On the Structure of Automorphism Groups of Finite Groups

Thesis

Submitted in the fulfillment of the requirements of the degree of

DOCTOR OF PHILOSOPHY

in

MATHEMATICS

by

ROHIT GARG
(Regn. No. 951211006)

to the

SCHOOL OF MATHEMATICS
THAPAR INSTITUTE OF ENGINEERING AND TECHNOLOGY
147 004 (PUNJAB), INDIA.
August - 2019

Declaration of Authorship

I hereby declare that the work which is being presented in this thesis entitled *"On the Structure of Automorphism Groups of Finite Groups"* submitted by me, for the award of the degree of Doctor of Philosophy in the School of Mathematics, Thapar Institute of Engineering and Technology, Patiala, is true and original record of my own independent and original research work carried out under the supervision of Dr. Deepak Gumber, Professor, School of Mathematics, Thapar Institute of Engineering and Technology, Patiala, India. The matter embodied in this thesis has not been submitted in part or full to any other university or institute for the award of any degree in India or Abroad and that the ideas and references cited herein have been duly acknowledged.

(Rohit Garg)

Regd. No. 951211006

CERTIFICATE

This is to certify that the thesis *"On the Structure of Automorphism Groups of Finite Groups"* which is submitted by Mr. Rohit Garg, in fulfillment of the requirement for the award of the degree of *Doctor of Philosophy* in the School of Mathematics, Thapar Institute of Engineering and Technology, Patiala, is a record of the candidate's own independent and original research work carried out by him under my supervision and guidance. The matter embodied in this thesis has not been submitted in part or full to any University or Institute for the award of any degree.

Attestation by supervisor

(Dr. Deepak Gumber)
Professor
School of Mathematics
Thapar Institute of Engineering and Technology
Patiala 147 004
INDIA.

Acknowledgements

I express my sincere regards and gratitude to my supervisor Dr. Deepak Gumber for his expert guidance, cool temperament, valuable suggestions, support, advice and continuous encouragement throughout the period of my research work.

I am thankful to Prof. S. S. Bhatia and Dr. Satish Kumar, Head, School of Mathematics, for providing necessary facilities to carry out this work, and to the Doctoral Committee members for their helpful and valuable advice.

I am also grateful to my friends Mandeep, Tarun, Sukhveer and all the research scholars of SoM for their timely help and for the moral support they provided during my research work. I am also thankful to Mr. Abhikash, Mr. Digamber, Mr. Magdoom, Mr. Harish and the other staff members for their help and cooperation.

Words are inadequate in paying regards to my parents. I would like to thank my mother whose heavenly blessings supported me spiritually throughout my life. I am forever grateful to my father, whose foresight and values paved the way for a privileged education and helped me to do better each day. I would also like to thank all members of my family for providing a loving environment for me.

And above all, I thank and pay my regards to the Almighty for his love and blessings.

August, 2019 ***(Rohit Garg)***

Dedicated
To
my
Family

Abstract

Let G be an arbitrary group and let $\mathrm{Aut}(G)$ denote the full automorphism group of G. An automorphism α of G is called a class-preserving automorphism if for each $x \in G$, there exists an element $g_x \in G$ such that $\alpha(x) = g_x^{-1} x g_x$; and is called an inner automorphism if for all $x \in G$, there exists a fix element $g \in G$ such that $\alpha(x) = g^{-1} x g$. The group $\mathrm{Inn}(G)$ of all inner automorphisms of G is a normal subgroup of the group $\mathrm{Aut}_c(G)$ of all class-preserving automorphisms of G. An automorphism α of G is called an nth class-preserving if for each $x \in G$, there exists an element $g_x \in \gamma_n(G)$, where $\gamma_n(G)$ denotes the nth term of the lower central series of G, such that $\alpha(x) = g_x^{-1} x g_x$. The set $\mathrm{Aut}_c^n(G)$ of all nth class-preserving automorphisms of G fixing $Z(G)$ element-wise is a normal subgroup of $\mathrm{Aut}(G)$. An automorphism α of G is called a central automorphism if it commutes with all inner automorphisms of G; or equivalently $g^{-1}\alpha(g) \in Z(G)$, the center of G, for all $g \in G$. The group of all central automorphisms of G is denoted as $\mathrm{Autcent}(G)$. An automorphism α of a group G is called a commuting automorphism if each element x in G commutes with its image $\alpha(x)$ under α . Let $A(G)$ denote the set of all commuting automorphisms of G. Observe that $\mathrm{Autcent}(G)$ is contained in $A(G)$. A group G is called an $A(G)$-group if the set $A(G)$ is a subgroup of $Aut(G)$.

In this thesis, we mainly study the structure of $A(G)$, $\mathrm{Autcent}(G)$ and $\mathrm{Aut}_c^n(G)$. We find some conditions on a finite p-group G such that $A(G)$ is a subgroup of $\mathrm{Aut}(G)$. We also find conditions on a finite p-group G such that $\mathrm{Aut}_c^n(G) = \mathrm{Autcent}(G)$ and $\mathrm{Autcent}(G) = Z(\mathrm{Inn}(G))$.

Chapter 1, contains the introductory part and some basic definitions. In chapter 2, we give necessary and sufficient conditions for a finite p-group G of class $n+1$ such that $\mathrm{Aut}_c^n(G) = \mathrm{Autcent}(G)$. As a consequence, we give a short proof of the main result of Yadav [45] which states that: Let G be a finite p-group of class 2 and let $p^{m_1}, \ldots, p^{m_d}$ be the invariants of $G/Z(G)$. Then $\mathrm{Aut}_c(G) = \mathrm{Autcent}(G)$ if and only if $\gamma_2(G) = Z(G)$ and $|\mathrm{Aut}_c(G)| = \prod_{i=1}^{d} |\Omega_{m_i}(\gamma_2(G))|$.

A group G is said to be metacyclic if it contains a cyclic normal subgroup Z such

that G/Z is cyclic. In chapter 3, we find some necessary and sufficient conditions on a finite non-abelian p-group G, where p is odd prime, with $G/Z(G)$ metacyclic such that G is an $A(G)$-group.

For $x \in G$, let $[x, G]$ denote the set $\{[x, g] \mid g \in G\}$. A non-abelian group G that has no non-trivial abelian direct factor is said to be purely non-abelian. Let G be a finite p-group and N be a non-trivial normal subgroup of G. The pair (G, N) is called a Camina pair if $N \subseteq [x, G]$ for all $x \in G - N$. A finite p-group G is called Frattinian if $Z(M) \neq Z(G)$ for all maximal subgroups M of G. A Frattinian p-group G satisfying $C_G(Z(\Phi(G))) = \Phi(G)$ is called strongly Frattinian. In chapter 4, we find some necessary conditions on a finite non-abelian p-group G such that G is an $A(G)$-group. In this chapter we give two theorems. In first one, we prove that if G is a finite non-abelian p-group such that $C_G(\Phi(G))$ is cyclic, then G is an $A(G)$-group. In second one, we prove that if G is a finite Frattinian p-group such that $G/Z(G)$ is purely non-abelian and $(G, Z(G))$ is a Camina pair, then G is strongly Frattinian, and if p is odd, then G is an $A(G)$-group.

In chapter 5, we study finite p-groups G for which $\mathrm{Autcent}(G)$ is of minimal order, that is, $\mathrm{Autcent}(G) = Z(\mathrm{Inn}(G))$. We give necessary and sufficient conditions on a finite p-group G such that $\mathrm{Autcent}(G) = Z(\mathrm{Inn}(G))$.

List of Research Papers

(1) Rohit Garg, *On finite p-groups whose central automorphisms are all nth class-preserving*, Bulletin of the Iranian Mathematical Society (2019), https://doi.org/10.1007/s41980-019-00266-8.

(2) Rohit Garg, *On commuting automorphisms of finite p-groups with a metacyclic quotient*, Mathematical Notes, **106(2)** (2019), 296-298.

(3) Rohit Garg, Deepak Gumber, *On commuting automorphisms of some p-groups*, Mathematical Notes (Communicated).

(4) Rohit Garg, *On finite p-groups whose central automorphisms are all inner*, BULLETIN MATHÉMATIQUE de la Société des Sciences Mathématiques de Roumanie (Communicated).

Contents

CHAPTER 1

Introduction and Basics

1.1 — Introduction

Let G be an arbitrary group and let $Z(G)$ and $\Phi(G)$ respectively denote the centre and the Frattini subgroup of G. Let $\mathrm{Aut}(G)$ denote the full automorphism group of G. An automorphism α of G is called a class-preserving automorphism if for each $x \in G$, there exists an element $g_x \in G$ such that $\alpha(x) = g_x^{-1} x g_x$; and is called an inner automorphism if for all $x \in G$, there exists a fix element $g \in G$ such that $\alpha(x) = g^{-1} x g$. The group $\mathrm{Inn}(G)$ of all inner automorphisms of G is a normal subgroup of the group $\mathrm{Aut}_c(G)$ of all class-preserving automorphisms of G. An automorphism φ of G is called a central automorphism if it commutes with all inner automorphisms of G; or equivalently $g^{-1}\varphi(g) \in Z(G)$, the center of G, for all $g \in G$. The set $\mathrm{Autcent}(G)$ of all central automorphisms of G fixes the commutator subgroup G' element-wise and is a normal subgroup of $\mathrm{Aut}(G)$.

Note that, for a finite p-group of class 2, we have

$$\mathrm{Aut}_c(G) \leq \mathrm{Autcent}(G) \leq \mathrm{Aut}(G).$$

In 1999, Mann [31, Question 10] asked the following question:

Do all p-groups have automorphisms that are not class preserving? If the answer is no, which are the groups that have only class preserving automorphisms?

The examples of finite p-groups G such that $\mathrm{Aut}_c(G) = \mathrm{Aut}(G)$ are already known in the literature. Such groups, having nilpotency class 2 were constructed by Heineken [19] in 1980 and that having nilpotency class 3 were constructed by Malinowska [29] in 1992.

The group of all central automorphisms is as large as possible when all automorphisms are central, that is $\mathrm{Autcent}(G) = \mathrm{Aut}(G)$, and is as small as possible when all central automorphisms are inner, that is $\mathrm{Autcent}(G) = Z(\mathrm{Inn}(G))$. Non-abelian p-groups G in which $\mathrm{Autcent}(G) = \mathrm{Aut}(G)$ have been well studied. In 1913, Miller [32] constructed a group G of order 2^6 and generated by three elements such that $\mathrm{Aut}(G)$ is abelian, that is, $\mathrm{Autcent}(G) = \mathrm{Aut}(G)$. Miller's group of order 64 is the smallest non-abelian group with an abelian automorphism group. In 1975, Jonah and Konvisser [23] constructed a group G of order p^8 and generated by four elements such that $\mathrm{Aut}(G)$ is abelian. In 1987, Curran [9] gave a method for constructing further examples of non-abelian 2-groups which have abelian automorphism groups. In 1995, Morigi [33] raised the following question:

What is the minimal number of generators for a non-abelian p-group having an abelian automorphism group, for p an odd prime?

He himself settled this question and proved that the minimal number of generators for a p-group having an abelian automorphism group is four, for p an odd prime. In

1998, Ban and Yu [4] proved that there is no group G such that $\mathrm{Aut}(G)$ is an abelian p-group of order $\leq p^{11}$, where $p > 2$. In 1982, Curran [8] constructed a group G of order 2^7 such that $\mathrm{Autcent}(G) = \mathrm{Aut}(G)$ is non-abelian. In 1984, Malone [28] constructed p-groups for odd primes such that $\mathrm{Autcent}(G) = \mathrm{Aut}(G)$ is non-abelian. Note that the groups considered by Curran and Malone have abelian direct factors. Examples of 2-groups G such that G does not have an abelian direct factor and $\mathrm{Autcent}(G) = \mathrm{Aut}(G)$ is non-abelian were constructed by Glasby [17] in 1986. In 2002, Malinowska [30, Problem 13] proposed the following problem:

For an odd prime p***, find a*** p***-group*** G ***which has no non-trivial abelian direct factor and*** $\mathrm{Autcent}(G) = \mathrm{Aut}(G)$ ***is non-abelian.***

In 2012, Jain and Yadav [22] gave the following example of such groups for $n \geq 2$ and p an odd prime:

$G = \langle a, b, c, d \mid a^{p^n} = b^{p^2} = c^{p^2} = d^p = 1, [a, b] = b^p, [a, c] = c^p, [a, d] = c^p, [b, c] = a^{p^{n-1}}, [b, d] = b^p, [c, d] = 1\rangle$.

In 2013, Yadav [45, Theorem A] gave necessary and sufficient conditions on a finite p-group G of class 2 such that $\mathrm{Aut}_c(G) = \mathrm{Autcent}(G)$. He also proved that, if G is a finite p-group of class 2 such that $\mathrm{Aut}_c(G) = \mathrm{Autcent}(G)$, then $d(G)$ is even. In 2013, Kalra and Gumber [24] proved that $\mathrm{Aut}_c(G) = \mathrm{Autcent}(G)$ if and only if $\mathrm{Aut}_c(G) \simeq \mathrm{Hom}(G/Z(G), \gamma_2(G))$ and $\gamma_2(G) = Z(G)$. As a consequence of this result, they obtained an easy and short proof of the main result of Curran and McCaughan [11] which states that: If G is a finite p-group, then $\mathrm{Autcent}(G) = \mathrm{Inn}(G)$ if and only if $G' = Z(G)$ and $Z(G)$ is cyclic. They also classified all finite p-groups G such that $\mathrm{Aut}_c(G) = \mathrm{Autcent}(G)$ when $Z(G)$ is cyclic or elementary

abelian. And consequently, they characterized all finite p-groups of order $p^n (n \leq 7)$ such that $\mathrm{Aut}_c(G) = \mathrm{Autcent}(G)$.

We call an automorphism α of G an nth class-preserving if for all $g \in G$, $\alpha(g) \in g^{\gamma_n(G)}$, where $\gamma_n(G)$ denotes the nth term of the lower central series of G. The set $\mathrm{Aut}_c^n(G)$ of all nth class-preserving automorphisms of G fixes $Z(G)$ element-wise and is a normal subgroup of $\mathrm{Aut}(G)$. Observe that $\mathrm{Aut}_c^n(G) = \mathrm{Aut}_c(G)$ for $n = 1$, and if G is a finite p-group of class $n + 1$, then $\mathrm{Aut}_c^n(G)$ is a normal subgroup of $\mathrm{Autcent}(G)$. In chapter 2, we give necessary and sufficient conditions for a finite p-group G of class $n + 1$ such that $\mathrm{Aut}_c^n(G) = \mathrm{Autcent}(G)$, and as a consequence obtain Theorem A of Yadav [45] as a particular case.

An automorphism α of a group G is called a commuting automorphism if each element x in G commutes with its image $\alpha(x)$ under α. Let $A(G)$ denote the set of all commuting automorphisms of G. Observe that $\mathrm{Autcent}(G)$ is contained in $A(G)$. Let $[g, \alpha] = g^{-1}\alpha(g)$, where $g \in G$ and $\alpha \in \mathrm{Aut}(G)$. Note that if $\alpha \in \mathrm{Autcent}(G)$ if and only if the function $g \to [g, \alpha]$ is a homomorphism, and $\alpha \in A(G)$ if and only if $[g^n, \alpha] = [g, \alpha]^n$ for all $g \in G$. A group G is said to be an $A(G)$-group if the set of all commuting automorphisms of G forms a subgroup of $\mathrm{Aut}(G)$. Many authors have done work on commuting and non-commuting elements of a group (see for example [12, 46]). Commuting maps like derivations and automorphisms were first studied for various classes of rings [5, 7, 15, 26, 37, 42]. In the year 1984, Herstein [20] proposed the following problem to American Mathematical Monthly:

If G ***is a simple non-abelian group, then prove that*** $A(G) = 1$**.**

In 1986, Laffey [25] observed that $A(G) = 1$ provided G has no nontrivial abelian

normal subgroups, while Pettet [25] proved that $A(G) = 1$ if $Z(G) = 1$ and $\gamma_2(G) = G$. Let $E_2(G) = \{g \in G \mid [g, x, x] = 1 \ \forall x \in G\}$ denote the set of right 2-Engel elements of G. In 2001, Deaconescu and Walls [13] have shown that there is a close connection between the right 2-Engel elements and the set of commuting automorphisms of a group. Deaconescu, Silberberg and Walls [14] in 2002, raised the following questions about $\mathrm{A}(G)$:

1. Is it true that the set $\mathrm{A}(G)$ is always a subgroup of $\mathrm{Aut}(G)$?

2. What conditions on G imply the equality $\mathrm{A}(G) = \mathrm{Autcent}(G)$?

3. Is it true that $\mathrm{A}(G) = 1$ if and only if $\mathrm{Autcent}(G) = 1$?

Regarding question 1, Deaconescu *et al.* [14] gave the following example of a group G of order 2^5 in which $A(G)$ doesn't form a subgroup:

$$G = \langle a, b, c, d \mid a^4 = b^2 = d^2 = 1, a^2 = c^2, [a, b] = [c, d] = a^2, [a, c] = [a, d] = [b, c] = [b, d] = 1\rangle$$

In 2013, Vosooghpour and Malayeri [43] showed that minimum order of a non-$A(G)$ p-group is p^5. In 2013, Fouladi and Orfi [16] proved that if G is either a finite AC-group or a p-group of maximal class or a metacyclic p-group, then G is an $A(G)$-group. They also proved that if G is a group of order p^n with a cyclic maximal subgroup, then $A(G)$ is a subgroup of $\mathrm{Aut}(G)$. In 2013, Vosooghpour, Kargarian and Malayeri [44] obtained the structure of $A(G)$, where G is a non-abelian p-group of order p^n with cyclic maximal subgroup. In 2015, Rai [35] gave some sufficient conditions on a finite p-group G such that $A(G)$ is a subgroup of $\mathrm{Aut}(G)$ and, as a consequence, proved that in a finite p-group G of co-class 2, where p is an odd prime, $A(G)$ is a subgroup of $\mathrm{Aut}(G)$. In 2016, Singh and Gumber [41] gave very

elementary and short proofs of main results of Rai and obtained some other related results. In 2019, Shahrabi, Malayeri and Vosooghpour [39] have proved that a finite 2-group G of almost maximal class is an $A(G)$-group. Recently in 2019, Rai [36] proved that the direct product of two finite $A(G)$-groups is also an $A(G)$-group. He also proved that $GL(n,q)$ for $n = 3$ or $q > n$, $PSL(2,q)$ and ZM-groups are $A(G)$-groups.

A group G is said to be metacyclic if it contains a cyclic normal subgroup Z such that G/Z is cyclic. In chapter 3, we prove that if G is a finite non-abelian p-group, where p is odd prime, such that $G/Z(G)$ is metacyclic, then G is an $A(G)$-group if and only if $cl(G) = 2$. Let $\alpha, \beta \in A(G)$ and $x \in G$. Then, by [14, Lemma 2.2], $\alpha(x) = xc_1$ and $\beta(x) = xc_2$ for some $c_1, c_2 \in C_G(G')$. Therefore, if $C_G(G')$ is abelian, then $[\alpha(x), \beta(x)] = [x^{-1}\alpha(x), \beta(x)] = [x^{-1}\alpha(x), x^{-1}\beta(x)] = 1$ because x^{-1} commutes with both $\alpha(x)$ and $\beta(x)$. Therefore G is an $A(G)$-group by [14, Lemma 2.4(ii), Lemma 2.2(vi)]. Observe that $Z_2(G) \leq C_G(G')$. Rai [35, Lemma 3.2] proved that if G is a finite p-group, where p is an odd prime, such that $Z_2(G)$ is abelian, then G is an $A(G)$-group. This raises the obvious question:

Is G an $A(G)$-group if $C_G(\Phi(G))$ is abelian?

In chapter 4, we prove that if G is a finite non-abelian p-group such that $C_G(\Phi(G))$ is cyclic, then G is an $A(G)$-group.

For $x \in G$, let $[x, G]$ denote the set $\{[x, g] \mid g \in G\}$. Let G be a finite p-group and N be a non-trivial normal subgroup of G. The pair (G, N) is called a Camina pair if $N \subseteq [x, G]$ for all $x \in G - N$. A finite p-group G is called Frattinian if $Z(M) \neq Z(G)$ for all maximal subgroups M of G. A Frattinian p-group G

satisfying $C_G(Z(\Phi(G))) = \Phi(G)$ is called strongly Frattinian. In 2013, Vosooghpour and Akhavan-Malayeri [43] showed that for each $n \geq 5$, there exists a non-$A(G)$ p-group of order p^n. They, in fact, proved that if G is an extra-special p-group of order $\geq p^5$, then G is not an $A(G)$-group. Observe that if G is a finite extra-special p-group, then G is Frattinian and $(G, Z(G))$ is a Camina pair. The converse is true if $cl(G) = 2$ (see Proposition 4.2.8). The following example shows that the converse is false if $cl(G) \geq 3$.

Example 1.1.1 *Let G be the group defined by the presentation*

$$G = \langle a, c \mid a^{p^n} = c^{p^{n+1}} = 1, c^a = c^{1+p} \rangle,$$

where p is an odd prime. Then

- $|G| = p^{2n+1}$.
- $Z(G) = \langle c^{p^n} \rangle$ *has order p and $(G, Z(G))$ is a Camina pair.*
- $\Phi(G) = G^p G' = \langle a^p, c^p \rangle$, *and thus G has $p + 1$ maximal subgroups. All the maximal subgroups have the center of order p^2.*
- *G has nilpotency class $n + 1$.*

These observations suggest the following natural question:

Does there exist a finite Frattinian p-group G with $(G, Z(G))$ a Camina pair which is an $A(G)$-group?

We answer this question in affirmative in chapter 4 when p is odd and $G/Z(G)$ is purely non-abelian. More precisely, we prove that if G is a finite Frattinian p-group

such that $G/Z(G)$ is purely non-abelian and $(G, Z(G))$ is a Camina pair, then G is strongly Frattinian, and if p is odd, then G is an $A(G)$-group.

In the recent past, there has been an interest in finding finite p-groups for which all central automorphisms are inner [10, 11, 18, 40]. Observe that the problem of finding finite p-groups G for which $\mathrm{Autcent}(G) \leq \mathrm{Inn}(G)$ is equivalent to finding finite p-groups G for which $\mathrm{Autcent}(G) = Z(\mathrm{Inn}(G))$, that is, $\mathrm{Autcent}(G)$ is minimal. In case of nilpotence class 2, this is equivalent to finding finite p-groups G for which $\mathrm{Autcent}(G) = \mathrm{Inn}(G)$. This case was settled by Curran and McCaughan [11] in 2001. They proved that if G is a finite p-group, then $\mathrm{Autcent}(G) = \mathrm{Inn}(G)$ if and only if $G' = Z(G)$ and $Z(G)$ is cyclic. In 2004, Curran [10] gave two necessary conditions for a finite non-abelian p-group G to have minimal number of central automorphisms. He proved that if G is a finite non-abelian p-group such that $\mathrm{Autcent}(G) = Z(\mathrm{Inn}(G))$, then $Z(G) \leq G'$ and $Z(\mathrm{Inn}(G))$ is not cyclic. These conditions are necessary but not sufficient. In 2013, Sharma and Gumber [40] proved that if G is a finite p-group of order p^5 or p^6, then $\mathrm{Autcent}(G) = Z(\mathrm{Inn}(G))$ if and only if G is of rank 2 and $|Z(G)| = p$. In 2015, Gumber and Kalra [18] characterized finite p-groups G of co-class up to 4 and groups of order up to p^7 for which $\mathrm{Autcent}(G)$ is minimal. They gave necessary and sufficient conditions on a finite p-group G for which $\mathrm{Autcent}(G) = Z(\mathrm{Inn}(G))$ in the case when $Z(G)$ is cyclic.

Let G be a finite p-group and let

$$G/G' \simeq C_{p^{\alpha_1}} \times C_{p^{\alpha_2}} \times \cdots \times C_{p^{\alpha_n}}$$

and

$$Z_2(G)/Z(G) \simeq C_{p^{\beta_1}} \times C_{p^{\beta_2}} \times \cdots \times C_{p^{\beta_m}}$$

be the cyclic decompositions of respective abelian groups, where $\alpha_i \geq \alpha_{i+1}$ and $\beta_i \geq \beta_{i+1}$ are positive integers. Let $W(G)/Z(G) = \Omega_1(Z_2(G)/Z(G))$. In chapter 5, we prove that if G is a finite non-abelian p-group such that $W(G)$ is non-abelian, then $\text{Autcent}(G) = Z(\text{Inn}(G))$ if and only if $Z(G) \simeq C_{p^{\gamma_1}}$ is cyclic and either $G/G' \simeq Z_2(G)/Z(G)$ or $d(G) = d(Z_2(G)/Z(G)), \beta_i = \gamma_1$ for $1 \leq i \leq r$ and $\beta_i = \alpha_i$ for $r+1 \leq i \leq n$, where $r, 1 \leq r \leq n$, is the largest such that $\alpha_r \geq \gamma_1$.

1.2 — Basics

In this section, we give a quick review of some of the basic facts of group theory that are assumed in the foregoing chapters. The definitions and proofs of results presented here can be found in any standard book on group theory. Let X be a nonempty subset of a group G. Define the subgroup generated by X, denoted by $\langle X \rangle$, to be the intersection of all subgroups of G which contain X. In a real sense $\langle X \rangle$ is the smallest subgroup of G containing X. Clearly $X = \langle X \rangle$ precisely when X itself is a subgroup. If X is non-empty, then $\langle X \rangle$ contains every finite product of the type

$$x_1^{m_1} x_2^{m_2} \cdots x_r^{m_r}, \;\; r \geq 1, \; x_i \in X, \; m_i = \pm 1,$$

and conversely all such products form a subgroup of G containing X. It follows that $\langle X \rangle$ consists of all such products. A cyclic group is thus generated by a single element. We shall denote a cyclic group of order m by C_m. The rank of a group G is the smallest cardinality of a generating set of G and is denoted by $d(G)$. That is,

$$d(G) = min\{|X| : X \subseteq G, \langle X \rangle = G\}.$$

The exponent of a group G is the least natural number n such that $g^n = 1$ for all $g \in G$ and is denoted by $exp(G)$. Observe that the least common multiple of the orders of the elements of a finite group G is the exponent of G. For a p-group G and a positive integer i, we write $\Omega_i(G) = \langle x \in G : x^{p^i} = 1\rangle$ and $\mho_i(G) = \langle x^{p^i} : x \in G\rangle$.

The commutator of two elements a and b of a group G is the element $[a, b] = a^{-1}b^{-1}ab$ of G and the commutator subgroup or the derived subgroup G' of G is the subgroup of G generated by all commutators of G. That is,

$$G' = \langle [a, b] : a, b \in G\rangle.$$

It is easy to see that G' is a normal subgroup of G. If X and Y are two subsets of G, then we define $[X, Y] = \langle [x, y] : x \in X, y \in Y\rangle$. Thus $[X, Y]$ is always a subgroup of G. Observe that $G' = [G, G]$. For $x \in G$, $[x, G]$ denotes the set of all commutators $[x, g]$, where $g \in G$. The followings are well known commutator identities

$$[x, yz] = [x, z][x, y][x, y, z]; \quad [xy, z] = [x, z][x, z, y][y, z],$$

where $x, y, z \in G$ and will be frequently used in the thesis without any reference.

Given a group G and a subgroup H of G, a series from H to G is a finite sequence

$$H = G_0 \leq G_1 \leq \cdots \leq G_n = G \tag{1.1}$$

of subgroups of G where each G_i is a subgroup of its successor. If $H = 1$, we say that (1.1) is a series for G. The subgroups G_i in this series are called terms. The length of the series is the number of terms excluding G itself. The series (1.1) is called proper if no two of the terms are equal, that is, $G_i < G_{i+1}$ for $i = 0, 1, ..., n - 1$. The series (1.1) is called subnormal series if each G_i is a normal subgroup of its

successor, and is called normal series if each G_i is a normal subgroup of G. The quotient groups G_{i+1}/G_i are called the factor groups of the series. The normal series above is called a central series if for each i, $G_{i+1}/G_i \leq Z(G/G_i)$. Let $Z_0 = 1$ and let $Z_{i+1}/Z_i = Z(G/Z_i)$ for $i \geq 0$. Observe that Z_1 is the center of G and Z_{i+1}/Z_i, being the center of G/Z_i, is normal in G/Z_i and hence Z_{i+1} is normal in G for all $i \geq 0$. It follows that the series

$$1 = Z_0 \leq Z_1 \leq Z_2 \leq \cdots$$

is a central series of G. The subgroup Z_i is called the i-th center and this series is called the upper central series of G.

We define subgroups $\gamma_i(G)$, $i \geq 1$, of G by setting

$$\gamma_1(G) = G, \;\; \gamma_{i+1}(G) = [\gamma_i(G), G].$$

Observe that $\gamma_2(G) = G'$, each $\gamma_i(G)$ is normal in G and $\gamma_{i+1}(G) \leq \gamma_i(G)$. The series

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \cdots \gamma_n(G) \geq \cdots$$

is called the lower central series of G. If the lower central series of a group G terminates in a finite number of steps at 1, and if c is the least natural number such that $\gamma_{c+1}(G) = 1$, then G is called a nilpotent group of class c. The class of a nilpotent group is denoted by $cl(G)$. Observe that if $cl(G) = 2$, then $G' \leq Z(G)$.

A proper subgroup M of G is maximal if whenever $M \subseteq H \subseteq G$, then either $H = M$ or $H = G$. The intersection of all the maximal subgroups of G is the Frattini subgroup $\Phi(G)$ of G. If G has no maximal subgroup, then $\Phi(G) = G$. An element g of G is called a non-generator of G if whenever $\langle H \cup \{g\} \rangle = G$, then

$\langle H \rangle = G$ for all $H \subseteq G$. An interesting fact of $\Phi(G)$ is that it is equal to the set of all non-generators of G.

Two elements a and b of G are called conjugate if there exists an element g of G such that $b = g^{-1}ag$. It is easily seen that "conjugacy" is an equivalence relation on G and therefore it partitions G into equivalence classes. The equivalence class that contains the element a of G is called the conjugacy class of a and is denoted as a^G. That is,

$$a^G = \{gag^{-1} : g \in G\}.$$

Let H be a non-empty subset of G. The set of elements of G which commute with every element of H is called the centralizer of H in G, and is denoted as $C_G(H)$. That is,

$$C_G(H) = \{g \in G : hg = gh \ \forall h \in H\}.$$

It is easy to see that $C_G(H)$ is a subgroup of G. If $H = \{h\}$ is singleton, then $C_G(\{h\})$ is simply denoted as $C_G(h)$.

A finite group G is called a purely non-abelian group if it has no non-trivial abelian direct factor. If $Z(G)$ is cyclic or if $Z(G) \leq \Phi(G)$, then G is purely non-abelian. Let G_1 and G_2 be groups, and let ϕ be a map from G_1 to G_2. Then the map ϕ is called a homomorphism from G_1 to G_2 if for all $g, h \in G_1$,

$$\phi(gh) = \phi(g)\phi(h).$$

Let ϕ be a homomorphism from G_1 to G_2. Then

(*i*) ϕ is called the trivial homomorphism if $\phi(a) = 1$ for all $a \in G_1$.

(*ii*) ϕ is called a monomorphism if it is injective.

(*iii*) ϕ is called an epimorphism if it is surjective.

(*iv*) ϕ is called an isomorphism if it is bijective.

(*v*) ϕ is called an endomorphism if it is a homomorphism of G_1 to itself.

(*vi*) ϕ is called an automorphism if it is an isomorphism of G_1 to itself.

The set of all automorphisms of G is a group under the usual operation of compositions of mappings. We call this group the full automorphism group of G and denote it by $\mathrm{Aut}(G)$.

Let A be an abelian group and let $\mathrm{Hom}(G, A)$ denote the set of all homomorphisms of G into A. For $f, g \in \mathrm{Hom}(G, A)$, define $fg(x) = f(x)g(x)$. Then $\mathrm{Hom}(G, A)$ becomes an abelian group under this operation. If A, B, C are all finite abelian groups, then $\mathrm{Hom}(A, B \times C) \simeq \mathrm{Hom}(A, B) \times \mathrm{Hom}(A, C)$ and $\mathrm{Hom}(A, B) \simeq \mathrm{Hom}(B, A)$. Also, $\mathrm{Hom}(C_m, C_n) \simeq C_d$, where $d = gcd(m, n)$.

A group G is called a p-group, where p is prime, if order of every element of G is a power of p.

CHAPTER 2

On finite p-groups whose central automorphisms are all nth class-preserving

2.1 — Introduction

Yadav [45, Theorem A] gave necessary and sufficient conditions on a finite p-group G of class 2 such that $\mathrm{Aut}_c(G) = \mathrm{Autcent}(G)$. We call an automorphism α of G an nth class-preserving if for all $g \in G$, $\alpha(g) \in g^{\gamma_n(G)}$, where $\gamma_n(G)$ denotes the nth term of the lower central series of G. The set $\mathrm{Aut}_c^n(G)$ of all nth class-preserving automorphisms of G fixes $Z(G)$ element-wise and is a normal subgroup of $\mathrm{Aut}(G)$. Observe that $\mathrm{Aut}_c^n(G) = \mathrm{Aut}_c(G)$ for $n = 1$, and if G is a finite p-group of class $n+1$, then $\mathrm{Aut}_c^n(G)$ is a normal subgroup of $\mathrm{Autcent}(G)$. In this chapter, we give necessary and sufficient conditions for a finite p-group G of class $n+1$ such that $\mathrm{Aut}_c^n(G) = \mathrm{Autcent}(G)$, and obtain, as a consequence, Theorem A of Yadav [45] as a particular case.

2.2 — Main Results

Let $\mathrm{Hom}(G, A)$ denote the group of all homomorphisms of G into an abelian group A. The following three well-known lemmas will be used very frequently without

further referring.

Lemma 2.2.1 *Let A, B and C be finite abelian groups. Then*

(*i*) $\mathrm{Hom}(A \times B, C) \simeq \mathrm{Hom}(A, C) \times \mathrm{Hom}(B, C)$,

(*ii*) $\mathrm{Hom}(A, B \times C) \simeq \mathrm{Hom}(A, B) \times \mathrm{Hom}(A, C)$, *and*

(*iii*) *if B is a proper subgroup of C, then* $|\mathrm{Hom}(A, B)| \leq |\mathrm{Hom}(A, C)|$.

Lemma 2.2.2 $\mathrm{Hom}(C_n, C_m) \simeq C_d$, *where C_i denotes the cyclic group of order i and d is the greatest common divisor of n and m.*

Lemma 2.2.3 *Let A be any finite abelian group. Then*

$$|\mathrm{Hom}(C_{p^n}, A)| = |\mathrm{Hom}(C_{p^n}, \Omega_n(A))|.$$

For normal subgroups X and Y of G, let $\mathrm{Aut}^X(G)$ and $\mathrm{Aut}_Y(G)$ respectively denote the subgroups of $\mathrm{Aut}(G)$ centralizing G/X and Y. We denote the intersection $\mathrm{Aut}^X(G) \cap \mathrm{Aut}_Y(G)$ by $\mathrm{Aut}_Y^X(G)$. The following lemma is a little modification of arguments of [2, Lemma 3].

Lemma 2.2.4 *Let G be any group and Y be a central subgroup of G contained in a normal subgroup X of G. Then* $\mathrm{Aut}_X^Y(G) \simeq \mathrm{Hom}(G/X, Y)$.

Proof. For any $\mu \in \mathrm{Aut}_X^Y(G)$, define the map $\psi_\mu : G/X \longrightarrow Y$ as $\psi_\mu(bX) = b^{-1}\mu(b)$.

Now

$$\begin{aligned}
\psi_\mu((b_1X)(b_2X)) &= \psi_\mu(b_1b_2X) \\
&= (b_1b_2)^{-1}\mu(b_1b_2) \\
&= b_2^{-1}b_1^{-1}\mu(b_1)\mu(b_2) \\
&= (b_1^{-1}\mu(b_1))(b_2^{-1}\mu(b_2)) \\
&= \psi_\mu(b_1X)\psi_\mu((b_2X).
\end{aligned}$$

Thus ψ_μ is a homomorphism. Define the map

$$\psi : \mathrm{Aut}_X^Y(G) \longrightarrow \mathrm{Hom}(G/X, Y)$$

as $\psi(\mu) = \psi_\mu$. Let $\mu_2(b) = by$ for some $y \in Y$. Then

$$\begin{aligned}
\psi_{\mu_1\mu_2}(bX) &= b^{-1}\mu_1\mu_2(b) \\
&= b^{-1}\mu_1(\mu_2(b)) \\
&= b^{-1}\mu_1(by) \\
&= b^{-1}\mu_1(b)\mu_1(y) \\
&= b^{-1}\mu_1(b)y \\
&= b^{-1}\mu_1(b)b^{-1}\mu_2(b) \\
&= \psi_{\mu_1}(bX)\psi_{\mu_2}(bX).
\end{aligned}$$

Now $\psi_\mu(bX) = 1$ implies that $\mu(b) = b$ for all $b \in G$. Thus ψ is a monomorphism. For any $\tau \in \mathrm{Hom}(G/X, Y)$, define the map $\mu : G \longrightarrow G$ as $\mu(g) = g\tau(gX)$ for all

$g \in G$. Since $Y \leq Z(G)$,

$$\begin{aligned}
\mu(g_1g_2) &= g_1g_2\tau(g_1g_2X) \\
&= g_1g_2\tau((g_1X)(g_2X)) \\
&= g_1g_2\tau(g_1X)\tau(g_2X) \\
&= (g_1\tau(g_1X))(g_2\tau(g_2X)) \\
&= \mu(g_1)\mu(g_2).
\end{aligned}$$

Now $\mu(g) = 1$ implies that $g = (\tau(gX))^{-1} \in Y \leq X$, and therefore $g = 1$. Thus μ is a monomorphism. It is easy to see that μ is onto, and therefore μ is an automorphism of G inducing identity on both X and G/Y and $\psi(\mu) = \tau$. Hence ψ is onto as well. □

Lemma 2.2.5 *Let G be a finite non-abelian p-group such that $\mathrm{Aut}_c^n(G) = \mathrm{Autcent}(G)$. Then $Z(G) \leq \Phi(G)$ and*

$$\mathrm{Aut}_c^n(G) \simeq \mathrm{Hom}(G/\gamma_2(G), \gamma_{n+1}(G)) \simeq \mathrm{Hom}(G/Z(G), \gamma_{n+1}(G)).$$

Proof. On the contrary, assume that $Z(G) \nleq \Phi(G)$. Choose an element h in $Z(G) \setminus M$ for some maximal subgroup M of G. Then $G = M\langle h\rangle$. There exists a non-trivial element z in $Z(G) \cap \Phi(G)$ of order p. We prove that the map $\alpha : G \to G$, defined as $\alpha(mh^i) = mh^iz^i$ for every $m \in M$ and for every $i, 0 \leq i \leq p-1$, is a central automorphism but not an nth class-preserving automorphism of G. Let $m_1, m_2 \in M$

and $0 \leq i, j \leq p-1$. Then

$$\begin{aligned} \alpha(m_1h^im_2h^j) &= \alpha(m_1m_2h^{i+j}) \\ &= m_1m_2h^{i+j}z^{i+j} \\ &= (m_1h^iz^i)(m_2h^jz^j) \\ &= \alpha(m_1h^i)\alpha(m_2h^j). \end{aligned}$$

Thus α is a homomorphism. It follows from $\alpha(mh^i) = 1$ that $mh^i = z^{-i} \in M$. Since α fixes M element-wise, $mh^iz^i = \alpha(mh^i) = mh^i$. It implies that $mh^i = z^{-i} = 1$, and therefore α is one-one. Now $(mh^i)^{-1}\alpha(mh^i) = z^i \in Z(G)$ for all i, $0 \leq i \leq p-1$. Thus α is a central automorphism. Since $\alpha(h) = hz \neq h$, α is not an nth class-preserving automorphism of G, which is a contradiction. Thus $Z(G) \leq \Phi(G)$. For any $y \in \gamma_n(G)$, the inner automorphism ι_y induced by y is an element of $\mathrm{Aut}_c^n(G)$. It follows that $x^{-1}\iota_y(x) = x^{-1}y^{-1}xy = [x, y] \in Z(G)$ for all $x \in G$ and thus $\gamma_{n+1}(G) \leq Z(G)$. Hence $\mathrm{Aut}_c^n(G) \simeq \mathrm{Hom}(G/\gamma_{n+1}(G), \gamma_{n+1}(G)) \simeq \mathrm{Hom}(G/\gamma_2(G), \gamma_{n+1}(G))$ and $\mathrm{Aut}_c^n(G) \simeq \mathrm{Hom}(G/Z(G), \gamma_{n+1}(G))$ by Lemma 2.2.4 because $\mathrm{Aut}_c^n(G)$ fixes $Z(G)$ element-wise. □

Let G be a finite non-abelian p-group of class $n+1$. Let

$$\begin{aligned} G/\gamma_2(G) &\simeq C_{p^{a_1}} \times C_{p^{a_2}} \times \cdots \times C_{p^{a_k}}, \\ \gamma_{n+1}(G) &\simeq C_{p^{b_1}} \times C_{p^{b_2}} \times \cdots \times C_{p^{b_l}}, \textit{and} \\ Z(G) &\simeq C_{p^{c_1}} \times C_{p^{c_2}} \times \cdots \times C_{p^{c_m}} \end{aligned}$$

be the cyclic decompositions of respective abelian groups, where $a_i \geq a_{i+1}, b_i \geq b_{i+1}$ and $c_i \geq c_{i+1}$ are positive integers. Since $\gamma_{n+1}(G)$ is a subgroup of $Z(G)$, $l \leq m$ and $b_j \leq c_j$ for all j, $1 \leq j \leq l$.

A non-abelian group G that has no non-trivial abelian direct factor is said to be purely non-abelian. Observe that a group G is purely non-abelian if $Z(G)$ is

contained in $\Phi(G)$.

Proposition 2.2.6 ([1, Theorem 1]) *If G is a purely non-abelian group, then there is a one-to-one correspondence between* $\mathrm{Autcent}(G)$ *and* $\mathrm{Hom}(G/G', Z(G))$.

Theorem 2.2.7 *Let G be a finite non-abelian p-group of class $n+1$. Then the following two statements are equivalent:*

(1) $\mathrm{Aut}_c^n(G) = \mathrm{Autcent}(G)$,

(2) $\mathrm{Aut}_c^n(G) \simeq \mathrm{Hom}(G/\gamma_2(G), \gamma_{n+1}(G))$ *and one of the following two conditions holds:*

   (a) $\gamma_{n+1}(G) = Z(G)$ *or*

   (b) $Z(G) \leq \Phi(G), l = m$, *and* $a_1 \leq b_s$, *where s is the largest integer between 1 and l such that $b_s < c_s$.*

Proof. First suppose that $\mathrm{Aut}_c^n(G) = \mathrm{Autcent}(G)$. Then, by Lemma 2.2.5, $Z(G) \leq \Phi(G)$ and $\mathrm{Aut}_c^n(G) \simeq \mathrm{Hom}(G/\gamma_2(G), \gamma_{n+1}(G))$, and by Proposition 2.2.6

$$|\,\mathrm{Autcent}(G)| = |\,\mathrm{Hom}(G/\gamma_2(G), Z(G))|.$$

Assume that $\gamma_{n+1}(G) < Z(G)$. Since

$$|\,\mathrm{Hom}(G/\gamma_2(G), \gamma_{n+1}(G))| = |\,\mathrm{Hom}(G/\gamma_2(G), Z(G))|,$$

it follows that

$$\prod_{i=1}^{k}\prod_{j=1}^{l} p^{\min\{a_i,b_j\}} = \prod_{i=1}^{k}\prod_{j=1}^{m} p^{\min\{a_i,c_j\}}.$$

Now $l \leq m$ and $b_j \leq c_j$ for each j, $1 \leq j \leq l$, therefore $\min\{a_i, b_j\} \leq \min\{a_i, c_j\}$ for all i, $1 \leq i \leq k$ and for all j, $1 \leq j \leq l$. If $l < m$, then $|\,\mathrm{Hom}(G/\gamma_2(G), \gamma_{n+1}(G))| <$

$|\operatorname{Hom}(G/\gamma_2(G), Z(G))|$, which is not so. Thus $l = m$ and $\min\{a_i, b_j\} = \min\{a_i, c_j\}$ for all i, $1 \leq i \leq k$ and for all j, $1 \leq j \leq l$. Since $\gamma_{n+1}(G) < Z(G)$, there exists some j between 1 and l such that $b_j < c_j$. Let s be the largest integer between 1 and l such that $b_s < c_s$. If $a_1 > b_s$, then $b_s = \min\{a_1, b_s\} = \min\{a_1, c_s\} > b_s$, a contradiction.

Conversely, if $\gamma_{n+1}(G) = Z(G)$ and $\operatorname{Aut}_c^n(G) \simeq \operatorname{Hom}(G/\gamma_2(G), \gamma_{n+1}(G))$, then the result holds trivially by using Proposition 2.2.6. We, therefore, suppose that $\operatorname{Aut}_c^n(G) \simeq \operatorname{Hom}(G/\gamma_2(G), \gamma_{n+1}(G))$, $Z(G) \leq \Phi(G), l = m$, and $a_1 \leq b_s$, where s is the largest integer between 1 and l such that $b_s < c_s$. Now

$$|\operatorname{Hom}(G/\gamma_2(G), \gamma_{n+1}(G))| = \prod_{i=1}^{k}\prod_{j=1}^{l} p^{\min\{a_i, b_j\}},$$

and

$$|\operatorname{Hom}(G/\gamma_2(G), Z(G))| = \prod_{i=1}^{k}\prod_{j=1}^{l} p^{\min\{a_i, c_j\}}.$$

Observe that $a_i \leq b_j \leq c_j$ for all i, $1 \leq i \leq k$ and for all j, $1 \leq j \leq s$, and $b_j = c_j$ for all j, $s+1 \leq j \leq l$. It follows that

$$\begin{aligned} |\operatorname{Hom}(G/\gamma_2(G), \gamma_{n+1}(G))| &= \prod_{i=1}^{k}\prod_{j=1}^{l} p^{\min\{a_i, b_j\}} \\ &= p^{s(a_1+a_2+\cdots+a_k)} \prod_{i=1}^{k}\prod_{j=s+1}^{l} p^{\min\{a_i, b_j\}}, \end{aligned}$$

and

$$\begin{aligned} |\operatorname{Hom}(G/\gamma_2(G), Z(G))| &= \prod_{i=1}^{k}\prod_{j=1}^{l} p^{\min\{a_i,c_j\}} \\ &= p^{s(a_1+a_2+\cdots+a_k)} \prod_{i=1}^{k}\prod_{j=s+1}^{l} p^{\min\{a_i,b_j\}}. \end{aligned}$$

Thus $|\operatorname{Hom}(G/\gamma_2(G), \gamma_{n+1}(G))| = |\operatorname{Hom}(G/\gamma_2(G), Z(G))|$. Since $Z(G) \leq \Phi(G)$, by Proposition 2.2.6 it follows that $|\operatorname{Autcent}(G)| = |\operatorname{Hom}(G/\gamma_2(G), Z(G))|$. Hence by the given hypothesis and the fact that $\operatorname{Aut}_c^n(G) \leq \operatorname{Autcent}(G)$, we have $\operatorname{Aut}_c^n(G) = \operatorname{Autcent}(G)$. □

We now give an example of a group which satisfies the hypothesis of the Theorem 2.2.7. Its GAP id is 740.

Let $G = \langle f_1, f_2, f_3, f_4, f_5, f_6, f_7\rangle$ be a 2-group of order 2^7 with the following relations:

$f_1^2 = f_2^2 = f_3^2 = f_6^2 = f_7^2 = 1, f_4^2 = f_5^2 = f_7, [f_2, f_1] = f_4, [f_3, f_1] = f_5, [f_3, f_2] = f_6, [f_4, f_1] = [f_5, f_1] = [f_6, f_1] = [f_4, f_2] = [f_4, f_3] = [f_5, f_3] = f_7, [f_5, f_2] = [f_6, f_2] = [f_6, f_3] = [f_5, f_4] = [f_6, f_4] = [f_6, f_5] = [f_7, f_1] = [f_7, f_2] = [f_7, f_3] = [f_7, f_4] = [f_7, f_5] = [f_7, f_6] = 1.$

In this group $G' = \Phi(G) = \langle f_4, f_5, f_6, f_7\rangle$, $\gamma_3(G) = Z(G)$, $f_7 \in Z(G)$.

By using the following commands in GAP:

$A := AutomorphismGroup(G);$
$I := InnerAutomorphismsAutomorphismGroup(A);$
$C := Centraliser(A, I);$
$Elements(C);$

we have the following eight central automorphisms:

$\phi_1(f_1f_2f_3f_4f_5) = f_1f_2f_3f_4f_5f_7, \phi_1(f_1f_4f_6f_7) = f_1f_4f_6, \phi_1(f_2f_7) = f_2$

$\phi_2(f_1f_2f_3f_4f_5) = f_1f_2f_3f_4f_5f_7, \phi_2(f_1f_4f_6f_7) = f_1f_4f_6, \phi_2(f_2f_7) = f_2f_7$

$\phi_3(f_1f_2f_3f_4f_5) = f_1f_2f_3f_4f_5f_7, \phi_3(f_1f_4f_6f_7) = f_1f_4f_6f_7, \phi_3(f_2f_7) = f_2$

$\phi_4(f_1f_2f_3f_4f_5) = f_1f_2f_3f_4f_5f_7, \phi_4(f_1f_4f_6f_7) = f_1f_4f_6f_7, \phi_4(f_2f_7) = f_2f_7$

$\phi_5(f_1f_2f_3f_4f_5) = f_1f_2f_3f_4f_5, \phi_5(f_1f_4f_6f_7) = f_1f_4f_6, \phi_5(f_2f_7) = f_2f_7$

$\phi_6(f_1f_2f_3f_4f_5) = f_1f_2f_3f_4f_5, \phi_6(f_1f_4f_6f_7) = f_1f_4f_6, \phi_6(f_2f_7) = f_2$

$\phi_7(f_1f_2f_3f_4f_5) = f_1f_2f_3f_4f_5, \phi_7(f_1f_4f_6f_7) = f_1f_4f_6f_7, \phi_7(f_2f_7) = f_2$

$\phi_8(f_1f_2f_3f_4f_5) = f_1f_2f_3f_4f_5, \phi_8(f_1f_4f_6f_7) = f_1f_4f_6f_7, \phi_8(f_2f_7) = f_2f_7.$

It is easy to see that

$$\begin{aligned}
\phi_1(f_1f_2f_3f_4f_5) &= f_1f_2f_3f_4f_5f_7\\
&= f_1f_2f_3f_4f_5f_4^2\\
&= f_1f_2f_3f_4f_4f_5f_4\\
&= f_1f_2f_4f_3[f_3,f_4]f_4f_5f_4\\
&= f_1f_2f_4f_3f_4f_5f_4f_7\\
&= f_1f_4f_2f_3f_4f_5f_4\\
&= f_7f_4f_1f_2f_3f_4f_5f_4\\
&= f_4^{-1}(f_1f_2f_3f_4f_5)f_4\\
\phi_1(f_1f_4f_6f_7) &= f_1f_4f_6\\
&= f_1f_4f_6f_7f_7\\
&= f_1f_4f_6f_7f_4^2\\
&= f_1f_4f_4f_6f_7f_4\\
&= f_7f_4f_1f_4f_6f_7f_4\\
&= f_4^{-1}(f_1f_4f_6f_7)f_4\\
\phi_1(f_2f_7) &= f_2\\
&= f_2f_7f_7\\
&= f_2f_7f_4^2\\
&= f_2f_4f_7f_4\\
&= f_7f_4f_2f_7f_4\\
&= f_4^{-1}(f_2f_7)f_4.
\end{aligned}$$

Thus $\phi_1 \in \mathrm{Aut}_c^2(G)$. Similarly we can show that the other seven central automorphisms also belong to $\mathrm{Aut}_c^2(G)$, and therefore $\mathrm{Autcent}(G) \leq \mathrm{Aut}_c^2(G)$. But $\mathrm{Aut}_c^2(G) \leq \mathrm{Autcent}(G)$, and hence $\mathrm{Aut}_c^2(G) = \mathrm{Autcent}(G)$.

Let G be a finite abelian p-group and let $G \simeq C_{p^{\alpha_1}} \times C_{p^{\alpha_2}} \times \cdots \times C_{p^{\alpha_r}}$ be the cyclic decomposition of G such that $\alpha_1 \geq \alpha_2 \geq \ldots \geq \alpha_r \geq 1$. The integers $p^{\alpha_1}, p^{\alpha_2}, \ldots, p^{\alpha_r}$ are unique for G and are called the invariants of G. Yadav [45, Theorem A] proved that if G is a finite p-group of class 2 and $p^{m_1}, \ldots, p^{m_d}$ are the invariants of $G/Z(G)$, then $\mathrm{Aut}_c(G) = \mathrm{Autcent}(G)$ if and only if $\gamma_2(G) = Z(G)$ and $|\mathrm{Aut}_c(G)| = \prod_{i=1}^{d} |\Omega_{m_i}(\gamma_2(G))|$. As a particular case of Theorem 2.2.7, we give a short proof of this result of Yadav. We, however, use Lemma 3.1(3) and Lemma 3.5 of Yadav [45].

Proposition 2.2.8 ([10, Lemma 2.8]) *Let A and B be abelian groups with C a proper subgroup or quotient of A, and D a proper subgroup or quotient of B, such that $|A|/|C| = n = |B|/|D|$, for some $n > 1$. Then* $\mathrm{Hom}(C, D)$ *is isomorphic to a proper subgroup of* $\mathrm{Hom}(A, B)$.

A subset $\{y_1, y_2, ..., y_d\}$ of a finite abelian group Y is said to be a minimal basis for Y if

$$Y = \langle y_1 \rangle \times \langle y_2 \rangle \times \cdots \times \langle y_d \rangle$$

and

$$|\langle y_1 \rangle| \geq |\langle y_2 \rangle| \geq \cdots \geq |\langle y_d \rangle| \geq 1.$$

A minimal generating set $\{x_1, x_2, ..., x_d\}$ of a finite p-group G of class 2 is said to be distinguished if the set $\{\overline{x_1}, \overline{x_2}, ..., \overline{x_d}\}$, where $\overline{x_i} = x_i Z(G)$, forms a minimal basis

for $G/Z(G)$.

Proposition 2.2.9 ([45, Lemma 3.5]) *Let G be a finite p-group of class 2 such that $Z(G) \leq \Phi(G)$. Then the following statements hold true:*

(1) *Any minimal basis $\{\overline{x_1}, \overline{x_2}, ..., \overline{x_d}\}$ for $\overline{G} = G/Z(G)$ provides a distinguished minimal generating set $\{x_1, x_2, ..., x_d\}$ for G*

(2) *Any element $x \in G \setminus \Phi(G)$ can be included in a distinguished minimal generating set for G.*

Proof. Since $Z(G) \in \Phi(G)$,

$$G/\Phi(G) \simeq (G/Z(G))/(\Phi(G)/Z(G)) \simeq \overline{G}/\Phi(\overline{G}).$$

Therefore the set $\{x_1\Phi(G), x_2\Phi(G), ..., x_d\Phi(G)\}$ minimally generates $G/\Phi(G)$, and thus the set $\{x_1, x_2, ..., x_d\}$ minimally generates G. Let $x \in G\setminus\Phi(G)$. Then $xZ(G) \in (G/Z(G)) \setminus (\Phi(G)/Z(G))$. Hence the result follows. □

Proposition 2.2.10 ([45, Lemma 3.1(3)]) *Let G be a finite p-group of class 2. Then for $x \in G \setminus Z(G)$, $\exp([x, G]) = |\overline{x}|$, where $\overline{x} = xZ(G) \in G/Z(G)$.*

Proof. Let $|\overline{x}| = p^c$. Then $x^{p^c} \in Z(G)$. Let $[x, g] \in [x, G]$ be any element. Then $[x, g]^{p^c} = [x^{p^c}, g] = 1$, and thus $\exp([x, G]) \leq p^c$. If possible, suppose that $\exp([x, G]) = p^b < p^c$. Now for all $g \in G$, we have $[x^{p^b}, g] = [x, g]^{p^b} = 1$. It follows that $x^{p^b} \in Z(G)$, which is a contradiction. Hence $\exp([x, G]) = |\overline{x}|$ for all $x \in G \setminus Z(G)$. □

Corollary 2.2.11 ([45, Theorem A]) *Let G be a finite p-group of class 2 and let $p^{m_1}, \ldots, p^{m_d}$ be the invariants of $G/Z(G)$. Then $\mathrm{Aut}_c(G) = \mathrm{Autcent}(G)$ if and only if $\gamma_2(G) = Z(G)$ and $|\mathrm{Aut}_c(G)| = \prod_{i=1}^{d} |\Omega_{m_i}(\gamma_2(G))|$.*

Proof. First suppose that $\mathrm{Aut}_c(G) = \mathrm{Autcent}(G)$. Then, by Lemma 2.2.5,

$$\mathrm{Aut}_c(G) \simeq \mathrm{Hom}(G/Z(G), \gamma_2(G)).$$

By Theorem 2.2.7, either $\gamma_2(G) = Z(G)$ or $Z(G) \leq \Phi(G), l = m$, and $a_1 \leq b_s$, where s is the largest integer between 1 and l such that $b_s < c_s$. If $\gamma_2(G) < Z(G)$, then $G/Z(G)$ is a proper quotient of $G/\gamma_2(G)$ and

$$|(G/\gamma_2(G))/(G/Z(G))| = |Z(G)/\gamma_2(G)| > 1.$$

It thus follows from Proposition 2.2.8 that $\mathrm{Hom}(G/Z(G), \gamma_2(G))$ is isomorphic to a proper subgroup of $\mathrm{Hom}(G/\gamma_2(G), Z(G))$, which is a contradiction because by Proposition 2.2.6,

$$|\,\mathrm{Aut}_c(G)| = |\,\mathrm{Autcent}(G)| = |\,\mathrm{Hom}(G/\gamma_2(G), Z(G))|.$$

Thus $\gamma_2(G) = Z(G)$. Let $G/Z(G) \simeq \langle \overline{x_1} \rangle \times \langle \overline{x_2} \rangle \times \cdots \times \langle \overline{x_d} \rangle$ such that the order of $\overline{x_i} = x_i Z(G)$ is p^{m_i} for all i, $1 \leq i \leq d$. It follows from Proposition 2.2.9 that $\{x_1, x_2, ..., x_d\}$ is a distinguished minimal generating set for G. The map

$$f \longmapsto (f(x_1), f(x_2), ..., f(x_d))$$

is an injective map from $\mathrm{Aut}_c(G)$ to $x_1^G \times x_2^G \times \cdots \times x_d^G$. So $|\,\mathrm{Aut}_c(G)| \leq \prod_{i=1}^{d} |x_i^G|$. Now, $\exp([x_i, G]) = |\overline{x_i}| = |x_i Z(G)|$ by Proposition 2.2.10. Therefore, $\mathrm{Hom}(\langle \overline{x_i} \rangle, [x_i, G]) \simeq$

$[x_i, G]$ and hence

$$\begin{aligned} |\operatorname{Aut}_c(G)| &= |\operatorname{Hom}(G/Z(G), \gamma_2(G))| \\ &= \prod_{i=1}^{d} |\operatorname{Hom}(\langle \overline{x_i} \rangle, \gamma_2(G))| \\ &\geq \prod_{i=1}^{d} |\operatorname{Hom}(\langle \overline{x_i} \rangle, [x_i, G])| \\ &= \prod_{i=1}^{d} |[x_i, G]| \\ &= \prod_{i=1}^{d} |x_i^G|. \end{aligned}$$

Thus $|\operatorname{Aut}_c(G)| = \prod_{i=1}^{d} |x_i^G|$ and $|\operatorname{Hom}(\langle \overline{x_i} \rangle, \gamma_2(G))| = |\operatorname{Hom}(\langle \overline{x_i} \rangle, [x_i, G])|$ for every i, $1 \leq i \leq d$. It follows from Lemma 2.2.3 that

$$\begin{aligned} |[x_i, G]| &= |\operatorname{Hom}(\langle \overline{x_i} \rangle, [x_i, G])| \\ &= |\operatorname{Hom}(\langle \overline{x_i} \rangle, \gamma_2(G))| \\ &= |\operatorname{Hom}(\langle \overline{x_i} \rangle, \Omega_{m_i}(\gamma_2(G)))| \\ &= |\Omega_{m_i}(\gamma_2(G))|. \end{aligned}$$

Hence $|\operatorname{Aut}_c(G)| = \prod_{i=1}^{d} |\Omega_{m_i}(\gamma_2(G))|$.

Conversely, suppose that $|\operatorname{Aut}_c(G)| = \prod_{i=1}^{d} |\Omega_{m_i}(\gamma_2(G))|$ and $\gamma_2(G) = Z(G)$. Then

$$\begin{aligned}
|\operatorname{Aut}_c(G)| &= \prod_{i=1}^{d} |\Omega_{m_i}(\gamma_2(G))| \\
&= \prod_{i=1}^{d} |\operatorname{Hom}(\langle \overline{x_i} \rangle, \Omega_{m_i}(\gamma_2(G)))| \\
&= \prod_{i=1}^{d} |\operatorname{Hom}(\langle \overline{x_i} \rangle, \gamma_2(G))| \\
&= |\operatorname{Hom}(G/Z(G), \gamma_2(G))| \\
&= |\operatorname{Hom}(G/\gamma_2(G), Z(G))| \\
&= |\operatorname{Autcent}(G)|.
\end{aligned}$$

It now follows from $\operatorname{Aut}_c(G) \leq \operatorname{Autcent}(G)$ that $\operatorname{Aut}_c(G) = \operatorname{Autcent}(G)$. □

CHAPTER 3

On commuting automorphisms of finite p-groups with a metacyclic quotient

3.1 — Introduction.

Let G be a group. An automorphism α of G is called a commuting automorphism if $\alpha(x)x = x\alpha(x)$ for all $x \in G$. The set of all commuting automorphisms of G is denoted by $A(G)$. It is well-known that $A(G)$ does not necessarily form a subgroup of $\mathrm{Aut}(G)$, but it has a number of interesting properties (see [14]). In 1984, Herstein [20] proposed the following problem:

If G ***is a simple non-abelian group, then prove that*** $A(G) = 1$***.***

In 1986, giving an answer to this problem, Laffey [25] proved that if G has no non-trivial abelian normal subgroup, then $A(G) = 1$. Pettet (see [25]), in his personal communication, observed that if $Z(G) = 1$ and $G' = G$, then $A(G) = 1$. A group G is called an $A(G)$-group if the set $A(G)$ is a subgroup of $\mathrm{Aut}(G)$. In 2013, Vosooghpour and Malayeri [43] showed that minimum order of a non-$A(G)$ p-group is p^5. In 2013, Vosooghpour, Kargarian and Malayeri [44] obtained the structure of $A(G)$, where G is a non-abelian p-group of order p^n with cyclic maximal subgroup.

In 2015, Rai [35] gave some sufficient conditions on a finite p-group G such that $A(G)$ is a subgroup of $\mathrm{Aut}(G)$ and, as a consequence, proved that in a finite p-group G of co-class 2, where p is an odd prime, $A(G)$ is a subgroup of $\mathrm{Aut}(G)$. In 2016, Singh and Gumber [41] gave very elementary and short proofs of main results of Rai and obtained other related results. In 2019, Shahrabi, Malayeri and Vosooghpour [39] proved that a finite 2-group G of almost maximal class is an $A(G)$-group. Recently in 2019, Rai [36] proved that the direct product of two finite $A(G)$-groups is also an $A(G)$-group. He also proved that $GL(n,q)$ for $n = 3$ or $q > n$, $PSL(2,q)$ and ZM-groups are $A(G)$-groups.

In [16, Theorem 4.2], the authors have proved that if G is a finite non-abelian metacyclic p-group, then G is an $A(G)$-group. Observe that if G is metacyclic, then $G/Z(G)$ is also metacyclic. But the converse need not be true. This raises the obvious question:

Is G ***an*** $A(G)$***-group if*** $G/Z(G)$ ***is metacyclic?***

In this chapter, we prove the following result:

Theorem 3.1.1 *Let G be a finite non-abelian p-group, where p is odd prime, such that $G/Z(G)$ is metacyclic. Then G is an $A(G)$-group if and only if $cl(G) = 2$.*

3.2 — Main Results

Let G be a finite non-abelian p-group such that $G/Z(G)$ is metacyclic. Then there is a normal subgroup $M/Z(G)$ of $G/Z(G)$ such that both $M/Z(G)$ and

$$(G/Z(G))/(M/Z(G)) = G/M$$

are cyclic. Let $G/M = \langle aM \rangle$ and let $M/Z(G) = \langle bZ(G) \rangle$. Then

$$G = \langle a, b, Z(G) \rangle.$$

Since $G' \leq M = \langle b, Z(G) \rangle$, b commutes with every commutator, and hence $[a,b]^i = [a,b^i]$ for all $i \geq 1$. Let $|bZ(G)| = p^m$. Then $[a,b]^{p^m} = [a,b^{p^m}] = 1$. But for $0 < n < m$, $[a,b]^{p^n} = [a,b^{p^n}] \neq 1$. Hence $|[a,b]| = p^m$. For the rest of the paper we fix the above notation.

Proposition 3.2.1 ([21, Aufgaben. 2(b), p. 259]) *Let M be an Abelian normal subgroup of a finite group G with cyclic factor group G/M. Then $|M| = |G'||M \cap Z(G)|$.*

Proposition 3.2.2 ([43, Lemma 2.2]) *Let G be a group of nilpotency class 2. If $d(G/Z(G)) = 2$, then G is an $A(G)$-group.*

Proposition 3.2.3 ([21, Satz. III.10.2(c)]) *Let G be a p-group. If G' is cyclic and $p > 2$, then G is regular.*

Lemma 3.2.4 *Let $(a,m) = d$. Then the linear congruence $ax \equiv b(mod\ m)$ has a solution if and only if $d \mid b$. Moreover if $d \mid b$, then it has exactly d solutions modulo m.*

Proof. Firstly assume that $ax \equiv b(mod\ m)$ has a solution $x = x_0$. Then there exists $y_0 \in \mathbb{Z}$ such that $ax_0 - b = my_0$. Since $(a,m) = d$, $d \mid (ax_0 - my_0)$. Thus $d \mid b$.

Conversely assume that $d \mid b$. Then there exists $r \in \mathbb{Z}$ such that $b = dr$. It

follows from $(a, m) = d$ that $d = ax_0 + my_0$ for some $x_0, y_0 \in \mathbb{Z}$. Therefore

$$\begin{aligned} b &= dr \\ &= (ax_0 + my_0)r \\ &= a(rx_0) + m(ry_0) \end{aligned}$$

implies that $a(rx_0) = b + m(-ry_0)$. Thus $x = rx_0$ is a solution of $ax \equiv b(mod\ m)$. For $t \in \mathbb{Z}$, we have $a(x_0 + \frac{m}{d}t) \equiv ax_0(mod\ m) \equiv b(mod\ m)$. So for $t \in \mathbb{Z}$, $a(x_0 + \frac{m}{d}t)$ is also a solution of $ax \equiv b(mod\ m)$. Let $t_1, t_2 \in \{0, 1, 2, ..., d-1\}$ such that $x_0 + t_1\frac{m}{d} \equiv x_0 + t_2\frac{m}{d}(mod\ m)$. Then $t_1 \equiv t_2(mod\ d)$. Since $0 \leq t_1, t_2 \leq d-1$, $t_1 = t_2$. Therefore the integers of the set

$$\{x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, ..., x_0 + (d-1)\frac{m}{d}\}$$

are incongruent modulo m. Let $y = x_0 + \frac{m}{d}t$ be any solution of $ax \equiv b(mod\ m)$. Then by division algorithm, there exists integers q and r, $0 \leq r < d$ such that $t = qd + r$. Now

$$\begin{aligned} y &= x_0 + \frac{m}{d}t \\ &= x_0 + \frac{m}{d}(qd + r) \\ &= x_0 + mq + \frac{m}{d}r \\ &\equiv x_0 + \frac{m}{d}r(mod\ m). \end{aligned}$$

Hence $ax \equiv b(mod\ m)$ has exactly d solutions modulo m. □

As a particular case of Lemma 3.2.4, we have the following result:

Corollary 3.2.5 ([3, Corollary 5.1]) *If $(a, c) = 1$, then a has an inverse, and it is unique modulo c.*

Lemma 3.2.6 *Let G be a finite non-abelian p-group, where p is odd prime, such that $G/Z(G)$ is metacyclic. Then*

(*i*) $G' = \langle [a, b] \rangle$,

(*ii*) *if* $cl(G) = 2$, *then* G *is an* $A(G)$*-group,*

(*iii*) *if* $cl(G) > 2$, *then* $[a, b] = b^{p^j} z$, *for some fix* j, $0 \leq j < m$ *and* $z \in Z(G)$,

(*iv*) *if* $a^{t-1} \in C_G(G')$, *where* $t \geq 1$, *then* $[a^{rt}, b] = [a^t, b]^{1+k+k^2+\cdots+k^{r-1}} z_1$ *for any* $r \geq 1$, *where* $k = 1 - p^j$ *and* $z_1 \in Z(G)$.

Proof. (*i*) By Proposition 3.2.1, $|M| = |G'||M \cap Z(G)| = |G'||Z(G)|$. Therefore $|G'| = |M|/|Z(G)| = p^m$, and hence $G' = \langle [a, b] \rangle$ because $|[a, b]| = p^m$.

(*ii*) Since $d(G/Z(G)) = 2$ and $cl(G) = 2$, it follows from Proposition 3.2.2 that G is an $A(G)$-group.

(*iii*) Since $[a, b] \in G' \leq \langle b \rangle Z(G)$, $[a, b] = b^{rp^j} z$, where $(r, p) = 1$ and $z \in Z(G)$. Since $|bZ(G)| = p^m$ and $cl(G) > 2$, $0 \leq j < m$. Since G' is cyclic, G is regular by Proposition 3.2.3. Thus $[a, b]^{p^m} = [a, b^{p^m}] = 1$ implies that $[a, b]^{p^m} = [a^{p^m}, b] = 1$. Therefore $a^{p^m} \in Z(G)$. Hence $G' = \{[a^s, b] \mid 0 \leq s < p^m\}$. Since $(r, p) = 1$, there exists some integer q such that $(q, p) = 1$ and $rq \equiv 1 (mod\ |b|)$ by Corollary 3.2.5. Thus $(b^{rp^j} z)^q = b^{rqp^j} z^q = b^{p^j} z$ is a generator of G'. Therefore $b^{p^j} z = [a^s, b]$ for some integer $s, 0 \leq s < m$. If $(s, p) \neq 1$, then $s = pt$ for some $t \geq 1$. Since G is regular, $[a, b]^{p^m t} = 1$ implies that $[a^{p^m t}, b] = 1$. It further implies that $[a^s, b]^{p^{m-1}} = 1$, which is not so as $|[a^s, b]| = p^m$. Therefore $(s, p) = 1$.

(*iv*) Let $r = 2$. Then

$$\begin{aligned}
[a^{2t}, b] &= [a^t, b][a^t, b, a^t][a^t, b] \\
&= [a^t, b]^2[a^t, b, a^t] \\
&= [a^t, b]a^{-t}[a^t, b]a^t \\
&= [a^t, b]a^{-t+1}a^{-1}[a^t, b]aa^{t-1} \\
&= [a^t, b][a^t, b]^k z_1 \\
&= [a^t, b]^{1+k} z_1.
\end{aligned}$$

Assume that $[a^{rt}, b] = [a^t, b]^{1+k+k^2+\cdots+k^{r-1}} z_2$ for any $r > 2$, where $k = 1 - p^j$ and $z_2 \in Z(G)$. Now

$$\begin{aligned}
[a^{(r+1)t}, b] &= [a^{rt}, b][a^{rt}, b, a^t][a^t, b] \\
&= [a^t, b]a^{-t}[a^{rt}, b]a^t \\
&= [a^t, b]a^{-t+1}a^{-1}[a^{rt}, b]aa^{t-1} \\
&= [a^t, b][a^{rt}, b]^k z_3 \\
&= [a^t, b]([a^t, b]^{1+k+k^2+\cdots+k^{r-1}} z_2)^k z_3 \\
&= [a^t, b]^{1+k+k^2+\cdots+k^r} z_4.
\end{aligned}$$

□

Proposition 3.2.7 ([14, Lemma 2.1]) *If $\alpha \in A(G)$ and $x, y \in G$, then $[\alpha(x), y] = [x, \alpha(y)]$.*

Proof. Since $xy^{-1}\alpha(xy^{-1}) = \alpha(xy^{-1})xy^{-1}$, $xy^{-1}\alpha(x)\alpha(y^{-1}) = \alpha(x)\alpha(y^{-1})xy^{-1}$. It implies that $\alpha(x^{-1})y^{-1}\alpha(x)y = x^{-1}\alpha(y^{-1})x\alpha(y)$. Hence $[\alpha(x), y] = [x, \alpha(y)]$. □

Proposition 3.2.8 ([14, Lemma 2.4(ii)]) *Let G be a group and $\alpha \in A(G)$. Then $\alpha^n \in A(G)$ for all integers n.*

Proof. Let $\alpha \in A(G)$ and let $x \in G$. Then for $n \in \{0, 1\}$, $[\alpha^n(x), x] = 1$. Assume that $[\alpha^m(x), x] = 1$ for any integer $m \geq 2$ and for all $x \in G$. By Proposition 3.2.7, we have

$$\begin{aligned} [\alpha^{m+2}(x), x] &= [\alpha^{m+1}(x), \alpha(x)] \\ &= \alpha([\alpha^m(x), x]) \\ &= 1. \end{aligned}$$

Hence $\alpha^n \in A(G)$ for all integers n. □

Proposition 3.2.9 ([14, Lemma 2.4(vi)]) *Let G be a group. Then $\alpha\beta \in A(G)$ if and only if $[\alpha(x), \beta(x)] = 1$ for all $x \in G$.*

Proof. Observe that $\alpha\beta \in A(G)$ if and only if $[x, \alpha\beta(x)] = 1$ for all $x \in G$ if and only if $[\alpha(x), \beta(x)] = 1$ for all $x \in G$ by Proposition 3.2.7. □

Proof of Theorem 3.1.1: If $cl(G) = 2$, then G is an $A(G)$-group by Lemma 3.2.6(ii). Conversely, suppose that G is an $A(G)$-group. We prove that $cl(G) = 2$. On the contradiction, assume that $cl(G) > 2$. Then $[a, b] = b^{p^j} z$, where $0 \leq j < m$ and $z \in Z(G)$ by Lemma 3.2.6(iii). Let $\alpha \in A(G)$. Then $\alpha(a) = a^{i_1} b^{j_1} c_1$ and $\alpha(b) = a^{i_2} b^{j_2} c_2$ for some $c_1, c_2 \in Z(G)$. Since $[x, \alpha(x)] = 1$ for all $x \in G$, we can write $\alpha(a) = a^{i_1} z_1$ and $\alpha(b) = b^{i_2} z_2$ for some $z_1, z_2 \in Z(G)$. Similarly for $\beta \in A(G)$, we can assume $\beta(a) = a^{i_3} z_3$ and $\beta(b) = b^{i_4} z_4$ for some $z_3, z_4 \in Z(G)$. Let $g \in G$.

Then $g = a^r b^s z_5$ for some $z_5 \in Z(G)$. Therefore, by using commutator identities

$$\begin{aligned}
[\alpha(g), \beta(g)] &= [\alpha(a^r b^s z_5), \beta(a^r b^s z_5)] \\
&= [\alpha(a)^r \alpha(b)^s, \beta(a)^r \beta(b)^s] \\
&= [a^{ri_1} b^{si_2}, a^{ri_3} b^{si_4}] \\
&= [a^{ri_1}, b^{si_4}][b^{si_2}, a^{ri_3}] \\
&= [a^{ri_1}, b]^{si_4} [a^{ri_3}, b]^{-si_2}.
\end{aligned}$$

Now $[a^{ri_1}, b] = [a^{i_1}, b]^{1+k+k^2+\cdots+k^r} z_6$ and $[a^{ri_2}, b] = [a^{i_2}, b]^{1+k+k^2+\cdots+k^r} z_7$ for some $z_6, z_7 \in Z(G)$ by Lemma 3.2.6(iv). It follows from Proposition 3.2.7 that $[a^{i_1}, b] = [a, b^{i_2}]$ and $[a^{i_3}, b] = [a, b^{i_4}]$. Hence

$$\begin{aligned}
[\alpha(g), \beta(g)] &= ([a^{i_1}, b]^{1+k+k^2+\cdots+k^r} z_6)^{si_4} ([a^{i_3}, b]^{1+k+k^2+\cdots+k^r} z_7)^{-si_2} \\
&= ([a, b^{i_2}]^{1+k+k^2+\cdots+k^r} z_6)^{si_4} ([a, b^{i_4}]^{1+k+k^2+\cdots+k^r} z_7)^{-si_2} \\
&= ([a, b]^{i_2(1+k+k^2+\cdots+k^r)} z_6)^{si_4} ([a, b]^{i_4(1+k+k^2+\cdots+k^r)} z_7)^{-si_2} \\
&= z_6^{si_4} z_7^{-si_2}.
\end{aligned}$$

Now we can take i_1, i_2, r, s such that $[\alpha(g), \beta(g)] \neq 1$. For example, let $i_1 = i_2 = 1, r = 2, s = 1$. Then

$$\begin{aligned}
[\alpha(g), \beta(g)] &= [a^2, b]^{i_4} [a^{2i_3}, b]^{-1} \\
&= ([a, b]^{2-p^j})^{i_4} ([a^{i_3}, b]^{1+k} z)^{-1} \\
&= ([a, b]^{2-p^j})^{i_4} ([a, b^{i_4}]^{2-p^j} z)^{-1} \\
&= z^{-1} \neq 1.
\end{aligned}$$

Hence G is not an $A(G)$-group by Proposition 3.2.9, which is a contradiction. Hence $cl(G) = 2$.

CHAPTER 4

On commuting automorphisms of some finite p-groups

4.1 — Introduction

Let G be a group. An automorphism α of G is called a commuting automorphism of G if for each $x \in G$, $\alpha(x)$ commutes with x. The set of all commuting automorphisms of G is denoted by $A(G)$. A group G is called an $A(G)$-group if the set $A(G)$ forms a subgroup of $\mathrm{Aut}(G)$.

Let $\alpha, \beta \in A(G)$ and $x \in G$. Then, by [14, Lemma 2.2], $\alpha(x) = xc_1$ and $\beta(x) = xc_2$ for some $c_1, c_2 \in C_G(G')$. Therefore, if $C_G(G')$ is abelian, then $[\alpha(x), \beta(x)] = [x^{-1}\alpha(x), \beta(x)] = [x^{-1}\alpha(x), x^{-1}\beta(x)] = 1$ because x^{-1} commutes with both $\alpha(x)$ and $\beta(x)$. Therefore G is an $A(G)$-group by Proposition 3.2.8 and Proposition 3.2.9. Observe that $Z_2(G) \leq C_G(G')$. Rai [35, Lemma 3.2] proved that if G is a finite p-group, where p is an odd prime, such that $Z_2(G)$ is abelian, then G is an $A(G)$-group. This raises the obvious question:

Is G an $A(G)$-group if $C_G(\Phi(G))$ is abelian?

In this chapter, we prove the following result:

Theorem 4.1.1 *Let G be a finite non-abelian p-group such that $C_G(\Phi(G))$ is cyclic. Then G is an $A(G)$-group.*

For $x \in G$, let $[x, G]$ denote the set $\{[x, g] \mid g \in G\}$. Let G be a finite p-group and N be a non-trivial normal subgroup of G. The pair (G, N) is called a Camina pair if $N \subseteq [x, G]$ for all $x \in G \setminus N$. A finite p-group G is called Frattinian if $Z(M) \neq Z(G)$ for all maximal subgroups M of G. A Frattinian p-group G satisfying $C_G(Z(\Phi(G))) = \Phi(G)$ is called strongly Frattinian. In 2013, Vosooghpour and Akhavan-Malayeri [43] showed that for each $n \geq 5$, there exists a non-$A(G)$ p-group of order p^n. They, in fact, proved that if G is an extra-special p-group of order $\geq p^5$, then G is not an $A(G)$-group. Observe that if G is a finite extra-special p-group, then G is Frattinian and $(G, Z(G))$ is a Camina pair. The converse is true if $cl(G) = 2$ (see Proposition 4.2.8). The following example shows that the converse is false if $cl(G) \geq 3$.

Example 4.1.2 *Let G be the group defined by the presentation*

$$G = \langle a, c \mid a^{p^n} = c^{p^{n+1}} = 1, c^a = c^{1+p} \rangle,$$

where p is an odd prime. Then

- $|G| = p^{2n+1}$.
- *$Z(G) = \langle c^{p^n} \rangle$ has order p and $(G, Z(G))$ is a Camina pair.*
- *$\Phi(G) = G^p G' = \langle a^p, c^p \rangle$, and thus G has $p + 1$ maximal subgroups. All the maximal subgroups have the center of order p^2.*
- *G has nilpotency class $n + 1$.*

These observations suggest the following natural question:

Does there exist a finite Frattinian p-group G with $(G, Z(G))$ a Camina pair which is an $A(G)$-group?

We answer this question in affirmative in this chapter when p is odd and $G/Z(G)$ is purely non-abelian. More precisely, we prove the following result:

Theorem 4.1.3 *Let G be a finite Frattinian p-group such that $G/Z(G)$ is purely non-abelian and $(G, Z(G))$ is a Camina pair. Then G is strongly Frattinian, and if p is odd, then G is an $A(G)$-group.*

4.2 — Main Results

In [44, Theorem 1.5], the authors have proved that if G is a finite non-abelian p-group with a cyclic maximal subgroup, then G is an $A(G)$-group. We generalize this by proving the following result.

Proposition 4.2.1 *Let G be a finite non-abelian p-group with an abelian maximal subgroup M. Then G is an $A(G)$-group.*

Proof. Since G is non-abelian, $M \leq MZ(G) < G$, and thus $Z(G) \leq M$. We prove that $C_G(g)$ is abelian for all $g \in G - Z(G)$. If $g \in M - Z(G)$, then $C_G(g) = M$ is abelian. Let $g \in G - M$. Then $G = M\langle g\rangle$ and thus $M \cap C_G(g) = Z(G)$. By Dedekind's Modular Law,

$$\begin{aligned} C_G(g) &= G \cap C_G(g) \\ &= M\langle g\rangle \cap C_G(g) \\ &= (M \cap C_G(g))\langle g\rangle \\ &= Z(G)\langle g\rangle. \end{aligned}$$

Thus $C_G(g)$ is abelian for all $g \in G - Z(G)$. Let $\alpha, \beta \in A(G)$ and $g \in G$. Then $[\alpha(g), \beta(g)] = 1$ and hence G is an $A(G)$-group by Proposition 3.2.9. □

Proposition 4.2.2 ([21, Satz. III.7.8(c)]) *If $Z(\Phi(G))$ is cyclic, $\Phi(G)$ is also cyclic.*

Proposition 4.2.3 ([6, Theorem 1.2]) *Let G be a non-abelian p-group of order p^{n+1} with cyclic maximal subgroup. Then G is isomorphic to one of the following groups:*

(i) $M_{p^{n+1}} = \langle a, b \mid a^{p^n} = b^p = 1, b^{-1}ab = a^{1+p^{n-1}} \rangle$, *where $n \geq 3$ and p is odd prime.*

(ii) $D_{2^{n+1}} = \langle a, b \mid a^{2^n} = b^2 = 1, bab = a^{-1} \rangle$.

(iii) $Q_{2^{n+1}} = \langle a, b \mid a^{2^n} = b^2 = a^{2^{n-1}}, b^{-1}ab = a^{-1} \rangle$.

(iv) $SD_{2^{n+1}} = \langle a, b \mid a^{2^n} = b^2 = 1, bab = a^{-1+2^{n-1}} \rangle$, *where $n \geq 3$.*

Proposition 4.2.4 ([21, Satz. III.10.7(a)]) *Let G be a regular p-group. Then $|G/\Omega_k(G)| = |\mho_k(G)|$.*

Proposition 4.2.5 ([21, Satz. III.8.2(a)]) *If the p-group G has only one subgroup of order p, then for $p > 2$, G is cyclic.*

Proof of Theorem 4.1.1: Observe that if $C_G(\Phi(G))$ is cyclic, then $Z(\Phi(G))$ is also cyclic, and therefore $\Phi(G)$ is cyclic by Proposition 4.2.2. Now $\Phi(G)$ is not contained in $Z(G)$, because if $\Phi(G) \leq Z(G)$, then $G = C_G(\Phi(G))$ is abelian. We therefore assume that $|\Phi(G)| > p$. Since $\Phi(G)$ is cyclic, $\Phi(G) = \langle x \rangle$ for some $x \in G$. Let $|\Phi(G)| = p^m, |G'| = p^r$ and $|G^p| = p^s$. We prove that either $\Phi(G) = G^p$ or $\Phi(G) = G'$. On the contradiction suppose that $r, s < m$. Without any loss of generality, we assume that $s \geq r$. Let $x = ab$, for some $a \in G'$ and $b \in G^p$. Then

$x^{p^s} = (ab)^{p^s} = a^{p^s}b^{p^s} = 1$, which is a contradiction. Hence either $\Phi(G) = G^p$ or $\Phi(G) = G'$.

We prove that $\Phi(G) = G^p$. On the contradiction suppose that $\Phi(G) \neq G^p$. Then $\Phi(G) = G' = \langle [a,b] \rangle$ for some $a, b \in G$. Since $|\Phi(G)| > p$, $|[a,b]| \geq p^2$. Let $H = \langle a, b \rangle$ and let $|H| = p^n$. Then H has no cyclic maximal subgroup, because if H has a cyclic maximal subgroup, then it follows from Proposition 4.2.3 that $[a,b] \in \langle a^p \rangle \leq G^p$, which contradicts our assumption. Since $\Phi(H) \leq \Phi(G)$ is cyclic, either $\Phi(H) = H^p$ or $\Phi(H) = H'$. If $\Phi(H) = H^p$, then $\Phi(H) = \langle h^p \rangle$ for some $h \in H$. Thus

$$p^{n-2} = |\Phi(H)| = |\langle h^p \rangle| < |\langle h \rangle|$$

implies that $\langle h \rangle$ is maximal in H, which is not so. Therefore $H^p < H' = \Phi(H)$, and hence p is odd because if $p = 2$, then $H' \leq H^2$. Since $H' = \Phi(H)$ is cyclic, H is regular by Proposition 3.2.3. Since $\Omega_s(H/\Omega_{r-s}(H)) = \Omega_r(H)/\Omega_{r-s}(H)$ for $r > s$, it follows from Proposition 4.2.4 that

$$\begin{aligned} |\Omega_1(H/\Omega_1(H))| &= |\Omega_2(H)/\Omega_1(H)| \\ &= |(H/\Omega_1(H))/(H/\Omega_2(H))| \\ &= |(H/\Omega_1(H))|/|(H/\Omega_2(H))| \\ &= |\mho_1(H)/\mho_2(H)| \\ &\leq p. \end{aligned}$$

Since H is regular, $H/\Omega_1(H)$ is regular and

$$\Omega_1(H) = \langle x \in H \mid x^p = 1 \rangle = \{x \in H \mid x^p = 1\}.$$

Thus $H/\Omega_1(H)$ has at most one subgroup of order p. Since p is odd, $H/\Omega_1(H)$ is

cyclic by Proposition 4.2.5, and so $H' \leq \Omega_1(H)$. Since H is regular, $\exp(\Omega_1(H)) = p$. It follows that $\exp(H') = p$, and therefore $|\Phi(H)| = |H'| = p$, which is again not possible because H' has an element $[a, b]$ of order $\geq p^2$. It follows that $\Phi(G) = G^p$.

Let $\Phi(G) = \langle g^p \rangle$ and let $h \in G - C_G(\Phi(G))$. Then $h^p \in C_G(\Phi(G))$, and therefore $\langle g, h \rangle$ has a cyclic maximal subgroup $\langle g \rangle$. Since $[g^p, h] \neq 1$, it follows from Proposition 4.2.3 that $p = 2$. Since $G' < \Phi(G) = \langle g^2 \rangle < \langle g \rangle$, $\langle g \rangle$ is normal in G and $G/\langle g \rangle$ has exponent 2. Let φ_a denote the inner automorphism of G induced by $a \in G$. Then

$$\begin{aligned} \varphi_a(\varphi_a(g^i)) &= \varphi_a(a^{-1}g^i a) \\ &= a^{-2}g^i a^2 \\ &= g^i. \end{aligned}$$

Thus every non-trivial automorphism induced on $\langle g \rangle$ by G has order 2. Therefore, its restriction on $\langle g^2 \rangle$ is trivial or inverting. It follows that $|G/C_G(\Phi(G))| = 2$, and hence G is an $A(G)$-group by Proposition 4.2.1.

Proposition 4.2.6 ([27, Corollary 2.4]) *If (G, H) is a Camina pair and G has class 2, then*

(*i*) *G is a special p-group; and*

(*ii*) *$H = G'$.*

Lemma 4.2.7 *Let G be a finite Frattinian p-group such that $(G, Z(G))$ is a Camina pair. Then $|Z(G)| = p$.*

Proof. Since $(G, Z(G))$ is a Camina pair, there exists $x \in G - Z(G)$ such that

$$Z(G) \subseteq [x, G] \subseteq G' \leq \Phi(G).$$

Thus $Z(G) \leq M$ for all maximal subgroups M of G and therefore $Z(G) \leq Z(M)$. Since G is Frattinian, $Z(G) < Z(M)$. Let $g \in G - M$ and $x \in Z(M) - Z(G)$. Then

$$\begin{aligned} [x, G] &= [x, \langle g \rangle M] \\ &= [x, M][x, \langle g \rangle][x, \langle g \rangle, M] \\ &= [x, \langle g \rangle] \\ &= \{[x, g^i] \mid 1 \leq i \leq p\}. \end{aligned}$$

It follows that $[x, G]$ has p elements, and hence $|Z(G)| = |[x, G]| = p$. □

Proposition 4.2.8 *Let G be a finite Frattinian p-group of nilpotence class 2 such that $(G, Z(G))$ is a Camina pair. Then G is extra-special.*

Proof. Since $cl(G) = 2$, G is a special p-group by Proposition 4.2.6. Thus G is an extra-special p-group, because $|Z(G)| = p$ by Lemma 4.2.7. □

Proposition 4.2.9 ([27, Theorem 2.2]) *Let (G, H) be a Camina pair, let $H = Z(G)$, and let G have class c. Then $Z_r(G)/Z_{r-1}(G)$ has exponent p for all $1 \leq r \leq c$.*

Proposition 4.2.10 ([14, Lemma 2.4(viii)]) *Let G be a group and let $\alpha \in A(G)$. Then $\alpha^2 \in \mathrm{Autcent}(G)$ if and only if $G' \leq C_G(\alpha)$.*

Proof. Let $\alpha^2 \in \mathrm{Autcent}(G)$. Then for all $y \in G$, $\alpha^2(y) = yz$ for some $z \in Z(G)$. Let $x, y \in G$. Then by Proposition 3.2.7,

$$\begin{aligned} \alpha^2 \in \mathrm{Autcent}(G) &\iff [x, y] = [x, \alpha^2(y)] \\ &\iff [x, y] = [\alpha(x), \alpha(y)] = \alpha([x, y]) \\ &\iff G' \leq C_G(\alpha). \end{aligned}$$

□

Proposition 4.2.11 ([14, Lemma 2.2]) *Let G be a group, let $\alpha \in A(G)$, and let $y \in G$. Then $[y, \alpha] \in C_G(G')$.*

Proof. Let $x, y, z \in G$. Then by Proposition 3.2.7,

$$\begin{aligned} [\alpha(xy), z] &= [\alpha(x)\alpha(y), z] \\ &= [\alpha(x), z][\alpha(x), z, \alpha(y)][\alpha(y), z] \\ &= [x, \alpha(z)][\alpha(x), z, \alpha(y)][y, \alpha(z)]. \end{aligned}$$

Also $[xy, \alpha(z)] = [x, \alpha(z)][x, \alpha(z), y][y, \alpha(z)]$. Since $[\alpha(xy), z] = [xy, \alpha(z)]$ by Proposition 3.2.7, $[x, \alpha(z)][\alpha(x), z, \alpha(y)][y, \alpha(z)] = [x, \alpha(z)][x, \alpha(z), y][y, \alpha(z)]$. Therefore $[\alpha(x), z, \alpha(y)] = [x, \alpha(z), y]$. Thus

$$\begin{aligned} [\alpha(x), z, \alpha(y)] = [\alpha(x), z, y] &\implies [[\alpha(x), z], \alpha(y)] = [[\alpha(x), z], y] \\ &\implies (\alpha(y))^{-1}[\alpha(x), z]\alpha(y) = y^{-1}[\alpha(x), z]y \\ &\implies y^{-1}\alpha(y) \in C_G([\alpha(x), z]) \\ &\implies y^{-1}\alpha(y) \in C_G(G'). \end{aligned}$$

Hence $[y, \alpha] \in C_G(G')$ for all $y \in G$ and for all $\alpha \in A(G)$. □

Let $E_2(G) = \{g \in G \mid [g, x, x] = 1 \ \forall x \in G\}$ denote the set of right 2-Engel elements of G.

Proposition 4.2.12 ([14, Proposition 2.5]) *Let G be a group. Then $E_2(G)$ is a subgroup of G and $E_2(G)' \leq Z_2(G)$.*

Proposition 4.2.13 ([14, Lemma 2.6(i)]) *Let G be a group and let $\alpha \in A(G)$. then $[G, \alpha] \leq E_2(G)$.*

Proof. Let $x, y \in G$. Then by Proposition 3.2.7 and Proposition 4.2.11,

$$\begin{aligned}
[x^{-1}\alpha(x), y] &= [x^{-1}, y][x^{-1}, y, \alpha(x)][\alpha(x), y] \\
&= [x^{-1}, y][[x^{-1}, y], (x^{-1}\alpha(x))x][x, \alpha(y)] \\
&= [x^{-1}, y][[x^{-1}, y], x][[x^{-1}, y], x^{-1}\alpha(x)][[x^{-1}, y], x^{-1}\alpha(x), x][x, \alpha(y)] \\
&= [x^{-1}, y][x^{-1}, y, x][x, \alpha(y)] \\
&= y^{-1}x^{-1}y(\alpha(y))^{-1}x\alpha(y) \\
&= y^{-1}x^{-1}(\alpha(y))^{-1}yxy^{-1}\alpha(y)y \\
&= y^{-1}[x, y^{-1}\alpha(y)]y.
\end{aligned}$$

Therefore

$$\begin{aligned}
[y, x^{-1}\alpha(x)] &= ([x^{-1}\alpha(x), y])^{-1} \\
&= (y^{-1}[x, y^{-1}\alpha(y)]y)^{-1} \\
&= y^{-1}([x, y^{-1}\alpha(y)])^{-1}y \\
&= y^{-1}([y^{-1}\alpha(y), x])y \\
&= y^{-1}(x^{-1}[y, x^{-1}\alpha(x)]x)y \\
&= (xy)^{-1}[y, x^{-1}\alpha(x)](xy).
\end{aligned}$$

It implies that $[y, x^{-1}\alpha(x)] \in C_G(xy)$ for all $x, y \in G$. Now, replacing y by $x^{-1}y$ gives that $[x^{-1}y, x^{-1}\alpha(x)] \in C_G(y)$. It follows that $[y, x^{-1}\alpha(x)] \in C_G(y)$. Thus $[x^{-1}\alpha(x), y, y] = 1$ for all $y \in G$, and hence $[G, \alpha] \leq E_2(G)$. □

Proposition 4.2.14 ([14, Theorem 1.4]) *If G is a group and $\alpha \in A(G)$, then $[G^2, \alpha] \subseteq Z_2(G)$.*

Proof. Let $x \in E_2(G) \cap C_G(G')$ such that $I_x \in \mathrm{Inn}(G)$. Then for all $y \in G$,

$$\begin{aligned}
[I_x(y), y] &= [(x^{-1}y)x, y] \\
&= [x^{-1}y, y][x^{-1}y, y, x][x, y] \\
&= [x^{-1}, y][x^{-1}, y, y][x, y] \\
&= [x^{-1}, y][x, y] \\
&= [x^{-1}, y]x^{-1}y^{-1}xy \\
&= x^{-1}[x^{-1}, y]y^{-1}xy \\
&= 1.
\end{aligned}$$

Thus $I_x \in A(G)$. Since $x \in C_G(G')$, I_x fixes G' element-wise, and therefore $I_x^2 \in \mathrm{Autcent}(G)$ by Proposition 4.2.10. Let $I_x^2(g) = gz$ for some $z \in Z(G)$. Then

$$\begin{aligned}
I_{x^2}(g) = gz &\implies g^{-1}x^{-2}gx^2 = z \\
&\implies x^2 \in Z_2(G).
\end{aligned}$$

Thus $(E_2(G) \cap C_G(G'))/Z_2(G)$ is an elementary abelian 2-group by Proposition 4.2.12. Since $[G, \alpha] \subseteq E_2(G) \cap C_G(G')$ by Proposition 4.2.11 and Proposition 4.2.13, $[G, \alpha]^2 \subseteq Z_2(G)$, and hence $[G^2, \alpha] \subseteq Z_2(G)$. □

Proposition 4.2.15 ([35, Lemma 3.2]) *Let p be an odd prime and let G be a finite p-group such that $Z_2(G)$ is abelian. Then G is an $A(G)$-group.*

Proof. Since p is odd, $G^2 = G$. Therefore, by Proposition 4.2.14, $x^{-1}\alpha(x), x^{-1}\beta(x) \in Z_2(G)$ for all $x \in G$ and for all $\alpha, \beta \in A(G)$. Since $Z_2(G)$ is abelian, $[\alpha(x), \beta(x)] = [x^{-1}\alpha(x), x^{-1}\beta(x)] = 1$ and thus G is an $A(G)$-group by Proposition 3.2.9. □

Proof of Theorem 4.1.3: It follows from [38, Theorem] that either

(*i*) $G = E_1E_2\cdots E_n$ is the central product of non-abelian p-groups E_i, where $[E_i, E_j] = 1$ for all $i \neq j$, $|E_i| = p^2|Z(G)|$, and $Z(G) = Z(E_i)$ for all $1 \leq i \leq n$ or

(*ii*) $G = E \cdot F$ is the central product of Frattinian subgroups E and F, where $C_F(Z(\Phi(F))) = \Phi(F), E = C_G(F)$ and $\Phi(E) \leq Z(G)$.

Moreover, in case (*ii*), either $E = Z(G)$ (and therefore $G = F$, because $E = Z(G) \leq \Phi(G)$) or E is a central product as in case (*i*).

If G is the central product as in (*i*), then since $|Z(G)| = p$ by Lemma 4.2.7, $|E_i| = p^3$ for each i and therefore G is extra-special, which is a contradiction to the fact that $cl(G) \geq 3$. Therefore, suppose that G has the structure as in case (*ii*). We prove that $G = F$. Contrary assume that $G \neq F$. Then $G \simeq (E \times F)/Z_0$, where $Z_0 \leq Z(G)$ is isomorphic to some subgroups of $Z(E)$ and $Z(F)$. Since $|Z(G)| = p$, either $Z_0 = 1$ or $Z_0 = Z(G)$. If $Z_0 = 1$, then $Z(G) \simeq Z(E) \times Z(F)$, which is not possible because $|Z(G)| = p$. So assume that $Z_0 = Z(G)$. Then $E \cap F = Z(G)$ and therefore $G/Z(G) \simeq E/Z(G) \times F/Z(G)$. This is a contradiction as $G/Z(G)$ is purely non-abelian and $E/Z(G)$ is abelian. Thus $G = F$. Then $C_G(Z(\Phi(G))) = \Phi(G)$ and hence G is strongly Frattinian. Now suppose that p is odd. Since $(G, Z(G))$ is a Camina pair, it follows from Proposition 4.2.9 that $Z_2(G)/Z(G)$ is elementary abelian and therefore $Z_2(G) \leq C_G(\Phi(G)) = Z(\Phi(G))$. Thus $Z_2(G)$ is abelian and hence G is an $A(G)$-group by Proposition 4.2.15.

CHAPTER 5

On finite p-groups whose central automorphisms are all inner

5.1 — Introduction

An automorphism α of a group G is called derival automorphism if $g^{-1}\alpha(g) \in G'$ for all $g \in G$. The set $D(G)$ of all derival automorphisms of G is a subgroup of $\mathrm{Aut}(G)$. An automorphism α of a group G is called a central automorphism if it commutes with all inner automorphisms, or equivalently, $g^{-1}\alpha(g) \in Z(G)$ for all $g \in G$. The set $\mathrm{Autcent}(G)$ of all central automorphisms of G fixes the commutator subgroup G' element-wise and is a normal subgroup of $\mathrm{Aut}(G)$. The groups G satisfying one of the following equalities have been well studied in the literature:

- $\mathrm{Autcent}(G) = \mathrm{Inn}(G)$ [11]
- $\mathrm{Autcent}(G) = Z(\mathrm{Inn}(G))$ [10, 18, 40]
- $D(G) = \mathrm{Inn}(G)$ [34].

Observe that the problem of finding finite p-groups G for which $\mathrm{Autcent}(G) \leq \mathrm{Inn}(G)$ is equivalent to finding finite p-groups G for which $\mathrm{Autcent}(G) = Z(\mathrm{Inn}(G))$,

that is, Autcent(G) is minimal. In case of nilpotence class 2, this is equivalent to finding finite p-groups G for which Autcent(G) = Inn(G). This case was settled by Curran and McCaughan [11] in 2001. They proved that if G is a finite p-group, then Autcent(G) = Inn(G) if and only if $G' = Z(G)$ and $Z(G)$ is cyclic. In 2004, Curran [10] gave two necessary conditions for a finite non-abelian p-group G to have minimal number of central automorphisms. He proved that if G is a finite non-abelian p-group such that Autcent(G) = Z(Inn(G)), then $Z(G) \leq G'$ and Z(Inn(G)) is not cyclic. These conditions are necessary but not sufficient. In 2013, Sharma and Gumber [40] proved that if G is a finite p-group of order p^5 or p^6, then Autcent(G) = Z(Inn(G)) if and only if G is of rank 2 and $|Z(G)| = p$. In 2015, Gumber and Kalra [18] characterized finite p-groups G of co-class up to 4 and groups of order up to p^7 for which Autcent(G) is minimal.

Let G be a finite p-group and let $G/G' \simeq \prod_{i=1}^{n} C_{p^{\alpha_i}}$ and $Z_2(G)/Z(G) \simeq \prod_{i=1}^{m} C_{p^{\beta_i}}$ be the cyclic decompositions of respective abelian groups, where $\alpha_i \geq \alpha_{i+1}$ and $\beta_i \geq \beta_{i+1}$ are positive integers. Gumber and Kalra [18, Theorem 2.1] gave necessary and sufficient conditions on G for which Autcent(G) = Z(Inn(G)) in the case when $Z(G)$ is cyclic. More precisely, they proved the following result:

Theorem 5.1.1 *Let G be a finite non-abelian p-group such that $Z(G) \simeq C_{p^{\gamma_1}}$ is cyclic. Then* Autcent(G) = Z(Inn(G)) *if and only if either $G/G' \simeq Z_2(G)/Z(G)$ or $d(G) = d(Z_2(G)/Z(G)), \beta_i = \gamma_1$ for $1 \leq i \leq r$ and $\beta_i = \alpha_i$ for $r+1 \leq i \leq n$, where $r, 1 \leq r \leq n$, is the largest such that $\alpha_r \geq \gamma_1$.*

Let G be a finite p-group and let $W(G)/Z(G) = \Omega_1(Z_2(G)/Z(G))$. In this chapter, we prove the following main result:

Theorem 5.1.2 *Let G be a finite non-abelian p-group such that $W(G)$ is non-abelian. Then* $\mathrm{Autcent}(G) = Z(\mathrm{Inn}(G))$ *if and only if $Z(G) \simeq C_{p^{\gamma_1}}$ is cyclic and either $G/G' \simeq Z_2(G)/Z(G)$ or $d(G) = d(Z_2(G)/Z(G)), \beta_i = \gamma_1$ for $1 \leq i \leq r$ and $\beta_i = \alpha_i$ for $r+1 \leq i \leq n$, where $r, 1 \leq r \leq n$, is the largest such that $\alpha_r \geq \gamma_1$.*

5.2 — Main Results

Observe that if $Z_2(G)/Z(G)$ is elementary abelian, then $W(G) = Z_2(G)$. It thus follows that there are a large number of finite p-groups G for which $W(G)$ is non-abelian. We start with the following lemma.

Lemma 5.2.1 *Let G be a finite non-abelian p-group such that*

$$\mathrm{Autcent}(G) = Z(\mathrm{Inn}(G)).$$

Then $C_G(W(G)) = \Phi(G)$.

Proof. Let M be a maximal subgroup of G and let $g_0 \in G - M$. Let $z_0 \in Z(G) \cap M$ be of order p. Now, we prove that the map $\alpha : G \to G$ defined as $\alpha(g_0) = g_0 z_0$ and $\alpha(m) = m$, for all $m \in M$, can be extended to a central automorphism of G. Let the map $\alpha : G \to G$ be defined as $\alpha(mg_0^i) = mg_0^i z_0^i$ for all $m \in M$ and for all i, $0 \leq i \leq p-1$. Let $m_1, m_2 \in M$ and $0 \leq i, j \leq p-1$. Then

$$\begin{aligned}
\alpha(m_1 g_0^i m_2 g_0^j) &= \alpha(m_1 g_0^i m_2 g_0^{-i} g_0^i g_0^j) \\
&= \alpha(m_1 (g_0^i m_2 g_0^{-i}) g_0^{i+j}) \\
&= m_1 (g_0^i m_2 g_0^{-i}) g_0^{i+j} z_0^{i+j} \\
&= (m_1 g_0^i z_0^i)(m_2 g_0^j z_0^j) \\
&= \alpha(m_1 g_0^i)\alpha(m_2 g_0^j).
\end{aligned}$$

Thus α is a homomorphism. It follows from $\alpha(mg_0^i) = 1$ that $mg_0^i = z_0^{-i} \in M$. Since α fixes M element-wise, $mg_0^i z_0^i = \alpha(mg_0^i) = mg_0^i$. It implies that $z_0^{-i} = 1$, and therefore $mg_0^i = 1$. Thus α is one-one. Now $(mg_0^i)^{-1}\alpha(mg_0^i) = z_0^i \in Z(G)$ for all i, $0 \leq i \leq p-1$. Thus α is a central automorphism. By assumption, $\alpha = \theta_{a_M}$, the inner automorphism induced by some $a_M \in G$. For any $x = mg_0^i \in G$, we have $\alpha(x) = \theta_{a_M}(x) = a_M^{-1} x a_M$. It follows that $xz_0^i = a_M^{-1} x a_M$. It implies that $a_M \in Z_2(G)$. Therefore

$$\begin{aligned} [x, a_M^p] &= [x, a_M]^p \\ &= z_0^{ip} \\ &= 1. \end{aligned}$$

Thus $a_M \in W(G)$. For any $m \in M$, we have

$$m = \alpha(m) = \theta_{a_M}(m) = a_M^{-1} m a_M.$$

It follows that $M = C_G(a_M)$. Since $[Z_2(G), G'] = 1$,

$$\begin{aligned} [W(G), \Phi(G)] &= [W(G), G^p G'] \\ &= [W(G), G'][W(G), G^p][W(G), G^p, G'] \\ &= [W(G), G'] \\ &= 1. \end{aligned}$$

Therefore $\Phi(G) \leq C_G(W(G))$. It thus follows that

$$\Phi(G) \leq C_G(W(G)) \leq \bigcap_M C_G(a_M) = \bigcap_M M = \Phi(G),$$

and hence $C_G(W(G)) = \Phi(G)$. □

Proposition 5.2.2 ([10, Corollary 3.7(i)]) *Let G be a non-abelian p-group. If* $\mathrm{Autcent}(G) = Z(\mathrm{Inn}(G))$*, then* $Z(G) \leq G'$.

Proposition 5.2.3 *Let G be a finite non-abelian p-group with non-abelian $W(G)$ such that* $\mathrm{Autcent}(G) = Z(\mathrm{Inn}(G))$*. Then $Z(G)$ is cyclic.*

Proof. It follows from Proposition 5.2.2 that $Z(G) \leq \Phi(G)$. For $x \in G$ and $H \leq G$, let $\overline{x}$ and $\overline{H}$ denote the coset $x\Phi(G)$ and the quotient group $H\Phi(G)/\Phi(G)$ respectively. For each $w \in W(G)$, define the map $f_w : \overline{W(G)} \to \Omega_1(Z(G))$ as $f_w(\overline{v}) = [v, w]$ for all $v \in W(G)$. Let $v_1, v_2 \in W(G)$. Then, since $Z_2(G) = \{x \in G \mid [x, y] \in Z(G)\ \forall y \in G\}$,

$$\begin{aligned} f_w(\overline{v_1}\ \overline{v_2}) &= [v_1v_2, w] \\ &= [v_1, w][v_1, w, v_2][v_2, w] \\ &= [v_1, w][v_2, w] \\ &= f_w(\overline{v_1})f_w(\overline{v_2}). \end{aligned}$$

Thus f_w is a homomorphism. For all $w_1, w_2 \in W(G)$, we have

$$\begin{aligned} f_{w_1w_2}(\overline{v}) &= [v, w_1w_2] \\ &= [v, w_2][v, w_1][v, w_1, w_2] \\ &= [v, w_2][v, w_1] \\ &= [v, w_1][v, w_2] \\ &= f_{w_1}(\overline{v})f_{w_2}(\overline{v}). \end{aligned}$$

Thus the map

$$f : W(G) \to \mathrm{Hom}(\overline{W(G)}, \Omega_1(Z(G)))$$

defined as $f(w) = f_w$ for all $w \in W(G)$ is then a homomorphism with

$$\mathrm{Ker}(f) = W(G) \cap C_G(W(G)) = W(G) \cap \Phi(G).$$

We prove that f is an epimorphism. Let $\alpha \in \mathrm{Hom}(\overline{W(G)}, \Omega_1(Z(G)))$. Since $\overline{G}$ is elementary abelian, the homomorphism α can be extended to the homomorphism $\beta : \overline{G} \to \Omega_1(Z(G))$ defined by

$$\beta(\overline{w}) = \begin{cases} \alpha(\overline{w}) & \text{if} \quad w \in W(G) \\ 1 & \text{if} \quad w \in G - W(G). \end{cases}$$

Define the map $\sigma_\beta : G \to G$ as $\sigma_\beta(g) = g\beta(\overline{g})$. Now

$$\begin{aligned} \sigma_\beta(g_1 g_2) &= g_1 g_2 \beta(\overline{g_1 g_2}) \\ &= g_1 g_2 \beta(\overline{g_1}\ \overline{g_2}) \\ &= g_1 g_2 \beta(\overline{g_1})\beta(\overline{g_2}) \\ &= (g_1 \beta(\overline{g_1}))(g_2 \beta(\overline{g_2})) \\ &= \sigma_\beta(g_1)\sigma_\beta(g_2). \end{aligned}$$

Now $\sigma_\beta(g) = 1$ implies that $g\beta(\overline{g}) = 1$. So

$$g = (\beta(\overline{g}))^{-1} \in \Omega_1(Z(G)) \leq \Phi(G).$$

Therefore $g = (\beta(\overline{g}))^{-1} = 1$. Also $g^{-1}\sigma_\beta(g) = \beta(\overline{g}) \in \Omega_1(Z(G)) \leq Z(G)$. Thus σ_β is a central automorphism. By assumption, $\sigma_\beta = \theta_a$ for some $a \in W(G)$. Therefore,

for each $w \in W(G)$,

$$\begin{aligned} \alpha(\overline{w}) &= \beta(\overline{w}) \\ &= w^{-1}\sigma_\beta(w) \\ &= w^{-1}\theta_a(w) \\ &= [w, a] \\ &= f_a(\overline{w}), \end{aligned}$$

and hence f is an epimorphism. It follows from second isomorphism theorem that

$$\frac{W(G)}{W(G) \cap \Phi(G)} \simeq \overline{W(G)} \simeq \mathrm{Hom}(\overline{W(G)}, \Omega_1(Z(G))),$$

and thus $d(Z(G)) = 1$. □

The proof of Theorem 5.1.2 now follows from Theorem 5.1.1 and Proposition 5.2.3.

List of References

[1] Adney, J. E. and Yen, T. *Automorphisms of a p-group*, Illinois J. Math. **9** (1965), 137-143.

[2] Alperin, J. L. *Groups with finitely many automorphisms.* Pacific J. Math. **12** (1962), 1-5.

[3] Andrews, G. E. *Number Theory*, W. B. Saunders Company, Philadelphia, London, Toront (1971).

[4] Ban, G. and Yu, S. *Minimal abelian groups that are not automorphism groups*, Arch. Math. **70** (1998), 427–434.

[5] Bell, H. E. and Martindale, W. S., *Centralizing mappings of semiprime rings*, Canad. Math. Bull. **30** (1987), 92-101.

[6] Berkovich, Y. *Groups of prime power order*, Vol.1, Walter de Gruyter, Berlin (2008).

[7] Bresar, M. *Commuting maps: A Survey*, Taiwan. J. Math. **8(3)** (2004), 361-397.

[8] Curran, M. J. *A non-abelian automorphism group with all automorphisms central*, Bull. Austral. Math. Soc., **26** (1982), 393-387.

[9] Curran, M. J. *Semidirect product groups with abelian automorphism groups*, J. Austral. Math. Soc. Ser. A **42** (1987), 84–91.

[10] Curran, M. J. *Finite groups with central automorphism group of minimal order.* Math. Proc. R. Ir. Acad. A **104(2)** (2004), 223-229.

[11] Curran, M. J. and McCaughan, D. J. *Central automorphisms that are almost inner*, Comm. Algebra, **29** (2001), 2081-2087.

[12] Das, A. K. *A survey on the estimation of commutativity in finite groups*, South-east Asian Bull. Math. **37** (2013), 161-180.

[13] Deaconescu, M. and Walls, G. L. *Right 2-engel elements and commuting automorphisms of groups*, J. Algebra **238** (2001), 479-484.

[14] Deaconescu, M., Silberberg, G. and Walls, G. L. *On commuting automorphisms of groups*, Arch. Math. **79** (2002), 423-429.

[15] Divinsky, N. *On commuting automorphisms of rings*, Trans. Roy. Soc. Canad. III **49** (1955), 19-22.

[16] Fouladi, S. and Orfi, R. *Commuting automorphisms of some finite groups*, Glas. Mat. Ser. III, **48(68)** (2013), 91-96.

[17] Glasby, S. P. *2-groups with every automorphism central*, J. Austral. Math. Soc. Ser. A **41** (1986), 233-236.

[18] Gumber, D. and Kalra, H. *Finite p-groups with central automorphism group of minimal order*, Comm. Algebra **43** (2015), 1802-1806.

[19] Heineken, H. *Nilpotente Gruppen, deren samtliche Normalteiler charakteristisch sind*, Arch. Math. (Besel) **33** (1980), 497-503.

[20] Herstein, I. N. *Problems and Solutions: Elementary Problems: E3039*, Amer. Math. Monthly **91(3)** (1984), 203.

[21] Huppert, B. *Endliche Gruppen I*, Springer-Verlag, Berlin, Heidelberg, New York (1967).

[22] Jain, V. K. and Yadav, M. K. *On finite p-groups whose automorphisms are all central*, Israel J. Math. **189** (2012), 225-236.

[23] Jonah, D. and Konvisser, M. *Some non-abelian p-groups with abelian automorphism groups*, Arch. Math. **26** (1975), 131–133.

[24] Kalra, H. and Gumber, D. *On equality of central and class preserving automorphisms of finite p-groups*, Indian J. Pure and Appl. Math. **44** (2013), 711-725.

[25] Laffey, T. J. *Problems and Solutions: Solutions of Elementary Problems: E3039*, Amer. Math. Monthly **93(10)** (1986), 816-817.

[26] Luh, J. *A note on commuting automorphisms of rings*, Amer. Math. Monthly **77** (1970), 61-62.

[27] Macdonald, I. D. *Some p-groups of Frobenius and extra-special type*, Israel J. Math. **40** (1981), 350-364.

[28] Malone, J. J. *p-groups with non-abelian automorphism groups and all automorphisms central*, Bull. Austral. Math. Soc., **29** (1984), 35-37.

[29] Malinowska, I. *On quasi-inner automorphisms of a finite p-group*, Publ. Math. Debrecen **41(1-2)** (1992), 73–77.

[30] Malinowska, I. *p-automorphisms of finite p-groups - problems and questions*, Advances in Group Theory, Aracne Editrice, Rome (2002), 111 - 127.

[31] Mann, A. *Some questions about p-groups*, J. Austral. Math. Soc. Ser. A **67(3)** (1999), 356–379.

[32] Miller, G. A. *A non-abelian group whose group of isomorphisms is abelian*, Messenger of Math. **43** (1913), 124–125.

[33] Morigi, M. *On the minimal number of generators of finite non-abelian p-groups having an abelian automorphism group*, Comm. Algebra **23(6)** (1995), 2045–2065.

[34] Narain, S. and Karan, R. *On equality of derival and inner automorphisms of some p-groups*, Cogent Math. and Stat. (2016), https://doi.org/10.1080/23311835.2016.1193103.

[35] Rai, P. K. *On commuting automorphisms of finite p-groups*, Proc. Japan Acad., Ser. A **91(5)** (2015), 57-60.

[36] Rai, P. K. *On commuting automorphisms of finite groups*, Ricerche di Matematica (2019), https://doi.org/10.1007/s11587-019-00444-0.

[37] Rehman, N. ur and Filippis, V. De *On n-commuting and n-skew-commuting maps with generalized derivations in prime and semiprime rings* , Sib. Math. J. **52(3)** (2011), 516-523.

[38] Schmid, P. *Frattinian p-groups*, Geom. Dedicata **36** (1990), 359-364.

[39] Shahrabi, N. A., Malayeri, M. A. and Vosooghpour, F. *Commuting automorphisms of finite 2-groups of almost maximal class, I*, J. Algebra Appl. (2019), https://doi.org/10.1142/S0219498819502086.

[40] Sharma, M. and Gumber, D. *On central automorphisms of finite p-groups*, Comm. Algebra **41** (2013), 1117-1122.

[41] Singh, S. and Gumber, D. *A note on commuting automorphisms of some finite p-groups*, Math. Notes **100(5)** (2016), 755-757.

[42] Tiwari, S. K., Sharma, R. K. and Dhara, B. *Derivations vanishing on commutators with generalized derivation of order 2 in prime rings* , Comm. Algebra **45(8)** (2017), 3542-3554.

[43] Vosooghpour, F. and Akhavan-Malayeri, M. *On commuting automorphisms of p-groups*, Comm. Algebra **41(4)** (2013), 1292-1299.

[44] Vosooghpour, F., Kargarian, Z. and Akhavan-Malayeri, M. *Commuting automorphisms of p-groups with cyclic maximal subgroups*, Commun. Korean Math. Soc. **28(4)** (2013), 643-647.

[45] Yadav, M. K. *On finite p-groups whose central automorphisms are all class preserving*, Comm. Algebra **41(12)** (2013), 4576-4592.

[46] Zhang, R., Chen, D. and Liu, S. *Characterizations of some groups by their sizes of the subset of pairwise non-commuting elements*, JP Journal of Algebra, Number Theory and Applications **24(2)** (2012), 125-135.