COMMUTATORS AND COMMUTATOR SUBGROUPS IN FINITE P-GROUPS

By
RAHUL KAUSHIK
MATH08201604003

Harish-Chandra Research Institute, Prayagraj

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

December, 2021

Homi Bhabha National Institute[1]

Recommendations of the Viva Voce Committee

As members of the Viva Voce Committee, we certify that we have read the dissertation prepared by **Rahul Kaushik** entitled "**Commutators and commutator subgroups in finite p-groups**" and recommend that it may be accepted as fulfilling the thesis requirement for the award of Degree of Doctor of Philosophy.

Chairman – Prof. C. S. Dalawat	Date: 11-05-2022
Guide / Convener – Prof. Manoj Kumar	Date: 11-05-2022
Examiner - Prof. R. P. Shukla	Date: 11-05-2022
Member 1- Prof. R. Thangadurai	Date: 11-05-2022
Member 2- Prof. D. Surya Ramana	Date: 11-05-2022
Member 3- Prof. Ratnakumar PK	Date: 11-05-2022

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: 11-05-2022

Place: Prayagraj

Prof. Manoj Kumar
Guide

[1] 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.

Rahul Kaushik

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.

Rahul Kaushik

List of Publications arising from the thesis

Journal

1. "Commutators and commutator subgroup of finite p-groups," Rahul Kaushik and Manoj K. Yadav, *J. Algebra*, **2021**, *568*, 314-348.

Others

1. "Commutators in groups of order p^7," Rahul Kaushik and Manoj K. Yadav, communicated.

Conferences

1. Presented a talk "Commutators and commutator subgroup of finite p-groups" in the 86th Annual Conference of The Mathematical Society, VIT Vellore, December, 2020.

2. Presented a talk "Commutators and commutator subgroup of finite p-groups" International Conference on Number Theory and Algebra, IIT BHU, December, 2020.

3. Presented a talk "Commutators and commutator subgroup of finite p-groups" 35th Annual Conference of the Ramanujan Mathematical Society, Central University of Rajasthan, December, 2020.

Rahul Kaushik

Dedicated to

my beloved family

Mr. Surender Kaushik and Mrs. Shakuntala Devi

Mr. Jitender Kumar and Mrs. Pooja

ACKNOWLEDGEMENTS

Working as a PhD student in HRI was a magnificent as wel
xperience for me. years,

Manoj K

T

ers Prof. C. S.

Banwari, J

AE

ff

, especia

G

hit, Rishabh, Priyanshu, Parul, S[illegible] [illegible]m, N[illegible] [illegible]. Anup, Prade[illegible] [illegible]. Tushar, Lalit, D[illegible] [illegible] [illegible]kur, Durgesh, Brijmo-[illegible]. I [illegible]ctoral fellow[illegible] [illegible]

[illegible] v [illegible]

U[illegible]

[illegible]

Contents

Summary

This thesis contributes to classification of finite p-groups upto isoclinism in which every element of the commutator subgroup is not a commutator. In the first part we classify finite p-groups having the commutator subgroup of order p^4 and exponent p. Second part consist of a classification of groups of order p^7. Moreover, we determine that the commutator length of groups in both the cases, is atmost 2.

Notations

G	a group
$H \leq G$	H is a subgroup of G
$[x, y]$	commutator $x^{-1}y^{-1}xy$ for $x, y \in G$
$\gamma_2(G)$	commutator subgroup of G
$\Phi(G)$	Frattini subgroup of G
$\gamma_i(G)$	i-th term of the lower central series of G
$\mathrm{Z}_i(G)$	i-th term of the upper central series of G
$d(G)$	cardinality of a minimal generating set of a finitely generated group G
$\mathrm{Z}(G)$	center of G
$\mathbb{F}_p$	Field of order p
$[H, K]$	set of all commutators $[h, k], h \in H, k \in K$
$\mathrm{C}_G(X)$	centralizer of $x \in G$
$\Omega_i(G)$	$\{x \in G \mid x^{p^i} = 1\}$
$\mho_i(G)$	$\{x^{p^i} \mid x \in G\}$
$\exp(G)$	exponent of G
$cl(G)$	commutator length of G
$c(G)$	nilpotency class of G

CHAPTER 1

Background and Preliminaries

This chapter has three sections. In the first section, we introduce the problem and present a historical background. In the second section, we introduce the concept of isoclinism of finite groups. In the last section of this chapter, we provide some definitions and results, which are used later in the thesis.

1.1 Background of the problem

Let G be a finite group and $\mathrm{K}(G) := \{[a, b] \mid a, b \in G\}$ the set of commutators. It is well known that $\mathrm{K}(G)$ generates the commutator subgroup $\gamma_2(G)$. Generally, a subgroup is not equal to its set of generators; in this respect, the commutator subgroup is no different. More precisely, $\mathrm{K}(G) \neq \gamma_2(G)$ in general. In the literature, the earliest example of a group G in which not every element of $\gamma_2(G)$ is a commutator, was given by W. B. Fite [7]. The order of the group in this example is 256. In 1980 R. M. Guralnick [10], proved that the smallest order of such a group G is 96. In fact, there are two such groups of order 96.

A natural question that has attracted the attention of several mathematicians over the past one century is whether the commutator subgroup $\gamma_2(G)$ is equal to K(G) or not for groups G in a given class of groups. In 1899, G. A. Miller [32] investigated the class of alternating groups A_n and proved that $K(A_n) = \gamma_2(A_n)$, for all $n \geq 5$. N. Ito [20] and O. Ore [36] reinvented the result of G. A. Miller in 1951, and O. Ore conjectured that every element of a non abelian finite simple group is a commutator. The conjecture was finally settled in 2010 by M. W. Liebeck, et al.[27]. It is also true that $K(G) = \gamma_2(G)$ for most of the finite quasi-simple groups [28]. Furthermore, the commutator length of all finite quasi-simple groups is at most 2. The commutator length of a finite group G, denoted by $cl(G)$, is the smallest positive integer n such that every element of $\gamma_2(G)$ can be written as a product of at most n commutators in G. Thus it is clear that $K(G) = \gamma_2(G)$ if and only if $cl(G) = 1$.

In the following Theorem, I. M. Issaacs [19] gave a way of constructing examples of finite groups G in which $K(G) \neq \gamma_2(G)$.

Theorem 1.1.1 *Let $G = M \wr N$ be the wreath product of finite groups M and N, where M is abelian and N is non-abelian. If*

$$\sum_{A\in\mathcal{A}} \left(\frac{1}{|M|}\right)^{[N:A]} \leq \frac{1}{|M|},$$

then $K(G) \neq \gamma_2(G)$, where $\mathcal{A}$ is the set of all maximal abelian subgroups of N. In particular, this inequality holds whenever $|M| \geq |\mathcal{A}|$

If we take $|M| = 2$ and N non abelian of order 6, then the resulting group G of order $2^7.3$ is an example such that $K(G) \neq \gamma_2(G)$ but the inequality of the preceding theorem does not hold. Thus the inequality is not neccessary condition here. Also the method given by I. M. Isaacs can be used to construct both solvable as well as perfect groups.

The solution of the above problem for non-perfect groups seems much more challenging. In 1902, W. B. Fite [7] proved that if a finite p-group G is of nilpotency class 2 and $G/\operatorname{Z}(G)$ is minimally generated by three elements, then $\operatorname{K}(G) = \gamma_2(G)$. He also gave examples of 2-groups G of nilpotency class 2 with $G/\operatorname{Z}(G)$ minimally generated by four elements and $\operatorname{K}(G) \neq \gamma_2(G)$. The smallest such 2-group is of order 2^8. There do exist such groups of order p^8 for all odd primes (see Theorem 3.1.1). In 1953, K. Honda [17] reinvented the famous character sum formula of F. G. Frobenius, in a slightly different form, for determining whether a given element of a finite group is a commutator or not. This result was used to prove that if the commutator subgroup $\gamma_2(G)$ of a finite group G is generated by a commutator, then each generator of $\gamma_2(G)$ is a commutator. In 1963, I. D. Macdonald [29] studied the groups with cyclic commuatator subgroups and showed that the commutator subgroup of such groups need not be generated by a commutator. Macdonald's result is summarized as follows:

Theorem 1.1.2 *Let G be a group such that $\gamma_2(G)$ is cyclic and either G is nilpotent or $\gamma_2(G)$ is infinite. Then $\gamma_2(G)$ is generated by a suitable commutator. Moreover, for any given positive integer n there exists a group G having cyclic commutator subgroup and generated by no set of fewer than n commutators.*

In 1973, D. M. Rodney [38] generalised the preceding work of Macdonald and proved that if G has cyclic commutator subgroup and either G is nilpotent or $\gamma_2(G)$ is infinite, then $\operatorname{K}(G) = \gamma_2(G)$. Later in 1977, he proved the following result:

Theorem 1.1.3 ([39]) *If G is finite and $\gamma_2(G)$ is elementary abelian of order p^3 for any prime integer p, then $\operatorname{K}(G) = \gamma_2(G)$.*

This result was further generalised by R. M. Guralnick [11], where he proved that if G is a finite group and $\gamma_2(G)$ is an abelian p-group minimally generated by at most 3 elements, where $p \geq 5$, then $\operatorname{K}(G) = \gamma_2(G)$. In 2019, G. A. Fernández-Alcober and I. De las Heras [5] relaxed the condition of commutativity of $\gamma_2(G)$ in the result of R. M. Guralnick [11], when $d(\gamma_2(G)) = 2$, and proved the following result.

Theorem 1.1.4 ([5]) *Let G be a finite p-group. If $\gamma_2(G)$ can be generated by 2 elements, then $\gamma_2(G) = \{[x, g] \mid g \in G\}$ for a suitable $x \in G$.*

I. De las Heras [15] proved a more general result in 2020, which is as follows:

Theorem 1.1.5 ([15]) *Let G be a finite p-group with $p \geq 5$. If $\gamma_2(G)$ can be generated by 3 elements, then $\mathrm{K}(G) = \gamma_2(G)$.*

A generalization of some of these results for commutators of higher weights has also been studied in the literature. The interested reader may refer to [3, 12, 13, 16]. If we take order of the group into consideration, then in 2005, L. C. Kappe and R. F. Morse [23] proved the following result:

Theorem 1.1.6 ([23]) $\mathrm{K}(G) = \gamma_2(G)$ *for all p-groups of order at most p^5 and for all 2-groups of order at most 2^6. Moreover, there exist groups of order p^6, $p > 2$, and 2^7 such that $\mathrm{K}(G) \neq \gamma_2(G)$.*

In the preceding result, counter example of the group G of order p^6, $p \geq 5$, is of nilpotency class 4 with $\gamma_2(G)$ 4-generated, and the groups of order 2^7 and 3^6 are of the nilpotency class 3 and 4 respectively, having the commutator subgroup generated by 3 elements. Examples of groups G of order p^8 and nilpotency class 2 such that $\mathrm{K}(G) \neq \gamma_2(G)$ were constructed by I. D. Macdonald [30, Exercise 5, Page 78]. The counter examples of groups of order 2^8 and p^6 admit elementary abelian commutator subgroups of order 2^4 and p^4 respectively.

Interested reader may refer to [24] for more detailed literature about the problem discussed above.

Remark 1.1.1 *It is evident that a condition only on the prime p or on the rank of $\gamma_2(G)$ for a finite group G can not ensure that $\mathrm{K}(G) \neq \gamma_2(G)$.*

1.2 Isoclinism

The following concept of isoclinism of groups is due to P. Hall [14]. He introduced it while studying the classification of prime power order groups. Let G be a group. Define a map $\alpha_X : G/\operatorname{Z}(G) \times G/\operatorname{Z}(G) \longrightarrow \gamma_2(G)$ such that $\alpha_X(g_1 \operatorname{Z}(G), g_2 \operatorname{Z}(G)) = [g_1, g_2]$ for $(g_1, g_2) \in G \times G$. This map is well defined, and called the commutator map. We say two groups G and H are *isoclinic* if there exists an isomorphism ϕ of the factor group $\bar{G} = G/\operatorname{Z}(G)$ onto $\bar{H} = H/\operatorname{Z}(H)$, and an isomorphism θ of the subgroup $\gamma_2(G)$ onto $\gamma_2(H)$ such that the following diagram is commutative

$$\begin{array}{ccc} \bar{G} \times \bar{G} & \xrightarrow{\alpha_G} & \gamma_2(G) \\ {\scriptstyle \phi\times\phi}\downarrow & & \downarrow{\scriptstyle \theta} \\ \bar{H} \times \bar{H} & \xrightarrow{\alpha_H} & \gamma_2(H). \end{array}$$

The resulting pair (ϕ, θ) is called an *isoclinism* of G onto H. Isoclinism is an equivalence relation among the groups. The equivalence classes under the isoclinism relation are called *isoclinism families*.

Definition 1.2.1 *A p-group G is called extra-special, if $\operatorname{Z}(G)$ and $\gamma_2(G)$ are equal, and of order p.*

In the following result P. Hall [14], proved the existence of an important group in each isolclinism class of groups.

Lemma 1.2.1 *In the isoclinism family of a group G, there exists a group H such that $\operatorname{Z}(H) \leq \gamma_2(H)$.*

Such a group H is called a *stem group* in the isoclinism family of G. The following result is a straightforward consequence of the preceding lemma.

Corollary 1.2.2 *Let G be a finite p-group such that $|\gamma_2(G)| = p$. Then G is isoclinic to an extra-special p-group.*

Lemma 1.2.2 *Let G and H be two isoclinic finite p-groups. Then $\mathrm{K}(G) = \gamma_2(G)$ if and only if $\mathrm{K}(H) = \gamma_2(H)$.*

Proof. Since isoclinism is an equivalence relation, it is sufficient to prove one side implication. So assume that $\mathrm{K}(G) = \gamma_2(G)$, and the map α_G in the above commutative diagram is surjective. Let $u \in \gamma_2(H)$ be an arbitrary element. There exists $(\bar{g}_1, \bar{g}_2) \in \bar{G} \times \bar{G}$ such that $\theta(a_G(\bar{g}_1, \bar{g}_2)) = u$. Thus there exists $(\bar{h}_1, \bar{h}_2) \in \bar{H} \times \bar{H}$, namely $(\phi(\bar{g}_1), \phi(\bar{g}_2))$, such that $a_H(\bar{h}_1, \bar{h}_2) = u$ proving that α_H is surjective, and the proof is complete. □

1.3 Key Lemmas

In this section, we provide some definitions and lemmas which will be used in further chapters.

Definition 1.3.1 *The Frattini subgroup $\Phi(G)$ of a group G is the intersection of all maximal subgroups of G. If G is a finite p-group, then $\Phi(G) = \mho_1(G)\gamma_2(G)$.*

Lemma 1.3.1 *Let G be a finite p-group with $\gamma_2(G)$ elementary abelian of order p^4. If the nilpotency class of G is at most 3, then $\mho_1(G) \leq \mathrm{Z}(G)$ for all $p \geq 3$. Otherwise the conclusion, in general, holds only for $p \geq 5$.*

Proof. Since $\gamma_2(G)$ is of order p^4, the nilpotency class of G is at most 5. Thus, $\gamma_2(G)$ being elementary abelian, for all $x, y \in G$, we have

$$[x, y^p] = [x, y]^p[x, y, y]^{\binom{p}{2}}[x, y, y, y]^{\binom{p}{3}}[x, y, y, y, y]^{\binom{p}{4}} = 1.$$

Hence $y^p \in Z(G)$. □

Remark 1.3.1 *If G is a stem group in the isoclinism family of groups satisfying the hypotheses of Lemma 1.3.1, then $\Phi(G) = \gamma_2(G)$.*

Lemma 1.3.2 *For a finite p-group G of nilpotency class at least 4, $\mathrm{Z}(G)\cap\gamma_2(G)$ cannot be maximal in $\gamma_2(G)$.*

Proof. Contrarily assume that $\mathrm{Z}(G)\cap\gamma_2(G)$ is maximal in $\gamma_2(G)$. Thus $|\gamma_2(G) : \mathrm{Z}(G)\cap\gamma_2(G)| = p$ and therefore the nilpotency class of $G/(\mathrm{Z}(G)\cap\gamma_2(G))$ is 2, which is possible only when $\gamma_3(G) \leq \mathrm{Z}(G)$, a contradiction. □

Definition 1.3.2 *We say that a finite p-group G is of conjugate type $\{1, p^r, p^s\}$ if this set constitutes the set of conjugacy class sizes of all elements of G, where $r \leq s$ are positive integers.*

Definition 1.3.3 *[9, p.28] A group G is said to be an amalgamated (internal) semidirect product of subgroups M by N over K, written $G = M \rtimes_K N$, if $M \trianglelefteq G$, $G = MN$ and $M \cap N = K$. In particular, if $[M, N] = 1$ then $K \leq Z(G)$, and we call G the central product of M by N over K, written $G = M \times_K N$.*

Lemma 1.3.3 *Let a finite group G be a central product of its subgroups M and N. Then $\mathrm{K}(G) = \gamma_2(G)$ if and only if $\mathrm{K}(M) = \gamma_2(M)$ and $\mathrm{K}(N) = \gamma_2(N)$.*

Lemma 1.3.4 *Let G be a group of order p^7 and nilpotency class 4 with $|\gamma_2(G)| = p^5$. Then $\gamma_2(G)$ is abelian.*

We now mention very elementary but extremely useful observations.

Lemma 1.3.5 *Let G be a finite group and H a normal subgroup of G. If $\mathrm{K}(G/H) \neq \gamma_2(G/H)$, then $\mathrm{K}(G) \neq \gamma_2(G)$.*

Proof. Let $\bar{G} = G/H$, and $\bar{x} \in \gamma_2(\bar{G})$ be an element which is not in $\mathrm{K}(\bar{G})$. Then its pre-image $x \notin \mathrm{K}(G)$. Hence $\mathrm{K}(G) \neq \gamma_2(G)$. □

Lemma 1.3.6 *Let G be a group and H a normal subgroup of G contained in* $\mathrm{K}(G)$ *such that* $\mathrm{K}(G/H) = \gamma_2(G/H)$*. Then the commutator length of G is at most* 2.

Lemma 1.3.7 *Let G be a finite group and $H \leq \gamma_2(G) \cap Z(G)$. If there exist* $x_1, x_2, \ldots, x_n$ *such that* $\gamma_2(G)/H = \bigcup_{i=1}^{n} [x_iH, G/H]$ *and* $H \subseteq \bigcap_{i=1}^{n} [x_i, G]$*, then* $\gamma_2(G) = \bigcup_{i=1}^{n} [x_i, G]$.

Proof. Let $g \in \gamma_2(G)$ be any element. Then $g = [x_i, a]h$ for some $1 \leq i \leq n$ where $h = [x_i, b] \in Z(G)$ and $a, b \in G$. Therefore $g = [x_i, b][x_i, a] = [x_i, ba] \in [x_i, G]$. ☐

Let G be a p-group of maximal class of order p^n, that is, the nilpotency class of G is $n-1$. Then $\mathrm{C}_i := \mathrm{C}_G(\gamma_i(G)/\gamma_{i+2}(G))$ are called *two-step centralizers* in G, where $1 \leq i \leq n-2$. It is clear that $\gamma_2(G) \leq \mathrm{C}_i$ for all $1 \leq i \leq n-2$. Also, all C_i are characteristic maximal subgroups of G. An element $s \in G$ is said to be *uniform* if $s \notin \bigcup_{i=1}^{n-2} \mathrm{C}_i$. It was proved by N. Blackburn [2] that every finite p-group of maximal class admits uniform elements. The following result follows from [18, III.14.23 Satz] (may also see [31]).

Theorem 1.3.4 *Let G be a finite p-group of maximal class. Then* $\mathrm{K}(G) = \gamma_2(G)$*. More precisely,* $\gamma_2(G) = [s, G]$ *for a uniform element s of G.*

The following result is from [6, Theorem 4.7] (also see [18, III.14.14 Hilfssatz]), which also follows from [2, Theorem 3.2] as a special case.

Theorem 1.3.5 *Let G be a p-group of maximal class of order at most p^{p+1}. Then* $\exp(G/\mathrm{Z}(G)) = \exp(\gamma_2(G)) = p$.

The following basic identities will be used throughout, mostly without any further reference.

Lemma 1.3.8 *Let x, y, z be elements of a group G and n be a positive integer. Then the following identities hold in G:*

(i) $[x, yz] = [x, z][x, y]^z$,

(ii) $[xy, z] = [x, z]^y[y, z]$,

(iii) $[x, y^n] = [x, y]^n$ *whenever y centralizes $[x, y]$.*

We will use the Hall-Witt identity extensively, which is as follows:

Lemma 1.3.6 *If $x,\ y,\ z \in G$, then*

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

We now mention some number theoretic results. For a prime integer p and $d \in \mathbb{F}_p$, the field of p elements, Legendre symbol, denoted by $(\frac{d}{p})$, is defined as

$$\left(\frac{d}{p}\right) = \begin{cases} 0 & d = 0, \\ 1 & d \text{ is quadratic residue } \pmod{p}, \\ -1 & d \text{ is non-quadratic residue } \pmod{p}. \end{cases}$$

Lemma 1.3.9 *Let p be an odd prime and $f(\lambda, \mu) = a\lambda^2 + b\lambda\mu + c\mu^2$ be a binary quadratic form over $\mathbb{F}_p^*$. If p divides $b^2 - 4ac$, then $f = 0$ has a nontrivial solution in $\mathbb{F}_p^*$.*

Proof. Let μ be a fixed element of $\mathbb{F}_p^*$. Then $f = a\lambda^2 + b\lambda\mu + c\mu^2$ will be a quadratic equation in λ, whose discriminant $(b^2 - 4ac)\mu^2$ is zero in $\mathbb{F}_p$. Thus $\lambda = -b\mu/2a$ is a nontrivial solution of $f = 0$. □

We say that a binary quadratic form $f(\lambda, \mu) = a\lambda^2 + b\lambda\mu + c\mu^2$ represents an integer r, if there exist some integers λ_0, μ_0 such that $f(\lambda_0, \mu_0) = r$. The following theorem and its corollary are proved in [33, Chapter 3, Page 153].

Theorem 1.3.7 *Let $n \neq 0$ and d be given integers. Then there exist a binary quadratic form having discriminant d that represents n if and only if the congruence $x^2 \equiv d \pmod{4|n|}$ has a solution.*

Corollary 1.3.8 *Let p be an odd prime and $d = 0$ or $1 \pmod 4$. There exists a binary quadratic form of discriminant d that represents p if and only if $(\frac{d}{p}) = 1$.*

Lemma 1.3.10 *Let $f(\lambda, \mu) = m\lambda^2 + n\lambda\mu - \mu^2$ and $g(\lambda, \mu) = \lambda^2 + n\lambda\mu - m\mu^2$, be two quadratic forms, where p is an odd prime and $m, n \in \mathbb{F}_p^*$. Then $f(\lambda, \mu) = 0$ admits only a trivial solution in $\mathbb{F}_p$ if and only if $g(\lambda, \mu) = 0$ does the same.*

Proof. Assume that $f(\lambda, \mu) = 0$ implies $\lambda = \mu = 0$ in $\mathbb{F}_p$. Let f represent p; meaning there exist $\lambda_0, \mu_0 \in \mathbb{Z}$ such that $f(\lambda_0, \mu_0) = p$. If both λ_0 and μ_0 are multiple of p, then p^2 divides p $(-\ m\lambda_0^2 + n\lambda_0\mu_0 - \mu_0^2)$, which is not possible. Hence, it follows that none of λ_0, μ_0 is congruent to zero modulo p. Thus $\lambda_0 \equiv a_0 \pmod p$ and $\mu_0 \equiv b_0 \pmod p$ for some $a_0, b_0 \in \mathbb{F}_p^*$ such that $f(a_0, b_0) \equiv 0 \pmod p$. This contradicts our assumption. Therefore f does not represent p. By our assumption and Lemma 1.3.9, $n^2 + 4m \in \mathbb{F}_p^*$, and since $n^2 + 4m \equiv 0, 1 \pmod 4$, it follows from Corollary 1.3.8 that $\left(\frac{n^2+4m}{p}\right) = -1$. Hence $x^2 \equiv n^2 + 4m \pmod p$ does not have a solution. Now let $g(\lambda, \mu) = 0$ admits a non-trivial solution. Thus g represents ps for some $s \in \mathbb{F}_p$, hence by Theorem 1.3.7 we get $x^2 \equiv n^2 + 4m \pmod{4ps}$ has a solution. Thus $x^2 \equiv n^2 + 4m \pmod p$ also has a solution, which is not possible. Hence $g(\lambda, \mu) = 0$ has only trivial solution. Converse also follows on the same lines. □

CHAPTER 2

Reduction Argument and 2-Groups

In this chapter we provide reduction argument for finite p-groups, $p \geq 2$, which reduces our study to the groups of smaller order. Further we give a classification of finite 2-groups G with $\gamma_2(G)$ elementary abelian of order 16 such that $\mathrm{K}(G) \neq \gamma_2(G)$.

2.1 Reduction argument

We start this section by defining breadth of an element.

Definition 2.1.1 *For a finite p-group G, the breadth of an element $x \in G$, denoted by $b(x)$, is defined as*

$$p^{b(x)} := |G : \mathrm{C}_G(x)|,$$

and the breadth of G, denoted by $b(G)$, is defined as

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

First we prove reduction theorem for odd primes. In 1999, G. Parmeggiani and B. Stellmacher [37] provided a classification of finite p-groups, $p \geq 3$, of breadth 3. They prove the following result.

Corollary 2.1.2 *Let p be an odd prime and G a finite p-group. Then $b(G) = 3$ if and only if one of the following holds:*

(i) $|\gamma_2(G)| = p^3$ *and* $|G : \mathrm{Z}(G)| \geq p^4$.

(ii) $|\gamma_2(G)| \geq p^4$ *and* $|G : \mathrm{Z}(G)| = p^4$.

(iii) $|\gamma_2(G)| = p^4$ *and there exists a normal subgroup H of G with $|H| = p$ and* $|G/H : \mathrm{Z}(G/H)| = p^3$.

We remark that the preceding result was also proved in [8, Corollary 3] for $p \geq 5$.

Remark 2.1.3 *Let G be a finite p-group with $|\gamma_2(G)| = p^4$. Then by [37, Theorem A] it follows that $b(G) \geq 3$. We will use this information throughout without any further reference.*

Using Theorem 2.1.2 we prove the following reduction theorem for finite p-groups, $p \geq 3$, which reduces our study mainly to the groups of small orders, mainly upto p^9.

Theorem 2.1.4 *Let L be a finite p-group of breadth 3 such that $\mathrm{Z}(L) \leq \gamma_2(L)$ and $\gamma_2(L)$ is elementary abelian of order p^4. If the nilpotency class of L is 3 and $p \geq 3$, then one of the following holds:*

(i) *There exists a 2-generator subgroup G of L of order p^6 having the same nilpotency class as that of L such that $\gamma_2(G) = \gamma_2(L)$. Moreover, if $|L| \geq p^7$, then*

L is an amalgamated semidirect product of G and a subgroup K with $|\gamma_2(K)| \le p$. Furthermore, if K is non-abelian, then it is isoclinic to an extraspecial p-group.

(ii) *There exists a 2-generator subgroup G of L of order p^5 having the same nilpotency class as that of L such that $\gamma_2(G) < \gamma_2(L)$. Moreover, $|L| \ge p^7$ and L is a central product of G and a subgroup K of nilpotency class 2, which is isoclinic to an extraspecial p-group.*

(iii) *There exists a 3-generator subgroup G of L of order p^7 having the same nilpotency class as that of L such that $\gamma_2(G) = \gamma_2(L)$. Moreover, if $|L| \ge p^8$, then L is an amalgamated semidirect product of G and a subgroup K with $|\gamma_2(K)| \le p$. Furthermore, if K is non-abelian, then it is isoclinic to an extraspecial p-group.*

If the nilpotency class of L is 4 and $p \ge 3$, then only (i) *holds.*

Proof. Since $b(L) = 3$, it follows from Theorem 2.1.2 that either $|L : \mathrm{Z}(L)| = p^4$ or L admits a subgroup H of order p such that $|L/H : \mathrm{Z}(L/H)| = p^3$. First let $|L : \mathrm{Z}(L)| = p^4$. Since the nilpotency class of L is at least 3 and $\mathrm{Z}(L) \le \gamma_2(L)$, it follows that $|\mathrm{Z}(L)| \le p^3$. Also $\mathrm{Z}(L)$ can not be of order p, otherwise L will be order p^5, which is not possible. If $\mathrm{Z}(L)$ is of order p^2, then clearly L is a 2-generator group of order p^6. If $\mathrm{Z}(L)$ is of order p^3, then it follows from Lemma 1.3.1 that L is a 3-generator group of order p^7. Moreover, when L is a 3-generator group of order p^7, then it follows from Lemma 1.3.2 that the nilpotency class of L is 3. Now consider the second case, which we divide into two subcases, depending on the nilpotency class of L.

First assume that the nilpotency class of L is 3. Then $H = \gamma_3(L)$, $H < \gamma_3(L)$ or $H \not\le \gamma_3(L)$. We consider these possibilities one by one. If $H = \gamma_3(L)$, then the nilpotency class of L/H is 2 and $|L/H : \mathrm{Z}(L/H)| = p^3$, and therefore, using Lemma 1.3.1, it follows that except three generators a, b, c (say) of L, all other generators $x_1, x_2, \ldots, x_k$, $k \ge 0$, are such that $[x_i, L] \le H$. Since $\mathrm{Z}(L) \le \gamma_2(L)$, we can, more precisely, say that $[x_i, L] = H$ for all $1 \le i \le k$. So it follows that

$\gamma_2(L)/H = \gamma_2(G)H/H$ is of order p^3, where $G := \langle a, b, c\rangle$ is a subgroup of L. We claim that $H \leq \gamma_2(G)$. As observed above $[x_i, L] = H$ is of order p, it follows that, for all $1 \leq i \leq k$, $\mathrm{C}_L(x_i)$ is maximal in L, and therefore contains $\gamma_2(L)$. Thus any generator h of H, which lies in $\gamma_3(L) = [\gamma_2(L), L]$, can be written as

$$h = [w_1^{\alpha_1} w_2^{\alpha_2} w_3^{\alpha_3}, a^{\beta_1} b^{\beta_2} c^{\beta_3} x_1^{n_1} \ldots x_k^{n_k}] = [w_1^{\alpha_1} w_2^{\alpha_2} w_3^{\alpha_3}, a^{\beta_1} b^{\beta_2} c^{\beta_3}] \in \gamma_3(G),$$

where w_1H, w_2H, w_3H generate $\gamma_2(G)H/H$. The nice presentation of h in the preceding statement is possible because $H \leq \mathrm{Z}(L)$ and $\gamma_2(L) \leq \mathrm{C}_L(x_i)$. Hence our claim follows, which, in turn, implies that $\gamma_2(G) = \gamma_2(L)$. Thus G is of order p^7 and nilpotency class 3. Let $K := \langle x_1, \ldots, x_k\rangle$ be a subgroup of L. Since $[x_i, L] = H$ for $1 \leq i \leq k$, we have $\gamma_2(K) \leq H$, which shows that the nilpotency class of K is at most 2. Since $\gamma_2(L) \leq G$, K acts on G by conjugation. Hence L takes the desired form. If K is non-abelian, then, in view of Corollary 1.2.2, K is isoclinic to an extraspecial p-group.

If $H < \gamma_3(L)$, then the nilpotency class of L/H is 3 and $|L/H : \mathrm{Z}(L/H)| = p^3$. Hence by the given hypothesis and Lemma 1.3.1, we conclude that L can be generated by $\{a, b, x_1, \ldots, x_k\}$ such that $[x_i, L] = H$. Now, using the same arguments as in the preceding case, the assertion follows by assuming $G := \langle a, b\rangle$ and $K := \langle x_1, \ldots, x_k\rangle$, where $|G| = p^6$.

Finally, if $H \not\leq \gamma_3(L)$, then, obviously, $H \cap \gamma_3(L) = 1$. Thus the nilpotency class of L/H is also 3. Again invoking the given hypothesis and Lemma 1.3.1, we can assume that L is generated by the set $\{a, b, x_1, \ldots, x_k\}$ such that $[x_i, L] = H$. Let $G_1 := \langle a, b\rangle$. Notice that $\gamma_2(G_1)H/H = \gamma_2(L)/H$ is of order p^3, $|G_1H/H| = p^5$, and G_1 and L agree on the nilpotency class. Since G_1 is 2-generator, $\gamma_2(G_1)/\gamma_3(G_1)$ is cyclic (of order p). Thus G_1 can not contain H, which implies that $|G_1| = p^5$. If $G_1 \leq \mathrm{C}_L(x_i)$, for all $1 \leq i \leq k$, then $K := \langle x_1, \ldots, x_k\rangle$ with $\gamma_2(K) = H$ is isoclinic to an extraspecial p-group, and therefore L is a central product of G_1 and K amalgamating some subgroup (possibly trivial). Hence $G = G_1$ and K are the desired subgroups. So assume that $G_1 \nleq C_L(x_i)$ for some i. Thus $[x_i, G_1] = H$, and the subgroup $G := \langle a, b, x_i \rangle$ of L is of order p^7. Hence, as argued above, one can easily see that G and $K := \langle x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k \rangle$ are the desired subgroups of L.

We now assume that the nilpotency class of L is 4. Then either $H = \gamma_4(L)$ or $H \neq \gamma_4(L)$. If $H \neq \gamma_4(L)$, then the nilpotency class of L/H is 4, which is not possible as $(L/H)/\mathrm{Z}(L/H)$, being of order p^3, can have nilpotency class at most 2. So assume that $H = \gamma_4(L)$. Then the nilpotency class of L/H is 3. Hence, by the given hypothesis, we conclude that L can be generated by $\{a, b, x_1, \ldots, x_k\}$ such that $[x_i, L] = H$. Since $|L/H : \mathrm{Z}(L/H)| = p^3$, it follows that $a^p, b^p \in \gamma_2(L)$. Now, using the same arguments as above, the assertion follows by assuming $G := \langle a, b \rangle$ and $K := \langle x_1, \ldots, x_k \rangle$, where $|G| = p^6$. This completes the proof of the theorem. □

Now we prove reduction theorem for 2-groups. In 2007, B. Wilkens [40] gave a classification of 2-group of breadth 3. The result is as follows:

Theorem 2.1.5 *Let L be a finite 2-group of breadth 3. Then one of the following holds:*

(i) $|\gamma_2(L)| \leq 2^3$.

(ii) $|L : \mathrm{Z}(L)| \leq 2^4$.

(iii) $|\gamma_2(L)| = 2^4$ *and there is R, $R \leq \Omega_1(\mathrm{Z}(L))$, $|R| = 2$, such that* $|L/R : \mathrm{Z}(L/R)| \leq 2^3$.

(iv) $|\gamma_2(L)| = 2^4$ *and L is a central product $G\,\mathrm{C}_L(G)$, with $\mathrm{C}_L(G)$ is abelian and G lies in one of the following five classes of groups:*

(1) *There are $i, j \in \mathbb{N}$ with $G \cong \hat{G}/\langle x^{4i}, y^{4j} \rangle$, where* $\gamma_1(\hat{G}) = 1 = \mho_2(\gamma_2(\hat{G})) = \mho_1(\gamma_3(\hat{G}))$, *and $\hat{G}$ is free in the category of these groups.*

(2) *There are* $i, j \in \mathbb{N}$ *with* $G \cong \hat{G}/\langle x^{4i}, y^{2j}\rangle$, *where*

$$\hat{G} = \langle x, y \mid [x, y]^y = [y, x], [y, {}_2x]^2 = 1 = [y, {}_3x]^2 = [y, {}_2x, y] = [y, {}_3x, y] = [y, {}_4x]\rangle .$$

(3) *There are* $i, j, k \in \mathbb{N}$ *with* $G \cong \hat{G}/\langle x^{4i}, y^{2j}, z^{2k}\rangle$, $\hat{G} = \langle x, y, z\rangle$ *has* $\gamma_4(G) = 1 = \mho_1(\gamma_3(G))$, *and apart from that, is defined by the relations*

$$[x, y]^4 = 1 = [x, y]^2[x, y, y] = [x, y, z] = [x, z]^2 = [x, z, z] = [x, z, y] = [x, z, x] = [y, z].$$

(4) *There are* $i, j, k, l \in \mathbb{N}$ *with* $G \cong \hat{G}/\langle x^{2i}, y^{2j}, a^{2k}, t^{2l}\rangle$, $\hat{G} = \langle a, t, x, y\rangle$ *of nilpotency class* 3 *with additional relations*

$[x, a]^2 = 1 = [x, a, w] = [y, t, w] = [y, t]^2$, $w \in \{a, t, x, y\}$, $[x, t] = [y, t][y, a] = 1$, $[x, y]^4 = 1 = [x, y, a] = [x, y, t] = [x, y, y][x, y]^2 = [x, y, x][x, y]^2$, $[t, a] \in \langle [x, y]^2\rangle$.

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

Now we present reduction theorem for 2-groups, which reduces our study to 2-groups of nilpotency class 2 and 3, and to groups of order 2^7 if the nilpotency class is 3.

Theorem 2.1.6 *Let* L *be a finite* 2*-group such that* $\mathrm{Z}(L) \leq \gamma_2(L)$, $\gamma_2(L)$ *is elementary abelian of order* 2^4 *and* $b(L) = 3$. *Then*

(i) *The nilpotency class of* L *is either* 2 *or* 3.

(ii) *If the nilpotency class of* L *is* 2, *then* $|L| \geq 2^8$.

(iii) *If the nilpotency class of* L *is* 3, *then there exists a* 3*-generator subgroup* G *of* L *of order* 2^7 *having the same nilpotency class as that of* L *such that* $\gamma_2(G) = \gamma_2(L)$. *Moreover, if* $|L| \geq 2^8$, *then* L *is an amalgamated semidirect* *product of G and a subgroup K with $|\gamma_2(K)| = 2$. If K is non-abelian, then it is isoclinic to an extraspecial 2-group.*

Proof. For the given group L, one of the assertions (ii) - (iv) of Theorem 2.1.5 holds true. We start by noting that $|L| \geq 2^7$. Also, if Theorem 2.1.5(iv) holds, then L is isomorphic to a group in class (5) of Theorem 2.1.5(iv), which consists of groups of nilpotency class 2. So we only need to take into consideration the assertions (ii) - (iii) of Theorem 2.1.5. Let the nilpotency class of L be at least 4. Then, by Lemma 1.3.2, $\mathrm{Z}(L)$ can not be maximal in $\gamma_2(L)$. So in the case when Theorem 2.1.5(ii) holds, we must get $|\gamma_2(L)/\mathrm{Z}(L)| \geq 4$. Since L is non-abelian, it follows that $|L| \leq 2^6$, which is not possible as observed above. Now assume that Theorem 2.1.5(iii) holds. Then there exists a central subgroup R of order 2 such that $|L/R : \mathrm{Z}(L/R)| \leq 8$. Also the nilpotency class of L/R is at least 3. This is possible only when $|\gamma_2(L/R) : \gamma_2(L/R) \cap \mathrm{Z}(L/R)| = 2$, which, by Lemma 1.3.2, implies that the nilpotency class of L/R is 3. Thus $(L/R)/\mathrm{Z}(L/R)$ is non-abelian, which is not possible as shown in the next paragraph. Hence the nilpotency class of L is either 2 or 3. Let the nilpotency class of L be 2 and $|L| = 2^7$. Then L is generated by at most three elements, which is not possible. Hence $|L| \geq 2^8$ in this case.

Now we assume that the nilpotency class of L is 3. If Theorem 2.1.5(ii) holds, then, by the given hypotheses, it follows that $|\gamma_2(L)/\mathrm{Z}(L)| = 2$. Hence L itself is a 3-generator group of order 2^7. Next assume that Theorem 2.1.5(iii) holds. Thus there exists a central subgroup R of order 2 such that $|L/R : \mathrm{Z}(L/R)| \leq 8$. In our case, it is easy to deduce that $|L/R : \mathrm{Z}(L/R)| = 8$. Set $\bar{L} = L/R$. We claim that $\bar{L}/\mathrm{Z}(\bar{L})$ is abelian. Contrarily assume that $\bar{L}/\mathrm{Z}(\bar{L})$ is non-abelian. Then the nilpotency class of $\bar{L}$ is 3 and $\bar{L} = \big\langle \bar{a}, \bar{b}, \mathrm{Z}(\bar{L}) \big\rangle$ for some $a, b \in L$, where $\bar{x}$ denotes xR for $x \in L$. Since the exponent of $\bar{L}/\mathrm{Z}(\bar{L})$ can not be 2, it follows that $[\bar{a}, \bar{b}] = (\bar{a}^{\epsilon_1}\bar{b}^{\epsilon_2})^2$ modulo $\mathrm{Z}(\bar{L})$, where $\epsilon_i \in \mathbb{F}_2$. Hence $\mathrm{C}_{\bar{L}}([\bar{a}, \bar{b}])$ is maximal in $\bar{L}$. This implies that $[[\bar{a}, \bar{b}], \bar{L}]$ is of order 2, which contradicts the fact that $|\gamma_2(\bar{L})| = 8$. The claim is now settled. Thus the nilpotency class of $\bar{L}$ is 2. If the exponent of $\bar{L}/\mathrm{Z}(\bar{L})$ is 4, then $\bar{L} = \langle \bar{a}, \bar{b}, \mathrm{Z}(\bar{L}) \rangle$ for some $a, b \in L$. This implies that $|\gamma_2(\bar{L})| = 2$, which again contradicts the fact that $|\gamma_2(\bar{L})| = 8$. Hence the exponent of $\bar{L}/\mathrm{Z}(\bar{L})$ is 2, and therefore $\bar{L} = \langle \bar{a}, \bar{b}, \bar{c}, \mathrm{Z}(\bar{L}) \rangle$ for some $a, b, c \in L$.

Let $G := \langle a, b, c \rangle$. As proved in the reduction theorem for p odd case, $\gamma_2(G) = \gamma_2(L)$, and therefore $|G| = 2^7$. Let $|L| \geq 2^8$. Then $L = \langle a, b, c, x_1, \ldots, x_k \rangle$ for some integer $k \geq 1$. Let $K := \langle x_1, \ldots, x_k \rangle$. Then $[x_i, K] = R$. It now follows that G and K are the desired subgroups, which completes the proof. □

2.2 2-Groups with $|\gamma_2(G)| = 16$ and $exp(\gamma_2(G)) = 2$

Recall that in Theorem 1.1.6, L. C. Kappe and R. F. Morse proved that $\mathrm{K}(G) = \gamma_2(G)$ for all 2-groups of order at most 2^6. They also constructed example of group G of order 2^7 having the nilpotency class 3 and commutator subgroup generated by 3 elements such that $\mathrm{K}(G) \neq \gamma_2(G)$. The counter examples of order 2^8 admit elementary abelian commutator subgroup of order 2^4. The groups of order p^7 will be investigated in the Chapter 4, in this section we provide a classification of finite 2-groups G (up to isoclinism) having $\gamma_2(G)$ elementary abelian of order 16 such that $\mathrm{K}(G) \neq \gamma_2(G)$. We start by the following definition:

Definition 2.2.1 *We say that a finite p-group G is of conjugate type* $\{1, p^r, p^s\}$ *if this set constitutes the set of conjugacy class sizes of all elements of G, where* $r \leq s$ *are positive integers.*

Here is the main theorem of this section.

Theorem 2.2.1 *Let G be a finite 2-group such that* $\mathrm{Z}(G) \leq \gamma_2(G)$ *and* $\gamma_2(G)$ *is elementary abelian of order* 16*. Then* $\mathrm{K}(G) \neq \gamma_2(G)$ *if and only if one of the following holds :*

(1) *G is isoclinic to the following special 2-group of order 2^9 presented as:*

$$\langle v_1, v_2, v_3, v_4, v_5 \mid [v_1, v_2] = [v_2, v_3] = [v_3, v_1] = [v_4, v_2] = [v_5, v_1] = 1, [v_3, v_4] = [v_3, v_5], [x, y, z] = 1 \text{ for all } x, y, z \in \{v_1, \ldots, v_5\}, v_i^2 = 1\ (1 \le i \le 5)\rangle.$$

(2) *G is of order 2^8 and nilpotency class 2 along with one of the following:*

(2a) *G admits a non-central element whose centralizer in G is a maximal subgroup.*

(2b) *G is of conjugate type $\{1, 4, 8\}$ and admits no generating set $\{x_1, x_2, x_3, x_4\}$ such that $[x_1, x_2] = 1 = [x_3, x_4]$.*

Moreover, if $\mathrm{K}(G) \neq \gamma_2(G)$, then the commutator length of G is 2.

We deduce the following result using GAP [4]. A theoretical proof goes on the lines of Lemma 3.4.1 in Chapter 3.

Lemma 2.2.2 *Let G be a group of order 2^7 with $b(G) = 3$ such that $\mathrm{Z}(G) \le \gamma_2(G)$ and $\gamma_2(G)$ elementary abelian of order 2^4. Then $\mathrm{K}(G) = \gamma_2(G)$.*

We again use GAP to establish the following two lemmas, whose theoretical proofs can be written on the lines of corresponding results of Section 3.2 for odd primes.

Lemma 2.2.3 *Let G be a finite p-group of order 2^8 having the nilpotency class 2 such that $\gamma_2(G)$ is elementary abelian of order 2^4. If G is not of conjugate type $\{1, 2^3\}$ or $\{1, 2^2, 2^3\}$, then $\mathrm{K}(G) \neq \gamma_2(G)$. Moreover, the commutator length of G is 2.*

Lemma 2.2.4 *Let G be a group of order 2^8, nilpotency class 2 and conjugate type $\{1, 2^3\}$ such that $\gamma_2(G)$ is elementary abelian of order 2^4. Then $\mathrm{K}(G) =$*

$\gamma_2(G)$.

Remark 2.2.2 *In the preceding lemma we first use [34, Theorem 1.3] and then the proof goes on similar lines as proof of Lemma 3.2.3 in Chapter 3.*

Lemma 2.2.5 *Let G be a group of order 2^8, nilpotency class 2 and conjugate type $\{1, 2^2, 2^3\}$ such that $\gamma_2(G)$ is elementary abelian of order 2^4. Then $\mathrm{K}(G) = \gamma_2(G)$ if and only if G admits a generating set $\{a, b, c, d\}$ such that $[a, b] = 1 = [c, d]$. Moreover, if $\mathrm{K}(G) \neq \gamma_2(G)$, then the commutator length of G is 2.*

Proof. Let G admit a generating set $\{a, b, c, d\}$ such that $[a, b] = 1 = [c, d]$. Then $\gamma_2(G) = \langle [a, c], [b, c], [a, d], [b, d] \rangle$. Given $\varepsilon, \lambda, \mu, \eta \in \mathbb{F}_2$, a straightforward computation shows that

$$[a, c]^{\varepsilon}[b, c]^{\lambda}[a, d]^{\mu}[b, d]^{\eta} = [a^{\alpha_1}b^{\alpha_2}c, a^{\beta_1}b^{\beta_2}d] \qquad (2.2.2)$$

for $\beta_1 = -\varepsilon$, $\beta_2 = -\lambda$, $\alpha_1 = \mu$, $\alpha_2 = \eta$. Thus $\mathrm{K}(G) = \gamma_2(G)$.

For the converse part we provide a contrapositive proof. We assume that G admits no generating set $\{x_1, x_2, x_3, x_4\}$ such that $[x_1, x_2] = 1 = [x_3, x_4]$. By the given hypothesis, we can always choose a generating set $\{a, b, c, d\}$ for G such that $[a, c] = 1$ and none of the other basic commutators of weight two in generators is trivial. So we can assume that

$$[c, d] = [a, b]^{t_1}[b, c]^{t_2}[b, d]^{t_3}[a, d]^{t_4},$$

where $t_i \in \mathbb{F}_2$ and $1 \leq i \leq 4$, and therefore $\gamma_2(G) = \langle [a, b], [b, c], [b, d], [a, d] \rangle$.

We can write the preceding equation as

$$[b, a^{-t_1}c^{t_2}d^{t_3}][d, a^{-t_4}c] = 1. \qquad (2.2.3)$$

We claim that $t_3 = 0$. If $t_3 = 1$, then replacing d by $d' := a^{-t_1}c^{t_2}d$ and a proper substitution reduces (2.2.3) to $[d', b^{-1}a^{-t_4}c] = 1$. Now replacing b by $b' := b^{-1}a^{-t_4}c$, we get a generating set $\{a, b', c, d'\}$ for G such that $\gamma_2(G) = \langle [a, b'], [b', c], [b', d'], [c, d'] \rangle$ and $[a, c] = 1 = [b', d']$, which contradicts our hypothesis. Our claim is now settled.

So now onwards we assume that $t_3 = 0$. Hence from (2.2.3) we get

$$[b, a^{-t_1}c^{t_2}][d, ca^{-t_4}] = 1.$$

Now replace c by $c' := ca^{-t_4}$ in the preceding equation and simple computation gives

$$[b, a^{-t_1}c^{t_2}] = [b, a^{-t_1}(c'a^{t_4})^{t_2}] = [b, a^{t_4t_2-t_1}c'^{t_2}].$$

Thus (2.2.3) reduces to

$$[b, a^{t_4t_2-t_1}c'^{t_2}][d, c'] = 1. \tag{2.2.4}$$

We claim that $t_4t_2 - t_1 \neq 0$. Contrarily assume that $t_4t_2 - t_1 = 0$. Then (2.2.4) takes the form $[b, c'^{t_2}][d, c'] = 1$, which gives $[b^{t_2}d, c'] = 1$. Now replacing d by $d' := b^{t_2}d$, we get a generating set $\{a, b, c', d'\}$ of G such that $[a, c'] = 1 = [d', c']$, which gives that the size of the conjugacy class of c' in G is 2, a contradiction to the given hypothesis. This settles our claim.

So we now assume $t_4t_2 - t_1 = 1$. Then replacing a by $a' := ac'^{t_2}$, we get a new generating set $\{a', b, c', d\}$ such that $\gamma_2(G) = \langle [a', b], [b, c'], [b, d], [a', d] \rangle$, $[a', c'] = 1$ and, by (2.2.4), $[a', b] = [c', d]$. Now we claim that $[a', b][b, c'][a', d] \notin \mathrm{K}(G)$. Contrarily assume that $[a', b][b, c'][a', d] \in \mathrm{K}(G)$. Thus

$$[a', b][b, c'][a', d] = [a'^{\alpha_1}b^{\alpha_2}c'^{\alpha_3}d^{\alpha_4}, a'^{\beta_1}b^{\beta_2}c'^{\beta_3}d^{\beta_4}],$$

for some $\alpha_i, \beta_j \in \mathbb{F}_2$, $1 \leq i, j \leq 4$. Expanding the right hand side and comparing powers both side, we get

$$\alpha_1\beta_4 + \alpha_4\beta_1 = 1, \tag{2.2.5}$$

$$\alpha_2\beta_4 + \alpha_4\beta_2 = 0, \tag{2.2.6}$$

$$\alpha_2\beta_3 + \alpha_3\beta_2 = 1, \tag{2.2.7}$$

$$\alpha_1\beta_2 + \alpha_2\beta_1 + \alpha_3\beta_4 + \alpha_4\beta_3 = 1. \tag{2.2.8}$$

First assume that $\alpha_2 = 0$. Then from (2.2.7) we get $\alpha_3 = \beta_2 = 1$, and hence from (2.2.6) we get $\alpha_4 = 0$, which using (2.2.5) gives $\alpha_1 = \beta_4 = 1$. But these values contradict (2.2.8). So assume that $\alpha_2 = 1$. If $\beta_2 = 0$, then (2.2.6) gives $\beta_4 = 0$ and (2.2.7) gives $\beta_3 = 1$. Substituting $\beta_4 = 0$ in (2.2.5) we get $\alpha_4 = \beta_1 = 1$, which contradict (2.2.8). Hence $\beta_2 \neq 0$.

Finally assume that $\alpha_2 = \beta_2 = 1$. Therefore above equations reduces to

$$\alpha_1\beta_4 + \alpha_4\beta_1 = 1, \tag{2.2.9}$$

$$\beta_4 + \alpha_4 = 0, \tag{2.2.10}$$

$$\beta_3 + \alpha_3 = 1, \tag{2.2.11}$$

$$\alpha_1 + \beta_1 + \alpha_3\beta_4 + \alpha_4\beta_3 = 1. \tag{2.2.12}$$

As, by (2.2.10), $\alpha_4 = \beta_4$, from (2.2.9) we get $\alpha_4 = 1 = \alpha_1 + \beta_1$. Now putting $\alpha_4 = \beta_4 = 1$ in (2.2.12) and using (2.2.11), we get $\alpha_1 + \beta_1 = 0$, which is not possible. Hence $[a', b][b, c'][a', d] \notin \mathrm{K}(G)$. The final assertion follows from Theorem 1.1.3 and Lemma 1.3.6. This completes the proof. □

Lemma 2.2.6 *Let G be a finite 2-group of nilpotency class 2 and order at least 2^9 such that $\mathrm{Z}(G) = \gamma_2(G)$, Theorem 2.1.5(iii) holds and $\gamma_2(G)$ is elementary abelian of order 2^4. Then $\mathrm{K}(G) = \gamma_2(G)$.*

Proof. If $b(G) = 4$, then we are done. So assume that $b(G) = 3$. By the given hypothesis there esixts a normal subgroup H of G of order 2 such that $|G/H : Z(G/H)| = 2^3$. Thus, using the fact that the exponent of $G/Z(G)$ is 2 (which follows from the given hypothesis), we can assume that

$$G = \langle a, b, c, x_1, \ldots, x_k\rangle,$$

where $k \geq 2$ and $[x_i, G] = H$ for $1 \leq i \leq k$. Let $S := \langle a, b, c\rangle$ be the subgroup of G generated by a, b, c. Notice that $|S| = 2^6$, therefore $K(S) = \gamma_2(S)$. If $S \leq C_G(x_i)$ for all $1 \leq i \leq k$, then, since $Z(G) = \gamma_2(G)$, G can written as a central product of S and a k-generator group isoclinic to an extraspecial p-groups generated by $\{x_1, \ldots, x_k\}$. Now using Lemma 1.3.3, we have $K(G) = \gamma_2(G)$. So assume that $[x_t, S] = H$ for some $t \in \{1, \ldots, k\}$. By reordering the set $\{x_1, \ldots, x_k\}$, if necessary, we can assume that $t = 1$. For simplicity of notation, we set $d := x_1$. Since $C_G(d)$ is a maximal subgroup of G, we can modify the generators a, b, c such that $\gamma_2(G) = \langle [a, b], [a, c], [b, c], [c, d]\rangle$, $[a, d] = [b, d] = 1$ and $H = \langle [c, d]\rangle$. We can also assume, by suitable modification of x_i, that $[c, x_i] = 1$ for all $2 \leq i \leq k$.

Let $\alpha_i \in \mathbb{F}_2$ for $1 \leq i \leq 4$. If any element of $\gamma_2(G)$ involves $[a, c]$, then the following identity holds:

$$[a, c][a, b]^{\alpha_1}[b, c]^{\alpha_2}[c, d]^{\alpha_3} = [cb^{\alpha_1}, ab^{-\alpha_2}d^{\alpha_3}],$$

and hence that element is a commutator. Now, if $[b, c]$ is involved in any element of $\gamma_2(G)$, then for any $\alpha_1, \alpha_3 \in \mathbb{F}_2$ we have

$$[b, c][a, b]^{\alpha_1}[c, d]^{\alpha_3} = [bd^{-\alpha_3}, a^{-\alpha_1}c].$$

So, it only remains to show that $[a, b][c, d]$ is a commutator. If $[a, x_i] = [c, d]$ for some $2 \leq i \leq k$, then

$$[a, b][c, d] = [a, bx_i].$$

Set $A := \langle x_2, \ldots, x_k \rangle$. Now suppose that $a \in C_G(A)$, but $b \notin C_G(A)$. So there must exist an x_i, $2 \leq i \leq k$, such that $[b, x_i] = [c, d]$. Then

$$[a, b][c, d] = [b, ax_i].$$

Let $a, b \in C_G(A)$. If $[d, x_i] = [c, d]$ for some $2 \leq i \leq k$, then

$$[a, b][c, d] = [ad, bx_i].$$

So finally assume that $a, b, c, d \in C_G(A)$. Notice that, in this case, $k \geq 3$ and $\gamma_2(A) = H$, since $[A, G] = H$. Hence $[x_i, x_j] = [c, d]^\beta$ for some $2 \leq i, j \leq k$, and therefore we have

$$[a, b][c, d] = [bx_i, ax_j].$$

This shows that each element of $\gamma_2(G)$ is a commutator, and the proof is complete. □

Let L be a 2-group of breadth 3 which satisfies Theorem 2.1.5(iv) and $\gamma_2(L)$ be elementary abelian of order 16. Then, by a careful inspection, it follows from Theorem 2.1.5 that L is isoclinic to the group T presented as

$$\begin{aligned} T \;=\; & \langle v_1, v_2, v_3, v_4, v_5 \mid [v_4, v_2] = [v_5, v_1] = 1, [v_1, v_2] = [v_3, v_4]^r, \\ & [v_2, v_3] = [v_3, v_4]^s, [v_3, v_1] = [v_3, v_4]^t, [v_3, v_4] = [v_3, v_5], v_i^{2k_i} = 1, \\ & [v_i^2, v_j] = 1 \; (1 \leq i, j \leq 5), [x, y, z] = 1 \text{ for all } x, y, z \in \{v_1, \ldots, v_5\} \rangle, \end{aligned} \tag{2.2.13}$$

for some positive integers k_i's and some $r, s, t \in \mathbb{F}_2$.

Lemma 2.2.7 *Let G be a finite 2-group of breadth 3 such that Theorem 2.1.5(iv) holds, $\mathrm{Z}(G) \leq \gamma_2(G)$ and $\gamma_2(G)$ is elementary abelian of order 2^4. Then G is isoclinic to the group T given by (2.2.13) for some $r, s, t \in \mathbb{F}_2$ and $k_i = 1$, $1 \leq i \leq 5$, and $\mathrm{K}(G) \neq \gamma_2(G)$ if and only if $r = s = t = 0$. Moreover, if $\mathrm{K}(G) \neq \gamma_2(G)$, then the commutator length of G is 2.*

Proof. It is not difficult to see that G is isoclinic to the group T given by (2.2.13) for $k_i = 1$, $1 \leq i \leq 5$ and some $r, s, t \in \mathbb{F}_2$. We now prove the second assertion. First assume that $r = s = t = 0$. We claim that $[v_4, v_1][v_4, v_3][v_5, v_2] \notin \mathrm{K}(G)$. Otherwise, there exist $\alpha_i, \beta_i \in \mathbb{F}_2$ such that

$$[v_4, v_1][v_4, v_3][v_5, v_2] = [v_4^{\alpha_1} v_5^{\alpha_2} {v_1}^{\alpha_3} {v_2}^{\alpha_4} {v_3}^{\alpha_5}, v_4^{\beta_1} v_5^{\beta_2} {v_1}^{\beta_3} {v_2}^{\beta_4} {v_3}^{\beta_5}].$$

Expanding the right side and comparing the powers of commutators, we get

$$\alpha_1\beta_2 + \alpha_2\beta_1 = 0, \tag{2.2.14}$$

$$\alpha_1\beta_3 + \alpha_3\beta_1 = 1, \tag{2.2.15}$$

$$\alpha_2\beta_4 + \alpha_4\beta_2 = 1, \tag{2.2.16}$$

$$\alpha_1\beta_5 + \alpha_5\beta_1 + \alpha_2\beta_5 + \alpha_5\beta_2 = 1. \tag{2.2.17}$$

First assume that $\alpha_1 = 0$. Then (2.2.15) gives $\alpha_3 = \beta_1 = 1$, hence by (2.2.14) we get $\alpha_2 = 0$, which gives $\alpha_4 = \beta_2 = 1$. But these values contradict (2.2.17). So now assume that $\alpha_1 = 1$. If $\beta_1 = 0$, then by (2.2.14) and (2.2.15) we get $\beta_2 = 0$ and $\beta_3 = 1$, respectively. As $\beta_2 = 0$, by (2.2.16) we get $\alpha_2 = \beta_4 = 1$; but these values contradict (2.2.17). Finally assume that $\alpha_1 = \beta_1 = 1$. Then by (2.2.14) and (2.2.16) we get $\alpha_2 = \beta_2 = 1$, which again contradict (2.2.17). Hence $[v_4, v_1][v_4, v_3][v_5, v_2] \notin \mathrm{K}(G)$.

Conversely, assume that at least one of r, s, t is non-zero. We'll show that

$\mathrm{K}(G) = \gamma_2(G)$. It is easy to see that except

$$[v_4, v_1][v_4, v_3][v_5, v_2], [v_4, v][v_4, v_1][v_4, v_3][v_5, v_2],$$

all elements of $\gamma_2(G)$ lie in $\mathrm{K}(G)$. We'll first show that $[v_4, v_1][v_4, v_3][v_5, v_2] \in \mathrm{K}(G)$. If $r = 1$, then $[v_1, v_2] = [v_3, v_4] = [v_4, v_3]$, and therefore

$$[v_4, v_1][v_5, v_2][v_4, v_3] = [v_4, v_1][v_5, v_2][v_1, v_2] = [v_4 v_5 v_1, v_1 v_2].$$

So let $r = 0$. If $t = 1$, then for any value of s we have

$$[v_4 v_5 v_1, v_1 v_2 v_3] = [v_4, v_1][v_1, v_3][v_5, v_2][v_5, v_3][v_1, v_3] = [v_4, v_1][v_4, v_3][v_5, v_2].$$

If $t = 0$ and $s = 1$, then

$$[v_4 v_5 v_2, v_1 v_2 v_3] = [v_4, v_1][v_4, v_3][v_5, v_2][v_5, v_3][v_2, v_3] = [v_4, v_1][v_4, v_3][v_5, v_2].$$

Now we take $[v_4, v_5][v_4, v_1][v_4, v_3][v_5, v_2]$. First let $r = 1$. Then

$$[v_4 v_5 v_1, v_5 v_1 v_2] = [v_4, v_5][v_4, v_1][v_5, v_2][v_1, v_2].$$

Next let $r = 0$. If $t = 1$, then

$$\begin{aligned}[v_4 v_5 v_1, v_5 v_1 v_2 v_3] &= [v_4, v_5][v_4, v_1][v_4, v_3][v_5, v_2][v_5, v_3][v_1, v_3] \\ &= [v_4, v_5][v_4, v_1][v_4, v_3][v_5, v_2].\end{aligned}$$

If $t = 0$ and $s = 1$, then we finally get

$$[v_4 v_1 v_2, v_5 v_1 v_3] = [v_4, v_5][v_4, v_1][v_4, v_3][v_1, v_3][v_2, v_5] = [v_4, v_5][v_4, v_1][v_4, v_3][v_5, v_2].$$

Hence $[v_4, v_5][v_4, v_1][v_4, v_3][v_5, v_2] \in \mathrm{K}(G)$.

Notice that $\gamma_2(G) = \langle [v_1, v_4], [v_2, v_5], [v_3, v_4], [v_4, v_5] \rangle$. For any $\alpha_i \in \{0, 1\}$, $1 \leq i \leq 4$, it is easy to see that

$$[v_1, v_4]^{\alpha_1}[v_2, v_5]^{\alpha_2}[v_3, v_4]^{\alpha_3}[v_4, v_5]^{\alpha_4} = [v_1^{\alpha_1}v_3^{\alpha_3}v_5^{-\alpha_4}, v_4][v_2^{\alpha_2}, v_5].$$

This proves that every element of $\gamma_2(G)$ can be written as a product of at most two elements from $\mathrm{K}(G)$, completing the proof. □

We can now write a proof of Theorem B.

Proof of Theorem B. Let G be a finite 2-groups such that $\gamma_2(G)$ is elementary abelian of order 16. Also let $\mathrm{Z}(G) \leq \gamma_2(G)$. As in the case of odd primes, we have $b(G) \geq 3$ in this case too. If $b(G) = 4$, then $\mathrm{K}(G) = \gamma_2(G)$. So we assume that $b(G) = 3$. Then it follows from Theorem 2.1.6 that the nilpotency class of G is either 2 or 3, and $|G| \geq 2^7$. If the nilpotency class of G is 2, then the assertion follows from Lemmas 2.2.3 - 2.2.7. If the nilpotency class of G is 3, then the assertion holds from Lemma 2.2.2. If $\mathrm{K}(G) \neq \gamma_2(G)$, then, that the commutator length is 2, follows from Lemma 2.2.3, Lemma 2.2.5 and Lemma 2.2.7, which completes the proof. □

CHAPTER 3

p-Groups with $|\gamma_2(G)| = p^4$ and $\exp(\gamma_2(G)) = p$, $p \geq 3$

In this chapter we classify finite p-groups G (up to isoclinism) with the commutator subgroup $\gamma_2(G)$ of order p^4 and exponent p such that $\mathrm{K}(G) \neq \gamma_2(G)$.

3.1 Introduction

Recall that in Theorem 1.1.5, I. De las Heras, proved that if G is a finite p-group and $\gamma_2(G)$ can be generated by 3 elements, then $\mathrm{K}(G) = \gamma_2(G)$. However $\mathrm{K}(G) \neq \gamma_2(G)$ when $\gamma_2(G)$ is minimally generated by 4 elements. In the following theorem we provide a classification of finite p-groups G (up to isoclinism) having $\gamma_2(G)$ of order p^4 and exponent p such that $\mathrm{K}(G) \neq \gamma_2(G)$.

Theorem 3.1.1 *Let G be a finite p-group with $\mathrm{Z}(G) \leq \gamma_2(G)$ and $\gamma_2(G)$ of order p^4 and exponent $p \geq 3$. Then $\mathrm{K}(G) \neq \gamma_2(G)$ if and only if one of the following holds:*

(1) *G is of order p^6 and nilpotency class 4 with $|\mathrm{Z}(G)| = p^2$.*

(2) *G is of order p^7 and nilpotency class 3 with $|\mathrm{Z}(G)| = p^3$.*

(3) *G is of order p^8 and nilpotency class 2 along with one of the following:*

(3a) *G admits a non-central element whose centralizer in G is a maximal subgroup.*

(3b) *G is of conjugate type $\{1, p^2, p^3\}$ and admits no generating set $\{x_1, x_2, x_3, x_4\}$ such that $[x_1, x_2] = 1 = [x_3, x_4]$.*

Moreover, if $\mathrm{K}(G) \neq \gamma_2(G)$, then the commutator length of G is 2.

3.2 Groups of nilpotency class 2

This section is devoted to the investigation of the question under consideration for the groups of nilpotency class 2.

Lemma 3.2.1 *Let G be a finite p-group of order p^8 having the nilpotency class 2 such that $\gamma_2(G)$ is elementary abelian of order p^4. If G is not of conjugate type $\{1, p^3\}$ or $\{1, p^2, p^3\}$, then $\mathrm{K}(G) \neq \gamma_2(G)$. Moreover, the commutator length of G is 2.*

Proof. By the given hypothesis it follows that $\mathrm{Z}(G) = \gamma_2(G)$ and G is minimally generated by 4 elements. Since G is minimally generated by 4 elements, by Remark 2.1.3 we have $b(G) = 3$. Again by the given hypothesis there exists an element $d \in G - \gamma_2(G)$ such that $\mathrm{C}_G(d)$ is maximal in G. We can always extend $\{d\}$ to a generating set $\{a, b, c, d\}$ for G such that $\gamma_2(G) = \langle [a, b], [a, c], [b, c], [c, d] \rangle$. We claim that $[a, b][c, d]$ is not in $\mathrm{K}(G)$. Contrarily assume that $[a, b][c, d] \in \mathrm{K}(G)$. Thus

$$[a, b][c, d] = [a^{\alpha_1} b^{\alpha_2} c^{\alpha_3} d^{\alpha_4}, a^{\beta_1} b^{\beta_2} c^{\beta_3} d^{\beta_4}],$$

for some $\alpha_i, \beta_j \in \mathbb{F}_p$, where $1 \leq i, j \leq 4$. Expanding the right hand side and comparing the powers of the generators of $\gamma_2(G)$, we get the following set of equations:

$$\beta_2\alpha_1 - \alpha_2\beta_1 = 1, \tag{3.2.1}$$

$$\beta_3\alpha_2 - \alpha_3\beta_2 = 0, \tag{3.2.2}$$

$$\beta_3\alpha_1 - \alpha_3\beta_1 = 0, \tag{3.2.3}$$

$$\beta_4\alpha_3 - \alpha_4\beta_3 = 1. \tag{3.2.4}$$

First assume that $\beta_3 \neq 0$. Then from (3.2.2) and (3.2.3), we get $\alpha_2 = \alpha_3\beta_2\beta_3^{-1}$ and $\alpha_1 = \alpha_3\beta_1\beta_3^{-1}$. Notice that these values of α_1 and α_2 contradict (3.2.1). Thus $\beta_3 = 0$. That $\alpha_3 \neq 0$ follows from (3.2.4) after inserting $\beta_3 = 0$. This then implies, along with (3.2.2) and (3.2.3), that $\beta_1 = \beta_2 = 0$, which contradicts (3.2.1). Hence the above system of equations has no solution, which settles our claim.

Let H be any subgroup of $\gamma_2(G)$ of order p. Then it follows from Theorem 1.1.3 that $\gamma_2(G/H) = \mathrm{K}(G/H)$. Hence by Lemma 1.3.6, the commutator length of G is 2, which completes the proof. □

The proof of the following lemma goes on the lines of the proof of Lemma 2.2.5.

Lemma 3.2.2 *Let G be a finite p-group of order p^8, nilpotency class 2 and conjugate type $\{1, p^2, p^3\}$ such that $\gamma_2(G)$ is elementary abelian of order p^4. Then $\mathrm{K}(G) = \gamma_2(G)$ if and only if G admit a generating set $\{a, b, c, d\}$ such that $[a, b] = 1 = [c, d]$. Moreover, if $\mathrm{K}(G) \neq \gamma_2(G)$, then the commutator length of G is 2.*

Proof. Let G admit a generating set $\{a, b, c, d\}$ such that $[a, b] = 1 = [c, d]$. Then $\gamma_2(G) = \langle [a, c], [b, c], [a, d], [b, d] \rangle$. For any given $\varepsilon, \lambda, \mu, \eta \in \mathbb{F}_p$, a straightforward computation shows that

$$[a,c]^{\varepsilon}[b,c]^{\lambda}[a,d]^{\mu}[b,d]^{\eta} = [a^{\alpha_1}b^{\alpha_2}c, a^{\beta_1}b^{\beta_2}d] \tag{3.2.5}$$

for $\beta_1 = -\varepsilon,\ \beta_2 = -\lambda,\ \alpha_1 = \mu,\ \alpha_2 = \eta$. Hence $\mathrm{K}(G) = \gamma_2(G)$.

For the converse part we provide a contrapositive proof. Let us assume that G admits no generating set $\{x_1, x_2, x_3, x_4\}$ such that $[x_1, x_2] = 1 = [x_3, x_4]$. By the given hypothesis, we can always choose a generating set $\{a, b, c, d\}$ for G such that $[a, c] = 1$ and none of the other basic commutators of weight two in generators is trivial. If $[c, d]$ cannot be written as a product of powers of the remaining basic commutators, then $[a, b][c, d]$ cannot lie in $\mathrm{K}(G)$. So we can assume that

$$[c,d] = [a,b]^{t_1}[b,c]^{t_2}[b,d]^{t_3}[a,d]^{t_4},$$

for some $t_i \in \mathbb{F}_p$, where $1 \leq i \leq 4$, and therefore $\gamma_2(G) = \langle [a,b], [b,c], [b,d], [a,d] \rangle$.

We can write the preceding equation as

$$[b, a^{-t_1}c^{t_2}d^{t_3}][d, a^{-t_4}c] = 1. \tag{3.2.6}$$

We claim that $t_3 = 0$. If $t_3 \neq 0$, then replacing d by $d' := a^{-t_1}c^{t_2}d^{t_3}$ and a proper substitution reduces (3.2.6) to $[d', b^{-1}a^{-t_4t_3^{-1}}c^{t_3^{-1}}] = 1$. Now replacing b by $b' := b^{-1}a^{-t_4t_3^{-1}}c^{t_3^{-1}}$, we get a generating set $\{a, b', c, d'\}$ for G such that $\gamma_2(G) = \langle [a,b'], [b',c], [b',d'], [c,d'] \rangle$ and $[a,c] = 1 = [b',d']$, which contradicts our hypothesis. Our claim is now settled.

Hence $t_3 = 0$, which reduces (3.2.6) to $[b, a^{-t_1}c^{t_2}][d, ca^{-t_4}] = 1$. Now replace c by $c' := ca^{-t_4}$. A simple computation gives

$$[b, a^{-t_1}c^{t_2}] = [b, a^{-t_1}(c'a^{t_4})^{t_2}] = [b, a^{t_4t_2-t_1}c'^{t_2}].$$

Thus (3.2.6) reduces to

$$[b, a^{t_4t_2-t_1}c'^{t_2}][d, c'] = 1. \tag{3.2.7}$$

We claim that $t_4t_2 - t_1 \neq 0$. If $t_4t_2 - t_1 = 0$, then (3.2.7) takes the form $[b, c'^{t_2}][d, c'] = 1$, which gives $[b^{t_2}d, c'] = 1$. Now replacing d by $d' := b^{t_2}d$, we get a generating set $\{a, b, c', d'\}$ of G such that $[a, c'] = 1 = [d', c']$, which gives that the size of the conjugacy class of c' in G is p, a contradiction to the given hypothesis. This settles our claim.

Thus $t_4t_2 - t_1 \neq 0$. Now replacing a by $a' := a^{t_4t_2-t_1}c'^{t_2}$, we get a new generating set $\{a', b, c', d\}$ such that $\gamma_2(G) = \langle [a', b], [b, c'], [b, d], [a', d] \rangle$, $[a', c'] = 1$ and, by (3.2.7), $[a', b]^{-1} = [c', d]$. We claim that $[b, c']^{\lambda}[a', d]^{\mu} \notin \mathrm{K}(G)$ for some $\lambda, \mu \in \mathbb{F}_p^*$. Contrarily assume that $[b, c']^{\lambda}[a', d]^{\mu} \in \mathrm{K}(G)$ for all $\lambda, \mu \in \mathbb{F}_p^*$. Thus

$$[b, c']^{\lambda}[a', d]^{\mu} = [a'^{\alpha_1}b^{\alpha_2}c'^{\alpha_3}d^{\alpha_4}, a'^{\beta_1}b^{\beta_2}c'^{\beta_3}d^{\beta_4}],$$

where $\alpha_i, \beta_j \in \mathbb{F}_p$ for $1 \leq i, j \leq 4$. Expanding the right hand side and comparing powers both side, we get following set of equations:

$$\alpha_1\beta_4 - \alpha_4\beta_1 = \mu, \tag{3.2.8}$$

$$\alpha_2\beta_4 - \alpha_4\beta_2 = 0, \tag{3.2.9}$$

$$\alpha_2\beta_3 - \alpha_3\beta_2 = \lambda, \tag{3.2.10}$$

$$\alpha_1\beta_2 - \alpha_2\beta_1 - \alpha_3\beta_4 + \alpha_4\beta_3 = 0. \tag{3.2.11}$$

First assume that $\alpha_2 = 0$. Then from (3.2.10) $\alpha_3\beta_2 = -\lambda$, therefore by (3.2.9) $\alpha_4 = 0$. Now by (3.2.8) $\alpha_1\beta_4 = \mu$. Since α_1 and α_3 are non-zero, by substituting the value of $\beta_2 = -\lambda\alpha_3^{-1}$ and $\beta_4 = \mu\alpha_1^{-1}$ in (3.2.11), we get $\lambda\alpha_1\alpha_3^{-1}+\mu\alpha_3\alpha_1^{-1} = 0$. Thus $(\alpha_1\alpha_3^{-1})^2 = -\lambda^{-1}\mu$, which is a contradiction because we can choose $\lambda, \mu \in \mathbb{F}_p^*$ such that $-\lambda^{-1}\mu$ is non square. Now we assume that $\alpha_2 \neq 0$. If $\alpha_4 = 0$, then (3.2.9) implies that $\beta_4 = 0$, which contradicts (3.2.8). So finally assume that both α_2 and α_4 are non zero. The augmented matrix of above system of equations, with β_i's as variables, is given by

$$M = \begin{bmatrix} -\alpha_4 & 0 & 0 & \alpha_1 & \mu \\ 0 & -\alpha_4 & 0 & \alpha_2 & 0 \\ 0 & -\alpha_3 & \alpha_2 & 0 & \lambda \\ -\alpha_2 & \alpha_1 & \alpha_4 & -\alpha_3 & 0 \end{bmatrix}.$$

Performing row operations

(i) $R_1 \to -\alpha_4^{-1}R_1,\ R_2 \to -\alpha_4^{-1}R_2$,

(ii) $R_4 \to R_4 + \alpha_2 R_1,\ R_3 \to R_3 + \alpha_3 R_2$,

(iii) $R_3 \to \alpha_2^{-1}R_3,\ R_4 \to R_4 - \alpha_1 R_2$,

(iv) $R_4 \to R_4 - \alpha_4 R_3$,

we get

$$M_1 = \begin{bmatrix} 1 & 0 & 0 & -\alpha_1\alpha_4^{-1} & -\mu\alpha_4^{-1} \\ 0 & 1 & 0 & -\alpha_2\alpha_4^{-1} & 0 \\ 0 & 0 & 1 & -\alpha_3\alpha_4^{-1} & \lambda\alpha_2^{-1} \\ 0 & 0 & 0 & 0 & -\mu\alpha_2\alpha_4^{-1} - \lambda\alpha_2^{-1}\alpha_4 \end{bmatrix}.$$

If the above system of equations admits a solution, then $\mu\alpha_2\alpha_4^{-1} + \lambda\alpha_2^{-1}\alpha_4 = 0$. This gives $(\alpha_2\alpha_4^{-1})^2 = -\lambda\mu^{-1}$, which is a contradiction again, because we can choose $\lambda, \mu \in \mathbb{F}_p^*$ such that $-\lambda\mu^{-1}$ is non square. Thus $\mathrm{K}(G) \neq \gamma_2(G)$. The final assertion holds by taking G/H, where H is any subgroup of $\gamma_2(G)$ of order p generated by a commutator, and then using Theorem 1.1.3 and Lemma 1.3.6. The proof of the lemma is now complete. □

Lemma 3.2.3 *Let G be a finite p-group of order p^8, nilpotency class 2 and conjugate type $\{1, p^3\}$ such that $\gamma_2(G)$ is elementary abelian of order p^4. Then*

$K(G) = \gamma_2(G)$.

Proof. Using [34, Lemma 3.14], we can assume that the exponent of G is p. Now, it follows from [34, Theorem 1.2] that G has the following presentation:

$$G = \langle a, b, c, d \mid a^p = b^p = c^p = d^p = 1, [c, d] = [a, b]^{-1}, [a, c] = [b, d]^{-r}, [[x, y], z] = 1\rangle$$

where $x, y, z \in \{a, b, c, d\}$ and r is any non-quadratic residue mod p. We'll show that for given $\lambda, \mu, \nu, \xi \in \mathbb{F}_p$, there exist $\alpha_i,\ \beta_i \in \mathbb{F}_p$ such that

$$[a, b]^{\lambda}[b, c]^{\mu}[b, d]^{\nu}[a, d]^{\xi} = [a^{\alpha_1}b^{\alpha_2}c^{\alpha_3},\ a^{\beta_1}b^{\beta_2}c^{\beta_3}d^{\beta_4}].$$

Solving both sides of the preceding equation and comparing the powers, we get

$$\alpha_1\beta_2 - \alpha_2\beta_1 - \alpha_3\beta_4 = \lambda, \quad (3.2.12)$$

$$\alpha_2\beta_3 - \alpha_3\beta_2 = \mu, \quad (3.2.13)$$

$$\alpha_2\beta_4 - r(\alpha_1\beta_3 - \alpha_3\beta_1) = \nu. \quad (3.2.14)$$

$$\alpha_1\beta_4 = \xi. \quad (3.2.15)$$

It is sufficient to show that this system of equations, β_i's as variables, admits a solution. The augmented matrix for this system of equations is as follows:

$$M = \begin{bmatrix} -\alpha_2 & \alpha_1 & 0 & -\alpha_3 & \lambda \\ 0 & -\alpha_3 & \alpha_2 & 0 & \mu \\ r\alpha_3 & 0 & -r\alpha_1 & \alpha_2 & \nu \\ 0 & 0 & 0 & \alpha_1 & \xi \end{bmatrix}.$$

Performing row operations

(i) $R_3 \to \alpha_2 R_3$,

(ii) $R_3 \to R_3 + r\alpha_3 R_1$,

(iii) $R_3 \to R_3 + r\alpha_1 R_2$,

the above matrix transforms to

$$M_1 = \begin{bmatrix} -\alpha_2 & \alpha_1 & 0 & -\alpha_3 & \lambda \\ 0 & -\alpha_3 & \alpha_2 & 0 & \mu \\ 0 & 0 & 0 & \alpha_2^2 - r\alpha_3^2 & \nu\alpha_2 + r\lambda\alpha_3 + r\mu\alpha_1 \\ 0 & 0 & 0 & \alpha_1 & \xi \end{bmatrix}.$$

It is easy to see that the above system of equations admits a solution only if

$$\xi(\alpha_2^2 - r\alpha_3^2) - \alpha_1(\nu\alpha_2 + r\lambda\alpha_3 + r\mu\alpha_1) = 0,$$

or equivalenty

$$r\mu\alpha_1^2 + (\nu\alpha_2 + r\lambda\alpha_3)\alpha_1 - \xi(\alpha_2^2 - r\alpha_3^2) = 0.$$

Viewing the preceding equation as a quadratic equation in α_1, notice that it has a solution in $\mathbb{F}_p$ if its discriminant is zero or a quadratic residue mod p. The discriminant, after an easy computation, takes the form

$$(\nu^2 + 4r\mu\xi)\alpha_2^2 + 2r\lambda\nu\alpha_2\alpha_3 + r^2(\lambda^2 - 4\mu\xi)\alpha_3^2. \tag{3.2.16}$$

Notice that (3.2.16) is of the form $f\alpha_2^2 + g\alpha_2\alpha_3 + h\alpha_3^2$, where $f, g, h \in \mathbb{F}_p$. For any fixed $\alpha_3 \in \mathbb{F}_p^*$, $F(x) := fx^2 + g\alpha_3 x + h\alpha_3^2$ is a quadratic polynomial with coefficients in $\mathbb{F}_p$. It is well known that there exist $\alpha_2 \in \mathbb{F}_p$ such that $F(\alpha_2)$ is either zero or a quadratic residue mod p. We can now easily compute α_1 such that the system of equations (3.2.12) - (3.2.15) admits a solution. This completes the proof. □

The proof of the following lemma goes on the lines of the proof of Lemma 2.2.6.

Lemma 3.2.4 *Let G be a finite p-group of order at least p^9, $p \geq 3$ with nilpotency class 2 such that $\gamma_2(G)$ is elementary abelian of order p^4 and $\mathrm{Z}(G) = \gamma_2(G)$. Then $\mathrm{K}(G) = \gamma_2(G)$.*

Proof. If $b(G) = 4$, then we are done. So assume that $b(G) = 3$. Theorem 2.1.2 now guarantees the existence of a normal subgroup H of G of order p such that $|G/H : \mathrm{Z}(G/H)| = p^3$. By the given hypothesis it follows that the exponent of $G/\mathrm{Z}(G)$ is p, thus we can assume that

$$G = \langle a, b, c, x_1, \ldots, x_k \rangle,$$

where $k \geq 2$ and $[x_i, G] = H$ for $1 \leq i \leq k$. Let $S := \langle a, b, c \rangle$ be the subgroup of G generated by a, b, c. Notice that $|S| = p^6$ and $|\gamma_2(S)| = p^3$, and therefore by Lemma 1.1.3 it follows that $\mathrm{K}(S) = \gamma_2(S)$. If $S \leq \mathrm{C}_G(x_i)$ for all $1 \leq i \leq k$, then, since $\mathrm{Z}(G) = \gamma_2(G)$, G can written as a central product of S and a k-generator group isoclinic to an extraspecial p-groups generated by $\{x_1, \ldots, x_k\}$. Now using Lemma 1.3.3, we have $\mathrm{K}(G) = \gamma_2(G)$. So assume that $S \not\leq \mathrm{C}_G(x_i)$ for some $t \in \{1, \ldots, k\}$, which implies $[x_t, S] = H$. By reordering the set $\{x_1, \ldots, x_k\}$, if necessary, we can assume that $t = 1$. For simplicity of notation, we set $d := x_1$. Since $\mathrm{C}_G(d)$ is a maximal subgroup of G, we can modify the generators a, b, c such that $\gamma_2(G) = \langle [a, b], [a, c], [b, c], [c, d] \rangle$, $[a, d] = [b, d] = 1$ and $H = \langle [c, d] \rangle$. By suitable modification of x_i we can also assume that $[c, x_i] = 1$ for all $2 \leq i \leq k$.

Let $\alpha_i \in \mathbb{F}_p$ for $1 \leq i \leq 4$. If $\alpha_3 \neq 0$, then the following identity holds:

$$[a, b]^{\alpha_1}[b, c]^{\alpha_2}[a, c]^{\alpha_3}[c, d]^{\alpha_4} = [cb^{\alpha_1\alpha_3^{-1}}, a^{-\alpha_3}b^{-\alpha_2}d^{\alpha_4}].$$

Thus any element of $\gamma_2(G)$ involving $[a, c]$ is a commutator. If $\alpha_3 = 0$ and $\alpha_2 \neq 0$, then for any $\alpha_1, \alpha_4 \in \mathbb{F}_p$ we have

$$[a, b]^{\alpha_1}[b, c]^{\alpha_2}[c, d]^{\alpha_4} = [bd^{-\alpha_4\alpha_2^{-1}}, a^{-\alpha_1}c^{\alpha_2}].$$

So, it only remains to show that elements of the form $[a, b]^{\alpha_1}[c, d]^{\alpha_4}$ are commutators, where both α_1 and α_4 are non-zero in $\mathbb{F}_p$. If $[a, x_i] = [c, d]^{\beta}$ for some $2 \leq i \leq k$ and $\beta \in \mathbb{F}_p^*$, then

$$[a, b]^{\alpha_1}[c, d]^{\alpha_4} = [a, b^{\alpha_1}x_i^{\beta^{-1}\alpha_4}].$$

Set $A := \langle x_2, \ldots, x_k\rangle$. Now suppose that $a \in \mathrm{C}_G(A)$, but $b \notin \mathrm{C}_G(A)$. So there must exist an x_i, $2 \leq i \leq k$, such that $[b, x_i] = [c, d]^{\beta}$, for some $\beta \in \mathbb{F}_p^*$. Then

$$[a, b]^{\alpha_1}[c, d]^{\alpha_4} = [b, a^{-\alpha_1}x_i^{\beta^{-1}\alpha_4}].$$

Next assume that $a, b \in \mathrm{C}_G(A)$. If $[d, x_i] = [c, d]^{\beta}$ for some $2 \leq i \leq k$ and $\beta \in \mathbb{F}_p^*$, then

$$[a, b]^{\alpha_1}[c, d]^{\alpha_4} = [ad, b^{\alpha_1}x_i^{\beta^{-1}\alpha_4}].$$

So finally assume that $a, b, c, d \in \mathrm{C}_G(A)$. Notice that, in this case, $k \geq 3$ and $\gamma_2(A) = H$, since $[A, G] = H$. Hence $[x_i, x_j] = [c, d]^{\beta}$ for some $2 \leq i, j \leq k$ and $\beta \in \mathbb{F}_p^*$, and therefore we have

$$[a, b]^{\alpha_1}[c, d]^{\alpha_4} = [bx_i, a^{-\alpha_1}x_j^{\alpha_4\beta^{-1}}].$$

This shows that $\mathrm{K}(G) = \gamma_2(G)$, and the proof is complete. □

3.3 Groups of nilpotency class 4

We start with the groups of order p^6. Up to isoclinism, there are only 3 groups of order p^6 whose commutator subgroup is elementary abelian of order p^4, $p \geq 3$ (see [22]).

Lemma 3.3.1 *Let G be a group of order p^6, $p \geq 3$ with $\gamma_2(G)$ elementary abelian of order p^4. Then $\mathrm{K}(G) = \gamma_2(G)$ if and only if $|\mathrm{Z}(G)| = p$. Moreover, if $\mathrm{K}(G) \neq \gamma_2(G)$, then the commutator length of G is 2.*

Proof. It follows from [22] that up to isoclinism there are only three groups G of order p^6, $p \geq 3$, such that $\gamma_2(G)$ is elementary abelian of order p^4. These fall under isoclinism families ϕ_{23}, ϕ_{40} and φ_{41}. All these groups are of nilpotency class 4. For any group G belonging to ϕ_{23}, we have $|\mathrm{Z}(G)| = p^2$ and it can be easily checked using GAP [4] or Magma [1] that $p \geq 5$. Let G be a representative from ϕ_{23}, which is presented as

$$\begin{aligned} G \;=\; & \langle \alpha, \alpha_1, \alpha_2, \alpha_3, \alpha_4, \gamma \mid [\alpha_i, \alpha] = \alpha_{i+1}, [\alpha_1, \alpha_2] = \gamma, \\ & \alpha^p = \gamma, {\alpha_1}^p = \alpha_{i+1}^p = \gamma^p = 1 \ (i = 1, 2, 3)\rangle. \end{aligned}$$

Notice that G is minimally generated by α and α_1, the exponent of $\gamma_2(G)$ is p and $[\alpha_1, [\alpha, \alpha_1]] = \gamma \in Z(G)$. Hence it follows from [23, Proposition 5.3] that $\mathrm{K}(G) \neq \gamma_2(G)$. More precisely, $\alpha_4\gamma \notin \mathrm{K}(G)$. However, considering G/H, where $H = \langle \gamma \rangle$, and using Theorem 1.1.5 and Lemma 1.3.6, it follows that the commutator length of G is 2.

For all groups G from the isoclinism families ϕ_{40} and φ_{41}, $|\mathrm{Z}(G)| = p$. If $p = 3$, then an easy GAP [4] computation shows that $\mathrm{K}(G) = \gamma_2(G)$ for such groups G. So we can assume that $p \geq 5$. Let G be a representative from ϕ_{40}, which is presented as

$$\begin{aligned} G &= \langle \alpha_1, \alpha_2, \beta, \beta_1, \beta_2, \gamma \mid [\alpha_1, \alpha_2] = \beta, [\beta, \alpha_i] = \beta_i, [\beta_1, \alpha_2] = [\beta_2, \alpha_1] = \gamma, \\ &\qquad \alpha^p = {\alpha_i}^p = \beta^p = {\beta_i}^p = \gamma^p = 1 \ (i = 1, 2)\rangle. \end{aligned}$$

Notice that $\gamma_2(G) = \langle \beta, \beta_1, \beta_2, \gamma\rangle$ and $\gamma_4(G) = \langle \gamma\rangle$. Let $i, j, k \in \mathbb{F}_p$. If $j \neq 0$, then

$$\gamma^l = [{\alpha_2}^{kj^{-1}} \alpha_1 \beta^{\frac{1-i}{2}}, \beta_2^{-l}]$$

and modulo $\gamma_4(G)$ we have

$$\beta^i \beta_1^j \beta_2^k = [{\alpha_2}^{kj^{-1}} \alpha_1 \beta^{\frac{1-i}{2}}, {\alpha_2}^i \beta^{-j}].$$

If $j = 0$, then

$$\gamma^l = [\alpha_2 \beta^{-\frac{1+i}{2}}, \beta_1^{-l}]$$

and modulo $\gamma_4(G)$ we have

$$\beta^i \beta_2^k = [\alpha_2 \beta^{-\frac{1-i}{2}}, {\alpha_1}^{-i} \beta^{-k}].$$

Thus, for $i, j, k \in \mathbb{F}_p$, it follows that

$$\gamma_2(G)/\gamma_4(G) = \Big(\bigcup_{\substack{i,k \\ j\neq 0}} [\bar{\alpha}_2^{kj^{-1}} \bar{\alpha}_1 \bar{\beta}^{\frac{1-i}{2}}, \bar{G}]\Big) \bigcup \Big(\bigcup_i [\bar{\alpha}_2 \bar{\beta}^{-\frac{1+i}{2}}, \bar{G}]\Big),$$

where $\bar{\alpha}_1 = \alpha_1\gamma_4(G)$, $\bar{\alpha}_2 = \alpha_2\gamma_4(G)$ and $\bar{\beta} = \beta\gamma_4(G)$. Also

$$\gamma_4(G) \subseteq \Big(\bigcap_{\substack{i,k \\ j\neq 0}} [{\alpha_2}^{kj^{-1}} \alpha_1 \beta^{\frac{1-i}{2}}, G]\Big) \bigcap \Big(\bigcap_i [\alpha_2 \beta^{-\frac{1+i}{2}}, G]\Big).$$

Hence $\mathrm{K}(G) = \gamma_2(G)$ by Lemma 1.3.7.

The group G, as presented below, is a representative from the isoclinism family ϕ_{41} for $p \geq 5$.

$$\begin{aligned} G &= \langle \alpha_1, \alpha_2, \beta, \beta_1, \beta_2, \gamma \mid [\alpha_1, \alpha_2] = \beta, [\beta, \alpha_i] = \beta_i, [\alpha_1, \beta_1] = \gamma, \\ &\qquad [\alpha_2, \beta_2] = \gamma^{-\nu}, \alpha^p = \alpha_i{}^p = \beta^p = \beta_i{}^p = \gamma^p = 1 \ (i = 1, 2)\rangle, \end{aligned}$$

where ν denotes the smallest positive integer which is a non-quadratic residue (mod p). As in the preceding case, it is easy to check that $\gamma_2(G)/\gamma_4(G)$ can be written as the union of the sets $[\bar{x}, G/\gamma_4(G)]$, where $\bar{x}$ runs over the elements of the set $S := \{\bar{\alpha}_2^{kj^{-1}} \bar{\alpha}_1 \bar{\beta}^{\frac{1-i}{2}}, \bar{\alpha}_2 \bar{\beta}^{-\frac{1+i}{2}} \mid i, j\ (\neq 0), k \in \mathbb{F}_p\}$ and $\gamma_4(G)$ is contained in the intersection of the sets $[x, G]$, where $\bar{x} \in S$. Hence $\mathrm{K}(G) = \gamma_2(G)$ by invoking Lemma 1.3.7 again, which completes the proof. □

Now we take up groups of order p^7.

Lemma 3.3.2 *Let L be a group of order p^7 and nilpotency class 4 with $b(L) = 3$, $\mathrm{Z}(L) \leq \gamma_2(L)$ and $\gamma_2(L)$ elementary abelian of order p^4. Then $\mathrm{K}(L) = \gamma_2(L)$.*

Proof. It follows from Lemma 1.3.2 that $\mathrm{Z}(G)$ can not be maximal in $\gamma_2(G)$, thus $|\mathrm{Z}(L)| \leq p^2$. By Theorem 2.1.4, L admits a subgroup G of order p^6 and nilpotency class 4 such that $\gamma_2(G) = \gamma_2(L)$. If $|\mathrm{Z}(G)| = p$, then by Lemma 3.3.1 we have $\mathrm{K}(G) = \gamma_2(G) = \gamma_2(L)$, and hence $\mathrm{K}(L) = \gamma_2(L)$. So assume that $|\mathrm{Z}(G)| = p^2$. By Theorem 2.1.2, there exists a normal subgroup H of L such that $|L/H : \mathrm{Z}(L/H)| = p^3$. We can take $L = \langle a, b, c\rangle$ such that $G = \langle a, b\rangle$. As observed in the proof of Theorem 2.1.4 (last paragraph), it follows that $H = \gamma_4(L)$. Thus $\bar{L} := L/H = \langle \bar{a}, \bar{b}, \bar{c}\rangle$ is of nilpotency class 3 such that $\bar{c} \in \mathrm{Z}(\bar{L})$, where $\bar{x} = xH$ for any $x \in L$. Since $c \notin \mathrm{Z}(L)$, we have $[c, L] = H$. Notice that $\gamma_2(\bar{L}) = \langle [\bar{a}, \bar{b}], [\bar{a}, [\bar{a}, \bar{b}]], [\bar{b}, [\bar{a}, \bar{b}]]\rangle$. Let $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_p$. If $\alpha_3 \neq 0$, then we can write

$$[\bar{a},\bar{b}]^{\alpha_1}[\bar{b},[\bar{a},\bar{b}]]^{\alpha_2}[\bar{a},[\bar{a},\bar{b}]]^{\alpha_3} = [\bar{a}\ \bar{b}^{\alpha_2\alpha_3^{-1}}[\bar{a},\bar{b}]^{\frac{1-\alpha_1}{2}}, \bar{b}^{\alpha_1}[\bar{a},\bar{b}]^{\alpha_3}].$$

If $\alpha_3 = 0$, then we can write

$$[\bar{a},\bar{b}]^{\alpha_1}[\bar{b},[\bar{a},\bar{b}]]^{\alpha_2} = [\bar{b}\ [\bar{a},\bar{b}]^{-\frac{1-\alpha_1}{2}}, \bar{a}^{-\alpha_1}[\bar{a},\bar{b}]^{\alpha_2}].$$

Hence, for $i,j \in \mathbb{F}_p$ and $\epsilon = 0,1$ such that i and ϵ are not simultaneously zero, we have

$$\gamma_2(\bar{L}) = \bigcup_{\epsilon,i,j} [\bar{a}^{\epsilon}\ \bar{b}^{i}[\bar{a},\bar{b}]^{j}, \bar{L}].$$

Notice that G lies in the isoclinism family ϕ_{23} of [22]. Therefore we can take $H = \langle [b,\gamma_3(G)] \rangle$. Since $\mathrm{C}_G(c)$ is maximal, by suitably modifying c, we can assume that $[b,c] = 1$ and $H = \langle [a,c] \rangle$. Then, for all $i,j \in \mathbb{F}_p$ and $\epsilon = 0,1$, it follows that $H \subseteq [a^{\epsilon}b^{i}[a,b]^{j}, L]$, where i and ϵ are not simultaneously zero. Hence $\mathrm{K}(L) = \gamma_2(L)$ by Lemma 1.3.7. □

3.4 Groups of nilpotency class 3

A group G is said to be a freest p-group of nilpotency class 2 on n generators if G is minimally generated by n elements, the nilpotency class of G is 2, $|\gamma_2(G)| = p^{n(n-1)/2}$ and $|G| = p^{n(n+1)/2}$. Throughout the remaining of this chapter $\epsilon \in \{0,1\}$.

Lemma 3.4.1 *Let G be a group of order p^7 and nilpotency class 3 with $b(G) = 3$, $|\mathrm{Z}(G)| \leq p^2$ and $\gamma_2(G)$ elementary abelian of order p^4. Then $\mathrm{K}(G) = \gamma_2(G)$.*

Proof. Notice that G is a stem group in its isoclinism family. In view of Lemma 1.3.1, it follows that G is minimally generated by 3 elements a, b, c (say). For notational convenience, set $\mathrm{C} = \mathrm{C}_G(\gamma_2(G))$. To enhance the readability of the proof, we divide it in several steps.

Step 1. *If* $|\,\mathrm{Z}(G)| = p$, *then* $\mathrm{C} = \gamma_2(G)$.

Proof. Since $|Z(G)| = p$, we have $|\gamma_3(G)| = p$, and therefore no non trivial element from the subgroup $\langle [a,b],[a,c],[b,c]\rangle$ can lie in $\gamma_3(G)$. If $|\,\mathrm{C}\,| = p^6$, then, without loss of generality, we can assume that $b, c \in \mathrm{C}$. By Hall-Witt identity we have

$$[[a,b],c][[c,a],b][[b,c],a] = 1,$$

which implies that $[b,c] \in \mathrm{Z}(G)$. As observed above, this is not possible.

If $|\,\mathrm{C}\,| = p^5$, then, without loss of generality, we can assume that $c \in \mathrm{C}$. If both $[a,[a,b]]$ and $[b,[a,b]]$ are trivial, then $[a,b] \in Z(G)$, which is not possible. By symmetry, we can assume that $\gamma_3(G) = \langle [a,[a,b]]\rangle$. Notice, by Hall-Witt identity, that $[a,[b,c]] = [b,[a,c]]$. First we assume that $[a,[b,c]]$ is trivial. If $[b,[b,c]]$ or $[a,[a,c]]$ is trivial, then $[b,c]$ or $[a,c]$, respectively, lies in $Z(G)$, which is again not possible. So assume that both $[b,[b,c]]$ and $[a,[a,c]]$ are non trivial. Then $[b,[a,b]] = [b,[b,c]]^t$ for some $t \in \mathbb{F}_p$. Also $[a,[a,b]] = [a,[a,c]]^s$ for some $s \in \mathbb{F}_p^*$. Hence both $[b,[a,b][b,c]^{-t}]$ and $[a,[a,b][a,c]^{-s}]$ are trivial, which implies that $[a,b][a,c]^{-s}[b,c]^{-t} \in Z(G)$, not possible.

Finally assume that $[a,[b,c]]$ is non trivial. Then $[b,[a,c]]$ is also non trivial. If $[b,[b,c]]$ is non trivial, then $[a,[b,c]] = [b,[b,c]]^s$ for some $s \in \mathbb{F}_p^*$, and therefore $[ab^{-s},[b,c]] = 1$. By replacing a by ab^{-s}, we get a modified generating set $\{a,b,c\}$ for G such that $c \in \mathrm{C}$ and $[a,[b,c]] = 1$. Similarly, if $[a,[a,c]]$ is non trivial, then we can modify the generating set for G such that $[b,[a,c]] = 1$. So, in both cases, we land up in first case, which we have already handled. So let $[b,[b,c]] = [a,[a,c]] = 1$. Then $[a,[a,b]][a,[b,c]]^{-s} = 1$, which implies that $[a,[a,b][b,c]^{-s}] = 1$ for some $s \in \mathbb{F}_p^*$. Similarly $[b,[a,b][a,c]^{-t}] = 1$ for some

$t \in \mathbb{F}_p$. This implies that $[a,b][b,c]^{-s}[a,c]^{-t} \in \mathrm{Z}(G)$, which is not possible. Thus C can not have order p^5. Hence $\mathrm{C} = \gamma_2(G)$.

Step 2. *If* $|\mathrm{Z}(G)| = p$, *then* $\mathrm{K}(G) = \gamma_2(G)$.

Proof. By Step 1 we have $\mathrm{C} = \gamma_2(G)$. Notice that $\bar{G} := G/\gamma_3(G)$ is the 3-generated freest group of nilpotency class 2 and order p^6. Let $\alpha_i \in \mathbb{F}_p$, $1 \le i \le 3$. For $\alpha_1 \neq 0$, we have

$$[\bar{a},\bar{b}]^{\alpha_1}[\bar{b},\bar{c}]^{\alpha_2}[\bar{a},\bar{c}]^{\alpha_3} = [\bar{a}\bar{c}^{-\alpha_2\alpha_1^{-1}}, \bar{b}^{\alpha_1}\bar{c}^{\alpha_3}],$$

where $\bar{x} = x\gamma_3(G)$ for $x \in G$. Also, for $\alpha_1 = 0$, we have

$$[\bar{b},\bar{c}]^{\alpha_2}[\bar{a},\bar{c}]^{\alpha_3} = [\bar{c}, \bar{a}^{-\alpha_3}\bar{b}^{-\alpha_2}].$$

Hence for $i \in \mathbb{F}_p$, we get

$$\gamma_2(\bar{G}) = \bigcup_{\epsilon,i} [\bar{a}^{\epsilon}\bar{c}^{i}, \bar{G}].$$

Since $\bar{G}$ is the freest group, by symmetry we can interchange a, b, c in the preceding equation.

To complete the proof of this step, it is sufficient to show that

$$\gamma_3(G) \subseteq \bigcap_{\epsilon,i} [x^{\epsilon}y^{i}, G]$$

for some $x \neq y$ in $\{a,b,c\}$, where $i \in \mathbb{F}_p$ such that ϵ and i are not simultaneously zero. First assume that $[a,[a,b]] \neq 1$, and therefore generates $\gamma_3(G)$. If $[c,[a,b]] \neq 1$, then $[c,[a,b]] = [a,[a,b]]^t$ for some $t \in \mathbb{F}_p^*$. Therefore, by modifying c by ca^{-t}, we get a new generating set $\{a,b,c\}$ for G such that $[c,[a,b]] = 1$ and $[a,[a,b]] \neq 1$. So we can always assume that $[c,[a,b]] = 1$. Since $c \notin \mathrm{C}$, either $[c,[b,c]]$ or $[c,[a,c]]$ is non trivial. Hence for $\epsilon = 0, 1$ and $i \in \mathbb{F}_p$, not simultaneously zero, it is easy to see that $\gamma_3(G) \subseteq \bigcap_{\epsilon,i} [a^\epsilon c^i, G]$.

Now let us assume that $[a,[a,b]] = 1$. Then, notice that, at least one of $[a,[b,c]]$ and $[a,[a,c]]$ is not trivial. If $[b,[a,b]] = 1$, then $[c,[a,b]] \neq 1$. Hence for $\epsilon = 0,1$ and $i \in \mathbb{F}_p$ not simultaneously zero, we get $\gamma_3(G) \subseteq \bigcap_{\epsilon,i} [c^\epsilon a^i, G]$. If $[b,[a,b]] \neq 1$, then $\gamma_3(G) \subseteq \bigcap_{\epsilon,i} [b^\epsilon a^i, G]$, where both ϵ and i are not simultaneously zero.

Step 3. *If* $|\,\mathrm{Z}(G)| = p^2$ *and* $|\gamma_3(G)| = p$, *then* $|\,\mathrm{C}\,| = p^5$.

Proof. If $|\,\mathrm{C}\,| = p^6$, then, without loss of generality, we can assume that $b, c \in \mathrm{C}$, and therefore by Hall-Witt identity it follows that $[b,c] \in \mathrm{Z}(G)$. Hence no non-trivial element of the form $[a,b]^r[a,c]^s$ can lie in $\mathrm{Z}(G)$, where $r, s \in \mathbb{F}_p$. If either $[a,[a,b]]$ or $[a,[a,c]]$ is trivial, then, $\gamma_3(G)$ being of order p, it follows that either $[a,b]$ or $[a,c]$, respectively, lie in $Z(G)$, which is not possible. If both $[a,[a,b]]$ and $[a,[a,c]]$ are non trivial, then $[a,[a,b]] = [a,[a,c]]^t$ for some $t \in \mathbb{F}_p^*$. Hence $[a,b][a,c]^{-t} \in Z(G)$, which is again not possible. Hence $|\,\mathrm{C}\,| \neq p^6$.

If $|\,\mathrm{C}\,| = p^4$, then $\mathrm{C} = \gamma_2(G)$. By a suitable modification in the generating set for G, we can assume that $[b,c] \in Z(G)$. Indeed, if one of $[a,b]$, $[a,c]$ and $[b,c]$ is in $\mathrm{Z}(G)$, then, after suitably renaming the generators, we can assume that $[b,c] \in \mathrm{Z}(G)$. If not, then, after renaming the generators, if necessary, we can assume that $[b,c] = [a,b]^r[a,c]^s$ modulo $\mathrm{Z}(G)$ for some $r, s \in \mathbb{F}_p$. This implies that, modulo $\mathrm{Z}(G)$, $[ba^{-s}, ca^r] = 1$. Thus the new generating set $\{a, ba^{-s}, ca^r\}$ has the required property. Once $[b,c] \in \mathrm{Z}(G)$, notice that both $[a,[a,b]]$ and $[a,[a,c]]$ can not be trivial; otherwise a will lie in C, which can not happen. By symmetry, we can assume that $[a,[a,b]]$ is non trivial and therefore generates $\gamma_3(G)$. By Hall-Witt identity we have $[c,[a,b]] = [b,[a,c]]$. We first assume that $[c,[a,b]]$ is trivial. Then none of the two elements $[c,[a,c]]$ and $[b,[a,b]]$ can be trivial. Indeed, if $[x,[a,x]] = 1$, then $x \in \mathrm{C}$ for $x = b, c$, which is not the case. Then $[a,[a,c]] = [c,[a,c]]^r$ for some $r \in \mathbb{F}_p$, which implies that

$[ac^{-r}, [a, c]] = 1$. Replacing a by ac^{-r}, we get a generating set $\{a' = ac^{-r}, b, c\}$ such that $\gamma_2(G) = \langle [a', b], [a', c], [b, c], [a', [a', b]] \rangle$. A straightforward computation shows that $[b, c] \in Z(G)$ and $[b, [a', c]] = [c, [a', b]] = 1 = [a', [a', c]]$; but $[c, [a', c]]$ and $[b, [a', b]]$ are non trivial. Now $[a', [a', b]] = [b, [a', b]]^t$ for some $t \in \mathbb{F}_p^*$, which implies that $a'b^{-t}$ lies in C, which is not possible.

Now we claim that when at least one the two elements $[b, [a, b]]$ and $[c, [a, c]]$ is non trivial, then we can modify the generating set for G such that $[c, [a, b]] = 1$, but $[b, [a, b]]$ and $[c, [a, c]]$ are both non trivial, and hence we fall in the preceding case. If $[b, [a, b]]$ is non trivial, then $[c, [a, b]] = [b, [a, b]]^t$ for some $t \in \mathbb{F}_p$. Replacing c by $b^{-t}c$, we get the required generating set. If $[c, [a, c]]$ is non trivial, then $[b, [a, c]] = [c, [a, c]]^r$ for some $r \in \mathbb{F}_p$. Now replacing b by $c^{-r}b$, we again get the required generating set.

Finally assume that $[b, [a, c]] = [c, [a, b]]$ is non trivial, and $[b, [a, b]]$ and $[c, [a, c]]$ are both trivial. Then $[a, [a, c]] = [b, [a, c]]^r$ for some $r \in \mathbb{F}_p$, which gives $[ab^{-r}, [a, c]] = 1$. Replacing a by ab^{-r}, we get a generating set $\{a' = ab^{-r}, b, c\}$ for G such that $\gamma_2(G) = \langle [a', b], [a', c], [b, c], [a', [a', b]] \rangle$, with $[b, c] \in Z(G)$ and $[a', [a', c]] = 1$. Notice that $[a', [a', b]] = [a, [a, b]]$ and $[c, [a', b]] = [c, [a, b]]$, both of which are non trivial. Hence $[a', [a', b]] = [c, [a', b]]^t$ for some $t \in \mathbb{F}_p^*$, which gives $[a'c^{-t}, [a', b]] = 1$. Since $[c, [a', c]] = [c, [a, c]] = 1$, it follows that $[a'c^{-t}, [a', c]] = 1$. Hence $a'c^{-t} \in$ C, which is not possible. We have handled all the cases, and the proof of this step is complete.

Step 4. *If* $|\operatorname{Z}(G)| = p^2$ *and* $|\gamma_3(G)| = p$, *then* $\operatorname{K}(G) = \gamma_2(G)$.

Proof. By Step 3, we know that $|\operatorname{C}| = p^5$. Without loss of generality we can assume that $c \in C$. We consider three different cases, namely $[b, c] \in \operatorname{Z}(G)$, $[a, c] \in \operatorname{Z}(G)$ and otherwise. Since $\bar{G} := G/\gamma_3(G)$ is the freest group, then, as explained in Step 2, for proving $\mathrm{K}(G) = \gamma_2(G)$, it is sufficient to show that

$$\gamma_3(G) \subseteq \bigcap_{\epsilon, i} [x^\epsilon y^i, G]$$

for some $x \neq y$ in $\{a, b, c\}$, where $\epsilon = 0, 1$ and $i \in \mathbb{F}_p$ such that ϵ and i are not simultaneously zero.

Case (i). Let $[b, c] \in \mathrm{Z}(G)$. Notice that all $[a, [b, c]]$, $[c, [a, b]]$ and $[b, [a, c]]$ are trivial. Then none of the two elements $[a, [a, c]]$ and $[b, [a, b]]$ can be trivial. Thus for any $t, i \in \mathbb{F}_p$ we have $[a, [a, c]]^t = [ab^i, [a, c]^t]$ and $[b, [a, b]]^t = [b, [a, b]^t]$, which implies that

$$\gamma_3(G) = \bigcap_{\epsilon, i} [a^\epsilon b^i, \gamma_2(G)] \subseteq \bigcap_{\epsilon, i} [a^\epsilon b^i, G],$$

where ϵ and i are not simultaneously zero. Hence $\mathrm{K}(G) = \gamma_2(G)$ by Lemma 1.3.7.

Case (ii). Next assume that $[a, c] \in \mathrm{Z}(G)$. This is symmetric to *Case (i)*, so the proof is omitted.

Case (iii). Let neither $[b, c]$ nor $[a, c]$ lie in $\mathrm{Z}(G)$. We can assume that none of the two elements $[b, c]$ and $[a, c]$ can be a power of the other. For, if $[b, c] = [a, c]^t$, for some $t \in \mathbb{F}_p^*$, then we can take a generating set $\{a, ba^{-t}, c\}$ such that $[ba^{-t}, c] \in \mathrm{Z}(G)$, and we fall in Case (i). We now modify the generating set for G to $\{a', b', c\}$ such that $[a', b'] \in \mathrm{Z}(G)$ and $c \in \mathrm{C}$. If $[a, b] \in \mathrm{Z}(G)$, then obviously we take $\{a' = a, b' = b, c\}$. If not, then, modulo $\mathrm{Z}(G)$, $[a, b] = [a, c]^r [b, c]^s$ for some $r, s \in \mathbb{F}_p$. This implies that, modulo $\mathrm{Z}(G)$, $[ac^s, bc^{-r}] = 1$. Thus if we take $\{a' = ac^s, b' = bc^{-r}, c\}$ as a generating set for G, then $[a', b'] \in \mathrm{Z}(G)$ and c still lies in C.

First assume that $[a', [a', c]] = [b', [b', c]] = 1$. Since $a', b' \notin C$, we have $[a', [b', c]] = [b', [a', c]] \neq 1$. For any $t, i \in \mathbb{F}_p$ we have $[a', [b', c]]^t = [a'b'^i, [b', c]^t]$

and $[b', [a', c]]^t = [b', [a', c]^t]$. Thus for $\epsilon = 0, 1$ and $i \in \mathbb{F}_p$, not simultaneously zero, we get

$$\gamma_3(G) = \bigcap_{\epsilon,i} [a^{\epsilon}b^i, \gamma_2(G)] \subseteq \bigcap_{\epsilon,i} [a^{\epsilon}b^i, G].$$

Now assume that $[b', [b', c]]$ or $[a', [a', c]]$ is non trivial. We only present the proof when $[b', [b', c]] \neq 1$. The other case goes on similar lines. Without loss of generality, we can assume $[a', [b', c]] = [b', [a', c]] = 1$. Indeed, if $[b', [a', c]] = 1$, then nothing to be done. Otherwise $[a', [b', c]] = [b', [b', c]]^s$, which gives $[a'b'^{-s}, [b', c]] = 1$. Replacing a' by $a'b'^{-s}$, we get the required generating set $\{\tilde{a} = a'b'^{-s}, b', c\}$ for which $[b', [\tilde{a}, c]] = [\tilde{a}, [b', c]] = 1$, $[\tilde{a}, b'] \in Z(G)$, $c \in C$ and $[\tilde{a}, [\tilde{a}, c]] \neq 1$. For any $t, i \in \mathbb{F}_p$ we have $[\tilde{a}, [\tilde{a}, c]]^t = [\tilde{a}b'^i, [\tilde{a}, c]^t]$ and $[b', [b', c]]^t = [b', [b', c]^t]$. Thus for $\epsilon = 0, 1$ and $i \in \mathbb{F}_p$, not simultaneously zero, we get

$$\gamma_3(G) = \bigcap_{\epsilon,i} [a^{\epsilon}b^i, \gamma_2(G)] \subseteq \bigcap_{\epsilon,i} [a^{\epsilon}b^i, G].$$

Hence $\mathrm{K}(G) = \gamma_2(G)$, which completes the proof of Step 4.

It only remains to handle the situation when $|\mathrm{Z}(G)| = |\gamma_3(G)| = p^2$. We claim that $b(G) = 4$ in this case. Contrarily assume that $b(G) = 3$. Then by Theorem 2.1.2 there exists a normal subgroup H of G such that $|G/H : \mathrm{Z}(G/H)| = p^3$. Since $\mathrm{Z}(G) = \gamma_3(G)$ is of order p^2, the nilpotency class of G/H is 3. So we can assume that $cH \in \mathrm{Z}(G/H)$. Notice that $|\gamma_2(G/H)/\gamma_3(G/H)|$ must be p^2, which is not possible as G/H admits only two non-central generators. Hence the claim follows, and the proof of the lemma is complete □

We now prove

Lemma 3.4.2 *Let G be a group of order p^7 and nilpotency class 3 with $b(G) = 3$, $|Z(G)| = p^3$ and $\gamma_2(G)$ elementary abelian of order p^4, where p is an odd prime. Then $\mathrm{K}(G) \neq \gamma_2(G)$. Moreover, the commutator length of G is 2.*

Proof. We start by noticing that $|\gamma_3(G)| \leq p^2$. Let $G = \langle a, b, c\rangle$. Then $\gamma_2(G) =$

$\langle [a,b],[b,c],[a,c],\gamma_3(G)\rangle$. Without loss of generality we can assume that $Z(G) = \langle [b,c],[a,c],\gamma_3(G)\rangle$. Indeed, modulo Z$(G)$, we can assume that c commutes with a and b. This, by Hall-Witt identity, implies that $c \in C_G(\gamma_2(G))$. Now we consider two cases, namely, $|\gamma_3(G)|$ is p or p^2.

First assume $|\gamma_3(G)| = p$. By suitably modifying the generating set $\{a,b,c\}$, if necessary, we can assume that $[a,[a,b]] \neq 1$ and $[b,[a,b]] = 1$. Hence $\gamma_3(G) = \langle [a,[a,b]]\rangle$. Now we claim that $[b,c][a,[a,b]]$ is not a commutator. Contrarily assume that

$$[b,c][a,[a,b]] = [a^{\alpha_1}b^{\alpha_2}c^{\alpha_3}[a,b]^{\alpha_4}, a^{\beta_1}b^{\beta_2}c^{\beta_3}[a,b]^{\beta_4}].$$

for some $\alpha_i, \beta_j \in \mathbb{F}_p$, where $1 \leq i,j \leq 4$. After solving and comparing the powers, we get

$$\beta_2\alpha_1 - \alpha_2\beta_1 = 0, \tag{3.4.1}$$
$$\beta_3\alpha_2 - \alpha_3\beta_2 = 1, \tag{3.4.2}$$
$$\beta_3\alpha_1 - \alpha_3\beta_1 = 0, \tag{3.4.3}$$
$$\alpha_2\binom{\beta_1}{2} - \beta_2\binom{\alpha_1}{2} + \beta_4\alpha_1 - \alpha_4\beta_1 = 1. \tag{3.4.4}$$

If $\alpha_2 = 0$, then from (3.4.2), we get α_3, β_2 are non zero. So (3.4.1) gives $\alpha_1 = 0$, which in turn, using (3.4.3) gives $\beta_1 = 0$. But these values contradict (3.4.4). Now let $\alpha_2 \neq 0$. Then from (3.4.1), $\beta_1 = \beta_2\alpha_1{\alpha_2}^{-1}$. Substituting β_1 in (3.4.4), we get

$$\alpha_1\big(\beta_4 + \alpha_2^{-1}\beta_2((\alpha_1\beta_2 - \alpha_2\beta_2)/2 - \alpha_4)\big) = 1;$$

hence $\alpha_1 \neq 0$. Substituting β_1 in (3.4.3), we get $\alpha_1(\beta_3 - \alpha_3\beta_2{\alpha_2}^{-1}) = 0$. Hence $\beta_3 = \alpha_3\beta_2{\alpha_2}^{-1}$, which contradicts (3.4.2). Our claim is now settled.

Now we assume $|\gamma_3(G)| = p^2$. Thus $\gamma_3(G) = \langle [a,[a,b]],[b,[a,b]]\rangle$. Notice that if neither $[a,c]$ nor $[b,c]$ lies in $\gamma_3(G)$, then one of them will be a power of the other modulo $\gamma_3(G)$. Then we can modify the generating set $\{a,b,c\}$ such that $[a,c] \in \gamma_3(G)$, without disturbing other setup. Let $[a,c] = [a,[a,b]]^{t_1}[b,[a,b]]^{t_2}$ for some $t_1, t_2 \in \mathbb{F}_p$. Then $[a, c[a,b]^{-t_1}] = [b,[a,b]]^{t_2}$. By replacing c with $c[a,b]^{-t_1}$, we get a modified generating set for G, which we still call $\{a,b,c\}$, such that $[a,c] = [b,[a,b]]^{t_2}$ and $c \in C_G(\gamma_2(G))$. If $t_2 = 0$, then $[a,c] = 1$, otherwise we can replace c by $c^{t_2^{-1}}$, and assume that $t_2 = 1$; hence $[a,c] = [b,[a,b]]$.

Let us assume that for given $\lambda, \nu \in \mathbb{F}_p^*$, there exist $\alpha_i, \beta_i \in \mathbb{F}_p$ such that

$$[b,c]^{\lambda}[a,[a,b]]^{\nu} = [a^{\alpha_1}b^{\alpha_2}c^{\alpha_3}[a,b]^{\alpha_4}, a^{\beta_1}b^{\beta_2}c^{\beta_3}[a,b]^{\beta_4}].$$

After solving and comparing the powers on both sides, we get

$$\beta_2\alpha_1 - \alpha_2\beta_1 = 0 \qquad (3.4.5)$$

$$\beta_3\alpha_2 - \alpha_3\beta_2 = \lambda \qquad (3.4.6)$$

$$\beta_1\beta_2\alpha_2 - \alpha_1\alpha_2\beta_2 - \alpha_1\binom{\beta_2}{2} + \beta_1\binom{\alpha_2}{2} + (\beta_3\alpha_1 - \alpha_3\beta_1) + \beta_4\alpha_2 - \alpha_4\beta_2 = 0 \qquad (3.4.7)$$

$$\alpha_2\binom{\beta_1}{2} - \beta_2\binom{\alpha_1}{2} + \beta_4\alpha_1 - \alpha_4\beta_1 = \nu, \qquad (3.4.8)$$

Using (3.4.5) in (3.4.7) and (3.4.8), we, respectively, get

$$(\beta_1\beta_2\alpha_2 - \alpha_1\alpha_2\beta_2)/2 + (\beta_3\alpha_1 - \alpha_3\beta_1) + \beta_4\alpha_2 - \alpha_4\beta_2 = 0 \qquad (3.4.9)$$

$$(\beta_1\beta_2\alpha_1 - \alpha_1\alpha_2\beta_1)/2 + \beta_4\alpha_1 - \alpha_4\beta_1 = \nu. \qquad (3.4.10)$$

We proceed in two different cases, namely, $[a,c] = 1$ and $[a,c] = [b,[a,b]]$.

Case(1). Let $[a,c] = 1$. Then (3.4.9) reduces to

$$(\beta_1\beta_2\alpha_2 - \alpha_1\alpha_2\beta_2)/2 + \beta_4\alpha_2 - \alpha_4\beta_2 = 0. \qquad (3.4.11)$$

If $\alpha_2 = 0$, then by (3.4.6), we get $\beta_2 \neq 0$, which using, (3.4.5), gives $\alpha_1 = 0$. Hence by (3.4.11), $\alpha_4 = 0$, which contradicts (3.4.10). If $\alpha_2 \neq 0$ and $\alpha_1 = 0$, then by (3.4.5) $\beta_1 = 0$, which contradicts (3.4.10). Hence, $\alpha_2 \neq 0$ implies $\alpha_1 \neq 0$. By symmetry we can take both β_1 and β_2 non zero. Hence we can assume that $\alpha_1, \alpha_2, \beta_1, \beta_2$ are all nonzero.

Computing the value of α_4 from (3.4.11) and substituting in (3.4.10), we get

$$(\beta_1\beta_2\alpha_1 - \alpha_1\alpha_2\beta_1)/2 + \beta_4\alpha_1 - ((\beta_1\alpha_2 - \alpha_1\alpha_2)/2 + \beta_4\alpha_2{\beta_2}^{-1})\beta_1 = \nu.$$

Using (3.4.5), it is easy to see that the left hand side of the preceding equation is zero, which contradicts the choice of ν. Hence for any $\lambda, \nu \in \mathbb{F}_p^*$, $[b,c]^\lambda[a,[a.b]]^\nu$ is not a commutator.

Case(2). Let $[a,c] = [b,[a,b]]$. If $\alpha_2 = 0$, then by (3.4.5), $\alpha_1 = 0$, and the equations (3.4.6), (3.4.9) and (3.4.10), respectively, reduces to

$$\begin{aligned} \alpha_3\beta_2 &= -\lambda \\ \alpha_3\beta_1 + \alpha_4\beta_2 &= 0 \\ \alpha_4\beta_1 &= -\nu. \end{aligned}$$

Solving this we get $({\beta_1}^{-1}\beta_2)^2 = -\lambda\nu^{-1}$, which is not possible for a choice of λ and μ such that $-\lambda\nu^{-1}$ is a non-quadratic residue mod p. Hence for any such $\lambda, \nu \in \mathbb{F}_p^*$, $[b,c]^\lambda[a,[a,b]]^\nu$ is not a commutator. If $\alpha_2 \neq 0$ and $\alpha_1 = 0$, then by (3.4.5) $\beta_1 = 0$, which contradicts (3.4.10). Hence, $\alpha_2 \neq 0$ implies $\alpha_1 \neq 0$. By symmetry we can take both β_1 and β_2 non zero. Hence we can assume that $\alpha_1, \alpha_2, \beta_1, \beta_2$ are all nonzero.

Using (3.4.5) in (3.4.9) and (3.4.10), we, respectively, get

$$\alpha_4 = (\beta_1\alpha_2 - \alpha_1\alpha_2)/2 + {\beta_2}^{-1}(\beta_3\alpha_1 - \alpha_3\beta_1) + \beta_4\alpha_2{\beta_2}^{-1}$$

and

$$\alpha_4 = (\beta_2\alpha_1 - \alpha_1\alpha_2)/2 + \beta_4\alpha_1{\beta_1}^{-1} - \nu{\beta_1}^{-1}.$$

Equating these equations and using (3.4.5), we get $(\beta_3\alpha_1 - \alpha_3\beta_1) = -\nu{\beta_1}^{-1}\beta_2$. Multiply both sides by ${\beta_1}^{-1}\beta_2$ and using (3.4.5) and (3.4.6), we further get $({\beta_1}^{-1}\beta_2)^2 = -\lambda\nu^{-1}$. Hence, as above, for λ and ν such that $-\lambda\nu^{-1}$ is a non-quadratic residue mod p, $[b,c]^\lambda[a,[a,b]]^\nu$ is not a commutator. The proof is now complete by taking G/H, where H is any subgroup of $\mathrm{Z}(G)$ of order p contained in $\mathrm{K}(G)$, and using Theorem 1.1.5 and Lemma 1.3.6. □

Lemma 3.4.3 *Let L be a finite p-group of order at least p^8 and nilpotency class 3 with $b(L) = 3$, $|\mathrm{Z}(L)| = p^3$, $\mathrm{Z}(L) \le \gamma_2(L)$ and $\gamma_2(L)$ elementary abelian of order p^4. Then $\mathrm{K}(L) = \gamma_2(L)$.*

Proof. Notice that $|\gamma_3(L)| \le p^2$. We first assume that $|\gamma_3(L)| = p$. Then by Theorem 2.1.2 there exists a normal subgroup H of L such that $|L/H : \mathrm{Z}(L/H)| = p^3$. If $H \ne \gamma_3(L)$, then it follows from Theorem 2.1.4 that L admits a 2-generator subgroup G such that $\gamma_2(G) = \gamma_2(L)$, which is not possible as $|\gamma_2(L)/\gamma_3(L)| = p^3$. Hence $H = \gamma_3(L)$, and therefore, again by Theorem 2.1.4, L admits a 3-generator subgroup G of order p^7 such that $\gamma_2(G) = \gamma_2(L)$.

If $|L| = p^8$, then $L = \langle a,b,c,d\rangle$ such that $G = \langle a,b,c\rangle$ and $[d,G] = H$. If $|L| \ge p^9$, then, for some integer $k \ge 2$, $L = \langle a,b,c,x_1,\dots,x_k\rangle$ such that $G = \langle a,b,c\rangle$ with $\gamma_2(G) = \gamma_2(L)$ and $[x_i, L] = H$ for $1 \le i \le k$. First assume that $[x_i, G] = H$ for some $1 \le i \le k$. Then the subgroup $M := \langle a,b,c,d\rangle$, where $d = x_i$, is of order p^8 such that $[d,G] = H$ and $\gamma_2(M) = \gamma_2(L)$. Hence it is sufficient to work with M. So this case reduces to the preceding situation when $|L| = p^8$.

It now follows from the proof of Lemma 3.4.2 that we can modify the generating set for G such that $\gamma_2(L) = \gamma_2(G) = \langle [a,b],[a,c],[b,c],[a,[a,b]]\rangle$

and $[c,[a,b]] = 1$. Notice that L/H is of nilpotency class 2, and therefore $\gamma_2(L/H) = \langle [\bar{a},\bar{b}], [\bar{a},\bar{c}], [\bar{b},\bar{c}] \rangle$, where $\bar{x} = xH$ for all $x \in L$. Also notice that $\bar{d} \in \mathrm{Z}(L/H)$.

If $[a,d] = [a,[a,b]]^t$ for some $t \in \mathbb{F}_p$, then $[a, d[a,b]^{-t}] = 1$. Replacing d by $d[a,b]^{-t}$, we can assume that $[a,d] = 1$. If $[c,d] \neq 1$, then $[c,d] = [a,[a,b]]^r$ for some $r \in \mathbb{F}_p^*$. Let $\alpha_i \in \mathbb{F}_p$, $1 \leq i \leq 4$. If $\alpha_1 \neq 0$, then we can write

$$[a,b]^{\alpha_1}[b,c]^{\alpha_2}[a,c]^{\alpha_3} = [ac^{-\alpha_2\alpha_1^{-1}}, b^{\alpha_1}c^{\alpha_3}]$$

modulo H and

$$[a,[a,b]]^{\alpha_4} = [ac^{-\alpha_2\alpha_1^{-1}}, [a,b]^{\alpha_4}].$$

If $\alpha_1 = 0$, then we can write

$$[b,c]^{\alpha_2}[a,c]^{\alpha_3} = [c, a^{-\alpha_3}b^{-\alpha_2}]$$

modulo H and

$$[a,[a,b]]^{\alpha_4} = [c, d^{\alpha_4 r^{-1}}].$$

Thus for $i \in \mathbb{F}_p$ and $\epsilon = 0,1$, we get

$$\gamma_2(L)/H = \bigcup_{\epsilon,i} [\bar{a}^{\epsilon}\bar{c}^{i}, \bar{L}]$$

and

$$H \subseteq \bigcap_{\epsilon,i} [a^{\epsilon}c^{i}, L],$$

where $\bar{x} = xH$ for $x \in L$, and i and ϵ are not simultaneously zero. Hence, by Lemma 1.3.7, $\mathrm{K}(L) = \gamma_2(L)$. Finally, if $[c,d] = 1$, then $[b,d] \neq 1$. The assertion now follows on the same lines as above.

Now we consider the remaining case for the group L with $|L| \geq p^9$, i.e.,

$[x_i, G] = 1$ for all $1 \le i \le k$. Then L is a central product of G and $K := \langle x_1, \ldots, x_k \rangle$ amalgamating H. Since $\mathrm{Z}(L) \le \gamma_2(L)$, K can not be abelian. Thus $H = \langle [x_i, x_j] \rangle$ for some $1 \le i < j \le k$. Then the subgroup $N := \langle a, b, c, d, e \rangle$, where $d = x_i$ and $e = x_j$, is of order p^9 such that $\gamma_2(N) = \gamma_2(L)$. Now on the lines of the preceding case, for $i \in \mathbb{F}_p$, it is not difficult to see that

$$\gamma_2(N)/H = \bigcup_i \, [\bar{a}\bar{c}^i\bar{d}, \bar{N}] \bigcup \, [\bar{c}\bar{d}, \bar{N}]$$

and

$$H \subseteq \bigcap_i \, [ac^i d, N] \bigcap \, [cd, N],$$

where $\bar{x} = xH$ for $x \in N$. Hence, again by Lemma 1.3.7, $\mathrm{K}(N) = \gamma_2(N)$.

Now assume that $|\gamma_3(L)| = p^2$. As in the above case, we can show that $H \not\le \gamma_3(L)$. Then, by Theorem 2.1.4, either (i) L admits a 2-generator subgroup G of order p^5 and nilpotency class 3 such that L is a central product of G and subgroup K with $|\gamma_2(K)| = p$ or (ii) L admits a 3-generator subgroup G of order p^7 and nilpotency class 3 such that $\gamma_2(G) = \gamma_2(L)$ and L is an amalgamated semidirect product of G and a subgroup K of nilpotency class at most 2. In case (i), it follows from Lemma 1.3.3 that $\mathrm{K}(L) = \gamma_2(L)$. So assume (ii).

If $|L| = p^8$, then $L = \langle a, b, c, d \rangle$ such that $G = \langle a, b, c \rangle$ and $\langle [d, G] \rangle = H$. If $|L| \ge p^9$, then, for some integer $k \ge 2$, $L = \langle a, b, c, x_1, \ldots, x_k \rangle$ such that $G = \langle a, b, c \rangle$ and $\langle [x_i, L] \rangle = H$ for $1 \le i \le k$. First assume that $[x_i, G] = H$ for some $1 \le i \le k$. Then the subgroup $M := \langle a, b, c, d \rangle$, where $d = x_i$, is of order p^8 such that $[d, G] = H$ and $\gamma_2(M) = \gamma_2(L)$. As observed above, it is sufficient to work with the situation when $|L| = p^8$.

As explained in the proof of Lemma 3.4.2, we can assume that $H = \langle [b, c] \rangle$,

$$\gamma_3(G) = \langle [a, [a, b]], [b, [a, b]] \rangle \,,$$

$[a, c] \in \gamma_3(G)$ and $c \in \mathrm{C}_G(\gamma_2(G))$. If $[b, d] = [b, c]^t$ for some $t \in \mathbb{F}_p$, then $[b, dc^{-t}] = 1$. Set $d' = dc^{-t}$. If $[c, d'] = [b, c]^s$ for some $s \in \mathbb{F}_p$, then $[c, d'b^s] = 1$. Replacing d by $d'b^s$, we can assume that $[b, d] = [c, d] = 1$. Let $[a, d] = [b, c]^r$ for some $r \in \mathbb{F}_p^*$. Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{F}_p$. If $\alpha_3 \neq 0$, then we can write

$$[a, b]^{\alpha_1}[b, [a, b]]^{\alpha_2}[a, [a, b]]^{\alpha_3} = [ab^{\alpha_2\alpha_3^{-1}}[a, b]^{\frac{1-\alpha_1}{2}}, b^{\alpha_1}[a, b]^{\alpha_3}]$$

modulo H and

$$[b, c]^{\alpha_4} = [ab^{\alpha_2\alpha_3^{-1}}[a, b]^{\frac{1-\alpha_1}{2}}, d^{\alpha_4 r^{-1}}].$$

If $\alpha_3 = 0$, then we can write

$$[a, b]^{\alpha_1}[b, [a, b]]^{\alpha_2} = [b[a, b]^{-\frac{\alpha_1+1}{2}}, a^{-\alpha_1}[a, b]^{\alpha_2}]$$

modulo H and

$$[b, c]^{\alpha_4} = [b[a, b]^{-\frac{\alpha_1-1}{2}}, c^{\alpha_4}].$$

Thus, for $i, j \in \mathbb{F}_p$ and $\epsilon = 0, 1$ such that i and ϵ are not simultaneously zero, we get

$$\gamma_2(L)/H = \bigcup_{\epsilon,i,j} [\bar{a}^{\epsilon}\bar{b}^{i}[a, b]^{j}, \bar{L}]$$

and

$$H \subseteq \bigcap_{\epsilon,i,j} [a^{\epsilon}b^{i}[a, b]^{j}, L],$$

where $\bar{x} = xH$ for $x \in L$. Hence $\mathrm{K}(L) = \gamma_2(L)$.

Finally assume that $[x_i, G] = 1$ for all $1 \leq i \leq k$. In this case, L is a central product of G and $K := \langle x_1, \ldots, x_k\rangle$ amalgamating some subgroup containing H. Since $\mathrm{Z}(L) \leq \gamma_2(L)$, K can not be abelian. Thus $H = \langle [x_i, x_j]\rangle$ for some $1 \leq i < j \leq k$. Then the subgroup $N := \langle a, b, c, d, e\rangle$, where $d = x_i$ and $e = x_j$, is of order p^9 such that $\gamma_2(N) = \gamma_2(L)$. For $i \in \mathbb{F}_p$, it is again easy to see that

$$\gamma_2(N)/H = \bigcup_i \, [\bar{a}\bar{b}^i\bar{d}\,[\bar{a},\bar{b}]^{\frac{1-\alpha_1}{2}}, \bar{N}] \, \bigcup \, [\bar{b}\bar{d}\,[\bar{a},\bar{b}]^{-\frac{\alpha_1+1}{2}}, \bar{N}]$$

and

$$H \subseteq \bigcap_i \, [ab^i d\,[a,b]^{\frac{1-\alpha_1}{2}}, N] \, \bigcap \, [bd\,[a,b]^{-\frac{\alpha_1-1}{2}}, N],$$

where $\bar{x} = xH$ for $x \in N$. Thus $\mathrm{K}(N) = \gamma_2(N)$, and the proof is complete. $\square$

3.5 Proof of Theorem 3.1.1

We are now ready to provide *Proof of Theorem 3.1.1.* Let G be a finite p-group such that $\gamma_2(G)$ is of order p^4 and exponent p. Also let $\mathrm{Z}(G) \leq \gamma_2(G)$. Notice that the nilpotency class of G is at most 5 and $|G| \geq p^6$. If $b(G) = 4$, then $\mathrm{K}(G) = \gamma_2(G)$. So by Remark 2.1.3 we can assume that $b(G) = 3$. If the nilpotency class of G is at most 3, then $\gamma_2(G)$ is abelian. When the nilpotency class of G is 2, the assertion follows from Lemmas 3.2.1 - 3.2.4. Now let the nilpotency class of G be 3. It follows from [22] that there is no such group of order p^6 and nilpotency class 3 which satisfies the given hypothesis. Hence $|G| \geq p^7$. If $|\mathrm{Z}(G)| \leq p^2$, then $\mathrm{K}(G) = \gamma_2(G)$ by Lemma 3.4.1. So assume that $|\mathrm{Z}(G)| = p^3$. Now if $|G| = p^7$, then by Lemma 3.4.2, we have $\mathrm{K}(G) \neq \gamma_2(G)$, otherwise by Lemma 3.4.3, we have $\mathrm{K}(G) = \gamma_2(G)$. Now it only remains to handle the cases when the nilpotency class of G is 4 or 5.

First let the nilpotency class of G be 4 and $b(G) = 3$. If $|G| = p^6$, then, $\gamma_2(G)/\gamma_3(G)$ being cyclic, $[\gamma_2(G), \gamma_2(G)] = [\gamma_2(G), \gamma_3(G)] = 1$; therefore $\gamma_2(G)$ is abelian. It now follows from Lemma 3.3.1 that $\mathrm{K}(G) = \gamma_2(G)$ if and only if $|\mathrm{Z}(G)| = p$. So assume that $|G| \geq p^7$. By Lemma 1.3.2 $\mathrm{Z}(G)$ can not be maximal in $\gamma_2(G)$, therfore $|\mathrm{Z}(G)| \leq p^2$. It follows from Theorem 2.1.2 that G admits a normal subgroup H of order p such that $|G/H : \mathrm{Z}(G/H)| = p^3$. In this case the only choice for H is $\gamma_4(G)$. If not, then G/H will be of nilpotency class 4, which is not possible as $(G/H)/\operatorname{Z}(G/H)$ can have nilpotency class at most 2. Thus G/H has nilpotency class 3. Since $\gamma_2(G/H) \neq \operatorname{Z}(G/H)$, it follows that $\gamma_2(G/H)\operatorname{Z}(G/H)$ has index p^2 in G/H, and therefore $\gamma_2(G/H)/\gamma_3(G/H)$ is cyclic. Since $H = \gamma_4(G)$, we also have that $\gamma_2(G)/\gamma_3(G)$ is cyclic, which, in the present case, implies that $\gamma_2(G)$ is abelian. Now invoking Theorem 2.1.4, there exists a 2-generator subgroup T of G such that $|T| = p^6$, $\gamma_2(T) = \gamma_2(G)$ and G is an amalgamated semidirect product of T and a subgroup K with $|\gamma_2(K)| \leq p$. Also $K = \langle x_1, \ldots, x_k \rangle$, for some $k \geq 1$ such that $[x_i, G] = H$ for $1 \leq i \leq k$. If $[x_i, T] = H$ for some $1 \leq i \leq k$, then the subgroup $M := \langle a, b, c \rangle$, where $c = x_i$ is of order p^7 such that $\gamma_2(M) = \gamma_2(G)$. Hence it follows from Lemma 3.3.2 that $\operatorname{K}(G) = \gamma_2(G)$. Now assume that $[x_i, T] = 1$ for all $1 \leq i \leq k$. Since $\operatorname{Z}(G) \leq \gamma_2(G)$, it follows that K is non-abelian. Thus G is a central product of T and K amalgamating a subgroup containing H. If $|\operatorname{Z}(G)| = p$, then $|\operatorname{Z}(T)| = p$, and therefore by Lemma 3.3.1 we have $\operatorname{K}(T) = \gamma_2(T)$. Hence $\operatorname{K}(G) = \gamma_2(G)$. Now we take the case when $|\operatorname{Z}(G)| = p^2$. Notice that $\gamma_2(K) = H$, and therefore there exists $x_i, x_j \in K$ such that $H = \langle [x_i, x_j] \rangle$ for some $1 \leq i < j \leq k$. Let $N := \langle a, b, c, d \rangle$, where $c = x_i$ and $d = x_j$. Then $\gamma_2(G) = \gamma_2(N)$. Set $\bar{N} = N/H$. As observed in the proof of Lemma 3.3.2,

$$\gamma_2(\bar{N}) = \left\langle [\bar{a}, \bar{b}], [\bar{a}, [\bar{a}, \bar{b}]], [\bar{b}, [\bar{a}, \bar{b}]] \right\rangle.$$

It is now not difficult to see that for $i, j \in \mathbb{F}_p$ we have

$$\gamma_2(\bar{N}) = \bigcup_{i,j} [\bar{a}^i \bar{b}^j \bar{c}, \bar{N}].$$

An easy computation also shows that $H \subseteq [a^i b^j c, N]$ for all $i, j \in \mathbb{F}_p$. Hence $\operatorname{K}(N) = \gamma_2(N)$ by Lemma 1.3.7, and therefore we have $\operatorname{K}(G) = \gamma_2(G)$.

Finally let the nilpotency class of G be 5. We claim that $b(G) = 4$. Contrarily assume that $b(G) = 3$. Since the nilpotency class of $G/\mathrm{Z}(G)$ is 4 and $\mathrm{Z}(G) \leq \gamma_2(G)$, we have $|\mathrm{Z}(G)| = p$. Hence, in view of Theorem 2.1.2, the only choice for normal subgroup H of G such that $|G/H : \mathrm{Z}(G/H)| = p^3$ is $\mathrm{Z}(G)$. Thus $|G/\mathrm{Z}(G) : \mathrm{Z}_2(G)/\mathrm{Z}(G)| = p^3$, which implies that $|G/\mathrm{Z}_2(G)| = p^3$, where $\mathrm{Z}_2(G)$ denotes the second center of G. This contradicts the fact that the nilpotency class of $G/\mathrm{Z}_2(G)$ is 3. Our claim is now settled. If $\mathrm{K}(G) \neq \gamma_2(G)$, then it follows from Lemma 3.2.1, Lemma 3.2.2, Lemma 3.3.1 and Lemma 3.4.2 that the commutator length of G is 2. The proof of the theorem is now complete. □

3.6 Examples

In this section we present various examples of groups, which occurred in this chapter and this shows that no class of groups considered in Theorem 3.1.1 is void. These examples are constructed from the structural information of the groups obtained in our proofs, and have been verified for $p = 3, 5, 7$ using GAP [4]. For notational convenience, we use long generating set instead of minimal one.

Groups of class 2. Let F be the freest p-group of nilpotency class 2 and exponent p on 4 generators, a, b, c, d (say), where p is an odd prime. Let $R := \langle [b, d], [a, d] \rangle$. Then $G := F/R$ is a group of nilpotency class 2 and order p^8 such that $\mathrm{K}(G) \neq \gamma_2(G)$. If we take $R_1 := \langle [a, b][c, d],\ [a, c][b, d]^r \rangle$, where r is any fixed non-square integer modulo p. Then it follows from [34, Theorem 1.2] that $G_1 := F/R_1$ is a group of order p^8, nilpotency class 2 and conjugate type $\{1, p^3\}$. For p-groups G, p odd, of nilpotency class 2 and order at least p^9, we know that $\mathrm{K}(G) = \gamma_2(G)$. Such examples of order $\geq p^{10}$ can be constructed by taking a central product of the group $G := F/R$ and any finite extraspecial p-group K amalgamating $\langle [\bar{c}, \bar{d}] \rangle = \gamma_2(K)$. Constructing such examples of order p^9 is also easy, as explained in the proof of Lemma 3.2.4.

Groups of class 3. We present five types of p-group of nilpotency class 3 and order p^7, where p is an odd prime. Consider the group presented as

$$\begin{aligned} G = \Big\langle & \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \gamma \mid [\alpha_2, \alpha_1] = \alpha_4, [\alpha_3, \alpha_1] = \alpha_5, [\alpha_3, \alpha_2] = \alpha_6, \\ & [\alpha_4, \alpha_2] = \gamma, [\alpha_5, \alpha_3] = \gamma, [\alpha_5, \alpha_2] = \gamma, [\alpha_6, \alpha_1] = \gamma, {\alpha_1}^p = \gamma, \\ & {\alpha_i}^p = \gamma^p = 1 \ (2 \leq i \leq 6) \Big\rangle. \end{aligned}$$

Notice that $|\,\mathrm{Z}(G)| = p$ and $\mathrm{K}(G) = \gamma_2(G)$.

The following group G is such that $|Z(G)| = p^2 = |\gamma_3(G)|$ and $\mathrm{K}(G) = \gamma_2(G)$:

$$\begin{aligned} G = \Big\langle & \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \gamma \mid [\alpha_i, \alpha_1] = \alpha_{i+2}, [\alpha_5, \alpha_1] = \gamma, \\ & {\alpha_i}^p = \gamma^p = 1 \ (1 \leq i \leq 6) \Big\rangle. \end{aligned}$$

The next group G is such that $|Z(G)| = p^2$, $|\gamma_3(G)| = p$ and $\mathrm{K}(G) = \gamma_2(G)$:

$$\begin{aligned} G = \Big\langle & \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \gamma \mid [\alpha_2, \alpha_1] = \alpha_4, [\alpha_3, \alpha_1] = \alpha_5, [\alpha_3, \alpha_2] = \alpha_6, \\ & [\alpha_4, \alpha_2] = \gamma, [\alpha_5, \alpha_3] = \gamma, {\alpha_1}^p = \gamma, {\alpha_i}^p = \gamma^p = 1 \ (2 \leq i \leq 6) \Big\rangle. \end{aligned}$$

We now present a group G such that $|Z(G)| = p^3$, $|\gamma_3(G)| = p$ and $\mathrm{K}(G) \neq \gamma_2(G)$:

$$\begin{aligned} G = \Big\langle & \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \gamma \mid [\alpha_2, \alpha_1] = \alpha_4, [\alpha_3, \alpha_1] = \alpha_5, \\ & [\alpha_3, \alpha_2] = \alpha_6, [\alpha_4, \alpha_1] = \gamma, {\alpha_i}^p = \gamma^p = 1 \ (1 \leq i \leq 6) \Big\rangle. \end{aligned}$$

Finally we present a group G such that $|Z(G)| = p^3$, $|\gamma_3(G)| = p^2$ and

$\mathrm{K}(G) \neq \gamma_2(G)$:

$$G = \Big\langle \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \gamma \mid [\alpha_2, \alpha_1] = \alpha_4, [\alpha_3, \alpha_1] = \alpha_5, [\alpha_4, \alpha_1] = \alpha_6, [\alpha_4, \alpha_2] = \gamma, {\alpha_i}^p = \gamma^p = 1 \ (1 \leq i \leq 6) \Big\rangle.$$

Groups of class 4. We present two types of p-groups of nilpotency class 4 and order p^7, where p is an odd prime. Consider the group presented as

$$G = \Big\langle \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \gamma \mid [\alpha_2, \alpha_1] = \alpha_4, [\alpha_4, \alpha_1] = \alpha_5, [\alpha_4, \alpha_2] = \alpha_6, [\alpha_4, \alpha_3] = [\alpha_5, \alpha_1] = [\alpha_6, \alpha_2] = \gamma, [\alpha_3, \alpha_1] = \gamma, {\alpha_i}^p = \gamma^p = 1 \ (2 \leq i \leq 6) \Big\rangle.$$

For this group $|Z(G)| = p$ and $\mathrm{K}(G) = \gamma_2(G)$.

The following is a group G such that $|Z(G)| = p^2$ and $\mathrm{K}(G) = \gamma_2(G)$:

$$G = \Big\langle \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \gamma \mid [\alpha_2, \alpha_1] = \alpha_4, [\alpha_4, \alpha_1] = \alpha_5, [\alpha_4, \alpha_2] = \alpha_6, [\alpha_3, \alpha_2] = [\alpha_5, \alpha_1] = \gamma, {\alpha_1}^p = \gamma, {\alpha_i}^p = \gamma^p = 1 \ (2 \leq i \leq 6) \Big\rangle.$$

CHAPTER 4

Groups of order p^7

In this chapter we give classification of groups G of order p^7 such that not every element of the commutator subgroup $\gamma_2(G)$ is a commutator.

4.1 Introduction

In Theorem 1.1.6, L. C. Kappe and R. F. Morse proved that $\mathrm{K}(G) = \gamma_2(G)$ for all p-groups G of order at most p^5, $p \geq 3$, and for all 2-groups G of order at most 2^6. They also exhibited groups of order 2^7 for which $\mathrm{K}(G) \neq \gamma_2(G)$. If G is of order p^6, then order of $\gamma_2(G)$ is at most p^4 and it is minimally generated by at most 4 elements. Thus a classification of groups G of order p^6, $p \geq 3$, such that $\mathrm{K}(G) \neq \gamma_2(G)$ follows from Theorem 1.1.5 and Theorem 3.1.1. To have some clarity on the larger perspectives of this problem, it is desirable to study specific and some more classes of p-groups. With this motive, our target in this chapter is to study groups G of order p^7 such that $\mathrm{K}(G) \neq \gamma_2(G)$. The main result of this chapter is as follows.

Theorem 4.1.1 *Let G be a group of order p^7, $p \geq 5$. Then the following* *statements hold:*

(1) *If* $d(\gamma_2(G)) \leq 3$ *or the nilpotency class of* G *is* 6*, then* $\mathrm{K}(G) = \gamma_2(G)$.

(2) *If* $|\gamma_2(G)| = p^4$ *and* $d(\gamma_2(G)) = 4$*, then* $\mathrm{K}(G) \neq \gamma_2(G)$ *if and only if the nilpotency class of* G *is either* 3 *or* 4 *and* $|\,\mathrm{Z}(G)| = p^3$.

(3) *If* $|\gamma_2(G)| = p^5$*,* $d(\gamma_2(G)) = 4$*,* $\exp(\gamma_2(G)) = p^2$ *and the nilpotency class of* G *is* 5*, then* $\mathrm{K}(G) \neq \gamma_2(G)$.

(4) *If* $|\gamma_2(G)| = p^5$*,* $d(\gamma_2(G)) \geq 4$ *and the nilpotency class of* G *is* 4*, then* $\mathrm{K}(G) \neq \gamma_2(G)$ *if and only if there exists a subgroup* $H \leq Z(G)$ *of order* p *such that* $|Z(G/H)| = p^2$.

(5) *If* $\gamma_2(G)$ *is elementary of order* p^5 *and the nilpotency class of* G *is* 5*, then* $\mathrm{K}(G) \neq \gamma_2(G)$.

(6) *If* $\gamma_2(G)$ *is non-abelian of order* p^5*, exponent* p *and the nilpotency class of* G *is* 5*, then* $\mathrm{K}(G) \neq \gamma_2(G)$ *if and only if* $|\gamma_5(G)| = p$ *and* $|\,\mathrm{Z}(G/\gamma_5(G))| = p^2$.

Moreover, the commutator length of G *is at most* 2.

Now we restate Theorem 4.1.1 in a slightly different way as follows:

Theorem 4.1.2 *Let* G *be a group of order* p^7*,* $p \geq 5$*. Then* $K(G) \neq \gamma_2(G)$*, if and only if one of the following holds:*

(a) $|\gamma_2(G)| = p^4$*,* $d(\gamma_2(G)) = 4$ *and the nilpotency class of* G *is either* 3 *or* 4 *and* $|\,\mathrm{Z}(G)| = p^3$.

(b) $|\gamma_2(G)| = p^5$*,* $d(\gamma_2(G)) \geq 4$ *and there exists a subgroup* $H \leq Z(G)$ *of order* p *such that* $|Z(G/H)| = p^2$.

Moreover, if $\mathrm{K}(G) \neq \gamma_2(G)$*, then the commutator length of* G *is* 2.

The proofs of Propositions 4.2.1, 4.2.2, 4.2.3 and 4.3.1 imply that conditions (3-6) in Theorem 4.1.1 are equivalent to condition (b) in Theorem 4.1.2. Thus Theorem 4.1.1 and Theorem 4.1.2 are equivalent. We remark that if Theorem 4.1.2(b) holds, then $|G/H| = p^6$ and further using Lemma 1.3.5 and Theorem 3.1.1(a) we get $\mathrm{K}(G) \neq \gamma_2(G)$. If $\mathrm{K}(G) \neq \gamma_2(G)$ with $|\gamma_2(G)| = p^5$ and $d(\gamma_2(G)) \geq 4$, then it follows from the proofs of Propositions 4.2.1, 4.2.2, 4.2.3 and 4.3.1 that there exists an H with the desired property. While proving Theorem 4.1.1, we obtain many interesting structural results on groups of order p^7. We use GAP [4] for handling the remaining cases of p, that is, 2 and 3, and derive the following conclusion.

Theorem 4.1.3 *For a group G of order 2^7, $\mathrm{K}(G) \neq \gamma_2(G)$ if and only if G is of nilpotency class 3, $\gamma_2(G)$ is a 3-generated abelian subgroup of order 2^4 and $|Z(G)| = 2^3$.*

Let G be a group of order 3^7. Then $K(G) \neq \gamma_2(G)$ if and only if one of the following holds:

(i) *The nilpotency class of G is 5, $\gamma_2(G)$ is a 3-generated subgroup of order 3^5 and $|\mathrm{Z}_2(G)| = 3^3$.*

(ii) *The nilpotency class of G is 4, $\gamma_2(G)$ is a 3-generated subgroup of order 3^4 and $|\mathrm{Z}(G)| = 3^3$.*

(iii) *The nilpotency class of G is 4, $\gamma_2(G)$ is a 4-generated subgroup of order 3^5.*

(iv) *The nilpotency class of G is 3, $\gamma_2(G)$ is a 4-generated subgroup and $|\mathrm{Z}(G)| = 3^3$.*

Moreover, the commutator length of G is at most 2.

We conclude this section by setting some notations for this particular chapter. For a finite p-group G, minimally generated by two elements, say α_1 and α_2, the following notations for commutators will be used throughout: $\beta = [\alpha_1, \alpha_2]$, $\beta_i = [\beta, \alpha_i]$, $\eta_{ij} = [\beta_i, \alpha_j]$ and $\xi_{ijk} = [\eta_{ij}, \alpha_k]$, where $i, j, k \in \{1, 2\}$.

4.2 Groups of nilpotency class 5

In this section we deal with groups G of order p^7 and nilpotency class 5 with $d(\gamma_2(G)) \geq 4$. As we will see, for most of these groups G, $\mathrm{K}(G) \neq \gamma_2(G)$.

Lemma 4.2.1 *Let G be a group of order p^7, $p \geq 3$ such that $\gamma_2(G)$ is a 4 generated subgroup of order p^5 and exponent p^2. Then $\exp(\gamma_3(G)) = p$ and $\beta^p \neq 1$, where β is as defined in the introduction.*

Proof. By the given hypothesis we can assume that G is generated by 2 elements, say α_1, α_2, and hence the nilpotency class of G is at least 4. First we claim that $\gamma_3(G)$ is abelian. If the nilpotency class of G is 4 or 5, then $[\gamma_3(G), \gamma_3(G)] \leq \gamma_6(G) = 1$, and hence $\gamma_3(G)$ is abelian. If the nilpotency class of G is 6, then $|\gamma_i(G)/\gamma_{i+1}(G)| = p$ for $2 \leq i \leq 5$. Now being $\gamma_3(G)/\gamma_4(G)$ of order p, and $[\gamma_3(G), \gamma_4(G)] = 1$, we get $\gamma_3(G)$ is abelian, and our claim is settled. Since $d(\gamma_2(G)) = 4$, it now follows that $|\Phi(\gamma_2(G))| = p$, which further implies that $\Phi(\gamma_2(G)) \leq \mathrm{Z}(G)$. Recall that $\beta = [\alpha_1, \alpha_2]$. Thus for any $x \in G$, we get

$$1 = [\beta^p, x] = [\beta, x]^p,$$

which implies that the exponent of $\gamma_3(G)$ is p. Now if $\beta^p = 1$, then for any $x \in \gamma_3(G)$ we get $(\beta x)^p = \beta^p x^p = \beta^p = 1$, and hence $\exp(\gamma_2(G)) = p$, which is not possible. Thus $\beta^p \neq 1$ and the proof is complete. □

Proposition 4.2.1 *Let G be a group of order p^7, $p \geq 5$, having nilpotency class 5 such that $\gamma_2(G)$ is a 4-generated subgroup of order p^5 and exponent p^2. Then the following statements hold:*

(i) $|\gamma_5(G)| = p$,

(ii) $|\mathrm{Z}(G/\gamma_5(G))| = p^2$ *and* $|\mathrm{Z}_2(G)| = p^3$,

(iii) $\mathrm{K}(G) \neq \gamma_2(G)$,

(iv) *The commutator length of G is* 2.

Proof. We start by noticing that $|\gamma_5(G)| \leq p^2$. For the first assertion, contrarily assume that the order of $\gamma_5(G)$ is p^2. Thus $\gamma_5(G) = \mathrm{Z}(G)$ and $\gamma_i(G)/\gamma_{i+1}(G)$ is of order p for every $i \in \{2, 3, 4\}$. By the given hypothesis we can assume that G is generated by 2 elements, say α_1, α_2. Recall that $\beta = [\alpha_1, \alpha_2]$. Since $d(\gamma_2(G)) = 4$, it follows that $|\Phi(\gamma_2(G))| = p$, which further implies that $\Phi(\gamma_2(G)) \leq \gamma_5(G)$. Let H be a complement of $\Phi(\gamma_2(G))$ in $\gamma_5(G)$. Then the quotient group $\bar{G} := G/H$ is a p-group of maximal class and order p^6. By Lemma 4.2.1 we get $\beta^p \neq 1$; hence $\exp(\gamma_2(\bar{G})) = p^2$, which is not possible by Theorem 1.3.5. Hence $\gamma_5(G)$ cannot be of order p^2, which estalishes assertion (i).

Now we prove assertion (ii). By assertion (i) we have $|\gamma_5(G)| = p$. It then follows from [2, Theorem 2.12] that $|\gamma_4(G)/\gamma_5(G)| = p$, and therefore $|\gamma_3(G)/\gamma_4(G)| = p^2$. If $|\mathrm{Z}(G)| = p^2$, then obviously $|\mathrm{Z}_2(G)| = p^3$ and, since $\gamma_4(G)/\gamma_5(G) \leq \mathrm{Z}(G/\gamma_5(G))$, it follows that $|\mathrm{Z}(G/\gamma_5(G))| = p^2$. So assume that $\mathrm{Z}(G) = \gamma_5(G)$. Obviously $|\mathrm{Z}_2(G)/\mathrm{Z}(G)| \leq p^2$. Again by Lemma 4.2.1 we get $\exp(\gamma_3(G)) = p$, and hence a regular computation shows that

$$[\alpha_1^p, \alpha_2] = [\alpha_1, \alpha_2]^p = [\alpha_1, \alpha_2^p].$$

We claim that both $\alpha_1^p,\ \alpha_2^p \notin \gamma_5(G)$. Otherwise, if $\alpha_1^p \in \gamma_5(G)$, then $[\alpha_1^p, \alpha_2] = \beta^p = 1$; not true. Hence $\alpha_1^p \notin \gamma_5(G)$, and using symmetry for α_2, we get $\alpha_2 \notin \gamma_5(G)$. If both $\alpha_1^p, \alpha_2^p \in \gamma_4(G)$, then, $\gamma_4(G)/\gamma_5(G)$ being of order p, $\alpha_1^p = (\alpha_2^p)^r$ modulo $\gamma_5(G)$ for some $r \in \mathbb{F}_p^*$, which implies that both α_1^p and α_2^p are central; not possible as just shown. Hence at least one of α_1^p and α_2^p lies outside $\gamma_4(G)$. Since $[\alpha_1^p, \alpha_2] = [\alpha_1, \alpha_2]^p = \beta^p \in \mathrm{Z}(G)$, it follows that $\alpha_1^p \in \mathrm{Z}_2(G)$. Similarly $\alpha_2^p \in \mathrm{Z}_2(G)$. Hence $\langle \gamma_4(G), \alpha_1^p, \alpha_2^p \rangle \leq \mathrm{Z}_2(G)$, and therefore $|\mathrm{Z}_2(G)/\mathrm{Z}(G)| \geq p^2$, which proves assertion (ii).

Assertion (iii) is now clear from assertion (ii), Lemma 3.3.1 and Lemma 1.3.5.

For assertion (iv) we consider two different cases, namely, $\gamma_2(G)$ is abelian or not. If $\gamma_2(G)$ is non-abelian, then notice that both $\mathrm{C}_G(\beta_1)$ and $\mathrm{C}_G(\beta_2)$ can not be maximal subgroups of G. Otherwise, $\gamma_2(G)$ would be abelian. Without loss of generality we can assume that $\mathrm{C}_G(\beta_1)$ is not maximal. Hence $[\beta_1, G] = \gamma_4(G) \subseteq \mathrm{K}(G)$. Since $\mathrm{K}(G/\gamma_4(G)) = \gamma_2(G/\gamma_4(G))$ from Theorem 1.1.6, the assertion follows from Lemma 1.3.6 and assertion (iii). Now assume that $\gamma_2(G)$ is abelian. Then it is not difficult to see that $[\alpha_i, \gamma_2(G)]$ are normal subgroups of G for $i = 1, 2$. Also, at least one of these subgroups is of order at least p^2. Let H be one with this property. Then, $|G/H|$ being at most p^5, it follows from Theorem 1.1.6 that $\mathrm{K}(G/H) = \gamma_2(G/H)$. The proof is now complete by Lemma 1.3.6 and assertion (iii). ☐

Lemma 4.2.2 *Let G be a group of order p^7, $p \geq 5$, such that $\gamma_2(G)$ is a 4-generated abelian subgroup of order p^5. Then the following statements hold:*

(i) The nilpotency class of G is at least 5,

(ii) If $p \geq 7$, then the nilpotency class of G is exactly 5.

Proof. By the given hypothesis we can assume that G is generated by 2 elements, say α_1, α_2. Hence it is clear that the nilpotency class of G can neither be 2 nor 3. So let the nilpotency class of G be 4. Then, $\gamma_2(G)$ being abelian, its exponent is p^2. As we know $\gamma_2(G)/\gamma_3(G) = \langle \beta\gamma_3(G)\rangle$. By Lemma 4.2.1, the order of β in G is p^2, $\exp(\gamma_3(G)) = p$ and $\Phi(\gamma_2(G)) = \langle \beta^p \rangle \leq \mathrm{Z}(G)$ is of order p. Then $p \leq |\gamma_3(G)/\gamma_4(G)| \leq p^2$; hence $p^3 \geq |\gamma_4(G)| \geq p^2$. First assume that $|\gamma_4(G)| = p^3$. Let K be a complement of $\Phi(\gamma_2(G))$ in $\gamma_4(G)$. Then $|K| = p^2$ and, hence the quotient group $\bar{G} := G/K$ is a p-group of order p^5 having the maximal class. Notice that the exponent of $\gamma_2(\bar{G})$ is p^2, which is not possible by Theorem 1.3.5.

Now we assume that $|\gamma_4(G)| = p^2$. If $|\,\mathrm{Z}(G)| = p^3$, then $u := \beta_1^r \beta_2^s \in \mathrm{Z}(G)$

for some $r, s \in \mathbb{F}_p$ not simultaneously zero. If $\beta^p \in \gamma_4(G)$, then, considering H to be a complement of $\langle \beta^p \rangle$ in $\gamma_4(G)$, it follows that $G/\langle H, u\rangle$ is a p-group of maximal class of order p^5 such that the exponent of its commutator subgroup is p^2, which is not possible by Theorem 1.3.5. If $\beta^p \notin \gamma_4(G)$, then we choose an element $v \in \gamma_3(G) - \gamma_4(G)$ such that $H := \langle \gamma_4(G), v\rangle$ is a complement of $\langle u \rangle$ in $\gamma_3(G)$. Now the quotient group G/H is a p-group of maximal class of order p^4 such that the exponent of its commutator subgroup is p^2, which is again not possible by Theorem 1.3.5.

Finally assume that $|Z(G)| = p^2$, that is, $\gamma_4(G) = Z(G)$. We claim that $\alpha_i^p \in \gamma_3(G) - \gamma_4(G)$ for $i = 1, 2$. Contrarily first assume that $\alpha_1^p \in \gamma_2(G) - \gamma_3(G)$. Then $\alpha_1^p = \beta^t g$ for some $t \in \mathbb{F}_p^*$ and $g \in \gamma_3(G)$. Thus,

$$1 = [\alpha_1^p, \alpha_1] = [\beta^t g, \alpha_1] = [\beta^t, \alpha_1][g, \alpha_1] = \beta_1^t [g, \alpha_1],$$

which implies that $\beta_1 \in \gamma_4(G)$; not possible. Now assume that $\alpha_1^p \in \gamma_4(G)$. Then, since $\exp(\gamma_3(G)) = p$ and $p \geq 5$, we obviously get

$$1 = [\alpha_2, {\alpha_1}^p] = [\alpha_2, \alpha_1]^p = \beta^{-p},$$

which is not true. The case for α_2 goes by symmetry, and the claim is settled. If ${\alpha_2}^p = (\alpha_1^p)^r$ for some $r \in \mathbb{F}_p^*$, then

$$\beta^p = [\alpha_1, \alpha_2^p] = [\alpha_1, \alpha_1^{pr}] = 1,$$

which is again not true. Hence α_1^p and α_2^p are both non-trivial and independent.

It is now clear that $\gamma_4(G) = \langle [\alpha_1^p, \alpha_2] \rangle \times \langle [\alpha_1, \alpha_2^p] \rangle$. If $\beta^p \in \langle [\alpha_1^p, \alpha_2] \rangle$, then consider $\bar{G} := G/\langle \alpha_2^p, [\alpha_2^p, \alpha_1] \rangle$. Otherwise consider $\bar{G} := G/\langle \alpha_1^p, [\alpha_1^p, \alpha_2] \rangle$. In both the cases $\bar{G}$ is a p-group of maximal class of order p^5 such that the exponent of its commutator subgroup is p^2, which is again not possible by Theorem 1.3.5. Hence the nilpotency class of G is at least 5. This completes the proof of assertion (i).

Since the exponent of $\gamma_2(G)$ is p^2, thus the assertion (ii) follows from assertion (i) and Theorem 1.3.5, and the proof is complete. □

Proposition 4.2.2 *Let G be a group of order p^7, $p \geq 5$, with nilpotency class 5 and $\gamma_2(G)$ elementary abelian of order p^5. Then the following statements hold:*

(i) $|\gamma_5(G)| = p$,

(ii) $|\operatorname{Z}(G/\gamma_5(G))| = p^2$ *and* $|\operatorname{Z}_2(G)| = p^3$,

(iii) $\operatorname{K}(G) \neq \gamma_2(G)$,

(iv) Commutator length of G is 2.

Proof. By the given hypothesis G is minimally generated by 2 elements, say α_1, α_2, and $|\gamma_5(G)| \leq p^2$. Contrarily assume that $|\gamma_5(G)| = p^2$. Let β, β_i, η_{ij} and ξ_{ijk} be as defined in the introduction (of this chapter). Without loss of generality we can assume that $\gamma_3(G) = \langle \beta_1, \gamma_4(G) \rangle$ and $\beta_2 \in \gamma_4(G)$. Thus $\eta_{21}, \eta_{22} \in \gamma_5(G)$. Now Hall-Witt identity

$$[\beta, \alpha_1^{-1}, \alpha_2]^{\alpha_1} [\alpha_1, \alpha_2^{-1}, \beta]^{\alpha_2} [\alpha_2, \beta^{-1}, \alpha_1]^{\beta} = 1,$$

gives $\eta_{12} = \eta_{21}\xi_{112}\xi_{121}^{-1}$. Hence $\eta_{12} \in \gamma_5(G)$, and therefore $\gamma_4(G) = \langle \eta_{11}, \gamma_5(G) \rangle$. It is now clear that $\gamma_5(G) = \langle \xi_{111}, \xi_{112} \rangle$. Again Hall-Witt identity

$$[\beta_1, {\alpha_2}^{-1}, \alpha_1]^{\alpha_2} [\alpha_2, {\alpha_1}^{-1}, \beta_1]^{\alpha_1} [\alpha_1, {\beta_1}^{-1}, \alpha_2]^{\beta_1} = 1,$$

gives $\xi_{112} = \xi_{121}$. Since $\xi_{121} = 1$, it follows that $\gamma_5(G) = \langle \xi_{111} \rangle$, which is absurd. Hence $|\gamma_5(G)| = p$, and assertion (i) holds.

It now follows from [2, Theorem 2.12] that $|\gamma_4(G)/\gamma_5(G)| = p$, and therefore $|\gamma_3(G)/\gamma_4(G)| = p^2$. By the given hypothesis, it follows that $|\operatorname{Z}(G)| \leq p^2$. If

$|\operatorname{Z}(G)| = p^2$, then $|\operatorname{Z}_2(G)| = p^3$ and $\operatorname{Z}(G/\gamma_5(G)) = (\gamma_4(G)/\gamma_5(G))(\operatorname{Z}(G)/\gamma_5(G))$ is of order p^2, and assertion (ii) holds in this case. So assume that $|\operatorname{Z}(G)| = p$. Since $\gamma_2(G)$ is elementary abelian, for any $x, y \in G$, we have

$$[x, y^p] = [x, y]^p[x, y, y]^{\binom{p}{2}}[x, y, y, y]^{\binom{p}{3}}[x, y, y, y, y]^{\binom{p}{4}} = 1,$$

which gives $G^p \leq \operatorname{Z}(G)$. Thus $\bar{G} := G/\gamma_5(G)$ is of order p^6, exponent p and nilpotency class 4 with $\gamma_2(\bar{G})$ elementary abelian of order p^4. It then follows from [22] that $\bar{G}$ lies in one of the isoclinism families $\Phi(23), \Phi(40)$ and $\Phi(41)$. We claim that $\bar{G}$ lies in $\Phi(23)$.

If $\bar{G} \in \Phi(40)$, then, since $\exp(\bar{G}) = p$ and isoclinic groups have same commutator structure, we may assume that

$$\begin{aligned}\bar{G} \;&=\; \langle \bar{\alpha}_1, \bar{\alpha}_2, \bar{\beta}, \bar{\beta}_1, \bar{\beta}_2, \bar{\gamma} \mid [\bar{\alpha}_1, \bar{\alpha}_2] = \bar{\beta}, [\bar{\beta}, \bar{\alpha}_i] = \bar{\beta}_i, [\bar{\beta}_1, \bar{\alpha}_2] = [\bar{\beta}_2, \bar{\alpha}_1] = \bar{\gamma},\\ &\quad \bar{\alpha}_i{}^p = \bar{\beta}^p = \bar{\beta}_i{}^p = \bar{\gamma}^p = 1; i = 1, 2\rangle.\end{aligned}$$

Since $[\bar{\beta}_i, \bar{\alpha}_i] = 1_{\bar{G}}$, we get $[\beta_i, \alpha_i] \in \gamma_5(G)$ for $i = 1, 2$. Hence $\gamma_4(G) = \langle [\beta_1, \alpha_2], \gamma_5(G)\rangle$ and $[\beta_2, \alpha_1] = [\beta_1, \alpha_2]h$, for some $h \in \operatorname{Z}(G)$. By Hall-Witt identity

$$[\beta_1, \alpha_2{}^{-1}, \alpha_1]^{\alpha_2}[\alpha_2, \alpha_1{}^{-1}, \beta_1]^{\alpha_1}[\alpha_1, \beta_1{}^{-1}, \alpha_2]^{\beta_1} = 1,$$

we get $[\beta_1, \alpha_2, \alpha_1] = 1$. Again using Hall-Witt identity

$$[\beta_2, \alpha_1{}^{-1}, \alpha_2]^{\alpha_1}[\alpha_1, \alpha_2{}^{-1}, \beta_2]^{\alpha_2}[\alpha_2, \beta_2{}^{-1}, \alpha_1]^{\beta_2} = 1,$$

we get $[\beta_2, \alpha_1, \alpha_2] = 1$. Hence $G = \operatorname{C}_G(\gamma_4(G))$, which is absurd.

If $\bar{G} \in \Phi(41)$, then using the presentation

$$\begin{aligned}\bar{G} \;&=\; \langle \bar{\alpha}_1, \bar{\alpha}_2, \bar{\beta}, \bar{\beta}_1, \bar{\beta}_2, \bar{\gamma} \mid [\bar{\alpha}_1, \bar{\alpha}_2] = \bar{\beta}, [\bar{\beta}, \bar{\alpha}_i] = \bar{\beta}_i, [\bar{\alpha}_1, \bar{\beta}_1]^{-\nu} = [\bar{\alpha}_2, \bar{\beta}_2] = \bar{\gamma}^{-\nu},\\ &\quad \bar{\alpha}_i^p = \bar{\beta}^p = \bar{\beta}_i^p = \bar{\gamma}^p = 1; i = 1, 2\rangle,\end{aligned}$$

one gets the same absurd conclusion as in the preceding case, where ν denotes the quadratic non-residue mod p. Hence $\bar{G} \in \Phi(23)$ and therefore $|Z(\bar{G})| = p^2$ by [22], which proves assertion (ii).

Assertion (iii) now follows from assertion (ii), Lemma 3.3.1 and Lemma 1.3.5. The proof of assertion (iv) is exactly the same as the proof of assertion (iv) of Proposition 4.2.1 for abelian $\gamma_2(G)$. The proof is complete. □

Proposition 4.2.3 *Let G be a group of order p^7, $p \geq 5$, having nilpotency class 5 such that $\gamma_2(G)$ is non-abelian of order p^5 and exponent p. Then $\mathrm{K}(G) \neq \gamma_2(G)$ if and only if $|\gamma_5(G)| = p$ and $|\mathrm{Z}(G/\gamma_5(G))| = p^2$. Moreover, if $\mathrm{K}(G) \neq \gamma_2(G)$, then the commutator length of G is 2.*

Proof. By the given hypothesis it follows that $|\gamma_5(G)| \leq |\mathrm{Z}(G)| \leq p^2$ and the commutator subgroup of $\gamma_2(G)$ is contained in $\gamma_5(G)$. First assume that $|\gamma_5(G)| = p$ and $|\mathrm{Z}(G/\gamma_5(G))| = p^3$. Thus $\mathrm{K}(G) \neq \gamma_2(G)$ by Lemma 3.3.1 and Lemma 1.3.5. Conversely, assume that either $|\gamma_5(G)| = p^2$ or $|\gamma_5(G)| = |\mathrm{Z}(G)| = p$ and $|\mathrm{Z}(G/\gamma_5(G))| = p^2$. Let $G = \langle \alpha_1, \alpha_2 \rangle$ and β, β_i, η_{ij} and ξ_{ijk}, where $i, j, k \in \{1, 2\}$, be as defined in the introduction (of this chapter).

Let us first assume that $|\gamma_5(G)| = |\mathrm{Z}(G)| = p^2$. Then $|\gamma_i(G)/\gamma_{i+1}(G)| = p$ for $2 \leq i \leq 4$. Now without loss of generality we can assume that $\beta_2 \in \gamma_4(G)$ and $\gamma_3(G) = \langle \beta_1, \gamma_4(G) \rangle$. Therefore $\eta_{21}, \eta_{22} \in \gamma_5(G)$. But by Hall-Witt identity

$$[\beta, \alpha_1^{-1}, \alpha_2]^{\alpha_1} [\alpha_1, \alpha_2^{-1}, \beta]^{\alpha_2} [\alpha_2, \beta^{-1}, \alpha_1]^{\beta} = 1,$$

we get $\eta_{12} = \xi_{112} {\xi_{121}}^{-1} \eta_{21}$; thus $\eta_{12} \in \gamma_5(G)$. Hence $\gamma_4(G) = \langle \eta_{11} \rangle \pmod{\gamma_5(G)}$ and therefore $\gamma_5(G) = \langle \xi_{111}, \xi_{112} \rangle$. Again the Hall-Witt identity

$$[\beta_1, {\alpha_2}^{-1}, \alpha_1]^{\alpha_2} [\alpha_2, {\alpha_1}^{-1}, \beta_1]^{\alpha_1} [\alpha_1, {\beta_1}^{-1}, \alpha_2]^{\beta_1} = 1,$$

gives $[\beta_1, \beta] = \xi_{112}$. Let $\beta_2 = {\eta_{11}}^r {\xi_{111}}^s {\xi_{112}}^t$ for some $r, s, t \in \mathbb{F}_p$, and $\bar{G} := G/H$ where $H = \langle \xi_{112} \rangle$. Then $\bar{G}$ is a p-group of maximal class of order p^6 with $\gamma_2(\bar{G})$

elementary abelian of order p^4. Notice that $\bar{\alpha}_1$ is a uniform element of $\bar{G}$. It is now easy to see that

$$\gamma_2(\bar{G}) = \{[\bar{\alpha}_2^a\bar{\beta}^b\bar{\beta}_1^c\bar{\eta}_{11}^d, \bar{\alpha}_1] \mid a, b, c, d \in \mathbb{F}_p\} = \{[\bar{\alpha}_2^a\bar{\beta}^b\bar{\beta}_1^c\bar{\eta}_{11}^d, \bar{G}] \mid a, b, c, d \in \mathbb{F}_p\}.$$

Since $\xi_{112} = [\beta_1, \beta] = [\eta_{11}, \alpha_2]$, it also follows that

$$H \subseteq \bigcap_{a,b,c,d} [\alpha_2^a\beta^b\beta_1^c\eta_{11}^d, G],$$

where $a, b, c, d \in \mathbb{F}_p$ not all simultaneously zero. Hence by Lemma 1.3.7 we have $\mathrm{K}(G) = \gamma_2(G)$.

Now assume that $|\gamma_5(G)| = |\mathrm{Z}(G)| = p$ and $|\mathrm{Z}(G/\gamma_5(G))| = p$. Let $H := Z(G)$ $(= \gamma_5(G))$ and $L := G/H$. Then L is of order p^6 and nilpotency class 4 such that $\gamma_2(L)$ is elementary abelian of order p^4 and $|\mathrm{Z}(L)| = p$. Hence, by [22], L lies in the isoclinism family $\Phi(40)$ or $\Phi(41)$. By Lemma 3.3.1 we know that $\mathrm{K}(L) = \gamma_2(L)$. We provide a detailed explanation when L lies in $\Phi(40)$. The other case goes on the same lines. Notice that any two isoclinic groups admit the same commutator relations. So, if L lies in $\Phi(40)$, then by [22] L has the following commutator relations:

$$R := \{[\bar{\alpha}_1, \bar{\alpha}_2] = \bar{\beta}, [\bar{\beta}, \bar{\alpha}_i] = \bar{\beta}_i, [\bar{\beta}_1, \bar{\alpha}_2] = [\bar{\beta}_2, \bar{\alpha}_1] = \bar{\eta}\},$$

where $\gamma_4(G)/\gamma_5(G) = \langle\eta\gamma_5(G)\rangle$. It is not difficult to see that $\bar{\alpha}_i^p = 1$ for $i = 1, 2$.

We claim that $\gamma_2(L) = \{[\bar{\alpha}_1^\epsilon\bar{\beta}^{a_1}\bar{\beta}_1^{a_2}\bar{\beta}_2^{a_3}, L] \mid a_1, a_2, a_3 \in \mathbb{F}_p, \epsilon \in \{0, 1\}\}$, where a_1 and a_2 are not simultaneously zero. To establish this claim, we are going to show that for given $u, v, w, x \in \mathbb{F}_p$, there exist $\epsilon, a_i, b_j \in \mathbb{F}_p$, where $1 \leq i \leq 3$, $1 \leq j \leq 5$ and a_1, a_2 not simultaneously zero, such that

$$[\bar{\alpha}_1^\epsilon\bar{\beta}^{a_1}\bar{\beta}_1^{a_2}\bar{\beta}_2^{a_3}, \bar{\alpha}_1^{b_1}\bar{\alpha}_2^{b_2}\bar{\beta}^{b_3}\bar{\beta}_1^{b_4}\bar{\beta}_2^{b_5}] = \bar{\beta}^u\bar{\beta}_1^v\bar{\beta}_2^w\bar{\eta}^x.$$

After expanding the left hand side and comparing the powers on both sides, we get

$$\begin{aligned} \epsilon b_2 &= u, \\ a_1 b_1 - \epsilon b_3 &= v, \\ a_1 b_2 + \epsilon \binom{b_2}{2} &= w, \\ a_1 b_1 b_2 + a_2 b_2 + a_3 b_1 - \epsilon b_5 &= x. \end{aligned}$$

If $u \neq 0$, then taking $\epsilon = 1$, $a_2 \in \mathbb{F}_p^*$ and $b_1 = 0$, we get $b_2 = u$, $b_3 = -v$, $a_1 = (w - \binom{u}{2})u^{-1}$, and $b_5 = ua_2 - x$. The remaining a_i's and b_i's can take arbitrary values in $\mathbb{F}_p$. Now let $u = 0$. Then taking $\epsilon = 0$, the above system of equations reduces to

$$a_1 b_1 = v, \tag{4.2.1}$$

$$a_1 b_2 = w, \tag{4.2.2}$$

$$a_1 b_1 b_2 + a_2 b_2 + a_3 b_1 = x. \tag{4.2.3}$$

If $v = w = 0$, then taking $a_1 = a_3 = 0$ and $a_2 \neq 0$, we get $b_2 = xa_2^{-1}$. If $v \neq 0$ and $w \neq 0$, then we can choose $b_1, b_2 \in \mathbb{F}_p^*$ such that $a_1 = vb_1^{-1} = wb_2^{-1}$. Now taking $a_3 = 0$ in (4.2.3), we get $a_2 = b_2^{-1}(x - a_1 b_1 b_2)$. If $v = 0$ and $w \neq 0$, then by equations (4.2.2) and (4.2.1), respectively, we get $a_1 = wb_2^{-1}$ and $b_1 = 0$, and by (4.2.3) we get $a_2 = xb_2^{-1}$. If $w = 0$ and $v \neq 0$, then by equations (4.2.1) and (4.2.2), respectively, we get $a_1 = vb_1^{-1}$ and $b_2 = 0$, and by (4.2.3) we get $a_3 = xb_1^{-1}$. Thus in all the cases we get the required ϵ, a_i's and b_i's, and therefore it follows that

$$\gamma_2(L) = \bigcup_{\epsilon, a_1, a_2, a_3} [\alpha_1^{\epsilon} \beta^{a_1} \beta_1^{a_2} \beta_2^{a_3}, L].$$

where a_1 and a_2 are not simultaneously zero.

As $\gamma_2(G)$ is non-abelian, we can assume that $[\beta, \beta_1] \neq 1$ and $[\beta, \beta_2] = 1$. For, if both are non-trivial, then $[\beta, \beta_1] = [\beta, \beta_2]^t$ for some $t \in \mathbb{F}_p^*$. Then modifying β_2 by $\beta_1\beta_2^{-t}$, we get $[\beta, \beta_2] = 1$. If $[\beta, \beta_1] = 1$, then interchanging the role of α_1 and α_2 works. By Hall-Witt identity

$$[\beta_1, {\alpha_1}^{-1}, \alpha_2]^{\alpha_1}[\alpha_1, {\alpha_2}^{-1}, \beta_1]^{\alpha_2}[\alpha_2, {\beta_1}^{-1}, \alpha_1]^{\beta_1} = 1,$$

we get $\xi_{121} = [\beta, \beta_1]$. Again by Hall-Witt identity

$$[\beta_2, {\alpha_1}^{-1}, \alpha_2]^{\alpha_1}[\alpha_1, {\alpha_2}^{-1}, \beta_2]^{\alpha_2}[\alpha_2, {\beta_2}^{-1}, \alpha_1]^{\beta_2} = 1,$$

we get $\xi_{212} = 1$. Thus $\alpha_2 \in C_G(\gamma_4(G))$. Therefore we get $\gamma_5(G) = \langle \xi_{121} \rangle$. Now, since $\gamma_5(G) = \langle [\alpha_1, \gamma_4(G)] \rangle = \langle [\beta, \beta_1] \rangle$, it follows that

$$\gamma_5(G) \subseteq \bigcap_{\epsilon, a_1, a_2, a_3} [\alpha_1^{\epsilon}\beta^{a_1}\beta_1^{a_2}\beta_2^{a_3}, G],$$

where a_1 and a_2 are not both zero. Hence, again by Lemma 1.3.7, $\mathrm{K}(G) = \gamma_2(G)$.

If L lies in $\Phi(41)$, then, on the same lines, one can show that

$$\gamma_2(G) = \{[\alpha_2^{\epsilon}\beta^{a_1}\beta_1^{a_2}\beta_2^{a_3}, G] \mid a_1, a_2, a_3 \in \mathbb{F}_p, \epsilon \in \{0, 1\}\}.$$

That the commutator length of G is 2 follows the same way as proved in Proposition 4.2.1. The proof is now complete. □

4.3 Groups of nilpotency class 4

Let G be a group of nilpotency class 4 and order p^7 with $\gamma_2(G)$ of order p^5 and minimally generated by at least 4 elements. By Lemma 1.3.4 we know that $\gamma_2(G)$ is abelian. Since the nilpotency class of G is 4, it follows from the proof of Lemma 4.2.2 that $\exp(\gamma_2(G))$ for such groups G can not be p^2. So we are left with only one possibility, which is elementary abelian $\gamma_2(G)$, that we will deal in this section.

Lemma 4.3.1 *Let G be a group of order p^7 and nilpotency class 4 with $\gamma_2(G)$ elementary abelian of order p^5. Then $\mathrm{Z}(G) = \gamma_4(G)$ is of order p^2.*

Proof. We can assume $G = \langle \alpha_1, \alpha_2 \rangle$. Let β, β_i and η_{ij} are as defined in the introduction (of this chapter). Then $\gamma_2(G)/\gamma_3(G) = \langle \beta\gamma_3(G) \rangle$. Obviously $|\gamma_4(G)| \leq p^3$. If $|\gamma_4(G)| = p^3$, then $\gamma_3(G) = \langle \gamma, \gamma_4(G) \rangle$ for any $\gamma \in \gamma_3(G) - \gamma_4(G)$. This implies that the order of $\gamma_3(G)/\gamma_4(G)$ will at least be p^2. Since $\gamma_3(G)/\gamma_4(G)$ is generated by at most 2 elements, it follows that its order can be at most p^2. Thus the order of $\gamma_4(G)$ is precisely p^2. Using Hall-Witt identity

$$[\beta, \alpha_1^{-1}, \alpha_2]^{\alpha_1}[\alpha_1, \alpha_2^{-1}, \beta]^{\alpha_2}[\alpha_2, \beta^{-1}, \alpha_1]^{\beta} = 1,$$

we have $\eta_{12} = \eta_{21}$.

Contrarily assume that $|\mathrm{Z}(G)| = p^3$. Since $|\gamma_4(G)| = p^2$, we have $Z(G) = \langle \beta_1^i\beta_2^j, \gamma_4(G) \rangle$ for some $i, j \in \mathbb{F}_p$ not both zero. If $i = 0$, then $\eta_{22} = \eta_{21} = 1$, which implies that $\gamma_4(G) = \langle \eta_{11} \rangle$; not possible. So let $i \in \mathbb{F}_p^*$. As $1 = [\beta_1^i\beta_2^j, \alpha_1] = \eta_{11}^i\eta_{21}^j$ and $1 = [\beta_1^i\beta_2^j, \alpha_2] = \eta_{12}^i\eta_{22}^j$, we get $\eta_{11} = {\eta_{12}}^{-ji^{-1}} = {\eta_{22}}^{j^2i^{-2}}$, which implies that the order $\gamma_4(G)$ is at most p; not possible. The proof is now complete. □

Let G satisfy the hypotheses of Lemma 4.3.1. Then $\mathrm{Z}(G) = \gamma_4(G)$ is of order p^2. Assume that $\gamma_4(G) = \langle \eta_{11}, \eta_{12} \rangle$ and $\eta_{22} = \eta_{11}^m\eta_{12}^n$, where $m, n \in \mathbb{F}_p$ not both zero. With this setting we have

Lemma 4.3.2 *Let G, m and n be as in the preceding paragraph. Then G admits a subgroup $H \leq Z(G)$ of order p such that $|Z(G/H)| = p^2$ if and only if the equation $m\lambda^2 + n\lambda\mu - \mu^2 = 0$ has a solution $\lambda = \lambda_0$ $(\neq 0)$ and $\mu = \mu_0$ in $\mathbb{F}_p$.*

Proof. First assume that G admits a subgroup $H \leq Z(G)$ of order p such that $|Z(G/H)| = p^2$. Obviously $H := \langle \eta_{11}^a\eta_{12}^b \rangle$ for some $a, b \in \mathbb{F}_p$ not simultaneously zero. Then there exist $i, j \in \mathbb{F}_p$ not both zero such that $[\beta_1^i\beta_2^j, \alpha_k] \in H$ for $k = 1, 2$; meaning, there exist $\lambda, \mu \in \mathbb{F}_p$ such that

$$\eta_{11}^i\eta_{12}^j = (\eta_{11}^a\eta_{12}^b)^\lambda$$

and

$$\eta_{11}^{mj}\eta_{12}^{i+nj} = (\eta_{11}^a\eta_{12}^b)^\mu.$$

Obviously $\lambda \neq 0$. Comparing powers on both sides in these equations, we get

$$i - a\lambda = 0 \pmod p, \quad j - b\lambda = 0 \pmod p,$$
$$i + nj - b\mu = 0 \pmod p, \quad mj - a\mu = 0 \pmod p.$$

Solving these equations for i, j we further get

$$\lambda a + (n\lambda - \mu)b = 0 \pmod p,$$
$$-\mu a + m\lambda b = 0 \pmod p.$$

Hence, the system of equations

$$\lambda x + (n\lambda - \mu)y = 0 \pmod p,$$
$$-\mu x + m\lambda y = 0 \pmod p.$$

admits a non-trivial solution $x = a$ and $y = b$ in $\mathbb{F}_p$. But it is possible only when the determinant $m\lambda^2 + n\lambda\mu - \mu^2$ of the matrix of this system of equations is zero. Hence the equation $m\lambda^2 + n\lambda\mu - \mu^2 = 0$, with given coefficients m and n, admits a non-trivial solution $\lambda = \lambda_0 \in \mathbb{F}_p^*$ and $\mu = \mu_0$ in $\mathbb{F}_p$.

Conversely, assume that $m\lambda^2 + n\lambda\mu - \mu^2 = 0$ admits a solution $\lambda = \lambda_0\ (\neq 0)$

and $\mu = \mu_0$ in $\mathbb{F}_p$. Consider the matrix

$$M = \begin{bmatrix} \lambda_0 & n\lambda_0 - \mu_0 \\ -\mu_0 & m\lambda_0 \end{bmatrix}.$$

Since the determinant of M is zero modulo p, the system of equations $MA^t = \mathbf{0}$ admits a non-trivial solution, where A^t denotes the transpose of the matrix $A = [a, b]$ and $\mathbf{0}$ denotes the 2×1 zero-matrix with entries in $\mathbb{F}_p$. Let $a = a_0$ and $b = b_0$ be a non trivial solution of $MA^t = \mathbf{0}$. Thus we get the following equations:

$$\lambda_0 a_0 + (n\lambda_0 - \mu_0)b_0 = 0 \pmod{p},$$
$$-\mu_0 a_0 + m\lambda_0 b_0 = 0 \pmod{p}.$$

Let $H := \langle \eta_{11}^{a_0}\eta_{12}^{b_0} \rangle$ and $\bar{G} := G/H$. Obviously $[\bar{\beta_1}^{a_0}\bar{\beta_2}^{b_0}, \bar{\alpha_1}] = \bar{\eta}_{11}^{a_0}\bar{\eta}_{12}^{b_0} = 1_{\bar{G}}$. Also, using the preceding set of equations, we get

$$[\bar{\beta_1}^{a_0}\bar{\beta_2}^{b_0}, \bar{\alpha}_2] = \bar{\eta}_{21}^{a_0}\bar{\eta}_{22}^{b_0} = \bar{\eta}_{11}^{mb_0}\bar{\eta}_{12}^{a_0+nb_0} = \bar{\eta}_{11}^{a_0\mu_0\lambda_0^{-1}}\bar{\eta}_{12}^{b_0\mu_0\lambda_0^{-1}} = (\bar{\eta}_{11}^{a_0}\bar{\eta}_{12}^{b_0})^{\mu_0\lambda_0^{-1}} = 1_{\bar{G}}.$$

Hence $\bar{\beta_1}^{a_0}\bar{\beta_2}^{b_0} \in Z(\bar{G})$. It now easily follows that $|\mathrm{Z}(\bar{G})| = p^2$, which completes the proof. □

Proposition 4.3.1 *Let G be a group of order p^7 having nilpotency class 4 such that $\gamma_2(G)$ elementary abelian of order p^5. Then $\mathrm{K}(G) \neq \gamma_2(G)$ if and only if there exist a subgroup $H \leq Z(G)$ of order p such $|Z(G/H)| = p^2$. Moreover, the commutator length of G is at most 2.*

Proof. Let $H \leq Z(G)$ be a subgroup of order p such that $|Z(G/H)| = p^2$. Then it follows from Lemma 3.3.1 and Lemma 1.3.5 that $\mathrm{K}(G) \neq \gamma_2(G)$, which proves the 'if' part. We provide a contrapositive proof of the 'only if' statement. Let there do not exist any $H \leq Z(G)$ of order p such $|Z(G/H)| = p^2$. We assume $G = \langle \alpha_1, \alpha_2 \rangle$. Let β, β_i and η_{ij} be as defined in the introduction (of this chapter). Then $\gamma_2(G)/\gamma_3(G) = \langle \beta\gamma_3(G) \rangle$. By Lemma 4.3.1 we know that $\mathrm{Z}(G) = \gamma_4(G)$ is of order p^2; hence $\gamma_3(G)/\gamma_4(G) = \langle \beta_1\gamma_4(G), \beta_2\gamma_4(G) \rangle$ is of order p^2 too. Also recall from Lemma 4.3.1 that $\eta_{12} = \eta_{21}$. It now follows from our assumption that $\eta_{11}, \eta_{12}, \eta_{22}$ are all non-trivial elements of $\gamma_4(G)$. Indeed, for example, if $\eta_{11} = 1$, then taking $H = \langle \eta_{12} \rangle$ we see that $|\,\mathrm{Z}(G/H)| = p^2$, a case which we are not considering. Assume that $\gamma_4(G) = \langle \eta_{11}, \eta_{22} \rangle$. Hence $\eta_{12} = \eta_{11}^r\eta_{22}^s$, where $r, s \in \mathbb{F}_p$. If $r = 0$, then taking $H = \langle \eta_{22} \rangle$, we get $\mathrm{Z}(\bar{G}) = \left\langle \bar{\eta}_{11}, \bar{\beta}_2 \right\rangle$ is of order p^2; not possible. If $s = 0$, then taking $H = \langle \eta_{11} \rangle$, we get the same conclusion. So let $r, s \in \mathbb{F}_p^*$. Then we can take $\gamma_4(G) = \langle \eta_{11}, \eta_{12} \rangle$, and $\eta_{22} = \eta_{11}^m\eta_{12}^n$, where $m, n \in \mathbb{F}_p$. The same conclusion holds when we take $\gamma_4(G) = \langle \eta_{12}, \eta_{22} \rangle$. Thus we can always consider $\gamma_4(G) = \langle \eta_{11}, \eta_{12} \rangle$, and $\eta_{22} = \eta_{11}^m\eta_{12}^n$ for some $m, n \in \mathbb{F}_p$ not both zero.

Notice that G satisfies all hypotheses of Lemma 4.3.2. Hence, under our supposition, the equation $m\lambda^2 + n\lambda\mu - \mu^2 = 0$ can only have the trivial solution modulo p. But, by Lemma 1.3.10, it is possible if and only if the equation $\lambda^2 + n\lambda\mu - m\mu^2 = 0$ also has only the trivial solution modulo p. Then, obviously, $m \in \mathbb{F}_p^*$.

We are going to prove that for any given choice of elements $u, v, w, x, y \in \mathbb{F}_p$, there exist elements $a_i, b_i \in \mathbb{F}_p$, $1 \leq i \leq 5$, such that

$$[{\alpha_1}^{a_1}{\alpha_2}^{a_2}\beta^{a_3}{\beta_1}^{a_4}{\beta_2}^{a_5}, {\alpha_1}^{b_1}{\alpha_2}^{b_2}\beta^{b_3}{\beta_1}^{b_4}{\beta_2}^{b_5}] = \beta^u{\beta_1}^v{\beta_2}^w{\eta_{11}}^x{\eta_{12}}^y.$$

Solving both sides and comparing the powers in the preceding equation we get

$$\begin{aligned} a_1b_2 - a_2b_1 &= u, \\ a_3b_1 - a_1b_3 + \binom{a_1}{2}b_2 - a_2\binom{b_1}{2} &= v, \end{aligned}$$

$$\begin{aligned}
a_3b_2 - a_2b_3 + a_1\binom{b_2}{2} - \binom{a_2}{2}b_1 + a_1a_2b_2 - a_2b_1b_2 &= w,\\
a_4b_1 - a_1b_4 + a_3\binom{b_1}{2} - \binom{a_1}{2}b_3 + \binom{a_1}{3}b_2 - a_2\binom{b_1}{3} + mA &= x,\\
a_5b_1 + a_4b_2 + a_3b_1b_2 - a_1b_5 - a_2b_4 - a_1a_2b_3 + \binom{a_2}{2}\binom{b_1}{2}&\\
-\binom{a_1}{2}\binom{b_2}{2} + a_2b_2\binom{a_1}{2} - a_2b_2\binom{b_1}{2} + nA &= y,
\end{aligned}$$

where $A = a_5b_2 - a_2b_5 + a_3\binom{b_2}{2} - \binom{a_2}{2}b_3 + a_1\binom{b_2}{3} - \binom{a_2}{3}b_1 + a_1\binom{a_2}{2}b_2 - a_2b_1\binom{b_2}{2} + a_1a_2\binom{b_2}{2} - \binom{a_2}{2}b_1b_2$. We shall call this system of equations *the original system of equations* (OSE) throughout the proof.

Case (i). $u \neq 0$. Taking $a_2 = a_5 = b_1 = b_5 = 0$ and $a_1 = 1$ in OSE, we get

$$\begin{aligned}
b_2 = u, \quad b_3 = -v, \quad a_3b_2 + \binom{b_2}{2} &= w,\\
-b_4 + m(a_3\binom{b_2}{2} + \binom{b_2}{3}) &= x,\\
a_4b_2 + n(a_3\binom{b_2}{2} + \binom{b_2}{3}) &= y.
\end{aligned}$$

Hence we get

$$\begin{aligned}
b_2 = u, \quad b_3 = -v, \quad a_3 = u^{-1}(w - \binom{u}{2}),\\
b_4 = m(a_3\binom{u}{2} + \binom{u}{3}) - x, \quad a_4 = u^{-1}(y - n(a_3\binom{u}{2} + \binom{u}{3})),
\end{aligned}$$

which are the required values of a_i's and b_i's.

Case (ii). $u = 0$. Let us fix $a_1 = a_2 = 0$. Then OSE reduces to

$$a_3b_1 = v, \quad a_3b_2 = w, \tag{4.3.1}$$

$$a_4b_1 + a_3\binom{b_1}{2} + m(a_5b_2 + a_3\binom{b_2}{2}) = x, \tag{4.3.2}$$

$$a_5b_1 + a_4b_2 + a_3b_1b_2 + n(a_5b_2 + a_3\binom{b_2}{2}) = y. \tag{4.3.3}$$

We now consider the following four possible subcases:

Subcase (i). $v = w = 0$. Taking $a_3 = b_2 = 0$ and $b_1 = 1$ in (4.3.2) and (4.3.3), we get $a_4 = x$ and $a_5 = y$. Notice that b_j, $3 \leq j \leq 5$, can take arbitrary values in $\mathbb{F}_p$.

Subcase (ii). $v = 0$, $w \neq 0$. Taking $b_1 = 0$ and $b_2 = 1$ in (4.3.1), (4.3.2) and (4.3.3), we get $a_3 = w$, $a_5 = xm^{-1}$ and $a_1 = y - na_5$. Again b_j, $3 \leq j \leq 5$, can take arbitrary values in $\mathbb{F}_p$.

Subcase (iii). $v \neq 0$, $w = 0$. Taking $b_1 = 1$ and $b_2 = 0$ in (4.3.1), (4.3.2) and (4.3.3), we get $a_3 = v$, $a_4 = x$ and $a_5 = y$. Further again b_j, $3 \leq j \leq 5$, can take arbitrary values in $\mathbb{F}_p$.

Subcase (iv). $v \neq 0$, $w \neq 0$. For this choice, we can choose $b_1, b_2 \in \mathbb{F}_p^*$ such that $a_3 := v\, b_1^{-1} = w\, b_2^{-1}$. Rewriting (4.3.2) and (4.3.3), we get

$$b_1 a_4 + m b_2 a_5 = x - a_3 \binom{b_1}{2} - m a_3 \binom{b_2}{2},$$
$$b_2 a_1 + (b_1 + n b_2) a_5 = y - a_3 b_1 b_2 - n a_3 \binom{b_2}{2}.$$

Viewing a_4 and a_5 as variables, the determinant of the matrix of this system of equations is $D := b_1^2 + n b_1 b_2 - m b_2^2$. As explained above, in the second para of this proof, D can not be zero. Hence we can solve the preceding system of equations to obtain a_4 and a_5. Taking b_j, $3 \leq j \leq 5$, any arbitrary elements of $\mathbb{F}_p$, we got the required a_i's and b_i's, and the proof of the main assertion is complete.

As we know $\beta_1 = [\beta, \alpha_1]$ and $\beta_2 = [\beta, \alpha_2]$ are both non-trivial. Using the fact that $\eta_{12} = \eta_{21}$ and $|\gamma_4(G)| = p^2$, it follows that α_1 can not centralise β_1 and β_2 both. Then $H := [\alpha_1, \gamma_2(G)] \subseteq \mathrm{K}(G)$ is a normal subgroup of G having order at least p^2. For, $\gamma_2(G)$ being abelian, we have $[\alpha_1, uv] = [\alpha_1, u][\alpha_1, v]$ for all $u, v \in \gamma_2(G)$. Since $|G/H| \leq p^5$, it follows from Theorem 1.1.6 that

$\mathrm{K}(G/H) = \gamma_2(G/H)$. The proof is now complete by Lemma 1.3.6. □

4.4 Proof of Theorem 4.1.1

So far we have handled groups of order p^7 with $|\gamma_2(G)| = p^5$ and $d(\gamma_2(G)) \geq 4$, $p \geq 5$. The situation when $d(\gamma_2(G)) \leq 3$ has already been taken care of by I. de Las Heras Theorem 1.1.5. So we are only left with the case when $|\gamma_2(G)| = p^4$ and $d(\gamma_2(G)) = 4$, which we'll consider now.

Lemma 4.4.1 *Let G be a group of order p^7 with $|\gamma_2(G)| = p^4$ and $d(\gamma_2(G)) = 4$. Then $\mathrm{K}(G) \neq \gamma_2(G)$ if and only if one of the following holds:*

(i) The nilpotency class of G is 3, $\mathrm{Z}(G) \leq \gamma_2(G)$ and $|\mathrm{Z}(G)| = p^3$,

(ii) The nilpotency class of G is 4, $\mathrm{Z}(G) \not\leq \gamma_2(G)$ and $|\mathrm{Z}(G)| = p^3$.

Moreover, the commutator length of G is at most 2.

Proof. By the given hypothesis the exponent of $\gamma_2(G)$ is p. If $\mathrm{Z}(G) \leq \gamma_2(G)$, then the assertion follows from Theorem 3.1.1. So assume that $Z(G) \not\leq \gamma_2(G)$. Thus $|\mathrm{Z}(G)| \geq p^2$. Notice that, in this case, the nilpotency class of G is at least 4. Obviously, $d(G)$ is either 2 or 3. If $d(G) = 2$, then there exists a minimal generating set $\{\alpha_1, \alpha_2\}$ such that $\alpha_2^p \in \mathrm{Z}(G) - \gamma_2(G)$, but $\alpha_2^{p^2} \in \gamma_2(G)$. Then, by Lemma 1.2.1, there exists a 2-generated group M of order p^6 such that M and G are isoclinic and $\mathrm{Z}(M) \leq \gamma_2(M)$. Also $|\mathrm{Z}(G)| = p|\mathrm{Z}(M)|$. It now follows from Theorem 3.1.1 that $\mathrm{K}(M) \neq \gamma_2(M)$ if and only if the nilpotency class of M is 4 and $\mathrm{Z}(M)$ is of order p^2. This, using Lemma 1.2.2, simply tells that $\mathrm{K}(G) \neq \gamma_2(G)$ if and only if the nilpotency class of G is 4 and $|\mathrm{Z}(G)| = p^3$.

We now assume that $d(G) = 3$. We can then choose a minimal generating set $\{\alpha_1, \alpha_2, \alpha_3\}$ for G such that $\alpha_3 \in \mathrm{Z}(G) - \gamma_2(G)$. By the given hypothesis $\alpha_3^p \in \gamma_2(G)$. Let $M := \langle \alpha_1, \alpha_2 \rangle$. Then the nilpotency class of M and G are equal, $\gamma_2(G) = \gamma_2(M)$, $|M| = p^6$, $\mathrm{Z}(M) \leq \gamma_2(M)$ and $|\mathrm{Z}(G)/\mathrm{Z}(M)| = p$. Notice that

M and G are isoclinic. Again invoking Theorem 3.1.1, $\mathrm{K}(M) \neq \gamma_2(M)$ if and only if the nilpotency class of M is 4 and $\mathrm{Z}(M)$ is of order p^2. One can now easily conclude that $\mathrm{K}(G) \neq \gamma_2(G)$ if and only if the nilpotency class of G is 4 and $|\,\mathrm{Z}(G)| = p^3$. That the commutator length of G is at most 2 follows from 3.3.1, which completes the proof. □

We are now ready to prove Theorem 4.1.1.

Proof of Theorem 4.1.1. If $d(\gamma_2(G)) \leq 3$, then $\mathrm{K}(G) = \gamma_2(G)$ by Theorem 1.1.5. Also when the nilpotency class of G is 6, then $\mathrm{K}(G) = \gamma_2(G)$ by Theorem 1.3.4. This proves assertion (1). So we only need to consider $d(\gamma_2(G)) \geq 4$ and the nilpotency class of G at most 5. If $|\gamma_2(G)| = p^4$, then assertion (2) follows from Lemma 4.4.1. The only case which remains is $|\gamma_2(G)| = p^5$. Notice that the nilpotency class of G is at least 4. We now go according to the nilpotency class of G. If the nilpotency class of G is 4, then $\gamma_2(G)$ is abelian by Lemma 1.3.4, and therefore it is elementary abelian by Lemma 4.2.2. Assertion (4) now follows from Proposition 4.3.1.

Next assume that the nilpotency class of G is 5. If $\gamma_2(G)$ is elementary abelian, then assertion (5) follows from Proposition 4.2.2. If it is non-abelian of exponent p, then assertion (6) follows from Proposition 4.2.3. Finally if the exponent of $\gamma_2(G)$ is p^2, then assertion (3) follows from Proposition 4.2.1. The proof is now complete. □

4.5 Examples

In this section we exhibit various examples of groups of order p^7 to show that no class of groups considered in Theorem 4.1.1 is void. These examples are constructed from the structural information of the groups obtained in this chapter, and have been verified for $p = 5, 7$ using GAP [4]. For notational convenience, we use long generating set instead of minimal one.

The following two groups satisfy the hypotheses of Proposition 4.2.1:

$$\begin{aligned} G \;=\; \Big\langle & \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7 \mid\; [\alpha_1, \alpha_2] = \alpha_3, [\alpha_3, \alpha_1] = \alpha_4, [\alpha_3, \alpha_2] = \alpha_5, \\ & [\alpha_4, \alpha_1] = \alpha_6, [\alpha_6, \alpha_1] = [\alpha_5, \alpha_2] = \alpha_7 = \alpha_3^p, \alpha_1^p = \alpha_5, \alpha_2^p = \alpha_6, \\ & {\alpha_i}^p = 1 \; (4 \le i \le 7) \Big\rangle. \end{aligned}$$

For this group G, $\gamma_2(G)$ is abelian of exponent p^2, $|\,\mathrm{Z}(G)| = p$ and $\mathrm{K}(G) \neq \gamma_2(G)$.

$$\begin{aligned} G \;=\; \Big\langle & \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7 \mid\; [\alpha_1, \alpha_2] = \alpha_3, [\alpha_3, \alpha_1] = \alpha_4, [\alpha_3, \alpha_2] = \alpha_5, \\ & [\alpha_4, \alpha_1] = \alpha_6, [\alpha_6, \alpha_2] = [\alpha_4, \alpha_3] = [\alpha_1, \alpha_5] = \alpha_7 = \alpha_3^p, \alpha_1^p = \alpha_6, \alpha_2^p = \alpha_5, \\ & {\alpha_i}^p = 1 \; (4 \le i \le 7) \Big\rangle. \end{aligned}$$

This is an example when $\gamma_2(G)$ is non-abelian of exponent p^2, $|\,\mathrm{Z}(G)| = p$ and $\mathrm{K}(G) \neq \gamma_2(G)$.

The next example satisfies the hypotheses of Proposition 4.2.2.

$$\begin{aligned} G \;=\; \Big\langle & \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7 \mid\; [\alpha_1, \alpha_2] = \alpha_3, [\alpha_3, \alpha_1] = \alpha_4, [\alpha_3, \alpha_2] = \alpha_5, \\ & [\alpha_4, \alpha_1] = \alpha_6, [\alpha_6, \alpha_1] = \alpha_7, {\alpha_i}^p = 1 \; (1 \le i \le 7) \Big\rangle. \end{aligned}$$

For this group G, $\gamma_2(G)$ is elementary abelian, $|\,\mathrm{Z}(G)| = p^2$ and $\mathrm{K}(G) \neq \gamma_2(G)$.

The following two groups satisfy the hypotheses of Proposition 4.2.3:

$$\begin{aligned} G \;=\; \Big\langle & \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7 \mid\; [\alpha_1, \alpha_2] = \alpha_3, [\alpha_3, \alpha_1] = \alpha_4, [\alpha_3, \alpha_2] = \alpha_5, \\ & [\alpha_4, \alpha_1] = \alpha_6, [\alpha_6, \alpha_2] = [\alpha_4, \alpha_3] = [\alpha_4, \alpha_2] = \alpha_7, {\alpha_i}^p = 1 \; (1 \le i \le 7) \Big\rangle. \end{aligned}$$

Notice that $\gamma_2(G)$ is non-abelian of exponent p, $|\,\mathrm{Z}(G)| = p^2$ and $\mathrm{K}(G) \neq \gamma_2(G)$ for this group.

$$G = \Big\langle \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7 \mid [\alpha_1, \alpha_2] = \alpha_3, [\alpha_3, \alpha_1] = \alpha_4, [\alpha_5, \alpha_1] = \alpha_6\alpha_7, [\alpha_3, \alpha_2] = \alpha_5, [\alpha_4, \alpha_2] = \alpha_6, [\alpha_6, \alpha_1] = [\alpha_3, \alpha_4] = \alpha_7, {\alpha_i}^p = 1 \ (1 \leq i \leq 7) \Big\rangle.$$

This is a group with $\gamma_2(G)$ non-abelian of exponent p, $|\,\mathrm{Z}(G)| = p$ and $\mathrm{K}(G) = \gamma_2(G)$.

The following two groups are of nilpotency class 4 and satisfy the hypotheses of Proposition 4.3.1:

$$G = \Big\langle \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7 \mid [\alpha_1, \alpha_2] = \alpha_3, [\alpha_3, \alpha_1] = \alpha_4, [\alpha_3, \alpha_2] = \alpha_5, [\alpha_4, \alpha_1] = \alpha_6, [\alpha_5, \alpha_2] = \alpha_7, {\alpha_i}^p = 1 \ (1 \leq i \leq 7) \Big\rangle.$$

For this group G, we have $\gamma_2(G)$ is elementary abelian, $|\,\mathrm{Z}(G)| = p^2$ and $\mathrm{K}(G) \neq \gamma_2(G)$.

$$G = \Big\langle \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7 \mid [\alpha_1, \alpha_2] = \alpha_3, [\alpha_3, \alpha_1] = \alpha_4, [\alpha_3, \alpha_2] = \alpha_5, [\alpha_5, \alpha_1] = [\alpha_4, \alpha_2] = \alpha_7, [\alpha_4, \alpha_1]^{\nu} = [\alpha_5, \alpha_2] = \alpha_6^{\nu}, {\alpha_i}^p = 1 \ (1 \leq i \leq 7) \Big\rangle,$$

where ν is a quadratic non-residue mod p. Notice that $\gamma_2(G)$ is abelian, $|\,\mathrm{Z}(G)| = p^2$ and $\mathrm{K}(G) = \gamma_2(G)$.

Finally we present two examples which satisfy the hypotheses of Lemma

4.4.1. These are as follows.

$$G = \Big\langle \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7 \mid [\alpha_1, \alpha_2] = \alpha_4, [\alpha_4, \alpha_1] = \alpha_5, [\alpha_4, \alpha_2] = \alpha_6,$$
$$[\alpha_6, \alpha_1] = [\alpha_5, \alpha_2] = \alpha_7 = \alpha_3^p, {\alpha_i}^p = 1 \ (1 \leq i \leq 7, i \neq 3)\Big\rangle.$$

Notice that $\gamma_2(G)$ is abelian, $|\,\mathrm{Z}(G)| = p^2$, the nilpotency class of G is 4 and $\mathrm{K}(G) = \gamma_2(G)$.

$$G = \Big\langle \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7 \mid [\alpha_1, \alpha_2] = \alpha_4, [\alpha_4, \alpha_1] = \alpha_5, [\alpha_4, \alpha_2] = \alpha_6,$$
$$[\alpha_5, \alpha_1] = \alpha_7 = \alpha_3^p, {\alpha_i}^p = 1 \ (1 \leq i \leq 7, i \neq 3)\Big\rangle.$$

For this group G, $\gamma_2(G)$ is abelian, $|\,\mathrm{Z}(G)| = p^3$, the nilpotency class of G is 4 and $\mathrm{K}(G) \neq \gamma_2(G)$.

Examples of the groups having nilpotency class 3 and satisfying the hypotheses of Lemma 4.4.1 are given in Chapter 3. One might use GAP for many more examples for adequate primes.

4.6 Statistical data

In this concluding section we present some stataistical data on groups of order p^7, $p = 2, 3, 5, 7$, using GAP [4]. Our motive is to compute the number of such groups G for each prime such that $\mathrm{K}(G) \neq \gamma_2(G)$ according to various parameters occured in relevant results in Chapter 3 and the present one.

There are in total 2328 non-isomorphic groups of order 2^7, which are classified in 115 isoclinism classes in [21]. It follows from [21] that all groups of order 2^7 (Theorem 4.1.3) in which $\mathrm{K}(G) \neq \gamma_2(G)$, fall in a single isoclinism class. All such groups, total 52 in number upto isomorphism, lie in the isoclinism class 36 of [21, Table 1].

It follows from the results occured in thesis that $cl(G) = 1$ or 2, when G is of order p^7. In all the tables that follow, the second last and the last columns represent the number of groups G such that $cl(G) = 1$ and $cl(G) = 2$, respectively. For want of space, we only display these conditions without the phrase 'the number of groups'. In Table 4.1-4.5 we consider groups of order p^7, $p = 3, 5, 7$, which occured in this thesis.

$c(G)$	$d(\gamma_2(G))$	$\lvert\gamma_2(G)\rvert$	$\lvert Z(G)\rvert$	$\lvert Z_2(G)\rvert$	$cl(G) = 1$	$cl(G) = 2$
3	4	3^4	$3, 3^2$	3^4	2821	0
3	4	3^4	3^3	3^5	0	645
4	3	3^4	$3, 3^2$	$3^3, 3^4$	953	0
4	3	3^4	3^3	3^4	0	44
4	4	3^5	3^2	$3^3, 3^4$	0	15
5	3	3^5	3	3^2	21	0
5	3	3^5	$3, 3^2$	3^3	0	53

Table 4.1: Groups of order 3^7

In Table 4.2 and Table 4.4, $\gamma_2(G)$ is a 4-generated subgroup of order 5^4 and 7^4, respectively.

$c(G)$	$\lvert Z(G)\rvert$	$\lvert Z_2(G)\rvert$	$\lvert\gamma_c(G)\rvert$	$cl(G)=1$	$cl(G)=2$
3	$5, 5^2$	5^4	$5, 5^2$	15609	0
3	5^3	5^5	$5, 5^2$	0	2085
4	$5, 5^2$	$5^3, 5^4$	5	2630	0
4	5^3	5^4	5	0	67
5	$5, 5^2$	$5^2, 5^3$	5	215	0

Table 4.2: Groups of order 5^7

In Table 4.3 and Table 4.5, $\gamma_2(G)$ is of order 5^5 and 7^5, respectively.

$c(G)$	$d(\gamma_2(G))$	$\lvert Z(G)\rvert$	$\exp(\gamma_2(G))$	$\lvert Z_2(G)\rvert$	$\lvert\gamma_c(G)\rvert$	$cl(G)=1$	$cl(G)=2$
4	5	5^2	5	5^4	5^2	18	43
5	4	$5, 5^2$	5	5^3	$\neq 5$	280	0
5	4	$5, 5^2$	5	$\neq 5^3$	5	244	0
5	4	$5, 5^2$	5	5^3	5	0	101
5	4	$5, 5^2$	5^2	5^3	5	0	55
5	5	$5, 5^2$	5	5^3	5	0	98
6	4	5	5^3	5^3	5	99	0

Table 4.3: Groups of order 5^7

$c(G)$	$\lvert Z(G)\rvert$	$\lvert Z_2(G)\rvert$	$\lvert\gamma_c(G)\rvert$	$cl(G)=1$	$cl(G)=2$
3	$7, 7^2$	7^4	$7, 7^2$	61227	0
3	7^3	7^5	$7, 7^2$	0	5459
4	$7, 7^2$	$7^3, 7^4$	7	6806	0
4	7^3	7^4	7	0	93
5	$7, 7^2$	$7^2, 7^3$	7	257	0

Table 4.4: Groups of order 7^7

$c(G)$	$d(\gamma_2(G))$	$\lvert Z(G)\rvert$	$\exp(\gamma_2(G))$	$\lvert Z_2(G)\rvert$	$\lvert\gamma_c(G)\rvert$	$cl(G)=1$	$cl(G)=2$
4	5	7^2	7	7^4	7^2	88	165
5^*	4	$7, 7^2$	7	7^3	$\neq 7$	607	0
5^*	4	$7, 7^2$	7	$\neq 7^3$	7	514	0
5	4	$7, 7^2$	7	7^3	7	0	179
5	4	$7, 7^2$	7^2	7^3	7	0	121
5	5	$7, 7^2$	7	7^3	7	0	120
5	4, 5	7	7	7^2	7	198	0

Table 4.5: Groups of order 7^7

We now present the overall data on groups of order p^7, $(p = 3, 5, 7)$ according to the nilpotency class. Let G be a group of order p^7 having the nilpotency class 2. Then $\gamma_2(G)$ is of order at most p^3, and hence $cl(G) = 1$ by R. M. Guralnick [11] when $p \geq 5$. For the remaining prime $p = 2, 3$, it follows from GAP [4] that $cl(G) = 1$. Now if the nilpotency class of G is 6, then $cl(G) = 1$ by Theorem 1.3.4. Data on the remaining classes is presented in Tables 4.6 - 4.8.

$\|G\|$	No. of groups	$cl(G) = 1$	$cl(G) = 2$
3^7	6050	5405	645
5^7	22652	20567	2085
7^7	76238	70779	5459

Table 4.6: Groups of nilpotency class 3

$\|G\|$	No. of groups	$cl(G) = 1$	$cl(G) = 2$
3^7	1309	1250	59
5^7	3274	3164	110
7^7	7890	7632	258

Table 4.7: Groups of nilpotency class 4

$\|G\|$	No. of groups	$cl(G) = 1$	$cl(G) = 2$
3^7	173	120	53
5^7	1188	934	254
7^7	2097	1677	420

Table 4.8: Groups of nilpotency class 5

We conclude with the remark that a classification of groups of order p^7, p odd, is given in [35]. Unfortunately we could not use this classification in any sensible way. But it seems that one may use this knowledge alongwith our characterization to obtain a finer classification of groups G of order p^7 such that $cl(G) = 2$.

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] N. Blackburn, *On a special class of p-groups,* Acta Math. **100** (1958), 45-92.

[3] R. R. Dark and M. L. Newell, *On conditions for commutators to form a subgroup*, J. London Math. Soc. (2) **17** (1978), 251-262.

[4] The GAP Group, *Groups Algorithms and Programming,* version 4.11.1 (2021), http://www.gap-system.org.

[5] G. Fernández-Alcober and I. de las Heras, *Commutators in finite p-groups with 2-generator derived subgroup*, Israel J. Math. **232** (2019), 109-124.

[6] G. Fernández-Alcober, *An introduction to finite p-groups: Regular p-groups and groups of maximal class,* 16th school of Algebra, Part-I, Mat. Contemp **20** (2001), 155-226.

[7] W. B. Fite, *On metabelian groups*, Trans. Amer. Math. Soc. **3** (1902), 331-353.

[8] N. Gavioli, A. Mann, V. Monti, A. Previtali and C. M. Scoppola, *Groups of prime power order with many conjugacy classes.* J. Algebra **202** (1998), 129-141.

[9] D. Gorenstein, *Finite Groups*, AMS Chelsea Pub., Second Ed. (1980).

[10] R. M. Guralnick, *Expressing group elements as commutators*, Rocky mountain J. Math. **10** (1980), 651-654.

[11] R. M. Guralnick, *Commutators and commutator subgroups*, Adv. Math. **45** (1982), 319-330.

[12] R. M. Guralnick, *Generation of the lower central series*, Glasgow Math. J. **23** (1982), 15-20.

[13] R. M. Guralnick, *Generation of the lower central series II*, Glasgow Math. J. **25** (1984), 193-201.

[14] P. Hall, *The classification of prime power groups*, Journal für die reine und angewandte Mathematik **182** (1940), 130-141.

[15] I. de las Heras, *Commutators in finite p-groups with 3-generator derived subgroup*, J. Algebra **546** (2020), 201-217.

[16] I. de las Heras and M. Morigi, *Lower central words in finite p-groups*, Publicacions Matemàtiques **65** (2021), no. 1, 243-269.

[17] K. Honda, *On commutators in finite groups*, Comment. Math. Univ. St. Paul **2** (1953), 9-12.

[18] B. Huppert, *Endliche Gruppen I*, New York, Springer, 1967.

[19] I. M. Isaacs, *Commutators and the commutator subgroup*, Amer. Math. Monthly, **84(9)**, (1977), 720-722, .

[20] N. Ito, *A theorem on the alternating group A_n $(n = 5)$*, Math. Japonicae **2** (1951), 59-60.

[21] R. James, M. F. Newman, E. A. O'Brien *The groups of order* 128, J. Algebra **129**, (1990), 136-158.

[22] R. James, *The groups of order p^6 (p an odd prime)*, Math. Comp. **34** (1980), 613-637.

[23] L.-C. Kappe and R. F. Morse, *On commutators in p-groups*, J. Group Theory **8** (2005), 415-429.

[24] L.-C. Kappe and R. F. Morse, *On commutators in groups*, in Groups St. Andrews 2005. Vol. 2, London Mathematical Society Lecture Note Series, Vol. 340, Cambridge University Press, Cambridge, 2007, pp. 531-558.

[25] R. Kaushik and M. K. Yadav, *Commutators and commutator subgroup of finite p-groups*, J. Algebra **568** (2021), 314-348.

[26] R. Kaushik and M. K. Yadav, *Commutators in groups of order p^7*, arXiv:2106.07205, 17 Pages.

[27] M. W. Liebeck, E. A. O'Brien, A. Shalev and P. H. Tiep, *The Ore conjecture*, J. Eur. Math. Soc. (JEMS) **12** (2010), 939-1008.

[28] M. W. Liebeck, E. A. O'Brien, A. Shalev and P. H. Tiep, *Commutators in finite quasisimple groups*, Bull. Lond. Math. Soc. **43** (2011), 1079-1092.

[29] I. D. Macdonald, *On cyclic commuatator subgroups*, J. London Math. Soc. **38** (1963), 419-422.

[30] I. D. Macdonald, *The Theory of Groups*, Clarendon Press, Oxford, (1968).

[31] M. A. Malayeri *On commutators in p-groups of maximal class and some consequences,* Math. Rep. (Bucur.) **20(70)** (2018), 285-290.

[32] G. A. Miller, *On the commutators of a given group*, Bull. Amer. Math. Soc. **6** (1899), 105-109.

[33] I. Niven, H. S. Zuckerman and H. L. Montgomery, *An Introduction of the Threory of Numbers*, John Wiley and Sons, Inc., Second Edition (1968).

[34] T. K. Naik and M. K. Yadav, *Finite p-groups of conjugate type* $\{1, p^3\}$, J. Group Theory **21** (2018), 65-82.

[35] E. A. O'Brien, M. R. Vaughan-Lee, *The groups with order* p^7 *for odd prime p*. J. Algebra **292** (2005), 243-258.

[36] O. Ore, *Some remarks on commutators*, Proc. Amer. Math. Soc. **2** (1951), 307-314.

[37] G. Parmeggiani and B. Stellmacher, *p-Groups of small breadth*, J. Algebra **213** (1999), 52-68.

[38] D. M. Rodney, *On cyclic derived subgroups*, J. London Math. Soc. **8** (1974), 642-646.

[39] D. M. Rodney, *Commutators and abelian groups*, J. Aust. Math. Soc. **24** (1977), 79-91.

[40] B. Wilkens, 2-*groups of breadth* 3, J. Algebra **318** (2007), 202-224.