automorphisms of the finite abelian p-group P. Then $P = C_P(A) \times [P, A]$.*

THEOREM 1.2 (D. Gorenstein (1968), Theorem 5.3.5). *If A is a p'-group of automorphisms of the finite p-group P, then $P = C_P(A)[A, P]$.*

THEOREM 1.3 (D. Gorenstein (1968), Theorem 5.3.6). *If A is a p'-group of automorphisms of the finite p-group P, then $[P, A, A] = [P, A]$. In particular, if $[P, A, A] = \langle 1 \rangle$, then $A = \langle 1 \rangle$.*

2. Theorem A

PROOF OF THEOREM A. By an argument of Macdonald (1963), it suffices to assume that G is finite. Now G is finite nilpotent if and only if G is the direct product of its Sylow subgroups. Thus it suffices to consider G as a finite p-group.

Let $G = \langle a_i \mid 1 \leqq i \leqq n \rangle$. If $c_{ij} = [a_i, a_j]$, then, because G' is an abelian p-group, we can select a minimal generating set from the c_{ij}'s.

There are eight possible configurations that may arise:

(1) $G' = \langle c_{12} \rangle$; (2) $G' = \langle c_{12}, c_{13} \rangle$;
(3) $G' = \langle c_{12}, c_{34} \rangle$; (4) $G' = \langle c_{12}, c_{13}, c_{14} \rangle$;
(5) $G' = \langle c_{12}, c_{13}, c_{23} \rangle$; (6) $G' = \langle c_{12}, c_{34}, c_{13} \rangle$;
(7) $G' = \langle c_{12}, c_{34}, c_{15} \rangle$; (8) $G' = \langle c_{12}, c_{34}, c_{56} \rangle$.

We consider the first three cases.

Case 1. Because G is nilpotent of class two we have that $c_{12}^{\alpha} = [a_1, a_2^{\alpha}]$, for all integers α.

Case 2. Here we have $c_{12}^{\alpha} c_{13}^{\beta} = [a_1, a_2^{\alpha} a_3^{\beta}]$ for all integers α and β.

Case 3. Let $c_{ij} = c_{12}^{\alpha_{ij}} c_{34}^{\beta_{ij}}$ for $(i, j) \in \{(1,3), (1,4), (2,3), (2,4)\}$. If $\alpha_{ij} \not\equiv 0 \,(\text{modulo}\, p)$, then there exists an integer ω such that

$$c_{ij} = c_{12}^{\alpha_{ij}\omega} c_{34}^{\beta_{ij}\omega} \quad \text{and} \quad \alpha_{ij}\omega \equiv 1 \,(\text{modulo} \mid c_{12} \mid).$$

https://doi.org/10.1017/S1446788700020073 Published online by Cambridge University Press

Consequently, $G' = \langle c_{ij}, c_{34}\rangle$, which is a presentation of the form discussed in Case (2).

Similarly, if $\beta_{ij} \not\equiv 0\,(\text{modulo}\, p)$, we are reduced to Case (2). So we may assume that $\alpha_{ij} \equiv \beta_{ij} \equiv 0\,(\text{modulo}\, p)$ for $(i,j) \in \{(1,3),(1,4),(2,3),(2,4)\}$.

We consider

$$\begin{aligned}[a_1 a_3, a_2^{\alpha} a_4^{\beta}] &= c_{12}^{\alpha} c_{14}^{\beta} c_{23}^{-\alpha} c_{34}^{\beta} \\ &= c_{12}^{\alpha(1-\alpha_{23})+\beta\alpha_{14}} c_{34}^{-\alpha\beta_{23}+\beta(1+\beta_{14})}.\end{aligned}$$

Let $p^m = \max(|c_{12}|, |c_{34}|)$.

Then for any integers r and s, $c_{12}^r c_{34}^s \in \mathbf{K}(G)$ if there exist solutions to the equations

$$\begin{aligned}(1-\alpha_{23})\alpha + \alpha_{14}\beta &\equiv r\,(\text{modulo}\, p^m) \\ -\beta_{23}\alpha + (1+\beta_{14})\beta &\equiv s\,(\text{modulo}\, p^m)\end{aligned} \tag{2.1}$$

Because $\alpha_{23} \equiv \beta_{23} \equiv \alpha_{14} \equiv \beta_{14} \equiv 0\,(\text{modulo}\, p)$ we have that

$$\begin{vmatrix} 1-\alpha_{23} & \alpha_{14} \\ -\beta_{23} & 1+\beta_{14} \end{vmatrix} \not\equiv 0\,(\text{modulo}\, p).$$

Therefore there exist solutions to the equations (2.1), completing the proof for Case (3).

The other cases follow in a similar fashion to complete the proof of the theorem.

We now give two examples of groups that demonstrate the fact that no generalization of Theorem A is readily apparent. Let

$$\begin{aligned}G_1 = \langle a_i \mid 1 \leqq i \leqq 4, a_i^2 = 1, [[a_i, a_j], a_k] = 1, \\ 1 \leqq i,j,k \leqq 4, [a_2, a_4] = [a_3, a_4] = 1\rangle\end{aligned}$$

and

$$\begin{aligned}G_2 = \langle a_i \mid 1 \leqq i \leqq 4, a_i^2 = 1, [[a_i, a_j], a_k] = 1, \\ 1 \leqq i,j,k \leqq 4, [a_1, a_2] = [a_3, a_4] = 1\rangle\end{aligned}$$

G_1 is a relatively well known example of a nilpotent group of class two, of order 256, such that $d(G_1') = 4$ and $G_1 \notin \mathbf{C}$ (c.f. R. Carmichael (1937), p. 39). In fact $[a_1, a_4][a_2, a_3] \notin \mathbf{K}(G_1)$. G_2 is also a nilpotent group of class two, of order 256, such that $d(G_2') = 4$, but one can easily demonstrate that $G_2 \in \mathbf{C}$.

https://doi.org/10.1017/S1446788700020073 Published online by Cambridge University Press

3. Theorem B

Theorem A is essentially a statement related to finite p-groups. By assuming that the groups concerned were nilpotent of class two we were able to deal with groups of arbitrary exponent.

In Theorem B we only assume the group to be metabelian such that the derived subgroup is a p-group. We are only able to handle the case where the derived subgroup is elementary abelian.

PROOF OF THEOREM B. Let S be a Sylow p-subgroup of G. Because $G' \subseteq S$ we have that $S \lhd G$. So, by the Schur–Zassenhaus Theorem (Gorenstein (1968), Theorem 6.2.1), $G = S \rtimes K$, where K is a complement to S in G. Again because $G' \subseteq S$, we have that K is abelian. By Theorem 1.1 we make the following crucial observation:

$$G' = [G', K] \times C_{G'}(K). \tag{3.1}$$

We continue by considering, in turn, the various possibilities arising from (3.1).

Case 1.

$$G' = [G', K]. \tag{3.2}$$

Let $G' = \langle a_1, a_2, a_3 \rangle$, where $a_i = [b_i, k_i]$, $b_i \in G'$, $k_i \in K$, for $1 \leqq i \leqq 3$. We may assume that $K = \langle k_1, k_2, k_3 \rangle$.

Suppose $C_{G'}(\langle k_1, k_2 \rangle) = \langle 1 \rangle$. Then, once again by Theorem 1.1, $G' = [G', \langle k_1, k_2 \rangle]$. Because K is abelian,

$$[G', \langle k_1, k_2 \rangle] = \langle [G', \langle k_1 \rangle], [G', \langle k_2 \rangle] \rangle.$$

Let $g \in G'$. Then $g = g_1 g_2$ for some $g_i \in [G', \langle k_i \rangle]$, $1 \leqq i \leqq 2$. If $h \in G'$, then

$$[h, k_i^2] = [h, k_i][h, k_i]^{k_i} = [h, k_i][h^{k_i}, k_i] = [hh^{k_i}, k_i], \quad 1 \leqq i \leqq 2.$$

Consequently, $g_i = [h_i, k_i]$, for some $h_i \in G'$, $1 \leqq i \leqq 2$. So, $g = g_1 g_2 = [h_1, k_1][h_2, k_2] = [k_1 h_2, k_2 h_1^{-1}]$, which implies that $G \in \mathbf{C}$.

We now consider the possibility that $C_{G'}(\langle k_1, k_2 \rangle) \neq \langle 1 \rangle$. By symmetry we may assume that

$$C_{G'}(\langle k_1, k_3 \rangle) \neq \langle 1 \rangle \neq C_{G'}(\langle k_2, k_3 \rangle).$$

If $C_{G'}(\langle k_r, k_s \rangle) \cap \langle C_{G'}(\langle k_r, k_t \rangle), C_{G'}(\langle k_s, k_t \rangle) \rangle \neq \langle 1 \rangle$, for $r, s, t \in \{1, 2, 3\}$ and r, s, t pairwise different, then $C_{G'}(\langle k_1, k_2, k_3 \rangle) = C_{G'}(K) \neq \langle 1 \rangle$. This is a contradiction because of (3.1) and (3.2). Consequently,

$$G' = C_{G'}(\langle k_1, k_2\rangle) \times C_{G'}(\langle k_1, k_3\rangle) \times C_{G'}(\langle k_2, k_3\rangle).$$

Let $C_{G'}(\langle k_1, k_2\rangle) = \langle g_1\rangle$, $C_{G'}(\langle k_1, k_3\rangle) = \langle g_2\rangle$ and $C_{G'}(\langle k_2, k_3\rangle) = \langle g_3\rangle$, where $\langle g_1\rangle \cong \langle g_2\rangle \cong \langle g_3\rangle \cong C_p$, the cyclic group of order p. Now $K \subseteq N_G(C_{G'}(\langle k_1, k_2\rangle))$, so $g_1^{k_3} = g_1^{r_1}$, for some $1 \leqq r_1 < p$. If $r_1 = 1$, then $\langle 1\rangle \neq \langle g_1\rangle \subseteq C_{G'}(\mathbf{K})$, a contradiction. So $r_1 \neq 1$. Similarly, $g_2^{k_2} = g_2^{r_2}$ and $g_3^{k_1} = g_3^{r_3}$, where $1 < r_2, r_3 < p$. Thus,

$$g_1^{r_1 - 1} = [g_1, k_3], \quad g_2^{r_2 - 1} = [g_2, k_2] \quad \text{and} \quad g_3^{r_3 - 1} = [g_3, k_1].$$

Now there exist $\lambda_i \in \mathbb{Z}$ such that $(r_i - 1)\lambda_i \equiv 1\ (\text{modulo}\ p)$ for $1 \leqq i \leqq 3$. Consequently, $g_1 = [g_1^{\lambda_1}, k_3]$, $g_2 = [g_2^{\lambda_2}, k_2]$ and $g_3 = [g_3^{\lambda_3}, k_1]$. Let $g \in G'$. Then, $g = g_1^{\alpha} g_2^{\beta} g_3^{\gamma}$, for some $\alpha, \beta, \gamma \in \mathbb{Z}$. We have

$$g = [g_1^{\lambda_1}, k_3]^{\alpha} [g_2^{\lambda_2}, k_2]^{\beta} [g_3^{\lambda_2}, k_1]^{\gamma} = [g_1^{\lambda_1\alpha} g_2^{\lambda_2\beta} g_3^{\lambda_3\gamma}, k_3 k_2 k_1],$$

completing the proof for Case (1).

Case 2.

$$G' = S' \cong C_p \times C_p \times C_p.$$

S induces a group of automorphisms on S', by conjugation. Let ϕ be the canonical homomorphism of S into $GL(3, p)$. Since S is a p-group we may consider $\phi(S) \subseteq STL(3, p)$ which is, by Dixon (1971), Theorem 1.4 A, a Sylow p-subgroup of $GL(3, p)$. Because S' is abelian, $\phi(S)$ is an abelian group. By Dixon (1971) Theorem 1.2 and Lemma 1.3, $STL(3, p)$ is nilpotent of class two and of order p^3. If $|\phi(S)| = 1$, then S centralizes S'. So S is nilpotent of class two and $d(S') = 3$. So, by Theorem A, $S \in \mathbf{C}$, which implies $G \in \mathbf{C}$. Therefore, either $|\phi(S)| = p$ or $|\phi(S)| = p^2$.

Let $S' = \langle g_1, g_2, g_3\rangle$, where we may assume that $g_i \in \mathbf{K}(G)$ for $1 \leqq i \leqq 3$. From Honda (1953), we see that it suffices to show that $g_1 g_2^{\alpha} g_3^{\beta} \in \mathbf{K}(G)$ and $g_2 g_3^{\beta} \in \mathbf{K}(G)$, where $\alpha, \beta \in \mathbb{Z}$. We consider the various possibilities for the structure of $\phi(S)$ in turn. Allowing for a suitable change of basis we have:

(i) $|\phi(S)| = p^2$.

So

$$\phi(S) = \left\langle \begin{pmatrix} 1 & \gamma & 0 \\ 0 & 1 & \delta \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\rangle \quad \text{where } \gamma, \delta \in \mathbb{Z}.$$

Various situations arise, depending on the values of γ, δ and p. Because $\mathbf{K}(G)$ is a characteristic subset of G it suffices to show that every element under consideration is conjugate to a commutator. Let $g \sim h$ denote that g is conjugate to h.

https://doi.org/10.1017/S1446788700020073 Published online by Cambridge University Press

(a) $\gamma \equiv 0 \,(\text{modulo}\, p)$. If $\delta \equiv 0 \,(\text{modulo}\, p)$, then $|\phi(S)| = p$. So $\delta \not\equiv 0(p)$. By considering how $\phi(S)$ acts upon S', we see that $g_1 \sim g_1 g_3$, $g_2 \sim g_2 g_3$ and $g_3 \in Z(S)$.

So S is nilpotent of class 3 and $S/\langle g_3\rangle$ is nilpotent of class 2. By Theorem A, $S/\langle g_3\rangle \in \mathbf{C}$. So $g_1 g_2^\alpha \langle g_3\rangle \in \mathbf{K}(S/\langle g_3\rangle)$ and consequently, $g_1 g_2^\alpha g_3^\lambda \in \mathbf{K}(S)$ for some $\lambda \in \mathbb{Z}$. Now $g_1 g_2^\alpha g_3^\lambda \sim g_1 g_2^\alpha g_3^\lambda g_3 \sim \cdots \sim g_1 g_2^\alpha g_3^{\lambda + r}$, where $r \in \mathbb{Z}$. So $g_1 g_2^\alpha g_3^\beta \in \mathbf{K}(S)$, where $\alpha, \beta \in \mathbb{Z}$. Now $g_2 \sim g_2 g_3^\delta \sim g_2 g_3^{2\delta} \sim \cdots \sim g_2 g_3^{r\delta}$, where $r \in \mathbb{Z}$. Since $\delta \not\equiv 0 \,(\text{modulo}\, p)$ we have that $g_2 g_3^\beta \in \mathbf{K}(S)$. Trivially, $g \in \mathbf{K}(S)$ implies $g \in \mathbf{K}(G)$.

(b) $\gamma \not\equiv 0$ (modulo p) and $p \neq 2$. Now

$$\begin{pmatrix} 1 & \gamma & 0 \\ 0 & 1 & \delta \\ 0 & 0 & 1 \end{pmatrix}^{r_1} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{r_2} = \begin{pmatrix} 1 & r_1\gamma & r_1(r_1 - 1)\gamma\delta/2 + r_2 \\ 0 & 1 & r_1\delta \\ 0 & 0 & 1 \end{pmatrix},$$

where $r_1, r_2 \in \mathbb{Z}$. By selecting suitable r_1 and r_2 we have $g_1 \sim g_1 g_2^\alpha g_3^\beta$, where $\alpha, \beta \in \mathbb{Z}$ and, consequently, $g_1 g_2^\alpha g_3^\beta \in \mathbf{K}(S)$.

To show that $g_2 g_3^\beta \in \mathbf{K}(S)$ we observe that there exists an $s \in S$, such that,

$$s^{-1} g_1 s = g_1 g_2 g_3^\beta \quad \text{and} \quad [g_1, s] = g_2 g_3^\beta.$$

(c) $p = 2$ and $\gamma \equiv 1 \,(\text{modulo}\, 2)$. Let $s_1, s_2 \in S$ be such that s_1 and s_2 induce the automorphisms given by

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & \delta \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{respectively.}$$

Then $g_1^{s_1} = g_1 g_2$, $g_1^{s_2} = g_1 g_3$, $g_1^{s_2 s_1} = g_1 g_2 g_3$ and $[g_1, s_2 s_1] = g_2 g_3$. Consequently, $S \in \mathbf{C}$, which implies $G \in \mathbf{C}$.

(ii) $|\phi(S)| = p$. There are two possibilities to consider

(a)
$$\phi(S) = \left\langle \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\rangle.$$

$S/\langle g_3\rangle$ is nilpotent of class two and by a similar argument to that used in (i) (a) we may conclude that $g_1 g_2^\alpha g_3^\beta \in \mathbf{K}(S)$, where $\alpha, \beta \in \mathbb{Z}$.

It remains to show that $g_2 g_3^\beta \in \mathbf{K}(S)$, where $\beta \in \mathbb{Z}$. Let $g_2 = [s_1, s_2]$ and $g_3 = [g_1, s_3]$ for some $s_1, s_2, s_3 \in S$. Now $[g_1, s] \in \langle g_3\rangle$ for all $s \in S$. So $[g_1, s_1] =$

g_3^λ for some $1 \leqq \lambda \leqq p$. If $\lambda \not\equiv 0 \pmod p$, then $[s_1, s_2 g_1^\mu] = g_2 g_3^{-\lambda\mu}$ and for a suitable choice of μ we have $-\lambda\mu \equiv \beta \pmod p$.

Thus it remains to consider the case $\lambda \equiv 0 \pmod p$. This means $[g_1, s_1] = 1$. Similarly we may assume $[g_1, s_2] = 1$. Since $g_1, [s_3, s_2], [s_3, s_1] \in S'$ which is abelian, we have $[s_3, s_2]^{g_1} = [s_3, s_2]$ and $[s_3, s_1]^{g_1} = [s_3, s_1]$. Let

$$[s_3, s_1] = g_1^{\omega_1} g_2^{\omega_2} g_3^{\omega_3} \quad \text{and} \quad [s_3, s_2] = g_1^{\omega_4} g_2^{\omega_5} g_3^{\omega_6}$$

where $\omega_i \in \mathbb{Z}$ for $1 \leqq i \leqq 6$.

We consider

$$g = [s_3 s_1^\zeta s_2^\mu, s_1^\gamma s_2^\delta g_1^\varepsilon], \quad \text{where } \zeta, \mu, \gamma, \delta, \varepsilon \in \mathbb{Z}.$$

Expanding the commutator gives

$$g = (g_1^{\omega_1} g_2^{\omega_2} g_3^{\omega_3})^\gamma (g_1^{\omega_4} g_2^{\omega_5} g_3^{\omega_6})^\delta g_3^{-\varepsilon} g_2^{\zeta\delta - \mu\gamma}.$$

We choose γ and δ such that $\omega_1\gamma + \omega_4\delta \equiv 0 \pmod p$ and, either $\gamma \not\equiv 0 \pmod p$ or $\delta \not\equiv 0 \pmod p$. We then choose ζ, μ and ε such that $g = g_2 g_3^\beta$.

(b) $$\phi(S) = \left\langle \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \right\rangle.$$

Let $g_1 = [s_1, s_2]$, where $s_1, s_2 \in S$. Suppose $g_1^{s_1} = g_1 g_2^\lambda$, where $\lambda \not\equiv 0 \pmod p$. Consequently, $g_2^{s_1} = g_2 g_3^\lambda$. So,

$$[s_1, s_2 g_1^\alpha g_2^\beta] = g_1 g_2^{-\alpha\lambda} g_3^{-\beta\lambda} \quad \text{and} \quad [s_1, g_1^\alpha g_2^\beta] = g_2^{-\alpha\lambda} g_3^{-\beta\lambda},$$

where $\alpha, \beta \in \mathbb{Z}$. In the second commutator we can choose α such that $\alpha\lambda \equiv -1 \pmod p$. Consequently, $S \in \mathbf{C}$.

Similarly, $g_1^{s_2} = g_1 g_2^\lambda$, where $\lambda \not\equiv 0 \pmod p$, implies that $S \in \mathbf{C}$.

So it only remains to consider the case $g_1^{s_1} = g_1^{s_2} = g_1$. Now there exists an $s \in S$ such that $g_1^s = g_1 g_2$ and $g_2^s = g_2 g_3$. Let $[s, s_2] = g_1^\gamma g_2^\delta g_3^\varepsilon$, where $\gamma, \delta, \varepsilon \in \mathbb{Z}$. Then,

$$[s s_1^{-\gamma+1}, s_2 g_1^\lambda g_2^\mu] = g_1 g_2^{\delta-\lambda} g_3^{\varepsilon-\mu}$$

and

$$[s s_1^{-\gamma}, s_2 g_1^\lambda g_2^\mu] = g_2^{\delta-\lambda} g_3^{\varepsilon-\mu}.$$

By suitably selecting λ and μ we see that $S \in \mathbf{C}$. This concludes the proof for Case (2).

Case 3.

$$[G', K] \neq G' \neq S'.$$

By Theorem 1.2 we have,

$$S = [S, K]C_S(K). \tag{3.3}$$

Now $K \subseteq N_G([S, K])$ and

$$[s_1, k]^{s_2} = [s_1 s_2, k][s_2, k]^{-1},$$

where $s_1, s_2 \in S$ and $k \in K$. Therefore,

$$[S, K] \lhd G. \tag{3.4}$$

By considering (3.3) and (3.4), remembering that G' is abelian, we see that

$$S' = \langle [[S, K], C_S(K)], C_S(K)' \rangle. \tag{3.5}$$

Because of (3.4) we have,

$$[[S, K], C_S(K)] \subseteq [S, K]. \tag{3.6}$$

By Theorem 1.3, $[S, K] = [[S, K], K]$. So,

$$[[S, K], C_S(K)] \subseteq [G', K]. \tag{3.7}$$

Noting that $C_S(K)' \subseteq C_{G'}(K)$ we have, by (3.5), (3.7) and (3.1),

$$S' = [[S, K], C_S(K)] \times C_S(K)'. \tag{3.8}$$

Again by Theorem 1.1,

$$S' = [S', K] \times C_{S'}(K). \tag{3.9}$$

Now,

$$C_S(K)' \subseteq C_{S'}(K) \subseteq C_{G'}(K), \quad [S', K] \subseteq [G', K]$$

and, by (3.6),

$$[[S, K], C_S(K)] \subseteq [G', K].$$

So, by (3.1),

$$C_S(K)' = C_{S'}(K). \tag{3.10}$$

If,

$$[[S, K], C_S(K)] \neq [S', K],$$

then there exist $x \in [[S, K], C_S(K)]$ and $y \in [S', K]$ such that $1 \neq xy \in C_{S'}(K)$. But

https://doi.org/10.1017/S1446788700020073 Published online by Cambridge University Press

$$\langle [[S,K],C_S(K)],[S',K]\rangle \subseteq [G',K]$$

and, by (3.1), $[G',K]\cap C_{G'}(K)=\langle 1\rangle$, a contradiction. Therefore,

$$[[S,K],C_S(K)]=[S',K]. \tag{3.11}$$

We consider the various possibilities for the structure of S'.

(i) $C_{S'}(K)\cong C_p$ and $[S',K]=\langle 1\rangle$. By (3.9),

$$S'\cong C_p. \tag{3.12}$$

Because $G=S\rtimes K$, $G'=\langle [S,K],S'\rangle$. Recalling that, by Theorem 1.3, $[S,K]=[[S,K],K]$, we see that

$$[S,K]=[G',K]\cong C_p\times C_p.$$

So, by (3.1),

$$C_{G'}(K)\cong C_p. \tag{3.13}$$

Let $g\in G'$. Then $g=g_1g_2$, where $g_1\in[G',K]$ and $g_2\in C_{G'}(K)$. By Theorem 1.3 we have $[G',K]=[[G',K],K]$. So

$$g_1=[s_1,k_1][s_2,k_2]=[k_2s_1,k_1s_2^{-1}],$$

where $k_1,k_2\in K$ and $s_1,s_2\in[G',K]$. By (3.10), (3.12) and (3.13), $C_{G'}(K)=C_{S'}(K)=C_S(K)'$. So $g_2=[s_3,s_4]$, where $s_3,s_4\in C_S(K)$. Consequently,

$$g=g_1g_2=[k_2s_1s_3,k_1s_2^{-1}s_4].$$

(ii) $C_{S'}(K)\cong[S',K]\cong C_p$. Because $C_S(K)\subseteq N_S([S',K])$ and S is a p-group,

$$[C_S(K),[S',K]]\subsetneqq[S',K].$$

Since $[S',K]\cong C_p$,

$$[C_S(K),[S',K]]=\langle 1\rangle. \tag{3.14}$$

Now $G'=\langle [S,K],S'\rangle$. So, by (3.9), $G'=\langle [S,K],C_{S'}(K)\rangle$. By Theorem 1.3, $[S,K]=[[S,K],K]$. So $G'=\langle [G',K],C_{S'}(K)\rangle$. Because $C_{S'}(K)\cong C_p$,

$$[G',K]=\langle g_1\rangle\times[S',K]\cong C_p\times C_p,$$

for some $g_1\in[G',K]\backslash S'$. Let $g\in G'$. Then $g=g_1^\alpha g_2g_3$, where $g_2\in[S',K]$, $g_3\in C_{S'}(K)$ and $\alpha\in\mathbf{Z}$. Suppose $\alpha\not\equiv 0\,(\text{modulo}\,p)$. Now, as in (i),

$$g_1^\alpha g_2=[k_1s_1,k_2s_2],$$

where $k_1,k_2\in K$ and $s_1,s_2\in[G',K]$. By (3.10), $g_3=[s_3,s_4]$, where $s_3,s_4\in C_S(K)$. Then, by (3.14), (3.11) and because $s_3,s_4\in C_S(K)$,

$$\begin{aligned}[k_1s_1s_3, k_2s_2s_4] &= [k_1s_1s_3, s_4][k_1s_1s_3, k_2s_2]^{s_4}\\ &= [k_1, s_4]^{s_1s_3}[s_1s_3, s_4][k_1s_1, k_2s_2]^{s_3s_4}[s_3, k_2s_2]^{s_4}\\ &= [s_1, s_4][s_3, s_4][k_1s_1, k_2s_2]^{s_3s_4}[s_3, k_2s_2]^{s_4}\end{aligned}$$

By (3.11), $[s_1, s_4][s_3, s_2] = g_2^{\mu}$ and

$$[k_1s_1, k_2s_2]^{s_3s_4} = [k_1s_1, k_2s_2]g_2^{\eta},$$

where $\mu, \eta \in \mathbf{Z}$. So,

$$[k_1s_1s_3, k_2s_2s_4] = g_1^{\alpha}g_2g_3g_2^{\mu+\eta}.$$

By (3.11) and (3.14) there exists an $s \in C_S(K)$ such that $g_1^s = g_1g_2^{\lambda}$, where $\lambda \in \mathbf{Z}$ and $\lambda \not\equiv 0\,(\text{modulo}\, p)$. Consequently, there exists an $\zeta \in \mathbf{Z}$ such that $\mu + \eta + \zeta\lambda\alpha \equiv 0\,(\text{modulo}\, p)$. Then,

$$[k_1s_1s_3, k_2s_2s_4]^{s^{\zeta}} = g_1^{\alpha}g_2g_3,$$

as required.

If $\alpha \equiv 0\,(\text{modulo}\, p)$ it suffices to show that $S \in \mathbf{C}$. Now $S' \simeq C_p \times C_p$. Let $H = S \times P$, where P is a p-group such that P' is cyclic of order p. Then, by Case (2), $H \in \mathbf{C}$. Consequently, $S \in \mathbf{C}$.

(iii) $C_{S'}(K) \simeq C_p \times C_p$. For similar reasons to those in the comment at the end of Case (3) (ii) we have that $C_S(K) \in \mathbf{C}$. By (3.1), $[G', K] \cong C_p$, so $[G', K] \subseteq \mathbf{K}(G)$. Let $g \in G'$. Then $g = g_1g_2$, where $g_1 \in C_{S'}(K)$ and $g_2 \in [G', K]$. By (3.10) $g_1 = [s_1, s_2]$, where $s_1, s_2 \in C_S(K)$ and $g_2 = [s_3, k]$, where $s_3 \in [G', K]$ and $k \in K$. Consequently,

$$g = [s_1, s_2][s_3, k] = [s_1s_3, ks_2],$$

because

$$\langle 1 \rangle = [C_S(K), [G', K]] \subsetneq [G', K].$$

(iv) $C_{S'}(K) = \langle 1 \rangle$. By (3.9), $S' = [S', K]$. Therefore $G' = [G', K]$, a contradiction. This completes the proof of the theorem.

4. Theorem C

Proof of Theorem C. By Gorenstein (1968), Theorem 7.4.4, we see that $S \subseteq N_G(S)'$. So it suffices to consider the case $S \lhd G$. We assume G to be a counter-example of minimal order and we obtain a contradiction.

Let $S = \langle c_1 \rangle \times \langle c_2 \rangle$, where we assume $c_1 \notin \mathbf{K}(G)$. Now G induces a p'-group of automorphisms upon S. Consequently, by Theorem 1.1, $S = [S, G] \times C_S(G)$. By the Focal Subgroup Theorem (Gorenstein (1968),

https://doi.org/10.1017/S1446788700020073 Published online by Cambridge University Press

Theorem 7.3.4), $[S, G] = S \cap G' = S$, so $C_S(G) = \langle 1 \rangle$. Thus, there exists a $g_1 \in G$ such that $c_1^{g_1} \neq c_1$. If g_1 induces a fixed point free automorphism upon S, then it immediately follows that $S \subseteq \mathbf{K}(G)$. So we may assume that $C_S(g_1) \neq \langle 1 \rangle$. We may assume that $c_2^{g_1} = c_2$. Let $c_1^{g_1} = c_1^v c_2^w$, for some $v, w \in \mathbf{Z}$.

Suppose that $[c_1, g] \in \langle [c_1, g_1] \rangle$ for every $g \in G$. Now, $[c_1^\lambda, g_1] = [c_1, g_1]^\lambda$, where $\lambda \in \mathbf{Z}$ and, consequently, $\langle [c_1, g_1] \rangle \subseteq \mathbf{K}(G)$. Therefore $c_1 \notin \langle [c_1, g_1] \rangle$. From D. Passman (1968), Proposition 12.1, G has a proper normal subgroup K such that

$$|G/K| \,\big|\, |S/\langle [c_1, g_1] \rangle|.$$

Therefore $|G/K| = p$. So G/K is abelian and $G' \subseteq K$. But $S \subseteq G'$ and, consequently, $|G/K|$ is a p'-number, a contradiction. So we may assume that there exists a $g_2 \in G$ such that $S = \langle [c_1, g_1], [c_1, g_2] \rangle$. Because S is an abelian normal subgroup of G the mapping ϕ defined by $\phi : s \to [s, g_2]$, where $s \in S$, is an endomorphism of S. Moreover $\phi(S) \subseteq \mathbf{K}(G)$. So, if $[c_2, g_2] \notin \langle [c_1, g_2] \rangle$, then $\phi(S) = S \subseteq \mathbf{K}(G)$. By the minimality of G we may assume that $G = \langle S, g_1, g_2 \rangle$. If $[c_2, g_2] = 1$, then $c_2 \in Z(G)$ and $C_S(G) \neq \langle 1 \rangle$, a contradiction. So $[c_2, g_2] \neq 1$ and $[c_2, g_2] = [c_1, g_2]^\alpha$, for some $\alpha \in \mathbf{Z}$, where $(\alpha, p) = 1$. So there exists a $\beta \in \mathbf{Z}$ such that $[c_2, g_2]^\beta = [c_1, g_2]$. But $[c_2, g_2]^\beta = [c_2^\beta, g_2]$ and if we substitute c_2^β for c_2 we may assume that $[c_1, g_2] = [c_2, g_2]$.

Let $c_1^{g_2} = c_1^t c_2^u$, then $c_2^{g_2} = c_1^{t-1} c_2^{u+1}$, where $t, u \in \mathbf{Z}$. If $g_2 g_1$ induces a fixed point free automorphism upon S, then $S \subseteq \mathbf{K}(G)$. So we may assume that $C_S(g_2 g_1) \neq \langle 1 \rangle$. Now,

$$c_1^{g_2 g_1} = (c_1^t c_2^u)^{g_1} = (c_1^v c_2^w)^t c_2^u = c_1^{vt} c_2^{wt+u}$$

and

$$c_2^{g_2 g_1} = (c_1^{t-1} c_2^{u+1})^{g_1} = (c_1^v c_2^w)^{t-1} c_2^{u+1} = c_1^{v(t-1)} c_2^{w(t-1)+u+1}.$$

Since $C_S(g_2 g_1) \neq \langle 1 \rangle$, there exist $\lambda, u \in \mathbf{Z}$ such that

$$(c_1^\lambda c_2^\mu)^{g_2 g_1} = c_1^\lambda c_2^\mu.$$

Thus,

$$vt\lambda + v(t-1)\mu \equiv \lambda \pmod{p}$$

$$(wt + u)\lambda + (w(t-1) + u + 1)\mu \equiv \mu \pmod{p}.$$

So we have,

$$\begin{aligned} (vt - 1)\lambda + v(t-1)\mu &\equiv 0 \pmod{p} \\ (wt + u)\lambda + (w(t-1) + u)\mu &\equiv 0 \pmod{p}. \end{aligned} \tag{4.1}$$

The equations (4.1) have a non-trivial solution if and only if

https://doi.org/10.1017/S1446788700020073 Published online by Cambridge University Press

$$\begin{vmatrix} vt-1 & v(t-1) \\ wt+u & w(t-1)+u \end{vmatrix} \equiv 0 \,(\text{modulo}\, p).$$

This reduces to,

$$u(v-1) - w(t-1) \equiv 0 \,(\text{modulo}\, p). \tag{4.2}$$

If $u \equiv 0 \,(\text{modulo}\, p)$, then $[c_1, g_2] = c_1^{t-1}$. Because $S = \langle [c_1, g_1], [c_1, g_2] \rangle$, $t - 1 \not\equiv 0 \,(\text{modulo}\, p)$. Consequently, from Honda (1953), $c_1 \in \mathbf{K}(G)$, a contradiction. So we may assume that $u \not\equiv 0 \,(\text{modulo}\, p)$.

If $v \equiv 1 \,(\text{modulo}\, p)$, then g_1 induces a p-automorphism upon S. So $v \not\equiv 1 \,(\text{modulo}\, p)$. Thus there exists an $\zeta \in \mathbb{Z}$ such that $(v-1)\zeta \equiv t - 1 \,(\text{modulo}\, p)$. We consider $\zeta((v-1)+w)$. By (4.2),

$$\zeta((v-1)+w) \equiv \zeta(w(t-1)/u + w) \,(\text{modulo}\, p).$$

But

$$\zeta((v-1)+w) \equiv t - 1 + \zeta w \,(\text{modulo}\, p),$$

by construction. Therefore,

$$t - 1 \equiv \zeta w(t-1)/u \,(\text{modulo}\, p).$$

So, either $t \equiv 1 \,(\text{modulo}\, p)$ or $\zeta w/u \equiv 1 \,(\text{modulo}\, p)$. If $t \equiv 1 \,(\text{modulo}\, p)$, then, by (4.2), $u(v-1) \equiv 0 \,(\text{modulo}\, p)$. But neither $u \equiv 0 \,(\text{modulo}\, p)$ nor $v - 1 \equiv 0 \,(\text{modulo}\, p)$, a contradiction. Finally, if $\zeta w/u \equiv 1 \,(\text{modulo}\, p)$, then $w \equiv \zeta u \,(\text{modulo}\, p)$. This implies $[c_1, g_1]^\zeta = [c_1, g_2]$, our final contradiction.

The following example gives a first approximation on how far $d(S)$ can be extended in any generalization of Theorem C. Let $H = C_p \wr (C_q \times C_q \times C_q)$, where p and q are different primes. By a routine calculation one can show that $H \notin \mathbf{C}$. The Sylow p-subgroup S of H is elementary abelian, such that $d(S) = q^3$, and is equal to $H' \times Z(H)$. Suppose that $G \cong H/Z(H)$. It follows that $G \notin \mathbf{C}$. Now G' is the Sylow p-subgroup of G and is elementary abelian such that $d(G') = q^3 - 1$. If $p \neq 2$ we can set $q = 2$ to obtain $d(G') = 7$, which is a reasonable bound to any extension of Theorem C.

Acknowledgement

The above paper forms a part of my Ph.D. thesis and I wish to thank Dr. H. Liebeck for his supervision of the research. I also wish to thank the referee for his helpful comments which corrected and shortened some of the proofs. Finally I am grateful to the Science Research Council and the University of Ibadan for their financial support.

References

R. D. Carmichael (1937), *Introduction to the Theory of Groups of Finite Order* (Ginn & Co., Boston, U.S.A.).

J. D. Dixon (1971), *The Structure of Linear Groups* (Van Nostrand, London).

D. Gorenstein (1968), *Finite Groups* (Harper & Row, New York).

K. Honda (1953), On Commutators in Finite Groups, *Commentarii Mathematici, Universitatis Sancti Pauli* (Tokyo), 2, 9–12.

I. D. Macdonald (1963), On Cyclic Commutator Subgroups, *J. London Math. Soc.*, 38, 419–422.

D. S. Passman (1968), *Permutation Groups* (Benjamin, New York).

D. M. Rodney (1974), On Cyclic Derived Subgroups, *J. London Math. Soc.* (2), 8, 642–646.

147 Station Road,
Hendon,
London,
England.