AUTOMORPHISMS OF GROUPS

By

PRADEEP KUMAR RAI

MATH08200904006

Harish-Chandra Research Institute, Allahabad

A thesis submitted to the

Board of Studies in Mathematical Sciences

In partial fulfillment of requirements

for the Degree of

DOCTOR OF PHILOSOPHY

of

HOMI BHABHA NATIONAL INSTITUTE

December, 2014

STATEMENT BY AUTHOR

This dissertation has been submitted in partial fulfilment of requirements for an advanced degree at Homi Bhabha National Institute (HBNI) and is deposited in the Library to be made available to borrowers under rules of the HBNI.

Brief quotations from this dissertation are allowable without special permission, provided that accurate acknowledgement of source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the Competent Authority of HBNI when in his or her judgement the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

Pradeep Kumar Rai

DECLARATION

I, hereby declare that the investigation presented in the thesis has been carried out by me. The work is original and has not been submitted earlier as a whole or in part for a degree / diploma at this or any other Institution / University.

Pradeep Kumar Rai

List of Publications arising from the thesis

Journal

1. "On finite p-groups with abelian automorphism group", Vivek K. Jain, Pradeep K. Rai and Manoj K. Yadav, *Internat. J. Algebra Comput.*, **2014**, *Vol. 23*, 1063-1077.

2. "On class-preserving automorphisms of groups", Pradeep K. Rai, *Ricerche Mat.*, **2014**, *Vol. 63*, 189-194.

3. "On IA-automorphisms that fix the center element-wise", Pradeep K. Rai, *Proc. Indian Acad. Sci. (Math. Sci.)*, **2014**, *Vol. 124*, 169-173.

4. "On Ш-rigidity of groups of order p^6", Pradeep K. Rai and Manoj K. Yadav, *J. Algebra*, **2015**, *Vol. 428*, 26-42.

Others

1. "On nilpotency of the group of outer class-preserving automorphisms of a group", Pradeep K. Rai, *Accepted for publication in J. Algebra Appl.*.

Pradeep Kumar Rai

DEDICATIONS

पिता जी व भैया की स्मृति में

अम्मा को,

उनके अनन्य आशीर्वादों की आकांक्षा के साथ,

समर्पित

ACKNOWLEDGEMENTS

Travelling on this road, Ph.D., has been a wonderful experience for me. At the end of this road, it is a very pleasant task to express my thanks to all those who contributed in many ways to the success of this journey and made it an unforgettable experience for me.

At this moment of accomplishment, first of all I would like to express my deep sense of gratitude to my guide Dr. Manoj Kumar Yadav. He has been very patient while rectifying my repeated mistakes during my Ph.D. work. I would like to thank him for interacting with me extensively and patiently on various topics in group theory, for encouraging my freedom of expression and for helping me in understanding the subject. This work would not have been possible without his guidance, support and encouragement.

I thank the members of my doctoral committee, Prof. B. Ramakrishnan and Dr. Punita Batra for their encouragement and insightful comments. I am also very much thankful to the faculty members of HRI who have taught me various courses in mathematics without which I could not have reached at this stage.

I would like to thank the administrative staff of HRI for their cooperation.

My time at HRI was made enjoyable in large part due to many friends that became a part of my life. I am grateful to all of them specially to Jay, Pradip, Kasi, Karam Deo, Indira, Jaban, Shailesh, Bhavin, Navin, Divyang, Ramesh, Eshita, Sneh, Abhishek Joshi and Vipul for the wonderful time spent with them. I am also thankful to Vivek Jain for being a collaborator of mine in my research work.

Last but far from the least I would like to thank the members of my family. My very special thanks go to my mother Usha Rai whom I owe everything I am today. Her unwavering faith and confidence in my abilities and in me is what has shaped me to be the person I am today. My thanks also go to my late grandfather Brahm Deo Rai who showed me the true worth of patience and my late father Satish Rai who sowed the seeds of higher education in me when I was very young at age.

Contents

SYNOPSIS

This Ph.D. thesis can be divided into three parts. In the first part we construct various types of non-special finite p-groups G such that the automorphism group of G is abelian. The second part deals with class-preserving automorphisms of groups. We prove some structural properties of the group of class-preserving automorphisms of a group. We then calculate the order of the group of class-preserving outer automorphisms of groups of order p^6 and study the connection between Ш-rigidity and Bogomolov multiplier of these groups. In the last part we consider the group of those IA automorphisms of a group that fix the center of the group element-wise and prove that for any two isoclinic groups these groups of automorphisms are isomorphic. We also give an application of this result.

For a given group G, we denote its center, commutator subgroup and Frattini subgroup by $\gamma_2(G)$, $\Phi(G)$ and $Z(G)$ respectively. The automorphism group and inner automorphism group of G are denoted by $\mathrm{Aut}(G)$ and $\mathrm{Inn}(G)$ respectively. By $|G|$ we denote the order of the group G. If H is a subgroup (proper subgroup) of G, then we write $H \leq G$ ($H < G$).

We now summarize our research work in the following sections.

1. Finite p-groups with abelian automorphism group

Throughout this section any unexplained p always denotes an odd prime. In 2008, Mahalanobis [48] published the following conjecture: *For an odd prime p, any finite p-group having abelian automorphism group is special.* Jain and Yadav [37] provided counter examples to this conjecture by constructing a class of non-special finite p-groups G such that $\mathrm{Aut}(G)$ is abelian. These counter examples, constructed in [37], enjoy the following properties: (i) $|G| = p^{n+5}$, where p is an odd prime and n is an integer ≥ 3; (ii) $\gamma_2(G)$ is a proper subgroup of $\mathrm{Z}(G) = \Phi(G)$; (iii) exponents of $\mathrm{Z}(G)$ and $G/\gamma_2(G)$ are same and it is equal to p^{n-1}; (iv) $\mathrm{Aut}(G)$ is abelian of exponent p^{n-1}.

Though the conjecture of Mahalanobis has been proved false, one might expect that some weaker form of the conjecture still holds true. Two obvious weaker forms of the conjecture are: (WC1) For a finite p-group G with $\mathrm{Aut}(G)$ abelian, $\mathrm{Z}(G) = \Phi(G)$ always holds true; (WC2) For a finite p-group G with $\mathrm{Aut}(G)$ abelian and $\mathrm{Z}(G) \neq \Phi(G)$, $\gamma_2(G) = \mathrm{Z}(G)$ always holds true. So, on the way to exploring some general structure on the class of such groups G, it is natural to ask the following question:

Question. Does there exist a finite p-group G such that $\gamma_2(G) \leq \mathrm{Z}(G) < \Phi(G)$ and $\mathrm{Aut}(G)$ is abelian?

Disproving (WC1) and (WC2), we provide affirmative answer to this question in the following theorem:

Theorem 1.0.1. *For every positive integer $n \geq 4$ and every odd prime p, there exists a group G of order p^{n+10} and exponent p^n such that*

1. *for $n = 4$, $\gamma_2(G) = \mathrm{Z}(G) < \Phi(G)$ and $\mathrm{Aut}(G)$ is abelian;*
2. *for $n \geq 5$, $\gamma_2(G) < \mathrm{Z}(G) < \Phi(G)$ and $\mathrm{Aut}(G)$ is abelian.*

Moreover, the order of $\mathrm{Aut}(G)$ is p^{n+20}.

One more weaker form of the above said conjecture is: (WC3) If $\mathrm{Aut}(G)$ is an elementary abelian p-group, then G is special. Berkovich and Janko [5, Problem 722] published the following long standing problem: *(Old problem) Study the p-groups G with elementary abelian* $\mathrm{Aut}(G)$.

We prove the following theorem which gives some structural information about

G when $\mathrm{Aut}(G)$ is elementary abelian.

Theorem 1.0.2. *Let G be a finite p-group such that $\mathrm{Aut}(G)$ is elementary abelian, where p is an odd prime. Then one of the following two conditions holds true:*

1. $\mathrm{Z}(G) = \Phi(G)$ *is elementary abelian;*

2. $\gamma_2(G) = \Phi(G)$ *is elementary abelian.*

Moreover, the exponent of G is p^2.

Now one might expect that for groups G with $\mathrm{Aut}(G)$ elementary abelian, both of the conditions in previous theorem hold true, i.e., WC(3) holds true, or, a little less ambitiously, (1) always holds true or (2) always holds true. In the following two theorems we show that none of the statements in the preceding sentence holds true.

Theorem 1.0.3. *There exists a group G of order p^9 such that $\mathrm{Aut}(G)$ is elementary abelian of order p^{20}, $\Phi(G) < \mathrm{Z}(G)$ and $\gamma_2(G) = \Phi(G)$ is elementary abelian.*

Theorem 1.0.4. *There exists a group G of order p^8 such that $\mathrm{Aut}(G)$ is elementary abelian of order p^{16}, $\gamma_2(G) < \Phi(G)$ and $\mathrm{Z}(G) = \Phi(G)$ is elementary abelian.*

The results of this section has been published in the paper [36].

2. Class-preserving automorphisms of groups

Let G be a group. An automorphism α of G is called class-preserving if it maps each group element to some conjugate of it. These automorphisms form a normal subgroup of $\mathrm{Aut}(G)$ which we denote by $\mathrm{Aut}_c(G)$. Obviously, $\mathrm{Inn}(G) \leq \mathrm{Aut}_c(G)$.

The factor group $\mathrm{Aut}_c(G)/\mathrm{Inn}(G)$ is denoted by $\mathrm{Out}_c(G)$. In 1911 Burnside [9] asked the following question: Does there exist any finite group G such that G has a non-inner class-preserving automorphism? In 1913, he himself answered this question affirmatively by constructing a group W of nilpotecy class 2 and of order p^6, p an odd prime [10]. More groups with non-inner class-preserving automorphisms were constructed in [8, 29, 31, 49, 69].

2.1 Some structural properties of $\mathrm{Aut}_c(G)$

In 1968, Sah [65], using homolgical techniques and some results of Schur and Wedderburn, proved that $\mathrm{Aut}_c(G)$ is solvable when G is finite solvable. Extending the result of Sah to arbitrary groups we prove the following theorem.

Theorem 2.1.1. *Let G be a solvable group of length l. Then $\mathrm{Aut}_c(G)$ is a solvable group of length either l or $l-1$.*

Next for an arbitrary group G we investigate the nilpotency of $\mathrm{Out}_c(G)$. Sah using a result of Hall, noticed that if G is a nilpotent group of class k, then $\mathrm{Aut}_c(G)$ is a nilpotent group of class $k-1$. The obvious corollary is, if G is a nilpotent group of class k, then $\mathrm{Out}_c(G)$ is a nilpotent group of class at most $k-1$. This bound on the nilpotency class of $\mathrm{Out}_c(G)$ is best possible when $k=2$. Sah remarked in his paper [65] that for the large values of k the corollary could presumably be improved. Yadav [73] and Malinowska [50] also asked in their surveys to improve this bound on the nilpotency class of $\mathrm{Out}_c(G)$.

Let $Z_j(G)$ denote the j-th term in the upper central series of G. As a corollary of our following theorem we improve the bound on the nilpotency class of $\mathrm{Out}_c(G)$ in some cases, e.g., p-groups of maximal class.

Theorem 2.1.2. *Let G be a group such that $\mathrm{Out}_c(G/Z_j(G))$ is a nilpotent group* *of class k. Then* $\mathrm{Out}_c(G)$ *is a nilpotent group of class at most* $j+k$*. Moreover, if* $\mathrm{Out}_c(G/Z_j(G))$ *is a trivial group, then* $\mathrm{Out}_c(G)$ *is a nilpotent group of class at most* j*.*

Corollary 2.1.3. *Let p be any prime and G be a finite p-group such that* $|G/Z_j(G)| \leq p^4$*. Then* $\mathrm{Out}_c(G)$ *is a nilpotent group of class at most* j*.*

Corollary 2.1.4. *Let p be any prime and G be a p-group of maximal class having order p^n, $n \geq 5$. Then the nilpotency class of* $\mathrm{Out}_c(G)$ *is at most* $n-4$*.*

Let $\gamma_k(G)$ denote the k-th term in the lower central series of G. We investigate the nilpotency of $\mathrm{Out}_c(G)$ for an arbitrary group G when $\gamma_k(G)/\gamma_k(G) \cap Z_j(G)$ for some $j, k \in \mathbb{N}$ is cyclic and prove the following theorem.

Theorem 2.1.5. *Let G be a group such that $\gamma_k(G)/\gamma_k(G) \cap Z_j(G)$ is cyclic. Then* $\mathrm{Out}_c(G)$ *is nilpotent of class at most* $j+k+1$*. Moreover, if* $\gamma_k(G)/\gamma_k(G) \cap Z_j(G)$ *is an infinite cyclic or a finite cyclic p-group, then* $\mathrm{Out}_c(G)$ *is nilpotent of class at most* $j+k$*.*

The results of this subsection are from the papers [60] and [61].

2.2 Ш-rigidity of groups of order p^6

Let G be a group which acts on itself by conjugation, and let $H^1(G,G)$ be the first cohomology pointed set. Denote by Ш(G) the subset of $H^1(G,G)$ consisting of the cohomology classes becoming trivial after restricting to every cyclic subgroup of G. The set Ш(G), for a given group G, is called the Shafarevich-Tate set of G. Following Kunyavskiĭ [45], we say that G is a Ш-rigid group if the set Ш(G) consists of one element. The Bogomolov multiplier $B_0(G)$ of a finite group G is defined as the subgroup of the Schur multiplier consisting of the cohomology classes vanishing after restriction to all abelian subgroups of G. Kang and Kunyavskiĭ in [41] observed that $B_0(G) = 0$ for most of the known classes of finite Ш-rigid groups G and asked the following question:

Question ([41, Question 3.2]). Let G be a finite Ш-rigid group. Is it true that $B_0(G) = 0$?

We study the rigidity property of groups of order p^6 for an odd prime p and answer the above question in affirmative for most of these groups. Our viewpoint on this study is a bit different. We study rigidity problem through automorphisms of groups. We make it more precise here. Ono proved that there is a bijection between $\mathrm{Out}_c(G)$ and Ш(G) for any finite group G [57, 2.12]. Therefore a finite group G is Ш-rigid if and only if $\mathrm{Out}_c(G) = 1$.

Groups of order p^6, for odd primes p, are classified in 43 isoclinism families by James [39]. These isoclinism families are denoted by Φ_k for $1 \leq k \leq 43$. That $\mathrm{Aut}_c(G)$, for non-abelian finite groups, is independent (upto isomorphism) of the choice of a group in a given isoclinism family is shown in [74, Theorem 4.1]. This result allows us to select and work with any group from each of 43 isoclinism families of groups of order p^6. The rigid groups of order p^5 for odd primes p are classified by Yadav [74]. In the following result we classify the rigid groups of order p^6 for odd primes p, and compute $|\text{Ш}(G)| = |\,\mathrm{Out}_c(G)|$ for the groups G which are not rigid.

Theorem 2.2.1. *Let G be a group of order p^6 for an odd prime p. Then $\mathrm{Out}_c(G) \neq 1$ if and only if G belongs to one of the isoclinism families Φ_k for $k = 7, 10, 13, 15, 18, 20, 21, 24, 30, 36, 38, 39$. Moreover,*

1. *if G belongs to one of the isoclinism families Φ_k for $k = 7, 10, 24, 30, 36, 38, 39$, then $|\,\mathrm{Out}_c(G)| = p$,*
2. *if G belongs to one of the isoclinism families Φ_k for $k = 13, 18, 20$, then*

$|\operatorname{Out}_c(G)| = p^2$, *and*

3. *if G belongs to one of the isoclinism families Φ_k for $k = 15, 21$, then* $|\operatorname{Out}_c(G)| = p^4$.

Next we investigate the question of Kang and Kunyavskiĭ for groups of order p^6 and prove the following.

Theorem 2.2.2. *Let G be a Ш-rigid group of order p^6 for a prime p. If G does not belong to the isoclinism families Φ_k for $k = 28, 29$, then its Bogomolov multiplier $B_0(G)$ is zero.*

Both the above theorems are from the paper [63].

3. IA automorphisms that fix the center element-wise

Let G be any group and σ be an automorphism of G. Following Bachmuth [2], we call σ an IA automorphism if $x^{-1}\sigma(x) \in \gamma_2(G)$ for each $x \in G$. The set of all IA automorphisms of G form a normal subgroup of $\operatorname{Aut}(G)$ and is denoted by $\operatorname{IA}(G)$. The set of all IA automorphisms that fix the center element-wise form a normal subgroup of $\operatorname{IA}(G)$ and is denoted by $\operatorname{IA}_z(G)$.

Notice that $\operatorname{Aut}_c(G) \leq \operatorname{IA}_z(G)$. As we also have mentioned earlier, Yadav has proved that if two finite groups G and H are isoclinic then $\operatorname{Aut}_c(G) \cong \operatorname{Aut}_c(H)$. In the following theorem we extend this result to $\operatorname{IA}_z(G)$ for an arbitrary group G.

Theorem 3.0.1. *Let G and H be any two isoclinic groups. Then there exists an isomorphism $\alpha\colon \operatorname{IA}_z(G) \to \operatorname{IA}_z(H)$ such that $\alpha(\operatorname{Aut}_c(G)) = \operatorname{Aut}_c(H)$.*

An automorphism α of a group G is called a central automorphism if $x^{-1}\alpha(x) \in Z(G)$ for all $x \in G$. The set of all central automorphisms form a normal subgroup of $\mathrm{Aut}(G)$ and is denoted by $\mathrm{Autcent}(G)$.

As an application of Theorem 3.0.1, we prove the following theorem.

Theorem 3.0.2. *Let G be a finite p-group.*

1. *Then* $\mathrm{IA}_z(G) = \mathrm{Autcent}(G)$ *if and only if* $\gamma_2(G) = Z(G)$.

2. *If the nilpotency class of G is 2, then* $\mathrm{IA}_z(G) = \mathrm{Inn}(G)$ *if and only if* $\gamma_2(G)$ *is cyclic.*

The following result of Curran and McCaughan [15] can be obtained as a consequence of Theorem 3.0.2.

Corrollary 3.0.3. *Let G be a finite p-group. Then* $\mathrm{Inn}(G) = \mathrm{Autcent}(G)$ *if and only if* $\gamma_2(G) = Z(G)$ *and* $\gamma_2(G)$ *is cyclic.*

The results of this section has been published in the paper [62].

Conventions and Notations

Let G be a group and $x, y, a \in G$. Then $[x, y]$ denotes the commutator $x^{-1}y^{-1}xy$, x^a denotes the conjugate of x by a, i.e., $a^{-1}xa$, x^G denotes the G-conjugacy class of x and $[x, G]$ denotes the set of all $[x, z]$, for $z \in G$. By $\langle x \rangle$ we denote the cyclic subgroup generated by x. Let H and K be two subgroups of a group G. Then $[H, K]$ denotes the subgroup generated by all commutators $[h, k]$ for $h \in H, k \in K$. By $Z(G)$ we denote the center of G and by $C_G(H)$ we denote the centralizer of H in G. The commutator and Frattini subgroup of G are denoted by $\gamma_2(G)$ and $\Phi(G)$, respectively. The group of all homomorphisms from a group H to a group K is denoted by $\mathrm{Hom}(H, K)$. We write $\gamma_i(G)$ for the i-th term in the lower central series of G, $\delta_i(G)$ for the i-th term in the derived series of G and $Z_i(G)$ for the i-th term in the upper central series of G. Let p be a prime number. By C_p we denote the cyclic group of order p. The subgroup of G generated by all the elements of order p is denoted by $\Omega_1(Z(G))$. Let $G^{p^i} = \left\langle x^{p^i} \mid x \in G \right\rangle$ and $G_{p^i} = \left\langle x \in G \mid x^{p^i} = 1 \right\rangle$, where $i \geq 1$ is an integer. If H is a subgroup (proper subgroup) of G, then we write $H \leq G$ ($H < G$) and if H is a normal subgroup of G, then we write $H \trianglelefteq G$. By $\mathrm{Aut}(G)$ and $\mathrm{Inn}(G)$ we denote the group of all automorphisms and the group of all inner automorphisms of G respectively. Let $N \trianglelefteq G$, then by $Aut^N(G)$ we denote the group of those automorphisms of G which induces the identity mapping on G/N. Finally, by a class c group we mean a group of nilpotency class c.

Chapter 1

Background and Preliminaries

In this chapter we collect some basic definitions and results which will be used in subsequent chapters. We begin with some basic group theoretic results, then we discuss central automorphisms and class-preserving automorphisms. The concept of isoclinism of groups and the Bogomolov multiplier of a group are introduced. We do not give many proofs in this chapter as most of the material presented, is either well known or easily available from the references.

1.1 Basic group theoretic results

The following few results are very basic and easy to prove.

Lemma 1.1.1 *Let G be a group and $x, y, z \in G$. Then,*

1. $[xy, z] = [x, z]^y [y, z]$, *and*
2. $[z, xy] = [z, y][z, x]^y$.

Lemma 1.1.2 *Let A, B and C be finite abelian groups. Then* $\mathrm{Hom}(A \times B,\ C) \cong \mathrm{Hom}(A,\ C) \times \mathrm{Hom}(B,\ C)$ *and* $\mathrm{Hom}(A,\ B \times C) \cong \mathrm{Hom}(A,\ B) \times \mathrm{Hom}(A,\ C)$.

Lemma 1.1.3 *Let C_r and C_s be two cyclic groups of order r and s respectively. Then* $\mathrm{Hom}(C_r, C_s) \cong C_d$, *where d is the greatest common divisor of r and s.*

Proposition 1.1.4 *Let G be a finite cyclic p-group for an odd prime p, then* $\mathrm{Aut}(G)$ *is cyclic.*

Proposition 1.1.5 *Let H be a subgroup of a group G. Then $N_G(H)/C_G(H)$ is isomorphic to a subgroup of* $\mathrm{Aut}(H)$.

Lemma 1.1.6 *Let H be cyclic normal subgroup of a group G. Then H centralizes the commutator subgroup of G.*

Lemma 1.1.7 *Let G be a non-abelian finite p-group. If there is an element of order p in the center but not in the Frattini subgroup then G has an abelian direct factor.*

The proof of following theorem can be found in [46, 2.1.2].

Theorem 1.1.8 *Let G be a finite abelian group and H a cyclic subgroup of maximal order in G. Then there exists a complement K of H in G; in particular $G = H \times K$.*

Let A be a group which acts on a group G. By $[A, G]$ and $[G, A]$ both, we denote the subgroup generated by $g^{-1}g^a$ for all $g \in G$ and $a \in A$. The following lemma can be found in [46, Page 176].

Lemma 1.1.9 *Let A be a group acting on a group G and X, Y, Z be subgroups of either G or A. Suppose that $[[X, Y], Z] = [[Y, Z], X] = 1$. Then also $[[Z, X], Y] = 1$.*

The following lemma can be found in [14].

Lemma 1.1.10 ([14], 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 $|A|/|C| = |B|/|D| > 1$. Then $\mathrm{Hom}(C, D)$ is isomorphic to a proper subgroup of $\mathrm{Hom}(A, B)$.*

1.2 Central automorphisms

Definition 1.2.1 An automorphism α of a group G is called a central automorphism if it induces the identity mapping on the central quotient $G/Z(G)$. In mathematical notations, if $x^{-1}\alpha(x) \in Z(G)$ for all $x \in G$, then we say that α is a central automorphism.

The set of all central automorphisms of G forms a normal subgroup of $\mathrm{Aut}(G)$. We denote this subgroup by $\mathrm{Autcent}(G)$. The following lemma can be easily proved.

Lemma 1.2.2 *Let G be a group, then $\mathrm{Autcent}(G) = C_{\mathrm{Aut}(G)}(\mathrm{Inn}(G))$.*

Corollary 1.2.3 *Let G be a group such that $\mathrm{Aut}(G)$ is abelian. Then all automorphisms of the group G are central, i.e., $\mathrm{Autcent}(G) = \mathrm{Aut}(G)$.*

Definition 1.2.4 A group G is called a purely non-abelian group if it does not have any non-trivial abelian direct factor, i.e., there does not exist any non-trivial abelian subgroup A and a subgroup N such that $G = A \times N$.

The following theorem is due to Adney and Yen [1].

Theorem 1.2.5 *Let G be a purely non-abelian finite p-group. Then $|\,\mathrm{Autcent}(G)| = |\,\mathrm{Hom}(G/\gamma_2(G), \mathrm{Z}(G))|$.*

Let A be an abelian p-group and $a \in A$. For a positive integer n, p^n is said to be the *height* of a in A, denoted by $\mathrm{ht}(a)$, if $a \in A^{p^n}$ but $a \notin A^{p^{n+1}}$. Let H be a p-group of class 2. We denote the exponents of $\mathrm{Z}(H)$, $\gamma_2(H)$, $H/\gamma_2(H)$ by p^a, p^b, p^c respectively and $d = \min(a, c)$. We define $R := \{z \in \mathrm{Z}(H) \mid \ |z| \leq p^d\}$ and $K := \{x \in H \mid \mathrm{ht}(x\gamma_2(H)) \geq p^b\}$. Notice that $K = H^{p^b}\gamma_2(H)$. Now we state the following important result of Adney and Yen.

Theorem 1.2.6 ([1], Theorem 4) *Let H be a purely non-abelian p-group of class 2, p odd, and let $H/\gamma_2(H) = \Pi_{i=1}^n \langle x_i\gamma_2(H)\rangle$. Then $\mathrm{Autcent}(H)$ is abelian if and only if*

1. *$R = K$, and*
2. *either $d = b$ or $d > b$ and $R/\gamma_2(H) = \left\langle x_1^{p^b}\gamma_2(H)\right\rangle$.*

The next two theorems were proved by Earnley in his Ph.D. thesis.

Theorem 1.2.7 ([17], Corollary 3.3) *Let G be a non-abelian finite p-group of exponent p, where p is an odd prime. Then $\mathrm{Aut}(G)$ is non-abelian.*

Theorem 1.2.8 ([17], Theorem 2.3) *Let G be a finite p-group such that $G = A \times N$ with $1 \neq A$ abelian and N purely non-abelian. Then $\mathrm{Aut}(G)$ is abelian if and only if A and N satisfy the following three conditions:*

1. *A is cyclic of order 2^n with $n > 1$;*
2. *N is a 2-group with $\mathrm{Aut}(N)$ abelian;*
3. *N is a special 2-group.*

The next two theorems are due to Jafari.

Theorem 1.2.9 ([35], Theorem 3.4) *Let G be a finite purely nonabelian p-group, p odd, then* $\mathrm{Autcent}(G)$ *is an elementary abelian p-group if and only if the exponent of $Z(G)$ is p or exponent of $G/\gamma_2(G)$ is p.*

A finite abelian p-group G is said to be *ce-group* if G can be written as a direct product of a cyclic group A of order p^n, $n > 1$ and an elementary abelian p-group B.

Theorem 1.2.10 ([35], Theorem 3.5) *Let G be a purely nonabelian 2-group. Then* $\mathrm{Autcent}(G)$ *is elementary abelian if and only if one of the following conditions holds:*

1. *the exponent of $G/\gamma_2(G)$ is 2;*
2. *the exponent of $Z(G)$ is 2;*
3. *the greatest common divisor of the exponents of $G/\gamma_2(G)$ and $Z(G)$ is 4 and $G/\gamma_2(G)$, $Z(G)$ are ce-groups having the properties that an elementary part of $Z(G)$ is contained in $\gamma_2(G)$ and there exists an element z of order 4 in a cyclic part of $Z(G)$ with $z\gamma_2(G)$ lying in a cyclic part of $G/\gamma_2(G)$ such that twice of the order of $z\gamma_2(G)$ is equal to the exponent of $G/\gamma_2(G)$.*

1.3 Isoclinism of groups

The concept of isoclinism was first introduced by Hall [26]. We say that two groups G and H are isoclinic if there exist isomorphisms φ of $G/Z(G)$ onto $H/Z(H)$ and θ of $\gamma_2(G)$ onto $\gamma_2(H)$, such that the following diagram commutes.

$$\begin{array}{ccc} G/Z(G) \times G/Z(G) & \xrightarrow{\varphi\times\varphi} & H/Z(H) \times H/Z(H) \\ {\scriptstyle a_G}\big\downarrow & & {\scriptstyle a_H}\big\downarrow \\ \gamma_2(G) & \xrightarrow{\theta} & \gamma_2(H), \end{array}$$

where $a_G(xZ(G), yZ(G)) = [x, y]$ for $x, y \in G$ and $a_H(kZ(H), lZ(H)) = [k, l]$ for $k, l \in H$. The pair (φ, θ) is called an isoclinism of G onto H.

In the same article [26] Hall proved the following result.

Theorem 1.3.1 *In every family of isoclinic groups there exists a group G such that $Z(G) \leq \gamma_2(G)$.*

The following lemma is due to Tappe.

Lemma 1.3.2 ([70], Lemma 1.5) *Let G and H be isoclinic groups and (φ, θ) be an isoclinism of G onto H. Then,*

1. *$\varphi(gZ(G)) = \theta(g)Z(H)$ for $g \in \gamma_2(G)$, and*

2. *$\theta(\gamma_2(G) \cap Z(G)) = \gamma_2(H) \cap Z(H)$.*

1.4 Class-preserving automorphisms

Definition 1.4.1 An automorphism α of a group G is called class-preserving if it maps each group element to a cojugate of it

The set of all class-preserving automorphisms of G forms a normal subgroup of $\mathrm{Aut}(G)$. We denote this subgroup by $\mathrm{Aut}_c(G)$. The following three lemmas can be easily proved.

Lemma 1.4.2 *Let G be a finite group. Let σ be an endomorphism of G such that $\sigma(x) \in x^G$ for all $x \in G$. Then $\sigma \in \mathrm{Aut}_c(G)$.*

Lemma 1.4.3 *Let G be a finite group. Let $x_1, x_2, ..., x_d$ be a minimal generating set for G. Then $|\mathrm{Aut}_c(G)| \leq \prod_{i=1}^{d} |{x_i}^G|$.*

Lemma 1.4.4 *Let H and K be any two groups. Then* $\operatorname{Aut}_c(H \times K) \cong \operatorname{Aut}_c(H) \times \operatorname{Aut}_c(K)$.

The next lemma is by Yadav which will be used frequently in Chapter 4.

Lemma 1.4.5 ([74], Lemma 2.2) *Let G be a finite p-group such that $Z(G) \leq [x, G]$ for all $x \in G - \gamma_2(G)$. Then* $|\operatorname{Aut}_c(G)| \geq |\operatorname{Autcent}(G)||G/Z_2(G)|$.

It is obvious that all inner automorphisms are class-preserving. The factor group $\operatorname{Aut}_c(G)/\operatorname{Inn}(G)$ is denoted by $\operatorname{Out}_c(G)$. The following result is due to Hertweck.

Proposition 1.4.6 ([31], Proposition 14.4) *Let G be a finite group and H be an abelian normal subgroup of G such that G/H is cyclic. Then* $\operatorname{Out}_c(G) = 1$.

The following result is due to Cheng [12].

Theorem 1.4.7 *Suppose that G is a finite p-group such that $\gamma_2(G) = \langle a \rangle$ is cyclic. Assume that either $p > 2$ or $p = 2$ and $[a, G] \leq \langle a^4 \rangle$. Then* $\operatorname{Out}_c(G) = 1$.

The following result of Yadav makes the study of group of class-preserving automorphism independent of the choice of the group from an isoclinic family.

Theorem 1.4.8 ([74], Theorem 4.1) *Let G and H be two finite isoclinic groups. Then* $\operatorname{Aut}_c(G)) \cong \operatorname{Aut}_c(H)$.

Using the above theorem Yadav classified the group G of order p^5 with non-trivial $\operatorname{Out}_c(G)$ in the following theorem.

Theorem 1.4.9 ([74], Theorem 5.5) *Let p be an odd prime and G be a group of order p^5. Then $\operatorname{Out}_c(G)$ is non-trivial if and only if G is isoclinic to one of* *the following groups (For the meaning of the notation $\alpha_i^{(p)}$, see Section 4.2):*

$$\begin{aligned}\Phi_7(1^5) &= \Big\langle \alpha, \alpha_1, \alpha_2, \alpha_3, \beta \mid [\alpha_i, \alpha] = \alpha_{i+1}, [\alpha_1, \beta] = \alpha_3, \alpha^p = \alpha_1^{(p)} = \beta^p = \\ &\qquad \alpha_{i+1}^p = 1 \ (i = 1, 2) \Big\rangle.\end{aligned}$$

$$\begin{aligned}\Phi_{10}(1^5) &= \Big\langle \alpha, \alpha_1, ..., \alpha_4 \mid [\alpha_i, \alpha] = \alpha_{i+1}, [\alpha_1, \alpha_2] = \alpha_4, \\ &\qquad \alpha^p = \alpha_1^{(p)} = \alpha_{i+1}^{(p)} = 1 \ (i = 1, 2, 3) \Big\rangle.\end{aligned}$$

Moreover, if $\mathrm{Out}_c(G)$ *is non-trivial, then* $|\,\mathrm{Out}_c(G)| = p$*.*

1.5 Ш-rigid groups

Let G be a group which acts on itself by conjugation, and let $H^1(G, G)$ be the first cohomology pointed set. Denote by Ш(G) the subset of $H^1(G, G)$ consisting of the cohomology classes becoming trivial after restricting to every cyclic subgroup of G. The set Ш(G), for a given group G, is called the Shafarevich-Tate set of G.

Definition 1.5.1 A group G is called a Ш-rigid group if the set Ш(G) consists of one element.

The following theorem, which establishes a relation between class-preserving automorphisms and Shafarevich-Tate set, was proved by Ono:

Theorem 1.5.2 ([57], Theorem 2.12) *Let G be a finite group. Then there is a bijection between* $\mathrm{Out}_c(G)$ *and* Ш(G)*.*

Corollary 1.5.3 *Let G be a finite group. Then G is* Ш*-rigid if and only if* $Out_c(G) = 1$*.*

1.6 Bogomolov multiplier

Definition 1.6.1 The Bogomolov multiplier $B_0(G)$ of a finite group G is defined as the subgroup of the Schur multiplier $H^2(G, \mathbb{C})$ consisting of the cohomology classes vanishing after restriction to all abelian subgroups of G.

Bogomolov showed in [6, 7] that $B_0(G)$ coincides with the unramified Brauer group $Br_{nr}(V/G)$ where V is a vector space defined over an algebraically closed field k of characteristic zero equipped with a faithful, linear, generically free action of G. The latter group is an important birational invariant of the quotient variety V/G; in particular, it equals zero whenever the variety V/G is k-rational (or even retract k-rational). It was introduced by Saltman in [66, 67] and used in constructing the first counter-example (for G of order p^9) to a problem by Emmy Noether on rationality of fields of invariants $k(x_1, ..., x_n)^G$, where k is algebraically closed and G acts on the variables x_i by permutations. The description of $B_0(G)$ provides a purely group-theoretic intrinsic recipe for the computation of $Br_{nr}(V/G)$. Moravec proved that the smallest power of p for which there exists a p-group G with $B_0(G) \neq 0$ is 5 (for odd p) and not 6, as claimed by Bogomolov. He also classified groups G of order p^5 for which $B_0(G) \neq 0$ in [52] using the following theorem [53].

Theorem 1.6.2 *If G_1 and G_2 are finite isoclinic groups, then $B_0(G_1) \cong B_0(G_2)$.*

Non-abelian groups of order p^6, for odd primes p, are classified in 42 isoclinism families by James [39], which are denoted by Φ_k for $2 \leq k \leq 43$. Using this classification Chen and Ma has tried to classify the non-abelian groups of order p^6, for primes $p > 3$, with $B_0(G) = 0$. They were unable to give the complete classification, the Bogomolov multiplier for the families Φ_k for $k = 15, 28, 29$ is still not known. The following theorem follows from [11, Table 1].

Theorem 1.6.3 *Let $p > 3$ be a prime number and G be a non-abelian group of order p^6. If G belongs to one of the isoclinism family Φ_k for $k = 2, ..., 6, 8, 9, 11, 12, 14,$ $16, 17, 19, 23, 25, 26, 27, 31, ..., 35, 37, 40, ..., 43,$ then $B_0(G) = 0$.*

Chapter 2

Finite p-Groups with Abelian Automorphism Group

In this chapter we construct various types of specific non-special finite p-groups having abelian automorphism group. We also find some structural information about the groups whose automorphism groups are elementary abelian. Throughout the chapter, any unexplained p always denotes an odd prime.

2.1 Abelian Automorphism Groups: Literature

Study of groups having abelian automorphism groups is an old problem in group theory. Though a lot of work has been done by many on the subject, not very significant is known about such groups. In this section we review the literature about such groups and give motivation behind theorems presented in this chapter. The story began in 1908 with the following question of Hilton [33]: *Whether a non-abelian group can have an abelian group of isomorphisms (automorphisms).* In 1913, Miller [51] constructed a non-abelian group G of order 64 such that $\mathrm{Aut}(G)$ is an elementary abelian group of order 128. More examples of such 2-

groups were constructed in [13, 38, 68]. For an odd prime p, the first example of a finite p-group G such that $\mathrm{Aut}(G)$ is abelian was constructed by Heineken and Liebeck [28] in 1974. In 1975, Jonah and Konvisser [40] constructed 4-generated groups of order p^8 such that $\mathrm{Aut}(G)$ is an elementary abelian group of order p^{16}, where p is any prime. In 1975, by generalizing the constructions of Jonah and Konvisser, Earnley [17, Section 4.2] constructed n-generated special p-groups G such that $\mathrm{Aut}(G)$ is abelian, where $n \geq 4$ is an integer and p is any prime number. Among other things, Earnley also proved that there is no p-group G of order p^5 or less such that $\mathrm{Aut}(G)$ is abelian. On the way to constructing finite p-groups of class 2 such that all normal subgroups of G are characteristic, in 1979 Heineken [29] produced groups G such that $\mathrm{Aut}(G)$ is abelian. In 1994, Morigi [54] proved that there exists no group of order p^6 whose group of automorphisms is abelian and constructed groups G of order p^{n^2+3n+3} such that $\mathrm{Aut}(G)$ is abelian, where n is a positive integer. In particular, for $n = 1$, it provides a group of order p^7 having an abelian automorphism group.

There have also been attempts to get structural information of finite groups having abelian automorphism group. In 1927, Hopkins [34], among other things, proved that a finite p-group G such that $\mathrm{Aut}(G)$ is abelian, can not have a non-trivial abelian direct factor. In 1995, Morigi [55] proved that the minimal number of generators for a p-group with abelian automorphism group is 4. In 1995, Hegarty [27] proved that if G is a non-abelian p-group such that $\mathrm{Aut}(G)$ is abelian, then $|\mathrm{Aut}(G)| \geq p^{12}$, and the minimum is obtained by the group of order p^7 constructed by Morigi. Moreover, in 1998, Ban and Yu [3] obtained independently the same result and proved that if G is a group of order p^7 such that $\mathrm{Aut}(G)$ is abelian, then $|\mathrm{Aut}(G)| = p^{12}$.

We remark here that all the examples (for an odd prime p) mentioned above are special p-groups. In 2008, Mahalanobis [48] published the following conjecture: *For an odd prime p, any finite p-group having abelian automorphism group is special.* Jain and Yadav [37] provided counter examples to this conjecture by constructing a class of non-special finite p-groups G such that $\mathrm{Aut}(G)$ is abelian. These counter examples, constructed in [37], enjoy the following properties: (i) $|G| = p^{n+5}$, where p is an odd prime and n is an integer ≥ 3; (ii) $\gamma_2(G)$ is a proper subgroup of $\mathrm{Z}(G) = \Phi(G)$; (iii) exponents of $\mathrm{Z}(G)$ and $G/\gamma_2(G)$ are same and it is equal to p^{n-1}; (iv) $\mathrm{Aut}(G)$ is abelian of exponent p^{n-1}.

Now we review non-special 2-groups having abelian automorphism group. In contrast to p-groups for odd primes, there do exist finite 2-groups G with $\mathrm{Aut}(G)$ abelian and G satisfies either of the following two properties: (P1) G is 3-generated; (P2) G has a non-trivial abelian direct factor. The first 2-group having abelian automorphism group was constructed by Miller [51] in 1913. This is a 3-generated group and, as mentioned above, it has order 64 with elementary abelian automorphism group of order 128. Earnley [17] showed that there are two more groups of order 64 having elementary abelian automorphism group. These groups are also 3-generated. Further Earnley gave a complete description of 2-groups satisfying (P2) and having abelian automorphism group and established the existence of such groups (see 1.2.8).

2.2 Groups G with $\mathrm{Aut}(G)$ abelian

Though the conjecture of Mahalanobis has been proved false, one might expect that some weaker form of the conjecture still holds true. Two obvious weaker forms of the conjecture are: (WC1) For a finite p-group G with $\mathrm{Aut}(G)$ abelian, $\mathrm{Z}(G) = \Phi(G)$ always holds true; (WC2) For a finite p-group G with $\mathrm{Aut}(G)$ abelian and $\mathrm{Z}(G) \neq \Phi(G)$, $\gamma_2(G) = \mathrm{Z}(G)$ always holds true. So, on the way to exploring some general structure on the class of such groups G, it is natural to ask the following question:

Question. Does there exist a finite p-group G such that $\gamma_2(G) \le \mathrm{Z}(G) < \Phi(G)$ and $\mathrm{Aut}(G)$ is abelian?

At the end of this section we will be able to answer this question.

Let G be a finite p-group of nilpotency class 2 generated by $x_1, x_2, \ldots, x_d$, where d is a positive integer. Let $e_{x_i} = x_1^{a_{i1}} x_2^{a_{i2}} \cdots x_d^{a_{id}} = \prod_{j=1}^{d} x_j^{a_{ij}}$, where $x_i \in G$ and a_{ij} are non-negative integers for $1 \le i, j \le d$. Since the nilpotency class of G is 2, we have

$$[x_k, e_{x_i}] = [x_k, \prod_{j=1}^{d} x_j^{a_{ij}}] = \prod_{j=1}^{d} [x_k, x_j^{a_{ij}}] = \prod_{j=1}^{d} [x_k, x_j]^{a_{ij}} \tag{2.1}$$

and

$$\begin{aligned} [e_{x_k}, e_{x_i}] &= [\prod_{l=1}^{d} x_l^{a_{kl}}, \prod_{j=1}^{d} x_j^{a_{ij}}] = \prod_{j=1}^{d}\prod_{l=1}^{d} [x_l^{a_{kl}}, x_j^{a_{ij}}] \\ &= \prod_{j=1}^{d}\prod_{l=1}^{d} [x_l, x_j]^{a_{kl}a_{ij}}. \end{aligned} \tag{2.2}$$

Equations (2.1) and (2.2) will be used for our calculations without any further reference.

Let $n \ge 4$ be a positive integer and p be an odd prime. Consider the following group:

$$\begin{aligned} G \;=\; \Big\langle & x_1,\ x_2,\ x_3,\ x_4 \mid x_1^{p^n} = x_2^{p^4} = x_3^{p^4} = x_4^{p^2} = 1,\ [x_1, x_2] = x_2^{p^2}, \\ & [x_1, x_3] = x_2^{p^2},\ [x_1, x_4] = x_3^{p^2},\ [x_2, x_3] = x_1^{p^{n-2}},\ [x_2, x_4] = x_3^{p^2}, \\ & [x_3, x_4] = x_2^{p^2} \Big\rangle. \end{aligned} \tag{2.3}$$

It is easy to see that G enjoys the properties given in the following lemma.

Lemma 2.2.1 *The group G is a regular p-group of nilpotency class 2 having order p^{n+10} and exponent p^n. For $n = 4$, $\gamma_2(G) = \mathrm{Z}(G) < \Phi(G)$ and for $n \geq 5$, $\gamma_2(G) < \mathrm{Z}(G) < \Phi(G)$.*

Let $e_{x_i} = x_1^{a_{i1}} x_2^{a_{i2}} x_3^{a_{i3}} x_4^{a_{i4}} = \Pi_{j=1}^{4} x_j^{a_{ij}}$, where $x_i \in G$ and a_{ij} are non-negative integers for $1 \leq i, j \leq 4$. Let α be an automorphism of G. Since the nilpotency class of G is 2 and $\gamma_2(G)$ is generated by $x_1^{p^{n-2}}$, $x_2^{p^2}$, $x_3^{p^2}$, we can write $\alpha(x_i) = x_i e_{x_i} = x_i \Pi_{j=1}^{4} x_j^{a_{ij}}$ for some non-negative integers a_{ij} for $1 \leq i, j \leq 4$.

Proposition 2.2.2 *Let G be the group defined in (2.3) and α be an automorphism of G such that $\alpha(x_i) = x_i e_{x_i} = x_i \Pi_{j=1}^{4} x_j^{a_{ij}}$, where a_{ij} are some non-negative integers for $1 \leq i, j \leq 4$. Then the following equations hold:*

$$a_{31} \equiv 0 \mod p^{n-2}, \tag{2.4}$$

$$-a_{32} + a_{13} + a_{13}a_{44} \equiv 0 \mod p^2, \tag{2.5}$$

$$-a_{33} + a_{44} + a_{11} + a_{11}a_{44} + a_{12} + a_{12}a_{44} \equiv 0 \mod p^2, \tag{2.6}$$

$$a_{21} \equiv 0 \mod p^{n-2}, \tag{2.7}$$

$$a_{44} - a_{22} + a_{33} + a_{33}a_{44} \equiv 0 \mod p^2, \tag{2.8}$$

$$a_{32} - a_{23} + a_{32}a_{44} \equiv 0 \mod p^2, \tag{2.9}$$

$$-a_{13} + a_{12}a_{23} - a_{13}a_{22} \equiv 0 \mod p^2, \tag{2.10}$$

$$a_{23} + a_{11} + a_{11}a_{22} + a_{11}a_{23} + a_{13}a_{24} - a_{14}a_{23} \equiv 0 \mod p^2, \tag{2.11}$$

$$-a_{23} + a_{24} + a_{11}a_{24} - a_{14} + a_{12}a_{24} - a_{14}a_{22} \equiv 0 \mod p^2, \tag{2.12}$$

$$a_{12} + a_{12}a_{33} - a_{13}a_{32} \equiv 0 \mod p^2, \tag{2.13}$$

$$\begin{aligned} &a_{32} + a_{33} + a_{11} - a_{22} - a_{14} + a_{11}a_{32} + a_{11}a_{33} + a_{13}a_{34} - a_{14}a_{33} \\ &\equiv 0 \mod p^2, \end{aligned} \tag{2.14}$$

$$a_{34} + a_{11}a_{34} + a_{12}a_{34} - a_{14}a_{32} - a_{23} \equiv 0 \mod p^2, \tag{2.15}$$

$$a_{23} - a_{32} + a_{23}a_{44} \equiv 0 \mod p^2, \tag{2.16}$$

$$-a_{33} + a_{44} + a_{22} + a_{22}a_{44} \equiv 0 \mod p^2, \tag{2.17}$$

$$-a_{11} + a_{33} + a_{22} + a_{22}a_{33} - a_{23}a_{32} \equiv 0 \mod p^2. \tag{2.18}$$

Proof. Let α be the automorphism of G such that $\alpha(x_i) = x_i e_{x_i}$, $1 \leq i \leq 4$ as defined above. Since $G_{p^2} = \langle x_1^{p^{n-2}}, x_2^{p^2}, x_3^{p^2}, x_4 \rangle$ is a characteristic subgroup of G, $\alpha(x_4) \in G_{p^2}$. Thus we get the following set of equations:

$$a_{41} \equiv 0 \mod p^{n-2}, \tag{2.19}$$

$$a_{4i} \equiv 0 \mod p^2, \text{ for } i = 2,\ 3. \tag{2.20}$$

We prove equations (2.4) - (2.6) by comparing the powers of x_i's in $\alpha([x_1, x_4]) = \alpha(x_3^{p^2})$.

$$\begin{aligned}
\alpha([x_1, x_4]) &= [\alpha(x_1), \alpha(x_4)] = [x_1 e_{x_1}, x_4 e_{x_4}] \\
&= [x_1, x_4][x_1, e_{x_4}][e_{x_1}, x_4][e_{x_1}, e_{x_4}] \\
&= [x_1, x_4]\textstyle\prod_{j=1}^4 [x_1, x_j]^{a_{4j}} \prod_{j=1}^4 [x_4, x_j]^{-a_{1j}} \prod_{j=1}^4 \prod_{l=1}^4 [x_l, x_j]^{a_{1l}a_{4j}} \\
&= [x_1, x_2]^{a_{42}+a_{11}a_{42}-a_{12}a_{41}} [x_1, x_3]^{a_{43}+a_{11}a_{43}-a_{13}a_{41}} \\
&\quad [x_1, x_4]^{1+a_{44}+a_{11}+a_{11}a_{44}-a_{14}a_{41}} [x_2, x_3]^{a_{12}a_{43}-a_{13}a_{42}} \\
&\quad [x_2, x_4]^{a_{12}+a_{12}a_{44}-a_{14}a_{42}} [x_3, x_4]^{a_{13}+a_{13}a_{44}-a_{14}a_{43}} \\
&= x_1^{p^{n-2}(a_{12}a_{43}-a_{13}a_{42})} \\
&\quad x_2^{p^2(a_{42}+a_{43}+a_{13}+a_{11}a_{42}-a_{12}a_{41}+a_{11}a_{43}-a_{13}a_{41}+a_{13}a_{44}-a_{14}a_{43})} \\
&\quad x_3^{p^2(1+a_{44}+a_{11}+a_{12}+a_{11}a_{44}-a_{14}a_{41}+a_{12}a_{44}-a_{14}a_{42})}.
\end{aligned}$$

On the other hand

$$\alpha([x_1, x_4]) = \alpha(x_3^{p^2}) = x_3^{p^2} x_1^{p^2 a_{31}} x_2^{p^2 a_{32}} x_3^{p^2 a_{33}} x_4^{p^2 a_{24}} = x_1^{p^2 a_{31}} x_2^{p^2 a_{32}} x_3^{p^2(1+a_{33})}.$$

Comparing the powers of x_1 and using (2.20), we get $a_{31} \equiv 0 \mod p^{n-2}$. Comparing the powers of x_2 and x_3, and using (2.19) - (2.20), we get

$$-a_{32} + a_{13} + a_{13}a_{44} \equiv 0 \mod p^2,$$

$$-a_{33} + a_{44} + a_{11} + a_{11}a_{44} + a_{12} + a_{12}a_{44} \equiv 0 \mod p^2.$$

Hence equations (2.4) - (2.6) hold.

Equations (2.7) - (2.9) are obtained by comparing the powers of x_1, x_2 and x_3 in $\alpha([x_3, x_4]) = \alpha(x_2^{p^2})$ and using equations (2.4), (2.19) and (2.20). Equations (2.10) - (2.12) are obtained by comparing the powers of x_1, x_2 and x_3 in $\alpha([x_1, x_2]) = \alpha(x_2^{p^2})$ and using equation (2.7). Equations (2.13) - (2.15) are obtained by comparing the powers of x_1, x_2 and x_3 in $\alpha([x_1, x_3]) = \alpha(x_2^{p^2})$ and using equations (2.4) and (2.7). Equations (2.16) - (2.17) are obtained by comparing the powers of x_2 and x_3 in $\alpha([x_2, x_4]) = \alpha(x_3^{p^2})$ and using equations (2.7), (2.19) and (2.20). The last equation (2.18) is obtained by comparing the powers of x_1 in $\alpha([x_2, x_3]) = \alpha(x_1^{p^{n-2}})$.

Theorem 2.2.3 *Let G be the group defined in (2.3). Then all automorphisms of G are central.*

Proof. We start with the claim that $1 + a_{44} \not\equiv 0 \mod p$. For, let us assume the contrary, i.e., p divides $1 + a_{44}$. Then

$$\alpha(x_4^p) = \alpha(x_4)^p = x_4^{p(1+a_{44})}(x_1^{a_{41}} x_2^{a_{42}} x_3^{a_{43}})^p \in \mathrm{Z}(G),$$

since $a_{4j} \equiv 0 \mod p^2$ for $1 \leq j \leq 3$ by equations (2.19) and (2.20). But this is not possible as $x_4^p \notin \mathrm{Z}(G)$. This proves our claim. Subtracting (2.16) from (2.5), we get $(1 + a_{44})(a_{13} - a_{23}) \equiv 0 \mod p^2$. Since p does not divide $1 + a_{44}$, we get

$$a_{13} \equiv a_{23} \mod p^2. \tag{2.21}$$

By equations (2.10) and (2.21) we have

$$a_{13}(1 - a_{12} + a_{22}) \equiv 0 \mod p^2. \tag{2.22}$$

Here we have three possibilities, namely (i) $a_{13} \equiv 0 \mod p^2$, (ii) $a_{13} \equiv 0 \mod p$, but $a_{13} \not\equiv 0 \mod p^2$, (iii) $a_{13} \not\equiv 0 \mod p$. We are going to show that cases (ii) and (iii) do not occur and in the case (i) $a_{ij} \equiv 0 \mod p^2$, $1 \leq i, j \leq 4$.

Case (i). Assume that $a_{13} \equiv 0 \mod p^2$. Equations (2.9) and (2.21), together with the fact that p does not divide $1+a_{44}$, gives $a_{32} \equiv 0 \mod p^2$. We claim that $1+a_{33} \not\equiv 0 \mod p$. Suppose p divides $1+a_{33}$. Since $a_{32} \equiv 0 \mod p^2$ and $a_{31} \equiv 0 \mod p^{n-2}$ (equation (2.4)), we get $\alpha(x_3^{p^3}) = x_1^{p^3 a_{31}} x_2^{p^3 a_{32}} x_3^{p^3(1+a_{33})} x_4^{p^3 a_{34}} = 1$, which is not possible. This proves our claim. So by equation (2.13), we get $a_{12} \equiv 0 \mod p^2$.

Subtracting (2.17) from (2.6), we get $(a_{11} - a_{22})(1 + a_{44}) \equiv 0 \mod p^2$. This implies that $a_{11} - a_{22} \equiv 0 \mod p^2$. Since $a_{i3} \equiv 0 \mod p^2$ for $i = 1, 2$, by equation (2.11) we get $a_{11}(1 + a_{11}) \equiv 0 \mod p^2$. Thus p^2 divides a_{11} or $1 + a_{11}$. We claim that p^2 can not divide $1+a_{11}$. For, suppose the contrary, i. e., $a_{11} \equiv -1 \mod p^2$. Since $n - 2 \geq 2$ and $a_{12} \equiv a_{13} \equiv 0 \mod p^2$, we get

$$\alpha(x_1)^{p^{n-2}} = x_1^{p^{n-2}(1+a_{11})} x_2^{p^{n-2} a_{12}} x_3^{p^{n-2} a_{13}} x_4^{p^{n-2} a_{14}} = 1.$$

This contradiction, to the fact that order of x_1 is p^n, proves our claim. Hence p^2 divides a_{11}. Since $a_{11} - a_{22} \equiv 0 \mod p^2$, by equation (2.17), it follows that $a_{33} \equiv a_{44} \mod p^2$. Putting the values a_{23}, a_{11} and a_{22} in (2.18), we get $a_{33} \equiv 0 \mod p^2$. Thus $a_{44} \equiv 0 \mod p^2$. Putting values of a_{32}, a_{33}, a_{11}, a_{22} and a_{13} in (2.14), we get $a_{14} \equiv 0 \mod p^2$. Putting values of a_{12}, a_{14}, a_{11} and a_{23} in (2.15), we get $a_{34} \equiv 0 \mod p^2$. Putting above values in (2.12), we get $a_{24} \equiv 0 \mod p^2$. Hence $a_{ij} \equiv 0 \mod p^2$ for $1 \leq i, j \leq 4$.

Case (ii). Assume that $a_{13} \equiv 0 \mod p$, but $a_{13} \not\equiv 0 \mod p^2$. Equation (2.22) implies that $(1 - a_{12} + a_{22}) \equiv 0 \mod p$. Now consider all the equations (2.7)-(2.18) mod p. Repeating the arguments of Case (i) after replacing p^2 by p, we get the following facts: (a) $a_{32} \equiv 0 \mod p$ (by (2.9)); (b) $a_{12} \equiv 0 \mod p$ (by (2.13)); (c) $a_{11} - a_{22} \equiv 0 \mod p$ (subtracting (2.17) from (2.6)); (d) $a_{11}(1 + a_{11}) \equiv 0 \mod p$ (by (2.11)). We claim that $a_{11} \equiv 0 \mod p$. For, suppose that $a_{11} + 1 \equiv 0 \mod p$. Since $n - 1 \geq 3$ and $a_{12} \equiv a_{13} \equiv 0 \mod p$, it follows that $\alpha(x_1)^{p^{n-1}} = x_1^{p^{n-1}(1+a_{11})} x_2^{p^{n-1}a_{12}} x_3^{p^{n-1}a_{13}} x_4^{p^{n-1}a_{14}} = 1$, which is a contradiction. This proves that p can not divide $a_{11} + 1$. Hence p divides a_{11}, and therefore by fact (c), we have $a_{22} \equiv 0 \mod p$. This gives a contradiction to the fact that $(1 - a_{12} + a_{22}) \equiv 0 \mod p$. Thus Case (ii) does not occur.

Case (iii). Finally assume that $a_{13} \not\equiv 0 \mod p$. Thus $(1 - a_{12} + a_{22}) \equiv 0 \mod p^2$, i.e., $1 + a_{22} \equiv a_{12} \mod p^2$ (we'll use this information throughout the remaining proof without referring). Notice that $(\alpha(x_2 x_1^{-1}))^{p^2} = x_1^{-p^2(1+a_{11})}$. Since the order of $(\alpha(x_2 x_1^{-1}))^{p^2}$ is p^{n-2}, p does not divide $(1 + a_{11})$. Putting the value of a_{32} from (2.16) into (2.9), we have $a_{23} = a_{23}(1 + a_{44})^2 \mod p^2$. Since $a_{23} \equiv a_{13} \mod p^2$ (equation (2.21)) and $a_{13} \not\equiv 0 \mod p$, it follows that $a_{23} \not\equiv 0 \mod p$. Hence $(1 + a_{44})^2 \equiv 1 \mod p^2$. This gives $a_{44}(a_{44} + 2) \equiv 0 \mod p^2$. Thus we have three cases (iii)(a) $a_{44} \equiv 0 \mod p^2$, (iii)(b) $a_{44} \equiv 0 \mod p$, but $a_{44} \not\equiv 0 \mod p^2$

and (iii)(c) $a_{44} \not\equiv 0 \mod p$. We are going to consider these cases one by one.

Case (iii)(a). Suppose that $a_{44} \equiv 0 \mod p^2$. Using this in (2.16) and (2.17), we get $a_{32} \equiv a_{23} \mod p^2$ and $a_{22} \equiv a_{33} \mod p^2$ respectively. Putting the value of a_{44} in (2.6), we have $a_{12} + a_{11} \equiv a_{33} \mod p^2$. Further, replacing a_{12} by $1 + a_{22}$ and a_{22} by a_{33}, we have $1 + a_{11} \equiv 0 \mod p^2$, which is a contradiction.

Case (iii)(b). Suppose that $a_{44} \equiv 0 \mod p$, but $a_{44} \not\equiv 0 \mod p^2$. Notice that by reading the equations $\mod p$, arguments of Case (iii)(a) show that $1+a_{11} \equiv 0 \mod p$, which is again a contradiction.

Case (iii)(c). Suppose that $a_{44} \not\equiv 0 \mod p$. This implies that $a_{44} \equiv -2 \mod p^2$. Putting this value of a_{44} in the difference of (2.8) and (2.6), we get $a_{11}+a_{12}-a_{22} \equiv 0 \mod p^2$. Since $1+a_{22} \equiv a_{12} \mod p^2$, this equation contradicts the fact that $1 + a_{11} \not\equiv 0 \mod p$.

Thus Case (iii) can not occur. This completes the proof of the theorem.

The following theorem gives the answer to the question raised at the beginning of this section.

Theorem 2.2.4 *For every positive integer $n \geq 4$ and every odd prime p, there exists a group G of order p^{n+10} and exponent p^n such that*

1. *for $n = 4$, $\gamma_2(G) = \mathrm{Z}(G) < \Phi(G)$ and $\mathrm{Aut}(G)$ is abelian;*
2. *for $n \geq 5$, $\gamma_2(G) < \mathrm{Z}(G) < \Phi(G)$ and $\mathrm{Aut}(G)$ is abelian.*

Moreover, the order of $\mathrm{Aut}(G)$ is p^{n+20}.

Proof. Let G be the group defined in (2.3). By Lemma 2.2.1, we have $|G| = p^{n+10}$, $\gamma_2(G) = \mathrm{Z}(G) < \Phi(G)$ for $n = 4$ and $\gamma_2(G) < \mathrm{Z}(G) < \Phi(G)$ for $n \geq 5$. By Theorem 2.2.3, we have $\mathrm{Aut}(G) = \mathrm{Autcent}(G)$. Thus to complete the proof of the theorem, it is sufficient to prove that $\mathrm{Autcent}(G)$ is an abelian group.

Since $Z(G) < \Phi(G)$, G is purely non-abelian. The exponents of $Z(G)$, $\gamma_2(G)$ and $G/\gamma_2(G)$ are p^{n-2}, p^2 and p^{n-2} respectively. Thus we get

$$R = \{z \in Z(G) \mid \ |z| \leq p^{n-2}\} = Z(G)$$

and

$$K = \{x \in G \mid \mathrm{ht}(x\gamma_2(G)) \geq p^2\} = G^{p^2}\gamma_2(G) = Z(G).$$

This shows that $R = K$. Also $R/\gamma_2(G) = Z(G)/\gamma_2(G) = \left\langle x_1^{p^2}\gamma_2(G)\right\rangle$. Thus all the conditions of Theorem 1.2.6 are now satisfied. Hence $\mathrm{Autcent}(G)$ is abelian. That the order of $\mathrm{Aut}(G)$ is p^{n+20} can be easily proved by using Lemmas 1.1.2, 1.1.3, Theorem 1.2.5 and the structures of $G/\gamma_2(G)$ and $Z(G)$. This completes the proof of the theorem.

2.3 Groups G with $\mathrm{Aut}(G)$ elementary abelian

As mentioned in the Section 2.1, all p-groups G (except the ones in [37]) available in the literature and having abelian automorphism group are special p-groups. Thus it follows that $\mathrm{Aut}(G)$, for all such groups G, is elementary abelian. One more weaker form of the conjecture of Mahalanobis is: (WC3) If $\mathrm{Aut}(G)$ is an elementary abelian p-group, then G is special. Berkovich and Janko [5, Problem 722] published the following long standing problem: *(Old problem) Study the p-groups G with elementary abelian* $\mathrm{Aut}(G)$.

The following theorem provides some structural information about a group G for which $\mathrm{Aut}(G)$ is elementary abelian.

Theorem 2.3.1 *Let G be a finite p-group such that* $\mathrm{Aut}(G)$ *is elementary abelian, where p is an odd prime. Then one of the following two conditions holds true:*

1. $\mathrm{Z}(G) = \Phi(G)$ *is elementary abelian;*

2. $\gamma_2(G) = \Phi(G)$ *is elementary abelian.*

Moreover, the exponent of G *is* p^2.

Proof. Since $\mathrm{Aut}(G)$ is elementary abelian, $G/Z(G)$ is elementary abelian and so $\Phi(G) \leq Z(G)$. Also from Theorem 1.2.8 G is purely non-abelian. It follows from Theorem 1.2.9 that either $Z(G)$ or $G/\gamma_2(G)$ is of exponent p. If the exponent of $Z(G)$ is p, then by Lemma 1.1.7 $Z(G) \leq \Phi(G)$. Hence $\mathrm{Z}(G) = \Phi(G)$ is elementary abelian. If the exponent of $G/\gamma_2(G)$ is p, then obviously $\gamma_2(G) = \Phi(G)$. Since the exponent of $\gamma_2(G)$ is equal to the exponent of $G/\mathrm{Z}(G)$, it follows that $\gamma_2(G) = \Phi(G)$ is elementary abelian. In any case the exponent of $\Phi(G)$ is p. Thus the exponent of G is at most p^2. That the exponent of G can not be p, follows from Theorem 1.2.7. Hence the exponent of G is p^2. This completes the proof of the theorem.

Let G be an arbitrary finite p-group such that $\mathrm{Aut}(G)$ is elementary abelian. Then it follows from the previous theorem that one of the following two conditions necessarily holds true: (C1) $\mathrm{Z}(G) = \Phi(G)$ is elementary abelian; (C2) $\gamma_2(G) = \Phi(G)$ is elementary abelian. *So one might expect that for such groups* G *both of the conditions (C1) and (C2) hold true, i.e., WC(3) holds true, or, a little less ambitiously, (C1) always holds true or (C2) always holds true.* In the following two theorems we show that none of the statements in the preceding sentence holds true.

Theorem 2.3.2 *There exists a group* G *of order* p^9 *such that* $\mathrm{Aut}(G)$ *is elementary abelian of order* p^{20}, $\Phi(G) < \mathrm{Z}(G)$ *and* $\gamma_2(G) = \Phi(G)$ *is elementary abelian.*

Theorem 2.3.3 *There exists a group G of order p^8 such that* $\mathrm{Aut}(G)$ *is elementary abelian of order p^{16}, $\gamma_2(G) < \Phi(G)$ and $\mathrm{Z}(G) = \Phi(G)$ is elementary abelian.*

First we proceed to construct p-group G as in Theorem 2.3.2

Let p be any prime, even or odd. Consider the group

$$\begin{aligned} G_1 \quad = \quad & \langle x_1, x_2, x_3, x_4, x_5 \mid x_1^{p^2} = x_2^{p^2} = x_3^{p^2} = x_4^{p^2} = x_5^p = 1, [x_1, x_2] = x_1^p, \\ & [x_1, x_3] = x_3^p, [x_1, x_4] = 1, [x_1, x_5] = x_1^p, [x_2, x_3] = x_2^p, [x_2, x_4] = 1, \\ & [x_2, x_5] = x_4^p, [x_3, x_4] = 1, [x_3, x_5] = x_4^p, [x_4, x_5] = 1\rangle. \end{aligned} \tag{2.23}$$

It is easy to see the following properties of G_1.

Lemma 2.3.4 *The group G_1 is a p-group having order p^9, $\gamma_2(G_1) = \Phi(G_1) <$ $\mathrm{Z}(G_1)$, $\Phi(G_1)$ is elementary abelian and the exponent of $Z(G_1)$ is p^2, where p is any prime. Moreover, if p is odd, then G_1 is regular.*

It can be checked by using GAP [23] that for $p = 2$, $\mathrm{Aut}(G_1)$ is elementary abelian. So we assume that p is odd. Let α be an arbitrary automorphism of G_1. Since the nilpotency class of G_1 is 2 and $\gamma_2(G_1)$ is generated by the set $\{x_i^p \mid 1 \leq i \leq 4\}$, we can write

$$\alpha(x_i) = x_i \prod_{j=1}^{5} x_j^{a_{ij}} \tag{2.24}$$

for some non-negative integers a_{ij} for $1 \leq i, j \leq 5$.

Lemma 2.3.5 *Let α be the automorphism of G_1 defined in (2.24). Then*

$$a_{4j} \equiv 0 \mod p \;\; \text{for} \;\; j = 1, 2, 3, 5. \tag{2.25}$$

Proof. Since $x_4 \in Z(G_1)$, it follows that $\alpha(x_4) = x_4^{1+a_{44}} x_1^{a_{41}} x_2^{a_{42}} x_3^{a_{43}} x_5^{a_{45}} \in Z(G_1)$. This is possible only when $a_{4j} \equiv 0 \mod p$ for $j = 1, 2, 3, 5$, which completes the proof of the lemma.

We'll make use of the following table in the proof of Theorem 2.3.2, which is produced in the following way. The equation in the kth row is obtained by applying α on the relation in kth row, then comparing the powers of x_i in the same row, and using preceding equations in the table and equations (2.25). For example, equation in 5th row is obtained by applying α on $[x_1, x_3] = x_3^p$, then comparing the powers of x_2 and using equations in 2nd and 3rd row.

Table 2.1: Table for the group G_1

No.	equations (read $\equiv 0 \mod p$)	relations	x_i's
1	a_{5j}, $1 \leq j \leq 4$	$x_5^p = 1$	$x_1, \dots, x_4$
2	a_{12}	$[x_1, x_5] = x_1^p$	x_2
3	a_{13}	$[x_1, x_5] = x_1^p$	x_3
4	a_{14}	$[x_1, x_5] = x_1^p$	x_4
5	a_{32}	$[x_1, x_3] = x_3^p$	x_2
6	$a_{55}(1 + a_{11})$	$[x_1, x_5] = x_1^p$	x_1
7	$a_{23}(1 + a_{11})$	$[x_1, x_2] = x_1^p$	x_3
8	$a_{21} + a_{21}a_{55}$	$[x_2, x_5] = x_4^p$	x_1
9	$a_{31} + a_{31}a_{55}$	$[x_3, x_5] = x_4^p$	x_1
10	$a_{35} + a_{11}a_{35} - a_{15}a_{31} - a_{31}$	$[x_1, x_3] = x_3^p$	x_1
11	$a_{11}(1 + a_{33})$	$[x_1, x_3] = x_3^p$	x_3
12	$a_{33}(1 + a_{22})$	$[x_2, x_3] = x_2^p$	x_2
13	$a_{55} + a_{33} + a_{33}a_{55} - a_{44}$	$[x_3, x_5] = x_4^p$	x_4
14	$a_{55} + a_{22} + a_{22}a_{55} + a_{23}(1 + a_{55}) - a_{44}$	$[x_2, x_5] = x_4^p$	x_4
15	$(a_{22} + a_{25})(1 + a_{11}) - a_{15}a_{21}$	$[x_1, x_2] = x_1^p$	x_1
16	$a_{35}(1 + a_{23} + a_{22}) - a_{25}(1 + a_{33}) - a_{24}$	$[x_2, x_3] = x_2^p$	x_4
17	$-a_{15} - a_{15}a_{22} - a_{15}a_{23}$	$[x_1, x_2] = x_1^p$	x_4
18	$-a_{15} - a_{15}a_{33} - a_{34}$	$[x_1, x_3] = x_3^p$	x_4

Now we are ready to prove Theorem 2.3.2. In the following proof, by (k) we mean the equation in the kth row of Table 2.1.

Proof of Theorem 2.3.2. Consider the group G_1 defined in 2.23. It follows from Lemma 2.3.4 that G_1 is of order p^9, $\Phi(G_1) < \mathrm{Z}(G_1)$ and $\gamma_2(G_1) = \Phi(G_1)$ is elementary abelian. It is easy to show that the order of $\mathrm{Autcent}(G_1)$ is p^{20}. As mentioned earlier, it can be checked using GAP that $\mathrm{Aut}(G_1)$ is elementary abelian for $p = 2$. We therefore assume that p is odd. We now prove that all automorphisms of G_1 are central. Let α be the automorphism of G_1 defined in (2.24), i.e., $\alpha(x_i) = x_i \prod_{j=1}^{5} x_i^{a_{ij}}$, where a_{ij} are non-negative integers for $1 \le i, j \le 5$. Since $G_1/\mathrm{Z}(G_1)$ is elementary abelian, it is sufficient to prove that $a_{ij} \equiv 0 \mod p$ for $1 \le i, j \le 5$.

Since $\alpha(x_1^p) = x_1^{p(1+a_{11})} \prod_{j=2}^{5} x_j^{pa_{1j}} \ne 1$, $x_5^p = 1$ and $a_{1j} \equiv 0 \mod p$ for $2 \le j \le 4$, it follows that $1 + a_{11}$ is not divisible by p. Therefore (6) and (7) give $a_{55} \equiv 0 \mod p$ and $a_{23} \equiv 0 \mod p$ respectively. Thus by (8) and (9) respectively, we get $a_{21} \equiv 0 \mod p$ and $a_{31} \equiv 0 \mod p$. Using the fact that $a_{31} \equiv 0 \mod p$, (10) reduces to the equation $a_{35}(1 + a_{11}) \equiv 0 \mod p$. Since $1 + a_{11}$ is not divisible by p, we get $a_{35} \equiv 0 \mod p$. Observe that $1 + a_{33}$ is not divisible by p. For, suppose p divides $1 + a_{33}$. Since a_{31}, a_{32}, a_{35} are divisible by p and $x_4 \in Z(G_1)$, it follows that $\alpha(x_3) \in Z(G_1)$, which is not true. Using this fact, it follows from (11) that $a_{11} \equiv 0 \mod p$. Using above information, (13), (14) and (15) reduce, respectively, to the following equations.

$$a_{33} - a_{44} \equiv 0 \mod p, \tag{2.26}$$

$$a_{22} - a_{44} \equiv 0 \mod p, \tag{2.27}$$

$$a_{22} + a_{25} \equiv 0 \mod p. \tag{2.28}$$

Subtracting equation (2.27) from equation (2.26), we get $a_{33} - a_{22} \equiv 0 \mod p$. Adding this to equation (2.28) gives $a_{33} + a_{25} \equiv 0 \mod p$. Using this fact after adding (12) to equation (2.28), we get $a_{22}(1 + a_{33}) \equiv 0 \mod p$. Since $1 + a_{33}$ is not divisible by p, $a_{22} \equiv 0 \mod p$. Thus equations (2.27) and (2.28) give $a_{44} \equiv 0 \mod p$ and $a_{25} \equiv 0 \mod p$ respectively. So $a_{33} \equiv 0 \mod p$ from equation 2.26. Now (16) and (17) give $a_{24} \equiv 0 \mod p$ and $a_{15} \equiv 0 \mod p$ respectively. Finally, from (18) we get $a_{34} \equiv 0 \mod p$. Hence all $a_{ij}'s$ are divisible by p, which shows that α is a central automorphism of G_1. Since α was an arbitrary automorphism of G_1, we get $\mathrm{Aut}(G_1) = \mathrm{Autcent}(G_1)$.

It now remains to prove that $\mathrm{Aut}(G_1)$ is elementary abelian. Notice that G_1 is purely non-abelian. Since $\gamma_2(G_1) = \Phi(G_1)$, the exponent of $G_1/\gamma_2(G_1)$ is p. That $\mathrm{Aut}(G_1) = \mathrm{Autcent}(G_1)$ is elementary abelian now follows from Theorem 1.2.9. This completes the proof of the theorem.

Now we proceed to construct a finite p-group G such that $\mathrm{Aut}(G)$ is elementary abelian, $\gamma_2(G) < \Phi(G)$ and $\Phi(G) = \mathrm{Z}(G)$ is elementary abelian. Let p be any prime, even or odd. Define the group

$$\begin{aligned} G_2 \;=\; & \langle x_1, x_2, x_3, x_4 \mid x_1^{p^2} = x_2^{p^2} = x_3^{p^2} = x_4^{p^2} = 1, [x_1, x_2] = 1, [x_1, x_3] = x_4^p, \\ & [x_1, x_4] = x_4^p, [x_2, x_3] = x_1^p, [x_2, x_4] = x_2^p, [x_3, x_4] = x_4^p \rangle. \end{aligned} \tag{2.29}$$

It is easy to prove the following lemma.

Lemma 2.3.6 *The group G_2 is a p-group of order p^8, $\gamma_2(G_2) < \Phi(G_2)$ and $\mathrm{Z}(G_2) = \Phi(G_2)$ is elementary abelian, where p is any prime. Moreover, if p is odd, then G_2 is regular.*

Again, It can be checked by using GAP that for $p = 2$, $\mathrm{Aut}(G_2)$ is elementary abelian. So from now onwards, we assume that p is odd. Let α be an arbitrary automorphism of G_2. Since the nilpotency class of G_2 is 2 and $\gamma_2(G_2)$ is generated by the set $\{x_1^p, x_2^p, x_4^p\}$, we can write

$$\alpha(x_i) = x_i \prod_{j=1}^{4} x_j^{a_{ij}} \tag{2.30}$$

for some non-negative integers a_{ij} for $1 \le i, j \le 4$.

The following table, which will be used in the proof of Theorem 2.3.3 below, is produced in a similar fashion as Table 1.

Table 2.2: Table for the group G_2

No.	equations	relations	x_i's
1	$a_{13} \equiv 0 \mod p$	$[x_2, x_3] = x_1^p$	x_3
2	$a_{23} \equiv 0 \mod p$	$[x_2, x_4] = x_2^p$	x_3
3	$a_{43} \equiv 0 \mod p$	$[x_1, x_3] = x_4^p$	x_3
4	$a_{41} \equiv 0 \mod p$	$[x_1, x_4] = x_4^p$	x_1
5	$a_{21} \equiv 0 \mod p$	$[x_2, x_4] = x_2^p$	x_1
6	$a_{24} \equiv 0 \mod p$	$[x_2, x_4] = x_2^p$	x_4
7	$a_{14} \equiv 0 \mod p$	$[x_2, x_3] = x_1^p$	x_4
8	$a_{44}(1 + a_{22}) \equiv 0 \mod p$	$[x_2, x_4] = x_2^p$	x_2
9	$a_{11} + a_{11}a_{44} \equiv 0 \mod p$	$[x_1, x_4] = x_4^p$	x_4
10	$a_{22} + a_{22}a_{33} + a_{33} - a_{11} \equiv 0 \mod p$	$[x_2, x_3] = x_1^p$	x_1
11	$-a_{42}(1 + a_{33}) \equiv 0 \mod p$	$[x_3, x_4] = x_4^p$	x_1
12	$a_{12} + a_{12}a_{44} - a_{42} \equiv 0 \mod p$	$[x_1, x_4] = x_4^p$	x_2
13	$a_{32} + a_{32}a_{44} - a_{34}a_{42} - a_{42} \equiv 0 \mod p$	$[x_3, x_4] = x_4^p$	x_2
14	$a_{34}(1 + a_{22}) - a_{12} \equiv 0 \mod p$	$[x_2, x_3] = x_1^p$	x_2
15	$a_{11}(1 + a_{33} + a_{34}) + a_{33} + a_{34} - a_{44} \equiv 0 \mod p$	$[x_1, x_3] = x_4^p$	x_4
16	$a_{31} + a_{31}a_{44} + a_{33} + a_{33}a_{44} \equiv 0 \mod p$	$[x_3, x_4] = x_4^p$	x_4

Now we are ready to prove Theorem 2.3.3. By (k), in the following proof, we mean the equation in the kth row of Table 2.2.

Proof of Theorem 2.3.3. Consider the group G_2 defined in 2.29. It follows from Lemma 2.3.6 that G_2 is of order p^8, $\gamma_2(G_2) < \Phi(G_2)$ and $\mathrm{Z}(G_2) = \Phi(G_2)$ is elementary abelian. It is again easy to show that the order of $\mathrm{Autcent}(G_2)$ is p^{16}. Since $\mathrm{Aut}(G_2)$ is elementary abelian for $p = 2$, assume that p is odd. As in the proof of Theorem 2.3.2, to show that all automorphisms of G_2 are central, it is sufficient to show that $a_{ij} \equiv 0 \mod p$ for $1 \leq i, j \leq 4$.

Since a_{21}, a_{23}, a_{24} are divisible by p, it follows that $(1 + a_{22})$ is not divisible by p. For, if p divides $(1 + a_{22})$, then $\alpha(x_2) \in Z(G_2)$, which is not possible. Using this fact, (8) gives $a_{44} \equiv 0 \mod p$. Thus from (9) we get $a_{11} \equiv 0 \mod p$. Now we observe from (10) that $(1 + a_{33})$ is not divisible by p. For, suppose, $(1 + a_{33})$ is divisible by p, then using the fact that $a_{11} \equiv 0 \mod p$, (10) gives $a_{33} \equiv 0 \mod p$, which is not possible. Thus (11) gives $a_{42} \equiv 0 \mod p$. Now using that a_{42} and a_{44} are divisible by p, (12) and (13) give $a_{12} \equiv 0 \mod p$ and $a_{32} \equiv 0 \mod p$ respectively. Since $a_{12} \equiv 0 \mod p$ and $(1 + a_{22})$ is not divisible by p, (14) gives $a_{34} \equiv 0 \mod p$. Using that a_{11}, a_{34} and a_{44} are divisible by p, (15) gives $a_{33} \equiv 0 \mod p$. Now using that a_{33} and a_{44} are divisible by p, equation (16) gives $a_{31} \equiv 0 \mod p$. Since a_{11} and a_{33} are divisible by p, equation (10) gives $a_{22} \equiv 0 \mod p$. Hence $a_{ij} \equiv 0 \mod p$ for $1 \leq i, j \leq 4$.

Since $\mathrm{Z}(G_2)$ is elementary abelian, $\mathrm{Aut}(G_2) = \mathrm{Autcent}(G_2)$ is elementary abelian by Theorem 1.2.9. This completes the proof of the theorem.

Let G be a purely non-abelian finite 2-group such that $\mathrm{Aut}(G)$ is elementary abelian. Thus $\mathrm{Aut}(G) = \mathrm{Autcent}(G)$. Then G satisfies one of the three conditions of Theorem 1.2.10. We here record that there exist groups G which satisfy exactly one condition of this theorem. It is easy to show that the 2-group G_1 constructed in (2.23) satisfies only the first condition of Theorem 1.2.10 and the 2-group G_2 constructed in (2.29) satisfies only the second condition of Theorem 1.2.10. That $\mathrm{Aut}(G_1)$ and $\mathrm{Aut}(G_2)$ are elementary abelian, can be checked using GAP. The examples of 2-groups G satisfying only the third condition of Theorem 1.2.10 with $\mathrm{Aut}(G)$ elementary abelian were constructed by Miller [51] and Curran [13].

The examples constructed in Theorems 2.2.4, 2.3.2 and 2.3.3 indicate that it is difficult to put an obvious structure on the class of groups G such that $\mathrm{Aut}(G)$ is abelian or even elementary abelian. We remark that many non-isomorphic groups, satisfying the conditions of the above theorems, can be obtained by making suitable changes in the presentations given in (2.3), (2.23) and (2.29). We conclude this chapter with a further remark that the kind of examples constructed in this chapter may be useful in cryptography (see [48] for more details).

Chapter 3

Class-preserving Automorphisms of Groups

In this chapter we will investigate some structural properties of groups of class-preserving automorphisms.

3.1 Class-preserving Automorphisms: Literature

Recall from Chapter 1 that an automorphism of a group G is called class-preserving if it maps each group element to a conjugate of it. The set of all class-preserving automorphisms form a normal subgroup of $\mathrm{Aut}(G)$ and we denote it by $\mathrm{Aut}_c(G)$. In 1911, Burnside [9] asked the following question: Does there exist a finite group G such that G has a non-inner class-preserving automorphism? In 1913, he himself gave an affirmative answer to this question. He constructed a group G of order p^6 isomorphic to the group W consisting of all 3×3 matrices

$$\begin{bmatrix} 1 & 0 & 0 \\ x & 1 & 0 \\ z & y & 1 \end{bmatrix}$$

with x, y, z in the field $\mathbb{F}_{p^2}$ of p^2 elements, where p is an odd prime. This group G is of nilpotency class 2 with elementary abelian $\mathrm{Aut}_c(G)$ of order p^8, while order of $\mathrm{Out}_c(G)$ is p^4. In 1947, Wall constructed finite groups G having non-inner class-preserving automorphism [71]. His examples also contain 2 groups smallest of which is a group of order 2^5. These groups are in fact the general linear group $\mathrm{GL}(1, \mathbb{Z}/m)$ where m is divisible by 8. In 1979, Heineken on the way to producing examples of finite group in which all normal subgroups are characteristic, constructed finite p-groups G of nilpotency class 2 with $\mathrm{Aut}(G) = \mathrm{Aut}_c(G)$ and $\mathrm{Out}_c(G) \neq 1$ [29]. So the group of class-preserving automorphisms can be as big as the whole automorphism group. One more example of such finite p-group G, having order p^6 and nilpotency class 3, was constructed by Malinowska [49]. She also constructed p-groups G of arbitrary nilpotency class $r > 2$ for any prime $p > 5$ such that $\mathrm{Out}_c(G) \neq 1$. In 2001, Hertweck constructed a family of Frobenius groups as subgroups of affine semi-linear groups $A\Gamma(\mathbb{F})$ where $\mathbb{F}$ is is a finite field, which possess class-preserving automorphisms that are not inner [31]. Many classes of groups, which do not have any non-inner class-preserving automorphism, also have been explored in the past. We will see examples of such groups in Chapter 4.

Given some structure on a group G, there also have been attempts to get some structural information about $\mathrm{Aut}_c(G)$. In 1968, Sah [65], using a result of Hall, noticed that if G is nilpotent of class c, then $\mathrm{Aut}_c(G)$ is nilpotent of class $c - 1$.

He, using homolgical techniques and some results of Schur and Wedderburn, also proved that $\mathrm{Aut}_c(G)$ is solvable when G is finite solvable. Further he proved that if G is a group admitting a composition series and for each composition factor F of G, the group $\mathrm{Aut}(F)/\mathrm{Inn}(F)$ is solvable, then $\mathrm{Out}_c(G)$ is solvable. An immediate corollary of this result and Schreier hypothesis (i.e., $\mathrm{Aut}(S)/\mathrm{Inn}(S)$ is solvable for every finite simple group S) is that, $\mathrm{Out}_c(G)$ is solvable for every finite group G. More results on the structure of $\mathrm{Aut}_c(G)$ were established in 1976 by Laue [47] who proved that, if G is a finite supersolvable group, then so is $\mathrm{Aut}_c(G)$. Further he proved that if G is a finite supersolvable group and $\Phi(G) = 1$, then $\mathrm{Out}_c(G)$ is nilpotent. He also proved that if G is a finite solvable group and each chief factor of G is complemented, then $\mathrm{Out}_c(G)$ is supersolvable. An optimal bound on $|\mathrm{Aut}_c(G)|$ for finite p-groups G was obtained by Yadav [72]. He proved that if G is group of order p^n, then $|\mathrm{Aut}_c(G)| \leq p^{(n^2-4)/4}$, if n is even, otherwise $|\mathrm{Aut}_c(G)| \leq p^{(n^2-1)/4}$. He also classified all finite p-groups which attain this bound. We refer the reader to [73] for a more comprehensive survey on the topic.

3.2 Solvability of $\mathrm{Aut}_c(G)$

Sah noticed that $\mathrm{Out}_c(G)$ is a non-abelian simple group if G is a restricted symmetric group on a countably infinite set. So the solvability of $\mathrm{Aut}_c(G)/\mathrm{Inn}(G)$ can not be extended to infinite groups G. In this section we investigate whether the other result of Sah, i.e., $\mathrm{Aut}_c(G)$ is solvable when G is finite solvable, can be extended to arbitrary groups.

We start with the following key lemma.

Lemma 3.2.1 *Let G be a group and $\alpha \in \delta_k(\mathrm{Aut}_c(G))$ for some $k \geq 1$. Then for each $x \in G$ there exists $b_x \in \delta_k(G)$ such that $\alpha(x) = b_x^{-1} x b_x$.*

Proof. Notice that, it is enough to prove the lemma for generators of $\delta_k(\mathrm{Aut}_c(G))$. We apply induction here. For $k = 1$, the lemma holds true. Suppose that for $k = i$, the lemma is true. Let $\alpha, \beta \in \delta_i(\mathrm{Aut}_c(G))$. For $x \in G$, let $\alpha(x) = y^{-1}xy$ and $\beta(x) = z^{-1}xz$ for some $y, z \in \delta_i(G)$. Then

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

Put

$$\begin{aligned}
b_x^{-1} &= \alpha^{-1}\beta^{-1}\alpha(z^{-1})\alpha^{-1}\beta^{-1}(y^{-1})\alpha^{-1}\beta^{-1}(z)\alpha^{-1}(y) \\
&= \alpha^{-1}\beta^{-1}(\alpha(z^{-1})y^{-1}z\beta(y))
\end{aligned}$$

$$
\begin{aligned}
&= \alpha^{-1}\beta^{-1}(\alpha(z^{-1})zz^{-1}y^{-1}zyy^{-1}\beta(y)) \\
&= \alpha^{-1}\beta^{-1}(\alpha(z^{-1})z[z,y]y^{-1}\beta(y)).
\end{aligned}
$$

Thus $[\alpha,\beta](x) = b_x^{-1}xb_x$. Since $y, z \in \delta_i(G)$, $[z,y] \in \delta_{i+1}(G)$. Now by induction hypothesis, notice that $\alpha(z^{-1})z,\ y^{-1}\beta(y) \in \delta_{i+1}(G)$. Thus it follows that $b_x^{-1} \in \delta_{i+1}(G)$. This completes the proof.

The following theorem extends Sah's result to an arbitrary group and also gives additional information on the solvability length of $\mathrm{Aut}_c(G)$.

Theorem 3.2.2 *Let G be a solvable group of length l. Then $\mathrm{Aut}_c(G)$ is a solvable group of length either l or $l-1$.*

Proof. Let G be a solvable group of length l. Then $\delta_{l+1}(G) = 1$. By Lemma 3.2.1 it follows that $\delta_{l+1}(\mathrm{Aut}_c(G)) = 1$, which shows that $\mathrm{Aut}_c(G)$ is solvable of length at most l. When $\delta_l(G) \leq Z(G)$, using Lemma 3.2.1 again, it follows that the solvable length of $\mathrm{Aut}_c(G)$ is $l-1$. Since $\mathrm{Inn}(G)$ is contained in $\mathrm{Aut}_c(G)$ and the solvable length of $\mathrm{Inn}(G)$ is at least $l-1$, the solvable length of $\mathrm{Aut}_c(G)$ can not be less than $l-1$. This proves the theorem.

We have the following direct consequence of Theorem 3.2.2.

Corollary 3.2.3 *If G is a metabelian group, then so is $\mathrm{Aut}_c(G)$.*

The following lemma can be proved on the lines of the Lemma 3.2.1.

Lemma 3.2.4 *Let G be a group and $\alpha \in \gamma_k(\mathrm{Aut}_c(G))$ for some $k \geq 1$. Then for each $x \in G$ there exists $b_x \in \gamma_k(G)$ such that $\alpha(x) = b_x^{-1}xb_x$.*

The following theorem can be easily proved using Lemma 3.2.4.

Theorem 3.2.5 *Let G be a nilpotent group of class c. Then $\mathrm{Aut}_c(G)$ is a nilpotent group of class $c-1$. Moreover, if G is residually nilpotent, then $\mathrm{Aut}_c(G)$ is also residually nilpotent.*

We have mentioned in the preceding section that if G is finite supersolvable group, then $\mathrm{Aut}_c(G)$ is supersolvable. The following theorem (which is true for arbitrary groups) puts some additional structure on $\mathrm{Aut}_c(G)$ when G is a finite supersolvable group.

Theorem 3.2.6 *Let G be a supersolvable group. Then $\mathrm{Aut}_c(G)$ is a nilpotent-by-abelian group.*

Proof. Since G is a supersolvable group, $\gamma_2(G)$ is nilpotent. Using Lemma 3.2.4 and applying the same technique as in the proof of Lemma 3.2.1, we can see that $\gamma_2(\mathrm{Aut}_c(G))$ is nilpotent. It now follows that $\mathrm{Aut}_c(G)$ is a nilpotent-by-abelian group.

3.3 Nilpotency of $\mathrm{Out}_c(G)$

In this section we investigate about the nilpotency of $\mathrm{Out}_c(G)$ for a given group G. We shall first establish a relation between the nilpotency of $\mathrm{Out}_c(G)$ and nilpotency of $\mathrm{Out}_c(G/Z_j(G))$. We start with the following lemma which generalizes a lemma of Gumber and Sharma [25].

Lemma 3.3.1 *Let G be a group and $N \trianglelefteq G$. If $\gamma_j(\mathrm{Aut}_c(G/N)) \leq \gamma_k(\mathrm{Inn}(G/N))$ for some $j, k \in \mathbb{N}$, then $\gamma_j(\mathrm{Aut}_c(G)) \leq (\gamma_k(\mathrm{Aut}_c(G)) \cap \mathrm{Aut}^N(G))\gamma_k(\mathrm{Inn}(G))$.*

Proof. Let $\alpha \in \gamma_j(\mathrm{Aut}_c(G))$. We will show that $\alpha \in (\gamma_k(\mathrm{Aut}_c(G)) \cap \mathrm{Aut}^N(G))$ $\gamma_k(\mathrm{Inn}(G))$. Without loss of generality we can assume $\alpha = [\alpha_1, \alpha_2, \ldots, \alpha_j]$, where $\alpha_i \in \mathrm{Aut}_c(G)$ for $i = 1, ..., j$. Let $\bar{\alpha}$ denotes the automorphism induced by α on G/N. Note that $\bar{\alpha} = [\bar{\alpha_1}, \bar{\alpha_2}, \ldots, \bar{\alpha_j}]$. Therefore $\bar{\alpha} \in \gamma_j(\mathrm{Aut}_c(G/N))$. Hence by the given hypothesis there exists some $a \in \gamma_k(G)$ such that $\bar{\alpha}(xN) = axa^{-1}N$ for all $x \in G$. It follows that $\alpha(x) = axa^{-1}n_x$ for some $n_x \in N$. Consider the automorphism $\beta = \sigma_a\alpha$, where σ_a denotes the inner automorphism induced by a, i.e., $\sigma_a(x) = a^{-1}xa$. Note that $x^{-1}\beta(x) = a^{-1}n_xa \in N$. Therefore $\beta \in \mathrm{Aut}^N(G)$. Without loss of generality we can assume that $k \leq j$. Therefore $\alpha \in \gamma_j(\mathrm{Aut}^c(G)) \leq \gamma_k(\mathrm{Aut}_c(G))$. Also, since $a \in \gamma_k(G)$, we have $\sigma_a \in \gamma_k(\mathrm{Inn}(G)) \leq \gamma_k(\mathrm{Aut}^c(G))$. Hence $\beta \in \gamma_k(\mathrm{Aut}_c(G)) \cap \mathrm{Aut}^N(G)$. Since $\alpha = (\sigma_a)^{-1}\beta$, it follows that $\alpha \in (\gamma_k(\mathrm{Aut}_c(G)) \cap \mathrm{Aut}^N(G))\gamma_k(\mathrm{Inn}(G))$. This proves the lemma.

An automorphism α of a group G is called an IA automorphism if it induces the identity mapping on the abelianization of the group, i.e., on $G/\gamma_2(G)$. We consider here the set of those IA automorphisms that fix the center element-wise. This set forms a normal subgroup of $\mathrm{Aut}(G)$ and we denote it by $\mathrm{IA}_z(G)$. Clearly, $\mathrm{Aut}_c(G) \leq \mathrm{IA}_z(G)$. Let $Z_i(G)$, for $i < 0$, denote the trivial group. We prove the following lemmas.

Lemma 3.3.2 *Let G be any group. Then for $j, k \in \mathbb{N}$,*

1. $[\gamma_k(G), \mathrm{Aut}^{Z_j(G)}(G)] \leq Z_{j-k+1}(G)$,
2. $[Z_j(G), \gamma_k(\mathrm{IA}_z(G))] \leq Z_{j-k}(G)$.

Proof. (1) Obviously $[G, \mathrm{Aut}^{Z_j(G)}(G)] \leq Z_j(G)$. Now we apply induction on k. Suppose $[\gamma_i(G), \mathrm{Aut}^{Z_j(G)}(G)] \leq Z_{j-i+1}(G)$. Note that $[G, \mathrm{Aut}^{Z_j(G)}(G), \gamma_i(G)] \leq$

$Z_{j-i}(G)$ and $[\mathrm{Aut}^{Z_j(G)}(G), \gamma_i(G), G] \leq Z_{j-i}(G)$. Therefore by Lemma 1.1.9, we get $[\gamma_{i+1}(G), \mathrm{Aut}^{Z_j(G)}(G)] \leq Z_{j-i}(G)$. This proves the result for all k.

(2) Note that if we prove the result for $k = 1$, then applying induction on k and Lemma 1.1.9, the result easily follows. So let us assume that $k = 1$. Let $\alpha \in IA_z(G)$. Clearly $[Z(G), \alpha] \leq \{1\}$. We will apply induction on j. Suppose $[Z_i(G), \alpha] \leq Z_{i-1}(G)$, in other words let α induces the identity mapping on $Z_i(G)/Z_{i-1}(G)$. Let $x \in Z_{i+1}(G)$ and $y \in G$. Then $[x, y] \in Z_i(G)$. Therefore $\alpha([x, y])Z_{i-1}(G) = [x, y]Z_{i-1}(G)$. So that $\alpha(x^{-1})y^{-1}y\alpha(y^{-1})\alpha(x)\alpha(y)Z_{i-1}(G) = [x, y]Z_{i-1}(G)$. But $y\alpha(y^{-1}) \in \gamma_2(G)$, $\alpha(x) \in Z_{i+1}(G)$ and $[\gamma_2(G), Z_{i+1}(G)] \leq Z_{i-1}(G)$, therefore we have $\alpha(x^{-1})y^{-1}\alpha(x)yZ_{i-1}(G) = [x, y]Z_{i-1}(G)$. This implies that

$$[\alpha(x)x^{-1}, y]y^{-1}xyZ_{i-1}(G) = y^{-1}xyZ_{i-1}(G).$$

Therefore $[\alpha(x)x^{-1}, y] \in Z_{i-1}(G)$. Since x, y and α were chosen arbitrarily, we get $[Z_{i+1}(G), \mathrm{IA}_z(G)] \leq Z_i(G)$. This completes the proof of the lemma.

Lemma 3.3.3 *Let G be a group and A be a subgroup of* $\mathrm{Aut}(G)$ *such that* $\mathrm{Inn}(G) \leq A \leq IA_z(G)$. *Then* $A \cap \mathrm{Aut}^{Z_j(G)}(G) = Z_j(A)$.

Proof. First we prove that $\mathrm{Aut}^{Z(G)}(G) = C_{\mathrm{Aut}(G)}(A)$. Since $\mathrm{Inn}(G) \leq A$, the inclusion $C_{\mathrm{Aut}(G)}(A) \leq \mathrm{Aut}^{Z(G)}(G)$ is obvious. Now suppose that $\alpha \in \mathrm{Aut}^{Z(G)}(G)$ and $\beta \in A$. Since α fixes $\gamma_2(G)$ element-wise and $x^{-1}\beta(x) \in \gamma_2(G)$, we get $\alpha\beta(x) = \alpha(xx^{-1}\beta(x)) = \alpha(x)x^{-1}\beta(x)$. But β fixes $Z(G)$ element-wise and $\alpha(x)x^{-1} \in Z(G)$, hence we get $\alpha\beta(x) = \beta(\alpha(x)x^{-1})\beta(x) = \beta\alpha(x)$. Since α and β were chosen arbitrarily, this shows that $\mathrm{Aut}^{Z(G)}(G) \leq C_{\mathrm{Aut}(G)}(A)$, and hence $\mathrm{Aut}^{Z(G)}(G) = C_{\mathrm{Aut}(G)}(A)$. It now follows that $A \cap \mathrm{Aut}^{Z(G)}(G) = Z(A)$. We now apply induction on j. Suppose that $A \cap \mathrm{Aut}^{Z_i(G)}(G) = Z_i(A)$. Let $\alpha \in A \cap \mathrm{Aut}^{Z_{i+1}(G)}(G)$ and $\beta \in A$. Let $x \in G$ and $\alpha(x) = xz_1$ and $\beta(x) = xg_2$

for some $z_1 \in Z_{i+1}(G)$ and $g_2 \in \gamma_2(G)$. Note that $\alpha^{-1}(x) = x\alpha^{-1}(z_1^{-1})$ and $\beta^{-1}(x) = x\beta^{-1}(g_2^{-1})$. Now consider

$$
\begin{aligned}
[\alpha, \beta](x) &= \alpha^{-1}\beta^{-1}\alpha\beta(x) \\
&= \alpha^{-1}\beta^{-1}\alpha(xg_2) \\
&= \alpha^{-1}\beta^{-1}(xz_1\alpha(g_2)) \\
&= \alpha^{-1}(\beta^{-1}(x)\beta^{-1}(z_1)\beta^{-1}\alpha(g_2)) \\
&= \alpha^{-1}(x\beta^{-1}(g_2^{-1})\beta^{-1}(z_1)\beta^{-1}\alpha(g_2)) \\
&= x\alpha^{-1}(z_1^{-1})\alpha^{-1}\beta^{-1}(g_2^{-1})\alpha^{-1}\beta^{-1}(z_1)\alpha^{-1}\beta^{-1}\alpha(g_2) \\
&= x\alpha^{-1}\beta^{-1}(\beta(z_1^{-1})g_2^{-1}z_1\alpha(g_2)) \\
&= x\alpha^{-1}\beta^{-1}(\beta(z_1^{-1})z_1[z_1, g_2]g_2^{-1}\alpha(g_2)).
\end{aligned}
$$

So that $x^{-1}[\alpha, \beta](x) = \alpha^{-1}\beta^{-1}(\beta(z_1^{-1})z_1[z_1, g_2]g_2^{-1}\alpha(g_2))$. By Lemma 3.3.2 we have $\beta(z_1^{-1})z_1, \quad g_2^{-1}\alpha(g_2) \in Z_i(G)$. Clearly $[z_1, g_2] \in Z_i(G)$. Therefore we get $x^{-1}[\alpha, \beta](x) \in Z_i(G)$. Hence $[\alpha, \beta] \in A \cap \mathrm{Aut}^{Z_i(G)}(G)$. By induction hypothesis we get $[\alpha, \beta] \in Z_i(A)$. Since β was chosen arbitrarily, we have $\alpha \in Z_{i+1}(A)$. This shows that $A \cap \mathrm{Aut}^{Z_{i+1}(G)}(G) \leq Z_{i+1}(A)$. Now assume that $\alpha \in Z_{i+1}(A)$. Therefore for all $\beta \in A$, $[\alpha, \beta] \in Z_i(A)$. By induction hypothesis $[\alpha, \beta] \in A \cap \mathrm{Aut}^{Z_i(G)}(G)$. Therefore, for all $x \in G$, $x^{-1}[\alpha, \beta](x) \in Z_i(G)$. Let β be the inner automorphism induced by some $y \in G$. It follows that $[x, y\alpha^{-1}(y^{-1})] \in Z_i(G)$ for all $x, y \in G$. Therefore $\alpha \in \mathrm{Aut}^{Z_{i+1}(G)}(G)$. Since α was chosen arbitrarily, we get $Z_{i+1}(A) \leq A \cap \mathrm{Aut}^{Z_{i+1}(G)}(G)$. This proves that $A \cap \mathrm{Aut}^{Z_{i+1}(G)}(G) = Z_{i+1}(A)$ and the proof is complete.

The following corollary is a direct consequence of Lemma 3.3.3.

Corollary 3.3.4 *Let G be a group. Then* $\mathrm{Aut}_c(G) \cap \mathrm{Aut}^{Z_j(G)}(G) = Z_j(\mathrm{Aut}_c(G))$.

Now we are ready to prove the following theorem which establishes a relation between nilpotency of $\mathrm{Out}_c(G)$ and $\mathrm{Out}_c(G/Z_j(G))$.

Theorem 3.3.5 *Let G be a group such that $\mathrm{Out}_c(G/Z_j(G))$ is a nilpotent group of class k. Then $\mathrm{Out}_c(G)$ is a nilpotent group of class at most $j+k$. Moreover, if $\mathrm{Out}_c(G/Z_j(G))$ is a trivial group, then $\mathrm{Out}_c(G)$ is a nilpotent group of class at most j.*

Proof. Since $\mathrm{Out}_c(G/Z_j(G))$ is a nilpotent group of class k, we have

$$\gamma_{k+1}(\mathrm{Aut}_c(G/Z_j(G))) \leq \mathrm{Inn}(G/Z_j(G)).$$

Therefore by Lemma 3.3.1 we have

$$\gamma_{k+1}(\mathrm{Aut}_c(G)) \leq (\mathrm{Aut}_c(G) \cap \mathrm{Aut}^{Z_j(G)}(G))\,\mathrm{Inn}(G).$$

Now applying Lemma 3.3.4 we get that $\gamma_{k+1}(\mathrm{Aut}_c(G)) \leq Z_j(\mathrm{Aut}_c(G))\,\mathrm{Inn}(G)$. It follows that $\gamma_{j+k+1}(\mathrm{Aut}_c(G)) \leq \gamma_{j+1}(\mathrm{Inn}(G))$. This proves that $\mathrm{Out}_c(G)$ is a nilpotent group of class at most $j+k$. Also one can prove on the same lines that if $\mathrm{Out}_c(G/Z_j(G))$ is a trivial group, then $\mathrm{Out}_c(G)$ is nilpotent group of class at most j.

In the previous section we have seen that if G is a nilpotent group of class k, then $\mathrm{Aut}_c(G)$ is a nilpotent group of class $k-1$. The obvious corollary is, if G is a nilpotent group of class k, then $\mathrm{Out}_c(G)$ is nilpotent of class $k-1$. This bound on the nilpotency class of $\mathrm{Out}_c(G)$ is best possible when $k=2$. Sah remarked in his paper [65] that for the large values of k the corollary could presumably be improved. Yadav [73] and Malinowska [50] also asked in their surveys to improve this bound on the nilpotency class of $\mathrm{Out}_c(G)$. We note here that $\mathrm{Out}_c(G)$ is trivial for all the groups of order less than or equal to p^4 for any prime p [43]. Having this in mind, the following corollary is an easy consequence of Theorem 3.3.5 and improves the bound on the nilpotency class of $\mathrm{Out}_c(G)$ in some cases, e.g., p-groups of maximal class.

Corollary 3.3.6 *Let p be any prime and G be a finite p-group such that $|G/Z_j(G)| \leq p^4$. Then $\mathrm{Out}_c(G)$ is a nilpotent group of class at most j.*

Corollary 3.3.7 *Let p be any prime and G be a p-group of maximal class having order p^n, $n \geq 5$. Then the nilpotency class of $\mathrm{Out}_c(G)$ is at most $n-4$.*

Now we will investigate the nilpotency of $\mathrm{Out}_c(G)$ for an arbitrary group G when $\gamma_k(G)/\gamma_k(G) \cap Z_j(G)$ for some $j, k \in \mathbb{N}$ is cyclic and prove the following theorem.

Theorem 3.3.8 *Let G be a group such that $\gamma_k(G)/\gamma_k(G) \cap Z_j(G)$ is cyclic then $\mathrm{Out}_c(G)$ is nilpotent of class at most $j+k+1$. Moreover, if $\gamma_k(G)/\gamma_k(G) \cap Z_j(G)$ is an infinite cyclic or a finite cyclic p-group, then $\mathrm{Out}_c(G)$ is nilpotent of class at most $j+k$.*

Theorem 3.3.8 easily follows form Theorem 3.3.12 which we shall prove at the end of this section.

A subgroup H of a group G is said to be *c-closed* (in G) if any two elements of H which are conjugate in G are also conjugate in H. We now prove the following lemma.

Lemma 3.3.9 *Let G be any group. Then $\gamma_i(\mathrm{Inn}(G))$ is c-closed in $\gamma_i(\mathrm{Aut}_c(G))$ for all $i \geq 1$.*

Proof. Let $\alpha \in \gamma_i(\mathrm{Aut}_c(G))$ and $\sigma_x \in \gamma_i(\mathrm{Inn}(G))$ induced by $x \in G$. Since $\mathrm{Inn}(G)$ is normal in $\mathrm{Aut}_c(G)$, let $\alpha^{-1}\sigma_x\alpha = \sigma_y$, the inner automorphism induced by $y \in G$. Now for any arbitrary element $g \in G$, we have

$$\sigma_y(g) = (\alpha^{-1}\sigma_x\alpha)(g) = \alpha^{-1}(x^{-1}\alpha(g)x) = \alpha^{-1}(x^{-1})g\alpha^{-1}(x).$$

Since $\alpha \in \gamma_i(\mathrm{Aut}_c(G))$, by Lemma 3.2.4 there exists an element $a_x \in \gamma_i(G)$ such that $\alpha(x) = a_x^{-1}xa_x$. Let σ denote the inner automorphism of G induced by $\alpha^{-1}(a_x) \in \gamma_i(G)$. Thus $\sigma \in \gamma_i(\mathrm{Inn}(G))$ and

$$\sigma^{-1}\sigma_x\sigma(g) = \sigma^{-1}(x^{-1}\sigma(g)x) = \sigma^{-1}(x^{-1})g\sigma^{-1}(x) = \alpha^{-1}(x^{-1})g\alpha^{-1}(x) = \sigma_y(g)$$

for all $g \in G$. Hence $\alpha^{-1}\sigma_x\alpha = \sigma^{-1}\sigma_x\sigma$. This proves the lemma.

The next lemma can be proved on the lines of proof of Lemma 3.3.9.

Lemma 3.3.10 *For any group G, $[\gamma_i(\mathrm{Aut}_c(G)), \gamma_j(\mathrm{Inn}(G))] \leq \gamma_{i+j}(\mathrm{Inn}(G))$ for all $i, j \geq 1$.*

Lemma 3.3.11 *For a group G, $C_{\mathrm{Aut}_c(G)}(\mathrm{Inn}(G)) = Z(\mathrm{Aut}_c(G))$.*

Proof. Since $Z(\mathrm{Aut}_c(G)) \leq C_{\mathrm{Aut}_c(G)}(\mathrm{Inn}(G))$, it is sufficient to show that any class-preserving automorphism α of G, which centralizes $\mathrm{Inn}(G)$, lies in the center of $\mathrm{Aut}_c(G)$. Let β be an arbitrary element of $\mathrm{Aut}_c(G)$. Then for each $x \in G$, there exist a_x such that $\beta(x) = x^{a_x}$. Notice that $x^{-1}\alpha(x) \in Z(G)$. Thus it follows that $\beta\alpha(x) = \alpha(x)^{a_x}$. Let σ_{a_x} be the inner automorphism induced by a_x. Then

$$\alpha\beta(x) = \alpha\sigma_{a_x}(x) = \sigma_{a_x}\alpha(x) = \sigma_{a_x}(\alpha(x)) = \beta(\alpha(x)) = \beta\alpha(x).$$

Since x was arbitrary, $\alpha\beta = \beta\alpha$. This proves that $\alpha \in Z(\mathrm{Aut}_c(G))$.

Theorem 3.3.8 is a direct consequence of the following theorem.

Theorem 3.3.12 *Let G be a group such that $\gamma_k(G)/\gamma_k(G) \cap Z_j(G)$ is cyclic. Then $\gamma_{j+k+1}(\mathrm{Aut}_c(G)) = \gamma_{j+k+1}(\mathrm{Inn}(G))$. Moreover, if $\gamma_k(G)$ is infinte cyclic or a finite cyclic p-group for an odd prime p, then $\gamma_{j+k}(\mathrm{Aut}_c(G)) = \gamma_{j+k}(\mathrm{Inn}(G))$.*

Proof. First we will prove the theorem for $j = 0$. So let G be a group such that $\gamma_k(G)$ is cyclic for some $k \geq 1$. Suppose that $\gamma_k(G)$ is infinite cyclic. Then $\mathrm{Aut}(\gamma_k(G))$ is cyclic of order 2. But then, by 1.1.5, $N_G(\gamma_k(G))/C_G(\gamma_k(G)) = G/C_G(\gamma_k(G))$ is also cyclic, generated by (say) $xC_G(\gamma_k(G))$. Thus $G = \big\langle x, C_G(\gamma_k(G))\big\rangle$. From Lemma 3.2.4 it follows that $\gamma_k(\mathrm{Aut}_c(G)) = \gamma_k(\mathrm{Inn}(G))$ and hence by Lemma 3.3.10, $\gamma_{k+1}(\mathrm{Aut}_c(G)) = \gamma_{k+1}(\mathrm{Inn}(G))$. Now suppose that $\gamma_k(G)$ is a finite cyclic group. Since $\gamma_k(G)$ is finite, $\mathrm{Aut}(\gamma_k(G))$ is finite and therefore by Proposition 1.1.5 $G/C_G(\gamma_k(G))$ is finite. Let $G = \langle x_1, x_2, ..., x_t,\ C_G(\gamma_k(G))\rangle$ and $\alpha \in \gamma_k(\mathrm{Aut}_c(G))$. Then by Lemma 3.2.4, α fixes $C_G(\gamma_k(G))$ element-wise and since $\gamma_k(G)$ is finite there are only finite no of choices for each $x_i's$ to get mapped to, under α. It follows that $\gamma_k(\mathrm{Aut}_c(G))$ is finite. Using Lemma 3.2.4 and applying the same technique as in it's proof, it is easy to see that if $\gamma_i(G)$ is abelian for some i, then $\gamma_i(\mathrm{Aut}_c(G))$ is abelian. So we have $\gamma_k(\mathrm{Aut}_c(G))$ abelian. Also, since $\gamma_k(G)$ is cyclic, $\gamma_k(\mathrm{Inn}(G))$ is cyclic. Notice that the exponents of $\gamma_k(\mathrm{Aut}_c(G))$ and $\gamma_k(\mathrm{Inn}(G))$ are equal, because by Lemma 3.2.4 each element in $\gamma_k(\mathrm{Aut}_c(G))$ fixes $\gamma_k(G)$ elementwise. Therefore from Theorem 1.1.8, we get

$\gamma_k(\mathrm{Aut}_c(G)) = \gamma_k(\mathrm{Inn}(G)) \times T$ for some $T \leq \gamma_k(\mathrm{Aut}_c(G)$. Next we want to show that $[T, \mathrm{Inn}(G)] \leq T$. Let $\gamma_k(G) = \langle y \rangle$ and $\alpha \in \gamma_k(\mathrm{Aut}_c(G))$. Let $x, z \in G$. By Lemma 3.2.4, we can assume that $\alpha(x) = y^{-r}xy^r$ and $\alpha(z) = y^{-t}zy^t$ for some $r, t \in \mathbb{Z}$. Thus by Lemma 1.1.6, we have $y \in Z(\gamma_2(G))$. Now consider

$$\begin{aligned}
\alpha([x,z]) &= \alpha(x^{-1})\alpha(z^{-1})\alpha(x)\alpha(z) \\
&= y^{-r}x^{-1}y^r y^{-t}z^{-1}y^t y^{-r}xy^r y^{-t}zy^t \\
&= y^{-t}y^{t-r}x^{-1}y^{r-t}z^{-1}y^{t-r}xy^{r-t}zy^t \\
&= y^{-t}x^{-1}[x^{-1}, y^{r-t}]z^{-1}[y^{r-t}, x^{-1}]xzy^t \\
&= y^{-t}x^{-1}\left[[y^{r-t}, x^{-1}], z\right]z^{-1}xzy^t \\
&= y^{-t}x^{-1}\left[[y^{r-t}, x^{-1}], z\right]z^{-1}xzy^t z^{-1}x^{-1}zz^{-1}xz \\
&= y^{-t}x^{-1}z^{-1}xzy^t z^{-1}x^{-1}z\left[[y^{r-t}, x^{-1}], z\right]z^{-1}xz \\
&= y^{-t}[x,z]y^t z^{-1}x^{-1}z\left[[y^{r-t}, x^{-1}], z\right]z^{-1}xz \\
&= [x,z]z^{-1}x^{-1}z\left[[y^{r-t}, x^{-1}], z\right]z^{-1}xz \\
&= x^{-1}\left[[y^{r-t}, x^{-1}], z\right]z^{-1}xz.
\end{aligned}$$

But $\alpha \in \gamma_k(\mathrm{Aut}_c(G))$ and $y \in Z(\gamma_2(G))$, so we have $\alpha([x,z]) = [x,z]$. It follows that $[x^{-1}, y^{r-t}] \in C_G(z)$. Similarly, $[z^{-1}, y^{t-r}] \in C_G(x)$. Now, let $\beta \in \mathrm{Inn}(G)$ be induced by z. Then,

$$\begin{aligned}
\beta^{-1}\alpha\beta(x) &= \beta^{-1}\alpha(z^{-1}xz) \\
&= \beta^{-1}(\alpha(z^{-1})y^{-r}xy^r\alpha(z)) \\
&= z\alpha(z^{-1})y^{-r}xy^r\alpha(z)z^{-1} \\
&= zy^{-t}z^{-1}y^{t-r}xy^{r-t}zy^t z^{-1} \\
&= zy^{-r}z^{-1}zy^{r-t}z^{-1}y^{t-r}xy^{r-t}zy^{t-r}z^{-1}zy^r z^{-1}
\end{aligned}$$

$$
\begin{aligned}
&= zy^{-r}z^{-1}[z^{-1}, y^{t-r}]x[y^{t-r}, z^{-1}]zy^{r}z^{-1} \\
&= zy^{-r}z^{-1}xzy^{r}z^{-1}.
\end{aligned}
$$

Let $zy^{-1}z^{-1} = y^{-m}$. Then $\beta^{-1}\alpha\beta(x) = y^{-mr}xy^{mr}$. Since α fixes y, we have $\beta^{-1}\alpha\beta(x) = \alpha^{m}(x)$. Notice that m does not depend on the arbitrarily chosen x, which shows that $\beta^{-1}\alpha\beta = \alpha^{m}$. Since z was chosen arbitrarily, for all $\sigma \in \mathrm{Inn}(G)$, we get $\sigma^{-1}\alpha\sigma \in \langle\alpha\rangle$. This proves that, for any subgroup S of $\gamma_k(\mathrm{Aut}_c(G))$, $[S, \mathrm{Inn}(G)] \leq S$. In particular, $[T, \mathrm{Inn}(G)] \leq T$. Now by Lemma 3.3.10, we have $[\gamma_k(\mathrm{Aut}_c(G)), \mathrm{Inn}(G)] = \gamma_{k+1}(\mathrm{Inn}(G))$, i.e., $[\gamma_k(\mathrm{Inn}(G)) \times T, \mathrm{Inn}(G)] = \gamma_{k+1}(\mathrm{Inn}(G))$. But then, $[T, \mathrm{Inn}(G)] \leq \gamma_k(\mathrm{Inn}(G)) \cap T = \{1\}$. Thus by Lemma 3.3.11, we have $T \leq Z(\mathrm{Aut}_c(G))$. Now

$$
\begin{aligned}
\gamma_{k+1}(\mathrm{Aut}_c(G)) &= [\gamma_k(\mathrm{Aut}_c(G)), \mathrm{Aut}_c(G)] \\
&= [\gamma_k(\mathrm{Inn}(G)) \times T, \mathrm{Aut}_c(G)] \\
&= [\gamma_k(\mathrm{Inn}(G)), \mathrm{Aut}_c(G)] \\
&= \gamma_{k+1}(\mathrm{Inn}(G)).
\end{aligned}
$$

Furthermore, if $\gamma_k(G)$ is a cyclic p-group for an odd prime p, then by Proposition 1.1.4 $\mathrm{Aut}(\gamma_k(G))$ is cyclic and hence $G/C_G(\gamma_k(G))$ is cyclic. It then follows from Lemma 3.2.4, that $\gamma_k(\mathrm{Aut}_c(G)) = \gamma_k(\mathrm{Inn}(G))$. Now suppose that j is any arbitrary natural number and $\gamma_k(G)/\gamma_k(G) \cap Z_j(G)$ is cyclic. It is a basic fact that $\gamma_k(G)/\gamma_k(G) \cap Z_j(G) \cong \gamma_k(G/Z_j(G))$. Therefore, by what we just proved $\gamma_{k+1}(\mathrm{Aut}_c(G/Z_j(G))) = \gamma_{k+1}(\mathrm{Inn}(G/Z_j(G)))$. Hence By Lemma 3.3.1 we get

$$
\gamma_{k+1}(\mathrm{Aut}_c(G)) \leq (\gamma_{k+1}(\mathrm{Aut}_c(G)) \cap \mathrm{Aut}^{Z_j(G)})\gamma_{k+1}(\mathrm{Inn}(G)).
$$

Therefore By Lemma 3.3.3 we get $\gamma_{k+1}(\mathrm{Aut}_c(G)) \leq Z_j(\mathrm{Aut}_c(G))\gamma_{k+1}(\mathrm{Inn}(G))$. Now it follows that $\gamma_{j+k+1}(\mathrm{Aut}_c(G)) = \gamma_{j+k+1}(\mathrm{Inn}(G))$. Finally if $\gamma_k(G)/\gamma_k(G) \cap Z_j(G)$ is infinite cyclic or a finite cyclic p-group for an odd prime p, then $\gamma_k(\mathrm{Aut}_c(G/Z_j(G))) = \gamma_k(\mathrm{Inn}(G/Z_j(G)))$. Applying the same arguments as before we get that $\gamma_{j+k}(\mathrm{Aut}_c(G)) = \gamma_{j+k}(\mathrm{Inn}(G))$. This completes the proof.

We would like to remark here that for a finite p-group G, p an odd prime, the result of Cheng stated in Theorem 1.4.7 gives a more general statement when $j = 0$ and $k = 2$.

Chapter 4

Ш-rigidity of Groups of Order p^6

In this chapter we calculate $|\operatorname{Out}_c(G)|$ for all the groups G of order p^6 for a prime p and study the connection between Ш-rigidity and Bogomolov multiplier of these groups. Throughout the chapter, Ш-rigid groups will be called rigid groups.

4.1 Ш-rigidity and Bogomolov multiplier

Recall (Theorem 1.5.2) that a finite group G is Ш-rigid if and only if $\operatorname{Out}_c(G) = 1$. Many mathematicians have studied the Ш-rigidity of various classes of groups. Some have used the Shafarevich-Tate set approach while some have taken the route of calculating $\operatorname{Out}_c(G)$. The following list tries to collect some known classes of Ш-rigid groups.

- symmetric groups [59];
- finite simple groups [20];
- p-groups of order at most p^4 [43];
- p-groups having a cyclic maximal subgroup [43];

- p-groups having a cyclic subgroup of index p^2 [44, 22];

- finite abelian-by-cyclic groups [31];

- groups such that the Sylow p-subgroups are cyclic for odd p, and either cyclic, or dihedral, or generalized quaternion for p = 2 [32];

- Blackburn groups [30];

- extraspecial p-groups [42];

- primitive supersolvable groups [47];

- unitriangular matrix groups over $\mathbb{F}_p$ and the quotients of their lower central series [4];

- Free groups [58];

- Free product of groups [56].

Kang and Kunyavskiĭ in [41] observed that the Bogomolov multiplier $B_0(G) = 0$ for most of the known classes of finite Ш-rigid groups G and asked following question:

Question([41, Question 3.2]). Let G be a finite Ш-rigid group. Is it true that $B_0(G) = 0$?

However this question does not have a positive solution in general (negative answer for a group of order 256 is now known), Kang and Kunyavskiĭ writes that it is tempting to understand whether there exists some intrinsic relationship between Ш-rigidity and Bogomolov multiplier.

4.2 Groups of order p^6

This chapter is devoted to studying the rigidity property of groups of order p^6 for a prime p and answering the above question in affirmative for most of these groups. We study rigidity problem through class-preserving automorphisms of groups.

As we also have mentioned earlier in the first chapter that non-abelian groups of order p^6, p odd prime, are classified in 42 isoclinism families by R. James which are denoted by Φ_k for $2 \leq k \leq 43$. Theorem 1.4.8 allows us to select and work with any group from each of 42 isoclinism families of non-abelian groups of order p^6. We list here the selected group from each isoclinic family with which we shall work. The presentation $\langle \alpha_1, \alpha_2, ..., \alpha_n | \; w_1 = w_2 = \cdots = w_k = 1 \rangle$ for the group G means that G is the largest group generated by the symbols $\alpha_1, \alpha_2, \ldots \alpha_n$ subject to the conditions $w_1(\alpha_1, \alpha_2, \ldots \alpha_n) = w_2(\alpha_1, \alpha_2, \ldots \alpha_n) = \cdots = w_k(\alpha_1, \alpha_2, \ldots \alpha_n) = 1$, where $w_i's$ represent words in at most n variables. In particular, $\alpha_{i+1}^{(p)}$ will denote the word $\alpha_{i+1}^{p} \alpha_{i+2}^{\binom{p}{2}} \cdots \alpha_{i+k}^{\binom{p}{k}} \cdots \alpha_{i+p}$, where i is a positive integer and $\alpha_{i+2}, \ldots, \alpha_{i+p}$ are suitably defined. All relations of the form $[\alpha, \beta] = 1$ (with α, β generators) have been omitted from the list and should be assumed when reading the list. Throughout the list ν denotes the smallest positive integer which is a non-quadratic residue $\pmod p$ and g denotes the smallest positive integer which is a primitive root $\pmod p$.

(1) C_p.

(2) $\Phi_2(1^6) = \Phi_2(1^5) \times C_p$, where

$$\Phi_2(1^5) = \left\langle \alpha, \alpha_1, \alpha_2 \mid [\alpha_1, \alpha] = \alpha_2, \alpha^p = \alpha_1^p = \alpha_2^p = 1 \right\rangle \times C_p \times C_p.$$

(3) $\Phi_3(1^6) = \Phi_3(1^5) \times C_p,$ where

$$\Phi_3(1^5) = \left\langle \alpha, \alpha_1, \alpha_2, \alpha_3 \mid [\alpha_i, \alpha] = \alpha_{i+1}, \alpha^p = \alpha_i^{(p)} = \alpha_3^p = 1 \ (i = 1, 2) \right\rangle \times C_p.$$

(4) $\Phi_4(1^6) = \Phi_4(1^5) \times C_p,$ where

$$\Phi_4(1^5) = \left\langle \alpha, \alpha_1, \alpha_2, \beta_1, \beta_2 \mid [\alpha_i, \alpha] = \beta_i, \alpha^p = \alpha_i^p = \beta_i^p = 1 \ (i = 1, 2) \right\rangle.$$

(5) $\Phi_5(1^6) = \Phi_5(1^5) \times C_p,$ where

$$\Phi_5(1^5) = \left\langle \alpha_1, \alpha_2, \alpha_3, \alpha_4, \beta \mid [\alpha_1, \alpha_2] = [\alpha_3, \alpha_4] = \beta, \alpha_i^p = \beta^p = 1 \ (i = 1, 2, 3, 4) \right\rangle.$$

(6) $\Phi_6(2211) = \Phi_6(221)a \times C_p,$ where

$$\begin{aligned} \Phi_6(221)a = \Big\langle \alpha_1, \alpha_2, \beta, \beta_1, \beta_2 \mid [\alpha_1, \alpha_2] = \beta, [\beta, \alpha_i] = \beta_i, \ \alpha_i^p = \beta^p \\ = \beta_i^p = 1 \ (i = 1, 2) \Big\rangle. \end{aligned}$$

(7) $\Phi_7(1^6) = \Phi_7(1^5) \times C_p,$ where

$$\Phi_7(1^5) = \Big\langle \alpha, \alpha_1, \alpha_2, \alpha_3, \beta \mid [\alpha_i, \alpha] = \alpha_{i+1}, [\alpha_1, \beta] = \alpha_3, \alpha^p = \alpha_1^{(p)} = \beta^p = \alpha_{i+1}^p = 1 \ (i = 1, 2) \Big\rangle.$$

(8) $\Phi_8(321)a = \Phi_8(32) \times C_p$, where

$$\Phi_8(32) = \Big\langle \alpha_1, \alpha_2, \beta \mid [\alpha_1, \alpha_2] = \beta = \alpha_1^p, \beta^{p^2} = \alpha_2^{p^2} = 1 \Big\rangle.$$

(9) $\Phi_9(1^6) = \Phi_9(1^5) \times C_p$, where

$$\Phi_9(1^5) = \Big\langle \alpha, \alpha_1, ..., \alpha_4 \mid [\alpha_i, \alpha] = \alpha_{i+1}, \quad \alpha^p = \alpha_1^{(p)} = \alpha_{i+1}^{(p)} = 1 \ (i = 1, 2, 3) \Big\rangle.$$

(10) $\Phi_{10}(1^6) = \Phi_{10}(1^5) \times C_p$, where

$$\Phi_{10}(1^5) = \Big\langle \alpha, \alpha_1, ..., \alpha_4 \mid [\alpha_i, \alpha] = \alpha_{i+1}, [\alpha_1, \alpha_2] = \alpha_4, \alpha^p = \alpha_1^{(p)} = \alpha_{i+1}^{(p)} = 1 \ (i = 1, 2, 3) \Big\rangle.$$

(11) $$\Phi_{11}(1^6) = \Big\langle \alpha_1, \beta_1, ..., \alpha_3, \beta_3 \mid [\alpha_1, \alpha_2] = \beta_3, [\alpha_2, \alpha_3] = \beta_1, [\alpha_3, \alpha_1] = \beta_2, \alpha_i^p = \beta_i^p = 1 \ (i = 1, 2, 3) \Big\rangle.$$

(12) $\Phi_{12}(1^6) = \Phi_2(111) \times \Phi_2(111)$, where

$$\Phi_2(111) = \Big\langle \alpha, \alpha_1, \alpha_2 \mid [\alpha_1, \alpha] = \alpha_2, \alpha^p = \alpha_1^p = \alpha_2^p = 1 \Big\rangle.$$

(13) $$\Phi_{13}(1^6) = \Big\langle \alpha_1, ..., \alpha_4, \beta_1, \beta_2 \mid [\alpha_1, \alpha_{i+1}] = \beta_i, [\alpha_2, \alpha_4] = \beta_2, \\ \alpha_i^p = \alpha_3^p = \alpha_4^p = \beta_i^p = 1 \ (i = 1, 2) \Big\rangle.$$

(14) $$\Phi_{14}(222) = \Big\langle \alpha_1, \alpha_2, \beta \mid [\alpha_1, \alpha_2] = \beta, \alpha_1^{p^2} = \alpha_2^{p^2} = \beta^{p^2} = 1 \Big\rangle.$$

(15) $$\Phi_{15}(1^6) = \Big\langle \alpha_1, ..., \alpha_4, \beta_1, \beta_2 \mid [\alpha_1, \alpha_{i+1}] = \beta_i, [\alpha_3, \alpha_4] = \beta_1, [\alpha_2, \alpha_4] = \beta_2^g, \\ \alpha_i^p = \alpha_3^p = \alpha_4^p = \beta_i^p = 1 \ (i = 1, 2) \Big\rangle.$$

(16) $$\Phi_{17}(1^6) = \Big\langle \alpha, \alpha_1, \alpha_2, \alpha_3, \beta, \gamma \mid [\alpha_i, \alpha] = \alpha_{i+1}, [\beta, \alpha] = \gamma, \\ \alpha^p = \alpha_1^{(p)} = \beta^p = \alpha_{i+1}^p = \gamma^p = 1 \ (i = 1, 2) \Big\rangle.$$

(17) $$\Phi_{17}(1^6) = \Big\langle \alpha, \alpha_1, \alpha_2, \alpha_3, \beta, \gamma \mid [\alpha_i, \alpha] = \alpha_{i+1}, [\beta, \alpha_1] = \gamma, \\ \alpha^p = \alpha_1^p = \beta^p = \alpha_{i+1}^p = \gamma^p = 1 \ (i = 1, 2) \Big\rangle.$$

(18) $$\Phi_{18}(1^6) = \Big\langle \alpha, \alpha_1, \alpha_2, \alpha_3, \beta, \gamma \mid [\alpha_i, \alpha] = \alpha_{i+1}, [\alpha_1, \beta] = \alpha_3, [\alpha, \beta] = \gamma, \\ \alpha^p = \alpha_1^{(p)} = \beta^p = \alpha_{i+1}^p = \gamma^p = 1 \ (i = 1, 2) \Big\rangle.$$

$$(19)\quad \Phi_{19}(1^6) = \Big\langle \alpha, \alpha_1, \alpha_2, \beta, \beta_1, \beta_2 \mid [\alpha_1, \alpha_2] = \beta, [\beta, \alpha_i] = \beta_i, [\alpha, \alpha_1] = \beta_1,$$
$$\alpha^p = \alpha_i^p = \beta^p = \beta_i^p = 1 \ (i = 1, 2) \Big\rangle.$$

Note : In the following presentation of the group $\Phi_{20}(1^6)$ we have $\alpha_2^{(p)} = \alpha_2^p \beta_1^{-\binom{p}{3}}$.

$$(20)\quad \Phi_{20}(1^6) = \Big\langle \alpha, \alpha_1, \alpha_2, \beta, \beta_1, \beta_2 \mid [\alpha_1, \alpha_2] = \beta, [\beta, \alpha_i] = \beta_i, [\alpha, \alpha_1] = \beta_2,$$
$$\alpha^p = \alpha_1^p = \alpha_2^{(p)} = \beta^p = \beta_i^p = 1 \ (i = 1, 2) \Big\rangle.$$

Note : In the following presentation of the group $\Phi_{21}(1^6)$ we have $\alpha_1^{(p)} = \alpha_1^p \beta_2^{-\binom{p}{3}}$ and $\alpha_2^{(p)} = \alpha_2^p \beta_1^{\binom{p}{3}}$.

$$(21)\quad \Phi_{21}(1^6) = \Big\langle \alpha, \alpha_1, \alpha_2, \beta, \beta_1, \beta_2 \mid [\alpha_1, \alpha_2] = \beta, [\beta, \alpha_i] = \beta_i, [\alpha, \alpha_1] = \beta_2,$$
$$[\alpha, \alpha_2] = \beta_1^\nu, \alpha^p = \alpha_i^{(p)} = \beta^p = \beta_i^p = 1 \ (i = 1, 2) \Big\rangle.$$

$$(22)\quad \Phi_{22}(1^6) = \Big\langle \alpha, \alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2 \mid [\alpha_i, \alpha] = \alpha_{i+1}, [\beta_1, \beta_2] = \alpha_3,$$
$$\alpha^p = \alpha_1^{(p)} = \beta_i^p = \alpha_{i+1}^p = 1 \ (i = 1, 2) \Big\rangle.$$

$$(23)\quad \Phi_{23}(1^6) = \Big\langle \alpha, \alpha_1, \alpha_2, \alpha_3, \alpha_4, \gamma \mid [\alpha_i, \alpha] = \alpha_{i+1}, [\alpha_1, \alpha_2] = \gamma,$$
$$\alpha^p = \alpha_1^{(p)} = \alpha_{i+1}^p = \gamma^p = 1 \ (i = 1, 2, 3) \Big\rangle.$$

$$(24)\quad \Phi_{24}(1^6) = \Big\langle \alpha, \alpha_1, \alpha_2, \alpha_3, \alpha_4, \beta \mid [\alpha_i, \alpha] = \alpha_{i+1}, [\alpha_1, \beta] = \alpha_4,$$
$$\alpha^p = \alpha_1^{(p)} = \beta^p = \alpha_{i+1}^p = 1 \ (i = 1, 2, 3) \Big\rangle.$$

(25) and (26) $\Phi_{25+x}(222) = \Big\langle \alpha, \alpha_1, \alpha_2, \alpha_3, \alpha_4 \mid [\alpha_i, \alpha] = \alpha_{i+1}, [\alpha_3, \alpha] = \alpha_4,$

$$\alpha_i^{(p)} = \alpha_{i+2}^{y}, \alpha^{p^2} = \alpha_{i+2}^{p} = 1 \ (i = 1, 2) \Big\rangle,$$

where $y = \nu^x$ and $x = 0$ (for Φ_{25}) or $x = 1$ (for Φ_{26}).

(27) $\Phi_{27}(1^6) = \Big\langle \alpha, \alpha_1, \alpha_2, \alpha_3, \alpha_4, \beta \mid [\alpha_i, \alpha] = \alpha_{i+1}, [\alpha_1, \beta] = [\alpha_1, \alpha_2] = \alpha_4,$

$$\alpha^p = \alpha_1^{(p)} = \beta^p = \alpha_{i+1}^{(p)} = 1 \ (i = 1, 2, 3) \Big\rangle.$$

(28) and (29) $\Phi_{28+x}(222) = \Big\langle \alpha, \alpha_1, \alpha_2, \alpha_3, \alpha_4 \mid [\alpha_i, \alpha] = \alpha_{i+1}, [\alpha_3, \alpha] = [\alpha_1, \alpha_2]$

$$= \alpha_4, \alpha_i^{(p)} = \alpha_{i+2}^{y}, \alpha^{p^2} = \alpha_{i+2}^{p} = 1 \ (i = 1, 2) \Big\rangle,$$

where $y = \nu^x$ and $x = 0$ (for Φ_{28}) or $x = 1$ (for Φ_{29}).

(30) $\Phi_{30}(1^6) = \Big\langle \alpha, \alpha_1, \alpha_2, \alpha_3, \alpha_4, \beta \mid [\alpha_i, \alpha] = \alpha_{i+1}, [\alpha_i, \beta] = \alpha_{i+2}, [\alpha_3, \alpha] = \alpha_4,$

$$\alpha^p = \alpha_i^{(p)} = \beta^p = \alpha_{i+2}^{p} = 1 \ (i = 1, 2) \Big\rangle.$$

(31) and (32) $\Phi_{31+x}(1^6) = \Big\langle \alpha, \alpha_1, \alpha_2, \beta_1, \beta_2, \gamma \mid [\alpha_i, \alpha] = \beta_i, [\alpha_1, \beta_1] = \gamma,$

$$[\alpha_2, \beta_2] = \gamma^y, \alpha^p = \alpha_i^p = \beta^p = \gamma^p = 1 \ (i = 1, 2) \Big\rangle,$$

where $y = \nu^x$ and $x = 0$ (for Φ_{31}) or $x = 1$ (for Φ_{32}).

Note : In the following presentation of the group $\Phi_{33}(1^6)$ we have $\alpha_2^{(p)} =$

$\alpha_2^p\gamma_1^{\binom{p}{3}}$.

$$(33)\quad \Phi_{33}(1^6) = \Big\langle \alpha, \alpha_1, \alpha_2, \beta_1, \beta_2, \gamma \mid [\alpha_i, \alpha] = \beta_i, [\beta_2, \alpha] = [\alpha_1, \beta_1] = \gamma, \\ \alpha^p = \alpha_1^p = \alpha_2^{(p)} = \beta_i^p = \gamma^p = 1 \ (i = 1, 2)\Big\rangle.$$

$$(34)\quad \Phi_{34}(321)a = \Big\langle \alpha, \alpha_1, \alpha_2, \beta_1, \beta_2, \gamma \mid [\alpha_i, \alpha] = \beta_i \ (i = 1, 2), [\beta_2, \alpha] = [\alpha_1, \beta_1] \\ = \beta_1^p = \gamma, \alpha^p = \beta_1, \alpha_1^p = \beta_2, \alpha_2^p = \beta_2^p = \gamma^p = 1\Big\rangle.$$

$$(35)\quad \Phi_{35}(1^6) = \Big\langle \alpha, \alpha_1, ..., \alpha_5 \mid [\alpha_i, \alpha] = \alpha_{i+1}, \alpha^p = \alpha_1^{(p)} = \alpha_{i+1}^{(p)} = 1 \\ (i = 1, 2, 3, 4)\Big\rangle.$$

$$(36)\quad \Phi_{36}(1^6) = \Big\langle \alpha, \alpha_1, ..., \alpha_5 \mid [\alpha_i, \alpha] = \alpha_{i+1}, [\alpha_1, \alpha_2] = \alpha_5, \\ \alpha^p = \alpha_1^{(p)} = \alpha_{i+1}^{(p)} = 1 \ (i = 1, 2, 3, 4)\Big\rangle.$$

Note: The following three families (37), (38) and (39) does not exist for $p = 3$.

$$(37)\quad \Phi_{37}(1^6) = \Big\langle \alpha, \alpha_1, ..., \alpha_5 \mid [\alpha_i, \alpha] = \alpha_{i+1}, [\alpha_2, \alpha_3] = [\alpha_3, \alpha_1] = [\alpha_4, \alpha_1] = \alpha_5, \\ \alpha^p = \alpha_1^p = \alpha_{i+1}^p = \alpha_5^p = 1 \ (i = 1, 2, 3)\Big\rangle.$$

$$(38)\quad \Phi_{38}(1^6) = \Big\langle \alpha, \alpha_1, ..., \alpha_5 \mid [\alpha_i, \alpha] = \alpha_{i+1}, [\alpha_1, \alpha_2] = \alpha_4\alpha_5^{-1}, [\alpha_1, \alpha_3] = \alpha_5, \\ \alpha^p = \alpha_1^{(p)} = \alpha_{i+1}^{(p)} = 1 \ (i = 1, 2, 3, 4)\Big\rangle.$$

(39) $\Phi_{39}(1^6) = \Big\langle \alpha, \alpha_1, ..., \alpha_5 \mid [\alpha_i, \alpha] = \alpha_{i+1}, [\alpha_1, \alpha_2] = \alpha_4, [\alpha_2, \alpha_3] = [\alpha_3, \alpha_1] =$

$$[\alpha_4, \alpha_1] = \alpha_5, \alpha^p = \alpha_1^p = \alpha_{i+1}^p = \alpha_5^p = 1 \ (i = 1, 2, 3)\Big\rangle.$$

(40) $\Phi_{40}(1^6) = \Big\langle \alpha_1, \alpha_2, \beta, \beta_1, \beta_2, \gamma \mid [\alpha_1, \alpha_2] = \beta, [\beta, \alpha_i] = \beta_i, [\beta_1, \alpha_2] =$

$$[\beta_2, \alpha_1] = \gamma, \alpha_i^p = \beta^p = \beta_i^p = \gamma^p = 1 \ (i = 1, 2)\Big\rangle.$$

(41) $\Phi_{41}(1^6) = \Big\langle \alpha_1, \alpha_2, \beta, \beta_1, \beta_2, \gamma \mid [\alpha_1, \alpha_2] = \beta, [\beta, \alpha_i] = \beta_i, [\alpha_1, \beta_1]^{-\nu} =$

$$[\alpha_2, \beta_2] = \gamma^{-\nu}, \alpha_i^p = \beta^p = \beta_i^p = \gamma^p = 1 \ (i = 1, 2)\Big\rangle.$$

(42) $\Phi_{42}(222)a_0 = \Big\langle \alpha_1, \alpha_2, \beta, \beta_1, \beta_2, \gamma \mid [\alpha_1, \alpha_2] = \beta, [\beta, \alpha_i] = \beta_i, [\alpha_1, \beta_2] =$

$$[\alpha_2, \beta_1] = \beta^p = \gamma, \alpha_1^p = \beta_1^{-1}\gamma^{-1/2},$$

$$\alpha_2^p = \beta_2\gamma^{1/2}, \beta_i^p = \gamma^p = 1 \ (i = 1, 2)\Big\rangle.$$

(43) $\Phi_{43}(222)a_0 = \Big\langle \alpha_1, \alpha_2, \beta, \beta_1, \beta_2, \gamma \mid [\alpha_1, \alpha_2] = \beta, [\beta, \alpha_i] = \beta_i, [\alpha_1, \beta_1]^{-\nu} =$

$$[\alpha_2, \beta_2] = \gamma^{-\nu}, \alpha_1^p = \beta_2\gamma^k,$$

$$\alpha_2^p = \beta_1\nu\gamma^l, \beta^p = \gamma^n, \beta_i^p = \gamma^p = 1 \ (i = 1, 2)\Big\rangle,$$

where $n = \nu + \binom{p}{3}$, and k, l are the smallest positive integers satisfying $(k-\nu)^2 - \nu(l+\nu)^2 \equiv 0 \pmod p$.

4.3 Groups G with trivial $\mathrm{Out}_c(G)$

In this section, we list those groups G for which $\mathrm{Out}_c(G)$ is trivial. We begin with the following lemma.

Lemma 4.3.1 *Let G be a purely non-abelian p-group, minimally generated by $\alpha_1, \alpha_2, ..., \alpha_t$. Suppose that $G/\gamma_2(G)$ is elementary abelian. If $\beta_i \in \Omega_1(Z(G))$ for $i = 1, ..., t$, then the map $\delta : \{\alpha_1, \alpha_2, ..., \alpha_t\} \to G$, defined as $\delta(\alpha_i) = \alpha_i\beta_i$, extends to a central automorphism of G.*

Proof. Note that the map $f_\delta : \{\alpha_i\gamma_2(G) | \; i = 1, ..., t\} \to \Omega_1(Z(G))$ defined as $\alpha_i\gamma_2(G) \to \beta_i$ for $i = 1, ..., t$, extends to a homomorphism from $G/\gamma_2(G)$ to $Z(G)$ because $G/\gamma_2(G)$ is elementary abelian. Now it follows from the proof of Theorem 1.2.5 that the map $g \to gf_\delta(g)$ for all $g \in G$ is a central automorphism of G. This proves the lemma.

Let G be a group minimally generated by $\alpha_1, \alpha_2, ..., \alpha_t$. Then note that any element of G can be written as $\eta\alpha_1^{k_1}\alpha_2^{k_2}...\alpha_t^{k_t}$ for some $\eta \in \gamma_2(G)$ and some $k_1, k_2, ..., k_t \in \mathbb{Z}$. Also note that any conjugate of an α_i can be written as $\alpha_i[\alpha_i, \eta\alpha_1^{k_1}\alpha_2^{k_2}...\alpha_t^{k_t}]$ for some $\eta \in \gamma_2(G)$ and some $k_1, k_2, ..., k_t \in \mathbb{Z}$. It follows that, an automorphism δ of G is class-preserving if and only if for every $k_1, k_2, ..., k_t \in \mathbb{Z}$ and for all $\eta_1 \in \gamma_2(G)$, there exist $l_1, l_2, ..., l_t \in \mathbb{Z}$ and $\eta_2 \in \gamma_2(G)$ (depending on $k_1, k_2, ..., k_t$ and η_1) such that

$$\left[\eta_1 \prod_{i=1}^{t} \alpha_i^{k_i}, \;\; \eta_2 \prod_{i=1}^{t} \alpha_i^{l_i}\right] = \left(\eta_1 \prod_{i=1}^{t} \alpha_i^{k_i}\right)^{-1} \delta\left(\eta_1 \prod_{i=1}^{t} \alpha_i^{k_i}\right).$$

We shall be using these facts and Lemma 1.1.1 very frequently in the proofs, without any further reference.

Lemma 4.3.2 *Let G be the group $\Phi_{11}(1^6)$. Then* $\mathrm{Out}_c(G) = 1$.

Proof. The group G is a special p-group, minimally generated by α_1, α_2 and α_3. The commutator subgroup $\gamma_2(G)$ is generated by $\beta_1 := [\alpha_2, \alpha_3], \beta_2 := [\alpha_3, \alpha_1], \beta_3 := [\alpha_1, \alpha_2]$. The conjugates of α_1, α_2 and α_3 are $\alpha_1\beta_3^t\beta_2^s$, $\alpha_2\beta_3^t\beta_1^r$ and $\alpha_3\beta_2^s\beta_1^r$ respectively, where r, s and t vary over Z. Since the exponent of $\gamma_2(G)$ is p, it follows that $|\alpha_i^G| = p^2$ for $i = 1, 2, 3$. Therefore by Lemma 1.4.3, $|\operatorname{Aut}_c(G)| \leq p^6$. Define a map $\delta : \{\alpha_1, \alpha_2, \alpha_3\} \to G$ such that $\alpha_1 \mapsto \alpha_1\beta_3^{t_1}\beta_2^{s_1}, \alpha_2 \mapsto \alpha_2\beta_3^{t_2}\beta_1^{r_2}$ and $\alpha_3 \mapsto \alpha_3\beta_2^{s_3}\beta_1^{r_3}$, for some $s_1, t_1, r_2, t_2, r_3, s_3 \in \mathbb{Z}$. By Lemma 4.3.1, this map extends to a central automorphism of G. Since δ fixes $\gamma_2(G)$ element-wise, for $k_1, l_1, m_1 \in \mathbb{Z}$ and $\eta \in \gamma_2(G)$,

$$\delta(\eta\alpha_1^{k_1}\alpha_2^{l_1}\alpha_3^{m_1}) = \eta\alpha_1^{k_1}\alpha_2^{l_1}\alpha_3^{m_1}\beta_1^{l_1r_2+m_1r_3}\beta_2^{k_1s_1+m_1s_3}\beta_3^{k_1t_1+l_1t_2}.$$

Therefore δ extends to a class-preserving automorphism if and only if for every $k_1, l_1, m_1 \in \mathbb{Z}$, and $\eta_1 \in \gamma_2(G)$ there exist k_2, l_2, m_2 (depending on k_1, l_1, m_1) and $\eta_2 \in \gamma_2(G)$ such that

$$[\eta_1\alpha_1^{k_1}\alpha_2^{l_1}\alpha_3^{m_1}, \eta_2\alpha_1^{k_2}\alpha_2^{l_2}\alpha_3^{m_2}] = \beta_1^{l_1r_2+m_1r_3}\beta_2^{k_1s_1+m_1s_3}\beta_3^{k_1t_1+l_1t_2}.$$

Expanding the left hand side, we get

$$\beta_1^{l_1m_2-l_2m_1}\beta_2^{k_2m_1-k_1m_2}\beta_3^{k_1l_2-k_2l_1} = \beta_1^{l_1r_2+m_1r_3}\beta_2^{k_1s_1+m_1s_3}\beta_3^{k_1t_1+l_1t_2}.$$

Comparing the powers of β_i's, we have that, δ extends to a class-preserving automorphism if and only if the following equations hold true:

$$l_1m_2 - l_2m_1 \equiv l_1r_2 + m_1r_3 \pmod{p}$$

$$k_2m_1 - k_1m_2 \equiv k_1s_1 + m_1s_3 \pmod{p}$$

$$k_1 l_2 - k_2 l_1 \equiv k_1 t_1 + l_1 t_2 \pmod p.$$

Let δ be a class-preserving automorphism. Choose $k_1 = 0$ and m_1, l_1 to be non-zero modulo p. Then $k_2 m_1 \equiv m_1 s_3 \pmod p$ and $-k_2 l_1 \equiv l_1 t_2 \pmod p$. It follows that $t_2 \equiv -s_3 \pmod p$. Similarly if we choose l_1 to be zero and k_1, m_1 to be non-zero modulo p, then $r_3 \equiv -t_1 \pmod p$, and if m_1 to be zero and l_1, k_1 to be non-zero modulo p, then $r_2 \equiv -s_1 \pmod p$. It follows that $|\operatorname{Aut}_c(G)| \leq p^3 = |\operatorname{Inn}(G)|$. Therefore $\operatorname{Out}_c(G) = 1$.

Lemma 4.3.3 *Let G be the group $\Phi_{17}(1^6)$. Then* $\operatorname{Out}_c(G) = 1$.

Proof. The group G is a class 3 p-group, minimally generated by α, α_1 and β. The commutator subgroup $\gamma_2(G)$ is abelian and generated by $\alpha_2 := [\alpha_1, \alpha], \alpha_3 := [\alpha_2, \alpha]$ and $\gamma := [\beta, \alpha_1]$. The center $Z(G)$ is of order p^2, generated by α_3 and γ. It is easy to see that $|\alpha_1^G| \leq p^2, |\alpha^G| \leq p^2$ and $|\beta^G| = p$. Therefore, applying Lemma 1.4.3, we have $|\operatorname{Aut}_c(G)| \leq p^5$. Define a map $\delta : \{\alpha, \alpha_1, \beta\} \to G$ such that $\alpha \mapsto \alpha, \alpha_1 \mapsto \alpha_1$ and $\beta \mapsto \alpha_1^{-1}\beta\alpha_1 = \beta\gamma$. Suppose that $|\operatorname{Aut}_c(G)| = p^5$. Then δ must extend to a class-preserving automorphism of G. Hence there exist elements $\eta_1 (= \alpha_2^{r_1}\alpha_3^{s_1}\gamma^{t_1}$ say$) \in \gamma_2(G)$ and $k_1, l_1, m_1 \in \mathbb{Z}$ such that $[\alpha\beta,\ \eta_1\alpha^{k_1}\alpha_1^{l_1}\beta^{m_1}] = \gamma$. It is a routine calculation to show that

$$[\alpha\beta, \eta_1\alpha^{k_1}\alpha_1^{l_1}\beta^{m_1}] = \alpha_2^{-l_1}\alpha_3^{-r_1}\gamma^{l_1},$$

which can not be equal to γ for any value of l_1 and r_1. Therefore δ is not a class-preserving automorphism, and hence $|\operatorname{Aut}_c(G)| \leq p^4$. But $|\operatorname{Inn}(G)| = p^4$, so we have $\operatorname{Aut}_c(G) = \operatorname{Inn}(G)$.

Lemma 4.3.4 *Let G be the group $\Phi_{19}(1^6)$. Then* $\operatorname{Out}_c(G) = 1$.

Proof. The group G is a class 3 p-group, minimally generated by α, α_1 and α_2. Note that the commutator subgroup $\gamma_2(G)$ is abelian and generated by $\beta := [\alpha_1, \alpha_2], \beta_1 := [\beta, \alpha_1]$ and $\beta_2 := [\beta, \alpha_2]$. The center $Z(G)$ is of order p^2, generated by β_1 and β_2. It is easy to see that $|\alpha_1^G| \leq p^2, |\alpha_2^G| \leq p^2$ and $|\alpha^G| = p$. Therefore $|\operatorname{Aut}_c(G)| \leq p^5$. Define a map $\delta : \{\alpha, \alpha_1, \alpha_2\} \to G$ such that $\alpha \mapsto \alpha_1^{-1}\alpha\alpha_1 = \alpha\beta_1, \alpha_1 \mapsto \alpha_1$ and $\alpha_2 \mapsto \alpha_2$. Suppose that $|\operatorname{Aut}_c(G)| = p^5$. Then δ must extend to a class-preserving automorphism of G. Hence there exist elements $\eta_1 (= \beta^{r_1}\beta_1^{s_1}\beta_2^{t_1}$ say) $\in \gamma_2(G)$ and $k_1, l_1, m_1 \in \mathbb{Z}$ such that $[\alpha_2\alpha,\ \eta_1\alpha^{k_1}\alpha_1^{l_1}\alpha_2^{m_1}] = \beta_1$. It is a routine calculation that

$$[\alpha_2\alpha,\ \eta_1\alpha^{k_1}\alpha_1^{l_1}\alpha_2^{m_1}] = \beta_2^{-l_1m_1-r_1}\beta^{-l_1}\beta_1^{l_1-l_1(l_1-1)/2},$$

which can not be equal to β_1 for any value of l_1, m_1 and r_1. Therefore δ does not extend to a class-preserving automorphism, and hence $|\operatorname{Aut}_c(G)| \leq p^4$. But $|\operatorname{Inn}(G)| = p^4$, therefore $\operatorname{Aut}_c(G) = \operatorname{Inn}(G)$.

Lemma 4.3.5 *Let G be the group $\Phi_{23}(1^6)$. Then* $\operatorname{Out}_c(G) = 1$.

Proof. The group G is a class 4 p-group, minimally generated by α, α_1. The commutator subgroup $\gamma_2(G)$ is abelian and generated by $\alpha_{i+1} := [\alpha_i, \alpha]$ for $1 \leq i \leq 3$ and $\gamma := [\alpha_1, \alpha_2]$. The center $Z(G)$ is of order p^2, generated by α_4 and γ. It is easy to check that $|\alpha^G| \leq p^3$ and $|\alpha_1^G| \leq p^2$. Therefore $|\operatorname{Aut}_c(G| \leq p^5$. Let $H = \langle \alpha_4 \rangle$. Since $\alpha_4 \in Z(G), H$ is normal. Consider the quotient group G/H. One can check that the group G/H belongs to the family Φ_6. Therefore it follows from Theorem 1.4.9 that $\operatorname{Aut}_c(G/H) = \operatorname{Inn}(G/H)$. Now define a map $\delta : \{\alpha, \alpha_1\} \to G$, such that $\delta(\alpha) = \alpha$ and $\delta(\alpha_1) = \alpha_2^{-1}\alpha_1\alpha_2 = \alpha_1\gamma$. Suppose that $|\operatorname{Aut}_c(G)| = p^5$. Then δ must extend to a class-preserving automorphism of G. Then it also induces a non-trivial class-preserving automorphism (say $\bar{\delta}$) of G/H.

But then $\bar{\delta}$ is an inner automorphism of G/H because $\mathrm{Aut}_c(G/H) = \mathrm{Inn}(G/H)$. Now note that $\bar{\delta}$ is also a central automorphism of G/H. It follows that it is induced by some element in $Z_2(G/H) = \langle \alpha_2 H, Z(G/H)\rangle$. Let $\bar{\delta}$ be induced by $\alpha_2^t H$ for some $t \in \mathbb{Z}$. Hence

$$\bar{\delta}(\alpha H) = (\alpha_2^t H)^{-1}\alpha H(\alpha_2^t H) = \alpha\alpha_3^{-t}H.$$

This must be equal to αH. But then $t = 0 \pmod p$ and hence $\bar{\delta}(\alpha_1 H) = \alpha_1 H$, a contradiction. Therefore we have $|\mathrm{Aut}_c(G)| \leq p^4$. But $|\mathrm{Inn}(G)| = p^4$, hence $\mathrm{Out}_c(G) = 1$.

Lemma 4.3.6 *Let G be the group $\Phi_{27}(1^6)$. Then* $\mathrm{Out}_c(G) = 1$.

Proof. The group G is a class 4 p-group, minimally generated by α, α_1, β. The commutator subgroup $\gamma_2(G)$ is abelian and generated by $\alpha_{i+1} := [\alpha_i, \alpha]$ for $1 \leq i \leq 2$ and $\alpha_4 := [\alpha_3, \alpha] = [\alpha_1, \beta] = [\alpha_1, \alpha_2]$. The center $Z(G)$ is of order p, generated by α_4. It is easy to check that $|\alpha^G| \leq p^3, |\alpha_1^G| \leq p^2$ and $|\beta^G| = p$. Therefore $|\mathrm{Aut}_c(G)| \leq p^6$. Define $\delta : \{\alpha, \alpha_1, \beta\} \to G$ such that $\delta(\alpha) = \alpha, \delta(\alpha_1) = \alpha_1$ and $\delta(\beta) = \alpha_1\beta\alpha_1^{-1} = \beta\alpha_4$. Suppose $|\mathrm{Aut}_c(G)| = p^6$. Then δ extends to a class-preserving automorphism of G. Also note that δ fixes α_2, therefore $\delta(\alpha_2\beta^{-1}) = \alpha_2\beta^{-1}\alpha_4^{-1}$. Since δ is a class-preserving automorphism, there exist some $g \in G$ such that $[\alpha_2\beta^{-1}, g] = \alpha_4^{-1}$. Note that $C_G(\alpha_2\beta^{-1}) = \langle \alpha_1, \alpha_2, \alpha_3, \alpha_4, \beta\rangle$. Therefore without loss of generality we can assume that $g = \alpha^{k_1}$. It can be calculated that

$$[\alpha_2\beta^{-1}, \alpha^{k_1}] = \alpha_3^{k_1}\alpha_4^{k_1(k_1-1)/2},$$

which, for any value of k_1, can never be equal to α_4^{-1}. Hence, we get a contradiction. Therefore $|\operatorname{Aut}_c(G)| \leq p^5$. But $|\operatorname{Inn}(G) = p^5$, therefore $\operatorname{Out}_c(G) = 1$.

Lemma 4.3.7 *Let* $G \in \{\Phi_{28}(222), \Phi_{29}(222)\}$. *Then* $\operatorname{Out}_c(G) = 1$.

Proof. The group G is a class 4 p-group, minimally generated by α and α_1. The commutator subgroup $\gamma_2(G)$ is abelian and generated by $\alpha_{i+1} := [\alpha_i, \alpha]$ for $1 \leq i \leq 2$ and $\alpha_4 := [\alpha_3, \alpha] = [\alpha_1, \alpha_2]$. The center $Z(G)$ is of order p, generated by α_4. Note that $\langle \alpha, \alpha_4 \rangle \leq C_G(\alpha)$ and hence $|C_G(\alpha)| \geq p^3$, therefore $|\alpha^G| \leq p^3$. Now note that, since $\alpha_2^{(p)} = \alpha_4^y$, we have for $p = 3, \alpha_2^p = \alpha_4^{y-1}$, and for $p > 3, \alpha_2^p = \alpha_4^y$. Following is a routine calculation.

$$[\alpha_1, \alpha^p] = \alpha_2^p \alpha_3^{p(p-1)/2} \alpha_4^{\sum_{n=1}^{p-2} n(n-1)/2} = \alpha_2^p \alpha_4^{(p-2)(p-1)p/3},$$

which, for $p = 3$, equals α_4^{y+1}, and for $p > 3$, equals α_4^y. But we have $[\alpha_1, \alpha_2^t] = \alpha_4^t$, therefore $\alpha_2^{y+1}\alpha^{-p} \in C_G(\alpha_1)$ for $p = 3$ and $\alpha_2^y \alpha^{-p} \in C_G(\alpha_1)$ for $p > 3$. Now it is easy to see that $|C_G(\alpha_1)| \geq p^4$. Hence $|\alpha_1^G| \leq p^2$. It follows from Lemma 1.4.3 that $|\operatorname{Aut}_c(G)| \leq p^5$. But $|G/Z(G)| = p^5$, therefore $\operatorname{Aut}_c(G) = \operatorname{Inn}(G)$.

Lemma 4.3.8 *Let* $G \in \{\Phi_k(1^6),\ \Phi_{34}(321)a \mid k = 31, ..., 33\}$. *Then* $\operatorname{Out}_c(G) = 1$.

Proof. The group G is a class 3 p-group, minimally generated by α, α_1 and α_2. The commutator subgroup $\gamma_2(G)$ is abelian and generated by $\beta_i := [\alpha_i, \alpha]$ for $i = 1, 2$ and $\gamma := [\alpha_1, \beta_1]$. Also for $k = 31, 32$, $[\alpha_2, \beta_2] = \gamma^y$ and for $k = 33$ and the group $\Phi_{34}(321)a$, $\gamma = [\beta_2, \alpha]$. The center $Z(G)$ is of order p, generated by γ. It is easy to see that, if $G \in \{\Phi_k(1^6) \mid k = 31, 32\}$, then $|\alpha_1^G| \leq p^2, |\alpha_2^G| \leq p^2, |\alpha^G| \leq p^2$, and if $G \in \{\Phi_{33}(1^6), \Phi_{34}(321)a\}$, then $|\alpha_1^G| \leq p^2, |\alpha_2^G| = p$ and $|\alpha^G| \leq p^3$. Therefore for all the four groups G, $|\operatorname{Aut}_c(G)| \leq p^6$. Define a map $\delta : \{\alpha, \alpha_1, \alpha_2\} \to G$ such that $\alpha \mapsto \alpha, \alpha_1 \mapsto \alpha_1$ and $\alpha_2 \mapsto \alpha^{-1}\alpha_2\alpha =$

$\alpha_2\beta_2$. Suppose that $|\operatorname{Aut}_c(G)| = p^6$. Then δ must extend to a class-preserving automorphism of G. Hence there exist elements $\eta_1 \in \gamma_2(G)$ and $k_1, l_1, m_1 \in \mathbb{Z}$ such that $[\alpha_1\alpha_2,\ \eta_1\alpha^{k_1}\alpha_1^{l_1}\alpha_2^{m_1}] = \beta_2$. It is a routine calculation that

$$[\alpha_1\alpha_2,\ \eta_1\alpha^{k_1}\alpha_1^{l_1}\alpha_2^{m_1}] = \beta_1^{k_1}\beta_2^{k_1}\gamma^a$$

for some $a \in \mathbb{Z}$. Clearly it can not be equal to β_2 for any value of k_1, l_1, m_1, r_1 and s_1. Therefore δ is not a class-preserving automorphism, and hence $|\operatorname{Aut}_c(G)| \leq p^5$. Since $|\operatorname{Inn}(G)| = p^5$, $\operatorname{Aut}_c(G) = \operatorname{Inn}(G)$.

Lemma 4.3.9 *Let $G \in \{\Phi_k(1^6), \Phi_{k'}(222)a_0 \mid k = 40, 41,\ k' = 42, 43\}$. Then* $\operatorname{Out}_c(G) = 1$.

Proof. The group G is a class 4 p-group, minimally generated by α_1 and α_2. The commutator subgroup $\gamma_2(G)$ is abelian and generated by $\beta := [\alpha_1, \alpha_2], \beta_i := [\beta, \alpha_i]$ for $i = 1, 2$ and γ, where, for $k = 40$, $\gamma := [\beta_1, \alpha_2] = [\beta_2, \alpha_1]$, for $k = 41$, $\gamma^{-\nu} := [\alpha_2, \beta_2] = [\alpha_1, \beta_1]^{-\nu}$, for $k' = 42$, $\gamma := [\alpha_1, \beta_2] = [\alpha_2, \beta_1]$ and for $k' = 43$, $\gamma^{-\nu} := [\alpha_2, \beta_2] = [\alpha_1, \beta_1]^{-\nu}$. The center $Z(G)$ is of order p, generated by γ. It is easy to see that $|\alpha_1^G| \leq p^3$ and $|\alpha_2^G| \leq p^3$. Therefore $|\operatorname{Aut}_c(G)| \leq p^6$. Define a map $\delta : \{\alpha_1, \alpha_2\} \to G$ such that $\alpha_1 \mapsto \alpha_1$ and $\alpha_2 \mapsto \alpha_2\beta_2$. Suppose that $|\operatorname{Aut}_c(G)| = p^6$. Then δ must extend to a class-preserving automorphism of G. Hence there exist elements $\eta_1 (= \beta^{r_1}\beta_1^{s_1}\beta_2^{t_1}\gamma^{u_1}$ say$) \in \gamma_2(G)$ and $k_1, l_1 \in \mathbb{Z}$ such that $[\alpha_1\alpha_2,\ \eta_1\alpha_1^{k_1}\alpha_2^{l_1}] = \beta_2$. It is a routine calculation to show that,

$$[\alpha_1\alpha_2,\ \eta_1\alpha_1^{k_1}\alpha_2^{l_1}] \ = \ \beta^{l_1-k_1}\beta_1^{-k_1(k_1-1)/2-r_1}\beta_2^{l_1(l_1+1)/2-k_1l_1-r_1}\gamma^a$$

for some $a \in \mathbb{Z}$. It is easy to see that, if powers of β and β_1 in the above expression are 0 modulo p, then the power of β_2 is also 0 modulo p. It follows that δ is not a class-preserving automorphism and hence $|\operatorname{Aut}_c(G)| \leq p^5$. Since $|\operatorname{Inn}(G)| = p^5$, we have $\operatorname{Out}_c(G) = 1$.

Now we are ready to prove the following theorem.

Theorem 4.3.10 *Let G belongs to one of the isoclinism family Φ_k for $k = 2, ..., 6, 8, 9, 11, 12, 14, 16, 17, 19, 23, 25, ..., 29, 31, ..., 35, 37, 40, ..., 43$. Then* $\operatorname{Out}_c(G) = 1$.

Proof. Let $G \in \{\Phi_k(1^6),\ \Phi_8(321)a,\ \mid k = 2, ..., 6, 9\}$, then, since $\Phi_k(1^6) = \Phi_k(1^5) \times C_p$, $\Phi_8(321)a = \Phi_8(32) \times C_p$, it follows from Lemma 1.4.4 and Theorem 1.4.9 that $\operatorname{Out}_c(G) = 1$. The group $\Phi_{12}(1^6)$ is a direct product of groups of order p^3. Since all class-preserving automorphism of a group of order p^3 are inner, it follows that $\operatorname{Out}_c(\Phi_{12}(1^6)) = 1$. Since the commutator subgroup $\gamma_2(\Phi_{14}(1^6))$ is cyclic, from Theorem 1.4.7, we have $\operatorname{Out}_c(\Phi_{14}(1^6)) = 1$. Next, we consider the group $\Phi_{16}(1^6)$ and note that the subgroup $H = \left\langle \beta, \alpha_1, \alpha_2, \alpha_3, \gamma \right\rangle$ of $\Phi_{16}(1^6)$ is a normal abelian subgroup such that $\Phi_{16}(1^6)/H$ is cyclic. It follows from Proposition 1.4.6 that $\operatorname{Out}_c(\Phi_{16}(1^6)) = 1$. Similarly, the subgroup $H = \left\langle \alpha_1, \alpha_2, \alpha_3, \alpha_4 \right\rangle$ of $\Phi_k(222)$, for $k = 25, 26$, is a normal abelian subgroup of $\Phi_k(222)$, such that $\Phi_k(222)/H$ is cyclic, therefore $\operatorname{Out}_c(\Phi_k(222)) = 1$ for $k = 25, 26$. Next we consider the group $\Phi_{22}(1^6)$. The group $\Phi_{22}(1^6)$ is minimally generated by $\alpha, \alpha_1, \beta_1, \beta_2$. It is easy to check that $|\alpha^{\Phi_{22}(1^6)}| \leq p^2, |\alpha_1^{\Phi_{22}(1^6)}| = p, |\beta_1^{\Phi_{22}(1^6)}| = p$, and $|\beta_2^{\Phi_{22}(1^6)}| = p$. It follows from Lemma 1.4.3 that $|\operatorname{Aut}_c(\Phi_{22}(1^6))| \leq p^5$. But $|\operatorname{Inn}(\Phi_{22}(1^6))| = p^5$. Therefore $\operatorname{Out}_c(\Phi_{22}(1^6)) = 1$. Similarly, in the group $\Phi_{35}(1^6)$, $|\alpha^{\Phi_{35}(1^6)}| \leq p^4$ and $|\alpha_1^{\Phi_{35}(1^6)}| = p$, and in the group $\Phi_{37}(1^6)$, $|\alpha^{\Phi_{37}(1^6)}| \leq p^3$ and $|\alpha_1^{\Phi_{37}(1^6)}| \leq p^2$. Therefore if $G \in \{\Phi_{35}(1^6), \Phi_{37}(1^6)\}$, then $|\operatorname{Aut}_c(G)| \leq p^5$. But $|\operatorname{Inn}(G)| = p^5$, hence $\operatorname{Out}_c(G) = 1$. This, along with lemmas 4.3.2-4.3.9, completes the proof of theorem.

4.4 Groups G with non-trivial $\mathrm{Out}_c(G)$

In this section we list those groups of order p^6 for which there exist a non-inner class-preserving automorphism.

Lemma 4.4.1 *Let G be the group $\Phi_{24}(1^6)$. Then $|\operatorname{Out}_c(G)| = p$.*

Proof. The group G is a class 4 p-group, minimally generated by α, α_1 and β. The commutator subgroup $\gamma_2(G)$ is abelian and generated by $\alpha_{i+1} := [\alpha_i, \alpha]$ for $i = 1, 2$ and $\alpha_4 := [\alpha_3, \alpha] = [\alpha_1, \beta]$. The center $Z(G)$ is of order p, generated by α_4. We will show that for every element $g \in G - \gamma_2(G), Z(G) \leq [g, G]$. Let $g = \eta_1 \alpha^{k_1} \alpha_1^{l_1} \beta^{m_1}$. Then

$$[g, \beta^{l_2}] = [\eta_1 \alpha^{k_1} \alpha_1^{l_1} \beta^{m_1}, \beta^{l_2}] = \alpha_4^{l_1 l_2}.$$

Therefore, if l_1 is non-zero modulo p, we have $Z(G) \leq [g, G]$. Let $l_1 \equiv 0 \pmod p$. Then, since $\alpha_1^p \in \gamma_2(G)$,

$$[g, \alpha_3^{k_2}] = [\eta_1 \alpha^{k_1} \alpha_1^{l_1} \beta^{m_1}, \alpha_3^{k_2}] = \alpha_4^{k_1 k_2}.$$

Therefore, if k_1 is non-zero modulo p, $Z(G) \leq [g, G]$. Now let $k_1 \equiv 0 \pmod p$. Then

$$[g, \alpha_1^{m_2}] = [\eta_1 \beta^{m_1}, \alpha_1^{m_2}] = \alpha_4^{-m_1 m_2}.$$

Therefore, if m_1 is non-zero modulo p, $Z(G) \leq [g, G]$. It follows that for every $g \in G - \gamma_2(G), Z(G) \leq [g, G]$. Hence by Lemma 1.4.5 and Theorem 1.2.5 we have,

$$|\operatorname{Aut}_c(G)| \geq |\operatorname{Autcent}(G)||G|/|Z_2(G)| = p^3 p^6 / p^3 = p^6.$$

But, $|\alpha^G| \leq p^3, |\alpha_1^G| \leq p^2$ and $|\beta^G| = p$. Therefore we have $|\operatorname{Aut}_c(G)| \leq p^6$. Hence $|\operatorname{Aut}_c(G)| = p^6$. Since $|G/Z(G)| = p^5$, $|\operatorname{Out}_c(G)| = p$.

Lemma 4.4.2 *Let G be the group $\Phi_{30}(1^6)$. Then $|\operatorname{Out}_c(G)| = p$.*

Proof. The group G is a class 4 p-group, minimally generated by α, α_1 and β. The commutator subgroup $\gamma_2(G)$ is abelian and generated by $\alpha_2 := [\alpha_1, \alpha]$, $\alpha_3 := [\alpha_2, \alpha] = [\alpha_1, \beta]$ and $\alpha_4 := [\alpha_3, \alpha] = [\alpha_2, \beta]$. The center $Z(G)$ is of order p, generated by α_4. It is easy to see that $|\alpha^G| \leq p^3, |\alpha_1^G| \leq p^2$, and $|\beta^G| \leq p^2$. Therefore $|\operatorname{Aut}_c(G)| \leq p^7$. Define a map $\delta : \{\alpha, \alpha_1, \beta\} \to G$ such that $\alpha \mapsto \alpha\alpha_4, \alpha_1 \mapsto \alpha_1$ and $\beta \mapsto \beta\alpha_4$. By Lemma 4.3.1, the map δ extends to a central automorphism. We will show that δ is also a non-inner class-preserving automorphism. Let $g = \eta_1\alpha^{k_1}\alpha_1^{l_1}\beta^{m_1}$. Then

$$[g, \alpha_3^{k_2}] = [\eta_1\alpha^{k_1}\alpha_1^{l_1}\beta^{m_1}, \alpha_3^{k_2}] = \alpha_4^{k_1k_2}.$$

Therefore, if k_1 is non-zero modulo p, we have $Z(G) \leq [g, G]$. Hence δ maps g to a conjugate of g. Now let $k_1 \equiv 0 \pmod{p}$, then

$$[g, \alpha_2^{m_2}] = [\eta_1\alpha_1^{l_1}\beta^{m_1}, \alpha_2^{m_2}] = \alpha_4^{-m_1m_2}.$$

It follows that, if m_1 is non-zero modulo p, δ maps g to a conjugate of g. Now let $m_1 \equiv 0 \pmod{p}$. But then, $\delta(\eta_1\alpha_1^{l_1}) = \eta_1\alpha_1^{l_1}$, because being a central automorphism δ fixes $\gamma_2(G)$ element-wise. We have shown that for every $g \in G$, $\delta(g)$ is a conjugate of g. Therefore δ is a class-preserving automorphism. Now suppose δ is an inner automorphism. Then being central, δ is induced by some element in $Z_2(G) = \langle\alpha_3, \alpha_4\rangle$. Since $\alpha_4 \in Z(G)$, we can assume that δ is induced by α_3^t for some integer t. But then $\delta(\beta) = \beta$, a contradiction. Therefore δ is non-inner class-preserving automorphism. Since $|\operatorname{Inn}(G)| = p^5$, it follows that $|\operatorname{Aut}_c(G)| \geq p^6$. Now define a map $\sigma : \{\alpha, \alpha_1, \beta\} \to G$ such that $\alpha \mapsto \alpha_1^{-1}\alpha\alpha_1 = \alpha\alpha_2^{-1}, \alpha_1 \mapsto \alpha_1$ and $\beta \mapsto \beta$. Suppose $|\operatorname{Aut}_c(G)| = p^7$. Then σ extends to a class-preserving automorphism. But then, $1 = \delta([\alpha, \beta]) = [\alpha\alpha_2^{-1}, \beta] = \alpha_4^{-1}$ which is not possible. Therefore, we have $|\operatorname{Aut}_c(G)| = p^6$. Since $|G/Z(G)| = p^5$, $|\operatorname{Out}_c(G)| = p$.

Lemma 4.4.3 *Let G be the group $\Phi_{36}(1^6)$. Then $|\operatorname{Out}_c(G)| = p$.*

Proof. The group G is of maximal class, minimally generated by α and α_1. The commutator subgroup $\gamma_2(G)$ is abelian and generated by $\alpha_{i+1} := [\alpha_i, \alpha]$ for $i = 1, ..., 3$ and $\alpha_5 := [\alpha_4, \alpha] = [\alpha_1, \alpha_2]$. The center $Z(G)$ is of order p, generated by α_5. We will show that for every element $g \in G - \gamma_2(G), Z(G) \leq [g, G]$. Let $g = \eta_1\alpha^{k_1}\alpha_1^{l_1}$. Then

$$[g, \alpha_4^{k_2}] = [\eta_1\alpha^{k_1}\alpha_1^{l_1}, \alpha_4^{k_2}] = \alpha_4^{-k_1k_2}.$$

Therefore, if k_1 is non-zero modulo p, we have $Z(G) \leq [g, G]$. Let $k_1 \equiv 0 \pmod p$. Then

$$[g, \alpha_2^{l_2}] = [\eta_1\alpha_1^{l_1}, \alpha_2^{l_2}] = \alpha_5^{l_1l_2}.$$

Therefore, if l_1 is non-zero modulo p, $Z(G) \leq [g, G]$. Let $l_1 \equiv 0 \pmod p$, then we have $g \in \gamma_2(G)$ because $\alpha_1^p \in \gamma_2(G)$. It follows that, for every $g \in G - \gamma_2(G), Z(G) \leq [g, G]$. Hence by Lemma 1.4.5 and Theorem 1.2.5 we get

$$|\operatorname{Aut}_c(G)| \geq |\operatorname{Autcent}(G)||G|/|Z_2(G)| = p^2p^6/p^2 = p^6.$$

But it is easy to see that $|\alpha^G| \leq p^4$ and $|\alpha_1^G| \leq p^2$. Therefore $|\operatorname{Aut}_c(G)| \leq p^6$. Hence $|\operatorname{Aut}_c(G)| = p^6$. Since $|G/Z(G)| = p^5$, we have $|\operatorname{Out}_c(G)| = p$.

Lemma 4.4.4 *Let G be the group $\Phi_{38}(1^6)$. Then $|\operatorname{Out}_c(G)| = p$.*

Proof. The group G is of maximal class, minimally generated by α, α_1. The commutator subgroup $\gamma_2(G)$ is abelian and generated by $\alpha_{i+1} := [\alpha_i, \alpha]$ for $i = 1, ..., 3$ and $\alpha_5 := [\alpha_4, \alpha] = [\alpha_1, \alpha_3]$. Also $[\alpha_1, \alpha_2] = \alpha_4\alpha_5^{-1}$. The center $Z(G)$ is generated by α_5. We show that for every element $g \in G - \gamma_2(G), Z(G) \leq [g, G]$. Let $g = \eta_1\alpha^{k_1}\alpha_1^{l_1}$. Then

$$[g, \alpha_4^{k_2}] = [\eta_1\alpha^{k_1}\alpha_1^{l_1}, \alpha_4^{k_2}] = \alpha_5^{-k_1k_2}.$$

Therefore, if k_1 is non-zero modulo p, $Z(G) \leq [g, G]$. Hence, let $k_1 \equiv 0 \pmod p$. Then

$$[g, \alpha_3^{l_2}] = [\eta_1\alpha_1^{l_1}, \alpha_3^{l_2}] = \alpha_5^{l_1l_2}.$$

Therefore, if l_1 is non-zero modulo p, we have $Z(G) \leq [g, G]$. If $l_1 \equiv 0 \pmod p$, then we have $g \in \gamma_2(G)$ because $\alpha_1^p \in \gamma_2(G)$. It follows that, for every $g \in G - \gamma_2(G)$, $Z(G) \leq [g, G]$. Therefore applying Lemma 1.4.5 and Theorem 1.2.5 we get

$$|\operatorname{Aut}_c(G)| \geq |\operatorname{Autcent}(G)||G|/|Z_2(G)| = p^2p^6/p^2 = p^6.$$

It is easy to check that, $|\alpha^G| \leq p^4$ and $|\alpha_1^G| \leq p^3$, hence the upper bound on $|\operatorname{Aut}_c(G)|$ is p^7. Suppose that $|\operatorname{Aut}_c(G)| = p^7$. Then, δ defined on the generators $\{\alpha, \alpha_1\}$ as $\delta(\alpha) = \alpha$ and $\delta(\alpha_1) = \alpha_2^{-1}\alpha_1\alpha_2 = \alpha_1\alpha_4\alpha_5^{-1}$ must extend to a class-preserving automorphism. Note that

$$\delta(\alpha_2) = \delta([\alpha_1, \alpha]) = [\alpha_1\alpha_4\alpha_5^{-1}, \alpha] = \alpha_2\alpha_5.$$

Since δ is a class-preserving automorphism, there exist $\eta_1 \in \gamma_2(G)$ and $k_1, l_1 \in \mathbb{Z}$ such that

$$[\alpha_2, \eta_1\alpha^{k_1}\alpha_1^{l_1}] = \alpha_5.$$

We have that

$$[\alpha_2, \eta_1\alpha^{k_1}\alpha_1^{l_1}] = \alpha_3^{k_1}\alpha_4^{k_1(k_1-1)/2-l_1}\alpha_5^{l_1-k_1l_1+\sum\limits_{n=1}^{k_1-2} n(n-1)/2},$$

which for no value of k, k_1 can be equal to α_5. This gives a contradiction. Hence $|\operatorname{Aut}_c(G)| = p^6$. Since $|G/Z(G)| = p^5$, we have $|\operatorname{Out}_c(G)| = p$.

Lemma 4.4.5 *Let G be the group $\Phi_{39}(1^6)$. Then $|\operatorname{Out}_c(G)| = p$.*

Proof. The group G is of maximal class, minimally generated by α, α_1. The commutator subgroup $\gamma_2(G)$ is generated by $\alpha_{i+1} := [\alpha_i, \alpha]$ for $i = 1, 2$, $\alpha_4 := [\alpha_3, \alpha] = [\alpha_1, \alpha_2]$, and $\alpha_5 := [\alpha_2, \alpha_3] = [\alpha_3, \alpha_1] = [\alpha_4, \alpha_1]$. Note that any element of $\gamma_2(G)$ can be written as $\alpha_2^r\alpha_3^s\alpha_4^t\alpha_5^u$ for some $r, s, t, u \in \mathbb{Z}$. The center $Z(G)$ is generated by α_5. It is easy to see that $|\alpha^G| \leq p^3$ and $|\alpha_1^G| \leq p^3$. Therefore $|\operatorname{Aut}_c(G)| \leq p^6$. Define a map $\delta : \{\alpha, \alpha_1\} \to G$ such that $\alpha \mapsto \alpha$, and $\alpha_1 \mapsto \alpha_2^{-1}\alpha_1\alpha_2 = \alpha_1\alpha_4$. We will show that δ extends to a class-preserving automorphism. It is easy to check that δ preserves all the defining relations of the group. Hence δ extends to an endomorphism. Note that δ fixes $\gamma_2(G)$ element-wise, therefore for $k_1, l_1 \in \mathbb{Z}$ and $\eta_1 = \alpha_2^{r_1}\alpha_3^{s_1}\alpha_4^{t_1}\alpha_5^{u_1} \in \gamma_2(G)$,

$$\delta(\eta_1\alpha^{k_1}\alpha_1^{l_1}) = \eta_1\alpha^{k_1}\alpha_1^{l_1}\alpha_4^{l_1}\alpha_5^{l_1(l_1-1)/2}.$$

It is a routine calculation that

$$[\eta_1\alpha^{k_1}\alpha_1^{l_1}, \alpha_3^{s_2}\alpha_4^{t_2}] = \alpha_5^{r_1s_2-l_1s_2-l_1t_2-l_1k_1s_2}\alpha_4^{-k_1s_2}.$$

Since $\delta(\eta_1\alpha^{k_1}) = \eta_1\alpha^{k_1}$, which is obviously a conjugate of $\eta_1\alpha^{k_1}$, let l_1 be non-zero modulo p. Now if k_1 is non-zero modulo p, then clearly there exist s_2 and t_2 such that

$$-k_1 s_2 \equiv l_1 \pmod p$$

and

$$r_1 s_2 - l_1 s_2 - l_1 t_2 - l_1 k_1 s_2 \equiv l_1(l_1 - 1)/2 \pmod p.$$

Suppose $k_1 \equiv 0 \pmod p$, then it can be calculated that

$$[\eta_1 \alpha_1^{l_1}, \alpha_2^{r_2} \alpha_4^{t_2}] = \alpha_5^{-s_1 r_2 + r_2 l_1 (l_1 - 1)/2 - l_1 t_2} \alpha_4^{l_1 r_2}.$$

Since l_1 is non-zero modulo p, clearly there exist r_2 and t_2 such that

$$l_1 r_2 \equiv l_1 \pmod p$$

and

$$-s_1 r_2 + r_2 l_1 (l_1 - 1)/2 - l_1 t_2 \equiv l_1(l_1 - 1)/2 \pmod p.$$

It follows that δ maps every element of G to a conjugate of itself. Therefore δ is a bijection, and hence a class-preserving automorphism. Now we show that δ is a non-inner automorphism. On the contrary, suppose that δ is an inner automorphism. Note that $g^{-1}\delta(g) \in Z_2(G)$. Thus it follows that δ is induced by some element in $Z_3(G) = \langle \alpha_3, \alpha_4, Z(G) \rangle$. Let it be induced by $\alpha_3^{s_1}\alpha_4^{t_1}$. Since $\delta(\alpha) = \alpha$, we have $\alpha_3^{-s_1}\alpha\alpha_3^{s_1} = \alpha$, which implies that $s_1 \equiv 0 \pmod p$. But then $\delta(\alpha_1) = \alpha_4^{-t_1}\alpha_1\alpha_4^{t_1} = \alpha_1\alpha_5^{-t_1}$, a contradiction. Therefore δ is a non-inner class preserving automorphism. Since $|\operatorname{Inn}(G)| = p^5$, we have $|\operatorname{Aut}_c G)| = p^6$, and $|\operatorname{Out}_c(G)| = p$.

Lemma 4.4.6 *Let G be the group $\Phi_{13}(1^6)$. Then $|\operatorname{Out}_c(G)| = p^2$.*

Proof. The group G is a special p-group, minimally generated by $\alpha_1, \alpha_2, \alpha_3$ and α_4. The commutator subgroup $\gamma_2(G)$ is generated by $\beta_1 := [\alpha_1, \alpha_2]$ and $\beta_2 := [\alpha_1, \alpha_3] = [\alpha_2, \alpha_4]$. The conjugates of $\alpha_1, \alpha_2, \alpha_3$ and α_4 are $\alpha_1\beta_1^r\beta_2^s$, $\alpha_2\beta_1^r\beta_2^s, \alpha_3\beta_2^s$ and $\alpha_4\beta_2^s$ respectively, where r and s vary over $\mathbb{Z}$. Since the exponent of $\gamma_2(G)$ is p, it follows that $|\alpha_1^G| = |\alpha_2^G| = p^2$ and $|\alpha_3^G| = |\alpha_4^G| = p$. Therefore by Lemma 1.4.3, $|\operatorname{Aut}_c(G)| \leq p^6$.

Define a map $\delta : \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} \to G$ such that $\alpha_1 \mapsto \alpha_1\beta_1^{r_1}\beta_2^{s_1}, \alpha_2 \mapsto \alpha_2\beta_1^{r_2}\beta_2^{s_2}$, $\alpha_3 \mapsto \alpha_3\beta_2^{s_3}$ and $\alpha_4 \mapsto \alpha_4\beta_2^{s_4}$, for some $r_1, s_1, r_2, s_2, s_3, s_4 \in \mathbb{Z}$. By Lemma 4.3.1, this map extends to a central automorphism of G. Since δ fixes $\gamma_2(G)$ element-wise, for $k_1, l_1, m_1, n_1 \in \mathbb{Z}$ and $\eta_1 \in \gamma_2(G)$,

$$\delta(\eta_1\alpha_1^{k_1}\alpha_2^{l_1}\alpha_3^{m_1}\alpha_4^{n_1}) = \eta\alpha_1^{k_1}\alpha_2^{l_1}\alpha_3^{m_1}\alpha_4^{n_1}\beta_1^{k_1r_1+l_1r_2}\beta_2^{k_1s_1+l_1s_2+m_1s_3+n_1s_4}.$$

Therefore δ extends to a class-preserving automorphism if and only if for every $k_1, l_1, m_1, n_1 \in \mathbb{Z}$, and $\eta_1 \in \gamma_2(G)$, there exist k_2, l_2, m_2, n_2 (depending on k_1, l_1, m_1, n_1) and $\eta_2 \in \gamma_2(G)$ such that

$$[\eta_1\alpha_1^{k_1}\alpha_2^{l_1}\alpha_3^{m_1}\alpha_4^{n_1}, \eta_2\alpha_1^{k_2}\alpha_2^{l_2}\alpha_3^{m_2}\alpha_4^{n_2}] = \beta_1^{k_1r_1+l_1r_2}\beta_2^{k_1s_1+l_1s_2+m_1s_3+n_1s_4}.$$

Expanding the left hand side, we get

$$\beta_1^{k_1l_2-k_2l_1}\beta_2^{k_1m_2-k_2m_1+l_1n_2-l_2n_1} = \beta_1^{k_1r_1+l_1r_2}\beta_2^{k_1s_1+l_1s_2+m_1s_3+n_1s_4}.$$

Comparing the powers of β_i's, we see that δ extends to a class-preserving automorphism if the following equations hold:

$$k_1l_2 - k_2l_1 \equiv k_1r_1 + l_1r_2 \pmod{p},$$

$$k_1m_2 - k_2m_1 + l_1n_2 - l_2n_1 \equiv k_1s_1 + l_1s_2 + m_1s_3 + n_1s_4 \pmod p.$$

It is easy to see that for any given k_1, l_1, m_1, n_1 there exist k_2, l_2, m_2, n_2 such that the above two equations are satisfied. Thus it follows that $|\operatorname{Aut}_c(G)| = p^6$. Since $|G/Z(G)| = p^4, |\operatorname{Out}_c(G)| = p^2$.

Lemma 4.4.7 *Let G be the group $\Phi_{18}(1^6)$. Then $|\operatorname{Out}_c(G)| = p^2$.*

Proof. The group G is a class 3 p-group, minimally generated by α, α_1, β. The commutator subgroup $\gamma_2(G)$ is abelian and generated by $\alpha_2 := [\alpha_1, \alpha], \alpha_3 := [\alpha_2, \alpha] = [\alpha_1, \beta]$ and $\gamma := [\alpha, \beta]$. The center $Z(G)$ is of order p^2, generated by α_3 and γ. Note that $|\alpha^G| \leq p^3, |\alpha_1^G| \leq p^2$ and $|\beta^G| \leq p^2$. It follows from Lemma 1.4.3 that $|\operatorname{Aut}_c(G)| \leq p^7$. Now define a map $\delta : \{\alpha, \alpha_1, \beta\} \to G$ such that $\alpha \mapsto \alpha\alpha_3^{r_1}\gamma^{s_1}, \alpha_1 \mapsto \alpha_1\alpha_3^{r_2}$ and $\beta \mapsto \beta\alpha_3^{r_3}$ for some $r_1, s_1, r_2, r_3 \in \mathbb{Z}$. By Lemma 4.3.1 this map extends to a central automorphism of G. Let $g = \eta_1\alpha^{k_1}\alpha_1^{l_1}\beta^{m_1}$, where $\eta_1 \in \gamma_2(G)$ and $k_1, l_1, m_1 \in \mathbb{Z}$. Let $k_1 \equiv 0 \pmod p$, then note that $\delta(g) = g\alpha_3^r$ for some $r \in \mathbb{Z}$ and

$$[g, \beta^{l_2}] = [\eta_1\alpha_1^{l_1}\beta^{m_1}, \beta^{l_2}] = \alpha_3^{l_1l_2}.$$

Therefore if l_1 is non-zero modulo p, we have $\langle\alpha_3\rangle \leq [g, G]$. Let $l_1 \equiv 0 \pmod p$. Note that $\alpha_1^p \in Z(G)$, hence

$$[g, \alpha_1^{m_2}] = [\eta_1\beta^{m_1}, \alpha_1^{m_2}] = \alpha_3^{-m_1m_2}.$$

Therefore if m_1 is non-zero modulo p, we have $\langle\alpha_3\rangle \leq [g, G]$. Thus we have shown that, if $k_1 \equiv 0 \pmod p$, then $g^{-1}\delta(g) \in [g, G]$. It follows that, if $k_1 \equiv 0 \pmod p$,

δ maps g to a conjugate of g. Now suppose k_1 is non-zero modulo p. Then

$$[g, \alpha_2^{k_2}] = [\eta_1 \alpha^{k_1} \alpha_1^{l_1} \beta^{m_1}, \alpha_2^{k_2}] = \alpha_3^{-k_1 k_2},$$

so that $\langle \alpha_3 \rangle \leq [g, Z_2(G)]$. Also, we have

$$[g, \beta^{n_2}] = [\eta_1 \alpha^{k_1} \alpha_1^{l_1} \beta^{m_1}, \beta^{n_2}] = \alpha_3^{l_1 n_2} \gamma^{k_1 n_2}.$$

Since $\beta \in Z_2(G)$ and $[g, Z_2(G)]$ is a subgroup, it follows that $Z(G) \leq [g, G]$. Because δ is a central automorphism, we have $g^{-1}\delta(g) \in [g, G]$. We have shown that, for every $g \in G$, $g^{-1}\delta(g) \in [g, G]$. It follows that δ is a class-preserving automorphism. Since r_1, s_1, r_2, r_3 were arbitrary, we have that $|\operatorname{Aut}_c(G) \cap \operatorname{Autcent}(G)| \geq p^4$. Applying Lemma 3.3.11 we get $|Z(\operatorname{Aut}_c(G))| \geq p^4$. Note that $\operatorname{Aut}_c(G)$ is non-abelian because G is a class 3 group. Therefore $|\operatorname{Aut}_c(G)| \geq p^6$. Now suppose that $|\operatorname{Aut}_c(G)| = p^7$. Then the map σ defined on the generators $\{\alpha, \alpha_1, \beta\}$ as $\alpha \mapsto \alpha, \alpha_1 \mapsto \alpha_1$ and $\beta \mapsto \alpha\beta\alpha^{-1} = \beta\gamma$ extends to a class-preserving automorphism. Hence there exist elements $\eta_2 \in \gamma_2(G)$ and $k_2, l_2, m_2 \in \mathbb{Z}$ such that $[\alpha_1\beta,\ \eta_2\alpha^{k_2}\alpha_1^{l_2}\beta^{m_2}] = \gamma$, but by a routine calculation it can be checked that

$$[\alpha_1\beta,\ \eta_2\alpha^{k_2}\alpha_1^{l_2}\beta^{m_2}] = \alpha_2^{k_2}\beta\alpha_3^{m_2 - l_2 + k_2(k_2-1)/2}\gamma^{-k_2},$$

which can not be equal to γ for any values of k_2, l_2, m_2. Therefore we get a contradiction. It follows that $|\operatorname{Aut}_c(G)| = p^6$. Hence $|\operatorname{Out}_c(G)| = p^2$ as $|\operatorname{Inn}(G)| = p^4$.

Lemma 4.4.8 *Let G be the group $\Phi_{20}(1^6)$. Then $|\operatorname{Out}_c(G)| = p^2$.*

Proof. The group G is a class 3 p-group, minimally generated by $\alpha, \alpha_1, \alpha_2$. The commutator subgroup $\gamma_2(G)$ is abelian and generated by $\beta := [\alpha_1, \alpha_2], \beta_1 :=$

$[\beta, \alpha_1]$ and $\beta_2 := [\beta, \alpha_2] = [\alpha, \alpha_1]$. The center $Z(G)$ is of order p^2, generated by β_1 and β_2. Note that $|\alpha^G| = p, |\alpha_1^G| \leq p^3$ and $|\alpha_2^G| \leq p^2$. It follows from Lemma 1.4.3 that $|\operatorname{Aut}_c(G)| \leq p^6$. Now define a map $\delta : \{\alpha, \alpha_1, \alpha_2\} \to G$ such that $\alpha \mapsto \alpha\beta_2^{t_1}, \alpha_1 \mapsto \alpha_1\beta_1^{s_2}\beta_2^{t_2}$ and $\alpha_2 \mapsto \alpha_2\beta_2^{t_3}$ for some $t_1, s_2, t_2, t_3 \in \mathbb{Z}$. By Lemma 4.3.1 this map extends to a central automorphism of G. Let $g = \eta_1\alpha^{k_1}\alpha_1^{l_1}\alpha_2^{m_1}$, where $\eta_1 = \beta^{u_1}\beta_1^{v_1}\beta_2^{w_1}$ and $k_1, l_1, m_1, u_1, v_1, w_1 \in \mathbb{Z}$. Note that, if $l_1 \equiv 0 \pmod p$, then $\delta(g) = g\beta_2^r$ for some $r \in \mathbb{Z}$. Consider

$$[g, \beta^{m_2}] = [\eta_1\alpha^{k_1}\alpha_2^{m_1}, \beta^{m_2}] = \beta_2^{-m_1m_2}.$$

Therefore if m_1 is non-zero modulo p, we have $\langle\beta_2\rangle \leq [g, G]$. Let $m_1 \equiv 0 \pmod p$. Note that $\alpha_2^p \in Z(G)$, hence

$$[g, \alpha_2^{u_2}] = [\eta_1\alpha^{k_1}, \alpha_2^{u_2}] = [\beta^{u_1}\beta_1^{v_1}\beta_2^{w_1}\alpha^{k_1},\ \alpha_2^{u_2}] = \beta_2^{u_1u_2}.$$

Therefore if u_1 is non-zero modulo p, we have $\langle\beta_2\rangle \leq [g, G]$. Let $u_1 \equiv 0 \pmod p$. Then

$$[g, \alpha_1^{k_2}] = [\alpha^{k_1}, \alpha_1^{k_2}] = \beta_2^{k_1k_2},$$

so that if k_1 is non-zero modulo p, then $\langle\beta\rangle \leq [g, G]$. Thus we have shown that, if $l_1 \equiv 0 \pmod p$, we have $g^{-1}\delta(g) \in [g, G]$. It follows that, if $l_1 \equiv 0 \pmod p$, δ maps g to a conjugate of g. Now suppose l_1 is non-zero modulo p, then

$$[g, \alpha^{l_2}] = [\eta_1\alpha^{k_1}\alpha_1^{l_1}\alpha_2^{m_1}, \alpha^{l_2}] = \beta_2^{-l_1l_2},$$

so that $\langle\beta_2\rangle \leq [g, Z_2(G)]$. Also we have

$$[g, \beta^{n_2}] = [\eta_1\alpha^{k_1}\alpha_1^{l_1}\alpha_2^{m_1}, \beta^{n_2}] = \beta_1^{-l_1n_2}\beta_2^{-m_1n_2}.$$

Since $\beta \in Z_2(G)$ and $[g, Z_2(G)]$ is a subgroup, it follows that $Z(G) \leq [g, G]$. Because δ is a central automorphism we have $g^{-1}\delta(g) \in [g, G]$. It follows that δ is a class-preserving automorphism. Since t_1, s_2, t_2, t_3 were arbitrary, we have that $|\operatorname{Aut}_c(G) \cap \operatorname{Autcent}(G)| \geq p^4$. Applying Lemma 3.3.11 we get $|Z(\operatorname{Aut}_c(G))| \geq p^4$. But $\operatorname{Aut}_c(G)$ is non-abelian since G is of class 3. Therefore $|\operatorname{Aut}_c(G)| \geq p^6$. Hence $|\operatorname{Aut}_c(G)| = p^6$. Since $|G/Z(G)| = p^4$, we have $|\operatorname{Out}_c(G)| = p^2$.

Now we are ready to prove the following theorem.

Theorem 4.4.9 *Let G be a group of order p^6.*

1. *If G belongs to one of the isoclinism family Φ_k for $k = 7, 10, 24, 30, 36, 38, 39$, then $|\operatorname{Out}_c(G)| = p$.*

2. *If G belongs to one of the isoclinism family Φ_k for $k = 13, 18, 20$, then $|\operatorname{Out}_c(G)| = p^2$.*

3. *If G belongs to one of the isoclinism family Φ_k for $k = 15, 21$, then $|\operatorname{Out}_c(G)| = p^4$.*

Proof. Let G be either the group $\Phi_7(1^6)$ or the group $\Phi_{10}(1^6)$. Then since $\Phi_7(1^6) = \Phi_7(1^5) \times C_p$ and $\Phi_{10}(1^6) = \Phi_{10}(1^5) \times C_p$, it follows from Theorem 1.4.9 that $|\operatorname{Out}_c(G)| = p$. With this observation in hands, (i) follows from Lemmas 4.4.1-4.4.5. It is readily seen that (ii) follows from Lemmas 4.4.6-4.4.8. Now let G be the group $\Phi_{15}(1^6)$. We observe that the James' list of groups of order p^6 and class 2 consists of exactly 5 isoclinism families Φ_k, for $k = 11..., 15$. For $k = 11, ..., 14$ we have seen that $|\operatorname{Aut}_c(\Phi_k)| \neq p^8$. But as shown by Burnside [10] there exists a group W of order p^6 and of nilpotency class 2 such that $|\operatorname{Aut}_c(W)| = p^8$. Therefore G must be isoclinic to the group W and $|\operatorname{Aut}_c(G)| = p^8$. Since $|G/Z(G)| = p^4$, we have $|\operatorname{Out}_c(G)| = p^4$. Next, it follows from [72, Proposition 5.8], that $|\operatorname{Out}_c(\Phi_{21}(1^6))| = p^4$. This completes the proof of the theorem.

Theorem 4.3.10 and Theorem 4.4.9 can be combined to state the following result:

Theorem 4.4.10 *Let G be a group of order p^6 for an odd prime p. Then $\operatorname{Out}_c(G) \neq 1$ if and only if G belongs to one of the isoclinism families Φ_k for $k = 7, 10, 13, 15, 18, 20, 21, 24, 30, 36, 38, 39$. Moreover,*

1. *if G belongs to one of the isoclinism families Φ_k for $k = 7, 10, 24, 30, 36, 38, 39$, then $|\operatorname{Out}_c(G)| = p$,*
2. *if G belongs to one of the isoclinism families Φ_k for $k = 13, 18, 20$, then $|\operatorname{Out}_c(G)| = p^2$, and*
3. *if G belongs to one of the isoclinism families Φ_k for $k = 15, 21$, then $|\operatorname{Out}_c(G)| = p^4$.*

Using GAP [24] it can be verified that the question of Kang and Kunyavskiĭ has an affirmative answer for groups of order 2^6 and 3^6 (Bogomolov multiplier of groups of order 2^6 is also computed in [16]). With this information the following theorem which provides an affirmative answer of the question of Kang and Kunyavskiĭ for most of the groups of order p^6, follows from Theorem 1.6.3 and Theorem 4.4.10.

Theorem 4.4.11 *Let G be a Ш-rigid group of order p^6 for a prime p. If G does not belong to the isoclinism families Φ_k for $k = 28, 29$, then its Bogomolov multiplier $B_0(G)$ is zero.*

Chapter 5

IA Automorphisms of Groups

In this chapter we study the group of those IA automorphisms which fix the center element-wise and prove that these groups are isomorphic for any two isoclinic groups. We also see some applications of this result for finite p-groups.

5.1 IA automorphisms that fix the center element-wise

Let G be any group and σ be an automorphism of G. Following Bachmuth [2], we call σ an IA automorphism if $x^{-1}\sigma(x) \in \gamma_2(G)$ for each $x \in G$. Bachmuth writes, explaining the reason behind the name IA, that "the letters I and A are used to remind the reader that these automorphisms are those which induce the identity automorphism in the abelianized group". The set of all IA automorphisms of G form a normal subgroup of $\mathrm{Aut}(G)$ and is denoted by $\mathrm{IA}(G)$. The set of all IA automorphisms that fix the center element-wise forms a normal subgroup of $\mathrm{IA}(G)$ and is denoted by $\mathrm{IA}_z(G)$. We note that $\mathrm{Autcent}(G)$ centralizes not only $\mathrm{Inn}(G)$, but also $\mathrm{IA}_z(G)$. Thus $\mathrm{Autcent}(G) = C_{\mathrm{Aut}(G)}(\mathrm{IA}_z(G))$.

Notice that any class-preserving automorphism is an IA automorphism which fixes the center element-wise and hence $\mathrm{Aut}_c(G) \leq \mathrm{IA}_z(G)$. We know from Theorem 1.5.2 that if two finite groups G and H are isoclinic then $\mathrm{Aut}_c(G) \cong \mathrm{Aut}_c(H)$. In the following theorem we extend this result of Yadav to the group $\mathrm{IA}_z(G)$ for any arbitrary group G.

Theorem 5.1.1 *Let G and H be any two isoclinic groups. Then there exists an isomorphism $\alpha\colon \mathrm{IA}_z(G) \to \mathrm{IA}_z(H)$ such that $\alpha(\mathrm{Aut}_c(G)) = \mathrm{Aut}_c(H)$.*

We first prove the following lemma.

Lemma 5.1.2 *Let G and H be isoclinic groups and (φ, θ) be an isoclinism of G onto H. Then for $b \in \gamma_2(G)$ and $a \in G$ such that $\varphi(aZ(G)) = kZ(H)$, we have $\theta(b^a)^{k^{-1}} = \theta(b)$.*

Proof. Let $\varphi(bZ(G)) = lZ(H)$, then

$$\theta(b^a)^{k^{-1}} = k\theta([a, b^{-1}])\theta(b)k^{-1} = k[k, l^{-1}]\theta(b)k^{-1} = lkl^{-1}\theta(b)k^{-1}.$$

But from Lemma 1.3.2, $l^{-1}\theta(b) \in Z(H)$. Hence by the preceding equation $\theta(b^a)^{k^{-1}} = \theta(b)$.

Proof of Theorem 5.1.1. Let (φ, θ) be an isoclinism of G onto H. Let $\sigma \in \mathrm{IA}_z(G)$. Define a map τ_σ by $\tau_\sigma(h) = h\theta(g^{-1}\sigma(g))$ for $h \in H$, where g is given by $\varphi^{-1}(hZ(H)) = gZ(G)$. Notice that τ_σ is well-defined because σ fixes $Z(G)$ element-wise. Next we show that $\tau_\sigma \in \mathrm{IA}_z(H)$. Let $h_1, h_2 \in H$ and $\varphi^{-1}(h_iZ(H)) = g_iZ(G)$ for $i = 1, 2$. Then,

$$\tau_\sigma(h_1h_2) \quad = \quad h_1h_2\theta(g_2^{-1}g_1^{-1}\sigma(g_1g_2))$$

$$\begin{aligned} &= h_1h_2\theta(g_2^{-1}g_1^{-1}\sigma(g_1)g_2g_2^{-1}\sigma(g_2)) \\ &= h_1h_2\theta(g_2^{-1}g_1^{-1}\sigma(g_1)g_2)h_2^{-1}h_2\theta(g_2^{-1}\sigma(g_2)). \end{aligned}$$

Applying Lemma 5.1.2, we obtain

$$\begin{aligned} \tau_\sigma(h_1h_2) &= h_1\theta(g_1^{-1}\sigma(g_1))h_2\theta(g_2^{-1}\sigma(g_2)) \\ &= \tau_\sigma(h_1)\tau_\sigma(h_2). \end{aligned}$$

Thus τ_σ is a homomorphism.

Now we show that τ_σ is a bijection. Let $\tau_\sigma(h) = 1$ and $\varphi^{-1}(hZ(H)) = gZ(G)$. Then $h\theta(g^{-1}\sigma(g)) = 1$. This implies that $h \in \gamma_2(H)$ and hence $g \in \gamma_2(G)Z(G)$. Without loss of generality we can assume that $g \in \gamma_2(G)$. Then we have $h\theta(g^{-1})\theta(\sigma(g)) = 1$. However, by Lemma 1.3.2, $h\theta(g^{-1}) \in Z(H)$, so that $\theta(\sigma(g)) \in Z(H) \cap \gamma_2(H)$. Using Lemma 1.3.2 again, $\sigma(g) \in Z(G)$, which implies $g \in Z(G)$. Hence $\sigma(g) = g$, as σ fixes the center element-wise. Thus $h = 1$ and hence τ_σ is an injective map. To show that it is a surjection, let $h \in H$ and $\varphi^{-1}(hZ(H)) = gZ(G)$. Since $g^{-1}\sigma^{-1}(g) \in \gamma_2(G)$, by Lemma 1.3.2 we have $\varphi(g^{-1}\sigma^{-1}(g)Z(G)) = \theta(g^{-1}\sigma^{-1}(g))Z(H)$ so that $\varphi^{-1}(\theta(g^{-1}\sigma^{-1}(g))Z(H)) = g^{-1}\sigma^{-1}(g)Z(G)$. Therefore by the definition of τ_σ we have

$$\begin{aligned} \tau_\sigma(\theta(g^{-1}\sigma^{-1}(g))) &= \theta(g^{-1}\sigma^{-1}(g))\theta(\sigma^{-1}(g^{-1})g\sigma(g^{-1}\sigma^{-1}(g))) \\ &= \theta(g^{-1}\sigma^{-1}(g))\theta(\sigma^{-1}(g^{-1})g\sigma(g^{-1})g) \\ &= \theta(\sigma(g^{-1})g) \end{aligned}$$

Let $h' = \theta(g^{-1}\sigma^{-1}(g))$. Since τ_σ is a homomorphism, we get

$$\tau_\sigma(hh') = \tau_\sigma(h)\tau_\sigma(h') = h\theta(g^{-1}\sigma(g))\theta(\sigma(g^{-1}(g)) = h.$$

As h was chosen arbitrarily, it follows that τ_σ is surjective and hence bijective. It is easy to see that τ_σ fixes $Z(H)$ element-wise, so that $\tau_\sigma \in \mathrm{IA}_z(H)$.

Define α as $\alpha(\sigma) = \tau_\sigma$. We show that α is an isomorphism. Let $\sigma_1, \sigma_2 \in \mathrm{IA}_z(G)$ and let $h \in H$ with $\varphi^{-1}(hZ(H)) = gZ(G)$. Then, $\tau_{\sigma_1}\tau_{\sigma_2}(h) = \tau_{\sigma_1}(h\theta(g^{-1}\sigma_2(g)))$. Using Lemma 1.3.2, we have $\varphi^{-1}(h\theta(g^{-1}\sigma_2(g))Z(H)) = \sigma_2(g)Z(G)$. Therefore $\tau_{\sigma_1}\tau_{\sigma_2}(h) = h\theta(g^{-1}\sigma_2(g))\theta(\sigma_2(g^{-1})\sigma_1\sigma_2(g))$, which equals $h\theta(g^{-1}\sigma_1\sigma_2(g))$, which is $\tau_{\sigma_1\sigma_2}(h)$. Since h was arbitrary, we have $\tau_{\sigma_1\sigma_2} = \tau_{\sigma_1}\tau_{\sigma_2}$ and hence α is a homomorphism.

To show that α is a bijection, notice that $(\varphi^{-1}, \theta^{-1})$ is an isoclinism of H onto G. So given a $\tau \in \mathrm{IA}_z(H)$, in the similar manner as above, $\sigma_\tau \in \mathrm{IA}_z(G)$ can be defined. Define $\beta\colon \mathrm{IA}_z(H) \to \mathrm{IA}_z(G)$ as $\beta(\tau) = \sigma_\tau$. Let $g \in G$ and $\varphi(gZ(G)) = hZ(H)$, then

$$\begin{aligned}
\beta\alpha(\sigma)(g) &= \beta(\tau_\sigma)(g) \\
&= g\theta^{-1}(h^{-1}\tau_\sigma(h)) \\
&= g\theta^{-1}(h^{-1}h\theta(g^{-1}\sigma(g))) \\
&= \sigma(g).
\end{aligned}$$

Since g was arbitrary, this shows that $\beta\alpha(\sigma) = \sigma$. However, as σ was arbitrary, $\beta\alpha = 1$. Similarly $\alpha\beta = 1$. Thus α is an isomorphism between $\mathrm{IA}_z(G)$ and $\mathrm{IA}_z(H)$.

It now remains to show that $\alpha(\mathrm{Aut}_c(G)) = \mathrm{Aut}_c(H)$. Let $\sigma \in \mathrm{Aut}_c(G)$.

To show that $\tau_\sigma \in \mathrm{Aut}_c(H)$, let $h \in H$ with $\varphi^{-1}(hZ(H)) = gZ(G)$. Then $\tau_\sigma(h) = h\theta(g^{-1}\sigma(g))$. However, σ is a class-preserving automorphism and so there exists an $a \in G$ such that $\sigma(g) = a^{-1}ga$. Hence, we have $\tau_\sigma(h) = h\theta([g,a])$. Suppose $\varphi(aZ(G)) = bZ(H)$, then by commutativity of the diagram in the definition of isoclinism we get $\tau_\sigma(h) = h[h,b]$, i.e., $\tau_\sigma(h) = b^{-1}hb$. This shows that $\tau_\sigma \in \mathrm{Aut}_c(H)$. So we have $\alpha(\mathrm{Aut}_c(G)) \le \mathrm{Aut}_c(H)$. Similarly we can show that $\beta(\mathrm{Aut}_c(H)) \le \mathrm{Aut}_c(G)$. We have already shown that $\alpha\beta = \beta\alpha = 1$, therefore $\alpha(\mathrm{Aut}_c(G)) = \mathrm{Aut}_c(H)$.

5.2 A necessary and sufficient condition for the equlity of $\mathrm{IA}_z(G)$ and $\mathrm{Autcent}(G)$

In the following theorem we give a necessary and sufficient condition to ensure that $\mathrm{IA}_z(G) = \mathrm{Autcent}(G)$, for a finite p-group G.

Theorem 5.2.1 *Let G be a finite p-group.*

1. *Then $\mathrm{IA}_z(G) = \mathrm{Autcent}(G)$ if and only if $\gamma_2(G) = Z(G)$.*

2. *If the nilpotency class of G is 2, then $\mathrm{IA}_z(G) = \mathrm{Inn}(G)$ if and only if $\gamma_2(G)$ is cyclic.*

Proof. (1) First suppose that $\gamma_2(G) = Z(G)$, then clearly $\mathrm{IA}(G) = \mathrm{Autcent}(G)$. Now each central automorphism fixes $\gamma_2(G) = Z(G)$ element-wise, therefore each IA automorphism fixes $Z(G)$ element-wise. This shows that $\mathrm{IA}_z(G) = \mathrm{Autcent}(G)$.

Conversely, suppose $\mathrm{IA}_z(G) = \mathrm{Autcent}(G)$. Then, since $\mathrm{Inn}(G) \le \mathrm{IA}_z(G)$, G must be a group of class 2. Now, we prove that G is purely non-abelian. Suppose to the contrary that $G = A \times N$, where A is non-trivial and abelian and N is purely non-abelian. Clearly $\mathrm{IA}_z(G) \cong \mathrm{IA}_z(N)$. Next, $|\operatorname{Autcent}(G)| > |\operatorname{Autcent}(A)||\operatorname{Autcent}(N)| \geq |\operatorname{Autcent}(N)|$. Therefore,

$$|\mathrm{IA}_z(G)| = |\mathrm{IA}_z(N)| \leq |\operatorname{Autcent}(N)| < |\operatorname{Autcent}(G)|,$$

which is a contradiction to the assumption that $\mathrm{IA}_z(G) = \operatorname{Autcent}(G)$. Hence G is purely non-abelian. Now by Theorem 1.3.1, there exists a group H isoclinic to G such that $Z(H) \leq \gamma_2(H)$. Since G is of class 2, H is also of class 2 and therefore $\gamma_2(H) = Z(H)$. By what we just proved, $\mathrm{IA}_z(H) = \operatorname{Autcent}(H)$. Now, since $Z(H) \leq \gamma_2(H)$, H is purely non-abelian, and hence by Theorem 1.2.5,

$$\begin{aligned} |\mathrm{IA}_z(H)| &= |\operatorname{Hom}(H/\gamma_2(H), Z(H))| \\ &= |\operatorname{Hom}(H/Z(H), \gamma_2(H))| \\ &= |\operatorname{Hom}(G/Z(G), \gamma_2(G))|. \end{aligned}$$

However, by Theorem 5.1.1, $|\mathrm{IA}_z(H)| = |\mathrm{IA}_z(G)|$, which, by the hypothesis and Theorem 1.2.5 equals $|\operatorname{Hom}(G/\gamma_2(G), Z(G))|$. Therefore, we have

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

It now follows from Lemma 1.1.10 that $\gamma_2(G) = Z(G)$.

(2) By Theorem 1.3.1, there exists a group H isoclinic to G such that $Z(H) \leq \gamma_2(H)$. Since G is of class 2, H is also of class 2 and $\gamma_2(H) = Z(H)$. Thus $\mathrm{IA}_z(H) = \operatorname{Autcent}(H)$ and hence by Theorem 1.2.5,

$$|\mathrm{IA}_z(H)| = |\operatorname{Hom}(H/Z(H), \gamma_2(H))|,$$

which in turn equals $|\operatorname{Hom}(G/Z(G), \gamma_2(G))|$ using the definition of isoclinism. Applying Theorem 5.1.1 we also have that $|\operatorname{IA}_z(H)| = |\operatorname{IA}_z(G)|$.

Now suppose that $\operatorname{IA}_z(G) = \operatorname{Inn}(G)$. Then

$$|\operatorname{IA}_z(G)| = |G/Z(G)| = |\operatorname{Hom}(G/Z(G), \gamma_2(G))|.$$

However, since G is of class 2, the exponents of $G/Z(G)$ and $\gamma_2(G)$ are the same. Hence the preceding equality gives that $\gamma_2(G)$ is cyclic.

Conversly, suppose that $\gamma_2(G)$ is cyclic. Then

$$|\operatorname{Hom}(H/Z(H), \gamma_2(H))| = |H/Z(H)| = |G/Z(G)| = |\operatorname{Inn}(G)|,$$

since $\gamma_2(G) \cong \gamma_2(H)$. This gives that $\operatorname{IA}_z(G) = \operatorname{Inn}(G)$.

The following corollary is a result of Curran and McCaughan [15], and is a consequence of Theorem 5.2.1.

Corollary 5.2.2 *Let G be a finite p-group. Then* $\operatorname{Inn}(G) = \operatorname{Autcent}(G)$ *if and only if* $\gamma_2(G) = Z(G)$ *and* $\gamma_2(G)$ *is cyclic.*

Bibliography

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

[2] S. Bachmuth, *Automorphisms of free metabelian groups*, Trans. Amer. Math. Soc. **118** (1965), 93-104.

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

[4] V. G. Bardakov, A. Y. Vesnin and M. K. Yadav, *Class preserving automorphisms of unitriangular groups*, Internat. J. Algebra Comput., **22** (2012), No. 3, DOI: 10.1142/ S0218196712500233.

[5] Y. Berkovich, Z. Janko, *Groups of prime power order - Volume 2* (Walter de Gruyter, Berlin, New York 2008).

[6] F. A. Bogomolov, *The Brauer group of quotient spaces by linear group actions*, Izv. Akad. Nauk SSSR Ser. Mat. **51** (1987), 485-516.

[7] F. A. Bogomolov, *The Brauer group of quotient spaces by linear group actions*, English transl. in Math. USSR Izv. **30** (1988), 455-485.

[8] P. A. Brooksbank and M.S. Mizuhara, *On groups with a class-preserving outer automorphism*. Involve, **7** (2013), No. 2, 171-179.

[9] W. Burnside, *Theory of groups of finite order*, 2nd Ed. Dover Publications, Inc., 1955. Reprint of the 2nd edition (Cambridge, 1911).

[10] W. Burnside, *On the outer automorphism of a p-group*, Proc. London Math. Soc. (2) **11** (1913), 40-42.

[11] Y. Chen and R. Ma, *Some groups of order p^6 with trivial Bogomolov multipliers*, (Available at arXiv:1302.0584v5).

[12] Y. Cheng, *On finite p-groups with cyclic commutator subgroup*, Arch. Math. **39**, 295-298 (1982).

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

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

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

[16] H. Chu, S. Hu, M. Kang and B. Kunyavskiĭ, *Noether's problem and the unramified Brauer groups for groups of order 64*, Intern. Math. Res. Notices **12** (2010), 2329-2366.

[17] B. E. Earnley, *On finite groups whose group of automorphisms is abelian* (Ph. D. thesis, Wayne State University, 1975), Dissertation Abstracts, V. 36, p. 2269 B.

[18] G. Ellis, *GAP package HAP - Homological Algebra Programming, Version 1.10.15*; 2014, (http://www.gap-system.org/Packages/hap.html).

[19] G. Endimioni, *Automorphisms fixing every normal subgroup of a nilpotent-by-abelian group*, Rend. Sem. Mat. Univ. Padova **120**, 73-77 (2008).

[20] W. Feit and G. M. Seitz, *On finite rational groups and related topics*, Illinois J. Math. **33** (1989), no. 1, 103-131.

[21] S. Franciosi and F. de Giovanni, *On automorphisms fixing normal subgroups of nilpotent groups*, Boll. Un. Mat. Ital. **B7**, 1161-1170 (1987).

[22] M. Fuma and Y. Ninomiya, *"Hasse principle" for finite p-groups with cyclic subgroups of index* p^2, Math. J. Okayama Univ. **46** (2004), 31-38.

[23] *The GAP Group, GAP - Groups, Algorithms, and Programming* (Version 4.4.12, 2008) (http://www.gap-system.org).

[24] The GAP Group, GAP - *Groups, Algorithms, and Programming, Version 4.7.2*; 2013, (http://www.gap-system.org).

[25] D. Gumber and M. Sharma, *Class-preserving automorphisms of some finite p-groups*, arXiv:1407.5921.

[26] P. Hall, *The classification of prime power groups*, J. Reine Angew. Math. **182** (1940), 130-141.

[27] P. Hegarty, *Minimal abelian automorphism groups of finite groups*, Rend. Sem. Mat. Univ. Padova **94** (1995), 121 - 135.

[28] H. Heineken, H. Liebeck, *The occurrence of finite groups in the automorphism group of nilpotent groups of class* 2, Arch. Math. (Basel) **25** (1974), 8 - 16.

[29] H. Heineken, *Nilpotente Gruppen, deren samtliche Normalteiler charakteristisch sind*, Arch. Math. (Basel) **33** (1979/80), 497 - 503.

[30] A. Herman and Y. Li, *class preserving automorphisms of Blackburn groups*, J. Aust. Math. Soc. **80** (2006), 351-358.

[31] M. Hertweck, *Contributions to the integral representation theory of groups*, Habilitationss-chrift, University of Stuttgart (2004). Available at http://elib.uni-stuttgart.de/opus/volltexte/2004/1638.

[32] M. Hertweck, *Class-preserving automorphisms of finite groups*, J. Algebra **241** (2001), 1-26.

[33] H. Hilton, *An introduction to the theory of groups of finite order* (Oxford, Clarendon Press,1908).

[34] C. Hopkins, *Non-abelian groups whose groups of isomorphisms are abelian*, The Annals of Mathematics, 2nd Ser., **29**, No. 1/4. (1927 - 1928), 508-520.

[35] M. H. Jafari, *Elementary abelian p-groups as central automorphism groups*, Comm. Algebra **34** (2006), 601 -607.

[36] Vivek K. Jain, Pradeep K. Rai and Manoj K. Yadav, *On finite p-groups with abelian automorphism group*, Internat. J. Algebra Comput., Vol. 23, no. 35, (2013), 1063-1077

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

[38] A. Jamali, Some new non-abelian 2-groups with abelian automorphism groups, *J. Group Theory*, **5** (2002), 53 - 57.

[39] R. James, *The groups of order p^6 (p an odd prime)*, Math. Comp. **34** (1980), 613-637.

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

[41] M. Kang, B. Kunyavskiĭ, *The Bogomolov multiplier of rigid finite groups*, Arch. Math., **102** (2014), 209-218.

[42] M. Kumar and L. R. Vermani, *"Hasse principle" for extraspecial p-groups*, Proc. Japan Acad. Ser. A Math. Sci. **76** (2000), 123-125.

[43] M. Kumar and L. R. Vermani, *"Hasse principle" for groups of order p^4*, Proc. Japan Acad. Ser. A Math. Sci. **77** (2001), 95-98.

[44] M. Kumar and L. R. Vermani, *On automorphisms of some p-groups*, Proc. Japan Acad. Ser. A Math. Sci. **78** (2002), 46-50.

[45] B. Kunyavskiĭ, *Local-global invariants of finite and infinite groups: Around Burnside from another side*, Expo. Math. **31** (2013), 256-273.

[46] H. Kurzweil and B. Stellmacher, *The theory of finite groups*, Springer-Verlag, (2004).

[47] R. Laue, *On outer automorphism groups*, Math. Z. **148** (1976), 177-188.

[48] A. Mahalanobis, *The Diffie-Hellman Key Exchange Protocol and non-abelian nilpotent groups*, Israel J. Math., **165** (2008), 161 - 187.

[49] I. Malinowska, *On quasi-inner automorphisms of a finite p-group*, Publ. Math. Debrecen **41** (1992), No. 1-2, 73-77.

[50] I. Malinowska, *p-automorphisms of finite p-groups: problems and questions*, Advances in Group Theory (1992), 111-127.

[51] G. A. Miller, A non-abelian group whose group of isomorphism is abelian, *Mess. of Math.* **43** (1913-1914), 124 - 125.

[52] P. Moravec, *Groups of order p^5 and their unramified Brauer groups*, J. Algebra **372** (2012), 320-327.

[53] P. Moravec, *Unramified Brauer groups and isoclinism*, Ars Math. Contemp. 7 (2014), 337-340.

[54] M. Morigi, *On p-groups with abelian automorphism group*, Rend. Sem. Mat. Univ. Padova **92** (1994), 47 - 58.

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

[56] M. V. Neshadim, *Free products of groups have no outer normal automorphisms*, Algebra and logic **35** (1996), 316-318.

[57] T. Ono, *"Shafarevich-Tate sets" for profinite groups*, Proc. Japan Acad. Ser. A **75** (1999), 96-97.

[58] T. Ono and H. Wada, *"Hasse principle" for free groups*, Proc. Japan Acad. Ser. A **75** (1999), 1-2.

[59] T. Ono and H. Wada, *"Hasse principle" for symmetric and alternating groups*, Proc. Japan Acad. Ser. A **75** (1999), 61-62.

[60] P. K. Rai, *On class-preserving automorphisms of groups*, Ricerche Mat., Vol. 63, no. 2, (2014), 189-194.

[61] P. K. Rai, *On nilpotency of the group of outer class-preserving automorphisms of a group*, Accepted for publication in J. Algebra Appl..

[62] P. K. Rai, *On IA-automorphisms that fix the center element-wise*, Proc. Indian Acad. Sci. (Math. Sci.) Vol. 124, no. 2, (2014), 169-173.

[63] P. K. Rai and M. K. Yadav, *On* Ш*-rigidity of groups of order* p^6, J. Algebra, Vol. 428, (2015), 26-42.

[64] D. J. S. Robinson, *A course in the theory of groups*, Springer-Verlag (1996).

[65] C. H. Sah, *Automorphisms of finite groups*, Journal of Algebra **10**, 47-68 (1968).

[66] D. J. Saltman, *Noether's problem over an algebraically closed field*, Invent. Math. **77** (1984), 71-84.

[67] D. J. Saltman, *The Brauer group and the center of generic matrices*, J. Algebra **97** (1985) 53-67.

[68] R. R. Struik, *Some non-abelian* 2*-groups with abelian automorphism groups*, Arch. Math. (Basel) **39** (1982), 299 - 302.

[69] F. Szechtman, *n-inner automorphisms of finite groups*, Proc. Amer. Math. Soc. **131** (2003), 3657-3664.

[70] J. Tappe, *On isoclinic groups*, Math. Z. **148** (1976), 147-153.

[71] G. E. Wall, *Finite groups with class preserving outer automorphisms*, J. London Math. Soc. **22** (1947), 315-320.

[72] M. K. Yadav, *Class preserving automorphisms of finite p-groups*, J. London Math. Soc. **75(3)** (2007), 755-772.

[73] M. K. Yadav, *Class preserving automorphisms of finite p-groups - A Survey*, Proc. Groups St. Andrews (Bath) 2009, LMS Lecture Note Series **388** (2011), 569 - 579.

[74] M. K. Yadav, *On automorphisms of some finite p-groups*, Proc. Indian Acad. Sci. (Math. Sci.) **118(1)** (2008), 1-11.