ON CENTRAL AUTOMORPHISMS THAT FIX THE CENTRE 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

Priya Shahi

Roll no. - 30703015

Under

the guidance of

Dr. Deepak Gumber

JULY 2009

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 "**On Central Automorphisms that Fix the Centre Elementwise** " in partial fulfillment of the requirements for the award of degree 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.

(Priya Shahi)

(Registration No. 30703015)

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

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

Countersigned by:

Dr. S.S. Bhatia 13-7-09
(Professor & Head)
School of Mathematics & Computer Applications
Thapar University, Patiala.

Dr. R.K. Sharma 24/7/09
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.

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.

(Priya Shahi)

TABLE OF CONTENTS

Chapter-1

INTRODUCTION

Throughout this thesis , p denotes a prime number and G denotes a finite group unless stated otherwise.We denote by $G', Z(G), \exp(G), Aut(G)$ and $Inn(G)$, respectively, the commutator subgroup, the center, the exponent, the automorphism group and the inner automorphism group of G.An automorphism σ of a group G is central if σ commutes with every automorphism in $Inn(G)$, or equivalently, if $g^{-1}\sigma(g)$ lies in the center of G, for all g in G. The central automorphisms fix the commutator subgroup G' of G element wise , and form a normal subgroup $Aut^{Z}(G)$,of the full automorphism group $Aut(G)$. We denote by $Aut_{Z}(G)$ the set of all those automorphisms of G which fix $Z(G)$ elementwise.We denote by $Aut_{Z}^{Z}(G) = Aut_{Z}(G) \cap Aut^{Z}(G)$, the group of all central automorphisms of G fixing $Z(G)$ element wise.

Non-abelian $p-$groups G in which all automorphisms are central, that is $Aut_{Z}(G) = Aut(G)$, have been well studied. If $Aut(G)$ is abelian then this is necessarily the case, and various papers such as [2], [4] , [8] , [10] , [11] have considered this situation. But even if $Aut(G)$ is non-abelian , all automorphisms may be central and this case has also been explored , for example in [3] , [7] , [9]. Curran [5] has proved that if $Aut_{Z}(G) = Z(Inn(G))$ then $Z(G) \leq G'$ and also $Aut_{Z}(G) = Z(Inn(G))$ if and only if $\mathrm{Hom}(G/G', Z(G)) \cong Z(Inn(G))$. Curran and McCaughan [6] have 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 this thesis we prove 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.All the main results in Chapter-3 of this thesis are proved in [1].

Chapter-2

NOTATIONS AND PRELIMINARIES

Definition 2.1(Cyclic Group)

A group G is said to be a cyclic group if there exists an element $b \in G$,such that every element of G is a power of b .The element b is called a generator of G and we denote G by $< b >$. If the composition in G were denoted additively then we could say that G is a cyclic group if there exists an element a of G such that every element of G is of the form na where n is an integer.

Definition 2.2(Quotient Group)

Let G be a group and let N be a normal subgroup of G .Then the set G/N of all cosets of N in G ,together with the binary composition defined by $(Na)(Nb) = Nab$ for all $Na, Nb \in G/N,$ is a group, and is called the quotient group of G by $N.$ Further if the binary composition in G is addition,each coset of N in G is denoted as $N + a,$ then the binary composition in G/N is also denoted additively i.e we write $(N + a) + (N + b) = N + (a + b).$

Definition 2.3 (Center)

The center of a group G , denoted by $Z(G)$,is the set of all $a \in G$ that commute with every element of G .It is easy to check that $Z(G)$ is a normal abelian subgroup of G .

Definition 2.4(Kernel of a homomorphism)

Let f be a homomorphism of a group G into a group G', then the kernel of f is the set $=\{x \in G \mid f(x) = e', \text{the identity of } G'.\}$. We shall denote the kernel of f by $Ker\ f$.

Theorem2.5 Let G and G' be any two groups, e and e', their respective identities. If f is a homomorphism of G into G', then

(1) $f(e) = e'$.

(2) $f(x^{-1}) = f(x)^{-1} \quad \forall x \in G$.

(3) $Ker\ f$ is normal subgroup of G.

Proof:

(1)Since $e.e = e, f(e)f(e) = f(e)$. However $f(e) \in G'$ gives $f(e) = e'f(e)$.

Thus $f(e)f(e) = e'f(e) \Rightarrow f(e) = e'$, by right cancellation in G'.

(2)For any $x \in G$, since $xx^{-1} = e$, we get $f(x)f(x^{-1}) = f(xx^{-1}) = f(e) = e'$. Similarly, $x^{-1}x = e$ gives $f(x^{-1})f(x) = e'$. Hence, $f(x^{-1}) = f(x)^{-1}$.

(3)Since $f(e) = e',\ e \in Ker\ f$. This shows $Ker\ f \neq \phi$.

Now let $a, b \in Ker\ f,\ x \in G.\ a \in Ker\ f\ , b \in Ker\ f$. So, $f(a) = e', f(b) = e'$.

i.e $f(a) = e', f(b^{-1}) = f(b)^{-1} = e'$. So, $f(ab^{-1}) = f(a)f(b)^{-1} = e'e' = e'$.

Hence, $ab^{-1} \in Ker\ f$. This proves that $Ker\ f$ is a subgroup of G.

It remains to show that it is also normal. Now, $f(x^{-1}ax) = f(x^{-1})f(a)f(x)$

$= f(x)^{-1}f(a)f(x) = f(x)^{-1}e'f(x) = f(x)^{-1}f(x) = e'$. Consequently $x^{-1}ax \in Ker\ f$.

Hence, $Ker\ f$ is a normal subgroup of G.

Theorem 2.6 If G is a group such that $G/Z(G)$ is cyclic, then G is abelian.

Proof: Put $N = Z(G)$ and let $G/N =< gN >$ for some $g \in G.$ Let $a, b \in G$ then $aN = (gN)^k = g^k N$ and $bN = (gN)^l = g^l N$ for some $k, l \in Z.$ Thus, $a = g^k n_1$ and $b = g^l n_2,\ \ n_1, n_2 \in N.$ This gives that $ab = g^{k+l} n_1 n_2$ and $ba = g^{l+k} n_1 n_2$ as $n_1, n_2 \in N = Z(G).$ Hence, $ab = ba.$

Definition 2.7 (Principle of well-ordering)

Every non-empty set of integers which is bounded below must possess a least element.

Theorem 2.8(Division Algorithm) If a and b are integers, $b \neq 0,$ then there exist integers q and r, such that $a = bq + r$ with $0 \leq r < |b|.$ Further if $a = bq_1 + r_1$ with $0 \leq r_1 < |b|,$ then $r = r_1$ and $q = q_1.$

Proof: Let $S = \{a - |b|s : s \in Z$ and $a - |b|s \geq 0\}.$ Since $|a||b| \geq |a| \geq -a,$ we get $a + |a||b| \geq 0.$ So that for $s = -|a|,\ a + |b||a| = a - |b|s \geq 0,$ gives $a - |b|s \in S.$ Hence S is non empty. By the well ordering principle S has a smallest member say $r.$ Then, $r = a - |b|t$ for some $t \in Z.$

Clearly $r \geq 0.$ We claim that $r < |b|.$ For let $r \geq |b|.$ Then $0 \leq r - |b| < r.$ However $r - |b| = a - |b|(1 + t)$ gives that $r - |b| \in S.$ This contradicts the fact that r is the smallest member of $S.$ Hence $0 \leq r < |b|.$ Thus, we have $a = |b|t + r$ with $0 \leq r < |b|$ -----(1)

If $b > 0, |b| = b.$ Then by putting $q = t,$ in (1) we get $a = bq + r.$ If $b < 0, |b| = -b.$ Then by putting $q = -(t),$ we get $a = bq + r.$ We now prove the uniqueness of q and $r.$ For let also $a = bq' + r', q', r' \in Z, 0 \leq r' < |b|.$ We get $bq + r = bq' + r'.$ So that $b(q - q') = r' - r.$

If $q \neq q', |b(q-q')| \geq |b|,$ but $|r'-r| \leq \max(r,r') < |b|;$ this leads to a contradiction. Hence $q = q'.$ Consequently $bq + r = bq + r'$ and hence $r = r'.$ This proves the theorem.

Theorem 2.9 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, where $o(a) = n.$ So there exists a positive integer q such that $m = nq.$ Now $a^m = a^{nq} = (a^n)^q = e^q = e.$

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

Theorem 2.10: Let G be a group and let $a \in G$ be an element of order $m.$ Then $o(a^k) = \frac{m}{(m,k)}$ where $k \in N.$

Proof: Let $o(a^k) = t.$ Now, $a^{kt} = (a^k)^t = e,$ but $o(a) = m.$ Thus by above theorem, $m \mid kt.$ Let $d = (m,k).$ Thus $d \mid m$ and $d \mid k.$ 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 $m \mid kt,$ so $m_1 d \mid k_1 dt.$ Thus $m_1 \mid k_1 t,$ but $(m_1, k_1) = 1.$ Hence $m_1 \mid t.$ ---------(1)

Again $(a^k)^{m_1} = a^{km_1} = a^{k_1 dm_1} = a^{k_1 m} = (a^m)^{k_1} = e,$ but $o(a^k) = t.$ Thus, $t \mid m_1.$ ----------(2)

From (1) and (2), we get $m_1 = t.$ This proves the theorem.

Definition 2.11 (Homomorphism) Let G and G' be any two groups and let '.' and '$*$' denote their respective binary compositions . A mapping $f : G \to G'$ is called a homomorphism if $f(a.b) = f(a) * f(b)\ \forall a, b \in G.$

A homomorphism f ,which at the same time is onto is called an epimorphism.

A homomorphism which is at the same time $1-1$ is called a monomorphism.

A homomorphism of a group G into itself is called an endomorphism of G .

A homomorphism f of a group G onto a group G' is called an isomorphism if f is a $1-1$ mapping.

Definition 2.12 (Automorphism)

An isomorphism of a group G onto itself is called an Automorphism of G .

Definition 2.13 (Inner Automorphism)

Let a be an element of a group G .The map $f_a : G \to G$ given by $f_a(x) = axa^{-1}$ $\forall\ x \in G$ becomes (proved below) an automorphism of G and is called an inner automorphism of G determined by a . $Inn(G)$ denotes the set of all inner automorphisms of G .Let $f_a(x) = f_a(y)$ then $axa^{-1} = aya^{-1}$ .Premultiplying by a^{-1} on both sides,we get $xa^{-1} = ya^{-1}$ .Again post multiplying by a on both sides,we get $x = y.$ Hence, f_a is one-one.For each $y \in G, \exists\ \ a^{-1}ya \in G$ s.t $f_a(a^{-1}ya) = a(a^{-1}ya)a^{-1} = y.$ Hence, f_a is onto.

Now, $f_a(xy) = a(xy)a^{-1} = axa^{-1}aya^{-1} = f_a(x)f_a(y).$

So, f_a is a homomorphism and hence f_a is an automorphism.

Theorem2.14(Fundamental Theorem of Homomorphism) Let G be a group.If N is a normal subgroup of G,then G/N is a homomorphic image of G.Conversely if any group G' is a homomorphic image of G then G' is isomorphic to some quotient group of G.In fact,if f is a homomorphism of G onto G',then $G' \cong G/Kerf$.

Proof: Define $f: G \to G/N$ by $f(a) = Na \quad \forall a \in G.$Since $f(ab) = Nab = (Na)(Nb)$ $= f(a)f(b) \quad \forall a,b \in G,$and for each $Nc \in G/N, f(c) = Nc,$we see that f is a homomorphism of G onto $G/N.$

Conversely let G' be a homomorphic image of $G,$then there exists a homomorphism g of G onto $G'.$Let $N = Ker\, g$ .We know that N is a normal subgroup of G (theorem 2.5).Consider the quotient group G/N .Define $f: G/N \to G'$ by $f(Na) = g(a) \quad \forall a \in G.$

Firstly we show that f is well defined.For this,let $a_1, a_2 \in G$ with $Na_1 = Na_2.$ So, $a_1 a_2^{-1} \in N$ i.e $g(a_1 a_2^{-1}) = e',$the identity of $G'.$So, $g(a_1)g(a_2)^{-1} = e'$and $g(a_1) = g(a_2).$Hence, $f(Na_1) = f(Na_2).$Consequently f is well-defined.Now for any $Na, Nb \in G/N.\ f[(Na)(Nb)] = f(Nab) = g(ab) = g(a)g(b) = f(Na)f(Nb).$This shows that f is a homomorphism.

Further $f(Na) = f(Nb)$ i.e $g(a) = g(b).$So, $g(a)g(b)^{-1} = e'.$And $g(ab^{-1}) = e'$ i.e $ab^{-1} \in Ker\, g = N.$Hence, $Na = Nb.$Thus, f is a $1-1$ mapping.

Lastly let $x \in G',$as g is onto $\exists \quad a \in G$ such that $g(a) = x.$Consequently $f(Na) = g(a) = x.$This proves that f is also onto.Hence f is an isomorphism of G/N onto G' and $G/N \cong G'.$This proves the theorem.

Theorem2.15 For any group G, $Inn(G)$ is a normal subgroup of $Aut(G)$.

Further $Inn(G) \cong G/Z(G)$, where $Z(G)$ denotes the center of G.

Proof: Clearly, $I \in Inn(G)$ as $I(x) = x = exe^{-1} = f_e(x)\ \forall\ x \in G$. Now for any $a \in G$, $x \in G$, $f_a \circ f_{a^{-1}}(x) = f_a[f_{a^{-1}}(x)] = f_a[a^{-1}x(a^{-1})^{-1}] = f_a(a^{-1}xa) = a(a^{-1}xa)a^{-1} = x = I(x)$. This implies $f_a \circ f_{a^{-1}} = I$. Similarly, $(f_{a^{-1}} \circ f_a)(x) = I(x)$. Thus, $f_{a^{-1}} \circ f_a = I = f_a \circ f_{a^{-1}}$ showing thereby that $(f_a)^{-1} = f_{a^{-1}} \in Inn(G)$. Also for any $f_a, f_b \in Inn(G)$. $f_a \circ f_b = f_a \circ f_b(x) = f_a[f_b(x)] = f_a[bxb^{-1}] = abxb^{-1}a^{-1} = (ab)x(ab)^{-1} = f_{ab}(x)$. Thus $f_a \circ f_b = f_{ab} \in Inn(G)$. Hence $Inn(G)$ is a subgroup of $Aut(G)$.

To show that $Inn(G)$ is a normal subgroup of $Aut(G)$, it only remains to prove that for any $f_a \in Inn(G)$, $\sigma \in Aut(G)$, $\sigma \circ f_a \circ \sigma^{-1} \in Inn(G)$.

Let $x \in G$, then $(\sigma \circ f_a \circ \sigma^{-1})(x) = \sigma(a)\sigma[\sigma^{-1}(x)]\sigma(a^{-1}) = \sigma(a)x[\sigma(a)]^{-1} = f_{\sigma(a)}(x)$.

$\sigma \circ f_a \circ \sigma^{-1} = f_{\sigma(a)} \in Inn(G)$. Now we consider the last part of the theorem. For this purpose define a mapping $\phi : G \to Inn(G)$ by $\phi(a) = f_a\ \forall\ a \in G$. Then $\phi(ab) = f_{ab} = f_a \circ f_b = \phi(a) \circ \phi(b)\ \forall\ a, b \in G$ shows that ϕ is a homomorphism. Clearly, ϕ is onto since each member of $Inn(G)$ is of the form f_a and by definition $f_a = \phi(a)$. Applying Fundamental Theorem of Homomorphism we get $G/Ker\phi \cong Inn(G)$. The result will follow if we show that $Ker\phi = Z(G)$. Now $a \in Ker\phi$ if and only if $\phi(a) = I$, the identity of $Inn(G)$ if and only if $f_a = I$ if and only if $f_a(x) = I(x)\ \forall\ x \in G$ if and only if $axa^{-1} = x$ (Definition of f_a) if and only if $a \in Z(G)$ (Definition of $Z(G)$. Hence, $Ker\ \phi = Z(G)$ and this completes the proof.

Definition 2.16

If G is a group,then G itself and $\{1\}$ are always subgroups.Any subgroup H of G other than G is called a **proper** subgroup,and we denote this by $H < G$; the subgroup 1 is often called the **trivial subgroup**.

Remark: If a group G is not abelian then $Z(G) \neq G$ and consequently $G/Z(G)$ is not a trivial group; further because of the above theorem $Inn(G)$ is also not a trivial group.Consequently if a group G is not abelian,then G has a non-trivial automorphism .If a group G is abelian,then each of its inner automorphism is identity,so the above theorem does not provide us a non-identity automorphism of an abelian group.

Definition 2.17 (Commutator)

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

Definition 2.18

Let S be a subset of a group G.A subgroup H of G is said to be 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 $< S >$.

Definition 2.19 (Commutator Subgroup)

The Commutator subgroup (or derived subgroup) of G ,denoted by G' ,is the subgroup of G generated by all the commutators.

Lemma 2.20 If S is any non-void subset of a group G,then the subgroup $< S >$ of G generated by S is the set of all finite products of the form $a_1 a_2 ... a_n$ where for each i,either $a_i \in S$ or $a^{-1} \in S$.

Proof: Let H be the set of all finite products of the form $a_1 a_2 ... a_n$; a_i or $a_i^{-1} \in S$, n any positive integer.Consider $x = a_1 a_2 .... a_n, y = b_1 b_2 ... b_m$ in H. Then $xy = a_1 a_2 ... a_n b_1 b_2 ... b_m$ is a product of finite number of elements $a_i b_j$ such that either the factor or its inverse is in S, consequently $xy \in H$.Further $x^{-1} = a_n^{-1} a_{n-1}^{-1} .... a_2^{-1} a_1^{-1}$.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 $a \in S, a \in K$ and hence $a^{-1} \in K$.Thus if $x = a_1 a_2 .... a_n : a_i \in S$ or $a^{-1} \in S$, 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 2.21 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 $x = g_1 g_2 .... g_t$ where for each $i = 1,2...,t, g_i$ 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 $a \in G$,
$a^{-1} x a = (a^{-1} g_1 a)(a^{-1} g_2 a)...(a^{-1} g_t a)$.
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 $a^{-1}xa \in G'$. This proves the result.

2)Consider $a,b \in G$ .Let G/H be abelian i.e $(aH)(bH) = (bH)(aH)$ $\forall\, aH, bH \in G/H$ So, $abH = baH$. Thus, $a^{-1}b^{-1}ab = (ba)^{-1}(ab) \in H$. 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, $(aH)(bH) = (bH)(aH)$. This establishes that G/H is abelian.

- A group G is commutative if and only if $G' = (e)$.

Definition 2.22 Let a,b be two integers . Integer a is called congruent to b modulo m, written as $a \equiv b(\mathrm{mod}\, m)$ if and only if $m \mid a-b$ or equivalently $a-b$ is an integral multiple of m. Thus, $a \equiv b(\mathrm{mod}\, m)$ if and only if $a-b \in (m)$, the subgroup of Z consisting of multiples of m .

Definition 2.23(Right Congruence modulo a subgroup)

Let G be a group and H be a subgroup of G .Given $a,b \in G, a$ is said to be right congruent to b modulo H {symbolically $a \equiv_r b(\mathrm{mod}\, H)$ } if and only if $ab^{-1} \in H$.

Theorem 2.24 If G is a group and H is a subgroup of G .Then the relation $\equiv_r$ of right congruence modulo H is an equivalence relation on G .Further for any $a \in G$ the set $\{ha \mid h \in H\}$ is the equivalence class to which a belongs.

Proof: Let $a,b \in G$ and e be identity of H.

1)Reflexivity: Since $aa^{-1} = e \in H, a \equiv_r a (\text{mod}\, H).$

2)Symmetry: $a \equiv_r b (\text{mod}\, H) \Rightarrow ab^{-1} \in H. \Rightarrow (ab^{-1})^{-1} \in H$

i.e $ba^{-1} \in H \Rightarrow b \equiv_r a (\text{mod}\, H).$

3)Transitivity: $a =_r b (\text{mod}\, H), b =_r c (\text{mod}\, H)$ i.e $ab^{-1} \in H, bc^{-1} \in H.$

Thus, $ac^{-1} = (ab^{-1})(bc^{-1}) \in H.$ Hence, $a \equiv_r c (\text{mod}\, H).$

Thus the relation of right congruence modulo H is an equivalence relation on $G.$ Let $Cl(a)$ denote the equivalence class to which a belongs i.e $Cl(a) = \{b \in G \mid b \equiv_r a (\text{mod}\, H)\}.$ Let Ha denote the set $\{ha \mid h \in H\}.$ Now $b \in Cl(a)$ i.e $b \equiv_r a (\text{mod}\, H).$ Thus $ba^{-1} \in H.$ So, $b = (ba^{-1})a \in Ha.$ Thus $Cl(a) \subseteq Ha.$ Again $c \in Ha$ *i.e* $c = ha$ for some $h \in H.$ Thus, $ca^{-1} = h \in H.$ So, $c \equiv_r a (\text{mod}\, H)$ *i.e* $c \in Cl(a).$ Thus, $Ha \subseteq Cl(a).$ Hence, $Cl(a) = Ha.$

Definition 2.25 (Exponent)

The exponent of a group G is the smallest positive integer n such that $x^n = 1$ $\forall$ $x \in G$ if such n exists ; otherwise it is $\propto$.For example,the exponent of S_3 is 6.

Lagrange Theorem 2.26 The Order of any subgroup of a finite group divides the order of the group.

Proof: Let G be a finite group and H a subgroup of G.Suppose $o(H) = n.$ For any $a \in G,$ define $f : H \to Ha$ such that $f(h) = ha.$ This mapping is onto as each member of Ha is of type $ha, h \in H.$ Further for any two elements $h_1, h_2 \in H,$ let $f(h_1) = f(h_2)$ so $h_1 a = h_2 a.$ i.e $h_1 = h_2.$ (right cancellation law).Hence f is a $1-1$ mapping of H onto $Ha.$ This means that $o(H) = o(Ha).$ Let $Ha_1, Ha_2, ..., Ha_t$ be the totality of distinct right cosets of H in $G.$ Then these t right cosets

constitute the totality of distinct equivalence classes in G determined by the relation of right congruence modulo H. Thus $Ha_1, Ha_2, ...Ha_t$ are disjoint subsets of G and $G = Ha_1 \cup Ha_2 \cup .... \cup Ha_t$. As seen above $o(Ha_i) = o(H) = n$ $\forall i = 1,2,...t$. Therefore, $o(G) = nt$. Hence $o(H) / o(G)$.

- It is evident from the proof of the above theorem that $o(G)/o(H)$ is equal to the number of right cosets of H in G. Similarly it can be proved that $o(G)/o(H)$ is equal to the number of left cosets of H in G.

- Lagrange's theorm shows that a finite group G of order n has exponent $\leq n$.

Theorem 2.27 Show that the Converse of Lagrange's theorem holds for cyclic groups.

Proof: Let $G =< a >$ be a cyclic group of order n generated by a. Let m divide n. Therefore, $\exists\ q \in Z$ such that $n = mq$. We know that, elements of G are of the form a^k, where $k \in Z$. Also, $o(a^k) = \dfrac{n}{(n,k)}$ (by theorem 2.10). Therefore,

$o(a^q) = \dfrac{n}{(n,q)} = \dfrac{n}{q} = m$. Therefore, $\exists$ an element $a^q \in G$, whose order is m. Therefore, $\exists$ a cyclic subgroup $H =< a^q >$ of order m.

For uniqueness: Let $H' =< a^l >$ be another subgroup of G of order m. Therefore, $o(a^l) = m$ i.e $(a^l)^m = e$. So, $a^{ml} = e$. By Division algorithm theorem, $\exists\ k, r \in Z$ such that $l = kq + r$, where $0 \leq r < q$. So, $ml = mkq + mr$, where $0 \leq mr < mq = n$. Therefore, $e = a^{ml} = a^{mkq+mr} = (a^{mq})^k a^{mr} = (a^n)^q . a^{mr} = e^q a^{mr} = a^{mr}$.

But $0 \le mr < n.$ Therefore above result is true if $mr = 0$ i.e $r = 0.$ So, $l = kq.$ Therefore, $a^l = a^{kq} = (a^q)^k.$ So, $H' \subseteq H.$ But $o(H') = o(H) = m.$ Hence $H' = H.$ Hence H is unique subgroup of G of order $m.$

Definition 2.28 (Lower central series)

The lower central series $\gamma_i(G)$ of a group G is defined inductively as follows: $\gamma_1(G) = G;\ \ \gamma_{i+1}(G) = [\gamma_i(G), G].$ Notice that $\gamma_2(G) = [\gamma_1(G), G] = [G, G] = G' = G^{(1)}.$ It is easy to check that $\gamma_{i+1}(G) \le \gamma_i(G).$

Definition 2.29

A group G is called a nilpotent group if there is a positive integer c such that $\gamma_{c+1}(G) = 1;$ the least such c is called the class of the nilpotent group G. Note that a group is nilpotent of class 1 if and only if it is abelian.

Definition 2.30

If p is a prime, then a ***p-group*** is a group in which every element has order a power of $p.$ ***For example***: Klien-4 group $G = \{1, a, b, c\}$ where $c = ab$ and $a^2 = b^2 = c^2 = 1.$ G is a 2-group.

Cauchy's Theorem For Abelian Groups 2.31 Let A be a finite abelian group and let p be a prime. If $p \mid o(A)$, then A has an element of order $p.$

Proof: We prove the result by induction on $o(A) = n.$ For $n = 1$ result is true. Assume result is true for all abelian groups of order $< n.$ If $o(A) = p$ i.e A is cyclic , then A has an element of order $p.$ So, suppose that $\exists\ \ b(\neq e) \in A$ such that $< b > \neq A.$ If p divides $|< b >|,$ then we are done.(By theorem 2.27).So

let p does not divide $|< b >|$ but $p \mid o(A)$. So, $p \mid \frac{|A|}{|< b >|}$ i.e p divides $|A/< b >|$. So by induction hypothesis $A/< b >$ has an element say $\bar{a}$ of order p. Thus, $(\bar{a})^p = < b >$. Hence, $\overline{a^p} = < b >$. (because $(aH)^m = a^m H$). Let $|a| = k$, then $a^k = 1$. So, $\overline{a^k} = \bar{1} = < b >$ i.e $\bar{a}^k = < b >$. Thus , $p \mid k = |a|$. Hence, $p \mid o(A)$ and $p \mid o(< a >)$. So, $< a >$ and hence A has an element of order p.

Theorem 2.32 A finite group G is a $p-$group if and only if $|G|$ is a power of p.

Proof: If $|G| = p^m$, then lagrange's theorem shows that G is a $p-$group.

Conversely,assume that there is a prime $q \neq p$ which divides $|G|$.

By Cauchy's theorem, G contains an element of order q, and this contradicts G being a $p-$group.

Lemma 2.33 Let G be a finite group and $f \in Aut(G)$. If $z \in Z(G)$, then $f(z) \in Z(G)$.

Proof: Let $z \in Z(G)$, then $zg = gz \quad \forall g \in G$. So, $f(zg) = f(gz)$.

Since f is a homomorphism, $f(z)f(g) = f(g)f(z)$. Thus, $f(z) \in Z(G)$. (because $f(g)$ ranges over whole G i.e f is onto.)

Chapter-3

MAIN RESULT

Lemma 3.1 The central automorphisms of G form a normal subgroup $Aut^Z(G)$ 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 $x^{-1}(fg)(x) \in Z(G)$. 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 $\phi^{-1}\psi\,\phi \in Aut^Z(G)$ $\forall$ $\phi \in Aut(G)$.

Consider, $a^{-1}(\phi^{-1}\psi\,\phi)a = a^{-1}\phi^{-1}(\psi(\phi(a))) = a^{-1}\phi^{-1}(\phi(a)\phi(a)^{-1}\psi(\phi(a)))$

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

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

Hence, $Aut^Z(G)$ is a normal subgroup of $Aut(G)$.

Theorem 3.2 Prove that the following two Statements are equivalent:

1)An automorphism σ of a group G is central if σ commutes with every automorphism in $Inn(G)$.

2)An automorphism σ of a group G is central if $g^{-1}\sigma(g)$ lies in the center of G, for all g in G.

Proof $(1) \rightarrow (2)$

Let σ commutes with every automorphism in $Inn(G)$ i.e $\sigma I_g \equiv I_g \sigma$. So, $\sigma I_g(x) = I_g\sigma(x)\ \forall x$. Then, $\sigma(gxg^{-1}) = g\sigma(x)g^{-1}$. Thus, $\sigma(g)\sigma(x)\sigma(g^{-1}) = g\sigma(x)g^{-1}$.

So, $g^{-1}\sigma(g)\sigma(x)\sigma(g)^{-1} = \sigma(x)g^{-1}$. Hence, $g^{-1}\sigma(g)\sigma(x) = \sigma(x)g^{-1}\sigma(g) \ \forall x.$

$(2) \rightarrow (1)$

Let $g^{-1}\sigma(g)$ lies in the center of G, for all g in G. i.e $g^{-1}\sigma(g) \in Z(G).$

So, $g^{-1}\sigma(g) = z.$ Thus, $\sigma(g) = gz.$

Consider, $(\sigma I_g)(x) = \sigma(gxg^{-1}) = \sigma(g)\sigma(x)\sigma(g)^{-1} = gz\sigma(x)z^{-1}g^{-1} = g\sigma(x)g^{-1}.$

Now consider, $(I_g\sigma)(x) = I_g(\sigma(x)) = g\sigma(x)g^{-1}.$ Hence, $\sigma I_g \equiv I_g\sigma.$

Lemma 3.3 $Aut_Z(G)$ is a normal subgroup of $Aut(G)$..

Proof: Let $\phi, \psi \in Aut_Z(G).$ So, $\phi(z) = z$ and $\psi(z) = z \ \forall \ z \in Z(G).$ Consider, $\phi\psi^{-1}(z)$ $= \phi(z) = z.$ (since ψ is an automorphism so $\psi^{-1}(z) = z$. Hence, $\phi\psi^{-1} \in Aut_Z(G)$ and $Aut_Z(G)$ is a subgroup of $Aut(G)$. Let $\sigma \in Aut(G)$ and $\phi \in Aut_Z(G)$. Consider $\sigma^{-1}\phi\sigma(z) = \sigma^{-1}\phi(\sigma(z)) = \sigma^{-1}\phi(z) = \sigma^{-1}(z) = z$. (As $\sigma \in Aut(G)$, so $\sigma^{-1}(z) = z$).

For example, $Inn(G) \in Aut_Z(G).$ i.e $Inn(G)$ fixes $Z(G)$ elementwise:

Let $x \in Z(G).$ Consider $I_g(x) = gxg^{-1} = gg^{-1}x = x.$ And $Inn(G) \in Aut^Z(G)$ if G is nilpotent of class 2. Let $I_g \in Inn(G)$ and $I_g : G \rightarrow G$ be defined by $I_g(x) = gxg^{-1}.$

Consider, $x^{-1}I_g(x) = x^{-1}gxg^{-1} = \left[x, g^{-1}\right] \in G' \leq Z(G).$

- And it is clear from the lemmas 3.1 and 3.3 that $Aut_Z^Z(G) \lhd Aut(G).$

Definition 3.4

If G and H are two groups, We denote by $\mathrm{Hom}(G,H)$ the set of all group homomorphisms from G to H.

Theorem 3.5 If H is abelian , then $\mathrm{Hom}(G,H)$ is 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:

1)**Associative Property:**

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

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

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

So, associative property holds.

2)**Existence of Identity:**

Let $I : G \to H$ be defined by $I(x) = 1 \ \ \forall x \in G.$ Clearly, $I \in \mathrm{Hom}(G,H).$

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

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

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

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

And, $(ff^{-1})(x) = f(x)f^{-1}(x) = f(x)(f(x))^{-1} = I.$

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

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

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

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

i.e $fg = gf$.

Lemma3.6 $\mathrm{Hom}(A\times B,C)\cong \mathrm{Hom}(A,C)\times \mathrm{Hom}(B,C)$.

Proof: Let A, B and C be abelian groups.

Let $\phi \in \mathrm{Hom}(A\times B,C)$. Then $\phi|_A \in \mathrm{Hom}(A,C)$ and $\phi|_B \in \mathrm{Hom}(B,C)$.

$\phi_A(a,0)=\phi(a,0)$ and $\phi_B(0,b)=\phi(0,b)$.

Define $f: \mathrm{Hom}(A\times B,C)\to \mathrm{Hom}(A,C)\times \mathrm{Hom}(B,C)$ by $f(\phi)=(\phi_A,\phi_B)$.

f is a homomorphism:

$f(\phi_1+\phi_2)=((\phi_1+\phi_2)_A,(\phi_1+\phi_2)_B)$

Consider $(\phi_1+\phi_2)_A=(\phi_1+\phi_2)_A(a,0)=(\phi_1+\phi_2)(a,0)=\phi_1(a,0)+\phi_2(a,0)$.

Similarly, $(\phi_1+\phi_2)_B=\phi_1(0,b)+\phi_2(0,b)$.

So, $f(\phi_1+\phi_2)=((\phi_1+\phi_2)_A,(\phi_1+\phi_2)_B)$

$=(\phi_1(a,0)+\phi_2(a,0),\phi_1(0,b)+\phi_2(0,b))$

$=(\phi_1(a,0),\phi_1(0,b))+(\phi_2(a,0),\phi_2(0,b))$

$=(\phi_{1A}(a,0),\phi_{1B}(0,b))+(\phi_{2A}(a,0),\phi_{2B}(0,b))$

$=(\phi_{1A},\phi_{1B})+(\phi_{2A},\phi_{2B})$

$=f(\phi_1)+f(\phi_2)$.

f is 1-1: Let $f(\phi_1)=f(\phi_2)$ i.e $(\phi_{1A},\phi_{1B})=(\phi_{2A},\phi_{2B})$. Thus $\phi_{1A}=\phi_{2A}$ and $\phi_{1B}=\phi_{2B}$.

$\phi_{1A}(a,0)=\phi_{2A}(a,0)$. So, $\phi_1(a,0)=\phi_2(a,0)$. Hence $\phi_1=\phi_2$.

Hence f is $1-1$.

f is onto: Let $g\in \mathrm{Hom}(A,C)$ and $h\in \mathrm{Hom}(B,C)$.

Let $\phi\in \mathrm{Hom}(A\times B,C)$ defined by $\phi(a,b)=g(a,0)+h(0,b)$.

$\phi_A(a,0)=g(a,0)+h(0,0)=g(a,0)$.

$\phi_B(0,b)=g(0,0)+h(0,b)=h(0,b)$.

So, $\forall\ g\in \mathrm{Hom}(A,C)$ and $h\in \mathrm{Hom}(B,C)$ $\exists\ \phi\in \mathrm{Hom}(A\times B,C)$ s.t $f(\phi)=(g,h)$.

Hence, f is onto.

Let A,B and C be abelian groups for the following three lemmas:

Lemma 3.7 $\mathrm{Hom}(A,B) = \mathrm{Hom}(B,A).$

Proof: Proof can be found in [12].

The following Lemma follows easily from above two lemmas.

Lemma 3.8 $\mathrm{Hom}(A, B\times C) = \mathrm{Hom}(A,B)\times \mathrm{Hom}(A,C).$

Lemma 3.9 $\mathrm{Hom}(C_m, C_n) \approx C_d$,where $d = \gcd(m,n).$

Proof: Proof can be found in [12].

Theorem 3.10 If A is an abelian group,then $\mathrm{Hom}(Z,A) \cong A$.

Proof: Let $a \in A$ .Define $T_a : Z \to A$ by $T_a(1) = a.$ Since, $Z = <1>.$ T_a can be extended to a homomorphism $T_a : Z \to A$.

$T_a(m) = T_a(1+1+.....m\ times) = T_a(1) + T_a(1) + ...m\ times = a + a + ...m\ times = ma = mT_a(1).$

$T_a(0) = 0.$ Define $\phi : A \to \mathrm{Hom}(Z,A)$ by $\phi(a) = T_a.$

Now we show that ϕ is a homomorphism.

$\phi(a+b) = T_{a+b}.\ T_{a+b}(1) = a + b = T_a(1) + T_b(1) = \phi(a) + \phi(b).$

So, $\phi\ (a+b) = \phi(a) + \phi(b).$

Hence, ϕ is a homomorphism.

If $T \in \mathrm{Hom}(Z,A)$,then $T(1) = b$ for some $b.$

Hence, $T \equiv T_b.$ So, ϕ is onto.

Let $\phi\ (a) = \phi\ (b)$ i.e $T_a \equiv T_b$ so $T_a(1) = T_b(1)$ .Thus, $a = b.$ And hence ϕ is $1-1.$

Thus, $A \cong \mathrm{Hom}(Z,A)$.

Theorem 3.11 $\mathrm{Hom}(Z_{p^m}, Z_{q^n}) = 1.$ if $p \neq q$.

Proof: Let $A = < a >$ and $B = < b >$ be two finite cyclic groups.

Let $T : A \to B$ be a non zero homomorphism. Let $T(a) = c \neq 0$. Let $|a| = n$. Then $0 = T(0) = T(na) = nT(a) = nc$. Thus, $|c|$ divides $n = |a|$. If $p \neq q$, then order of no element of Z_{q^n} can divide p^m. So, $\mathrm{Hom}(Z_{p^m}, Z_{q^n}) = 1.$ if $p \neq q$. (i.e there will be only zero homomorphism).

Theorem 3.12 $\mathrm{Hom}(Z_{p^m}, Z_{p^n}) \cong Z_{p^{\min(m,n)}}$.

Proof: Let $Z_{p^m} = < a >$. For each non zero $c \in Z_{p^n}$, $|c|$ divides $|a|$, we have a non zero homomorphism $T_c : Z_{p^m} \to Z_{p^n}$ given by $T_c(a) = c$. If $m \geq n$, then each $0 \neq c \in Z_{p^n}$ is s.t $|c| / p^n$ and hence $|c| / p^m$. So, $|\mathrm{Hom}(Z_{p^m}, Z_{p^n})| = p^n$. Let $Z_{p^n} = < b >$ and $T_b(a) = b$. If $c \in Z_{p^n}$, then $c = rb$. Thus, $T_c \equiv T_{rb}$. $T_{rb}(a) = rb = r(T_b(a))$.

And, $rT_b(a) = (rT_b)(a)$. Hence, $T_{rb} = rT_b$. So, $T_c = T_{rb} \equiv rT_b$.

So, $\mathrm{Hom}(Z_{p^m}, Z_{p^n}) = < T_b >$. Hence, $\mathrm{Hom}(Z_{p^m}, Z_{p^n}) \cong Z_{p^n}$.

So, $|\mathrm{Hom}(Z_{p^m}, Z_{p^n})| = p^n$ if $m \geq n$. -------(1)

Let $n \geq m$. $\mathrm{Hom}(Z_{p^m}, Z_{p^n}) \cong \mathrm{Hom}(Z_{p^n}, Z_{p^m})$. (lemma 3.7)

$|\mathrm{Hom}(Z_{p^n}, Z_{p^m})| = p^m$. by (1)

Lemma 3.13 Let a, b be two elements of finite order, of a group G such that $o(a)$ and $o(b)$ are co-prime and $ab = ba$. Then $o(ab) = o(a)o(b)$.

Proof: Let $o(a) = m$ and $o(b) = n$. Let $H = < ab >$ be the subgroup of G generated by ab. Since, $(ab)^{mn} = a^{mn}b^{mn} = e$, we get $o(H) = o(ab) \mid mn$. Now, $(ab)^m = a^m b^m = b^m$

$\in H$, since $a^m = e$. As $(m,n) = 1$, and $o(b) = n$, we have $o(b^m) = o(b) = n$. Since $b^m \in H$ so, $o(b^m) \mid o(H)$. Hence, $n \mid o(H)$. Similarly, $m \mid o(H)$. Thus, we have $mn \mid o(H)$. Hence $o(H) = mn = o(ab)$. This proves the lemma.

Lemma 3.14 The order of any element of a finite abelian group G divides the largest order of an element of G.

Proof: Let there exists an $a \in G$ such that $o(a) = k$ and for every $b \in G, o(b) \le o(a) = k$. Suppose on the contrary there exists $b \in G$ such that $o(b)$ does not divide k. This implies that there exists a prime number p such that for some positive integer $t, p^t \mid o(b)$ but p^t does not divide $o(a)$. This means that we can write $o(b) = p^\alpha q, o(a) = p^\beta s$ such that $(p,q) = 1, (p,s) = 1,$ and $\beta < \alpha$. Let $b_0 = b^q, a_0 = a^{p^\beta}$. Then $o(b_0) = p^\alpha$, and $o(a_0) = s$. Lemma 3.13 gives $o(a_0 b_0) = p^\alpha s$ $> p^\beta s = o(a)$. This contradicts our assumption. Hence lemma follows.

Definition 3.15(Internal Direct Product)

A group G is said to be an internal direct product of its subgroups $H_1, H_2, ...H_n$ if it satisfies the following conditions:

(i) For $i \ne j$ $a_i \in H_i, a_j \in H_j \Rightarrow a_i a_j = a_j a_i$.

(ii) Each $x \in G$ is uniquely expressible as $x = x_1 x_2 ... x_n, x_i \in H_i, 1 \le i \le n,$ in the sense that if also $x = y_1 y_2 ... y_n, y_i \in H_i, 1 \le i \le n,$ then $x_i = y_i \forall i$. If the binary composition in G is addition, we say that G is an internal direct sum of $H_1, H_2, ...H_n,$ and write $G = H_1 \oplus H_2 \oplus .... \oplus H_n$.

Fundamental Theorem of finite abelian groups 3.16 Every Abelian group G of order n, is a direct product $G = G_1 \times G_2 \times .... \times G_t$,where G_i are cyclic subgroups of order n_i such that n_{i+1} / n_i and the integers n_i are uniquely determined.Further $n = n_1 n_2 ... n_t$.

Proof: We prove the result by induction on $o(G)$.If $o(G) = 1$,the result holds trivially.Suppose $o(G) = n > 1$ and that result holds for all abelian groups of order $< o(G)$.

Let g_1 be an element of G of largest order n_1. Let $G_1 =< g_1 >$. If $G = G_1$,then G itself is cyclic.Let $G \neq G_1$. Then $1 < O(G / G_1) < n.$ By the induction hypothesis $G / G_1 = \overline{H_2} \times \overline{H_3} \times ... \times \overline{H_t}$ where each $\overline{H_i}$ is a cyclic subgroup of $\overline{G} = G / G_1$ of order $n_i > 1$ such that $n_{i+1} \mid n_i \quad \forall\ i = 2,3,4,...,t-1,$ and $n / n_1 = O(\overline{G}) = n_2 n_3 ... n_t$. -----(1)

Now each $\overline{H_i} = H_i / G_1$ for some subgroup H_i of G containing G_1.Choose $h_i \in H_i$ such that $\overline{h_i} = h_i G_1$ is a generator of $\overline{H_i}$. Then $\overline{h_i}^{n_i} = \bar{e} = \overline{G_1}$ i.e $h_i^{n_i} \in G_1 =< g_1 >$.So, $h_i^{n_i} = g_1^{m_i}$ for some m_i such that $1 \le m_i \le n_1$.Let $\alpha_i = (m_i, n_i)$. Then $m_i = \alpha_i \beta_i$ for some $\beta_i \ge 1, n_1 = \alpha_i \gamma_i$ for some $\gamma_i \ge 1$ and $(\beta_i, \gamma_i) = 1$. Now, $o(g_1) = n_1 = \alpha_i \gamma_i$ so $o(g_1^{\alpha_i}) = \gamma_i$ .As $(\gamma_i, \beta_i) = 1, o(g_1^{\alpha_i \beta_i}) = o(g_1^{\alpha_i}).$ However , $h_i^{n_i} = g_1^{\alpha_i \beta_i}$. So, $o(h_i^{n_i}) = \gamma_i$. On the other hand $o(\overline{h_i}) \mid o(h_i)$ i.e $n_i \mid o(h_i)$ .So $o(h_i^{n_i}) = \dfrac{o(h_i)}{n_i}$. Hence, $o(h_i) = o(h_i^{n_i}) n_i = \gamma_i n_i.$ ---------(2)

Since $o(h_i) \mid n_1,$ the largest order(lemma 3.14) and $n_1 = \alpha_i \gamma_i,$ we have $\gamma_i n_i \mid \alpha_i \gamma_i$. So $n_i \mid \alpha_i$ so $\alpha_i = n_i \delta_i$ for some $\delta_i \ge 1$. Then $h_i^{n_i} = g_1^{n_i \delta_i \beta_i}$. Put $g_i = h_i (g_1)^{-\delta_i \beta_i} \quad \forall i = 2,3,...t.$ We see that $\overline{g_i} = g_i G_1 = \overline{h_i}, g_i^{n_i} = h_i^{n_i} (g_1)^{-n_i \delta_i \beta_i} = e.$

This yields $o(g_i) = n_i$. Define $H =< g_2 >< g_3 > .... < g_t >$. H is subgroup of G such that $o(H) \mid n_2 n_3 ... n_t$. Let $f : G \to G/G_1$ be the natural homomorphism. Since $f(H) =< \overline{g_2} > \times < \overline{g_3} > \times ... \times < \overline{g_t} > = \overline{H_2} \times \overline{H_3} \times \overline{H_4} \times .... \times \overline{H_t} = G/G_1$ and also $f(H) = (HG_1)/G_1$, we get $G = HG_1 = G_1 H =< g_1 >< g_2 > .... < g_t >$. The fact that $o(G) = n = n_1 n_2 ... n_t = o(g_1) o(g_2) .... o(g_t)$ gives $G =< g_1 > \times < g_2 > \times ..... \times < g_t >$.

Also, $o(< g_i >) = o(g_i) = n_i$ such that $n_{i+1} \mid n_i$.

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

$= K_1 \times K_2 \times .... \times K_u$ --------(4)

be two decompositions of G into internal direct product of cyclic subgroups,such that for $i = 1,2,...,t, j = 1,2,....,u, o(H_i) = n_i, o(K_j) = m_j$, for $i \le t-1, n_{i+1} / n_i$ and for $j \le u-1, m_{j+1} \mid m_j$. Consider $g \in G$, then (3) gives $g = h_1 h_2 ... h_t; h_i \in H_i$. Since $o(h_i) \mid o(H_i) = n_i$ and $n_i \mid n_1$, we get $h_i^{n_1} = e.$

Consequently $g^{n_1} = h_1^{n_1} h_2^{n_1} .... h_t^{n_1} = e.$ Thus, $o(g) \le n_1 \forall g \in G$. 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 largest order of an element of $G.$ Similarly m_1 is the largest order of an element of $G.$ Thus $n_1 = m_1$. Suppose we have proved that $n_1 = m_1, n_2 = m_2, ..., n_{i-1} = m_{i-1}$ for some $i;$ we shall prove that $n_i = m_i$. Suppose on the contrary $n_i \ne m_i$, and to be definite let $n_i > m_i$. Define $K = \{x^{m_i} \mid x \in G\}$. Since for any $x, y \in G, x^{m_i} y^{-m_i} = (xy^{-1})^{m_i} \in K$, we get that K is a subgroup of $G.$ Suppose that for $k = 1,2,....,t, H_k =< a_k >$ and for each $j = 1,2,....,u, K_j =< b_j >$. Since for $j \ge i, o(K_j) = m_j \mid m_i, b_j^{m_i} = e.$

Hence $K =< b_1^{m_i} > \times < b_2^{m_i} > \times .... \times < b_{i-1}^{m_i} >$.

Thus $o(K) = \frac{m_1}{m_i} \frac{m_2}{m_i} .... \frac{m_{i-1}}{m_i}$, since $o(b_j) = m_j \forall j.$ ----------(5)

Since also $G = < a_1 > \times ....\times < a_t >$ (from (3))

We have $K = < a_1^{m_i} > \times < a_2^{m_i} > \times .... < a_t^{m_i} >$. Now $o(a_k^{m_i}) = \frac{n_k}{(m_i, n_k)} \quad \forall k = 1,2,....,t.$

Consequently $o(K) = \frac{n_1}{(m_i, n_1)} \frac{n_2}{(m_i, n_2)} ..... \frac{n_i}{(m_i, n_i)} \frac{n_{i+1}}{(m_i, n_{i+1})} ..... \frac{n_t}{(m_i, n_t)}$ ----------(6)

Now $m_i \mid m_j$ and $m_j = n_j \quad \forall j < i,$ by our hypothesis.

Thus $\frac{n_j}{(m_i, n_j)} = \frac{m_j}{(m_i, m_j)} = \frac{m_i}{m_i} \quad \forall j < i.$

Hence from (5) and (6) we obtain

$1 = \frac{n_i}{(m_i, n_i)} ..... \frac{n_t}{(m_i, n_t)}$ ----------(7)

However $m_i < n_i$ gives $\frac{n_i}{(m_i, n_i)} > 1.$ As a consequence,(7) cannot hold.This gives $m_i = n_i.$ Hence by induction $m_i = n_i \ \forall i.$ However $n = n_1 n_2 ... n_t = m_1 m_2 ... m_u.$ Thus we must also have $t = u.$ This completes the theorem.

<u>Corollary 3.17</u> Every finite abelian $p-$group G is expressible as an internal direct product of cyclic groups $G = G_1 \times G_2 .... \times G_r$ such that $o(G_i) = p^{m_i}$ $\forall i = 1,2,...r$ and $m_j \geq m_{j+1} \quad \forall j = 1,2,...r-1.$ Further p^{m_i} are uniquely determined.

<u>Proof:</u> By the above theorem,we can express $G = G_1 \times G_2 \times .... \times G_r$ ---------(1) such that each G_i is a cyclic subgroup of order n_i and $n_{j+1} \mid n_j \quad \forall j \leq r-1.$

Since G is a $p-$group,each G_i is a $p-$group,we have $O(G) = p^m$ for some $m,$ and $n_i = o(G_i) = p^{m_i} \forall i.$ Since $n_{j+1} \mid n_j,$ we have $m_{j+1} \leq m_j \quad \forall j \leq r-1.$

If $G = H_1 \times H_2 \times .... \times H_s$ ----------(2) is another decomposition of G into cyclic subgroups such that $o(H_i) = p^{u_i} \ \forall i = 1,2,...,s$ and $u_j \geq u_{j+1} \quad \forall j \leq s-1,$ we see that $o(H_{j+1}) \mid o(H_j) \quad \forall j = 1,2,...,s-1.$ This establishes the corollary.

Theorem 3.18 Suppose K is an abelian $p-$group of exponent p^c,and A is Cyclic of order divisible by p^c.Then $\mathrm{Hom}(K,A)$ is isomorphic to K.

Proof: Given A is cyclic of order divisible by p^c,therefore $|\mathrm{A}|= p^c m$ for some positive integer m.Since K is an abelian $p-$group of exponent p^c.

Therefore,$|K|= p^{c+t}$.

Let $K = K_1 \times K_2 \times K_3 .....$ (theorem 3.16) (Here no K_i is of order $> p^c$)

$\mathrm{Hom}(K,A) = \mathrm{Hom}(K_1,A) \times \mathrm{Hom}(K_2,A) \times .....$ (lemma 3.6)

$= K_1 \times K_2 \times K_3 \times .....$ (lemma 3.9)

$= K.$

i.e $\mathrm{Hom}(K,A)$ is isomorphic to K.

Definition 3.19 (Rank)

A finite abelian group has **RANK** n if it is a direct sum of n cyclic groups and n is minimal possible.

Lemma 3.20 Suppose K is an abelian $p-$group of rank r,and A is cyclic of order p.Then $\mathrm{Hom}(K,A)$ is isomorphic to $(C_p)^r$.

Proof : Let $K = C_{p^{n_1}} \times C_{p^{n_2}} \times .....\times C_{p^{n_r}}$. (definition of rank)

$\mathrm{Hom}(K,A) = \mathrm{Hom}(C_{p^{n_1}},C_p) \times .....\times \mathrm{Hom}(C_{p^{n_r}},C_p)$ (lemma 3.6)

$\cong C_p \times C_p \times .....\times C_p = (C_p)^r .$(lemma 3.9)

Lemma 3.21 If G is nilpotent group of class 2,then $\exp(G') = \exp(G/Z(G))$.

Proof: Lemma 0.4 [11].

Definition 3.22 (Purely non abelian group)

A non-abelian group G which has no non-trivial abelian direct factor is said to be purely non-abelian.

Let G be a purely non-abelian $p-$group,of nilpotent class 2. Let $G/Z(G)$ and G' have exponent p^c,with ranks r and d respectively.If $r=1, G/Z(G)$ is cyclic and G is abelian but we have taken G is non-abelian.So $r \geq 2.$ .Let $Z(G)$ have rank z.As G is of class 2 so $G' \leq Z(G)$..So,$Z(G)$ has exponent at least p^c.

Lemma 3.23 $|\mathrm{Hom}(G/Z(G), Z(G))| \geq |G/Z(G)|\, p^{r(z-1)}$.

Proof: Let $Z(G) \cong C_1 \times C_2 \times .... \times C_z$ because $Z(G)$ have rank z.

$\mathrm{Hom}(G/Z(G), Z(G)) \cong \mathrm{Hom}(G/Z(G), C_1) \times ..... \times \mathrm{Hom}(G/Z(G), C_z)$ since $Z(G)$ has z direct factors and at least one of these say C_1 is of order p^c.

$\mathrm{Hom}(G/Z(G), Z(G)) \cong G/Z(G) \times \mathrm{Hom}(G/Z(G), C_2) \times ..... \times \mathrm{Hom}(G/Z(G), C_z)$ (by theorem 3.18)

$\mathrm{Hom}(G/Z(G), Z(G)) \geq G/Z(G) \times \mathrm{Hom}(G/Z(G), C_p) \times ..... \times \mathrm{Hom}(G/Z(G), C_p)$

$\cong G/Z(G) \times (C_p)^r \times ..... \times (C_p)^r$. (by lemma 3.20)

Therefore, $|\mathrm{Hom}(G/Z(G), Z(G))| \geq |G/Z(G)|\, p^{r(z-1)}$.

Lemma 3.24 If G is a finite $p-$group,then $Aut_z^z(G) \cong \mathrm{Hom}\,(G/Z(G), Z(G))$.

Proof: Let $f \in Aut_Z^Z(G)$.Define $\sigma_f : G/Z(G) \to Z(G)$ by $\sigma_f\,(gZ(G)) = g^{-1}f(g)$.

As $f \in Aut_z^z(G)$ so $g^{-1}f(g) \in Z(G).$ Let $gZ(G) = hZ(G)$ then $h = gz\,; z \in Z(G)$.Now

$\sigma_f\,(hZ(G)) = h^{-1}f(h) = (gz)^{-1}f(gz) = z^{-1}g^{-1}f(gz) = z^{-1}g^{-1}f(g)f(z) = z^{-1}g^{-1}f(g)z =$

$g^{-1}f(g) = \sigma_f(gZ(G))$. (As f fixes each element of $Z(G)$).Hence, σ_f is well defined.Define $\sigma : Aut_Z^Z(G) \to \text{Hom}(G/Z(G), Z(G))$ by $\sigma(f) = \sigma_f$. Consider,

$\sigma(f+g) = \sigma_{f+g} = \sigma_{f+g}(hZ(G)) = h^{-1}(f+g)(h) = h^{-1}(f(h)+g(h)) = h^{-1}f(h) + h^{-1}g(h) =$

$\sigma_f + \sigma_g = \sigma(f) + \sigma(g)$. Hence, σ is a homomorphism.

Let $\sigma(f_1) = \sigma(f_2)$ i.e $\sigma_{f_1} = \sigma_{f_2}$. Thus $\sigma_{f_1}(gZ(G)) = \sigma_{f_2}(gZ(G)) \ \forall gZ(G) \in G/Z(G)$.

So $g^{-1}f_1(g) = g^{-1}f_2(g)$ i.e $f_1(g) = f_2(g) \ \forall g \in G$. Hence $f_1 = f_2$. Therefore, σ is 1-1.Now for each $h \in \text{Hom}(G/Z(G), Z(G))$, the map f defined by $f(g) = gh(gZ(G))$ for all $g \in G$ is a central automorphism fixing $Z(G)$ elementwise and $\sigma(f) = h$. Let $f(x) = 1$. i.e $xh(xZ(G)) = 1$ so $h(xZ(G)) = x^{-1}$ and $x^{-1} \in Z(G)$. Hence $x \in Z(G)$ and $xZ(G) = Z(G)$. So $xh(xZ(G)) = 1$ i.e $xh(Z(G)) = 1$. And since $h(Z(G)) = 1$ so $x = 1$. Hence f is 1-1.Now, Since G is finite and f is $1-1$.. So, f is onto.

Let $g_1, g_2 \in G$. $f(g_1g_2) = g_1g_2h(g_1g_2Z(G)) = g_1g_2h(g_1Z(G)g_2Z(G))$

$= g_1g_2(h(g_1Z(G))h(g_2Z(G))) = g_1h(g_1Z(G))g_2h(g_2Z(G)) = f(g_1)f(g_2)$. So, f is an automorphism.Since, $g^{-1}f(g) = g^{-1}(gh(gZ(G))) = h(gZ(G)) \in Z(G)$ as

$h: G/Z(G) \to Z(G)$. So, f is a central automorphism.

Let $g \in Z(G)$. $f(g) = gh(gZ(G)) = gh(Z(G)) = g.1 = g$.

Hence, f fixes $Z(G)$ elementwise.So $f \in Aut_Z^Z(G)$ and $\sigma(f) = h$. So,it follows that σ is a group isomorphism and $Aut_z^z(G) \cong \text{Hom}(G/Z(G), Z(G))$.

Theorem 3.25 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.

Proof: Suppose first that $Aut_z^z(G) = Inn(G)$ and G is non abelian .Let $g \in G$. Then the inner automorphism θ_g induced by g is a central automorphism and so

$[x,g] = x^{-1}\theta_g(x) \in Z(G)$ for all $x \in G.$ This shows that G is nilpotent of class 2.Since G is nilpotent of class 2,exp$(G/Z(G))$=exp$(G')=p^c$ for some natural number c.(from lemma 3.21).Let $G/Z(G)$ and $Z(G)$ have ranks r and z,respectively.As G is nilpotent of class 2, it follows from lemmas 2.15, 3.23 and 3.24 that $|G/Z(G)|=|Inn(G)|=|Aut_z^z(G)|=|\mathrm{Hom}(G/Z(G),Z(G))| \geq |G/Z(G)|\,p^{r(z-1)}$.Since $r \geq 2, z = 1,$ it follows that $Z(G)$ is cyclic.

Conversely,if G is abelian,then it is clear that $Aut_z^z(G) = Inn(G)$=1.Assume that G is nilpotent of class 2 and $Z(G)$ is cyclic.Since, $G' < Z(G)$ (as G is nilpotent of class 2) so $G/Z(G)$ is an abelian p-group(Theorem 2.21).Since $Z(G)$ is cyclic and $G' < Z(G)$,so G' is cyclic i.e $G'=<a>$ and exponent of G' will be order of G' only . Hence, $G/Z(G)$ is of exponent $|G'|$.

It follows from theorem 3.18 that $\mathrm{Hom}(G/Z(G),Z(G)) \cong G/Z(G).$ Therefore $Aut_z^z(G) \cong \mathrm{Hom}(G/Z(G),Z(G)) \cong G/Z(G) \cong Inn(G)$.Since G is nilpotent of class 2, $Inn(G) \leq Aut_z^z(G)$ and hence $Aut_z^z(G) = Inn(G).$

References:

[1]Mehdi Shabani Attar On central automorphism that fix the centre elementwise. *Arch. Math.* **89**(2007), 296-297

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

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

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

[5] M.J. Curran finite groups with central automorphism group of minimal order, *Mathematical and proceedings of the Royal Irish Academy*, **104(A)**, (2004). 223-229.

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

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

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

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

[10] G.A. Miller A non-abelian group whose group of isomorphism is abelian. *Messenger of Math*. **43**(1913). 124-125.

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

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