TAMKANG JOURNAL OF MATHEMATICS
Volume 53, Number 2, 97-108, June 2022
DOI:10.5556/j.tkjm.53.2022.3370

Characterizing Some Rings of Finite Order

Jutirekha Dutta, Dhiren Kumar Basnet and Rajat Kanti Nath

Abstract. In this paper, we compute the number of distinct centralizers of some classes of finite rings. We then characterize all finite rings with n distinct centralizers for any positive integer $n \leq 5$. Further we give some connections between the number of distinct centralizers of a finite ring and its commutativity degree.

1 Introduction

Finite abelian groups have been completely characterized up to isomorphism for a long time but finite rings have yet to be characterized. The problem of characterizing finite rings up to isomorphism has received considerable attention in recent years (see [2, 8, 10, 12, 13]) starting from the works of Eldridge [11] and Raghavendran [15]. In this paper we characterize finite rings in terms of their number of distinct centralizers. Given a ring R and an element $r \in R$, the subrings $C(r) = \{s \in R : rs = sr\}$ and $Z(R) = \{s \in R : rs = sr \text{ for all } r \in R\}$ are known as *centralizer* of r in R and *center* of R respectively. We write $\text{Cent}(R)$ to denote the set of all centralizers in R. Firstly we compute the order of $\text{Cent}(R)$ for some classes of finite rings R. Motivated by the works of Belcastro and Sherman [3] and Ashrafi [1], we define n-centralizer ring for any positive integer n. A ring R is said to be n-*centralizer* ring if $|\text{Cent}(R)| = n$, for any positive integer n. We then characterize n-centralizer finite rings for all $n \leq 5$, adapting similar techniques that are used by Belcastro and Sherman [3] in order to characterize n-centralizer finite groups for $n \leq 5$. It is worth mentioning that $6, 7$-centralizer finite rings have been characterized in [9].

Further, we conclude the paper by noting some interesting connections between $d(R)$ and $|\text{Cent}(R)|$, where $d(R)$ is the probability that a randomly chosen pair of elements of R commute. For any finite ring R we have $d(R) = \frac{1}{|R|^2} \sum_{r \in R} |C(r)|$. This $d(R)$ is also known as *commutativity*

2010 *Mathematics Subject Classification*. 16U70.
Key words and phrases. Finite ring, centralizer, commutativity degree.
Corresponding author: Rajat Kanti Nath.

degree or *commuting probability* of R and it was introduced by MacHale [14] in the year 1976. Some characterizations of finite rings in terms of commutativity degree can be found in [14, 5, 6].

Throughout the paper R denotes a finite ring possibly non-associative and non-unital. For any subring S of R, R/S and $\frac{R}{S}$ denote the additive quotient group and $|R : S|$ denotes the index of the additive subgroup S in the additive group R. Note that the isomorphisms considered are the additive group isomorphisms. Also for any two non-empty subsets A and B of a ring R, we write $A + B = \{a + b : a \in A, b \in B\}$. We shall use the fact that for any non-commutative ring R, the additive group $\frac{R}{Z(R)}$ is not a cyclic group (see [14, Lemma 1]).

2 Some computations of $|\operatorname{Cent}(R)|$

In this section, we compute $|\operatorname{Cent}(R)|$ for some classes of finite rings. However, first we prove some results which are useful for subsequent results as well as for the next sections.

Proposition 2.1. *R is a commutative ring if and only if R is a 1-centralizer ring.*

Proof. The proposition follows from the fact that a ring R is commutative if and only if $C(r) = R$ for each $r \in R$. □

Proposition 2.2. *Let R, S be two rings. Then*

$$\operatorname{Cent}(R \times S) = \operatorname{Cent}(R) \times \operatorname{Cent}(S).$$

Proof. It can be easily seen that $C((r, s)) = C(r) \times C(s)$ for any $r \in R$ and $s \in S$. This proves the proposition. □

The following lemmas play an important role in finding lower bound of $|\operatorname{Cent}(R)|$ for any non-commutative ring R.

Lemma 2.1. *Let R be a ring. Then $Z(R)$ is the intersection of all centralizers in R.*

Proof. It is clear that $Z(R) \subseteq \bigcap_{r \in R} C(r)$. Now, for any $s \in \bigcap_{r \in R} C(r)$ we have $rs = sr$ for all $r \in R$. Therefore $s \in Z(R)$. Hence the lemma follows. □

Lemma 2.2. *If R is a ring, then R is the union of centralizers of all non-central elements of R.*

Proof. It is clear that $\bigcup_{r \in R - Z(R)} C(r) \subseteq R$. Again, for any $s \in Z(R)$, we have by Lemma 2.1, $s \in C(r)$ for all $r \in R$. So $s \in \bigcup_{r \in R - Z(R)} C(r)$. Also for any $s \in R - Z(R)$, we have $s \in C(s)$ and so $s \in \bigcup_{r \in R - Z(R)} C(r)$. Hence the lemma follows. □

Lemma 2.3. *A ring R cannot be written as a union of two of its proper subrings.*

Proof. The lemma follows from the well-known fact that a group can not be written as a union of two of its proper subgroups. □

Theorem 2.1. *For any non-commutative ring R, $|\operatorname{Cent}(R)| \geq 4$.*

Proof. Since R is non-commutative, so $|\operatorname{Cent}(R)| \geq 2$. If $|\operatorname{Cent}(R)| = 2$, then, by Lemma 2.2, R is equal to a proper subset of itself, which is not possible. Also by Lemma 2.3, $|\operatorname{Cent}(R)| \neq 3$. Hence the theorem follows. □

Note that the ring $R = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \right\}$, where $0, 1 \in \mathbb{Z}_2$, has 4 distinct centralizers. So the above result is the best one possible.

At this point, the following question, similar to the question posed by Belcastro and Sherman [3, p. 371], arises naturally.

Question 2.2. Does there exist an n-centralizer ring for any positive integer $n \neq 2, 3$? Can we characterize an n-centralizer ring?

The following results show the existence of n-centralizer rings for some values of n.

Proposition 2.3. *There exists a $(p + 2)$-centralizer ring for any prime p.*

Proof. We consider the ring

$$R = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} : a, b \in \mathbb{Z}_p \right\}.$$

For any element $\begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix}$ of $C\left(\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}\right)$ we have $xb - ay = 0$.

Clearly, $C\left(\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}\right) = R$. Using simple calculations, we have for any $a \neq 0$ and $l \in \mathbb{Z}_p$,

$C\left(\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}\right) = \left\{ \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} : x \in \mathbb{Z}_p \right\}$ and $C\left(\begin{bmatrix} la & a \\ 0 & 0 \end{bmatrix}\right) = \left\{ \begin{bmatrix} lx & x \\ 0 & 0 \end{bmatrix} : x \in \mathbb{Z}_p \right\}$.

Hence $|\operatorname{Cent}(R)| = p + 2$. □

The above proposition is a particular case of the following theorem.

Theorem 2.3. *Let R be a non-commutative ring of order p^2, where p is a prime. Then $|\operatorname{Cent}(R)| = p + 2$.*

Proof. For any $x \in R - Z(R)$, we consider $C(x)$. As $C(x)$ is an additive subgroup of R we have $|C(x)| = 1, p$ or p^2. Clearly, $|C(x)| \neq 1, p^2$, as $x, 0_R \in C(x)$ and R is non-commutative, where 0_R is the additive identity in R. Hence $C(x)$ is additive cyclic group of order p and so $Z(R) = \{0_R\}$.

Let $x, y \in R - Z(R)$. If there exists an element $t\ (\neq 0_R) \in C(x) \cap C(y)$ then $C(x) = C(y)$, as $C(x), C(y)$ are additive cyclic groups of order p. Thus for any $x, y \in R - Z(R)$ we have either $C(x) \cap C(y) = \{0_R\}$ or $C(x) = C(y)$. Therefore the number of centralizers of non-central elements is

$$\frac{|R| - |Z(R)|}{p - 1} = \frac{p^2 - 1}{p - 1} = p + 1.$$

Hence $|\operatorname{Cent}(R)| = p + 2$. □

Theorem 2.4. *Let p be a prime number and R be a non-commutative ring of order p^3 with unity 1_R. Then* $|\operatorname{Cent}(R)| = p + 2$.

Proof. Let x be an arbitrary element of $R - Z(R)$. Then $C(x)$ is an additive subgroup of R and so $|C(x)| = 1, p, p^2$ or p^3. Here $|C(x)| \neq 1, p^3$ as $x, 0_R \in C(x)$, where 0_R is the additive identity in R and R is non-commutative. If $|C(x)| = p$ then $|Z(R)| = 1$, which is not possible as $0_R, 1_R \in Z(R)$. So $|C(x)| = p^2$ and this gives $|Z(R)| = p$.

Now, we suppose that $y \in R - Z(R)$ and $y \in C(x)$. Let $z \in C(x)$ be an arbitrary element. We know that $Z(R) \subset Z(C(x))$ and so $|Z(C(x))| > 1$. Therefore $|C(x) : Z(C(x))| = 1$ or p and so $C(x)$ is commutative. Thus $z \in C(y)$, as $y \in C(x)$. So $C(x) \subseteq C(y)$. Also $|C(x)| = |C(y)|$. Hence, $C(x) = C(y)$; and if $y \notin C(x)$ then $C(x) \cap C(y) = Z(R)$. Therefore the number of centralizers of non-central elements of R is

$$\frac{|R| - |Z(R)|}{|C(x)| - |Z(R)|} = \frac{p^3 - p}{p^2 - p} = p + 1.$$

Thus $|\operatorname{Cent}(R)| = p + 2$. □

As an application of the above theorem, it follows that the ring

$$R = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, b, c \in \mathbb{Z}_p \right\}$$

having order p^3 is a $(p + 2)$-centralizer ring. The following theorem, which is a generalization of Theorem 2.3, gives another class of $(p + 2)$-centralizer rings .

Theorem 2.5. *Let R be a ring and $\frac{R}{Z(R)} \cong \mathbb{Z}_p \times \mathbb{Z}_p$, where p is a prime. Then* $|\operatorname{Cent}(R)| = p + 2$.

Proof. We write $Z := Z(R)$. Since $R/Z \cong \mathbb{Z}_p \times \mathbb{Z}_p$ we have

$$\frac{R}{Z} = \langle Z + a, Z + b \ : \ p(Z + a) = p(Z + b) = Z; a, b \in R\rangle.$$

If S/Z is additive non-trivial subgroup of R/Z then $|S/Z| = p$. Therefore any additive proper subgroup of R properly containing Z has p disjoint right cosets. Hence the proper additive subgroups of R properly containing Z are

$$\begin{aligned}
S_m &= Z \cup (Z + (a + mb)) \cup (Z + 2(a + mb)) \cup \cdots \cup (Z + (p-1)(a + mb)),\\
&\quad \text{where } 1 \le m \le (p-1),\\
S_p &= Z \cup (Z + a) \cup (Z + 2a) \cup \cdots \cup (Z + (p-1)a) \text{ and}\\
S_{p+1} &= Z \cup (Z + b) \cup (Z + 2b) \cup \cdots \cup (Z + (p-1)b).
\end{aligned}$$

Now for any $x \in R - Z$, we have $Z + x$ is equal to $Z + k$ for some $k \in \{ma, mb, a + mb, 2(a + mb), \dots, (p-1)(a+mb) : 1 \le m \le (p-1)\}$. Therefore $C(x) = C(k)$. Again, let $y \in S_j - Z$ for some $j \in \{1, 2, \dots, (p+1)\}$, then $C(y) \ne S_q$, where $1 \le q\ (\ne j) \le (p+1)$. Thus $C(y) = S_j$. Hence $|\operatorname{Cent}(R)| = p + 2$. □

Further, we have the following theorem analogous to Lemma 2.7 of [1, p. 142].

Theorem 2.6. *Let R be a non-commutative ring whose order is a power of a prime p. Then $|\operatorname{Cent}(R)| \ge p + 2$, and equality holds if and only if $\frac{R}{Z(R)} \cong \mathbb{Z}_p \times \mathbb{Z}_p$.*

Proof. Let R be a non-commutative ring whose order is a power of a prime p. Suppose $k = |\operatorname{Cent}(R)|$. Let $A_1, \dots, A_k$ be the distinct centralizers of R such that $|A_1| \ge \cdots \ge |A_k|$ and $A_1 = R$. So $R = \bigcup\limits_{i=2}^{k} A_i$ and by Cohn's Theorem in [7, p. 44], we have $|R| \le \sum\limits_{i=3}^{k} |A_i|$ (as A_i's are additive groups). Also $|A_i| \le \frac{|R|}{p}$, where $i \ne 1$. Hence

$$|R| \le \underbrace{\frac{|R|}{p} + \cdots + \frac{|R|}{p}}_{(k-2)-\text{times}}$$

which implies $|R| \le (k-2)\frac{|R|}{p}$ and so $k \ge p + 2$. That is $|\operatorname{Cent}(R)| \ge p + 2$.

For the equality, if $\frac{R}{Z(R)} \cong \mathbb{Z}_p \times \mathbb{Z}_p$ then by Theorem 2.5, we have $|\operatorname{Cent}(R)| = p+2$. Conversely, we assume that $l = |\operatorname{Cent}(R)| = p + 2$. Suppose $A_1, A_2, \dots, A_l$ are distinct centralizers of R such that $|A_1| \ge \cdots \ge |A_l|$ and $A_1 = R$. So $R = \bigcup\limits_{i=2}^{l} A_i$ and by Cohn's Theorem in [7, p.

44], we have $|R| \leq \sum_{i=3}^{l}|A_i|$. Also $|A_i| \leq \frac{|R|}{p}$, where $i \neq 1$. Suppose, there exists an A_i such that $|A_i| < \frac{|R|}{p}$ for $3 \leq i \leq l$ then

$$|R| < \underbrace{\frac{|R|}{p} + \cdots + \frac{|R|}{p}}_{(l-2)-\text{times}} = (l-2)\frac{|R|}{p} = |R|,$$

a contradiction. Hence $|A_3| = \frac{|R|}{p}, \dots, |A_l| = \frac{|R|}{p}$. Also $|A_2| \geq \cdots \geq |A_l|$, so $|A_i| = \frac{|R|}{p}$, where $2 \leq i \leq l$. Hence $\sum_{i=3}^{l}|A_i| = (l-2)\frac{|R|}{p} = |R|$. Therefore $\sum_{i=3}^{l}|A_i| = |R|$ if and only if $A_2 + A_m = R$, for all $m \neq 2$ and $A_k \cap A_l \subseteq A_2$ for all $k \neq l$ (By Cohn's Theorem in [7, p. 44]). Interchanging A_i's we have $A_2 \cap A_3 = Z(R)$. Thus

$$|R| = |A_2 + A_3| = \frac{|A_2||A_3|}{|A_2 \cap A_3|} = \frac{|R|^2}{p^2|Z(R)|}$$

which gives $|R : Z(R)| = p^2$. Hence $\frac{R}{Z(R)} \cong \mathbb{Z}_p \times \mathbb{Z}_p$, since R is non-commutative. This completes the proof. □

3 4-centralizer rings

In this section, we give a characterization of finite 4-centralizer rings analogous to Theorem 2 of [3, p. 367]. The following lemma is useful in characterization of 4-centralizer rings.

Lemma 3.1. *Let R be a 4-centralizer finite ring. Then at least one of the centralizers of non-central elements has index 2 in R.*

Proof. Let A, B, C be the three proper centralizers of R. Suppose none of A, B, C has index 2, that is $|R : A| \geq 3, |R : B| \geq 3, |R : C| \geq 3$. Then as $R = A \cup B \cup C$, we have

$$|R| \leq |A| + |B| + |C| - 2|Z(R)| \leq \frac{|R|}{3} + \frac{|R|}{3} + \frac{|R|}{3} - 2|Z(R)| < |R|,$$

which is a contradiction. Hence the lemma follows. □

We have the following characterization of finite 4-centralizer rings.

Theorem 3.1. *Let R be a non-commutative finite ring. Then $|\operatorname{Cent}(R)| = 4$ if and only if $\frac{R}{Z(R)} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.*

Proof. If $\frac{R}{Z(R)} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ then by Theorem 2.5, we have $|\operatorname{Cent}(R)| = 4$.

Conversely, let $|\operatorname{Cent}(R)| = 4$ then R has exactly four distinct centralizers, say R, A, B, C where A, B, C are three distinct centralizers of non-central elements of R.

By Lemma 2.3, R can not be written as the union of two of its proper subrings of R. Therefore we may choose $a \in A - (B \cup C)$, $b \in B - (C \cup A)$ and $c \in C - (A \cup B)$ respectively. It can be easily seen that $C(a) = A$, $C(b) = B$ and $C(c) = C$. By Lemma 3.1, at least one of the centralizers A, B, C, say A has index 2 in R, that is $|R : A| = 2$.

Now, let $x \in (A \cap B) - Z(R)$ then $C(x) \neq R$. If $C(x) = A$ then $a, b \in C(x)$. So, $C(x) \neq A$. Similarly it can be seen that $C(x) \neq B$. If $C(x) = C$ then $x \in A \cap B \cap C = Z(R)$ (using Lemma 2.1), which is a contradiction. Therefore $|\operatorname{Cent}(R)|$ must be at least 5, which is again a contradiction. So $A \cap B = A \cap B \cap C = Z(R)$. Similarly it can be seen that $B \cap C = Z(R)$, $A \cap C = Z(R)$. Again A, B, C are additive subgroups of R, therefore

$$|R| \geq |A + B| = \frac{|A||B|}{|A \cap B|} = \frac{|A||B|}{|Z(R)|}$$

which gives $|B| \leq 2|Z(R)|$. Since $Z(R) \subset B$, so $\frac{|B|}{2} \leq |Z(R)| < |B|$. Hence $|B| = 2|Z(R)|$. Similarly $|C| = 2|Z(R)|$. Therefore

$$|R| = |A| + |B| + |C| - 2|Z(R)| = \frac{|R|}{2} + 2|Z(R)|$$

which gives $|R : Z(R)| = 4$ and hence $\frac{R}{Z(R)} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. □

4 5-centralizer rings

In this section, we give a characterization of finite 5-centralizer rings analogous to Theorem 4 of [3, p. 369]. The following lemmas are useful in this regard.

Lemma 4.1. *Let R be a ring and $R = A \cup B \cup C$, where A, B, C are the proper distinct subrings. We put $K = A \cap B \cap C$, $L = A \cap B - K$, $M = A \cap C - K$, $N = B \cap C - K$ and $A' = A - (B \cup C)$, $B' = B - (A \cup C)$, $C' = C - (A \cup B)$. Then*

(a) $L = M = N = \emptyset$,

(b) $A' + B' \subseteq C'$, $B' + C' \subseteq A'$ *and* $C' + A' \subseteq B'$,

(c) $A' + A' \subseteq K$, $B' + B' \subseteq K$ *and* $C' + C' \subseteq K$,

(d) $|R : K| = 4$.

Proof. (a) We consider $l \in L$ and $c' \in C'$. Then $c' + l \in A$ or B or C. If $c' + l \in A$ then $c' + l + (-l) = c' \in A$, a contradiction. If $c' + l \in B$ then $c' + l + (-l) = c' \in B$, a contradiction. If $c' + l \in C$ then $(-c') + c' + l = l \in C$, a contradiction. Since $C' \neq \emptyset$, we must have $L = \emptyset$. Similarly $M = N = \emptyset$.

(b) Let $a' \in A'$, then $a' \in A \Rightarrow -a' \in A \Rightarrow -a' \in K$ or A'. If $-a' \in K$ then $a' \in K$, a contradiction. Hence $-a' \in A'$. Similarly if $b' \in B'$ then $-b' \in B'$ and if $c' \in C'$ then $-c' \in C'$. Suppose $a' \in A', b' \in B'$ then $a' + b' \in K$ or A' or B' or C'. If $a' + b' \in A' \subseteq A$ then $b' = -a' + a' + b' \in A$, a contradiction. If $a' + b' \in B' \subseteq B$, then $a' = a' + b' + (-b') \in B$, a contradiction. If $a' + b' \in K$, then $a' + b' \in A$, a contradiction. Hence $a' + b' \in C'$. Thus $A' + B' \subseteq C'$. Similarly it can be seen that $B' + C' \subseteq A'$ and $C' + A' \subseteq B'$.

(c) Let $a', {a_1}' \in A' \subseteq A$. So $a' + {a_1}' \in A \Rightarrow\ a' + {a_1}' \in A'$ or K. Let $a' + {a_1}' \in A'$. We consider $b' + a' + {a_1}'$, for some $b' \in B'$. Then by second part we have $b' + (a' + {a_1}') \in C'$ and $(b' + a') + {a_1}' \in B'$. So $b' + a' + {a_1}' \in B' \cap C'$, a contradiction. Similarly we can show the other two.

(d) From part (a), we have $R = K \cup A' \cup B' \cup C'$. Let $k + a' \in K + a'$ where $k \in K, a' \in A'$ then $k + a' \in A = K \cup A'$. If $k + a' \in K$ then $a' \in K$, a contradiction. So $K + a' \subseteq A'$. Again $x' \in A'$ gives $x' + (-a') \in K$ (by part (c)). So, $x' \in K + a'$. Hence $K + a' = A'$. Similarly it can be seen that $K + b' = B', K + c' = C'$, where $b' \in B', c' \in C'$. Therefore $|R : K| = 4$. □

Lemma 4.2. *Let R be a 5-centralizer finite ring and A, B, C, D be the four proper centralizers of R. Then*

(a) $|R| = |A| + |B| + |C| + |D| - 3|Z(R)|$.

(b) *If S and T are distinct proper centralizers of R, then*

$$\frac{|S||T|}{|R|} \leq |Z(R)| \leq \frac{|R|}{6}.$$

Proof. Let $a \in A - (B \cup C), b \in B - (A \cup C)$ and $c \in C - (A \cup B)$. Suppose there does not exist any $a \in A - (B \cup C)$ such that $C(a) = A$. Then $C(a) = D$ for all $a \in A - (B \cup C)$. Therefore $A - (B \cup C) \subseteq D - (B \cup C)$. Interchanging the roles of A and D we get $A - (B \cup C) = D - (B \cup C)$, which gives $A \cup B \cup C = D \cup B \cup C = R$. Again, by Lemma 4.1(a), we have $B \cap C = C \cap D$ and so $Z(R) = A \cap B \cap C$. Therefore, by Lemma 4.1(d), we have $R/Z(R) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. This gives $|\operatorname{Cent}(R)| = 4$, contradiction. Hence $C(a) = A$. Similarly $C(b) = B$ and $C(c) = C$.

(a) Let us assume without loss of generality that D is a subset of $A \cup B \cup C$. Then $R = A \cup B \cup C \cup D = A \cup B \cup C$. Now, by Lemma 4.1, we have $|R : K| = 4$ where $K = A \cap B \cap C = Z(R)$. Thus by Theorem 3.1, $|\operatorname{Cent}(R)| = 4$, which is a contradiction. Therefore no one of A, B, C or D is contained in the union of the other three.

Let $r \in (A \cap B) - (C \cup D)$ then $r \in C(a) \cap C(b)$ which gives $a, b \in C(r)$. But $a \notin C(b)$, so $C(r) \neq A, B$. Again $r \notin C, D$; so $C(r) \neq C, D$. Also $C(r) \neq R$, since $r \in R - Z(R)$. Therefore $|\operatorname{Cent}(R)|$ must be at least 6, a contradiction. Hence $(A \cap B) - (C \cup D) = \emptyset$. This shows that no element of R is in exactly two proper centralizers.

Let $r \in (A \cap B \cap C) - D$ then $r \in C(a) \cap C(b) \cap C(c)$. Therefore $a, b, c \in C(r)$. But $b \notin C(a), c \notin C(b)$. So $C(r) \neq A, B, C$. Also $C(r) \neq D, R$; as $r \notin D$ and $r \notin Z(R)$. Therefore $|\operatorname{Cent}(R)|$ must be at least 6, a contradiction. Hence $A \cap B \cap C - D = \emptyset$. Thus no element of R is in exactly three proper centralizers.

From above, it can be seen clearly that

$$|R| = |A \cup B \cup C \cup D| = |A| + |B| + |C| + |D| - 3|Z(R)|.$$

(b) Note that for any two proper centralizers S and T of R we have $S \cap T = Z(R)$, since no element of R is in exactly two as well as three proper centralizers. Also any proper centralizers of R are additive subgroups of R, so $\frac{|S||T|}{|S+T|} = |S \cap T| = |Z(R)|$. Since $S + T \subseteq R$ we have $|Z(R)| \geq \frac{|S||T|}{|R|}$.

Again by part (a),

$$\begin{aligned} |R| &= |A| + |B| + |C| + |D| - 3|Z(R)| \\ &\geq 2|Z(R)| + 2|Z(R)| + 2|Z(R)| + 2|Z(R)| - 3|Z(R)|. \end{aligned}$$

Thus $|R : Z(R)| \geq 5$. If $|R : Z(R)| = 5$ then $\frac{R}{Z(R)} \cong \mathbb{Z}_5$, a contradiction. Therefore $|Z(R)| \leq \frac{|R|}{6}$. So, $\frac{|S||T|}{|R|} \leq |Z(R)| \leq \frac{|R|}{6}$. □

We would like to mention here that the group theoretic analogues of Lemma 4.1 and Lemma 4.2 can be found in [4, p. 52-53] and [3, p. 370] respectively. Now we prove the main theorem of this section which characterizes finite 5-centralizer rings.

Theorem 4.1. *Let R be a finite ring. Then $|\operatorname{Cent}(R)| = 5$ if and only if $\frac{R}{Z(R)} \cong \mathbb{Z}_3 \times \mathbb{Z}_3$.*

Proof. Let $\frac{R}{Z(R)} \cong \mathbb{Z}_3 \times \mathbb{Z}_3$, then by Theorem 2.5, we get $|\operatorname{Cent}(R)| = 5$.

Conversely, let $|\operatorname{Cent}(R)| = 5$. Let A, B, C, D be the four proper centralizers of R. Then by Lemma 4.2(b), $\frac{|A||B|}{|R|} \leq |Z(R)| \leq \frac{|R|}{6}$. Our aim is to get more near lower bound for $|Z(R)|$. We may assume without loss of generality that $|A| \geq |B| \geq |C| \geq |D|$. Suppose $|A| < \frac{|R|}{3}$, as $1 < |A| \leq \frac{|R|}{2}$. That is $|A| \leq \frac{|R|}{4}$. Now by Lemma 4.2(a), $|R| \leq |R| - 3|Z(R)| < |R|$, a contradiction. Hence $|A| = \frac{|R|}{2}$ or $|A| = \frac{|R|}{3}$. If $|A| = \frac{|R|}{2}$, then $|R| = |A| + |B| + |C| + |D| - 3|Z(R)|$ gives $\frac{|R|}{2} < |B| + |C| + |D|$ and so $\frac{|R|}{6} < |B|$. Also, applying Lemma 4.2(b) on A and B we have $\frac{|R|}{6} < |B| \leq \frac{|R|}{3}$. So $|B|$ is one of $\frac{|R|}{3}$, $\frac{|R|}{4}$ or $\frac{|R|}{5}$. Reapplying Lemma 4.2(b) on A and B we have,

$$\frac{|A||B|}{|R|} \leq |Z(R)| \leq \frac{|R|}{6}$$

which gives $\frac{|R|}{10} \leq |Z(R)| \leq \frac{|R|}{6}$. Thus $|Z(R)|$ is one of $\frac{|R|}{6}, \frac{|R|}{7}, \frac{|R|}{8}, \frac{|R|}{9}$ or $\frac{|R|}{10}$. Let $|Z(R)| = \frac{|R|}{7}, \frac{|R|}{9}$ then 2 divides 7 and 9, which is not possible. If $|Z(R)| = \frac{|R|}{6}$ then $\frac{R}{Z(R)} \cong \mathbb{Z}_6$, a contradiction. Let $|Z(R)| = \frac{|R|}{8}$ then $\frac{|R|}{8}$ divides $|B|$. If $|B| = \frac{|R|}{3}, \frac{|R|}{5}$ then $3, 5$ divides 8, a contradiction. Therefore $|B| = \frac{|R|}{4}$. By Lemma 4.2(a), we have $\frac{5|R|}{8} = |C| + |D|$. Also $|B| \geq |C| \geq |D|$. So $|C| + |D| \leq \frac{|R|}{2} < \frac{5|R|}{8} = |C| + |D|$, a contradiction. If $|Z(R)| = \frac{|R|}{10}$, then $\frac{|R|}{10}$ divides $|B|$. If $|B| = \frac{|R|}{3}, \frac{|R|}{4}$ then $3, 4$ divides 10, a contradiction. Therefore $|B| = \frac{|R|}{5}$. Now Lemma 4.2(a) gives, $|C| + |D| = \frac{6|R|}{10}$. Also $|B| \geq |C| \geq |D|$, therefore $|C| + |D| \leq \frac{2|R|}{5} < \frac{6|R|}{10} = |C| + |D|$, a contradiction.

If $|A| = \frac{|R|}{3}$ then Lemma 4.2(a) gives, $\frac{2|R|}{3} < |B| + |C| + |D|$ which gives $\frac{2|R|}{3} < 3|B|$ and so $|B| \geq \frac{|R|}{4}$. Also $|A| \geq |B|$, so $|B| = \frac{|R|}{3}$ or $\frac{|R|}{4}$. Again, applying Lemma 4.2(b) on A and B we get,

$$\frac{|A||B|}{|R|} \leq |Z(R)| \leq \frac{|R|}{6}$$

which gives $\frac{|R|}{12} \leq |Z(R)| \leq \frac{|R|}{6}$. Therefore $|Z(R)|$ is one of $\frac{|R|}{6}, \frac{|R|}{7}, \frac{|R|}{8}, \frac{|R|}{9}, \frac{|R|}{10}, \frac{|R|}{11}$ or $\frac{|R|}{12}$. Now if $|Z(R)| = \frac{|R|}{7}, \frac{|R|}{8}, \frac{|R|}{10}, \frac{|R|}{11}$ then 3 divides $7, 8, 10, 11$, a contradiction. Let $|Z(R)| = \frac{|R|}{6}$ then as above we get a contradiction. Let $|Z(R)| = \frac{|R|}{9}$ then $\frac{R}{Z(R)} \cong \mathbb{Z}_3 \times \mathbb{Z}_3$. Let $|Z(R)| = \frac{|R|}{12}$ and $|B| = \frac{|R|}{3}$ then applying Lemma 4.2(b) on A and B we have, $\frac{|R|}{9} \leq \frac{|R|}{12}$, a contradiction. If $|B| = \frac{|R|}{4}$ then Lemma 4.2(a) gives, $|C| + |D| = \frac{4|R|}{6}$. Also $|C|, |D| \leq \frac{|R|}{4}$, so $|C| + |D| \leq \frac{3|R|}{6} < \frac{4|R|}{6} = |C| + |D|$, which is not possible. Hence $\frac{R}{Z(R)} \cong \mathbb{Z}_3 \times \mathbb{Z}_3$. □

5 Relation between $|\operatorname{Cent}(R)|$ and $d(R)$

Note that $d(R) = 1$ if and only if R is commutative. Therefore, by Proposition 2.1, we have $|\operatorname{Cent}(R)| = 1$ if and only if $d(R) = 1$. By Theorem 3.1 and Theorem 1 of [14, p. 31], we have the following result.

Proposition 5.1. *Let R be a non-commutative finite ring. Then $|\operatorname{Cent}(R)| = 4$ if and only if $d(R) = \frac{5}{8}$.*

In [14, p. 31], MacHale also proved the following theorem:

Theorem 5.1. *Let R be a non-commutative finite ring and p the smallest prime dividing the order of R. Then $d(R) \leq \frac{1}{p^3}(p^2 + p - 1)$, with equality if and only if $|R : Z(R)| = p^2$.*

Now by Theorem 2.5 and Theorem 5.1, we have the following interesting connection between $d(R)$ and $|\operatorname{Cent}(R)|$.

Proposition 5.2. *Let R be a non-commutative finite ring and p the smallest prime dividing the order of R. If $d(R) = \frac{1}{p^3}(p^2 + p - 1)$ then $|\operatorname{Cent}(R)| = p + 2$.*

We conclude the paper by noting that the converse of Proposition 5.2 holds for some finite non-commutative rings. In particular, by Theorem 2.6 and Theorem 5.1, we have the following result.

Proposition 5.3. *Let R be a non-commutative ring whose order is a power of a prime p. If* $|\operatorname{Cent}(R)| = p + 2$ *then* $d(R) = \frac{1}{p^3}(p^2 + p - 1)$.

Acknowledgments

The authors would like to thank the referee for his/her valuable comments and suggestions. The first author is grateful to the Department of Mathematical Sciences, Tezpur University for its support while this investigation was carried out as a part of her Ph. D. thesis.

References

[1] A. R. Ashrafi, On finite groups with a given number of centralizers, Algebra Colloq., **7** (2000), 139–146.

[2] M. Behboodi, R. Beyranvand, A. Hashemi and H. Khabazian, Classification of finite rings: theory and algorithm, Czechoslovak Math. J., **64** (2014), 641–658.

[3] S. M. Belcastro and G. J. Sherman, Counting centralizers in finite groups, Math. Magazine, **67** (1994), 366–374.

[4] M. Bruckheimer, A. C. Bryan and A. Muir, Groups which are the union of three subgroups, Amer. Math. Monthly, **77** (1970), 52–57.

[5] S. M. Buckley, D. MacHale and A. Ní Shé, Finite rings with many commuting pairs of elements. Available from: `http://archive.maths.nuim.ie/staff/sbuckley/Papers/bms.pdf`.

[6] S. M. Buckley and D. MacHale, Contrasting the commuting probabilities of groups and rings. Available from: `http://archive.maths.nuim.ie/staff/sbuckley/Papers/bm_g-vs-r.pdf`.

[7] J. H. E. Cohn, On n-sum groups, Math. Scand., **75** (1994), 44–58.

[8] C. J. Chikunji, A Classification of a certain class of completely primary finite rings, Ring and Module Theory, Trends in Mathematics 2010, Springer Basel, pp 83–90.

[9] J. Dutta, D. K. Basnet and R. K. Nath, A note on n-centralizer finite rings, An. Stiint. Univ. Al. I. Cuza Iasi. Mat. (N.S.), **LXIV** (2018), 161–171.

[10] J. B. Derr, G. F. Orr and P. S. Peck, Noncommutative rings of order p^4, J. Pure Appl. Algebra, **97** (1994), 109–116.

[11] K. E. Eldridge, Orders for finite noncommutative rings with unity, Amer. Math. Monthly, **75** (1968), 512–514.

[12] B. Fine, Classification of finite rings of order p^2, Math. Magazine, **66** (1993), 248–252.

[13] R. W. Goldbach and H. L. Claasen, Classification of not commutative rings with identity of order dividing p^4, Indag. Math., **6** (1995), 167–187.

[14] D. MacHale, Commutativity in finite rings, Amer. Math. Monthly, **83** (1976), 30–32.

[15] R. Raghavendran, A class of finite rings, Compositio Math., **22** (1970), 49–57.

Jutirekha Dutta Department of Mathematical Sciences, Tezpur University, Napaam-784028, Sonitpur, Assam, India.

E-mail: jutirekhadutta@yahoo.com

Dhiren Kumar Basnet Department of Mathematical Sciences, Tezpur University, Napaam-784028, Sonitpur, Assam, India.

E-mail: dbasnet@tezu.ernet.in

Rajat Kanti Nath Department of Mathematical Sciences, Tezpur University, Napaam-784028, Sonitpur, Assam, India.

E-mail: rajatkantinath@yahoo.com