Centralizers and the maximum size of the pairwise noncommuting elements in finite groups

Seyyed Majid Jafarian Amiri* and Hojjat Rostami†

Abstract

In this article, we determine the structure of all nonabelian groups $G$ such that $G$ has the minimum number of the element centralizers among nonabelian groups of the same order. As an application of this result, we obtain the sharp lower bound for $\omega(G)$ in terms of the order of $G$ where $\omega(G)$ is the maximum size of a set of the pairwise noncommuting elements of $G$.

Keywords: finite group, centralizer, CA-group.

2000 AMS Classification: 20D60

Received: 02.02.2016 Accepted: 14.07.2016 Doi: 10.15672/HJMS.20164519332

1. Introduction and main results

Throughout this paper $G$ will be a finite group and $Z(G)$ will be its center. For a positive integer $n$, let $Z_n$ and $D_{2n}$ be the cyclic group of order $n$ and the dihedral group of order $2n$, respectively. For a group $G$, we define $\text{Cent}(G) = \{C_G(x) : x \in G\}$ where $C_G(x)$ is the centralizer of the element $x$ in $G$. It is clear that $G$ is abelian if and only if $|\text{Cent}(G)| = 1$. Also it is easy to see that there is no group $G$ with $|\text{Cent}(G)| = 2$ or 3.

Starting with Belcastro and Sherman [7], many authors have investigated the influence of $|\text{Cent}(G)|$ on the group $G$ [see [1], [4], [6], [7], [17-21] and [27-29]]. In the present paper, we describe the structures of all groups having minimum number of centralizers among all nonabelian groups of the same order, that is:

*Department of Mathematics, Faculty of Sciences, University of Zanjan, P.O.Box 45371-38791, Zanjan, Iran
Email: sm_jafarian@znu.ac.ir

†Department of Mathematics, Faculty of Sciences, University of Zanjan, P.O.Box 45371-38791, Zanjan, Iran
Email: h.rostami991@gmail.com
1.1. Theorem. Let $G$ be a nonabelian group of order $n$. If $|\text{Cent}(G)| \leq |\text{Cent}(H)|$ for all nonabelian groups $H$ of order $n$, then one of the following holds:

1. $G$ is nilpotent, $|\text{Cent}(G)| = p + 2$ and $\frac{\omega_G}{\omega(G)} \cong Z_p \times Z_p$ where $p$ is the smallest prime such that $p^3$ divides $n$. 
2. $G$ is nonnilpotent, $|\text{Cent}(G)| = p^m + 2$ and $\frac{\omega_G}{\omega(G)} \cong (Z_p)^m \times Z_l$ where $l > 0$ and $p^m$ is the smallest prime-power divisor of $n$ such that $p^m - 1$ and $n$ are not relatively prime.

The following corollary are immediate consequence of Theorem 1.1.

1.2. Corollary. Suppose that $n$ is even and $G$ is a nonabelian group of order $n$. If $|\text{Cent}(G)| \leq |\text{Cent}(H)|$ for all nonabelian groups $H$ of order $n$, then $|\text{Cent}(G)| = 4$ or $p + 2$ where $p$ is the smallest odd prime divisor of $n$ and also $\frac{\omega_G}{\omega(G)}$ is isomorphic to one of the following groups:

\[ Z_2 \times Z_2, Z_p \times Z_p, D_2p. \]

1.3. Remark. We notice that both conditions (1) and (2) of Theorem 1.1 may happen for some positive integer $n$. For example there exist two groups $G_1$ and $G_2$ of order 54 such that $|\text{Cent}(G_1)| = |\text{Cent}(G_2)| = 5$, $\frac{\omega_G}{\omega(G)} \cong Z_3 \times Z_3$ and $\frac{\omega_G}{\omega(G)} \cong D_6$.

There are interesting relations between centralizers and pairwise noncommuting elements in groups (see Proposition 2.5 and Lemma 2.6 of [1]). Let $G$ be a finite nonabelian group and let $X$ be a subset of pairwise noncommuting elements of $G$ such that $|X| \geq |Y|$ for any other set of pairwise noncommuting elements $Y$ in $G$. Then the subset $X$ is said to have the maximum size, and this size is denoted by $\omega(G)$. Also $\omega(G)$ is the maximum clique size in the noncommuting graph of a finite group $G$. The noncommuting graph of a group $G$ is defined as a graph whose $G \setminus Z(G)$ is the set of vertices and two vertices are joined if and only if they do not commute. By a famous result of Neumann [22] answering a question of Erdős, the finiteness of $\omega(G)$ is equivalent to the finiteness of the factor group $\frac{G}{\omega(G)}$ which follows that $|\text{Cent}(G)|$ is finite. Also, if $G$ has a finite number of centralisers, then it is easy to see that $\omega(G)$ is finite. Various attempts have been made to find $\omega(G)$ for some groups $G$. Pyber [24] has proved that there exists a constant $c$ such that $\frac{\omega_G}{\omega(G)} \leq c\omega(G)$. Chin [13] has obtained upper and lower bounds of $\omega(G)$ for extra-special groups $G$ of odd order. Isaacs has shown that $\omega(G) = 2m + 1$ for any extra-special group $G$ of order $2^{2m+1}$ (see page 40 of [11]). Brown in [9] and [10] has investigated $\omega(S_n)$ where $S_n$ is the symmetric group on $n$ letters. Also Bertram, Ballester-Bolinches and Cossey gave lower bounds for the maximum size of non-commuting sets for certain solvable groups [5]. Recently authors [17, 20] have determined all groups $G$ with $\omega(G) = 5$ and obtained $\omega(G)$ for certain groups. Known upper bounds for this invariant were recently used to prove an important result in modular representation theory ( [13]). In this article we determine the structure of nonabelian groups $G$ of order $n$ such that $\omega(G) \leq \omega(H)$ for all nonabelian groups $H$ of order $n$.

1.4. Theorem. Let $G$ be a nonabelian group of order $n$. If $\omega(G) \leq \omega(H)$ for all nonabelian groups $H$ of order $n$, then one of the following holds:

1. $G$ is nilpotent, $\omega(G) = p + 1$ and $\frac{\omega_G}{\omega(G)} \cong Z_p \times Z_p$ where $p$ is the smallest prime such that $p^3$ divides $n$.
2. $G$ is nonnilpotent, $\omega(G) = p^m + 1$ and $\frac{\omega_G}{\omega(G)} \cong (Z_p)^m \times Z_l$ where $l > 0$ and $p^m$ is the smallest prime-power divisor of $n$ such that $p^m - 1$ and $n$ are not relatively prime.

Throughout this paper we will use usual notation which can be found in [25] and [15].
2. Proofs of the main results

The following lemmas are useful in the proof of the main theorem.

2.1. Lemma. Let \( G, G_1, \ldots, G_n \) be finite groups. Then

1. If \( H \leq G \), then \(|\text{Cent}(H)| \leq |\text{Cent}(G)|\);
2. If \( G = \prod_{i=1}^{n} G_i \), then \(|\text{Cent}(G)| = \prod_{i=1}^{n} |\text{Cent}(G_i)|\).

Proof. The proof is clear. \( \square \)

In Lemma 2.7 of [4], it was shown that if \( p \) is a prime, then \(|\text{Cent}(G)| \geq p + 2\) for all nonabelian \( p \)-groups \( G \) and the equality holds if and only if \( \frac{G}{\text{Z}(G)} \cong \mathbb{Z}_p \times \mathbb{Z}_p \). In the following we generalize this result for all nilpotent groups.

2.2. Lemma. Let \( G \) be a nilpotent group and \( p \) be a prime divisor of \(|G|\) such that a Sylow \( p \)-subgroup of \( G \) is nonabelian. Then \(|\text{Cent}(G)| \geq p + 2\) with equality if and only if \( \frac{G}{\text{Z}(G)} \cong \mathbb{Z}_p \times \mathbb{Z}_p \).

Proof. Suppose that \( P \) is a Sylow \( p \)-subgroup of \( G \). Then we have \(|\text{Cent}(G)| \geq |\text{Cent}(P)| \geq p + 2\) by Lemma 2.1.1 and Lemma 2.7 of [4], as wanted.

Now, assume that \(|\text{Cent}(G)| = p + 2\). Since \( G \) is nilpotent, each Sylow \( q \)-subgroup of \( G \) is abelian for each prime divisor \( q \neq p \) of \(|G|\) by Lemma 2.1.2. Consequently \( \frac{G}{\text{Z}(G)} \cong \mathbb{Z}_p \times \mathbb{Z}_p \) which is isomorphic to \( \mathbb{Z}_p \times \mathbb{Z}_p \) by Lemma 2.7 of [4]. The converse holds similarly. \( \square \)

Recall that a minimal nonnilpotent group is a nonnilpotent group whose proper subgroups are all nilpotent. In 1924, O. Schmidt [26] studied such groups. The following result plays an important role in the proof of Theorem 1.1.

2.3. Lemma. Let \( G \) be a minimal nonnilpotent group. Then \( \frac{G}{\text{Z}(G)} \) is Frobenius such that the Frobenius kernel is elementary abelian and the Frobenius complement is of prime order.

Proof. By Theorem 9.1.9 of [25], we have \( G = PQ \) where \( P \) is a unique Sylow \( p \)-subgroup of \( G \) and \( Q \) is a cyclic Sylow \( q \)-subgroup of \( G \) for some distinct primes \( p \) and \( q \). Also by Exercise 9.1.11 of [25], the Frattini subgroups of \( P \) and \( Q \) are contained in \( \text{Z}(G) \). It follows that \( \frac{P \text{Z}(G)}{\text{Z}(G)} \) is elementary and \( \frac{Q \text{Z}(G)}{\text{Z}(G)} \) is of order \( q \). Since all Sylow subgroups of \( \frac{G}{\text{Z}(G)} \) are abelian, Theorem 10.1.7 of [25] gives that \( (\frac{G}{\text{Z}(G)})' \cap \text{Z}(\frac{G}{\text{Z}(G)}) = \{1\} \). Since \( P = [P, Q] \), we have \( \frac{P \text{Z}(G)}{\text{Z}(G)} \leq \frac{G \text{Z}(G)}{\text{Z}(G)} \) and so \( \text{Z}(\frac{G}{\text{Z}(G)}) \) is a \( q \)-group. On the other hand since \( G \) is not nilpotent, \( \text{Z}(\frac{G}{\text{Z}(G)}) = \{1\} \). Now it is easy to see that \( \frac{G}{\text{Z}(G)} \) is a Frobenius group. \( \square \)

2.4. Proposition. Let \( \frac{G}{\text{Z}(G)} = \frac{K}{\text{Z}(G)} \rtimes \frac{H}{\text{Z}(G)} \) be a Frobenius group such that \( H \) is abelian. If \( \text{Z}(G) < \text{Z}(K) \), then \(|\text{Cent}(G)| = |\text{Cent}(K)| + |\text{K}/\text{Z}(G)| + 1\) and if \( \text{Z}(G) = \text{Z}(K) \), then \(|\text{Cent}(G)| = |\text{Cent}(K)| + |\text{K}/\text{Z}(G)|\). Also \( \omega(G) = \omega(K) + |\text{K}/\text{Z}(G)|\).

Proof. See Proposition 3.1 of [18] and its proof. \( \square \)

Recall that a group \( G \) is a CA-group if the centralizer of every noncentral element of \( G \) is abelian. R. Schmidt [26] determined all CA-groups (see Theorem A of [14]). Now we are ready to prove the main result.

Proof of Theorem 1.1.

Suppose that \( G \) is a nilpotent group. Since \( G \) is not abelian, a Sylow \( q \)-subgroup of \( G \) is not abelian for some prime \( q \). It follows from Lemma 2.2 that \(|\text{Cent}(G)| \geq q + 2\).
But there exists a nonabelian group $H := Q \times Z_2^p$ of order $n$ where $Q$ is a nonabelian group of order $q^m$ and we see that $|\text{Cent}(H)| = q + 2$. Since $G$ has the minimum number of the element centralizer, we must have $|\text{Cent}(G)| = p + 2$ and $p$ must be the smallest prime such that $p^s$ divides $n$. Also $\frac{G}{\text{Z}(G)} \cong Z_p \times Z_p$ by Lemma 2.2, as wanted.

Now, assume that $G$ is a nilpotent group of order $n$. Then there exist two prime divisors $q$ and $r$ of $n$ such that $q$ divides $r^k - 1$ for some positive integer $k$ by Corollary 1 of [23]. We claim that if $p^m$ is the smallest prime-power divisor of $n$ such that $gcd(p^m - 1, n) \neq 1$, then $|\text{Cent}(G)| \geq p^m + 2$.

Since $G$ is finite and nilpotent, $G$ contains a minimal nonnilpotent subgroup $M$. It follows from Lemma 2.3 that $\frac{M}{\text{Z}(M)}$ is Frobenius with the kernel $\frac{K}{\text{Z}(M)}$ and the complement $\frac{H}{\text{Z}(M)}$. Note that $|\frac{K}{\text{Z}(M)}| = p_1$ and $|\frac{H}{\text{Z}(M)}| = p_2$ for some primes $p_1$ and $p_2$ such that $p_2 | p_1 - 1$. It follows from Proposition 2.4 that $|\text{Cent}(M)| \geq |\frac{K}{\text{Z}(M)}| + 2 = p_1 + 2$. Since $M$ is a subgroup of $G$, we have $|\text{Cent}(G)| \geq |\text{Cent}(M)| \geq p_1 + 2$ which is equal or greater than $p^m + 2$ by hypothesis. This proves the claim. Now we want to find the structure of nonnilpotent groups $G$ for which the equality occurs.

Assume that $|\text{Cent}(G)| = p^m + 2$. We shall prove that $\frac{G}{\text{Z}(G)} \cong (Z_p)^m \times Z_4$ for some positive integer $t$. By hypothesis and the previous paragraph, there is a subgroup $G$ of $M$ such that $\frac{M}{\text{Z}(M)}$ is Frobenius with the kernel $\frac{K}{\text{Z}(M)}$ of order $p^m$ and the Frobenius complement $\frac{H}{\text{Z}(M)}$, which is cyclic of prime order. Since $|\frac{K}{\text{Z}(M)}| + |\text{Cent}(K)| \leq |\text{Cent}(G)|$ by Proposition 2.4 and $|\text{Cent}(M)| \leq |\text{Cent}(G)| = p^m + 2$, we have $|\text{Cent}(M)| = p^m + 2$ and $|\text{Cent}(K)| = 1$. It follows that $K$ is abelian and so $M$ is a CA-group by Theorem A (II) of [14]. Next, we show that $G$ is a CA-group.

Since $M$ is a CA-group, we have $p^m + 1$ is the maximum size of a set of pairwise non-commuting elements of $M$ by Lemma 2.6 of [1] and so the maximum size of a set of pairwise non-commuting elements of $G$ is at least $p^m + 1$. Since $|\text{Cent}(G)| = p^m + 2$, the maximum size of a set of pairwise non-commuting elements of $G$ must be $p^m + 1$. Therefore $G$ is a CA-group by Lemma 2.6 of [1]. Now we apply Theorem A of [14].

Note, first, that if $8$ divides $|G| = n$, then by hypothesis $|\text{Cent}(G)| \leq |\text{Cent}(D_8 \times Z_2^p)| = 4$ and so $|\text{Cent}(G)| = 4$. Therefore $\frac{G}{\text{Z}(G)} \cong Z_2 \times Z_2$ by Fact 3 of [7] and so $G$ is nilpotent, a contradiction. Hence $8$ does not divide $n$ and so $|\text{Cent}(G)| \geq 5$ by Fact 4 of [7]. Also if $6$ divides $n$, then $|\text{Cent}(G)| \leq |\text{Cent}(D_6 \times Z_2^p)| = 5$ which implies $|\text{Cent}(G)| = 5$. Therefore $\frac{G}{\text{Z}(G)} \cong D_6$ by Fact [7] and so we have the result. Thus we may assume that $6$ does not divide $n$. Now since $G$ is not nilpotent, $G$ satisfies (I), (II) or (III) of Theorem A of [14]. Therefore $G$ has an abelian subgroup $A$ of prime index $r$ or $\frac{G}{\text{Z}(G)} = \frac{K}{\text{Z}(G)} \times \frac{A}{\text{Z}(G)}$ is a Frobenius group with the Frobenius kernel $\frac{K}{\text{Z}(G)}$ and the Frobenius complement $\frac{A}{\text{Z}(G)}$. In the first case, we have $|G'| = p^m$ by Theorem 2.3 of [6] and so $\frac{G}{\text{Z}(G)} = p^m r$ by Lemma 4 (page 303) of [8]. Consequently $\frac{G}{\text{Z}(G)} = \frac{A}{\text{Z}(G)} \times \frac{K}{\text{Z}(G)}$ where $|\frac{K}{\text{Z}(G)}| = r$ and $|\frac{A}{\text{Z}(G)}| = p^m$. By the property of $p^m$, the number of Sylow $r$-subgroup of $\frac{G}{\text{Z}(G)}$ is $p^m$ and so $\frac{G}{\text{Z}(G)}$ is Frobenius. Again by the property of $p^m$, $\frac{A}{\text{Z}(G)}$ is characteristically simple which implies that it is elementary, as wanted.

In the second case, it follows from (II)-(III) of Theorem A of [14] that $T$ is abelian and $K$ is abelian or $K = QZ(G)$ where $Q$ is a normal Sylow $q$-subgroup of $G$ for some prime $q$. If $K$ is abelian, then $Z(G) < Z(K)$ and so $|\text{Cent}(G)| = |\frac{K}{\text{Z}(G)}| + 2$ by Proposition 2.4. Therefore $|\frac{K}{\text{Z}(G)}| = p^m$. By the property of $p^m$, $\frac{K}{\text{Z}(G)}$ is elementary. On the other hand $\frac{T}{\text{Z}(G)}$ is cyclic by Corollary 6.17 of [15] and so we have the result.

If $K = QZ(G)$, then $|\frac{K}{\text{Z}(G)}| = q^n$ and since $\frac{G}{\text{Z}(G)}$ is Frobenius, we have $|\frac{T}{\text{Z}(G)}|$ divides $q^n - 1$. It follows that $p^m \leq q^n$ by hypothesis. On the other hand $p^m + 2 = |\text{Cent}(G)| \geq$
|\frac{|K|}{|Z(K)|}| + 2 by Proposition 2.4 and this implies that $p^m = q^n$. It follows from Proposition 2.4 that $|\text{Cent}(K)| = 1$ and $K$ is abelian. The rest of the proof is similar to the previous case.

**Proof of Theorem 1.4**

The proof is similar to the previous theorem. If $G$ is nilpotent, then $\omega(G) \geq p + 1$ where $p$ is the smallest prime such that $p^3$ divides $|G|$ and the equality holds if and only if $G/Z(G) \cong Z_p \times Z_p$.

Now suppose that $G$ is non-nilpotent. Then $G$ contains a minimal non-nilpotent subgroup $M$ and so $\frac{M}{Z(M)} = \frac{K}{Z(K)} \times \frac{H}{Z(M)}$ is Frobenius such that $|\frac{K}{Z(K)}| = p^m$ and $|\frac{H}{Z(M)}| = p_2$ by Lemma 2.3. Since $H$ is abelian and has at least $p^m$ conjugates in $G$, say $H = H_1, H_2, \ldots, H_{p^m}$, we see $\{x_1, \ldots, x_{p^m}\}$ is a subset of pairwise noncommuting elements of $M$ where $x_i \in H_i \setminus \{1\}$. It follows that $\omega(G) \geq p^m + 1 \geq p^m + 1$. The remainder of the proof is similar to Theorem 1.1.

**Acknowledgment.** The authors would like to thank the referee for his/her careful reading and valuable comments.

**References**


