

# ON FINITE P-GROUPS OF CONJUGATE RANK 1

*By*  
**TUSHAR KANTA NAIK**  
**MATH08201304007**

**Harish-Chandra Research Institute, Allahabad**

*A thesis submitted to the*  
*Board of Studies in Mathematical Sciences*  
*In partial fulfillment of requirements*  
*for the Degree of*  
**DOCTOR OF PHILOSOPHY**  
*of*  
**HOMI BHABHA NATIONAL INSTITUTE**







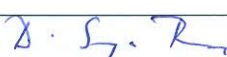

**June, 2018**



# Homi Bhabha National Institute<sup>1</sup>

## Recommendations of the Viva Voce Committee

As members of the Viva Voce Committee, we certify that we have read the dissertation prepared by Tushar Kanta Naik entitled "On Finite P-Groups of Conjugate Rank 1" and recommend that it may be accepted as fulfilling the thesis requirement for the award of Degree of Doctor of Philosophy.

Chairman - Prof. B. Ramakrishnan		Date: 22.10.18
Guide / Convener – Prof. Manoj Kumar		Date: 22.10.2018
Examiner – Prof. R. P. Shukla		Date: 22/10/18
Member 1- Prof. Punita Batra		Date: 22.10.18
Member 2- Prof. D. Surya Ramana		Date: 22/10/18
Member 3- Prof. P. K. Ratnakumar		Date: 22/10/18

Final approval and acceptance of this thesis is contingent upon the candidate's submission of the final copies of the thesis to HBNI.

I/We hereby certify that I/we have read this thesis prepared under my/our direction and recommend that it may be accepted as fulfilling the thesis requirement.

Date: 22.10.2018

Place: Allahabad

  
Prof. Manoj Kumar  
Guide

<sup>1</sup> This page is to be included only for final submission after successful completion of viva voce.



## **STATEMENT BY AUTHOR**

This dissertation has been submitted in partial fulfillment of requirements for an advanced degree at Homi Bhabha National Institute (HBNI) and is deposited in the Library to be made available to borrowers under rules of the HBNI.

Brief quotations from this dissertation are allowable without special permission, provided that accurate acknowledgement of source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the Competent Authority of HBNI when in his or her judgment the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

**TUSHAR KANTA NAIK**



## **DECLARATION**

I, hereby declare that the investigation presented in the thesis has been carried out by me. The work is original and has not been submitted earlier as a whole or in part for a degree / diploma at this or any other Institution / University.

**TUSHAR KANTA NAIK**





## List of Publications arising from the thesis

### Journal

1. “Finite  $p$ -groups of conjugate type  $\{1, p^3\}$ ”, Tushar Kanta Naik and Manoj Kumar Yadav, *J. Group Theory*, **2018**, *21(1)*, 65-82.

### Others

1. “Finite  $p$ -groups of nilpotency class 3 with two conjugacy class sizes”, Tushar Kanta Naik, Manoj Kumar Yadav and Rahul Dattatraya Kitture, arxiv link: <https://arxiv.org/pdf/1708.03245.pdf>
2. “On the probability distribution associated to commutator word map in finite groups II”, Tushar Kanta Naik, <https://arxiv.org/pdf/1805.00091.pdf>

TUSHAR KANTA NAIK



## **Dedicated to**

My father Late Surendar Naik



## **ACKNOWLEDGEMENTS**

I have accumulated a substantial debt of gratitude in my personal and mathematical journey so far. I take immense pleasure to acknowledge the people who have played an indispensable part in my life.

This note of acknowledgement would be nothing but irrelevant without mentioning the main architect of my mathematical life, my supervisor Prof. Manoj Kumar Yadav.

I have greatly benefited from his patience; many a times he has listened to my naive ideas carefully and corrected my mistakes. I am happy to find his presence and useful advice in any academic or non-academic matter, however trivial it might be. I thank him for all his careful guidance, affectionate encouragement and endless support. This thesis is the result of his enterprising supervision.

Though I heavily miss my father's physical presence, I always find his teachings and his emotional presence with me. He was a respected teacher in my school and it was his motivation that I developed fascination for mathematics as a subject. This thesis is a tribute to him, who believed in me more than I do in myself.



# Contents

Conventions and Notations	iii
Synopsis	v
<b>1 Background</b>	<b>1</b>
1.1 Literature and Definitions . . . . .	1
1.2 Isoclinism . . . . .	9
1.3 Key Lemmas . . . . .	10
<b>2 Finite <math>p</math>-groups of conjugate type <math>(1, p^3)</math></b>	<b>13</b>
2.1 Introduction . . . . .	13
2.2 Technical Lemmas . . . . .	15
2.3 Proof of Theorems 2.1.1 and 2.1.2 . . . . .	30
<b>3 Finite <math>p</math>-groups of nilpotency class 3 with two conjugacy class sizes</b>	<b>35</b>
3.1 Introduction . . . . .	35
3.2 Key results . . . . .	37
3.3 Examples . . . . .	53

3.4	Proof of Main Theorem [Theorem 3.1.3] . . . . .	56
<b>4</b>	<b>On the probability distribution associated to commutator word map in finite groups</b>	<b>77</b>
4.1	Introduction . . . . .	78
4.2	Key Results . . . . .	80
4.3	Proof of Theorem 4.1.2 . . . . .	85
4.4	Proof of Theorem 4.1.3 . . . . .	90
	<b>Bibliography</b>	<b>97</b>

---



# Conventions and Notations

Symbol	Description
$Z(G)$	center of $G$
$\Phi(G)$	frattini subgroup of $G$
$G'$	commutator subgroup of $G$
$\gamma_3(G)$	third term of the lower central series of $G$
$H \leq G$	$H$ is subgroup of $G$
$H < G$	$H$ is proper subgroup of $G$
$H \trianglelefteq G$	$H$ is normal subgroup of $G$
$H \triangleleft G$	$H$ is proper normal subgroup of $G$
$H^\#$	set of non-trivial elements of $H$
$[x, y]$	$x^{-1}y^{-1}xy$ , the commutator of $x$ and $y$
$[x, y, z]$	$[[x, y], z]$
$C_H(x)$	the centralizer of $x$ in $H$
$x^G$	the conjugacy class of $x$ in $G$
$[G, x]$	the set $\{[g, x] \mid g \in G\}$
$exp(G)$	exponent of $G$
$\setminus$	set minus
$ A $	cardinality of the set $A$
$U_n(q)$	group of lower unitriangular matrices with entries from field of order $q$
$[x]$	integral part of $x$



# Synopsis

Study of finite groups having only two conjugacy class sizes goes back to 1953, when N. Ito studied them first time and proved that such groups are more or less finite  $p$ -groups. It was later proved that the nilpotency class of such finite  $p$ -groups is at most 3. Conjugate rank of such a group is defined to be 1. This thesis deals with classification of such groups.

The thesis contains three principal parts. The first part deals with finite  $p$ -groups of conjugate type  $(1, p^3)$ . If a finite group  $G$  has only two conjugacy class sizes 1 and  $p^n$ ,  $n \geq 1$ , then we say that  $G$  is of conjugate type  $(1, p^n)$ . In 1999, K. Ishikawa [11] classified (up to isoclinism) finite  $p$ -groups of conjugate type  $(1, p)$  and  $(1, p^2)$ . We contribute in the same line of research by presenting classification (up to isoclinism) of finite  $p$ -groups of conjugate type  $(1, p^3)$ .

In the second part of thesis, we present a complete classification (up to isoclinism) of finite  $p$ -groups of conjugate type  $(1, p^n)$  and nilpotency class 3.

The last part of the thesis deals with the probability distribution associated to commutator word map in finite  $p$ -groups of conjugate rank 1. Let  $P(G)$  denote the set of sizes of fibers (for section 0.3 for definition) of non-trivial commutators of the commutator word map. We prove that  $|P(G)| = 1$ , for any finite group  $G$  of conjugate rank 1 and nilpotency class 3. We also show that for given  $n \geq 1$ ,

there exists a finite group  $G$  of conjugate rank 1 and nilpotency class 2 such that  $|P(G)| = n$ .

## 0.1 Finite $p$ -groups of conjugate type $(1, p^3)$

A finite group  $G$  is said to be of *conjugate type*  $(1 = m_0, m_1, \dots, m_r)$ ,  $m_i < m_{i+1}$ , if  $m_i$ 's are precisely the different sizes of conjugacy classes of  $G$ . We also say that such groups  $G$  are of *conjugate rank*  $r$ .

In 1953, N. Ito started the study of finite groups with few conjugacy class sizes. He proved the following result.

**Theorem 0.1.1** [13] *If  $G$  is a finite group of conjugate type  $(1, m)$ , then  $m = p^n$ , for some prime  $p$  and integer  $n \geq 1$ , and  $G$  is isoclinic to a non-abelian  $p$ -group.*

Nearly half a century later, K. Ishikawa proved following important result.

**Theorem 0.1.2** [12] *Let  $G$  be a finite  $p$ -groups of conjugate type  $(1, p^n)$ . Then nilpotency class of  $G$  is at most 3, for odd primes  $p$  and exactly 2 for  $p = 2$ .*

In a different paper [11], Ishikawa classified finite  $p$ -groups of conjugate type  $(1, p^n)$ , up to isoclinism, for  $n \leq 2$ .

The natural problem which arises here is: *classify finite  $p$ -groups of conjugate type  $(1, p^n)$ , where  $n \geq 3$ .*

For any positive integer  $r \geq 1$  and prime  $p \geq 2$ , consider the following group constructed by N. Ito [13].

$$G_r = \langle a_1, \dots, a_{r+1} \mid [a_i, a_j] = b_{ij}, [a_k, b_{ij}] = 1, \quad (1)$$

$$a_i^p = a_{r+1}^p = b_{ij}^p = 1, 1 \leq i < j \leq r+1, 1 \leq k \leq r+1 \rangle.$$


---

Ito showed that the group  $G_r$  (defined above) is of conjugate type  $(1, p^r)$ . Here we give necessary and sufficient conditions for some quotients of  $G_r$  to be of conjugate rank 1.

**Lemma 0.1.3** [20] *Suppose  $G = G_{n-1}$  (as defined in (1.1)) is generated by  $a_1, a_2, \dots, a_n$ , where  $n \geq 4$ . Suppose that  $M < Z(G) = G'$  with  $|M| = p$ . Then  $G/M$  is of conjugate type  $(1, p^{n-1})$  if and only if  $M$  can be reduced to the form*

$$M = \langle [a_1, a_2][a_3, a_4][a_5, a_6] \dots [a_{2m-1}, a_{2m}] \rangle, \text{ where } 2 \leq m \leq \lfloor n/2 \rfloor.$$

For simplicity of notation, say  $G_3$  is generated by  $a, b, c$  and  $d$ .

**Lemma 0.1.4** [20] *Suppose  $G = G_3$  and  $N < Z(G) = G'$  with  $|N| = p^2$ . Then  $G/N$  is of conjugate type  $(1, p^3)$  if and only if  $N$  can be reduced to the following form*

$$N = \langle [a, b][c, d], [a, c][b, d]^r \rangle, \text{ where } r \text{ is any fixed non-square integer modulo } p.$$

A finite group  $G$  is said to be a *Camina group* if  $x^G = xG'$  for all  $x \in G \setminus G'$ , where  $x^G$  denotes the conjugacy class of  $x$  in  $G$ .

We provide a classification of all finite  $p$ -groups of conjugate type  $(1, p^3)$ ,  $p > 2$ , upto isoclinism, in the following theorem.

**Theorem 0.1.5** [20] *Let  $G$  be a finite  $p$ -group of conjugate type  $(1, p^3)$ ,  $p > 2$ . Then the nilpotency class of  $G$  is 2 and  $G$  is isoclinic to one of the following groups:*

1. *A finite Camina  $p$ -group of nilpotency class 2 with commutator subgroup of order  $p^3$ ;*
2. *The group  $G_3$  (as defined in (1));*

3. The quotient group  $G_3/M$ , where  $M$  is a normal subgroup of  $G_3$  given by  $M = \langle [a, b][c, d] \rangle$ ;
4. The quotient group  $G_3/N$ , where  $N$  is a normal subgroup of  $G_3$  given by  $N = \langle [a, b][c, d], [a, c][b, d]^t \rangle$ ; with  $t$  any fixed integer non-square modulo  $p$ .

Now, we consider a more general family of finite  $p$ -groups of class 2 and conjugate type  $(1, p^3)$  to include the case  $p = 2$ .

Let  $\hat{G}_n$  denote the family consisting of  $(n+1)$ -generator non-abelian special  $p$ -groups  $G$  of order  $p^{(n+1)(n+2)/2}$ . Then it follows that all groups of this family are of conjugate type  $(1, p^n)$ . It also turns out that any two groups in  $\hat{G}_n$  are isoclinic. So, all groups in the family  $\hat{G}_3$  are of conjugate type  $(1, p^3)$ , where  $p$  is any prime including 2. Let  $\hat{\mathcal{G}}_3$  denote the subfamily of  $\hat{G}_3$  consisting of 2-groups. For simplicity of notation, we assume that a group  $\mathcal{G}$  from  $\hat{\mathcal{G}}_3$  is minimally generated by the set  $\{a, b, c, d\}$ .

Here we give necessary and sufficient conditions for some quotients of  $\mathcal{G}$  to be of conjugate type  $(1, 8)$ , where  $\mathcal{G} \in \hat{\mathcal{G}}_3$ . Following two results are analogous to Lemma 0.1.3 and Lemma 0.1.4, for  $p = 2$ .

**Lemma 0.1.6** [20] *Let  $G = \langle a, b, c, d \rangle \in \hat{\mathcal{G}}_3$ . Then  $G/M$  with  $|M| = 2$  is of conjugate type  $(1, 8)$  if and only  $N$  can be reduced to the form  $M = \langle [a, b][c, d] \rangle$ .*

**Lemma 0.1.7** [20] *Let  $G = \langle a, b, c, d \rangle \in \hat{\mathcal{G}}_3$ . Then  $G/N$  with  $|N| = 4$  is of conjugate type  $(1, 8)$  if and only  $N$  can be reduced to the form*

$$N = \langle [a, b][c, d], [a, c][b, d][c, d] \rangle.$$

In the following theorem we provide a classification of 2-groups of conjugate

---

type (1, 8) upto isoclinism.

**Theorem 0.1.8** [20] *Let  $G$  be a finite 2-group of conjugate type (1, 8) and nilpotency class 2. Then  $G$  is isoclinic to one of the following groups:*

1. *A finite Camina 2-group with commutator subgroup of order 8;*
2. *A fixed group  $\mathcal{G}$  in the family  $\hat{\mathcal{G}}_3$ , defined above;*
3. *The quotient group  $\mathcal{G}/M$ , where  $M$  is a normal subgroup of  $\mathcal{G}$  such that  $M = \langle [a, b][c, d] \rangle$ ;*
4. *The quotient group  $\mathcal{G}/N$ , where  $N$  is a normal subgroup of  $\mathcal{G}$  such that  $N = \langle [a, b][c, d], [a, c][b, d][c, d] \rangle$ .*

## 0.2 Finite $p$ -groups of nilpotency class 3 with 2 conjugacy class sizes

Ito [13] constructed a group  $W$  of conjugate type (1,  $p^2$ ) and nilpotency class 3. Presentation of  $W$  is as follows:

$$W = \langle a_1, a_2, b, c_1, c_2 \mid [a_1, a_2] = b, [a_i, b] = c_i \\ a_i^p = b^p = c_i^p = [a_i, c_i] = [a_1, c_2] = [a_2, c_1] = 1 \ (i = 1, 2) \rangle.$$

After that nothing much was known about finite  $p$ -groups of conjugate type (1,  $p^n$ ) and nilpotency class 3. In 1996, the examples of  $p$ -group of nilpotency class 3 and of conjugate type (1,  $p^{2m}$ ) appeared in the construction of certain Camina  $p$ -groups of nilpotency class 3 by Dark and Scoppola [4, p. 796-797]. It can be shown that for a given integer  $m \geq 1$  and a prime  $p > 2$ , the  $p$ -group

---

of conjugate type  $(1, p^{2m})$  and class 3, constructed by Dark and Scoppola, is isomorphic to  $\mathcal{H}_m/\mathbf{Z}(\mathcal{H}_m)$ , where  $\mathcal{H}_m$  is presented as follows.

$$\mathcal{H}_m = \left\{ \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ a & 1 & 0 & 0 & 0 \\ c & b & 1 & 0 & 0 \\ d & ab - c & a & 1 & 0 \\ f & e & c & b & 1 \end{bmatrix} : a, b, c, d, e, f \in \mathbb{F}_{p^m} \right\}. \quad (2)$$

In view of these examples, a natural question which arises here is the following:

**Question.** Does there exist a finite  $p$ -group of nilpotency class 3 and conjugate type  $(1, p^n)$ , for an odd prime  $p$  and odd integer  $n \geq 5$ ?

We answer this question, by proving the following much general result.

**Theorem 0.2.1** [21] *Let  $p > 2$  be a prime and  $n \geq 1$  an integer. Then there exist finite  $p$ -groups of nilpotency class 3 and conjugate type  $(1, p^n)$  if and only if  $n$  is even. For each positive even integer  $n = 2m$ , every finite  $p$ -group of nilpotency class 3 and of conjugate type  $(1, p^n)$  is isoclinic to the group  $\mathcal{H}_m/\mathbf{Z}(\mathcal{H}_m)$ , where  $\mathcal{H}_m$  is as in (3.1).*

### 0.3 Probability distribution associated to commutator word map

Let  $G$  be a finite group and  $K(G)$  denotes the set of commutators of  $G$ . For  $g \in K(G)$ , we define *fiber* of  $g$  as,  $fiber(g) := \{(x, y) \in G \times G \mid [x, y] = g\}$ . In 2008, Pournaki and Sobhani [25] introduced the notion of  $Pr_g(G)$ , which is defined as follows:

---



$$Pr_g(G) = |\{(x, y) \in G \times G : [x, y] = g\}|/|G|^2 = |fiber(g)|/|G|^2.$$

Nath and Yadav[23] introduced the set  $P(G)$ , which is defined as follows:

$$P(G) = \{Pr_g(G) : 1 \neq g \in K(G)\}.$$

Nath and Yadav[23] proved that  $|P(G_r)| = 1$ , for all  $r \geq 2$ , where  $G_r$  is the group as defined in (1.1). They asked the following question: *Is it true that  $|P(G)| = 1$  for all finite  $p$ -groups  $G$  of conjugate rank 1 and nilpotency class 2 ?*

We negatively answer this in the following theorem.

**Theorem 0.3.1 [22]** *Let  $n \geq 2$  be a given positive integer. Then there always exist a group  $G$  of conjugate rank 1 and nilpotency class 2 such that  $|P(G)| = n$ .*

For finite  $p$ -groups of conjugate rank 1 and nilpotency class 3, we prove the following result.

**Theorem 0.3.1 [22]** *Let  $G$  be a finite  $p$ -group of conjugate type  $(1, p^{2n})$  and nilpotency class 3. Then for  $g \in G'$ ,*

$$Pr_g(G) = \begin{cases} \frac{p^{3n} + p^{2n} - 1}{p^{5n}}, & \text{if } g = 1 \\ \frac{p^{2n} - 1}{p^{5n}}, & \text{if } 1 \neq g \in G'. \end{cases}$$

Hence  $|P(G)| = 1$ .

This theorem rectifies a faulty statement [23, Theorem 5.13], where it was proved that  $|P(G)| > 1$ , for a finite  $p$ -group  $G$  of conjugate type  $(1, p^2)$  and nilpotency class 3.

---



# CHAPTER 1

## Background

*This chapter has three sections. In the first section, we present some basic definitions and literature on finite  $p$ -groups of conjugate rank 1. In the second section, we introduce the concept of isoclinism of finite groups. In the last section of this chapter, we collect some results, which are used later in the thesis. We do not give many proofs in this chapter as almost all the material presented, is either well known or easily available from the references.*

*We mainly, with a little diversion, present what is relevant to this thesis, and by no means this chapter is a complete overview of the subject.*

### 1.1 Literature and Definitions

Throughout this thesis, all the groups are finite, unless stated otherwise. In particular,  $G$  always stands for a finite group.

**Definition 1.1.1 (Conjugacy class)** *For any element  $x \in G$ , the conjugacy*

class of  $x$  in  $G$  is defined as

$$x^G = \{y^{-1}xy \mid y \in G\}.$$

It is well known that  $x \in x^G$  and  $|C_G(x)||x^G| = |G|$ . Hence  $|x^G| = 1$  if and only if  $|C_G(x)| = |G|$ , i.e.,  $x^G = \{x\}$  if and only if  $x$  belongs to the center of  $G$ . In other words  $|x^G| > 1$  (i.e., there exists  $y \neq x \in x^G$ ) if and only if  $x \notin Z(G)$ .

**Definition 1.1.2 (Conjugate type and conjugate rank)**  $G$  is said to be of conjugate type  $(1 = m_0, m_1, \dots, m_r)$ ,  $m_i < m_{i+1}$ , if  $m_i$ 's are precisely the different sizes of all conjugacy classes of  $G$ . In this case, we say that  $G$  is of conjugate rank  $r$ .

**Remark 1.1.3**  $G$  is of conjugate rank 0 if and only if  $G$  is abelian, and  $G$  is of conjugate rank 1 if and only if there exists an integer  $m > 1$  such that  $|x^G| = m$  for all  $x \in G \setminus Z(G)$ .

N. Ito initiated the study of finite groups with few conjugacy class sizes. In a series of paper “On finite groups with given conjugate type I, II, III” ([13], [14], [15]), he studied finite groups of conjugate rank 1, 2 and 3 respectively. He proved [13] the following path-breaking result for groups of conjugate rank 1.

**Theorem 1.1.4** [13] *Let  $G$  be a finite group with exactly two conjugacy class sizes, namely 1 and  $m$ . Then the following hold:*

(i)  $m$  is a power of some prime  $p$ , say  $m = p^n$ .

(ii)  $G = P \times A$ , where  $P$  is the non-abelian sylow  $p$ -subgroup of  $G$  and  $A$  is an abelian  $p'$  subgroup of  $G$ . In particular,  $G$  is nilpotent.

**Remark 1.1.5** *To understand finite groups of conjugate rank 1 it is sufficient to study finite  $p$ -groups of conjugate rank 1.*

**Remark 1.1.6** *As  $p$ -group of conjugate type  $(1, p^n)$  and  $p$ -group of conjugate rank 1 both are equivalent, we use one of either terminology as per convenience.*

In the same paper [13], N. Ito gave examples of  $p$ -groups of conjugate rank 1 with nilpotency class 2 and 3 separately, which opened the path for future research.

For any positive integer  $r \geq 1$  and prime  $p > 2$ , N. Ito constructed the following group of conjugate rank 1 with nilpotency class 2.

**Example 1.1.7 (Example 1, [13])**

$$G_r = \langle a_1, \dots, a_{r+1} \mid [a_i, a_j] = b_{ij}, [a_k, b_{ij}] = 1, \quad (1.1) \\ a_i^p = a_{r+1}^p = b_{ij}^p = 1, 1 \leq i < j \leq r+1, 1 \leq k \leq r+1 \rangle.$$

Note that the group  $G_r$  defined in (1.1) is a special  $p$ -group (see Definition 1.1.8) of order  $p^{(r+1)(r+2)/2}$  with exponent  $p$  and  $|G_r'| = p^{r(r+1)/2}$ . The group  $G_r$  enjoys the property  $C_{G_r}(x) = \langle x, Z(G_r) \rangle$ , for all  $x \in G_r \setminus Z(G_r)$ . In particular  $G_r$  is of conjugate type  $(1, p^r)$  and nilpotency class 2.

**Definition 1.1.8 (Special  $p$ -group)** *A  $p$ -group  $G$  is called special, if its commutator, center and frattini subgroup are all equal and elementary abelian.*

**Definition 1.1.9 (Extra special  $p$ -group)** *A  $p$ -group  $G$  is called extra-special, if it is special and  $|Z(G)| = p$ .*

For prime  $p > 2$ , N. Ito constructed the following group of nilpotency class 3 and conjugate rank 1.

---

**Example 1.1.10 (Example 2, [13])**

$$W = \langle a, b, h, z_1, z_2 \mid [a, b] = h, [a, h] = z_1, [b, h] = z_2 \quad (1.2) \\ a^p = b^p = h^p = z_i^p = [a, z_i] = [b, z_i] = 1 \ (i = 1, 2) \rangle.$$

Note that the group  $W$  defined in (1.2) is of order  $p^5$  with nilpotency class 3 and exponent  $p$ . The center,  $Z(W)$  and commutator subgroup,  $W'$  of  $W$  are elementary abelian  $p$ -groups of order  $p^2$  and  $p^3$  respectively.  $C_W(x) = \langle x, Z(W) \rangle$  and  $C_W(h) = W'$ , for each  $x \in W \setminus W'$  and  $y \in W' \setminus Z(W)$ . In particular  $W$  is of conjugate type  $(1, p^2)$ .

Now, we take a diversion from our discussion on finite  $p$ -groups of conjugate rank 1, and recall some related results on groups of higher conjugate ranks. In 1970, N. Ito proved following results for groups of conjugate rank 2 and 3 separately.

**Theorem 1.1.11 (Page 231, [14])** *Let  $G$  be a finite group of conjugate rank 2, then  $G$  is solvable.*

**Theorem 1.1.12 (Page 267, [15])** *Let  $G$  be a finite simple group of conjugate rank 3, then  $G$  is isomorphic with some  $SL(2, 2^m)$ , for  $m \geq 2$ .*

In 2009, S. Dolfi and E. Jabara studied finite groups of conjugate rank 2 and characterized all such groups  $G$  except the case when  $|G|$  is a prime power. Before stating their results, we collect some related terminology used in their work.

**Definition 1.1.13 (Frobenius group)** *Let  $G$  be a group and  $H$  be a non-trivial subgroup of  $G$  such that  $H \cap H^x = 1$ , for all  $x \in G \setminus H$ . In this case  $G$  is called a Frobenius group.*

---

**Definition 1.1.14** ( $\mathbf{O}_p(G)$ ) *Let  $G$  be a group and  $p$  be a prime number. Then the following two statements are equivalent:*

- (i)  *$H$  is the intersection of all sylow  $p$ -subgroups of  $G$ .*
- (ii)  *$H$  is the unique largest normal  $p$ -subgroup of  $G$ .*

*In this case the subgroup  $H$  is denoted by  $\mathbf{O}_p(G)$ .*

**Definition 1.1.15** (*F*-group) *A non-abelian group  $G$  is an *F*-group, if for every  $x, y \in G \setminus Z(G)$ , we have that  $C_G(x) \leq C_G(y)$  implies  $C_G(x) = C_G(y)$ .*

**Theorem 1.1.16** (**Theorem A**, [6]) *A finite group  $G$  has conjugate rank 2 if and only if, up to an abelian direct factor, either of the following cases hold:*

- (A)  *$G$  is a  $p$ -group of conjugate rank 2; or*
- (B)  *$G = KL$  with  $K \trianglelefteq G$ ,  $(|K|, |L|) = 1$  and one of the following occurs:*
  - (B1) *Both  $K$  and  $L$  are abelian,  $Z(G) \leq L$  and  $G/Z(G)$  is a Frobenius group;*
  - (B2)  *$K$  is abelian,  $L$  is a non-abelian  $p$ -group,  $M = \mathbf{O}_p(G)$  is an abelian subgroup of index  $p$  in  $L$  and  $G/M$  is a Frobenius group;*
  - (B3)  *$K$  is a  $p$ -group of conjugate rank 1,  $L$  is abelian,  $Z(K) = Z(G) \cap K$  and  $G/Z(G)$  is a Frobenius group.*

**Theorem 1.1.17** (**Theorem B**, [6]) *Let  $G$  be a finite group of conjugate rank 2. Then  $G$  is either an *F*-group or the direct product of an abelian group and a group of prime power order.*

**Theorem 1.1.18** (**Corollary C**, [6]) *Let  $G$  be a finite group of conjugate type  $(1, m, n)$ . If  $m$  and  $n$  are not coprime, then either  $m$  or  $n$  is a prime power.*

---

The following theorem was due to J. Cossey and T. O. Hawkes, where they proved the existence of  $p$ -groups of given conjugate type.

**Theorem 1.1.19 (Page 49, [3])** *Let  $p$  be a prime and  $0 = e_0 < e_1 < \cdots < e_n$  be integers. Then there exists a  $p$ -group  $G$  of nilpotency class 2 such that,  $G$  is of conjugate type  $(1 = p^0, p^{e_1}, \dots, p^{e_m})$ .*

The preceding result is actually a dual of the following result, which was proved by I. M. Isaacs.

**Theorem 1.1.20 (Page 552, [10])** *Let  $p$  be a prime and  $0 = e_0 < e_1 < \cdots < e_n$  be integers. Then there exists a  $p$ -group  $G$  of nilpotency class  $\leq 2$  such that the set of irreducible complex character degrees of  $G$  is exactly  $(1 = p^0, p^{e_1}, \dots, p^{e_m})$ .*

In a short survey prepared for the workshop Finite Groups and Their Automorphisms, Bogazici University, Istanbul, June 7-11, 2011, A. Mann raised a problem, which is as follows.

**Problem 1.1.21 (Problem 1, [19])** *Find other constructions, in particular ones that produce groups of higher class.*

After this much diversion, we come back to  $p$ -groups of conjugate rank 1. In 1970, I. M. Isaacs [9] proved the following beautiful result, from which, exact nilpotency class for 2-groups of conjugate rank 1 can be derived.

**Theorem 1.1.22 (Page 501, [9])** *Let  $G$  be a finite group, which contain a proper normal subgroup  $N$  such that all the conjugacy classes of  $G$ , which lie outside  $N$  have same lengths. Then either  $G/N$  is cyclic or every non-identity element of  $G/N$  is of prime order.*

Putting  $N = Z(G)$  in Theorem 1.1.22, we get

---



**Corollary 1.1.23** *Let  $G$  be a finite  $p$ -group with conjugate type  $(1, p^n)$ . Then both  $G'$  and  $G/Z(G)$  are of exponent  $p$ .*

Putting  $p = 2$  in Corollary 1.1.23, we get

**Corollary 1.1.24** *Let  $G$  be a finite 2-group with conjugate type  $(1, 2^n)$ . Then  $G/Z(G)$  is abelian and thus the nilpotency class of  $G$  is exactly 2.*

Apart from above result (Corollary 1.1.24), not much progress was made to understand finite groups of conjugate rank 1. It was K. Ishikawa, who came with some major breakthrough ([11], [12]). Not only he gave an exact bound for nilpotency class of groups of conjugate rank 1, but he also initiated the study of groups of conjugate type  $(1, p^n)$ , for  $n \geq 1$ . He proved the following important results.

**Theorem 1.1.25 (Page 119, [12])** *Let  $G$  be a  $p$ -group with exactly two conjugacy class sizes;  $p$  be a odd prime. Then the nilpotency class of  $G$  is either 2 or 3.*

**Theorem 1.1.26 (Proposition 3.1, [11])** *A finite  $p$ -group  $G$  has exactly two conjugacy class sizes 1 and  $p$  if and only if  $G$  is isoclinic (see Section 1.2 for definition) to an extra special  $p$ -group (see Definition 1.1.9).*

**Theorem 1.1.27 (Theorem 4.2, [11])** *Let  $G$  be a finite  $p$ -group of conjugate type  $(1, p^2)$  and nilpotency class 3. Then  $G$  is isoclinic to  $W$  (as defined in (1.2)).*

**Theorem 1.1.28 (Theorem 4.1, [11])** *Let  $G$  be a finite  $p$ -group of conjugate type  $(1, p^2)$  and nilpotency class 2. Then  $G$  is isoclinic to one of the following:*

- (i) *A camina  $p$ -group (see definition 1.1.29)  $H$  with  $|H'| = p^2$ .*

(ii)  $G_2$ , as defined in (1.1), for  $r = 2$ .

We recall  $G_2$  below;

$$G_2 = \langle a_1, a_2, a_3 \mid [a_i, a_j] = b_{ij}, [a_k, b_{ij}] = 1, \\ a_i^p = a_3^p = b_{ij}^p = 1, 1 \leq i < j \leq 3, 1 \leq k \leq 3 \rangle.$$

**Definition 1.1.29 (Camina group)** *A finite group  $G$  is said to be a Camina group if  $x^G = xG'$  for all  $x \in G \setminus G'$ .*

**Example 1.1.30 (Camina Group)** *For an integer  $m > 1$ , let*

$$\mathcal{H} = \left\{ \left[ \begin{array}{ccc} 1 & \alpha_1 & \alpha_2 \\ 0 & 1 & \alpha_3 \\ 0 & 0 & 1 \end{array} \right] : \alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_{p^m} \right\},$$

where  $\mathbb{F}_{p^m}$  is a finite field of  $p^m$  elements. It is easy to check that  $\mathcal{H}$  is a Camina  $p$ -group of nilpotency class 2 with  $|\mathcal{H}'| = p^m$ . This group is minimally generated by  $2m$  elements.

Let  $H$  be a finite Camina  $p$ -group of nilpotency class 2 with  $|H'| = p^m$ . Let  $A$  be any subgroup of  $H'$  of order  $p^{m-n}$ , where  $n < m$ . Then it is easy to see that  $H/A$  is a Camina group of conjugate type  $(1, p^n)$ .

**Remark 1.1.31** *For a given integer  $n \geq 1$ , the number of generators of Camina groups of conjugate type  $(1, p^n)$  and nilpotency class 2 can not be bounded.*

## 1.2 Isoclinism

The concept of isoclinism of groups was introduced by P. Hall [8]. Let  $X$  be a finite group and  $\bar{X} = X/Z(X)$ . Then commutation in  $X$  gives a well defined map  $a_X : \bar{X} \times \bar{X} \mapsto \gamma_2(X)$  such that  $a_X(xZ(X), yZ(X)) = [x, y]$  for  $(x, y) \in X \times X$ . Two finite groups  $G$  and  $H$  are called *isoclinic* if there exists an isomorphism  $\phi$  of the factor group  $\bar{G} = G/Z(G)$  onto  $\bar{H} = H/Z(H)$ , and an isomorphism  $\theta$  of the subgroup  $G'$  onto  $H'$  such that the following diagram is commutative

$$\begin{array}{ccc} \bar{G} \times \bar{G} & \xrightarrow{a_G} & G' \\ \phi \times \phi \downarrow & & \downarrow \theta \\ \bar{H} \times \bar{H} & \xrightarrow{a_H} & H'. \end{array}$$

The resulting pair  $(\phi, \theta)$  is called an *isoclinism* of  $G$  onto  $H$ .

Notice that isoclinism is an equivalence relation among finite groups. The equivalence classes of finite groups with respect to the isoclinism relation are called as *isoclinism families*.

The following two results follow from [8].

**Proposition 1.2.1** *Let  $G$  and  $H$  be two isoclinic finite  $p$ -groups. Then  $G$  and  $H$  are of the same conjugate type.*

**Proposition 1.2.2** *Let  $G$  be a finite  $p$ -group. Then there exists a group  $H$  in the isoclinism family of  $G$  such that  $Z(H) \leq H'$ .*

Group  $H$  which occurred in Proposition 1.2.2 is called a *stem group* in its isoclinism family. In the light of the preceding two results, for the classification of finite  $p$ -groups of conjugate type  $(1, p^n)$  upto isoclinism, we only need to consider a stem group from the respective isoclinism family.

---

## 1.3 Key Lemmas

As mentioned earlier, here we collect some results which will be used in upcoming chapters more often. We start with the following important result given by N. Ito.

**Proposition 1.3.1 (Proposition 3.2, [13])** *Let  $G$  be a finite  $p$ -group of conjugate type  $(1, p^n)$ . Then the number of elements in any minimal generating set is at least  $n$ , and the order of the subgroup of all the elements of order  $p$  of  $Z(G)$  is at least  $p^n$ .*

Before going forward, we recall the notion of breadth in finite  $p$ -groups.

**Definition 1.3.2 (Breadth)** *Let  $G$  be a finite  $p$ -group and  $x \in G$  be such that  $|x^G| = p^{b(x)}$ . Then  $b(x)$  is called the breadth of  $x$ . The breadth of  $G$ , denoted by  $b(G)$ , is defined as  $\max\{b(x) \mid x \in G\}$ .*

The following important result is due to Vaughan-Lee.

**Proposition 1.3.3 (Page 278, [27])** *Let  $G$  be a finite  $p$ -group such that  $b(G) = n$ . Then  $|G'| \leq p^{n(n+1)/2}$ .*

The following characterization of  $p$ -groups of breadth 3,  $p$  odd primes is due to Parmeggiani and Stellmacher. Similar result was proved earlier by Gavioli *et al.*, (Corollary 3, [7]) for all primes  $p \geq 5$ .

**Proposition 1.3.4 (Page 53, [24])** *Let  $G$  be a  $p$ -group,  $p > 2$ . Then  $b(G) = 3$  if and only if one of the following holds:*

(i)  $|G'| = p^3$  and  $[G : Z(G)] \geq p^4$ .

(ii)  $|G'| = p^4$  and there exists  $H \triangleleft G$  with  $|H| = p$  and  $[G/H : Z(G/H)] = p^3$ .

---

(iii)  $|G'| \geq p^4$  and  $[G : Z(G)] = p^4$ .

A similar result for  $p = 2$  is proved by Wilkens (Pages 203-204, [29]), a consequence of which is stated in the last section of Chapter 2, for the groups having conjugate type (1, 8).

Now, we recall the famous Hall-Witt Identity.

**Lemma 1.3.5 (Hall-Witt Identity)** *If  $x, y, z \in G$ , then*

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

We conclude this chapter with the following two elementary facts, proofs of which are immediate from the Hall-Witt identity.

**Lemma 1.3.6** *Let  $G$  be a group of nilpotency class 3 and  $x, y, z \in G$  such that  $[x, z], [y, z] \in Z(G)$ . Then  $[x, y, z] = 1$ .*

**Lemma 1.3.7** *Let  $G$  be a group of nilpotency class 3 and  $x, y \in G$  such that  $[x, y] \in Z(G)$ . Then  $[x, z, y] = [y, z, x]$ , for all  $z \in G$ .*



# CHAPTER 2

## Finite $p$ -groups of conjugate type

$$(1, p^3)$$

*K. Ishikawa classified (up to isoclinism) finite groups of conjugate type  $(1, p)$  and  $(1, p^2)$ . Following his footsteps, we present the classification (up to isoclinism) of finite  $p$ -groups of conjugate type  $(1, p^3)$  in this chapter.*

### 2.1 Introduction

Recall that the group  $G_r$  defined in (1.1) (preceding chapter) is of conjugate type  $(1, p^r)$  and nilpotency class 2. In particular  $G_3$  is of conjugate type  $(1, p^3)$  and nilpotency class 2. For simplicity of notation, now onwards we assume that  $G_3$  is generated by  $a, b, c$ , and  $d$ . Now, we recall the group  $G_3$  below.

$$G_3 = \langle a, b, c, d \mid x^p = [x, y]^p = [x, y, z] = 1, \quad (2.1) \\ x, y, z \in \{a, b, c, d\} \rangle.$$

In the following theorem we provide a classification of all finite  $p$ -groups of conjugate type  $(1, p^3)$ ,  $p > 2$ , upto isoclinism.

**Theorem 2.1.1** *Let  $G$  be a finite  $p$ -group of conjugate type  $(1, p^3)$ ,  $p > 2$ . Then the nilpotency class of  $G$  is 2 and  $G$  is isoclinic to one of the following groups:*

- (i) *A finite Camina  $p$ -group of nilpotency class 2 with commutator subgroup of order  $p^3$ ,*
- (ii) *The group  $G_3$ , defined in (2.1),*
- (iii) *The quotient group  $G_3/M$ , where  $M$  is a normal subgroup of  $G_3$  given by  $M = \langle [a, b][c, d] \rangle$ ,*
- (iv) *The quotient group  $G_3/N$ , where  $N$  is a normal subgroup of  $G_3$  given by  $N = \langle [a, b][c, d], [a, c][b, d]^t \rangle$  with  $t$  any fixed integer non-square modulo  $p$ .*

Since the nilpotency class of a finite 2-group of conjugate type  $(1, 2^n)$  for all  $n \geq 1$  is 2 (see Corollary 1.1.24), classification problem reduces to finite 2-groups of class 2. To include the case  $p = 2$ , we consider a more general class of finite  $p$ -groups of class 2 and conjugate type  $(1, p^3)$ .

Let  $\hat{G}_n$  denote the family consisting of  $(n + 1)$ -generator non-abelian special  $p$ -groups  $G$  of order  $p^{(n+1)(n+2)/2}$ . Then it follows that all groups of this family are of conjugate type  $(1, p^n)$ . It also turns out that any two groups in  $\hat{G}_n$  are isoclinic (see Remark 2.2.13). So, all groups in the family  $\hat{G}_3$  are of conjugate type  $(1, p^3)$ , where  $p$  is any prime including 2.

Let  $\hat{\mathcal{G}}_3$  denote the subfamily of  $\hat{G}_3$  consisting of 2-groups. For simplicity of notation, we assume that a group  $\mathcal{G}$  from  $\hat{\mathcal{G}}_3$  is minimally generated by the

---



set  $\{a, b, c, d\}$ . A magma check shows that this family has exactly 989 non-isomorphic groups [1].

Now we are ready to state our next result which provides a classification of 2-groups of conjugate type  $(1, 8)$  upto isoclinism.

**Theorem 2.1.2** *Let  $G$  be a finite 2-group of conjugate type  $(1, 8)$  and nilpotency class 2. Then  $G$  is isoclinic to one of following groups:*

- (i) *A finite Camina 2-group with commutator subgroup of order 8;*
- (ii) *A fixed group  $\mathcal{G}$  in the family  $\hat{\mathcal{G}}_3$ , defined above;*
- (iii) *The quotient group  $\mathcal{G}/M$ , where  $M$  is a normal subgroup of  $\mathcal{G}$  such that  $M = \langle [a, b][c, d] \rangle$ ;*
- (iv) *The quotient group  $\mathcal{G}/N$ , where  $N$  is a normal subgroup of  $\mathcal{G}$  such that  $N = \langle [a, b][c, d], [a, c][b, d][c, d] \rangle$ .*

## 2.2 Technical Lemmas

Here we prove some lemmas, which we require to prove our main results of this chapter (Theorems 2.1.1 and 2.1.2).

**Lemma 2.2.1** *Let  $G$  be a finite  $p$ -group of conjugate type  $(1, p^3)$ ,  $p > 2$ . Then one of the following holds:*

- (i)  $|G'| = p^3$  and  $[G : Z(G)] \geq p^4$ ;
- (ii)  $|G'| \geq p^4$  and  $[G : Z(G)] = p^4$ .

*Proof.* Suppose that there exists a normal subgroup  $H$  of  $G$  such that  $|H| = p$  and  $[G/H : Z(G/H)] = p^3$ . Then, since  $G$  is of conjugate type  $(1, p^3)$  and  $|H|$

---

$= p$ , it follows that  $Z(G/H) = Z(G)/H$ . Thus,

$$p^3 = [G/H : Z(G/H)] = [G/H : Z(G)/H] = [G : Z(G)].$$

But, since  $G$  is of conjugate type  $(1, p^3)$ , we have  $[G : C_G(x)] = p^3$ , for all  $x \in G \setminus Z(G)$ . Since  $x \in C_G(x) \setminus Z(G)$ , we have  $Z(G) < C_G(x)$ ; contradicting the equality  $[G : Z(G)] = [G : C_G(x)] = p^3$ . Hence there can not exist any  $H < G$  with  $|H| = p$  and  $[G/H : Z(G/H)] = p^3$ . The proof is now complete from Proposition 1.3.4.  $\square$

**Definition 2.2.2 (Autoclinism)** *For a given group  $G$ , an isoclinism  $(\phi, \theta)$  from  $G$  onto itself is called an autoclinism of  $G$ .*

It is not difficult to prove the following result.

**Lemma 2.2.3** *Let  $G$  be a group from the family  $\hat{G}_n$  (defined above). Then a bijection between any two minimal generating sets for  $G$  extends to an autoclinism of  $G$ .*

For the groups  $G := G_r$  defined in (1.1), the following more general result holds true.

**Lemma 2.2.4** *A bijection between any two minimal generating sets for  $G := G_r$  extends to an automorphism of  $G$ .*

We have noticed above that any group  $G$  from the family  $\hat{G}_{n-1}$  is of conjugate type  $(1, p^{n-1})$  with  $|G| = p^{n(n+1)/2}$  and  $G$  is minimally generated by  $n$  elements. The following two results characterize all finite  $n$ -generator special  $p$ -groups of order  $p^{n(n+1)/2-1}$  and conjugate type  $(1, p^{n-1})$ .

---

**Lemma 2.2.5** *Let  $G \in \hat{G}_{n-1}$  be a group generated by  $n \geq 4$  elements  $a_1, a_2, \dots, a_n$ . Suppose that  $M < Z(G) = G'$  with  $|M| = p$ . Then  $G/M$  is of conjugate type  $(1, p^{n-1})$  if and only if  $M$  can be reduced to the form*

$$M = \langle [a_1, a_2][a_3, a_4][a_5, a_6] \dots [a_{2m-1}, a_{2m}] \rangle, \text{ where } 2 \leq m \leq \lfloor n/2 \rfloor.$$

*Proof.* Notice that  $|G| = p^{n(n+1)/2}$ . Also notice that any bijection between two minimal generating sets for  $G$  extends to an autoclinism of  $G$  by Lemma 2.2.3. Set  $\bar{G} = G/M$ ; then  $|\bar{G}| = p^{(n(n+1)/2)-1}$ . Since  $G$  is of conjugate type  $(1, p^{n-1})$  and  $|M| = p$ , we have

$$Z(G)/M = Z(\bar{G}) = \bar{G}' = \Phi(\bar{G})$$

is an elementary abelian  $p$ -group of order  $p^{(n(n-1)/2)-1}$ .

Thus  $[\bar{G} : Z(\bar{G})] = p^n$ . Hence  $\bar{G}$  is of conjugate type  $(1, p^{n-1})$  if and only if each non-central element of  $\bar{G}$  commutes only with its own powers up to the central elements.

Let  $\bar{x}, \bar{y} \in \bar{G} \setminus Z(\bar{G})$  be such that no one is a power of the other (reading modulo  $Z(\bar{G})$ ). Then it is not difficult to see that  $[x, y] \neq 1$  in  $G$ . Hence, if  $[\bar{x}, \bar{y}] = 1$  in  $\bar{G}$ , then  $[x, y] \in M^\#$ .

Any given central subgroup  $M_1$  of order  $p$ , without loss of generality, can be written as

$$M_1 = \langle [a_1, a_2][a_1, a_3]^{\alpha_{1,3}} \dots [a_i, a_j]^{\alpha_{i,j}} \dots [a_{n-1}, a_n]^{\alpha_{n-1,n}} \rangle,$$

where  $1 \leq i < j \leq n$ . Now applying the autoclinism induced by the map

---

$a_2 \mapsto a_2 a_3^{-\alpha_{1,3}} \dots a_n^{-\alpha_{1,n}}$ ,  $a_i \mapsto a_i$  for  $i \neq 2$ ,  $M_1$  gets mapped to

$$M_2 = \langle [a_1, a_2][a_2, a_3]^{\alpha_{2,3}} \dots [a_i, a_j]^{\alpha_{i,j}} \dots [a_{n-1}, a_n]^{\alpha_{n-1,n}} \rangle$$

with  $2 \leq i < j \leq n$  and modified  $\alpha_{i,j}$ . Notice that  $G/M_1$  is isoclinic to  $G/M_2$ , and therefore both  $G/M_1$  and  $G/M_2$  are of the same conjugate type. We now apply another autoclinism induced by the map  $a_1 \mapsto a_1 a_3^{\alpha_{2,3}} \dots a_n^{\alpha_{2,n}}$ ,  $a_i \mapsto a_i$  for  $i \neq 1$ , and see that  $M_2$  gets mapped to

$$M_3 = \langle [a_1, a_2][a_3, a_4]^{\alpha_{3,4}} \dots [a_i, a_j]^{\alpha_{i,j}} \dots [a_{n-1}, a_n]^{\alpha_{n-1,n}} \rangle$$

with  $3 \leq i < j \leq n$  and modified  $\alpha_{i,j}$ .

Take  $x = a_1^{j_1} a_2^{j_2} \dots a_n^{j_n}$  and  $y = a_1^{k_1} a_2^{k_2} \dots a_n^{k_n}$  be such that none is power of the other (reading modulo  $Z(G)$ ). Then  $[x, y] \in M_3^\#$  only when the following two conditions hold true:

- (i)  $j_3 = j_4 = \dots = j_n = k_3 = k_4 = \dots = k_n = 0$ ;
- (ii)  $\alpha_{i,j} = 0$ ,  $3 \leq i < j \leq n$ .

Hence  $G/M_3$  is of conjugate type  $(1, p^{n-1})$  if and only if at least one  $\alpha_{i,j}$  is non-zero modulo  $p$ . We now conclude that  $G/M_3$  is of conjugate type  $(1, p^{n-1})$  if and only if

$$M_3 = \langle [a_1, a_2][a_3, a_4]^{\alpha_{3,4}} \dots [a_i, a_j]^{\alpha_{i,j}} \dots [a_{n-1}, a_n]^{\alpha_{n-1,n}} \rangle$$

with  $3 \leq i < j \leq n$  and at least one  $\alpha_{i,j}$  is non-zero modulo  $p$ . We can assume that  $\alpha_{3,4} \neq 0$ .

Make further reductions by applying an autoclinism of  $G$  which is a composition of the autoclinisms induced by the maps (1)  $a_4 \mapsto a_4^{-1}$ ,  $a_i \mapsto a_i$  for  $i \neq 4$ , (2)

$a_4 \mapsto a_4 a_5^{-\alpha_{3,5}} a_6^{-\alpha_{3,6}} \cdots a_n^{-\alpha_{3,n}}$ ,  $a_i \mapsto a_i$  for  $i \neq 4$  and (3)  $a_3 \mapsto a_3 a_5^{\alpha_{4,5}} a_6^{\alpha_{4,6}} \cdots a_n^{\alpha_{4,n}}$ ,  $a_i \mapsto a_i$  for  $i \neq 3$ . This action reduces  $M_3$  to  $M_4$ , which is of the following form

$$M_4 = \langle [a_1, a_2][a_3, a_4][a_5, a_6]^{\alpha_{5,6}} \cdots [a_i, a_j]^{\alpha_{i,j}} \cdots [a_{n-1}, a_n]^{\alpha_{n-1,n}} \rangle$$

with  $5 \leq i < j \leq n$  and modified  $\alpha_{i,j}$  again.

Finally, if all  $\alpha_{i,j}$  are 0 modulo  $p$ , we are done by taking  $M = M_4$ . If not, then finite repetitions of the above process reduce  $M_4$  to the desired form  $M$ , completing the proof.  $\square$

**Corollary 2.2.6** *Let  $K$  be an  $n$ -generator special  $p$ -group of order  $p^{n(n+1)/2-1}$  and conjugate type  $(1, p^{n-1})$ . Then  $K$  is isoclinic to  $G/M$ , where  $G = \langle a_1, a_2, \dots, a_n \rangle \in \hat{G}_{n-1}$  and  $M < Z(G) = G'$  with  $|M| = p$  is of the form*

$$M = \langle [a_1, a_2][a_3, a_4][a_5, a_6] \cdots [a_{2m-1}, a_{2m}] \rangle, \text{ where } 2 \leq m \leq \lfloor n/2 \rfloor.$$

*Proof.* Notice that the group  $K$ , given in the statement, is isomorphic to a quotient of some group  $G$  from the family  $\hat{G}_{n-1}$  by a subgroup of order  $p$  contained in  $G'$ . Now the proof follows from the preceding lemma.  $\square$

In particular, if, for an odd prime  $p$ , we take a  $p$ -group  $G$  from the class  $\hat{G}_{n-1}$  such that the exponent of  $G$  is  $p$ , then  $G$  is isomorphic to the group  $G_{n-1}$  defined in (1.1). Then by Lemma 2.2.4 a bijection between any two minimal generating sets for  $G := G_{n-1}$ , extends to an automorphism of  $G$ . Therefore, on the lines of the proofs of Lemma 2.2.5 and Corollary 2.2.6 (replacing autoclinism by automorphism and isoclinic by isomorphic), we can prove the following.

**Lemma 2.2.7** *Let  $K$  be an  $n$ -generator special  $p$ -group of order  $p^{n(n+1)/2-1}$ , exponent  $p$  and conjugate type  $(1, p^{n-1})$ , where  $p$  is an odd prime. Then  $K$  is*

isomorphic to  $G_{n-1}/M$ , where  $G_{n-1}$  is the group as defined in (1.1) generated by  $a_1, a_2, \dots, a_n$  and  $M < Z(G) = G'$  with  $|M| = p$  is of the form

$$M = \langle [a_1, a_2][a_3, a_4][a_5, a_6] \dots [a_{2m-1}, a_{2m}] \rangle, \text{ where } 2 \leq m \leq \lfloor n/2 \rfloor.$$

For the case  $n = 3$ , the preceding lemma was proved by Brahana [2]. For the application point of view, we state it explicitly as a corollary.

**Corollary 2.2.8** *Let  $K$  be a 4-generator special  $p$ -group of order  $p^9$ , exponent  $p$  and conjugate type  $(1, p^3)$ , where  $p$  is an odd prime. Then  $K$  is isomorphic to  $G_3/M$ , where  $G_3$  is generated by  $a, b, c, d$  and  $M < Z(G) = G'$  with  $|M| = p$  is of the form*

$$M = \langle [a, b][c, d] \rangle.$$

Now onward we concentrate only on the groups  $G$  from the family  $\hat{G}_3$ .

**Lemma 2.2.9** *Let  $G$  be a group from the family  $\hat{G}_3$  which is generated by  $a, b, c$  and  $d$ . Suppose that  $N < Z(G) = G'$  with  $|N| = p^2$ . Then  $G/N$  is of conjugate type  $(1, p^3)$  if and only if  $N$  can be reduced to the following form*

$$N = \langle [a, b][c, d], [a, c][b, d]^r \rangle, \text{ where } r \text{ is any fixed non-square integer modulo } p.$$

*Proof.* Notice that  $|G| = p^{10}$ . Set  $\bar{G} = G/N$ ; then  $|\bar{G}| = p^8$ . Since  $G$  is of conjugate type  $(1, p^3)$  and  $|N| = p^2$ , we have

$$Z(G)/N = Z(\bar{G}) = \bar{G}' = \Phi(\bar{G})$$

is an elementary abelian  $p$ -group of order  $p^4$ . Thus  $[\bar{G} : Z(\bar{G})] = p^4$ . Hence  $\bar{G}$  is of conjugate type  $(1, p^3)$  if and only if each non-central element of  $\bar{G}$  commutes

---

only with its own powers up to the central elements.

Let  $\bar{x}, \bar{y} \in \bar{G} \setminus Z(\bar{G})$  be such that no one is a power of the other (reading modulo  $Z(\bar{G})$ ). Then it is not difficult to see that  $[x, y] \neq 1$  in  $G$ . Hence, if  $[\bar{x}, \bar{y}] = 1$  in  $\bar{G}$ , then  $[x, y] \in N^\#$ .

Any given central subgroup  $N_1$  of order  $p^2$ , without loss of generality, can be written as one of the following two types:

$$(i)N_1 = \langle [a, b][a, d]^{i_1}[b, c]^{i_2}[b, d]^{i_3}[c, d]^{i_4}, [c, d] \rangle.$$

$$(ii)N_1 = \langle [a, b][a, d]^{i_1}[b, c]^{i_2}[b, d]^{i_3}[c, d]^{i_4}, [a, c][a, d]^{j_1}[b, c]^{j_2}[b, d]^{j_3}[c, d]^{j_4} \rangle.$$

If  $N_1$  is of type (i), then  $\bar{c}$  commutes with  $\bar{d}$ , although  $\bar{c} \notin \langle Z(\bar{G}), \bar{d} \rangle$ . Hence  $\bar{G}$  can not be of conjugate type  $(1, p^3)$ . Therefore we only need to consider  $N_1$  as in type (ii). Now applying the autoclinism induced by the map  $a \mapsto a, b \mapsto bd^{-i_1}, c \mapsto cd^{-j_1}, d \mapsto d$ ,  $N_1$  gets mapped to  $N_2$ , where

$$N_2 = \langle [a, b][b, c]^{i_1}[b, d]^{i_2}[c, d]^{i_3}, [a, c][b, c]^{j_1}[b, d]^{j_2}[c, d]^{j_3} \rangle$$

with modified powers of the basic commutators. Notice that  $G/N_1$  and  $G/N_2$  are isoclinic. We now apply another autoclinism induced by the map  $a \mapsto ac^{i_1}d^{i_2}, b \mapsto b, c \mapsto c, d \mapsto d$ , and see that  $N_2$  gets mapped to

$$N_3 = \langle [a, b][c, d]^i, [a, c][b, c]^{j_1}[b, d]^{j_2}[c, d]^{j_3} \rangle$$

again with modified powers of commutators. Note that  $i$  is non-zero modulo  $p$ , otherwise  $G/N_3$  can not be of conjugate type  $(1, p^3)$ . Thus the map  $a \mapsto a,$

---

$b \mapsto b, c \mapsto c, d \mapsto d^{i-1}$  extends to an autoclanism of  $G$  and maps  $N_3$  to

$$N_4 = \langle [a, b][c, d], [a, c][b, c]^{j_1}[b, d]^{j_2}[c, d]^{j_3} \rangle$$

with modified  $j_2$  and  $j_3$ . Again note that  $j_2$  can not be zero modulo  $p$ , otherwise  $[c, ab^{j_1}d^{-j_3}] = 1$  and so  $G/N_3$  can not be of conjugate type  $(1, p^3)$ . Therefore the map  $a \mapsto a, b \mapsto b, c \mapsto c, d \mapsto c^{-j_1 j_2^{-1}} d$  is well defined. The autoclanism of  $G$  induced by this map takes  $N_4$  to  $N_5$ , where, after modifying powers,

$$N_5 = \langle [a, b][c, d], [a, c][b, d]^{i_1}[c, d]^{i_2} \rangle.$$

Now let  $x = a^{j_1} b^{j_2} c^{j_3} d^{j_4}$  and  $y = a^{k_1} b^{k_2} c^{k_3} d^{k_4}$  be such that none is power of the other (reading modulo  $Z(G)$ ). If  $[x, y] \in N_5^\#$ , then at least one of  $j_1$  and  $k_1$  has to be non-zero modulo  $p$ . Without loss of generality we take  $j_1$  to be non-zero. Now we can write  $y$  as  $y = a^{k_1} b^{k_2} c^{k_3} d^{k_4} = (a^{j_1} b^{j_2} c^{j_3} d^{j_4})^{k_1 j_1^{-1}} b^{l_2} c^{l_3} d^{l_4} z_1$ , where  $z_1 \in Z(G)$  and  $l_2, l_3, l_4$  are some suitable integers. So we can modify  $x$  and  $y$  as  $x = a^{j_1} b^{j_2} c^{j_3} d^{j_4}$  with  $j_1$  non-zero and  $y = b^{l_2} c^{l_3} d^{l_4}$ . Now  $l_2$  has to be non-zero modulo  $p$  and  $l_4$  has to be 0.

Using similar argument, we can remove power of  $b$  in  $x$ . So we can modify  $x$  and  $y$  by  $x = a^{j_1} c^{j_3} d^{j_4}$  and  $y = b^{l_2} c^{l_3}$ . Now  $j_3$  has to be 0. So, finally we have reduced  $x$  and  $y$  to  $x = a^{j_1} d^{j_4}$  and  $y = b^{l_2} c^{l_3}$ . If  $[x, y] \in N_5^\#$ , then  $[x^{j_1^{-1}}, y^{l_2^{-1}}]$  also belongs to  $N_5^\#$ . Also  $x^{j_1^{-1}} = a d^j z_2$  and  $y^{l_2^{-1}} = b c^k z_3$ , where  $z_2$  and  $z_3$  are some central elements. Therefore  $[x^{j_1^{-1}}, y^{l_2^{-1}}] = [a, b][a, c]^k [b, d]^j [c, d]^{jk}$ . So if  $[x, y] \in N_5^\#$ , then  $[a, b][a, c]^k [b, d]^j [c, d]^{jk} \in N_5^\#$ , and therefore can be written as a product of powers of generators of  $N_5^\#$ . Now comparing power of the basic

---



commutators, we get

$$j \equiv ki_1 \pmod{p} \text{ and } jk \equiv ki_2 + 1 \pmod{p}.$$

Solving these we have

$$k^2i_1 - ki_2 - 1 \equiv 0 \pmod{p}.$$

This is possible only when  $i_2^2 + 4i_1$  is a square modulo  $p$ . From this, we conclude that  $G/N_5$  is of conjugate type  $(1, p^3)$  if and only if  $N_5$  is of the following form

$$N_5 = \langle [a, b][c, d], [a, c][b, d]^{i_1}[c, d]^{i_2} \rangle; \text{ where } i_2^2 + 4i_1 \text{ is a non-square modulo } p.$$

Now we consider two cases, namely: Case 1.  $i_2 \neq 0$ ; Case 2.  $i_2 = 0$ , and take these one by one.

**Case 1:** Let  $r$  be a fixed integer non-square modulo  $p$ . Then  $r$  must be non-zero. Being non-square,  $i_2^2 + 4i_1$  is also non-zero. Thus  $\frac{i_2^2 + 4i_1}{4r}$  is a non-zero square modulo  $p$ . Thus there exists a non-zero  $l$  such that  $l^2 = \frac{i_2^2 + 4i_1}{4r}$ . Set  $t = \frac{i_2}{2}$ .

Now applying the autoclinism of  $G$  induced by the map  $a \mapsto a^l d^t$ ,  $b \mapsto b$ ,  $c \mapsto b^t c^l$ ,  $d \mapsto d$ ,  $N_5$  gets mapped to

$$\begin{aligned} N_6 &= \langle [a, b]^l [c, d]^l, [a, b]^{lt} [a, c]^{l^2} [b, d]^{ti_2 + i_1 - t^2} [c, d]^{li_2 - lt} \rangle \\ &= \langle ([a, b][c, d])^l, ([a, b][c, d])^{lt} ([a, c]^{l^2} [b, d]^{ti_2 + i_1 - t^2}) \rangle \\ &= \langle [a, b][c, d], [a, c]^{l^2} [b, d]^{ti_2 + i_1 - t^2} \rangle \\ &= \langle [a, b][c, d], [a, c]^{\frac{i_2^2 + 4i_1}{4r}} [b, d]^{\frac{i_2^2 + 4i_1}{4}} \rangle \\ &= \langle [a, b][c, d], ([a, c][b, d]^r)^{\frac{i_2^2 + 4i_1}{4r}} \rangle \end{aligned}$$

$$\begin{aligned}
&= \langle [a, b][c, d], [a, c][b, d]^r \rangle \\
&= N.
\end{aligned}$$

Hence we are done in this case.

**Case 2:** In this case  $i_1$  must be a non-square. If  $i_1 = r$ , then we are done. If not, then  $i_1^{-1}r$  must be a non-zero square, and therefore there exists a non-zero integer  $l$  such that  $i_1^{-1}r = l^2$ .

Now the autoconjugation of  $G$  induced by the map  $a \mapsto a$ ,  $b \mapsto b$ ,  $c \mapsto c^{l^{-1}}$ ,  $d \mapsto d^l$  maps  $N_5$  to

$$\begin{aligned}
N_7 &= \langle [a, b][c, d], [a, c]^{l^{-1}}[b, d]^{li_1} \rangle \\
&= \langle [a, b][c, d], ([a, c][b, d]^{l^2i_1})^{l^{-1}} \rangle \\
&= \langle [a, b][c, d], [a, c][b, d]^{l^2i_1} \rangle \\
&= \langle [a, b][c, d], [a, c][b, d]^r \rangle \\
&= N.
\end{aligned}$$

The proof is now complete. □

The following result characterizes all 4-generator special groups of order  $p^8$  and conjugate type  $(1, p^3)$ .

**Corollary 2.2.10** *Let  $K$  be a 4-generator special  $p$ -group of order  $p^8$  and conjugate type  $(1, p^3)$ . Then  $K$  is isoclinic to  $G/N$ , where  $G = \langle a, b, c, d \rangle \in \hat{G}_3$  and  $N < Z(G) = G'$  with  $|N| = p^2$  is of the form*

$N = \langle [a, b][c, d], [a, c][b, d]^r \rangle$ , where  $r$  is any fixed non-square integer modulo  $p$ .

---

*Proof.* Notice that the group  $K$ , given in the statement, is isomorphic to a quotient of some group  $G$  from the family  $\hat{G}_3$  by a subgroup of order  $p^2$  contained in  $G'$ . Now the proof follows from the preceding lemma.  $\square$

In particular, if, for an odd prime  $p$ , we take a  $p$ -group  $G$  from the class  $\hat{G}_3$  such that the exponent of  $G$  is  $p$ , then  $G$  is isomorphic to the group  $G_3$  defined in (2.1). Then by Lemma 2.2.4 a bijection between any two minimal generating sets for  $G_3$ , extends to an automorphism of  $G$ . Therefore, on the lines of the proofs of Lemma 2.2.15 and Corollary 2.2.8 (replacing autoclinism by automorphism and isoclinic by isomorphic), we can prove the following result, which has also been proved by Brahana [2, Section 2]. But the proof in the present text is in modern terminology.

**Lemma 2.2.11** *Let  $K$  be a 4-generator special  $p$ -group of order  $p^8$ , exponent  $p$  and conjugate type  $(1, p^3)$ , where  $p$  is an odd prime. Then  $K$  is isomorphic to  $G_3/N$ , where  $G_3$  is the group defined in (2.1) and  $N < Z(G) = G'$  with  $|N| = p^2$  is of the form*

$$N = \langle [a, b][c, d], [a, c][b, d]^r \rangle, \text{ where } r \text{ is any fixed non-square integer modulo } p.$$

Now we consider the family  $\hat{G}_3$  of 2-groups defined in the introduction of this chapter. We start with the following result which tells that certain type of quotient groups of any two groups in  $\hat{G}_3$  are isoclinic.

**Lemma 2.2.12** *Let  $G = \langle a, b, c, d \rangle$  and  $G^* = \langle s, u, v, w \rangle$  be two groups from the family  $\hat{G}_3$ . Then the following hold true.*

(i)  $G$  and  $G^*$  are isoclinic.

(ii) If  $M = \langle [a, b][c, d] \rangle \leq G'$  and  $M^* = \langle [s, u][v, w] \rangle \leq (G^*)'$ , then  $G/M$

and  $G^*/M^*$  are isoclinic.

(iii) If

$$N = \langle [a, b][c, d], [a, c][b, d][c, d] \rangle \leq G'$$

and

$$N^* = \langle [s, u][v, w], [s, v][u, w][v, w] \rangle \leq (G^*)',$$

then  $G/N$  and  $G^*/N^*$  are isoclinic.

*Proof.* We sketch proof only for (i). Note that both  $G/Z(G)$  and  $G^*/Z(G^*)$  are elementary abelian 2-groups of order  $2^4$ , generated by  $\{aZ(G), bZ(G), cZ(G), dZ(G)\}$  and  $\{sZ(G^*), uZ(G^*), vZ(G^*), wZ(G^*)\}$  respectively. Similarly, both  $G'$  and  $(G^*)'$  are elementary abelian 2-groups generated by the sets consisting of all 6 basic commutators

$$\{[a, b], [a, c], [a, d], [b, c], [b, d], [c, d]\}$$

and

$$\{[s, u], [s, v], [s, w], [u, v], [u, w], [v, w]\}$$

respectively. Now the map  $a \mapsto s, b \mapsto u, c \mapsto v$  and  $d \mapsto w$  extends to an isomorphism from  $G/Z(G)$  onto  $G^*/Z(G^*)$ , which induces an isomorphism from  $G'$  onto  $(G^*)'$ , making  $G$  and  $G^*$  isoclinic.  $\square$

**Remark 2.2.13** *The second and third assertions of the preceding lemma hold true in the bigger family  $\hat{G}_3$ . And by the same argument as given in the preceding proof, one can easily prove that any two groups in  $\hat{G}_n$  are isoclinic. We have stated this result for the family  $\hat{G}_3$  because we here need it only for 2-groups.*

The following lemma is immediate from Corollary 2.2.6, using Lemma 2.2.12,

---

when restricted to the family  $\hat{\mathcal{G}}_3$ .

**Lemma 2.2.14** *Let  $K$  be a 4-generator special 2-group of order  $2^9$  and conjugate type  $(1, 8)$ . Then  $K$  is isoclinic to  $G/M$ , where  $G = \langle a, b, c, d \rangle \in \hat{\mathcal{G}}_3$  is any fixed group and  $M < Z(G) = G'$  with  $|M| = 2$  is of the form*

$$M = \langle [a, b][c, d] \rangle.$$

The following lemma is analogous to Lemma 2.2.9 for  $p = 2$ , and therefore the proof is mostly a duplication of the the proof of Lemma 2.2.9 with necessary modifications.

**Lemma 2.2.15** *Let  $G = \langle a, b, c, d \rangle \in \hat{\mathcal{G}}_3$ . Then  $G/N$  with  $|N| = 4$  is of conjugate type  $(1, 8)$  if and only  $N$  can be reduced to the form*

$$N = \langle [a, b][c, d], [a, c][b, d][c, d] \rangle.$$

*Proof.* Notice that  $|G| = 2^{10}$  and  $|G'| = 2^6$ . Both  $G/Z(G)$  and  $G' = Z(G)$  are elementary abelian. Set  $\bar{G} = G/N$ ; then  $|\bar{G}| = 2^8$ . Since  $G$  is of conjugate type  $(1, 8)$  and  $|N| = 4$ , it follows that

$$Z(G)/N = Z(\bar{G}) = \bar{G}' = \Phi(\bar{G})$$

is an elementary abelian 2-group of order  $2^4$ . Thus  $[\bar{G} : Z(\bar{G})] = 2^4$ . Hence  $\bar{G}$  is of conjugate type  $(1, 8)$  if and only if each non-central element of  $\bar{G}$  commutes only with its own powers up to the central elements.

Let  $\bar{x}, \bar{y} \in \bar{G} \setminus Z(\bar{G})$  be such that no one is a power of the other (reading modulo  $Z(\bar{G})$ ). Then it is not difficult to see that  $[x, y] \neq 1$  in  $G$ . Hence, if  $[\bar{x}, \bar{y}] = 1$  in  $\bar{G}$ , then  $[x, y] \in N^\#$ . Any given central subgroup  $N_1$  of order 4,

without loss of generality, can be written as one of the following two types:

- (i)  $N_1 = \langle [a, b][a, d]^{i_1}[b, c]^{i_2}[b, d]^{i_3}[c, d]^{i_4}, [c, d] \rangle.$
- (ii)  $N_1 = \langle [a, b][a, d]^{i_1}[b, c]^{i_2}[b, d]^{i_3}[c, d]^{i_4}, [a, c][a, d]^{j_1}[b, c]^{j_2}[b, d]^{j_3}[c, d]^{j_4} \rangle.$

If  $N_1$  is of type (i), then  $\bar{c}$  commutes with  $\bar{d}$ , although  $\bar{c} \notin \langle Z(\bar{G}), \bar{d} \rangle$ . Hence  $\bar{G}$  can not be of conjugate type  $(1, p^3)$ . Therefore we only need to consider  $N_1$  as in type (ii). Now, as done in the proof of Lemma 2.2.9, we can reduce  $N_1$  to the form

$$N_2 = \langle [a, b][c, d], [a, c][b, d]^{i_1}[c, d]^{i_2} \rangle.$$

Here  $i_1$  can not be 0, else  $c$  will commute with  $ad^{-i_2}$ ; so  $i_1 = 1$ . Again  $i_2$  can not be 0, else  $ad^{-1}$  will commute with  $bc$ ; so  $i_2 = 1$ , and hence  $N_2 = \langle [a, b][c, d], [a, c][b, d][c, d] \rangle.$

Now consider  $x = a^{j_1}b^{j_2}c^{j_3}d^{j_4}$  and  $y = a^{k_1}b^{k_2}c^{k_3}d^{k_4}$  be such that none is power of the other (reading modulo  $Z(G)$ ). If  $[x, y] \in N_2^\#$ , then, on the lines of the proof of Lemma 2.2.9, it follows that  $[a, b][a, c]^k[b, d]^j[c, d]^{jk} \in N_2^\#$ , and therefore can be written as a product of powers of generators of  $N_2^\#$ .

Now comparing powers of the basic commutators, we get

$$j \equiv k \pmod{2} \text{ and } jk \equiv k + 1 \pmod{2}$$

Solving these we have

$$k^2 - k - 1 \equiv 0 \pmod{2}.$$

This is not possible. Hence no non-central element commutes with other ele-

---

ments except its power (modulo center) in  $G/N_2$  if and only if

$$N_2 = \langle [a, b][c, d], [a, c][b, d][c, d] \rangle.$$

This completes the proof. □

Now using Lemma 2.2.12, the preceding lemma gives

**Corollary 2.2.16** *Let  $K$  be a 4-generator special 2-group of order  $2^8$  and conjugate type  $(1, 8)$ . Then  $K$  is isoclinic to  $G/N$ , where  $G = \langle a, b, c, d \rangle \in \hat{\mathcal{G}}_3$  be any fixed group and  $N < Z(G) = G'$  with  $|N| = 4$  is of the form*

$$N = \langle [a, b][c, d], [a, c][b, d][c, d] \rangle.$$

We conclude this section with the following result which is valid only for odd primes.

**Lemma 2.2.17** *Every isoclinism family of finite  $p$ -groups of nilpotency class 2 and conjugate type  $(1, p^n)$  contains a group of exponent  $p$ , where  $p$  is an odd prime.*

*Proof.* Notice that the isoclinism family of a finite  $p$ -group  $G$  of nilpotency class 2 and conjugate type  $(1, p^n)$  contains a special  $p$ -group  $H$  (say). Then  $H$  has the following presentation:

$$H = \left\langle x_1, x_2, \dots, x_d : [x_i, x_j, x_k] = 1, [x_i, x_j]^p = 1, \right. \\ \left. x_i^p = \prod_{j < k} [x_j, x_k]^{c_{ijk}}, \prod_{j < k} [x_j, x_k]^{d_{ijk}} = 1 \right\rangle,$$

where  $c_{ijk}, d_{ijk} \in \mathbb{Z}$ . Let  $F/R$  be a free presentation of  $H$ , and  $R_1$  denote the subgroup of  $R$  which is the normal closure of  $\{[x_i, x_j, x_k], [x_i, x_j]^p, \prod_{j < k} [x_j, x_k]^{d_{ijk}}\}$

---

in  $F$ . Let  $\bar{F} := F/R_1$ . Then the group  $\bar{F}/\bar{F}^p$  lies in the isoclinism family of  $G$  and is of exponent  $p$ .  $\square$

## 2.3 Proof of Theorems 2.1.1 and 2.1.2

We are now ready to prove our main results (Theorems 2.1.1 and 2.1.2) of this chapter.

**Proof of Theorem 2.1.1** Let  $G$  be a finite  $p$ -group of conjugate type  $(1, p^3)$ ,  $p > 2$ . Then by Theorem 1.1.25,  $G$  can be of nilpotency class 2 or 3. Without loss of any generality, by Proposition 1.2.2, we can always assume that  $Z(G) \leq G'$ . First assume that  $G$  is of class 3. We are going to show that this case can not occur, and therefore  $G$  must have nilpotency class 2.

By Proposition 1.3.1,  $|Z(G)| \geq p^3$ . Since  $Z(G) < G'$ ; so  $|G'| \geq p^4$ . Then it follows from Lemma 2.2.1 that  $[G : Z(G)] = p^4$ . Since  $Z(G) < G'$ ; we have  $[G : G'] \leq p^3$ . But, if  $[G : G'] \leq p^2$ , then  $G$  can be minimally generated by at most 2 elements, which contradicts Proposition 1.3.1. Thus  $|G : G'| = p^3$  and minimal generating set for  $G$  has exactly 3 elements. Assume that  $G = \langle a, b, c \rangle$ .

Now we have  $[G : Z(G)] = p^4$  and  $[G : G'] = p^3$ . So, at least one of the three commutators  $[a, b]$ ,  $[a, c]$  and  $[b, c]$  lies outside center. By the symmetry, we can assume that  $[a, b] \in G' \setminus Z(G)$ . Set  $[a, b] = \alpha$ . Then clearly  $G' = \langle \alpha, Z(G) \rangle$ . So there exist integers  $i_1$  and  $i_2$  such that

$$[a, c] = [a, b]^{i_1} \beta_1, \text{ where } \beta_1 \in Z(G)$$

and

$$[b, c] = [a, b]^{i_2} \beta_2, \text{ where } \beta_2 \in Z(G).$$



Replacing  $c$  by  $a^{i_2}b^{-i_1}c$ , we get  $[a, c], [b, c] \in Z(G)$ . Then  $[\alpha, c] = 1$  (by Lemma 1.3.6). An arbitrary element of  $G$  can be written as  $g = a^{j_1}b^{j_2}c^{j_3}\alpha_1^{j_4}z$ ; where  $z \in G' = Z(G)$  and  $0 \leq j_k \leq p-1$  for  $k = 1, 2, 3, 4$ . Then

$$\alpha^G = \{(a^{j_1}b^{j_2})^{-1}\alpha a^{j_1}b^{j_2} \mid 0 \leq j_k \leq p-1, k = 1, 2\}.$$

Thus  $|\alpha^G| \leq p^2$ , which contradicts the fact that  $G$  is of conjugate type  $(1, p^3)$ . Hence the nilpotency class of  $G$  must be 2.

Now onward we assume that the nilpotency class of  $G$  is 2. Since  $Z(G) \leq G'$ , we have  $Z(G) = G'$ . By Corollary 1.1.23,  $G/Z(G)$  and  $G'$  are elementary abelian  $p$ -groups. So, finally we have  $Z(G) = G' = \Phi(G)$ . By Proposition 1.3.1 and Proposition 1.3.3, we have  $p^3 \leq |Z(G)| = |G'| \leq p^6$ . Thus, by Lemma 2.2.1, there can be two possibilities, namely

- (i)  $|G'| = p^3$  and  $[G : Z(G)] \geq p^4$  or
- (ii)  $|G'| \geq p^4$  and  $[G : Z(G)] = p^4$ .

In case (i),  $G$  is a Camina group with  $|G'| = p^3$ .

So it remains to consider case (ii) only. In this case, we have  $p^4 \leq |G'| = |Z(G)| \leq p^6$  and  $[G : Z(G)] = p^4 = [G : G'] = [G : \Phi(G)]$ . Thus  $G/\Phi(G)$  is an elementary abelian  $p$ -group of order  $p^4$ . Hence  $G$  is minimally generated by 4 elements. By Lemma 2.2.17 we can assume  $G$  to be of exponent  $p$  upto isoclinism. Thus  $G$  is isoclinic to  $G_3$  or to a central quotient  $G_3/H$ , where  $H$  is a non-trivial central subgroup of  $G_3$  with  $|H| \leq p^2$ . Hence the order of  $H$  is either  $p$  or  $p^2$ . Proof of the theorem is now complete by Corollary 2.2.8 and Lemma 2.2.11. □

Before proceeding to the proof of Theorem 2.1.2, we state the following result which is a consequence of the main result of Wilkens [29] stated on pages

---

203 – 204.

**Theorem 2.3.1** *Let  $G$  be a finite 2-group of nilpotency class 2 and conjugate type (1, 8). Then one of the following holds:*

(i)  $|G'| = 2^3$ .

(ii)  $[G : Z(G)] = 2^4$ .

(iii)  $|G'| = 2^4$  and there exists  $R$  with  $R \leq \Omega_1(Z(G))$  and  $|R| = 2$  such that  $|G/R : Z(G/R)| = 2^3$ .

(iv)  $|G'| = 2^4$  and  $G$  is central product  $HC_G(H)$ , where  $C_G(H)$  is abelian and  $H$  is the group given as follows:

There are  $i, j, k, l$  and  $m \in \mathbb{N}$  such that  $H \cong \tilde{H} / \langle x^{2i}, v^{2j}, v_1^{2k}, v_2^{2l}, v_3^{2m} \rangle$ , where  $\tilde{H} = \langle x, v, v_1, v_2, v_3 \rangle$  is of class 2 with  $\Phi(\tilde{H}) \leq Z(\tilde{H})$  and is otherwise defined by  $[v_2, x] = [v_1, v] = [v_3, x][v_3, v] = 1$ ,  $[v_i, v_j] \in \langle [v_3, x] \rangle$ .

We are now ready for the final proof.

**Proof of Theorem 2.1.2** Let  $\mathcal{G}$  be a finite 2-group of nilpotency class 2 and conjugate type (1, 8). Then  $\mathcal{G}$  is isomorphic to one of the groups  $G$  in (i), (ii), (iii) and (iv) of the preceding theorem. We are going to show that third and fourth possibilities can not occur. Suppose that (iii) occurs. Then  $|G'| = 2^4$  and there exists  $R$  with  $R \leq \Omega_1(Z(G))$  and  $|R| = 2$  such that  $|G/R : Z(G/R)| = 2^3$ . Since  $G$  is of conjugate type (1, 8) and  $|R| = 2$ , we have  $Z(G/R) = Z(G)/R$ . Then from the fact that  $|G/R : Z(G/R)| = 2^3$ , we get  $|G : Z(G)| = 2^3$ , which contradicts our hypothesis that  $G$  is of conjugate type (1, 8).

Next consider the case (iv)(5). So  $G \cong HC_G(H)$ , where  $\tilde{H}$  is a 2-group of class 2. It is easy to see that the conjugacy class of the image of  $v_3$  in  $H$  is of

---

length at most 2. Hence  $H$  is not of conjugate type  $(1, 8)$  and so is for  $G$ . So we are left with only two cases (i) and (ii).

In case (i),  $|G'| = 2^3$ , which forces  $\mathcal{G}$  to be isoclinic to a Camina 2-group with commutator subgroup of order 8.

Finally we consider the case (ii). For any group  $G$ , in this case, we have  $[G : Z(G)] = 2^4$ . Since  $G$  is of conjugate type  $(1, 8)$ , we have  $[G : C_G(x)] = 2^3$ , and consequently  $[C_G(x) : Z(G)] = 2$  for all  $x \in G \setminus Z(G)$ . Hence for all  $x \in G \setminus Z(G)$ ,  $x^2 \in Z(G)$ , i.e.,  $G/Z(G)$  is an elementary abelian 2-group. Thus  $G' \leq Z(G)$ , and therefore  $G$  is of class 2.

By Proposition 1.2.2 we can assume  $Z(G) = G'$ . By Proposition 1.3.3,  $|G'| = |Z(G)| \leq 2^6$ . Since,  $G$  being conjugate type  $(1, 8)$ ,  $|G'| \geq 2^3$ , it follows that  $2^7 \leq |G| = 2^{10}$ . Since  $G$  is of class 2, obviously  $G' = Z(G)$  is elementary abelian. Therefore the exponent of  $G$  is 4. If  $|G| = 2^7$ , then  $G$  is a Camina group, which is not possible by [17, Theorem 3.2]. Hence  $2^8 \leq |G| \leq 2^{10}$ , and therefore  $G$  must be isomorphic to some group  $T$  in the family  $\hat{\mathcal{G}}$  or its central quotient  $T/K$  with  $|K| \leq 4$ . Now the proof is complete by Lemmas 2.2.12, 2.2.14 and Corollary 2.2.16. □



# CHAPTER 3

## Finite $p$ -groups of nilpotency class 3 with two conjugacy class sizes

*In this chapter, we prove that “for a prime  $p > 2$  and an integer  $n \geq 1$ , finite  $p$ -groups of nilpotency class 3 and having only two conjugacy class sizes 1 and  $p^n$  exist if and only if  $n$  is even; moreover, for a given even positive integer, such a group is unique up to isoclinism.”*

### 3.1 Introduction

It has been known (from Corollary 1.1.24) that there does not exist 2-groups of conjugate rank 1 and nilpotency class 3. But very little was known about  $p$ -groups of conjugate rank 1 and nilpotency class 3, for odd primes  $p$ . Till now, we have learnt that

- (i) There is no finite  $p$ -group of nilpotency class 3 and of conjugate type  $(1, p)$

[Theorem 1.1.26],

- (ii) There is a unique group (up to isoclinism) of nilpotency class 3 and of conjugate type  $(1, p^2)$  [Theorem 1.1.27],
- (iii) There is no finite  $p$ -group of nilpotency class 3 and of conjugate type  $(1, p^3)$  [Theorem 2.1.1].

Apart from these, there are examples of  $p$ -group of nilpotency class 3 and of conjugate type  $(1, p^{2m})$  for all  $m \geq 1$ . These examples appeared in the construction of certain Camina  $p$ -groups of nilpotency class 3 by Dark and Scoppola (page 796-797, [4]). For a given integer  $m \geq 1$  and a prime  $p > 2$ , they constructed the following group,

$$\mathcal{H}_m = \left\{ \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ a & 1 & 0 & 0 & 0 \\ c & b & 1 & 0 & 0 \\ d & ab - c & a & 1 & 0 \\ f & e & c & b & 1 \end{bmatrix} : a, b, c, d, e, f \in \mathbb{F}_{p^m} \right\}, \quad (3.1)$$

where  $\mathbb{F}_{p^m}$  denotes the finite field with  $p^m$  elements. It is not difficult to see that  $\mathcal{H}_m/Z(\mathcal{H}_m)$  is of conjugate type  $(1, p^{2m})$  and class 3 (see Section 3.3 for more details). Also note that  $\mathcal{H}_1/Z(\mathcal{H}_1) \cong W$  (defined in (1.2)).

In view of the above example and observation, the following natural question arises.

**Question 3.1.1** *Does there exist a finite  $p$ -group of nilpotency class 3 and conjugate type  $(1, p^n)$ , for an odd prime  $p$  and odd integer  $n \geq 5$ ?*

**Question 3.1.2** *Are there other examples of finite  $p$ -groups of nilpotency class 3 and conjugate type  $(1, p^n)$ , for an odd prime  $p$  and even integer  $n$ , different*

from the one given in (3.1).

We answer these questions, by proving the following much general result, which is the main theorem of this chapter.

**Theorem 3.1.3** *Let  $p > 2$  be a prime and  $n \geq 1$  an integer. Then there exist finite  $p$ -groups of nilpotency class 3 and conjugate type  $(1, p^n)$  if and only if  $n$  is even. For each positive even integer  $n = 2m$ , every finite  $p$ -group of nilpotency class 3 and of conjugate type  $(1, p^n)$  is isoclinic to the group  $\mathcal{H}_m/Z(\mathcal{H}_m)$ , where  $\mathcal{H}_m$  is as in (3.1).*

In view of Corollary 1.1.24, Theorem 1.1.26 and Proposition 1.2.2, we only need to consider finite  $p$ -groups  $G$  satisfying the following conditions:

- (1)  $G$  is of nilpotency class 3 and conjugate type  $(1, p^n)$ ,  $n \geq 2$ .
- (2)  $Z(G) \leq G'$ .
- (3)  $p > 2$ .

For notational convenience, we set

**Hypothesis (A1).** We say that a finite  $p$ -group  $G$  satisfies *Hypothesis (A1)*, if (1)-(3) above hold for  $G$ .

## 3.2 Key results

In this section we determine some important invariants associated to a finite  $p$ -group satisfying Hypothesis (A1).

**Lemma 3.2.1** *Let  $G$  satisfy Hypothesis (A1). Then  $[G' : Z(G)] < p^n$ .*

---

*Proof.* Let  $[G : G'] = p^m$  for some integer  $m \geq 1$ . Since the nilpotency class of  $G$  is 3,  $G'$  is abelian. Hence by the given hypothesis, for any  $y \in G' \setminus Z(G)$ , we have

$$p^n = [G : \mathbb{C}_G(y)] \leq [G : G'] = p^m;$$

hence  $n \leq m$ .

Suppose that  $[G' : Z(G)] = p^k$  with  $n \leq k$ . We prove this lemma by the method of contradiction. Our plan is to count the cardinality of following set in two different ways:

$$X = \left\{ (\langle xG' \rangle, \langle yZ(G) \rangle) \mid x \in G \setminus G', y \in G' \setminus Z(G), [x, y] = 1 \right\}.$$

Note that  $X$  is well defined. For, if  $\langle xG' \rangle = \langle x_1G' \rangle$  and  $\langle yZ(G) \rangle = \langle y_1Z(G) \rangle$ , then  $x_1 = xh$  and  $y_1 = yz$  for some  $h \in G'$  and  $z \in Z(G)$  and thus  $[x_1, y_1] = [xh, yz] = [x, y][x, z][h, yz] = [x, y]$ . By Corollary 1.1.23  $G/Z(G)$  is of exponent  $p$ . As  $Z(G) < G'$ , we get

$$\exp(G/G') = \exp(G/Z(G)) = \exp(G'/Z(G)) = p.$$

Hence there are  $(p^k - 1)/(p - 1)$  subgroups of order  $p$  in  $G'/Z(G)$ . Fix some  $y_0 \in G' \setminus Z(G)$ . Since  $G'$  is abelian,  $G' \subseteq C_G(y_0)$  and  $[C_G(y_0) : G'] = p^{m-n}$ . As there are  $(p^{m-n} - 1)/(p - 1)$  subgroups of order  $p$  in  $C_G(y_0)/G'$ , we get

$$|X| = \left( \frac{p^k - 1}{p - 1} \right) \left( \frac{p^{m-n} - 1}{p - 1} \right) = \frac{(p^{m-n} - 1)(p^k - 1)}{(p - 1)^2}.$$

On the other hand, fix  $x_0 \in G \setminus G'$ . Set  $C_{G'}(x_0) := C_G(x_0) \cap G'$ . If  $p^n \leq [G' : C_{G'}(x_0)]$ , then there are at least  $p^n$  conjugates of  $x_0$  in  $G'$ . Thus, by the given hypothesis, there are exactly  $p^n$  conjugates of  $x_0$  in  $G'$ . Consequently we have

---



$$x_0^G = x_0^{G'}.$$

Let  $\{x_1, \dots, x_m\}$  be a minimal generating set of  $G$ . Then  $x_0^{x_i} = x_0^{h_i}$  for some  $h_i \in G'$ ; hence  $x_0^{x_i h_i^{-1}} = x_0$  for  $1 \leq i \leq m$ . Hence  $\{x_1 h_1^{-1}, \dots, x_m h_m^{-1}\}$  is also a generating set for  $G$ , which centralizes  $x_0$ , which implies that  $x_0 \in Z(G)$ , a contradiction. Thus  $[G' : C_{G'}(x_0)] \leq p^{n-1}$  and  $[C_{G'}(x_0) : Z(G)] \geq p^{k+1-n} \geq p$ . Consequently, there are at least  $(p^{k+1-n} - 1)/(p - 1)$  subgroups  $\langle y Z(G) \rangle$  of order  $p$  in  $G'/Z(G)$  with  $[x_0, y] = 1$ . Counting all together, we get

$$|X| \geq \frac{(p^m - 1)(p^{k+1-n} - 1)}{(p - 1)^2}.$$

Comparing the size of  $X$ , we get

$$(p^m - 1)(p^{k+1-n} - 1) \leq (p^{m-n} - 1)(p^k - 1),$$

which on simplification gives

$$p + p^{-k} + p^{n-m} \leq 1 + p^{1-m} + p^{n-k} < 3,$$

a contradiction on the choice of  $p$ . Hence  $[G' : Z(G)] < p^n$ . □

Before proceeding further, we recall the notion of relative breadth and some related terminology from [24].

**Definition 3.2.2 (Relative breadth)** *Let  $G$  be a finite  $p$ -group. For  $x \in G$  and an abelian normal subgroup  $A$  of  $G$ , the relative breadth of  $x$  with respect to  $A$  in  $G$  is denoted by  $b_A(x)$  and defined as*

$$p^{b_A(x)} = [A : C_A(x)].$$


---

We collect the following terminology from (page 52, [24]).

$$b_A(G) = \max\{b_A(x) \mid x \in G\}.$$

$$B_A(G) = \{x \in G \mid b_A(x) = b_A(G)\}.$$

For the ease of notation, we denote  $B_A(G)$  by  $B_A$ .

**Lemma 3.2.3** *Let  $G$  satisfy Hypothesis (A1). Then  $B_{G'} = \{x \in G \mid C_{G'}(x) = Z(G)\}$  and  $\langle B_{G'} \rangle = G$ .*

*Proof.* Let  $[G : G'] = p^m$  for some integer  $m$ . As in the proof of Lemma 3.2.1, we have  $m \geq n$ . Let  $[G' : Z(G)] = p^k$ . Then, by Lemma 3.2.1,  $k \leq n - 1$ .

Note that  $b_{G'}(G) \leq [G' : Z(G)] = p^k$ . So to show  $B_{G'} = \{x \in G \mid C_{G'}(x) = Z(G)\}$ , we need to show that there exist  $x \in G$  such that  $C_{G'}(x) = Z(G)$ . Define

$$T := \{x \in G \mid x \text{ commutes with some element } y \in G' \setminus Z(G)\}.$$

Note that  $T = \{x \in G \mid Z(G) < C_{G'}(x)\} = \cup C_G(h)$ , where union is taken over all subgroups  $\langle hG' \rangle$  of order  $p$  in  $G'/Z(G)$ . By Corollary 1.1.23,  $\exp(G/Z(G)) = p$ , and hence  $\exp(G'/Z(G)) = p$ . So there are  $\frac{(p^k-1)}{p-1}$  of subgroups order  $p$  in  $G'/Z(G)$ .

Fix some  $h_0 \in G' \setminus Z(G)$ . Since  $G$  is of nilpotency class 3,  $G'$  is abelian and  $G' \leq C_G(h_0)$ . As  $G$  is of conjugate type  $(1, p^n)$ , we have  $[G : C_G(h_0)] = p^n$  and therefore  $|C_G(h_0)| = |G'|p^{m-n}$ . This is true for all  $h_0 \in G' \setminus Z(G)$ . Thus,

$$|T| \leq |G'|p^{m-n}\frac{(p^k-1)}{p-1} < |G'|p^{m-n+k} \leq |G'|p^{m-1} < |G|.$$

Consequently,  $T$  is a proper subset of  $G$ , and therefore there exists an element

$x \in G \setminus G'$  such that  $C_{G'}(x) = Z(G)$ . Thus

$$B_{G'} = \{x \in G \mid C_{G'}(x) = Z(G)\} = G \setminus T.$$

If  $\langle B_{G'} \rangle = H < G$ , then  $|H| \leq |G'|p^{m-1}$ . Thus, since  $p$  is odd, we have

$$|G| = |T \cup B_{G'}| \leq |G'|p^{m-1} + |G'|p^{m-1} < |G'|p^m = |G|,$$

which is a contradiction. Hence  $\langle B_{G'} \rangle = G$ , which completes the proof.  $\square$

Now we compute the index of  $G'$  in  $G$  in the following lemma.

**Lemma 3.2.4** *If  $G$  satisfy Hypothesis (A1), then  $[G : G'] = p^n$ .*

*Proof.* For  $n = 2$ , the result is proved in Theorem 1.1.27. So we assume that  $n > 2$ . Since  $G'$  is abelian, it follows that  $[G : G'] \geq p^n$ . If  $[G : G'] = p^n$ , then there is nothing to prove. So assume that  $[G : G'] = p^{n+m}$  with  $m > 0$ . We now prove this lemma by the method of contradiction. Let  $[G' : Z(G)] = p^k$ , where  $k \leq n - 1$  (by Lemma 3.2.1). We complete the proof in several steps.

**Step 1.** *For all  $h \in G' \setminus Z(G)$ ,  $C_G(h) = C_G(G')$ .*

It follows from Lemma 3.2.3 that we can choose an element  $x_1 \in G$  such that

$$C_{G'}(x_1) = C_G(x_1) \cap G' = Z(G).$$

Let  $\{x_1, x_2, \dots, x_{m+k}, \dots, x_{m+n}\}$  be a minimal generating set for  $G$  such that  $C_G(x_1) = \langle x_1, x_2, \dots, x_{m+k}, Z(G) \rangle$ .

If  $\{[x_1, x_i] \mid m+k < i \leq m+n\} \subseteq Z(G)$ , then  $[x_1, x_i] \in Z(G)$  for all  $i$  with  $1 \leq i \leq m+n$ . By Lemma 1.3.6, we get  $[x_r, x_s] \in C_G(x_1) \cap G' = Z(G)$  for all  $r, s$  with  $1 \leq r, s \leq m+n$ . This implies  $G' \subseteq Z(G)$ , a contradiction. Thus there

---

exists at least one  $i$ ,  $m+k < i \leq m+n$  such that  $[x_1, x_i] \notin Z(G)$ . Without loss of generality, we can assume that  $[x_1, x_{m+n}] \notin Z(G)$ .

Now consider the following subgroup,

$$K = \langle [x_1, x_{m+n}], [x_2, x_{m+n}], \dots, [x_{m+k}, x_{m+n}], Z(G) \rangle.$$

Since  $[G' : Z(G)] = p^k$ , among the commutators  $[x_i, x_{m+n}]$ ,  $1 \leq i \leq m+k$ , at most  $k$  are independent over  $Z(G)$  (these can be viewed as elements of the vector space  $G'/Z(G)$ ). We can assume, without loss of generality, that for some integer  $l$  with  $1 \leq l \leq k$ ,  $[x_1, x_{m+n}], [x_2, x_{m+n}], \dots, [x_l, x_{m+n}]$  are independent elements modulo  $Z(G)$ , and generate  $K$  along with  $Z(G)$ . Now, we proceed to show that

$$l = k \quad \text{and} \quad K = G'.$$

For any  $t$  with  $l < t \leq m+k$ , we have

$$[x_t, x_{m+n}] \equiv [x_1, x_{m+n}]^{i_1} [x_2, x_{m+n}]^{i_2} \cdots [x_l, x_{m+n}]^{i_l} \pmod{Z(G)}.$$

Let  $x'_t = x_t x_1^{-i_1} \cdots x_l^{-i_l}$ . Then  $[x'_t, x_{m+n}] \in Z(G)$ . Thus, with  $C_G(x_1) = \langle x_1, x_2, \dots, x_{m+k}, Z(G) \rangle$ , we can assume, modifying  $x_t$  by  $x'_t$  (if necessary), that

$$[x_t, x_{m+n}] \in Z(G) \text{ for } l < t \leq m+k. \tag{3.2}$$

Note that, even after above modification ( $x_t$  by  $x'_t$ , for  $l < t \leq m+k$ , wherever necessary),  $[x_1, x_j] = 1$  and thus by Lemma 1.3.6, we get  $[x_i, x_j] \in C_G(x_1) \cap G' = Z(G)$ , for any  $i, j \leq m+k$ . In particular,  $[x_i, x_t] \in Z(G)$ , for  $1 \leq i \leq l$  and  $l < t \leq m+k$ . Consequently by (3.2) and Lemma 1.3.6,

$$[x_t, [x_i, x_{m+n}]] = 1 \quad (1 \leq i \leq l < t \leq m+k).$$

Thus for any  $i$  with  $1 \leq i \leq l$ ,  $\langle x_{l+1}, \dots, x_{m+k}, G' \rangle \leq C_G([x_i, x_{m+n}])$ ; so  $p^n = [G : C_G([x_i, x_{m+n}])] \leq p^{m+n-(m+k-l)} = p^{n-k+l} \leq p^n$ . Unless  $l = k$ , the last inequality is strict. Consequently, we get

(i)  $k = l$ ,

(ii)  $K = \langle [x_1, x_{m+n}], [x_2, x_{m+n}], \dots, [x_k, x_{m+n}], Z(G) \rangle = G'$ , and

(iii)  $C_G([x_i, x_{m+n}]) = \langle x_{k+1}, x_{k+2}, \dots, x_{k+m}, G' \rangle := H$  (say), for all  $i$ ,  $1 \leq i \leq k$ .

By (ii) and (iii), we get  $C_G(h) = H = C_G(G')$  for all  $h \in G' \setminus Z(G)$ . This completes the proof of Step 1.

Observe that, by Lemma 3.2.3,

$$G \setminus H = \{x \in G \mid C_{G'}(x) = Z(G)\} = B_{G'},$$

which implies that  $C_H(x) \cap G' = Z(G)$  for all  $x \in G \setminus H$ .

**Step 2.** For any  $y \in G \setminus H$ , there exist elements  $h_1, h_2, \dots, h_m \in G'$  such that

$$\langle x_{k+i}h_i \mid 1 \leq i \leq m \rangle Z(G) / Z(G) = (C_G(y) \cap H) / Z(G)$$

and

$$|(C_G(y) \cap H) / Z(G)| = p^m.$$

Let  $y \in G \setminus H$  be an arbitrary element. Then  $C_{G'}(y) = Z(G)$ . Consider a minimal generating set  $Y := \{y = y_1, y_2, \dots, y_{m+k}, \dots, y_{m+n}\}$  of  $G$  such that

---

$C_G(y_1) = \langle y_1, y_2, \dots, y_{m+k}, Z(G) \rangle$ . As in Step 1, we can modify (if necessary) the elements  $y_{k+1}, \dots, y_{m+k}$  so that

$$\langle y_{k+1}, y_{k+2}, \dots, y_{m+k}, G' \rangle = H = \langle x_{k+1}, x_{k+2}, \dots, x_{m+k}, G' \rangle.$$

Consequently, for  $1 \leq i \leq m$ , it follows that  $x_{k+i} = (\prod_{j=1}^m y_{k+j}^{a_{ij}}) h_i^{-1}$  for some integers  $a_{ij}$  and some element  $h_i \in G'$ . Hence  $x_{k+i} h_i \in C_G(y)$ , which shows that

$$\langle x_{k+i} h_i \mid 1 \leq i \leq m \rangle Z(G) / Z(G) \leq (C_G(y) \cap H) / Z(G). \quad (3.3)$$

Note that for  $1 \leq i, j \leq m$ ,  $[x_{k+i} h_i, x_{k+j} h_j] \in Z(G)$ . Thus

$$|\langle x_{k+i} h_i \mid 1 \leq i \leq m \rangle Z(G) / Z(G)| = p^m. \quad (3.4)$$

By the vary choice of  $y_{k+1}, \dots, y_{m+k}$ , it follows that

$$\langle y_{k+1}, \dots, y_{k+m}, Z(G) \rangle = C_G(y) \cap H;$$

hence  $|(C_G(y) \cap H) / Z(G)| = p^m$ . This, along with (3.3) and (3.4), proves Step 2.

**Step 3.** *The cardinality of*

$$S := \left\{ (\langle x Z(G) \rangle, \langle y Z(G) \rangle) \mid x \in G \setminus H, y \in H \setminus G', [x, y] = 1 \right\}$$

is  $p^{m+k}(p^n - 1)(p^m - 1)/(p - 1)^2$ .

Since the exponent of  $G/Z(G)$  is  $p$ , it follows that  $G/Z(G)$ ,  $H/Z(G)$  and  $G'/Z(G)$  have  $(p^{n+m+k} - 1)/(p - 1)$ ,  $(p^{m+k} - 1)/(p - 1)$  and  $(p^k - 1)/(p - 1)$

number of subgroups of order  $p$  respectively. Consequently

$$|\{\langle xZ(G) \rangle \mid x \in G \setminus H\}| = \frac{p^{m+k}(p^n - 1)}{p - 1} \quad (3.5)$$

and

$$|\{\langle yZ(G) \rangle \mid y \in H \setminus G'\}| = \frac{p^k(p^m - 1)}{p - 1}. \quad (3.6)$$

For each  $x \in G \setminus H$ , by Step 2, we have  $|(\mathbb{C}_G(x) \cap H)/Z(G)| = p^m$ ; hence

$$|\{\langle yZ(G) \rangle \mid y \in H \setminus G', [x, y] = 1\}| = \frac{p^m - 1}{p - 1}. \quad (3.7)$$

Hence, by (3.5) and (3.7), we have

$$|S| = \frac{p^{m+k}(p^n - 1)(p^m - 1)}{(p - 1)^2}, \quad (3.8)$$

and the proof of Step 3 is complete.

**Step 4.** *In this step, we proceed to get the final contradiction.*

Note that there exists some element  $y_0 \in H \setminus G'$  such that

$$|\{\langle xZ(G) \rangle \mid x \in G \setminus H, [x, y_0] = 1\}| \geq \frac{p^m(p^n - 1)}{p - 1}. \quad (3.9)$$

For, if there is no such  $y_0$ , then for each  $y \in H \setminus G'$ , we get

$$|\{\langle xZ(G) \rangle \mid x \in G \setminus H, [x, y] = 1\}| < \frac{p^m(p^n - 1)}{p - 1}.$$

But then

$$|S| < \frac{p^{m+k}(p^n - 1)(p^m - 1)}{(p - 1)^2},$$

which is absurd.

---

Note that;

$$(i) \quad G' \leq \mathbb{C}_G(y_0) \text{ and } [C_G(y_0) : G'] = p^m.$$

$$(ii) \quad |G/H| = p^n \text{ and } |H/G'| = p^m.$$

$$(iii) \quad |\mathbb{C}_G(y_0)H/H| |\mathbb{C}_H(y_0)/G'| = [C_G(y_0) : G'] = p^m.$$

Assume that  $|\mathbb{C}_G(y_0)H/H| = p^{n-s}$  and  $|\mathbb{C}_H(y_0)/G'| = p^{m-r}$ , for some integers  $s$  and  $r$ . From (iii) it follows that  $n = s + r$ . Then

$$|\mathbb{C}_H(y_0)/Z(G)| = p^{k+(m-r)} \text{ and } |\mathbb{C}_G(y_0)/Z(G)| = p^{k+m}.$$

Thus

$$\begin{aligned} |\{\langle xZ(G) \rangle \mid x \in G \setminus H, [x, y_0] = 1\}| &= \frac{(p^{k+m} - 1) - (p^{k+m-r} - 1)}{p - 1} \\ &= \frac{p^{m+k-r}(p^{n-s} - 1)}{p - 1}. \end{aligned}$$

The preceding equation along with (3.9) gives

$$p^m(p^n - 1)/(p - 1) \leq p^{m+k-r}(p^{n-s} - 1)/(p - 1).$$

Since  $n = r + s$ , after simplification, the preceding inequality gives

$$p^n - 1 \leq p^{k-r}(p^{n-s} - 1) = p^k - p^{k-r}.$$

Hence, by Lemma 3.2.1,

$$p^n \leq p^k + 1 \leq p^{n-1} + 1.$$

which is absurd. Hence the proof is complete.  $\square$



As an immediate consequence of the preceding lemma, we get the following important information about centralizers of elements in  $G$ , which we use frequently without any further reference.

**Corollary 3.2.5** *If  $G$  satisfies Hypothesis (A1), then for all  $h \in G' \setminus Z(G)$  and  $x \in G \setminus G'$  the following hold:*

(i)  $C_G(h) = G'$ .

(ii)  $C_G(x) \cap G' = Z(G)$ .

(iii)  $[C_G(x) : Z(G)] = [G' : Z(G)] = p^n$ .

**Theorem 3.2.6** *Let  $G$  satisfy Hypothesis (A1). If  $[G' : Z(G)] = p^m$ , then  $n = 2m$ .*

*Proof.* Consider  $x, y \in G$  such that  $[x, y] \notin Z(G)$ . We consider two cases, namely (1)  $n > 2m$  and (2)  $n < 2m$ , and get contradiction in both.

**Case 1.**  $n > 2m$

Write  $\bar{G} = G/Z(G)$ . Note that

(i)  $\bar{G}$  is of order  $p^{m+n}$  and nilpotency class 2.

(ii)  $\bar{G}' = Z(\bar{G}) = G'/Z(G)$ , and are of order  $p^m$ .

So, we get

$$[\bar{G} : C_{\bar{G}}(\bar{x})] \leq p^m \quad \text{and} \quad [\bar{G} : C_{\bar{G}}(\bar{y})] \leq p^m.$$

Consequently

$$[C_{\bar{G}}(\bar{x}) : Z(\bar{G})] \geq p^{n-m} \leq [C_{\bar{G}}(\bar{y}) : Z(\bar{G})].$$

Since  $[\bar{G} : Z(\bar{G})] = p^n < p^{2(n-m)}$ , there exists  $\bar{w} \in (C_{\bar{G}}(\bar{x}) \cap C_{\bar{G}}(\bar{y})) \setminus Z(\bar{G})$ , i.e.,  $[x, w], [y, w] \in Z(G)$  with  $w \notin G'$ . By Lemma 1.3.6,  $[x, y] \in C_G(w) \cap G' = Z(G)$ , a contradiction to our supposition that  $[x, y] \notin Z(G)$ .

---

**Case 2.**  $n < 2m$ .

Since  $G$  is of nilpotency class 3 and  $[x, y] \notin Z(G)$ , both  $x$ , and  $y$  can not lie in  $G'$ . By Corollary 3.2.5,  $C_G(x) \cap G' = Z(G) = C_G(y) \cap G'$ . Thus, we get

$$[C_G(x)G' : G'] = [C_G(x) : C_G(x) \cap G'] = [C_G(x) : Z(G)] = p^m,$$

and similarly  $[C_G(y)G' : G'] = p^m$ . Since  $2m > n$ , we have  $[G : G'] = p^n < p^{2m}$ . Hence  $C_G(x)G' \cap C_G(y)G'$  contains  $G'$  properly. Consider  $w \in (C_G(x)G' \cap C_G(y)G') \setminus G'$ . As  $G$  is of nilpotency class 3, it is easy to see that  $[w, x], [w, y] \in Z(G)$ . Thus by Lemma 1.3.6,  $[x, y] \in C_G(w) \cap G' = Z(G)$ , a contradiction again. Hence  $n = 2m$ , and the proof is complete.  $\square$

Before proceeding further, we strengthen Hypothesis (A1) as follows:

**Hypothesis (A2).** We say that a finite  $p$ -group  $G$  satisfies *Hypothesis (A2)*, if  $G$  is of nilpotency class 3 and of conjugate type  $(1, p^{2m})$  with  $Z(G) \leq G'$ .

Now we recall the following result of Verardi [28] (also see [Lemma 1.2, [18]]), which we need for determining the structure of  $G/Z(G)$  when  $G$  satisfies Hypothesis (A2).

**Theorem 3.2.7** [18, Lemma 1.2] *For an odd prime  $p$ , let  $G$  be a Camina  $p$ -group of order  $p^{3m}$ , of exponent  $p$  and of nilpotency class 2. Let  $[G : G'] = p^{2m}$  and there are two elementary abelian subgroups  $A^*, B^*$  of  $G$  such that  $G = A^*B^*$ ,  $A^* = A \times G'$ ,  $B^* = B \times G'$ , and thus  $G = ABG'$ . Then the following statements are equivalent:*

1.  $G$  is isomorphic to  $U_3(p^m)$ .
2. All the centralizers of non-central elements of  $G$  are abelian.

**Theorem 3.2.8** *Let  $G$  satisfy Hypothesis (A2). Write  $\overline{G} = G/Z(G)$  and  $\overline{x} = xZ(G)$  for  $x \in G$ . Then the following hold:*

(i)  $\overline{C_G(x)G'} = C_{\overline{G}}(\overline{x})$  and  $|C_{\overline{G}}(\overline{x})| = p^{2m}$  for  $x \in G \setminus G'$ .

(ii)  $\overline{G}$  is a Camina  $p$ -group of order  $p^{3m}$ , exponent  $p$ , and  $|\overline{G}'| = p^m$ .

(iii) All the centralizers of non-central elements in  $\overline{G}$  are elementary abelian of order  $p^{2m}$ .

(iv) If  $A = C_{\overline{G}}(\overline{x})$  and  $B = C_{\overline{G}}(\overline{y})$  for  $\overline{x}, \overline{y} \notin Z(\overline{G})$  are distinct centralizers in  $\overline{G}$ , then  $A \cap B = Z(\overline{G})$  and  $\overline{G} = AB$ .

(v)  $\overline{G}$  is isomorphic to  $U_3(p^m)$ .

*Proof.* (i) By Lemma 3.2.4 and Theorem 3.2.6, we have  $[G : G'] = p^{2m}$  and  $[G' : Z(G)] = p^m$ ; hence

$$|\overline{G}| = p^{3m} \quad \text{and} \quad |\overline{G}'| = p^m.$$

Further, for  $h \in G' \setminus Z(G)$ ,  $C_G(h) = G'$ , by Corollary 3.2.5.

Fix  $x \in G \setminus G'$ . Since  $\overline{G}$  is of nilpotency class 2,  $\overline{G}'$  is contained in the centralizer of every element in  $\overline{G}$ . Hence  $\overline{C_G(x)G'} \leq C_{\overline{G}}(\overline{x})$ . By Corollary 3.2.5,  $[C_G(x) : Z(G)] = [G' : Z(G)] = p^m$  with  $C_G(x) \cap G' = Z(G)$ . So, we get,  $[C_G(x)G' : Z(G)] = p^{2m}$  and  $[G : C_G(x)G'] = p^m$ . Hence

$$|C_{\overline{G}}(\overline{x})| \geq p^{2m} \quad \text{and} \quad [\overline{G} : C_{\overline{G}}(\overline{x})] \leq p^m.$$

If possible, suppose that  $|C_{\overline{G}}(\overline{x})| > p^{2m}$ , that is,  $[\overline{G} : C_{\overline{G}}(\overline{x})] < p^m$ . Note that  $\overline{x} \notin Z(\overline{G})$ . For, let  $\overline{x} \in Z(\overline{G})$ . For any minimal generating set  $\{x_1, \dots, x_{2m}\}$  of  $G$ ,  $\{\overline{x}_1, \dots, \overline{x}_{2m}\}$  is also a minimal generating set for  $\overline{G}$ . Then  $[\overline{x}, \overline{x}_i] = 1$ , that is

---

$[x, x_i] \in Z(G)$  for  $1 \leq i \leq 2m$ . Then by Lemma 1.3.6, for  $1 \leq i \leq 2m$ ,  $[x_i, x_j] \in C_G(x) \cap G' = Z(G)$  (by Corollary 3.2.5); hence  $G' \subseteq Z(G)$ , a contradiction.

Then there exists  $t \in G$  such that  $[t, x] \notin Z(G)$ . Since  $|\overline{G}'| = p^m$ , we have  $|\overline{G} : C_{\overline{G}}(\bar{t})| \leq p^m$ , and therefore it follows that  $C_{\overline{G}}(\bar{x}) \cap C_{\overline{G}}(\bar{t})$  contains  $\overline{G}'$  properly. Take  $\bar{w} \in C_{\overline{G}}(\bar{x}) \cap C_{\overline{G}}(\bar{t}) \setminus \overline{G}'$ . Then  $[w, x], [w, t] \in Z(G)$  with  $w \notin G'$ . By Lemma 1.3.6,  $[x, t] \in C_G(w) \cap G' = Z(G)$ , a contradiction. Thus  $|C_{\overline{G}}(\bar{x})| = p^{2m} = |\overline{C_G(x)G'}|$ . This proves assertion (i).

(ii) By Corollary 1.1.23,  $\exp(\overline{G}) = p$ . Now the assertion (ii) follows from assertion (i).

(iii) Consider any  $x \in G \setminus G'$ . For  $y_1, y_2 \in \mathbb{C}_G(x)$ , by Lemma 1.3.6,  $[y_1, y_2] \in \mathbb{C}_G(x) \cap G' = Z(G)$ . Hence  $[\mathbb{C}_G(x), \mathbb{C}_G(x)] \leq Z(G)$ . Since  $G$  is of nilpotency class 3, we have

$$[C_G(x)G', C_G(x)G'] = [C_G(x), C_G(x)][C_G(x), G'][G', G'] \leq Z(G),$$

i.e.,  $C_{\overline{G}}(\bar{x}) = \overline{C_G(x)G'}$  is abelian. Since  $\overline{G}$  is of exponent  $p$ , then so is  $C_{\overline{G}}(\bar{x})$ . This completes the proof of (iii).

(iv) It is given that  $A = C_{\overline{G}}(\bar{x})$  and  $B = C_{\overline{G}}(\bar{y})$  are distinct proper subgroups of  $\overline{G}$ , and are abelian by assertion (iii). Thus for any element  $\bar{w} \in A \cap B$ , it follows that  $|C_{\overline{G}}(\bar{w})| \geq |AB| > p^{2m}$ . Hence, by (iii),  $\bar{w} \in Z(\overline{G})$ . Since  $|\overline{G}| = p^{3m}$ ,  $|Z(\overline{G})| = p^m$  and  $|A| = |B| = p^{2m}$ , we have  $\overline{G} = AB$ .

(v) The assertion follows by (ii)-(iv) along with Theorem 3.2.7.  $\square$

**Corollary 3.2.9** *Let  $G$  satisfy Hypothesis (A2) and  $x, y \in G \setminus G'$  such that  $[x, y] \in Z(G)$ . Then there exists an element  $h \in G'$  such that  $[x, yh] = 1$ .*

*Proof.* Let  $\overline{G} = G/Z(G)$ . As  $[x, y] \in Z(G)$ ,  $\bar{y} \in C_{\overline{G}}(\bar{x}) = \overline{C_G(x)G'}$  (by Theorem 3.2.8). Thus, we get  $y = x_0 h' z$ , for some  $x_0 \in C_G(x)$ ,  $h' \in G'$  and  $z \in Z(G)$ .

Putting  $h = (h'z)^{-1} \in G'$ , we get that  $x_0 = yh \in C_G(x)$ . This completes the proof.  $\square$

**Lemma 3.2.10** *Let  $G$  satisfy Hypothesis (A2). Then  $Z(G) = \gamma_3(G)$ , and is elementary abelian of order  $p^{2m}$ .*

*Proof.* Since  $G'$  is elementary abelian (by Corollary 1.1.23), so are  $\gamma_3(G)$  and  $Z(G)$ . Consider  $x_1 \in G \setminus G'$ . Recall that  $[G : G'] = p^{2m}$ ,  $C_G(x_1) \cap G' = Z(G)$ , and  $[C_G(x_1) : Z(G)] = [G' : Z(G)] = p^m$ . Consider  $y_1 \in G \setminus C_G(x_1)G'$ . Let

$$C_G(x_1) = \langle x_1, \dots, x_m, Z(G) \rangle = A$$

and

$$C_G(y_1) = \langle y_1, \dots, y_m, Z(G) \rangle = B.$$

Then  $C_{\overline{G}}(\overline{x}_1) = \langle \overline{x}_1, \dots, \overline{x}_m, \overline{G}' \rangle = \overline{A}$  and  $C_{\overline{G}}(\overline{y}_1) = \langle \overline{y}_1, \dots, \overline{y}_m, \overline{G}' \rangle = \overline{B}$  are distinct proper subgroups of  $\overline{G}$ . Hence, by Theorem 3.2.8(iv), they generate  $\overline{G}$ . It follows that  $\{x_1, \dots, x_m, y_1, \dots, y_m\}$  is a (minimal) generating set for  $G$ . Define

$$[x_1, y_i] = h_i, \quad 1 \leq i \leq m.$$

By Theorem 3.2.8(ii),  $h_1, \dots, h_m$  are independent modulo  $Z(G)$ , and  $G' = \langle h_1, \dots, h_m, Z(G) \rangle$ . Since  $x_1, \dots, x_m, y_1, \dots, y_m$  are independent modulo  $G' = C_G(h_1)$ , it follows that  $[h_1, x_1], \dots, [h_1, x_m], [h_1, y_1], \dots, [h_1, y_m]$  are independent, and they generate a subgroup  $K$  of order  $p^{2m}$  in  $\gamma_3(G)$ . Define

$$[h_1, x_i] = z_i, \quad \text{and} \quad [h_1, y_i] = z_{m+i}, \quad 1 \leq i \leq m.$$

Now, we proceed to show that  $K = \langle z_1, \dots, z_{2m} \rangle = \gamma_3(G)$ . It is sufficient to show that for any  $h \in G' \setminus Z(G)$ ,  $[h, x_i], [h, y_i] \in K$  for  $1 \leq i \leq m$ .

---

For any  $h \in G' \setminus Z(G)$  and fixed  $i$  with  $1 \leq i \leq m$ , consider  $[h, x_i]$ . Since  $\langle [x_1, y_1], \dots, [x_1, y_m], Z(G) \rangle = G'$ , there exists  $y \in B$  such that  $h \equiv [x_1, y] \pmod{Z(G)}$ . Then by Lemma 1.3.7, we have

$$[h, x_i] = [[x_1, y], x_i] = [[x_i, y], x_1].$$

Again, since  $\langle [x_1, y_1], \dots, [x_m, y_1], Z(G) \rangle = G'$ , there exists  $x \in A$  such that  $[x_i, y] \equiv [x, y_1] \pmod{Z(G)}$ . Therefore, again by Lemma 1.3.7, we get

$$[h, x_i] = [[x_i, y], x_1] = [[x, y_1], x_1] = [[x_1, y_1], x] = [h_1, x] \in K.$$

Similarly we can show that  $[h, y_i] \in K$ ,  $1 \leq i \leq m$ ; hence  $K = \gamma_3(G)$  and is of order  $p^{2m}$ .

It only remains to show that  $Z(G) = \gamma_3(G)$ . For this, since  $[x_1, y_1], \dots, [x_1, y_m]$  are independent modulo  $Z(G)$  and  $G' = \langle [x_1, y_1], \dots, [x_1, y_m], Z(G) \rangle$ , it suffices to prove that

$$G' = \langle [x_1, y_1], \dots, [x_1, y_m], \gamma_3(G) \rangle. \quad (3.10)$$

Note that  $\gamma_3(G) = \langle z_1, \dots, z_{2m} \rangle \subseteq Z(G)$ . If (3.10) does not hold, then there exist  $z \in Z(G) \setminus \gamma_3(G)$  and a commutator  $[x_i, y_j]$  for some  $i, j$  with  $1 \leq i, j \leq m$ , such that

$$[x_i, y_j] = [x_1, y_1]^{e_1} \cdots [x_1, y_m]^{e_m} z,$$

where  $e_i \in \mathbb{F}_p$ , for  $1 \leq i \leq m$ . Let  $y = y_1^{e_1} \cdots y_m^{e_m}$ . Then the preceding equation implies

$$[x_i, y_j] \equiv [x_1, y] z \pmod{\gamma_3(G)}. \quad (3.11)$$

Consequently  $[x_i, y_j] \equiv [x_1, y] \pmod{Z(G)}$ . Since  $[x_1, x_i] \equiv [y, y_j] \equiv 1 \pmod{Z(G)}$ , it follows that  $[x_1 y_j, x_i y] \equiv [x_1, y][y_j, x_i] \equiv 1 \pmod{Z(G)}$ .

Hence, by Corollary 3.2.9, there exists  $h \in G'$  such that  $[x_1y_j, x_iyh] = 1$ . Since  $G/\gamma_3(G)$  is of nilpotency class 2, using (3.11), we get

$$\begin{aligned} 1 = [x_1y_j, x_iyh] &\equiv [x_1, x_i][x_1, y][x_i, y_j]^{-1}[y_j, y] \pmod{\gamma_3(G)} \\ &\equiv z^{-1}[y_j, y] \pmod{\gamma_3(G)}. \end{aligned}$$

Since  $y_j, y \in \mathbb{C}_G(y_1)$ , we have  $\bar{y}_j, \bar{y} \in \mathbb{C}_{\bar{G}}(\bar{y}_1)$ , which is abelian by Theorem 3.2.8(iii); hence  $[\bar{y}_j, \bar{y}] = 1$ , i.e.,  $[y_j, y] \in Z(G)$ . Again by Corollary 3.2.9, there exists  $h_1 \in G'$  such that  $[y_j, yh_1] = 1$ . Then  $[y_j, y] = [y_j, h_1]^{-1} \in \gamma_3(G)$ . Thus, we get

$$1 \equiv z^{-1} \pmod{\gamma_3(G)}, \quad \text{a contradiction.}$$

This proves that (3.10) holds. Hence the proof is complete. □

### 3.3 Examples

In this section, we describe the examples of  $p$ -groups of conjugate type  $(1, p^{2m})$  and class 3, from the construction by Dark and Scoppola [4].

For an odd prime  $p$  and an integer  $m \geq 1$ , let  $q = p^m$  and  $\mathbb{F}_q$  denote the field of order  $q$ . Consider the set  $\mathcal{G}$  of quintuples  $(a, b, c, d, e)$  over  $\mathbb{F}_q$ . Define an operation ‘.’ on  $\mathcal{G}$  as follows. For any two quintuples  $(a, b, c, d, e)$  and  $(x, y, z, u, v)$ , define  $(a, b, c, d, e).(x, y, z, u, v)$  to be the quintuple

$$(a + x, b + y, c + z + bx, d + u + az + (ab - c)x, e + v + cy + b(xy - z)).$$

A routine check shows that  $\mathcal{G}$  is a group under this operation, with identity

---

element  $(0, 0, 0, 0, 0)$ , which we denote by  $\mathbf{0}$ , and

$$(a, b, c, d, e)^{-1} = (-a, -b, -c + ab, -d, -e).$$

Then  $(a, b, c, d, e).(x, y, z, u, v).(a, b, c, d, e)^{-1}.(x, y, z, u, v)^{-1}$  is the quintuple

$$(0, 0, bx - ay, 2az - 2cx + a^2y - bx^2, 2(c - ab)y - 2b(z - xy) - ay^2 + b^2x).$$

It is easy to see that

1.  $\mathcal{G}' = \{(0, 0, c, d, e) \mid c, d, e \in \mathbb{F}_q\}$ .
2.  $\gamma_3(\mathcal{G}) = \{(0, 0, 0, d, e) \mid d, e \in \mathbb{F}_q\} = Z(\mathcal{G})$ .

Consider  $(0, 0, c, d, e) \in \mathcal{G}' \setminus Z(\mathcal{G})$ . Then  $c \neq 0$ . If

$$[(0, 0, c, d, e), (x, y, z, u, v)] = \mathbf{0},$$

then by the commutator formula above,  $-2cx = 2cy = 0$ . Since characteristic of  $\mathbb{F}_q$  is odd and  $c \neq 0$ ,  $x = y = 0$ . Noting that  $\mathcal{G}'$  is abelian, it follows that the centralizer of any element of  $\mathcal{G}' \setminus Z(\mathcal{G})$  is  $\mathcal{G}'$ , which has index  $q^2 = p^{2m}$  in  $\mathcal{G}$ .

Next fix  $g = (a, b, c, d, e)$  with  $(a, b) \neq (0, 0)$ . Then  $(x, y, z, u, v)$  centralizes  $g$  if and only if

$$bx - ay = 0, \tag{3.12}$$

$$2az - 2cx + a^2y - bx^2 = 0, \tag{3.13}$$

$$2(c - ab)y - 2b(z - xy) - ay^2 + b^2x = 0. \tag{3.14}$$

Suppose  $a \neq 0$ . For arbitrary  $x, u, v \in \mathbb{F}_q$ , we see that  $y$  is uniquely determined from (3.12) and then  $z$  is uniquely determined from (3.13). Further the values



of  $y, z$  obtained satisfy (3.14). Hence the centralizer of  $(a, b, c, d, e)$  has order  $q^3 = p^{3m}$ , and therefore has index  $p^{2m}$  in  $\mathcal{G}$ . Similarly, if  $a = 0$  and  $b \neq 0$ , then it follows that the centralizer of  $(a, b, c, d, e)$  in  $\mathcal{G}$  has index  $p^{2m}$ . Hence  $\mathcal{G}$  is of conjugate type  $(1, p^{2m})$ .

We show that the group  $\mathcal{G}$  has a nice description in terms of a matrix group over  $\mathbb{F}_q$ . Consider the following collection of unitriangular matrices over  $\mathbb{F}_q$ :

$$\mathcal{H}_m = \left\{ \begin{bmatrix} 1 & & & & \\ a & 1 & & & \\ c & b & 1 & & \\ d & ab - c & a & 1 & \\ f & e & c & b & 1 \end{bmatrix} : a, b, c, d, e, f \in \mathbb{F}_q \right\}.$$

It is easy to see that  $\mathcal{H}_m$  is a *subgroup* of  $U_5(q)$ . Denote the general element of  $\mathcal{H}_m$  by  $(a, b, c, d, e, f)$ . An easy computation shows that  $Z(\mathcal{H}_m) = \{(0, 0, 0, 0, 0, f) \mid f \in \mathbb{F}_q\}$ . Therefore, we have a natural homomorphism  $\mathcal{H}_m \rightarrow \mathcal{H}_m/Z(\mathcal{H}_m)$ , in which we identify

$$(a, b, c, d, e, f)Z(\mathcal{H}_m) \longleftrightarrow (a, b, c, d, e).$$

Then one can check that the product  $(a, b, c, d, e)(x, y, z, u, v)$  in  $\mathcal{H}_m/Z(\mathcal{H}_m)$  is the same as  $(a, b, c, d, e).(x, y, z, u, v)$  in  $\mathcal{G}$ . Hence  $\mathcal{H}_m/Z(\mathcal{H}_m)$  is isomorphic to  $\mathcal{G}$ , and therefore is of conjugate type  $(1, p^{2m})$  and class 3.

As a conclusion of the preceding discussion, we obtain

**Lemma 3.3.1** *For any even integer  $n \geq 1$  and an odd prime  $p$ , there exists a finite  $p$ -group of nilpotency class 3 and of conjugate type  $(1, p^n)$ .*

---

### 3.4 Proof of Main Theorem [Theorem 3.1.3]

Let  $G$  be a  $p$ -group of nilpotency class 3 such that  $G/Z(G)$  is isomorphic to the group  $U_3(p^m)$ . Our strategy for proving the theorem is to obtain presentations of groups  $G$  satisfying Hypothesis (A2) from a presentation of  $U_3(p^m)$ ; then we proceed to show that the groups, given by the presentations obtained, belong to the same isoclinism family.

We start with finding some structure constants of  $U_3(p^m)$ . Let  $\mathbb{F}_{p^m}$  denote the field of order  $p^m$ . Then  $\mathbb{F}_{p^m} = \mathbb{F}_p(\alpha)$ , where  $\alpha$  satisfies a monic irreducible polynomial of degree  $m$  over  $\mathbb{F}_p$ . Consider the following matrices in  $U_3(p^m)$  for any integer  $i \geq 1$ :

$$X_i = \begin{bmatrix} 1 & & \\ 0 & 1 & \\ 0 & \alpha^{i-1} & 1 \end{bmatrix}, \quad Y_i = \begin{bmatrix} 1 & & \\ \alpha^{i-1} & 1 & \\ 0 & 0 & 1 \end{bmatrix}, \quad H_i = \begin{bmatrix} 1 & & \\ 0 & 1 & \\ \alpha^{i-1} & 0 & 1 \end{bmatrix}.$$

Then it is easy to see that  $\{X_1, \dots, X_m, Y_1, \dots, Y_m\}$  is a minimal generating set for  $U_3(p^m)$  and  $\{H_1, \dots, H_m\}$  is a minimal generating set for the center (which is also equal to the commutator subgroup) of  $U_3(p^m)$ . Further, these matrices satisfy the following relations.

$$X_i^p = Y_i^p = H_i^p = 1, \tag{3.15}$$

$$[X_i, X_j] = [Y_i, Y_j] = 1, \tag{3.16}$$

$$[H_i, X_j] = [H_i, Y_j] = 1, \tag{3.17}$$

$$[X_i, Y_j] = H_{i+j-1} \text{ for all } i, j \geq 1. \tag{3.18}$$

Since  $\mathbb{F}_p(\alpha)$  is a vector space over  $\mathbb{F}_p$  with basis  $(1, \alpha, \dots, \alpha^{m-1})$ , for  $\alpha^{i+j-2} \in$

---

$\mathbb{F}_p(\alpha)$ , there exist unique  $\kappa_{i,j,1}, \dots, \kappa_{i,j,m} \in \mathbb{F}_p$  such that

$$\alpha^{i+j-2} = \kappa_{i,j,1} + \kappa_{i,j,2} \alpha + \dots + \kappa_{i,j,m} \alpha^{m-1}.$$

Then, by (3.18), we have

$$H_{i+j-1} = H_1^{\kappa_{i,j,1}} H_2^{\kappa_{i,j,2}} \dots H_m^{\kappa_{i,j,m}} = [X_1, Y_1^{\kappa_{i,j,1}} Y_2^{\kappa_{i,j,2}} \dots Y_m^{\kappa_{i,j,m}}],$$

which in turn implies that

$$[X_i, Y_j] = [X_1, Y_1^{\kappa_{i,j,1}} Y_2^{\kappa_{i,j,2}} \dots Y_m^{\kappa_{i,j,m}}], \quad 1 \leq i, j \leq m. \quad (3.19)$$

The constants  $\kappa_{i,j,l}$  for  $1 \leq i, j, l \leq m$ , which we call *the structure constants* of  $U_3(p^m)$ , will be frequently used in the remaining part of the proof. The generators  $X_i, Y_i, H_i$  ( $1 \leq i \leq m$ ), the constants  $\kappa_{i,j,l}$ , and the relations (3.15) - (3.19) give a presentation of the group  $U_3(p^m)$ . From (3.18), it follows that  $[X_i, Y_j] = [X_j, Y_i]$  for all  $i, j \geq 1$ , and so

$$\kappa_{i,j,l} = \kappa_{j,i,l}. \quad (3.20)$$

Also, combining (3.19) with the relation  $[X_i, Y_j] = [X_j, Y_i]$ , we obtain

$$[X_j, Y_i] = [X_1^{\kappa_{i,j,1}} X_2^{\kappa_{i,j,2}} \dots X_m^{\kappa_{i,j,m}}, Y_1], \quad 1 \leq i, j \leq m. \quad (3.21)$$

We now build up a presentation of a finite  $p$ -group  $G$  such that  $G/Z(G) \cong U_3(p^m)$ .

**Lemma 3.4.1** *Fix a prime  $p > 2$  and an integer  $m \geq 2$ . Let  $H$  be a  $p$ -group of*

---

nilpotency class 3 and of conjugate type  $(1, p^{2m})$ . Then there exists

$$\alpha_{i,j,l}, \beta_{i,j,l}, \gamma_{i,j,l}, \delta_{i,j,l}, \lambda_{i,j,l}, \mu_{i,j,l}, \epsilon_{i,l}, \nu_{i,l} \in \mathbb{F}_p \quad (1 \leq i, j \leq m, 1 \leq l \leq 2m),$$

such that  $H$  is isoclinic to the group  $G$  admitting the following presentation:

$$G = \left\langle x_1, \dots, x_m, y_1, \dots, y_m, h_1, h_2, \dots, h_m, z_1, z_2, \dots, z_{2m} \mid \right. \\ \left. x_i^p = \prod_{l=1}^{2m} z_l^{\epsilon_{i,l}}, \quad y_i^p = \prod_{l=1}^{2m} z_l^{\nu_{i,l}}, \quad h_i^p = 1 \quad (1 \leq i \leq m), \quad z_i^p = 1 \quad (1 \leq i \leq 2m), \right. \\ \left. (R0) \right.$$

$$[z_k, z_r] = [z_k, x_i] = [z_k, y_i] = [z_k, h_i] = 1 \quad (1 \leq k, r, \leq 2m, 1 \leq i \leq m), \\ (R1)$$

$$[h_i, h_j] = 1 \quad (1 \leq i, j \leq m), \\ (R2)$$

$$[h_i, x_j] = \prod_{l=1}^{2m} z_l^{\gamma_{i,j,l}} \quad (1 \leq i, j \leq m), \\ (R3)$$

$$[h_i, y_j] = \prod_{l=1}^{2m} z_l^{\delta_{i,j,l}} \quad (1 \leq i, j \leq m), \\ (R4)$$

$$[x_i, x_j] = \prod_{l=1}^{2m} z_l^{\alpha_{i,j,l}} \quad (1 \leq i, j \leq m), \\ (R5)$$

$$[y_i, y_j] = \prod_{l=1}^{2m} z_l^{\beta_{i,j,l}} \quad (1 \leq i, j \leq m), \\ (R6)$$

$$[x_i, y_j] = [x_1, y_1^{\kappa_{i,j,1}} y_2^{\kappa_{i,j,2}} \dots y_m^{\kappa_{i,j,m}}] \prod_{l=1}^{2m} z_l^{\lambda_{i,j,l}} \quad (1 \leq i, j \leq m), \\ (R7)$$

$$[x_j, y_i] = [x_1^{\kappa_{i,j,1}} x_2^{\kappa_{i,j,2}} \dots x_m^{\kappa_{i,j,m}}, y_1] \prod_{l=1}^{2m} z_l^{\mu_{i,j,l}} \quad (1 \leq i, j \leq m), \\ (R8)$$

$$[x_1, y_i] = h_i, \quad [h_1, x_i] = z_i, \quad [h_1, y_i] = z_{m+i} \quad (1 \leq i \leq m) \Big\rangle, \\ (R9)$$

where  $\kappa_{i,j,l}$ ,  $1 \leq i, j, l \leq m$ , are the structure constants of  $U_3(p^m)$ .

*Proof.* By Propositions 1.2.1 and 1.2.2,  $H$  is isocline to a group  $G$  satisfying hypothesis (A2). Then by Lemma 2.2.9, Theorem 2.2.14 and Lemma 3.2.3,

$$[G : G'] = p^{2m} = |Z(G)|, \quad \text{and} \quad [G' : Z(G)] = p^m.$$

The desired presentation of  $G$  is obtained from the presentation of  $U_3(p^m)$  ( $\cong G/Z(G)$ ) described just before the lemma. As  $G$  is of nilpotency class 3,  $G'$  is abelian and consequently elementary abelian by Corollary 1.1.23. As  $Z(G) \leq G'$ ,  $Z(G)$  is also elementary abelian.

Since  $|Z(G)| = p^{2m}$ ,  $Z(G)$  is minimally generated by  $2m$  elements  $z_1, z_2, \dots, z_{2m}$  (say). Let  $\varphi : G \rightarrow U_3(p^m)$  denote a surjective homomorphism with  $\ker \varphi = Z(G)$ . Let  $X_i$ 's,  $Y_i$ 's and  $H_i$ 's be the generators of  $U_3(p^m)$  considered in the discussion preceding the lemma.

Choose  $x_1, \dots, x_m, y_1, \dots, y_m, h_1, \dots, h_m$  in  $G$  such that

$$\varphi(x_i) = X_i, \quad \varphi(y_i) = Y_i \quad \text{and} \quad \varphi(h_i) = H_i \quad (1 \leq i \leq m).$$

It follows that the set

$$\{x_1, \dots, x_m, y_1, \dots, y_m, h_1, h_2, \dots, h_m, z_1, z_2, \dots, z_{2m}\} \text{ generates } G,$$

and

$$\{h_1, h_2, \dots, h_m, z_1, z_2, \dots, z_{2m}\} \text{ generates } G'.$$

Since  $\ker \varphi = Z(G)$  and  $\varphi(x_i^p) = 1$ ,  $1 \leq i \leq m$ , there exist some  $\epsilon_{i,l} \in \mathbb{F}_p$ ,  $1 \leq l \leq 2m$ , such that  $x_i^p = \prod_l z_l^{\epsilon_{i,l}}$ . Similarly there exist some  $\nu_{i,l} \in \mathbb{F}_p$ ,  $1 \leq l \leq 2m$ , such that  $y_i^p = \prod_l z_l^{\nu_{i,l}}$ ,  $1 \leq i \leq m$ . Since  $G'$  is elementary abelian, we get  $h_i^p = 1$ ,  $[h_i, h_j] = 1$ ,  $1 \leq i, j \leq m$  and  $z_i^p = 1$ ,  $1 \leq i \leq 2m$ . This

---

gives all the relations in (R0) and (R2). Since  $z_i \in Z(G)$ , the relations (R1) are the obvious commutator relations of  $z_i$ 's with the other generators of  $G$ . The relations (3.16), (3.17), (3.19) and (3.21) of  $U_3(p^m)$  give the relations (R3)-(R8) for some  $\alpha$ 's,  $\beta$ 's,  $\gamma$ 's,  $\delta$ 's,  $\lambda$ 's and  $\mu$ 's in  $\mathbb{F}_p$ .

It remains to obtain relations (R9). Since, for  $1 \leq i \leq m$ ,  $[X_1, Y_i] = H_i$ , by the choice of  $x_1, y_i$  and  $h_i$ , we have

$$[x_1, y_i] \equiv h_i \pmod{Z(G)}.$$

Thus  $[x_1, y_i] = h_i w_i$  for some  $w_i \in Z(G)$ . Replacing  $h_i$  by  $h_i w_i$ , which do not violate any of the preceding relations, we can assume, without loss of generality, that

$$[x_1, y_i] = h_i, \quad 1 \leq i \leq m. \quad (3.22)$$

Finally, we have  $h_1 \in G' \setminus Z(G)$ . Further,  $G$  is of conjugate type  $(1, p^{2m})$ , and  $[G : G'] = p^{2m}$  with  $G'$  abelian. Therefore  $C_G(h_1) = G'$ . Since  $x_1, \dots, x_m, y_1, \dots, y_m$  are independent modulo  $C_G(h_1) = G'$ , it follows that the  $2m$  commutators

$$[h_1, x_1], \dots, [h_1, x_m], [h_1, y_1], \dots, [h_1, y_m]$$

are independent, and they belong to  $\gamma_3(G) = Z(G)$ , which is elementary abelian of order  $p^{2m}$ . Thus, without loss of generality, we can take  $[h_1, x_i] = z_i$  and  $[h_1, y_i] = z_{m+i}$  for  $1 \leq i \leq m$ . This, along with (3.22), gives relations (R9).  $\square$

**Theorem 3.4.2** *Given an even integer  $n = 2m \geq 2$  and an odd prime  $p$ , there is a unique finite  $p$ -group satisfying Hypothesis (A2), upto isoclinism. Moreover, such a group is isoclinic to the group  $\mathcal{H}_m / Z(\mathcal{H}_m)$ .*

Assuming Theorem 3.4.2, we are now ready to prove our main theorem ( Theo-

---

rem 3.1.3).

**Proof of Theorem 3.1.3:** For an integer  $n \geq 1$  and a prime  $p$ , let  $G$  be a finite  $p$ -group of nilpotency class 3 and of conjugate type  $(1, p^n)$ . In view of Propositions 1.2.1 and 1.2.2, we can assume that  $Z(G) \leq G'$ . Then, by Theorem 3.2.6,  $n$  is even. Conversely, if  $n \geq 1$  is an even integer and  $p$  is an odd prime, then that there exists a finite  $p$ -group of nilpotency class 3 and of conjugate type  $(1, p^n)$ , follows from Theorem 3.3.1. This proves the first assertion of Main Theorem. The second one follows from Theorem 3.4.2.  $\square$

The rest of this section is devoted to the proof of Theorem 3.4.2. For  $m = 1$ , Theorem 3.4.2 has been proved by Ishikawa in [Theorem 4.2, [11]]. Thus, assume that  $m \geq 2$ .

In remaining part of this chapter, now onwards, for a prime  $p$ , and integer  $m \geq 1$ ,  $G$  (or more precisely,  $G(\alpha, \beta, \gamma, \delta, \lambda, \mu, \epsilon, \nu)$ ) always denotes a group of conjugate type  $(1, p^{2m})$ , admitting the presentation as in Lemma 3.4.1, where  $\alpha$ 's,  $\beta$ 's,  $\gamma$ 's,  $\delta$ 's,  $\lambda$ 's,  $\mu$ 's,  $\epsilon$ 's, and  $\nu$ 's belong to  $\mathbb{F}_p$ . Further, let the homomorphism  $\varphi : G \rightarrow U_3(p^m)$ ,

$$x_i \mapsto X_i, \quad y_i \mapsto Y_i, \quad \text{and } h_i \mapsto H_i$$

be as in the proof of Lemma 3.4.1.

First, we proceed to show that there is a unique choice for  $\alpha$ 's,  $\beta$ 's,  $\gamma$ 's,  $\delta$ 's,  $\lambda$ 's and  $\mu$ 's for which the group  $G$  considered in Lemma 3.4.1 is of conjugate type  $(1, p^{2m})$ . We start with simplifying the relations of  $G$  without any loss of generality.

---

**Lemma 3.4.3** *We can choose generators  $x_j$ 's and  $y_j$ 's of  $G$  such that*

$$[x_1, x_j] = [y_1, y_j] = 1 \quad (j = 2, \dots, m).$$

*Proof.* Fix  $j$  with  $2 \leq j \leq m$ . Since  $[x_1, x_j] \in Z(G)$ , by Corollary 3.2.9, there exists  $h_j \in G'$  such that  $[x_1, x_j h_j] = 1$ . Thus replacing  $x_j$  by  $x_j h_j$ , if necessary, we can assume that  $[x_1, x_j] = 1$ . Similarly, we can choose  $y_j$ 's such that  $[y_1, y_j] = 1$ .  $\square$

**Theorem 3.4.4** *In the relations (R3) and (R4), for  $1 \leq i, j \leq m$ , we have*

$$[h_i, x_j] = [h_j, x_i] = z_1^{\kappa_{i,j,1}} z_2^{\kappa_{i,j,2}} \cdots z_m^{\kappa_{i,j,m}}$$

and

$$[h_i, y_j] = [h_j, y_i] = z_{m+1}^{\kappa_{i,j,1}} z_{m+2}^{\kappa_{i,j,2}} \cdots z_{2m}^{\kappa_{i,j,m}}.$$

*In particular,  $\gamma$ 's and  $\delta$ 's (in the relations (R3) and (R4)) are uniquely determined by the structure constants  $\kappa_{i,j,l}$  of  $U_3(p^m)$ .*

*Proof.* Since  $H_i = [X_1, Y_i]$  in  $U_3(p^m)$  for  $1 \leq i \leq m$ , we get  $h_i \equiv [x_1, y_i] \pmod{Z(G)}$  in  $G$ . Therefore

$$[h_i, x_j] = [[x_1, y_i], x_j].$$

Since  $[x_1, x_j] \in Z(G)$ , by Lemma 1.3.7, we get

$$[h_i, x_j] = [[x_1, y_i], x_j] = [[x_j, y_i], x_1].$$

From the relation (R8),  $[x_j, y_i] \equiv [x_1^{\kappa_{i,j,1}} x_2^{\kappa_{i,j,2}} \cdots x_m^{\kappa_{i,j,m}}, y_1] \pmod{Z(G)}$ . Then,

---



again by Lemma 1.3.7, we get

$$\begin{aligned}
 [h_i, x_j] &= [x_j, y_i, x_1] = [x_1^{\kappa_{i,j,1}} x_2^{\kappa_{i,j,2}} \cdots x_m^{\kappa_{i,j,m}}, y_1, x_1] \\
 &= [x_1, y_1, x_1^{\kappa_{i,j,1}} x_2^{\kappa_{i,j,2}} \cdots x_m^{\kappa_{i,j,m}}] \\
 &= [h_1, x_1^{\kappa_{i,j,1}} x_2^{\kappa_{i,j,2}} \cdots x_m^{\kappa_{i,j,m}}] \\
 &= z_1^{\kappa_{i,j,1}} z_2^{\kappa_{i,j,2}} \cdots z_m^{\kappa_{i,j,m}}.
 \end{aligned}$$

Since the structure constants  $\kappa_{i,j,l}$  are symmetric in  $i, j$  (see Lemma 3.20),  $[h_i, x_j] = [h_j, x_i]$ . This proves the first assertion of the Lemma, and the second one goes on the same lines.  $\square$

As an immediate consequence of the preceding result, we have

**Corollary 3.4.5** *Consider the elements  $x = x_1^{a_1} \cdots x_m^{a_m}$ ,  $x' = x_1^{b_1} \cdots x_m^{b_m}$ ,  $y = y_1^{c_1} \cdots y_m^{c_m}$  and  $y' = y_1^{d_1} \cdots y_m^{d_m}$  in  $G$ . If*

$$[x, y, x'] = \prod_{l=1}^{2m} z_l^{r_l} \quad \text{and} \quad [y, x, y'] = \prod_{l=1}^{2m} z_l^{s_l},$$

for some  $r_l, s_l \in \mathbb{F}_p$ , then the values of  $r_l$  and  $s_l$  are uniquely determined by the structure constants of  $U_3(p^m)$  and, respectively, by  $a_i$ 's,  $b_i$ 's,  $c_i$ 's and  $a_i$ 's,  $c_i$ 's,  $d_i$ 's.

Up to now, we have shown the uniqueness of  $\gamma$ 's and  $\delta$ 's (Theorem 3.4.4). Next we show the uniqueness of  $\lambda$ 's and  $\mu$ 's. First we prove some lemmas.

**Lemma 3.4.6** *For  $1 \leq i, j \leq m$ , the following hold:*

(i)  $[x_i, x_j] \in \langle z_1, \dots, z_m \rangle$ .

(ii)  $[y_i, y_j] \in \langle z_{m+1}, \dots, z_{2m} \rangle$ .

*Proof.* Fix  $i, j$  with  $1 \leq i, j \leq m$ . Since  $[x_i, x_j] \in Z(G)$ , by Corollary 3.2.9, there exists  $h \in G'$  (depending on  $x_i, x_j$ ) such that  $[x_i, x_j h] = 1$ . Then

$$[x_i, x_j] = [x_i, h]^{-1} = [h, x_i].$$

Since  $G' = \langle h_1, h_2, \dots, h_m, Z(G) \rangle$ , by Theorem 3.4.4,  $[h, x_i] \in \langle z_1, \dots, z_m \rangle$ , proving the first assertion. The second assertion follows on the same lines.  $\square$

Before proceeding further, we recall the following commutator identities in a finite  $p$ -group  $G$  of nilpotency class 3 with  $p$  odd, which will be used in computations without any reference. Note that, in this case  $G'$  is abelian, so the ordering of commutators is immaterial. For  $a, b, c \in G$ ,

$$(i) [ab, c] = [a, c][b, c][a, c, b] \text{ and } [a, bc] = [a, b][a, c][a, b, c];$$

$$(ii) [a^i, b^j, c^k] = [a, b, c]^{ijk} \text{ (since } G \text{ is of class 3);}$$

$$(iii) [a^s, b] = [a, b]^s [a, b, a]^{\binom{s}{2}} \text{ and } [a, b^s] = [a, b]^s [a, b, b]^{\binom{s}{2}} \quad (s \in \mathbb{F}_p),$$

where  $\binom{s}{2} = \frac{s(s-1)}{2}$  in  $\mathbb{F}_p$ ,  $p > 2$ .

**Lemma 3.4.7** *For  $x = x_1^{a_1} \cdots x_m^{a_m}$  and  $y = y_1^{a_1} \cdots y_m^{a_m}$  in  $G$ , the following hold:*

$$(i) [x_1, y] \equiv [x, y_1] \pmod{Z(G)}.$$

(ii) *If  $[x_1, y] = [x, y_1] \prod_{i=1}^{2m} z_i^{c_i}$ , then  $c_i$ 's are uniquely determined by  $a_i$ 's and the structure constants of  $U_3(p^m)$ .*

*Proof.* If  $a_i = 0$  for all  $i$ , then  $x = y = 1$ , and so  $c_i = 0$  for all  $i$ , there is nothing to prove. Thus, assume that not all  $a_i$ 's are 0. In  $U_3(p^m)$ , consider  $X = X_1^{a_1} \cdots X_m^{a_m}$  and  $Y = Y_1^{a_1} Y_2^{a_2} \cdots Y_m^{a_m}$ . Since  $[X_i, Y_j] = [X_j, Y_i]$  for all  $i, j$  (by (3.18)), we have  $[X_1, Y] = [X, Y_1]$ ; hence  $[x_1, y] \equiv [x, y_1] \pmod{Z(G)}$  in  $G$ . This proves assertion (i).

---

We prove assertion (ii) in two steps, as the arguments of Step 1 will be used further.

**Step 1.** For  $m+1 \leq l \leq 2m$ ,  $c_l$  is uniquely determined by the structure constants of  $U_3(p^m)$ .

With  $X, Y$  as in the proof of assertion (i), we have  $[X_1, Y] = [X, Y_1]$ , which implies that  $[X_1 Y_1^r, X Y^r] = 1$  for any  $r \in \mathbb{F}_p$ ; hence, in  $G$ , we get that  $[x_1 y_1^r, x y^r] \equiv 1 \pmod{Z(G)}$ . By Corollary 3.2.9, there exists an element  $h(r)$ , depending on  $r$ , in  $G'$  such that

$$[x_1 y_1^r, x y^r h(r)] = 1.$$

Since  $[x_1, x] = [y_1, y] = 1$  (see Lemma 3.4.3), we have

$$\begin{aligned} 1 = [x_1 y_1^r, x y^r h(r)] &= [x_1, y]^r [x_1, y, y]^{\binom{r}{2}} [x_1, y, y_1]^{r^2} [x_1, h(r)] \\ &\quad [y_1, x]^r [y_1, x, y_1]^{\binom{r}{2}} [y_1, x, y]^{r^2} [y_1, h(r)]^r. \end{aligned}$$

Consequently, by the given hypothesis, we get

$$\begin{aligned} \left(\prod_{l=1}^{2m} z_l^{c_l}\right)^{-r} &= ([x_1, y][y_1, x])^{-r} = [x_1, y]^{\binom{r}{2}} [x_1, y, y_1]^{r^2} [x_1, h(r)] \\ &\quad [y_1, x, y_1]^{\binom{r}{2}} [y_1, x, y]^{r^2} [y_1, h(r)]^r. \end{aligned} \quad (3.23)$$

By Theorem 3.4.4,  $[G', y], [G', y_1] \leq \langle z_{m+1}, \dots, z_{2m} \rangle$  and  $[x_1, h(r)] \in \langle z_1, \dots, z_m \rangle$ ; hence all the commutators on the right side of (3.23), except  $[x_1, h(r)]$ , belong to  $\langle z_{m+1}, \dots, z_{2m} \rangle$ . Thus

$$\left(\prod_{l=1}^m z_l^{-c_l}\right)^r = [x_1, h(r)] \quad (3.24)$$

and

$$\left( \prod_{l=m+1}^{2m} z_l^{-c_l} \right)^r = [x_1, y, y]^{(2)} [x_1, y, y_1]^{r^2} [y_1, x, y_1]^{(2)} [y_1, x, y]^{r^2} [y_1, h(r)]^r. \quad (3.25)$$

Since, by Theorem 3.4.4,  $z_i = [h_1, x_i] = [h_i, x_1]$  for  $1 \leq i \leq m$ , we have

$$\prod_{l=1}^m z_l^{-c_l} = \prod_{l=1}^m [x_1, h_l]^{c_l} = [x_1, h_1^{c_1} \cdots h_m^{c_m}] = [x_1, \tilde{h}],$$

where  $\tilde{h} = h_1^{c_1} \cdots h_m^{c_m}$ , which is independent of  $r$ . Then from (3.24) we get  $[x_1, h(r)] = [x_1, \tilde{h}]^r$ , which implies that  $\tilde{h}^r h(r)^{-1} \in C_G(x_1) \cap G' = Z(G)$ . Hence

$$h(r) \equiv \tilde{h}^r \pmod{Z(G)}.$$

Using this in (3.25), we get

$$\left( \prod_{l=m+1}^{2m} z_l^{-c_l} \right)^r = [x_1, y, y]^{(2)} [x_1, y, y_1]^{r^2} [y_1, x, y_1]^{(2)} [y_1, x, y]^{r^2} [y_1, \tilde{h}]^{r^2}.$$

Since this equation holds for all  $r \in \mathbb{F}_p$ , for  $r = 1$  and  $r = -1$ , we, respectively, get

$$\prod_{l=m+1}^{2m} z_l^{-c_l} = [x_1, y, y_1] [y_1, x, y] [y_1, \tilde{h}]$$

and

$$\prod_{l=m+1}^{2m} z_l^{c_l} = [x_1, y, y] [x_1, y, y_1] [y_1, x, y_1] [y_1, x, y] [y_1, \tilde{h}].$$

From these equations, we obtain

$$\prod_{l=m+1}^{2m} z_l^{2c_l} = [x_1, y, y][y_1, x, y_1].$$

By Corollary 3.4.5, the right hand side of the preceding equation is uniquely determined by  $a_i$ 's and the structure constants of  $U_3(p^m)$ , so are  $c_l$  for  $m + 1 \leq l \leq 2m$ .

**Step 2.** For  $1 \leq l \leq m$ ,  $c_l$  is uniquely determined by the structure constants of  $U_3(p^m)$ .

With  $X, Y$  as in the proof of assertion (i), we have  $[Y, X_1] = [Y_1, X]$ , which implies that  $[Y_1 X_1^r, Y X^r] = 1$  for any  $r \in \mathbb{F}_p$ ; hence, in  $G$ , we get

$$[y_1 x_1^r, y x^r] \equiv 1 \pmod{Z(G)}.$$

By Corollary 3.2.9, there exists an element  $k(r)$ , depending on  $r$ , in  $G'$  such that  $[y_1 x_1^r, y x^r k(r)] = 1$ . With appropriate modifications in Step (1), it follows that  $c_l$  for  $1 \leq l \leq m$  are uniquely determined by  $a_i$ 's and the structure constants of  $U_3(p^m)$ .

Finally by Step 1 and Step 2,  $c_l$  for  $1 \leq l \leq 2m$  are uniquely determined by  $a_i$ 's and the structure constants of  $U_3(p^m)$ .  $\square$

**Lemma 3.4.8** *In the relations (R7), namely, for  $1 \leq i, j \leq m$ ,*

$$[x_i, y_j] = [x_1, y_1^{\kappa_{i,j,1}} y_2^{\kappa_{i,j,2}} \cdots y_m^{\kappa_{i,j,m}}] \prod_{l=1}^{2m} z_l^{\lambda_{i,j,l}}, \quad (3.26)$$

$\lambda_{i,j,l}$ ,  $m + 1 \leq l \leq 2m$ , are uniquely determined by the structure constants of  $U_3(p^m)$ .

---

*Proof.* For simplicity, we fix  $i, j \leq m$  and write  $y_1^{\kappa_{i,j,1}} y_2^{\kappa_{i,j,2}} \cdots y_m^{\kappa_{i,j,m}} = y$ . Since  $[x_i, y_j] \equiv [x_1, y] \pmod{Z(G)}$ , we have  $[x_1 y_j^r, x_i y^r] \equiv 1 \pmod{Z(G)}$  for any  $r \in \mathbb{F}_p$ .

That  $\lambda_{i,j,l}$ ,  $m+1 \leq l \leq 2m$ , are uniquely determined by the structure constants of  $U_3(p^m)$ , follows on the lines (without any extra work) of Step 1 of Lemma 3.4.7.  $\square$

By the symmetry of  $x_i$ 's and  $y_i$ 's, the following lemma is dual of the preceding one.

**Lemma 3.4.9** *In the relations (R8), namely, for  $1 \leq i, j \leq m$ ,*

$$[x_j, y_i] = [x_1^{\kappa_{i,j,1}} x_2^{\kappa_{i,j,2}} \cdots x_m^{\kappa_{i,j,m}}, y_1] \prod_{l=1}^{2m} z_l^{\mu_{i,j,l}}, \quad (3.27)$$

$\mu_{i,j,l}$ ,  $1 \leq l \leq m$ , are uniquely determined by the structure constants of  $U_3(p^m)$ .

We are now ready to prove the uniqueness of  $\lambda$ 's and  $\mu$ 's.

**Theorem 3.4.10** *In the relations (R7) and (R8),  $\lambda_{i,j,l}$  and  $\mu_{i,j,l}$ ,  $1 \leq i, j \leq m$ ,  $1 \leq l \leq 2m$ , are uniquely determined by the structure constants of  $U_3(p^m)$ .*

*Proof.* The proof involves a careful application of Lemmas 3.4.7, 3.4.8 and 3.4.9. Interchanging  $i$  and  $j$  in (3.27), and observing the fact that  $\kappa_{i,j,l} = \kappa_{j,i,l}$ , we get

$$[x_i, y_j] = [x_1^{\kappa_{i,j,1}} x_2^{\kappa_{i,j,2}} \cdots x_m^{\kappa_{i,j,m}}, y_1] \prod_{l=1}^{2m} z_l^{\mu_{j,i,l}}. \quad (3.28)$$

By Lemma 3.4.9,  $\mu_{j,i,l}$ ,  $1 \leq i, j, l \leq m$ , are uniquely determined by the structure constants of  $U_3(p^m)$ .

---

By (3.26) and (3.28), we get

$$[x_1, y] = [x, y_1] \prod_{l=1}^{2m} z_l^{\mu_{j,i,l} - \lambda_{i,j,l}},$$

where  $x = x_1^{\kappa_{i,j,1}} \cdots x_m^{\kappa_{i,j,m}}$  and  $y = y_1^{\kappa_{i,j,1}} \cdots y_m^{\kappa_{i,j,m}}$ . By Lemma 3.4.7,  $\mu_{j,i,l} - \lambda_{i,j,l}$ ,  $1 \leq i, j, \leq m$ ,  $1 \leq l \leq 2m$ , are uniquely determined by the structure constants of  $U_3(p^m)$ .

Hence  $\lambda_{i,j,l}$ ,  $1 \leq i, j, \leq m$ ,  $1 \leq l \leq m$ , are uniquely determined by the structure constants of  $U_3(p^m)$ . This, together with Lemma 3.4.6, completes the uniqueness of  $\lambda$ 's.

Similarly,  $\mu_{i,j,l}$ ,  $1 \leq i, j \leq m$ ,  $1 \leq l \leq 2m$ , are uniquely determined by the structure constants of  $U_3(p^m)$ .  $\square$

Finally we prove the uniqueness of  $\alpha$ 's and  $\beta$ 's in the relations (R5) and (R6). Although the proofs are almost similar to the proofs of the previous cases, these can not go verbatim. Thus, we give complete proof of uniqueness of  $\alpha$ 's and  $\beta$ 's.

We need the following preliminary lemma.

**Lemma 3.4.11** *For any  $i$  with  $1 \leq i \leq m$  and  $c_j, c'_j, d_j, d'_j \in \mathbb{F}_p$  for  $1 \leq j \leq m$ , assume that the commutator equations*

$$[h_1^{c_1} \cdots h_m^{c_m}, x_i] = z_1^{d_1} \cdots z_m^{d_m}$$

and

$$[h_1^{c'_1} \cdots h_m^{c'_m}, y_i] = z_{m+1}^{d'_1} \cdots z_{2m}^{d'_m}$$

hold in the group  $G$ . Then there exists an  $m \times m$  invertible matrix  $A$ , whose

---

entries are the structure constants  $\kappa_{i,j,l}$  of  $U_3(p^m)$ , such that

$$\begin{bmatrix} c_1 & \cdots & c_m \end{bmatrix} A = \begin{bmatrix} d_1 & \cdots & d_m \end{bmatrix}$$

and

$$\begin{bmatrix} c'_1 & \cdots & c'_m \end{bmatrix} A = \begin{bmatrix} d'_1 & \cdots & d'_m \end{bmatrix}$$

*Proof.* Since  $h_1, h_2, \dots, h_m$  are independent modulo  $C_G(x_i)$ , it follows that  $[h_1, x_i], [h_2, x_i], \dots, [h_m, x_i]$  are independent, and lie in  $\langle z_1, z_2, \dots, z_m \rangle$  (by Theorem 3.4.4). In other words,  $\{[h_1, x_i], [h_2, x_i], \dots, [h_m, x_i]\}$  is also a basis for the vector space  $\langle z_1, z_2, \dots, z_m \rangle$  over  $\mathbb{F}_p$ . From Theorem 3.4.4,  $[h_j, x_i] = z_1^{\kappa_{j,i,1}} z_2^{\kappa_{j,i,2}} \cdots z_m^{\kappa_{j,i,m}}$ . The desired matrix  $A$  is the matrix of change of basis from  $\{z_1, \dots, z_m\}$  to  $\{[h_1, x_i], [h_2, x_i], \dots, [h_m, x_i]\}$ , which is given by

$$A = (a_{r,s}),$$

where  $a_{r,s} = \kappa_{r,i,s}$  for  $1 \leq r, s \leq m$ . This proves the first part. Changing  $x_i$  by  $y_i$  and  $z_i$  by  $z_{m+i}$ , similarly, we get the second assertion.  $\square$

**Theorem 3.4.12** *In the relations (R5) and (R6),  $\alpha_{i,j,l}$  and  $\beta_{i,j,l}$ ,  $1 \leq i, j \leq m$ ,  $1 \leq l \leq 2m$ , are uniquely determined by the structure constants of  $U_3(p^m)$ .*

*Proof.* Fix  $i, j$  with  $1 \leq i, j \leq m$ . Consider the relations (R7):

$$[x_i, y_j] = [x_1, y_1^{\kappa_{i,j,1}} y_2^{\kappa_{i,j,2}} \cdots y_m^{\kappa_{i,j,m}}] \prod_{l=1}^{2m} z_l^{\lambda_{i,j,l}}.$$

Since  $\kappa_{i,j,l} = \kappa_{j,i,l}$ , interchanging  $i$  and  $j$ , we get

$$[x_j, y_i] = [x_1, y_1^{\kappa_{i,j,1}} y_2^{\kappa_{i,j,2}} \cdots y_m^{\kappa_{i,j,m}}] \prod_{l=1}^{2m} z_l^{\lambda_{j,i,l}}.$$



From the preceding two equations, we obtain

$$[x_i, y_j] = [x_j, y_i] \prod_{l=1}^{2m} z_l^{\lambda_{i,j,l} - \lambda_{j,i,l}}. \quad (3.29)$$

Hence  $[x_i, y_j] \equiv [x_j, y_i] \pmod{Z(G)}$ . Since  $[x_i, x_j] \equiv [y_i, y_j] \equiv 1 \pmod{Z(G)}$ , it follows that  $[x_i y_i^r, x_j y_j^r] \equiv 1 \pmod{Z(G)}$  for all  $r \in \mathbb{F}_p$ . By Corollary 3.2.9, there exists an element  $k(r)$ , depending on  $r$ , in  $G'$  such that  $[x_i y_i^r, x_j y_j^r k(r)] = 1$ . Then

$$\begin{aligned} 1 = [x_i y_i^r, x_j y_j^r k(r)] &= [x_i, x_j] [x_i, y_j]^r [x_i, y_j, y_j]^{(r)} [x_i, y_j, y_i]^{r^2} [x_i, k(r)] \\ &\quad [y_i, x_j]^r [y_i, x_j, y_i]^{(r)} [y_i, x_j, y_j]^{r^2} [y_i, y_j]^{r^2} [y_i, k(r)]^r \end{aligned}$$

Using (3.29), we get

$$\begin{aligned} \left( \prod_{l=1}^{2m} z_l^{\lambda_{i,j,l} - \lambda_{j,i,l}} \right)^{-r} &= \left( [x_i, x_j] [x_i, k(r)] \right) \left( [x_i, y_j, y_j]^{(r)} [x_i, y_j, y_i]^{r^2} \right. \\ &\quad \left. [y_i, x_j, y_i]^{(r)} [y_i, x_j, y_j]^{r^2} [y_i, y_j]^{r^2} [y_i, k(r)]^r \right). \end{aligned}$$

Using Theorem 3.4.4 and Lemma 3.4.5, it follows that  $[x_i, x_j] [x_i, k(r)] \in \langle z_1, \dots, z_m \rangle$  and the rest of the terms in the right side of the preceding equation belong to  $\langle z_{m+1}, \dots, z_{2m} \rangle$ . Thus

$$\left( \prod_{l=1}^m z_l^{\lambda_{j,i,l} - \lambda_{i,j,l}} \right)^r = [x_i, x_j] [x_i, k(r)] \quad (3.30)$$

and

$$\begin{aligned} \left( \prod_{l=m+1}^{2m} z_l^{\lambda_{j,i,l} - \lambda_{i,j,l}} \right)^r &= [x_i, y_j, y_j]^{(r)} [x_i, y_j, y_i]^{r^2} [y_i, x_j, y_i]^{(r)} \\ &\quad [y_i, x_j, y_j]^{r^2} [y_i, y_j]^{r^2} [y_i, k(r)]^r. \end{aligned} \quad (3.31)$$

Since  $[h_1, x_i], [h_2, x_i], \dots, [h_m, x_i]$  are independent and belong to  $\langle z_1, z_2, \dots, z_m \rangle$  (see Theorem 3.4.4), we get

$$\langle z_1, z_2, \dots, z_m \rangle = \langle [h_1, x_i], [h_2, x_i], \dots, [h_m, x_i] \rangle,$$

Hence there exists  $\tilde{k} \in G'$ , independent of  $r$ , such that  $\prod_{l=1}^m z_l^{-\lambda_{i,j,l} + \lambda_{j,i,l}} = [x_i, \tilde{k}]$ .

Similarly there exists  $\hat{k} \in G'$ , independent of  $r$ , such that

$$[x_i, x_j] = [x_i, \hat{k}^{-1}]. \quad (3.32)$$

Therefore from (3.30), we get  $[x_i, \tilde{k}]^r = [x_i, \hat{k}^{-1}][x_i, k(r)]$ , which implies that  $\tilde{k}^r \hat{k} k(r)^{-1} \in C_G(x_i) \cap G' = Z(G)$ . Hence

$$k(r) \equiv \tilde{k}^r \hat{k} \pmod{Z(G)}.$$

Using this in (3.31), we get

$$\begin{aligned} \prod_{l=m+1}^{2m} z_l^{r(\lambda_{j,i,l} - \lambda_{i,j,l})} &= [x_i, y_j, y_j]^{(r)} [x_i, y_j, y_i]^{r^2} [y_i, x_j, y_i]^{(r)} [y_i, x_j, y_j]^{r^2} \\ &\quad [y_i, \tilde{k}]^{r^2} [y_i, y_j]^{r^2} [y_i, \hat{k}]^r. \end{aligned}$$

Writing this equation for  $r = 1$  and  $r = -1$ , we get

$$\prod_{l=m+1}^{2m} z_l^{\lambda_{j,i,l} - \lambda_{i,j,l}} = [x_i, y_j, y_i] [y_i, x_j, y_j] [y_i, \tilde{k}] [y_i, y_j] [y_i, \hat{k}]$$

and

$$\prod_{l=m+1}^{2m} z_l^{\lambda_{i,j,l} - \lambda_{j,i,l}} = [x_i, y_j, y_j] [x_i, y_j, y_i] [y_i, x_j, y_i] [y_i, x_j, y_j] [y_i, \tilde{k}]$$

$$[y_i, y_j][y_i, \hat{k}]^{-1}.$$

Preceding two equations give

$$\prod_{l=m+1}^{2m} z_l^{2(\lambda_{j,i,l} - \lambda_{i,j,l})} = [x_i, y_j, y_j]^{-1} [y_i, x_j, y_i]^{-1} [y_i, \hat{k}]^2.$$

Rearranging the terms, we get

$$\prod_{l=m+1}^{2m} z_l^{(\lambda_{j,i,l} - \lambda_{i,j,l})} [x_i, y_j, y_j]^{1/2} [x_i, y_j, y_i]^{1/2} = [y_i, \hat{k}].$$

Note that the left side of the preceding equation is of the form  $z_{m+1}^{d_1} \cdots z_{2m}^{d_m}$ . By Corollary 3.4.5 and Theorem 3.4.10,  $d_i$ 's are uniquely determined by the structure constants of  $U_3(p^m)$ . Let  $\hat{k} = h_1^{c_1} \cdots h_m^{c_m} \pmod{Z(G)}$ . Thus, we have the commutator equation

$$z_{m+1}^{d_1} \cdots z_{2m}^{d_m} = [y_i, h_1^{c_1} \cdots h_m^{c_m}].$$

By Lemma 3.4.11, it follows that  $c_i$ 's are uniquely determined by the structure constants of  $U_3(p^m)$ .

By Lemma 3.4.6,  $\alpha_{i,j,l} = 0$  for  $l > m$ . Then by (3.32), we have

$$\prod_{l=1}^m z_l^{\alpha_{i,j,l}} = [x_i, x_j] = [\hat{k}, x_i] = [h_1^{c_1} \cdots h_m^{c_m}, x_i].$$

Again, by Lemma 3.4.11, it follows that  $\alpha_{i,j,l}$ ,  $1 \leq i, j \leq m$ ,  $1 \leq l \leq 2m$ , are uniquely determined by the structure constants of  $U_3(p^m)$ .

That  $\beta_{i,j,l}$ ,  $1 \leq i, j \leq m$ ,  $1 \leq l \leq 2m$ , are uniquely determined by the structure constants of  $U_3(p^m)$ , follows on the same lines.  $\square$

Before proceeding for the proof of Theorem 3.4.2, we summarize the preceding discussion of this section.

For simplicity, fix a prime  $p > 2$ , an integer  $m \geq 2$ , and a finite  $p$ -group  $H$  of nilpotency class 3 and of conjugate type  $(1, p^{2m})$ . Then, there exist  $\alpha_{i,j,l}, \beta_{i,j,l}, \gamma_{i,j,l}, \delta_{i,j,l}, \lambda_{i,j,l}, \mu_{i,j,l}, \epsilon_{i,l}, \nu_{i,l} \in \mathbb{F}_p$  ( $1 \leq i, j \leq m, 1 \leq l \leq 2m$ ) such that  $H$  is isoclinic to the group  $G$  with presentation as in Lemma 3.4.1. By Theorems 3.4.4, 3.4.10 and 3.4.12,  $\alpha_{i,j,l}, \beta_{i,j,l}, \gamma_{i,j,l}, \delta_{i,j,l}, \lambda_{i,j,l}, \mu_{i,j,l}$ , are uniquely determined.

In particular, the isoclinism type of the group  $H$  depends only on  $\epsilon_{i,l}$  and  $\nu_{i,l}$ ,  $1 \leq i, j \leq m, 1 \leq l \leq 2m$ . Thus, for the proof of Theorem 3.4.2, we fix those unique  $\alpha_{i,j,l}, \beta_{i,j,l}, \gamma_{i,j,l}, \delta_{i,j,l}, \lambda_{i,j,l}, \mu_{i,j,l} \in \mathbb{F}_p$  ( $1 \leq i, j \leq m, 1 \leq l \leq 2m$ ), for which, a group given by the presentation as in Lemma 3.4.1 is of conjugate type  $(1, p^{2m})$ , for some  $\epsilon$ 's and  $\nu$ 's in  $\mathbb{F}_p$ . Then we denote the resulting group with presentation as in Lemma 3.4.1 by  $G(\epsilon, \nu)$ .

**Lemma 3.4.13** *For any choice of  $\epsilon_{i,l}, \nu_{i,l}, \epsilon'_{i,l}, \nu'_{i,l} \in \mathbb{F}_p$ ,  $1 \leq i \leq m, 1 \leq l \leq 2m$ , the groups  $G(\epsilon, \nu)$  and  $G(\epsilon', \nu')$  are isoclinic.*

*Proof.* Consider the presentation of  $G(\epsilon, \nu)$  as in Lemma 3.4.1. To distinguish the generators of  $G(\epsilon, \nu)$  and  $G(\epsilon', \nu')$ , we write the presentation of  $G(\epsilon', \nu')$  as in Lemma 3.4.1, where we replace  $x_i$  by  $\hat{x}_i$ ,  $y_i$  by  $\hat{y}_i$ ,  $h_i$  by  $\hat{h}_i$ , and  $z_l$  by  $\hat{z}_l$  for  $1 \leq i \leq m, 1 \leq l \leq 2m$ . For simplicity, we denote the groups  $G(\epsilon, \nu)$  and  $G(\epsilon', \nu')$  by  $G_1$  and  $G_2$  respectively.

It follows, from the construction of  $G_1$  and  $G_2$ , that the map

$$x_i Z(G_1) \mapsto \hat{x}_i Z(G_2), \quad y_i Z(G_1) \mapsto \hat{y}_i Z(G_2), \quad h_i Z(G_1) \mapsto \hat{h}_i Z(G_2)$$

extends to an isomorphism  $\phi : G_1/Z(G_1) \rightarrow G_2/Z(G_2)$ . Since  $G'_1$  and  $G'_2$  are

---

elementary abelian, it is clear that the map

$$h_i \mapsto \hat{h}_i, \quad z_l \mapsto \hat{z}_l$$

extends to an isomorphism  $\theta : G'_1 \rightarrow G'_2$ . Consider the diagram

$$\begin{array}{ccc} \overline{G}_1 \times \overline{G}_1 & \xrightarrow{a_{G_1}} & G'_1 \\ \phi \times \phi \downarrow & & \downarrow \theta \\ \overline{G}_2 \times \overline{G}_2 & \xrightarrow{a_{G_2}} & G'_2, \end{array}$$

where  $a_{G_1}$  and  $a_{G_2}$  are the commutation maps as defined in Section 1.2 of Chapter 1.

From the commutator relations of  $G_1$  and  $G_2$  (that is, the relations (R1)-(R9) of  $G_1$ , and correspondingly those of  $G_2$ ), it follows that the above diagram commutes for the generators of  $G_1$  and  $G_2$  taken in their presentation. A routine calculation now shows that the diagram commutes.

Stitching all the above pieces together, we get

**Proof of Theorem 3.4.2:** For a prime  $p > 2$  and integer  $n = 2m \geq 2$ , let  $H$  be a finite  $p$ -group of nilpotency class 3 and of conjugate type  $(1, p^n)$ . If  $m = 1$ , then the result follows from Theorem 1.1.27. Thus, we can assume that  $m \geq 2$ .

By Lemma 3.4.1, there exist  $\alpha$ 's,  $\beta$ 's,  $\gamma$ 's,  $\delta$ 's,  $\lambda$ 's,  $\mu$ 's,  $\epsilon$ 's and  $\nu$ 's in  $\mathbb{F}_p$  such that  $H$  is isoclinic to a group  $G$  with the presentation as in Lemma 3.4.1. By Theorems 3.4.4, 3.4.10 and 3.4.12,  $\alpha$ 's,  $\beta$ 's,  $\gamma$ 's,  $\delta$ 's,  $\lambda$ 's, and  $\mu$ 's are uniquely determined by the structure constants of  $U_3(p^m)$ . By Lemma 3.4.13, the isoclinism type of  $G$  is independent of the choice of  $\epsilon$ 's and  $\nu$ 's in  $\mathbb{F}_p$ .

Thus, for any  $m \geq 1$ ,  $H$  is uniquely determined up to isoclinism, and hence is isoclinic to the group  $\mathcal{H}_m / Z(\mathcal{H}_m)$  (see Section 3.3). □



# CHAPTER 4

## On the probability distribution associated to commutator word map in finite groups

*Let  $P(G)$  denote the set of sizes of fibers (for section 4.1 for definition) of non-trivial commutators of the commutator word map. In this chapter, we prove that  $|P(G)| = 1$ , for any finite group  $G$  of nilpotency class 3 with exactly two conjugacy class sizes. We also show that for given  $n \geq 1$ , there exists a finite group  $G$  of nilpotency class 2 with exactly two conjugacy class sizes such that  $|P(G)| = n$ .*

## 4.1 Introduction

Let  $\mathbb{G}$  denote the family of all finite groups. Define  $Pr : \mathbb{G} \rightarrow \mathbb{Q} \cap (0, 1]$  as follows:

$$Pr(G) = \frac{|\{(x, y) \in G \times G \mid xy = yx\}|}{|G|^2}, \quad \text{for } G \in \mathbb{G}.$$

$Pr(G)$  is called the commuting probability of  $G$ . Various probability distributions associated to commutator word map have been subject of active research in recent years (see [5], [23], [25], [26]). In 2008, Pournaki and Sobhani [25] introduced the notion of  $Pr_g(G)$ , which is defined as follows:

$$Pr_g(G) = \frac{|\{(x, y) \mid [x, y] = g\}|}{|G|^2}, \quad \text{for } g \in G.$$

Note that  $Pr_1(G) = Pr(G)$ , where 1 denotes the identity element in the group. In [25], Pournaki and Sobhani computed  $Pr_g(G)$  for finite groups  $G$ , which have only two different irreducible complex character degrees. They also obtained explicit formulas for  $Pr_g(G)$ , when  $G$  is a finite group with  $|G'| = p$ , where  $p$  is a prime integer. Motivated by this, Nath and Yadav [23] studied  $Pr_g(G)$ , when  $G$  is either of conjugate type  $(1, p^n)$  or a Camina  $p$ -group.

Denote by  $K(G)$  the set  $\{[x, y] \mid (x, y) \in G \times G\}$ . For  $g \in K(G)$ , define *fiber* of  $g$  as follows:

$$fiber(g) := \{(x, y) \in G \times G \mid [x, y] = g\}. \quad (4.1)$$

Note that, formula for  $Pr_g(G)$  can be re-written as follows:

$$Pr_g(G) = \begin{cases} \frac{|fiber(g)|}{|G|^2}, & \text{if } g \in K(G) \\ 0, & \text{otherwise.} \end{cases}$$



Following the notation used by Nath and Yadav [23], we recall the notion of  $P(G)$ , which is defined as follows:

$$P(G) = \{Pr_g(G) \mid 1 \neq g \in K(G)\}.$$

Note that

$$|P(G)| = |\{\text{fiber}(g) \mid 1 \neq g \in K(G)\}|. \quad (4.2)$$

Here, we restrict our attention to finite  $p$ -groups of conjugate type  $(1, p^n)$ . Since nilpotency class of such a group can be either 2 or 3, we consider following two family;  $\mathcal{G}_2$ , the family of finite  $p$ -groups of nilpotency class 2 and conjugate type  $(1, p^n)$ ,  $n \geq 1$ , and  $\mathcal{G}_3$ , the family of finite  $p$ -groups of nilpotency class 3 and conjugate type  $(1, p^n)$ ,  $n \geq 1$ .

Recall that the group  $G_r$  (defined in 1.1) and Camina  $p$ -groups of class 2 are two major examples of groups from family  $\mathcal{G}_2$ . Nath and Yadav [23] computed  $Pr_g(G_r)$  and proved that  $|P(G_r)| = 1$ , for all  $r \geq 1$ . They also gave explicit formula for  $Pr_g(G)$ , when  $G$  is a Camina  $p$ -group of nilpotency class 2 and proved that  $|P(G)| = 1$ , for such a group  $G$ . Then they asked the following question:

**Question 4.1.1** *Is it true that  $|P(G)| = 1$  for all finite  $p$ -groups  $G$  of conjugate type  $(1, p^n)$  and nilpotency class 2 ?*

In an attempt to answer this, we prove the following theorem, in this chapter.

**Theorem 4.1.2** *Let  $n \geq 1$  be a given positive integer. Then there always exist a group  $G$  (depending on  $n$ ) in  $\mathcal{G}_2$  such that  $|P(G)| = n$ .*

For groups belonging to  $\mathcal{G}_3$ , we prove the following result.

---

**Theorem 4.1.3** *Let  $G \in \mathcal{G}_3$  be a finite  $p$ -group of conjugate type  $(1, p^{2n})$ . Then for  $g \in G'$ ,*

$$Pr_g(G) = \begin{cases} \frac{p^{3n} + p^{2n} - 1}{p^{5n}}, & \text{if } g = 1 \\ \frac{p^{2n} - 1}{p^{5n}}, & \text{if } 1 \neq g \in G'. \end{cases}$$

Hence  $|P(G)| = 1$ .

We remark that this theorem rectifies a faulty statement [23, Theorem 5.13], where it was claimed that  $|P(G)| > 1$ , for a finite  $p$ -group  $G$  of conjugate type  $(1, p^2)$  and nilpotency class 3.

## 4.2 Key Results

Proof of following interesting result can be found in [Lemma 3.5, [25]] and [Theorem 2.3, [23]].

**Lemma 4.2.1** *Let  $G$  and  $H$  be two isoclinic groups with isoclinism  $(\phi, \theta)$ . Then  $Pr_g(G) = Pr_{\theta(g)}(H)$ .*

In the light of the preceding result, for any finite group  $G$ , we only need to consider a stem group from the isoclinic family of  $G$  to compute  $Pr_g(G)$  or  $P(G)$ .

For a finite group  $G$  and an element  $g \in K(G)$ , we define

$$T_g = \{x \in G \mid g \in [x, G]\}$$

and

$$TZ_g = \{xZ(G) \in G/Z(G) \mid g \in [x, G]\}.$$


---

Note that

$$|T_g| = |Z(G)||TZ_g|.$$

Following useful expression of  $Pr_g(G)$  is due to Das and Nath [5].

**Lemma 4.2.2** *Let  $G$  be a finite group and  $g \in G$ . Then*

$$Pr_g(G) = \frac{1}{|G|} \sum_{x \in T_g} \frac{1}{|x^G|}.$$

We remark that for any finite group  $G$  and element  $1 \neq g \in G$ ,

$$Pr_1(G) - Pr_g(G) \geq \frac{1}{[G : Z(G)]}.$$

If  $G$  is finite group with exactly two conjugacy class sizes, then we can further simplify the formula of  $Pr_g(G)$ .

**Lemma 4.2.3** *Let  $G$  be a finite group of conjugate type  $(1, p^n)$  and  $g \in K(G)$ .*

*Then*

$$Pr_g(G) = \begin{cases} \frac{1}{[G : Z(G)]} \frac{|TZ_g|}{p^n}, & \text{if } g \neq 1 \\ \frac{1}{[G : Z(G)]} \left(1 + \frac{[G : Z(G)] - 1}{p^n}\right), & \text{if } g = 1 \end{cases}$$

*Proof.* Suppose  $1 \neq g \in K(G)$ . Then for each  $x \in T_g$ ,  $|x^G| = p^n$ . By Lemma 4.2.2, we get

$$Pr_g(G) = \frac{1}{|G|} \sum_{x \in T_g} \frac{1}{p^n} = \frac{|T_g|}{|G|p^n} = \frac{|Z(G)||TZ_g|}{|G|p^n} = \frac{1}{[G : Z(G)]} \frac{|TZ_g|}{p^n}.$$


---

Now let  $g = 1$ . Then note that  $T_g = G$ . By Lemma 1.3.6, we get

$$\begin{aligned}
 Pr_1(G) &= \frac{1}{|G|} \sum_{x \in G} \frac{1}{|x^G|} \\
 &= \frac{1}{|G|} \sum_{x \in Z(G)} \frac{1}{|x^G|} + \frac{1}{|G|} \sum_{x \in G \setminus Z(G)} \frac{1}{|x^G|} \\
 &= \frac{|Z(G)|}{|G|} + \frac{1}{|G|} \frac{|G| - |Z(G)|}{p^n} \\
 &= \frac{1}{[G : Z(G)]} \left( 1 + \frac{[G : Z(G)] - 1}{p^n} \right).
 \end{aligned}$$

This completes the proof. □

Nath and Yadav [23] gave explicit formula for  $Pr_g(G_r)$ , for  $r \geq 1$ .

**Lemma 4.2.4** *Let  $G_r$  be as defined in 1.2. Then*

$$Pr_g(G_r) = \begin{cases} \frac{p^2 - 1}{p^{2r+1}}, & \text{if } g \neq 1 \\ \frac{p^{r+1} + p^r - 1}{p^{2r+1}}, & \text{if } g = 1 \end{cases}$$

Using preceding lemma and the formula  $Pr_g(G) = \frac{|fiber(g)|}{|G|^2}$ , we get an expression for the sizes of fibers in  $G_r$ .

**Lemma 4.2.5** *Let  $G_r$  be as defined in (1.1). Then*

$$|fiber(g)| = \begin{cases} (p^2 - 1)p^{r^2+r+1}, & \text{if } g \neq 1 \\ (p^{r+1} + p^r - 1)p^{r^2+r+1}, & \text{if } g = 1 \end{cases}$$

From preceding Lemma, we get an expression for  $|K(G)|$ .

---

**Lemma 4.2.6** *Let  $G_r$  be as defined in 1.1. Then  $|K(G_r)| - 1 = \frac{(p^{r+1} - 1)(p^r - 1)}{p^2 - 1}$ .*

*Proof.* For any finite group  $G$ , we know that  $\sum_{g \in K(G)} |\text{fiber}(g)| = |G|^2$ . Thus we get,  $\sum_{g \in K(G) \setminus 1} |\text{fiber}(g)| = |G|^2 - |\text{fiber}(1)|$ . Therefore by Lemma 4.2.5, we have

$$\begin{aligned} (|K(G_r)| - 1)(p^2 - 1)p^{r^2+r+1} &= p^{r^2+3r+2} - (p^{r+1} + p^r - 1)p^{r^2+r+1} \\ &= (p^{r^2} + r + 1)(p^{2r+1} - p^{r+1} - p^r + 1) \\ &= (p^{r^2} + r + 1)(p^{r+1} - 1)(p^r - 1). \end{aligned}$$

Hence  $|K(G_r)| - 1 = \frac{(p^{r+1} - 1)(p^r - 1)}{p^2 - 1}$ .

**Lemma 4.2.7** *Suppose  $G = G_{n-1}$  (as defined in (1.1)) is generated by  $a_1, a_2, \dots, a_n$ , with  $n \geq 4$ . Then there do not exist  $x, y \in G$  such that*

$$[x, y] = [a_1, a_2]^{i_1} [a_3, a_4]^{i_2} \dots [a_{2m-1}, a_{2m}]^{i_m}, \quad (4.3)$$

where  $2 \leq m \leq \lfloor n/2 \rfloor$  and  $i_k \not\equiv 0 \pmod{p}$ , for  $k = 1, 2, \dots, m$ .

*Proof.* We prove this lemma by the method of contradiction. Suppose that there exist  $x$  and  $y \in G$  satisfying equation (4.3). Let  $x = a_1^{j_1} a_2^{j_2} \dots a_n^{j_n}$  and  $y = a_1^{k_1} a_2^{k_2} \dots a_n^{k_n}$  (reading modulo  $Z(G)$ ). As  $i_1 \not\equiv 0 \pmod{p}$ , at least one of  $j_1$  and  $k_1$  has to be non-zero modulo  $p$ . Without loss of generality, we take  $j_1$  to be non-zero. Then we can write  $y$  as

$$y = a_1^{k_1} a_2^{k_2} \dots a_n^{k_n} = (a_1^{j_1} a_2^{j_2} \dots a_n^{j_n})^{k_1 j_1^{-1}} (a_2^{l_2} a_3^{l_3} \dots a_n^{l_n} z_1) = x^{k_1 j_1^{-1}} (a_2^{l_2} a_3^{l_3} \dots a_n^{l_n} z_1),$$

where  $z_1 \in Z(G)$  and  $l_2, l_3, l_4$  are some suitable integers. Now

$$[x, y] = [x, y_1], \quad \text{where } y_1 = a_2^{l_2} a_3^{l_3} \dots a_n^{l_n}.$$

Computing  $[x, y_1]$ , we get that  $[a_1, a_2^{j_1 l_2} a_3^{j_1 l_3} \dots a_n^{j_1 l_n}]$  is exactly the commutator involving  $a_1$  in left-hand side of equation (4.3). Comparing it with right-hand side of equation (4.3), we see that  $l_2$  has to be non-zero modulo  $p$ , in particular  $l_2 = i_1 j_1^{-1}$  and  $l_3, l_4, \dots, l_n$  have to be zero modulo  $p$ . Thus we have

$$y_1 = a_2^{i_1 j_1^{-1}} \quad \text{with } j_1 \text{ non-zero modulo } p.$$

Now, again computing  $[x, y]$ , considering commutator involving  $a_2$  and comparing with equation (4.3), we see that  $j_2, j_3, \dots, j_n$  have to be zero modulo  $p$ . So we have  $x = a_1^{j_1}$  and  $y_1 = a_2^{i_1 j_1^{-1}}$  with  $j_1$  non-zero. Therefore  $[x, y] = [x, y_1] = [a_1, a_2]^{i_1}$ , a contradiction to given hypothesis.  $\square$

**Lemma 4.2.8** *Suppose  $G = G_n$  (as defined in (1.1)) is generated by  $a_1, a_2, \dots, a_n$ , with  $n \geq 6$ . Then there do not exist  $x, y, z$  and  $w \in G$  such that*

$$[x, y][z, w] = [a_1, a_2]^{i_1} [a_3, a_4]^{i_2} \dots [a_{2m-1}, a_{2m}]^{i_m}, \quad (4.4)$$

where  $3 \leq m \leq \lfloor n/2 \rfloor$  and  $i_k \not\equiv 0 \pmod{p}$ , for  $k = 1, 2, \dots, m$ .

*Proof.* We also prove this lemma by the method of contradiction. Suppose that there exist  $x, y, z$  and  $w \in G$  satisfying equation (4.4). Let  $x = a_1^{j_1} a_2^{j_2} \dots a_n^{j_n}$ ,  $y = a_1^{k_1} a_2^{k_2} \dots a_n^{k_n}$ ,  $z = a_1^{l_1} a_2^{l_2} \dots a_n^{l_n}$  and  $w = a_1^{t_1} a_2^{t_2} \dots a_n^{t_n}$  (reading modulo  $Z(G)$ ). As  $i_1 \not\equiv 0 \pmod{p}$ , at least one of  $j_1, k_1, l_1$  and  $t_1$  has to be non-zero modulo  $p$ . Without loss of generality, we take  $j_1$  to be non-zero. So  $\{x, a_2, a_3, \dots, a_n\}$  also forms a generating set for  $G$ .

Let  $N$  be the subgroup of  $G$  generated by  $x, a_2$  and their commutators with  $G$ . It is easy to see that  $N$  is a normal subgroup. Set  $\overline{G} = G/N$ . Now  $\{\overline{a_3}, \overline{a_4}, \dots, \overline{a_n}\}$  is a generating set for  $\overline{G}$  and easy to see that  $\overline{G} \cong G_{n-2}$ , as

defined in (1.2). In  $\overline{G}$ , (4.4) reduced to

$$[\overline{z}, \overline{w}] = [\overline{a_3}, \overline{a_4}]^{i_2} \dots [\overline{a_{2m-1}}, \overline{a_{2m}}]^{i_m},$$

where  $3 \leq m \leq \lfloor n/2 \rfloor$  and  $i_k \not\equiv 0 \pmod{p}$ , for  $k = 2, 3, \dots, m$ . This is not possible by Lemma 4.2.7. Thus there do not exist  $x, y, z$  and  $w \in G$  satisfying equation (4.4). This completes the proof.  $\square$

### 4.3 Proof of Theorem 4.1.2

We are now ready to prove Theorem 4.1.2.

**Proof of Theorem 4.1.2:** We know that  $|P(G_r)| = 1$  for all  $r \geq 1$ , from [Theorem B, [23]]. Therefore, we only need to prove the statement for  $n \geq 2$ . For given  $n \geq 2$ , consider  $G = G_m$ , with  $m = n^2 + n - 3$ . Note that  $G$  is of nilpotency class 2 and conjugate type  $(1, p^m)$ . Suppose that  $G$  is generated by  $a_1, a_2, \dots, a_m, a_{m+1}$ . Then consider the central subgroup  $H$  as follows:

$$\begin{aligned} H = \langle & [a_1, a_2][a_3, a_4], \\ & [a_5, a_6][a_7, a_8], [a_5, a_6][a_9, a_{10}], \\ & [a_{11}, a_{12}][a_{13}, a_{14}], [a_{11}, a_{12}][a_{15}, a_{16}], [a_{11}, a_{12}][a_{17}, a_{18}], \\ & \vdots \\ & [a_{\alpha+1}, a_{\alpha+2}][a_{\alpha+3}, a_{\alpha+4}], [a_{\alpha+1}, a_{\alpha+2}][a_{\alpha+5}, a_{\alpha+6}] \dots [a_{\alpha+1}, a_{\alpha+2}] \\ & [a_{\alpha+2n-1}, a_{\alpha+2n}] \rangle; \end{aligned}$$

where  $\alpha = (n - 2)(n + 1)$ .

Note that  $|H| = p^{n(n-1)/2}$  and  $\alpha + 2n = n^2 + n - 2 = m + 1$ .

Set  $\tilde{G} := G/H$ . Note that  $[\tilde{a}_1, \tilde{a}_3] \neq 1$  in  $\tilde{G}$ . Thus  $\tilde{G}$  is non-abelian, in particular, nilpotency class of  $\tilde{G}$  is 2. Our aim is to show that  $\tilde{G}$  has exactly two conjugacy class sizes and  $|P(\tilde{G})| = n$ . We complete the proof in two steps.

**Claim 1:**  $\tilde{G}$  has exactly two conjugacy class sizes.

It is sufficient to prove that each non-central element commutes only with its powers (reading modulo center). Let  $\tilde{x}, \tilde{y} \in \tilde{G}$  be such that neither is a power of the other. It is not difficult to see that  $[x, y] \neq 1$  in  $G$ . Hence, if  $[\tilde{x}, \tilde{y}] = 1$  in  $\tilde{G} = G/H$ , then  $[x, y] \in H^\#$ , the set of non-trivial elements of  $H$ . Suppose that

$$\begin{aligned} 1 \neq [x, y] &= ([a_1, a_2][a_3, a_4])^{i_{1,1}} \\ &\quad ([a_5, a_6][a_7, a_8])^{i_{2,1}} ([a_5, a_6][a_9, a_{10}])^{i_{2,2}} \\ &\quad ([a_{11}, a_{12}][a_{13}, a_{14}])^{i_{3,1}} ([a_{11}, a_{12}][a_{15}, a_{16}])^{i_{3,2}} ([a_{11}, a_{12}][a_{17}, a_{18}])^{i_{3,3}} \\ &\quad \vdots \\ &\quad ([a_{\alpha+1}, a_{\alpha+2}][a_{\alpha+3}, a_{\alpha+4}])^{i_{n-1,1}} ([a_{\alpha+1}, a_{\alpha+2}][a_{\alpha+5}, a_{\alpha+6}])^{i_{n-1,2}} \dots \\ &\quad ([a_{\alpha+1}, a_{\alpha+2}][a_{\alpha+2n-1}, a_{\alpha+2n}])^{i_{n-1,n-1}}. \end{aligned}$$

Since  $[x, y] \neq 1$ , at least one  $i_{j,k}$  is non-zero (mod  $p$ ). After simplification, we get

$$\begin{aligned} [x, y] &= [a_1, a_2]^{i_{1,1}} [a_3, a_4]^{i_{1,1}} \\ &\quad [a_5, a_6]^{i_{2,1}+i_{2,2}} [a_7, a_8]^{i_{2,1}} [a_9, a_{10}]^{i_{2,2}} \\ &\quad [a_{11}, a_{12}]^{i_{3,1}+i_{3,2}+i_{3,3}} [a_{13}, a_{14}]^{i_{3,1}} [a_{15}, a_{16}]^{i_{3,2}} [a_{17}, a_{18}]^{i_{3,3}} \\ &\quad \vdots \\ &\quad [a_{\alpha+1}, a_{\alpha+2}]^{i_{n-1,1}+i_{n-1,2}+\dots+i_{n-1,n-1}} [a_{\alpha+3}, a_{\alpha+4}]^{i_{n-1,1}} [a_{\alpha+5}, a_{\alpha+6}]^{i_{n-1,2}} \dots \end{aligned}$$



$$[a_{\alpha+2n-1}, a_{\alpha+2n}]^{i_{n-1, n-1}}.$$

Note that in the right-hand side at least two commutators have non-zero power. Thus, by Lemma 4.2.7,  $[x, y] \notin H^\#$  and consequently  $[\tilde{x}, \tilde{y}] \neq 1$  in  $\tilde{G}$ . Hence  $\tilde{G}$  has exactly two conjugacy class sizes.

**Claim 2:**  $|P(\tilde{G})| = n$ .

Here our plan is to show that

$$|\{|\text{fiber}(g)| \mid 1 \neq g \in K(\tilde{G})\}| = n.$$

First, note the following elementary facts:

(i)  $K(\tilde{G}) = K(G)$ .

(ii) For any  $h \in K(G)$ ,  $|\text{fiber}(\tilde{h})| = \frac{|\text{fiber}(h)|}{|H|^2} = \frac{(p^2 - 1)p^{m(m-1)/2}}{p^{n(n-1)}}$ .

The last equality in (ii) is due to Lemma 4.2.5.

For each  $h \in K(G)$ , set  $A_h := K(G) \cap hH$ . We claim that for each  $x \in A_h$ ,

$$\text{fiber}(\tilde{x}) = \text{fiber}(\tilde{h}) = \cup_{y \in A_h} \text{fiber}(\tilde{y}) \tag{4.5}$$

The first equality of (4.5) holds because of the fact:  $x \in A_h \Rightarrow \tilde{x} = \tilde{h}$  in  $\tilde{G}$ .

Now, we proceed to show the second equality of (4.5).

Suppose  $(\tilde{a}, \tilde{b}) \in \text{fiber}(\tilde{h})$ , i.e.,  $[\tilde{a}, \tilde{b}] = \tilde{h}$ . Then there exist some  $y \in hH$  such that  $[a, b] = y$ , i.e.,  $(a, b) \in \text{fiber}(y)$ . This implies  $(\tilde{a}, \tilde{b}) = (a, b) \in \text{fiber}(\tilde{y})$ . By definition of  $A_h$ ,  $y \in A_h$ . Hence  $\text{fiber}(\tilde{h}) \subseteq \cup_{y \in A_h} \text{fiber}(\tilde{y})$ . Similarly reverse inclusion can be shown by backtracking the above steps. This completes the proof of second equality of (4.5) and hence (4.5) holds true.

Now, for  $h \in K(G)$  and  $x \in A_h$ , by (4.5), we get

$$|\text{fiber}(\tilde{x})| = |A_h| \frac{(p^2 - 1)p^{m(m-1)/2}}{p^{n(n-1)}}.$$

Hence, to show  $|\{|\text{fiber}(\tilde{x})| \mid 1 \neq g \in K(\tilde{G})\}| = n$ , it is sufficient to show that

$$|\{|A_h| \mid 1 \neq h \in K(G)\}| = n.$$

Note that  $h \in A_h$ , for all  $h \in K(G)$ . Now fix some  $h \in K(G) \setminus 1$ . If  $h \neq g \in A_h$ , then

$$gh^{-1} = h', \text{ for some } 1 \neq h' \in H.$$

As both  $g, h^{-1} \in K(G)$ , consider  $g = [a, b]$  and  $h^{-1} = [c, d]$ , for some  $a, b, c, d \in G$ . Thus, we get

$$[a, b][c, d] = h'.$$

By Lemma 4.2.8 and presentation of  $H$ , this is only possible when  $h'$  is of the form

$$h' = [a_{2i-1}, a_{2i}]^\alpha [a_{2j-1}, a_{2j}]^\alpha \text{ or } h' = [a_{2i-1}, a_{2i}]^\alpha [a_{2j-1}, a_{2j}]^{-\alpha},$$

for some suitable indices  $i, j$  and integer  $1 \leq \alpha \leq p - 1$ , with either  $g = [a_{2i-1}, a_{2i}]^\alpha$  and  $h^{-1} = [a_{2j-1}, a_{2j}]^{\pm\alpha}$  or vice versa.

Using this observation, presentation of  $H$ , Lemma 4.2.7 and Lemma 4.2.8, we proceed to compute  $A_h$ , for all  $h \in K(G) \setminus 1$ . First we partition  $K(G) \setminus 1$  as

---

$K(G) \setminus 1 = K(G)_1 \cup K(G)_2$ , where

$$K(G)_1 = \{[a_{2i-1}, a_{2i}]^\beta \mid 1 \leq \beta \leq p-1, 1 \leq i \leq (m+1)/2\}$$

and  $K(G)_2 = (K(G) \setminus 1) \setminus K(G)_1$ .

Note that if  $h \in K(G)_2$ , then  $A_h = \{h\}$ . Now we proceed to compute  $A_h$ , for  $h \in K(G)_1$ . For simplification of notation, now onwards, we denote  $[a_i, a_j]$  by  $h_{i,j}$  in this proof.

$$\begin{aligned} A_{h_{1,2}^{k_1}} &= \{h_{1,2}^{k_1}, h_{3,4}^{-k_1}\}, \\ A_{h_{5,6}^{k_2}} &= \{h_{5,6}^{k_2}, h_{7,8}^{-k_2}, h_{9,10}^{-k_2}\}, \\ A_{h_{11,12}^{k_3}} &= \{h_{11,12}^{k_3}, h_{13,14}^{-k_3}, h_{15,16}^{-k_3}, h_{17,18}^{-k_3}\}, \\ &\vdots \\ A_{h_{\alpha+1, \alpha+2}^{k_{n-1}}} &= \{h_{\alpha+1, \alpha+2}^{k_{n-1}}, h_{\alpha+5, \alpha+6}^{-k_{n-1}}, h_{\alpha+3, \alpha+4}^{-k_{n-1}}, \dots, h_{\alpha+2n-1, \alpha+2n}^{-k_{n-1}}\}, \end{aligned}$$

for all  $1 \leq k_i \leq p-1, i = 1, 2 \dots n-1$ .

So, we get  $\{|A_h| \mid 1 \neq h \in K(G)\} = \{1, 2, \dots, n\}$ . Hence

$$|P(\tilde{G})| = |\{fiber(g) \mid 1 \neq g \in K(\tilde{G})\}| = |\{|A_h| \mid 1 \neq h \in K(G)\}| = n.$$

This completes the proof. □

## 4.4 Proof of Theorem 4.1.3

We recall some results from preceding chapter. We start with an elementary result which follows from Lemma 3.2.4, Theorem 3.2.6, Lemma 3.2.10 and definition of conjugate type.

**Lemma 4.4.1** *Let  $G$  be a stem  $p$ -group of class 3 with conjugate type  $(1, p^{2n})$ . Then the following hold true:*

- (i)  $|Z(G)| = p^{2n}$ ,  $|G' : Z(G)| = p^n$  and  $|G : G'| = p^{2n}$ .
- (ii) For each  $g \in G \setminus Z(G)$ ,  $|g^G| = [G : C_G(x)] = p^{2n}$  and  $|C_G(x) : Z(G)| = p^n$ .

Following technical result on finite  $p$ -groups of conjugate type  $(1, p^{2n})$  and nilpotency class 3 follows from Section 3.4 of preceding chapter.

**Lemma 4.4.2** *Let  $G$  be a stem  $p$ -group of class 3 with conjugate type  $(1, p^{2n})$ . Then there exists a generating set of  $G$ , say  $\{a_1, \dots, a_n, b_1, \dots, b_n\}$  such that the following hold true:*

- (i)  $G' = \langle h_1, \dots, h_n, Z(G) \rangle$ , where  $h_i = [a_i, b_i]$  for  $i = 1 \dots n$ ;
- (ii)  $Z(G) = \langle z_1, z_2, \dots, z_{2n} \rangle$ , where  $[h_1, a_i] = z_i$  and  $[h_1, b_i] = z_{n+i}$  for  $i = 1, \dots, n$ .
- (iii) Say  $A = \{\prod_{i=1}^n a_i^{k_i} \mid 0 \leq k_i \leq p-1\}$  and  $B = \{\prod_{i=1}^n b_i^{l_i} \mid 0 \leq l_i \leq p-1\}$ .

Then

- (1)  $[x, y] \in Z(G)$ , for  $x, y \in A$  or  $x, y \in B$ .
- (2)  $[x, y] \notin Z(G)$ , for  $1 \neq x \in A$  and  $1 \neq y \in B$ .
- (3)  $\{[a, b_i] \mid 1 \leq i \leq n\}$  generates  $G'$  over  $Z(G)$ , for any  $1 \neq a \in A$ .
- (4)  $\{[a_i, b] \mid 1 \leq i \leq n\}$  generates  $G'$  over  $Z(G)$ , for any  $1 \neq b \in B$ .

(iv) Say  $Z_1 = \langle z_1, \dots, z_n \rangle$  and  $Z_2 = \langle z_{n+1}, \dots, z_{2n} \rangle$ . Then for any  $1 \neq a \in A$ ,  $1 \neq b \in B$  and  $h \in G' \setminus Z(G)$ ,

$$(1) [h, A] = Z_1 = [a, G'].$$

$$(2) [h, B] = Z_2 = [b, G'].$$

(v) For each  $h \in G' \setminus Z(G)$ ,  $[h, G] = Z(G)$ .

Set  $\bar{G} = G/Z(G)$  and consider  $\Phi$  to be the canonical homomorphism from  $G$  onto  $\bar{G}$ . For  $g \in G \setminus G'$ , define

$$H_g = \Phi^{-1}(C_{\bar{G}}(\bar{g})). \quad (4.6)$$

Note that

$$H_g = C_g(G)G'.$$

As  $C_g(G) \cap G' = Z(G)$  and  $[G_g(G) : Z(G)] = p^n = [G' : Z(G)]$ , we have  $[H_g : Z(G)] = p^{2n}$ .

**Lemma 4.4.3** *Let  $g \in G \setminus G'$ . Then for any  $x \in H_g \setminus G'$ ,  $[G', x] = [G', g]$ .*

*Proof.* Take an arbitrary element of  $[G', x]$ , say  $[[g, y], x]$ , for some  $y \in G$ . As  $x \in H_g$ , so  $[x, g] \in Z(G)$ . Then by Lemma 1.3.7, we get  $[[g, y], x] = [[x, y], g]$  and so  $[G', x] \subseteq [G', g]$ . Similarly we can show the reverse inclusion and hence  $[G', x] = [G', g]$ .  $\square$

**Lemma 4.4.4** *Given any  $h \in G' \setminus Z(G)$  and any  $ab \neq 1$ , for some  $a \in A$  and  $b \in B$ , there always exists some  $h^* \in G'$  such that  $h \in [abh^*, G]$ .*

*Proof.* Without loss of generality we can assume that  $a \neq 1$ . By Lemma

---

4.4.2(iii)(3), there exists some  $b^* \in B$  such that

$$[a, b^*] = h \pmod{Z(G)}.$$

Now  $[ab, b^*] = hw_1w_2$ , for some  $w_1 \in Z_1$  and  $w_2 \in Z_2$ . By Lemma 4.4.2(iv)(1), there exists some  $h_1 \in G'$  such that  $[a, h_1] = w_1^{-1}$ . So

$$[ab, b^*h_1] = [ab, b^*][a, h_1][b, h_1] = hw_1w_2w_1^{-1}[b, h_1] = hw_2w_3$$

where  $w_3 = [b, h_1] \in Z_2$  (by Lemma 4.4.2(iv)(2)). Again using Lemma 4.4.2(iv)(2), we get some  $h^* \in G'$  such that  $[h^*, b^*] = (w_2w_3)^{-1}$ . Therefore

$$[abh^*, b^*h_1] = [ab, b^*h_1][h^*, b^*h_1] = hw_2w_3(w_2w_3)^{-1} = h.$$

This completes the proof. □

Now we are ready to prove Theorem 4.1.3.

**Proof of Theorem 4.1.3:** Let  $G \in \mathcal{G}_3$  be a finite  $p$ -group of conjugate type  $(1, p^{2n})$ . Then  $|G| = p^{5n}$  and  $[G : Z(G)] = p^{3n} = |G'|$ . By Lemma 4.2.3, we get

$$Pr_1(G) = \frac{1}{p^{3n}} + \frac{1}{p^{2n}} \left(1 - \frac{1}{p^{3n}}\right) = \frac{p^{3n} + p^{2n} - 1}{p^{5n}}.$$

Note that

$$\sum_{g \in K(G)} Pr_g(G) = 1.$$


---

Thus

$$\sum_{g \in K(G) \setminus 1} Pr_g(G) = 1 - Pr_1(G) = \frac{p^{5n} - p^{3n} - p^{2n} + 1}{p^{5n}} = (p^{3n} - 1) \frac{p^{2n} - 1}{p^{5n}}.$$

**Claim:**  $Pr_g(G) \geq \frac{p^{2n} - 1}{p^{5n}}$ , for each  $g \in G' \setminus 1$ .

By Lemma 4.2.3, it is sufficient to show that  $|TZ_g| \geq p^{2n} - 1$ , for all  $g \in G' \setminus 1$ .

**Case 1:**  $g \in Z(G) \setminus 1$ .

Consider any  $\alpha \in G' \setminus Z(G)$ . By Lemma 4.4.2(v), there exist some  $\beta \in G \setminus G'$  such that  $[\alpha, \beta] = g$ . Now consider  $H_\beta$  (as defined in (4.6)). Take  $x \in H_\beta \setminus Z(G)$ , then either  $x \in H_\beta \setminus G'$  or  $x \in G' \setminus Z(G)$ . If  $x \in H_\beta \setminus G'$ , then by Lemma 4.4.3,  $g = [\alpha, \beta] \in [G', \beta] = [G', x]$ . If  $x \in G' \setminus Z(G)$ , then by Lemma 4.4.2(v),  $g \in [G', x]$ . So

$$|TZ_g| \geq \frac{(H_\beta \setminus Z(G))Z(G)}{Z(G)} = p^{2n} - 1.$$

**Case 2:**  $g \in G' \setminus Z(G)$ .

By Lemma 4.4.4, we get

$$|TZ_g| \geq |\{ab : a \in A, b \in B \text{ and } ab \neq 1\}| = p^{2n} - 1.$$

Hence our claim holds true. Then by the counting argument, we get  $Pr_g(G) = \frac{p^{2n} - 1}{p^{5n}}$ , for each  $h \in G' \setminus 1$ . This completes the proof.  $\square$









# Bibliography

- [1] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I: The user language*, J. Symbolic Comput. **24** (1997), 235-265.
- [2] H. R. Brahana, *Finite metabelian groups and Plucker line-coordinates*, Amer. J. Math. **62** (1940), 365-379.
- [3] J. Cossey and T. O. Hawkes, *Sets of  $p$ -powers as conjugacy class sizes*, Proc. Amer. Math. Soc. **128** (2000), 49-51.
- [4] R. Dark and C. M. Scoppola, *On Camina groups of prime power order*, J. Algebra **181** (1996), 787-802.
- [5] A. K. Das and R. K. Nath, *On generalized relative commutativity degree of finite groups*, Int. Electronic. J. Algebra **7** (2010), 140-151.
- [6] S. Dolfi and E. Jabara, *The structure of finite groups of conjugate rank 2*, Bull. London Math. Soc. **41**(5) (2009), 916-926.
- [7] N. Gavioli, A. Mann, V. Monti, A. Previtalli and C. M. Scoppola, *Groups of prime power order with many conjugacy classes*, J. Algebra **202** (1998), 129-141.

- 
- [8] P. Hall, *The classification of prime-power groups*, J. Reine Angew. Math. **182** (1940), 130-141.
- [9] I. M. Isaacs, *Groups with many equal classes*, Duke Math. J. **37**(3) (1970), 501-506.
- [10] I. M. Isaacs, *Sets of  $p$ -powers as irreducible character degrees*, Proc. Amer. Math. Soc. **96**(4) (1986), 551-552.
- [11] K. Ishikawa, *Finite  $p$ -groups up to isoclinism, which have only two conjugacy lengths*, J. Algebra **220** (1999), 333-345.
- [12] K. Ishikawa, *On finite  $p$ -groups which have only two conjugacy lengths*, Israel J. Math. **129**(1) (2002), 119-123.
- [13] N. Ito, *On finite groups with given conjugate types I*, Nayoga Math. J. **6** (1953), 17-28.
- [14] N. Ito, *On finite groups with given conjugate types II*, Osaka J. Math. **7** (1970), 231-251.
- [15] N. Ito, *On finite groups with given conjugate types III*, Mathematische Zeitschrift **117** (1970), 267-271.
- [16] N. Ito, *Simple groups of conjugate rank 4*, J. Algebra **20** (1972), 226-249.
- [17] I. D. Macdonald, *Some  $p$ -groups of Frobenius and extra-special type*, Israel J. Math. **40** (1981), 350-364.
- [18] A. Mann and C. M. Scoppola, *On  $p$ -groups of Frobenius type*, Arch. Math. (Basel) **56**(4) (1991), 320-332.
-

- 
- [19] A. Mann, *Conjugacy classes in finite  $p$ -groups*,  
(link: [http://istanbulgroup.metu.edu.tr/Mann\\_Lecture1.pdf](http://istanbulgroup.metu.edu.tr/Mann_Lecture1.pdf) )
- [20] T. K. Naik and M. K. Yadav, *Finite  $p$ -groups of conjugate type  $\{1, p^3\}$* ,  
J. Group Theory **21**(1) (2018), 65-82.
- [21] T. K. Naik, R. D. Kitture and M. K. Yadav, *Finite  $p$ -Groups of Nilpotency Class 3 with Two Conjugacy Class Sizes*, submitted.  
(arxiv link: <https://arxiv.org/abs/1708.03245.pdf> )
- [22] T. K. Naik, *On the probability distribution associated to commutator word map in finite groups II*, submitted.  
(arxiv link: <https://arxiv.org/pdf/1805.00091.pdf> )
- [23] R. K. Nath and M. K. Yadav, *On the probability distribution associated to commutator word map in finite groups*, Internat. J. Algebra and Comput. **25** (2015), 1107-1124.
- [24] G. Parmeggiani and B. Stellmacher,  *$p$ -groups of small breadth*, J. Algebra **213** (1999), 52-68.
- [25] M. R. Pouranki and R. Sobhani, *Probability that the commutator of two group element is equal to a given element*, J. Pure and Applied Algebra **212** (2008), 727-734.
- [26] A. Shalev, *Word maps, conjugacy classes and a noncommutative Waring-type theorem*, Ann. Math. **170**(3) (2009), 1383-1416.
- [27] M. R. Vaughan-Lee, *Breadth and commutator subgroups of  $p$ -groups*, J. Algebra **32** (1974), 278-285.
-

- [28] L. Verardi, *Gruppi semiextraspeciali di esponente  $p$* , Ann. Mat. Pura Appl. **148**(4) (1987), 131-171.
- [29] B. Wilkens, *2-Groups of breadth 3*, J. Algebra **318** (2007), 202-224.
-



