EXISTENCE OF NONINNER AUTOMORPHISMS OF ORDER p IN SOME FINITE p-GROUPS

Thesis Submitted In Partial Fulfillment of The Requirements for

The Award of Degree of

Masters of Science

in

Mathematics & Computing

Submitted by

Shivani

Under the Guidance of

Dr. Hemant Kalra

Assistant Professor

School of Mathematics

THAPAR UNIVERSITY

PATIALA - 147004, INDIA

July, 2017

Certificate

It is certified that the work contained in this thesis entitled " **EXISTENCE OF NONINNER AUTOMORPHISMS OF ORDER p IN SOME FINITE p-GROUPS** " in partial fulfillment of the requirements for the award of degree of Master of Science in Mathematics and Computing to the School of Mathematics, Thapar University, Patiala is an authentic record of my own work studied under the supervision of Dr. Hemant Kalra.

The matter embodied in this thesis has not been submitted by me for the award of any other degree of this or any other University/Institute.

Shivani

Shivani

(Roll No. 301503027)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

Hemant Kalra

Dr. Hemant Kalra

Assistant Professor,

Thapar University, Patiala.

Acknowledgement

I feel privileged to express my sincere regards and gratitude to all those people who helped in completion of this thesis which marks the end of my beautiful and memorable journey to achieve Master's degree.

My first and sincere appreciation goes to Dr. Hemant Kalra, my supervisor for all I have learned from him and for his continuous help and support in all stages of this thesis. His insights and clarity of thoughts have been present at every moment of this work and I owe a great intellectual debt to him. I would like to thank him for encouraging and helping me to shape my interests and ideas. Also, i would like to thank Dr. A.K. Lal, Head of Department, Thapar University,Patiala. Their advices and discussions were valuable and their attitude towards research always inspired me.

I express my gratitude to all the faculty members and staff of the Department of Mathematics, Thapar University, for their support. Above all I would like to thank my parents for their love, blessings and support. I would also like to thank my friends for their moral support that helped me to work harder each day and finally, I thank and pay my regards to the Almighty for his love and blessings.

Abstract

A long standing conjecture [10, Problem 4.13] asserts that every finite non-abelian p-group has a noninner automorphism of order p. The work presented in this dissertation has been divided into three chapters. The first chapter is introductory. In chapter II, apart from setting up the notations and terminology to be used in sequel, we have presented some known results inter-related to our result. In chapter III, we studied the main results of Attar[14]. In the first theorem we prove the validity of the conjecture for the following cases:
(1) $\Phi(G)$ *is cyclic* ;
(2) exp(G) $=p^{m-2}$;
(3) $s = \text{rank(Z(G))} \geq (m-1)/2$, where $|G| = p^m$;
(4) $s = \text{rank(Z(G))} \geq 2$ *and* $[G : Z(G)] \leq p^4$.
In the second theorem, we show that a finite p-group of maximal class has at least $p(p-1)$ noninner automorphisms of order p which fix $\Phi(G)$ elementwise.

Contents

CHAPTER 1

1 Introduction

Let G be a finite group. The set of all the automorphisms of G is denoted by Aut(G). An automorphism β of G is said to be inner if for all $g \in G$, there exist a fix $a \in G$ such that $\beta(y) = a^{-1}ya$. The set of all inner automorphisms of G is denoted by Inn(G). An automorphism which is not inner is called a noninner automorphism.

Throughout this thesis, G denotes a finite group unless or otherwise stated. A long standing conjecture [10, Problem 4.13] asserts that every finite non-abelian p-group has a noninner automorphism of order p. This conjecture was first attacked by Lieback [9] in 1965. He proved that every finite p-group(p odd) of class 2 has a noninner automorphism of order p which fixes $\Phi(G)$ elementwise. For 2 groups of class 2, Abdollahi [1] proved that these groups have a noninner automorphism of order 2 fixing $\Phi(G)$ or $\Omega_1(Z(G))$ elementwise. Abdollahi [3],[2] proved the validity of the conjecture for finite p-groups of nilpotency class 3 or $G/Z(G)$ is powerful. Jamali and Viseh [8] proved that every finite 2-group with cyclic commutator subgroup has a noninner automorphism of order 2 fixing $\Phi(G)$ elementwise. If G is a finite p-group and M is a proper normal subgroup of G, then (G,M) is said to be a camina pair if for all $x \in G\backslash M$, $xM \subseteq x^G$. Ghoraishi [6] proved the validity of the conjecture for finite p-group G, where p is an odd prime, such that $(G, Z(G))$ is a Camina pair. Deaconescu and Silberberg [5] proved that if G is a finite p-group such that $C_G(Z\Phi(G)) \neq \Phi(G)$, then G has a noninner automorphism of order p leaving $\Phi(G)$ fixed elementwise. This reduced the verification of the conjecture to degenerate case in which $C_G(Z\Phi(G)) = \Phi(G)$. In [14,Theorem], Attar proved the validity of the conjecture for finite p-groups of maximal class.

In this dissertation, we prove main results of Attar [14]. In the first theorem we prove the validity of the conjecture for the following cases:

(1) $\Phi(G)$ *is cyclic* ;
(2) exp(G) $=p^{m-2}$;
(3) $s = \text{rank(Z(G))} \geq (m-1)/2$, where $|G| = p^m$;
(4) $s = \text{rank(Z(G))} \geq 2$ *and* $[G : Z(G)] \leq p^4$.
In the second theorem, we show that a finite p-group of maximal class has at least $p(p-1)$ noninner automorphisms of order p which fix $\Phi(G)$ elementwise.

CHAPTER 2

2 Preliminaris and Notations

Definition 2.0.1. (Commutator) Let x and y be two elements of a group G. The **commutator** of x and y is denoted by $[x, y]$ and is defined as :

$$[x, y] = x^{-1}y^{-1}xy.$$

The higher commutators are defined inductively as :

$[x_1, x_2, ..., x_k] = [[x_1, x_2, ..., x_{k-1}], x_k]$, where $k > 2$ and $x_i \in G$ for $1 \leq i \leq n$.

Definition 2.0.2. (Subgroup generated by a subset of a Group) Let B be a subset of a group G. A subgroup A of G is said to be generated by B if it satisfies the following conditions:

1. $B \subseteq A$.

2. If X is any subgroup of G containing B, then $A \subseteq X$.

It is the intersection of family of subgroups of G that contain B and is denoted by $\langle B \rangle$.

Definition 2.0.3. (Commutator Subgroup) The **commutator subgroup** or the **derived subgroup** is the subgroup generated by the commutators of elements of G, denoted by

$$G' = [G, G] = \langle [x, y] : x, y \in G \rangle.$$

Definition 2.0.4. (Homomorphism) Given two groups $(G, *)$ and $(H, .)$, a group homomorphism from $(G, *)$ to $(H, .)$ is a function $f : G \longrightarrow H$ such that for all $x, y \in G$,

$$f(x * y) = f(x).f(y).$$

Definition 2.0.5. (Isomorphism) Let $(G, *)$ and $(H, .)$ be two groups. We say that G and H are isomorphic if there is a bijective map $f : G \to H$, which respects the group structure. That is to say, for every g and h in G,

$$f(g * h) = f(g).f(h).$$

The map f is called an isomorphism. The isomorphic groups G and H are denoted by $G \cong H$.

Definition 2.0.6. (Automorphism) An Automorphism of a group G is an isomorphism of G onto G. The set of all automorphisms of G is denoted by Aut(G).

Theorem 2.0.1. *The set Aut(G) of all automorphisms of a group G forms a group under composition of mappings.*

Proof. Let Aut(G) be the collection of all automorphisms of a group G. That is Aut(G) = {f : f is an automorphism of G }. We prove that (Aut(G), .) forms a group.

(1) **Closure property:** Let $f, g \in$ Aut(G) and $h = fg$. Now, h is a bijection since it is a composition of two bijective functions.

Thus we need to show that $h(ab) = h(a)h(b)$ for all $a, b \in G$.

Consider,

$$h(ab) = fg(ab) = f(g(ab)) = f(g(a)g(b)) = f(g(a))f(g(b)) = h(a)h(b)$$

thus, h is an automorphism of G.

(2) **Associativity :** We know that composition of mappings is associative i.e. for f, g and $h \in \text{Aut(G)}, (fg)h = f(gh)$. Therefore, composite of automorphisms is associative.

(3) **Existence of Identity :** The identity function $i : G \to G$ is defined as $i(x) = x$ for all $x \in G$. Clearly, it is one-one, onto map that preserves adjacency i.e. $i(ab) = i(a)i(b)$ for all $a, b \in G$. Thus i is an automorphism.

For any $f \in \text{Aut(G)}$, there exists $i \in \text{Aut(G)}$ such that $fi = if = f$. Thus i is an identity element of Aut(G).

(4) **Existence of inverse :** Let $f \in \text{Aut(G)}$. Since f is a one-one map of G onto itself, f^{-1} exists and it maps from $G \to G$ such that $ff^{-1} = f^{-1}f = i$. We need to show that $f^{-1} \in \text{Aut(G)}$. The map f^{-1} is a bijection as it is inverse of bijective function.

Next we need to show that: $f^{-1}(ab) = f^{-1}(a)f^{-1}(b)$ for all $a, b \in G$.

Let $a, b \in G$. Then there exists $a', b' \in G$ such that :

$$f^{-1}(a) = a' \implies f(a') = a$$

and

$$f^{-1}(b) = b' \implies f(b') = b$$

Therefore,

$$f(a'b') = f(a')f(b') = ab$$

$$\implies f^{-1}(ab) = a'b' = f^{-1}(a)f^{-1}(b)$$

Thus, $f^{-1}(ab) = f^{-1}(a)f^{-1}(b)$ for all $a, b \in G$. Therefore, f^{-1} is an automorphism i.e. $f^{-1} \in \text{Aut(G)}$. So, each element of Aut(G) possesses

inverse. Thus, Aut(G) forms a group with respect to composite composition and is referred to as group of automorphisms of G. □

Definition 2.0.7. (Inner Automorphism) Let G be a group and a be fixed element of G. Then the mapping $f_a : G \to G$ defined by

$$f_a(x) = x^a = a^{-1}xa$$

for all $x \in G$ is called the inner automorphism of G determined by a. The set of all inner automorphisms of G is denoted by Inn(G).

Theorem 2.0.2. *Inner automorphisms of a group G form a subgroup of* Aut(G).

Proof. Clearly Inn(G) is nonempty, $i \in$ Inn(G) as

$$i(x) = x = exe^{-1} = f_e(x) \; for \; all \; x \in G.$$

For any $f_a, f_b \in$ Inn(G) simple computation shows that $f_a \circ f_b = f_{ab} \in$ Inn(G).

Now for any two elements, a, x in G,

$$f_a \circ f_{a^{-1}}(x) = f_a[f_{a^{-1}}(x)] = f_a(a^{-1}xa) = a(a^{-1}xa)a^{-1} = x = i(x)$$

thus, $f_a \circ f_{a^{-1}} = i$
Similarly $f_{a^{-1}} \circ f_a = i$.
Thus, $f_{a^{-1}} \circ f_a = i = f_a \circ f_{a^{-1}}$ and hence $(f_a)^{-1} = f_{a^{-1}} \in$ Inn(G).

□

Definition 2.0.8. (p-Group) A Group G is said to be a p-group if each element of G is of order a power of some fixed prime number p.
Example: Dihedral group $D_8 = \langle a^4 = 1, b^2 = 1, ba = a^{-1}b \rangle$ is a 2-group.

Elements of D_8 are $\{a, a^2, a^3, 1, b, ab, a^2b, a^3b\}$.
Here, $|a| = |a^3| = 4$, $|a^2| = |b| = |ab| = |a^2b| = |a^3b| = 2$.

Definition 2.0.9. (**Elementary Abelian p-group**) An abelian p-group G is said to be elementary abelian, if order of each non-trivial element of G is p.

Definition 2.0.10. (Rank of a Group) The rank of a group G, denoted by $rank(G)$, refer to the smallest cardinality of a generating set for G, that is

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

Remark: $Rank(D_8) = 2$.

Definition 2.0.11. (Powerful p-group) A finite p-group G is called **powerful** if the commutator subgroup $G' = [G, G]$ is contained in the subgroup $G^p = \{g^p | g \in G\}$ for odd p, or if G' is contained in the subgroup G^4 for $p = 2$.

Definition 2.0.12. (Centre of a group) The centre of a group G, denoted by $Z(G)$ is the set of elements in G that commute with every element of G. Symbolically,

$$Z(G) = \{a \in G |\ ax = xa \text{ for all } x \in G\}.$$

Example: Centre of quaternion group Q_8

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

is { 1,-1 }.

Definition 2.0.13. (Conjugacy Class) Any two elements $a, b \in G$ are called conjugate if there exists an element $g \in G$ with

$$g^{-1}ag = b.$$

It can be easily seen that the relation of conjugacy among the elements of G is an equivalence relation and it partitions G into equivalence classes.
Equivalence class of an element $a \in G$ is defined as

$$Cl(a) = \{b \in G | \text{ there exists } g \in G \text{ with } b = g^{-1}ag\}$$

and is called the **conjugacy class of a**.

Definition 2.0.14. (Centralizer) Let A be a non-empty subset of G, then

$$C_G(A) = \{x \in G | \ xa = ax \text{ for all } a \in A\}.$$

Clearly, $C_G(A)$ forms a subgroup of G.
In particular, the centralizer of an element g of a group G is the set of elements of G which commute with g,

$$C_G(g) = \{x \in G | \ xg = gx\}.$$

Remark: Number of conjugates of g in the group G is $[G : C_G(x)]$.

Definition 2.0.15. (The class equation) For any finite group G,

$$|G| = \sum_x [G : C_G(x)],$$

where the sum runs over one element x from each conjugacy class of G.

Lemma 2.0.3. *If G is a nontrivial finite p-group, then G has a nontrivial centre.*

Proof. Let $x \in G$ be any element, then $Cl(x) = x$ if and only if $x \in Z(G)$. Thus, by extracting out these elements, the class equation can be written in the form

$$|G| = |Z(G)| + \sum_{x \in X} [G : C_G(x)] \tag{2.1}$$

where X is the subset of G containing exactly one element from each non-central conjugacy of G.

By Lagrange's theorem, $|C_G(x)| \mid |G|$. Now, $x \in Z(G)$ if and only if $C_G(x) = G$.
If $x \notin Z(G)$, then $C_G(x) < G$ and since, G is a finite p-group, $|G| = p^n$.

Thus, $|C_G(x)| \leq p^{n-1}$, which implies that $\frac{|G|}{|C_G(x)|} \geq p$.

So, $[G : C_G(x)] \geq p$, which implies $p \mid [G : C_G(x)]$. Therefore, p divides $\sum_{x \in X}[G : C_G(x)]$.
Thus, p divides $|G| - \sum_{x \in X}[G : C_G(x)]$. It follows from (2.1), that p divides $|Z(G)|$ and hence $|Z(G)| \neq 1$.

□

Theorem 2.0.4. *In a p-group, $Z(G) \cap N$ is non-empty, where N is any non-trivial normal subgroup of G.*

Proof. From class equation, we have

$$G = Z(G) \cup (\cup_{a \in X} Cl(a))$$
$$N = N \cap G = N \cap (Z(G) \cup (\cup_{a \in X} Cl(a))$$
$$= (N \cap Z(G)) \cup (N \cap ((\cup_{a \in X} Cl(a)))$$

Hence,

$$|N| = |Z(G) \cap N| + \sum_{a \in X} |Cl(a) \in N| \tag{2.2}$$

If $a \in N$, then $Cl(a) \subset N$, so $Cl(a) \cap N = Cl(a)$.
Suppose that $a \notin N$ and $Cl(a) \cap N \neq \phi$. Let $y \in Cl(a) \cap N$. Then, $y \in Cl(a)$ and $y \in N$. Let $y = g^{-1}ag$, for some $g \in G$. Then $g^{-1}ag \in N \Longrightarrow$

$g(g^{-1}ag)g^{-1} = a \in N$, a contradiction. So, $Cl(a) \cap N = \phi$.

Thus, $Cl(a) \cap N = Cl(a)$ or ϕ for all $a \in X$.
$\implies |Cl(a) \cap N|$ is 0 or $|Cl(a)|$.
$\implies |Cl(a) \cap N|$ is 0 or $[G : C_G(a)]$

But, $p \mid [G : C_G(a)]$ for all $a \in X$. So, $p \mid |Cl(a) \cap N|$ for all $a \in X$.

$\implies$

$$p| \sum_{a \in X} |Cl(a) \cap N|$$

Also, $p \mid |N|$. Therefore, it follows from (2.2) that,

$$p \mid |Z(G) \cap N|$$

and hence $Z(G) \cap N$ is non-trivial. □

Definition 2.0.16. (Non Generator) An element $g \in G$ is a non generator if whenever $\langle X \cup g \rangle = G$, we have $\langle X \rangle = G$ for $X \subseteq G$.

Definition 2.0.17. (Maximal Subgroup) A subgroup H of a group G is said to be **maximal subgroup** if $H \neq G$ and there does not exist any subgroup K of G such that $H < K < G$.
Example: In $S_n (n > 2)$, A_n is a maximal normal subgroup.

Definition 2.0.18. (Characteristic Subgroup) A subgroup H of a group G is said to be characteristic subgroup if for every automorphism f of G, $f(H) \subseteq H$.
Thus, a **characteristic subgroup** is the one which is invariant under every automorphism of G.

Definition 2.0.19. (Frattini subgroup) Let G be a finite group. The frattini subgroup is the intersection of all maximal subgroups of G and is denoted by $\Phi(G)$.
If G has no maximal subgroup then $\Phi(G) = G$.

Theorem 2.0.5. *For all finite groups G, the set of non-generators of G equals the Frattini subgroup of G. Consequently, if $G = H\Phi(G)$ for some H, then $G = H$.*

Proof. Suppose a is a non-generator of G and H is a maximal subgroup. If $a \notin H$, then $\langle H, a\rangle > H$, and so by maximality $\langle H, a\rangle = G$. But a is a nongenerator, and hence $H = G$ which contradicts the maximality of H (maximal subgroups are always proper).
Therefore $a \in H$, and as this holds for all maximal subgroups H, we also have $a \in \Phi(G)$.
Conversely: Suppose $a \in \Phi(G)$, so a belongs to all maximal subgroups of G. We will show that a is a non-generator. Assume that, for some set X, $a \notin X$ and $\{a\} \cup X$ generates G.
If $\langle X\rangle \neq G$, then there exists a maximal subgroup J of G which contains $\langle X\rangle$, possibly $\langle X\rangle$ itself, that is, $\langle X\rangle \leq J < G$.

By supposition, $a \in J$ and so $\langle a, X\rangle \leq J$. But $\langle a, X\rangle = G$, hence $G \leq J$ which is impossible. Hence $\langle X\rangle = G$ and a is a non-generator. Finally, let

$$G = H\Phi(G) = \langle H, \Phi(G)\rangle$$

so, $G = \langle H\rangle = H \Longrightarrow G = H$.

□

Theorem 2.0.6. *Let G be a group and $\Phi(G)$ denotes the Frattini subgroup of G. Then $\Phi(G)$ is Characteristic subgroup of G.*

Proof. Let H be a maximal subgroup of G and α is an automorphism of G, and let K be any subgroup of G such that $\alpha(H) < K \Longrightarrow H < (\alpha)^{-1}(K)$. Thus $(\alpha)^{-1}(K) = G$ by the maximality of H. Therefore, $K = G$ and hence $\alpha(H)$ is a maximal subgroup of G.
Consider $M = \{K|\ K$ is a maximal subgroup of $G\ \}$. Now, each automorphism α of G induces a bijective map from M to itself which means that

for every $H \in M$, $\alpha(H) \in M$. Thus, for every automorphism α of G, we have

$$\alpha(\Phi(G)) = \alpha(\bigcap_{H \text{ maximal in } G} H) = \bigcap_{H \text{ maximal in } G} (\alpha(H))$$

which is the same as intersection of all maximal subgroups H of G. Thus, $\Phi(G)$ is characteristic. □

Lemma 2.0.7. *Let M be a normal subgroup of G then G/M is abelian if and only if $G' \leq M$.*

Proof. Let G/M be abelian and for any two elements $a, b \in G$, we have

$$\begin{aligned} (aM)(bM) &= (bM)(aM) \\ \implies (ab)M &= (ba)M \\ \implies (ba)^{-1}(ab)M &= M \\ \implies (ba)^{-1}(ab) &\in M \\ \implies a^{-1}b^{-1}ab &\in M \\ \implies [a,b] &\in M \end{aligned}$$

Therefore, $G' \leq M$.
Conversely, let $G' < M$ and $aM, bM \in G/M$ be any two elements.
Since, $G' < M$, $[a,b] \in M$

$$\begin{aligned} \implies a^{-1}b^{-1}ab &\in M \\ \implies a^{-1}b^{-1}abM &= M \\ \implies (aM)^{-1}(bM)^{-1}aMbM &= M \\ \implies aMbM &= bMaM \end{aligned}$$

Thus, G/M is abelian.

□

Theorem 2.0.8. *Let G be a finite p-group. Then $G/\Phi(G)$ is elementary abelian.*

Proof. Since every maximal subgroup M of a p-group is normal and of index p i.e. $[G : M] = p$, G/M is a cyclic group of order p. Hence $G' \leq M$ for all maximal subgroups M by Lemma 2.0.7. Also, $\Phi(G)$ is the intersection of all maximal subgroups, thus $G' \leq \Phi(G)$ and hence by Lemma 2.0.7, $G/\Phi(G)$ is abelian.
Also, since G/M has order p, $(Mx)^p = M$ for all $x \in G$, which implies that $x^p \in M$ for all $x \in G$ and this holds for every maximal subgroup M of G. Thus, $x^p \in \Phi(G)$ and hence every element of $G/\Phi(G)$ is order p. Thus $G/\Phi(G)$ is elementary abelian.
Remark: It follows from the proof of above theorem that for a finite p-group G, $G' \leq \Phi(G)$.

□

Definition 2.0.20. (Normal Series) A subnormal series of a group G is a chain of subgroups,

$$1 = A_0 \lhd A_1 \lhd A_2 ..... \lhd A_n = G$$

where each A_i is a normal subgroup of A_{i+1} and not necessarily of G. Each quotient group A_{i+1}/A_i are called the **factor groups** of the series.
If in addition each A_i is normal in G, then the series is called a **normal series**.

Definition 2.0.21. (Lower Central Series) In any arbitrary group G, we define subgroups $\gamma_i(G)$ as:

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

for $i \geq 1$. Observe that $\gamma_2(G) = G'$, each $\gamma_i(G)$ is normal in G and $\gamma_{i+1}(G) \leq \gamma_1(G)$.

Thus, the series

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \gamma_3(G) \geq ...$$

is known as the **lower central series** of G.

Example: In dihedral group D_8, lower central series is:

$$G = \gamma_3(G) \geq \gamma_2(G) \geq 1.$$

Here, $\gamma_2(G) = \{a^2, 1\} = G'$.

Definition 2.0.22. (Upper central series) The upper central series of G, denoted by $Z_i(G)$ for $i \geq 0$ is the chain of subgroups defined by

$$Z_0(G) = 1;$$

$$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$$

where each $Z_i(G) \lhd G$. Then $Z(G/Z_i(G))$ is a normal subgroup of $G/Z_i(G)$. So corresponds to a normal subgroup $Z_{i+1}(G)$ of G containing $Z_i(G)$. In this way we define a chain of subgroups

$$1 = Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq ....$$

each of which is normal in G. Here $Z_1(G) = Z(G)$.

The subgroup $Z_i(G)$ is called the i^{th}*centre* of G and the sequence is called **upper central series.**

Definition 2.0.23. (Nilpotent Group) A group G is said to be **nilpotent** if $\gamma_{c+1}(G) = 1$ for some c. The least such c is the **nilpotency class** of G.

(1) If G is abelian, then $\gamma_2(G) = \{e\}$.

Definition 2.0.24. (Group of Maximal Class) A finite p-group G of order p^{n+1} is said to be of maximal class if nilpotency class of G is n.

Example: Dihedral group D_8 is of nilpotency class 2.

Lemma 2.0.9. *If $\phi : G \longrightarrow K$ is a surjective homomorphism, then $\gamma_i(G)\phi = \gamma_i(K)$ for all i.*

Proof. By Induction on i. Note that $\gamma_1(G)\phi = G\phi = K = \gamma_1(K)$.
Suppose $\gamma_i(G)\phi = \gamma_i(K)$. If $x \in \gamma_i(G)$ and $y \in G$, then

$$[x, y]\phi = [x\phi, y\phi] \in [\gamma_i(G)\phi, G\phi] = [\gamma_i(K), K] = \gamma_{i+1}(K)$$

so, $\gamma_{i+1}(G)\phi = [\gamma_i(G), G]\phi \leq \gamma_{i+1}(K)$.
On the other hand, if $a \in \gamma_i(K)$ and $b \in K$, then $a = x\phi$ and $b = y\phi$ for some $x \in \gamma_i(G)$ and $y \in G$. So,

$$[a, b] = [x\phi, y\phi] = [x, y]\phi \in [\gamma_i(G), G]\phi = \gamma_{i+1}(G)\phi$$

thus, $\gamma_{i+1}(K) = [\gamma_i(K), K] \leq \gamma_{i+1}(G)\phi$.
Therefore,

$$\gamma_i(G)\phi = \gamma_i K \text{ for all } i.$$

□

Theorem 2.0.10. *Every finite p-group is nilpotent.*

Proof. Let G be a finite p-group and $|G| = p^n$. We proceed by induction on $|G|$.
If $|G| = 1$, then $\gamma_1(G) = G = 1$, so G is nilpotent of class 1.
Now, suppose $|G| = p^n$. By Lemma 2.0.3 $Z(G) \neq 1$. Since $Z(G)$ is non-trivial and normal subgroup of G, we consider the quotient group $G/Z(G)$. This is a p-group of order smaller than $|G|$, so by induction it is nilpotent, say

$$\gamma_{c+1}(G/Z(G)) = 1$$

Let $\pi : G \longrightarrow G/Z(G)$ be the natural homomorphism. Then, by using Lemma 2.0.9

$$\gamma_{c+1}(G)\pi = \gamma_{c+1}(G/Z(G)) = 1$$

so, $\gamma_{c+1}(G) \leq ker\pi = Z(G)$. Thus,

$$\gamma_{c+2}(G) = [\gamma_{c+1}(G), G] \leq [Z(G), G] = 1.$$

Thus G is nilpotent. □

Definition 2.0.25. (Internal Direct Product) Let $H_1, H_2, ..., H_k$ be the subgroups of a group G. We say that G is the internal direct product of $H_1, H_2, ..., H_k$ if it satisfies the following conditions:
1. $H_i \lhd G$ for all $i = 1, 2, ..., k$
2. $G = H_1H_2..H_k$.
3. $H_i \cap (H_1H_2...\bar{H}_i...H_k) = 1$, where $H_1H_2...\bar{H}_i...H_k$ means the product of all H_j excluding H_i.

If G is the internal direct product of $H_1, H_2, ..., H_k$ then $G \cong H_1 \times H_2 \times .... \times H_k$.

Lemma 2.0.11. *Let G is a finite abelian p-group and a be any element of maximal order. If $o(a) = p^k$ then $x^{p^k} = e$ for all $x \in G$.*

Theorem 2.0.12. *Let G be a finite abelian p-group and a be an element of maximal order in G. Then there is a subgroup H of G such that $G \cong \langle a \rangle \times H$.*

Proof. Let $a \in G$ be an element of maximal order, say $o(a) = p^k$. Consider all subgroups K of G such that $\langle a \rangle \cap K = \{e\}$. Let H be maximal with respect to these subgroups.
That is, if $H < K \leq G$, then $\langle a \rangle \cap K \neq \{e\}$. Since G is abelian, all subgroups are normal. Moreover $\langle a \rangle \cap H = \{e\}$ by definition.
Therefore to prove that $G \cong \langle a \rangle \times H$, we only need to show that $G = \langle a \rangle H$.
Suppose $G \neq \langle a \rangle H$, then there exists $y \in G$ such that $y \notin \langle a \rangle H$.
Let $r = min\ \{m \in N |\ y^{p^m} \in \langle a \rangle H\}$. By Lemma 2.0.11, $y^{p^k} = \{e\} \in H$, so $r \leq k$. Let $x = y^{p^{r-1}}$. So $x \notin \langle a \rangle H$ since r was the smallest such power.
However, $x^p = y^{p^r} \in \langle a \rangle H$. Therefore, we have found an element $x \in G$ such that $x \notin \langle a \rangle H$, but $x^p \in \langle a \rangle H$.

Since $x^p \in \langle a \rangle H$, we have $x = a^q h$ for some $q \in Z$, $h \in H$. Again using above Lemma 2.0.11, we get the following

$$e = x^{p^k} = (x^p)^{p^{k-1}} = (a^q h)^{p^{k-1}} = a^{qp^{k-1}} h^{p^{k-1}}$$

Hence, $a^{qp^{k-1}} = h^{(-p)^{k-1}} \in H$. However $a^{qp^{k-1}} \in \langle a \rangle \cap H = \{e\}$. Therefore, $a^{qp^{k-1}}$ implies $o(a) \mid qp^{k-1}$, and since $o(a) = p^k$, so $p^k \mid qp^{k-1}$ which implies $p \mid q$.
So, $q = ps$ for some $s \in z$. Also since, $x \notin \langle a \rangle H$, so $xa^{(-s)} \notin H$.
However we have that

$$(xa^{(-s)})^p = x^p a^{(-p)s} = x^p a^{(-q)} = h \in H$$

Consider, $K = \langle xa^{(-s)} \rangle H$. Clearly, $H \subseteq K$. Also $xa^{(-s)} \in K$ but $xa^{(-s)} \notin H$, so $H \neq K$.
By maximality of H, $\langle a \rangle \cap K \neq \{e\}$. Let $b \in \langle a \rangle \cap K$ where $b \neq e$.
Therefore, there exists t , $u \in Z$ and $h^{'} \in H$ such that $b = a^t = (xa^{(-s)})^u h^{'}$
Claim: p does not divide u.
Suppose if possible, $p \mid u$. Then $u = pv$ for some $v \in Z$, so we have

$$b = (xa^{(-s)})^u h^{'} = (xa^{(-s)})^{pv} h^{'} = ((xa^{(-s)})^p)^v h^{'}$$

Since, $(xa^{(-s)})^p \in H$. Therefore, $((xa^{(-s)})^p)^v h^{'} \in H$ and thus $b \in H$. Also, we have $b \in \langle a \rangle$, therefore $b \in \langle a \rangle \cap H = \{e\}$, which is a contradiction since $b \neq e$.
Hence, p does not divide u.
Now, since p is a prime, $(p, u) = 1$. So, there exists integer w and d such that $pw + ud = 1$.
Therefore,

$$x = x^{pw+ud} = (x^p)^w (x^u)^d$$

But, $x^p \in \langle a \rangle H$, then $(x^p)^w \in \langle a \rangle H$. Moreover $a^t = (xa^{(-s)})^u h^{'}$, so

$$x^u = a^t a^{su} (h^{'})^{(-1)} \in \langle a \rangle H$$

which implies $x \in \langle a \rangle H$ and this is a contradiction.
Thus, $G = \langle a \rangle H$, and hence G is the internal direct product of $\langle a \rangle$ and H. Therefore, $G \cong \langle a \rangle \times H$.

So, we can repeat this process on H to get $H \cong \langle c \rangle \times H_1$ for some $c \in H$, $H_1 \leq H$ etc. Since G is finite, eventually this process will end and consequently will have expressed G as a direct product of cyclic groups. In other words, any p-group G can be expressed as an internal direct product of cyclic subgroups. □

Theorem 2.0.13. *Every Finite abelian p-group can be written as direct product of cyclic groups.*

Proof. Let $|G| = p^n$. We will prove this by using induction on n.
If $n = 1$, $|G| = p$, which implies $G = \langle a \rangle$, where a is an element of order p.
Assume that result is true for all finite abelian p-groups of order less than p^n.
Now, let $|G| = p^n$. It follows from Theorem 2.0.12 that $G \cong \langle a \rangle \times H$. Here, $H < G$ and thus by induction hypothesis

$$H \cong \langle a_1 \rangle \times \langle a_2 \rangle \times ... \times \langle a_r \rangle.$$

Therefore,

$$G \cong \langle a \rangle \times \langle a_1 \rangle \times \langle a_2 \rangle \times ... \times \langle a_r \rangle.$$

□

Definition 2.0.26. If G and H are two groups, $Hom(G, H)$ refers to the set of all group homomorphisms from G to H.

Lemma 2.0.14. ***Properties of Hom:***
(1) If H is abelian, then $Hom(G, H)$ forms an abelian group with the binary operation defined by $(fg)(x) = f(x)g(x)$ for all f, g in $Hom(G, H)$ and for all $x \in G$.

Proof. **Associative Property:** Let f, g and $h \in Hom(G, H)$ and let $x \in G$. Now,

$$((fg)h)(x) = (fg)(x)h(x) = f(x)g(x)h(x)$$

$$(f(gh))(x) = f(x)g(x)h(x)$$

Thus, $((fg)h)(x) = (f(gh))(x)$ for all $x \in G$. So associative law holds.

Existence of Identity: Let $i : G \longrightarrow H$ defined by $i(x) = x$ for all $x \in G$. Clearly i is a homomorphism from G to H and thus, $i \in Hom(G, H)$.

Let $f \in Hom(G, H)$. Thus,

$$(fi)(x) = f(x)i(x) = f(x) = i(x)f(x) = (if)(x) \; \forall \; x \in G$$

So, $fi = f = if$ for all $f \in Hom(G, H)$. Thus, i is the identity element of $Hom(G, H)$.

Existence of Inverse: Let $f \in Hom(G, H)$. We define $f^{(-1)} : G \longrightarrow H$ by $f^{(-1)}(x) = (f(x))^{(-1)}$ for all $x \in G$.

Let $x, y \in G$.

$$\begin{aligned} f^{(-1)}(xy) &= (f(xy))^{(-1)} \\ &= (f(x)f(y))^{(-1)} \\ &= (f(y))^{(-1)}(f(x))^{(-1)} \\ &= f^{(-1)}(y)f^{(-1)}(x) \\ &= f^{(-1)}(x)f^{(-1)}(y) \end{aligned}$$

Thus, $f^{(-1)}(xy) = f^{(-1)}(x)f^{(-1)}(y)$ for all $x, y \in G$ which implies that $f^{(-1)} \in Hom(G, H)$.
Let $x \in G$. Now, $(ff^{(-1)})(x) = f(x)f^{(-1)}(x) = f(x)(f(x))^{(-1)} = i$.
Similarly, $(f^{(-1)}f)(x) = f^{(-1)}(x)f(x) = (f(x))^{(-1)}f(x) = i$.
Thus, $ff^{(-1)} = f^{(-1)}f = i$, $f \in Hom(G, H)$ and i refers to the identity element of $Hom(G, H)$. So, $f^{(-1)}$ is the inverse of f. Thus, inverse of every

element exist in $Hom(G, H)$.

Commutative Property: Let $f, g \in Hom(G, H)$

Now, $(fg)(x) = f(x)g(x) = g(x)f(x) = (gf)(x)$ for all $x \in G$. So, $fg = gf$ where $f, g \in Hom(G, H)$.
Thus, $Hom(G, H)$ forms an abelian group.

(2) [12] Let G , H and K be three finite abelian groups . Then

$$Hom(G, H \times K) \cong Hom(G, H) \times Hom(G, K)$$
$$Hom(H \times K, G) \cong Hom(H, G) \times Hom(K, G)$$

(3) [12] If C_m and C_n denotes the cyclic group of order m,n respectively, then

$Hom(C_m, C_n) \cong C_g$, where $g = g.c.d(m, n)$.

Theorem 2.0.15. *Every subgroup of a cyclic group is cyclic.*

Proof. Let $G = \langle a \rangle$ be a cyclic group and let H be a subgroup of G.
If $H = e$, then trivially H is cyclic.
Suppose that $H \neq e$ so there exists $a^n \in H$ such that $a^n \neq e$.
Then $a^{-n} = (a^n)^{-1} \in H$.
As either n or $-n$ is a positive integer, we can say that $a^n \in H$ for some positive integer n.
Let k be the least positive integer such that $a^k \in H$.
If we show that $H = \langle a^k \rangle$, then it will follow that H is a cyclic subgroup.
For this let $b \in H$, as $b \in G, b = a^m$ for some integer m.

By division algorithm,

$$m = kq + r$$

for some integers q, r with $0 \leq r < k$.
Now, $a^r = a^m(a^k)^{-q} \in H$. The minimality of k implies $r = 0$.
Thus, $m = kq$ and $b = (a^k)^q$.
Hence, $H = \langle a^k \rangle$.
This proves the result.

□

Definition 2.0.27. (Exponent of a Finite Group) The exponent of a finite group G, denoted by $exp(G)$, is the smallest positive integer m such that for every $g \in G$, we have $g^m = 1$.
For every finite group G, $exp(G)$ divides $|G|$.
Example: In $Q_8 = \{1, 1, i, i, j, j, k, k\}$, the ring of quaternions of order eight, since $|i| = |i| = |j| = |j| = |k| = |k| = 4$ and $1^4 = (-1)^4 = 1$, it follows that $exp\ (Q_8) = 4$.

Theorem 2.0.16. *If $H_1 \leq H$. then $C_G(H_1) \leq C_G(H)$.*

Proof. Let $x \in C_G(H)$, then x commutes with every element of H.
Since $H_1 \leq H$, x commutes with every element of H_1. This implies

$$x \in C_G(H_1)$$
$$\implies C_G(H) \leq C_G(H_1).$$

□

Definition 2.0.28. In a p-group G, $\Omega_1(G)$ is the subgroup of G generated by all the elements of G having order less than or equal to p.
Symbolically,

$$\Omega_1(G) = \langle x \in G |\ |x|\ \leq p \rangle.$$

CHAPTER 3

3 Main Results

All the results presented here are from [13].
It follows from [1], [9] and [13] that if G is a finite p-group of class 2 or of maximal class, then G has a noninner automorphism of order p fixing $\Phi(G)$ or $\Omega_1(Z(G))$ elementwise. Deaconescu and Silberberg [5] reduced the verification of the conjecture to the degenerate case where $C_G(Z(\Phi(G))) = \Phi(G)$. In the next theorem, we will consider finite p-groups G such that class of G is not equal to 2 or $m-1$, where $|G| = p^m$ and $C_G(Z(\Phi(G))) = \Phi(G)$.

Theorem 3.0.1. *Let G be a nonabelian finite p-group of order p^m satisfying one of the following conditions:*
(1) $\Phi(G)$ is cyclic;
(2) exp(G) $=p^{m-2}$;
(3) s = rank(Z(G)) $\geq (m-1)/2$ where $|G| = p^m$;
(4) s = rank(Z(G)) ≥ 2 and $[G : Z(G)] \leq p^4$.
Then G has a noninner automorphism of order p leaving either $\Phi(G)$ or $\Omega_1(Z(G))$ fixed elementwise.

Proof. Assume that $C_G(Z(\Phi(G))) = \Phi(G)$. Since $C_G(Z(\Phi(G))) = \Phi(G)$, $Z(G) \leq C_G(\Phi(G)) = Z(\Phi(G))$ and hence $\frac{Z_2(G) \cap Z(\Phi(G))}{Z(G)}$ will form a group.

(1) Since $\Phi(G)$ is cyclic,

$$\frac{Z_2(G) \cap Z(\Phi(G))}{Z(G)} = \frac{Z_2(G) \cap \Phi(G)}{Z(G)} \leq \frac{\Phi(G)}{Z(G)}$$

is cyclic. Hence by [13, Theorem], G has a noninner automorphism of order p that fixes $\Phi(G)$ elementwise.

(2) Let a be element of G of order p^{m-2}. Assume that $C_G(a) \neq \langle a \rangle$. Choose $x \in C_G(a) \backslash \langle a \rangle$. Since G is non abelian, $\langle x, a \rangle = M$ is a maximal

abelian subgroup of G. Therefore, by Theorem 2.0.16,

$$M \leq C_G(M) \leq C_G(\Phi(G)) = C_G(Z(\Phi(G))) = \Phi(G),$$

which is a contradiction. Thus $C_G(a) = \langle a \rangle$.
Suppose that p is odd. Then, by [11, Proposition 5] G is isomorphic, for $m \geq 4$, to

$$G_7 = \langle x, y, z | x^{p^{m-2}} = 1, y^p = 1, z^p = 1, y^{-1}xy = x^{1+p^{m-3}}, z^{-1}xz = xy, yz = zy \rangle;$$

and for $m \geq 5$,to

$$G_8 = \langle x, y |\ x^{p^{m-2}} = 1, y^{p^2} = 1, y^{-1}xy = x^{1+p^{m-4}} \rangle;$$
$$G_{10} = \langle x, y |\ x^{p^{m-2}} = 1, x^{p^{m-3}} = y^{p^2}, x^{-1}ya = y^{1-p} \rangle.$$

If G is isomorphic to G_7, then

$$M = \langle x, y |\ x^{p^{m-2}} = 1, y^p = 1, y^{-1}xy = x^{1+p^{m-3}} \rangle$$

is a maximal subgroup of G and $Z(G) = Z(M) = \langle x^p \rangle$.
Consider the map ϕ defined by $\phi(x) = x$, $\phi(y) = y$ and $\phi(z) = x^{p^{m-3}}z$.

Claim: ϕ is a noninner automorphism of order p.

$$\phi(x)^{p^{m-2}} = (\phi(x))^{p^{m-2}} = x^{p^{m-2}} = 1,$$

$$\phi(y^p) = (\phi(y))^p = y^p = 1,$$

$$\phi(z^p) = (\phi(z))^p = (x^{p^{m-3}}z)^p = x^{p^{m-3}}.z\ x^{p^{m-3}}.z.....(p - times).$$

Since $x^{p^{m-3}} \in Z(G)$,

$$\begin{aligned} \phi(z^p) &= (x^{p^{m-3}})^{(1+1+....+(p-times))}.z^p \\ &= (x^{p^{m-2}}).z^p \\ &= 1. \end{aligned}$$

Also

$$\phi(x^{-1}y^{-1}xy) = (\phi(x))^{-1}(\phi(y))^{-1}\phi(x)\phi(y) = x^{-1}y^{-1}xy = x^{p^{m-3}} = \phi(x^{p^{m-3}})$$

and

$$\phi(x^{-1}z^{-1}xz) = (\phi(x))^{-1}(\phi(z))^{-1}\phi(x)\phi(z) = x^{-1}z^{-1}x^{-(p)^{m-3}}x\ x^{p^{m-3}}z.$$

Since $Z(G) = \langle x^{p^{m-3}} \rangle$,

$$x^{-1}z^{-1}x^{-(p)^{m-3}}\ x^{p^{m-3}}\ x\ z = x^{-1}z^{-1}x\ z = y = \phi(y).$$

Also,

$$\begin{aligned} yz &= zy \\ \implies y^{-1}z^{-1}yz &= 1 \\ \phi(y^{-1}z^{-1}yz) &= (\phi(y))^{-1}(\phi(z))^{-1}\phi(y)\phi(z) \\ &= y^{-1}z^{-1}yz \\ &= y^{-1}yz^{-1}z \\ &= 1. \end{aligned}$$

Thus, ϕ is an automorphism of G.

Let, if possible, ϕ be inner determined by $g \in G$. Then

$\phi_g(x) = g^{-1}xg = x \Longrightarrow gx = xg$

$\phi_g(y) = g^{-1}yg = y \Longrightarrow gy = yg$

Therefore, g commutes with every element of maximal subgroup M. By Theorem 2.0.16, $C_G(M) \leq C_G(\Phi(G)) = Z(\Phi(G)) \leq M$. Thus, $g \in M$ and hence, $g \in Z(M)$. Since $Z(M) = Z(G)$, $g \in Z(G)$, which means that $\phi_g(z) = g^{-1}zg = z$ which is a contradiction. So, ϕ is not inner.

Now,

$$\begin{aligned} \phi^p(x) &= \phi^{p-1}\phi(x) \\ &= \phi^{p-1}(x) \end{aligned}$$

Continuing this way, we get $\Phi^p(x) = x$. Also,

$$\begin{aligned} \phi^p(y) &= \phi^{p-1}\phi(y) \\ &= \phi^{p-1}(y) \end{aligned}$$

Continuing this way, we get $\phi^p(y) = y$.
Consider,

$$\begin{aligned} \phi^p(z) &= \phi^{p-1}\phi(z) \\ &= \phi^{p-1}(x^{p^{m-3}}z) \\ &= \phi^{p-2}\{\phi(x^{p^{m-3}})\phi(z)\} \\ &= \phi^{p-1}(x^{p^{m-3}}\ x^{p^{m-3}}z) \\ \textit{Continuing this for } p-\textit{steps, we get} &= x^{p^{m-2}}z \\ &= z. \end{aligned}$$

Thus $\phi^p(z) = z$.

Hence ϕ is a noninner automorphism of order p, which fixes $Z(G)$ elementwise.

Now, let G be isomorphic to G_8.

Thus, $G' = \langle x^{p^{m-4}} \rangle$ and $Z(G) = \langle x^{p^2} \rangle$.

If $m = 5$, then $\Phi(G) = \langle x^p, y^p \rangle$, whence $Z(\Phi(G)) = Z(G) = \langle x^{p^2} \rangle$. Thus,

$$C_G(Z(\Phi(G))) = C_G(Z(G)) = G \neq \Phi(G)$$

a contradiction.
If $m \geq 6$, then $G^{'} \leq Z(G)$ and hence G is of class 2, a contradiction.
Finally let G be isomorphic to G_{10}.
Thus, $Z(G) = \langle x^{p^2} \rangle$ and $G' = \langle y^p \rangle$.
Set $\bar{x} = xZ(G)$ and $\bar{y} = yZ(G)$.
Hence,

$$\bar{G} = G/Z(G) = \langle \bar{x}, \bar{y} | \bar{x}^{p^2} = \bar{y}^{p^2} = \bar{1}, [\bar{x}, \bar{y}] = \bar{y}^p \rangle$$

Therefore, $\bar{G}' = \langle \bar{y}^p \rangle \leq \bar{G}^p$.
Thus, $G/Z(G)$ is a powerful p-group and so, G has a noninner automorphism of order p that fixes $\Phi(G)$ elementwise by [2].
Now, let $p = 2$, by [11, Proposition 7] G is isomorphic for $m \geq 5$, to

$G_{15} = \langle x, y, z |\ x^{2^{m-2}} = 1, y^2 = 1, z^2 = 1, y^{-1}xy = x^{1+2^{m-3}}, z^{-1}xz = x^{-1+2^{m-3}}, yz = zy \rangle$,

$G_{16} = \langle x, y, z |\ x^{2^{m-2}} = 1, y^2 = 1, z^2 = 1, y^{-1}xy = x^{1+2^{m-3}}, z^{-1}xz = x^{-1+2^{m-3}}, z^{-1}yz = x^{2^{m-3}}y \rangle$,

$G_{17} = \langle x, y, z |\ x^{2^{m-2}} = 1, y^2 = 1, z^2 = 1, y^{-1}xy = x^{1+2^{m-3}}, z^{-1}xz = xy, yz = zy \rangle$,

$G_{18} = \langle x, y, z |\ x^{2^{m-2}} = 1, y^2 = 1, z^2 = y, y^{-1}xy = x^{1+2^{m-3}}, z^{-1}xz = x^{-1}y\rangle$,

for $m \geq 6$, to
$G_{20} = \langle x, y |\ x^{2^{m-2}} = 1, y^4 = 1, y^{-1}xy = x^{-1+2^{m-4}}\rangle$,

$G_{21} = \langle x, y |\ x^{2^{m-2}} = 1, x^{2^{m-3}} = y^4, x^{-1}yx = y^{-1}\rangle$,

$G_{24} = \langle x, y, z |\ x^{2^{m-2}} = 1, y^2 = 1, z^2 = 1, y^{-1}xy = x^{1+2^{m-3}}, z^{-1}xz = x^{-1+2^{m-4}}y, yz = zy\rangle$,

$G_{25} = \langle x, y, z |\ x^{2^{m-2}} = 1, y^2 = 1, z^2 = x^{2^{m-3}}, y^{-1}xy = x^{1+2^{m-3}}, z^{-1}xz = x^{-1+2^{m-4}}y, yz = zy\rangle$,

and for $m = 5$, to
$G_{26} = \langle x, y, z |\ x^8 = 1, y^2 = 1, z^2 = x^4, y^{-1}xy = x^5, z^{-1}xz = xy, yz = zy\rangle$.
If G is one of the groups G_{15} or G_{16}, then

$G' = \langle x^2y\rangle \cong C_{2^{m-3}}$ and $Z(G) = \langle x^{2^{m-3}}\rangle \cong C_2$

Consider the map ϕ defined by $\phi(x) = x^{-1}$, $\phi(y) = y$ and $\phi(z) = z$.
Here, ϕ is a noninner automorphism of order two which fixing $Z(G)$ elementwise.

If G is a group G_{17}, then $G' = \langle x^{2^{m-3}}, y\rangle \cong C_2 \times C_2$
and $Z(G) =< x^4 > \cong C_{2^{m-4}}$.
Hence, the map ϕ defined by $\phi(x) = xz$, $\phi(y) = y$, $\phi(z) = z$ is an automorphism of G.
Also,

$$\phi^2(x) = \phi(xz) = \phi(x)\phi(z) = xz^2 = x,$$

$$\phi^2(y) = y\text{and}$$

$$\phi^2(z) = z.$$

Thus, order of ϕ is 2. Since z is a generator of G, ϕ cannot be an inner automorphism of G.

If G is the group G_{18}, then the map ϕ defined by $\phi(x) = xy$, $\phi(y) = y$ and $\phi(z) = z^{-1}$ is a noninner automorphism of order two which fixes $\Omega_1(Z(G))$ elementwise.
If G is the group G_{20}, then $G' = \langle x^2 \rangle \cong C_{2^{m-3}}$ and $Z(G) = \langle x^{2^{m-3}} \rangle \cong C_2$.

Consider the map ϕ defined by $\phi(x) = x^{-1}$ and $\phi(y) = y$ and $\phi(z) = z$. A Simple computation shows that ϕ is a noninner automorphism of order 2 which fixes $Z(G)$ elementwise.

If G is a group G_{21}, then $G' = \langle y^2 \rangle \cong C_4$ and $Z(G) = \langle x^2 \rangle \cong C_{2^{m-3}}$. Since $|G/Z(G)| = 8$ and nilpotency class of G is more than 2, we have $Z_2(G)/Z(G) \cong C_2$ and by [1,Theorem] G has a noninner central automorphism of order two which fixes $\Phi(G)$ elementwise.

Let G be one of the groups G_{24} or G_{25}. Then,

$$G' = \langle x^2 y \rangle \cong C_{2^{m-3}}$$

and

$$Z(G) = \langle x^{2^{m-3}} \rangle \cong C_2.$$

The map ϕ defined by $\phi(x) = xy$, $\phi(y) = y$ and $\phi(z) = yz$ is an automorphism of order two which fixes $Z(G)$ elementwise.
Since $y \notin \Omega_2(G)$, ϕ is noninner.

Let G be the group G_{26}. Then $G' = \langle x^4, y \rangle \cong C_2 \times C_2$ and $Z(G) = \langle x^4 \rangle \cong C_2$.
The map ϕ defined by $\phi(x) = xz$, $\phi(y) = y$ and $\phi(z) = z^{-1}$ is a noninner

automorphism of order two which fixes $Z(G)$ elementwise.

(3) If $s = 1$, then $m = 3$ and $|G| = p^3$, so $\Phi(G) = Z(G) \cong C_p$.

Thus, $C_G(Z(\Phi(G))) = G \neq \Phi(G)$, which is a contradiction. Therefore, $s \geq 2$.
We claim that

$$\frac{Z_2(G) \cap C_G(\Phi(G))}{Z(G)} \ncong Hom(\frac{G}{\Phi(G)}, Z(G)).$$

Assume to the contrary that

$$\frac{Z_2(G) \cap C_G(\Phi(G))}{Z(G)} \cong Hom(\frac{G}{\Phi(G)}, Z(G)).$$

Since $C_G(Z\Phi(G)) = \Phi(G)$, $C_G(\Phi(G)) = Z(G)$ and also $Z(G) \leq Z(\Phi(G))$. Now consider the nonabelian group G and $s = rank(Z(G)) \geq (m-1)/2$. By Theorem 2.0.8 and Lemma 2.0.14,

$$|\frac{G}{Z(G)}| \geq |\frac{Z_2(G) \cap C_G(\Phi(G))}{Z(G)}| = |Hom(\frac{G}{\Phi(G)}, Z(G))| \geq p^{2s} \geq p^{m-1}.$$

a contradiction, because G is nonabelian.
Hence, by [13,Proposition 2.5], G has a noninner automorphism of order p which fixes $\Phi(G)$ elementwise.

(4) Since nilpotency class of G is more than 2, $G/Z(G)$ is nonabelian, $|G/Z(G)| = p^3$ or p^4.

If $|G/Z(G)| = p^3$, then

$$|Z_2(G)/Z(G)| = p.$$

Hence by [13, Theorem], G has a noninner automorphism of order p which fixes $\Phi(G)$ elementwise.
Now, let $|G/Z(G)| = p^4$. In view of [13, Theorem], we can assume that $Z_2(G)/Z(G)$ is not cyclic. Therefore $Z_2(G)/Z(G) \cong C_p \times C_p$.
It follows from $s \geq 2$ and $d(G) \geq 2$ that

$$|Hom(G/\Phi(G), Z(G)| \geq p^4$$

and also,
if

$$\frac{Z_2(G) \cap C_G(\Phi(G))}{Z(G)} \cong Hom(G/\Phi(G), Z(G))$$

then

$$\frac{|Z_2(G)|}{|Z(G)|} \geq \frac{|Z_2(G) \cap C_G\Phi(G)}{|Z(G)|} \geq p^4,$$

which contradicts $\frac{Z_2(G)}{Z(G)} \cong C_p \times C_p$.

Hence, by [13, Propostion 2.5], G has a noninner automorphism of order p which fixes $\Phi(G)$ elementwise.

□

Theorem 3.0.2. *If G is a group of order p^n $(n \geq 4)$ and of maximal class, then G has at least p(p-1) noninner automorphisms of order p which fix $\Phi(G)$ elementwise.*

Proof. Since G is of maximal class, $|Z_2(G)| = p^2$. It follows from step 1 of [15], that $C_G(Z_2(G))$ is a maximal subgroup of G, say N_0.

Since, G is of maximal class by [4, Page 53], G has $p+1$ maximal subgroups.

Let $N_1.....N_p$ denote the maximal subgroups other than N_0.

For the sake of clarity, we divide the proof into following three steps:

Step 1: *Claim:* G is not a union of $N_1.....N_p$.
Since G is of maximal class , $|\Phi(G)| = p^{n-2}$.
For $i = 2, ...p, |N_i \cap N_1| = p^{n-2}$ and so, $|N_i \backslash N_1| = p^{n-1} - p^{n-2} = p^{n-2}(p-1)$.
Hence,

$$|(\bigcup_{i=1}^{p} N_i)\backslash N_1)| \leq \sum_{i=2}^{p} |N_i \backslash N_1| = p^{n-2}(p-1)^2 < p^n - p^{n-1} = |G \backslash N_1|.$$

Step 2: $Z(N_i) = Z(G) \cong C_p$ for $i = 1, ..., p$.

Suppose that $|Z(N)| > p$ for some $N = N_i$. Since by [4, Lemma 2.2] $Z_2(G)$ is the only normal subgroup of G of order p^2 and $Z(N)$ is normal in G, we have $Z_2(G) \leq Z(N)$. Therefore

$$N \leq C_G(Z(N)) \leq C_G(Z_2(G)) = N_0,$$

which is a contradiction.

Step 3: G has at least $p(p-1)$ noninner automorphisms of order p which fix $\Phi(G)$ elementwise.

By Step 1, we can pick $x \in G \backslash (N_1 \cup ..... \cup N_p)$. Thus,

$$G = \langle x \rangle N_1 = \langle x \rangle N_2 = ... = \langle x \rangle N_p.$$

By Step 2, $Z(N_j) = Z(G) \cong C_p$ for all $1 \leq j \leq p$.

Thus $Z(G) \leq \Phi(G)$ and $Z(G) = Z(N_j) = C_G(N_j)$. Let $Z(G) = \langle z \rangle$.
For $1 \leq j \leq p$, consider the map β_j defined on G by $\beta_j(x^i n_j) = x^i n_j z^i$ for every $n_j \in N_j$ and every $i \in \{0, 1, ..., p-1\}$.

$$\beta_j(n_j) = n_j \text{ for all } n_j \in N_j$$
$$\beta(x^i) = x^i z^i$$

Consider the map $\beta_1 : N_1\langle x \rangle \longrightarrow N_1\langle x \rangle$. Let $n_1 x^i, n_2 x^{i_1} \in N_1\langle x \rangle$ where $n_1, n_2 \in N_1$

$$\begin{aligned} \beta_1(n_1 x^i n_2 x^{i_1}) &= \beta_1(n_1 (n_2)' x^i x^{i_1}) \\ &= n_1 n_2{}' x^{i+i_1} z^{i+i_1} \\ &= n_1 x^i z^i n_2{}' x^{i_1} z^{i_1} \\ &= \beta_1(n_1 x^i)\beta_1(n_2 x^{i_1}) \end{aligned}$$

Thus, β is a homomorphism.
For any element $nx^i \in N\langle x \rangle$,
$(\beta_1)^p(nx^i) = (\beta_1)^{p-1}(\beta_1)(nx^i) = \beta_1^{p-1}(n_1 x^i z^i) = n_1 x^i z^{pi} = n_1 x^i$

Thus β_1 is a noninner automorphism of order p which fixes $\Phi(G)$ elementwise.
Similarly it can be easily seen that all β_i are noninner automorphisms of order p.

Let $\beta_j = \beta_k$ for some $i \leq j \neq k \leq p$.
Pick any $x_0 \in N_j \backslash N_k$. Since $G = \langle x \rangle N_k$, we have $x_0 = x^u n_k$ for some

$0 < u < p$ and some $n_k \in N_k$.

Then,

$$x_0 = \beta_j(x_0) = \beta_k(x_0) = x^u m_k z^u.$$

Therefore, $z^u = 1$ and so p must divide u, a contradiction.
It can be verified that if β_j is one of the above automorphisms, then $\beta_j^2, ..., \beta_j^{p-1}$ are noninner automorphisms of order p which fix $\Phi(G)$ elementwise.

As above it can be seen that $\beta_j^s \neq \beta_j^t$ for all $1 \leq j \neq k \leq p$ and $1 \leq s, t \leq p-1$.
Therefore, G has atleast $p(p-1)$ noninner automorphisms of order p which fix $\Phi(G)$ elementwise. □

References

[1] A. Abdollahi, *Finite p-groups of class 2 have noninner automorphisms of order p*, J.Algebra **312** (2007), 876-879.

[2] A. Abdollahi, *Powerful p-groups have noninner automorphisms of order p and some cohomology*, J.Algebra **323** (2010), 779-789.

[3] A. Abdollahi, M. Ghoraishi and B. Wilkens, *Finite p-groups of class 3 have noninner automorphism of order p*, Beitr. Algebra Geom. **54**(1) (2013), 363-381.

[4] N. Blackburn, *On a special class of p-groups*, Acta, Math. **100** (1958), 45-92.

[5] M. Deaconescu and G. Silberberg, *Noninner automorphisms of order p of finite p-groups*, J. Algebra **250** (2002), 283-287.

[6] S. M. Ghoraishi, *A note on automorphisms of finite p-groups*, Bull. Aust. Soc. **87** (2013), 24-26.

[7] B. Huppert, *Endliche Gruppen I* (Springer, Berlin, 1967).

[8] A. R. Jamali and M. Viseh, *On the existence of noninner automorphisms of order two in finite 2-groups*, Bull.Aust.Math.Soc. **87** (2013), 278-287.

[9] H. Lieback, *Outer automorphism in nilpotent p-groups of class 2*, J. Lond. Math. Soc. **40** (1965), 268-275.

[10] V. D. Mazeorov and E. I. Khukhro (Eds.), *Unsolved problems in group theory, in: The Kourovka Notebook*, Vol 16 (Russian Academy of Sciences, Siberian Division, Institute of Mathematics, Novosibirisk, 2006).

[11] Y. Ninomoya, *Finite p-groups with cyclic subgroups of index p^2*, Math. J. Okayama Univ. **36** (1994), 1-21.

[12] J. J Rotman, *An Introduction to the theory of groups*, 4th Ed. Springer Verlog New York Inc (1995).

[13] M. Shabani-Attar, *On a conjecture about automorphisms of finite p-groups*, Arch. Math. **93** (2009), 399-403.

[14] M. Shabani-Attar, *Existence of noninner automorphisms of order p in some finite p-groups*, Bull. Aust. Math. Soc. **87** (2013), 272-277.

[15] M. Shabani-Attar, *A necessary condition for nonabelian finite p-groups with second centre of order p^2*, Indian J. Pure Appl. Math. **42**(3) (2011), 183-186.