Spring 2016

On The Number Of Distinct Cyclic Subgroups Of A Given Finite Group

Joseph Dillstrom

ON THE NUMBER OF DISTINCT CYCLIC SUBGROUPS OF A GIVEN FINITE GROUP

A Masters Thesis

Presented to

The Graduate College of

Missouri State University

In Partial Fulfillment

Of the Requirements for the Degree

Master of Science, Mathematics

By

Joseph A. Dillstrom

May 2016

ON THE NUMBER OF DISTINCT CYCLIC SUBGROUPS OF A GIVEN FINITE GROUP

Mathematics

Missouri State University, May 2016

Master of Science

Joseph A. Dillstrom

ABSTRACT

In the study of finite groups, it is a natural question to consider the number of distinct cyclic subgroups of a given finite group. Following an article by M. Tărnăuceanu in the *American Mathematical Monthly*, we consider arithmetic relations between the order of a finite group and the number of its cyclic subgroups. We classify several infinite families of finite groups in this fashion and expand upon an open problem posed in the article.

KEYWORDS: abstract algebra, group theory, finite group, cyclic subgroup, Lagrange's Theorem,

This abstract is approved as to form and content

Dr. Richard Belshoff
Chairperson, Advisory Committee
Missouri State University

ON THE NUMBER OF DISTINCT CYCLIC SUBGROUPS OF A GIVEN FINITE GROUP

By

Joseph A. Dillstrom

A Masters Thesis
Submitted to The Graduate College
Of Missouri State University
In Partial Fulfillment of the Requirements
For the Degree of Master of Science, Mathematics

May 2016

Approved:

Dr. Richard Belshoff, Chairperson

Dr. Les Reid, Member

Dr. Cameron Wickham, Member

Dr. Julie J. Masterson, Graduate College Dean

ACKNOWLEDGEMENTS

I would first like to thank Dr. Joseph Siler at OTC, who showed me the beauty of mathematics in a way that no one had before, and inspired me to pursue the subject as a field of study.

Second, I would like to thank my thesis advisor, Dr. Richard Belshoff, for his patience and for his kindness. The combination of his rigorous approach to the subject and his easygoing style of teaching were a perfect fit for the way I learn and he has been a very positive infuence. I would also like to thank Dr. Les Reid for his interest in the project and his feedback throughout.

Finally, I would like to thank my parents, whose affection and support mean the world to me.

TABLE OF CONTENTS

LIST OF TABLES

1. INTRODUCTION

In the study of finite groups, it is natural to consider their cyclic subgroup structure. Since every element generates a finite cyclic subgroup, determining the number of distinct cyclic subgroups of a given finite group G can give a sense of how many "transformations" of elements are possible within the group. In the *American Mathematical Monthly* article which served as the starting point for our research, M. Tărnăuceanu notes that this problem is relatively unexplored in the literature [1]. For groups of small order this can be accomplished relatively quickly by hand, but applying the same procedure to groups of large order can be computationally unfeasible.

In this spirit we characterize certain arithmetic relations between the order of a finite group $|G|$ and the number of its distinct cyclic subgroups $|C(G)|$. We also classify the cyclic subgroup structure of certain infinite families of finite groups. In particular we characterize the finite groups satisfying $|C(G)| = k$ for $k \in \{1, \ldots, 4\}$. We also supply alternative proofs of the theorems in the AMM article that characterize the finite groups satisfying $|C(G)| = |G|$ and $|C(G)| = |G| - 1$. We conclude by expanding the open problem posed by Tărnăuceanu to characterize the finite groups satisfying $|C(G)| = |G| - 2$.

2. BACKGROUND

In this section we will fix our notation and briefly review some properties of finite groups. Given a finite group G, we will use the notation $C(G)$ for the set of its cyclic subgroups, and we will use $|C(G)|$ for the cardinality of $C(G)$. We will denote a generic cyclic group of order n by C_n.

We begin by stating some results of cyclic groups that we will make use of throughout the paper. Since cyclic groups themselves are well understood, we state the results without proof. The statements of the results are taken from Dummit and Foote's *Abstract Algebra* [2].

PROPOSITION 2.1: Let $G = \langle x \rangle$. If $|x| = n < \infty$, then $|x^a| = \frac{n}{(n,a)}$, where $(n, a) = \gcd(n, a)$.

PROPOSITION 2.2: Assume that $H = \langle x \rangle$ is cyclic and $|x| = n < \infty$. Then $H = \langle x^a \rangle$ if and only if $(a, n) = 1$. In particular, the number of generators of H is $\phi(n)$, where $\phi(n)$ is Euler's phi-function.

PROPOSITION 2.3: Let H be a cyclic group. If $|H| = n < \infty$, then for each positive integer a dividing n there is a unique cyclic subgroup of H of order a. Furthermore, for every integer m, $\langle x^m \rangle = \langle x^{(n,m)} \rangle$, so that the subgroups of H correspond bijectively with the positive divisors of n. Thus, $|C(H)| = \tau(n)$, where $\tau(n)$ is the number of divisors function.

Two cornerstones of finite group theory are Lagrange's Theorem and Cauchy's Theorem. We make extensive use of both in our results and state them here without proof.

THEOREM 2.4: (Lagrange's Theorem) If G is a finite group and H is a subgroup of G, then the order of H divides the order of G, i.e. $|H| \mid |G|$.

Two useful corollaries of Lagrange's Theorem are as follows:

COROLLARY 2.5: If G is a finite group and $x \in G$, then the order of x divides the order of G.

COROLLARY 2.6: If G is a group of prime order p, then G is cyclic, hence $G \cong C_p$.

By Proposition 2.3, the converse of Lagrange's Theorem holds in a cyclic group. Thus, for a finite group G, if $H \leq G$ is a cyclic subgroup of order m with divisors $d_1, d_2, \ldots, d_k$, then H (hence G) contains cyclic subgroups C_i of orders d_i, $i \in \{1, \ldots, k\}$. We will occasionally make use of this observation when we need to establish a contradiction, so we record it here as a corollary.

COROLLARY 2.7: Let G be a finite group, H be a cyclic subgroup of G of order m, and $d_1, \ldots, d_k$ be the positive divisors of m. Then G contains cyclic subgroups C_{d_i}, $i \in \{1, \ldots, k\}$.

THEOREM 2.8: (Cauchy's Theorem) If G is a finite group and p is a prime dividing $|G|$, then G contains an element of order p.

The advantage of Cauchy's Theorem in our research is that we can guarantee a lower bound of $|C(G)|$ by considering the prime factorization of $|G|$. In certain instances this will allow us to narrow down the number of distinct prime powers of $|G|$ subject to certain assumptions about $|C(G)|$.

We also make use of the first part of Sylow's Theorem throughout our paper. The notation and statement of the theorem also come from Dummit and Foote [2].

DEFINITION 2.9: If G is a group of order $p^\alpha m$, where $p \nmid m$, then a subgroup of order p^α is called a *Sylow p-subgroup* of G. The number of Sylow p-subgroups of G will be denoted n_p.

THEOREM 2.10: (Sylow 1) Let G be a group of order $p^\alpha m$, $p \nmid m$. Then Sylow p-subgroups exist, i.e. $n_p \geq 1$.

We will also rely on certain results concerning semi-direct products and nor-

mal subgroups, and we will introduce these results as they become necessary.

3. LOWER END RESULTS FOR $|C(G)|$

We begin by considering the groups of order less than or equal to 10 (up to isomorphism). Since there are relatively few of these groups, we use them as a "baseline" for considering the subgroup structure of higher order groups in related families.

Table 1: Groups of small order (up to isomorphism)

$\lvert G\rvert$	# Of Groups	Isomorphism Type
1	1	$\langle e \rangle$
2	1	C_2
3	1	C_3
4	2	C_4, $C_2 \times C_2 \cong V_4$
5	1	C_5
6	2	C_6, $D_6 \cong S_3$
7	1	C_7
8	5	C_8, $C_4 \times C_2$, C_2^3, D_8, Q_8
9	2	C_9, $C_3 \times C_3$
10	2	C_{10}, D_{10}

Observe that nearly all groups (up to isomorphism) of order less than or equal to 10 are either cyclic, dihedral, or direct products of cyclic groups. The one outlier is the quaternion group Q_8. Since $|C(G)|$ for cyclic groups G is given by Proposition 2.3, we seek characterizations of $|C(G)|$ for direct products of cyclic groups and for the dihedral group D_{2n}. Our main objective is to characterize the finite groups satisfying $|C(G)| = k$ for $k \in \{1, \ldots, 4\}$. This will tell us which finite groups have relatively few cyclic subgroups and provide "lower end" results for $|C(G)|$.

By hand calculations we record $|C(G)|$ for these groups of small order and note the arithmetic relations between $|G|$ and $|C(G)|$ that arise in Table 2.

Table 2: Calculations and observations of $|C(G)|$

G	$\lvert C(G)\rvert$	Note
$\langle e \rangle$	1	$\lvert C(G)\rvert = 1$
C_2	2	$\lvert C(G)\rvert = \lvert G\rvert$
C_3	2	$\lvert C(G)\rvert = \lvert G\rvert - 1$
C_4	3	$\lvert C(G)\rvert = \lvert G\rvert - 1$
$C_2 \times C_2$	4	$\lvert C(G)\rvert = \lvert G\rvert$
C_5	2	$\lvert C(G)\rvert = 2$
C_6	4	$\lvert C(G)\rvert = \lvert G\rvert - 2$
$D_6 \cong S_3$	5	$\lvert C(G)\rvert = \lvert G\rvert - 1$
C_7	2	$\lvert C(G)\rvert = 2$
C_8	4	$\lvert C(G)\rvert = \frac{\lvert G\rvert}{2}$
$C_4 \times C_2$	6	$\lvert C(G)\rvert = \lvert G\rvert - 2$
C_2^3	8	$\lvert C(G)\rvert = \lvert G\rvert$
D_8	7	$\lvert C(G)\rvert = \lvert G\rvert - 1$
Q_8	5	$\lvert C(G)\rvert = \lvert G\rvert - 3$
C_9	3	$\lvert C(G)\rvert = \frac{\lvert G\rvert}{3}$
$C_3 \times C_3$	5	$\lvert C(G)\rvert = \lvert G\rvert - 4$
C_{10}	4	$\lvert C(G)\rvert = \lvert G\rvert - 6$
D_{10}	7	$\lvert C(G)\rvert = \lvert G\rvert - 3$

The groups of small order all seem to have similar arithmetic relations between their orders and their number of cyclic subgroups. In fact, we can easily dispense of the case when $|C(G)| = 1$.

PROPOSITION 3.1: Let G be a finite group. Then $|C(G)| = 1$ if and only if $G = \langle e \rangle$.

Proof. The reverse implication follows immediately by Lagrange's Theorem. For the converse, suppose that $|C(G)| = 1$. Then G must be the trivial group, for if G contained another element then it would generate a cyclic subgroup distinct from $\langle e \rangle$, contrary to hypothesis. □

From the table it appears that the only finite groups G satisfying $|C(G)| = 2$ are the cyclic groups of prime order. This is indeed the case.

PROPOSITION 3.2: Let G be a finite group. Then $|C(G)| = 2$ if and only if $G = C_p$ for some prime p.

Proof. ($\Leftarrow$) Let $G = C_p$ for some prime p. Then G is cyclic, so that every subgroup of G is cyclic, and by Lagrange's Theorem every cyclic group of order p has exactly two subgroups, namely $\langle e \rangle$ and G.

($\Rightarrow$) Suppose that $|C(G)| = 2$ and write $|G| = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Certainly $\langle e \rangle \in C(G)$. By Cauchy's Theorem there exist $x_1, \ldots, x_k \in G$ and $H_1, H_2, \ldots, H_k < G$, where $H_i = \langle x_i \rangle$ and $|H_i| = p_i$. Since G has only one nontrivial cyclic subgroup, it follows that G has only one prime factor, hence $|G| = p^\alpha$ for some prime p and $\alpha \in \mathbb{Z}^+$.

Now, the only nontrivial cyclic subgroup of G is of order p. By Lagrange, the possible orders of elements in G are $1, p, \ldots, p^{\alpha-1}, p^\alpha$. If there exists an element of order p^β, $\beta \in \{2, \ldots, \alpha\}$, then $|C(G)| > 2$ by Corollary 2.7, contrary to hypothesis. Then every nonidentity element of G has order p and must generate the same cyclic subgroup by hypothesis. Thus, $\alpha = 1$, so that $|G| = p$, or $G = C_p$ for some prime p.

This completes the proof. □

Observe that the only groups in Table 2 satisfying $|C(G)| = 3$ are cyclic groups of order p^2 for $p = 2, 3$. This fact holds for any prime p as we show below. The proof relies upon a corollary of the fact that any group of prime power order has a non-trivial center, which we state as a lemma without proof. It also relies on knowing $|C(C_p \times C_p)|$; we classify $|C(G)|$ for when G is the elementary abelian p-group C_p^n.

LEMMA 3.3: If $|G| = p^2$ for some prime p, then G is abelian. More precisely, G is isomorphic to either C_{p^2} or $C_p \times C_p$. [2]

LEMMA 3.4: Let p be prime. If $G = C_p^n$, then $|C(G)| = 2 + \sum_{k=1}^{n-1} p^k$.

Proof. Let $G = C_p \times C_p \cdots \times C_p$. Since G is an elementary abelian p-group, every nonidentity element has order p. Then G contains $p^n - 1$ elements of order p. Each resulting cyclic subgroup has order p and can therefore be generated by any of the $p - 1$ non-identity elements in the subgroup. Thus, the number of cyclic subgroups of order p in G is given by

$$\frac{p^n - 1}{p - 1} = \frac{(p-1)(p^{n-1} + \cdots + p + 1)}{p - 1} = 1 + p + \cdots + p^{n-1}.$$

Since the above sum does not include the trivial subgroup, it follows that $|C(G)| = 2 + p + \cdots + p^{n-1} = 2 + \sum_{k=1}^{n-1} p^k$. □

THEOREM 3.5: Let G be a finite group. Then $|C(G)| = 3$ if and only if $G = C_{p^2}$ for some prime p.

Proof. ($\Leftarrow$) Suppose that $G = C_{p^2}$ for some prime p. Then G is cyclic and has a unique cyclic subgroup for every divisor of p^2, and since $\tau(p^2) = 3$, it follows that $|C(G)| = 3$ by Proposition 2.3.

($\Rightarrow$) Suppose that $|C(G)| = 3$ and write $|G| = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. By Cauchy's Theorem there exist $x_1, x_2, \ldots, x_k \in G$ and $H_1, H_2, \ldots, H_k < G$, where $H_i = \langle x_i \rangle$

and $|H_i| = p_i$. Since each H_i is of prime order, each H_i is cyclic, and by hypothesis it follows that G has at most two prime factors, say p_1 and p_2, and at most two corresponding cyclic subgroups H_1 and H_2.

Case 1: $|G|$ has one prime factor.

If $|G|$ has only one prime factor, then $|G| = p^\alpha$ for some $\alpha \in \mathbb{Z}^+$. If $\alpha = 1$, then $|C(G)| = 2$ by Proposition 3.2. If $\alpha = 2$, then by Lemma 3.3 either $G = C_{p^2}$ or $G = C_p \times C_p$. If $G = C_{p^2}$ then $|C(G)| = 3$ by above. If $G = C_p \times C_p$ then by Lemma 3.4 $|C(G)| = p + 2$, and $p + 2 = 3 \iff p = 1$, a contradiction.

Suppose that $\alpha \geq 3$. By Cauchy there exists $x \in G$, $|x| = p$. There cannot exist an element of order p^β, $\beta \geq 3$ and $\beta \leq \alpha$, since then $|C(G)| \geq 4$. Thus every nonidentity element of G has order p or p^2. By hypothesis G has one remaining cyclic subgroup, say H, which then must have order p or p^2.

Consider $|H| = p$. Every nonidentity element not in $\langle x \rangle$ must be in H. Now

$$|G| - |\langle x \rangle| = p^\alpha - p = p(p^{\alpha-1} - 1).$$

Thus $|G| - |\langle x \rangle| = |H| - 1$, or $p(p^{\alpha-1} - 1) = p - 1$, which implies that $p \mid (p - 1)$, a contradiction.

Now consider $|H| = p^2$. Then by Cauchy there exists $y \in H$, $|y| = p$. If $x \neq y$, then $|C(G)| = 4$, a contradiction. If $x = y$, then $\langle x \rangle < H$, so that G contains $p^\alpha - p^2 = p^2(p^{\alpha-2} - 1)$ nonidentity elements not in H. There must always be such elements, since $|G| - |H| = 0 \iff p^\alpha - p^2 = 0 \iff p^\alpha = p^2 \iff \alpha = 2$, but $\alpha \geq 3$. Each of these elements generates a cyclic subgroup not contained in H. But H contains all the cyclic subgroups of G, a contradiction.

Case 2 $|G|$ has two prime factors.

Write $|G| = p_1^{\alpha_1} p_2^{\alpha_2}$. By Cauchy there exist $x, y \in G$ such that $|\langle x \rangle| = p_1$ and $|\langle y \rangle| = p_2$. Thus, $|C(G)| \geq 3$. We show that $|C(G)| > 3$. Consider $\langle xy \rangle$. Without

loss of generality suppose that $xy \in \langle x \rangle$. Then $xy = x^k$ for some $k \in \mathbb{Z}^+$. By cancellation $y = x^{k-1}$, so that $e = y^{p_2} = (x^{k-1})^{p_2}$, hence $|x^{k-1}| \mid p_2$. But $|x^{k-1}| = p_1$, so that $p_1 \mid p_2$, a contradiction. Thus $\langle xy \rangle \not\in \langle x \rangle$, so that $\langle xy \rangle \not< \langle x \rangle$. Similarly, $\langle xy \rangle \not< \langle y \rangle$, and therefore $|C(G)| \geq 4$.

In either case $|C(G)| = 3$ follows only when $G = C_{p^2}$.

This completes the proof. □

The case when $|C(G)| = 4$ is considerably more involved than the previous three results and relies upon two lemmas.

LEMMA 3.6: Let G be a group of order pq, where p and q are prime with $p < q$. There is only one subgroup of G of order q. [3]

LEMMA 3.7: All of the Sylow subgroups of a finite group are normal if and only if the group is isomorphic to the direct product of its Sylow subgroups. [4]

We are now ready to characterize which groups satisfy $|C(G)| = 4$.

THEOREM 3.8: Let G be a finite group. Then $|C(G)| = 4$ if and only if $G = C_2 \times C_2$, $G = C_{pq}$, or $G = C_{p^3}$.

Proof. ($\Leftarrow$) By Lemma 3.4 $|C(C_2 \times C_2)| = 4$, and by Proposition 2.3 $|C(C_{pq})| = \tau(pq) = 4$ and $|C(C_{p^3})| = \tau(p^3) = 4$.

($\Rightarrow$) Assume $|C(G)| = 4$ and write $n = |G| = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. By Cauchy's Theorem and the hypothesis we must have $k \leq 3$, so $|G| = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}$. We consider three cases.

Case 1: $|G| = p^\alpha$ ($|G|$ has one prime factor)

If $\alpha = 1$, then $G = C_p$ and $|C(G)| = 2$ by Proposition 3.2, a contradiction.

If $\alpha = 2$, then $|G| = p^2$ and by Lemma 3.3 G is abelian. Moreover $G \cong C_{p^2}$ or $G \cong C_p \times C_p$. If $G = C_{p^2}$, then $|C(G)| = 3$ by Theorem 3.5, a contradiction. If $G = C_p \times C_p$, then by Lemma 3.4 $|C(G)| = p + 2$, hence $|C(G)| = 4 \iff p = 2$, so that $G = C_2 \times C_2$.

If $\alpha = 3$, then $|G| = p^3$. If G is abelian, then G is isomorphic to one of C_{p^3}, $C_p \times C_{p^2}$, or $C_p \times C_p \times C_p$. If $G = C_p \times C_p \times C_p$, then $|C(G)| = 2 + p + p^2$ by Lemma 3.4, hence $|C(G)| = 4 \iff p + p^2 = 2 \iff p = 1$, a contradiction. If $G = C_p \times C_{p^2}$, write $G = \langle x \rangle \times \langle y \rangle$, where $|x| = p$ and $|y| = p^2$. Since $\langle y \rangle = C_{p^2}$, $\langle y \rangle$ contains an element of order p, say z. Then G has cyclic subgroups $\langle e \rangle$, $C_p \times \langle e \rangle = \langle (x, e) \rangle$, $\langle e \rangle \times C_p = \langle (e, z) \rangle$, $C_p \times C_p = \langle (x, z) \rangle$, and $\langle e \rangle \times C_{p^2} = \langle (e, y) \rangle$, hence $|C(G)| \geq 5$, a contradiction. If $G = C_{p^3}$, then $|C(G)| = 4$.

Now suppose that G is non-abelian. For $p = 2$, $G = D_8$ or $G = Q_8$. By Table 2, $|C(D_8)| = 7$ and $|C(Q_8| = 5$. For an odd prime p, by p. 179 of Dummit and Foote [2] there are precisely two non-abelian groups of order p^3 (up to isomorphism). The first is the Heisenberg Group over C_p, which has the presentation

$$\langle x, a, b \ \mid \ x^p = a^p = b^p = e, \ ab = ba, \ xax^{-1} = ab, \ xbx^{-1} = b \rangle.$$

Since $x, a, b \in G$ are distinct elements of order p it follows immediately that $|C(G)| \geq 4$. Consider $ab \in G$. If $ab \in \langle a \rangle$ or $ab \in \langle b \rangle$, then $ab = a^k$ or $ab = b^k$ for some $k \in \mathbb{Z}^+$, hence $b = a^{k-1}$ or $a = b^{k-1}$, a contradiction. Suppose then that $ab = x^k$ for some $k \in \mathbb{Z}^+$. Then by the presentation $x^k = ab \iff x^k = xax^{-1} \iff x^k = a$, a contradiction. Since a and b commute it follows that $\langle ab \rangle$ is a distinct cyclic subgroup of order p, hence $|C(G)| \geq 5$, a contradiction.

The other non-abelian group G of order p^3 has the presentation

$$\langle x, y \ \mid \ x^p = y^{p^2} = e, \ xyx^{-1} = y^{1+p} \rangle.$$

Let $z = y^p$. Then G has the cyclic subgroups $\langle e \rangle$, $\langle x \rangle$, $\langle z \rangle$, and $\langle y \rangle$, hence $|C(G)| \geq 4$. Consider $xy \in G$. Then $xy = x^k \iff y = x^{k-1}$, a contradiction, hence $xy \notin \langle x \rangle$. Similarly, for $k \in \{1, \ldots, p-1\}$, $xy = z^k \implies x = y^{pk-1} \in \langle y \rangle$, a contradiction. Also $xy = y^k \implies x = y^{k-1} \in \langle y \rangle$, a contradiction. Thus $\langle xy \rangle$ is a distinct cyclic

subgroup and $|C(G)| \geq 5$.

Now consider $|G| = p^\alpha$ for $\alpha \geq 4$. By Cauchy there exists $x \in G$, $|x| = p$. By hypothesis G cannot contain an element of order p^β, $\beta \geq 4$ and $\beta \leq \alpha$, since then $|C(G)| \geq 5$. Thus every nonidentity element has order p, p^2, or p^3.

Suppose that G contains an element of order p^3, say y. Then $\langle y \rangle = C_{p^3} < G$ and $|C(\langle y \rangle)| = 4$, so that by hypothesis $\langle y \rangle$ contains all the cyclic subgroups of G. There are then $p^\alpha - p^3 = p^3(p^{\alpha-3} - 1)$ (nonidentity) elements in G not contained in $\langle y \rangle$. Each of these elements generates a cyclic subgroup not contained in $\langle y \rangle$. But $\langle y \rangle$ contains all of the cyclic subgroups of G, a contradiction. Thus every nonidentity element of G has order p or p^2. The two remaining cyclic subgroups of G, say H and K, must then have orders of either p or p^2.

Subcase 1: $|H| = |K| = p$.

In this case the only nontrivial cyclic subgroups of G have order p. By hypothesis H, K, and $\langle x \rangle$ must intersect trivially (otherwise $|C(G)| < 4$), and every nonidentity element of G is contained in one of these cyclic subgroups. Thus, every nonidentity element of G has order p, so that G is the elementary abelian p-group C_p^α. Since $\alpha \geq 4$, by Lemma 3.4

$$|C(G)| = 2 + \sum_{k=1}^{\alpha-1} p^k = 2 + p + p^2 + p^3 \geq 16,$$

which is a contradiction.

Subcase 2: $|H| = p$, $|K| = p^2$ (Without loss of generality).

By Cauchy there exists $z \in K$, $|z| = p$. If $\langle z \rangle \neq \langle x \rangle$ or $\langle z \rangle \neq H$, then $|C(G)| = 5$, a contradiction. Thus $\langle z \rangle$ must be one of $\langle x \rangle$ or H. Without loss of generality suppose that $\langle z \rangle = H$. Then $H < K$. There are then $|G| - |K| - |\langle x \rangle| + 1$ nonidentity elements in G not contained in K or $\langle x \rangle$. Moreover, G must always

have such "leftover" elements, since

$$\begin{aligned} |G| - |K| - |\langle x \rangle| + 1 = 0 &\iff p^\alpha - p^2 - p + 1 = 0 \\ \iff p^\alpha - p^2 = p - 1 &\iff p(p^{\alpha-1} - p) = p - 1 \\ &\iff p \mid (p-1) \end{aligned}$$

a contradiction. Each of these elements generates a cyclic subgroup not contained in K or $\langle x \rangle$. But the cyclic subgroups of G are precisely those contained in K or $\langle x \rangle$. This is a contradiction.

Subcase 3: $|H| = |K| = p^2$

By hypothesis we must have that $H \neq K$. By Cauchy there exists $h \in H$, $k \in K$ such that $|h| = |k| = p$. If one of $\langle h \rangle$ or $\langle k \rangle$ equals $\langle x \rangle$ then $|C(G)| = 5$. If neither $\langle h \rangle$ nor $\langle k \rangle$ equals $\langle x \rangle$ then $|C(G)| = 6$. Therefore we must have that $\langle h \rangle = \langle k \rangle = \langle x \rangle$. It follows that $|H \cap K| = p$. There are then $|G| - |H| - |K| + |H \cap K|$ nonidentity elements in G not contained in H or K. There must always be such "leftover" elements, since

$$\begin{aligned} |G| - |H| - |K| + |H \cap K| = 0 &\iff p^\alpha - p^2 - p^2 + p = 0 \\ \iff p^\alpha - p^2 = p^2 - p &\iff p^2(p^{\alpha-2} - 1) = p(p-1) \iff \\ p(p^{\alpha-2} - 1) = (p-1) &\iff p \mid (p-1) \end{aligned}$$

a contradiction. Each of these elements generates a cyclic subgroup not contained in H or K. But the cyclic subgroups of G are precisely those contained in H or K. This is a contradiction.

To summarize Case 1, $|C(G)| = 4$ implies that $G = C_{p^3}$ or $G = C_2 \times C_2$.

Case 2: $|G| = p^\alpha q^\beta$ ($|G|$ has two prime factors)

Without loss of generality suppose that $p < q$. By Cauchy let $x, y \in G$ such that $|x| = p$, $|y| = q$. Observe that $\langle xy \rangle$ is a distinct cyclic subgroup from $\langle x \rangle$ or $\langle y \rangle$. Thus G has four distinct cyclic subgroups: $\langle x \rangle$, $\langle y \rangle$, $\langle xy \rangle$, and $\langle e \rangle$. By Sylow 1 there exist Sylow subgroups $A, B < G$ such that $|A| = p^\alpha$ and $|B| = q^\beta$. Let $a \in A$ and consider $\langle a \rangle$. Then $|a|$ must divide p^α, and since $|C(G)| = 4$ we must have that $\langle a \rangle = \langle x \rangle$. Since $a \in A$ is arbitrary it follows that $A = \langle x \rangle$. By a similar argument $B = \langle y \rangle$, hence $\alpha = \beta = 1$ and $|G| = pq$.

Either G is abelian or non-abelian. If G is abelian then by page 143 of Dummit and Foote [2] G is cyclic, so that $G = C_{pq}$ and $|C(G)| = \tau(pq) = 4$.

If G is non-abelian, let $x, y \in G$, where $|x| = p$, $|y| = q$. By Lemma 3.6 $\langle y \rangle$ is the unique cyclic subgroup of order q in G. Thus, $|C(G)| \geq 3$. Now, the cyclic subgroups $\langle x \rangle$ and $\langle y \rangle$ account for $p - 1$ and $q - 1$ distinct elements in G, respectively. Including the identity element this accounts for $(p - 1) + (q - 1) + 1 = p + q - 1$ distinct elements in G. There are then

$$pq - (p + q - 1) = pq - p - q + 1 = p(q - 1) - (q - 1) = (p - 1)(q - 1)$$

remaining elements in G which must be of order p. Each of these elements generates a cyclic subgroup which accounts for $p - 1$ distinct elements in the group. Thus there are $q - 1$ of these elements in G.

When $q = 2$, there exists 1 distinct cyclic subgroup of order p not equal to $\langle x \rangle$, hence $|C(G)| = 4$, but $q = 2$ implies that $p < 2$, a contradiction.

When $q = 3$, there are 2 distinct cyclic subgroups of order p in G not equal to $\langle x \rangle$, hence $|C(G)| = 5$, a contradiction.

For any prime $q > 3$, $q - 1 > 2$, hence $|C(G)| > 5$, a contradiction.

Thus in this case $|C(G)| = 4$ only when $G = C_{pq}$.

Case 3: $|G| = p^\alpha q^\beta r^\gamma$ ($|G|$ has three prime factors)

By Cauchy's Theorem again there exists $x, y, z \in G$ such that $|x| = p$, $|y| = q$, $|z| = r$, and by hypothesis G does not contain any more cyclic subgroups (excluding the trivial subgroup). By Sylow 1 there exist Sylow subgroups $A, B, C < G$ with $|A| = p^\alpha$, $|B| = q^\beta$, $|C| = r^\gamma$. Let $a \in A$ and consider $\langle a \rangle$. Then $|a|$ must divide p^α, so that $\langle a \rangle = \langle x \rangle$. Thus $A = \langle x \rangle$, and by similar arguments we obtain $B = \langle y \rangle$ and $C = \langle z \rangle$. Hence $|G| = pqr$. Now either all the Sylow subgroups are normal in G or at least one of the Sylow subgroups A, B, C is not normal in G. In the first case, by Lemma 3.7 G is isomorphic to the direct product of A, B, and C, hence $G \cong A \times B \times C = C_p \times C_q \times C_r$. Then G contains isomorphic copies of C_p, C_q, and C_r, hence $|C(G)| = 4$, but G also contains an isomorphic copy of $C_p \times C_q \cong C_{pq}$, hence $|C(G)| \geq 5$, a contradiction. For the second case, suppose without loss of generality that $A \not\trianglelefteq G$. Then $n_p \geq 2$, so that G contains a distinct Sylow p-subgroup from A, say D, where $|D| = p$. Then D is cyclic, hence $|C(G)| \geq 5$, a contradiction.

Thus $|C(G)| \neq 4$ when $|G|$ has three distinct prime factors.

This completes the proof. □

We conclude the first section with a classification of $|C(G)|$ for the dihedral group $G = D_{2n}$.

PROPOSITION 3.9: For all $n \in \mathbb{N}$, $|C(D_{2n})| = n + \tau(n)$.

Proof. Let $n \in \mathbb{N}$, and consider

$$D_{2n} = \langle r, s \mid r^n = s^2 = e,\ rs = sr^{-1} \rangle.$$

By the presentation of D_{2n}, $\langle s \rangle$ is a cyclic subgroup of order 2. Observe that for each $k \in \{1, 2, \ldots, n-1\}$, $\langle sr^k \rangle$ is a distinct cyclic subgroup of order 2. For, given

k,

$$(sr^k)^2 = sr^k sr^k = sr^k r^{-k} s = sr^0 s = s^2 = e.$$

Since each of the sr^k are distinct, it follows that there are $n-1$ cyclic subgroups of order 2 generated by the sr^k. Consider now the rotational subgroup $\langle r \rangle$. Since $\langle r \rangle \cong C_n$, it follows that the number of cyclic subgroups of $\langle r \rangle$ is equal to the number of cyclic subgroups of C_n. Then by Corollary 2.7 $|C(\langle r \rangle)| = \tau(n)$, so that

$$\begin{aligned} |C(D_{2n})| &= 1 + (n-1) + \tau(n) \\ &= n + \tau(n) \end{aligned}$$

which proves the claim. □

4. HIGHER END RESULTS FOR $|C(G)|$.

In this section we turn our attention to classifying which finite groups have a large number of cyclic subgroups relative to their order. M. Tărnăuceanu states a result for $|C(G)| = |G|$ in his paper, which we prove. We also supply an alternate proof of his result that characterizes the finite groups satisfying $|C(G)| = |G| - 1$. Finally, we expand the open problem in the paper by characterizing the finite groups satisfying $|C(G)| = |G| - 2$.

We begin by considering the case when the order of G and the number of distinct cyclic subgroups of G are equal. In this case every distinct element generates a distinct cyclic subgroup in G. By Table 1 it appears that the groups of small order satisfying $|C(G)| = |G|$ are the trivial group and the elementary abelian 2-groups $G = C_2^n$ for $n = 1, 2, 3$. In fact, the only finite groups satisfying $|C(G)| = |G|$ are precisely $G = \langle e \rangle$ and those in this infinite family, as we now prove.

THEOREM 4.1: Let G be a finite group. Then $|C(G)| = |G|$ if and only if $G = C_2^n$ for $n \in \mathbb{N} \cup \{0\}$.

Proof. ($\Leftarrow$) The result is obvious when $G = \langle e \rangle$. Let $G = C_2^n$ for some $n \in \mathbb{N}$. Then every nonidentity element of G has order 2, so that any two distinct elements in G generate distinct cyclic subgroups, hence $|C(G)| = |G|$.

($\Rightarrow$) Suppose that $|G| = |C(G)|$. Then the map $\psi : G \to C(G)$ defined by $\psi(x) = \langle x \rangle$ is a bijection. Let $x \in G$ and suppose that $m = |x| > 2$. For every positive integer m, $(m - 1, m) = 1$. Set $k = m - 1$ and $y = x^k = x^{-1}$. Observe that $x \neq y$ since $|x| = m > 2$. Then by Proposition 2.1 $|y| = \frac{m}{(k,m)} = m$, so that y also generates $\langle x \rangle$. But then $\psi(x) = \psi(y)$ and $x \neq y$, so that ψ is not a bijection, a contradiction. Thus $m \in \{1, 2\}$. If G contains no elements of order 2 then G is the trivial group. Otherwise, every nonidentity element of G has order 2.

Thus $G = C_2^n$, so that G is the elementary abelian 2-group. $\square$

It is simple to show that Theorem 4.1 is the maximal case in the relationship of $|C(G)|$ and $|G|$ for finite groups.

PROPOSITION 4.2: For every finite group G, $|C(G)| \leq |G|$.

Proof. Let G be a finite group and suppose that $|C(G)| > |G|$. Then the map $\phi : G \to C(G)$ defined by $\phi(x) = \langle x \rangle$ is not onto, so that there exists $H \in C(G)$ such that $\phi(g) \neq H$ for all $g \in G$. But H must be generated by some element in G. This is a contradiction. $\square$

We base our proof of the next two results on Tărnăuceanu's proof for the $|C(G)| = |G| - 1$ case. In order to do so, we isolate Tărnăuceanu's "set-up" of the problem as a remark.

REMARK 4.3: Let $|G| = n$ and $d_1 = 1, d_2, \ldots, d_k$ be the positive divisors of n. If $n_i = |\{H \in C(G) \mid |H| = d_i\}|$, $i \in \{1, 2, \ldots, k\}$, then $\sum_{i=1}^{k} n_i \, \phi(d_i) = n$, where $\phi(x)$ is Euler's phi function. [1]

The identity above holds since every element $x \in G$ generates a cyclic subgroup whose order d_i is one of the divisors of n by Proposition 2.3. Each cyclic subgroup has $\phi(d_i)$ generators by Proposition 2.2. Thus the total number of elements in G is equal to the sum of the number of distinct cyclic subgroups of order d_i $(i = 1, \ldots, k)$ times the number of generators of each subgroup.

Our proof also relies on three elementary results. The first result states that the order of an element in a finite group is invariant under conjugation. The second and third result, taken together, characterize when the product set HK of two subgroups $H, K < G$ is itself a subgroup of G.

PROPOSITION 4.4: Let G be a finite group and $x \in G$ with $|x| = n$. Then $|gxg^{-1}| = n \ \ \forall \, g \in G$.

Proof.

$$\begin{aligned}(gxg^{-1})^n &= gxg^{-1}gxg^{-1}\dots gxg^{-1} \\ &= gx(g^{-1}g)x(g^{-1}g)x(g^{-1}g)\dots(g^{-1}g)xg^{-1} \\ &= gx^ng^{-1} = gg^{-1} = e\end{aligned}$$

If $k < n$, then the calculation of $(gxg^{-1})^k$ upon cancellation will yield gx^kg^{-1}, so that the minimality of $|x| = n$ forces $|gxg^{-1}| = n$. □

PROPOSITION 4.5: If H and K are subgroups of a group G, then $HK < G$ if and only if $HK = KH$. [2]

COROLLARY 4.6: If $H, K < G$ and one of H or K are normal in G then $HK < G$.

Proof. (Corollary 4.6) Without loss of generality consider $H \trianglelefteq G$. Then $gH = Hg$ for all $g \in G$, so that upon restriction to elements in K, $kH = Hk$ for all $k \in K$, or $KH = HK$. □

We now present an alternate proof characterizing the finite groups G satisfying $|C(G)| = |G| - 1$. Our proof follows Tărnăuceanu's own up until the bullet points.

THEOREM 4.7: Let G be a finite group. Then $|C(G)| = |G| - 1$ if and only if G is one of C_3, C_4, S_3, or D_8.

Proof. ($\Leftarrow$) Observe that $|C(C_3)| = \tau(3) = 2$ and $|C(C_4)| = \tau(4) = 3$ by Proposition 2.3, and $|C(S_3)| = |C(D_6)| = 3+\tau(3) = 5$ and $|C(D_8)| = 4+\tau(4) = 7$ by Proposition 3.9, so that the result holds for each group.

($\Rightarrow$) Let G be a finite group of order n and suppose that $|C(G)| = |G| - 1$. By Remark 4.3 we have $\sum_{i=1}^{k} n_i\,\phi(d_i) = n$, where $d_1 = 1, \dots, d_k$ are the positive

divisors of n and $n_i = |\{H \in C(G) \mid |H| = d_i\}|$. By hypothesis we have that $|C(G)| = \sum_{i=1}^{k} n_i = n - 1$, hence

$$\sum_{i=1}^{k} n_i \left(\phi(d_i) - 1\right) = 1.$$

This implies that

- There exists $i_0 \in \{1, 2, \ldots, k\}$ such that $n_{i_0} = 1$ and $\phi(d_{i_0}) = 2$ (i.e. $d_{i_0} \in \{3, 4, 6\}$);
- For $i \neq i_0$ either $n_i = 0$ or $\phi(d_i) = 1$ (i.e. $d_i \in \{1, 2\}$).

Thus G has a unique cyclic subgroup of order 3, 4, or 6, and arbitrarily (finitely) many cyclic subgroups of order 2. Moreover, $|G| = 2^{\alpha}3^{\beta}$. Observe that G cannot contain an element of order 6, for then G also contains an element of order 3, a contradiction. We consider two cases and prove each by a series of claims.

Case 1: G has a unique cyclic subgroup of order 3.

Let $H = \langle h \rangle$, $|h| = 3$.

Claim 1: $H \trianglelefteq G$.

We show $gHg^{-1} \subseteq H \; \forall \, g \in G$. Certainly $geg^{-1} \in H \; \forall \, g \in G$. Let $x \in H$, $x \neq e$. Then $|gxg^{-1}| = 3 \; \forall \, g \in G$, and since H is the unique cyclic subgroup of order 3 in G, H must contain all elements of order 3 in G. Thus $gxg^{-1} \in H$ $\forall \, g \in G$, so that $gHg^{-1} \subseteq H \; \forall \, g \in G$ and $H \trianglelefteq G$.

Claim 2: H is a Sylow 3-subgroup of G.

By Sylow 1 there exists $A < G$, $|A| = 3^{\beta}$. By hypothesis A cannot contain an element of order 3^{β} for $\beta \geq 2$. Thus every nonidentity element $a \in A$ must have order 3. But H contains all elements of G of order 3, so that we must have $A = H$. This proves the claim. Moreover, $\beta = 1$, so that $|G| = 2^{\alpha}3$.

Now either $H = G$ or $H < G$. If $H = G$ then $G = C_3$. Suppose then that $H < G$.

Claim 3: $ghg^{-1} = h^2 \ \ \forall\, g \in G - H$.

Let $g \in G - H$. Then $|ghg^{-1}| = 3$, so that $ghg^{-1} = h$ or $ghg^{-1} = h^2$. If $ghg^{-1} = h$, then $gh = hg \ \ \forall\, g \in G$. By hypothesis we must have $|g| = 2$. Since g and h commute it follows that $|gh| = \text{lcm}(|g|, |h|) = 6$, a contradiction since G contains no elements of order 6. Thus $ghg^{-1} = h^2$, or $ghg^{-1} = h^{-1}$.

Now let $k \in G - H$ and $K = \langle k \rangle$. By hypothesis $|K| = 2$, and since $k \notin H$, $H \cup K = \{e\}$. Moreover, since $H \trianglelefteq G$ it follows that $HK < G$ by Corollary 4.6.

Claim 4: $G = HK$

Suppose that $HK \neq G$. Then $\exists\ x \in G$, $x \notin HK$, and by hypothesis $|x| = 2$. Consider conjugation by xk. By Claim 3 $(xk)h(xk)^{-1} = h^2 \iff xkhk^{-1}x^{-1} = h^2$. By Claim 3 again $khk^{-1} = h^2$, hence $xh^2x^{-1} = h^2 \iff xh^2 = h^2x$. Thus, x and h^2 commute, so that $|xh^2| = \text{lcm}(|x|, |h^2|) = 6$, a contradiction.

Thus $G = HK$, so that $|G| = 6$ and G has the presentation

$$\langle h, k \mid h^3 = k^2 = e,\ kh = h^{-1}k \rangle$$

whence it follows that $G \cong D_6 \cong S_3$.

Case 2: G has a unique cyclic subgroup of order 4.

Let $H = \langle h \rangle$, where $|h| = 4$. Observe that by hypothesis we must have $\beta = 0$, so that $|G| = 2^\alpha$.

Claim 1: $H \trianglelefteq G$.

Certainly $geg^{-1} \in H\ \forall\, g \in G$. Let $x \in H$, $x \neq e$, so that $|x| = 2$ or $|x| = 4$. If $|x| = 4$, then $x = h$ or $x = h^3$, and $|gxg^{-1}| = 4 \ \ \forall\, g \in G$. Since H contains all the elements of order 4 in G by uniqueness it follows that $gxg^{-1} \in H\ \forall\, g \in G$. If $|x| = 2$, then $x = h^2$ and $|gxg^{-1}| = 2\ \forall\, g \in G$. Suppose that $gxg^{-1} \notin H$ for some $g \in G$. Then $g \notin H$. Set $y = gxg^{-1}$. Then

$$gxg^{-1} = y \iff gh^2g^{-1} = y \iff ghg^{-1}ghg^{-1} = y \iff (ghg^{-1})^2 = y.$$

By the previous case $ghg^{-1} \in H$ and $|ghg^{-1}| = 4$, hence $ghg^{-1} = h$ or $ghg^{-1} = h^3$. In either case $(ghg^{-1})^2 = h^2$, hence $y = h^2 \in H$, a contradiction. Thus $gxg^{-1} \in G$ for all $g \in G, x \in H$, so that $H \trianglelefteq G$.

Now either $H = G$ or $H < G$. If $H = G$ then $G = C_4$. Suppose then that $H < G$.

Claim 2: $ghg^{-1} = h^{-1} \ \ \forall\, g \in G - H$.

Let $g \in G - H$. Then $|g| = 2$ and $|ghg^{-1}| = 4$, and since $H \trianglelefteq G$ either $ghg^{-1} = h$ or $ghg^{-1} = h^3 = h^{-1}$. If $ghg^{-1} = h$, then $gh = hg$. Since g and h commute, $|gh| = \text{lcm}(|g|, |h|) = 4$, hence $gh = h$ or $gh = h^3$. Then either $g = e$ or $g = h^2$, which both imply that $g \in H$, a contradiction. Thus $ghg^{-1} = h^{-1}\ \forall\, g \in G - H$.

Now let $k \in G - H$ and $K = \langle k \rangle$. Then $|K| = 2$ and since $k \notin H$, $H \cap K = \{e\}$. Moreover, since $H \trianglelefteq G$, $HK < G$.

Claim 3: $G = HK$.

Suppose that $G \neq HK$. Then there exists $x \in G$, $x \notin HK$. By hypothesis $|x| = 2$. Consider conjugation by xk. Then by Claim 2

$$(xk)h(xk)^{-1} = h^{-1} \iff x(khk^{-1})x^{-1} = h^{-1} \iff xh^{-1}x^{-1} = h^{-1}.$$

By Claim 2 again $xh^{-1}x^{-1} = h$, so that the above holds if and only if $h = h^{-1}$, which implies that $|h| = 2$, a contradiction. Therefore $G = HK$, so that $|G| = 8$ and G has the presentation

$$\langle h, k \mid h^4 = k^2 = e,\ kh = h^{-1}k \rangle$$

hence $G \cong D_8$. This completes the proof. □

We conclude this section by presenting a characterization of the finite groups G satisfying $|C(G)| = |G| - 2$. The proof for this result is more involved than the proof for the $|C(G)| = |G| - 1$ result as the number of cases to consider is effectively

tripled by the consequences of Remark 4.3.

In two cases of the proof we form internal semidirect products out of product sets of subgroups of G and then show that these semi-direct products are isomorphic to direct products. We make use of the following results concerning semidirect products:

PROPOSITION 4.8: Suppose G is a group with subgroups H and K such that

(1) $H \trianglelefteq G$

(2) $H \cap K = \{e\}$

Let $\phi : K \to \mathrm{Aut}(H)$ be the homomorphism defined by mapping $k \in K$ to the automorphism of left conjugation by k on H. Then $HK \cong H \rtimes K$. In particular, if $G = HK$ with H and K satisfying (1) and (2), then G is the semidirect product of H and K. [2]

PROPOSITION 4.9: Let H and K be groups and let $\phi : K \to \mathrm{Aut}(H)$ be a homomorphism. Then the following are equivalent:

(1) The identity (set) map between $H \rtimes K$ and $H \times K$ is a group homomorphism (hence an isomorphism)

(2) ϕ is the trivial homomorphism from K into $\mathrm{Aut}(H)$

(3) $K \trianglelefteq H \rtimes K$. [2]

THEOREM 4.10: Let G be a finite group. Then $|C(G)| = |G| - 2$ if and only if G is one of the following groups: $C_4 \times C_2$, $C_2 \times D_8$, C_6, or D_{12}.

Proof. ($\Leftarrow$) By Proposition 2.3 $|C(C_6)| = \tau(6) = 4$, and by Proposition 3.9 $|C(D_{12})| = 6 + \tau(6) = 10$. That the result holds for the other two groups follows by hand calculation.

($\Rightarrow$) Suppose that $|C(G)| = |G| - 2$ and let $|G| = n$. Then by Remark 4.3 $n = \sum_{i=1}^{k} n_i\,\phi(d_i)$, where $d_1 = 1, \ldots, d_k$ are the positive divisors of n and $n_i = |\{H \in C(G) \mid |H| = d_i\}|$. By hypothesis we have that $|C(G)| = \sum_{i=1}^{k} n_i = n - 2$, hence

$$\sum_{i=1}^{k} n_i\,(\phi(d_i) - 1) = 2$$

which implies that one of the following must hold:

a.) There exists $i_0 \in \{1, 2, \ldots, k\}$ such that $n_{i_0} = 1$ and $\phi(d_{i_0}) = 3$.

b.) There exists $i_0 \in \{1, 2, \ldots, k\}$ such that $n_{i_0} = 2$ and $\phi(d_{i_0}) = 2$ (i.e. $d_{i_0} \in \{3, 4, 6\}$) and

   i.) For an $i \neq i_0$ either $n_i = 0$ or $\phi(d_i) = 1$ (i.e. $d_i \in \{1, 2\}$).

c.) There exist $i, j \in \{1, \ldots, k\}$ such that $n_i = n_j = 1$ and $\phi(d_i) = \phi(d_j) = 2$ (hence $d_i, d_j \in \{3, 4, 6\}$) and

   i.) For $l \neq i$ and $l \neq j$ either $n_l = 0$ or $\phi(d_l) = 1$ (i.e. $d_l \in \{1, 2\}$).

Since $\phi(d_{i_0}) \neq 3$ for all $d_{i_0} \in \mathbb{N}$, we may discard *a.*). In the remaining cases G has two cyclic subgroups H and K of orders 3, 4, or 6. Under *b.*), we obtain $|H| = |K|$, so that *b.*) yields the three subcases: $(|H|, |K|) = (3, 3)$, $(|H|, |K|) = (4, 4)$, and $(|H|, |K|) = (6, 6)$. Under *c.*), we obtain that $|H| \neq |K|$, so that *c.*) yields the three subcases: $(|H|, |K|) = (3, 4)$, $(|H|, |K|) = (3, 6)$, and $(|H|, |K|) = (4, 6)$. In either *b.*) or *c.*) G contains arbitrarily (finitely) many elements of order 2, and no other cyclic subgroups. Since the subcases will themselves contain subcases we simply write the subcases as cases 1 through 6 with the understanding that the first three cases proceed from b.) and that the last three proceed from c.).

Case 1: $(|H|, |K|) = (3, 3)$.

Let $H = \langle x \rangle$, $K = \langle y \rangle$, where $x \neq y$. Consider $xyx^{-1} \in G$. Then $|xyx^{-1}| = 3$. Suppose that $xyx^{-1} \in H$. Then $xyx^{-1} = x^k$ for some $k \in \mathbb{Z}^+$, which implies that

$y = x^k \in H$, a contradiction. Thus $xyx^{-1} \in K$. Then either $xyx^{-1} = y$ or $xyx^{-1} = y^2$.

Subcase 1: $xyx^{-1} = y$.

If $xyx^{-1} = y$, then $xy = yx$. Since x and y commute, $|xy| = 3$, hence $xy \in H$ or $xy \in K$. If $xy \in H$, then $xy = x^k$ for some $k \in \mathbb{Z}^+$, hence $y = x^{k-1} \in H$, a contradiction. Similarly, if $xy \in K$, we obtain $x = y^{k-1} \in K$, a contradiction.

Subcase 2: $xyx^{-1} = y^2$.

In this subcase $xy = y^2x$. Consider $|xy|$.

$$\begin{aligned} xy &= y^2x \\ (xy)^2 &= xyxy = xyy^2x = x^2 \\ (xy)^3 &= (xy)^2xy = x^2xy = y \\ (xy)^4 &= (xy)^2(xy)^2 = x^4 = x \\ (xy)^5 &= (xy)(xy)^4 = (y^2x)x = y^2x^2 \\ (xy)^6 &= (xy)^2(xy)^4 = x^3 = e. \end{aligned}$$

Thus $|xy| = 6$, so that G contains a cyclic subgroup of order 6, a contradiction. Thus, Case 1 does not hold.

Case 2: $(|H|, |K|) = (4, 4)$.

Let $x, y \in G$ such that $x \neq y$ and $H = \langle x \rangle$ and $K = \langle y \rangle$. Consider yxy^{-1}. Then $|yxy^{-1}| = 4$, so either $yxy^{-1} \in H$ or $yxy^{-1} \in K$. If $yxy^{-1} \in K$, $yxy^{-1} = y^k$ for some $k \in \mathbb{Z}^+$, hence $x = y^{k-1} \in K$, a contradiction. Thus, $yxy^{-1} \in H$, so that either $yxy^{-1} = x$ or $yxy^{-1} = x^{-1}$.

Subcase 1: $yxy^{-1} = x^{-1}$.

In this subcase $yx = x^{-1}y$. Consider $|yx|$. Then

$$\begin{aligned} yx &= x^{-1}y \\ (yx)^2 &= yxyx = yxx^{-1}y = y^2 \\ (yx)^3 &= yx(yx)^2 = yxy^2 \\ (yx)^4 &= yx^2(yx)^2 = y^2y^2 = e. \end{aligned}$$

Thus $|yx| = 4$, so that $yx \in H$ or $yx \in K$. If $yx \in H$, then either $yx = x$ or $yx = x^3$, which implies that either $y = e \in H$ or $y = x^2 \in H$, a contradiction. Similarly, $yx \in K$ implies that either $x = e \in K$ or $x = y^2 \in K$, a contradiction. Thus $yxy^{-1} \neq x^{-1}$.

Subcase 2: $yxy^{-1} = x$.

In this case $yx = xy$. Either $H \cap K = \{e\}$ or $H \cap K \neq \{e\}$.

Subcase 2a: $H \cap K = \{e\}$.

Since the generators of H and K commute, $HK < G$. Then $|HK| = \frac{|H||K|}{|H \cap K|} = 16$. Consider $xy \in HK$. Then $|xy| = \text{lcm}(|x|, |y|) = 4$, hence xy is one of x, x^{-1}, y, or y^{-1}. These conditions imply that either $y = e$, $y = x^2$, $x = e$, or $x = y^2$, respectively. Each is a contradiction.

Subcase 2b: $H \cap K \neq \{e\}$.

In this case $|H \cap K| = 2$ or $|H \cap K| = 4$. If $|H \cap K| = 4$, then $H \cap K = H$ or $H \cap K = K$, hence $H = K$, a contradiction. Thus $|H \cap K| = 2$, so that $H \cap K = \{e, x^2\} = \{e, y^2\}$, hence $x^2 = y^2$. Consider $\langle x, y\rangle = HK$. Then $|\langle x, y\rangle| = |HK| = 8$. We obtain the presentation

$$HK = \langle x, y \mid x^2 = y^2,\ x^4 = y^4 = e,\ xy = yx\rangle.$$

The orders of the nonidentity elements in HK are given below:

- Elements of order 4: x, x^2, y, $y = x^2y$
- Elements of order 2: $x^2 = y^2$, xy, $x^3y = xy^3$

Thus HK is an abelian group containing four elements of order 4 and three elements of order 2. Up to isomorphism there are three abelian groups of order 8, namely C_8, C_2^3, and $C_4 \times C_2$. Of these, $C_4 \times C_2$ is the only group with the same order structure as HK. It follows that $HK \cong C_4 \times C_2$.

Now either $G = HK$ or $HK < G$. If $G = HK$ then $G \cong C_4 \times C_2$ and we are done. Suppose then that $HK < G$. Then there exists $z \in G$ such that $z \notin HK$ and $|z| = 2$. Let $I = HK$ and $J = \langle z \rangle$.

Claim 1: $I \trianglelefteq G$.

We show that if $g \in G$, $gIg^{-1} \subseteq I$. Let $a \in I$ and $g \in G$. Then $a = x^iy^j$ for some $i, j \in \{1, \ldots, 4\}$. Observe that

$$\begin{aligned} gag^{-1} &= gx^iy^jg^{-1} \\ &= gxg^{-1}gx^{i-1}g^{-1}gyg^{-1}gy^{j-1}g^{-1} \\ &= \cdots = (gxg^{-1})^i(gyg^{-1})^j. \end{aligned}$$

Thus it suffices to show that $gxg^{-1} \in \langle x \rangle = H$ and $gyg^{-1} \in \langle y \rangle = K$ for all $g \in G$.

Lemma: $gxg^{-1} \in H$ for all $g \in G$.

Since $|gxg^{-1}| = 4$, $gxg^{-1} \in \{x, x^{-1}, y, y^{-1}\}$. If $gxg^{-1} = x$ or $gxg^{-1} = x^{-1}$, we are done. If $gxg^{-1} = y$, then $gx = yg$ for all $g \in G$. In particular, when $g = y$, we obtain $yx = y^2 \Rightarrow x = y$, a contradiction. If $gxg^{-1} = y^{-1}$, then $gx = y^{-1}g$ for all $g \in G$. In particular, when $g = y$, $yx = e \Rightarrow y = x^{-1} \in H$, a contradiction. Thus $gxg^{-1} \in H$. By interchanging x and y above, we obtain $gyg^{-1} \in K$. Since $g \in G$ is

arbitrary the lemma follows.

Thus, $gag^{-1} = x^{\alpha}y^{\beta} \in I$, hence $gIg^{-1} \subseteq I$ for all $g \in G$, so that $I = HK \trianglelefteq G$. Moreover, $IJ < G$ by Corollary 4.6 and $I \cap J = \{e\}$. Now let $\phi : J \to \mathrm{Aut}(I)$ be the homomorphism defined by mapping $z \in J$ to the automorphism of left conjugation by z on I. Then by Proposition 4.8 $IJ \cong I \rtimes J$.

We now show that $HJ = \langle x, z\rangle \cong D_8$. Observe that $HJ < G$ since $H \trianglelefteq G$ by the lemma.

Claim 2: $zxz^{-1} = z^{-1}$.

Consider $zxz^{-1} \in G$. Then $|zxz^{-1}| = 4$, hence $zxz^{-1} \in \{x, x^{-1}, y, y^{-1}\}$. If $zxz^{-1} = x$, then $zx = xz$. Since z and x commute, it follows that $|zx| = \mathrm{lcm}(|x|, |z|) = 4$, so that $xz \in \{x, x^{-1}, y, y^{-1}\}$. The first two equations imply that $z \in H$, and the second equations imply that $z \in J = HK$, a contradiction. If $zxz^{-1} = y$, then $zx = yz$, and $(zx)^2 = zxzx = yzzx = yx$, and since x and y commute zx must have order 4, but $zx \notin H$ and $zx \notin K$ (otherwise $z \in H$ or $z \in K$). If $zxz^{-1} = y^{-1}$, then $zx = y^{-1}z$. Now $(zx)^2 = zxzx = y^{-1}zzx = y^{-1}x$, and since x and y^{-1} commute zx must have order 4, but as before $zx \notin H$ and $zx \notin K$.
Thus $zxz^{-1} = x^{-1}$, so that z conjugates x to its inverse, which proves the claim.

Observe that since $z \in G$ is arbitrary the claim holds for any element $a \in G$ where $a \notin I = HK$. Observe also that by interchanging x and y we obtain that any element not in I also conjugates y to its inverse. The presentation for HJ is then given by

$$HJ = \langle x, z \mid x^4 = z^2 = e,\ zx = x^{-1}z\rangle$$

hence it follows that $HJ = \langle x, z\rangle \cong D_8$.

Claim 3: $IJ = G$.

Either $IJ < G$ or $IJ = G$. Suppose that $IJ < G$. Then there exists $a \in G$ where $a \notin IJ$, and by hypothesis $|a| = 2$. Now since $a \notin I$, by Claim 2 and the

remark following the claim $axa^{-1} = x^{-1}$. Moreover, $az \notin I$, hence

$$(az)x(az)^{-1} = azxz^{-1}a^{-1} = ax^{-1}a^{-1} = x$$

which implies that $(az)x = x(az)$. Then, since az and x commute, it follows that $|(az)x| = \text{lcm}(|az|, |x|) = 4$, but $(az)x \notin I$, a contradiction. Thus $G = IJ$.

Claim 4: $G = IJ \cong D_8 \times C_2$.

Thus far we have established that $G = IJ \cong I \rtimes J$ and that $HJ = \langle x, z \rangle \cong D_8$. Since $[G : HJ] = 2$, $HJ \trianglelefteq G$. Let $L = \langle xy \rangle$. Then $|L| = 2$ and $HJ \cap L = \{e\}$, so that $(HJ)L \cong HJ \rtimes L$ by Proposition 4.8. Since $|(HJ)L| = 16$, it follows that $G = (HJ)L \cong HJ \rtimes L \cong D_8 \rtimes C_2$. To show that $D_8 \rtimes C_2 \cong HJ \rtimes L \cong HJ \times L \cong D_8 \times C_2$, by Proposition 4.9 it suffices to show that $L \trianglelefteq HJ \rtimes L$.

Claim 5: $L \trianglelefteq HJ \rtimes L$.

Clearly $geg^{-1} \in L$ for all $g \in G$. Consider $xy \in L$. Then, since every element of G is of the form $x^i y^j z^k$, by Claim 2

$$\begin{aligned} g(xy)g^{-1} &= (x^i y^j z^k)xy(x^i y^j z^k)^{-1} \\ &= x^i y^j (z^k xyz^{-k}) y^{-j} x^{-i} \\ &= x^i y^j x^{-1} y^{-1} y^{-j} x^{-i} \\ &= x^{-1} y^{-1} = x^3 y^3 \\ &= x x^2 y^2 y = xy. \end{aligned}$$

Thus $g(xy)g^{-1} \in L$ for all $g \in G$, so that $L \trianglelefteq HJ \rtimes L$. Finally, we obtain $G \cong D_8 \times C_2$, which concludes the case.

Case 3: $(|H|, |K|) = (6, 6)$.

If $|H| = |K| = 6$, then by Cauchy's Theorem there exists $h \in H$, $k \in K$ such that $|h| = |k| = 3$, hence G contains two cyclic subgroups of order 3, contrary to

hypothesis.

Case 4: $(|H|, |K|) = (3, 4)$.

Let $H = \langle x \rangle$ and $K = \langle y \rangle$. Consider $yxy^{-1} \in G$. Then $|yxy^{-1}| = 3$, hence $yxy^{-1} = x$ or $yxy^{-1} = x^2$. If $yxy^{-1} = x$, then $yx = xy$. Since x and y commute, $|xy| = \text{lcm}(|x|, |y|) = 12$, so that G contains an element of order 12, a contradiction. If $yxy^{-1} = x^2$, then $yx = x^2y$. Consider $|yx|$.

$$
\begin{aligned}
yx &= x^2y \\
(yx)^2 &= (yx)(yx) = yxx^2y = y^2 \\
(yx)^3 &= (yx)(yx)^2 = yxy^2 = x^2yy^2 = x^2y^3 \\
(yx)^4 &= (yx)(yx)^3 = yxx^2y^3 = yx^3y^3 = y^4 = e
\end{aligned}
$$

Thus $|yx| = 4$, so that $yx \in K$, hence $yx = y$ or $yx = y^3$. Then either $x = e$ or $x = y^2 \in K$, a contradiction.

Therefore Case 4.) does not hold.

Case 5: $(|H|, |K|) = (6, 3)$.

Let $H = \langle y \rangle$ and $\langle x \rangle$ be the unique cyclic subgroup of order 3 in G. Then $\langle x \rangle < H$, for if it were not, then H contains a cyclic subgroup of order 3 not equal to $\langle x \rangle$, contradicting uniqueness. Now either $H = G$ or $H < G$. If $H = G$, then $H \cong C_6$. Suppose then that $H < G$. Then there exists $z \in G$, $z \notin H$, and by hypothesis $|z| = 2$. Set $K = \langle z \rangle$.

Claim 1: $zyz^{-1} = y^{-1}$

Consider $zyz^{-1} \in G$. Then $|zyz^{-1}| = 6$, hence $zyz^{-1} = y$ or $zyz^{-1} = y^{-1}$. If $zyz^{-1} = y$, then $zy = yz$ and $|yz| = \text{lcm}(|y|, |z|) = 6$, so that $yz = y$ or $yz = y^{-1}$, which implies that either $z = e$ or $z = y^{-2} \in H$, a contradiction.

Claim 2: $H \trianglelefteq G$.

Since $z \in G$ above is arbitrary, $gyg^{-1} = y^{-1} \in H$ for all $g \in G$, where $g \notin H$. Clearly for all $g \in H$, $gyg^{-1} \in H$, so that $H \trianglelefteq G$. It follows that $HK < G$ by Corollary 4.6. Since $z \notin H$ it is clear that $H \cap K = \{e\}$. Let $\phi : K \to \mathrm{Aut}(H)$ be the automorphism defined by mapping $k \in K$ to the automorphism of left conjugation by k in H. Then $HK \cong H \rtimes K < G$ by Proposition 4.8. By Claim 1 HK has the presentation

$$HK = \langle y, z \mid y^6 = z^2 = e,\ zy = y^{-1}z \rangle$$

so that $HK \cong D_{12}$.

Claim 3: $G = HK$

Suppose that there exists $g \in G$, $g \notin HK$. Then by hypothesis $|g| = 2$. Also $zg \notin HK$, since otherwise $g \in HK$, and $|zg| = 2$. By Claim 1 it follows that

$$y^{-1} = zgy(zg)^{-1} = zgyg^{-1}z^{-1} = zy^{-1}z^{-1} = y$$

which implies that $|y| = 2$, a contradiction. Therefore $G = HK$, so that $G \cong D_{12}$.

Case 6: $(|H|, |K|) = (4, 6)$

If $|K| = 6$, then K contains a cyclic subgroup of order 3, but this contradicts the fact that H is the only other cyclic subgroup not of order 2 in G.

This completes the proof. $\square$

5. CONCLUSION

Classifying the number of distinct cyclic subgroups of a given finite group G is an interesting problem that is surprisingly under-explored in the literature [1]. Moreover, the cyclic subgroup structure of a finite group is subject to some interesting constraints. Cauchy's Theorem provides a natural bound for "lower end" considerations of $|C(G)|$, while Tărnăuceanu's identity in Remark 4.3 determines what cases need to be considered when $|C(G)|$ is large relative to $|G|$.

Our research establishes characterizations of $|C(G)| = k$ for $k \in \{1, \ldots, 4\}$, classifies $|C(G)|$ for dihedral groups and elementary abelian p-groups, provides alternate proofs for $|C(G)| = |G| - k$, $k \in \{0, 1\}$, and also characterizes the case of $k = 2$. The $k = 2$ case contributes to the open problem posed by Tărnăuceanu in his article. Given the number of cases that arose for the $k = 2$ problem, it may be necessary to find a stronger point of entry than Remark 4.3.

Another problem that we would like to explore in further research is to characterize when $|C(G)|$ is a quotient of $|G|$. In particular, we are interested in obtaining classifications of finite groups satisfying $|C(G)| = \frac{|G|}{k}$ for $k \in \mathbb{N}$, $k \geq 2$. We supplied an original proof that the $k = 1$ case is satisfied only when G is an elementary abelian 2-group. We are interested to see if any patterns emerge among the groups satisfying this relation as k increases.

We hoped to prove the following two conjectures but our other results took one too many mornings to establish. We conclude our remarks by stating them here.

CONJECTURE 5.1: Let G be a finite group. Then $|C(G)| = 5$ if and only if G is isomorphic to one of the following groups: D_6, $C_3 \times C_3$, Q_8, or C_{p^4}.

CONJECTURE 5.2: Let G be a finite group. Then $|C(G)| = |G| - 3$ if and only

if G is isomorphic to one of the following groups: C_5, Q_8, or D_{10}.

REFERENCES

[1] M. Tărnăuceanu, *Finite Groups With a Certain Number of Cyclic Subgroups,* Article, *American Mathematical Monthly* (AMM), 2015. (2016)

[2] Dummit, D., and Foote, F. *Abstract Algebra,* Wiley, Vermont, 2004. (2016)

[3] Conrad, Keith. *Consequences of Cauchy's Theorem,* Lecture Notes: University of Connecticut, math.uconn.edu/ kconrad/blurbs/grouptheory/cauchyapp.pdf. (2016)

[4] Conrad, Keith. *Consequences of the Sylow Theorems,* Lecture Notes: University of Connecticut, math.uconn.edu/ kconrad/blurbs/grouptheory/sylowapp.pdf. (2016)