ON DOUBLE CENTRALIZER SUBGROUPS
OF SOME FINITE p-GROUPS

YING CHENG

ABSTRACT. Let $A$ be a maximal abelian normal subgroup of a finite $p$-group $G$ ($p > 2$) such that $[G, A]$ is cyclic. Then (i) $C_G(C_G(D)) = D$ and $[G : C_G(D)] = [D : Z(G)]$ for every $Z(G) \leq D \leq G$; (ii) $[G : Z(G)] = [G, A]^2$ and every faithful absolutely irreducible representation of $G$ is of degree $[G : A]$. The case $p = 2$ will also be mentioned.

1. Introduction. Let $p$ be a prime number. For a finite $p$-group $Q$, we write $\Omega(Q)$ for $\Omega_2(Q)$ if $p = 2$ and $\Omega_t(Q)$ if $p > 2$, where $\Omega_t(Q) = \langle x \in Q | x^{p^t} = 1 \rangle$. Besides this, the notation is standard (cf. [3 or 5]).

The main result of this paper is

THEOREM A. Let $A$ be a maximal abelian normal subgroup of a finite $p$-group $G$. Suppose $[G, A]$ is cyclic and $\Omega([G, A]) \subseteq Z(G)$. Then

(i) $C_G(C_G(D)) = D$ and $[G : C_G(D)] = [D : Z(G)]$ for every $Z(G) \leq D \leq A$;


Theorem A(i) and the first part of Theorem A(ii) are special cases of the following:

THEOREM B. Let $A \supseteq Z(G)$ be an abelian normal subgroup of a finite $p$-group $G$. Suppose $[G, A]$ is cyclic and $\Omega([G, A]) \leq Z(G)$. Then $C_A(C_G(D)) = D$ and $[G : C_G(D)] = [D : Z(G)]$ for every $Z(G) \leq D \leq A$.

We note that in case $p > 2$, the condition $\Omega([G, A]) \leq Z(G)$ is automatically satisfied.

In §§3 and 4 we will prove these results by applying the double centralizer property in the theory of an Azumaya algebra $B$ over a commutative ring (with identity) [2, Chapter II]: $C_B(C_B(E)) = E$ for every separable subalgebra $E$ of $B$. In [1], a purely group-theoretical method is given to prove that if $G$ is a finite $p$-group with cyclic commutator subgroup $G'$ such that $\Omega(G') \leq Z(G)$, then $C_G(C_G(D)) = D$ for every $Z(G) \leq D \leq G$. In §5, we will also briefly indicate how to prove this result by the theory of Azumaya algebras.

Finally, we remark that Theorem A(ii) generalizes [5, III, 13.7(c) and 5, V, 16.14]. G. A. How [4] has an independent proof of Theorem A(ii).

Received by the editors February 24, 1982.

1980 Mathematics Subject Classification. Primary 20D15.

Key words and phrases. Commutator subgroup, Azumaya algebras.
2. Preliminaries. In this section, we will prove two easy lemmas (possibly known).

**Lemma 1.** Let \( U \neq 1 \) be a cyclic subgroup of a finite abelian group \( V \). Then \( V \) can be embedded into the units group of a commutative ring \( R \) such that

(i) \( R \) contains the rational number field \( \mathbb{Q} \),
(ii) \( g - 1 \) is not a zero divisor for any nonidentity element \( g \in U \leq R \).

**Proof.** First of all, \( V \) can be embedded into a finite homocyclic abelian group, say \( A \). As \( U \) is cyclic, we may assume \( A = A_1 \times A_2 \times \cdots \times A_t \) so that \( A_i \) (1 \( \leq i \leq t \)) is cyclic, \( U \neq A_1 \), and \( |A_1| = |A_2| = \cdots = |A_t| \). Let \( A_i = \langle a_i \rangle \) for \( 1 \leq i \leq t \). \( \{a_1a_2 \ldots a_i, a_2, \ldots, a_i\} \) is a base for \( A \). The coordinates of nonidentity elements of \( \langle a_i \rangle \) in this base are nonidentity. Embed \( A = \langle a_1a_2 \ldots a_i \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_i \rangle \) into the units group of the ring \( R = \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \cdots \oplus \mathbb{C} \), the direct sum of \( t \) copies of the complex field \( \mathbb{C} \). In this embedding, it is easy to see that (i) and (ii) are satisfied.

**Lemma 2.** Let \( G = \langle x, y \rangle \) be a finite \( p \)-group with cyclic commutator subgroup \( G' \) such that \( \Omega(G') \leq C_G(x) \). Suppose \( [x^p, y] = 1 \). Then \([x, y]^p = 1\).

**Proof.** For convenience, let \( z = [x, y] \). If \( p > 2 \), then \( G \) is regular and \([x^p, y] = [x, y]^p = 1\). (In fact, one can prove this more directly.)

Now let \( p = 2 \). The condition \([x^2, y] = 1\) is equivalent to \( z^4 = z^{-1} \). Assume \( z \notin C_G(x) \) and \( z^2 \in C_G(x) \) with minimal \( r \). That is \( r \geq 1 \) and \( z^2 = z^{-1} \). This implies \( z^2 = 1 \). \( z^2 = 1 \) is of order 4 and is not in \( C_G(x) \), a contradiction. Therefore, \( z \in C_G(x) \) and \( z^2 = 1 \).

3. Proof of Theorem B. By Lemma 1, we may embed \( Z = Z(G) \) into the units group of a commutative ring \( R \) such that (1) \( R \) contains the rational number field \( \mathbb{Q} \), and (2) \( g - 1 \) is not a zero divisor for any nonidentity element \( g \in [G, A] \cap Z \). Let \( \{x_1 = 1, x_2, \ldots, x_r\} \) be a set of coset representatives of \( Z \) in \( A \). Denote \( S \) as a free \( R \)-module with free basis \( x_j, 1 \leq i \leq r \). Define a multiplication on \( S \), distributively, as \( x_i \cdot x_j = ax_k \), where \( x_k \) is the coset representative of \( x_i \cdot x_j \) and \( a \in Z \cap A \). Clearly, \( S \) is an \( R \)-algebra and \( A \) can be viewed, in the natural way, as a subgroup of units group of \( S \). It is easy to see that the relation \( ag = a \) for \( a \in S, g \in [G, A] \cap Z \) implies \( a = 0 \).

\( \bar{G} = G/C_G(A) \), with elements denoted as \( \bar{g} \) for \( g \in G \), acts on \( A \) by conjugation. For convenience, we denote the action as \( \bar{g}(x) = g x g^{-1} \) for \( g \in G \) and \( x \in A \). We may extend the action of \( \bar{G} \) to \( S \). Then \( \bar{G} \) is a subgroup of \( R \)-automorphisms of \( S \). Now we may construct a new \( R \)-algebra \( B \) as in the classical way: First let \( \{u_{\bar{g}} | \bar{g} \in \bar{G}\} \) be a free basis for a (left) \( S \)-module. Define multiplication in this module by letting \( (au_{\bar{g}})(bu_{\bar{h}}) = a\bar{g}(b)u_{\bar{gh}} \) for all \( a, b \in S, g, h \in G \) and extending by linearity. Of course, \( \{x_i u_{\bar{g}} | \bar{g} \in \bar{G}, 1 \leq i \leq r\} \) is a free basis for the \( R \)-algebra \( B \). Now, we will show that \( B \) is a central separable \( R \)-algebra.

First it is easy to show that the element

\[
\frac{1}{r} \sum_{1 \leq i \leq r} x_i u_{\bar{g}} \otimes u_{\bar{g}}^{-1} x_i^{-1} \in B \otimes B^{op}
\]

is a central separable \( R \)-algebra.
is a separability idempotent for $B$ [2, Chapter II]. So $B$ is a separable $R$-algebra. For every $D \leq A$ which contains $Z$, let $RD$ denote the $R$-subalgebra of $S$ generated by $D$. As above, it is easy to show that $RD$ is a separable $R$-subalgebra of $B$. We claim that $C_B(RD) \leq SC_G(D)$, the $S$-subalgebra of $B$ generated by $u_\tilde{g}$ for $\tilde{g} \in C_G(D)$. Suppose $z = \sum_{\tilde{g} \in \tilde{G}} u_{\tilde{g}} \tilde{g} \in C_B(RD)$. If $\tilde{h} \notin C_G(D)$, then there is $d \in D$ with minimal order such that $[d, \tilde{h}^{-1}] \neq 1$. So $[d^p, \tilde{h}^{-1}] = 1$. By Lemma 2, $[d, \tilde{h}^{-1}]$ is of order $p$ and hence is in $[G, A] \cap Z$.

$$z = d^{-1}zd = \sum a_\tilde{g}d^{-1}u_{\tilde{g}}d = \sum a_\tilde{g}d^{-1}gd^{-1}u_{\tilde{g}} = \sum a_{\tilde{g}}[d, g^{-1}]u_{\tilde{g}}.$$  
So $a_\tilde{g}[d, h^{-1}] = a_\tilde{g}$ and $a_\tilde{g} = 0$. This proves that $C_B(RD) \leq SC_G(D)$. In particular, we have $C_B(S) = C_B(RA) \leq SC_G(A) = S$.

Suppose $z \in Z(B) = C_B(B)$. Then $z \in S$. Let $z = a_1x_1 + a_2x_2 + \cdots + a_rx_r$, where $a_i \in R$. For fixed $i$, $2 \leq i \leq r$, let $g$ be an element of $G$ with minimal order so that $[g^{-1}, x_i^{-1}] \neq 1$. Then $[g^{-p}, x_i^{-1}] = 1$. By Lemma 2, $[g^{-1}, x_i^{-1}]$ is of order $p$ and hence is in $[G, A] \cap Z$.

$$z = d^{-1}zd = \sum_{j=1}^r a_jx_j = \sum_{j=1}^r a_jx_jg^{-1}u_{\tilde{g}} = \sum_{j=1}^r a_j[g^{-1}, x_j]x_ju_{\tilde{g}}.$$  
So $a_i[g^{-1}, x_i] = a_i$ and $a_i = 0$. Therefore, $z \in R$ and $Z(B) = R$. That is, $B$ is a central separable $R$-algebra.

We note that $S$ is actually a Galois extension of $R$ with Galois group $\tilde{G}$ and $B = \Delta(S : \tilde{G})$ in the notation of [2, Chapter III]. Since we do not need this fact, we will not prove it here.

Now, for every $Z < D < A$, by double centralizer properties in the theory of Azumaya algebras [2, Chapter II], we have $RD = C_B(C_B(RD))$. Then $RD = C_B(C_B(RD)) \supseteq C_B(SC_G(D)) \supseteq R(SC_G(C_G(D))) \cap A$.

As $D = RD \cap A \supseteq C_B(C_G(D)) \cap A = C_A(C_G(D)) \supseteq D$, so $D = C_A(C_G(D))$. This proves the first result in Theorem B.

To prove the second result, let $|A/Z| = p^n$ and $|D/Z| = p^r$ and take a series $Z = D_0 < D_1 < \cdots < D_r = D < D_{r+1} < \cdots < D_n = A$, with $[D_{i+1} : D_i] = p$ ($0 \leq i < n$). Then $G = C_G(D_0) \supseteq C_G(D_1) \supseteq \cdots \supseteq C_G(D_n) = C_G(A)$.

Applying $C_A(\cdot)$ to the above series, we get the original series. So $[C_G(D_i) : C_G(D_{i+1})] = p$ for all $i$. Hence $[G : C_G(D)] = p^r$ and $[G : C_G(D)] = [D : Z]$. This completes the proof of the theorem.

4. Proof of Theorem A and a corollary. Theorem A(i) and the first part of Theorem A(ii) follow easily from Theorem B. Now let $\sigma$ be a faithful absolutely irreducible representation of $G$ over a field $F$. $\sigma$ maps $G$ into $M = \text{Mat}_n(F)$, the full matrix ring of degree $n$ over $F$. Let $\{x_1 = 1, x_2, \ldots, x_r\}$ be a set of coset representatives of $Z$ in $A$. Let $\{y_1 = 1, y_2, \ldots, y_r\}$ be a set of right coset representatives of $A$ in $G$. We first claim that $\{\sigma(x_1y_j) \mid 1 \leq i, j \leq r\}$ is a linearly independent set over $F$ and $\text{Fo}(G)$ is a central separable $F$-algebra. In fact, the proof is the same as the method we used to prove that $B$ is central in Theorem B. Here we omit the detail. Since $\sigma$ is absolutely...
irreducible over $F$, $C_M(Fo(G)) = F$. Then

$$n^2 = [M : F] = [Fo(G) : F][C_M(Fo(G)) : F] = [Fo(G) : F] = [G : Z].$$

This completes the proof of Theorem A.

As a corollary to Theorem A(ii) and [6, Theorem 8], we get

**Corollary.** Let $A$ be a maximal abelian normal subgroup of a finite $p$-group $G$. Suppose $[G, A]$ is cyclic and $\Omega([G, A]) \leq Z(G)$. Then all maximal abelian normal subgroups of $G$ are of order $|Z(G)||[G: Z(G)]^{1/2}$. If, in addition, $p > 2$, then all maximal abelian subgroups of $G$ are of order $|Z(G)||[G: Z(G)]^{1/2}$.

5. **Finite $p$-groups with cyclic commutator subgroup.** In this section, we will briefly indicate how to apply the method we used in §3 to the finite $p$-groups with cyclic commutator subgroup.

**Theorem C [1, Theorem 2].** Let $G$ be a finite $p$-group with cyclic commutator subgroup $G'$. Suppose $\Omega(G') \leq Z(G)$. Then $C_Z(C_G(D)) = D$ for every $Z(G) \leq D \leq G$.

**Proof.** As in §2, we embed $Z = Z(G)$ into a good commutative ring $R$ so that $g - 1$ is not a zero divisor for every $g \in G' \cap Z$. Let $\{g_1 = 1, g_2, \ldots, g_s\}$ be a set of coset representatives of $Z$ in $G$. Let this set be a free $R$-basis for an $R$-module $B$. Define a multiplication on $B$ so that $B$ forms an $R$-algebra and $G$ can be viewed as in the units group of $B$. For every $Z \leq D \leq G$, let $RD$ be the $R$-subalgebra of $B$ generated by $D$. By the same method we used in §3, we can obtain that $RD$ is a separable $R$-algebra and $C_B(RD) = RC_G(D)$. In particular, $C_B(B) = C_B(RG) = RC_G(G) = R$. So $B$ is an Azumaya algebra over $R$. As $RD$ is a separable $R$-algebra, we get

$$RD = C_B(C_B(RD)) = C_B(RC_G(D)) = RC_G(C_G(D)).$$

By taking the intersection with $G$, we get $D = C_G(C_G(D))$. This completes the proof.

**References**


DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CHICAGO, CHICAGO, ILLINOIS 60637