FINITE p-GROUPS IN WHICH EACH CENTRAL AUTOMORPHISM FIXES THE CENTER ELEMENTWISE

Thesis submitted in partial fulfillment of the requirement for

the award of the degree of

Masters of Science

In

Mathematics and Computing

Submitted by

Rohit Garg

Roll no. – 300903014

Under

the guidance of

Dr. Deepak Gumber

JULY 2011

School of Mathematics and Computer Applications

Thapar University

Patiala-147004(PUNJAB)

INDIA

Dedicated to

God,

Parents and Teachers.

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled **"Finite p-Groups in which each Central Automorphism Fixes the Centre elementwise"** in partial fulfillment of the requirements for the award of **Master of Science,** School of Mathematics and Computer Applications, Thapar University, Patiala is an authentic record of my own work carried out under the supervision of **Dr. Deepak Gumber.**

The matter presented in this thesis has not been submitted for the award of any other degree of this or any other university.

Rohit Garg
(Rohit Garg)

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

(Dr. Deepak Gumber)
Supervisor
Assistant Professor
SMCA, Thapar University, Patiala.

Countersigned by:

Dr. S.S. Bhatia 15/7
(Professor & Head)
School of Mathematics & Computer Applications
Thapar University, Patiala.

Dr. S.K. Mohapatra
Dean of Academic Affairs
Thapar University
Patiala.

ACKNOWLEDGEMENT

I feel privileged to express my sincere regards and gratitude to my supervisor Dr. Deepak Gumber for their expert guidance, cool temperament, valuable suggestions, support, advice and continuous encouragement throughout the course of my thesis work.

I am highly obliged to Prof. S.S. Bhatia, Head SMCA, Thapar University, Patiala, for their motivation and inspiration that trigged me for thesis work.

I would like to thank all the staff members and my co-students who were always there at the need of the hour and provided with all the help and facilities, which I required for the completion of my thesis. I am also thankful to the authors whose works I have consulted and quoted in this work.

I also extend my thanks to Mr. Hemant Kalra, the research scholar, School of Mathematics and Computer Applications, Thapar University, Patiala, who helped me at each step when I needed.

Last but not the least I would like to thank God for not letting me down at the time of crisis and showing me the silver lining in the dark clouds.

(Rohit Garg)

TABLE OF CONTENTS

Chapter-1
INTRODUCTION

Throughout p denotes a prime number. Let G be a finite group. We denote by G', $Z(G), \Phi(G)$, $Aut(G)$ and $Inn(G)$, respectively the commutator subgroup, the center, the Frattini subgroup, the automorphism group and the inner automorphism group of G. A non-abelian group G is called purely non-abelain if it has no non-trivial abelian direct factor. If G and H are two groups, we denote by $Hom(G,H)$ the set of all homomorphisms from G to H. Note that if H is abelian, then $Hom(G,H)$ is 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 $x \in G$. An automorphism α of G is called a central automorphism if $x^{-1}\alpha(x) \in Z(G)$ for each $x \in G$.

The set of all central automorphisms of G, denoted by $Aut_z(G)$, fixes G' elementwise and form a normal subgroup of the full automorphism group of G. We denote by $Aut_z^z(G)$ the group of all central automorphisms of G fixing $Z(G)$ element-wise. Curran and McCaughan [3] characterized finite p-groups G for which $Aut_z(G) = Inn(G)$. They proved that if G is a finite p-group, then $Aut_z(G) = Inn(G)$ if and only if $G' = Z(G)$ and $Z(G)$ is cyclic.

In [2] Attar proved that if G is a finite p-group, then $Aut_z^z(G) = Inn(G)$ if and only if G is abelian or G is nilpotent of class 2 and $Z(G)$ is cyclic. In [5] Curran gave necessary and sufficient conditions on finite p-group G of nilpotency class 2 such that each central automorphism of G fixes the center of G element-wise (that is $Aut_z(G) = Aut_z^z(G)$). In [7] Yadav gave a similar characterization for finite p-group G of nilpotency class 2 such that each central automorphism of G fixes the center of G element-wise.

Attar in [8] generalized Yadav [7] and Curran's [5] result. He find necessary and sufficient condition for a finite p-group of arbitrary nilpotency class such that $Aut_z(G) = Aut_z^z(G)$. We explain his results in our thesis.

Let G be a finite p-group. Let

$$G/G' = C_{p^{a_1}} \times C_{p^{a_2}} \times \ldots \times C_{p^{a_k}} ,$$

where $C_{p^{a_i}}$ is a cyclic group of order $p^{a_i}, 1 \leq i \leq k$, and $a_1 \geq a_2 \geq \ldots \geq a_k \geq 1$.

Let

$$G/G'\,Z(G) = C_{p^{b_1}} \times C_{p^{b_2}} \times \ldots \times C_{p^{b_l}}$$

and

$$Z(G) = C_{p^{c_1}} \times C_{p^{c_2}} \times \ldots \times C_{p^{c_m}} ,$$

where $b_1 \geq b_2 \geq \ldots \geq b_l \geq 1$, and $c_1 \geq c_2 \geq \ldots \geq c_m \geq 1$.

Since $G/G'\,Z(G)$ is a quotient of G/G', we have $l \leq k$ and $b_i \leq a_i$ for all $1 \leq i \leq l$.

The following theorem is the main theorem of our thesis:

Theorem: Let G be a non-abelian finite p-group. Then $Aut_z(G) = Aut_z^z(G)$ if and only if $Z(G) \leq G'$ or $Z(G) \leq \Phi(G), k = l$ and $c_1 \leq b_t$ where t is the largest integer between 1 and k such that $a_t > b_t$.

Chapter-2

PRELIMINARIES AND NOTATIONS

Definition 2.1 (***Center of a Group***)

The *center* $Z(G)$, of a group G is the subset of elements in G that commute with every element of G. In symbols, $Z(G) = \{a \in G \mid ax = xa \ \ \forall x \in G\}$.

The center is a subgroup of G.

For example, If $G = D_4 = \{x, y \mid x^2 = 1, y^4 = 1, yx = xy^3\}$, then $Z(G) = \{1, y^2\}$.

Remark: G is abelian iff $Z(G) = G$.

Proposition 2.2 $Z(G)$ is a normal subgroup of G.

Proof: Since e $\in Z(G)$, so $Z(G)$ is non-empty.

Now we will show that $Z(G)$ is a subgroup of G.

Let $a \in Z(G)$, so $ax = xa \ \ \forall\, x \in G$

$\Rightarrow a^{-1}x = xa^{-1} \ \ \forall\, x \in G$

$\Rightarrow a^{-1} \in Z(G)$.

Let $a, b \in Z(G)$, then $ax = xa$ and $bx = xb \ \ \forall\, x \in G$

$\Rightarrow abx = axb = xab \ \ \forall\, x \in G$

$\Rightarrow ab \in Z(G)$

Therefore $Z(G) \leq G$.

Now we will show that $Z(G)$ is normal in G.

Let $a \in Z(G), g \in G$ be any element.

Now $gag^{-1} = gg^{-1}a = a \in Z(G)$. So $Z(G)$ is normal in G. □

Theorem 2.3 Let G be a group and $Z(G)$ be the center of G. If $G/Z(G)$ is cyclic then G is abelian.

Proof: Let $gZ(G)$ be a generator of the factor group $G/Z(G)$, and let $a, b \in G$.

Then there exists integers i and j such that

$$aZ(G) = (gZ(G))^i = g^iZ(G)$$

and $bZ(G) = (gZ(G))^j = g^jZ(G)$

Thus, $a = g^ix$ for some $x \in Z(G)$

and $b = g^jy$ for some $y \in Z(G)$

Now $ab = (g^ix)(g^jy) = g^i(xg^j)y$

$= g^i(g^jx)y$, since $x \in Z(G)$

$= (g^ig^j)(xy) = (g^jg^i)(yx)$

$= (g^jy)(g^ix)$, since $y \in Z(G)$

$= ba$

Hence G is abelian. □

Definition 2.4 (***Commutator***)

If $a, b \in G$, the *commutator* of a and b denoted by $[a, b]$ and defined by $[a, b] = a^{-1}b^{-1}ab$.

Definition 2.5 (***Subgroup generated by subset of a Group***)

Let S be a subset of a group G. A subgroup H of G is said to be *subgroup generated by* S if it satisfies the following conditions.

1. $S \subseteq H$
2. If K is any subgroup of G such that $S \subseteq K$ then $H \subseteq K$.

We denote the subgroup generated by S by $\langle S \rangle$.

Definition 2.6 (***Rank of a Group G***)

The *rank* of a group G is the minimal size of a generating set of G, and is denoted $d(G)$. That is $d(G) = min\{|X| : X \subseteq G, \langle X \rangle = G\}$. For example, $d(D_4) = 2$.

Definition 2.7 (***Commutator Subgroup***)

The *commutator subgroup* G' of a group G is the subgroup generated by all the commutators of x and y. (That is, every element of G' has the form ${a_1}^{i_1}{a_2}^{i_2}{a_3}^{i_3}\ldots..{a_k}^{i_k}$, where each a_j has the form $x^{-1}y^{-1}xy$, each $i_j = \pm 1$, and k is any positive integer.)

For example, If $G = D_4$, then $Z(G) = \{1, y^2\}$.

Remark: G is abelian iff $G' = \{e\}$.

Lemma 2.8 If S is any non-void subset of a group G, then the subgroup $\langle S\rangle$ of G generated by S is the set of all finite products of the form $a_1a_2a_3\ldots..a_n$, where for each i, either $a_i \in S$ or ${a_i}^{-1} \in S$ and n is any positive integer.

Proof: Let H be the set of all finite products of the form $a_1a_2a_3\ldots..a_n$, where for each i , either $a_i \in S$ or ${a_i}^{-1} \in S$ and n be any positive integer.

Consider $x = a_1a_2a_3\ldots..a_n$, $y = b_1b_2b_3\ldots..b_m$ in H.

Then $xy = a_1a_2a_3\ldots..a_nb_1b_2b_3\ldots..b_m$ is a product of finite number of elements a_ib_j such that either the factor or its inverse is in S, consequently $xy \in H$.

Further $x^{-1} = {a_n}^{-1}{a_{n-1}}^{-1}\ldots..{a_2}^{-1}{a_1}^{-1}$.

Consider any ${a_i}^{-1}$. Since a_i or ${a_i}^{-1}$ is in S, and $a_i = ({a_i}^{-1})^{-1}$, we see that either ${a_i}^{-1}$ or $({a_i}^{-1})^{-1}$ is in S, hence $x^{-1} \in H$. This proves that H is a subgroup of G.

Clearly, $S \subseteq H$. Consider any subgroup K of G containing S. Then for each $a \in S$, we have $a \in K$ and hence $a^{-1} \in K$. Thus if $x = a_1a_2a_3\ldots..a_n;\ a_i \in S$ or ${a_i}^{-1} \in S$, is any element of H, then $x \in K$, since $a_i \in K\ \forall\ i$.

Hence $H \subseteq K$. This proves that H is the subgroup of G generated by S. □

Theorem 2.9 Let G be a group and G' be its commutator subgroup, then

1. G' is a normal subgroup of G.
2. For any normal subgroup H of G, G/H is an abelian group if and only if H contains G'.

Proof: 1. Let $a, b \in G$, since $(a^{-1}b^{-1}ab)^{-1} = b^{-1}a^{-1}ba$ is again a commutator, it follows from the above lemma that each element of G' is a product of finite number of commutators.

Consider $x \in G'$, then $x = g_1 g_2 g_3 \ldots\ldots g_t$ where for each $i = 1, 2, \ldots\ldots, t,\ g_i$ is a commutator, so that $g_i = {a_i}^{-1}{b_i}^{-1}a_i b_i$ for some $a_i, b_i \in G$.

Now for any $a \in G, a^{-1}xa = (a^{-1}g_1 a)(a^{-1}g_2 a)\ldots\ldots(a^{-1}g_t a)$.

Further

$a^{-1}g_i a = a^{-1}{a_i}^{-1}{b_i}^{-1}a_i b_i a = (a^{-1}a_i a)^{-1}(a^{-1}b_i a)^{-1}(a^{-1}a_i a)(a^{-1}b_i a) = c^{-1}d^{-1}cd;$ where $c = a^{-1}a_i a,\ d = a^{-1}b_i a$. Thus $a^{-1}g_i a$ is again a commutator.

Hence $a^{-1}xa$ is a product of commutators; by definition $a^{-1}xa \in G'$.

2. Consider $a, b \in G$. Let G/H be abelian. So $abH = baH\ \ \forall\ aH, bH \in G/H$.

Thus $a^{-1}b^{-1}ab \in H$. Thus H contains every commutator $a^{-1}b^{-1}ab$.

Consequently as G' is generated by all the commutators, $G' \subseteq H$.

Conversely let $G' \subseteq H$. Then $a^{-1}b^{-1}ab \in G'$ gives $a^{-1}b^{-1}ab \in H$ i.e $abH = baH$.

Thus $(aH)(bH) = (bH)(aH)\ \ \forall\ \ aH, bH \in G/H$. So G/H is abelian. □

Definition 2.10 (***Exponent of a Group***)

Let G be a finite group. Let k be the least positive integer such that $a^k = 1$ for all $a \in G$. Then k is called the *exponent* of G. Observe that k is the l.c.m of orders of all elements of G. For example, the exponent of D_4 is 4.

Lemma 2.11 Let G be a finite group and let $a \in G$ be an element of order n . Then $a^m = e$ if and only if n is a divisor of m .

Proof: Firstly let n is a divisor of m . So there exists a positive integer q such that $m = nq$. Now $a^m = a^{nq} = (a^n)^q = e$.

Conversely let $a^m = e$. Suppose m is not divisible by n . Dividing m by n, so $m = nq + r$ where $q, r \in I$ and $0 \leq r < n$. Thus $e = a^m = a^{nq+r} = a^{nq}.a^r = e.a^r = a^r$, a contradiction

Thus $r = 0$ and hence m is divisible by n. □

Theorem 2.12 Let G be a group and a be an element of order m . Then

$o(a^k) = \dfrac{m}{(m,k)}, k \in \mathbb{N}$.

Proof: Let $o(a^k) = t$. Now $a^{kt} = e$ but $o(a) = m$. Thus by lemma 2.11, $m|kt$.

Let $d = (m, k)$. Thus $d|m$ and $d|k$. Let $m = m_1 d$ and $k = k_1 d$ where $(m_1, k_1) = 1$. So $\frac{m}{d} = m_1$.

Thus we need to prove $m_1 = t$.

Now $m|kt$, so $m_1 d|k_1 dt$. Thus $m_1|k_1 t$, but $(m_1, k_1) = 1$.

Hence $m_1|t$ ... (1)

Again $(a^k)^{m_1} = a^{km_1} = a^{k_1 dm_1} = a^{k_1 m} = (a^m)^{k_1} = e$, but $o(a^k) = t$.

Hence $t|m_1$ ... (2)

From (1) and (2), we get $m_1 = t$. □

Definition 2.13 (***Centralizer of a Subgroup***)

If H is a subgroup of G, then by $C_G(H)$, the *centralizer* of H in G, we mean the set $\{x \in G \mid xh = hx \ \ \forall \ h \in H\}$.

Proposition 2.14 $C_G(H)$ is a subgroup of G.

Proof: Let $x \in C_G(H)$. Then $xh = hx \ \ \forall \ h \in H$

$\Rightarrow hx^{-1} = x^{-1}h \qquad \forall \ h \in H$

$\Rightarrow x^{-1} \in C_G(H)$

Let $x, y \in C_G(H)$. Then $xh = hx$ and $yh = hy \ \ \forall \ h \in H$

Now $xyh = xhy = hxy \ \ \forall \ h \in H$

So $xy \in C_G(H)$

Therefore $C_G(H) \leq G$. □

Definition 2.15 (***Normalizer of a Subgroup***)

If H is a subgroup of G, then by $N_G(H)$, the *normalizer* of H in G, we mean the set $\{x \in G \mid xHx^{-1} = H\}$.

Proposition 2.16 $N_G(H)$ is a subgroup of G.

Proof: Let $x \in N_G(H)$.

Then $xH = Hx \Rightarrow x^{-1}xHx^{-1} = x^{-1}Hxx^{-1} \Rightarrow Hx^{-1} = x^{-1}H$

so $x^{-1} \in N_G(H)$.

Let $x, y \in N_G(H)$, then $xH = Hx$ and $yH = Hy$

Now $xyH = xHy = Hxy$. So $xy \in N_G(H)$

Therefore $N_G(H) \leq G$. □

Proposition 2.17 If $H \leq G$, then H is normal in $N_G(H)$.

Proof: For all $a \in H$ we have $aH = Ha$.

Since $H \subseteq N_G(H)$ i.e H is a subgroup of G contained in $N_G(H)$.

Also for all $a \in N_G(H)$, we have $aH = Ha$.

So H is normal in $N_G(H)$. □

Proposition 2.18 If H and K are subgroups of G and H is a normal subgroup of K, then $K \subseteq N_G(H)$, i.e $N_G(H)$ is the largest subgroup of G in which H is normal.

Proof: Let $H \subseteq K \subseteq G$ such that H is a normal subgroup of K and K is a subgroup of G.

Now we will show that $K \subseteq N_G(H)$.

Let $k \in K$ be any element, then $Hk = kH$, since H is a normal subgroup of K.

So by the definition of $N_G(H), k \in N_G(H)$

Therefore $k \in N_G(H) \ \ \forall \ k \in K$

Hence $K \subseteq N_G(H)$. □

Proposition 2.19 H is a normal subgroup of G iff $N_G(H) = G$.

Proof: Firstly, let H is a normal subgroup of G.

Then $\forall\ g \in G$, we have $Hg = gH$. So $g \in N_G(H)$. Therefore $G \subseteq N_G(H)$.

But $N_G(H) \subseteq G$ always, hence $G = N_G(H)$.

Conversely let $N_G(H) = G$.

Therefore $N_G(H) = \{x \in G \mid xH = Hx\} = G$. So $xH = Hx \ \ \forall\, x \in G$.

Hence H is a normal subgroup of G. □

Proposition 2.20 $C_G(H)$ is normal in $N_G(H)$.

Proof: Let $a \in C_G(H)$, then $ah = ha \ \ \forall\, h \in H$.

Let $g \in N_G(H)$, then $gH = Hg$. Therefore $g^{-1}H = Hg^{-1}$. So $g^{-1}h = h_1g^{-1}$ for some $h, h_1 \in H$

Now $(gag^{-1})h = gah_1g^{-1} = gh_1ag^{-1} = h(gag^{-1})$.

So $C_G(H)$ is normal in $N_G(H)$. □

Definition 2.21 (***Conjugate elements***)

If a, b are any two elements of a group G, then b is said to be *conjugate* to a if $b = xax^{-1}$ for some $x \in G$, and we write it as $b \sim a$.

Lemma 2.22 The relation of conjugacy in a group G is an equivalence relation.

Proof: Define a relation $\sim$ on G as follows:

$a \sim b$ iff $a = gbg^{-1}$ for some $g \in G$.

Let a, b, c be any arbitrary elements of G.

Since $a = eae^{-1}$. Thus $a \sim a$.

Therefore $\sim$ is reflexive.

Let $a \sim b$. So there exists $g \in G$ such that $a = gbg^{-1}$.

Thus $g^{-1}ag = g^{-1}a(g^{-1})^{-1} = b$. So $b \sim a$.

Therefore $\sim$ is symmetric.

Let $a \sim b$ and $b \sim c$. So there exists $g, h \in G$ such that $a = gbg^{-1}$ and $b = hch^{-1}$.

Now $a = gbg^{-1} = g(hch^{-1})g^{-1} = (gh)c(gh)^{-1}$. So $a \sim c$.

Therefore $\sim$ is transitive.

Hence the relation of conjugacy in a group G is an equivalence relation. □

Lemma 2.23 Let G be a group. Then the set of conjugacy classes of G is a partition of G.

Proof: Define a relation $\sim$ on G as follows

$a \sim b$ iff $a = gbg^{-1}$ for some $g \in G$.

By lemma 2.22, $\sim$ is an equivalence relation on G.

The equivalence class of a in G is the set $cl(a) = \{gag^{-1} | \ g \in G\}$, which is also the *conjugacy class of* a .

Thus the set of conjugacy classes of G is a partition of G. □

Lemma 2.24 (***The Number of Conjugates of*** $\boldsymbol{a}$)

Let G be a finite group and let a be an element of G. Then $|cl(a)| = [G: C_G(a)]$.

Proof: Consider a function $T: cl(a) \to G/C_G(a)$ such that $T(xax^{-1}) = xC_G(a)$.

Let $xax^{-1}, yay^{-1} \in cl(a)$, where $x, y \in G$ such that

$T(xax^{-1}) = T(yay^{-1})$

$\Rightarrow \ xC_G(a) = yC_G(a) \Rightarrow \ x^{-1}y \in C_G(a) \Rightarrow \ x^{-1}ya = ax^{-1}y$

$\Rightarrow \ xx^{-1}yay^{-1} = xax^{-1}yy^{-1} \Rightarrow yay^{-1} = xax^{-1}$

Therefore T is one-one.

Clearly for $xC_G(a) \in G/C_G(a)$, where $x \in G$, we have $T(xax^{-1}) = xC_G(a)$

Therefore T is onto. Hence $|cl(a)| = [G: C_G(a)]$. □

Theorem 2.25 (***The Class Equation***)

For any finite group $G, |G| = \sum[G: C_G(a)]$, where the sum runs over one element a from each conjugacy class of G. □

Definition 2.26 (***Maximal Subgroup***)

Let G be a group. A subgroup N of G is called a *maximal subgroup* if

1. $N \neq G$.
2. If $N \leq H \leq G$, then $H = N$ or $H = G$.

Definition 2.27 (***p-group***)

A group of order p^n, where p is a prime, is called a *p-group.*

Theorem 2.28 Let G be a p-group. Then

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

Proof: First observe that $cl(a) = \{a\}$ if and only if $a \in Z(G)$. Thus by culling out these elements, we may write the class equation in the form

$|G| = |Z(G)| + \sum_{a \in X}[G: C_G(a)]$, where X is a subset of G contains exactly one element from each conjugacy class with more than one element.

1. By *Lagrange's Theorem*, $|C_G(a)| \mid |G|$

Now $a \in Z(G) \Leftrightarrow C_G(a) = G$. If $a \notin \mathrm{Z}(G)$ then $C_G(a) < G$

$\Rightarrow |C_G(a)| \leq p^{n-1}$

$\Rightarrow \dfrac{|G|}{|C_G(a)|} \geq p$

So $[G: C_G(a)] \geq p$

$\Rightarrow p \mid [\mathrm{G}: C_G(a)] \Rightarrow p \mid \sum_{a \in X}[G: C_G(a)]$

$\Rightarrow p \mid (|G| - \sum_{a \in X}[G: C_G(a)])$ i.e $p \mid |Z(G)|$

So $Z(G)$ is non-trivial.

2. We have $G = Z(G) \cup (\bigcup_{a \in X} cl(a))$

$N = N \cap G = N \cap (Z(G) \cup (\bigcup_{a \in X} cl(a)))$

$= \big(N \cap Z(G)\big) \cup (N \cap (\bigcup_{a \in X} cl(a))$

Hence $|N| = |Z(G) \cap N| + \sum_{a \in X}|cl(a) \cap N|$ ... (1)

If $a \in N$, then $cl(a) \subset N$. In this case $cl(a) \cap N = cl(a)$.

Suppose $a \notin N$ and $cl(a) \cap N \neq \emptyset$. Let $y \in cl(a) \cap N$.

Then $y \in cl(a)$ and $y \in N$. Let $y = gag^{-1}$, where $g \in G$

Then $gag^{-1} \in N \Rightarrow g^{-1}(gag^{-1})g = a \in N$, a contradiction, so $cl(a) \cap N = \emptyset$.

Thus $cl(a) \cap N = cl(a)$ or $\emptyset \quad \forall\, a \in X$

$\Rightarrow |cl(a)) \cap N|$ is 0 or $|cl(a)|$ i.e 0 or $[G: C_G(a)]$

But $p \mid [G: C_G(a)] \quad \forall\, a \in X$. So $p \mid |cl(a) \cap N| \quad \forall\ a \in X$

$\Rightarrow \ p \mid \sum_{a \in X} |cl(a) \cap N|$

Also $p \mid |N|$

Therefore by (1), $p \mid |Z(G) \cap N|$. Hence $Z(G) \cap N$ is non-trivial.

3. Let K be a maximal normal subgroup of G contained in H.

The quotient group G/K is of order $p^r (r > 0)$

Now by part-1, $Z(G/K)$ is non-trivial.

Let $L/K = Z(G/K)$.

Now $L/K \lhd G/K$, so $L \lhd G$.

Clearly L cannot be in H, because otherwise maximality of K is lost.

Let $h \in H, l \in L$, then $hK \in G/K$ and $lK \in L/K$

Because $L/K = Z(G/K)$, so

$(lK)(hK) = (hK)(lK)$

$\Rightarrow lhK = hlK \Rightarrow l^{-1}hl \in hK \subset H$.

Therefore $L \subset N_G(H)$. This implies that $H \neq N_G(H)$.

Because $H \subset N_G(H)$, it follows that H is properly contained in $N_G(H)$.

4. If H is a maximal subgroup of G, then by part-3, $H < N_G(H)$ implies that

$N_G(H) = G$; therefore by proposition 2.19, $H \lhd G$. □

Definition 2.29 (***Group Homomorphism***)

A *homomorphism* ϕ from a group G to a group $\bar{G}$ is a mapping from G into $\bar{G}$ that preserves the group operation; that is, $\phi(ab) = \phi(a)\phi(b) \ \forall\, a, b \in G$.

Some Standard Definitions

A *monomorphism* is an injective homomorphism.

An *epimorphism* is a surjective homomorphism.

An *isomorphism* is a bijective homomorphism.

An *endomorphism* is a homomorphism of a group to itself.

An *automorphism* is an isomorphism of a group with itself.

Definition 2.30 (***Kernel of a Homomorphism***)

The *kernel* of a homomorphism ϕ from a group G to a group $\bar{G}$ with identity $\bar{e}$ is the set $\{x \in G \mid \phi(x) = \bar{e}\}$. The kernel of ϕ is denoted by Ker ϕ.

Theorem 2.31 Let G and $\bar{G}$ be any two groups, e and $\bar{e}$, their respective identities. If ϕ is a homomorphism of G onto $\bar{G}$. Then

1. $\phi(e) = \bar{e}$.
2. ϕ is a monomorphism if and only if Ker $\phi = \{e\}$.

Proof: 1. Since $e.e. = e, \phi(e)\phi(e) = \phi(e)$.

However $\phi(e) \in \bar{G}$ gives $\phi(e) = \bar{e}\phi(e)$.

Thus $\phi(e)\phi(e) = \bar{e}\phi(e) \Rightarrow \phi(e) = \bar{e}$, by right cancellation in $\bar{G}$.

2. Let ϕ be a homomorphism of a group G into a group $\bar{G}$.

Suppose that ϕ is 1-1. Let $x \in$ ker ϕ.

Then $\phi(x) = \bar{e}$.

Also by part-1, $\phi(e) = \bar{e}$. Thus $\phi(e) = \phi(x) \Rightarrow x = e$.

This proves that ker $\phi = \{e\}$.

Conversely let ker $\phi = \{e\}$.

Let $x, y \in G$, be such that $\phi(x) = \phi(y)$.

Then $\phi(x)\phi(y)^{-1} = \bar{e} \Rightarrow \phi(xy^{-1}) = \bar{e}$

$\Rightarrow xy^{-1} \in$ ker $\phi = \{e\}$

$\Rightarrow xy^{-1} = e \Rightarrow x = y$.

Hence ϕ is 1-1. □

Definition 2.32 (***Internal Direct Product of H and K***)

Let H and K be normal subgroups of a group G. We say that G is the *internal direct product of H* and K and write $G = H \times K$ if $G = HK$ and $H \cap K = \{e\}$.

Definition 2.33 (***Internal Direct Product of*** $\boldsymbol{H_1 \times H_2 \times \ldots \times H_n}$)

Let $H_1, H_2, \ldots, H_n$ be a finite collection of normal subgroups of G. We say that G is the *internal direct product* of $H_1, H_2, \ldots, H_n$ and write $G = H_1 \times H_2 \times \ldots \times H_n$, if

1. $G = H_1 H_2 \ldots H_n = \{h_1 h_2 \ldots h_n | h_i \in H_i\}$
2. $(H_1 H_2 \ldots H_i) \cap H_{i+1} = \{e\}$ for $i = 1,2, \ldots, n-1$.

Theorem 2.34 (***Fundamental Theorem of Finite Abelian Groups***)

Every Abelian group G of order n is an internal direct product $G = G_1 \times G_2 \times \ldots \times G_t$, where G_l are cyclic subgroups of order n_l such that $n_{l+1} | n_l$ and the integers n_l are uniquely determined. Further $n = n_1 n_2 \ldots n_t$.

Proof: We prove the result by induction on $o(G)$. If $o(G) = 1$, the result holds trivially.

Suppose $o(G) = n > 1$ and the result holds for all abelian groups of order $< o(G)$.

Let n_1 be the exponent of G and g_1 be the element of G of order n_1.

Let $G_1 = \langle g_1 \rangle$. If $G = G_1$, then G itself is cyclic. Let $G \neq G_1$. Then

$1 < o(G/G_1) < n$.

By induction hypothesis $G/G_1 = H_1 \times H_2 \times \ldots \times H_t$, where each H_l is a cyclic subgroup of $\bar{G} = G/G_1$ of order $n_l > 1$ such that $n_{l+1} | n_l \ \forall \ \ l = 2,3,2, \ldots, t-1$, and

$$\frac{n}{n_1} = o(\bar{G}) = n_2 n_3 \ldots n_t \ . \qquad \ldots (1)$$

Now each $\overline{H_l} = H_l/G_1$ for some subgroup H_l of G containing G_1.

Choose $h_l \in H_l$ such that $\bar{h_l} = h_l/G_1$ is a generator of $\overline{H_l}$.

Then $\bar{h_l}^{n_l} = \bar{e} = G_1 \ \Rightarrow {h_l}^{n_l} \in G_1 \ = \langle g_1 \rangle \Rightarrow \ {h_l}^{n_l} = {g_1}^{m_l}$ for some m_l such that $1 \leq m_l < n_1$.

Let $\alpha_l = (m_l, n_1)$. Then

$m_l = \alpha_l \beta_l$ for some $\beta_l \geq 1, n_1 = \alpha_l \gamma_l$ for some $\gamma_l \geq 1$ and $(\beta_l, \gamma_l) = 1$.

Now $o(g_1) = n_1 = \alpha_l\gamma_l \Rightarrow o({g_1}^{\alpha_l}) = \gamma_l$.

As $(\gamma_l, \beta_l) = 1$, so by theorem 2.11, $o\left({g_1}^{\alpha_l\beta_l}\right) = o({g_1}^{\alpha_l})$.

However ${h_l}^{n_l} = {g_1}^{\alpha_l\beta_l}$. So $o({h_l}^{n_l}) = \gamma_l$.

On the other hand $o(\overline{h_l})|o(h_l) \Rightarrow n_l|o(h_l) \Rightarrow o({h_l}^{n_l}) = \frac{o(h_l)}{n_l}$

$\Rightarrow o(h_l) = o({h_l}^{n_l})n_l = \gamma_l n_l$. ... (2)

Since $o(h_l)|n_l$, the exponent of G and $n_1 = \alpha_l\gamma_l$, we have $\gamma_l n_l|\alpha_l\gamma_l$.

So $n_l|\alpha_l \Rightarrow \alpha_l = n_l\delta_l$ for some $\delta_l \geq 1$. Then ${h_l}^{n_l} = {g_1}^{n_l\delta_l\beta_l}$.

Put $g_l = h_l(g_1)^{-\delta_l\beta_l} \quad \forall\, l = 2,3,\ldots,t$.

We see that $\overline{g_l} = g_l G_1 = \overline{h_l}$, ${g_l}^{n_l} = {h_l}^{n_l}(g_1)^{-n_l\delta_l\beta_l} = e$. This yield $o(g_l) = n_l$.

Define $H = \langle g_2\rangle\langle g_3\rangle\ldots\langle g_t\rangle$. H is subgroup of G such that $o(H)|n_2n_3\ldots n_t$.

Let $f: G \to G/G_1$ be the natural homomorphism.

Since $f(H) = \langle\overline{g_2}\rangle \times \langle\overline{g_3}\rangle \times\ldots\times \langle\overline{g_t}\rangle = \overline{H_2} \times \overline{H_3} \times\ldots\times \overline{H_t} = G/G_1$

and also $f(H) = (HG_1)/G_1$, we get $G = HG_1 = G_1H = \langle g_2\rangle\langle g_3\rangle\ldots\langle g_t\rangle$.

The fact that $o(G) = n = n_1n_2\ldots n_t = o(g_1)o(g_2)\ldots.o(g_t)$ gives $G = \langle g_1\rangle \times \langle g_2\rangle \times\ldots\times \langle g_t\rangle$.

Also $o(\langle g_l\rangle) = o(g_l) = n_l$ such that $n_{l+1}|n_l$.

Suppose $G = H_1 \times H_2 \times \ldots \times H_t$ ... (3)

$= K_1 \times K_2 \times \ldots \times K_t$ ... (4)

Be two decompositions of G into internal direct product of cyclic subgroups, such that for $l = 1,2,\ldots,t\,, j = 1,2,\ \ldots, u, o(H_l) = n_l, o\left(K_j\right) = m_j$, for $l \leq t-1, n_{l+1}|n_l$ and for $j \leq u-1, m_{j+1}|m_j$.

Consider $g \in G$, then (3) gives $g = h_1h_2\ldots h_t\ ;\ h_l \in H_l$.

Since $o(h_l)|o(H_l) = n_l$ and $n_l|n_1$, we get ${h_l}^{n_l} = e$.

Consequently $g^{n_1} = {h_1}^{n_1}{h_2}^{n_2}\ldots{h_l}^{n_l} = e$. Thus $o(g) \leq n_1 \quad \forall\, g \in G$.

Further as H_1 is cyclic group of order n_1, H_1 contains an element of order n_1.

Hence n_1 is the exponent of G.

Similarly m_1 is the exponent of G. Thus $n_1 = m_1$.

Suppose we have proved that $n_1 = m_1, n_2 = m_2, \ldots, n_{l-1} = m_{l-1}$ for some l.

We shall prove that $n_l = m_l$.

Suppose on the contrary $n_l \neq m_l$, and to be definite let $n_l > m_l$.

Define $K = \{x^{m_l} | \ x \in G\}$. Since for any $x, y \in G, x^{m_l} y^{-m_l} = (xy^{-1})^{m_l} \in K$, we get that K is a subgroup of G.

Suppose that for $k = 1,2,\ldots,t$, $H_k = \langle a_k \rangle$ and for each $j = 1,2,\ldots,u$, $K_j = \langle b_j \rangle$.

Since for $j \geq l$, $o(K_j) = m_j | m_l$, ${b_j}^{m_l} = e$.

Hence $K = \langle {b_1}^{m_l} \rangle \times \langle {b_2}^{m_l} \rangle \times \ldots \times \langle {b_{l-1}}^{m_l} \rangle$.

Since $o(b_j) = m_j \quad \forall \ j$

Thus

$$o(K) = \frac{m_1}{m_l}\frac{m_2}{m_l} \ldots \frac{m_{l-1}}{m_l}, \qquad \ldots (5)$$

Since also $G = \langle a_1 \rangle \times \langle a_2 \rangle \times \ldots \times \langle a_t \rangle$ [from (3)]

We have $K = \langle {a_1}^{m_l} \rangle \times \langle {a_2}^{m_l} \rangle \times \ldots \times \langle {a_t}^{m_l} \rangle$.

Now by theorem 2.12, we have

$$o({a_k}^{m_l}) = \frac{n_k}{(m_l, n_l)} \quad \forall \ k = 1,2,\ldots,t \ .$$

Consequently

$$o(K) = \frac{n_1}{(m_l, n_1)}\frac{n_2}{(m_l, n_2)} \cdots \frac{n_l}{(m_l, n_l)}\frac{n_{l+1}}{(m_l, n_{l+1})} \cdots \frac{n_t}{(m_l, n_t)} \qquad \ldots (6)$$

Now $m_l | m_j$ and $m_j = n_j \quad \forall \ j < l$, by our hypothesis.

Thus

$$\frac{n_j}{(m_l, n_j)} = \frac{m_j}{(m_l, m_j)} = \frac{m_l}{m_l} \quad \forall \ j < l.$$

Hence from (5) and (6) we obtain,

$$1 = \frac{n_l}{(m_l, n_l)} \cdots \frac{n_t}{(m_l, n_t)} \qquad \ldots (7)$$

However $m_l < n_l$ gives

$$\frac{n_l}{(m_l, n_l)} > 1.$$

As a consequence, (7) cannot hold. This gives $m_l = n_l$.

Hence by induction $m_l = n_l \quad \forall \ l$.

However $n = n_1 n_2 \ldots n_t = m_1 m_2 \ldots m_u$. This we must also have $t = u$.

This completes the theorem. □

Definition 2.35 If G and H are two groups, we denote by $Hom(G, H)$ the set of all group homomorphisms from G to H.

Theorem 2.36 If H is abelian, then $Hom(G, H)$ is 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: 1. Associative Property:

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

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

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

So associative property holds.

2. Existence of Identity:

Let $I: G \to H$ be defined by $I(x) = x \quad \forall\, x \in G$. Clearly $I \in Hom(G, H)$.

Let $f \in Hom(G, H)$. Then $(fI)(x) = f(x)I(x) = f(x) = I(x)f(x) = (If)(x)$.

So I is the identity.

3. Existence of Inverse:

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

Define $f^{-1}: G \to H$ by $f^{-1}(x) = (f(x))^{-1}$.

Now $f^{-1}(xy) = \big(f(xy)\big)^{-1} = \big(f(x)f(y)\big)^{-1}$

$= \big(f(y)\big)^{-1}\big(f(x)\big)^{-1} = f^{-1}(y)f^{-1}(x)$

$= f^{-1}(x)f^{-1}(y)$.

Thus $f^{-1} \in Hom(G, H)$.

Now $(ff^{-1})(x) = f(x)f^{-1}(x)$

$= f(x)\big(f(x)\big)^{-1} = I.$

Similarly $(f^{-1}f)(x) = f^{-1}(x)f(x)$

$= \big(f(x)\big)^{-1}f(x) = I.$

So f^{-1} is the inverse of f.

4. Commutative Property:

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

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

$= g(x)f(x) = (gf)(x).$

So $fg = gf$. □

Lemma 2.37 Let A and B be abelian groups. Then $Hom(A, B) = Hom(B, A)$.

Proof: Proof can be found in [6]. □

Theorem 2.38 $Hom\big(Z_{p^m}, Z_{p^n}\big) \cong Hom\left(Z_{p^{min(m,n)}}\right)$.

Proof: Let $Z_{p^m} = \langle a \rangle$. For any non zero $c \in Z_{p^n}$, such that $|c|$ divides $|a|$, we have a non-zero homomorphism $H_c: Z_{p^m} \to Z_{p^n}$ given by $H_c(a) = c$.

If $m \geq n$, then each $0 \neq c \in Z_{p^n}$ is such that $|c| \mid p^n$ and hence $|c| \mid p^m$.

So $\big|Hom\big(Z_{p^m}, Z_{p^n}\big)\big| = p^n$.

Let $Z_{p^n} = \langle b \rangle$ and $H_b(a) = b$.

If $c \in Z_{p^n}$, then $c = rb$. Thus $T_c \equiv T_{rb}$.

So $T_{rb}(a) = rb = r\big(T_b(a)\big) = (rT_b)(a)$.

Hence $T_{rb} \equiv rT_b$. Therefore $T_c \equiv T_{rb} \equiv rT_b$.

So $Hom\big(Z_{p^m}, Z_{p^n}\big) = \langle T_b \rangle$.

Hence $Hom\big(Z_{p^m}, Z_{p^n}\big) \cong Z_{p^n}$.

Now let $n \geq m$. Then similarly $Hom(Z_{p^n}, Z_{p^m}) \cong Z_{p^m}$.

By lemma 2.37, $Hom(Z_{p^m}, Z_{p^n}) = Hom(Z_{p^n}, Z_{p^m})$.

So $Hom(Z_{p^m}, Z_{p^n}) \cong Z_{p^m}$.

Hence $Hom(Z_{p^m}, Z_{p^n}) \cong Hom\left(Z_{p^{min(m,n)}}\right)$. □

Definition 2.39 (***Frattini subgroup*** $\boldsymbol{\Phi(G)}$)

If G is a group, then its *Frattini subgroup* $\Phi(G)$ is defined as the intersection of all maximal subgroups of G.

For example, $\Phi(G) = \{1, y^2\}$.

Definition 2.40 (***Nongenerator element of a Group***)

An element $x \in G$ is called a *nongenerator* if it can be omitted from any generating set i.e if $G = \langle x, Y \rangle$, then $G = \langle Y \rangle$.

Theorem 2.41 For any group G, the Frattini subgroup $\Phi(G)$ is the set of all nongenerators.

Proof: Let x be a nongenerator of G, and let M be a maximal subgroup of G.

If $x \notin M$, then $G = \langle x, M \rangle = M$, a contradiction, therefore $x \in M$, for all M, and so $x \in \Phi(G)$.

Conversely if $z \in \Phi(G)$, assume that $G = \langle z, Y \rangle$.

If $\langle Y \rangle \neq G$, then there exists a maximal subgroup M with $\langle Y \rangle \leq M$.

But $z \in M$, and so $G = \langle z, Y \rangle \leq M$, a contradiction.

Therefore z is a nongenerator. □

Definition 2.42 (***Elementary Abelian*** $\boldsymbol{p}$***-group***)

An *elementary abelian* p*-group* is a finite abelian group where every nontrivial element has order p, where p is a prime. For example, Klein four-group is elementary abelian 2-group.

Lemma 2.43 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 $\Phi(G) \leq H$.

Proof: Firstly notice that every maximal subgroup of a p-group is normal, and of index p.
This means that if M is a maximal subgroup of G, then G/M is cyclic of order p.
Hence by theorem 2.9(part-2), $G' \leq M$ for all maximal subgroups M; consequently $G' \leq \Phi(G)$, and so $G/\Phi(G)$ is abelian.

Also, since G/M has order p (for M a maximal subgroup of G), we know that $(xM)^p = M$ for all $x \in G$; i.e, $x^p \in M$ for all $x \in G$ and all maximal subgroups M.
Thus $x^p \in \Phi(G)$, and so if $x\Phi(G) \in G/\Phi(G)$, then $x\Phi(G)$ has order p.
Hence $G/\Phi(G)$ is elementary abelian.

Now suppose that G/H is elementary abelian of order p^n.
Then G/H is generated by n cosets x_iH of G/H, each of order p.
We know then that

$$G/\mathrm{H} \cong \langle x_1H\rangle \times \langle x_2H\rangle \times \ldots \times \langle x_nH\rangle.$$

Now, this group has n maximal subgroups, H_i/H, each generated by $\{x_jH : j \neq i\}$.
Since this is direct product, the intersection satisfies

$$\bigcap_{1\leq j\leq n} H_j/H = 1.$$

This means that the intersection of all H_j is H.

But the H_j/H are maximal subgroups of G/H, and hence H_j are maximal subgroups of G.
This clearly implies that their intersection contains $\Phi(G)$. Hence

$$H = \bigcap_{1\leq j\leq n} H_j \geq \Phi(G).$$

Hence $H \geq \Phi(G)$. □

Theorem 2.44 Let G^p denote the group generated by the set $\{g^p : g \in G\}$; i.e the smallest group containing all elements of order p. Then $\Phi(G) = G'G^p$.
Proof: Since $\Phi(G)$ contains all x^p, as we saw in the proof of lemma 2.43, $G^p \leq \Phi(G)$.
Also, $G' \leq \Phi(G)$ since $G/\Phi(G)$ is abelian. Thus $G'G^p \leq \Phi(G)$.

Since $x^p \in G^p \leq G'G^p$ for all $x \in G$. So if $xG'G^p \in G/G'G^p$, then $xG'G^p$ has order p.

Hence $G/G'G^p$ is elementary abelian, and so $\Phi(G) \leq G'G^p$ by lemma 2.43.

Hence $\Phi(G) = G'G^p$. □

Definition 2.45 (***Central Automorphism of G***)

An automorphism α of G is called a *central automorphism* if $x^{-1}\alpha(x) \in Z(G)$ for each $x \in G$. The central automorphisms of G is denoted by $Aut_z(G)$.

We denote by $Aut_z^z(G)$ the group of all central automorphisms of G fixing $Z(G)$ elementwise.

For example, Let α be a homomorphism defined on D_4 such that $\alpha(x) = xy^2, \alpha(y) = y^3$.

Here α is a central automorphism of D_4 fixing $Z(D_4)$ elementwise.

Lemma 2.46 The central automorphisms of G, denoted by $Aut_z(G)$ form a normal subgroup of the full automorphism group.

Proof: Let $f, g \in Aut_z(G)$. We have to show that $fg \in Aut_z(G)$ i.e $x^{-1}(fg)(x) \in Z(G)$ for each $x \in G$.

Now $x^{-1}(fg)(x) = x^{-1}(f(g(x))) = x^{-1}(f(xx^{-1}g(x)))$

$= x^{-1}f(x)f(x^{-1}g(x)) \in Z(G)$.

Hence $Aut_z(G)$ form a subgroup of the full automorphism group.

Let $\phi \in Aut(G)$ and $\psi \in Aut_z(G)$.

We have to show that $\phi^{-1}\psi\phi \in Aut_z(G) \quad \forall\, \phi \in Aut(G)$.

Let $g \in G$. Then

$g^{-1}(\phi^{-1}\psi\phi)(g) = g^{-1}\phi^{-1}\left(\psi\big(\phi(g)\big)\right)$

$= g^{-1}\phi^{-1}\left(\phi(g)\phi(g)^{-1}\psi\big(\phi(g)\big)\right) = g^{-1}\phi^{-1}(\phi(g)z)$, where $z \in Z(G)$

$= g^{-1}\phi^{-1}\big(\phi(g)\big)\phi^{-1}(z) = g^{-1}g\phi^{-1}(z) = \phi^{-1}(z) \in Z(G)$.

Hence $Aut_z(G)$ is a normal subgroup of $Aut(G)$. □

Lemma 2.47 $Aut_z^z(G)$ is a normal subgroup of $Aut(G)$.

Proof: Let $f, g \in Aut_z^z(G)$. So $f(z) = z$ and $g(z) = z \quad \forall\, z \in Z(G)$.

Consider $(fg^{-1})(z) = f\big(g^{-1}(z)\big) = f(z) = z$.

So $fg^{-1} \in Aut_z^z(G)$.

Therefore $Aut_z^z(G)$ is a subgroup of $Aut(G)$.

Let $\phi \in Aut(G)$ and $\psi \in Aut_z^z(G)$.

Consider $(\phi^{-1}\psi\phi)(z) = \phi^{-1}\psi\big(\phi(z)\big) = \phi^{-1}(\phi(z)) = \phi^{-1}\phi(z) = z$

Therefore $Aut_z^z(G)$ is a normal subgroup of $Aut(G)$. □

Lemma 2.48 The central automorphisms $Aut_z(G)$ of G fixes G' elementwise.

Proof: We know that

$G' = \langle [x, y] = x^{-1}y^{-1}xy \mid x, y \in G \rangle$.

Let $\alpha \in Aut_z(G)$ and $[g, h] \in G'$, where $g, h \in G$.

Therefore $[g, h]^{-1}\alpha([g, h]) \in Z(G)$.

Let $[g, h]^{-1}\alpha([g, h]) = z_1 \in Z(G)$.

$\Rightarrow\ (g^{-1}h^{-1}gh)^{-1}\alpha(g^{-1}h^{-1}gh) = z_1$

$\Rightarrow\ (h^{-1}g^{-1}hg)\alpha(g^{-1})\alpha(h^{-1})\alpha(g)\alpha(h) = z_1$

$\Rightarrow\ h^{-1}g^{-1}h(g^{-1})^{-1}\alpha(g^{-1})\alpha(h^{-1})\alpha(g)\alpha(h) = z_1$

$\Rightarrow\ h^{-1}g^{-1}hz_2\alpha(h^{-1})\alpha(g)\alpha(h) = z_1$, where $(g^{-1})^{-1}\alpha(g^{-1}) = z_2 \in Z(G)$.

$\Rightarrow\ h^{-1}g^{-1}z_2h\alpha(h^{-1})\alpha(g)\alpha(h) = z_1$

$\Rightarrow\ h^{-1}g^{-1}z_2(h^{-1})^{-1}\alpha(h^{-1})\alpha(g)\alpha(h) = z_1$

$\Rightarrow\ h^{-1}g^{-1}z_2z_3\alpha(g)\alpha(h) = z_1$, where $(h^{-1})^{-1}\alpha(h^{-1}) = z_3 \in Z(G)$.

$\Rightarrow\ h^{-1}g^{-1}z_2\alpha(g)z_3\alpha(h) = z_1$

$\Rightarrow\ h^{-1}g^{-1}(g^{-1})^{-1}\alpha(g^{-1})\alpha(g)(h^{-1})^{-1}\alpha(h^{-1})\alpha(h) = z_1$

$\Rightarrow\ h^{-1}g^{-1}g\alpha(g)^{-1}\alpha(g)h\alpha(h)^{-1}\alpha(h) = z_1$

$\Rightarrow z_1 = 1$

Therefore $\alpha[g, h] = [g, h] \quad \forall\ [g, h] \in G'$.

Hence $Aut_z(G)$ fixes G'elementwise. □

Lemma 2.49 Let G be a finite abelian group and let $d(G) = k$. Let $H \lhd G$, then $d(G/H) \leq k$.

Proof: Let $G = \langle x_1, x_2, \ldots, x_k \rangle$. Let $xH \in G/H$, where $x \in G$.

Let $x = {x_1}^{l_1} {x_2}^{l_2} \ldots {x_k}^{l_k};\ l_i \in \mathbb{Z}$.

Then $xH = {x_1}^{l_1} {x_2}^{l_2} \ldots {x_k}^{l_k} H$

$= (x_1 H)^{l_1} (x_2 H)^{l_2} \ldots (x_k H)^{l_k}$.

So $d(G/H) \leq k$. □

Theorem 2.50 Let G be a non-abelian finite p-group. Prove that $G/G'\,Z(G)$ is a quotient of G/G'.

Proof: Clearly $G' \leq G'$, so by theorem 2.9, G/G' is abelian.

Also $G' \leq G'Z(G)$ and $G'Z(G) \lhd G$, so by theorem 2.9, $G/G'\,Z(G)$ is abelian.

Therefore by theorem 2.34(*Fundamental Theorem of Finite Abelian Groups*),

let $G/G' = C_{p^{a_1}} \times C_{p^{a_2}} \times \ldots \times C_{p^{a_k}}$, where $C_{p^{a_i}}$ is acyclic group of order $p^{a_i}, 1 \leq i \leq k$,

and $a_1 \geq a_2 \geq \ldots \geq a_k \geq 1$.

Let $G/G'\,Z(G) = C_{p^{b_1}} \times C_{p^{b_2}} \times \ldots \times C_{p^{b_l}}$.

And $Z(G) = C_{p^{c_1}} \times C_{p^{c_2}} \times \ldots \times C_{p^{c_m}}$, where $b_1 \geq b_2 \geq \ldots \geq b_l \geq 1$,

and $c_1 \geq c_2 \geq \ldots \geq c_m \geq 1$.

Now $G/G'\,Z(G) = {G/G'}\Big/{G'Z(G)/G'}$.

Also $G'Z(G)/G' \lhd G/G'$. Therefore ${G/G'}\Big/{G'Z(G)/G'}$ is a quotient of G/G'.

Hence $G/G'\,Z(G)$ is a quotient of G/G'.

Hence by lemma 2.49, $l \leq k$ and $b_i \leq a_i$ for all $1 \leq i \leq l$. □

Theorem 2.51 [4, Theorem 2.3**]** For any non-abelian finite group G the map $\theta: Aut_z^z(G) \to Hom\big(G, Z(G)\big)$ is a homomorphism and $\bar{\theta}: Aut_z^z(G) \to Hom\big(G/G'\,Z(G), Z(G)\big)$ is an isomorphism.

Proof: Define the map $\theta: Aut_z^z(G) \to Hom\big(G, Z(G)\big)$

By $\theta(\sigma) = f_\sigma$, where $f_\sigma(g) = g^{-1}\sigma(g) \quad \forall\ g \in G$.

Suppose $\alpha, \beta \in Aut_z^z(G)$. Then for any $g \in G$,

$f_{\alpha\beta}(g) = g^{-1}\alpha\big(\beta(g)\big) = g^{-1}\alpha\big(gg^{-1}\beta(g)\big) = g^{-1}\alpha\big(g\big)\alpha(g^{-1}\beta(g)\big)$

$= \ g^{-1}\alpha(g)g^{-1}\beta(g)$, since $g^{-1}\beta(g) \in Z(G)$ and is fixed by α.

That is, $f_{\alpha\beta}(g) = f_\alpha(g)f_\beta(g)$,

So $\theta(\alpha\beta) = \theta(\alpha)\theta(\beta)$ and θ is a homomorphism.

Define the map $\bar{\theta}: Aut_z^z(G) \to Hom\big(G/G'\,Z(G), Z(G)\big)$ by

$\bar{\theta}(\sigma) = \bar{f_\sigma}$, where $\bar{f_\sigma}\big(gG'Z(G)\big) = f_\sigma(g)$ for any $g \in G$.

Firstly we will prove that $\bar{\theta}$ is well defined.

Let $\sigma_1, \sigma_2 \in Aut_z^z(G)$, such that $\sigma_1 = \sigma_2$

$\Rightarrow \ \sigma_1(g) = \sigma_2(g) \qquad \forall\ g \in G$

$\Rightarrow\ gf_{\sigma_1}(g) = gf_{\sigma_2}(g) \quad \forall\ g \in G$

$\Rightarrow\ f_{\sigma_1}(g) = f_{\sigma_2}(g) \qquad \forall\ g \in G$

$\Rightarrow\ \bar{f}_{\sigma_1}\big(gG'Z(G)\big) = \bar{f}_{\sigma_2}\big(gG'Z(G)\big) \qquad \forall\ gG'Z(G) \in G/G'\,Z(G)$

$\Rightarrow\ \bar{f}_{\sigma_1} = \bar{f}_{\sigma_2}$

$\Rightarrow\ \bar{\theta}(\sigma_1) = \bar{\theta}(\sigma_2)$

Therefore $\bar{\theta}$ is well defined.

Reverse steps show that $\bar{\theta}$ is 1-1.

Now we will prove that $\bar{\theta}$ is a homomorphism.

Let $\sigma_1, \sigma_2 \in Aut_z^z(G)$.

Now $\bar{\theta}(\sigma_1\sigma_2) = \bar{f}_{\sigma_1\sigma_2}$, where $\bar{f}_{\sigma_1\sigma_2}\big(gG'Z(G)\big) = f_{\sigma_1\sigma_2}(g) = f_{\sigma_1}(g)f_{\sigma_2}(g) \quad \forall\ g \in G$

Therefore $\bar{\theta}(\sigma_1\sigma_2) = \bar{f}_{\sigma_1\sigma_2} = f_{\sigma_1\sigma_2} = f_{\sigma_1}f_{\sigma_2} = \bar{\theta}(\sigma_1)\bar{\theta}(\sigma_2)$.

So $\bar{\theta}$ is a homomorphism.

Now we will prove that $\bar{\theta}$ is onto.

Let $f \in Hom\big(G/G'\,Z(G), Z(G)\big)$.

Define $\sigma_f : G \to G$ by $\sigma_f(g) = gf(\bar{g})$, where $\bar{g} = gG'Z(G)$.

Firstly we will prove that σ_f is a homomorphism.

Let $g_1, g_2 \in G$. Then

$\sigma_f(g_1g_2) = g_1g_2gf(\overline{g_1g_2})$

$= g_1g_2f(\overline{g_1})f(\overline{g_2})$, since f is a homomorphism

$= g_1f(\overline{g_1})g_2f(\overline{g_2})$, since $f(\overline{g_1}) \in Z(G)$

$= \sigma_f(g_1)\sigma_f(g_2)$

Therefore σ_f is a homomorphism.

Now we will prove that σ_f is 1-1.

Let $g \in \ker \sigma_f$, such that $\sigma_f(g) = 1$

$\Rightarrow gf(\bar{g}) = 1 \Rightarrow g = (f(\bar{g}))^{-1} \in Z(G)$. So $g \in Z(G)$.

Now $\bar{g} = gG'Z(G) = G'Z(G)$, since $g \in Z(G)$.

Therefore $1 = \sigma_f(g) = gf(\bar{g}) = gf\big(G'Z(G)\big) = g.1 = g$, since $f \in Hom\big(G/G'\,Z(G), Z(G)\big)$

and hence by theorem 2.31(part-1), $f\big(G'Z(G)\big) = 1$, where 1 is the identity of $Z(G)$.

So $g = 1$ and hence by theorem 2.31(part-2), σ_f is 1-1.

Now we will prove that σ_f fixing $Z(G)$ element-wise.

Let $z \in Z(G)$. Now $\sigma_f(z) = zf(\bar{z}) = zf\big(zG'Z(G)\big) = zf\big(G'Z(G)\big) = z.1 = z$

Therefore σ_f fixes $Z(G)$ element-wise.

Therefore σ_f is a homomorphism, 1-1 and fixes $Z(G)$ element-wise. So $\sigma_f \in Aut_z^z(G)$.

Therefore for each $f \in Hom\big(G/G'\,Z(G), Z(G)\big)$, we have $\sigma_f \in Aut_z^z(G)$. So $\bar{\theta}$ is onto.

Hence $\bar{\theta}$ is an isomorphism. □

Chapter-3

MAIN RESULT

Theorem: Let G be a non-abelian finite p-group.Then $Aut_z(G) = Aut_z^z(G)$ if and only if $Z(G) \leq G'$ or $Z(G) \leq \Phi(G), k = l$ and $c_1 \leq b_t$ where t is the largest integer between 1 and k such that $a_t > b_t$.

Proof: Let G be a finite p-group. Let

$$G/G' = C_{p^{a_1}} \times C_{p^{a_2}} \times \ldots \times C_{p^{a_k}} ,$$

where $C_{p^{a_i}}$ is acyclic group of order $p^{a_i}, 1 \leq i \leq k$, and $a_1 \geq a_2 \geq \ldots \geq a_k \geq 1$.

Let

$$G/G'\,Z(G) = C_{p^{b_1}} \times C_{p^{b_2}} \times \ldots \times C_{p^{b_l}}$$

and

$$Z(G) = C_{p^{c_1}} \times C_{p^{c_2}} \times \ldots \times C_{p^{c_m}} ,$$

where $b_1 \geq b_2 \geq \ldots \geq b_l \geq 1$, and $c_1 \geq c_2 \geq \ldots \geq c_m \geq 1$.

Since $G/G'\,Z(G)$ is a quotient of G/G', we have $l \leq k$ and $b_i \leq a_i$ for all $1 \leq i \leq l$, by theorem 2.50.

Suppose that $Aut_z(G) = Aut_z^z(G)$ and $Z(G) \nleq G'$.

We claim that $Z(G) \leq \Phi(G)$. Assume on the contradiction that $Z(G) \nleq \Phi(G)$.

Choose an element g in $Z(G)$ such that $g \notin M$ for some maximal subgroup M of G.

Now by theorem 2.28(part-4), we have M is normal. Also $\langle g \rangle$ is normal.

And $M \cap \langle g \rangle = 1$. So by definition 2.32(*Internal Direct Product of H and K*), $G = M\langle g \rangle$.

Since M is a non-trivial normal subgroup of G, so by theorem 2.28(part-2), $Z(G) \cap M$ is non-trivial. Let $1 \neq z \in Z(G) \cap M$ such that $z^p = 1$ by *Cauchy's Theorem.*

Also we know that $\Omega_1\big(Z(G)\big) = \langle x \in Z(G) \mid x^p = 1 \rangle$.

Therefore $1 \neq z \in \Omega_1\big(Z(G)\big) \cap M$.

Define the map $\alpha: G \to G$ by

$\alpha(mg^k) = mg^k z^k$ for every $m \in M$ and every $k \in \{0, 1, .., p-1\}$.

We claim that α is a central automorphism.

Firstly we will prove that α is a homomorphism.

Let $m_1 g^{k_1}, m_2 g^{k_2} \in G$. Then

$$\begin{aligned}\alpha(m_1 g^{k_1} m_2 g^{k_2}) &= \alpha(m_1 m_2 g^{k_1} g^{k_2}), \text{ since } g \in Z(G)\\ &= \alpha(m_1 m_2 g^{k_1+k_2}) = m_1 m_2 g^{k_1+k_2} z^{k_1+k_2}\\ &= m_1 m_2 g^{k_1} g^{k_2} z^{k_1} z^{k_2}\\ &= m_1 g^{k_1} z^{k_1} m_2 g^{k_2} z^{k_2}, \text{ since } g, z \in Z(G)\\ &= \alpha(m_1 g^{k_1})\alpha(m_2 g^{k_2})\end{aligned}$$

Therefore α is a homomorphism.

Now we will prove that α is 1-1.

Let $mg^k \in G$ such that $\alpha(mg^k) = 1$

$\Rightarrow\ mg^k z^k = 1\ \Rightarrow\ m = z^{-k} g^{-k} \in Z(G)$. Therefore $M \subseteq Z(G)$.

But M is a maximal subgroup of G. So $M = Z(G)$.

By theorem 2.3, we get G is abelian. Which is not so.

Now we will prove that $x^{-1}\alpha(x) \in Z(G) \quad \forall\, x \in G$.

Let $mg^k \in G$. Then $\alpha(mg^k) = mg^k z^k$

$\Rightarrow (mg^k)^{-1}\alpha(mg^k) = (mg^k)^{-1} mg^k z^k$

$\Rightarrow (mg^k)^{-1}\alpha(mg^k) = z^k \in Z(G)$

Therefore $x^{-1}\alpha(x) \in Z(G) \quad \forall\, x \in G$.

Hence α is a central automorphism.

But $Aut_z(G) = Aut_z^z(G)$, so α is a central automorphism fixing $Z(G)$ elementwise.

Therefore $g = \alpha(g) = gz$.

Hence $z = 1$, which is a contradiction.

Hence $Z(G) \leq \Phi(G)$.

Since $Z(G) \leq \Phi(G)$, it follows that G is purely non-abelian.

Also $l = rank\big(G/G'\,Z(G)\big) = rank(G/G') = k$.

Since $Aut_z(G) = Aut_z^z(G)$, therefore by [1, Theorem 1] and by theorem 2.51,

$$\big|Hom\big(G/G',Z(G)\big)\big| = \big|Hom\big(G/G'\,Z(G),Z(G)\big)\big|$$

Hence by theorem 2.38,

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

Since by theorem 2.50, $a_i \geq b_i$ for all $1 \leq i \leq k$, we have

$min\{a_i, c_j\} \geq min\{b_i, c_j\}$ for all $1 \leq i \leq k$ and $1 \leq j \leq m$, we have

$min\{a_i, c_j\} = min\{b_i, c_j\}$ for all $1 \leq i \leq k$ and $1 \leq j \leq m$.

Since $Z(G) \not\leq G'$, there exists some $1 \leq i \leq k$ such that $a_i > b_i$.

Let t be the largest integer between 1 and k such that $a_t > b_t$.

We claim that $c_1 \leq b_t$.

Suppose for a contradiction that $c_1 > b_t$.

Thus $b_t = min\{c_1, b_t\} = min\{c_1, a_t\}$, which is impossible.

Conversely if $Z(G) \leq G'$, then by lemma 2.48, every central automorphism fixes G'

and hence it fixes $Z(G)$ and so $Aut_z(G) = Aut_z^z(G)$.

Now assume that $Z(G) \leq \Phi(G), k = l$ and $c_1 \leq b_t$ where t is the largest integer between 1 and k such that $a_t > b_t$.

Since $Z(G) \leq \Phi(G), G$ is purely non-abelian and so

$$|Aut_z(G)| = \big|Hom\big(G/G',Z(G)\big)\big| = \prod_{1\leq i\leq k,1\leq j\leq m} p^{min\{a_i,\,c_j\}}$$

On the other hand we have

$$|Aut_z^z(G)| = \big|Hom\big(G/G'\,Z(G),Z(G)\big)\big| = \prod_{1\leq i\leq l,1\leq j\leq m} p^{min\{b_i,\,c_j\}}$$

Since $b_t \geq c_1$, we have

$$b_1 \geq b_2 \geq \ldots \geq b_{t-1} \geq b_t \geq c_1 \geq c_2 \geq \ldots \geq c_m \geq 1.$$

Therefore $c_j \leq b_i \leq a_i$ for all $1 \leq j \leq m$ and $1 \leq i \leq t$,

Hence $min\{a_i, c_j\} = c_j = min\{b_i, c_j\}$ for all $1 \leq j \leq m$ and $1 \leq i \leq t$.

Since $a_i = b_i$ for all $i > t$, we have $min\{a_i, c_j\} = min\{b_i, c_j\}$ for all $1 \leq j \leq m$ and $t + 1 \leq i \leq k$. Thus $min\{a_i, c_j\} = min\{b_i, c_j\}$ for all $1 \leq j \leq m$ and $1 \leq i \leq k$.

Therefore $Aut_z(G) = Aut_z^z(G)$. □

REFERENECES

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

[2] M.S. Attar, *On central Automorphisms that fix the centre elementwise*, Arch. Math. 89 (2007), 296-297.

[3] M.J. Curran, D. J. McCaughan, *Central automorphisms that are almost inner*, Comm. Algebra 29 (2001), 5, 2081-2087.

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

[5] M.J. Curran, *Direct products with abelian automorphism groups*, Comm. Algebra 35 (2007), 389-397.

[6] J.J. Rotman, *An introduction to the theory of groups*, 4th Edition, Springer-Verlag, New York, 1995.

[7] M.K. Yadav, *On central Automorphisms fixing the center element-wise*, Comm. Algebra, 37 (2009), 4325-4331.

[8] M.S. Attar, *Finite p-Groups in which each central Automorphism fixes centre elementwise*, Comm. Algebra (To appear).