CLASS PRESERVING AUTOMORPHISMS OF FINITE p-GROUPS

A Thesis Submitted in partial fulfillment of the requirements for the award of degree of

Masters of Science

in

Mathematics and Computing

Submitted by

Swati

Reg. No. - 301403020

Under the guidance of

Dr. Deepak Kumar Gumber

Associate Professor

School of Mathematics

Thapar University

Patiala-147004(PUNJAB)

INDIA

July, 2016

Certificate

I hereby certify that the work which is being presented in the thesis entitled **"Class Preserving Automorphisms Of Finite p-Groups"** in partial fulfillment of the requirements for the award of the degree of Master of Science in the School of Mathematics, Thapar University, Patiala is a record of my own research work carried out under the supervision of Dr. Deepak Kumar Gumber.
The matter embodied in this thesis has not been submitted in part or full to any other university or institute for the award of any degree or diploma.

Swati
(301403020)

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

15-7-16

Dr. Deepak Kumar Gumber
Associate Professor
School of Mathematics
Thapar University, Patiala.

Countersigned by:

Dr. A.K. Lal
(Professor and Head)
School of Mathematics
Thapar University, Patiala.

Dr. S.S. Bhatia
(Dean of Academic Affairs)
Thapar University, Patiala.

Acknowledgement

This thesis marks the end of the beautiful journey to achieve my Masters degree. Throughout this journey I have been supported and guided by several people. I would like to take this opportunity to express my gratitude to all those people.

My first and sincere appreciation goes to Dr. Deepak Kumar Gumber, 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.

It is with immense gratitude that I acknowledge Dr.S.S.Bhatia,Dean of Academic Affairs and Dr.A.K.Lal,Head of Department, Thapar University,Patiala. Their advices and discussions were invaluable to me and their attitude towards research always inspired me. I really appreciate them for always being so supportive.

It gives me great pleasure in acknowledging the help from research scholar Rohit, SOM Thapar University and Vinay Madhusudanan, MIT Pune. They have been a great source of knowledge and inspiration. Thank you for always being so helpful and supportive.

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, support, encouragement, sacrifice, and unwavering belief in me. Without them, I would not be the person I am today. I would also like to convey my sincere thanks to my brothers Hiten and Sameer 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.

July 2016 *Swati*

Dedicated to
God, Parents and Teachers

Contents

CHAPTER 1

Introduction

Let G be a finite p-group and $\mid G \mid = p^n$, where p is a prime and n is a non-negative integer. We denote the group of all automorphisms of G by $\mathrm{Aut}(G)$. An automorphism α of G is called a class preserving automorphism if for each element $x \in G$, there exists an element $g_x \in G$ such that $\alpha(x) = g_x^{-1} x g_x$, and is said to be an inner automorphism if for all $x \in G$, there exists a fixed element $g \in G$ such that $\alpha(x) = g^{-1} x g$. The set of all class preserving automorphisms of G forms a normal subgroup of $\mathrm{Aut}(G)$ and is denoted by $\mathrm{Aut}_c(G)$.

The interest in the study of class preserving automorphisms dates back to 1911 when W. Burnside [2] asked the following question : Does there exist any finite group G such that G has a non-inner class preserving automorphism ? In 1913, Burnside [3] himself gave an affirmative answer to his question by constructing a group G of order p^6 isomorphic to the group W consisting of all 3 * 3 matrices

$$M = \begin{pmatrix} 1 & 0 & 0 \\ x & 1 & 0 \\ z & y & 1 \end{pmatrix}$$

where $x, y, z \in F_{p^2}$, the field consisting of p^2 elements and p being an odd prime. For this group G, $\mathrm{Inn}(G) < \mathrm{Aut}_c(G)$ where $\mathrm{Inn}(G)$ denotes the group of all inner

automorphisms of G. He also proved that $\mathrm{Aut}_c(G)$ is an elementary abelian p-group of order p^8. The central focus of this thesis is to provide a neat bound for $\mathrm{Aut}_c(G)$. The second chapter depicts the notations used throughout this thesis and consists of basic definitions and proofs of important results that are used frequently in the foregoing chapters. In the third chapter, we define Camina groups, originally introduced by A.R.Camina [4], which provide a motivation for studying class preserving automorphisms. We also prove some key lemmas related to our results. In the fourth chapter, we prove our main theorem ([1], Theorem 5.5) stated as follows : *Let G be a non-trivial finite p-group of order p^n. Then*

$$| \mathrm{Aut}_c(G) | \leq \begin{cases} p^{\frac{(n^2-4)}{4}} & \text{if n is even,} \\ p^{\frac{(n^2-1)}{4}} & \text{if n is odd.} \end{cases}$$

CHAPTER 2

Preliminaries and Notations

Definition 2.1 (**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 :*

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

Now, we can define a higher commutator of $x_1, x_2, \ldots, x_k$ inductively as :

$$[x_1, x_2, \ldots, x_k] = [[x_1, x_2, \ldots, x_{k-1}], x_k], \quad \textit{where} \quad k \geq 2$$

Definition 2.2 (**Subgroup generated by a subset of a Group**) *Let N be a subset of a group G. A subgroup M of G is said to be generated by N if it satisfies the following conditions:*

1. *$N \subseteq M$*

2. *If X is any subgroup of G containing N, then $M \subseteq X$.*

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

Definition 2.3 (**Commutator Subgroup**) *The* ***commutator subgroup*** *or the* ***derived subgroup*** *is the subgroup generated by the commutators of elements of G, denoted by*

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

Thus, every element of G' is of the form $m_1^{i_1} m_2^{i_2} \dots m_k^{i_k}$, where each m_i is a commutator of the form $x^{-1}y^{-1}xy$, each $i_j = \pm 1$ and k is any positive integer. In general, if H and K are two subgroups of a group G, then

$$[H, K] = \langle\ [a, b] : a \in H, b \in K\ \rangle.$$

A higher commutator subgroup of any r subgroups $H_1, H_2, \dots, H_r$ of G is defined inductively by the formula :

$$[H_1, H_2, \dots, H_r] = [[H_1, H_2, \dots, H_{r-1}], H_r]. \qquad where \quad r \geq 2$$

Proposition 2.4 *Let G be a group.*

1. *The commutator subgroup G' is a normal subgroup of G and G/G' is abelian.*

2. *If H is a normal subgroup of G and G/H is abelian, then $G' \leq H$.*

Proof. (i) The inverse of a commutator is itself a commutator:

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

Therefore, every element of G' is a finite product of commutators. Now for any

$a \in G$, we have

$$\begin{aligned} a^{-1}[x,y]a &= a^{-1}(x^{-1}y^{-1}xy)a \\ &= a^{-1}x^{-1}aa^{-1}y^{-1}aa^{-1}xaa^{-1}ya \\ &= (a^{-1}x^{-1}a)(a^{-1}y^{-1}a)(a^{-1}xa)(a^{-1}ya) \\ &= [a^{-1}xa, a^{-1}ya] \\ &= [x^a, y^a] \end{aligned}$$

Therefore $G' \lhd G$.

Let a and b be two elements of a group G. Then $a^{-1}b^{-1}ab = [a,b] = g$ for some element g of G'. This implies $ab = bag$. Therefore

$$(aG')(bG') = (ab)G' = (ba)G' = (bG')(aG'),$$

proving (i).

(ii) If G/H is abelian, then for any two elements $a, b \in G$, we have

$$\begin{aligned} (aH)(bH) = (bH)(aH) \Rightarrow (ab)H = (ba)H \Rightarrow (ba)^{-1}(ab)H = H \\ \Rightarrow (ba)^{-1}(ab) \in H \Rightarrow a^{-1}b^{-1}ab \in H \Rightarrow [a,b] \in H, \end{aligned}$$

and so we have $G' \leq H$, which proves (ii). □

Proposition 2.5 *Let H and K be subgroups of a group G. If K is a normal subgroup of G and $K \leq H$, then $[H,G] \leq K$ if and only if $H/K \leq Z(G/K)$.*

Proof. Let $[H,G] \leq K$. Then for all $g \in G$ and $h \in H, h^{-1}g^{-1}hg \in K$; i.e. $hgK = ghK$, or that $hK \in Z(G/K)$. Conversely, if $hK \in Z(G/K)$, then for all $g \in G, ghK = hgK$, and so $[h,g] \in K$. This means that $[h,G] \subseteq K$, and thus if this is true for all $h \in H$, then $[H,G] \leq K$. □

Lemma 2.6 *Let G be a group and x, y, z be elements of G. Then*

$$1.\ [xy, z] = [x, z]^y[y, z] = [x, z][x, z, y][y, z].$$

$$2.\ [x, yz] = [x, z][x, y]^z = [x, z][x, y][x, y, z].$$

Lemma 2.7 (**Hall Witt identity**) *Let G be a group and x, y, z be three elements of G. Then*

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

Theorem 2.8 (**Three Subgroup Lemma**) *Let X, Y and Z be three subgroups of a group G and N be a normal subgroup of G. If $[X, Y, Z]$ and $[Y, Z, X]$ are both contained in N, then so is $[Z, X, Y]$.*

Proof. Let $x \in X, y \in Y, z \in Z$. Since $[X, Y, Z]$ and $[Y, Z, X]$ are both contained in N, then $[x, y^{-1}, z]^y$ and $[y, z^{-1}, x]^z$ are elements of N because $N \lhd G$. Therefore by Lemma (2.7),

$$([x, y^{-1}, z]^y[y, z^{-1}, x]^z)^{-1} = [z, x^{-1}, y]^x \in N.$$

Since N is normal in G, so we have $[z, x^{-1}, y] \in N$ that means $[Z, X, Y] \leq N$. □

Definition 2.9 (**Internal Direct Product**) *Let $H_1, H_2, \ldots, H_k$ be the subgroups of a group G. We say that G is the internal direct product of $H_1, H_2, \ldots, H_k$ if it satisfies the following conditions:*

1. *$H_i \lhd G$ for all $i = 1, 2, \ldots, k$*
2. *$G = H_1H_2 \cdots H_k$*
3. *$H_i \cap (H_1H_2 \cdots \hat{H}_i \cdots H_k) = 1$, where $H_1H_2 \cdots \hat{H}_i \cdots H_k$ means the product of all H excluding H_i.*

Theorem 2.10 *If G is the internal direct product of $H_1, H_2, \ldots, H_k$, then $G \cong H_1 \times H_2 \times \cdots \times H_k$.*

Theorem 2.11 (**F**undamental Theorem of Finite Abelian Groups) *Every finite abelian group is isomorphic to the direct product of cyclic groups of prime power order. Furthermore, any two such decompositions have the same number of factors of each order. In symbols, if G is a finite abelian group of order $p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}$, then*

$$G \cong C_{p_1^{n_1}} \times C_{p_2^{n_2}} \times \ldots \times C_{p_k^{n_k}}.$$

Definition 2.12 (**Elementary Abelian p-Group**) *An abelian p-group G, which is the direct product of cyclic groups of order p, is called an elementary abelian p-group.*

Definition 2.13 (**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 $g^m = 1$.*

Definition 2.14 (**Normalizer**) *Let A be a non-empty subset of the group G.The set*

$$N_G(A) = \{x \in G \mid xA = Ax\}.$$

is called the normalizer of A in G.

Definition 2.15 (**Centralizer**) *Let A be a non-empty subset of G, then*

$$C_G(A) = \{x \in G \mid xa = ax \ \forall \ a \in A\}.$$

Clearly , $C_G(A)$ forms a subgroup of G.

Definition 2.16 (**Center of a Group**) *The center of a group G, denoted by $Z(G)$ is the set of elements in G that commute with every element of G. Symbolically,*

$$Z(G) = \{a \in G \mid ax = xa \ \forall \ x \in G\}.$$

Clearly, $Z(G)$ forms a normal subgroup of G and $Z(G) = G$ if and only if G is abelian.

Definition 2.17 (**Conjugate**) *We say that an element y of a group G is conjugate to an element x of G if there exists an element $a \in G$ such that*

$$y = x^a = a^{-1}xa.$$

The relation of Conjugacy among the elements of a group G is an equivalence relation, and therefore partitions G into equivalence classes.

Definition 2.18 (**Conjugacy Class**) *The conjugacy class of an element x of G consists of all the elements of the group that are conjugate to x.*

$$x^G = \{x^a \mid a \in G\}$$

Theorem 2.19 (**The Number of Conjugates of** x) *Let G be a finite group and let $x \in G$. Then,*

$$\mid x^G \mid = [G : C_G(x)]$$

This means that there are as many conjugates of x as there are distinct left cosets of $N_G(x)$ in G.

Remark 2.20

- *$x^G = x$ if and only if $x \in Z(G)$.*
- *The conjucacy classes consisting of only one element are, therefore, called central conjucacy classes.*

Theorem 2.21 (**The class equation**) *For any finite group G,*

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

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

Definition 2.22 (**Maximal Subgroup**) *Let G be a non-trivial group. A proper subgroup M of G is said to be maximal subgroup of G if there exists no subgroup N such that $M < N < G$.*

Theorem 2.23 *Let G be a finite group whose order is a power of a prime p.Then:*

1. *$Z(G)$ is non-trivial.*
2. *If H is a proper subgroup of G, then H is properly contained in $N_G(H)$.*
3. *Every maximal subgroup of G is normal.*

Proof. 1. We know that $Cl(x) = x$ 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 that contains exactly one element from each non-central conjugacy class of G. By Lagrange's Theorem, $| C_G(x) |$ divides the $| G |$. Now, $x \in Z(G)$ if and only if $C_G(x) = G$. If $x \notin Z(G)$, $C_G(x) < G$. Let $| G |= p^n$. Thus, $| C_G(x) | \leq p^{n-1}$ which implies that $\frac{|G|}{|C_G(x)|} \geq p$. So, $[G : C_G(x)] \geq p$.

Therefore, p divides $[G : C_G(x)]$ which signifies that p divides $\sum_{x \in X} [G : C_G(x)]$ $\Rightarrow p$ divides $| (G) | - \sum_{x \in X} [G : C_G(x)]$.

Thus, from (2.1), it follows that p divides $| Z(G) |$ and hence, $| Z(G) | \neq 1$.

2. Let K be a maximal normal subgroup of G contained in H. So, the quotient group G/K is of order $p^s (s > 0)$.Thus, by part (1), $Z(G/K)$ is non-trivial and let us assume that $Z(G/K) = R/K$. Now, $R/K \lhd G/K$, it follows that $R \lhd G$. Clearly, $R \not\subseteq H$, because otherwise maximality of K will be lost.

   Let $h \in H, r \in R$, then $hK \in G/K$ and $rK \in R/K$. Since, $R/K = Z(G/K)$, and so

   $$(rK)(hK) = (hK)(rK) \Rightarrow (rh)K = (hr)K,$$

   Thus, $h^{-1}r^{-1}hr \in K$ and so $r^{-1}hr \in hK \subset H$. Therefore, $R \subset N_G(H)$ which implies that $H \neq N_G(H)$. Since $H \subset N_G(H)$, it follows that H is properly contained in $N_G(H)$.

3. Let H be a maximal subgroup of G. Since, H is a proper subgroup of G, therefore by part (2), $H < N_G(H)$ and since H is maximal, $N_G(H) = G$.

   Now, $N_G(H) = \{g \in G \mid gH = Hg\} = G$ which implies that $gH = Hg \ \forall \ g \in G$. Thus, $H \lhd G$ and hence, every maximal subgroup of G is normal.

□

Theorem 2.24 *Let G be a finite p-group and let $K \lhd G$. Then K is a maximal subgroup of G if and only if G/K has prime order.*

Proof. Since $K \lhd G$, $\mid G/K \mid > 1$. Now, K is a maximal subgroup of G if and only if G/K has no non trivial proper subgroup. If possible, assume that $H/K < G/K$ which implies that $K < H < G$, which contradicts the maximality of K. Thus, G/K has no non-trivial proper subgroup; that is if and only if G/K is a finite cyclic group of prime order for some prime p. □

Definition 2.25 (**Non-Generator of a Group**) *Let G be a group and $y \in G$. An element y is said to be non-generator if whenever G is generated by y and a set Y, then $G = \langle Y \rangle$.*

Definition 2.26 (**Frattini Subgroup**) *Let G be a finite group. The Frattini subgroup is the intersection of all maximal subgroups of G and is denoted by $\Phi(G)$.*

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

Proposition 2.27 *Let G be a group. Then, $\Phi(G)$ is the set of all non-generators of G. Consequently, if $G = H\Phi(G)$ for some H, then $G = H$.*

Proof. Let y be a non-generator of G and let N be a maximal subgroup of G. Then $\langle N, y \rangle \geq N$ and since N is maximal, either $\langle N, y \rangle = N$ or $\langle N, y \rangle = G$. If $\langle N, y \rangle = G$, then, since y is a non-generator, $\langle N \rangle = G$, which is clearly a contradiction since N is maximal. Thus, $\langle N, y \rangle = N$ which implies that $y \in N$. This is true for all maximal subgroups N of G, thus $y \in \Phi(G)$.

Conversely, suppose that $y \in \Phi(G)$. Let G be generated by some set X, together with y which means that $G = \langle X, y \rangle$. We denote by M, the group $\langle X \rangle$. Since, $M \neq G$ which implies that M is contained in some maximal subgroup N of G. But $y \in N$, since y is an element of $\Phi(G) \leq N$ and so, $\langle X, y \rangle \leq N < G$, a contradiction. Thus, $\langle X \rangle = G$ which means that $M = G$ for all sets X for which $\langle X, y \rangle = G$. Thus, y is a non-generator of G.

Finally, $G = H\Phi(G) = \langle H, \Phi(G) \rangle$, so $G = \langle H \rangle = H \Rightarrow G = H$. □

Lemma 2.28 *Let G be a group and $\Phi(G)$ denotes the Frattini subgroup of G. Then, $\Phi(G)$ is a characteristic subgroup of G. (A characteristic subgroup is one which is invariant under every automorphism of G)*

Proof. If H is a maximal subgroup of G and α is an automorphism of G, then $\alpha(H)$ is a maximal subgroup of G. Let K be any subgroup of G such that $\alpha(H) \leq K \Rightarrow H \leq \alpha^{-1}(K)$, then $\alpha^{-1}(K) = G$ because H is maximal. Therefore, $K = G$.

Consider, $M = \{K \mid K \text{ is a maximal subgroup of G}\}$. 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 any 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 same as the intersection of all maximal subgroups H of G because α induces a permutation of M. Thus, $\Phi(G)$ is characteristic in G.

Since every characteristic subgroup is normal, thus $\Phi(G)$ is a normal subgroup of G. □

Proposition 2.29 *Let G be a finite p-group.Then, $G/\Phi(G)$ is elementary abelian, and if H is another normal subgroup of G such that G/H is elementary abelian, then $\Phi(G) \leq H$. Alternatively, $\Phi(G)$ is the unique smallest normal subgroup of G having elementary Abelian factor.*

Proof. By Theorem 2.23, part (3) and Theorem 2.24, it follows that every maximal subgroup M of a p - group is normal and is of index p i.e. $[G : M] = p$. This implies that G/M is a cyclic group of order p. Hence, $G' \leq M$ for all maximal subgroups M; consequently $G' \leq \Phi(G)$, and so $G/\Phi(G)$ is abelian by theorem (2.4). Also, since G/M has order p, (for M a maximal subgroup of G), we know that $(Mx)^p = M$ for all $x \in G$ which implies that $x^p \in M$ for all $x \in G$ and every maximal subgroup M of G. Thus, $x^p \in \Phi(G)$, and so if $\Phi(G)x \in G/\Phi(G)$, then $\Phi(G)x$ has order p which

proves that $G/\Phi(G)$ is elementary abelian.

Suppose that G/H is elementary abelian of order p^r. Then G/H is generated by r cosets Hx_i of G/H, each of order p. Thus,

$$G/H \cong \langle Hx_1 \rangle \times \langle Hx_2 \rangle \times \langle Hx_3 \rangle \times \ldots \langle Hx_r \rangle.$$

Now, this group has r maximal subgroups, H_i/H, each generated by $\{Hx_k : k \neq i\}$. Since,its a direct product, the intersection satisfies :

$$\bigcap_{1 \leq k \leq r} H_k/H = 1.$$

This means that the intersection of all H_k is H (where H_k is the corresponding subgroup in G to H_k/H, the preimage of H_k/H). But the H_k are maximal subgroups of G/H, and hence of G. This clearly implies that their intersection contains $\Phi(G)$. Thus,

$$H = \bigcap_{1 \leq k \leq r} H_k \geq \Phi(G).$$

□

Lemma 2.30 *Let G be a finite p-group. Then, $G' \leq \Phi(G)$.*

Proof. It follows from Theorem 2.24 that G/M is cyclic and hence abelian for every maximal subgroup M of G. Therefore by Proposition (2.4), part(2) we have $G' \leq M$ for every maximal subgroup M of G and thus $G' \leq \Phi(G)$, because $\Phi(G)$ is the intersection of all maximal subgroups of G. □

Proposition 2.31 *Let G be a finite p-group and let G^p denote the group generated by the set $\{g^p : g \in G\}$ i.e. the smallest group containing all the elements of order p. Then, $\Phi(G) = G'G^p$.*

Proof. It follows from Proposition 2.29 and Lemma 2.30, that $G'G^p \leq \Phi(G)$. On the other hand, since $G/G'G^p$ is elementary abelian, so we have $\Phi(G) \leq G'G^p$ and hence $\Phi(G) = G'G^p$.

□

Theorem 2.32 (**Burnside Basis Theorem**) *Let G be a finite p-group, and suppose that $[G : \Phi(G)] = p^d$. If $G/\Phi(G)$ is generated by elements $\Phi(G)x_i$, for $1 \leq i \leq d$, then G is generated by x_i. Furthermore, any generating set of G contains a subset Z such that $G = \langle Z \rangle$ and $G/\Phi(G)$ is generated by the images of the elements of Z.*

Proof. Let us assume that $\langle x_1, x_2, \ldots, x_d \rangle \leq G$ and we call it H. Since, we are in a finite p-group, we have maximal subgroups, and so, H being a proper subgroup of G is contained within some maximal subgroup M of G. Now $\Phi(G) \leq M$, thus

$$\langle \Phi(G)x_1, \Phi(G)x_2, \ldots, \Phi(G)x_d \rangle \leq M/\Phi(G) < G/\Phi(G).$$

This brings a contradiction to the fact that the cosets $\Phi(G)x_i$ generate $G/\Phi(G)$, therefore

$$G = \langle x_1, x_2, \ldots, x_d \rangle.$$

Now suppose that X is any generating set. Then, the images of X under the quotient $G \to G/\Phi(G)$ must generate $G/\Phi(G)$. Now, we can choose a subset $\{z_1, z_2, ..., z_d\}$ of d elements of X such that

$$G/\Phi(G) = \langle \Phi(G)z_1, \Phi(G)z_2, \ldots, \Phi(G)z_d \rangle$$

and therefore, $G = \langle z_1, z_2, \ldots, z_d \rangle$. □

Definition 2.33 (**Special p-groups**) *A finite p-group G is said to be Special p-group if $Z(G) = [G, G] = \Phi(G)$ is elementary abelian.*

Definition 2.34 (**Extra Special p-groups**) *A finite p-group G is said to be Extra Special $Z(G) = [G, G] = \Phi(G)$ is cyclic group of order p.*

Examples:

- Quaternion Group, Q_8 - A non-abelian group of order 8.
- Dihedral Group $D_8 = \langle\ x, a : x^2 = 1,\ a^4 = 1,\ (xa)^2 = 1\rangle$.
- Any non-abelian group of order p^3 is extra special.

Definition 2.35 (**Central Series**) *A normal series*

$$1 = B_0 \leq B_1 \leq B_2 \ldots \leq B_n = G \tag{2.2}$$

in a group G is called a ***central series*** *if*

$$B_{i+1}/B_i \leq Z(G/B_i),\ 0 \leq i \leq n-1, \tag{2.3}$$

or, equivalently, if

$$[G, B_{i+1}] \leq B_i,\ 0 \leq i \leq n-1. \tag{2.4}$$

Definition 2.36 (**Nilpotent Group**) *A group G is said to be nilpotent if it possesses a central series.*

Definition 2.37 (**Upper Central Series**) *In an arbitrary group G, we define an ascending chain of normal subgroups $Z_i(G)$,*

$$1 = Z_0(G) \leq Z_1(G) = Z(G) \leq Z_2(G) \leq \ldots \tag{2.5}$$

where

$$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G)) \quad for\ i\ \geq 0.$$

The subgroup $Z_i(G)$ is called the $i-th$ center of G, and the sequence (2.5) is called the upper central series of G.

Remark 2.38 *1. A group G is said to be nilpotent if and only if the upper central series terminates at G in a finite number of steps. In such a case, the upper central series is referred to as the shortest central series in G and $G(\neq 1)$ is nilpotent with class equal to the length of the series. i.e. Nilpotency class of G = Length of the Upper Central Series.*

2. If G is finite, the series terminates at a subgroup called the hypercenter.

Definition 2.39 (**Lower Central Series**) *In any arbitrary group G, we define subgroups $\gamma_i(G)$ as :*

$$\gamma_1(G) = G \quad , \quad \gamma_{i+1}(G) = [G, \gamma_i(G)] \quad for \quad i \geq 1. \tag{2.6}$$

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

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.

Remark 2.40 *1. We observe that*

$$\gamma_i(G)/\gamma_{i+1}(G) \leq Z(G/\gamma_{i+1}(G))$$

and each $\gamma_i(G)$ is a fully-invariant subgroup of G.

2. If the lower central series terminates in a finite number of steps at 1 and k is the least positive integer such that $\gamma_k(G) = 1$, then by (2.4) and (2.6); the

series

$$G = \gamma_1(G) \geq \gamma_2(G) \geq ...\gamma_k(G) = 1$$

is a central series in G and thus implying that G is nilpotent.

3. *Nilpotency class of G = Length of the lower central series.*

Definition 2.41 (**Class of a Group**) *The smallest positive integer c for which $Z_c(G) = G$(or equivalently $\gamma_{c+1}(G) = 1$) is referred to as the class of G.*

Lemma 2.42 *Let $G = \gamma_1(G) \geq \gamma_2(G) \geq \gamma_3(G) \geq \ldots$ be the lower central series of an arbitrary group G.*

$$[\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G) \quad for \quad i, j \geq 1.$$

Proof. We'll prove the result by induction on j. For $j = 1$, we have $[\gamma_i(G), \gamma_1(G)] = \gamma_{i+1}(G)$ by (2.6) . Thus, the result holds for $j = 1$. Let us assume that it is true for $j = k$ and for all i

$$[\gamma_i(G), \gamma_k(G)] \leq \gamma_{i+k}(G). \tag{2.7}$$

We need to prove it for $j = k + 1$.

$$[\gamma_i(G), \gamma_{k+1}(G)] \leq \gamma_{i+(k+1)}(G)$$

$$Now,\ [\gamma_i(G), \gamma_{k+1}(G)] = [\gamma_{k+1}(G), \gamma_i(G)] = [[\gamma_k(G), \gamma_1(G)], \gamma_i(G)] = [\gamma_k(G), G, \gamma_i(G)] \tag{2.8}$$

Since, $\gamma_{i+(k+1)}(G)$ is a normal subgroup of G ; therefore, by Theorem (2.8), it is sufficient to show that

$$[G, \gamma_i(G), \gamma_k(G)] \leq \gamma_{i+(k+1)}(G) \ \ and \ \ [\gamma_i(G), \gamma_k(G), G] \leq \gamma_{i+(k+1)}(G).$$

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

Since,the result holds for $j = k$ and for all i, thus from (2.7):

$$[\gamma_{i+1}(G), \gamma_k(G)] \leq \gamma_{i+(1+k)}$$

Therefore,

$$[G, \gamma_i(G), \gamma_k(G)] \leq \gamma_{i+(k+1)}(G) \tag{2.9}$$

On the other hand, we have

$$[\gamma_i(G), \gamma_k(G), G] = [[\gamma_i(G), \gamma_k(G)], G] \leq [\gamma_{i+k}(G), G] = \gamma_{i+(k+1)}(G) \tag{2.10}$$

$$[\gamma_i(G), \gamma_k(G), G] \leq \gamma_{i+(k+1)}(G) \tag{2.11}$$

From (2.9) and (2.11), it follows that :

$$[\gamma_k(G), G, \gamma_i(G)] \leq \gamma_{i+(k+1)}(G)$$

Thus, from (2.8) :

$$[\gamma_i(G), \gamma_{k+1}(G)] \leq \gamma_{i+(k+1)}(G).$$

Thus, the result holds for $j = k + 1$. Hence, by induction, we conclude that it is true for all positive integers j. Therefore,

$$[\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G)$$

□

Definition 2.43 (**Homomorphism**) *Given two groups* $(G, *)$ *and* $(H, \cdot)$*, a group homomorphism from* $(G, *)$ *to* $(H, \cdot)$ *is a function* $f : G \to H$ *such that for all* $x, y \in G$*, it holds that :*

$$f(x * y) = f(x) \cdot f(y)$$

A one-one(injective) homomorphism from G to H is referred to as a monomorphism.

A homomorphism that is onto (surjective) is called an epimorphism.

An endomorphism is a homomorphism $f : G \to G$, that is one with the same domain and codomain.

Definition 2.44 (**Kernel of a Homomorphism**) *Let $f : G \to H$ be a homomorphism. Let e' denote the identity element of H.The set of all elements x in G such that $f(x) = e'$ is called the kernel of f, and is denoted by* $\mathrm{Ker}(f)$ *or* $\mathrm{Ker}\, f$.

$$\mathrm{Ker}(f) = \{x \in G : f(x) = e'\}$$

Remark 2.45 *The kernel of a group homomorphism $f : G \to H$ is a normal subgroup of G ; moreover, f is injective if and only $\ker f$ consists of e' alone where e' refers to the identity element of H.*

Definition 2.46 *If G and H are two groups,* $\mathrm{Hom}(G, H)$ *refers to the set of all group homomorphisms from G to H.*

Theorem 2.47 *If H is abelian, then* $\mathrm{Hom}(G, H)$ *forms an abelian group with the binary operation defined by $(fg)(x) = f(x)g(x)$ for all f, g in* $\mathrm{Hom}(G, H)$ *and for all $x \in G$.*

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

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

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

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

Existence of Identity : Let $i : G \to H$ 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 $f \in \text{Hom}(G, H)$. Thus,

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

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

Existence of Inverse : Let $f \in \text{Hom}(G, H)$. We define $f^{-1} : G \to H$ 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 $f^{-1} \in \text{Hom}(G, H)$.

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, $ff^{-1} = f^{-1}f = i$, $f \in \text{Hom}(G, H)$ and i refers to the identity element of $\text{Hom}(G, H)$. So, f^{-1} is the inverse of f. Thus, inverse of every element exists in $\text{Hom}(G, H)$.

Commutative Property : Let $f, g \in \text{Hom}(G, H)$.

Now,$(fg)(x) = f(x)g(x) = g(x)f(x) = (gf)(x)$ for all $x \in G$.

So, $fg = gf$ where $f, g \in \text{Hom}(G, H)$.

Thus, $\mathrm{Hom}(G, H)$ forms an abelian group. □

Remark 2.48 *1. Let G, H and K be three finite abelian groups. Then*

$$\mathrm{Hom}(G, H \times K) \cong \mathrm{Hom}(G, H) \times \mathrm{Hom}(G, K)$$

$$\mathrm{Hom}(H \times K, G) \cong \mathrm{Hom}(H, G) \times \mathrm{Hom}(K, G)$$

2. If C_m denotes the cyclic group of order m,

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

Definition 2.49 (**Isomorphism**) *Let $(G, *)$ and $(H, \cdot)$ 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,*

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

The map f is called an isomorphism. The isomorphic groups are usually denoted by $G \cong H$. In other words, an isomorphism $f : G \to H$ is a homomorphism such that there exists another homomorphism $g : H \to G$ such that two compositions $f \circ g$ and $g \circ f$ are the identity homomorphisms on H and G, respectively.

Definition 2.50 (**Automorphisms**) *Let G be a group. An isomorphism of G with itself is called an automorphism. Thus, it's a bijective map $f : G \to G$ such that $f(ab) = f(a)f(b)$ for all $a, b \in G$.*

An automorphism can be thought of as a symmetry preserving permutation from a group to itself that preserve its operation.

The trivial automorphism is the identity function $i : G \to G$ such that

$i(x) = x$ for all $x \in G$, which is also known as $\epsilon(x)$.

Theorem 2.51 *The set of all automorphisms of a group forms a group with respect to composite of functions as the composition.*

Proof. Let A be the collection of all automorphisms of a group G.

Then, $A = \{f : f \text{ is an automorphism of } G\}$.

We shall prove that $(A, \circ)$ forms a group.

Closure Property : Let $f, g \in A$ and $h = f \circ g$. We'll show that $h \in A$ i.e. it is a bijection and preserves adjacency.

Now, h is a bijection since it is a composition of two bijective functions.

For adjacency preservation, we know that f and g preserve adjacency. Thus, we need to show that $h(ab) = h(a)h(b)$ for all $a, b \in G$.

L.H.S :

$$h(ab) = f \circ g(ab) = f(g(ab)) = f(g(a)g(b)) = f(g(a))f(g(b))$$

R.H.S :

$$h(a)h(b) = (f \circ g(a))(f \circ g(b)) = f(g(a))f(g(b)$$

Therefore, **LHS = RHS**.

Thus, h is an automorphism and hence closure law holds.

Associativity : We know that composite of mappings is associative. i.e. for f, g and $h \in A$, $(f \circ g) \circ h = f \circ (g \circ h)$. Therefore, composite of automorphisms is associative.

Existence of Identity : The identity function $i : G \to G$ is defined as $i(x) = x$ for all $x \in G$. Clearly, it is a 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 $f \in A \; \exists \; i \in A$ such that $f \circ i = i \circ f = f$. Thus, i is an identity element of G.

Existence of Inverse Let $f \in A$. Since f is a one-one map of G onto itself, therefore f^{-1} exists and its a map from $G \to G$ such that $f \circ f^{-1} = f^{-1} \circ f = e$. We need to show that $f^{-1} \in A$ i.e. f^{-1} is a bijection and f^{-1} preserves adjacency. We know that f^{-1} is a bijection as it is the inverse of a 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:

$$f^{-1}(a) = a' \Leftrightarrow f(a') = a \quad \textit{and}$$

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

Therefore,

$$\begin{aligned} f^{-1}(ab) &= f^{-1}(f(a')f(b')) \\ &= f^{-1}(f(a'b')) \\ &= a'b', \qquad \textit{since} \;\; f^{-1} \circ f = i. \\ &= f^{-1}(a)f^{-1}(b) \end{aligned}$$

Thus, $f^{-1}(ab) = f^{-1}(a)f^{-1}(b)$ for all $a, b \in G$. Therefore, f^{-1} is an automorphism i.e. $f^{-1} \in A$. So, each element of A possesses inverse. Thus, A forms a group with respect to composite composition and is referred to as group of automorphisms of G, usually denoted by $\mathrm{Aut}(G)$. □

Definition 2.52 (**Inner Automorphism**) *Let G be a group and a be a fixed element of G. Then, the mapping*

$$f_a : G \to G \;\; \text{defined by} \;\; f_a(x) = x^a = a^{-1}xa \; \forall \; x \in G.$$

is an automorphism of G known as inner automorphism.

For a group G, the inner automorphism group is defined by

$$\mathrm{Inn}(G) = \{f_a : a \in G\}$$

where f_a is an automorphism defined by $f_a(x) = a^{-1}xa$, for all $x \in G$.

Clearly, $\mathrm{Inn}(G)$ *forms a normal subgroup of* $\mathrm{Aut}(G)$.

CHAPTER 3

Camina Groups

Definition 3.1 (**Camina Pair**) *Let G be a finite group and H be a proper non-trivial normal subgroup of G. Then (G, H) is said to be a Camina Pair if for all $x \in G \setminus H, xH \subseteq x^G$.*

Observe that the following two conditions are equivalent :

1. $xH \subseteq \{x^g : g \in G\}\ \forall\ x \in G \setminus H$.

2. $H \subseteq \{[x, g] : g \in G\}\ \forall\ x \in G \setminus H$.

Definition 3.2 (**Camina Group**) *A group G is called a Camina group if $(G, \gamma_2(G))$ is a Camina pair.*

Lemma 3.3 ([1], Lemma 3.1) *If (G, H) is a Camina pair and N is a normal subgroup of G such that $N \subset H$, then $(G/N, H/N)$ is a Camina pair.*

Proof. Since (G, H) is a Camina pair, so H is a proper normal subgroup of G such that $H \subseteq [x, G]$ for all $x \in G \setminus H$. It follows that $h = [x, m]$ for some $m \in G$ and $h \in H$.

Now,

$$N \lhd G, H \lhd G \ \ and \ \ N \leq H \leq G \Rightarrow N \lhd H.$$

In order to show that $(G/N, H/N)$ forms a Camina pair, we need to prove :

1. $H/N \lhd G/N$,

2. $H/N \subseteq [xN, G/N]\ \forall\ xN \in (G/N) \setminus (H/N)$.

Firstly, let $gN \in G/N$ and $hN \in H/N$. We need to show that $(gN)^{-1}(hN)(gN) \in H/N$. Now,

$$\begin{aligned}(gN)^{-1}(hN)(gN) &= (g^{-1}N)(hN)(gN)\\ &= (g^{-1}hg)N\\ &= h_1N; h_1 = g^{-1}hg \in H\\ &\in H/N.\end{aligned}$$

Thus, $(gN)^{-1}(hN)(gN) \in H/N\ \forall\ hN \in H/N$ and $gN \in G/N$.

This proves the normality condition.

Secondly, hN be an arbitrary element of H/N.

By hypothesis, we have $h = [x, m]$ for some $m \in G$. Thus,

$$\begin{aligned}hN &= [x, m]N\\ &= (x^{-1}m^{-1}xm)N\\ &= (x^{-1}N)(m^{-1}N)(xN)(mN)\\ &= (xN)^{-1}(mN)^{-1}(xN)(mN)\\ &= [xN, mN] \in [xN, G/N] \text{ where } m \in G.\end{aligned}$$

Thus, $hN \in [xN, G/N]\ \forall\ h \in H$ and $x \in G \setminus H$

$\Rightarrow$ $H/N \subseteq [xN, G/N]\ \forall\ xN \in (G/N) \setminus (H/N)$.

Therefore, $(G/N, H/N)$ forms a Camina pair. $\square$

The next Theorem follows from [7] and [8].

Theorem 3.4 *Let G be finite Camina p-group of class 3 such that $[G : \gamma_2(G)] = p^t$, $[\gamma_2(G), \gamma_3(G)] = p^s$ and $\mid \gamma_3(G) \mid = p^r$. Then*

1. *$(G, \gamma_3(G))$ is a Camina pair, $\gamma_3(G) = Z(G)$, $t = 2s$ and s is even,*

2. *$s \geq r$,*

3. *$\gamma_i(G)/\gamma_{i+1}(G)$ has exponent p , for $i = 1, 2$.*

Lemma 3.5 ([7] , Lemma 2.1) *If (G, H) is a Camina pair and G has class c, then $H = \gamma_s(G)$ and $H = Z_{c-s+1}(G)$ for some $1 < s \leq c$.*

Proof. Since (G, H) is a Camina pair, therefore $1 \neq H \neq G$ and H is a normal subgroup of G such that $H \subseteq [x, G]$ for all $x \in G \setminus H$. We prove that $Z(G) \leq H$. Let $z \in Z(G) \setminus H$. By definition of Camina pair, $zH \subseteq z^G = z$. This leads to a contradiction. Therefore, $Z(G) \leq H$. Thus, by Lemma 3.3, $(G/Z(G), H/Z(G))$ is a Camina pair. By the similar argument, $Z(G/Z(G)) \leq H/Z(G)$ which means that $Z_2(G) \leq H$. Continuing like this, we get that $H = Z_{c-s+1}(G)$ for some s with $1 < s \leq c$. We know that $\gamma_i(G) \leq Z_{c-i+1}(G)$ for all i. Let us Assume that $\gamma_i(G) < Z_{c-i+1}(G) = H$. Thus, by Lemma 3.3, $(G/\gamma_i(G), H/\gamma_i(G))$ forms a Camina pair, and so

$$\gamma_{i-1}(G)/\gamma_i(G) \leq Z(G/\gamma_i(G)) \leq H/\gamma_i(G).$$

Thus, $\gamma_{i-1}(G) \leq H = Z_{c-i+1}(G)$ for all i. This implies that $\gamma_c(G) \leq Z_0(G) = 1$, which leads to a contradiction since G has class c.

Therefore,

$$\gamma_s(G) = Z_{c-s+1}(G) = H.$$

□

Lemma 3.6 ([1], Lemma 3.3) *Let G be a group and K be a subgroup of G such that $\gamma_2(G) = \gamma_2(K)$. Then $\gamma_i(G) = \gamma_i(K)\ \forall\ i \geq 2$.*

Proof. Here, $\gamma_2(G) = G' = [G, G]$ and $\gamma_2(K) = K' = [K, K]$. **Firstly**, we'll prove that $\gamma_i(K)$ is a normal subgroup of G for all $i \geq 1$. Since $\gamma_2(G) = \gamma_2(K) \leq K \leq G$ and any subgroup containing the commutator subgroup is a normal subgroup of G, thus $K \lhd G$. For $i = 1$, we have $\gamma_2(K) = \gamma_2(G) = G'$ and $G' = [G, G]$ is a normal subgroup of G. Thus, $\gamma_2(K) \lhd G$. Let us assume that the result holds for $i = j > 1$ i.e. $\gamma_j(K) \lhd G$. We need to prove that $\gamma_{j+1}(K) = [\gamma_j(K), K] \lhd G$. Observe that

$$\begin{aligned}
\gamma_{j+1}(K) = [\gamma_j(K), K] &= (\gamma_j(K))^{-1}K^{-1}\gamma_j(K)K \\
&= \gamma_j(K)K\gamma_j(K)K \\
&= (K\gamma_j(K))\gamma_j(K)K \\
&= K(\gamma_j(K)\gamma_j(K))K \\
&= K\gamma_j(K)K \\
&= KK\gamma_j(K) \\
&= K\gamma_j(K)\ \lhd\ G.
\end{aligned}$$

Thus, $\gamma_{j+1}(K) \lhd G$ and so the result holds for $i = j + 1$. Therefore, by principle of mathematical induction, the result holds for all positive integers i.

Next, Assume that $\gamma_j(G) = \gamma_j(K)$ holds for $i = j \geq 2$. We'll prove that $\gamma_{j+1}(G) = \gamma_{j+1}(K)$.

Trivially,

$$\gamma_{j+1}(K) \leq \gamma_{j+1}(G) \tag{3.1}$$

Now,

$$\gamma_{j+1}(G) = [\gamma_j(G), G] = [\gamma_j(K), G] = [\gamma_{j-1}(K), K, G]. \tag{3.2}$$

Observe that

$[K, G, \gamma_{j-1}(K)] \leq [G, G, \gamma_{j-1}(K)] = [\gamma_2(G), \gamma_{j-1}(K)] = [\gamma_2(K), \gamma_{j-1}(K)] \leq \gamma_{j+1}(K)$

by Lemma 2.42, and

$[G, \gamma_{j-1}(K), K] = [[G, \gamma_{j-1}(K)], K] \leq [[G, \gamma_{j-1}(G)], K] = [\gamma_j(G), K] = [\gamma_j(K), K] = \gamma_{j+1}(K)$,

Hence, by eqn.(3.2) and Theorem 2.8, we have

$$\gamma_{j+1}(G) = [\gamma_{j-1}(K), K, G] \leq \gamma_{j+1}(K). \tag{3.3}$$

From (3.1) and (3.3), the result holds for $i = j + 1$. Therefore, by Principle of Mathematical Induction, we conclude that $\gamma_i(G) = \gamma_i(K)$ for all $i \geq 2$. □

Theorem 3.7 ([7] , Theorem 2.2) *Let (G, H) be a Camina pair, let $H = Z(G)$, and G has class c. Then, $Z_s(G)/Z_{s-1}(G)$ has exponent p for $1 \leq s \leq c$.*

Proof. We will firstly prove that if $N < Z(G)$, then $Z(G/N) = Z(G)/N$. Let $gN \in Z(G)/N$ where $g \in Z(G)$. Consider $bN \in G/N$. Thus, $(gN)(bN) = (gb)N = (bg)N = (bN)(gN)$, $g \in Z(G)$ and $b \in G$. So, $gN \in Z(G/N)$, $g \in Z(G)$ and therefore, $Z(G)/N \leq Z(G/N)$. On the other hand, since $N < Z(G) = H$, thus by Lemma 3.3, $(G/N, H/N)$ is a Camina pair, thus $Z(G/N) \leq H/N$ which means that $Z(G/N) \leq Z(G)/N$. Hence, $Z(G/N) = Z(G)/N$.

Let us consider $N = Z(G)^p$. It thus follows that $Z(G/Z(G)^p) = Z(G)/Z(G)^p$ where $Z(G)^p < Z(G)$. By a well known commutator identity ([6], s. 253, 1.3 Hilfsatz) $[Z_2(G)^p, G] \leq Z(G)^p$, thus from Proposition 2.5, we have $Z_2(G)^p/Z(G)^p \leq$

$Z(G)/Z(G)^p$ which means that $Z_2(G)^p \leq Z(G)$. Thus, $Z_2(G)/Z_1(G)$ is elementary abelian. Therefore, $Z_2(G)/Z_1(G)$ has exponent p.

Thus, we deduce that $Z_{s+1}(G)/Z_s(G)$ has exponent p for each $s > 1$ by ([6], s. 266, 2.13 Satz). Substituting $s = c-1, G/Z_{c-1}(G)$ has exponent p. But by ([6], s. 265, 2.11 Haupsatz), $[\gamma_{c-1}(G), Z_{c-1}(G)] = 1$.. Now, the exponent of $[\gamma_{c-1}(G), G]$ is p by ([6], s.253, 1.3 Hilfsatz) which means that $\gamma_c(G)$ has exponent p and thus by Lemma 3.5, we have $\gamma_c(G) = H = Z(G)$. Therefore, $Z(G)$ has exponent p as well. □

Corollary 3.8 *If (G, H) is a Camina pair and G has class 2, then*

1. *G is a special p-group; and*

2. *$H = Z(G)$.*

Proof. By Lemma 3.5, $H = \gamma_2(G)$ and $H = Z_1(G) = Z(G)$. Thus, $H = Z(G) = \gamma_2(G)$. By Theorem 3.7, both H as well as G/H have exponent p. This implies that H as well as G/H are elementary abelian p-groups. Thus, by Proposition 2.29, $\Phi(G) \leq H$. Also, $H = \gamma_2(G) \leq \Phi(G)$. So, $H = \Phi(G) = Z(G) = \gamma_2(G)$ i.e. $\Phi(G) = Z(G) = \gamma_2(G)$ is elementary abelian, thus G is a special p-group. □

Lemma 3.9 ([1], Lemma 3.4) *Let G be a Camina p-group of class 2, with a minimal generating set $\{x_1, x_2, \ldots, x_t\}$, where $t > 2$. Then $H = \langle x_1, x_2, \ldots, x_{t-1}\rangle$ satisfies $\gamma_2(G) = \gamma_2(H)$.*

In particular, H is a maximal subgroup of G.

Proof. Since G is a Camina p-group of class 2, by Corollary 3.8, G is a special p-group, and so $G/\gamma_2(G)$ is an elementary abelian p-group of order p^t, and that $\gamma_2(G) = Z(G)$ is an elementary abelian p-group of order p^s (say), for some positive

integer s. Now, we will prove the result with the help of mathematical induction. Assume that $s = 1$, so $G' = Z(G) = \Phi(G)$ is an elementary abelian p-group of order p that means G is extra special p-group. Now, by ([12], Theorem 5.3.8), the order of G is an odd power of p and thus the order of $G/\gamma_2(G)$ is an even power of p. So, t is even. Clearly, $\gamma_2(H) \leq \gamma_2(G)$. If possible, let $\gamma_2(H) \neq \gamma_2(G)$, then $\gamma_2(H) = 1$ because $\mid \gamma_2(G) \mid = p$. It follows that H is abelian and thus $HZ(G)$ is an abelian subgroup of G. Observe that the maximal order of an abelian subgroup of an extra special group G of order p^{1+t} is $p^{1+(t/2)}$, therefore $\mid HZ(G) \mid \leq p^{1+(t/2)}$. Since $\mid HZ(G) \mid = p^t$, thus we get $p^t \leq p^{1+(t/2)}$.This implies that $t \leq 1 + (t/2)$, which on simplification gives $t \leq 2$. It is a clear contradiction since $t > 2$. Thus, our assumption is wrong and hence $\gamma_2(H) = \gamma_2(G)$ for $s = 1$.

Now, suppose that $s > 1$. If possible, assume that $\gamma_2(H) \neq \gamma_2(G)$, then $\gamma_2(H) \leq M$ for some maximal subgroup M of $\gamma_2(G) = Z(G)$. Let $\overline{G} = G/M$ and define a map $\alpha : G \to \overline{G}$ given by $\alpha(g) = gM = \overline{g}$ for every $g \in G$. Clearly, α is an isomorphism. Next, we show that $\overline{G}$ is an extra special p-group which means that $(G/M)' = Z(G/M) = \Phi(G/M)$ is a cyclic group of order p. Also, $\Phi(G/M) = \Phi(G)/M$ by ([11], Lemma 11.8(ii)) and $Z(G/M) = Z(G)/M$ as proved in a section of Theorem 3.7. Thus

$$(G/M)' = G'M/M = G'/M$$

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

$$\Phi(G/M) = \Phi(G)/M = G'/M.$$

Since M is a maximal subgroup of G', thus by Theorem 2.24, $\mid G'/M \mid = p$ and hence $(G/M)' = Z(G/M) = \Phi(G/M)$ is a cyclic group of order p. Now, α maps

$\{x_1, x_2, \ldots, x_t\}$ to $\{\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_t\}$ which thus forms the minimal generating set of $\overline{G}$. Clearly, the subgroup $H = \{x_1, x_2, \ldots, x_t\}$ is mapped onto $\{\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_t\} = \overline{H}$ (say) in $\overline{G}$. Now, $\gamma_2(\overline{H}) = \gamma_2(H/M) = \gamma_2(H)M/M = M/M = 1$. Observe that $|\ \gamma_2(\overline{G})\ | = |\ \gamma_2(G/M)\ | = |\ \gamma_2(G)M/M\ | = |\ \gamma_2(G)/M\ | = p$. Thus, the lemma holds for $\overline{G}$. So $\gamma_2(\overline{H}) = \gamma_2(\overline{G}) \neq 1$, a contradiction and hence $\gamma_2(H) = \gamma_2(G)$.

□

Proposition 3.10 ([1], Proposition 3.5) *Let $\{x_1, x_2, \ldots, x_t\}$ be a minimal generating set for a Camina p-group G of class 3. Then $H = \langle x_1, x_2, \ldots, x_{t-1}\rangle$ satisfies $\gamma_2(H) = \gamma_2(G)$.*

In particular, H is a maximal subgroup of G. Moreover, $\gamma_2(G) \not\leq Z(H)$.

Proof. Consider $|\ G/\gamma_2(G)\ | = p^t, |\ \gamma_2(G)/\gamma_3(G)\ | = p^s$ and $|\ \gamma_3(G)\ | = p^r$. Since G is a Camina p-group of class 3, thus by Theorem 3.4, $(G, \gamma_3(G))$ is a Camina pair, $\gamma_3(G) = Z(G), t = 2s$, s is even and $s \geq r > 0$. So, $t > 2$. Since $(G, \gamma_2(G))$ is a Camina pair and $\gamma_3(G)$ is a normal subgroup of G contained in $\gamma_2(G)$, thus it follows from Lemma 3.3 that $(G/\gamma_3(G), \gamma_2(G)/\gamma_3(G))$ is a Camina pair. Since $\gamma_2(G/\gamma_3(G)) = \gamma_2(G)\gamma_3(G)/\gamma_3(G) = \gamma_2(G)/\gamma_3(G)$, thus $(G/\gamma_3(G), (G/\gamma_3(G))')$ is a Camina pair and hence $G/\gamma_3(G)$ is a Camina p-group of class 2 as $\gamma_3(G/\gamma_3(G)) = \gamma_3(G)\gamma_3(G)/\gamma_3(G) = \gamma_3(G)/\gamma_3(G) = 1$. Now, $G/\gamma_3(G) = \langle x_1\gamma_3(G), x_2\gamma_3(G), \ldots, x_t\gamma_3(G)\rangle$ and $H\gamma_3(G)/\gamma_3(G) = \langle x_1\gamma_3(G), x_2\gamma_3(G), \ldots, x_{t-1}\gamma_3(G)\rangle$, so by Lemma 3.9, $\gamma_2(G/\gamma_3(G)) = \gamma_2(H\gamma_3(G)/\gamma_3(G))$. Since

$$\gamma_2(G/\gamma_3(G)) = \frac{\gamma_2(G)\gamma_3(G)}{\gamma_3(G)} = \frac{\gamma_2(G)}{\gamma_3(G)} \quad \text{and} \quad \gamma_2(H\gamma_3(G)/\gamma_3(G)) = \frac{\gamma_2(H)\gamma_3(G)}{\gamma_3(G)},$$

it follows that

$$\frac{\gamma_2(G)}{\gamma_3(G)} = \frac{\gamma_2(H)\gamma_3(G)}{\gamma_3(G)}.$$

Therefore,

$$\gamma_2(H)\gamma_3(G) = \gamma_2(G) \tag{3.4}$$

Let us consider the case when $r = 1$. Clearly, $\gamma_2(H) \leq \gamma_2(G)$. If possible, let us suppose that $\gamma_2(H) < \gamma_2(G)$. From Theorem 3.4(3), $\gamma_2(G)/\gamma_3(G)$ has exponent p and thus it is an elementary abelian p-group of order p^s. Since $\mid \gamma_3(G) \mid = p^r = p$ as $r = 1$, thus it follows from (3.4) that $\gamma_2(G)$ is the direct product of its elementary abelian subgroups $\gamma_2(H) \cong \gamma_2(G)/\gamma_3(G)$ and $\gamma_3(G) = Z(G)$. Now, $H \leq C_G(Z(G))$. Also, as $\gamma_2(H) < \gamma_2(G)$ which implies that $\gamma_3(H) = [\gamma_2(H), H] < [\gamma_2(G), H] \leq \gamma_3(G)$, therefore $\gamma_3(H) = 1$ because $\mid \gamma_3(G) \mid = p$. Thus $H \leq C_G(\gamma_2(H))$, so by (3.4), $H \leq C_G(\gamma_2(G))$ and therefore, $H\gamma_2(G) \leq C_G(\gamma_2(G))$ because $\gamma_2(G)$ is abelian. Since $[G : H\gamma_2(G)] = p$ and $[G : C_G(\gamma_2(G))] = p^s$ ([9], Theorem 1.3(iv)), thus it follows from $H\gamma_2(G) \leq C_G(\gamma_2(G))$ that $p^s = [G : C_G(\gamma_2(G)] \leq [G : H\gamma_2(G)] = p$, which is a contradiction since s is a positive even integer. Therefore, $\gamma_2(H) = \gamma_2(G)$ for $r = 1$.

Next, we suppose that $r > 1$ and $\gamma_2(H) < \gamma_2(G)$. From (3.4), it follows that $\gamma_2(H) \bigcap \gamma_3(G) < \gamma_3(G)$. Thus, $\gamma_2(H) \bigcap \gamma_3(G) \leq M$ for some maximal subgroup M of $\gamma_3(G) = Z(G)$. By Lemma 3.3, $(G/M, \gamma_2(G)/M)$ is a Camina pair and since $\gamma_2(G/M) = \gamma_2(G)M/M = \gamma_2(G)/M$, thus $(G/M, \gamma_2(G/M))$ is a Camina pair and therefore, $\overline{G} = G/M$ is a Camina p-group of class 3. Consider the mapping $\alpha : G \to \overline{G}$ defined by $\alpha(g) = \overline{g}$ for all $g \in G$. Since $\gamma_2(G)$ maps to $\gamma_2(G)/M = \gamma_2(G)M/M = \gamma_2(G/M) = \gamma_2(\overline{G})$ and similarly $\gamma_3(G)$ maps to $\gamma_3(\overline{G})$

under α, therefore $\{x_1, x_2, \ldots, x_t\}$ maps to $\{\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_t\}$ which thus forms a minimal generating set for $\overline{G}$. The subgroup $H = \langle x_1, x_2, \ldots, x_{t-1}\rangle$ is mapped onto $\langle \overline{x}_1, \overline{x}_2, \ldots, \overline{x}_{t-1}\rangle = \overline{H} = HM/M$ in $\overline{G}$. Observe that

$| \gamma_3(\overline{G}) | = | \gamma_3(G/M) | = | \gamma_3(G)M/M | = | \gamma_3(G)/M | = p$,

$| \overline{G}/\gamma_2(\overline{G}) | = | (G/M)/\gamma_2(G/M) | = | (G/M)/(\gamma_2(G)/M) | = | G/\gamma_2(G) | = p^t$ and

$| \gamma_2(\overline{G})/\gamma_3(\overline{G}) | = | \gamma_2(G/M)/\gamma_3(G/M) | = | (\gamma_2(G)/M)/(\gamma_3(G)/M) | = | \gamma_2(G)/\gamma_3(G) |$

$= p^s$.

Since the proposition holds for $r = 1$, $\gamma_2(\overline{H}) = \gamma_2(\overline{G})$ and hence $\gamma_2(H)M = \gamma_2(G)$. Now, $\gamma_3(G) = \gamma_2(G) \bigcap \gamma_3(G) = \gamma_2(H)M \bigcap \gamma_3(G) = \gamma_2(H)M \bigcap \gamma_3(G)M = (\gamma_2(H) \bigcap \gamma_3(G))M$

$= M < \gamma_3(G)$, which is a contradiction, thus $\gamma_2(H) = \gamma_2(G)$.

Next, we will show that $\gamma_2(G) \notin Z(H)$. If possible, suppose that $\gamma_2(G) \leq Z(H)$ which implies that $\gamma_2(H) \leq Z(H)$ as $\gamma_2(H) = \gamma_2(G)$. So, $\gamma_3(H) = [\gamma_2(H), H] = 1$. Now, by lemma 3.6, it follows that $\gamma_3(G) = \gamma_3(H) = 1$ but G is a Camina p-group of class 3, therefore $\gamma_3(G) \neq 1$, a contradiction. Thus, $\gamma_2(G) \notin Z(H)$. □

Lemma 3.11 ([1], Lemma 3.6) *Let G be a Camina p-group of class 3 such that $| \gamma_3(G) | \geq p^2$. Let H be any maximal subgroup of G. Then, $Z(H) = Z(G)$.*

Proof. By Theorem 2.24, G/H is a cyclic group of order p. Let $x \in G \setminus H$ be arbitrary. Then $G/H = \langle xH\rangle = H\langle x\rangle$. Now, by Theorem 3.4 ;

$$Z(G) = \gamma_3(G) \leq \gamma_2(G) = \Phi(G) \leq H$$

Thus, it follows that $Z(G) \leq Z(H)$. If possible, suppose that $Z(G) < Z(H)$. Let $1 \neq z \in Z(H) \setminus Z(G)$. If $z \in \gamma_2(G) \setminus \gamma_3(G)$, then $[z, G] = \gamma_3(G)$ because $(G, \gamma_3(G))$

is a Camina pair and if $z \in G \setminus \gamma_2(G)$, then $[z, G] = \gamma_2(G)$ as $(G, \gamma_2(G))$ is a Camina pair. Since $Z(G) = \gamma_3(G) \leq \gamma_2(G)$, so in both cases, we have

$p^2 \leq | \gamma_3(G) | = | Z(G) | \leq | [z, G] | = | [z, H\langle x \rangle] | = | [z, \langle x \rangle] | = p,$

since $x^p \in H$ and $z \in Z(H)$. This contradiction proves that $Z(G) = Z(H)$. □

CHAPTER 4

Proof of the Main Theorem

All the results presented here are from [1].

Throughout this chapter, the group G will be a finite p-group of order p^n. Let $\{x_1, x_2, \ldots, x_d\}$ be the minimal generating set for G. Let $\alpha \in \mathrm{Aut}_c(G)$. i.e. $\alpha(x_i) \in x_i^G$ for all $i, 1 \leq i \leq d$. It implies there are at most $\mid x_i^G \mid$ choices for the images of x_i under the mapping α for all $i, 1 \leq i \leq d$. Therefore,

$$\mid \mathrm{Aut}_c(G) \mid \ \leq \ \prod_{i=1}^{d} \mid x_i^G \mid \tag{4.1}$$

Let $\mid \gamma_2(G) \mid = p^m$. Then, by Theorem 2.32, we have $d \leq n - m$. Also, $\mid x_i^G \mid \leq \mid \gamma_2(G) \mid = p^m$ for all i, $1 \leq i \leq d$. Substituting the values in (4.1), we get:

$$\mid \mathrm{Aut}_c(G) \mid \leq \prod_{i=1}^{d} p^m = p^{md} \leq (p^m)^{n-m} = p^{m(n-m)}. \tag{4.2}$$

Theorem 4.1 *Let G be a finite p-group. If equality holds in* (4.2)*, i.e.*

$$\mid Aut_c(G) \mid = p^{md} = p^{m(n-m)} \tag{4.3}$$

then G is either an abelian p-group or a non-abelian Camina special p-group.

Proof. If G is abelian, then the proof is trivial. Let us assume that G is non - abelian. Since G has minimal generating set of d elements and $\gamma_2(G) \leq \Phi(G)$, so

$G/\gamma_2(G)$ has minimal generating set of d elements. Also, $G/\gamma_2(G)$ is abelian by Theorem 2.4, thus from Theorem 2.11 and (4.3), $G/\gamma_2(G)$ is the direct product of d non-trivial cyclic p-groups and hence it must be elementary abelian. Thus, it follows that if any arbitrary element $x \in G \setminus \gamma_2(G)$, then $x \in \{x_1, x_2, \ldots, x_{n-m}\}$. Now, we prove that $[x, G] = \gamma_2(G)$. If possible, suppose that $[x, G] \subset [G, G]$, then

$$| x^G | = | x[x, G] | = | [x, G] | < | [G, G] | = | \gamma_2(G) | = p^m.$$

Thus, from (4.1), $| Aut_c(G) | < p^{md} = p^{m(n-m)}$, a contradiction to (4.3). So, $[x, G] = [G, G] = \gamma_2(G)$ for all $x \in G \setminus \gamma_2(G)$ which implies that G is a Camina group. Thus, it follows from ([5], Main Theorem) that the nilpotency class of G is ≤ 3.

Since an automorphism maps generators to generators, thus it follows from (4.3) that we can define a class preserving automorphism α as follows:

$$\alpha(x_i) = x_i y_i \text{ for } 1 \leq i \leq n - m, \text{ where } y_i \in \gamma_2(G).$$

In particular, if we choose $y_1 = y_2 = \cdots = y_{n-m-1} = 1$ and $y_{n-m} = y \in \gamma_2(G)$, we get an α such that :

$$\alpha(x_i) = x_i, 1 \leq i \leq n - m - 1 \text{ and } \alpha(x_{n-m}) = x_{n-m} y.$$

where y is an arbitrary element of $\gamma_2(G)$.

We will now prove that the class of G is not equal to 3. If possible, suppose that class of G is 3. Let $G = \langle x_1, x_2, \ldots, x_{n-m} \rangle$. Thus, from Proposition 3.10, $H = \langle x_1, x_2, \ldots, x_{n-m-1} \rangle$ is a maximal subgroup of G such that $\gamma_2(H) = \gamma_2(G)$ and $\gamma_2(G) \not\leq Z(H)$. Since $\gamma_2(G) \neq Z(H)$, so there exists a non-trivial element $y \in \gamma_2(G) \setminus Z(H)$. So, by previous paragraph, we can select $\alpha \in \mathrm{Aut}_c(G)$ such that :

$$\alpha(x_i) = x_i, \ 1 \leq i \leq n - m - 1 \text{ and } \alpha(x_{n-m}) = x_{n-m} y.$$

Observe that $\alpha(h) = h$ for all $h \in H$ which implies that α centralizes H and $g^{-1}\alpha(g) \in H$ for all $g \in G$ which implies that α centralizes G/H as well. By ([6], Satz I.17.1), $\alpha(x_{n-m}) = x_{n-m}y$ for some $y \in Z(H)$, a contradiction. Thus, the class of G is less than or equal to 2. But G is non - abelian, so class of G is 2, and therefore by Corollary 3.8, G is a special p-group. □

Proposition 4.2 *Let G be a finite p-group of class 2. Then $\exists$ a monomorphism $f : \mathrm{Aut}_c(G) \to \mathrm{Hom}(G/Z(G), \gamma_2(G))$.*

Proof. Let $\phi \in \mathrm{Aut}_c(G)$. Define a map $f_\phi : G/Z(G) \to \gamma_2(G)$ by $f_\phi(gZ(G)) = g^{-1}\phi(g)$ for all $g \in G$. Now, we'll show that this map is well - defined and is a homomorphism.

f_ϕ is well - defined : Let $g_1Z(G), g_2Z(G) \in G/Z(G)$ such that $g_1Z(G) = g_2Z(G)$. It follows that $g_1 = g_2z$ for some $z \in Z(G)$. Now,

$$\begin{aligned} f_\phi(g_1Z(G)) = g_1^{-1}\phi(g_1) &= (g_2z)^{-1}\phi(g_2z) \\ &= z^{-1}g_2^{-1}\phi(g_2)\phi(z) \\ &= z^{-1}(g_2^{-1}\phi(g_2))z \\ &= (g_2^{-1}\phi(g_2))z^{-1}z \\ &= g_2^{-1}\phi(g_2) \\ &= f_\phi(g_2Z(G)). \end{aligned}$$

Thus, f_ϕ is a well-defined map.

f_ϕ is a homomorphism : Let $g_1Z(G), g_2Z(G) \in G/Z(G)$. Now,

$$\begin{aligned} f_\phi((g_1Z(G))(g_2Z(G))) &= f_\phi((g_1g_2)Z(G)) \\ &= (g_1g_2)^{-1}\phi(g_1g_2) \\ &= g_2^{-1}g_1^{-1}\phi(g_1)\phi(g_2) \\ &= (g_1^{-1}\phi(g_1))(g_2^{-1}\phi(g_2)) \quad g_1^{-1}\phi(g_1) \in \gamma_2(G) \leq Z(G) \\ &= f_\phi(g_1Z(G))f_\phi(g_2Z(G)). \end{aligned}$$

Therefore, f_ϕ is a homomorphism and thus $f_\phi \in \mathrm{Hom}(G/Z(G), \gamma_2(G))$.

Now, define a map $f : \mathrm{Aut}_c(G) \to \mathrm{Hom}(G/Z(G), \gamma_2(G))$ by

$$f(\phi) = f_\phi, \text{ where } f_\phi(gZ(G)) = g^{-1}\phi(g) \text{ for all } g \in G.$$

f is a homomorphism :

Let $\phi_1, \phi_2 \in \mathrm{Aut}_c(G)$. Then $f(\phi_1 \circ \phi_2) = f_{\phi_1 \ \circ \ \phi_2}$. Now,

$$\begin{aligned} f_{\phi_1 \ \circ \ \phi_2}(gZ(G)) &= g^{-1}\phi_1 \circ \phi_2(g) \\ &= g^{-1}\phi_1(\phi_2(g)) \\ &= g^{-1}\phi_1((gg^{-1})\phi_2(g)) \\ &= g^{-1}\phi_1(g(g^{-1}\phi_2(g)) \\ &= g^{-1}\phi_1(gz), \text{ where } z = g^{-1}\phi_2(G) \in \gamma_2(G) \leq Z(G). \\ &= g^{-1}\phi_1(g)\phi_1(z) \\ &= g^{-1}\phi_1(g)z \\ &= (g^{-1}\phi_1(g))(g^{-1}\phi_2(G)) \\ &= f_{\phi_1}(gZ(G))f_{\phi_2}(gZ(G)). \end{aligned}$$

Thus, $f(\phi_1 \circ \phi_2) = f(\phi_1)f(\phi_2)$ and hence f is a homomorphism.

f **is injective :** In order to show that f is injective , we will prove that $\mathrm{Ker}(f) = 1$.

Now,

$$\begin{aligned}\mathrm{Ker}(f) &= \{\phi \in \mathrm{Aut}_c(G) : f(\phi) = 1\} \\ &= \{\phi \in \mathrm{Aut}_c(G) : f_\phi = 1\}\end{aligned}$$

Observe that $1 = f_\phi(gZ(G)) = g^{-1}\phi(g)$ which means $\phi = 1$. Thus, $\mathrm{Ker}(\phi) = 1$.

Hence, f is a monomorphism from $\mathrm{Aut}_c(G)$ into $\mathrm{Hom}(G/Z(G), \gamma_2(G))$. □

Proposition 4.3 *Let G be a finite p-group of class 2. Then $\exists$ an isomorphism $f : \mathrm{Aut}_c(G) \to \mathrm{Hom}_c(G/Z(G), \gamma_2(G))$, where*

$$\mathrm{Hom}_c(G/Z(G), \gamma_2(G)) = \{f \in \mathrm{Hom}(G/Z(G), \gamma_2(G)) : f(gZ(G)) \in [g, G] \text{ for all } g \in G\}.$$

Proof. Let $\phi \in \mathrm{Aut}_c(G)$. Define a map $f_\phi : G/Z(G) \to \gamma_2(G)$ by $f_\phi(gZ(G)) = g^{-1}\phi(g)$ for all $g \in G$. Here, f_ϕ is well-defined and a homomorphism as proved in Proposition 4.2. Since $\phi \in \mathrm{Aut}_c(G), \phi(g) \in g^G$ which implies that $g^{-1}\phi(g) \in [g, G]$, and thus $f_\phi(gZ(G)) \in [g, G]$. Hence $f_\phi \in \mathrm{Hom}_c(G/Z(G), \gamma_2(G))$. Thus, from Proposition 4.2, it follows that f is a one-one homomorphism.

Now, we will show that f is onto. Let $\psi \in \mathrm{Hom}_c(G/Z(G), \gamma_2(G))$. Consider $\alpha_\psi : G \to G$ defined by $\alpha_\psi(g) = g\psi(gZ(G))$ for all $g \in G$.

α_ψ **is well - defined :** Let $g_1, g_2 \in G$ such that $g_1 = g_2$. Then

$$\begin{aligned}\alpha_\psi(g_1) &= g_1\psi(g_1Z(G)) \\ &= g_2\psi(g_2Z(G)) \\ &= \alpha_\psi(g_2).\end{aligned}$$

Thus, α_ψ is a well - defined map.

α_ψ **is injective :** In order to prove that α_ψ is injective, we'll show that $\mathrm{Ker}(\psi) = 1$.

Now, $\mathrm{Ker}(\alpha_\psi) = \{g \in G : \alpha_\psi(g) = 1\} = \{g \in G : g\psi(gZ(G)) = 1\}$. Observe that

$$1 = g\psi(gZ(G)) \Rightarrow g^{-1} = \psi(gZ(G)) \in [g, G] \subseteq \gamma_2(G) \leq Z(G).$$

$$\Rightarrow g \in Z(G).$$

Therefore, $g^{-1} = \psi(Z(G)) = 1$ that means $g = 1$. Thus, $\mathrm{Ker}(\alpha_\psi) = 1$.

α_ψ **is a homomorphism :** Let $g_1, g_2 \in G$. Then

$$\begin{aligned}
\alpha_\psi(g_1g_2) &= (g_1g_2)\psi((g_1g_2)Z(G)) \\
&= (g_1g_2)\psi((g_1Z(G))(g_2Z(G))) \\
&= (g_1g_2)\psi(g_1Z(G))\psi(g_2Z(G)) \\
&= g_1(g_2\psi(g_1Z(G)))\psi(g_2Z(G)) \\
&= g_1(\psi(g_1Z(G))g_2)\psi(g_2Z(G)), \psi(g_1Z(G)) \in [g, G] \leq \gamma_2(G) \leq Z(G) \\
&= (g_1\psi(g_1Z(G)))(g_2\psi(g_2Z(G))) \\
&= \alpha_\psi(g_1)\alpha_\psi(g_2).
\end{aligned}$$

Thus, α_ψ is a homomorphism.

α_ψ **is surjective :** Since G is a finite group, α_ψ is onto.

α_ψ **is class preserving :** Observe that $g^{-1}\alpha_\psi(g) = \psi(gZ(G)) \in [g, G]$ for all $g \in G$.

i.e. $\alpha_\psi(g) \in g^G$. Thus, α_ψ is class preserving. Hence, $\alpha_\psi \in \mathrm{Aut}_c(G)$.

Lastly, we want to show that $f(\alpha_\psi) = \psi$ which means that $f_{\alpha_\psi} = \psi$.

Observe that

$$\begin{aligned} f_{\alpha_\psi}(gZ(G)) &= g^{-1}(\alpha_\psi(g)) \\ &= g^{-1}(g\psi(gZ(G))) \\ &= (g^{-1}g)\psi(gZ(G)) \\ &= \psi(gZ(G)). \end{aligned}$$

Therefore, f is an onto map.

Hence, $f : \mathrm{Aut}_c(G) \to \mathrm{Hom}_c(G/Z(G), \gamma_2(G))$ is an isomorphism. □

The next lemma follows from ([10], p.335).

Lemma 4.4 *Let H and K be two elementary groups of order p^r and p^s respectively. Let*

$$H = \times_{i=1}^{r} H_i \quad \text{and} \quad K = \times_{j=1}^{s} K_j$$

where H_i and K_j are cyclic groups of order p , $1 \leq i \leq r$ and $1 \leq j \leq s$. Then, by Remark 2.48

$$\mathrm{Hom}(H, K) = \mathrm{Hom}(\times_{i=1}^{r} H_i, \times_{j=1}^{s} K_j) \cong \times_{i=1,j=1}^{r,s} \mathrm{Hom}(H_i, K_j).$$

It follows that $\mathrm{Hom}(H, K)$ *is an elementary abelian group of order p^{rs}.*

Theorem 4.5 *Let G be a finite p-group. Then* (4.3) *holds if and only if G is either an abelian p-group, or a non-abelian Camina special p-group.*

Proof. Let G be a finite p-group of order p^n and $\mid \gamma_2(G) \mid = p^m$. If G is abelian, then $\mid \gamma_2(G) \mid = 1$ implying $m = 0$. Thus, $\mid \mathrm{Aut}_c(G) \mid = 1 = p^{m(n-m)}$ and hence equality holds in (4.3) in this case.

Now, we assume that G is a non-abelian Camina special p-group. Then $\gamma_2(G) = [x, G]$ for all $x \in G \setminus \gamma_2(G)$. But $\gamma_2(G) = Z(G)$ as G is a special p-group. So, $\gamma_2(G) = [x, G]$ for all $x \in G \setminus Z(G)$. Also, for all $x, y \in G \setminus Z(G), [x, G][y, G] = [xy, G]$ such that $xy \notin Z(G)$. Consider $f \in \mathrm{Hom}(G/Z(G), \gamma_2(G))$. Then

$$f(xZ(G)) = f(\overline{x}) \in \gamma_2(G) = [x, G].$$

So, $f \in \mathrm{Hom}_c(G/Z(G), \gamma_2(G))$. Thus, $\mathrm{Hom}(G/Z(G), \gamma_2(G)) \leq \mathrm{Hom}_c(G/Z(G), \gamma_2(G))$. Clearly, $\mathrm{Hom}_c(G/Z(G), \gamma_2(G)) \leq \mathrm{Hom}(G/Z(G), \gamma_2(G))$. Therefore,

$$\mathrm{Hom}_c(G/Z(G), \gamma_2(G)) = \mathrm{Hom}(G/Z(G), \gamma_2(G)). \tag{4.4}$$

Since G is a special p-group, so $\gamma_2(G)$ and $G/Z(G)$ are elementary abelian p-groups such that $| \gamma_2(G) | = p^m$ and $| G/Z(G) | = p^{n-m}$. Thus, by Lemma 4.4,

$$\mathrm{Hom}(G/Z(G), \gamma_2(G)) = \mathrm{Hom}(\times_{i=1}^{n-m} C_i, \times_{j=1}^{m} C_j) \cong \times_{i=1,j=1}^{n-m,m} \mathrm{Hom}(C_i, C_j)$$

where C_i and C_j are cyclic groups of order p , $1 \leq i \leq n-m$ and $1 \leq j \leq m$. In particular , $\mathrm{Hom}(G/Z(G), \gamma_2(G))$ is an elementary abelian group of order $p^{(n-m)m}$. Therefore from (4.4) and Proposition 4.3 , we have

$$| \mathrm{Aut}_c(G) | = | \mathrm{Hom}_c(G/Z(G), \gamma_2(G)) | = | \mathrm{Hom}(G/Z(G), \gamma_2(G)) | = p^{m(n-m)}.$$

The converse has already been shown in Theorem (4.1). □

Theorem 4.6 *Let G be a non-trivial p-group having order p^n. Then :*

$$| \mathrm{Aut}_c(G) | \leq \begin{cases} p^{\frac{(n^2-4)}{4}} & \text{if } n \text{ is even,} \\ p^{\frac{(n^2-1)}{4}} & \text{if } n \text{ is odd.} \end{cases}$$

Proof. If G is abelian, then the proof is trivial. Assume that G is a non-abelian group and $| \gamma_2(G) | = p^m$. Observe that $| x^G | \leq | \gamma_2(G) | = p^m$ for all $x \in G$. Let

$\mid \Phi(G) \mid :=: p^t$. Since $\gamma_2(G) \leq \Phi(G)$ by Lemma 2.30, so $p^m \leq p^t$ which implies that $m \leq t$. Also $[G : \Phi(G)] = \mid G/\Phi(G) \mid = p^{n-t}$. Thus, by Theorem 2.32, it follows that from any generating set of G, we can choose $n - t$ elements that will thus generate G. Now, $n - t$ is maximum if $t = m$. Also, $1 \leq m \leq n - 2$ because $G/\gamma_2(G)$ cannot be cyclic.

Since, if $m = n$, then $\mid G/\gamma_2(G) \mid = 1$ which implies that $G/\gamma_2(G)$ is cyclic and thus G is cyclic. Also, if $m = n - 1$, then $\mid G/\gamma_2(G) \mid = p$, again making $G/\gamma_2(G)$ and hence G cyclic. Since every cyclic group is abelian, thus this brings a contradiction to our assumption that G is non - abelian.

Hence, $\mid G/\gamma_2(G) \mid \geq p^2$ implying $p^m \leq p^{n-2}$ that gives $m \leq n - 2$.

Now, if n is even, then the possible values of $m(n - m)$ are as follows

$$\{n - 1,\ 2(n - 2),\ 3(n - 3),\ \ldots,\ n^2/4\}$$

Notice that maximum value of $m(n - m)$ is $n^2/4$.

If n is odd, then the possible values for $m(n - m)$ are

$$\{n - 1,\ 2(n - 2),\ 3(n - 3),\ \ldots,\ (n + 1)(n - 1)/4\}$$

In this case, the maximum value of $m(n-m)$ is $(n^2-1)/4$. Substituting these values in (4.2), we get:

$$\mid \mathrm{Aut}_c(G) \mid \leq \begin{cases} p^{\frac{n^2}{4}} & \text{if n is even,} \\ p^{\frac{(n^2-1)}{4}} & \text{if n is odd.} \end{cases}$$

So, if n is odd, we get the desired result i.e. $\mid \mathrm{Aut}_c(G) \mid \leq p^{\frac{(n^2-1)}{4}}$ Thus, we assume that n is even. Suppose that $\mid \mathrm{Aut}_c(G) \mid = p^{n^2/4}$ which is the case when $m = n/2$. So, let us suppose that $m = n/2$. Therefore, $\mid \mathrm{Aut}_c(G) \mid = p^{m(n-m)}$ and so equality holds in relation (4.2). By Theorem 4.1, it follows that G is a Camina special p-group

because G is non-abelian. Thus, by ([7], Theorem 3.2) we have $n-m$ is even and $n-m \geq 2m$. Observe that $n-m$ refers to the minimal number of generators of G. Now $n-m \geq 2m$ implies that $m \leq n/3$, a contradiction. So, it follows that there exists no finite p-group for which $\mid \mathrm{Aut}_c(G) \mid = p^{n^2/4}$. Therefore, $\mid \mathrm{Aut}_c(G) \mid < p^{n^2/4}$. Thus,

$$\mid \mathrm{Aut}_c(G) \mid \leq p^{\frac{n^2}{4}-1} = p^{(n^2-4)/4}.$$

Combining the two cases, we get :

$$\mid \mathrm{Aut}_c(G) \mid \leq \begin{cases} p^{\frac{(n^2-4)}{4}} & \text{if n is even,} \\ p^{\frac{(n^2-1)}{4}} & \text{if n is odd.} \end{cases}$$

□

List of References

[1] MANOJ K. YADAV, *Class preserving automorphisms of finite p-Groups*, J. London Math. Soc. (2) **75** (2007), 755-772.

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

[3] W. BURNSIDE, *Theory of groups of finite order*, 2nd edn (Dover, New York, 1955).

[4] A. R. CAMINA, *Some conditions which almost characterize Frobenius groups*, Israel J. Math. **31** (1978), 153-160.

[5] R. DARK and C. M. SCOPPOLA, *On Camina groups of prime power order*, J. Algebra **181** (1996), 787-802.

[6] B. HUPPERT, *Endliche Gruppen* ***I*** (Springer, Berlin, 1967).

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

[8] I. D. MACDONALD, *More on p-groups of Frobenius type*, Israel J. Math. **56** (1986), 335-344.

[9] A. MANN and C. M. SCOPPOLA, *On p-groups of Frobenius type*, Arch. Math. (Basel) **56** (1991), 320-332.

[10] J. J. ROTMAN, *An introduction to the theory of groups*, 4th edn (Springer, New York, 1995).

[11] JOHN S. ROSE, *A course on group theory*, 1st edn , Cambridge University Press, 1978.

[12] DEREK J.S. ROBINSON, *A Course in the theory of groups*, 2nd edn , Springer-Verlag, 1982.