

SOME THEOREMS ABOUT THE
AUTOMORPHISM GROUP OF
CERTAIN p -GROUPS

Thesis for the Degree of Ph. D.
MICHIGAN STATE UNIVERSITY
JAMES E. VANDEVENTER
1970



This is to certify that the

thesis entitled

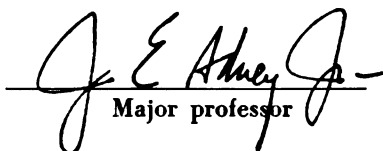
Some Theorems About the
Automorphism Group of
Certain p -Groups

presented by

James E. VanDeventer

has been accepted towards fulfillment
of the requirements for

Ph.D. degree in Mathematics


Major professor

Date 1 April 1970

1000

ABSTRACT

SOME THEOREMS ABOUT THE AUTOMORPHISM GROUP OF CERTAIN p -GROUPS

By

James E. VanDeventer

There are several possible types of relations between a finite group G and its group of automorphisms $A(G)$. One relation is concerned with the size of G as compared to the size of $A(G)$. For example, there is a conjecture that $|G|$ divides $|A(G)|$ if G is a finite nonabelian p -group, where $|G|$ denotes the order of G . Another relation concerns which conditions on G guarantee a certain type of automorphism of G . An example of this type of relation is Gaschütz's result that a finite nonabelian p -group possesses an outer automorphism of p -power order. Still a third type of relation concerns how knowledge about $A(G)$ influences information about the structure of G . Thompson has shown that if a finite group G possesses a fixed point free automorphism of prime order, then G must be nilpotent. In this dissertation, we consider several questions of this nature.

Let G be a p -group, p a prime. Otto has shown that if G is abelian and $|G| = p^n$, $n > 2$, then $|G|$ divides $|A(G)|$ if, and only if, G is not cyclic. He has also shown that if G is a p -group with no abelian direct factors, of order p^n and nilpotence class $m - 1$, G/G_2 is elementary abelian, and $|G_i/G_{i+1}| = p$ for $i = 2, 3, \dots, m-1$ where G_i is the i^{th} member of the descending

central series, then $|G|$ divides $|A(G)|$. Faudree has shown that if G is a finite nonabelian nilpotent class two p -group, then $|G|$ divides $|A(G)|$.

A p -group G , $p \neq 2$, is said to satisfy the conditions (W) if:

- 1). G has nilpotence class at least three,
- 2). G has no abelian direct factors,
- 3). G' is cyclic and $|G'| = p^h$,
- 4). $|G' \cap Z(G)| = p^m$ where $m < h$,
- 5). $|G/\phi(G)| = p^r$.

In this dissertation, we prove the following theorems:

Theorem II.1: If G is a p -group satisfying the conditions (W) , and $Z(G) \leq G'$, then G is a central product of the form $G = \hat{A}B$ where $\hat{A} = \langle x_1, x_2 \mid x_1^{p^h} = x_2^{p^{h+m}} = 1, [x_2, x_1] = x_2^{tp^m}, (t, p) = 1 \rangle$ and B is a p -group of nilpotence class two.

Theorem II.3: If G is a p -group satisfying the conditions (W) , and $Z(G) \leq G'$, then $|G|$ divides $|A(G)|$.

Theorem II.4: If G is a p -group satisfying the conditions (W) , $Z(G) = Z^* \otimes A$ where $Z^* = Z(G) \cap G'$, and $\exp A \geq \exp Z^*$, then $|G|$ divides $|A(G)|$.

Theorem II.5: If G is a p -group satisfying the conditions (W) , $Z(G) = Z^* \otimes A$ where $Z^* = Z(G) \cap G'$, and $h \geq 2m$, then $|G|$ divides $|A(G)|$.

For a p -group G with no abelian direct factors, one knows, in a certain sense, the size of $I(G)$ and the size of the group of central automorphisms $A_c(G)$. It would be useful to know what conditions, if any, are necessary and/or sufficient that $A_c(G) \leq I(G)$.

In connection with this problem, Sanders has shown that a p -group G , $p \neq 2$, of nilpotence class exactly two has $A_c(G) \leq I(G)$ if, and only if, $G' = Z(G)$ is cyclic.

We prove the following theorems which are concerned with the problem:

Theorem II.2: If G is a p -group satisfying the conditions W), and $Z(G) \leq G'$, then $A_c(G) \leq I(G)$.

Theorem III.1: If G is a p -group, $p \neq 2$, with no abelian direct factors and such that $A_c(G) \leq I(G)$, then $Z(G) \leq G'$.

Theorem III.2: If G is a p -group, $p \neq 2$, with no abelian direct factors, $A_c(G) \leq I(G)$, and $Z(G)$ is not cyclic, then $Z_2(G) \leq \phi(G)$.

It is also conjectured that if G is a p -group, $p \neq 2$, with no abelian direct factors and such that $A_c(G) \leq I(G)$, then $Z(G)$ must be cyclic.

SOME THEOREMS ABOUT THE AUTOMORPHISM GROUP
OF CERTAIN p -GROUPS

By

James E. ^{dwinn} VanDeventer

A THESIS

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

Department of Mathematics

1970

10-1-40
10-1-40
10-1-40

DEDICATION

TO JOAN

ACKNOWLEDGMENT

I want to thank Professor J.E. Adney for his guidance throughout the preparation and writing of the dissertation. His patience and encouragement has served as a source of inspiration for the completion of this work.

TABLE OF CONTENTS

Chapter		Page
I	INTRODUCTION	1
II	SOME SUFFICIENCY CONDITIONS FOR $ G $ TO DIVIDE $ A(G) $	6
III	SOME NECESSARY CONDITIONS FOR $A_c(G) \leq I(G)$	36
	BIBLIOGRAPHY	43
	APPENDIX	44

NOTATION

G is a finite group

$G = \langle x_1, x_2, \dots, x_r \rangle$ means that G is generated by the set of elements $\{x_1, x_2, \dots, x_r\}$ where $x_i \in G$.

$\langle x_1, \dots, x_r | \mathcal{R} \rangle$ denotes the group generated by the symbols x_1, \dots, x_r subject to the relations \mathcal{R} .

$H \leq G$ denotes H is a subgroup of G .

$H \trianglelefteq G$ denotes H is a normal subgroup of G .

$G = AB$ denotes G is a product of the two subgroups A and B .

$\langle x_1, x_2 \rangle \leq G$ denotes the subgroup of G generated by the set of elements $\{x_1, x_2\}$.

$|x|$ denotes the order of the element x .

$|G|$ denotes the order of G .

$a|b$ denotes a divides b .

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

$$[x, y, z] = [[x, y], z]$$

$$[H, K] = \langle [h, k] \mid h \in H, k \in K \rangle$$

$$G' = G_2 = [G, G]$$

$G_{k+1} = [G_k, G]$ for $k \geq 1$ is the k^{th} member of the descending central series for G .

$Z(G)$ denotes the center of G .

$Z_2(G) = \langle y \in G \mid [x, y] \in Z(G) \text{ for all } x \in G \rangle$ is the second center of G .

$\phi(G)$ denotes the Frattini subgroup of G .

$A(G)$ denotes the automorphism group of G .

$I(G)$ denotes the group of inner automorphisms of G .

$A_c(G) = \{\alpha \in A(G) \mid x^{-1}x^\alpha \in Z(G) \text{ for all } x \in G\}$ is the group of central automorphisms of G .

$1|G$ is the identity automorphism of G .

$\alpha|H$ is the automorphism of $H \leq G$ obtained by restricting $\alpha \in A(G)$ to H .

$\text{Hom}(H, K)$ denotes the set of homomorphisms from the group H into the group K .

For $y \in G$, π_y denotes the inner automorphism of G which is obtained by conjugation by y .

$G \xrightarrow{\zeta} H$ denotes ζ is a homomorphism from G to H .

CHAPTER I

Introduction

The question of possible relations between a group G and its automorphism group $A(G)$ has been considered in several papers. One type of relation is concerned with how their sizes are related. An example of this type of relation is the conjecture that the order of a finite, nonabelian p -group divides the order of its automorphism group. Another type of relation is concerned with how knowledge about the group can guarantee the existence of certain types of automorphisms. The result of Gaschütz [4], which states that a finite p -group possesses an outer automorphism of p -power order, is concerned with this type of relation. A third type of relation is concerned with how knowledge about the automorphism group helps determine the structure of the group. An example of this type of relation is Thompson's result [9], which states that if a finite group has a fixed point free automorphism of prime order, then the group is nilpotent.

As stated above, it is conjectured that if G is a finite, nonabelian p -group, then $|G|$ divides $|A(G)|$. Since $|I(G)| = |G|/|Z(G)|$, and for a finite p -group, p divides $|Z(G)|$, the conjecture is concerned with whether or not there exist sufficient p -powered outer automorphisms of G . The result of Gaschütz on the existence of a p -power outer automorphism still leaves the question of the size of the automorphism group unanswered.

The conjecture has been proven true for certain classes of p -groups. In [3], Faudree has shown that if G is a finite, non-abelian p -group of nilpotence class two, then $|G|$ divides $|A(G)|$. Otto has shown in [6] that if G is an abelian p -group of order p^n , $n \neq 2$, then $|G|$ divides $|A(G)|$ if, and only if, G is not cyclic. In the same paper he has also shown that if G is a p -group of order p^n , of nilpotence class $m - 1$, where $3 \leq m \leq n$, G/G_2 is elementary abelian, and $|G_i/G_{i+1}| = p$ for $i = 2, \dots, m-1$, where G_i is the i^{th} member of the descending central series of G , then $|G|$ divides $|A(G)|$.

A p -group G is said to have no abelian direct factors if G is not abelian and has no nontrivial abelian direct factors. In the above mentioned paper by Otto, it is shown that if G is a direct product $P \otimes B$ of two subgroups P and B , where P is abelian of order p^r and B has no abelian direct factors, then $p^r \cdot |A(B)|_p$ divides $|A(G)|$, where $|A(B)|_p$ denotes the highest power of p dividing $|A(B)|$. This result allows us to consider only p -groups which have no abelian direct factors, that is, if the conjecture is true for p -groups with no abelian direct factors, then the conjecture is true for p -groups.

One very nice property is possessed by p -groups with no abelian direct factors. Adney and Yen have shown in [1] that if G is a p -group, $p \neq 2$, with no abelian direct factors, then $A_c(G)$, the group of central automorphisms of G , is a p -group. A central automorphism α of a group G is one for which $g^{-1}g^\alpha \in Z(G)$ for all $g \in G$. In the paper by Adney and Yen, it has been shown that if G is a p -group with no abelian direct factors, then

$|A_c(G)| = |\text{Hom}(G/G', Z(G))|$. Also, if $\alpha \in A_c(G)$, then $f_\alpha: x \rightarrow x^{-1}x^\alpha$ is a homomorphism of G into $Z(G)$, and if $\beta \in \text{Hom}(G/G', Z)$ and $G \cong G/G'$, then γ defined by $g^\gamma = g\beta$ is such that $\gamma \in A_c(G)$. Thus for a p -group G , $p \neq 2$, with no abelian direct factors, we know how to construct all possible central automorphisms.

For notation purposes we make the following definition:

Let G be a finite p -group, $p \neq 2$. G is said to satisfy the conditions (W) if:

- 1). G has no abelian direct factors,
- 2). G has nilpotence class at least three,
- 3). G' is cyclic and $|G'| = p^h$,
- 4). $|Z(G) \cap G'| = p^m$ where $m < h$,
- 5). $|G/\phi(G)| = p^r$.

In Chapter II, we give several examples of groups satisfying the conditions (W) , and we prove the following theorems, which concern the conjecture that $|G| \mid |A(G)|$.

Theorem II.3: If G is a p -group satisfying the conditions (W) , and $Z(G) \leq G'$, then $|G|$ divides $|A(G)|$.

Theorem II.4: If G is a p -group satisfying the conditions (W) , $Z(G) = Z^* \otimes A$ where $Z^* = Z(G) \cap G'$ and $\exp A \geq \exp Z^*$, then $|G|$ divides $|A(G)|$.

Theorem II.5: If G is a p -group satisfying the conditions (W) , $Z(G) = Z^* \otimes A$ where $Z^* = Z(G) \cap G'$ and $h \geq 2m$, then $|G|$ divides $|A(G)|$.

Since a p -group always has an outer automorphism of p -power order, we know that a Sylow p -subgroup of $A(G)$ always properly

contains $I(G)$. The outer automorphism may or may not be a central automorphism. For example, in [7], Sanders has shown that if G is a p -group of nilpotence class two, then $A_c(G) \leq I(G)$ if, and only if, $G' = Z(G)$ is cyclic. Thus there exist p -groups which have all their outer automorphisms being noncentral automorphisms.

Regarding sufficient conditions on a group G to guarantee $A_c(G) \leq I(G)$, we prove in Chapter II the following theorem for p -groups of class at least three, which extends Sanders' result in a certain direction.

Theorem II.2: Let G be a p -group, $p \neq 2$, with no abelian direct factors, of nilpotence class at least three and such that $Z(G) \leq G'$, and G' is cyclic. Then $A_c(G) \leq I(G)$.

It is not known what conditions are necessary to place on a p -group G to insure $A_c(G) \leq I(G)$. In Chapter III, we obtain some necessary conditions for $A_c(G) \leq I(G)$. We first prove that if $A_c(G) \leq I(G)$ for a finite p -group, $p \neq 2$, then one must have $G' \geq Z(G)$. This result is sufficient to give that not only does $|A_c(G)| = |\text{Hom}(G/G', Z)|$, but $A_c(G) \cong \text{Hom}(G/G', Z)$. This follows from a condition in Sanders' work [7], which states: Let G be a group with no abelian direct factors. Let $R = \{\gamma(g) : g \in G, \gamma \in \text{Hom}(G, Z)\}$ and let $B = \bigcap (\ker \gamma)$. Then $\text{Hom}(G, Z) \cong A_c(G)$ if, and only if, $R < B$. Since $\text{Hom}(G, Z) \cong \text{Hom}(G/G', Z)$, we have the desired result. [See Appendix, III].

If $y \in Z_2(G)$, then $[g, y] \in Z(G)$ for all $g \in G$. Thus conjugation by an element in $Z_2(G)$ induces a central automorphism of G . Also, if $\pi_y \in A_c(G)$, where $g^{\pi_y} = y^{-1}gy$, then $g^{-1}g^{\pi_y} \in Z(G)$ for all $g \in G$, and hence $y \in Z_2(G)$. Now if $A_c(G) \leq I(G)$, we have

$A_c(G) \cong Z_2(G)/Z(G)$. Since $A_c(G) \leq I(G)$ implies $G' \geq Z(G)$, so $A_c(G) \cong \text{Hom}(G/G', Z)$, we have $Z_2(G)/Z(G) \cong A_c(G) \cong \text{Hom}(G/G', Z)$.

This result is used to prove:

Theorem III.2: Let G be a p -group, $p \neq 2$, with no abelian direct factors, $A_c(G) \leq I(G)$ and $Z(G)$ is not cyclic. Then $Z_2(G) \leq \phi(G)$.

This theorem gives us information about the lattice of G if $A_c(G) \leq I(G)$ and $Z(G)$ is not cyclic. It is our conjecture that if G is a p -group with $A_c(G) \leq I(G)$, then $Z(G)$ is cyclic. So far, however, this has not been proven, but is a direction for further research.

CHAPTER II

Some Sufficiency Conditions for $|G|$ to Divide $|A(G)|$

Let G be a finite p -group, $p \neq 2$. G is said to satisfy the conditions (W) if:

- 1). G has no abelian direct factors,
- 2). G has nilpotence class at least three,
- 3). G' is cyclic and $|G'| = p^h$,
- 4). $|Z(G) \cap G'| = p^m$ where $m < h$,
- 5). $|G/\phi(G)| = p^r$.

We shall now give several examples of p -groups which satisfy the conditions (W).

Example 1): Let $\hat{A} = \langle x_1, x_2 \mid x_1^{p^h} = x_2^{p^{h+m}} = 1, [x_2, x_1] = x_2^{p^m}, m < h \rangle$. One can easily show by induction that $(x_1^k)^{-1} x_2 x_1^k = x_2^{(1+p^m)^k}$. Using this formula, we have the following subgroups of \hat{A} . $\hat{A}' = \hat{A}_2 = \langle x_2^{p^m} \rangle$ and thus $|\hat{A}'| = p^h$. $Z(\hat{A}) = \langle x_2^{p^h} \rangle$ since $(x_1^{p^k})^{-1} x_2 x_1^{p^k} = x_2$ if, and only if, $x_2^{(1+p^m)p^k} = x_2^{1+p^{m+k}+p^{m+k+1}+\dots} = x_2$ if, and only if, $p^{h+m} \mid p^{m+k}$, or $k \geq h$. But $|x_1| = p^h$, so $x_1^{p^k} \in Z(\hat{A})$ if, and only if, $x_1^{p^k} = 1$. Since $\hat{A}' = \langle x_2^{p^m} \rangle$, $x_2 \in C_A(\hat{A}')$, so $[x_2^k, y] = [x_2, y]^k$ for all $y \in \hat{A}$. $x_2^k \in Z(\hat{A})$ if, and only if, $(x_2^k)^{-1} x_1^{-1} x_2^k = x_1^{-1}$, or $[x_2^k, x_1] = 1 = [x_2, x_1]^k = x_2^{kp^m}$. But $|x_2| = p^{h+m}$, so $p^h \mid k$, and we have $Z(\hat{A}) = \langle x_2^{p^h} \rangle$. Since $\hat{A}_2 = \hat{A}'$, we have $\hat{A}_3 = \langle [\hat{A}, \hat{A}_2] \rangle = \langle x_2^{p^{2m}} \rangle$, and in general, $\hat{A}_{k+1} = \langle [\hat{A}, \hat{A}_k] \rangle = \langle x_2^{p^{km}} \rangle$. Since $m < h$ and

$|x_2| = p^{h+m}$, $\hat{A}_3 \neq \langle 1 \rangle$ and the nilpotence class of \hat{A} is at least three. Since $Z(\hat{A}) = \langle x_2^{p^h} \rangle$, we have $Z(\hat{A}) \leq \phi(\hat{A})$ and hence \hat{A} has no abelian direct factors. We note that $Z(\hat{A}) \leq \hat{A}'$.

Example 2): Let $G = \langle x_1, x_2 \mid x_1^{p^{h+2m}} = x_2^{p^{h+m}} = 1, [x_2, x_1] = x_2^{p^m}, m < h \rangle$. One can show that $(x_1^k)^{-1} x_2 x_1^k = x_2^{(1+p^m)^k}$ and as above, use this to obtain that: $G' = \langle x_2^{p^h} \rangle$, $|G'| = p^h$, $G_{k+1} = \langle x_2^{p^{km}} \rangle$, and $Z(G) = \langle x_1^{p^h}, x_2^{p^h} \rangle = \langle x_1^{p^h} \rangle \otimes \langle x_2^{p^h} \rangle$. $|Z(G) \cap G'| = |\langle x_2^{p^h} \rangle| = p^m$. Also $Z(G) \leq \phi(G)$, so we have G can have no abelian direct factors. Since $m < h$, $G_3 \neq \langle 1 \rangle$ and G has nilpotence class at least three. We note that since $|x_1| = p^{h+2m}$ and $|x_2| = p^{h+m}$, we have $\exp Z(G) \geq \exp (Z(G) \cap G')$.

Example 3): Let $G = \langle x_1, x_2 \mid x_1^{p^{h+s}} = x_2^{p^{h+m}} = 1, [x_2, x_1] = x_2^{p^m}, 1 \leq s < m < h \rangle$. This example is similar to the immediately above example. The difference is in this example, $Z(G) = \langle x_1^{p^h} \rangle \otimes \langle x_2^{p^h} \rangle$, and we have $\exp (Z(G)) = \exp (Z(G) \cap G') \geq \exp \langle x_1^{p^h} \rangle$.

Example 4): Let $G = \left\langle x_1, x_2, x_3, x_4 \mid \begin{array}{l} x_1^{p^h} = x_2^{p^{h+m}} = x_3^{p^m} = x_4^{p^m} = 1, \\ [x_3, x_4] = x_2^{p^h}, [x_i, x_j] = 1 \end{array} \right\rangle$. One can show $G' = \langle x_2^{p^m} \rangle$, $[x_2, x_1] = x_2^{p^m}$ for $i = 1, 2, ; j = 3, 4, m < h$. $G_{k+1} = \langle x_2^{p^{km}} \rangle$. Since $m < h$, $G_3 \neq \langle 1 \rangle$, so G has nilpotence class at least three. $Z(G) = \langle x_2^{p^h} \rangle \leq \phi(G)$, thus G has no abelian direct factors.

G is a central product of the form $\hat{A}B$, where \hat{A} is the group in the first example, and $B = \langle x_3, x_4, c \mid x_3^{p^m} = x_4^{p^m} = c^{p^m} = 1, [x_3, x_4] = c, [x_3, c] = [x_4, c] = 1 \rangle$. We have $B' = Z(B) = \langle c \rangle$. \hat{A}

and B are joined by amalgamating $\langle x_2^{p^h} \rangle$ and $\langle c \rangle$.

For the remainder of Chapter II, we shall assume that G is a p -group, $p \neq 2$, which satisfies the conditions (W). Also, for notational purposes, we let $G' = \langle a \rangle$, $G \xrightarrow{K} G/C(G')$ and $G \hookrightarrow G/G'$.

Since G' is cyclic, we have $G' \leq C(G')$. Also, $G/C(G') \cong A(G')$ which is cyclic since G' is a cyclic p -group and $p \neq 2$. Thus $G/C(G') = \langle \bar{x} \rangle$ is a cyclic p -group and we must have if $g \in G$ is such that $\langle g^K \rangle = \langle \bar{x} \rangle$, then $g \notin \phi(G)$.

Remark A: For $g \in G$, let $g^{-1}ag = a^{1+s(g)p^j(g)}$ where $(s(g), p) = 1$ and $j(g) \geq 1$, that is, we set $j(g) = h$ if $g \in C(G')$. Then $j(g) \geq m$.

Proof: We note that $g^{-1}a^k g = (g^{-1}ag)^k = a^{k(1+sp^j)}$ where $s = s(g)$, $j = j(g)$. Since $|G'| = p^h$, $|Z(G) \cap G'| = p^m$ and $G' = \langle a \rangle$, we have $Z(G) \cap G' = \langle a^{p^{h-m}} \rangle$. Thus $g^{-1}a^{p^{h-m}} g = a^{p^{h-m}(1+sp^j)} = a^{p^{h-m}+sp^{h-m+j}} = a^{p^{h-m}}$, or $a^{sp^{h-m+j}} = 1$. But $(s, p) = 1$, so $a^{p^{h-m+j}} = 1$, or $p^{h-m+j} \equiv 0 \pmod{p^h}$. Thus $h-m+j \geq h$, or $j \geq m$.

Remark B: Let $g \in G$, $s = s(g)$, $j = j(g)$. Then for $k \geq 0$, $(g^k)^{-1}a^k g^k = a^{(1+sp^j)^k}$, and hence for all $g \in G$, $g^{p^{h-m}} \in C(G')$.

Proof: If $k = 0$, then $(g^0)^{-1}a^0 g^0 = a = a^{(1+sp^j)^0}$. Assume the formula is true for $k = n$. Then $(g^{n+1})^{-1}a^{n+1} g^{n+1} = g^{-1}((g^n)^{-1}a^ng^n)g = g^{-1}a^{(1+sp^j)^n}g = (g^{-1}ag)^{(1+sp^j)^n} = (a^{1+sp^j})^{(1+sp^j)^n} = a^{(1+sp^j)^{n+1}}$. Hence, by induction, the formula is true for $k \geq 0$.

Let $k = p^{h-m}$, then $(g^{p^{h-m}})^{-1}a^{p^{h-m}} g^{p^{h-m}} = a^{(1+sp^j)p^{h-m}} = a^{1+sp^{h-m+j}+sp^{h-m+j+1}} = a$ since by Remark A, $j \geq m$, so $h-m+j \geq h$ and $|G'| = p^h$. Thus $g^{p^{h-m}} \in C(G')$.

Remark C: For some $g \in G$, $j(g) = m$.

Proof: Suppose not, then by Remark A, $m \neq j(g)$ for all $g \in G$. Let $j = \min\{j(g) \mid g \in G\}$, then $m \neq j$. For $g \in G$, we have $g^{-1}a^p^{h-j}g = a^p^{h-j}(1+s(g)p^j(g)) = a^p^{h-j} + s(g)p^{h-j+j(g)} = a^p^{h-j}$ since $j(g) \geq j$ and $|G'| = p^h$. Thus $a^p^{h-j} \in Z(G) \cap G'$. But $|a^p^{h-j}| = p^j$, $|Z(G) \cap G'| = p^m$ and $m \neq j$, a contradiction. Thus for some $g \in G$, $j(g) = m$.

Since $g^p^{h-m} \in C(G')$ for all $g \in G$, we have $|G/C(G')| \leq p^{h-m}$. By Remark C, there exists $g \in G$ with $j(g) = m$. For this g we have $g^{-1}ag = a^{1+sp^m}$ where $s = s(g)$. By Remark B, $(g^p^{h-m-1})^{-1}ag^p^{h-m-1} = a^{(1+sp^m)p^{h-m-1}} = a^{1+sp^{h-1}+\beta p^h} \neq a$ since $a^{sp^{h-1}} \neq 1$. Thus $g^p^{h-m-1} \notin C(G')$ and we have $|G/C(G')| = p^{h-m}$.

Remark D: If $\langle g^K \rangle = \langle \bar{x} \rangle$, where $G \xrightarrow{K} G/C(G')$, then $j(g) = m$.

Proof: Since $\langle g^K \rangle = \langle \bar{x} \rangle$, we may assume $g^K = \bar{x}$. Since $|\langle \bar{x} \rangle| = p^{h-m}$, $g^p^{h-m-1} \notin C(G')$. Let $j = j(g)$, $s = s(g)$, then we have $g^{-1}ag = a^{1+sp^j}$ where $j \geq m$. $(g^p^{h-m-1})^{-1}ag^p^{h-m-1} = a^{(1+sp^j)p^{h-m-1}} = a^{1+sp^{h-m-1+j}+\beta p^{h-m+j}} \neq a$. Hence $a^p^{h-m-1+j} \neq 1$, so $h-m-1+j \neq h$, or $j \neq m+1$. But by Remark A, $j \geq m$. Thus $m \leq j \neq m+1$, and so $m = j$.

Remark E: If $g \in G$ is such that $\langle g^K \rangle = \langle \bar{x} \rangle$, then there exists $y \in G$ such that $G' = \langle a \rangle = \langle [y, g] \rangle$.

Proof: Suppose not. Then for all $y \in G$, we must have $[y, g] \in \langle a^p \rangle$. Let $a = [x_1, x_2]$. Since $g^{-1}ag = a^{1+sp^m}$, where $(s, p) = 1$, we have $a^{1+sp^m} = g^{-1}ag = g^{-1}[x_1, x_2]g = g^{-1}x_1^{-1}g g^{-1}x_2^{-1}g g^{-1}x_1 g g^{-1}x_2 g = x_1^{-1}[x_1^{-1}, g]x_2^{-1}[x_2^{-1}, g]x_1[x_1, g]x_2[x_2, g]$

$$\begin{aligned}
&= x_1^{-1} [x_1^{-1}, g] x_2^{-1} [x_2^{-1}, g] x_1 x_2 [x_1, g] [x_1, g, x_2] [x_2, g] \\
&= x_1^{-1} [x_1^{-1}, g] x_2^{-1} x_1 x_2 [x_2^{-1}, g] [x_2^{-1}, g, x_1 x_2] [x_1, g] [x_1, g, x_2] [x_2, g] \\
&= x_1^{-1} x_2^{-1} x_1 x_2 [x_1^{-1}, g] [x_1^{-1}, g, x_2^{-1} x_1 x_2] [x_2^{-1}, g] [x_2^{-1}, g, x_1 x_2] \\
&\quad [x_1, g] [x_1, g, x_2] [x_2, g] \\
&= [x_1, x_2] [x_1^{-1}, g] [x_1^{-1}, g, x_2^{-1} x_1 x_2] [x_2^{-1}, g] [x_2^{-1}, g, x_1 x_2] \\
&\quad [x_1, g] [x_1, g, x_2] [x_2, g]
\end{aligned}$$

But, by (10.2.1.2) of [5], $[ab, c] = [a, c][a, c, b][b, c]$, so $[a, c][b, c] = [ab, c][a, c, b]^{-1}$ if G' is abelian. Hence $[x_1^{-1}, g][x_1, g] = [x_1^{-1} x_1, g][x_1^{-1}, g, x_1]^{-1}$ and $[x_2^{-1}, g][x_2, g] = [x_2^{-1} x_2, g][x_2^{-1}, g, x_2]^{-1}$, so $a^{1+sp^m} = [x_1, x_2][x_1^{-1}, g, x_2^{-1} x_1 x_2][x_2^{-1}, g, x_1 x_2][x_1^{-1}, g, x_1]^{-1}[x_2^{-1}, g, x_2]^{-1}$. $g^{-1}ag = a^{1+sp^m}$ yields $a^{-1}g^{-1}ag = a^{sp^m}$, or since $a = [x_1, x_2]$ and $a^{1+sp^m} = g^{-1}ag$, we have

$$\langle [x_1^{-1}, g, x_2^{-1} x_1 x_2][x_2^{-1}, g, x_1 x_2][x_1^{-1}, g, x_1]^{-1}[x_2^{-1}, g, x_2]^{-1} \rangle = \langle a^{p^m} \rangle.$$

However, since $[y, g] \in \langle a^p \rangle$ for all $y \in G$, and by Remark A, $w^{-1}a^p w = a^{p(1+s(w)p^{j(w)})}$, where $j(w) \geq m$, we have $(a^p)^{-1}w^{-1}a^p w = [a^p, w] \in \langle a^{p^{m+1}} \rangle$. Thus $[x_1^{-1}, g, x_2^{-1} x_1 x_2]$, $[x_2^{-1}, g, x_1 x_2]$, $[x_1^{-1}, g, x_1]^{-1}$ and $[x_2^{-1}, g, x_2]^{-1}$ are all elements of $\langle a^{p^{m+1}} \rangle$, and so we must have $\langle a^{p^m} \rangle = \langle [x_1^{-1}, g, x_2^{-1} x_1 x_2][x_2^{-1}, g, x_1 x_2][x_1^{-1}, g, x_1]^{-1}[x_2^{-1}, g, x_2]^{-1} \rangle \leq \langle a^{p^{m+1}} \rangle$. But this is a contradiction.

Thus if $g \in G$ is such that $\langle g^K \rangle = \langle \bar{x} \rangle$, then there exists $y \in G$ such that $G' = \langle [y, g] \rangle$.

Lemma II.1: If G is a p -group, $p \neq 2$, satisfying the conditions (W) , then there exists a minimal generating set $\{x_1, c_2, \dots, c_r\}$ for G with the properties $\langle x_1^K \rangle = \langle \bar{x} \rangle$ and $c_i \in C(G')$ for $i = 2, \dots, r$. Furthermore, x_1 may be chosen such that $|\langle x_1 \rangle \cap G'|$ is minimal.

Proof: By condition 5) of (W), a minimal generating set for G contains r -elements. Let $x_1 \in G$ be such that $\langle x_1^K \rangle = \langle \bar{x} \rangle$. Then $x_1 \notin \phi(G)$, so there exists a minimal generating set for G containing x_1 , say $G = \langle x_1, x_2, \dots, x_r \rangle$. Without loss of generality, we can assume $x_1^K = \bar{x}$. Let $x_2^K = \bar{x}^w$. Then $(x_2(x_1^w)^{-1})^K = x_2^K((x_1^w)^{-1})^K = \bar{x}^w(\bar{x}^w)^{-1} = \bar{1}$, so we have $x_2(x_1^w)^{-1} \in C(G') = \ker K$. Thus $x_2 = x_1^w c_2$ where $c_2 \in C(G')$. $G \neq \langle x_1, x_3, \dots, x_r \rangle$ since there are r -elements in a minimal generating set for G . $x_2 = x_1^w c_2 \in \langle x_1, c_2, x_3, \dots, x_r \rangle$, so $G = \langle x_1, c_2, x_3, \dots, x_r \rangle$, $x_1^K = \bar{x}$, $c_2 \in C(G')$ and $\{x_1, c_2, x_3, \dots, x_r\}$ is a minimal generating set for G .

Now suppose $G = \langle x_1, c_2, \dots, c_{k-1}, x_k, \dots, x_r \rangle$ where $x_1^K = \bar{x}$, $c_i \in C(G')$, $c_i \notin \phi(G)$ for $i = 2, \dots, k-1 < r$. Let $x_k^K = \bar{x}^s$, then $(x_k(x_1^s)^{-1})^K = (x_k^K)((x_1^s)^{-1})^K = \bar{x}^s(\bar{x}^s)^{-1} = \bar{1}$. Hence we have $x_k(x_1^s)^{-1} \in C(G')$, and $x_k = x_1^s c_k$ where $c_k \in C(G')$.

$G \neq \langle x_1, c_2, \dots, c_{k-1}, x_{k+1}, \dots, x_r \rangle$ since there are r -elements in a minimal generating set for G . $x_k = x_1^s c_k \in \langle x_1, c_2, \dots, c_k, x_{k+1}, \dots, x_r \rangle$ and we must therefore have $G = \langle x_1, c_2, \dots, c_k, x_{k+1}, \dots, x_r \rangle$. Thus $\{x_1, c_2, \dots, c_k, x_{k+1}, \dots, x_r\}$ is a minimal generating set for G with the properties $x_1^K = \bar{x}$, $c_i \in C(G')$ for $i = 2, \dots, k \leq r$. Thus by induction, we have proven that there exists a minimal generating set for G of the form $G = \langle x_1, c_2, \dots, c_r \rangle$ where $\langle x_1^K \rangle = \langle \bar{x} \rangle$, $c_i \in C(G')$ for $i = 2, \dots, r$.

Since the only property of the element x_1 that was used in the above proof was that $\langle x_1^K \rangle = \langle \bar{x} \rangle$, we may now choose x_1 to be an element of G such that $\langle x_1^K \rangle = \langle \bar{x} \rangle$ and $|\langle x_1 \rangle \cap G'| = \min\{|\langle x \rangle \cap G'| \mid \langle x^K \rangle = \langle \bar{x} \rangle\}$.

Corollary II.1: In the notation of Lemma II.1, c_2 may be chosen such that $G' = \langle [c_2, x_1] \rangle$.

Proof: By Remark E, since $\langle x_1^K \rangle = \langle \bar{x} \rangle$, there exists $y \in G$ such that $G' = \langle a \rangle = \langle [y, x_1] \rangle$. Let $y = x_1^t (\prod_{i=2}^r c_i^{n_i}) a^k$. Then

$$[y, x] = [x_1^t (\prod_{i=2}^r c_i^{n_i}) a^k, x_1] = [x_1^t, x_1] [x_1^t, x_1, (\prod_{i=2}^r c_i^{n_i}) a^k] [(\prod_{i=2}^r c_i^{n_i}) a^k, x_1]$$

$$= [(\prod_{i=2}^r c_i^{n_i}) a^k, x_1].$$

Using the facts $[ab, c] = [a, c][a, c, b][b, c]$ and $c_i \in C(G')$, $a \in C(G')$, we have $[y, x_1] = [(\prod_{i=2}^r c_i^{n_i}) a^k, x_1] = (\prod_{i=2}^r [c_i, x_1]^{n_i}) [a, x_1]^k$. Thus $G' = \langle [y, x_1] \rangle = \langle (\prod_{i=2}^r [c_i, x_1]^{n_i}) [a, x_1]^k \rangle \leq \langle [c_2, x_1], [c_3, x_1], \dots, [c_r, x_1], [a, x_1] \rangle$. $[a, x_1] \in \langle a^{p^m} \rangle \leq \phi(G')$, so we have $G' = \langle [c_2, x_1], [c_3, x_1], \dots, [c_r, x_1] \rangle$. Since G' is cyclic, by choosing i such that $|[c_i, x_1]| = \max\{|[c_j, x_1]| : j = 2, \dots, r\}$, we have $G' = \langle [c_i, x_1] \rangle$. Now reindex, if necessary, to set $i = 2$, and we have $G' = \langle [c_2, x_1] \rangle$.

We now have that $x_1^{-1} [c_2, x_1] x_1 = [c_2, x_1]^{1+tp^m}$ where $(t, p) = 1$.

Lemma II.2: Let G be a p -group, $p \neq 2$, satisfying the conditions (W) , and suppose $G = \langle x_1, c_2, \dots, c_r \rangle$ where $\langle x_1^K \rangle = \langle \bar{x} \rangle$, $c_i \in C(G')$ for $i = 2, \dots, r$, and $G' = \langle [c_2, x_1] \rangle$. Then $[c_i, c_j] \in Z(G) \cap G'$ for $i, j = 2, \dots, r$.

Proof: By (10.2.1.5) of [5], we have $[x, y, z][y, z, x][z, x, y] = [y, x][z, x][z, y]^x [x, y][x, z]^y [y, z]^x [x, z][z, x]^y = 1$ since G' is abelian. Thus $[x_1, c_i, c_j][c_i, c_j, x_1][c_j, x_1, c_i] = 1$. But $c_i, c_j \in C(G')$ gives $[x_1, c_i, c_j] = 1 = [c_j, x_1, c_i]$. Thus $[c_i, c_j, x_1] = 1$, that is $[c_i, c_j]^{-1} x_1^{-1} [c_i, c_j] x_1 = 1$. Since $[c_i, c_j] \in G'$, $[c_i, c_j] = [c_2, x_1]^k$ for some k . Thus

$x_1^{-1}[c_i, c_j]x_1 = x_1^{-1}[c_2, x_1]^k x_1 = (x_1^{-1}[c_2, x_1]x_1)^k = [c_i, x_1]^{k(1+tp^m)}$
 $= [c_i, c_j]^{1+tp^m}$. Hence $[c_i, c_j]^{-1}x_1^{-1}[c_i, c_j]x_1 = [c_i, c_j]^{-1}[c_i, c_j]^{1+tp^m}$
 $= [c_i, c_j]^{tp^m} = 1$, and we have $|[c_i, c_j]| \leq p^m$. But $|Z(G) \cap G'| = p^m$
 and since G' is cyclic, we must have $[c_i, c_j] \in Z(G) \cap G'$ for
 $i, j = 2, \dots, r$.

Remark F: If $g^{-1}[c_2, x_1]g = [c_2, x_1]^{1+sp^w}$ where $(s, p) = 1$
 and $w \geq m$, then $(g^k)^{-1}y g^k = y[y, g] \frac{(1+sp^w)^k - 1}{sp^w}$ for $k \geq 1$.

Proof: $g^{-1}yg = yy^{-1}g^{-1}yg = y[y, g] = y[y, g] \frac{(1+sp^w) - 1}{sp^w}$.
 Now assume the formula is true for $k = n$ and let $[y, g] = [c_2, x_1]^u$.

$$\begin{aligned}
 \text{Then } (g^{n+1})^{-1}y g^{n+1} &= g^{-1}(g^n)^{-1}y g^n g = g^{-1}y[y, g] \frac{(1+sp^w)^n - 1}{sp^w} g \\
 &= g^{-1}yg(g^{-1}[y, g]g) \frac{(1+sp^w)^n - 1}{sp^n} = y[y, g](g^{-1}[c_2, x_1]g)^u \frac{(1+sp^w)^n - 1}{sp^w} \\
 &= y[y, g][c_2, x_1]^{(1+sp^w)^u} \frac{(1+sp^w)^n - 1}{sp^w} \\
 &= y[y, g] \frac{sp^w}{sp} [y, g] \frac{(1+sp^w)^{n+1} - 1 - sp^w}{sp^w} = y[y, g] \frac{(1+sp^w)^{n+1} - 1}{sp^w}.
 \end{aligned}$$

Thus, by induction, the Remark is proven.

Lemma II.3: If $g \in G$ is such that $G' = \langle [g, x_1] \rangle$, then
 $|g^G| \geq p^m$, where $G \wr G/G'$.

Proof: Let $g^{-1}ag = a^{1+sp^r}$ where $(s, p) = 1$, $r \geq m$
 and $G' = \langle a \rangle$. By Remark F, $(g^{p^{m-1}})^{-1}x_1 g^{p^{m-1}} = x_1[x_1, g] \frac{(1+sp^r)^{p^{m-1}} - 1}{sp^r}$
 $= x_1[x_1, g]^{p^{m-1} + \beta p^m}$. Hence we have $\langle [g^{p^{m-1}}, x_1] \rangle = \langle [x_1, g]^{p^{m-1}} \rangle$
 $= \langle [c_2, x_1]^{p^{m-1}} \rangle$ since $G' = \langle a \rangle = \langle [c_2, x_1] \rangle = \langle [g, x_1] \rangle$.

If $|g^G| \not\geq p^m$, then $g^{p^{m-1}} \in G'$, so $g^{p^{m-1}} = [c_2, x_1]^k$
 for some k . Thus $\langle [g^{p^{m-1}}, x_1] \rangle = \langle [[c_2, x_1]^k, x_1] \rangle = \langle [c_2, x_1]^{p^{m-1}} \rangle$.

But $x_1^{-1}[c_2, x_1]^k x_1 = [c_2, x_1]^{k(1+tp^m)}$, so we have

$[[c_2, x_1]^k, x_1] = [c_2, x_1]^{ktp^m}$ and $\langle [[c_2, x_1]^k, x_1] \rangle \leq \langle [c_2, x_1]^{p^m} \rangle$
 $\neq \langle [c_2, x_1]^{p^{m-1}} \rangle$, a contradiction. Thus we must have $|g^G| \geq p^m$.

Lemma II.4: Let G satisfy the conditions (W), and $\{x_1, c_2, \dots, c_r\}$ be as in the conclusion of Lemma II.1. Also suppose $G' = \langle [c_2, x_1] \rangle$.

1). If $Z(G) \leq G'$, then $|c_2| = p^{h+m}$ and $G' = \langle c_2^{p^m} \rangle$.

2). If $Z(G) = Z^* \otimes A$ where $Z^* = Z(G) \cap G'$ and

$\exp Z = \exp Z^* \not\supseteq \exp A$, then $|c_2| = p^{h+m}$ and
 $\langle c_2^{p^{2m-1}} \rangle = \langle [c_2, x_1]^{p^{m-1}} \rangle$.

Proof: Consider the following conjugation relations:

$$\begin{aligned} (c_2^{tp^m})^{-1} x_1 c_2^{tp^m} &= x_1 [x_1, c_2^{tp^m}] = x_1 [x_1, c_2]^{tp^m}. \quad (c_2^{tp^m})^{-1} c_j c_2^{tp^m} \\ &= c_j [c_j, c_2^{tp^m}] = c_j [c_j, c_2]^{tp^m} = c_j \quad \text{for all } j = 2, \dots, r \text{ by} \end{aligned}$$

Lemma II.4.

$$\begin{aligned} \text{Also } [c_2, x_1]^{-1} x_1 [c_2, x_1] &= x_1 x_1^{-1} [c_2, x_1]^{-1} x_1 [c_2, x_1] \\ &= x_1 (x_1^{-1} [c_2, x_1] x_1)^{-1} [c_2, x_1] = x_1 ([c_2, x_1]^{(1+tp^m)})^{-1} [c_2, x_1] \\ &= x_1 ([c_2, x_1]^{tp^m})^{-1} = x_1 [x_1, c_2]^{tp^m}. \quad [c_2, x_1]^{-1} c_j [c_2, x_1] = c_j \text{ since} \\ c_j &\in C(G') \text{ for } j = 2, \dots, r. \end{aligned}$$

Thus we have $\pi_{[c_2, x_1]} = \pi_{c_2^{tp^m}}$ where π_y denotes the

inner automorphism of G induced by conjugation by the element y .

Hence we have $[c_2, x_1]z = c_2^{tp^m}$ where $z \in Z(G)$.

1). If $Z(G) \leq G'$, then $\langle [c_2, x_1]z \rangle = \langle [c_2, x_1] \rangle = \langle c_2^{p^m} \rangle$
and $|[c_2, x_1]z| = |[c_2, x_1]| = |c_2^{p^m}| = p^h$, so $|c_2| = p^{h+m}$.

2). If $Z(G) = Z^* \otimes A$ and $\exp Z(G) = \exp Z^* \not\supseteq \exp A$,

then $([c_2, x_1]z)^{p^{m-1}} = [c_2, x_1]^{p^{m-1}} z^{p^{m-1}} \in G'$. Thus

$([c_2, x_1]z)^{p^{m-1}} = c_2^{tp^{2m-1}} \in G'$ and we have $\langle c_2^{p^{2m-1}} \rangle \leq G'$.

$|c_2^{tp^m}| = |c_2^{p^m}| = |[c_2, x_1]z| = p^h$, so $|c_2| = p^{h+m}$. Thus we have
 $|<c_2^{p^{2m-1}}>| = p^{h-m+1}$ and since G' is cyclic, we now have
 $<c_2^{p^{2m-1}}> = <[c_2, x_1]^{p^{m-1}}>$.

Remark G: If $y = x_1 c_2^a$, then for $k \geq 0$ we have

$$y^k = x_1^k (c_2^a)^k [c_2, x_1]^{\frac{a}{(tp^m)^2} ((1+tp^m)^k - 1 - ktp^m)}.$$

Proof: Let $k = 0$. Then $y^0 = 1$

$$= x_1^0 (c_2^a)^0 [c_2, x_1]^{\frac{a}{(tp^m)^2} ((1+tp^m)^0 - 1)}$$
. Assume the formula is true
for $k = n$. Then $y^{n+1} = y y^n = x_1 c_2^a x_1^n (c_2^a)^n [c_2, x_1]^{\frac{a}{(tp^m)^2} ((1+tp^m)^n - 1 - ntp^m)}$

$$= x_1^{n+1} c_2^a [c_2^a, x_1^n] (c_2^a)^n [c_2, x_1]^{\frac{a}{(tp^m)^2} ((1+tp^m)^n - 1 - ntp^m)}$$

$$= x_1^{n+1} (c_2^a)^{n+1} [c_2, x_1^n]^a [c_2, x_1]^{\frac{a}{(tp^m)^2} ((1+tp^m)^n - 1 - ntp^m)}$$
 since
 $c_2 \in C(G')$.

By Remark F, $[c_2, x_1^n] = [c_2, x_1]^{\frac{(1+tp^m)^n - 1}{tp^m}}$, so

$$y^{n+1} = x_1^{n+1} (c_2^a)^{n+1} [c_2, x_1]^{\frac{a}{(tp^m)^2} (tp^m((1+tp^m)^n - 1) - tp^m)}$$

$$= x_1^{n+1} (c_2^a)^{n+1} [c_2, x_1]^{\frac{a}{(tp^m)^2} ((1+tp^m)^{n+1} - 1 - (n+1)tp^m)}$$
 and by induction, we have proven the formula.

Lemma II.5: Let G be a p -group, $p \neq 2$, satisfying the conditions (W), and let $\{x_1, c_2, \dots, c_r\}$ be a minimal generating set of G satisfying the conclusions of Lemma II.1. Let x_1 be chosen such that $|<x_1> \cap G'|$ is minimal, and suppose

$G' = \langle [c_2, x_1] \rangle$. Then $|x_1| \geq p^h$.

Also, $\langle x_1 \rangle \cap G' = \langle 1 \rangle$ if either of the following conditions hold:

- 1). $Z(G) \leq G'$,
- 2). $Z(G) = Z^* \otimes A$ where $Z^* = Z(G) \cap G'$,
 $\exp Z(G) = \exp Z^* \not\leq \exp A$ and $h \geq 2m$.

Proof: $(x_1^{p^{h-1}})^{-1} c_2 x_1^{p^{h-1}} = c_2 [c_2, x_1]^{\frac{(1+tp^m)p^{h-1}-1}{(tp^m)}}$
 $= c_2 [c_2, x_1]^{p^{h-1} + \beta p^h} \neq c_2$ since $[c_2, x_1]^{p^{h-1}} \neq 1$. Thus
 $x_1^{p^{h-1}} \notin C(\langle c_2 \rangle)$, hence $|x_1| \geq p^h$. Also, since $c_2 \in C(G')$, we
have $x_1^{p^{h-1}} \notin G'$. $x_1^{p^h} \in Z(G)$ since $(x_1^{p^h})^{-1} g x_1^{p^h} =$
 $g [g, x_1]^{\frac{(1+tp^m)p^h-1}{tp^m}} = g [g, x_1]^{p^h + \beta p^{h+1}} = g$ since $|G'| = p^h$.

If $\langle x_1 \rangle \cap G' \neq \langle 1 \rangle$, then $\langle x_1 \rangle \cap G' \leq Z(G) \cap G'$. Under
either of the conditions 1) or 2) of Lemma II.5, we have
 $\exp Z(G) = p^m$. Thus $p^h \leq |x_1| \leq p^{h+m}$, so assume $|x_1| = p^{h+g}$
where $0 \leq g \leq m$. Also we have, by Lemma II.4, $\langle c_2^{p^{2m-1}} \rangle =$
 $\langle [c_2, x_1]^{p^{m-1}} \rangle \geq Z(G) \cap G'$ under condition 2) of Lemma II.5, or
 $\langle c_2 \rangle \geq Z(G) \cap G'$ under condition 1) of Lemma II.5. Let
 $x_1^{p^{h+g-1}} = z^{rp^{m-1}}$ where $\langle z \rangle = Z(G) \cap G'$. Then for some α ,
where $(\alpha, p) = 1$, $(z^{rp^{m-1}})^{-1} = c_2^{\alpha p^{h+m-1}}$.

Set $y = x_1 c_2^{\alpha p^{m-g}}$. Then $y^{p^{h-1}} =$

$$x_1^{p^{h-1}} c_2^{\alpha p^{h+m-g-1}} [c_2, x_1]^{\frac{\alpha p^{m-g}}{(tp^m)^2} ((1+tp^m)p^{h-1}-1-tp^{h+m-1})}.$$

$x_1^{p^{h-1}} \notin C(\langle c_2 \rangle)$ implies $y^{p^{h-1}} \notin C(\langle c_2 \rangle)$, so $y^{p^{h-1}} \notin G'$.

$$\begin{aligned}
y^p^{h+g-1} &= x_1^p^{h+g-1} c_2^{\alpha p^{h+m-1}} [c_2, x_1]^{\frac{\alpha p^{m-g}}{(tp^m)^2}} ((1+tp^m)^p)^{h+g-1} {}^{-1-tp^{h+g+m-1}} \\
&= (z^{rp^{m-1}}) (z^{rp^{m-1}})^{-1} [c_2, x_1]^{\frac{\alpha p^{m-g}}{(tp^m)^2}} \beta p^{h+m+g} = 1 \quad \text{since } |G'| = p^h.
\end{aligned}$$

Thus $|y| \neq |x_1|$.

$y^K = (x_1 c_2^{\alpha p^{m-g}})^K = x_1^K (c_2^{\alpha p^{m-g}})^K = x_1^K$, so since $\langle x_1^K \rangle = \langle \bar{x} \rangle$, we have $\langle y^K \rangle = \langle \bar{x} \rangle$. Now suppose that $y^p^{h+u} \in G'$ where $0 \leq u \leq g-1$. Then $y^p^{h+u} = x_1^p^{h+u} c_2^{\alpha p^{h+u+m-g}} [c_2, x_1]^{\frac{\alpha p^{m-g}}{(tp^m)^2}} ((1+tp^m)^p)^{h+u} {}^{-1-tp^{h+u+m-g}}$. If $Z(G) \leq G'$, then $c_2^{\alpha p^{h+u+m-g}} \in G'$ since $G' = \langle c_2^{p^m} \rangle$. If $Z(G) = Z^* \otimes A$, $\exp Z^* \neq \exp A$ and $h \geq 2m$, then $\langle c_2^{p^{2m-1}} \rangle \leq G'$ and also $h+u+m-g \geq h \geq 2m-1$, so $c_2^{\alpha p^{h+u+m-g}} \in G'$. In either case, since $y^p^{h+u} \in G'$, we must also have $x_1^p^{h+u} \in G'$. Thus $|\langle y \rangle \cap G'| \neq |\langle x_1 \rangle \cap G'|$, a contradiction to the minimality of $|\langle x_1 \rangle \cap G'|$. Thus $\langle x_1 \rangle \cap G' = \langle 1 \rangle$.

Theorem II.1: Let G be a p -group, $p \neq 2$, satisfying the conditions (W), and suppose $Z(G) \leq G'$. Then G is a central product of the form $G = \hat{A}B$ where $\hat{A} = \langle x_1, c_2 | x_1^p = c_2^{p^{h+m}} = 1, [c_2, x_1] = c_2^{tp^m} \rangle$ and B is a p -group of nilpotence class two having a cyclic center.

Proof: The proof consists of three steps. First we find a new minimal generating set for G consisting of $\{x_1, c_2, g_3, \dots, g_r\}$, where x_1, c_2 are as before, but $g_i \in Z_2(G)$ for $i = 3, \dots, r$. Next we analyse $\langle x_1, c_2 \rangle \leq G$. Thirdly, we write G as the desired central product.

Step 1: Let G be a p -group, $p \neq 2$, satisfying the conditions (W) and also such that $Z(G) \leq G'$. By Lemma II.1,

$G = \langle x_1, c_2, \dots, c_r \rangle$ where $\langle x_1^K \rangle = \langle \bar{x} \rangle$ and $c_i \in C(G')$. By Corollary II.1, $G' = \langle [c_2, x_1] \rangle$. By Lemma II.4, we have $|c_2| = p^{h+m}$ and $G' = \langle [c_2, x_1] \rangle = \langle c_2^{p^m} \rangle$. By Lemma II.5 and the assumption $|\langle x_1 \rangle \cap G'|$ is minimal, we have $|x_1| = p^h$ and $\langle x_1 \rangle \cap G' = \langle 1 \rangle$, since $x_1^{p^h} \in Z(G) \leq G'$ and $\langle x_1 \rangle \cap G' = \langle 1 \rangle$.

For $i \geq 3$, we wish to show we can replace each c_i in our minimal generating set by a g_i , where $g_i \in Z_2(G)$. Since $[c_j, c_i] \in Z(G) \cap G'$ for $i, j \geq 2$, if $[x_1, c_i] \in Z(G)$, we have $c_i \in Z_2(G)$. Thus suppose $[x_1, c_i] \notin Z(G)$. $Z(G) \not\leq G'$ and G' cyclic imply that $Z(G) \not\leq \langle [x_1, c_i] \rangle$.

$$\begin{aligned} [x_1, c_i] x_1 [x_1, c_i]^{-1} &= x_1 x_1^{-1} [x_1, c_i] x_1 [x_1, c_i]^{-1} \\ &= x_1 (x_1^{-1} [c_2, x_1]^k x_1) [x_1, c_i]^{-1} \text{ where } [x_1, c_i] = [c_2, x_1]^k \\ &= x_1 [c_2, x_1]^{k(1+tp^m)} [x_1, c_i]^{-1} = x_1 [x_1, c_i]^{(1+tp^m)} [x_1, c_i]^{-1} \\ &= x_1 [x_1, c_i]^{tp^m}. \end{aligned}$$

$$[x_1, c_i] c_j [x_1, c_i]^{-1} = c_j \text{ for } j \geq 2 \text{ since } c_j \in C(G').$$

$$\begin{aligned} \text{Also } (c_i^{tp^m})^{-1} x_1 c_i^{tp^m} &= x_1 [x_1, c_i]^{tp^m} = x_1 [x_1, c_i]^{tp^m} (c_i^{tp^m})^{-1} c_j c_i^{tp^m} \\ &= c_j [c_j, c_i]^{tp^m} = c_j [c_j, c_i]^{tp^m} = c_j \text{ by Lemma II.2.} \end{aligned}$$

Thus $\pi_{[x_1, c_i]^{-1}} = \pi_{c_i^{tp^m}}$, so $[x_1, c_i]^{-1} z = c_i^{tp^m}$ where $z \in Z(G)$. But $Z(G) \not\leq \langle [x_1, c_i] \rangle$, so $\langle [x_1, c_i] \rangle = \langle c_i^{p^m} \rangle \leq \langle c_i \rangle$. Moreover, $Z(G) \not\leq \langle [c_2, x_1]^{p^{h-m-1}} \rangle \leq \langle [x_1, c_i] \rangle \cap \langle [c_2, x_1] \rangle \leq \langle c_i \rangle \cap \langle c_2 \rangle$.

Let $H_i = \langle c_2, c_i \rangle$. H_i is two-generated since $G' \leq H_i$ and c_j, c_i are in a minimal generating set for G . $H_i' \leq Z(G) = Z$ since $[c_2, c_i] \in Z(G)$. Let $H_i \xrightarrow{\gamma} H_i/Z$. H_i/Z is abelian and two-generated since $Z \leq G'$ and since $c_i^{tp^m} \in \langle [x_1, c_i] \rangle \leq G'$, we have

$|c_i^Y| \leq p^h$ because $|c_i| \leq p^{h+m}$. $|c_2^Y| = p^h$ since $G' = \langle c_2^{p^m} \rangle$. Thus $|c_2^Y| \geq |c_i^Y|$, so if H_i/Z is cyclic, $H_i/Z = \langle c_2^Y \rangle$. Thus $c_i^Y = (c_2^Y)^k$ for some k , or $c_i = c_2^k z$. But $Z(G) \leq G' \leq \langle c_2 \rangle$ then implies $c_i \in \langle c_2 \rangle$. Thus $G = \langle x_1, c_2, \dots, c_{i-1}, c_{i+1}, \dots, c_r \rangle$, a contradiction to the minimality of the generating set $\{x_1, c_2, \dots, c_r\}$.

Since H_i/Z is two-generated and c_2^Y is an element of highest order in H_i/Z , we have that $H_i/Z = \langle c_2^Y \rangle \otimes \langle b \rangle$, and $\langle c_2^Y \rangle \cap \langle b \rangle = \bar{1}$. Let $g_i \in H_i$ be such that $g_i^Y = b$. Then $H_i/Z = \langle c_2^Y \rangle \otimes \langle g_i^Y \rangle$ and $\langle c_2 \rangle \cap \langle g_i \rangle \leq Z$. $c_i^Y = (g_i^Y)^w (c_2^Y)^s$ for some w, s , so $c_i = g_i^w c_2^s z$ where $z \in Z(G) \leq G' \leq \langle c_2 \rangle$, so $c_i = g_i^w c_2^u$ for some w, u .

$G \neq \langle x_1, c_2, \dots, c_{i-1}, c_{i+1}, \dots, c_r \rangle$, but since $c_i = g_i^w c_2^u \in \langle x_1, c_2, \dots, c_{i-1}, g_i, c_{i+1}, \dots, c_r \rangle$, we have $G = \langle x_1, c_2, \dots, c_{i-1}, g_i, c_{i+1}, \dots, c_r \rangle$.

$g_i \in H_i = \langle c_2, c_i \rangle$ implies $g_i = c_i^a c_2^d$ for some a, d . Thus $[c_j, g_i] = [c_j, c_i^a c_2^d] = [c_j, c_2^d][c_j, c_i^a][c_j, c_i^a, c_2^d] = [c_j, c_2^d][c_j, c_i^a] \in Z(G)$ for $j = 2, \dots, r$. Also, $g_i \in C(G')$ since $c_2, c_i \in C(G')$.

$[x_1, g_i] \in Z(G)$ and hence $g_i \in Z_2(G)$, for if $[x_1, g_i] \notin Z(G)$ we have:

$$\begin{aligned} [x_1, g_i] x_1 [x_1, g_i]^{-1} &= x_1 x_1^{-1} [x_1, g_i] x_1 [x_1, g_i]^{-1} = x_1 [x_1, g_i]^{tp^m} \\ [x_1, g_i] c_j [x_1, g_i] &= c_j \text{ for } j = 2, \dots, r. \quad (g_i^{tp^m})^{-1} x_1 g_i^{tp^m} \\ &= x_1 [x_1, g_i]^{tp^m} = x_1 [x_1, g_i]^{tp^m} \text{ since } g_i \in C(G'). \quad (g_i^{tp^m})^{-1} c_j g_i^{tp^m} \\ &= c_j [c_j, g_i]^{tp^m} = c_j [c_j, g_i]^{tp^m} = c_j \text{ since } [c_j, g_i] \in Z(G). \end{aligned}$$

Thus we have $\pi_{[x_1, g_i]^{-1}}^{-1} = \pi_{g_i}^{tp^m}$, or $[x_1, g_i]^{-1} z = g_i^{tp^m}$ where $z \in Z(G)$. But $[x_1, g_i] \notin Z(G)$ and we must have

$\langle [x_1, g_i] \rangle = \langle g_i^{tp^m} \rangle = \langle g_i^{p^m} \rangle$. Also, $[c_2, x_1]^{p^{h-m-1}} \in \langle [x_1, g_i] \rangle$, so $[c_2, x_1]^{p^{h-m-1}} \in \langle g_i \rangle$. But $[c_2, x_1]^{p^{h-m-1}} \notin Z(G)$ on the one hand, and on the other $[c_2, x_1]^{p^{h-m-1}} \in \langle c_2 \rangle \cap \langle g_i \rangle$. However, $\langle c_2 \rangle \cap \langle g_i \rangle \leq Z(G)$, thus we have a contradiction. Thus $[x_1, g_i] \in Z(G)$, and we replace c_i by $g_i \in Z_2(G)$ in our minimal generating set for G .

Proceeding in this manner, we can write G in the form

$$G = \langle x_1, c_2, g_3, \dots, g_r \rangle \text{ where } \langle x_1^K \rangle = \langle \bar{x} \rangle, c_2 \in C(G'),$$

$$G' = \langle [c_2, x_1] \rangle = \langle c_2^{p^m} \rangle \text{ and } g_i \in Z_2(G), i = 3, \dots, r.$$

Step 2: Let $\hat{A} = \langle x_1, c_2 \rangle$. $\hat{A} \trianglelefteq G$ since $G' = \langle c_2^{p^m} \rangle \leq \hat{A}$.

$\hat{A} = \langle x_1, c_2 | x_1^{p^h} = c_2^{p^{h+m}} = 1, [c_2, x_1] = c_2^{tp^m}, (t, p) = 1 \rangle$. Let $w = up^k$ where $(u, p) = 1$. $x_1^w \in Z(\hat{A})$ if, and only if $x_1^{p^k} \in Z(\hat{A})$, that is, if and only if, $(x_1^{p^k})^{-1} c_2 x_1^{p^k} = c_2$. But $(x_1^{p^k})^{-1} c_2 x_1^{p^k} = c_2 [c_2, x_1] \frac{(1+tp^m)^{p^k} - 1}{tp^m} = c_2$ if, and only if, $[c_2, x_1] \frac{(1+tp^m)^{p^k} - 1}{tp^m} = 1$, or we must have $k \geq h$. But $x_1^{p^k} = 1$ if $k \geq h$, so $\langle x_1 \rangle \cap Z(\hat{A}) = 1$.

$c_2^w \in Z(\hat{A})$ if, and only if $(c_2^w)^{-1} x_1^{-1} c_2^w = x_1^{-1}$, or

$[c_2^w, x_1] = 1$ which is true if, and only if $p^h | w$.

If $x_1^d c_2^e \in Z(\hat{A})$, then $(x_1^d c_2^e)^{-1} x_1 x_1^d c_2^e = (c_2^e)^{-1} x_1 c_2^e = x_1$, or $c_2^e \in Z(\hat{A})$. Then $(x_1^d c_2^e) (c_2^e)^{-1} = x_1^d \in Z(\hat{A})$. But $x_1^d \in Z(\hat{A})$ implies $x_1^d = 1$, so we have $Z(\hat{A}) = \langle c_2^{p^h} \rangle$.

Letting $w = up^k$ where $(u, p) = 1$, we have $x_1^w \in Z_2(\hat{A})$

if, and only if, $x_1^{p^k} \in Z_2(\hat{A})$, if, and only if,

$$c_2^{-1} (x_1^{p^k})^{-1} c_2 x_1^{p^k} \in Z(\hat{A}), \text{ or equivalently } c_2^{-1} c_2 [c_2, x_1] \frac{(1+tp^m)^{p^k} - 1}{tp^m} \in Z(\hat{A}).$$

$$\text{But } [c_2, x_1] \frac{(1+tp^m)^{p^k} - 1}{tp^m} = [c_2, x_1]^{p^k + \beta p^{k+1}} = c_2^{p^{k+m} + \beta p^{k+m+1}} \in Z(\hat{A})$$

if, and only if $k+m \geq h$, or $k \geq h-m$.

$c_2^d \in Z_2(\hat{A})$ if, and only if, $[c_2, x_1]^d \in Z(\hat{A})$, which is equivalent with $c_2^{dp^m} \in Z(\hat{A})$. Thus $c_2^d \in Z(\hat{A})$ if, and only if, $p^{h-m} | d$.

If $x_1^w c_2^d \in Z_2(\hat{A})$, then $x_1^{-1} (x_1^w c_2^d)^{-1} x_1 x_1^w c_2^d \in Z(\hat{A})$, or $x_1^{-1} (c_2^d)^{-1} x_1 c_2^d \in Z(\hat{A})$ and we have $c_2^d \in Z_2(\hat{A})$. Thus $(x_1^w c_2^d) (c_2^d)^{-1} = x_1^w \in Z_2(\hat{A})$. Thus $Z_2(\hat{A}) = \langle x_1^{p^{h-m}}, c_2^{p^{h-m}} \rangle$.

$|A_c(\hat{A})| = |\text{Hom}(\hat{A}/\hat{A}', Z(\hat{A}))| = p^{2m}$ since we have \hat{A} is a p -group, $p \neq 2$, with no abelian direct factors. Also if $\hat{A} \twoheadrightarrow \hat{A}/\hat{A}'$, then since $\langle x_1 \rangle \cap G' = \langle x_1 \rangle \cap \hat{A}' = \langle 1 \rangle$, we have $|x_1^Y| = p^h$, $|c_2^Y| = p^m$, and $\langle x_1^Y \rangle \cap \langle c_2^Y \rangle = \langle \bar{1} \rangle$, so $\hat{A}/\hat{A}' = \langle x_1^Y \rangle \otimes \langle c_2^Y \rangle$. $|Z_2(\hat{A})/Z(\hat{A})| = |\langle x_1^{p^{h-m}}, c_2^{p^{h-m}} \rangle / \langle c_2^{p^h} \rangle| = p^{2m}$. Thus we have $|A_c(\hat{A})| = |Z_2(\hat{A})/Z(\hat{A})| = |A_c(\hat{A}) \cap I(\hat{A})|$. Thus $A_c(\hat{A}) \leq I(\hat{A})$.

Step 3: We now have $G = \langle x_1, c_2, g_3, \dots, g_r \rangle$ where

$g_i \in Z_2(G)$, $i = 3, \dots, r$, and $\hat{A} = \langle x_1, c_2 \rangle \trianglelefteq G$ such that $A_c(\hat{A}) \leq I(\hat{A})$.

We note that in Step 2, we have shown that $\hat{A}' = G'$ and $Z(\hat{A}) = Z(G)$.

Since $g_i \in Z_2(G)$, we have $\pi_{g_i}|_{\hat{A}} \in A_c(\hat{A}) \leq I(\hat{A})$. Thus there exists

$y_i \in \hat{A}$ such that $\pi_{g_i}|_{\hat{A}} = \pi_{y_i}|_{\hat{A}}$. It is known that if T is a

group, $B \leq T$ and for $x, y \in T$ we have $\pi_x|_B = \pi_y|_B$, then

$xy^{-1} \in C_T(B)$. Since $\pi_{g_i}|_{\hat{A}} = \pi_{y_i}|_{\hat{A}}$, we have $g_i y_i^{-1} \in C_G(\hat{A})$, or

that $g_i = y_i d_i$ where $d_i \in C_G(\hat{A})$. Since $Z_2(\hat{A}) \leq \phi(\hat{A})$ and

$\hat{A} \trianglelefteq G$, we have by 7.3.17 of [8] that $Z_2(\hat{A}) \leq \phi(G)$. Thus $y_i \in \phi(G)$.

If $d_i \in \phi(G)$, then $g_i \in \phi(G)$, a contradiction to g_i being in a minimal generating set for G . Thus $d_i \notin \phi(G)$.

$G \neq \langle x_1, c_2, g_3, \dots, g_{i-1}, g_{i+1}, \dots, g_r \rangle$, but since $y_i \in \langle x_1, c_2 \rangle$,

$g_i = y_i d_i \in \langle x_1, c_2, g_3, \dots, g_{i-1}, d_i, g_{i+1}, \dots, g_r \rangle$. Thus we replace

g_i by d_i . Proceeding in this manner, we can write

$G = \langle x_1, c_2, d_3, \dots, d_r \rangle$ where $d_i \in C_G(\hat{A})$ for $i = 3, \dots, r$.

Set $B = \langle d_3, \dots, d_r \rangle$, $\hat{A} = \langle x_1, c_2 \rangle \trianglelefteq G$. Then $G = \hat{A}B$, $B \leq C_G(\hat{A})$ so $\hat{A} \trianglelefteq G$, $B \trianglelefteq G$. $\hat{A} \cap B \leq Z(\hat{A})$ and we have that G is a central product of the desired form since $Z(B) \leq Z(G)$ which is cyclic.

Corollary II.2: $\hat{A} = \langle x_1, x_2 | x_2^{p^{h+m}} = x_1^{p^h} = 1, [x_2, x_1] = x_2^{tp^m}, (t, p) = 1, m < h \rangle$ is a group such that all its central automorphisms are inner automorphisms.

Proof: Step 2 of Theorem II.1.

Theorem II.2: Let G be a p -group, $p \neq 2$, with $Z(G) \not\leq G'$ and G' is cyclic. Then $A_c(G) \leq I(G)$.

Proof: Since $Z(G) \not\leq G'$, G has no abelian direct factors. G' cyclic and $Z(G) \not\leq G'$ yield G has nilpotence class at least three, and $Z(G) \cap G' = Z(G) \leq G'$, thus G satisfies the conditions (W), and also the hypothesis of Theorem II.1. Thus we have $G = \hat{A}B$ as a central product where $\hat{A} = \langle x_1, c_2 | x_1^{p^h} = c_2^{p^{h+m}} = 1, [c_2, x_1] = c_2^{tp^m}, (t, p) = 1, m < h \rangle$, $G' = \hat{A}' = \langle c_2^{p^m} \rangle$, $|G'| = p^h$, $Z(G) = Z(\hat{A}) = \langle c_2^{p^h} \rangle$, $|Z(G)| = p^m$, and $Z(G) \leq G'$. G a central product of \hat{A} and B gives $\hat{A} \cap B \leq Z(G) \leq G'$. Using the results of Step 2 of Theorem 1, and the fact that $B \leq C_G(\hat{A})$, we have

$Z_2(G) = \langle x_1^{p^{h-m}}, c_2^{p^{h-m}}, B \rangle$. Thus

$$\left| \frac{Z_2(G)}{Z(G)} \right| = \frac{|\langle x_1^{p^{h-m}}, c_2^{p^{h-m}} \rangle| |B|}{|Z(G)| |\langle x_1^{p^{h-m}}, c_2^{p^{h-m}} \rangle \cap B|} = \frac{p^{3m}}{p^m} \frac{|B|}{|G' \cap B|}$$

since $Z(G) = \langle c_2^{p^h} \rangle \leq \langle c_2^{p^{h-m}} \rangle$ and $\hat{A} \cap B \leq Z(G) \cap B \leq \langle c_2^{p^{h-m}} \rangle \cap B \leq G' \cap B$.

$$G/G' = \frac{\hat{A}B}{G'} = \frac{\hat{A}(BG')}{G'} = \frac{\hat{A}}{G'} \cdot \frac{BG'}{G'}.$$

Let $yG' \in \frac{\hat{A}}{G'} \cap \frac{BG'}{G'}$, then $yG' \in \hat{A}/G'$, but $G' \leq \hat{A}$ so $y \in \hat{A}$.

Also $yG' \in BG'/G'$, thus $y \in BG'$. Hence $y \in \hat{A} \cap BG' = G'(\hat{A} \cap B) = G'$.

Thus $yG' = \bar{1}$ and we have $\frac{\hat{A}}{G'} \cap \frac{BG'}{G'} = \bar{1}$. Thus

$$\begin{aligned} \frac{G}{G'} &= \frac{\hat{A}}{G'} \otimes \frac{BG'}{G'} \cong \frac{\hat{A}}{G'} \otimes \frac{B}{B \cap G'} \quad |A_c(G)| = |\text{Hom}(G/G', Z(G))| \\ &= |\text{Hom}(\hat{A}/G', Z(G))| |\text{Hom}(\frac{B}{B \cap G'}, Z(G))| = p^{2m} |\text{Hom}(\frac{B}{B \cap G'}, Z(G))| \\ &= p^{2m} \frac{|B|}{|B \cap G'|} \text{ since if } b \in B, \text{ then } [y, b] \in Z(G) \text{ for all } y \in G \end{aligned}$$

because B is of nilpotence class two and B centralizes \hat{A} .

But $[y, b^{p^m}] = [y, b]^{p^m} = 1$ since $|Z(G)| = p^m$. Thus

$\exp \frac{B}{B \cap G'} \leq p^m$ since $b^{p^m} \in Z(G) \leq G'$ for all $b \in B$. Thus

$$\begin{aligned} \text{Hom}(\frac{B}{B \cap G'}, Z(G)) &\cong \frac{B}{B \cap G'}. \text{ We now have } |Z_2(G)/Z(G)| \\ &= |A_c(G) \cap I(G)| = |A_c(G)|, \text{ or } A_c(G) \leq I(G). \end{aligned}$$

Theorem II.3: If G is a p -group, $p \neq 2$, satisfying the conditions (W) and $Z(G) \leq G'$, then $|G|$ divides $|A(G)|$.

Proof: By Theorem II.1, $G = \hat{A}B$ where B is a p -group of nilpotence class two, $\hat{A} = \langle x_1, c_2 | x_1^{p^h} = c_2^{p^{h+m}} = 1, [c_2, x_1] = c_2^{tp^m}, (t, p) = 1 \rangle$ and $\hat{A} \cap B \leq Z(\hat{A}) = Z(G) = \langle c_2^{p^h} \rangle = \langle [c_2, x_1]^{p^{h-m}} \rangle$.

$$\begin{aligned} \text{Define } \phi \text{ on } \hat{A} \text{ by: } x_1^\phi &= x_1, c_2^\phi = x_1^{p^{h-m}} c_2. \\ (x_1^\phi)^{p^h} &= x_1^{p^h} = 1. (c_2^\phi)^{p^{h+m}} = (x_1^{p^{h-m}} c_2)^{p^{h+m}} \\ &= (x_1^{p^{h-m}})^{p^{h+m}} c_2^{p^{h+m}} [c_2, x_1^{p^{h-m}}]^{\frac{p^{h+m}(p^{h+m}-1)}{2}} = 1 \text{ since } x_1^{p^{h-m}} \in Z_2(\hat{A}). \\ [c_2^\phi, x_1^\phi] &= [x_1^{p^{h-m}} c_2, x_1] = [c_2, x_1] \text{ and } (c_2^\phi)^{tp^m} \\ &= (x_1^{p^{h-m}} c_2)^{tp^m} = x_1^{tp^h} c_2^{tp^m} [c_2, x_1^{p^{h-m}}]^{\frac{tp^m(tp^m-1)}{2}} = c_2^{tp^m}. \end{aligned}$$

Thus $\phi|_{\hat{A}'} = 1|_{\hat{A}'}$. For $x_1^a c_2^b \in \hat{A}$, define $(x_1^a c_2^b)^\phi = (x_1^a)^\phi (c_2^b)^\phi$.

$$\begin{aligned} (x_1^a c_2^b x_1^c c_2^d)^\phi &= (x_1^{a+c} c_2^{b+d} [c_2^b, x_1^a])^\phi \\ &= (x_1^{a+c})^\phi (c_2^{b+d})^\phi [c_2^b, x_1^a] \text{ since } \phi|_{\hat{A}'} = 1|_{\hat{A}'}. \end{aligned}$$

$$\begin{aligned}
&= x_1^{a+c} (x_1^{p^{h-m}} c_2)^{(b+d)} [c_2^b, x_1^a] = x_1^{a+c+p^{h-m}(b+d)} c_2^{(b+c)} \\
&\quad [c_2^b, x_1^c] [c_2, x_1^{p^{h-m}}] \frac{(b+d)(b+d-1)}{2} . \\
&(x_1^a c_2^b)^\phi (x_1^c c_2^d)^\phi = x_1^a (c_1^{p^{h-m}} c_2)^b x_1^c (x_1^{p^{h-m}} c_2)^d \\
&= x_1^{a+bp^{h-m}} c_2^b [c_2, x_1^{p^{h-m}}] \frac{b(b-1)}{2} x_1^c x_1^{dp^{h-m}} c_2^d [c_2, x_1^{p^{h-m}}] \frac{d(d-1)}{2} \\
&= x_1^{a+c+bp^{h-m}} c_2^b [c_2^b, x_1^c] x_1^{dp^{h-m}} c_2^d [c_2, x_1^{p^{h-m}}] \frac{b(b-1)+d(d-1)}{2} \\
&= x_1^{a+c+(b+d)p^{h-m}} c_2^b [c_2^b, x_1^{dp^{h-m}}] c_2^d [c_2^b, x_1^c] [c_2, x_1^{p^{h-m}}] \frac{b(b-1)+d(d-1)}{2} \\
&= x_1^{a+c+(b+d)p^{h-m}} c_2^{b+d} [c_2^b, x_1^c] [c_2, x_1^{p^{h-m}}] \frac{b(b-1)+d(d-1)+2bd}{2} \\
&= x_1^{a+c+p^{h-m}(b+d)} c_2^{b+d} [c_2^b, x_1^c] [c_2, x_1^{p^{h-m}}] \frac{(b+d)(b+d-1)}{2} .
\end{aligned}$$

Thus $\phi \in A(\hat{A})$ and $\phi|_{\hat{A}} = 1|_{\hat{A}}$, so $\phi|_{\hat{A} \cap B} = 1|_{\hat{A} \cap B}$.

Define ϕ^* on G by: $x_1^{\phi^*} = x_1^\phi$, $c_2^{\phi^*} = c_2^\phi$, $d_i^{\phi^*} = d_i$.

Thus $\phi^*|_B = 1|_B$, and $\phi^*|_{\hat{A} \cap B} = \phi|_{\hat{A} \cap B} = 1|_{\hat{A} \cap B}$ since

$\hat{A} \cap B \leq Z(G) = Z(\hat{A})$. Hence $\phi^* \in A(G)$.

$$c_2^{(\phi^*)^k} = x_1^{kp^{h-m}} c_2 \text{ since if } k=1, c_2^{\phi^*} = c_2^\phi = x_1^{p^{h-m}} c_2.$$

Assume true for $k=n$. Then $c_2^{(\phi^*)^{n+1}} = (c_2^{(\phi^*)^n})^{\phi^*}$

$$= (x_1^{np^{h-m}} c_2)^{\phi^*} = x_1^{np^{h-m}} c_2^{\phi^*} = x_1^{(n+1)p^{h-m}} c_2. \text{ Using this formula,}$$

$$\text{we see } c_2^{(\phi^*)^{p^m-1}} = x_1^{p^{h-1}} c_2 \neq c_2, c_2^{(\phi^*)^{p^m}} = x_1^{p^h} c_2 = c_2,$$

$$x_1^{(\phi^*)^{p^m}} = x_1, d_i^{(\phi^*)^{p^m}} = d_i. \text{ Thus } p^m || |\phi^*| \text{ and } |\phi^*| \nmid p^{m-1},$$

hence $|\phi^*| = p^m$, $(\phi^*)^k \notin I(G)$ for $k=1, 2, \dots, p^m-1$, because if

$$(\phi^*)^k \in I(G), \text{ then } c_2^{(\phi^*)^k} = x_1^{kp^{h-m}} c_2 = y^{-1} c_2 y \text{ for some } y \in G.$$

Thus $x_1^{kp^{h-m}} = [c_2, y] \in G'$. But $\langle x_1 \rangle \cap G' = 1$, a contradiction.

$|\langle \phi^* \rangle I(G)| = p^m \frac{|G|}{|Z(G)|} = p^m \frac{|G|}{p^m} = |G|$, and we have $|G|$ divides $|\langle \phi^* \rangle I(G)|$, so $|G|$ divides $|A(G)|$.

Theorem II.4: If G is a p -group, $p \neq 2$, satisfying the conditions (W), $Z(G) = Z^* \otimes A$ where $Z^* = Z(G) \cap G'$, and $\exp A \geq \exp Z^*$, then $|G|$ divides $|A(G)|$.

Proof: By Lemma II.1 and Corollary II.1, we have

$G = \langle x_1, c_2, \dots, c_r \rangle$ where $\langle x_1^K \rangle = \langle \bar{x} \rangle$, $c_i \in C(G')$ and $G' = \langle [c_2, x_1] \rangle$. By Lemma II.5 and its proof, we know $|x_1| \geq p^h$ and $x_1^{p^{h-1}} \notin C_G(\langle c_2 \rangle)$, so $x_1^{p^{h-1}} \notin G'$.

Consider $\hat{K} = \langle x_1, c_2 \rangle$. $G' \leq \hat{K}$ so $\hat{K} \trianglelefteq G$. Let $\hat{K} \twoheadrightarrow \hat{K}/G'$. We wish to show \hat{K}/G' is a two-generated abelian group of type (p^a, p^b) where $a \geq h$, $b \geq m$.

Clearly \hat{K}/G' is abelian and at most two-generated. If \hat{K}/G' is cyclic, then $\hat{K}/G' = \langle x_1^\gamma \rangle$ or $\hat{K}/G' = \langle c_2^\gamma \rangle$. If $\hat{K}/G' = \langle x_1^\gamma \rangle$, then $c_2 = x_1^w g$ where $g \in G'$. But $G' \leq \phi(G)$, so $G = \langle x_1, c_3, \dots, c_r, G' \rangle = \langle x_1, c_3, \dots, c_r \rangle$, a contradiction to the assumption that a minimal generating set for G has r -elements. A similar argument shows $\hat{K}/G' \neq \langle c_2^\gamma \rangle$. Thus \hat{K}/G' is a two-generated abelian group.

If $|x_1^\gamma| \geq |c_2^\gamma|$, x_1^γ may be chosen as one generator of \hat{K}/G' , so $\hat{K}/G' = \langle x_1^\gamma \rangle \otimes \langle \bar{y} \rangle$. Now let $g \in \hat{K}$ be such that $g^\gamma = \langle \bar{y} \rangle$. Then $\hat{K}/G' = \langle x_1^\gamma \rangle \otimes \langle g^\gamma \rangle$. $c_2^\gamma \in \hat{K}/G'$, so $c_2^\gamma = (x_1^\gamma)^r (g^\gamma)^s$, or $c_2 = x_1^{r^s} g^s u$, where $u \in G'$. Since $G' = \langle [c_2, x_1] \rangle$, we have $G' = \langle [x_1^{r^s} g^s u, x_1] \rangle$. $[x_1^{r^s} g^s u, x_1] = [x_1^{r^s} g^s, x_1] [x_1^{r^s} g^s, x_1, u] [u, x_1] = [x_1^{r^s} g^s, x_1] [u, x_1]$. But $u \in G'$ implies $[u, x_1] \in G'^{(p)}$, thus $G' = \langle [x_1^{r^s} g^s, x_1] \rangle$.

$[x_1^r g^s, x_1] = [x_1^r, x_1][x_1^r, x_1, g^s][g^s, x_1] = [g^s, x_1]$. Thus $G' = \langle [g^s, x_1] \rangle \leq \langle [g, x_1]^s \rangle \leq \langle [g, x_1] \rangle = G'$ since $[g^s, x_1] = [g, x_1]^s w$ where w is a product of elements of the form $[g^k, x_1, g]$, and hence $w \in G'(p)$.

$G' = \langle [g, x_1] \rangle$ implies, by Lemma 3, $|g^Y| \geq p^m$. Thus if $|x_1^Y| \geq |c_2^Y|$, we have $\hat{K}/G' = \langle x_1^Y \rangle \otimes \langle g^Y \rangle$, and $|x_1^Y| \geq p^h$, $|g^Y| \geq p^m$. Hence \hat{K}/G' is of type (p^a, p^b) where $a \geq h$, $b \geq m$.

Now suppose $\hat{K}/G' = \langle c_2^Y \rangle \otimes \langle \bar{y} \rangle$. $|c_2^Y| \geq p^m$ since in Lemma 4, we have shown $[c_2, x_1]z = c_2^{tp^m}$ where $z \in Z(G)$, and hence $|c_2^Y| \geq p^m$. We wish to show $|\bar{y}| \geq p^h$.

$$|\bar{y}| = \left| \frac{\langle c_2^Y \rangle \otimes \langle \bar{y} \rangle}{\langle c_2^Y \rangle} \right| = \left| \frac{\hat{K}/G'}{\langle c_2^Y \rangle} \right| = \left| \frac{\hat{K}/G'}{\langle c_2, G' \rangle / G'} \right|.$$

It is sufficient to show that if $x_1^u \in \langle c_2, G' \rangle$, then $p^h | u$, since in $\langle x_1, c_2 \rangle \xrightarrow{Y} \langle c_2^Y \rangle \otimes \langle \bar{y} \rangle \xrightarrow{J} \langle \bar{y} \rangle$, we have $(x_1^u)^{YJ} = ((x_1^Y)^u)^J = (x_1^{YJ})^u = \bar{1}$ if, and only if, $x_1^u \in \langle c_2, G' \rangle$.

If $x_1^u \in \langle c_2, G' \rangle$, then for some k, n we have $x_1^u = c_2^k [c_2, x_1]^n$. $G' \leq C_G(\langle c_2 \rangle)$ implies $x_1^u \in C_G(\langle c_2 \rangle)$. But $x_1^{p^{h-1}} \notin C_G(\langle c_2 \rangle)$, thus $x_1^u \in C_G(\langle c_2 \rangle)$ implies $p^h | u$.

In either case, we have \hat{K}/G' is a two-generated abelian group of type (p^a, p^b) where $a \geq h$, $b \geq m$. Now suppose

$$\exp A \geq \exp Z^* \text{ and } Z(G) = Z^* \otimes A. \quad |I(G)| = \frac{|G|}{|Z(G)|},$$

$$|A_c(G)| = |\text{Hom}(G/G', A)| |\text{Hom}(G/G', Z^*)|. \quad |A_c(G) \cap I(G)| \leq$$

$$|\text{Hom}(G/G', Z^*)| \text{ since if } \alpha \in A_c(G) \cap I(G), x^{-1}x^\alpha \in Z(G) \text{ for}$$

all $x \in G$, and since $\alpha = \pi_y$, $x^{-1}x^\alpha = x^{-1}x^{\pi_y} \in G'$ for all $x \in G$,

thus $x^{-1}x^\alpha \in Z(G) \cap G' = Z^*$. Thus α induces a homomorphism

from G/G' into Z^* , and hence $|A_c(G) \cap I(G)| \leq |\text{Hom}(G/G', Z^*)|$.

$$|A_c(G)I(G)| = \frac{|\text{Hom}(G/G', A)| |\text{Hom}(G/G', Z^*)| \left| \frac{G}{Z(G)} \right|}{|A_c(G) \cap I(G)|} \geq$$

$$\left| \frac{G}{Z(G)} \right| |\text{Hom}(G/G', A)| = |G| |\text{Hom}(G/G', A)| / |Z^*| |A|.$$

Let $a \in A$ be such that $|a| = \exp A$. Let $G \xrightarrow{\zeta} G/G'$. Then $|a^\zeta| = |a|$ since if $(a^\zeta)^k = \bar{1}$, then $(a^k)^\zeta = \bar{1}$, or $a^k \in G' \cap Z(G) = Z^*$. Thus $a^k \in Z^* \cap A = \langle 1 \rangle$ and $|a^\zeta| = |a|$. Thus there exists $\bar{y} \in G/G'$ with the property \bar{y} is in a minimal generating set for G/G' and $|\bar{y}| \geq \exp A$.

Since \hat{K}/G' is a subgroup of G/G' of type (p^a, p^b) , where $a \geq h$, $b \geq m$, by Theorem 5.5.7 of [8], we know G/G' is at least two-generated, say by the above \bar{y} and \bar{g} , and is such that $|\bar{y}| \geq \exp A$, $|\bar{g}| \geq p^m$. Thus $|\text{Hom}(G/G', A)| \geq |A| p^m = |A| |Z^*|$. Hence we have $|G|$ divides $|A_c(G)I(G)|$, so $|G|$ divides $|A(G)|$.

Theorem II.5: If G is a p -group satisfying the conditions (W), $Z(G) = Z^* \otimes A$ where $Z^* = Z(G) \cap G'$ and $h \geq 2m$, then $|G|$ divides $|A(G)|$.

Proof: If $\exp A \geq \exp Z^*$, we have G satisfies the hypothesis of Theorem 4, thus $|G|$ divides $|A(G)|$. Thus we assume $\exp A \neq \exp Z^*$. Then we have $\exp Z = p^m$.

By Lemma II.1 and Corollary II.1, we may assume

$G = \langle x_1, c_2, c_3, \dots, c_r \rangle$ where $\langle x_1^K \rangle = \langle \bar{x} \rangle$, $c_i \in C(G')$ for $i = 2, \dots, r$ and $G' = \langle [c_2, x_1] \rangle$. By Lemma II.4, we have $|c_2| = p^{h+m}$ and $\langle c_2^{p^{2m-1}} \rangle = \langle [c_2, x_1]^{p^{m-1}} \rangle$. By Lemma II.5, $|x_1| \geq p^h$ and $\langle x_1 \rangle \cap G' = \langle 1 \rangle$.

Now, since $h \geq 2m$, we have $h-m \geq m \geq m-1$, thus $\langle [c_2, x_1]^{p^{m-1}} \rangle \neq \langle [c_2, x_1]^{p^m} \rangle = Z^*$. Hence we know that $\langle c_2 \rangle \geq \langle c_2^{p^{2m-1}} \rangle \neq Z^*$.

By Lemma II.2, $[c_i, c_j] \in Z(G) \cap G'$, thus if $[x_1, c_i] \in Z(G)$, $c_i \in Z_2(G)$. If $c_i \notin Z_2(G)$, we replace c_i , for $i = 3, \dots, r$, by d_i , where $d_i \in Z_2(G)$ to obtain a new minimal generating set for G of the form $\{x_1, c_2, d_3, \dots, d_r\}$ where $\langle x_1^K \rangle = \langle \bar{x} \rangle$, $c_2 \in C(G')$, $d_i \in Z_2(G)$, $i = 3, \dots, r$ and $G' = \langle [c_2, x_1] \rangle$. To obtain d_i , we proceed as follows:

Since $[x_1, c_i] \notin Z(G) \cap G'$, we have

$$[x_1, c_i] x_1 [x_1, c_i]^{-1} = x_1 x_1^{-1} [x_1, c_i] x_1 [x_1, c_i]^{-1} = x_1 x_1^{-1} [c_2, x_1]^k x_1 [x_1, c_i]^{-1}$$

where $[x_1, c_i] = [c_2, x_1]^k = x_1 [c_2, x_1]^{k(1+tp^m)} [x_1, c_i]^{-1} = x_1 [x_1, c_i]^{tp^m}$.

$$[x_1, c_i] c_j [x_1, c_i]^{-1} = c_j \quad \text{for } j = 2, \dots, r \text{ since } c_j \in C(G').$$

$$(c_i^{tp^m})^{-1} x_1 c_i^{tp^m} = x_1 [x_1, c_i]^{tp^m} = x_1 [x_1, c_i]^{tp^m} \quad \text{since } c_i \in C(G).$$

$$(c_i^{tp^m})^{-1} c_j c_i^{tp^m} = c_j [c_j, c_i]^{tp^m} = c_j [c_j, c_i]^{tp^m} = c_j \quad \text{since}$$

$$[c_j, c_i] \in Z^* \quad \text{and} \quad \exp Z^* = p^m. \quad \text{Thus we have } \pi_{[x_1, c_i]^{-1}} = \pi_{c_i^{tp^m}},$$

$$\text{or } [x_1, c_i]^{-1} z = [c_i, x_1] z = c_i^{tp^m}, \quad \text{where } z \in Z(G). \quad \text{Since}$$

$$[x_1, c_i] \notin Z(G), \quad c_i^{tp^m} \notin Z(G).$$

Let $H_i = \langle c_2, c_i, Z(G) \rangle$ and consider $H_i \xrightarrow{J} H_i / Z(G)$. Since $H_i' = \langle [c_2, c_i] \rangle$, $H_i' \leq Z(G)$ and $H_i / Z(G)$ is abelian. $c_2^J \neq \bar{1}$ since $c_2^J = \bar{1}$ implies $c_2 \in Z(G)$, thus $c_2^{p^{2m-1}} \in Z(G)$, thus $\langle [c_2, x_1]^{p^{m-1}} \rangle \leq Z(G)$, a contradiction. $c_i^J \neq \bar{1}$ since $c_i^J = \bar{1}$ implies $c_i^{tp^m} \in Z(G)$ which is impossible.

If $H_i / Z(G)$ is cyclic, then either $H_i / Z(G) = \langle c_2^J \rangle$ or $H_i / Z(G) = \langle c_i^J \rangle$. If $H_i / Z(G) = \langle c_2^J \rangle$, then $c_i = c_2^a z_i$, where $z_i \in Z(G)$. $G \neq \langle x_1, c_2, \dots, c_{i-1}, c_{i+1}, \dots, c_r \rangle$, but $c_i = c_2^a z_i = \langle x_1, c_2, \dots, c_{i-1}, z_i, c_{i+1}, \dots, c_r \rangle = G$. Thus replace c_i by z_i . Since $z_i \in Z(G)$, $z_i \in Z_2(G)$. If $H_i / Z(G) = \langle c_i^J \rangle$, then $c_2 = c_i^b z$ where $z \in Z(G)$. If $(b, p) = 1$, then $c_i = c_2^e z_i$ where

$z_i \in Z(G)$ and $H_i/Z(G) = \langle c_2^J \rangle$. Thus we are in the above case.

If $p|b$, then since $G' = \langle [c_2, x_1] \rangle$, we have $G' = \langle [c_i^b z, x_1] \rangle$.

But $[c_i^b z, x_1] = [c_i, x_1]^b \in G'^{(p)}$ since $p|b$. But this is

impossible, thus we must have $(p, b) = 1$. Thus if $H_i/Z(G)$ is cyclic, we can replace c_i by d_i , where $d_i \in Z_2(G)$, in a minimal generating set for G which contains x_1 and c_2 .

If $H_i/Z(G)$ is two-generated, then since $|c_2^J| = p^m$ and $|c_i^J| \leq p^m$, we may assume that $H_i/Z(G) = \langle c_2^J \rangle \otimes \langle \bar{b} \rangle$. Let $g_i \in H_i$ be such that $g_i^J = \bar{b}$. Then $H_i/Z(G) = \langle c_2^J \rangle \otimes \langle g_i^J \rangle$, and $\langle c_2 \rangle \cap \langle g_i \rangle \leq Z(G)$. Since $g_i \in H_i = \langle c_2, c_i, Z(G) \rangle$, we have $g_i \in C(G')$. Let $c_i^J = (c_2^J)^k (g_i^J)^b$. Then $c_i = c_2^k g_i^b z$, where $z \in Z(G)$. Set $d_i = g_i^b z$, so $c_i = c_2^k d_i$. We note $d_i^J = (g_i^J)^b$, so $\langle d_i \rangle \cap \langle c_2 \rangle \leq Z(G)$. $G \neq \langle x_1, c_2, \dots, c_{i-1}, c_{i+1}, \dots, c_r \rangle$, but $c_i = c_2^k d_i \in \langle x_1, c_2, \dots, c_{i-1}, d_i, c_{i+1}, \dots, c_r \rangle = G$. Thus d_i is in a minimal generating set for G which contains x_1 and c_2 .

Since $d_i = (c_2^k)^{-1} c_i$, we have $[c_j, d_i] \in Z(G) \cap G'$ for $j = 2, \dots, r$. If $[x_1, d_i] \in Z(G) \cap G'$, then $d_i \in Z_2(G)$. Thus suppose $[x_1, d_i] \notin Z(G) \cap G'$, then $[c_2, x_1]^{p^{m-1}} \in \langle [x_1, d_i] \rangle$. Also

$$\begin{aligned} [x_1, d_i] x_1 [x_1, d_i]^{-1} &= x_1 x_1^{-1} [x_1, d_i] x_1 [x_1, d_i]^{-1} \\ &= x_1 x_1^{-1} [c_2, x_1]^k x_1 [x_1, d_i]^{-1} \text{ where } [c_2, x_1]^k = [x_1, d_i], \\ &= x_1 [c_2, x_1]^{k(1+tp^m)} [x_1, d_i]^{-1} = x_1 [x_1, d_i]^{1+tp^m} x_1 [x_1, d_i]^{-1} = x_1 [x_1, d_i]^{tp^m}. \\ [x_1, d_i] c_j [x_1, d_i]^{-1} &= c_j \text{ for } j = 2, \dots, r. (d_i^{tp^m})^{-1} x_1 d_i^{tp^m} = \\ x_1 [x_1, d_i]^{tp^m} &= x_1 [x_1, d_i]^{tp^m} \text{ since } d_i \in C(G'). (d_i^{tp^m})^{-1} c_j d_i^{tp^m} = \\ c_j [c_j, d_i]^{tp^m} &= c_j [c_j, d_i]^{tp^m} = c_j \text{ since } [c_j, d_i] \in Z^* \text{ and } \exp Z^* = p^m. \end{aligned}$$

Thus $\pi_{[x_1, d_i]^{-1}} = \pi_{d_i^{tp^m}}$, so $[x_1, d_i]^{-1} z = d_i^{tp^m}$ where $z \in Z(G)$. Thus $[d_i, x_1] z = d_i^{tp^m}$, and $[d_i, x_1]^J = (d_i^{tp^m})^J$. Since

$[c_2, x_1]^p \in \langle [x_1, d_i] \rangle = \langle [d_i, x_1] \rangle$ and $Z^* \not\leq \langle [c_2, x_1]^{p^{m-1}} \rangle$, we now have $\bar{1} \neq ([c_2, x_1]^{p^{m-1}})^J \in \langle c_2^J \rangle \cap \langle d_i^J \rangle = \bar{1}$. But this is impossible, thus we must have $[x_1, d_i] \in Z(G) \cap G'$. We now replace c_i by d_i so we may assume $G = \langle x_1, c_2, d_3, \dots, d_r \rangle$ where $\langle x_1^K \rangle = \langle \bar{x} \rangle$, $|x_1| \geq p^h$, $G' = \langle [c_2, x_1] \rangle$, $\langle x_1 \rangle \cap G' = \langle 1 \rangle$, $c_2 \in C(G')$ and $d_i \in Z_2(G)$ for $i = 3, \dots, r$.

Set $\tilde{A} = \langle x_1, c_2 \rangle$, $B = \langle d_3, \dots, d_r \rangle$. Then $\tilde{A} \trianglelefteq G$ since $G' \leq \tilde{A}$ and we have $G = \tilde{A}B$, $\tilde{A} \cap B \leq \tilde{A} \cap Z_2(G)$.

Let $\tilde{A} \cong \tilde{A}/G'$. Since $\langle c_2^{p^{2m-1}} \rangle \leq G'$, we have $(c_2^{p^{2m-1}})^p = \bar{1}$, so $|c_2^p| \leq p^{2m-1}$. Since $\langle x_1 \rangle \cap G' = \langle 1 \rangle$, $|x_1^p| = |x_1| = p^{h+s}$ where $0 \leq s \leq m$. $h \geq 2m$ implies $|x_1^p| \geq |c_2^p|$, thus x_1^p is an element of \tilde{A}/G' of highest order, so we may assume

$\tilde{A}/G' = \langle x_1^p \rangle \otimes \langle \bar{b} \rangle$. Let $g \in \tilde{A}$ be such that $g^p = \bar{b}$. Then $\tilde{A}/G' = \langle x_1^p \rangle \otimes \langle g^p \rangle$.

$c_2^p = (x_1^p)^a (g^p)^b$ so $c_2 = x_1^a g^b w$, where $w \in G'$. Since $G' = \langle [c_2, x_1] \rangle$, we have $G' = \langle [x_1^a g^b w, x_1] \rangle$.

$$\begin{aligned} [x_1^a g^b w, x_1] &= [x_1^a g^b, x_1] [x_1^a g^b, x_1, w] [w, x_1] \\ &= [x_1^a, x_1] [x_1^a, x_1, g^b] [g^b, x_1] [x_1^a g^b, x_1, w] [w, x_1] = [g^b, x_1] [w, x_1]. \end{aligned}$$

$w \in G'$ implies $[w, x_1] \in G'^{(p)}$, thus $G' = \langle [g^b, x_1] \rangle \leq \langle [g, x_1] \rangle$ since $[g^b, x_1] = [g, x_1]^b u$ where u is a product of elements of the form $[g^k, x_1, g]$ which are in $G'^{(p)}$. By Lemma II.3, we have $|g^p| \geq p^m$. Thus \tilde{A}/G' is abelian of type (p^a, p^b) where $a \geq h$, $b \geq m$. Thus by 5.5.7 of [8], we have G/G' contains a subgroup of type (p^a, p^b) where $a \geq h$, $b \geq m$.

We may assume that $c_2^p = (x_1^p)^a (g^p)^b$, or that $c_2 = x_1^a g^b w$, where $w \in G'$. Now define ϕ on x_1, g by $x_1^\phi = x_1$, $g^\phi = x_1^{p^{h+s-m}} g$.

Then, since $G' = \langle [g, x_1] \rangle$, we have $[g^\phi, x_1^\phi] = [x_1^{p^{h+s-m}}, g, x_1] = (x_1^{p^{h+s-m}} g)^{-1} x_1^{-1} x_1^{p^{h+s-m}} g x_1 = g^{-1} x_1^{-1} g x_1 = [g, x_1]$, so $\phi|_{G'} = 1|_{G'}$. Also, $(g^\phi)^{p^m} = (x_1^{p^{h+s-m}} g)^{p^m} = x_1^{p^{h+s-m}} g^{p^m} [g, x_1^{p^{h+s-m}}]^{p^m} = \frac{(p^m-1)}{2} = g^{p^m}$ since $x_1^{p^{h+s-m}} \in Z_2(G)$ and $\exp Z^* = p^m$.

If $y \in \tilde{A}$, y can be written in the form $y = x_1^a g^b u$ where $u \in G'$. Define ϕ on \tilde{A} by $y^\phi = (x_1^a)^\phi (g^b)^\phi u$. ϕ is well-defined, for if $x_1^{a(1)} g^{b(1)} u_1 = x_1^{a(2)} g^{b(2)} u_2$, where $u_i \in G'$ for $i = 1, 2$, then $x_1^{a(1)-a(2)} = g^{b(2)} u_2 u_1^{-1} (g^{b(1)})^{-1}$. Thus $(x_1^{a(1)-a(2)})^\rho = (g^{b(2)-b(1)})^\rho = \bar{1}$ since $\tilde{A}/G' = \langle x_1^\rho \rangle \otimes \langle g^\rho \rangle$. Hence $x_1^{a(1)-a(2)} \in G'$, but $\langle x_1 \rangle \cap G' = \langle 1 \rangle$, so we have $x_1^{a(1)} = x_2^{a(2)}$. Thus $g^{b(1)} u_1 = g^{b(2)} u_2$. But then we have $g^{b(1)-b(2)} = u_2 u_1^{-1}$, so $(g^{b(1)-b(2)})^\rho = \bar{1}$. $|g^\rho| \geq p^m$ implies $p^m | (b(1)-b(2))$. But $(g^{p^m})^\phi = g^{p^m}$, so $(g^{b(1)-b(2)})^\phi = g^{b(1)-b(2)} = u_2 u_1^{-1}$, or $(g^{b(1)})^\phi ((g^{b(2)})^\phi)^{-1} = u_2 u_1^{-1}$ which implies $(g^{b(1)})^\phi u_1 = (g^{b(2)})^\phi u_2$. Thus ϕ is well-defined.

For $g_1, g_2 \in G'$, we have:

$$\begin{aligned}
 (x_1^a g^b g_1 x_1^c g^d g_2)^\phi &= (x_1^a g^b x_1^c g_1 [g_1, x_1^c] g^d g_2)^\phi \\
 &= (x_1^{a+c} g^b [g^b, x_1^c] g_1 g^d [g_1, x_1^c] [g_1, x_1^c, g^d] g_2)^\phi \\
 &= (x_1^{a+c} g^b [g^b, x_1^c] g^d g_1 [g_1, g^d] [g_1, x_1^c] [g_1, x_1^c, g^d] g_2)^\phi \\
 &= (x_1^{a+c} g^{b+d} [g^b, x_1^c] [g^b, x_1^c, g^d] g_1 [g_1, g^d] [g_1, x_1^c] [g_1, x_1^c, g^d] g_2)^\phi \\
 &= x_1^{a+c} (x_1^{p^{h+s-m}} g)^{b+d} w \text{ where} \\
 w &= [g^b, x_1^c] [g^b, x_1^c, g^d] g_1 [g_1, g^d] [g_1, x_1^c] [g_1, x_1^c, g^d] g_2, \\
 &= x_1^{a+c+(b+d)p^{h+s-m}} g^{b+d} [g, x_1^{p^{h+s-m}}]^{\frac{(b+d)(b+d-1)}{2}} w.
 \end{aligned}$$

$$\begin{aligned}
(x_1^a g^b g_1)^p (x_1^c g^d g_2)^p &= x_1^a (x_1^p)^{h+s-m} g^b g_1 x_1^c (x_1^p)^{h+s-m} g^d g_2 \\
&= x_1^{a+bp^{h+s-m}} g^b [g, x_1^p]^{p^{h+s-m} \frac{b(b-1)}{2}} g_1 x_1^c x_1^{dp^{h+s-m}} g^d [g, x_1^p]^{p^{h+s-m} \frac{d(d-1)}{2}} g_2 \\
&= x_1^{a+bp^{h+s-m}} g^b g_1 x_1^c x_1^{dp^{h+s-m}} g^d g_2 [g, x_1^p]^{p^{h+s-m} \frac{b(b-1)+d(d-1)}{2}} \\
&\quad \text{since } x_1^p \in Z_2(G) \\
&= x_1^{a+bp^{h+s-m}} g^b x_1^c g_1 [g_1, x_1^c] x_1^{dp^{h+s-m}} g^d g_2 [g, x_1^p]^{p^{h+s-m} \frac{b(b-1)+d(d-1)}{2}} \\
&= x_1^{a+c+bp^{h+s-m}} g^b [g^b, x_1^c] x_1^{dp^{h+s-m}} g_1 [g_1, x_1^c] g^d g_2 [g_1 x_1^p]^{p^{h+s-m} \frac{b(b-1)+d(d-1)}{2}} \\
&= x_1^{a+c+bp^{h+s-m}} g^b x_1^{dp^{h+s-m}} [g^b, x_1^c] g_1 g^d [g_1, x_1^c] [g_1, x_1^c, g^d] g_2 \\
&\quad [g, x_1^p]^{p^{h+s-m} \frac{b(b-1)+d(d-1)}{2}} \\
&= x_1^{a+c+(b+d)p^{h+s-m}} g^b [g^b, x_1^{dp^{h+s-m}}] [g^b, x_1^c] g^d g_1 [g_1, g^d] \\
&\quad [g_1, x_1^c] [g_1, x_1^c, g^d] g_2 [g, x_1^p]^{p^{h+s-m} \frac{b(b-1)+d(d-1)}{2}} \\
&= x_1^{a+c+(b+d)p^{h+s-m}} g^b [g^b, x_1^c] g^d g_1 [g_1, g^d] [g_1, x_1^c] [g_1, x_1^c, g^d] g_2 \\
&\quad [g, x_1^p]^{p^{h+s-m} \frac{b(b-1)+d(d-1)}{2}} [g^b, x_1^{dp^{h+s-m}}] \\
&= x_1^{a+c+(b+d)p^{h+s-m}} g^{b+d} [g^b, x_1^c] [g^b, x_1^c, g^d] g_1 [g_1, g^d] \\
&\quad [g_1, x_1^c] [g_1, x_1^c, g^d] g_2 [g, x_1^p]^{p^{h+s-m} \frac{(b+d)(b+d-1)}{2}} \\
&= x_1^{a+c+(b+d)p^{h+s-m}} g^{b+d} [g, x_1^p]^{p^{h+s-m} \frac{(b+d)(b+d-1)}{2}} .
\end{aligned}$$

Thus $\phi \in A(\tilde{A})$.

$g^{\phi^k} = x_1^{kp^{h+s-m}} g$ for $k \geq 1$. The formula is true for $k = 1$. Thus assume it is true for $k = n$. Then $g^{\phi^{n+1}} = (g^{\phi^n})^{\phi} =$

$$(x_1^{np^{h+s-m}} g)^{\phi} = x_1^{np^{h+s-m}} x_1^{p^{h+s-m}} g = x_1^{(n+1)p^{h+s-m}} g.$$

Since $x_1^{\phi^{p^m}} = x_1$ and $g^{\phi^{p^m}} = x_1^{p^m p^{h+s-m}} g = g$, we have $|\phi| \mid p^m$. $g^{\phi^{p^{m-1}}} = x_1^{p^{h+s-1}} g \neq g$, so $|\phi| > p^{m-1}$ and we have $|\phi| = p^m$.

Because $c_2 = x_1^a g w$ where $w \in G'$, we have $c_2^{\phi} = x_1^a x_1^{p^{h+s-m}} g w = x_1^{p^{h+s-m}} c_2$. $(c_2^{p^m})^{\phi} = (c_2^{\phi})^{p^m} = (x_1^{p^{h+s-m}} c_2)^{p^m} = x_1^{p^{h+s}} c_2^{p^m} [c_2, x_1^{p^{h+s-m}}]^{p^m} = c_2^{p^m}$. Thus we have $\phi|_{\langle c_2^{p^m} \rangle} =$

$$1|_{\langle c_2^{p^m} \rangle}, \phi|_{\langle x_1 \rangle} = 1|_{\langle x_1 \rangle} \text{ and } \phi|_{G'} = 1|_{G'}. \text{ Thus}$$

$$\phi|_{\langle x_1, c_2^{p^m}, G' \rangle} = 1|_{\langle x_1, c_2^{p^m}, G' \rangle}.$$

Let $y \in \tilde{A} \cap B$, then $y \in Z_2(G)$. Suppose $y = x_1^r c_2^s g_1$, where $g_1 \in G'$. $[x_1, y] \in Z(G)$, so $[x_1, y] = [x_1, x_1^r c_2^s g_1] = x_1^{-1} g_1^{-1} (c_2^s)^{-1} (x_1^r)^{-1} x_1 x_1^r c_2^s g_1 = x_1^{-1} (c_2^s g_1)^{-1} x_1 c_2^s g_1 = [x_1, c_2^s g_1] \in Z(G)$. Moreover, since $[c_2, c_2^s g_1] \in Z(G)$ and $[d_i, c_2^s g_1] \in Z(G)$, we have $c_2^s g_1 \in Z_2(G)$. Thus

$x_1^r c_2^s g_1 (c_2^s g_1)^{-1} = x_1^r \in Z_2(G)$. But $x_1^r \in Z_2(G)$ if, and only if, $p^{h-m} \mid r$ using Remark F, the fact $|Z(G) \cap G'| = p^m$ and that

$d_i \in Z_2(G)$. Also, since $[c_2, x_1] = c_2^{tp^m} z$ where $z \in Z(G)$, we have $g_1 = c_2^{kp^m} z_1$, where $z_1 \in Z(G)$. Since $c_2^s g_1 \in Z_2(G)$,

$c_2^{s+kp^m} z_1 \in Z_2(G)$, or $c_2^{s+kp^m} \in Z_2(G)$. But $c_2^b \in Z_2(G)$ if, and only if, $[c_2^b, x_1] \in Z(G)$, or equivalently, $[c_2, x_1]^b \in Z(G)$. But $[c_2, x_1]^b \in Z(G)$, if, and only if, $p^{h-m} \mid b$. Thus $p^{h-m} \mid (s+kp^m)$, so

$np^{h-m} = s + kp^m$, or $np^{h-m} - kp^m = s$. But $h \geq 2m$ implies $h-m \geq m$, so $np^{h-m} - kp^m = p^m(np^{h-2m} - k) = s$, or $p^m | s$.

Thus we have $Z_2(G) \cap \tilde{A} \leq \langle x_1^{p^{h-m}}, c_2^{p^m}, G' \rangle = D$. But $D \leq \langle x_1, c_2^{p^m}, G' \rangle$, so we have $\phi_D = 1|_D$ and hence $\phi|_{\tilde{A} \cap B} = 1|_{\tilde{A} \cap B}$.

In [2], Demana has proven the following theorem:

Theorem 1.2: Let $G = AB$ where $A \trianglelefteq G$. Let $\alpha \in A(A)$, $\beta \in A(B)$. A necessary and sufficient condition that there exists $\gamma \in A(G)$ such that $\gamma|_A = \alpha$ and $\gamma|_B = \beta$ is:

$$1). \quad \alpha|_{A \cap B} = \beta|_{A \cap B},$$

$$2). \quad \pi_b \alpha = \alpha \pi_b \beta \text{ on } A \text{ where } b \in B.$$

Defining ϕ^* in G by $\phi^*|_{\tilde{A}} = \phi|_{\tilde{A}}$ and $d_i^{\phi^*} = d_i$, we have $\phi^* \in A(G)$ since:

$$1). \quad \phi^*|_{\tilde{A} \cap B} = \phi|_{\tilde{A} \cap B} = 1|_{\tilde{A} \cap B} = \phi^*|_B,$$

2). $\pi_b \phi = \phi \pi_b$ on \tilde{A} where $b \in B$. This is because, for $b \in B$, $b \in Z_2(G)$, $a^{\pi_b \phi} = (b^{-1}ab)^{\phi} = (a[a, b])^{\phi} = a^{\phi}[a, b]$, and $a^{\phi \pi_b} = b^{-1}a^{\phi}b = a^{\phi}[a^{\phi}, b]$. Let $a = x_1^v g^u g_1$, where $g_1 \in G'$. Then $a^{\phi} = x_1^v (x_1^{p^{h+s-m}} g)^u g_1 = x_1^v x_1^{up^{h+s-m}} g^u [g, x_1^{p^{h+s-m} \frac{u(u-1)}{2}}] g_1$
 $= x_1^{up^{h+s-m}} [g, x_1^{p^{h+s-m} \frac{u(u-1)}{2}}] x_1^v g^u g_1 = x_1^{up^{h+s-m}} [g, x_1^{p^{h+s-m} \frac{u(u-1)}{2}}] a.$
Thus $[a^{\phi}, b] = [x_1^{up^{h+s-m}} [g, x_1^{p^{h+s-m} \frac{u(u-1)}{2}}] a, b]$
 $= [x_1^{up^{h+s-m}} [g, x_1^{p^{h+s-m} \frac{u(u-1)}{2}}], b] [x_1^{up^{h+s-m}} [g, x_1^{p^{h+s-m} \frac{u(u-1)}{2}}], b, a] [a, b]$
 $= [a, b] \text{ since } b \in Z_2(G), [g, x_1^{p^{h+s-m}}] \in Z(G) \text{ and } h+s-m \geq m.$
Since $|\phi| = p^m$, we have $|\phi^*| = p^m$.

Now consider $|A_c(G)I(G)|$. $|I(G)| = |G|/|Z(G)|$,
 $|A_c(G)| = |\text{Hom}(G/G', Z^*)| |\text{Hom}(G/G', A)|$, and $|A_c(G) \cap I(G)| \leq$
 $|\text{Hom}(G/G', Z^*)|$. Thus

$$|A_c(G)I(G)| = \frac{|I(G)||A_c(G)|}{|A_c(G) \cap I(G)|} \geq \frac{|G|}{|Z|} \frac{|\text{Hom}(G/G', A)| |\text{Hom}(G/G', Z^*)|}{|\text{Hom}(G/G', Z^*)|} =$$

$$\frac{|G| |\text{Hom}(G/G', A)|}{|Z^*| |A|}.$$

Since \tilde{A}/G' is a subgroup of G/G' of type (p^a, p^b) where $a \geq h$, $b \geq m$, we have $|\text{Hom}(G/G', A)| \geq |A|^2$.
 Thus $|A_c(G)I(G)| \geq \frac{|G||A|^2}{|Z^*||A|} = \frac{|G||A|}{|Z^*|} = \frac{|G||A|}{p^m}$.

Since $|\langle \alpha_1 \rangle \cap Z(G)| = p^s$ and $\langle \alpha_1 \rangle \cap G' = \langle 1 \rangle$, we have $|A| \geq p^s$. Thus $|A_c(G)I(G)| \geq |G|/p^{m-s}$.

Now consider $|A_c(G)I(G) \langle \phi^* \rangle|$. We claim $(\phi^*)^k \notin A_c(G)I(G)$ for $k = 1, 2, \dots, p^{m-s} - 1$. For suppose $(\phi^*)^k \in A_c(G)I(G)$. Then $(\phi^*)^k = \alpha \pi_y$ where $\alpha \in A_c(G)$ and $y \in G$. $g(\phi^*)^k = g(\alpha)^k = x_1^{kp^{h+s-m}} g = g^{\alpha \pi_y} = (g g_\alpha)^\pi y = y^{-1} g y g_\alpha$ where $g_\alpha \in Z(G)$. Then we have $x_1^{kp^{h+s-m}} = [y, g^{-1}] g_\alpha$, or $x_1^{kp^{h+s-m}} g_\alpha^{-1} = [y, g^{-1}]$.
 $(x_1^{kp^{h+s-m}} g_\alpha^{-1})^{p^m} = x_1^{kp^{h+s-m}} (g_\alpha^{p^m})^{-1} = 1$ since $|x_1| = p^{h+s}$ and $\exp Z(G) = p^m$. Thus $[y, g^{-1}]^{p^m} = 1$, or $[y, g^{-1}] \in Z(G) \cap G'$.
 Thus $[y, g^{-1}] g_\alpha \in Z(G)$ and we have $x_1^{kp^{h+s-m}} \in Z(G)$. $x_1^{p^{h-1}} \notin Z(G)$ so we have $p^h | kp^{h+s-m}$, or $p^{m-s} | k$. But for $k = 1, 2, \dots, p^{m-s} - 1$, p^{m-s} does not divide k .

Thus $|I(G)A_c(G) \langle \phi^* \rangle| \geq p^{m-s} |I(G)A_c(G)| = p^{m-s} |G|/p^{m-s} = |G|$ and we have $|G|$ divides $|A(G)|$.

CHAPTER III

Some Necessary Conditions for $A_c(G) \leq I(G)$

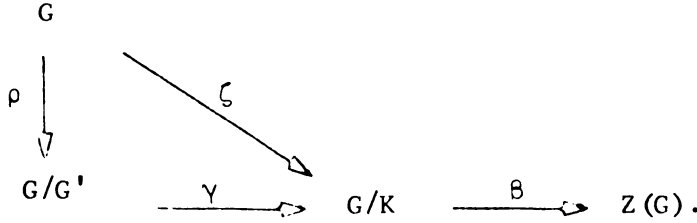
We shall now assume that G is a p -group, $p \neq 2$, having no abelian direct factors. For such a group G , there are two p -subgroups of $A(G)$ which are of interest, namely $A_c(G)$ and $I(G)$. They are of interest because we know their sizes and, in a certain sense, how one obtains the automorphisms in them. A question arises as to what, if any, are necessary and/or sufficient conditions that $A_c(G) \leq I(G)$.

As was mentioned in the introduction, Sanders has shown that all the central automorphisms of a nilpotence class two group G are inner automorphisms if, and only if, $G' = Z(G)$ is cyclic. We shall give a different proof than Sanders gave of this fact at the end of this chapter. Also, Theorem II.2 of Chapter II gives us one sufficiency condition for $A_c(G) \leq I(G)$, that being G is a p -group, $p \neq 2$ with $Z(G) \leq G'$ and G' is cyclic.

The assumption that $A_c(G) \leq I(G)$ should somehow place a restriction on what the lattice of subgroups for G can look like. We shall prove that if $A_c(G) \leq I(G)$, then $Z(G) \leq G'$. Furthermore, if $Z(G)$ is not cyclic, we shall show that $Z_2(G) \leq \phi(G)$. It is our conjecture that if $A_c(G) \leq I(G)$ for a finite p -group G , $p \neq 2$, then not only must $Z(G) \leq G'$, but $Z(G)$ must be cyclic.

Lemma III.1: Let G be a p -group with no abelian direct factors. Let $K \trianglelefteq G$ with $G' \leq K$ and let $G \xrightarrow{\zeta} G/K$. If $\beta \in \text{Hom}(G/K, Z(G))$, then for α defined by $g^\alpha = g g^{\zeta\beta}$, $\alpha \in A_c(G)$.

Proof: Since $G/K \cong G/G'/K/G'$, there exists $\gamma: G/G' \rightarrow G/K$ such that $g^{p\gamma} = g^\zeta$.



Then $g^\alpha = g g^{\zeta\beta} = g g^{p\gamma\beta} = g g^{p(\gamma\beta)}$. $\gamma\beta \in \text{Hom}(G/G', Z(G))$, thus by the proof of Theorem 1 of [1], $\alpha \in A_c(G)$.

Remark: A necessary condition for a p -group G , $p \neq 2$, with no abelian direct factor to have $A_c(G) \leq I(G)$ is that $Z(G) \leq \phi(G)$.

Proof: Suppose $A_c(G) \leq I(G)$, but $Z(G) \not\leq \phi(G)$. Let $z \in Z(G)$ be such that $z \notin \phi(G)$, and let $\{z, x_1, \dots, x_r\}$ be a minimal generating set for G containing z . Let $a \in Z(G) \cap \phi(G)$ be such that $|a| = p$.

Suppose $G \xrightarrow{\eta} G/\phi(G) = \langle \bar{z} \rangle \otimes \langle \bar{x}_1 \rangle \otimes \dots \otimes \langle \bar{x}_r \rangle$, where $z^\eta = \bar{z}$, $x_i^\eta = \bar{x}_i$ for $i = 1, \dots, r$. Define $\beta: \frac{G}{\phi(G)} \rightarrow \langle a \rangle$ by $(\bar{z})^\beta = a$, $\bar{x}_i^\beta = 1$ for $i = 1, \dots, r$. $\beta \in \text{Hom}(\frac{G}{\phi(G)}, Z(G))$. Let α be defined by $g^\alpha = g g^{\eta\beta}$. Then by Lemma III.1, $\alpha \in A_c(G)$ and we have $z^\alpha = z z^{\eta\beta} = za \neq z$ since $a \neq 1$. Thus $\alpha \notin I(G)$ since $\alpha|_{Z(G)} \neq 1|_{Z(G)}$. But this is a contradiction to $A_c(G) \leq I(G)$. Thus we must have $Z(G) \leq \phi(G)$.

Theorem III.1: Let G be a p -group with no abelian direct factors and such that $A_c(G) \leq I(G)$. Then $Z(G) \leq G'$.

Proof: By the above remark, we know that $Z(G) \leq \phi(G)$.

Suppose that $Z(G) \not\leq G'$ and let $y \in Z(G)$ be such that $y \notin G'$.

We consider two cases.

Case 1). $\exp G/G' \geq \exp Z(G)$. Let $\{x_1, \dots, x_r\}$ be a minimal generating set for G such that in $G \cong G/G' = \langle a_1 \rangle \otimes \dots \otimes \langle a_r \rangle$, $x_i^\zeta = a_i$ and $|a_1| \geq \exp Z(G)$.

Define $\beta: G/G' \rightarrow \langle y \rangle$ by $a_1^\beta = y$, $a_i^\beta = 1$ for $i = 2, \dots, r$. Since $|y| \leq \exp Z \leq |a_1|$, we have $\beta \in \text{Hom}(G/G', Z(G))$. Defining α by $g^\alpha = g g^{\zeta\beta}$, we have $\alpha \in A_c(G) \leq I(G)$. Thus there exists $h \in G$ such that $\alpha = \pi_h$. Since $x_1^\alpha = x_1 x_1^{\zeta\beta} = x_1 y$, we have $h^{-1} x_1 h = x_1 y$, or $[x_1, h] = y \in G'$. But this is a contradiction since $y \notin G'$. Thus Case 1) cannot happen and we must have $\exp G/G' < \exp Z(G)$.

Case 2). Suppose $\exp G/G' < \exp Z(G)$. Let $\{x_1, \dots, x_r\}$ be a minimal generating set for G with the property that in $G \cong G/G' = \langle a_1 \rangle \otimes \dots \otimes \langle a_r \rangle$, $x_i^\zeta = a_i$. Let $z \in Z(G)$ be such that $|z| = \exp Z(G) = p^t$. Since $\exp Z(G) > \exp G/G'$, we have $|a_i| < p^t$ for $i = 1, \dots, r$.

$y \notin G'$ implies $y^\zeta \neq \bar{1}$, thus $y^\zeta = \prod_{i=1}^r a_i^{n_i}$ where for some i , $a_i^{n_i} \neq \bar{1}$, say $a_1^{n_1} \neq \bar{1}$. Let $|a_1| = p^s$ where $0 < s < t$.

Define $\beta: G/G' \rightarrow \langle z \rangle$ by $a_1^\beta = z^{p^{t-s}}$, $a_i^\beta = 1$ for $i \neq 1$.

$(a_1^{p^s})^\beta = (a_1^\beta)^{p^s} = (z^{p^{t-s}})^{p^s} = z^{p^t} = 1$, thus $\beta \in \text{Hom}(G/G', Z(G))$.

Defining α by $g^\alpha = g g^{\zeta\beta}$, we have $\alpha \in A_c(G)$.

$y^\alpha = y y^{\zeta\beta} = y \left(\prod_{i=1}^r a_i^{n_i} \right)^\beta = y z^{n_1 p^{t-s}}$. Since $a_1^{n_1} \neq 1$, $p^s \nmid n_1$.

Hence $z_1^{n_1 p^{t-s}} \neq 1$, so $y^\alpha \neq y$. But if $\alpha \in I(G)$, then since $y \in Z(G)$, $y^\alpha = y$. Since $A_c(G) \leq I(G)$, we again have a contradiction and case 2) cannot happen.

Thus we must have $Z(G) \leq G'$.

Theorem III.2: Let G be a p -group, $p \neq 2$, with no abelian direct factors satisfying the following conditions:

- 1). $A_c(G) \leq I(G)$,
- 2). $Z(G)$ is not cyclic.

Then $Z_2(G) \leq \phi(G)$.

Proof: Suppose $Z_2 = Z_2(G) \not\leq \phi(G)$. Let $y \in Z_2$ be such that $y \notin \phi(G)$, and let $\{y, x_2, \dots, x_r\}$ be a minimal generating set for G containing y . Let $Z(G) = \langle w_1 \rangle \otimes \langle w_2 \rangle \otimes \dots \otimes \langle w_q \rangle$ where $|w_i| = p^{m_i}$, $m_1 \geq m_2 \geq \dots \geq m_q$.

Suppose $G \xrightarrow{\eta} \frac{G}{\phi(G)} = \langle \bar{y} \rangle \otimes \langle \bar{x}_2 \rangle \otimes \dots \otimes \langle \bar{x}_r \rangle$ where $y^\eta = \bar{y}$, $x_i^\eta = \bar{x}_i$ for $i = 2, \dots, r$. Set $z_j = w_j^{p^{m_j-1}}$. Then we have for $j = 1, \dots, q$, $|z_j| = |w_j^{p^{m_j-1}}| = p$. Now define $\beta_j: \frac{G}{\phi(G)} \rightarrow \Omega_1(Z(G))$ by $\bar{y}^{\beta_j} = z_j$, $\bar{x}_i^{\beta_j} = 1$ for $i = 2, \dots, r$. If we define α_j by $g^{\alpha_j} = g g_j^{\beta_j}$, then by Lemma III.1, we have $\alpha_j \in A_c(G) \leq I(G)$.

Hence there exists $g_j \in Z_2$, $j = 1, \dots, q$ with the property that

$$\alpha_j = \pi_{g_j}.$$

Let $M = \langle x_2, \dots, x_r, \phi \rangle$. Since $(y^p)^{\alpha_j} = (y^{\alpha_j})^p = (yz_j)^p = y^p z_j^p = y^p$, we have $\alpha_j|_M = 1|_M$.

$\alpha_j|_M = 1|_M$ and α_j inner imply that $M \leq C_G(\langle g_j \rangle)$. Since M is a maximal subgroup of G , we must either have $C_G(\langle g_j \rangle) = M$ or $C_G(\langle g_j \rangle) = G$. If $C_G(\langle g_j \rangle) = G$, then $g_j \in Z(G)$, thus $\alpha_j = \pi_{g_j} = 1|_G$. But $y^{\alpha_j} = y z_j \neq y$, thus $g_j \notin Z(G)$. Hence we must have $C_G(\langle g_j \rangle) = M$.

$|G : M| = p = \text{the number of conjugates of } g_j$. Since $y^{\alpha_j} = y^{\pi g_j} = y z_j$, we have

$$g_j^{-1} y g_j = y z_j, \text{ or } y g_j y^{-1} = g_j z_j,$$

$$y^2 g_j (y^2)^{-1} = y (y g_j y^{-1}) y = g_j z_j^2,$$

...

$$y^{p-1} g_j (y^{p-1})^{-1} = g_j z_j^{p-1}.$$

Since $|z_j| = p$, we have the p conjugates of g_j are precisely the elements $g_j, g_j z_j, g_j z_j^2, \dots, g_j z_j^{p-1}$.

By Theorem III.1, we have, since $A_c(G) \leq I(G)$, that $Z(G) \leq G'$. Thus $\text{Hom}(G/G', Z(G)) \cong A_c(G)$. Since $\frac{G}{\phi(G)^u}$ is r -generated, $\frac{G}{\phi(G)^u} = \langle a_1 \rangle \otimes \langle a_2 \rangle \otimes \dots \otimes \langle a_r \rangle$. Let $|a_i| = p^{u_i}$ and let $G \xrightarrow{\zeta} G/G'$.

$$g_j^\zeta \neq \bar{1}, \text{ for if } g_j \in G', \text{ then } g_j \in G' \cap Z_2 \leq Z(Z_2).$$

Thus, since $y \in Z_2$, $y^{\pi g_j} = y z_j = y^{\alpha_j} \neq y$. Thus let

$$g_1^\zeta = a_1^{s_1} a_2^{s_2} \dots a_r^{s_r} \text{ and } g_2^\zeta = a_1^{t_1} a_2^{t_2} \dots a_r^{t_r}.$$

Since $|z_j| = p$, we have $|\beta_j| = p$ and thus $|\alpha_j| = p$.

$(\alpha_j)^p = (\pi g_j)^p = \pi g_j^p = 1|_G$ so we have $g_j^p \in Z(G) \leq G'$. Thus

$$(g_j^\zeta)^p = (g_j^p)^\zeta = \bar{1}, \text{ so } a_1^{ps_1} a_2^{ps_2} \dots a_r^{ps_r} = \bar{1} = a_1^{pt_1} a_2^{pt_2} \dots a_r^{pt_r}.$$

Hence we have $s_i \equiv 0 \pmod{p^{u_i-1}}$ and $t_i \equiv 0 \pmod{p^{u_i-1}}$.

Because $y \in Z_2(G)$, $\pi y \in A_c(G)$. Since $g_j^{\pi y^{-1}} = g_j z_j$, $y^{-1} \notin Z(G)$, so $y \notin Z(G)$ and $\pi y \neq 1|_G$. Moreover, since

$A_c(G) \cong \text{Hom}(G/G', Z(G))$, there exists $\gamma \in \text{Hom}(G/G', Z(G))$ such

that $(g_j^\zeta)^\gamma = z_j$ for $j = 1, \dots, q$, and in particular, for

$j = 1, 2$. Suppose, wolog, γ is given by $a_i^\gamma = w_1^{b_i} w_2^{h_i}$. Then

$$(g_1 \zeta)^\gamma = w_1^{\sum_{i=1}^r b_i s_i} w_2^{\sum_{i=1}^r h_i s_i} = z_1 = w_1^{p^{m_1-1}},$$

$$(g_2 \zeta)^\gamma = w_1^{\sum_{i=1}^r b_i t_i} w_2^{\sum_{i=1}^r h_i t_i} = z_2 = w_2^{p^{m_2-1}} \quad \text{and we have:}$$

$$\sum_{i=1}^r b_i s_i \equiv p^{m_1-1} \pmod{p^{m_1}}, \quad \sum_{i=1}^r h_i s_i \equiv 0 \pmod{p^{m_2}},$$

$$\sum_{i=1}^r b_i t_i \equiv 0 \pmod{p^{m_1}}, \quad \sum_{i=1}^r h_i t_i \equiv p^{m_2-1} \pmod{p^{m_2}}.$$

If $|w_1| = |w_2|$, define γ^* by $a_i^{\gamma^*} = w_1^{h_i} w_2^{b_i}$. Since

$$\gamma \in \text{Hom}(G/G', Z(G)), \quad \gamma^* \in \text{Hom}(G/G', Z(G)).$$

$$(g_1 \zeta)^{\gamma^*} = w_1^{\sum_{i=1}^r h_i s_i} w_2^{\sum_{i=1}^r b_i s_i} = w_2^{\sum_{i=1}^r b_i s_i} \neq 1 \quad \text{since } |w_1| = |w_2|$$

implies $m_1 = m_2$. Defining α^* by $g^{\alpha^*} = g \zeta^{\gamma^*}$, we have

$\alpha^* \in A_c(G) \leq I(G)$. Thus there exists $x \in G$ such that $\alpha^* = \pi_x$.

$\pi_x = g_1^{\alpha^*} = g_1 g_1^{\zeta^{\gamma^*}} = g_1 w_2^{\sum_{i=1}^r b_i s_i} \neq g_1$. Thus $g_1 w_2^{\sum_{i=1}^r b_i s_i}$ is conjugate to g_1 . But this is a contradiction since the conjugates of g_1 are $g_1, g_1 z_1, \dots, g_1 z_1^{p-1}$.

Now suppose $|w_1| \geq |w_2|$. Since $\sum_{i=1}^r h_i t_i \equiv p^{m_2-1} \pmod{p^{m_2}}$,

for some k we must have $h_k t_k \not\equiv 0 \pmod{p^{m_2}}$. For one such k ,

define δ on G/G' by $a_k^\delta = (w_1^{p^{m_1-m_2}})^{h_k}$, $a_i^\delta = 1$ for $i \neq k$.

Since $|w_1^{p^{m_1-m_2}}| = p^{m_2} = |w_2|$ and $g_k^\gamma = w_1^{b_k} w_2^{h_k}$, we have

$\delta \in \text{Hom}(G/G', Z(G))$.

$$(g_2 \zeta)^\delta = \left(\sum_{i=1}^r a_i^{t_i} \right)^\delta = (w_1^{p^{m_1-m_2}})^{h_k t_k} = w_1^{h_k t_k p^{m_1-m_2}} \neq 1$$

since $h_k t_k \not\equiv 0 \pmod{p^{m_2}}$. Now define δ^* by $g^{\delta^*} = g \zeta^\delta$. Since

$\delta \in \text{Hom}(G/G', Z(G))$, we have $\delta^* \in A_c(G) \leq I(G)$. Thus there exists $x \in G$ such that $\delta^* = \pi_x$.

$$g_2^{\pi_x} = g_2^{\delta^*} = g_2 g_2^{\zeta \delta} = g_2 w_1^{h_k t_k p^{m_1 - m_2}} \neq g_2. \text{ Thus}$$

$g_2 w_1^{h_k t_k p^{m_1 - m_2}}$ is conjugate to g_2 . But this is a contradiction since the conjugates of g_2 are $g_2, g_2^{z_2}, \dots, g_2^{z_2^{p-1}}$.

Thus we must have $Z_2(G) \leq \phi(G)$.

We now prove a result of Sanders.

Theorem: Let G be a p -group, $p \neq 2$, of nilpotence class two. Then $A_c(G) \leq I(G)$ if, and only if, $Z(G) = G'$ is cyclic.

Proof: Let $G' = Z(G)$ be cyclic. Then G has no abelian direct factors and we know $|A_c(G)| = |\text{Hom}(G/G', Z(G))|$.
 $\exp G/G' = \exp G/Z(G) \leq \exp Z(G)$ since $G' = Z(G)$ and $G = Z_2(G)$.
 Thus, because $Z(G)$ is cyclic, we have $\text{Hom}(G/G', Z(G)) \cong G/G'$.
 Thus $|A_c(G)| = |G/G'| = |G/Z(G)| = |I(G)|$ and $A_c(G) \leq I(G)$.

Now suppose $A_c(G) \leq I(G)$. G has no abelian direct factors, for suppose $G = P \otimes B$ where $P = \langle x \rangle$ is cyclic. Let $z \in Z(B)$ be such that $|z| = p$. For $g \in G$, $g = x^k b$ where $b \in B$. Define α on G by $g^\alpha = (xz)^k b$. Since G is a direct product of P and B and $z \in Z(B)$, α is a well-defined automorphism of G .
 $g^{-1} g^\alpha = (x^k b)^{-1} (xz)^k b = z^k \in Z(B) \leq Z(G)$, thus $\alpha \in A_c(G)$. But $x^\alpha = xz \neq x$, so $\alpha \notin I(G)$, contradiction to $A_c(G) \leq I(G)$.

Since G has no abelian direct factors and $A_c(G) \leq I(G)$, by Theorem III.1, $Z(G) \leq G'$. But G of nilpotence class two implies $G' \leq Z(G)$. Thus $G' = Z(G)$. By Theorem III.2, if $Z(G)$ is not cyclic, then $Z_2(G) \leq \phi(G)$. But $Z_2(G) = G$, thus $Z_2(G) \leq \phi(G)$ is impossible. Hence $Z(G) = G'$ is cyclic.

BIBLIOGRAPHY

BIBLIOGRAPHY

1. J.E. Adney and Ti Yen, Automorphisms of a p-group, Illinois J. Math. 9 (1965), 137-143.
2. Franklin Demana, Some theorems on extending automorphisms, Ph.D. Thesis, Michigan State University (1966).
3. R. Faudree, A Note on the Automorphism Group of a p-group, Proc. Amer. Math. Soc. 19 (1968), 1379-1382.
4. W. Gaschütz, Nichtabelsche p-Gruppen besitzen äussere p-Automorphisms, J. Algebra 4 (1966), 1-2.
5. M. Hall, The Theory of Groups, (New York: The Macmillan Company, 1959).
6. A.D. Otto, Central Automorphisms of a Finite p-Group, Trans. Amer. Math. Soc. 125 (1966), 280-287.
7. P.R. Sanders, Some results in the theory of automorphisms of finite groups, M.Sc. Thesis, University of London, 1967.
8. W.R. Scott, Group Theory, (Englewood Cliffs, New Jersey: Prentice Hall, Inc., 1964).
9. J. Thompson, Finite groups with fixed-point free automorphisms of prime order, Proc. Natl. Acad. Sci. U.S. 45 (1959), 578-581.
10. H.J. Zassenhaus, The Theory of Groups, (New York: Chelsea Publishing Company, 1958).

APPENDIX

APPENDIX

I. For p a prime, $p \neq 2$, $(1+tp^m)^p \equiv 1+tp^{m+k} \pmod{p^{m+k+1}}$

where $(t,p) = 1$, $m \geq 1$, $k \geq 1$.

The proof is by an easy induction argument.

II. If $c \in C_G(G')$, $k \geq 1$, then $[x, c^k] = [x, c]^k$.

Proof: $[x, c^1] = [x, c]$. Assume true for $k = n \geq 1$.

Then $[x, c^{n+1}] = [x, c^n c] = [x, c^n][x, c][x, c, c^n] = [x, c]^n[x, c]$
 $= [x, c]^{n+1}$ since $c \in C(G')$.

III. An automorphism α of a group G is called central if $x^{-1}x^\alpha \in Z(G)$ for all $x \in G$. The set of all central automorphisms of G forms a group called $A_c(G)$.

If $\alpha \in A_c(G)$, then $f_\alpha: x \rightarrow x^{-1}x^\alpha$ is a homomorphism of G into $Z(G)$. If $f \in \text{Hom}(G, Z)$, then $\alpha_f: x \rightarrow xf(x)$ defines an endomorphism of G . α_f is an automorphism if, and only if, $f(x) \neq x^{-1}$ for every $x \in G$, $x \neq 1$.

Adney and Yen show in [1] the following:

Theorem: For a group G with no abelian direct factors, the correspondence $\alpha \rightarrow f_\alpha$ defines a 1-1 mapping of $A_c(G)$ onto $\text{Hom}(G, Z)$.

Corollary: If G is a p -group, $p \neq 2$, with no abelian direct factors, then $A_c(G)$ is also a p -group.

$\text{Hom}(G, Z(G)) \cong \text{Hom}(G/G', Z(G))$ since if $\gamma \in \text{Hom}(G, Z(G))$, $G' \leq \ker \gamma$.

Sanders, in [7], shows the following:

Let G be a p -group with no abelian direct factors. Let

$$R = \{\gamma(g) \mid g \in G, \gamma \in \text{Hom}(G, Z)\} \quad \text{and} \quad B = \bigcap_{\gamma \in \text{Hom}(G, Z(G))} \ker \gamma.$$

Then $\text{Hom}(G, Z) \cong A_c(G)$ if, and only if, $R < B$.

Proof: If $\gamma_\alpha, \gamma_\beta \in \text{Hom}(G, Z)$, then $(\gamma_\alpha \gamma_\beta)(g) = \gamma_\alpha(g) \gamma_\beta(g)$.

Let $\alpha, \beta \in A_c(G)$ be such that α corresponds to γ_α , β corresponds

to γ_β . $(\alpha\beta)(g) = \alpha(\beta(g)) = \alpha(g\gamma_\beta(g)) = \alpha(g)\alpha(\gamma_\beta(g))$

$= g\gamma_\alpha(g)\gamma_\beta(g)\gamma_\alpha(\gamma_\beta(g))$. $\alpha\beta$ thus corresponds to $\gamma_\alpha\gamma_\beta$ if, and

only if, $\gamma_\alpha(\gamma_\beta(g)) = 1$, or $R < B$.

MICHIGAN STATE UNIVERSITY LIBRARIES



3 1293 03177 3330