THE MACDONALD GROUP

A Thesis

Submitted to the Faculty of Graduate Studies and Research

in Partial Fulfillment of the Requirements

for the Degree of

Master of Science

in

Mathematics

University of Regina

By

Alexander Montoya Ocampo

Regina, Saskatchewan

February, 2024

UNIVERSITY OF REGINA

FACULTY OF GRADUATE STUDIES AND RESEARCH

SUPERVISORY AND EXAMINING COMMITTEE

Alexander Montoya Ocampo, candidate for the degree of **Master of Science in Mathematics,** has presented a thesis titled, ***The Macdonald group,*** in an oral examination held on **November 28, 2023**. The following committee members have found the thesis acceptable in form and content, and that the candidate demonstrated satisfactory knowledge of the subject material.

External Examiner:	Dr Gerald Williams, University of Essex*
Supervisor(s):	Dr Fernando Szechtman, Department of Mathematics and Statistics
Committee Member:	Dr Allen Herman, Department of Mathematics and Statistics
Committee Member:	Dr Bruce Gilligan, Department of Mathematics and Statistics
Chair of Defense:	Dr Carlos David Londoño Sulkin, Department of Anthropology

*Attended via Zoom conferencing

Abstract

Given $\alpha \in \mathbb{Z}$, the Macdonald group $G(\alpha)$ is defined by

$$G(\alpha) = \langle\, A, B \mid A^{[A,B]} = A^{\alpha},\ B^{[B,A]} = B^{\alpha} \,\rangle.$$

It is known that $G(\alpha)$ is finite if and only if $\alpha \neq 1$, in which case the prime factors of $|G(\alpha)|$ are those of $\alpha - 1$. It is also known that $G(\alpha)$ is nilpotent in certain cases. We show that $G(\alpha)$ is always nilpotent, so that for $\alpha \neq 1$, $G(\alpha)$ is the direct product of its Sylow subgroups.

In the first third of the thesis, we determine the order, upper and lower central series, nilpotency class, and exponent of each of these Sylow subgroups.

For the remaining two thirds of the thesis we concentrate on the Sylow 2-subgroup $J = J(\alpha)$ of $G(\alpha)$, so we assume that $\alpha = 1 + 2^m\ell$, where $m \geq 1$ and ℓ is odd. We show that J has presentation

$$J = \langle\, x, y \mid x^{[x,y]} = x^{1+2^m\ell},\ y^{[y,x]} = y^{1+2^m\ell},\ x^{2^{3m-1}} = 1 = y^{2^{3m-1}} \,\rangle,$$

order 2^{7m-3}, and nilpotency class 5 if $m > 1$ and 3 if $m = 1$.

In the middle third of the thesis, we determine the automorphism groups of the 2-groups J, $H = J/Z(J)$ and $K = H/Z(H)$, where $|H| = 2^{6m-3}$ and $|K| = 2^{5m-3}$. Explicit multiplication, power, and commutator formulas for J, H, and K are given, and used in the calculation of $\mathrm{Aut}(J)$, $\mathrm{Aut}(H)$, and $\mathrm{Aut}(K)$.

In the final third of the thesis, we consider the infinite family of finite 2-groups $\{J(\alpha)\}_{\alpha\neq 1}$ and settle the following isomorphism problem: given $\alpha \neq 1 \neq \alpha' \in \mathbb{Z}$, when are $J(\alpha)$ and $J(\alpha')$ isomorphic?

Dedication

To my parents and all the people that believed
in me and gave me their help.

Acknowledgements

I thank Volker Gebhardt and Eamonn O'Brien for their help with Magma/GAP computations, and Andrea Previtali and the referees for a careful reading of the papers and useful comments and corrections.

Special thanks to Fernando Szechtman and Bruce Gilligan for their guidance and support throughout the realization of this project.

Additionally, I express my gratitude to Gerald Williams for his dedication in reviewing the conclusive draft of this thesis and for participating as the external examiner during its defense.

And finally, but not least, I thank Maritza, Carlos, and Solstice for their companionship and consideration.

Contents

Chapter 1

Introduction

In 1962, Macdonald [1] investigated the group

$$G(\alpha,\beta) = \langle\, A, B \mid A^{[A,B]} = A^{\alpha},\ B^{[B,A]} = B^{\beta} \,\rangle, \quad \alpha,\beta \in \mathbb{Z}.$$

In this thesis, our main object of study is the Macdonald group in one parameter $\alpha \in \mathbb{Z}$, namely the group $G = G(\alpha) = G(\alpha,\alpha)$.

Our motivation for this study is manifold. First of all, Macdonald's paper [1] is beautifully written, and he determined various basic structural properties of the groups $G(\alpha,\beta)$ through elegant arguments. However, his proof of the nilpotence of $G(\alpha,\beta)$ is incomplete. He did show in detail that $G(\alpha,\beta)$ is nilpotent when $\alpha = 1$, or $\beta = 1$, or $\gcd(\alpha-1,6) = 1 = \gcd(\beta-1,6)$, and stated that the remaining cases followed similarly. We beg to differ. Our discrepancy stems from an innocent looking error, found in [1, Section 5], where it is stated that if $\alpha > 1$, $\alpha = 1+3k$, and $k \equiv -1 \mod 3$, then for $\delta_\alpha = \alpha^\alpha - (1+\alpha+\cdots+\alpha^{\alpha-1})$, one has $v_3((\alpha-1)\delta_\alpha) = 4$. This is only valid if $v_3(k+1) = 1$, as seen in Proposition 3.1 below. If $\alpha > 1$ and $\beta > 1$, the values of $v_p((\alpha-1)\delta_\alpha)$ and $v_q((\beta-1)\delta_\beta)$, where p and q are prime factors of $\alpha-1$ and $\beta-1$, respectively, play an essential role in the structure of $G(\alpha,\beta)$ and in particular in bounding the order and nilpotency class of $G(\alpha,\beta)$ (provided nilpotence is first established). As seen in Sections 3.1 and 3.2, considerable effort is required to establish the nilpotence of $G(\alpha)$, especially when $\alpha = 1+3k$ and $k \equiv -1 \mod 3$.

Secondly, Macdonald left open the question of the precise order and class of his groups $G(\alpha,\beta)$ as complicated. He came back to this question in [2], ten years after the appearance of [1], with a general computer program that allowed him, in particular, to determine the order and nilpotency class of the Sylow 3-subgroup of $G(34,7)$, found to be 3^{10} and 7, respectively, less than the bounds given in [1]. In this thesis, we settle this problem for the groups $G(\alpha)$.

Thirdly, for α and β different from one, $G(\alpha, \beta)$ is a finite group that admits a finite presentation with as many generators as relations. These groups are called *interesting* by Johnson [8, Chapter 7]. A more widely used synonym is finite groups with deficiency zero. Such groups have been studied by several authors. The intensity of this study increased since the discovery by Mennicke [13] of the first family of finite groups requiring 3 generators and 3 relations, in 1959. He considered the groups

$$M(a, b, c) = \langle\, x, y, z \mid x^y = x^a,\ y^z = y^b,\ z^x = z^c \,\rangle$$

with $a, b, c \in \mathbb{Z}$ and proved them to be finite when $a = b = c \geq 2$.

It is easy to see that $M(a, b, c)$ does require 3 generators whenever $a - 1$, $b - 1$, $c - 1$ share a prime factor. The problem of the finiteness of the general Mennicke groups $M(a, b, c)$ was studied by Macdonald and Wamsley [14], Schenkman [15], and Jabara [16]. A sufficient condition is that $|a|, |b|, |c| \geq 2$. Upper bounds for the order of $M(a, b, c)$ were provided by Johnson and Robertson [17], Albar and Al-Shuaibi [19], and Jabara [16]. The actual order of $M(a, b, c)$ is known only in certain cases (see [13, 18, 19, 16]). As exemplified by the Mennicke groups $M(a, b, c)$, it may be quite difficult to determine the order and other structural properties of the members of a given family of finite groups with deficiency zero.

In the fourth place, once the nilpotence of the finite group $G(\alpha)$ is established, it follows that $G(\alpha)$ is the direct product of its Sylow subgroups $G(\alpha)_p$, where $p \in \mathbb{N}$ runs through all prime factors of $\alpha - 1$, and our study of $G(\alpha)$ yields detailed structural information about the infinite family of finite p-groups $G(\alpha)_p$. It should be noted that, according to Wamsley [22], the Sylow subgroups $G(\alpha)_p$ are themselves interesting, except perhaps when $p = 2$. The study of finite p-groups, is quite active, as seen in [24, 25, 26, 27, 28], for instance. We hope that our investigation of the groups $G(\alpha)_p$ contributes in this regard. We find a presentation as well as the order, upper and lower central series, nilpotency class, and exponent of $G(\alpha)_p$, among other structural properties.

Fifth, the automorphism groups of finite p-groups, have been the object of considerable attention, from various angles, one of which is simply to investigate the actual structure of $\mathrm{Aut}(T)$ when T is a finite p-group of one type or another, see [32, 33, 34, 35, 36], for instance, all of which provide recent and detailed studies of the automorphism groups of metacyclic p-groups. The structure of J is considerably more complicated, in this thesis we study $\mathrm{Aut}(J)$ where $J = J(\alpha) = G(\alpha)_2$ with $\alpha = 1 + 2^m\ell$, ℓ odd, and $m \geq 1$.

Another incentive for our investigation of $\mathrm{Aut}(J)$ is to apply it to the question that arises by replacing α with another integer $\alpha' = 1 + 2^m\ell'$ with ℓ' odd: when are the finite 2-groups

$J(\alpha)$ and $J(\alpha')$ isomorphic? This turns out to be a nontrivial isomorphism problem, settled in Chapter 6, where the automorphism groups $\mathrm{Aut}(J)$, $\mathrm{Aut}(H)$, and $\mathrm{Aut}(K)$, of

$$J = J(\alpha) = \langle\, x, y \mid x^{[x,y]} = x^{\alpha},\ y^{[y,x]} = y^{\alpha},\ x^{2^{3m-1}} = y^{2^{3m-1}} = 1 \,\rangle,$$

$$H = J/Z(J) = \langle\, x, y \mid x^{[x,y]} = x^{\alpha},\ y^{[y,x]} = y^{\alpha},\ x^{2^{2m-1}} = y^{2^{2m-1}} = 1 \,\rangle,$$

$$K = H/Z(H) = \langle\, x, y \mid x^{[x,y]} = x^{\alpha},\ y^{[y,x]} = y^{\alpha},\ x^{2^{2m-1}} = y^{2^{2m-1}} = [x,y]^{2^{m-1}} = 1 \,\rangle$$

play a critical role.

We found it difficult to distinguish nonisomorphic groups that appear similar in so many respects and we were unable to detect a structural property to tell them apart. This phenomenon is not unique, see [23], for instance. In our case, we used an isomorphism searching technique, as described in Section 6.2, together with our knowledge of the automorphism group of the groups involved.

In analyzing $\mathrm{Aut}(J)$ we found the structure of the factor $\mathrm{Aut}(J)/\mathrm{Aut}_4(J)$ and that of $\mathrm{Aut}_4(J)/\mathrm{Inn}(J)\mathrm{Aut}_3(J)$ so challenging that we felt compelled to derive explicit multiplication, power, and commutator formulas for J, as exhibited in Section 5.1. Our commutator formula from Theorem 5.3 plays a key role in the structure of the Wamsley groups $W(\alpha, \beta, \gamma)$ as defined in [20]. See [21] for details of this application. As very little is known at the moment about the Wamsley groups, this application provides a sixth reason for the existence of this work. These formulas as well as the orders of the automorphism groups of J, H, and K agree with the output produced by the algebra software GAP and Magma (that we used heavily) for all tested values of α.

A seventh and final reason to produce this work is that our strategy to approach $\mathrm{Aut}(T)$, when T is J, H, or K, may be of use to study the automorphism groups of other finite nilpotent groups T.

This thesis is organized as follows:

• Chapter 1: Introduction.

• Chapter 2 lists the results we require from group theory and from Macdonald's paper [1].

• Chapter 3 contains the required calculations for a proof that $G(\alpha)$ is nilpotent. In particular, Sections 3.1 and 3.3 contains some useful valuation calculations of expressions that arise naturally in $G(\alpha)$, while Section 3.2 contains the proof for the nilpotence of $G(\alpha)$.

• In Chapter 4 we study the internal structure of the Sylow subgroups, $G(\alpha)_p$, of $G(\alpha)$. In particular, in Sections 4.1 and 4.2 we give a presentation for each Sylow subgroup of $G(\alpha)$

and find an upper bound for its order. The proof that this upper bound is sharp is fairly laborious and is postponed to an appendix at the end of the chapter in order to maintain the flow of the thesis (of course, this appendix does not depend on any intermediate results). Relying on the constructions given in the appendix, Section 4.3 yields the order of $G(\alpha)_p$, a normal form for its elements, as well as some basic structural properties. The upper and lower central series of $G(\alpha)_p$, together with its nilpotency class, are found in Section 4.4. The exponent of $G(\alpha)_p$ is determined in Section 4.5. All of this is combined in Section 4.6 to produce the order, nilpotency class, and exponent of $G(\alpha)$ in terms of α.

• In Chapter 5 we restrict ourselves to the case $p = 2$ and study the automorphism group $\mathrm{Aut}(J)$ of $J = J(\alpha) = G(\alpha)_2$. Since this is a difficult task we had to develop a new strategy to achieve our goal. This strategy is as follows:

We will see that the groups J, H, and K, defined above, respectively, have order 2^{7m-3}, 2^{6m-3}, and 2^{5m-3}, and nilpotency class 5, 4, and 3 if $m > 1$, and 3, 2, and 1 if $m = 1$. We proceed to determine their automorphism groups.

Given a nilpotent group T of class c, we let $\langle 1\rangle = Z_0(T)$, $Z_1(T)$, $Z_2(T)$, $\ldots$, $Z_c(T) = T$ stand for the terms of the upper central series of T, so that $Z_{i+1}(T)/Z_i(T)$ is the center of $T/Z_i(T)$, and we write $\mathrm{Aut}_i(T)$ for the kernel of the canonical map $\mathrm{Aut}(T) \to \mathrm{Aut}(T/Z_i(T))$. This induces the following normal series in $\mathrm{Aut}(T)$:

$$\langle 1\rangle = \mathrm{Aut}_0(T) \subseteq \mathrm{Aut}_1(T) \subseteq \cdots \subseteq \mathrm{Aut}_c(T) = \mathrm{Aut}(T). \tag{1.1}$$

In order to determine $\mathrm{Aut}(T)$ we want to compute the factors $\mathrm{Aut}_{i+1}(T)/\mathrm{Aut}_i(T)$ of (1.1) for all $0 \leq i < c$. An imbedding tool, namely Proposition 5.47, allows us to derive information from the foregoing sections of (1.1) arising from $T/Z(T)$ to those arising from T. Thus, we begin our work with $T = K = H/Z(H)$, continue with $T = H = J/Z(J)$, and culminate it with $T = J$. We will get the desired information of $\mathrm{Aut}(J)$ as a consequence of this. All of this is done for $m > 1$ since the much simpler case $m = 1$ is settled at the beginning of the chapter.

In Section 5.1 we present some structural formulas for J whose proofs are placed at the end of the chapter in an appendix. Section 5.2 lists some properties of the upper central series of J that follow from Chapter 4, and Sections 5.4, 5.3, and 5.5 have the main results for $\mathrm{Aut}(K)$, $\mathrm{Aut}(H)$, and $\mathrm{Aut}(J)$, respectively.

The automorphism groups of all remaining Sylow subgroups of $G(\alpha)$ are studied in [5], but for the exceptional case $p = 3$ and $\alpha \equiv 7 \mod 9$.

• In Chapter 6 we study the following isomorphism problem that arises in the class $\{J(\alpha)\}_{\alpha\neq 1}$: given $\alpha \neq 1 \neq \alpha'$, when are $J(\alpha)$ and $J(\alpha')$ isomorphic?

Macdonald [1] showed that $J(\alpha)$ is trivial if and only if α is even, which solves the problem when α or α' is even. Now, let $\alpha = 1+2^m\ell$, $\alpha' = 1+2^m\ell'$ with ℓ, ℓ' odd and $m \geq 1$. As hinted above and seen more thoroughly below, the groups J, H, and K possess several structural properties that are completely independent of ℓ, and they are difficult to differentiate from their corresponding counterparts when α is replaced by α'.

In this chapter, we find necessary and sufficient conditions for the existence of an isomorphism arising from the substitution $\alpha \leftrightarrow \alpha'$.

There are infinitely many substitutions $\alpha \leftrightarrow \alpha'$ to consider, although a quick observation leaves only finitely many to be analyzed. Indeed, it is easy to see that: if $\alpha' \equiv \alpha \mod 2^{3m-1}$ then $J(\alpha') \cong J(\alpha)$. The same observations are valid for H and K, the moduli being 2^{2m-1} in this case. However, these evident sufficient conditions are too strong, as the given isomorphisms actually hold under weaker conditions, as indicated below.

In Section 6.1 we present sufficient conditions. In Section 6.2 we develop a tool that will allow us to address the necessary conditions of the problem. In Sections 6.3, 6.4, and 6.5 we find necessary conditions for K, H, and J. In Section 6.6 we show that even when $J(\alpha)$ and $J(\alpha')$ are not isomorphic, they still have a lot of properties in common. In Section 6.7 we summarize the main results of the chapter and, finally, Section 6.8 is an appendix that contains some long calculations used in Section 6.5.

The isomorphism problem for all the remaining Sylow subgroups of $G(\alpha)$ is studied in [6].

Chapter 2

Preliminaries

In this thesis we will be making heavy use of the papers [1, 3, 4, 5, 6].

For a general background in group theory see [7, 8, 9, 10].

Let p be a prime number and n a nonzero integer. We define $v_p(n)$ as the exponent of p in the prime factorization of n, this is, $n = p^{v_p(n)}t$ where $t \in \mathbb{Z}$ is such that $p \nmid t$.

Given a group T and $a, b \in T$, we write

$$[a,b] = a^{-1}b^{-1}ab,\ b^a = a^{-1}ba,\ {}^ab = aba^{-1},$$

recalling that

$$[a,bc] = [a,c][a,b]^c,\ [bc,a] = [b,a]^c\,[c,a]. \tag{2.1}$$

We let $\langle 1\rangle = Z_0(T)$, $Z_1(T)$, $Z_2(T)$, ... stand for the terms of the upper central series of T, so that $Z_{i+1}(T)/Z_i(T)$ is the center of $T/Z_i(T)$.

Given $X, Y \subseteq T$, we define $[X,Y] = \langle\ [x,y] \mid x \in X,\ y \in Y\ \rangle$. If $X = Y = T$, we call $[T,T]$ the derived subgroup of T. We write $T = \gamma_1(T)$, $\gamma_2(T)$, $\gamma_3(T)$, ... for the terms of the lower central series of T, so that $\gamma_{i+1}(T) = [T, \gamma_i(T)]$.

We write $\mathrm{Aut}_i(T)$ for the kernel of the canonical map $\mathrm{Aut}(T) \to \mathrm{Aut}(T/Z_i(T))$. Note that each $\mathrm{Aut}_i(T)$ is a normal subgroup of $\mathrm{Aut}(T)$. The automorphisms of T belonging to $\mathrm{Aut}_i(T)$ will be said to be i-central, while those in $\mathrm{Aut}_1(T)$ will simply be said to be central. Note that central and inner automorphisms commute with each other.

We let $\delta : T \to \mathrm{Aut}(T)$ stand for the canonical map $a \mapsto a\delta$, where $a\delta$ is conjugation by a, namely the map $b \mapsto b^a$. Observe that for $a \in T$, $a\delta \in \mathrm{Aut}_i(T)$ if and only if $a \in Z_{i+1}(T)$, so that

$$\mathrm{Inn}(T) \cap \mathrm{Aut}_i(T) = Z_{i+1}(T)\delta \cong Z_{i+1}(T)/Z(T).$$

The order of a torsion element A of T will be denoted by $|A|$.

If S is a normal subgroup of T, we sometimes write $\overline{T}$ for T/S and $\bar{t}$ for $tS \in \overline{T}$.

Function composition proceeds from left to right.

Furthermore, for $n \in \mathbb{Z}$, by T^n we will understand two different things depending on the chapter we are on: In Chapters 3 and 4, T^n stands for the subgroup of T generated by all t^n, with $t \in T$, whereas in Chapters 5 and 6, we let T^n stands for the direct product of n copies of T.

Given a ring R with $1 \neq 0$, we write $\mathrm{Heis}(R)$ for the Heisenberg group over R (see [8, Chapter 5] for the case $R = \mathbb{Z}$).

We will use the following result found in [7, 5.1.7]:

Theorem 2.2. *Let T be any group, $X, Y \subseteq T$, and define $X^Y = \langle\, x^y \mid x \in X,\ y \in Y \,\rangle$. If H and K are subgroups of T such that $H = \langle X \rangle$ and $K = \langle Y \rangle$, then $[H, K] = [X, Y]^{HK}$.*

2.1 Cyclic extensions

The following well-known gadget (see [11] and [12, Chapter III, Section 7]) will be used repeatedly and implicitly to construct a model (see Definition 4.11) of the Sylow 2-subgroup, J, of $G(\alpha)$ in the appendix found in Section 4.7.

Let E be any group and suppose that T is a normal subgroup of E such that E/T is cyclic of order $n \in \mathbb{N}$. Then there is some coset gT such that $E/T \cong \langle gT \rangle$ and we know that $g^n T = (gT)^n = T$, so $g^n \in T$ (moreover, n is the smallest positive integer such that $g^n \in T$). Since g induces an automorphism of T, we let $\Omega = g\delta \in \mathrm{Aut}(T)$ and $t = g^n$. Then $t^\Omega = t^g = t$ and $\Omega^n = t\delta \in \mathrm{Aut}(T)$.

Summarizing we have the following:

- a group T,
- $n \in \mathbb{N}$,
- $t \in T$,
- $\Omega \in \mathrm{Aut}(T)$ that satisfies $t^\Omega = t$ and $\Omega^n = t\delta$.

Now, we ask the following question: using the above "ingredients" can we reconstruct the group E? The answer is yes as we will see in Proposition 2.3, but first let's see how the multiplication in E behaves.

Note that the full list of cosets of T in E is $\{T, gT, g^2T, \ldots, g^{n-1}T\}$. Then every element of E can be uniquely written in the form $g^k x$ where $0 \leq k < n$ is an integer and $x \in T$ and it can be identified with the pair (k, x). The multiplication is as follows

$$(g^i x)(g^j y) = g^i g^j (g^{-j} x g^j) y = g^{i+j} x^{g^j} y = g^{i+j} x^{\Omega^j} y$$

where $g^{i+j} = g^{i+j-n} t$ if $i + j \geq n$. Thus the product $(g^i x)(g^j y)$ can be identified with the pair $(i + j, x^{\Omega^j} y)$ if $i + j < n$, and with $(i + j - n, t x^{\Omega^j} y)$ if $i + j \geq n$. This inspires the following result.

Proposition 2.3. *Let T be any group and $\mathbb{Z}/n\mathbb{Z}$ the cyclic group of order $n \in \mathbb{N}$. Suppose that $t \in T$ and that $\Omega \in \mathrm{Aut}(T)$ is such that $t^\Omega = t$ and $\Omega^n = t\delta$. Then there is a group E containing T as a normal subgroup, such that $E/T \cong \mathbb{Z}/n\mathbb{Z}$, and for some $g \in E$ of order n modulo T, we have $g^n = t$ and $\Omega = g\delta$.*

Proof. Let $E = \{(k, x) \mid k \in \mathbb{Z},\ 0 \leq k < n,\ x \in T\}$ and define the following operation on E:

$$(i, x) \cdot (j, y) = (i + j, x^{\Omega^j} y), \text{ if } i + j < n,$$
$$(i, x) \cdot (j, y) = (i + j - n, t x^{\Omega^j} y), \text{ if } i + j \geq n.$$

It is routinary to verify that E is a group under this operation, with identity $(0, 1_T)$, and for any element $(k, x) \in E$ its inverse is given by

$$(k, x)^{-1} = \begin{cases} (0, x^{-1}), & \text{if } k = 0, \\ (n - k, (x^{-1})^{\Omega^{n-k}} t^{-1}), & \text{if } k \neq 0. \end{cases}$$

Moreover, it is easy to verify that, $T_0 = \{(0, x) \mid x \in T\}$ is a normal subgroup of E such that $T_0 \cong T$, where $t \in T$ is represented by the element $(0, t) \in T_0$ and $g = (1, 1_T)$ has order n modulo T_0 and satisfies $g^n = (0, t)$. Also, as $(k, x) = g^k \cdot (0, x)$ for all $(k, x) \in E$, then $E/T_0 = \langle gT_0 \rangle \cong \mathbb{Z}/n\mathbb{Z}$ and, since $(0, x)^g = (0, x^\Omega)$, then $\Omega = g\delta$. □

2.2 General background on the Macdonald group

The following results can be found in [1]:

Given $\alpha, \beta \in \mathbb{Z}$ define the Macdonald group by

$$G(\alpha, \beta) = \langle\ A, B \mid A^{[A,B]} = A^\alpha,\ B^{[B,A]} = B^\beta\ \rangle$$

and denote $G(\alpha) = G(\alpha, \alpha)$.

Proposition 2.4.

1. $G(\alpha,\beta)\cong G(\beta,\alpha)$,
2. $G(0,\beta)\cong\mathbb{Z}/|\beta-1|\mathbb{Z}$ *if* $\beta\neq 1$,
3. $G(0,1)\cong\mathbb{Z}$.

Note 2.5. It is readily seen that $G(1)$ is the integral Heisenberg group

$$\mathrm{Heis}(\mathbb{Z})=\left\{\begin{pmatrix}1&i&k\\0&1&j\\0&0&1\end{pmatrix}\;\middle|\;i,j,k\in\mathbb{Z}\right\}=\left\langle\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix},\ \begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}\right\rangle.$$

with isomorphism given by

$$A\mapsto\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix},\ B\mapsto\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}.$$

Moreover, $G(1,\beta)$ is infinite for every $\beta\in\mathbb{Z}$, since adding the relation $B=1$ produces the quotient group $\langle\, A,B\mid A^{[A,B]}=A,\ B^{[B,A]}=B^{\beta},\ B=1\,\rangle\cong\langle\, A\mid A=A\,\rangle\cong\mathbb{Z}$.

Corollary 2.6. *$G(\alpha,\beta)$ is finite if and only if $\alpha\neq 1\neq\beta$.*

Proof. The fact that $G(\alpha,\beta)$ is finite when $\alpha\neq 1$ and $\beta\neq 1$ is proved in [1, Section 4]. The converse follows from Note 2.5. □

Proposition 2.7. *Suppose $\alpha\neq 0\neq\beta$, let $u,v,w\in\mathbb{Z}$ with $v\geq 0$, $w>0$, and denote $C=[A,B]$. The following formulas hold in $G(\alpha,\beta)$:*

1. $(A^uC^v)^w=C^{wv}A^{u\alpha^v(1+\alpha^v+\ldots+\alpha^{(w-1)v})}$,
2. $(A^w)^B=C^wA^{\alpha(1+\alpha+\ldots+\alpha^{w-1})}$,
3. $(B^uC^{-v})^w=C^{-wv}B^{u\beta^v(1+\beta^v+\ldots+\beta^{(w-1)v})}$,
4. $(B^w)^A=C^{-w}B^{\beta(1+\beta+\ldots+\beta^{w-1})}$,
5. $[A,B^\beta]^C=[A^\alpha,B]$.

Proposition 2.8. *There exists $f\in\mathrm{Aut}(G(\alpha))$ such that $f(A)=B$ and $f^2=1_{\mathrm{Aut}(G(\alpha))}$. In particular, $|A|=|B|$ in $G(\alpha)$.*

Consider the following expressions of α from [1, Equations (2.4) and (2.22)]:

$$\gamma = \alpha^{\alpha} - (1 + \alpha + \cdots + \alpha^{\alpha-1}), \text{ if } \alpha > 0 \tag{2.9}$$

$$\xi = 2 + \alpha + \cdots + \alpha^{-\alpha-1}, \text{ if } \alpha < 0. \tag{2.10}$$

According to [1, Equations (2.10), (2.11), and (2.12)], we have

$$A^{\gamma}B^{\gamma} = 1,\ A^{(\alpha-1)\gamma} = 1 = B^{(\alpha-1)\gamma}, \quad \alpha > 0, \tag{2.11}$$

and, as explained in [1, Page 606], we have

$$A^{\xi}B^{\xi} = 1, \quad \alpha < 0. \tag{2.12}$$

From [1, Page 611] it follows that

$$(\alpha-1)\gamma = \frac{[(\alpha-1)^2+1]}{2}(\alpha-1)^3 + (\alpha-2)\binom{\alpha}{3}(\alpha-1)^3 + (\alpha-2)\binom{\alpha}{4}(\alpha-1)^4 + \cdots. \tag{2.13}$$

The following result will be of use later.

Proposition 2.14. *Let $\alpha, \beta \in \mathbb{Z}$ be different from 1 and let $p \in \mathbb{N}$ be a prime. Then p is a factor of $|G(\alpha, \beta)|$ if and only if p is a factor of $(\alpha - 1)(\beta - 1)$.*

Proof. The argument starting at the bottom of page 602 and ending at the top of page 603 of [1] shows that if p is a factor of $(\alpha - 1)(\beta - 1)$, then p is a factor of $|G(\alpha, \beta)|$.

By [1, Section 4], the prime factors of $|A|$ must be prime factors of $\alpha - 1$ and the prime factors of $|B|$ must be prime factors of $\beta - 1$. Thus, $|A|$ is a factor of a power of $\alpha - 1$ and $|B|$ is a factor of a power of $\beta - 1$. It follows from the argument given in the middle of page 603 of [1] that $|C|$ is a factor of a power of $\alpha - 1$. By Lemma 4.7 (which is independent of previous results), $|G(\alpha, \beta)|$ is a factor of $|A||B||C|$. We deduce that if p is a factor of $|G(\alpha, \beta)|$, then p must be a factor of $(\alpha - 1)(\beta - 1)$. □

Corollary 2.15. $G(0, 0) \cong G(0, 2) \cong G(2, 2) \cong \langle 1 \rangle$.

Now we are ready to begin our study of $G(\alpha)$. As cases $\alpha \in \{0, 1, 2\}$ are already covered in Note 2.5 and Corollary 2.15 we suppose $\alpha \notin \{0, 1, 2\}$ for the remainder of the document.

Chapter 3

Nilpotency of G and valuation calculations

3.1 Valuation calculations

Recall the definition of γ given in Equation (2.9).

Proposition 3.1. *Suppose $\alpha > 0$, $p \in \mathbb{N}$ is a prime factor of $\alpha - 1$, and $v_p(\alpha - 1) = m$. Then*

$$v_p(\gamma) = \begin{cases} 2m, & \text{if } p > 3, \\ 2m-1, & \text{if } p = 2, \\ 2m, & \text{if } p = 3, \text{ with } m > 1 \text{ or } (\alpha-1)/3 \equiv 1 \mod 3, \\ 2+s, & \text{if } p = 3, \text{ where } \alpha = 1+3k,\ k = -1+3^s u,\ s,u \in \mathbb{N},\ \gcd(3,u) = 1. \end{cases}$$

Moreover, in the last case, we have $\gamma = 3^{2+s}t$, where $t \in \mathbb{N}$ and $t \equiv -u \mod 3$.

Proof. From (2.13)

$$(\alpha-1)\gamma = \frac{[(\alpha-1)^2+1]}{2}(\alpha-1)^3 + (\alpha-2)\binom{\alpha}{3}(\alpha-1)^3 + (\alpha-2)\binom{\alpha}{4}(\alpha-1)^4 + \cdots,$$

so $v_p(\gamma) = 2m$ if $p > 3$, and $v_p(\gamma) = 2m-1$ if $p = 2$. If $p = 3$ put $\alpha = 1 + 3^m k$ with $3 \nmid k$, so that

$$(\alpha-1)\gamma = \frac{[1 + 3^{2m}k^2 + (-1+3^m k)^2(1+3^m k)3^{m-1}k]}{2}(\alpha-1)^3 + (\alpha-2)\binom{\alpha}{4}(\alpha-1)^4 + \cdots.$$

If $m > 1$ or $k \equiv 1 \mod 3$, we infer $v_3(\gamma) = 2m$. Suppose next $p = 3$, $m = 1$ and $k = -1+3^s u$, where $s, u \in \mathbb{N}$ and $\gcd(3, u) = 1$. We then have

$$\alpha^\alpha = \alpha^{\alpha-1}\alpha = \alpha^{\alpha-1}(1 + (\alpha - 1)) = \alpha^{\alpha-1} + (\alpha - 1)\alpha^{\alpha-1},$$

so

$$\gamma = \alpha^\alpha - (1 + \alpha + \cdots + \alpha^{\alpha-1}) = \alpha^\alpha - \alpha^{\alpha-1} - (1 + \alpha + \cdots + \alpha^{\alpha-2}) = (\alpha - 1)\alpha^{\alpha-1} - \frac{\alpha^{\alpha-1} - 1}{\alpha - 1},$$

that is,

$$\gamma = 3k(1 + 3k)^{3k} - \frac{(1 + 3k)^{3k} - 1}{3k}. \tag{3.2}$$

Now

$$(1 + 3k)^3 = 1 + 3^2k + 3^3k^2 + 3^3k^3 = 1 + 3^2k + 3^3k^2(1 + k) = 1 + 3^2k + 3^{3+s}k^2u,$$

and therefore

$$(1 + 3k)^{3k} = (1 + 3^2k + 3^{3+s}k^2u)^k = \sum_{i+j+\ell=k} \frac{k!}{i!j!\ell!} 1^i 3^{2j} k^j 3^{(3+s)\ell} (k^2u)^\ell.$$

Splitting off the case $\ell = 0$, we obtain

$$(1 + 3k)^{3k} = \sum_{0\le j\le k} \binom{k}{j} 3^{2j}k^j + \sum_{\substack{i+j+\ell=k \\ \ell\ge 1}} \frac{k!}{i!j!\ell!} 1^i 3^{2j} k^j 3^{(3+s)\ell} (k^2u)^\ell.$$

All terms in the second summand, except for the term with $j = 0, \ell = 1$, are multiples of $3^{3+s+1}k$, so

$$(1 + 3k)^{3k} = \left(\sum_{0\le j\le k} \binom{k}{j} 3^{2j}k^j \right) + 3^{3+s}k^3u + 3^{3+s+1}kw, \quad w \in \mathbb{Z},$$

$$3k(1 + 3k)^{3k} = \left(\sum_{0\le j\le k} \binom{k}{j} 3^{2j+1}k^{j+1} \right) + 3^{3+s}r, \quad r \in \mathbb{Z},$$

$$\frac{(1 + 3k)^{3k} - 1}{3k} = \left(\sum_{1\le j\le k} \binom{k}{j} 3^{2j-1}k^{j-1} \right) + 3^{2+s}k^2u + 3^{3+s}w.$$

Since $\gcd(3, k^2u) = 1$, we may now go back to (3.2) and deduce that, provided 3^{3+s} is a factor of

$$P = \sum_{0\le j\le k} \binom{k}{j} 3^{2j+1}k^{j+1} - \sum_{1\le j\le k} \binom{k}{j} 3^{2j-1}k^{j-1},$$

we indeed have $v_3(\gamma) = 2 + s$, with $\gamma = 3^{2+s}t$, $t \in \mathbb{N}$, $t \equiv -k^2u \equiv -u \mod 3$. To see that $3^{3+s} \mid P$, put $f = j - 1$, so that $j = f + 1$, $2j - 1 = 2f + 1$, and

$$\sum_{1\le j\le k} \binom{k}{j} 3^{2j-1}k^{j-1} = \sum_{0\le f\le k-1} \binom{k}{f+1} 3^{2f+1}k^f.$$

Therefore

$$\begin{aligned} P &= \sum_{0\le f\le k} \binom{k}{f} 3^{2f+1}k^{f+1} - \sum_{0\le f\le k-1} \binom{k}{f+1} 3^{2f+1}k^f \\ &= 3^{2k+1}k^{k+1} + \sum_{0\le f\le k-1} 3^{2f+1}k^f \left(k\binom{k}{f} - \binom{k}{f+1} \right) \\ &= 3^{2k+1}k^{k+1} + \sum_{0\le f\le k-1} 3^{2f+1}k^f \binom{k}{f} \frac{f(k+1)}{f+1} \\ &= 3^{2k+1}k^{k+1} + \sum_{1\le f\le k-1} 3^{2f+1}k^f \binom{k}{f} \frac{f3^su}{f+1}. \end{aligned}$$

As $3^su = k + 1$, we have $k + 1 \ge 3^s$. On the other hand, $3^s = (1 + 2)^s \ge 1 + 2s > 1 + s$, so $2(k-1) \ge k-1 \ge s$, and therefore $2k+1 \ge 3+s$. It follows that $v_3(3^{2k+1}k^{k+1}) = 2k+1 \ge 3+s$. Fix any f such that $1 \le f \le k - 1$, and set $g = v_3(f + 1)$. Then $f + 1 \ge 3^g$, which implies, as above, that $f - 1 \ge g$. Thus, $\frac{3^su}{f+1} \in \mathbb{Q}$, with $v_3(\frac{3^su}{f+1}) = s - g \ge s - (f - 1)$. Moreover, $\binom{k}{f} f \in \mathbb{N}$, so $v_3(\binom{k}{f} f) \ge 0$. Our calculation of P shows that $3^{2f+1}k^f \binom{k}{f} \frac{f3^su}{f+1}$ is a positive integer, and we have

$$v_3\left(3^{2f+1}k^f \binom{k}{f} \frac{f3^su}{f+1}\right) \ge 2f + 1 + (s - g) \ge 2f + 1 + s - (f - 1) = s + f + 2 \ge s + 3. \ \square$$

Consider the following function of α:

$$\mu = \alpha^{\alpha^2+1} - (1 + \alpha + \cdots + \alpha^{\alpha^2-1}). \tag{3.3}$$

Proposition 3.4. *Suppose that $\alpha \ne -1$, and let $p \in \mathbb{N}$ be a prime factor of $\alpha - 1$ with $v_p(\alpha - 1) = m$. Then $\mu \ne 0$, $v_p((\alpha - 1)\mu) \ge 3m$ if $p = 2$, and*

$$v_p((\alpha - 1)\mu) = \begin{cases} 3m, & \text{if } p > 3, \\ 4, & \text{if } p = 3, \alpha = 1 + 3k, k \in \mathbb{Z}, k \equiv -1 \mod 9. \end{cases}$$

Proof. As $|\alpha| \ge 2$, we see that $|\alpha^{\alpha^2+1}| > |1 + \alpha + \cdots + \alpha^{\alpha^2-1}|$, so $\mu \ne 0$.

We have $(\alpha - 1)\mu = \alpha^{\alpha^2+2} - \alpha^{\alpha^2+1} - (\alpha^{\alpha^2} - 1) = \alpha^{\alpha^2}(\alpha^2 - \alpha - 1) + 1$, where

$$\alpha^{\alpha^2} = (1+(\alpha-1))^{\alpha^2} = 1+\binom{\alpha^2}{1}(\alpha-1)+\binom{\alpha^2}{2}(\alpha-1)^2+\binom{\alpha^2}{3}(\alpha-1)^3+\binom{\alpha^2}{4}(\alpha-1)^4+\cdots.$$

Thus, setting $\nu = (\alpha^2 - \alpha - 1)$, we deduce

$$\begin{aligned}
&(\alpha-1)\mu \\
&= \alpha(\alpha-1) + \nu\binom{\alpha^2}{1}(\alpha-1) + \nu\binom{\alpha^2}{2}(\alpha-1)^2 + \nu\binom{\alpha^2}{3}(\alpha-1)^3 + \nu\binom{\alpha^2}{4}(\alpha-1)^4 + \cdots \\
&= \frac{((\alpha-1)^2 + 3(\alpha-1) + 2)}{2}((\alpha-1)^2(\alpha+1)+1)(\alpha-1)^3 + \nu\binom{\alpha^2}{3}(\alpha-1)^3 + \cdots,
\end{aligned}$$

which proves the result when $p \neq 3$. Suppose next $p = 3$ and $\alpha = 1 + 3k$, where $k \in \mathbb{Z}$ satisfies $k \equiv -1 \mod 9$. Put

$$S = \alpha(\alpha+1),\ T = S\frac{\alpha\nu}{2},$$

$$U = T\frac{(\alpha-1)(\alpha^2-2)}{3},\ V = U\frac{(\alpha^2-3)(\alpha-1)}{4}.$$

Then

$$(\alpha-1)\mu = (S+T+U+V)(\alpha-1)^3 + \nu\binom{\alpha^2}{5}(\alpha-1)^5 + \nu\binom{\alpha^2}{6}(\alpha-1)^6 + \cdots,$$

where

$$S \equiv 2,\ T \equiv -1,\ U \equiv 2,\ V \equiv 3 \qquad \mod 9.$$

Thus $S+T+U+V \equiv -3 \mod 9$, so $v_3(S+T+U+V) = 1$, whence $v_3((\alpha-1)\mu) = 4$. □

3.2 Nilpotence of G

We maintain the following presentation of $G = G(\alpha)$ throughout this section:

$$\langle\, A, B \mid A^{[A,B]} = A^{\alpha},\ B^{[B,A]} = B^{\alpha} \,\rangle,$$

setting $C = [A, B]$, and observing the existence of an automorphism $A \leftrightarrow B$, say θ of G, satisfying $C \leftrightarrow C^{-1}$. Recalling the definition (3.3) of μ, we set $\mu_0 = \alpha\mu$.

Proposition 3.5. *We have*

$$A^{\mu_0}B^{\mu_0} = 1,\ A^{(\alpha-1)\mu_0} = 1 = B^{(\alpha-1)\mu_0}.$$

Proof. If $\alpha = -1$ then $\mu_0 = 0$ and there is nothing to do. Suppose henceforth that $\alpha \neq -1$. As conjugation by C^2 is an automorphism of G, we see that

$$[A, B^{\alpha^2}]^{C^2} = [A^{\alpha^2}, B]. \tag{3.6}$$

Regarding the left hand side of (3.6), we have

$$(B^{\alpha^2})^A = (B^A)^{\alpha^2} = (BC^{-1})^{\alpha^2} = C^{-\alpha^2} B^{\alpha(1+\alpha+\cdots+\alpha^{\alpha^2-1})},$$

which successively implies

$$(B^{-\alpha^2})^A = B^{-\alpha(1+\alpha+\cdots+\alpha^{\alpha^2-1})} C^{\alpha^2},$$

$$[A, B^{\alpha^2}] = (B^{-\alpha^2})^A B^{\alpha^2} = B^{-\alpha(1+\alpha+\cdots+\alpha^{\alpha^2-1})} C^{\alpha^2} B^{\alpha^2}, \tag{3.7}$$

$$[A, B^{\alpha^2}]^{C^2} = C^{-2} B^{-\alpha(1+\alpha+\cdots+\alpha^{\alpha^2-1})} C^{\alpha^2} B^{\alpha^2} C^2. \tag{3.8}$$

As for the right hand side of (3.6), applying θ to (3.7) and then inverting yields

$$[A^{\alpha^2}, B] = A^{-\alpha^2} C^{\alpha^2} A^{\alpha(1+\alpha+\cdots+\alpha+\alpha^{\alpha^2-1})}. \tag{3.9}$$

It follows from (3.6) that the right hand sides of (3.8) and (3.9) are equal. Thus

$$\begin{aligned} B^{-\alpha(1+\alpha+\cdots+\alpha^{\alpha^2-1})} C^{\alpha^2} B^{\alpha^2} C^2 &= C^2 A^{-\alpha^2} C^{\alpha^2} A^{\alpha(1+\alpha+\cdots+\alpha^{\alpha^2-1})} \\ &= C^2 A^{-\alpha^2} C^{-2} C^{\alpha^2+2} A^{\alpha(1+\alpha+\cdots+\alpha^{\alpha^2-1})} \\ &= A^{-1} C^{\alpha^2+2} A^{\alpha(1+\alpha+\cdots+\alpha^{\alpha^2-1})}. \end{aligned}$$

On the other hand,

$$\begin{aligned} B^{-\alpha(1+\alpha+\cdots+\alpha^{\alpha^2-1})} C^{\alpha^2} B^{\alpha^2} C^2 &= B^{-\alpha(1+\alpha+\cdots+\alpha^{\alpha^2-1})} C^{\alpha^2+2} C^{-2} B^{\alpha^2} C^2 \\ &= B^{-\alpha(1+\alpha+\cdots+\alpha^{\alpha^2-1})} C^{\alpha^2+2} B \\ &= B^{-\alpha(1+\alpha+\cdots+\alpha^{\alpha^2-1})} C^{\alpha^2+2} B C^{-(\alpha^2+2)} C^{\alpha^2+2} \\ &= B^{-\alpha(1+\alpha+\cdots+\alpha^{\alpha^2-1})} B^{\alpha^{\alpha^2+2}} C^{\alpha^2+2} \\ &= B^{\mu_0} C^{\alpha^2+2}. \end{aligned}$$

Applying θ to the second and fifth terms of the right hand side above and then inverting, gives

$$A^{-1} C^{\alpha^2+2} A^{\alpha(1+\alpha+\cdots+\alpha^{\alpha^2-1})} = C^{\alpha^2+2} A^{-\mu_0},$$

so

$$B^{\mu_0} C^{\alpha^2+2} = C^{\alpha^2+2} A^{-\mu_0}.$$

Let α_0 be the inverse of α modulo the order of A. We then have

$$B^{\mu_0} = C^{\alpha^2+2} A^{-\mu_0} C^{-(\alpha^2+2)} = A^{-\mu_0 \alpha_0^{\alpha^2+2}}.$$

Conjugating this central element by C^{α^2+2} yields $B^{\mu_0} = A^{-\mu_0}$. Conjugating $A^{\mu_0} \in Z(G)$ by C and $B^{\mu_0} \in Z(G)$ by C^{-1}, we derive $A^{\mu_0(\alpha-1)} = 1 = B^{\mu_0(\alpha-1)}$. □

Recall equation (2.11).

Definition 3.10. *We refer to α as 3-admissible if one of the following 3 possibilities occurs: $v_3(\alpha-1)=0$; $v_3(\alpha-1)>1$; $v_3(\alpha-1)=1$ and $(\alpha-1)/3\equiv 1 \mod 3$.*

Theorem 3.11. *The Macdonald group $G(\alpha)$ is nilpotent of class at most 7.*

Proof. As indicated in [1, Section 5], we may assume that $\alpha>1$ and we make this assumption. Set

$$f(\alpha)=\begin{cases}(\alpha-1)^2, & \text{if } 2\nmid(\alpha-1) \text{ and } \alpha \text{ is 3-admissible},\\ (\alpha-1)^2/2, & \text{if } 2|(\alpha-1) \text{ and } \alpha \text{ is 3-admissible},\\ 3(\alpha-1)^2, & \text{if } 2\nmid(\alpha-1) \text{ and } \alpha \text{ is not 3-admissible},\\ 3(\alpha-1)^2/2, & \text{if } 2|(\alpha-1) \text{ and } \alpha \text{ is not 3-admissible}.\end{cases}$$

We claim that $A^{f(\alpha)}B^{f(\alpha)}=1$. To see the claim, we will repeatedly and implicitly use the fact that $|G(\alpha)|$ and $\alpha-1$ share the same prime factors (Proposition 2.14). Now, if α is 3-admissible then $A^{f(\alpha)}B^{f(\alpha)}=1$ by (2.11) and Proposition 3.1. Suppose next α is not 3-admissible, so that $\alpha=1+3k$, $k\in\mathbb{N}$, and $k\equiv -1 \mod 3$. If $k=-1+3u$, $u\in\mathbb{N}$, and $3\nmid u$, then $A^{f(\alpha)}B^{f(\alpha)}=1$ by (2.11) and Proposition 3.1. Assume next $k\equiv -1 \mod 9$. If $2\nmid(\alpha-1)$ then $A^{f(\alpha)}B^{f(\alpha)}=1$ by Propositions 3.4 and 3.5. Assume finally that $2|(\alpha-1)$. Then $A^{3^s(\alpha-1)^2/2}B^{3^s(\alpha-1)^2/2}=1$, $s\in\mathbb{N}$, by (2.11) and Proposition 3.1, and $A^{3(\alpha-1)^2 2^t}B^{3(\alpha-1)^2 2^t}=1$, $t\geq 0$, by Propositions 3.4 and 3.5. Since all factors are in $Z(G)$ and $\gcd(3^s(\alpha-1)^2/2, 3(\alpha-1)^2 2^t)=3(\alpha-1)^2/2$, it follows that $A^{f(\alpha)}B^{f(\alpha)}=1$ also in this case. This proves the claim. In particular, $A^{f(\alpha)}, B^{f(\alpha)}\in Z(G)$, so conjugating $A^{f(\alpha)}\in Z(G)$ by C and $B^{f(\alpha)}\in Z(G)$ by C^{-1}, we obtain $A^{(\alpha-1)f(\alpha)}=1=B^{(\alpha-1)f(\alpha)}$.

A careful calculation reveals that $\alpha^{f(\alpha)/(\alpha-1)}\equiv 1 \mod f(\alpha)$, so $C^{f(\alpha)/(\alpha-1)}\in Z_2(G)$. Next set

$$g(\alpha)=\begin{cases}\alpha-1, & \text{if } 2\nmid(\alpha-1),\\ (\alpha-1)/2, & \text{if } 2\mid(\alpha-1),\end{cases} \qquad \text{and} \qquad h(\alpha)=f(\alpha)/g(\alpha).$$

Another careful calculation shows that $1+\alpha+\cdots+\alpha^{h(\alpha)-1}\equiv h(\alpha) \mod f(\alpha)$, which implies

$$\alpha(1+\alpha+\cdots+\alpha^{h(\alpha)-1})\equiv \alpha h(\alpha)\equiv h(\alpha) \mod f(\alpha). \tag{3.12}$$

We have

$$(A^{h(\alpha)})^B=(A^B)^{h(\alpha)}=(AC)^{h(\alpha)}=C^{h(\alpha)}A^{\alpha(1+\alpha+\cdots+\alpha^{h(\alpha)-1})}.$$

Here $C^{h(\alpha)}\in Z_2(G)$, as $C^{f(\alpha)/(\alpha-1)}\in Z_2(G)$, and $A^{\alpha(1+\alpha+\cdots+\alpha^{h(\alpha)-1})}\equiv A^{h(\alpha)} \mod Z(G)$ by (3.12). It follows that $A^{h(\alpha)}\in Z_3(G)$, and applying θ we deduce $B^{h(\alpha)}\in Z_3(G)$.

Suppose first that α is 3-admissible. Then $h(\alpha) = \alpha - 1$. Since $A^C = A^{\alpha-1}A$ and ${}^CB = B^{\alpha-1}B$, with $A^{\alpha-1}, B^{\alpha-1} \in Z_3(G)$, we infer $C \in Z_4(G)$, whence $Z_5(G) = G$.

Suppose next that α is not 3-admissible. Then $h(\alpha) = 3(\alpha - 1)$. Moreover, $3|(\alpha - 1)$, so $\alpha^3 \equiv 1 \mod 3(\alpha - 1)$, whence $C^3 \in Z_4(G)$. We claim that $A^3 \in Z_5(G)$. Indeed, we have

$$(A^3)^B = (A^B)^3 = (AC)^3 = C^3 A^{\alpha(1+\alpha+\alpha^2)}, \tag{3.13}$$

where $C^3 \in Z_4(G)$. Moreover, we have $\alpha = 1 + 3k$, with $k \in \mathbb{Z}$, which readily gives $1 + \alpha + \alpha^2 \equiv 3 \mod 9$, and therefore $\alpha(1 + \alpha + \alpha^2) \equiv 3 \mod 9$. Moreover, $\alpha = 1 + 3k$ also implies $\alpha \equiv 1 \mod k$, so $\alpha(1 + \alpha + \alpha^2) \equiv 3 \mod k$. As $\gcd(3, k) = 1$, it follows that $\alpha(1 + \alpha + \alpha^2) \equiv 3 \mod 9k$, that is, $\alpha(1 + \alpha + \alpha^2) \equiv 3 \mod 3(\alpha - 1)$. But $A^{3(\alpha-1)} \in Z_3(G)$, so (3.13) implies $A^3 \in Z_5(G)$, as claimed. Applying θ, we deduce $B^3 \in Z_5(G)$. Since $A^C = A^{\alpha-1}A$ and ${}^CB = B^{\alpha-1}B$, with $A^{\alpha-1}, B^{\alpha-1} \in Z_5(G)$ and $3|(\alpha-1)$, we infer $C \in Z_6(G)$, whence $Z_7(G) = G$. □

3.3 More valuation calculations

We adopt the following conventions for the remainder of the document: $p \in \mathbb{N}$ stands for a prime factor of $\alpha - 1$, $m = v_p(\alpha - 1)$, and $J = J(\alpha)$ is the Sylow p-subgroup of $G(\alpha)$. By Case 1 we mean that either $p > 3$ or else $p = 3$, where $m > 1$ or $(\alpha - 1)/3 \equiv 1 \mod 3$. By Case 2 we understand that $p = 2$. By Case 3 we signify that $p = 3$, $m = 1$, and $(\alpha - 1)/3 \equiv -1 \mod 3$.

Proposition 3.14. *Suppose $\alpha < 0$, $\alpha \neq -2$. Then*

$$v_p(\xi) = \begin{cases} 2m, & \text{in Case 1,} \\ 2m - 1, & \text{in Case 2,} \\ 3, & \text{if } p = 3, \alpha = 1 + 3k, k = -1 + 3u, \text{ and } \gcd(3, u) = 1. \end{cases} \tag{3.15}$$

Proof. If $\alpha = -1$ then $\xi = 2$ and the result holds. Suppose henceforth that $\alpha \neq -1$. Then $\alpha \leq -3$, so $(-\alpha)^{-\alpha} > 2 - \alpha$, whence $\xi \neq 0$.

We have

$$\xi = 2 + \alpha + \cdots + \alpha^{-\alpha-1} = 1 + \frac{\alpha^{-\alpha} - 1}{\alpha - 1} = \frac{\alpha - 1 + \alpha^{-\alpha} - 1}{\alpha - 1},$$

where

$$\alpha^{-\alpha} = (1+(\alpha-1))^{-\alpha} = 1+(-\alpha)(\alpha-1)+\binom{-\alpha}{2}(\alpha-1)^2+\binom{-\alpha}{3}(\alpha-1)^3+\binom{-\alpha}{4}(\alpha-1)^4+\cdots,$$

so

$$\alpha-1+\alpha^{-\alpha}-1=\alpha-1+(-\alpha)(\alpha-1)+\binom{-\alpha}{2}(\alpha-1)^2+\binom{-\alpha}{3}(\alpha-1)^3+\binom{-\alpha}{4}(\alpha-1)^4+\cdots,$$

and therefore

$$\xi=[-1+\binom{-\alpha}{2}](\alpha-1)+\binom{-\alpha}{3}(\alpha-1)^2+\binom{-\alpha}{4}(\alpha-1)^3+\cdots. \tag{3.16}$$

Suppose first we are in Case 1. Write (3.16) in the form

$$\xi=-\frac{[(\alpha-1)(\alpha+2)-1](\alpha+2)(\alpha-1)^2}{6}+\binom{-\alpha}{4}(\alpha-1)^3+\cdots$$

This yields (3.15) when $p\neq 3$. Suppose next $p=3$, so that $\alpha=1+3^m k$, where $k\in\mathbb{Z}$ and $3\nmid k$. Then $\alpha+2=3(3^{m-1}k+1)$ and, by hypothesis, either $m>1$ or else $m=1$ and $k\equiv 1$ mod 3. In both cases $v_3(\alpha+2)=1$, which completes the proof of (3.15) in Case 1.

Suppose next that $p=2$. We see that (3.15) holds by writing (3.16) in the form

$$\xi=\frac{(\alpha+2)(\alpha-1)^2}{2}+\binom{-\alpha}{3}(\alpha-1)^2+\binom{-\alpha}{4}(\alpha-1)^3+\cdots.$$

Suppose finally that $p=3$, $\alpha=1+3k$, $k=-1+3u$, and $\gcd(3,u)=1$. Write (3.16) in the form

$$\begin{aligned}\xi&=\frac{[3-\alpha(\alpha+1)](\alpha+2)(\alpha-1)^2}{6}+\binom{-\alpha}{4}(\alpha-1)^3+\binom{-\alpha}{5}(\alpha-1)^4+\cdots\\&=\frac{(4[3-\alpha(\alpha+1)]+\alpha(\alpha+1)(\alpha+3)(\alpha-1))}{8}(1+k)(\alpha-1)^2+\binom{-\alpha}{5}(\alpha-1)^4+\cdots.\end{aligned}$$

As $v_3(k+1)=1$, this proves (3.15) in this case. □

Recall equation (2.12). Conjugating the central elements A^ξ and B^ξ by C and C^{-1}, respectively, we obtain

$$A^{(\alpha-1)\xi}=1=B^{(\alpha-1)\xi},\quad \alpha<0. \tag{3.17}$$

Chapter 4

Structure of the Sylow p-subgroup, J, of G

4.1 A presentation of J

Proposition 4.1. *Let T be a group with presentation $\langle X \mid R \rangle$, and let $\pi : F \to T$ be a corresponding epimorphism with kernel $\overline{R}$, the normal closure of R in a free group F on X. Let $\sigma : T \to U$ be a group epimorphism, and let V be any subset of F such that $\langle V \rangle^\pi = \ker(\sigma)$. Then U has presentation $\langle X \mid R \cup V \rangle$.*

Proof. Notice that $\ker(\pi\sigma)$ is the preimage of $\ker(\sigma)$ under π. As $\ker(\sigma) = \langle V \rangle^\pi$ and $\ker(\pi) = \overline{R}$, it follows that $\ker(\pi\sigma) = \overline{R}\langle V \rangle = \overline{R \cup V}$. □

Corollary 4.2. *Let T be a finite nilpotent group with presentation $\langle X \mid R \rangle$, and let $\pi : F \to T$ be a corresponding epimorphism with kernel $\overline{R}$, the normal closure of R in a free group F on X. Let $p \in \mathbb{N}$ be a prime, and let P be the Sylow p-subgroup of T. For $x \in X$, let n_x be any natural number such that $x^{n_x} \in \overline{R}$, that is $(x^\pi)^{n_x} = 1$, and set $m_x = v_p(n_x)$. Then P has presentation $\langle X \mid R \cup V \rangle$, where $V = \{x^{p^{m_x}} \mid x \in X\}$.*

Proof. As T is a finite nilpotent group, we have $T = P \times Q$, where Q is the direct product of all other Sylow subgroups of T. Let $\sigma : T \to P$ and $\tau : T \to Q$ be projections corresponding to the decomposition $T = P \times Q$. Then $\langle V \rangle^\pi = Q = \ker(\sigma)$, so Proposition 4.1 applies. □

We next apply Corollary 4.2 when $T = G$ has presentation $\langle\, x, y \mid x^{[x,y]} = x^\alpha,\ y^{[y,x]} = y^\alpha \,\rangle$.

Theorem 4.3. *The Sylow p-subgroup J of G has presentation*

$$\langle\, x, y \mid x^{[x,y]} = x^{\alpha},\ y^{[y,x]} = y^{\alpha},\ x^{p^{3m}} = 1,\ y^{p^{3m}} = 1 \,\rangle \text{ in Case 1,} \tag{4.4}$$

$$\langle\, x, y \mid x^{[x,y]} = x^{\alpha},\ y^{[y,x]} = y^{\alpha},\ x^{2^{3m-1}} = 1,\ y^{2^{3m-1}} = 1 \,\rangle \text{ in Case 2,} \tag{4.5}$$

$$\langle\, x, y \mid x^{[x,y]} = x^{\alpha},\ y^{[y,x]} = y^{\alpha},\ x^{81} = 1,\ y^{81} = 1 \,\rangle \text{ in Case 3.} \tag{4.6}$$

Proof. Suppose first we are in Case 1, Case 2, or else Case 3 with $\alpha = 1 + 3k$, $k = -1 + 3u$, and $\gcd(3, u) = 1$. If $\alpha > 0$ the result follows from (2.11), Proposition 3.1, and Corollary 4.2. If $\alpha < 0$ the result follows from (3.17), Proposition 3.14, and Corollary 4.2.

Suppose next we are in Case 3, with $\alpha = 1 + 3k$, $k = -1 + 9v$, and $v \in \mathbb{Z}$. The result then follows from Proposition 3.4, Proposition 3.5, and Corollary 4.2. □

The given presentations make it obvious that the isomorphism type of $J(\alpha)$ is invariant within the congruence class of α modulo p^{3m} for (4.4), modulo 2^{3m-1} for (4.5), and modulo 81 for (4.6). We may thus assume without loss that $\alpha > 0$ and we make this assumption for the remainder of the document.

4.2 An upper bound for the order of J

We see from Theorem 4.3 that J is generated by elements A and B subject to the defining relations $A^{[A,B]} = A^{\alpha}$, $B^{[B,A]} = B^{\alpha}$, as well as $A^{p^{3m}} = 1 = B^{p^{3m}}$ in Case 1, $A^{2^{3m-1}} = 1 = B^{2^{3m-1}}$ in Case 2, and $A^{81} = 1 = B^{81}$ in Case 3. We also have the additional relations $A^{p^{2m}} B^{p^{2m}} = 1$ in Case 1 and $A^{2^{2m-1}} B^{2^{2m-1}} = 1$ in Case 2, due to (2.11) and Proposition 3.1, as well as $A^{27} B^{27} = 1$ in Case 3, due to Propositions 3.4 and 3.5. In any case, we set $C = [A, B]$. We proceed to derive further relations amongst A, B, and C, as well as additional properties of J.

The defining relations of J ensure the existence of an automorphism $A \leftrightarrow B$, $C \leftrightarrow C^{-1}$, of J. Alternatively, use the fact that J is a characteristic subgroup of G.

Lemma 4.7. *Let T be a group generated by elements X, Y, Z of finite order satisfying:*

$$X^Z = X^u,\ Y^Z = Y^v \text{ for some integers } u, v;\ X^Y \in \langle X, Z\rangle;\ Y^X \in \langle Y, Z\rangle.$$

Then T is the product of the subgroups $\langle X\rangle, \langle Y\rangle, \langle Z\rangle$ in any of the six possible orderings. In particular, T is a finite group whose order is a factor of $|X||Y||Z|$.

Proof. As Z normalizes $\langle X\rangle$ and $\langle Y\rangle$, we have

$$\langle X, Z\rangle = \langle X\rangle\langle Z\rangle = \langle Z\rangle\langle X\rangle,\ \langle Y, Z\rangle = \langle Y\rangle\langle Z\rangle = \langle Z\rangle\langle Y\rangle.$$

By hypothesis, conjugation by Y sends $\langle X\rangle$ into $\langle X\rangle\langle Z\rangle$; as conjugation by Y preserves $\langle Z\rangle\langle Y\rangle$, we see that conjugation by Y preserves $\langle X\rangle\langle Z\rangle\langle Y\rangle$. Thus $Y^{-i}\langle X\rangle\langle Z\rangle\langle Y\rangle Y^i \subseteq \langle X\rangle\langle Z\rangle\langle Y\rangle$ for any $i \in \mathbb{Z}$, which implies $\langle Y\rangle\langle X\rangle\langle Z\rangle\langle Y\rangle \subseteq \langle X\rangle\langle Z\rangle\langle Y\rangle$. As the reverse inclusion is clear, we have $\langle Y\rangle\langle X\rangle\langle Z\rangle\langle Y\rangle = \langle X\rangle\langle Z\rangle\langle Y\rangle$. This shows that $\langle X\rangle\langle Z\rangle\langle Y\rangle$ is closed under multiplication. As $\langle X\rangle\langle Z\rangle\langle Y\rangle$ is a finite subset of T, it is a subgroup of T. Since $\langle X\rangle\langle Z\rangle\langle Y\rangle$ contains X, Y and Z, we infer $T = \langle X\rangle\langle Z\rangle\langle Y\rangle$.

Our hypotheses ensure that the roles of X and Y are interchangeable in the above argument, so T is the product of $\langle X\rangle, \langle Z\rangle, \langle Y\rangle$ in any order. Since the order of $\langle X, Z\rangle = \langle X\rangle\langle Z\rangle$ is a factor of $|X||Z|$, it follows that $|T|$ is a factor of $|X||Z||Y|$. □

Lemma 4.8. *Let a, b, k be integers such that $a \geq 1$ and $b \geq 0$, and suppose that p is odd. Then there is an integer t such that*

$$(1 + kp^a)^{p^b} = 1 + kp^{a+b} + ktp^{2a+b}.$$

Proof. This follows easily by induction on b. □

Lemma 4.9. *Let a, b, k be integers with $a, b \geq 1$. Then there is an integer t such that*

$$(1 + k2^a)^{2^b} = 1 + k2^{a+b} + k^2 2^{2a+b-1} + kt2^{2a+b}.$$

Proof. This follows easily by induction on b. □

Proposition 4.10. *Every element of J can be written in the form $A^i B^j C^k$, where $0 \leq i < i_0$, $0 \leq j < j_0$, $0 \leq k < k_0$, and $(i_0, j_0, k_0) = (p^{3m}, p^{2m}, p^{2m})$ in Case 1, in which case $A^{p^{3m}} = B^{p^{3m}} = C^{p^{2m}} = A^{p^{2m}} B^{p^{2m}} = 1$ and $|J| \leq p^{7m}$, $(i_0, j_0, k_0) = (2^{3m-1}, 2^{2m-1}, 2^{2m-1})$ in Case 2, in which case $A^{2^{3m-2}} = C^{2^{2m-1}} = B^{2^{3m-2}}$, $A^{2^{3m-1}} = B^{2^{3m-1}} = C^{2^{2m}} = A^{2^{2m-1}} B^{2^{2m-1}} = 1$, and $|J| \leq 2^{7m-3}$, and $(i_0, j_0, k_0) = (81, 27, 27)$ in Case 3, in which case $A^{81} = B^{81} = C^{27} = A^{27} B^{27} = 1$ and $|J| \leq 3^{10}$.*

Proof. Suppose first we are in Case 1. Then $A^{p^{2m}} B^{p^{2m}} = 1$, so $A^{p^{2m}} \in Z(J)$. Therefore,

$$A^{p^{2m}} = (A^{p^{2m}})^B = (A^B)^{p^{2m}} = (AC)^{p^{2m}} = C^{p^{2m}} A^{\alpha(1+\alpha+\cdots+\alpha^{p^{2m}-1})}.$$

Using Lemma 4.8 with $\alpha = 1 + kp^m$ and $b = 2m$, we see that $(\alpha^{p^{2m}} - 1)/(\alpha - 1) \equiv p^{2m} \bmod p^{3m}$, so $\alpha(\alpha^{p^{2m}} - 1)/(\alpha - 1) \equiv p^{2m} \bmod p^{3m}$, and $C^{p^{2m}} = 1$. The result now follows from Lemma 4.7.

Suppose next we are in Case 2. Then $A^{2^{2m-1}}B^{2^{2m-1}} = 1$, so $A^{2^{2m-1}} \in Z(J)$. Therefore,

$$A^{2^{2m-1}} = (A^{2^{2m-1}})^B = (A^B)^{2^{2m-1}} = (AC)^{2^{2m-1}} = C^{2^{2m-1}}A^{\alpha(1+\alpha+\cdots+\alpha^{2^{2m-1}-1})}.$$

Using Lemma 4.9 with $\alpha = 1 + k2^m$, with k odd, and $b = 2m-1$, we see that

$$(\alpha^{2^{2m-1}} - 1)/(\alpha - 1) \equiv 2^{2m-1} + 2^{3m-2} \mod 2^{3m-1},$$

whence $\alpha(\alpha^{2^{2m-1}} - 1)/(\alpha - 1) \equiv 2^{2m-1} + 2^{3m-2} \mod 2^{3m-1}$, so $C^{2^{2m-1}}A^{2^{3m-2}} = 1$. As $A^{2^{3m-2}}$ is its own inverse, it is equal to both $C^{2^{2m-1}}$ and $B^{2^{3m-2}}$, so $C^{2^{2m}} = 1$. The result now follows from Lemma 4.7.

Suppose finally we are in Case 3. Then $A^{27}B^{27} = 1$, so $A^{27} \in Z(J)$. Therefore,

$$A^{27} = (A^{27})^B = (A^B)^{27} = (AC)^{27} = C^{27}A^{\alpha(1+\alpha+\cdots+\alpha^{26})}.$$

Using Lemma 4.8 with $\alpha = 1 + 3k$ and $b = 3$, we see that $(\alpha^{27} - 1)/(\alpha - 1) \equiv 27 \mod 81$, which implies $\alpha(\alpha^{27} - 1)/(\alpha - 1) \equiv 27 \mod 81$, whence $C^{27} = 1$. The result now follows from Lemma 4.7. □

4.3 Order and basic properties of J

Definition 4.11. *By a* model *of J we understand a group T that is an image of J and whose order attains the upper bound stated in Proposition 4.10, that is, $|T| = p^{7m}$ in Case 1, $|T| = 2^{7m-3}$ in Case 2, and $|T| = 3^{10}$ in Case 3.*

Theorem 4.12. *Suppose we are in Case 1, 2, or 3. Then there is a model of J.*

The proof of this theorem is very long and requires many calculations which can be found in the appendix in Section 4.7.

Theorem 4.13. *Every element of J can be written uniquely in the form*

$$A^iB^jC^k, \quad 0 \le i < i_0,\ 0 \le j < j_0,\ 0 \le k < k_0,$$

where

1. $(i_0, j_0, k_0) = (p^{3m}, p^{2m}, p^{2m})$ *in Case 1, in which case* $|J| = p^{7m}$,
2. $(i_0, j_0, k_0) = (2^{3m-1}, 2^{2m-1}, 2^{2m-1})$ *in Case 2, in which case* $|J| = 2^{7m-3}$,
3. $(i_0, j_0, k_0) = (81, 27, 27)$ *in Case 3, in which case* $|J| = 3^{10}$.

Proof. Immediate consequence of Proposition 4.10 and Theorem 4.12. □

In Proposition 4.14 below, the automorphism $A \leftrightarrow B$ of J yields the corresponding results when we interchange the roles of A and B.

Proposition 4.14.

1. *A and C have respective orders p^{3m} and p^{2m} in Case 1, 2^{3m-1} and 2^{2m} in Case 2, and 81 and 27 in Case 3. Moreover, $A^{2^{3m-2}} = C^{2^{2m-1}}$ has order 2 in Case 2.*

2. *In Case 1, $\langle A, C\rangle = \langle A\rangle \rtimes \langle C\rangle$ has order p^{5m}. In Case 2, $\langle A\rangle \cap \langle C\rangle = \langle A^{2^{3m-2}}\rangle$ has order 2, and $\langle A, C\rangle$ has order 2^{5m-2}, with defining relations*

$$A^{2^{3m-1}} = 1,\ A^{2^{3m-2}} = C^{2^{2m-1}},\ A^C = A^\alpha.$$

   In Case 3, $\langle A, C\rangle = \langle A\rangle \rtimes \langle C\rangle$ has order 3^7.

3. *The group $\langle A\rangle \cap \langle B\rangle = \langle A, C\rangle \cap \langle B\rangle$ is equal to $\langle A^{p^{2m}}\rangle$ and has order p^m in Case 1, to $\langle A^{2^{2m-1}}\rangle$ and has order 2^m in Case 2, and to $\langle A^{27}\rangle$ and has order 3 in Case 3.*

Proof.

1. Proposition 4.10 and the uniqueness statement of Theorem 4.13 imply that A and C have the stated order.

2. Clearly $\langle C\rangle$ normalizes $\langle A\rangle$. Suppose first we are in Cases 1 or 3. That $\langle A\rangle \cap \langle C\rangle$ is trivial follows from part (a) and the uniqueness statement of Theorem 4.13. That $\langle A, C\rangle = \langle A\rangle \rtimes \langle C\rangle$ has order p^{5m} in Case 1 and order 3^7 in Case 3 follows from part (a). Suppose next we are in Case 2. That $\langle A\rangle \cap \langle C\rangle = \langle A^{2^{3m-2}}\rangle$ has order 2 follows from Proposition 4.10 and the uniqueness statement of Theorem 4.13. Thus, $\langle A, C\rangle = \langle A\rangle\langle C\rangle$ has order 2^{5m-2} and satisfies the stated relations. Any group generated by elements A and C satisfying the stated relations has order $\leq 2^{5m-2}$, so these are defining relations.

3. Proposition 4.10 and the uniqueness statement of Theorem 4.13 imply that $\langle A\rangle \cap \langle B\rangle$ is equal to $\langle A^{p^{2m}}\rangle$ in Case 1, to $\langle A^{2^{2m-1}}\rangle$ in Case 2, and to $\langle A^{27}\rangle$ in Case 3. We have $J = \langle A, C\rangle\langle B\rangle$ by Lemma 4.7, where $|J| = p^{7m}$, $|\langle A, C\rangle| = p^{5m}$, $|\langle B\rangle| = p^{3m}$ in Case 1, $|J| = 2^{7m-3}$, $|\langle A, C\rangle| = 2^{5m-2}$, $|\langle B\rangle| = 2^{3m-1}$ in Case 2, and $|J| = 3^{10}$, $|\langle A, C\rangle| = 3^7$, $|\langle B\rangle| = 3^4$ in Case 3. Thus, $\langle A, C\rangle \cap \langle B\rangle$ must have order p^m in Case 1, 2^m in Case 2, and 3 in Case 3, and is therefore equal to $\langle A\rangle \cap \langle B\rangle$. □

Proposition 4.15. *We have $C_J(A) = \langle A\rangle$ and $C_J(B) = \langle B\rangle$. Also $N_J(A) = \langle A, C\rangle$ and $N_J(B) = \langle B, C\rangle$.*

Proof. Let $x \in N_J(B)$. By Lemma 4.7, we have $x = B^j A^i C^k$ for some $i, j, k \in \mathbb{N}$ and $i \geq 2$. Then

$$B^s = B^x = B^{B^j A^i C^k} = B^{A^i C^k} = (BA^{(\alpha-1)(\alpha+2\alpha^2+\cdots+(i-1)\alpha^{i-1})}C^{-i})^{C^k},$$

for some $s \in \mathbb{N}$, so

$$B^s = B^{\beta^k} A^{(\alpha-1)(\alpha+2\alpha^2+\cdots+(i-1)\alpha^{i-1})\alpha^k} C^{-i},$$

where β is the inverse of α modulo the order of B. Therefore

$$B^{s-\beta^k} = A^{(\alpha-1)(\alpha+2\alpha^2+\cdots+(i-1)\alpha^{i-1})\alpha^k} C^{-i}$$

is in $\langle A, C\rangle \cap \langle B\rangle$, which equals $\langle A\rangle \cap \langle B\rangle$ by Proposition 4.14. Thus C^{-i} is in $\langle A\rangle \cap \langle C\rangle$.

Suppose first we are in Case 1. Then $\langle A\rangle \cap \langle C\rangle$ is trivial and hence $i \equiv 0 \mod p^{2m}$ by Proposition 4.14. As $A^{p^{2m}} B^{p^{2m}} = 1$, we infer $x = B^\ell C^k$, $\ell \in \mathbb{N}$, which proves that $N_J(B) = \langle B, C\rangle$.

Suppose next we are in Case 2. Then $\langle A\rangle \cap \langle C\rangle = \langle C^{2^{2m-1}}\rangle$ and hence $i \equiv 0 \mod 2^{2m-1}$ by Proposition 4.14. As $A^{2^{2m-1}} B^{2^{2m-1}} = 1$, we deduce $x = B^\ell C^k$, $\ell \in \mathbb{N}$, so $N_J(B) = \langle B, C\rangle$.

Suppose finally we are in Case 3. Then $\langle A\rangle \cap \langle C\rangle$ is trivial and hence $i \equiv 0 \mod 27$ by Proposition 4.14. As $A^{27} B^{27} = 1$, it follows that $x = B^\ell C^k$, $\ell \in \mathbb{N}$, and $N_J(B) = \langle B, C\rangle$.

The automorphism $A \leftrightarrow B$ now yields $N_J(A) = \langle A, C\rangle$.

Assume now that $x \in C_J(B)$. By the above, $x = B^\ell C^k$, where $k, \ell \in \mathbb{N}$, so $C^k \in C_J(B)$.

Suppose first we are in Case 1. Then $\alpha^k \equiv 1 \mod p^{3m}$. It follows from Lemma 4.8 that the order of α modulo p^{3m} is p^{2m}, so $k \equiv 0 \mod p^{2m}$, whence $x \in \langle B\rangle$.

Suppose next we are in Case 2. Then $\alpha^k \equiv 1 \mod 2^{3m-1}$. By Lemma 4.9, the order of α modulo 2^{3m-1} is 2^{2m-1}, so $k \equiv 0 \mod 2^{2m-1}$. As $C^{2^{2m-1}} = B^{2^{3m-2}}$, we infer $x \in \langle B\rangle$.

Suppose finally we are in Case 3. Then $\alpha^k \equiv 1 \mod 81$. We deduce from Lemma 4.8 that the order of α modulo 81 is 27, and therefore $k \equiv 0 \mod 27$, so $x \in \langle B\rangle$.

Thus $C_J(B) = \langle B\rangle$ in all cases.

The automorphism $A \leftrightarrow B$ now yields $C_J(A) = \langle A\rangle$. □

4.4 Upper and lower central series of J

The next two results describe the upper and lower central series of J in all cases.

Theorem 4.16.

1. *In Case 1, the nilpotency class of J is 5, and*

$$Z_1(J) = \langle A^{p^{2m}} \rangle,\ Z_2(J) = \langle A^{p^{2m}}, C^{p^m} \rangle,\ Z_3(J) = \langle A^{p^m}, B^{p^m}, C^{p^m} \rangle,$$

$$Z_4(J) = \langle A^{p^m}, B^{p^m}, C \rangle.$$

2. *In Case 2, if $m > 1$, the nilpotency class of J is 5, and*

$$Z_1(J) = \langle A^{2^{2m-1}} \rangle,\ Z_2(J) = \langle A^{2^{2m-1}}, C^{2^{m-1}} \rangle,\ Z_3(J) = \langle A^{2^m}, B^{2^m}, C^{2^{m-1}} \rangle,$$

$$Z_4(J) = \langle A^{2^{m-1}}, B^{2^{m-1}}, C \rangle.$$

3. *In Case 3, the nilpotency class of J is 7, and*

$$Z_1(J) = \langle A^{27} \rangle,\ Z_2(J) = \langle A^{27}, C^9 \rangle,\ Z_3(J) = \langle A^9, B^9, C^9 \rangle,$$

$$Z_4(J) = \langle A^9, B^9, C^3 \rangle,\ Z_5(J) = \langle A^3, B^3, C^3 \rangle,\ Z_6(J) = \langle A^3, B^3, C \rangle.$$

Moreover, in Cases 1 and 3, the terms of the upper and lower central series of J coincide, in reverse order, while in Case 2, if $m > 1$, we have

$$\gamma_2(J) = \langle A^{2^m}, B^{2^m}, C \rangle,\ \gamma_3(J) = \langle A^{2^m}, B^{2^m}, C^{2^m} \rangle,\ \gamma_4(J) = \langle A^{2^{2m}}, [A, B^{2^m}] \rangle,$$

$$\gamma_5(J) = \langle A^{2^{2m}} \rangle.$$

Proof. We have $Z(J) = C_J(A) \cap C_J(B) = \langle A \rangle \cap \langle B \rangle$ by Proposition 4.15. Here $\langle A \rangle \cap \langle B \rangle$ is equal to $\langle A^{p^{2m}} \rangle$ in Case 1, to $\langle A^{2^{2m-1}} \rangle$ in Case 2, and to $\langle A^{27} \rangle$ in Case 3, by Proposition 4.14.

Set $H = J/Z(J)$. Let $a, b, c \in H$ be the images of A, B, C under the canonical projection. Then $a^{p^{2m}} = b^{p^{2m}} = c^{p^{2m}} = 1$ in Case 1, $a^{2^{2m-1}} = b^{2^{2m-1}} = c^{2^{2m-1}} = 1$ in Case 2, and $a^{27} = b^{27} = c^{27} = 1$ in Case 3. Moreover, by Proposition 4.14, the order of H is p^{6m} in Case 1, 2^{6m-3} in Case 2, and 3^9 in Case 3. Furthermore, by Lemma 4.7, every element of H can be written as a product of elements from $\langle a \rangle, \langle b \rangle$, and $\langle c \rangle$, in any fixed order. This implies uniqueness of expression and that the given upper bounds for the orders of a, b, c are the actual orders of these elements.

We claim that $C_H(b)$ is equal to $\langle b, c^{p^m} \rangle$ in Case 1, $\langle b, c^{2^{m-1}} \rangle$ in Case 2, and $\langle b, c^9 \rangle$ in Case 3. Indeed, let $x \in C_H(b)$. Then $x = b^j a^i c^k$ for some $i, j, k \in \mathbb{N}$ with $i \geq 2$. The same argument used in the proof of Proposition 4.15 now yields $i \equiv 0 \mod p^{2m}$ in Case 1, $i \equiv 0 \mod 2^{2m-1}$ in Case 2, and $i \equiv 0 \mod 27$ in Case 3, so $x = b^j c^k$, which now implies $\alpha^k \equiv 1 \mod p^{2m}$ in

Case 1, $\alpha^k \equiv 1 \mod 2^{2m-1}$ in Case 2, and $\alpha^k \equiv 1 \mod 27$ in Case 3. In Case 1 the order of α modulo p^{2m} is p^m, in Case 2 the order of α modulo 2^{2m-1} is 2^{m-1}, and in Case 3 the order of α modulo 27 is 9, by Lemmas 4.8 and 4.9. So $k \equiv 0 \mod p^m$ in Case 1, $k \equiv 0 \mod 2^{m-1}$ in Case 2, and $k \equiv 0 \mod 9$ in Case 3, and therefore x is in $\langle b, c^{p^m} \rangle$ in Case 1, $\langle b, c^{2^{m-1}} \rangle$ in Case 2, and $\langle b, c^9 \rangle$ in Case 3. This proves one inclusion in every case. By the above, $\alpha^{p^m} \equiv 1 \mod p^{2m}$ in Case 1, $\alpha^{2^{m-1}} \equiv 1 \mod 2^{2m-1}$ in Case 2, and $\alpha^9 \equiv 1 \mod 27$, so the reverse inclusion is clear, which proves the claim. The automorphism $a \leftrightarrow b$ of H now yields that $C_H(a)$ is equal to $\langle a, c^{p^m} \rangle$ in Case 1, $\langle a, c^{2^{m-1}} \rangle$ in Case 2, and $\langle a, c^9 \rangle$ in Case 3. Thus $Z(H)$ is equal to $\langle a, c^{p^m} \rangle \cap \langle b, c^{p^m} \rangle$ in Case 1, $\langle a, c^{2^{m-1}} \rangle \cap \langle b, c^{2^{m-1}} \rangle$ in Case 2, and $\langle a, c^9 \rangle \cap \langle b, c^9 \rangle$ in Case 3. The normal form of the elements of H forces this intersection to be $\langle c^{p^m} \rangle$ in Case 1, $\langle c^{2^{m-1}} \rangle$ in Case 2, and $\langle c^9 \rangle$ in Case 3. The preimage of this group under the canonical projection $J \to H$ is $\langle A^{p^{2m}}, C^{p^m} \rangle$ in Case 1, $\langle A^{2^{2m-1}}, C^{2^{m-1}} \rangle$ in Case 2, and $\langle A^{27}, C^9 \rangle$ in Case 3, which confirms the stated description of $Z_2(J)$ in all cases.

Next set $K = J/Z_2(J)$. Let $u, v, w \in K$ be the images of A, B, C under the canonical projection. Then $u^{p^{2m}} = v^{p^{2m}} = w^{p^m} = 1$ in Case 1, $u^{2^{2m-1}} = v^{2^{2m-1}} = w^{2^{m-1}} = 1$ in Case 2, and $u^{27} = v^{27} = w^9 = 1$ in Case 3. Moreover, by Proposition 4.14, the order of K is p^{5m} in Case 1, 2^{5m-3} in Case 2, and 3^8 in Case 3. Furthermore, by Lemma 4.7, every element of K can be written as a product of elements from $\langle u \rangle, \langle v \rangle$, and $\langle w \rangle$, in any fixed order. This implies uniqueness of expression and that the given upper bounds for the orders of u, v, w are the actual orders of these elements.

We claim that $C_K(v)$ is equal to $\langle v, u^{p^m} \rangle$ in Case 1, $\langle v, u^{2^m} \rangle$ in Case 2, and $\langle v, u^9 \rangle$ in Case 3. Indeed, let $x \in C_K(v)$. Then $x = v^j u^i w^k$ for some $i, j, k \in \mathbb{N}$ with $i \geq 2$. The same argument used in the proof of Proposition 4.15 now yields $i \equiv 0 \mod p^m$ in Case 1, $i \equiv 0 \mod 2^{m-1}$ in Case 2, and $i \equiv 0 \mod 9$ in Case 3. Moreover, in Case 2, we also obtain

$$(i-1)i/2 \equiv 1 + 2 + \cdots + i - 1 \equiv \alpha + 2\alpha^2 + \cdots + (i-1)\alpha^{i-1} \equiv 0 \mod 2^{m-1}.$$

We use for the first time that $m > 1$. As $i \equiv 0 \mod 2^{m-1}$, then i is even. Since $(i-1)i/2 \equiv 0 \mod 2^{m-1}$ and $i - 1$ is odd, we infer $i \equiv 0 \mod 2^m$. On the other hand, in Case 1, we have

$$(u^{p^m})^v = (u^v)^{p^m} = (uw)^{p^m} = w^{p^m} u^{\alpha(1+\alpha+\cdots+\alpha^{p^m-1})} = u^{p^m}$$

since $\alpha(\alpha^{p^m} - 1)/(\alpha - 1) \equiv p^m \mod p^{2m}$ by Lemma 4.8; in Case 2, we have

$$(u^{2^m})^v = (u^v)^{2^m} = (uw)^{2^m} = w^{2^m} u^{\alpha(1+\alpha+\cdots+\alpha^{2^m-1})} = u^{2^m},$$

since $\alpha(\alpha^{2^m} - 1)/(\alpha - 1) \equiv 2^m \mod 2^{2m-1}$ by Lemma 4.9; and in Case 3, we have

$$(u^9)^v = (u^v)^9 = (uw)^9 = w^9 u^{\alpha(1+\alpha+\cdots+\alpha^8)} = u^9$$

since $\alpha(\alpha^9-1)/(\alpha-1) \equiv 9 \mod 27$ by Lemma 4.8. Thus $C_K(v)$ contains u^{p^m} in Case 1, u^{2^m} in Case 2, and u^9 in Case 3. It follows that $w^k \in C_K(v)$ in all cases, which implies $\alpha^k \equiv 1 \mod p^{2m}$ in Case 1, $\alpha^k \equiv 1 \mod 2^{2m-1}$ in Case 2, and $\alpha^k \equiv 1 \mod 27$ in Case 3. Exactly as above, this implies $k \equiv 0 \mod p^m$ in Case 1, $k \equiv 0 \mod 2^{m-1}$ in Case 2, and $k \equiv 0 \mod 9$ in Case 3. This proves the claim. The automorphism $u \leftrightarrow v$ of K now yields that $C_K(u)$ is equal to $\langle u, v^{p^m} \rangle$ in Case 1, $\langle u, v^{2^m} \rangle$ in Case 2, and $\langle u, v^9 \rangle$ in Case 3. Thus $Z(H)$ is equal to $\langle u, v^{p^m} \rangle \cap \langle v, u^{p^m} \rangle$ in Case 1, $\langle u, v^{2^m} \rangle \cap \langle v, u^{2^{m-1}} \rangle$ in Case 2, and $\langle u, v^9 \rangle \cap \langle v, u^9 \rangle$ in Case 3. The normal form of the elements of K forces this intersection to be $\langle u^{p^m}, v^{p^m} \rangle$ in Case 1, $\langle u^{2^m}, v^{2^m} \rangle$ in Case 2, and $\langle u^9, v^9 \rangle$ in Case 3. The preimage of this group under the canonical projection $J \to K$ is $\langle A^{p^m}, B^{p^m}, C^{p^m} \rangle$ in Case 1, $\langle A^{2^{2m}}, B^{2^{2m}}, C^{2^{m-1}} \rangle$ in Case 2, and $\langle A^9, B^9, C^9 \rangle$ in Case 3, which confirms the stated description of $Z_3(J)$ in all cases.

Suppose next we are in Case 1, and let

$$M = \langle\, x, y, z \mid x^{p^m} = 1,\ y^{p^m} = 1,\ z^{p^m} = 1,\ [x,y] = z,\ [x,z] = 1,\ [y,z] = 1 \,\rangle \cong \mathrm{Heis}(\mathbb{Z}/p^m\mathbb{Z}).$$

Consider the assignment $A \mapsto x$, $B \mapsto y$. The defining relations of J are preserved, which yields a group epimorphism $f : J \to M$. As M has exponent p^m, we have $J^{p^m} \subseteq \ker(f)$. Recalling that $Z_3(J) = \langle A^{p^m}, B^{p^m}, C^{p^m} \rangle$, it follows that $Z_3(J) \subseteq J^{p^m}$. On the other hand, if $A^i B^j C^k \in \ker(f)$, then the normal form of the elements of M implies that all of i, j, k are multiples of p^m, so $\ker(f) \subseteq Z_3(J)$. This proves that $Z_3(J) = J^{p^m} = \ker(f)$, whence $J/Z_3(J) \cong M$. As $Z(M) = \langle z \rangle$, it follows that $Z_4(J) = \langle A^{p^m}, B^{p^m}, C \rangle$. Given that $C \in Z_4(J)$, we deduce $Z_5(J) = J$.

Suppose next we are in Case 2, and let

$$M = \langle\, x, y, z \mid x^{2^m} = 1,\ y^{2^m} = 1,\ z^{2^{m-1}} = 1,\ [x,y] = z,\ [x,z] = 1,\ [y,z] = 1 \,\rangle,$$

a quotient of the Heisenberg group over $\mathbb{Z}/2^m\mathbb{Z}$ by the 2^{m-1}th power of its center. Consider the assignment $A \mapsto x$, $B \mapsto y$. The defining relations of J are preserved, which yields a group epimorphism $f : J \to M$. Recalling that $Z_3(J) = \langle A^{2^m}, B^{2^m}, C^{2^{m-1}} \rangle$, we deduce $Z_3(J) \subseteq \ker(f)$. Moreover, if $A^i B^j C^k \in \ker(f)$, then the normal form of the elements of M implies that i, j are multiples of 2^m and k is a multiple of 2^{m-1}, which proves $Z_3(J) = \ker(f)$, whence $J/Z_3(J) \cong M$. As the nilpotency class of M is 2, that of J is 5. In fact, as $Z(M) = \langle x^{2^{m-1}}, y^{2^{m-1}}, z \rangle$, it follows that $Z_4(J) = \langle A^{2^{m-1}}, B^{2^{m-1}}, C \rangle$. Given that $C \in Z_4(J)$, we deduce $Z_5(J) = J$.

Suppose next we are in Case 3, and set $L = J/Z_3(J)$. As $|Z(K)| = 9$, we have $|L| = 3^6$. Repeating with L the analysis made with H, we find $|Z(L)| = 3$ and $Z_4(J) = \langle A^9, B^9, C^3 \rangle$.

Next set $T = J/Z_4(J)$. Since $|Z(L)| = 3$, we have $|T| = 3^5$. Mimicking with T the argument used with K, we find $|Z(T)| = 9$, $Z_5(J) = \langle A^3, B^3, C^3\rangle$, and $|J/Z_5(J)| = 3^3$. Let

$$M = \langle\, r, s, t \mid r^3 = 1,\ s^3 = 1,\ t^3 = 1,\ [r,s] = t,\ [r,t] = 1,\ [s,t] = 1 \,\rangle \cong \mathrm{Heis}(\mathbb{Z}/3\mathbb{Z}).$$

Then $A \mapsto r$, $B \mapsto s$ extends to an epimorphism $f : J \to M$. As M has exponent 3, we have $J^3 \subseteq \ker(f)$. But $Z_5(J) = \langle A^3, B^3, C^3\rangle$, so $Z_5(J) \subseteq J^3$. As $|J/Z_5(J)| = 3^3$, we infer $Z_5(J) = J^3 = \ker(f)$ and $J/Z_5(J) \cong M$. Since $Z(M) = \langle t\rangle$, it follows that $Z_6(J) = \langle A^3, B^3, C\rangle$. Given that $C \in Z_6(J)$, we deduce $Z_7(J) = J$.

It remains to show that the lower central series of J is as stated. We will make use of the formulas:

$$[A, B^i] = B^{(\alpha-1)(\alpha+2\alpha^2+\cdots+(i-1)\alpha^{i-1})}C^i,\ [B, A^i] = A^{(\alpha-1)(\alpha+2\alpha^2+\cdots+(i-1)\alpha^{i-1})}C^{-i},\ i \geq 2. \quad (4.17)$$

Suppose first we are Case 1 (resp. Case 3). Since $J = Z_5(J)$ (resp. $J = Z_7(J)$), we infer $\gamma_2(J) \subseteq Z_4(J)$ (resp. $\gamma_2(J) \subseteq Z_6(J)$). But $[A, B] = C$, $[A, C] = A^{\alpha-1}$, and $[B, C^{-1}] = B^{\alpha-1}$, so $A^{p^m}, B^{p^m}, C \in \gamma_2(J)$. Thus $Z_4(J) = \gamma_2(J)$ (resp. $Z_6(J) = \gamma_2(J)$). It follows that $\gamma_3(J) \subseteq Z_3(J)$ (resp. $\gamma_3(J) \subseteq Z_5(J)$). As above, $A^{p^m}, B^{p^m} \in \gamma_3(J)$. Due to (4.17), we see that $C^{p^m} \in \gamma_3(J)$, so $\gamma_3(J) = Z_3(J)$ (resp. $\gamma_3(J) = Z_5(J)$). This implies $\gamma_4(J) \subseteq Z_2(J)$ (resp. $\gamma_4(J) \subseteq Z_4(J)$). Making use of Lemma 4.8, we find that $v_p(\alpha^{p^m} - 1) = 2m$, which gives $A^{p^{2m}}, B^{p^{2m}} \in \gamma_4(J)$. As

$$\alpha + 2\alpha^2 + \cdots + (p^m - 1)\alpha^{p^m-1} \equiv 1 + 2 + \cdots + (p^m - 1) \equiv 0 \mod p^m,$$

the case $i = p^m$ of (4.17) ensures that $C^{p^m} \in \gamma_4(J)$, so $\gamma_4(J) = Z_2(J)$ (resp. $\gamma_4(J) = Z_4(J)$). We infer $\gamma_5(J) \subseteq Z(J)$ (resp. $\gamma_5(J) \subseteq Z_3(J)$). As above, $A^{p^{2m}}, B^{p^{2m}} \in \gamma_5(J)$, and the case $i = p^{2m}$ of (4.17) ensures that $C^{p^{2m}} \in \gamma_5(J)$. Thus $\gamma_5(J) = Z(J)$ (resp. $\gamma_5(J) = Z_3(J)$). This completes the proof in Case 1.

Suppose next we are in Case 3. From $\gamma_5(J) = Z_3(J)$, we infer $\gamma_6(J) \subseteq Z_2(J)$. As $v_3(\alpha^9 - 1) = 27$, we deduce $A^{27} \in \gamma_6(J)$. Since $\alpha \equiv -2 \mod 9$, we see that $\alpha + 2\alpha^2 + \cdots + 8\alpha^8 \equiv 0 \mod 9$. Thus (4.17) yields $C^9 \in \gamma_6(J)$, which implies $\gamma_6(J) = Z_2(J)$. Thus $\gamma_7(J) \subseteq Z(J)$, with $A^{27} \in \gamma_7(J)$ as above, so $\gamma_7(J) = Z(J)$. This completes the proof in Case 3.

Suppose finally we are in Case 2. For any $i \geq 1$, Theorem 2.2 implies that $\gamma_{i+1}(J)$ is the normal subgroup generated by the set of all possible brackets between $\{A, B\}$ and any fixed generating subset S_i of $\gamma_i(J)$. Taking $S_1 = \{A, B\}$, we find that $\gamma_2(J) = \langle A^{2^m}, B^{2^m}, C\rangle$, which is the normal closure of $\{C\}$. Alternatively, since $\langle A^{2^m}, B^{2^m}, C\rangle$ is a normal subgroup of J contained in $[J, J]$ with abelian quotient, it must be equal to it. In both cases, normality

follows from (4.17). Taking $S_2 = \{A^{2^m}, B^{2^m}, C\}$, we find that $\gamma_3(J) = \langle A^{2^m}, B^{2^m}, C^{2^m}\rangle$, where normality follows from (4.17) and Lemma 4.9. Taking $S_3 = \{A^{2^m}, B^{2^m}, C^{2^m}\}$, we find that $\gamma_4(J) = \langle A^{2^{2m}}, [A, B^{2^m}]\rangle$, where $[A, B^{2^m}] = B^{\ell 2^{2m-1}} C^{2^m}$, with ℓ odd, by (4.17). As $A^{2^{2m}}, B^{2^{2m-1}} \in Z(J)$ and $\langle A^{2^{2m}}\rangle = \langle B^{2^{2m}}\rangle$, the normality of $\langle A^{2^{2m}}, [A, B^{2^m}]\rangle$ is ensured, as well as the fact that $\gamma_5(J) = \langle A^{2^{2m}}\rangle$. □

Proposition 4.18. *Suppose $m = 1$ and $p = 2$. Then J is isomorphic to the generalized quaternion group*

$$Q_{16} = \langle\, u, v \mid u^4 = v^2,\ u^v = u^{-1} \,\rangle$$

of order 16, $Z(J) = \langle A^2\rangle = \gamma_3(J)$, $Z_2(J) = \langle A^2, C\rangle = \gamma_2(J)$, the nilpotency class of J is 3, and the exponent of J is 8.

Proof. The first part of the proof of Theorem 4.16 shows that $Z(J) = \langle A^2\rangle$ and $Z_2(J) = \langle A^2, C\rangle$. The latter is a subgroup of J of order 4 by Proposition 4.14 and $|J| = 16$ by Theorem 4.13, so $J/Z_2(J)$ is abelian and therefore $Z_3(J) = J$. Thus the nilpotency class of J is 3. From $Z_3(J) = J$ we deduce $\gamma_2(J) \subseteq Z_2(J)$. But $C, A^2 \in \gamma_2(J)$, so $\gamma_2(J) = Z_2(J)$. This implies $\gamma_3(J) \subseteq Z(J)$. As $A^2 \in \gamma_3(J)$, we infer $\gamma_3(J) = Z(J)$. Since $v_2(\alpha - 1) = 1$, Theorem 4.3 ensures that J has presentation

$$\langle\, A, B \mid A^{[A,B]} = A^{-1},\ B^{[B,A]} = B^{-1},\ A^4 = 1 = B^4 \,\rangle,$$

which, in accordance with the discussion following Theorem 4.3, is independent of α, as all integers of the form $1 + 2k$, with k odd, are congruent modulo 4. Set $D = AB$. Since $A^2 = B^2 = C^2$ by Proposition 4.10, we have $D^2 = ABAB = ABBAC = C$, so $D^4 = A^2$, and $D^A = BA = D^{-1}$. Thus J is an epimorphic image of the generalized quaternion group $Q_{16} = \langle\, u, v \mid u^4 = v^2,\ u^v = u^{-1} \,\rangle$ of order 16. As $|J| = 16$, we have $J \cong Q_{16}$. As the order of D is 8, this is the exponent of J. □

4.5 Exponent of J

Proposition 4.19. *Suppose we are in Case 1. Then $Z(J) = J^{p^{2m}}$, $Z_3(J) = J^{p^m}$ is abelian of order p^{4m} with presentation*

$$\langle\, X, Y, Z \mid XY = YX,\ YZ = ZY,\ XZ = ZX,\ X^{p^{2m}} = 1,\ X^{p^m} Y^{p^m} = 1,\ Z^{p^m} = 1 \,\rangle,$$

$J/Z_3(J) \cong \mathrm{Heis}(\mathbb{Z}/p^m\mathbb{Z})$, and J has exponent p^{3m}.

Proof. That $Z_3(J) = J^{p^m}$ was established in the proof of Theorem 4.16. Referring to the group $\langle X_0, Y_0\rangle$ constructed in Theorem 4.12, we have an isomorphism $J \to \langle X_0, Y_0\rangle$, defined by $A \mapsto X_0$, $B \mapsto Y_0$. Then $Z_3(J) = \langle A^{p^m}, B^{p^m}, C^{p^m}\rangle$ corresponds to $\langle X, Y, Z\rangle$, which gives the desired order and presentation of $Z_3(J)$. As $Z_3(J)$ is abelian, $A^{p^{2m}}B^{p^{2m}} = 1$, and $C^{p^{2m}} = 1$, we infer $J^{p^{2m}} = Z(J)$. The fact that $J/Z_3(J) \cong \mathrm{Heis}(\mathbb{Z}/p^m\mathbb{Z})$ was demonstrated in the proof of Theorem 4.16. Thus, there is an epimorphism $f : J \to \mathrm{Heis}(\mathbb{Z}/p^m\mathbb{Z})$, where $\ker(f) = Z_3(J) = J^{p^m}$ has exponent p^{2m}. Let $g \in J$. Then $g^{p^m} \in \ker(f)$, so $g^{p^{3m}} = 1$. Since A has order p^{3m} by Proposition 4.14, the result follows. □

Proposition 4.20. *Suppose we are in Case 2 and $m > 1$. Then $Z_3(J)$ is abelian of order 2^{4m-2}, with presentation*

$$\langle\, x, y, z \mid xy = yx,\ xz = zx,\ yz = zy,\ x^{2^{2m-2}} = z^{2^m},\ x^{2^{m-1}}y^{2^{m-1}} = 1,\ x^{2^{2m-1}} = 1\,\rangle,$$

$J/Z_3(J) \cong \mathrm{Heis}(\mathbb{Z}/2^m\mathbb{Z})/U$, where U is the 2^{m-1}th power of the center of $\mathrm{Heis}(\mathbb{Z}/2^m\mathbb{Z})$, and J has exponent 2^{3m-1}.

Proof. Referring to the group $\langle x_0, y_0\rangle$ constructed in the proof of Theorem 4.12, we have an isomorphism $J \to \langle x_0, y_0\rangle$ such that $A \mapsto x_0$ and $B \mapsto y_0$. Then $Z_3(J) = \langle A^{2^m}, B^{2^m}, C^{2^{m-1}}\rangle$ corresponds to $\langle x, y, z\rangle$, which gives the desired order and presentation of $Z_3(J)$. The fact that $J/Z_3(J) \cong \mathrm{Heis}(\mathbb{Z}/2^m\mathbb{Z})/U$ was demonstrated in the proof of Theorem 4.16. Thus, there is an epimorphism $f : J \to \mathrm{Heis}(\mathbb{Z}/2^m\mathbb{Z})/U$, where $\ker(f) = Z_3(J)$ has exponent 2^{2m-1}. A matrix calculation shows that $\mathrm{Heis}(\mathbb{Z}/2^m\mathbb{Z})$ has exponent 2^{m+1} and that $\mathrm{Heis}(\mathbb{Z}/2^m\mathbb{Z})/U$ has exponent 2^m. Let $g \in J$. Then $g^{2^m} \in \ker(f)$, so $g^{2^{3m-1}} = 1$. Since A has order 2^{3m-1} by Proposition 4.14, the result follows. □

Proposition 4.21. *Suppose we are in Case 3. Then*

1. *We have $Z_5(J) = \langle A^3, B^3, C^3\rangle = J^3$, where $J/Z_5(J) \cong \mathrm{Heis}(\mathbb{Z}/3\mathbb{Z})$*
2. *The group $Z_3(J) = \langle A^9, B^9, C^9\rangle = J^9$ is abelian of exponent 9, and $Z_5(J)/Z_3(J) \cong (\mathbb{Z}/3\mathbb{Z})^3$.*
3. *We have $Z(J) = \langle A^{27}\rangle = J^{27}$ and the exponent of J is equal to 81.*

Proof.

1. This was demonstrated in the proof of Theorem 4.16.

2. We already know that $Z_3(J) = \langle A^9, B^9, C^9 \rangle$ from Theorem 4.16. Clearly $\langle A^9, B^9, C^9 \rangle \subseteq J^9$. Referring to the group $\langle x_0, y_1 \rangle$ constructed in the proof of Theorem 4.12, we have an isomorphism $J \to \langle x_0, y_1 \rangle$ such that $A \mapsto x_0$ and $B \mapsto y_1$. Then $Z_3(J)$ corresponds to $\langle x^3, y, z^3 \rangle$ and $Z_5(J)$ corresponds to $\langle x, y_0, z \rangle$. The stated defining relations of $\langle x, y, z \rangle$ show that $\langle x, y, z^3 \rangle$ is abelian and its subgroup $\langle x^3, y, z^3 \rangle$ has exponent 9, while the stated defining relations of $\langle x, y_0, z \rangle$ prove that $Z_5(J)/Z_3(J)$ is abelian of exponent 3 and order 27, so $Z_5(J)/Z_3(J) \cong (\mathbb{Z}/3\mathbb{Z})^3$. This and part (a) yield $J^9 \subseteq \langle A^9, B^9, C^9 \rangle$.

3. That $Z(J) = J^{27}$ follows from $A^{27}B^{27} = 1$ and parts (a) and (b). As A has order 81, this is the exponent of J. □

4.6 Order, nilpotency class, and exponent of G

Recall that α is 3-admissible if one the following three possibilities occur: $3 \nmid (\alpha - 1)$; the multiplicity of 3 as a factor of $\alpha - 1$ is larger than 1; $3|(\alpha - 1)$ and $(\alpha - 1)/3 \equiv 1 \mod 3$.

Theorem 4.22. *The nilpotency class of the Macdonald group $G(\alpha)$ is equal to 3 if $\alpha \in \{-1, 3\}$; 5 if $\alpha \notin \{-1, 3\}$ and α is 3-admissible; and 7 if $3|(\alpha - 1)$ and $(\alpha - 1)/3 \equiv -1 \mod 3$. Moreover, the order and exponent of $G(\alpha)$ are respectively equal to $|\alpha - 1|^7$ and $|\alpha - 1|^3$ if $2 \nmid (\alpha - 1)$ and α is 3-admissible; $|\alpha - 1|^7/8$ and $|\alpha - 1|^3/2$ if $v_2(\alpha - 1) > 1$ and α is 3-admissible; $|\alpha - 1|^7/8$ and $|\alpha - 1|^3$ if $v_2(\alpha - 1) = 1$ and α is 3-admissible; $27|\alpha - 1|^7$ and $3|\alpha - 1|^3$ if $2 \nmid (\alpha - 1)$ and α is not 3-admissible; $27|\alpha - 1|^7/8$ and $3|\alpha - 1|^3/2$ if $v_2(\alpha - 1) > 1$ and α is not 3-admissible; and $27|\alpha - 1|^7/8$ and $3|\alpha - 1|^3$ if $v_2(\alpha - 1) = 1$ and α is not 3-admissible.*

Proof. By Theorem 3.11, $G(\alpha)$ is the direct product of its Sylow subgroups, whose orders, nilpotency classes, and exponents are given in Theorems 4.13 and 4.16 and Propositions 4.18, 4.19, 4.20, and 4.21. □

4.7 Appendix 1

In the following proofs we will be implicitly using Proposition 2.3 to obtain the desired extensions.

Suppose first we are in Case 1. It turns out that $Z_3(J) = \langle A^{p^m}, B^{p^m}, C^{p^m} \rangle$, a normal abelian subgroup of J of order p^{4m}. The defining relations of J allow us to see how A, B, and C conjugate the given generators of $Z_3(J)$. This prompts the construction of J below.

Proof of Theorem 4.12 for Case 1: We have $\alpha = 1 + kp^m$, with $k \in \mathbb{N}$. By adding p^{3m} to α, if necessary, we may assume that k is even.

We start with an abelian group $\langle X, Y, Z\rangle$ of order p^{4m} and defining relations

$$XY = YX,\ YZ = ZY,\ XZ = ZX,\ X^{p^{2m}} = 1,\ X^{p^m}Y^{p^m} = 1,\ Z^{p^m} = 1.$$

We next construct a cyclic extension $\langle X, Y, Z_0\rangle$ of $\langle X, Y, Z\rangle$ of order p^{5m}, where $Z_0^{p^m} = Z$, by means of an automorphism Ω of $\langle X, Y, Z\rangle$ that fixes Z and such that Ω^{p^m} is conjugation by Z, that is, the trivial automorphism. In order to achieve this goal, we consider the assignment

$$X \mapsto X^{1+kp^m},\ Y \mapsto Y^{1-kp^m},\ Z \mapsto Z,$$

where $\beta = 1 - kp^m$ is the inverse of α modulo p^{2m}. We easily verify that the defining relations of $\langle X, Y, Z\rangle$ are preserved. Thus the above assignment extends to an endomorphism Ω of $\langle X, Y, Z\rangle$, which is clearly surjective and hence an automorphism.

We have $\alpha^{p^m} \equiv 1 \mod p^{2m}$ by Lemma 4.8, so $\beta^{p^m} \equiv 1 \mod p^{2m}$, whence Ω^{p^m} is the trivial automorphism of $\langle X, Y, Z\rangle$. This produces the required extension, where Ω is conjugation by Z_0. We readily verify that $\langle X, Y, Z_0\rangle$ has defining relations:

$$X^{Z_0} = X^\alpha,\ {}^{Z_0}Y = Y^\alpha,\ XY = YX,\ X^{p^{2m}} = 1,\ X^{p^m}Y^{p^m} = 1,\ Z_0^{p^{2m}} = 1.$$

We next construct a cyclic extension $\langle X_0, Y, Z_0\rangle$ of $\langle X, Y, Z_0\rangle$ of order p^{6m} with $X_0^{p^m} = X$, by means of an automorphism Ψ of $\langle X, Y, Z_0\rangle$ that fixes X and such that Ψ^{p^m} is conjugation by X. For this purpose, recalling that k is even, we set

$$c = \begin{cases} 0, & \text{if } p \neq 3, \\ k^2 3^{2m-1}, & \text{if } p = 3, \end{cases} \qquad b = \begin{cases} p^m k/2, & \text{if } p \neq 3, \\ 3^m k/2 + k^2 3^{2m-1}, & \text{if } p = 3, \end{cases}$$

so that $b = p^m k/2 + c$, and consider the assignment

$$X \mapsto X,\ Y \mapsto Z_0^{-p^m} Y^{1+b} = Z^{-1}Y^{1+b},\ Z_0 \mapsto Z_0 X^{-k}.$$

Let us verify that the defining relations of $\langle X, Y, Z_0\rangle$ are preserved. This is obvious for the first and fourth relations. As for the sixth, we need to see that $(Z_0X^{-k})^{p^{2m}} = 1$. This holds because

$$(Z_0X^{-k})^{p^{2m}} = Z_0^{p^{2m}} X^{-k(\alpha^{p^{2m}}-1)/(\alpha-1)} = 1$$

by Lemma 4.8. The second, third and fifth relations are easily seen to be preserved, using that $Z_0^{-p^m} = Z^{-1}$ commutes with X and Y, as well as $Z^{p^m} = 1 = Y^{p^{2m}}$. Thus the above

assignment extends to an endomorphism Ψ of $\langle X, Y, Z_0\rangle$. As $\gcd(1+b, p^{2m}) = 1$, Ψ is an automorphism. We next show that Ψ^{p^m} is conjugation by X. By definition, Ψ^{p^m} fixes X. Moreover,

$$Z_0\Psi^{p^m} = Z_0X^{-kp^m} = Z_0X^{1-\alpha},\ Z_0^X = Z_0Z_0^{-1}X^{-1}Z_0X = Z_0X^{-\alpha}X = Z_0X^{1-\alpha}.$$

It remains to verify that Ψ^{p^m} fixes Y. By definition, we have

$$Y\Psi = Z^{-1}YY^b,$$

which implies that Ψ fixes $Y^{\alpha-1}$ and Y^b. On the other hand, use of Lemma 4.8 yields

$$\begin{aligned} Z\Psi = Z_0^{p^m}\Psi = (Z_0\Psi)^{p^m} = (Z_0X^{-k})^{p^m} = Z_0^{p^m}X^{-k(\alpha^{p^m}-1)/(\alpha-1)} = ZX^{-kp^m} = ZX^{1-\alpha} \\ = ZY^{\alpha-1}. \end{aligned}$$

Thus

$$Y\Psi^2 = (Z^{-1}YY^b)\Psi = Z^{-1}Y^{1-\alpha}Z^{-1}YY^bY^b = Z^{-2}YY^{1-\alpha}Y^{2b},$$

$$Y\Psi^3 = (Z^{-2}YY^{1-\alpha}Y^{2b})\Psi = Z^{-2}Y^{2(1-\alpha)}Z^{-1}YY^bY^{1-\alpha}Y^{2b} = Z^{-3}YY^{3(1-\alpha)}Y^{3b},$$

and in general

$$Y\Psi^i = Z^{-i}YY^{\binom{i}{2}(1-\alpha)}Y^{ib}, \quad i \geq 2.$$

In particular,

$$Y\Psi^{p^m} = Z^{-p^m}YY^{\binom{p^m}{2}(1-\alpha)}Y^{p^mb} = Y.$$

This produces the required extension, where Ψ is conjugation by X_0. We readily verify that $\langle X_0, Y, Z_0\rangle$ has defining relations

$$X_0^{p^{3m}} = 1,\ X_0^{Z_0} = X_0^{\alpha},\ Y^{X_0} = Z_0^{-p^m}Y^{1+b},\ {}^{Z_0}Y = Y^{\alpha},$$

$$X_0^{p^m}Y = YX_0^{p^m},\ X_0^{p^{2m}}Y^{p^m} = 1,\ Z_0^{p^{2m}} = 1.$$

Here $X_0^{Z_0} = X_0^{\alpha}$ is equivalent to $Z_0^{X_0} = Z_0X^{-k} = Z_0X_0^{-kp^m} = Z_0X_0^{1-\alpha}$.

We finally construct a cyclic extension $\langle X_0, Y_0, Z_0\rangle$ of $\langle X_0, Y, Z_0\rangle$ of order p^{7m} with $Y_0^{p^m} = Y$, by means of an automorphism Π of $\langle X_0, Y, Z_0\rangle$ that fixes Y and such that Π^{p^m} is conjugation by Y. With this aim in mind, we consider the assignment

$$X_0 \mapsto X_0Z_0,\ Y \mapsto Y,\ Z_0 \mapsto Y^kZ_0.$$

Let us verify that the defining relations of $\langle X_0, Y, Z_0\rangle$ are preserved. Regarding the first relation,

$$(X_0Z_0)^{p^{3m}} = Z_0^{p^{3m}}X_0^{\alpha(\alpha^{p^{3m}}-1)/(\alpha-1)} = 1$$

by Lemma 4.8. Likewise, the seventh relation is preserved, as Lemma 4.8 ensures

$$(Y^k Z_0)^{p^{2m}} = Y^{k(\alpha^{p^{2m}}-1)/(\alpha-1)} Z_0^{p^{2m}} = Y^{kp^{2m}} Z_0^{p^{2m}} = 1.$$

The preservation of the fourth relation is obvious. Regarding the fifth relation, Lemma 4.8 yields

$$(X_0 Z_0)^{p^m} = Z_0^{p^m} X_0^{\alpha(\alpha^{p^m}-1)/(\alpha-1)} = Z X^{\ell}, \quad \ell \in \mathbb{Z},$$

where both factors commute with Y. As for the sixth relation, observe that

$$(X_0 Z_0)^{p^{2m}} = Z_0^{p^{2m}} X_0^{\alpha(\alpha^{p^{2m}}-1)/(\alpha-1)} = X_0^{p^{2m}}$$

by Lemma 4.8, so $(X_0 Z_0)^{p^{2m}} Y^{p^m} = X_0^{p^{2m}} Y^{p^m} = 1$. In regards to the third relation, we must prove

$$Y^{X_0 Z_0} = (Y^k Z_0)^{-p^m} Y Y^b.$$

Note that $(Y^b)^{Z_0} = Y^b$, so

$$Y^{X_0 Z_0} = (Z_0^{-p^m} Y Y^b)^{Z_0} = Z_0^{-p^m} Y^{Z_0} Y^b = Z_0^{-p^m} Y^{1-kp^m} Y^b.$$

On the other hand, Lemma 4.8 ensures that

$$(Y^k Z_0)^{p^m} = Y^{k(\alpha^{p^m}-1)/(\alpha-1)} Z_0^{p^m} = Y^{kp^m} Z_0^{p^m},$$

so

$$(Y^k Z_0)^{-p^m} Y Y^b = Z_0^{-p^m} Y^{-kp^m} Y Y^b = Z_0^{-p^m} Y^{1-kp^m} Y^b,$$

as required. The preservation of the second relation requires more work. We must show that

$$(X_0 Z_0)^{Y^k Z_0} = (X_0 Z_0)^{\alpha}. \tag{4.23}$$

We begin by obtaining a formula for $X_0^{Y^k}$. From $X_0^{-1} Y X_0 = Y^{X_0} = Z^{-1} Y Y^b$, we deduce $Y^{-1} X_0^{-1} Y = Z^{-1} Y^b X_0^{-1}$, and therefore

$$X_0^Y = X_0 Y^{-b} Z. \tag{4.24}$$

Thus

$$X_0^{Y^k} = X_0 Y^{-bk} Z^k = X_0 Y^{-bk} Z_0^{kp^m}. \tag{4.25}$$

We next obtain a formula for $Z_0^{Y^k}$. From $Z_0 Y Z_0^{-1} = {}^{Z_0}Y = Y^{\alpha}$, we infer $Y^{-1} Z_0 Y = Y^{\alpha-1} Z_0$. Noting that $[Z_0, Y^{\alpha-1}] = 1$, we infer $Z_0^Y = Z_0 Y^{\alpha-1}$, and hence

$$Z_0^{Y^k} = Z_0 Y^{k(\alpha-1)}. \tag{4.26}$$

Using (4.25), (4.26), and $[Z_0, Y^{\alpha-1}] = 1$, we obtain

$$(X_0Z_0)^{Y^k} = X_0Y^{-bk}Z_0^{kp^m}Z_0Y^{k(\alpha-1)} = X_0Y^{k(-b+(\alpha-1))}Z_0^{\alpha}.$$

As Z_0 commutes with Y^b and $Y^{\alpha-1}$, we infer

$$(X_0Z_0)^{Y^kZ_0} = X_0^{\alpha}Y^{k(-b+(\alpha-1))}Z_0^{\alpha}. \tag{4.27}$$

On the other hand, we have

$$(X_0Z_0)^{\alpha} = Z_0^{\alpha}X_0^{\alpha(\alpha^{\alpha}-1)/(\alpha-1)}. \tag{4.28}$$

Taking into account (4.27) and (4.28), as well as the fact that Z_0 commutes with Y^b and $Y^{\alpha-1}$, we see that (4.23) is equivalent to

$$X_0^{\alpha(\alpha^{\alpha}-1)/(\alpha-1)} = X_0^{\alpha\alpha^{\alpha}}\,Y^{k(-b+(\alpha-1))}. \tag{4.29}$$

Making use of the fundamental relation $X_0^{p^{2m}}Y^{p^m} = 1$ and the meanings of b and c, we find that

$$Y^{k(\alpha-1)} = X_0^{-(\alpha-1)^2},\ Y^{-kb} = X_0^{(\alpha-1)^2/2+kc3^m}.$$

Thus (4.29) is equivalent to

$$X_0^{\alpha(\alpha^{\alpha}-1)/(\alpha-1)} = X_0^{\alpha\alpha^{\alpha}-(\alpha-1)^2/2+kc3^m}. \tag{4.30}$$

Here

$$\alpha^{\alpha} = (1+(\alpha-1))^{\alpha} = 1+\alpha(\alpha-1)+\binom{\alpha}{2}(\alpha-1)^2+\binom{\alpha}{3}(\alpha-1)^3+\binom{\alpha}{4}(\alpha-1)^4+\cdots \tag{4.31}$$

We see from (4.31) that $\alpha^{\alpha} \equiv 1+\alpha(\alpha-1) \mod p^{3m}$, so

$$\alpha\alpha^{\alpha} \equiv \alpha+\alpha^2(\alpha-1) \mod p^{3m}. \tag{4.32}$$

We also derive from (4.31) that

$$(\alpha^{\alpha}-1)/(\alpha-1) \equiv \alpha+\binom{\alpha}{2}(\alpha-1)+\binom{\alpha}{3}(\alpha-1)^2 \mod p^{3m},$$

and since $\alpha p^{2m} \equiv p^{2m} \mod p^{3m}$, we infer

$$\alpha(\alpha^{\alpha}-1)/(\alpha-1) \equiv \alpha^2+(\alpha-1)^2/2+\binom{\alpha}{3}(\alpha-1)^2 \mod p^{3m}. \tag{4.33}$$

From (4.32) and (4.33) we see that (4.30) follows from

$$\alpha^2+(\alpha-1)^2/2+\binom{\alpha}{3}(\alpha-1)^2\equiv\alpha+\alpha^2(\alpha-1)-(\alpha-1)^2/2+kc3^m \mod p^{3m},$$

which is equivalent to

$$\alpha^2+(\alpha-1)^2+\binom{\alpha}{3}(\alpha-1)^2\equiv\alpha+\alpha^2(\alpha-1)+kc3^m \mod p^{3m}. \tag{4.34}$$

Here

$$\alpha^2+(\alpha-1)^2\equiv 1+2(\alpha-1)+2(\alpha-1)^2\equiv\alpha+\alpha^2(\alpha-1) \mod p^{3m},$$

so (4.34) means

$$\binom{\alpha}{3}(\alpha-1)^2\equiv kc3^m \mod p^{3m},$$

which is readily seen to be true whether $p\neq 3$ or $p=3$. This completes the verification that the second defining relation of $\langle X_0,Y,Z_0\rangle$ is preserved, which ensures the existence of an automorphism Π of $\langle X_0,Y,Z_0\rangle$ fixing Y and extending the given assignment. We must now verify that Π^{p^m} is conjugation by Y. By definition, $Y\Pi^{p^m}=Y$ and

$$Z_0\Pi^{p^m}=Y^{kp^m}Z_0=Y^{\alpha-1}Z_0=Z_0^Y.$$

It remains to show that $X_0\Pi^{p^m}=X_0^Y$. The calculation of X_0^Y is achieved in (4.24). On the other hand, repeated application of $X_0\Pi=X_0Z_0$, $Y=Y\Pi$, $Z_0\Pi=Y^kZ_0$ yields

$$X_0\Pi^i=X_0Y^{k\alpha(1+2\alpha+3\alpha^2+\cdots+(i-1)\alpha^{i-2})}Z_0^i,\quad i\geq 2.$$

Set $U=k\alpha(1+2\alpha+3\alpha^2+\cdots+(p^m-1)\alpha^{p^m-2})$. We are thus reduced to show that

$$U\equiv -b \mod p^{2m}.$$

Now

$$\alpha^i=(1+(\alpha-1))^i\equiv 1+i(\alpha-1) \mod p^{2m},\quad i\geq 0,$$

so

$$U\equiv k\alpha(1+2+\cdots+(p^m-1)+(\alpha-1)(1\times 2+2\times 3+\cdots+(p^m-2)\times(p^m-1))) \mod p^{2m}.$$

As is well-known, we have

$$\sum_{1\leq i\leq n} i=\frac{n(n+1)}{2},\ \sum_{1\leq i\leq n} i^2=\frac{n(n+1)(2n+1)}{6},\quad n\geq 1,$$

which implies

$$\sum_{1\le i\le n-2} i(i+1) = \frac{(n-2)(n-1)n}{3}, \quad n \ge 3.$$

Set $n = p^m$. We then have

$$k\alpha\frac{(n-1)n}{2} \equiv \frac{k\alpha(p^m-1)p^m}{2} \equiv \frac{-kp^m}{2} \mod p^{2m},$$

so we are reduced to show that

$$k\alpha(\alpha-1)\frac{(n-2)(n-1)n}{3} \equiv -c \mod p^{2m},$$

which is readily seen to be true whether $p \neq 3$ or $p = 3$. This produces the required extension, where Π is conjugation by Y_0. From $X_0^{Y_0} = X_0Z_0$, we deduce $[X_0, Y_0] = Z_0$, whence $\langle X_0, Y_0, Z_0\rangle = \langle X_0, Y_0\rangle$. Moreover, we have $X_0^{Z_0} = X_0^\alpha$ and $Y_0^{-1}Z_0Y_0 = Z_0^{Y_0} = Y^kZ_0 = Y_0^{kp^m}Z_0 = Y_0^{\alpha-1}Z_0$, which implies ${}^{Z_0}Y_0 = Y^\alpha$. Finally, we also have $X_0^{p^{3m}} = 1 = Y_0^{p^{3m}}$. □

Note 4.35. The attentive reader will notice that if $p = 3$ the restriction $m > 1$ or $(\alpha-1)/3 \equiv 1 \mod 3$ was never used in the above proof. Thus, if $m = 1$ and $(\alpha-1)/3 \equiv -1 \mod 3$, the above proof still constructs an image of J of order 3^7. However, $|J| = 3^{10}$ in this case, as seen in the proof for Case 3 below.

Suppose next we are in Case 2. It transpires that $\langle A^{2^m}, B^{2^m}, C^{2^{m-1}}\rangle$, a normal abelian subgroup of J of order 2^{4m-2}, equal to $Z_3(J)$ if $m > 1$ and to $Z_2(J)$ if $m = 1$. Using the defining relations of J, we can determine the precise way in which A, B, and C conjugate the given generators of $Z_3(J)$, which suggest the following construction of J.

Proof of Theorem 4.12 for Case 2: We have $\alpha = 1 + 2^mk$, with $k \in \mathbb{N}$ odd. We start with an abelian group $\langle x, y, z\rangle$ of order 2^{4m-2} generated by elements x, y, z subject to the defining relations:

$$xy = yx,\ xz = zx,\ yz = zx,\ z^{2^m} = x^{2^{2m-2}},\ x^{2^{m-1}}y^{2^{m-1}} = 1,\ x^{2^{2m-1}} = 1.$$

We next construct a cyclic extension $\langle x, y, z_0\rangle$ of $\langle x, y, z\rangle$ of order 2^{5m-3}, where $z_0^{2^{m-1}} = z$, by means of an automorphism Ω of $\langle x, y, z\rangle$ that fixes z and such that $\Omega^{2^{m-1}}$ is conjugation by z, that is, the trivial automorphism. In order to achieve this goal, we consider the assignment

$$x \mapsto x^\alpha,\ y \mapsto y^\beta,\ z \mapsto z,$$

where $\beta = 1 - 2^mk$ is the inverse of α modulo 2^{2m}. The defining relations of $\langle x, y, z\rangle$ are easily seen to be preserved. Thus the above assignment extends to an endomorphism Ω of

$\langle x, y, z\rangle$ which is clearly surjective and hence an automorphism of $\langle x, y, z\rangle$. Let us verify that $\Omega^{2^{m-1}}$ acts trivially on x, y, z. This is obviously true for z, and since $\alpha^{2^{m-1}} \equiv 1 \mod 2^{2m-1}$ and $\beta^{2^{m-1}} \equiv 1 \mod 2^{2m-1}$, it is also true of x and y. This produces the required extension, where Ω is conjugation by z_0. We readily verify that $\langle x, y, z_0\rangle$ has defining relations:

$$xy = yx,\ x^{z_0} = x^{\alpha},\ {}^{z_0}y = y^{\alpha},\ z_0^{2^{2m-1}} = x^{2^{2m-2}},\ x^{2^{m-1}}y^{2^{m-1}} = 1,\ x^{2^{2m-1}} = 1.$$

We next construct a cyclic extension $\langle x_0, y, z_0\rangle$ of $\langle x, y, z_0\rangle$ of order 2^{6m-3}, where $x_0^{2^m} = x$, by means of an automorphism Ψ of $\langle x, y, z_0\rangle$ that fixes x and such that Ψ^{2^m} is conjugation by x. For this purpose, we consider the assignment

$$x \mapsto x,\ y \mapsto z_0^{-2^m}y^{1+2^{m-1}k} = z^{-2}y^{1+2^{m-1}k},\ z_0 \mapsto z_0x^{-k}.$$

Let us verify that the defining relations of $\langle x, y, z_0\rangle$ are preserved. This is easily seen to be true for the first, second, and sixth relations. As for the fifth relation, since k is odd, we have

$$(z^{-2}y^{1+2^{m-1}k})^{2^{m-1}} = z^{-2^m}y^{2^{2m-2}k}y^{2^{m-1}} = x^{-2^{2m-2}}y^{2^{2m-2}}y^{2^{m-1}} = x^{-2^{2m-2}}x^{-2^{2m-2}}y^{2^{m-1}} = y^{2^{m-1}},$$

as required. Regarding the fourth relation, we have

$$(z_0x^{-k})^{2^{2m-1}} = z_0^{2^{2m-1}}x^{-k(1+\alpha+\cdots+\alpha^{2^{2m-1}-1})} = z_0^{2^{2m-1}} = x^{2^{2m-2}},$$

since $(\alpha^{2^{2m-1}} - 1)/(\alpha - 1) \equiv 0 \mod 2^{2m-1}$. In regards to third relation, we have

$${}^{(z_0x^{-k})}(z^{-2}y^{1+2^{m-1}k}) = z^{-2}y^{\alpha(1+2^{m-1}k)} = z^{-2\alpha}y^{\alpha(1+2^{m-1}k)} = (z^{-2}y^{1+2^{m-1}k})^{\alpha},$$

as $2\alpha \equiv 2 \mod 2^{m+1}$. Thus the above assignment extends to an endomorphism Ψ of $\langle x, y, z_0\rangle$. Since $x, y^{1+2^{m-1}k}, z_0 \in \mathrm{im}(\Psi)$ and $x^{2^{m-1}}y^{2^{m-1}} = 1$, it follows that Ψ is surjective and hence an automorphism of $\langle x, y, z_0\rangle$.

Let us verify that Ψ^{2^m} acts via conjugation by x on x, y, z. This is obviously true for x. As for z_0, from $x^{z_0} = x^{\alpha}$ we derive $z_0^x = z_0x^{1-\alpha} = z_0x^{-2^mk} = z_0^{\Psi^{2^m}}$. Regarding y, carefully using the defining relations of $\langle x, y, z_0\rangle$ we see by induction that $y^{\Psi^n} = z^{-2n}y^{1+n(2-n)2^{m-1}k}$ for all $n \in \mathbb{N}$. In particular,

$$y^{\Psi^{2^m}} = z^{-2(2^m)}yy^{(2-2^m)2^{2m-1}k} = y = y^x.$$

This produces the required extension, where Ψ is conjugation by x_0. We readily verify that $\langle x_0, y, z_0\rangle$ has defining relations:

$$y^{x_0} = z_0^{-2^m}y^{1+2^{m-1}k},\ x_0^{z_0} = x_0^{\alpha},\ {}^{z_0}y = y^{\alpha},\ z_0^{2^{2m-1}} = x_0^{2^{3m-2}},\ x_0^{2^{2m-1}}y^{2^{m-1}} = 1,\ x_0^{2^{3m-1}} = 1,$$

where $x_0^{z_0} = x_0^{\alpha}$ is equivalent to the given relation $z_0^{x_0} = z_0 x^{-k} = z_0 x_0^{1-\alpha}$.

We finally construct a cyclic extension $\langle x_0, y_0, z_0\rangle$ of $\langle x_0, y, z_0\rangle$ of order 2^{7m-3}, where $y_0^{2^m} = y$, by means of an automorphism Π of $\langle x_0, y, z_0\rangle$ that fixes y and such that Π^{2^m} is conjugation by y. For this purpose, we consider the assignment

$$x_0 \mapsto x_0 z_0,\ y \mapsto y,\ z_0 \mapsto y^k z_0.$$

Let us verify that the defining relations of $\langle x_0, y, z_0\rangle$ are preserved. This is obviously true for the third relation. As for the first relation, we have

$$y^{x_0 z_0} = (z_0^{-2^m} y^{1+2^{m-1}k})^{z_0} = z_0^{-2^m} y^{\beta(1+2^{m-1}k)} = z_0^{-2^m} y^{\beta+2^{m-1}k},$$

since $\beta 2^{m-1}k \equiv 2^{m-1}k \mod 2^{2m-1}$. On the other hand,

$$(y^k z_0)^{-2^m} y^{1+2^{m-1}k} = (y^{k(1+\alpha+\cdots+\alpha^{2^m-1})} z_0^{2^m})^{-1} y^{1+2^{m-1}k},$$

where $(\alpha^{2^m}-1)/(\alpha-1) \equiv 2^m \mod 2^{2m-1}$, so

$$(y^k z_0)^{-2^m} y^{1+2^{m-1}k} = (y^{2^m k} z_0^{2^m})^{-1} y^{1+2^{m-1}k} = z_0^{-2^m} y^{-2^m k} y^{1+2^{m-1}k} = z_0^{-2^m} y^{\beta+2^{m-1}k},$$

as required. Regarding the sixth relation, we have

$$(x_0 z_0)^{2^{3m-1}} = z_0^{2^{3m-1}} x_0^{\alpha(1+\alpha+\cdots+\alpha^{2^{3m-1}-1})} = z_0^{2^{3m-1}} = 1,$$

since $(\alpha^{2^{3m-1}}-1)/(\alpha-1) \equiv 0 \mod 2^{3m-1}$. In regards to the fifth relation, we have

$$(x_0 z_0)^{2^{2m-1}} = z_0^{2^{2m-1}} x_0^{\alpha(1+\alpha+\cdots+\alpha^{2^{2m-1}-1})} = z_0^{2^{2m-1}} x_0^{2^{2m-1}-2^{3m-2}} = x_0^{2^{2m-1}},$$

as $\alpha(\alpha^{2^{2m-1}}-1)/(\alpha-1) \equiv 2^{2m-1} - 2^{3m-2} \mod 2^{3m-1}$ by Lemma 4.9. We next deal with the fourth relation. We have

$$(y^k z_0)^{2^{2m-1}} = y^{k(1+\alpha+\cdots+\alpha^{2^{2m-1}-1})} z_0^{2^{2m-1}} = z_0^{2^{2m-1}} = x_0^{2^{3m-2}},$$

using once again that $(\alpha^{2^{2m-1}}-1)/(\alpha-1) \equiv 0 \mod 2^{2m-1}$. On the other hand, we have

$$(x_0 z_0)^{2^{3m-2}} = z_0^{2^{3m-2}} x_0^{\alpha(1+\alpha+\cdots+\alpha^{2^{3m-2}-1})} = z_0^{2^{3m-2}} x_0^{2^{3m-2}-2^{4m-3}} = x_0^{2^{4m-3}} x_0^{2^{3m-2}-2^{4m-3}} = x_0^{2^{3m-2}}.$$

Indeed, setting $\gamma = \alpha^{2m-1}$, then $\gamma - 1 \equiv 0 \mod 2^{3m-1}$, so $(\gamma^{2^{m-1}}-1)/(\gamma-1) \equiv 2^{m-1} \mod 2^{3m-1}$, and therefore

$$\alpha\frac{\alpha^{2^{3m-2}}-1}{\alpha-1} \equiv \alpha\frac{\alpha^{2^{m-1}}-1}{\alpha-1}\frac{\gamma^{2^{m-1}}-1}{\gamma-1} \equiv (2^{2m-1} - 2^{3m-2})2^{m-1} \equiv 2^{3m-2} - 2^{4m-3} \mod 2^{3m-1}.$$

It remains to verify that the second relation is preserved. From $z_0 y z_0^{-1} = y^\alpha$, we infer $y^{-1} z_0 y = y^{\alpha-1} z_0$, so $z_0^y = y^{2^m k} z_0$ and therefore $z_0^{y^k} = y^{2^m k^2} z_0$. Moreover, from $x_0^{-1} y x_0 = z^{-2} y^{1+2^{m-1}k}$, we deduce $y^{-1} x_0^{-1} y = z^{-2} y^{2^{m-1}k} x_0^{-1}$, hence $x_0^y = x_0 y^{-2^{m-1}k} z^2$, and therefore $x_0^{y^k} = x_0 y^{-2^{m-1}k^2} z^{2k}$. Thus

$$\begin{aligned}(x_0 z_0)^{y^k z_0} &= (x_0 y^{-2^{m-1}k^2} z^{2k} y^{2^m k^2} z_0)^{z_0} = (x_0 y^{2^{m-1}k^2} z_0^\alpha)^{z_0} = x_0^\alpha y^{\beta 2^{m-1}k^2} z_0^\alpha \\ &= x_0^{\alpha - 2^{2m-1}\beta k^2} z_0^\alpha = z_0^\alpha z_0^{-\alpha} x_0^{\alpha - 2^{2m-1}\beta k^2} z_0^\alpha = z_0^\alpha x_0^{\alpha^\alpha(\alpha - 2^{2m-1}\beta k^2)}.\end{aligned}$$

Here

$$\alpha^\alpha \equiv 1 + \alpha(\alpha-1) \equiv 1 + 2^m k + 2^{2m} k^2 \mod 2^{3m-1},$$

and

$$\alpha - 2^{2m-1}\beta k^2 \equiv 1 + 2^m k - 2^{2m-1} k^2 \mod 2^{3m-1},$$

so

$$\begin{aligned}\alpha^\alpha(\alpha - 2^{2m-1}\beta k^2) &\equiv (1 + 2^m k + 2^{2m} k^2)(1 + 2^m k - 2^{2m-1} k^2) \\ &\equiv 1 + 2^{m+1} k + 3 \times 2^{2m-1} k^2 \mod 2^{3m-1}.\end{aligned}$$

It follows that

$$(x_0 z_0)^{y^k z_0} = z_0^\alpha x_0^{1 + 2^{m+1}k + 3 \times 2^{2m-1}k^2}.$$

On the other hand, we have $(x_0 z_0)^\alpha = z_0^\alpha x_0^{\alpha(1+\alpha+\cdots+\alpha^{\alpha-1})}$, where

$$\frac{\alpha^\alpha - 1}{\alpha - 1} \equiv \alpha + \alpha(\alpha-1)^2/2 \equiv 1 + 2^m k + 2^{2m-1} k^2 \mod 2^{3m-1},$$

so

$$\alpha \frac{\alpha^\alpha - 1}{\alpha - 1} \equiv \alpha(1 + 2^m k + 2^{2m-1} k^2) \equiv 1 + 2^{m+1} k + 3 \times 2^{2m-1} k^2 \mod 2^{3m-1},$$

and therefore

$$(x_0 z_0)^\alpha = z_0^\alpha x_0^{1 + 2^{m+1}k + 3 \times 2^{2m-1}k^2},$$

as required. Thus the given assignment extends to an endomorphism Π of $\langle x_0, y, z_0 \rangle$, which is clearly surjective and hence an automorphism Π of $\langle x_0, y, z_0 \rangle$. We next verify that Π^{2^m} acts as conjugation by y on x_0, y, z_0. This is obvious for y. As for z_0, we have $z_0^{\Pi^{2^m}} = y^{2^m k} z_0 = z_0^y$, as computed earlier. Regarding x_0, we easily see by induction that $x_0^{\Pi^n} = x_0 y^{k(\alpha + 2\alpha^2 + 3\alpha^3 + \cdots + (n-1)\alpha^{n-1})} z_0^n$ for all $n \in \mathbb{N}$, where the indicated sum has $n-1$ terms and is equal to 0 when $n = 1$. Now $\alpha^i \equiv (1 + (\alpha-1))^i \equiv 1 + i(\alpha-1) \mod 2^{2m-1}$ for all $i \in \mathbb{N}$, so

$$\begin{aligned}&\alpha + 2\alpha^2 + 3\alpha^3 + \cdots + (n-1)\alpha^{n-1} \\ &\quad \equiv 1 + \cdots + (n-1) + (\alpha-1)(1^2 + \cdots + (n-1)^2) \mod 2^{2m-1}, \quad n \in \mathbb{N},\end{aligned}$$

that is,

$$\alpha + 2\alpha^2 + 3\alpha^3 + \cdots + (n-1)\alpha^{n-1} \equiv \frac{(n-1)n}{2} + (\alpha - 1)\frac{(n-1)n(2(n-1)+1)}{6}, \quad n \in \mathbb{N}.$$

In particular, for $n = 2^m$, we have

$$\begin{aligned}\alpha + 2\alpha^2 + 3\alpha^3 + \cdots + (2^m - 1)\alpha^{2^m-1} &\equiv 2^{2m-1} - 2^{m-1} + 2^{2m-1}k\frac{(2^m-1)(2^{m+1}-1)}{3} \\ &\equiv -2^{m-1} \mod 2^{2m-1}.\end{aligned}$$

It follows that $x_0^{\Pi^{2^m}} = x_0 y^{-2^{m-1}k} z_0^{2^m} = x_0^y$, as computed earlier.

This produces the required extension, where Π is conjugation by y_0. We already had $x_0^{z_0} = x_0^\alpha$. Moreover, the new relation $z_0^{y_0} = y^k z_0 = y_0^{2^m k} z_0 = y_0^{\alpha-1} z_0$ is equivalent to ${}^{z_0}y_0 = y_0^\alpha$. Furthermore, from $x_0^{y_0} = x_0 z_0$ we infer $[x_0, y_0] = z_0$, so $\langle x_0, y_0, z_0\rangle = \langle x_0, y_0\rangle$. As $x_0^{2^{3m-1}} = 1 = y_0^{2^{3m-1}}$ the proof is complete. □

Suppose finally that we are in Case 3. It turns out that $\langle A^3, B^9, C^3\rangle$ is a normal subgroup of J of order 3^6. The defining relations of J allow us see how A, B, and C act on $\langle A^3, B^9, C^3\rangle$ by conjugation, which prompts the construction of the model of J below.

Proof of Theorem 4.12 for Case 3: We have $\alpha = 1 + 3k$, where $k \in \mathbb{N}$ and $k \equiv -1 \mod 3$. We start with a group $\langle x, y, z\rangle$ of order 3^6 generated by elements x, y, z subject to defining relations:

$$x^{27} = 1,\ xy = yx,\ x^9y^3 = 1,\ z^9 = 1,\ x^z = x^{-8},\ yz = zy.$$

Note that $\langle x, y, z\rangle$ is a semidirect product of $\mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ by $\mathbb{Z}/9\mathbb{Z}$, where $[z, x^3] = 1 = [z^3, x]$.

We next construct a cyclic extension $\langle x, y_0, z\rangle$ of $\langle x, y, z\rangle$ of order 3^7, where $y_0^3 = y$, by means of an automorphism Ω_1 of $\langle x, y, z\rangle$ that fixes y and such that Ω_1^3 is conjugation by y, that is, the trivial automorphism. For this purpose, we consider the assignment

$$x \mapsto x^{-8}z^3,\ y \mapsto y,\ z \mapsto y^{-3}z.$$

All defining relations of $\langle x, y, z\rangle$ are obviously preserved. Thus the above assignment extends to an endomorphism Ω_1 of $\langle x, y, z\rangle$, which is clearly surjective and hence an automorphism. We next verify that Ω_1^3 agrees with conjugation by y on x, y, and z. This is obviously true for y and z, and noting that Ω_1 fixes z^3, we find that it is also true for x. This produces

the required extension, where Ω_1 is conjugation by y_0. We readily verify that $\langle x, y_0, z\rangle$ has defining relations:

$$x^{27} = 1,\ x^{y_0} = x^{-8}z^3,\ x^9y_0^9 = 1,\ z^9 = 1,\ x^z = x^{-8},\ z^{y_0} = y_0^{-9}z.$$

We next construct a cyclic extension $\langle x, y_0, z_0\rangle$ of $\langle x, y_0, z\rangle$ of order 3^8, where $z_0^3 = z$, by means of an automorphism Ω_2 of $\langle x, y_0, z\rangle$ that fixes z and such that Ω_2^3 is conjugation by z. With this goal in mind, we consider the assignment

$$x \mapsto x^\alpha,\ y_0 \mapsto y_0^\beta,\ z \mapsto z,$$

where $\beta \in \mathbb{Z}$ satisfies $\alpha\beta \equiv 1 \mod 27$. It is easy to see that all defining relations of $\langle x, y_0, z\rangle$ are preserved. Thus the above assignment extends to an endomorphism Ω_2 of $\langle x, y_0, z\rangle$, which is clearly surjective and hence an automorphism. We next verify that Ω_2^3 agrees with conjugation by z on x, y_0, and z. This is obviously true for z, and noting that $\alpha^3 \equiv -8 \mod 27$ and $\beta^3 \equiv 10 \mod 27$, we find that it is also true for x and y. This produces the required extension, where Ω_2 is conjugation by z_0. We readily verify that $\langle x, y_0, z_0\rangle$ has defining relations:

$$x^{27} = 1,\ x^{y_0} = x^{-8}z_0^9,\ x^9y_0^9 = 1,\ z_0^{27} = 1,\ x^{z_0} = x^\alpha,\ {}^{z_0}y_0 = y_0^\alpha.$$

We next construct a cyclic extension $\langle x_0, y_0, z_0\rangle$ of $\langle x, y_0, z_0\rangle$ of order 3^9, where $x_0^3 = x$, by means of an automorphism Ω_3 of $\langle x, y_0, z_0\rangle$ that fixes x and such that Ω_3^3 is conjugation by x. For this purpose, we consider the assignment

$$x \mapsto x,\ y_0 \mapsto z_0^{-3}y_0^{-2},\ z_0 \mapsto z_0x^{-k}.$$

The first, fourth and fifth defining relations of $\langle x, y_0, z_0\rangle$ are easily seen to be preserved. As for the third, as z commutes with y, it suffices to verify that $(z^{-1}y_0)^9 = y_0^9$. As indicated earlier, $y_0^z = y_0^{10}$, so indeed $(z^{-1}y_0)^9 = y_0^{10+10^2+\cdots+10^9}z^{-9} = y_0^9$, since $10(10^9 - 1)/9 \equiv 9 \mod 27$.

Regarding the second relation, we need to verify that $x^{z_0^{-3}y_0^{-2}} = x^{-8}(z_0x^{-k})^9$. As z normalizes $\langle x\rangle$, y commutes with x, and z^3 commutes with x, we have

$$x^{z_0^{-3}y_0^{-2}} = x^{z^{-1}y_0} = (x^{10})^{y_0} = (x^{y_0})^{10} = (x^{-8}z^3)^{10} = xz^3.$$

On the other hand,

$$(z_0x^{-k})^9 = z_0^9x^{-k(1+\alpha+\cdots+\alpha^8)} = z^3x^{-9k} = x^{-9k}z^3,$$

since $(\alpha^9-1)/(\alpha-1)\equiv 9 \mod 27$. Thus

$$x^{-8}(z_0x^{-k})^9 = x^{-8}x^{-9k}z^3 = xx^{-9-9k}z^3 = xz^3,$$

as $9(k+1)\equiv 0 \mod 27$. This proves that the second relation is preserved.

In regards to the sixth relation, we need to verify that ${}^{z_0x^{-k}}(z_0^{-3}y_0^{-2}) = (z_0^{-3}y_0^{-2})^\alpha$. We have

$$(z_0^{-3}y_0^{-2})^\alpha = (z^{-1}y_0y_0^{-3})^\alpha = (z^{-1}y_0)^\alpha y^{-\alpha}.$$

Here

$$(z^{-1}y_0)^\alpha = y_0^{10(1+10+\cdots+10^{\alpha-1})}z^{-\alpha} = y_0^{10\alpha}z^{-\alpha},$$

since $(10^\alpha-1)/9\equiv\alpha \mod 27$. Since $k\equiv -1 \mod 3$, we infer

$$(z_0^{-3}y_0^{-2})^\alpha = y_0^{10\alpha}z^{-\alpha}y^{-\alpha} = y_0^{7\alpha}z^{-\alpha} = y_0^{7\alpha}z^2.$$

On the other hand, from $x^{y_0} = x^{-8}z^3$ we deduce $(y_0^{-1})^x = x^{-9}z^3y_0^{-1}$. Here y_0, x^3, z^3 commute with each other, so $y_0^x = y_0x^9z^{-3}$. As x commutes with z^3 and $k\equiv -1 \mod 3$, it follows that ${}^{x^{-k}}y_0 = y_0^{x^k} = y_0x^{-9}z^3$. In addition, from $x^z = x^{-8}$, we deduce ${}^{x^{-1}}z^{-1} = x^{-9}z^{-1} = z^{-1}x^{-9}$, so ${}^{x^{-k}}z^{-1} = z^{-1}x^{-9k} = z^{-1}x^9$. Therefore, ${}^{x^{-k}}(z_0^{-3}y_0^{-2}) = z^{-1}x^9y_0^{-2}x^{-9}z^3 = y_0^7z^2$, whence ${}^{z_0x^{-k}}(z_0^{-3}y_0^{-2}) = y_0^{7\alpha}z^2$. This demonstrates that the sixth relation is preserved. Thus the above assignment extends to an endomorphism Ω_3 of $\langle x, y_0, z_0\rangle$, which is clearly surjective and hence an automorphism. We next verify that Ω_3^3 agrees with conjugation by x on x, y_0, and z_0. This is obvious for x. Moreover, Ω_3^3 sends z_0 to $z_0x^{-3k} = z_0x^{1-\alpha}$, and the given relation $x^{z_0} = x^\alpha$ is equivalent to $z_0^x = z_0x^{1-\alpha}$. We claim that Ω_3^3 sends y_0 to $y_0^x = x^9z^{-3}y_0$. Indeed, the hypothesis $k\equiv -1 \mod 3$ implies $1+\alpha+\alpha^2\equiv 3 \mod 27$, so

$$z^{\Omega_3} = (z_0^3)^{\Omega_3} = (z_0x^{-k})^3 = z_0^3x^{-k(1+\alpha+\alpha^2)} = z_0^3x^{-3k} = zx^{-3k},$$

and therefore $(z^{-1})^{\Omega_3} = z^{-1}x^{3k}$. By definition, we also have $y_0^{\Omega_3} = z^{-1}y_0^{-2}$, so

$$y_0^{\Omega_3^2} = z^{-1}x^{3k}(z^{-1}y_0^{-2})^{-2} = z^{-1}x^{3k}(y_0^2z)^2 = x^{3k}(y_0^2)^zy_0^2z = x^{3k}y_0^{-5}z,$$

$$y_0^{\Omega_3^3} = x^{3k}(z^{-1}y_0^{-2})^{-5}zx^{-3k} = x^{3k}(y_0^2z)^5zx^{-3k} = x^{3k}z^5y_0^{2\times 10(1+10+\cdots+10^4)}zx^{-3k} = x^{3k}z^5y_0^{10}zx^{-3k},$$

since $(10^5-1)/9\equiv 14 \mod 27$, so $2\times 10\times 14\equiv 10 \mod 27$. As $x^9y_0^9 = 1$ and $[x^3, z] = 1 = [x^3, y_0]$, we infer

$$y_0^{\Omega_3^3} = z^5y_0^{10}z = z^5y_0^9y_0z = x^{-9}z^6y_0^z = x^{-9}z^6y_0^{10} = x^9z^{-3}y_0,$$

as required. This produces the required extension, where Ω_3 is conjugation by x_0. We see that $\langle x_0, y_0, z_0\rangle$ has defining relations:

$$x_0^{81} = 1,\ y_0^{x_0} = z_0^{-3}y_0^{-2},\ x_0^{27}y_0^9 = 1,\ z_0^{27} = 1,\ x_0^{z_0} = x_0^{\alpha},\ {}^{z_0}y_0 = y_0^{\alpha}.$$

Observe that $x_0^{z_0} = x_0^{\alpha}$ is equivalent to $z_0^{x_0} = z_0x_0^{1-\alpha} = z_0x_0^{-3k} = z_0x^{-k}$, and that $y_0^{x_0} = z_0^{-3}y_0^{-2}$ implies $(x_0^3)^{y_0} = x^{y_0} = x^{-8}z_0^9 = x_0^{-24}z_0^9$. Indeed, we have just seen that $x_0^{-3}y_0x_0^3 = y_0^{x_0^3} = y_0^x = y_0z_0^{-9}x^9 = y_0z_0^{-9}x_0^{27}$, so $(x_0^{-3})^{y_0} = z_0^{-9}x_0^{24}$.

We finally construct a cyclic extension $\langle x_0, y_1, z_0\rangle$ of $\langle x_0, y_0, z_0\rangle$ of order 3^{10}, where $y_1^3 = y_0$, by means of an automorphism Ω_4 of $\langle x_0, y_0, z_0\rangle$ that fixes y_0 and such that Ω_4^3 is conjugation by y_0. With this goal in mind, we consider the assignment

$$x_0 \mapsto x_0z_0,\ y_0 \mapsto y_0,\ z_0 \mapsto y_0^kz_0.$$

We proceed to show that the defining relations of $\langle x_0, y_0, z_0\rangle$ are preserved.

We have $(x_0z_0)^{81} = z_0^{81}x_0^{\alpha(\alpha^{81}-1)/(\alpha-1)} = 1$, because $(\alpha^{81}-1)/(\alpha-1) \equiv 0 \mod 81$.

We next claim that $y_0^{x_0z_0} = (y_0^kz_0)^{-3}y_0^{-2}$. Indeed, on the one hand, we have $y_0^{x_0z_0} = (z_0^{-3}y_0^{-2})^{z_0} = z_0^{-3}y_0^{-2\beta}$, and on the other hand, since $1+\alpha+\alpha^2 \equiv 3 \mod 27$, we have $(y_0^kz_0)^3 = y_0^{k(1+\alpha+\alpha^2)}z_0^3 = y_0^{3k}z_0^3$, so $(y_0^kz_0)^{-3}y_0^{-2} = z_0^{-3}y_0^{-3k-2}$, and we are left to show that $2\beta \equiv 3k+2 \mod 27$ or, equivalently, $(3k+2)(3k+1) \equiv 2 \mod 27$, which is true because $k \equiv -1 \mod 3$.

We next prove that $(x_0z_0)^{27}y_0^9 = 1$. This is equivalent to $(x_0z_0)^{27} = x_0^{27}$, which is true, since $(x_0z_0)^{27} = z_0^{27}x_0^{\alpha(\alpha^{27}-1)/(\alpha-1)}$, $z_0^{27} = 1$, and $(\alpha^{27}-1)/(\alpha-1) \equiv 27 \mod 81$.

We next show that $(y_0^kz_0)^{27} = 1$. We already computed $(y_0^kz_0)^3 = y_0^{3k}z_0^3$, where $y_0^3 = y$ and $z_0^3 = z$ commute, so $(y_0^kz_0)^{27} = (y_0^{3k}z_0^3)^9 = y_0^{27k}z_0^{27} = 1$.

Next, from ${}^{z_0}y_0 = y_0^{\alpha}$, we derive ${}^{y_0^kz_0}y_0 = y_0^{\alpha}$, so the sixth relation is also preserved.

As for the fifth and last relation, we need to see that $(x_0z_0)^{y_0^kz_0} = (x_0z_0)^{\alpha}$. We have,

$$(x_0z_0)^{\alpha} = z_0^{\alpha}x_0^{\alpha(1+\alpha+\cdots+\alpha^{\alpha-1})}.$$

To find a formula for $x_0^{y_0}$, we start with $x_0^{-1}y_0x_0 = y_0^{x_0} = z_0^{-3}y_0^{-2}$, and derive

$$(x_0^{-1})^{y_0}x_0 = y_0^{-1}x_0^{-1}y_0x_0 = y_0^{-1}z_0^{-3}y_0^{-2} = y_0^{-1}z_0^{-3}y_0y_0^{-3} = (z^{-1})^{y_0}y^{-1}.$$

Here we use the given relation $z^{y_0} = y_0^{-9}z = y^{-3}z$ to deduce $(z^{-1})^{y_0} = z^{-1}y^3$, where y and z commute. Thus

$$(x_0^{-1})^{y_0} = (z^{-1})^{y_0}y^{-1}x_0^{-1} = z^{-1}y^2x_0^{-1},$$

$$x_0^{y_0} = x_0 y^{-2} z.$$

Repeatedly using $x_0^{y_0} = x_0 y^{-2} z$, $z^{y_0} = y^{-3} z$, $y^9 = 1$, and $[y, z] = 1$, we find that

$$x_0^{y_0} = x_0 y^7 z,\ x_0^{y_0^2} = x_0 y^2 z^2,\ x_0^{y_0^3} = x_0 y^3 z^3,\ x_0^{y_0^4} = x_0 y z^4,\ x_0^{y_0^5} = x_0 y^5 z^5,$$

$$x_0^{y_0^6} = x_0 y^6 z^6,\ x_0^{y_0^7} = x_0 y^4 z^7,\ x_0^{y_0^8} = x_0 y^8 z^8,\ x_0^{y_0^9} = x_0,$$

where the last relation is compatible with $x_0^{27} y_0^9 = 1$. Since $k \in \mathbb{N}$ and $k \equiv -1 \mod 3$, we deduce

$$x_0^{y_0^k} = x_0 y^k z^k.$$

On the other hand, from $z_0 y_0 z_0^{-1} = {}^{z_0} y_0 = y_0^\alpha$, we derive $y_0^{-1} z_0 y_0 z_0^{-1} = y_0^{\alpha-1}$, so $z_0^{y_0} = y_0^{\alpha-1} z_0$, and therefore

$$z_0^{y_0^k} = y_0^{(\alpha-1)k} z_0 = y_0^{3k^2} z_0 = y^{k^2} z_0.$$

It follows that

$$(x_0 z_0)^{y_0^k} = x_0 y^k z^k y^{k^2} z_0 = x_0 y^{k(k+1)} z_0^\alpha,$$

$$(x_0 z_0)^{y_0^k z_0} = (x_0 y^{k(k+1)} z_0^\alpha)^{z_0} = x_0^\alpha y^{k(k+1)\beta} z_0^\alpha.$$

Here $k + 1 \equiv 0 \mod 3$, $\beta \equiv 1 \mod 3$, and $y^9 = 1$, so

$$(x_0 z_0)^{y_0^k z_0} = x_0^\alpha y^{k(k+1)} z_0^\alpha.$$

Now $k + 1 = 3u$ with $u \in \mathbb{N}$. Making use of relations $x^9 y^3 = 1$, $x_0^3 = x$, and $y^9 = 1$, we see that

$$y^{k(k+1)} = y^{(-1+3u)3u} = y^{-3u} = x^{9u} = x_0^{27u},$$

$$(x_0 z_0)^{y_0^k z_0} = x_0^\alpha x_0^{27u} z_0^\alpha.$$

Thus, we are left to show that

$$z_0^\alpha x_0^{\alpha(1+\alpha+\cdots+\alpha^{\alpha-1})} = x_0^\alpha x_0^{27u} z_0^\alpha. \tag{4.36}$$

From $x_0^{z_0} = x_0^\alpha$, $\alpha \equiv 1 \mod 3$, and $x_0^{81} = 1$, we see that $[x_0^{27}, z_0] = 1$. Thus (4.36) is equivalent to

$$x_0^{\alpha(1+\alpha+\cdots+\alpha^{\alpha-1})} = x_0^{\alpha\alpha^\alpha} x_0^{27u},$$

that is,

$$x_0^{-27u} = x_0^{\alpha\gamma}.$$

Assume first $v_3(k+1) \geq 2$. Then $3|u$, so $x_0^{-27u} = 1$. Moreover, $v_3(\gamma) \geq 4$ by Proposition 3.1, so $x_0^{\alpha\gamma} = 1$ as well. Suppose next that $v_3(k+1) = 1$. Then $v_3(\gamma) = 3$ with $\gamma = 27t$, $t \in \mathbb{N}$,

and $t \equiv -u \mod 3$ by Proposition 3.1, so $\alpha\gamma \equiv (1+3k)27t \equiv 27t \equiv -27u \mod 81$, and $x_0^{\alpha\gamma} = x_0^{-27u}$. This proves that the fifth defining relation of $\langle x_0, y_0, z_0\rangle$ is preserved. Thus the above assignment extends to an endomorphism Ω_4 of $\langle x_0, y_0, z_0\rangle$, which is clearly surjective and hence an automorphism. We next verify that Ω_4^3 agrees with conjugation by y_0 on x_0, y_0, and z_0. This is obvious for y_0. Moreover, from $z_0^{\Omega_4} = y_0^k z_0$, we infer $z_0^{\Omega_4^3} = y_0^{3k} z_0 = y_0^{\alpha-1} z_0$, which is indeed equal to $z_0^{y_0}$ is indicated earlier. Applying the definition of Ω_4 twice yields

$$x_0^{\Omega_4^2} = x_0 z_0 y_0^k z_0 = x_0 y_0^{k\alpha} z_0^2,$$

and a third application gives

$$x_0^{\Omega_4^3} = x_0 z_0 y_0^{k\alpha} (y_0^k z_0)^2 = x_0 y_0^{k(\alpha+2\alpha^2)} z.$$

On the other hand, we computed earlier $x_0^{y_0} = x_0 y^{-2} z$, and we are reduced to demonstrate that $k(\alpha+2\alpha^2) \equiv -6 \mod 27$. Making the substitution $\alpha = 1+3k$, with $k = -1+3u$, we see that this congruence holds. This produces the required extension, where Ω_4 is conjugation by y_1. Thus $x_0^{y_1} = x_0 z_0$, so $z_0 = [x_0, y_1]$, which implies that $\langle x_0, y_1, z_0\rangle = \langle x_0, y_1\rangle$. Moreover, we have $x_0^{z_0} = x_0^{z_0}$ and $y_1^{-1} z_0 y_1 = z_0^{y_1} = y_0^k z_0 = y_1^{3k} z_0$, so $z_0 y_1 z_0^{-1} = y_1^{1+3k}$, that is, ${}^{z_0}y_1 = y_1^{\alpha}$. Finally, we also have $x_0^{81} = 1 = y_1^{81}$, with $|\langle x_0, y_1\rangle| = 3^{10}$, so the proof is complete. □

Chapter 5

Automorphism Group of the Sylow 2-subgroup, J, of G

In this chapter we restrict ourselves to Case 2 and study the automorphism group of J.

Recall the definition of T^n given in Chapter 2 for a group T and $n \in \mathbb{N}$.

From Theorem 4.3 we have

$$J = \langle\, A, B \mid A^{[A,B]} = A^{\alpha},\ B^{[B,A]} = B^{\alpha},\ A^{2^{3m-1}} = 1,\ B^{2^{3m-1}} = 1 \,\rangle, \quad C = [A, B]. \tag{5.1}$$

Let θ be the automorphism of J satisfying $A \leftrightarrow B$, $C \leftrightarrow C^{-1}$.

In Sections 4.2 and 4.3 we saw that the following relations hold:

$$A^{2^{2m-1}} B^{2^{2m-1}} = 1,\ A^{2^{3m-2}} = B^{2^{3m-2}} = C^{2^{2m-1}}. \tag{5.2}$$

By Proposition 4.20, $Z_3(J)$ is an abelian group of order 2^{4m-2}, and J has exponent 2^{3m-1}.

If $m = 1$, by Proposition 4.18, J is nilpotent of class 3, and isomorphic to the generalized quaternion group $Q = \langle\, u, v \mid u^4 = v^2,\ u^v = u^{-1} \,\rangle$ of order 16. We thus have $\mathrm{Aut}(Q) = \mathrm{Hol}(\mathbb{Z}/8\mathbb{Z})$, the holomorph of the cyclic group of order 8; $Q/Z_1(Q) \cong D_8$, the dihedral group of order 8, with $\mathrm{Aut}(D_8) = D_8$; $Q/Z_2(Q) \cong (\mathbb{Z}/2\mathbb{Z})^2$, with $\mathrm{Aut}((\mathbb{Z}/2\mathbb{Z})^2) = \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$.

5.1 Structural formulas for J

We fix the following integers throughout this chapter: $s = 2^{m-1}$, $u = s^2$, as well as $r = s/2$ provided $m > 1$. In this notation, we have $|A| = 4us = |B|$, $|C| = 4u$, $A^{2u}B^{2u} = 1$, $A^{2us} = C^{2u} = B^{2us}$, and $Z_1(J) = \langle A^{2u} \rangle$.

For all $n \in \mathbb{Z}$, define

$$\phi(n) = \frac{n(n-1)}{2}, \qquad \varphi(n) = \frac{n(n-1)(n-2)}{6}.$$

All statements below are useful when dealing with automorphisms of J, but since their proof is tedious and requires a lot of calculations we put them in the appendix in Section 5.6.

Theorem 5.3. *For all $n, t \in \mathbb{Z}$ the following identities hold in J:*

$$[C^n, A^t] = A^{-2s\ell nt - 4u\ell^2\phi(n)t}, \tag{5.4}$$

$$[C^n, B^t] = B^{2s\ell nt - 4u\ell^2\phi(n+1)t}, \tag{5.5}$$

$$[A^n, B^t] = A^{\exp A} B^{\exp B} C^{\exp C} A^{\xi_1}, \tag{5.6}$$

where $\exp A = -2s\ell\phi(n)t$, $\exp B = 2s\ell n\phi(t)$, $\exp C = nt - 2s\ell\phi(n)\phi(t)$, *and*

$$\xi_1(n,t) = 2u\ell^2\{2\varphi(n+1)t + (2n-7)\phi(n)\phi(t) - 2n\phi(t) - (3n+1)n\varphi(t)\}.$$

Theorem 5.7. *Let $i, j, k, a, b, c \in \mathbb{Z}$. Then $(A^iB^jC^k)(A^aB^bC^c) = A^{\exp A}B^{\exp B}C^{\exp C}A^{\xi_2}$, where*

$$\begin{aligned}
\exp A &= i + a + 2s\ell\{j\phi(a) - ka\},\\
\exp B &= j + b + 2s\ell\{kb - jab - \phi(j)a\},\\
\exp C &= k + c - ja + 2s\ell\{jka - \phi(j+1)\phi(a)\},\\
\xi_2(j,k,a,b) &= 2u\ell^2\{\phi(j)\phi(a)(-2j + 2a - 2b + 5) - 2\phi(j)a(j + k + b - 1)\\
&\quad - j\phi(a)(4k - 2a + 1) + 2\phi(k)(a - b) - ka(j - 2)\\
&\quad - 2j(ab + \varphi(a+1)) + (3a+1)a\varphi(j)\}.
\end{aligned}$$

Corollary 5.8. *Let $a, b, c \in \mathbb{Z}$. Then $(A^aB^bC^c)^{-1} = A^{\exp A}B^{\exp B}C^{\exp C}A^{\xi_3}$, where*

$$\begin{aligned}
\exp A &= -a - 2s\ell(\phi(a+1)b + ac),\\
\exp B &= -b + 2s\ell(a\phi(b+1) + bc),\\
\exp C &= -c - ab - 2s\ell\phi(a+1)\phi(b),\\
\xi_3 &= 4u\ell^2\{a\phi(b) - \phi(a)b\}c + \xi_2(0, -c, -a - 2s\ell\phi(a+1)b, -b + 2s\ell a\phi(b+1))\\
&\quad + \xi_2(-b, 0, -a, 0).
\end{aligned}$$

Proposition 5.9. *Let $i, j, k, a, b, c \in \mathbb{Z}$. Then*

$$[A^iB^jC^k, A^aB^bC^c] \equiv A^{\exp A}B^{\exp B}C^{\exp C} \mod Z_1(J),$$

where

$$\begin{aligned}
\exp A &= 2s\ell\{j\phi(a) - \phi(i)b + ic - ka\},\\
\exp B &= 2s\ell\{i\phi(b) - \phi(j)a + kb + j(ib - ab - c)\},\\
\exp C &= ib - ja + 2s\ell\{\phi(a)(\phi(j) + jb) - \phi(i)(\phi(b) + jb) + ijc - kab\}.
\end{aligned}$$

Theorem 5.10. *Let $a, b, c, n, k, t \in \mathbb{Z}$. Then $(A^aB^bC^c)^n = A^{\exp A}B^{\exp B}C^{\exp C}A^{\xi_4}$, where*

$$\begin{aligned}
\exp A &= na + 2s\ell\{a^2b\varphi(n) + (\phi(a)b - ac)\phi(n)\},\\
\exp B &= nb + 2s\ell\{(b(c - ab) - a\phi(b))\phi(n) - 2ab^2\varphi(n)\},\\
\exp C &= nc - ab\phi(n) + 2s\ell\{a^2\phi(b)\varphi(n) + \phi(a)\phi(b)\phi(n) - a^2b^2\sigma_2(1, n)\\
&\qquad - (\phi(a)b - ac)b\varphi(n + 1)\},\\
\xi_4 &= 2u\ell^2\{a(\varphi(b) + 2\phi(b) - 2\phi(c))\phi(n) + a^2(3\varphi(b) - 2b\phi(b))(2\varphi(n) + \phi(n))\\
&\quad + 2a\phi(b)c\varphi(n) - 2a^2b\phi(b)(\sigma_1(1, n) - \varphi(n))\\
&\quad + (2bc + 7\phi(b))(a^2\varphi(n) + \phi(a)\phi(n))\\
&\quad - 2\phi(b)(a + b)(\sigma_1(a, n) - a\varphi(n)) - 2b\sigma_2(a, n)\\
&\quad + (2\phi(b) - 2c - b)(a^2b\sigma_2(1, n) + (\phi(a)b - ac)\varphi(n + 1))\\
&\quad + 2b(a(\phi(a)b - ac) + b^2(\phi(a) - a^2))(\sigma_1(1, n) + \varphi(n + 1))\\
&\quad + 2a^2b^2(a - b)(\sigma_3(n) + \sigma_1(1, n) - \varphi(n))\\
&\quad - 2c((c - ab)b\varphi(n + 1) - 2ab^2\sigma_2(1, n))\\
&\quad + 2b(\sigma_1(ab, n) + (\phi(c + 1) - abc)\phi(n) - ab(2c + 1)\varphi(n))\},
\end{aligned}$$

$$\sigma_1(k, t) = \frac{k\phi(t)(k\phi(t) - 1)}{2}, \quad \sigma_2(k, t) = \frac{k\phi(t)(k^2\phi(t) - 1)}{6},$$

$$\sigma_3(t) = \frac{1}{6}\left(\frac{(t - 1)t(6(t - 1)^3 + 9(t - 1)^2 + t - 2)}{30} - 3\phi(t)^2 + 4\varphi(t) + 2\phi(t)\right).$$

5.2 Order of the terms of the upper central series of J

Unless otherwise stated we assume from now on that $m > 1$. It follows from Proposition 4.14 and Theorem 4.16 that $|Z_1(J)| = 2^m$. By (5.1) and Theorem 4.16, we have $Z_2(J) = \langle A^{2^{2m-1}}\rangle\langle C^{2^{m-1}}\rangle$, so Theorem 4.13, Proposition 4.14, and (5.2) yield $|Z_2(J)| = 2^{2m}$. By (5.1),

there is an epimorphism $f : J \to (\mathbb{Z}/2^{m-1}\mathbb{Z}) \times (\mathbb{Z}/2^{m-1}\mathbb{Z})$, whose kernel contains $Z_4(J)$ by Theorem 4.16. As $|J| = 2^{7m-3}$, we infer $|\ker(f)| = 2^{5m-1}$. But Theorem 4.13 ensures $|Z_4(J)| \geq 2^{5m-1}$, so $Z_4(J) = \ker(f)$ has order 2^{5m-1}. The order of $Z_3(J)$ was indicated in the beginning of this chapter, so we have

$$\begin{gathered} |Z_1(J)| = 2^m,\ |Z_2(J)| = 2^{2m}, |Z_3(J)| = 2^{4m-2},\ |Z_4(J)| = 2^{5m-1}, \\ |J| = 2^{7m-3}, |\mathrm{Inn}(J)| = 2^{6m-3}. \end{gathered} \tag{5.11}$$

5.3 The automorphism group of $K = J/Z_2(J)$

Set $K = J/Z_2(J)$. It follows from (5.1), Theorem 4.16, and Proposition 4.1 that K has presentation

$$K = \langle\, a, b \mid a^{[a,b]} = a^{\alpha},\ b^{[b,a]} = b^{\alpha},\ a^{2^{2m-1}} = 1,\ b^{2^{2m-1}} = 1,\ [a,b]^{2^{m-1}} = 1 \,\rangle, \tag{5.12}$$

and we set $c = [a, b]$. We have an automorphism $a \leftrightarrow b$, $c \leftrightarrow c^{-1}$, say μ, of K.

We deduce from Theorem 4.16 that

$$Z_1(K) = \langle a^{2^m}, b^{2^m} \rangle,\ Z_2(K) = \langle a^{2^{m-1}}, b^{2^{m-1}}, c \rangle. \tag{5.13}$$

The indicated orders from (5.11) yield

$$|Z_1(K)| = 2^{2(m-1)},\ |Z_2(K)| = 2^{3m-1},\ |K| = 2^{5m-3},\ |\mathrm{Inn}(K)| = 2^{3m-1}.$$

We may now deduce from Theorem 4.13 that every element of K can be written in one and only one way in the form $a^i b^j c^k$, where $0 \leq i, j < 2^{2m-1}$ and $0 \leq k < 2^{m-1}$, and that $|a| = |b| = 2^{2m-1}$ and $|c| = 2^{m-1}$.

Proposition 5.14. *For every $x, y \in Z_1(K)$ the assignment $a \mapsto ax,\ b \mapsto$ by extends to a central automorphism $\Omega_{(x,y)}$ of K that fixes $Z_2(K)$ pointwise. Moreover, the corresponding map, say $\Omega : Z_1(K) \times Z_1(K) \to \mathrm{Aut}(K)$, is a group monomorphism whose image is $\mathrm{Aut}_1(K)$. In particular, $|\mathrm{Aut}_1(K)| = 2^{4(m-1)}$.*

Proof. Let $x, y \in Z_1(K)$. Then $[ax, by] = [a, b] = c$ by (2.1). As $Z_1(K)$ has exponent 2^{m-1}, the defining relations of K are preserved. This yields an endomorphism $\Omega_{(x,y)}$ of K. Note that $\Omega_{(x,y)}$ fixes $Z_2(K)$ pointwise, because $c \mapsto [ax, by] = c$, and

$$a^{2^m} \mapsto (ax)^{2^m} = a^{2^m} x^{2^m} = a^{2^m},\ b^{2^m} \mapsto (by)^{2^m} = b^{2^m} y^{2^m} = b^{2^m}.$$

It is now easy to see that $\Omega_{(x,y)} \circ \Omega_{(x',y')} = \Omega_{(x,y)(x',y')}$. As $\Omega_{(1,1)} = 1_K$, each $\Omega_{(x,y)}$ is an automorphism of K. It is clear that $\Omega_{(x,y)}$ is trivial only when (x, y) is trivial. Finally, by definition, every central automorphism of K must be of the form $\Omega_{(x,y)}$ for some $x, y \in Z_1(K)$. □

Proposition 5.15. *We have* $\mathrm{Inn}(K) \cap \mathrm{Aut}_1(K) = \langle c\delta, a^{2^{m-1}}\delta, b^{2^{m-1}}\delta \rangle$, $|\mathrm{Inn}(K) \cap \mathrm{Aut}_1(K)| = 2^{m+1}$, $|\mathrm{Inn}(K)\mathrm{Aut}_1(K)| = 2^{6m-6}$, *and* $\mathrm{Inn}(K)\mathrm{Aut}_1(K) \subseteq \mathrm{Aut}_2(K)$.

Proof. Given that $Z_2(K)/Z_1(K)$ is generated by the cosets of $a^{2^{m-1}}$, $b^{2^{m-1}}$, c and has order 2^{m+1}, we deduce that $Z_2(K)/Z_1(K) \cong \mathrm{Inn}(K) \cap \mathrm{Aut}_1(K) = \langle a^{2^{m-1}}\delta, b^{2^{m-1}}\delta, c\delta \rangle$ has order 2^{m+1}.

We infer from Proposition 5.14 that $|\mathrm{Inn}(K)\mathrm{Aut}_1(K)| = 2^{6m-6}$. On the other hand, it is obvious that $\mathrm{Aut}_1(K) \subseteq \mathrm{Aut}_2(K)$. As $b^a = bc^{-1}$, $a^b = ac$, with $c \in Z_2(K)$, we deduce that $\mathrm{Inn}(K)$ is included in $\mathrm{Aut}_2(K)$ as well. □

Recalling the meaning of s and u, as given in Section 5.1, we have $a^{2u} = 1 = b^{2u}$, $c^s = 1$, $Z_1(K) = \langle a^{2s}, b^{2s} \rangle$, and $Z_2(K) = \langle a^s, b^s, c \rangle$.

The following three corollaries are consequences of the main results of Section 5.1.

Corollary 5.16. *For all* $n, t \in \mathbb{Z}$ *the following identities hold in* K*:*

$$\begin{aligned}
[c^n, a^t] &= a^{-2s\ell nt}, \\
[c^n, b^t] &= b^{2s\ell nt}, \\
[a^n, b^t] &= a^{-2s\ell\phi(n)t} b^{2s\ell n\phi(t)} c^{nt - 2s\ell\phi(n)\phi(t)}.
\end{aligned}$$

Corollary 5.17. *Let* $i, j, k, n, t, q \in \mathbb{Z}$. *Then* $[a^i b^j c^k, a^n b^t c^q] \equiv c^{it-jn} \mod Z_1(K)$.

Note 5.18. Given $x, y \in K$, there exist $t \in \mathbb{Z}$ and $z \in Z_1(K)$ such that $[x, y]^s = (c^t z)^s$, so $[x, y]^s = 1$.

Corollary 5.19. *Let* $i, j, k, n \in \mathbb{Z}$. *Then* $(a^i b^j c^k)^n = a^{\exp a} b^{\exp b} c^{\exp c}$, *where*

$$\begin{aligned}
\exp a &= ni + 2s\ell\{i^2 j\varphi(n) + (\phi(i)j - ik)\phi(n)\}, \\
\exp b &= nj + 2s\ell\{(j(k - ij) - i\phi(j))\phi(n) - 2ij^2\varphi(n)\}, \\
\exp c &= nk - ij\phi(n).
\end{aligned}$$

Note 5.20. If $s \mid \phi(n)$, then $s \mid \varphi(n)$ and $(a^i b^j c^k)^n = a^{ni} b^{nj} c^{nk}$. Thus, the exponent of K is $2u$.

It follows from Notes 5.18 and 5.20 that for any $x, y \in K$, the assignment $a \mapsto x, b \mapsto y$ extends to an endomorphism of K if and only if it preserves the first and second defining relations of K.

Corollary 5.21. *Let $i, j, k, n, t, q \in \mathbb{Z}$. Then $(a^i b^j c^k)(a^n b^t c^q) = a^{\exp a} b^{\exp b} c^{\exp c}$, where*

$$\begin{aligned}\exp a &= i + n + 2s\ell\{j\phi(n) - kn\},\\ \exp b &= j + t + 2s\ell\{kt - jnt - \phi(j)n\},\\ \exp c &= k + q - jn.\end{aligned}$$

Proposition 5.22. *For any $x, y \in Z_2(K)$, the assignment $a \mapsto ax$, $b \mapsto$ by extends to a 2-central automorphism $\Gamma_{(x,y)}$ of K that fixes $Z_1(K)$ and $Z_2(K)/Z_1(K)$ pointwise. Thus, $|\mathrm{Aut}_2(K)| = 2^{6m-2}$ and the map $g : Z_2(K) \times Z_2(K) \to \mathrm{Aut}_2(K)/\mathrm{Aut}_1(K)$, given by $(x, y) \mapsto \Gamma_{(x,y)}\mathrm{Aut}_1(K)$ is a group epimorphism with kernel $Z_1(K)^2$, so that $\mathrm{Aut}_2(K)/\mathrm{Aut}_1(K) \cong (Z_2(K)/Z_1(K))^2$.*

Proof. Let $x, y \in Z_2(K)$. Then $x = a^{si} b^{sj} c^k$ and $y = a^{sn} b^{st} c^q$ for some $i, j, k, n, t, q \in \mathbb{Z}$.

By (2.1), we have

$$[ax, by] \equiv [a, b] \mod Z_1(K). \tag{5.23}$$

Since $Z_2(K)$ is abelian, $[x, c] = 1$. Then

$$(ax)^{[ax,by]} = (ax)^c = a^c a^{si} b^{sj} c^k = a^{\alpha+si} b^{sj} c^k.$$

As $s \mid \phi(\alpha)$, Note 5.20 gives

$$(ax)^\alpha = (a^{1+si} b^{sj} c^k)^\alpha = a^{\alpha(1+si)} b^{\alpha sj} c^{\alpha k} = a^{\alpha+si} b^{sj} c^k.$$

Thus $(ax)^{[ax,by]} = (ax)^\alpha$. By the automorphism $a \leftrightarrow b$, $(by)^{[by,ax]} = (by)^\alpha$. Thus all defining relations of K are preserved and the given assignment extends to an endomorphism $\Gamma_{(x,y)}$ of K.

Since $s \mid \phi(2sn)$, Note 5.20 gives

$$a^{2s}\Gamma_{(x,y)} = (a^{1+si} b^{sj} c^k)^{2s} = a^{2s(1+si)} b^{2uj} c^{2sk} = a^{2s},$$

and likewise for b, so $\Gamma_{(x,y)}$ fixes $Z_1(K)$ and the nilpotency of K ensures $\Gamma_{(x,y)}$ is an automorphism.

By Corollary 5.19 there exists $z_1 \in Z_1(K)$ such that

$$a^s\Gamma_{(x,y)} = (a^{1+si} b^{sj} c^k)^s = a^{s(1+si)} b^{uj} c^{sk-(1+si)sj\phi(s)} z_1 = a^s(a^{ui} b^{uj} z_1).$$

Applying the automorphism $a \leftrightarrow b$ to the above equality yields $(by)^s = b^s(b^{un}a^{ub}z_2)$ for some $z_2 \in Z_1(K)$, so $b^s\Gamma_{(x,y)} = b^s(b^{un}a^{ub}z_2)$. Also, from (5.23), there exists $z \in Z_1(K)$ such that $c\Gamma_{(x,y)} = cz$. Thus $\Gamma_{(x,y)}$ fixes $Z_2(K)/Z_1(K)$ pointwise. □

Proposition 5.24. *For $n, t \in \mathbb{Z}$ such that $nt \equiv 1 \mod 2^{2m-1}$, the assignment*

$$a \mapsto a^n,\ b \mapsto b^t \tag{5.25}$$

extends to an automorphism f_n of K. The corresponding map $f : (\mathbb{Z}/2^{2m-1}\mathbb{Z})^\times \to \mathrm{Aut}(K)$ is a group monomorphism, whose image will be denoted by S.

Proof. Since $[a, b] \in Z_2(K)$, (2.1) yields

$$[a^n, b^t] \equiv [a, b]^{nt} \equiv [a, b] \mod Z_1(K). \tag{5.26}$$

This implies that the first two defining relations of K are preserved, which produces an endomorphism f_n of K. As f is clearly a homomorphism, f_n has inverse f_t and is then an automorphism. Evidently, f is a monomorphism. □

We have that $|S| = \varphi(2^{2m-1}) = 2^{2m-2} = 2^m\varphi(2^{m-1})$, where φ is Euler's totient function.

Proposition 5.27. *We have $f_n \in \mathrm{Aut}_2(K)$ if and only if $n \equiv 1 \mod 2^{m-1}$. Moreover,*

$$\mathrm{Aut}_2(K) \cap S = \langle f_{1+2^{m-1}} \rangle,\ |\mathrm{Aut}_2(K) \cap S| = 2^m,\ S/(\mathrm{Aut}_2(K) \cap S) \cong (\mathbb{Z}/2^{m-1}\mathbb{Z})^\times.$$

Proof. Note that $f_n \in \mathrm{Aut}_2(K)$ if and only if $a^{n-1}, b^{t-1} \in Z_2(K) = \langle a^{2^{m-1}}, b^{2^{m-1}}, c \rangle$. The normal form of the elements of K makes the last condition equivalent to $n \equiv 1 \mod 2^{m-1}$.

Let T be the kernel of the canonical group epimorphism $(\mathbb{Z}/2^{2m-1}\mathbb{Z})^\times \to (\mathbb{Z}/2^{m-1}\mathbb{Z})^\times$. Thus, T corresponds to $\mathrm{Aut}_2(K) \cap S$ under f, whence

$$\mathrm{Aut}_2(K)S/\mathrm{Aut}_2(K) \cong S/(\mathrm{Aut}_2(K) \cap S) \cong (\mathbb{Z}/2^{2m-1}\mathbb{Z})^\times/T \cong (\mathbb{Z}/2^{m-1}\mathbb{Z})^\times.$$

Moreover, as $|T| = \varphi(2^{2m-1})/\varphi(2^{m-1}) = 2^m$, it follows that $|\mathrm{Aut}_2(K) \cap S| = 2^m$. But $f_{1+2^{m-1}}$ is in $\mathrm{Aut}_2(K) \cap S$ and has order 2^m, so it generates $\mathrm{Aut}_2(K) \cap S$. □

Proposition 5.28. *The assignment $a \mapsto ab^r,\ b \mapsto b$ extends to an automorphism, say Φ, of K.*

Proof. By Corollary 5.17, $[ab^r, b] \equiv c \mod Z_1(K)$ and, by Corollary 5.16, $[b^r, c] = b^u$, so

$$(ab^r)^{[ab^r,b]} = (ab^r)^c = a^\alpha b^{r+u}.$$

On the other hand, Note 5.20 ensures that

$$(ab^r)^\alpha = a^\alpha b^{\alpha r} = a^\alpha b^{r+u}.$$

Thus $(ab^r)^{[ab^r,b]} = (ab^r)^\alpha$ and the given assignment extends to an endomorphism Φ of K. Since ab^r and b generate K, then Φ is surjective and hence an automorphism. □

In agreement with our convention on function composition, if V is a module over a commutative ring R with identity and V admits a finite basis $\{v_1, \ldots, v_n\}$, in order to make the correspondence between $\mathrm{Aut}(V)$ and $\mathrm{GL}_n(R)$ an isomorphism, we will construct the matrix of a given automorphism of V row by row instead of column by column.

Theorem 5.29. *The canonical map $P : \mathrm{Aut}(K) \to \mathrm{Aut}(K/Z_2(K))$ is a group homomorphism with kernel $\mathrm{Aut}_2(K)$ and image $(S\langle\mu, \Phi\rangle)^P$, so that $\mathrm{Aut}(K) = \mathrm{Aut}_2(K)S\langle\mu, \Phi\rangle$. Moreover, if $m > 2$ then $\mathrm{Aut}(K)/\mathrm{Aut}_2(K) \cong ((\mathbb{Z}/2^{m-1}\mathbb{Z})^\times \times (\mathbb{Z}/2\mathbb{Z})^2) \rtimes \mathbb{Z}/2\mathbb{Z}$, with $\mathbb{Z}/2\mathbb{Z}$ acting by inversion on $(\mathbb{Z}/2^{m-1}\mathbb{Z})^\times$ and by switching factors on $(\mathbb{Z}/2\mathbb{Z})^2$, and if $m = 2$ then $\mathrm{Aut}(K)/\mathrm{Aut}_2(K) \cong \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$. In particular, $\mathrm{Aut}(K)$ has order 2^{7m-1} if $m > 2$, and $2^{11} \times 3$ if $m = 2$, in which case P is surjective. Furthermore, if $m > 2$ (resp. $m = 2$) then every element of $\mathrm{Aut}(K)$ can be written uniquely in the form $gf_n\Phi^i(\Phi^\mu)^j\mu^k$ (resp. $g(\mu\Phi)^i\mu^k$), where $g \in \mathrm{Aut}_2(K)$, $1 \le n < 2^{m-1}$ is odd, and $0 \le i, j, k \le 1$ (resp. $0 \le i \le 2$ and $0 \le k \le 1$).*

Proof. Note that $K/Z_2(K)$ is a free module over $\mathbb{Z}/2^{m-1}\mathbb{Z}$ of rank 2, so P gives rise to a homomorphism $D : \mathrm{Aut}(K) \to (\mathbb{Z}/2^{m-1}\mathbb{Z})^\times$, $\Psi \mapsto D_\Psi$, the determinant of Ψ^P.

Let $\Psi \in \mathrm{Aut}(K)$. Then

$$a^\Psi = a^i b^j z,\ b^\Psi = a^e b^f w \quad i, j, e, f \in \mathbb{N}, z, w \in Z_2(K).$$

Let d be any positive integer that maps into D_Ψ under $\mathbb{Z} \to \mathbb{Z}/2^{m-1}\mathbb{Z}$. Since $c \in Z_2(K)$, we have

$$c^\Psi \equiv [a^i b^j z, a^e b^f w] \equiv c^{if-je} \equiv c^d \mod Z_1(K). \tag{5.30}$$

Taking $z = a^{sg}b^{sh}c^k$ with $g, h, k \in \mathbb{Z}$ and applying Corollary 5.21, we obtain $a^i b^j z = a^{i+sg+ujg} b^{j+sh} c^k$. Thus, Note 5.20 yields

$$(a^i b^j z)^\alpha = a^{\alpha(i+sg+ujg)} b^{\alpha(j+sh)} c^{\alpha k} = a^{i+sg+ujg+2s\ell i} b^{j+sh+2s\ell j} c^k.$$

Since $\alpha^d \equiv 1 + 2s\ell d \mod 2u$, $(1 - 2s\ell)^d \equiv 1 - 2s\ell d \mod 2u$, and $b^c = b^{1-2s\ell}$, we have

$$(a^i b^j z)^{c^d} = a^{\alpha^d(i+sg+ujg)} b^{(1-2s\ell)^d(j+sh)} c^k = a^{i+sg+ujg+2s\ell id} b^{j+sh-2s\ell jd} c^k.$$

As Ψ preserves the relations $a^c = a^\alpha$ and $b^c = b^\alpha$ it follows from (5.30) that $(a^i b^j z)^{c^d} = (a^i b^j z)^\alpha$ and $(a^e b^f w)^{c^d} = (a^e b^f w)^\alpha$. Therefore, from above, $a^{2s\ell i(d-1)} b^{-2s\ell j(d+1)} = 1$, and similarly, $a^{2s\ell e(d-1)} b^{-2s\ell f(d+1)} = 1$. From this we infer

$$i(d-1) \equiv 0,\ j(d+1) \equiv 0,\ e(d-1) \equiv 0,\ f(d+1) \equiv 0 \mod 2^{m-1}. \tag{5.31}$$

Since d is invertible modulo 2^{m-1}, at least one of i, j must be invertible modulo 2^{m-1} by (5.30).

Assume until further notice that $m > 2$. If $2 \nmid i$ then (5.31) yields $d \equiv 1 \mod 2^{m-1}$, whence $2j \equiv 0 \mod 2^{m-1}$, that is, $j \equiv 0 \mod 2^{m-2}$. Since $m > 2$, we infer $2 \nmid f$. From $d \equiv 1 \mod 2^{m-1}$ we also obtain $2e \equiv 0 \mod 2^{m-1}$, that is, $e \equiv 0 \mod 2^{m-2}$. If $2 \nmid j$ then replacing Ψ by $\mu\Psi$ the previous case yields $D_\Psi = -1$, $2 \nmid e$, and $i, f \equiv 0 \mod 2^{m-2}$.

We have shown that $D_\Psi = \pm 1$ as well as the following: if $D_\Psi = 1$ then $if \equiv 1 \mod 2^{m-1}$ and $j, e \equiv 0 \mod 2^{m-2}$, while if $D_\Psi = -1$ then $je \equiv -1 \mod 2^{m-1}$ and $i, f \equiv 0 \mod 2^{m-2}$.

Going back to the general case $m > 1$, we fix the $\mathbb{Z}/2^{m-1}\mathbb{Z}$-basis $\{aZ_2(K), bZ_2(K)\}$ of $K/Z_2(K)$, and identify $\mathrm{Aut}(K/Z_2(K))$ with $\mathrm{GL}_2(\mathbb{Z}/2^{m-1}\mathbb{Z})$. We then have the following matrices:

$$M_n = f_n^P = \begin{pmatrix} [n] & 0 \\ 0 & [t] \end{pmatrix},\ Q = \mu^P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ R = \Phi^P = \begin{pmatrix} 1 & w \\ 0 & 1 \end{pmatrix},$$

where $z \mapsto [z]$ is the canonical projection $\mathbb{Z} \to \mathbb{Z}/2^{m-1}\mathbb{Z}$, $n \in \mathbb{Z}$ is odd with inverse t modulo 2^{m-1}, and $w = [2^{m-2}]$. Set $U = \{M_n \mid n \in \mathbb{Z},\ n \text{ odd}\}$, a group of order $\varphi(2^{m-1}) = 2^{m-2}$, and $T = R^Q$.

Suppose first $m > 2$. Then $V = U\langle R\rangle\langle T\rangle$ is an abelian group of order 2^m isomorphic to $(\mathbb{Z}/2^{m-1}\mathbb{Z})^\times \times (\mathbb{Z}/2\mathbb{Z})^2$. Moreover, every element of V has determinant 1, so $Q \notin V$, but Q normalizes V, conjugating every M_r into its inverse, and R and T into each other. Therefore $W = V \rtimes \langle Q\rangle$ is a group of order 2^{m+1}. If $D_\Psi = 1$ then $if \equiv 1 \mod 2^{m-1}$ and $j, e \equiv 0 \mod 2^{m-2}$, which makes it obvious that $\Psi^P \in V$. Thus, if $D_\Psi = -1$ then $\Psi^P \in W$. This proves

$$\mathrm{Aut}(K)^P = W = U\langle R\rangle\langle T\rangle\langle Q\rangle = (S\langle\Phi\rangle\langle\Phi^\mu\rangle\langle\mu\rangle)^P.$$

As $\ker(P) = \mathrm{Aut}_2(K)$, we see that $\mathrm{Aut}(K) = \mathrm{Aut}_2(K)S\langle\Phi\rangle\langle\Phi^\mu\rangle\langle\mu\rangle$ and $\mathrm{Aut}(K)/\mathrm{Aut}_2(K) \cong W$. Since $|\mathrm{Aut}_2(K)| = 2^{6m-2}$ by Proposition 5.22, and $|W| = 2^{m+1}$ by the above, we deduce $|\mathrm{Aut}(K)| = 2^{7m-1}$ with uniqueness of expression.

Suppose next $m = 2$. Then T, Q generate $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ and P is surjective, so by Proposition 5.22

$$|\mathrm{Aut}(K)| = |\mathrm{Aut}_2(K)| \times |\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})| = 2^{10} \times 6 = 2^{11} \times 3,$$

with uniqueness of expression and $\mathrm{Aut}(K)/\mathrm{Aut}_2(K) \cong \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$. □

Corollary 5.32. *Every automorphism of K has determinant ± 1 when acting on $K/Z_2(K)$. Moreover, if $m > 2$ then $\mathrm{Aut}_2(K)S\langle\Phi, \Phi^\mu\rangle$ is the kernel of the corresponding determinant map, as well as the pointwise stabilizer of $cZ_1(K)$ when $\mathrm{Aut}(K)$ acts on $K/Z_1(K)$.*

We next obtain a description of $\mathrm{Aut}(K)$ in terms of group extensions.

Theorem 5.33. *We have the following series of normal subgroups of $\mathrm{Aut}(K)$:*

$$1 \subseteq \mathrm{Aut}_1(K) \subseteq \mathrm{Aut}_2(K) \subseteq \mathrm{Aut}(K), \tag{5.34}$$

where $\mathrm{Aut}_1(K) \cong (\mathbb{Z}/2^{m-1}\mathbb{Z})^4$, $\mathrm{Aut}_2(K)/\mathrm{Aut}_1(K) \cong (\mathbb{Z}/2^{m-1}\mathbb{Z})^2 \times (\mathbb{Z}/2\mathbb{Z})^4$, and the factor $\mathrm{Aut}(K)/\mathrm{Aut}_2(K) \cong ((\mathbb{Z}/2^{m-1}\mathbb{Z})^\times \times (\mathbb{Z}/2\mathbb{Z})^2) \rtimes \mathbb{Z}/2\mathbb{Z}$, with $\mathbb{Z}/2\mathbb{Z}$ acting by inversion on $(\mathbb{Z}/2^{m-1}\mathbb{Z})^\times$ and by switching factors on $(\mathbb{Z}/2\mathbb{Z})^2$ if $m > 2$, while $\mathrm{Aut}(K)/\mathrm{Aut}_2(K) \cong \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ if $m = 2$.

Proof. Immediate consequence of Propositions 5.14 and 5.22, and Theorem 5.29. □

Our next result is designed for later use, but it can also be used to insert an additional normal subgroup of $\mathrm{Aut}(K)$ to the series (5.34), namely $\mathrm{Inn}(K)\mathrm{Aut}_1(K)$.

Proposition 5.35. *We have*

$$\mathrm{Aut}_2(K)/\mathrm{Inn}(K)\mathrm{Aut}_1(K) \cong Z_2(K)^2/(Z_1(K) \times \langle c\rangle)^2 \cong (\mathbb{Z}/2\mathbb{Z})^4. \tag{5.36}$$

Moreover, $\mathrm{Aut}_2(K)/\mathrm{Inn}(K)\mathrm{Aut}_1(K)$ is generated by the cosets of $\psi_1, \psi_2, \psi_3, \psi_4 \in \mathrm{Aut}_2(K)$, where these automorphisms are respectively given by

$$a \mapsto a^{1+s}, b \mapsto b;\ a \mapsto a, b \mapsto b^{1+s};\ a \mapsto ab^s, b \mapsto b;\ a \mapsto a, b \mapsto ba^s,$$

and whose existence is ensured by Proposition 5.22.

Proof. Let $g : Z_2(K)^2 \to \mathrm{Aut}_2(K)/\mathrm{Aut}_1(K)$ be the epimorphism defined in Proposition 5.22, and let $\pi : \mathrm{Aut}_2(K)/\mathrm{Aut}_1(K) \to \mathrm{Aut}_2(K)/\mathrm{Inn}(K)\mathrm{Aut}_1(K)$ be the canonical projection.

From $\Gamma_{(1,c^{-1})} = a\delta$ and $\Gamma_{(1,c)} = b\delta$ we deduce $\langle c\rangle^2 g = \mathrm{Inn}(K)\mathrm{Aut}_1(K)/\mathrm{Aut}_1(K) = \ker\pi$. Since $\ker g = Z_1(K)^2$, we deduce $\ker g\pi = (Z_1(K) \times \langle c\rangle)^2$. The first isomorphism theorem now yields (5.36). Moreover, $\mathrm{Aut}_2(K)/\mathrm{Inn}(K)\mathrm{Aut}_1(K)$ is generated by the images of $(a^s, 1), (b^s, 1), (1, a^s), (1, b^s)$ under the epimorphism $Z_2(K)^2 \to \mathrm{Aut}_2(K)/\mathrm{Inn}(K)\mathrm{Aut}_1(K)$, namely the cosets of $\psi_1, \psi_2, \psi_3, \psi_4$. □

All factors of the new series $1 \subseteq \mathrm{Aut}_1(K) \subseteq \mathrm{Inn}(K)\mathrm{Aut}_1(K) \subseteq \mathrm{Aut}_2(K) \subseteq \mathrm{Aut}(K)$ have already been computed, except for the second, which can be determined as follows:

$$\begin{aligned}&\mathrm{Inn}(K)\mathrm{Aut}_1(K)/\mathrm{Aut}_1(K)\\ &\quad\cong \mathrm{Inn}(K)/\mathrm{Aut}_1(K)\cap\mathrm{Inn}(K) \cong K\delta/Z_2(K)\delta \cong K/Z_2(K) \cong (\mathbb{Z}/2^{m-1}\mathbb{Z})^2.\end{aligned}$$

This is compatible with Proposition 5.35 and the structure of $\mathrm{Aut}_2(K)/\mathrm{Aut}_1(K)$.

5.4 The automorphism group of $H = J/Z_1(J)$

Set $H = J/Z_1(J)$. It follows from (5.1), Theorem 4.16, and Proposition 4.1 that H has presentation

$$H = \langle\, A, B \mid A^{[A,B]} = A^{\alpha},\ B^{[B,A]} = B^{\alpha},\ A^{2^{2m-1}} = 1,\ B^{2^{2m-1}} = 1 \,\rangle, \tag{5.37}$$

and we set $C = [A, B]$, noting that $C^{2^{2m-1}} = 1$ by (5.2). Observe the automorphism $A \leftrightarrow B$, $C \leftrightarrow C^{-1}$, say ν, of H. It follows from Theorem 4.16 that

$$Z_1(H) = \langle C^{2^{m-1}}\rangle,\ Z_2(H) = \langle A^{2^m}, B^{2^m}, C^{2^{m-1}}\rangle,\ Z_3(H) = \langle A^{2^{m-1}}, B^{2^{m-1}}, C\rangle.$$

As $Z_3(J)$ is abelian, so is $Z_2(H) \cong Z_3(J)/Z_1(J)$, and (5.11) yields

$$|Z_1(H)| = 2^m,\ |Z_2(H)| = 2^{3m-2},\ |Z_3(H)| = 2^{4m-1},\ |H| = 2^{6m-3},\ |\mathrm{Inn}(H)| = 2^{5m-3}.$$

We may now deduce from Theorem 4.13 that every element of H can be written uniquely in the form $A^iB^jC^k$, where $0 \le i, j, k < 2^{2m-1}$, and that $|A| = |B| = |C| = 2^{2m-1}$.

Recalling the notation of Section 5.1, we have $A^{2u} = B^{2u} = C^{2u} = 1$, $Z_1(H) = \langle C^s\rangle$, $Z_2(H) = \langle A^{2s}, B^{2s}, C^s\rangle$, and $Z_3(H) = \langle A^s, B^s, C\rangle$.

The following four corollaries follow from the main results in Section 5.1.

Corollary 5.38. *For all $n, t \in \mathbb{Z}$ the following identities hold in H:*

$$\begin{aligned}[C^n, A^t] &= A^{-2s\ell nt},\\ [C^n, B^t] &= B^{2s\ell nt},\\ [A^n, B^t] &= A^{-2s\ell\phi(n)t}B^{2s\ell n\phi(t)}C^{nt-2s\ell\phi(n)\phi(t)}.\end{aligned}$$

Corollary 5.39. *Let $i, j, k, a, b, c \in \mathbb{Z}$. Then $(A^iB^jC^k)(A^aB^bC^c) = A^{\exp A}B^{\exp B}C^{\exp C}$, where*

$$\begin{aligned}\exp A &= i + a + 2s\ell\{j\phi(a) - ka\},\\ \exp B &= j + b + 2s\ell\{kb - jab - \phi(j)a\},\\ \exp C &= k + c - ja + 2s\ell\{jka - \phi(j+1)\phi(a)\}.\end{aligned}$$

Corollary 5.40. *Let $i, j, k, a, b, c \in \mathbb{Z}$. Then $[A^iB^jC^k, A^aB^bC^c] = A^{\exp A}B^{\exp B}C^{\exp C}$, where*

$$\begin{aligned}
\exp A &= 2s\ell\{j\phi(a) - \phi(i)b + ic - ka\},\\
\exp B &= 2s\ell\{i\phi(b) - \phi(j)a + kb + j(ib - ab - c)\},\\
\exp C &= ib - ja + 2s\ell\{\phi(a)(\phi(j) + jb) - \phi(i)(\phi(b) + jb) + ijc - kab\}.
\end{aligned}$$

Corollary 5.41. *Let $a, b, c, n, k, t \in \mathbb{Z}$. Then $(A^aB^bC^c)^n = A^{\exp A}B^{\exp B}C^{\exp C}$, where*

$$\begin{aligned}
\exp A &= na + 2s\ell\{a^2b\varphi(n) + (\phi(a)b - ac)\phi(n)\},\\
\exp B &= nb + 2s\ell\{(b(c - ab) - a\phi(b))\phi(n) - 2ab^2\varphi(n)\},\\
\exp C &= nc - ab\phi(n) + 2s\ell\{a^2\phi(b)\varphi(n) + \phi(a)\phi(b)\phi(n) - a^2b^2\sigma_2(1, n)\\
&\qquad - (\phi(a)b - ac)b\varphi(n + 1)\}.
\end{aligned}$$

Note 5.42. If $s \mid \phi(n)$, then $s \mid \varphi(n)$ and $s \mid \varphi(n + 1)$, so

$$(A^aB^bC^c)^n = A^{na}B^{nb}C^{nc - ab\phi(n) - 2s\ell a^2b^2\sigma_2(1,n)}.$$

In particular, $(A^aB^bC^c)^{2u} = C^{uab}$ and the exponent of H is 2^{2m}.

Proposition 5.43. *For every $x, y \in Z_2(H)$ the assignment $A \mapsto Ax$, $B \mapsto By$ extends to a 2-central automorphism $\Pi_{(x,y)}$ of H that fixes $Z_2(H)$ pointwise. Moreover, the corresponding map $\Pi : Z_2(H) \times Z_2(H) \to \mathrm{Aut}(H)$ is a group monomorphism whose image is $\mathrm{Aut}_2(H)$. In particular, $|\mathrm{Aut}_2(H)| = 2^{6m-4}$.*

Proof. By Corollary 5.38, $[B, A^{2sa}] = C^{-2sa}$ and $[C^s, B^{2s}] = 1$. Let $x = A^{2si}B^{2sj}C^{sk}$ as well as $y = A^{2sa}B^{2sb}C^{sc}$. Then

$$By = BA^{2sa}B^{2sb}C^{sc} = A^{2sa}BC^{-2sa}B^{2sb}C^{sc} = A^{2sa}B^{1+2sb}C^{s(c-2a)}.$$

Applying Corollary 5.40 to

$$[Ax, By] = [A^{1+2si}B^{2sj}C^{sk}, A^{2sa}B^{1+2sb}C^{s(c-2a)}] = A^{\exp A}B^{\exp B}C^{\exp C}$$

gives $\exp A \equiv 0 \mod 2u$, $\exp B \equiv 0 \mod 2u$, $\exp C \equiv 1 + 2s(i + b) \mod 2u$, so

$$[Ax, By] = C^{1+2s(i+b)}. \tag{5.44}$$

As $C^{2s(i+b)} \in Z_1(H)$ and, by Corollary 5.38, $[A^{1+2si}, C] = A^{2s\ell}$ and $[B^{2sj}, C] = 1$, then

$$(Ax)^{[Ax,By]} = (A^{1+2si}B^{2sj}C^{sk})^C = A^{\alpha+2si}B^{2sj}C^{sk}.$$

On the other hand, Note 5.42 yields

$$(Ax)^\alpha = (A^{1+2si}B^{2sj}C^{sk})^\alpha = A^{\alpha(1+2si)}B^{\alpha 2sj}C^{\alpha sk} = A^{\alpha+2si}B^{2sj}C^{sk}.$$

Thus $(Ax)^{[Ax,By]} = (Ax)^\alpha$. By the automorphism $A \leftrightarrow B$, $(By)^{[By,Ax]} = (By)^\alpha$.

By Note 5.42, $(Ax)^{2u} = (A^{1+2si}B^{2sj}C^{sk})^{2u} = C^{u(1+2si)(2sj)} = 1$. By the automorphism $A \leftrightarrow B$, $(By)^{2u} = 1$. Thus the given assignment extends to an endomorphism Π of H.

Now, by Note 5.42, $(A^{2s})\Pi_{(x,y)} = (Ax)^{2s} = (A^{1+2si}B^{2sj}C^{sk})^{2s} = A^{2s}$ and, by the automorphism $A \leftrightarrow B$, $(By)^{2s} = B^{2s}$, so $(B^{2s})\Pi_{(x,y)} = B^{2s}$. Also, from (5.44), $(C^s)\Pi_{(x,y)} = [Ax, By]^s = C^s$. Thus $\Pi_{(x,y)}$ fixes $Z_2(H)$ pointwise and the nilpotency of H ensures $\Pi_{(x,y)}$ is an automorphism. We may now continue as in the proof of Proposition 5.14. □

Corollary 5.45. *We have* $\mathrm{Inn}(H) \cap \mathrm{Aut}_2(H) = \langle C\delta, A^{2^{m-1}}\delta, B^{2^{m-1}}\delta \rangle$, $|\mathrm{Inn}(H) \cap \mathrm{Aut}_2(H)| = 2^{3m-1}$, $|\mathrm{Inn}(H)\mathrm{Aut}_2(H)| = 2^{8m-6}$, *and* $\mathrm{Inn}(H)\mathrm{Aut}_2(H) \subseteq \mathrm{Aut}_3(H)$.

Proof. As $Z_3(H)/Z_1(H)$ has order 2^{3m-1} and is generated by the cosets of $C, A^{2^{m-1}}, B^{2^{m-1}}$, it follows that $\mathrm{Inn}(H) \cap \mathrm{Aut}_2(H) = \langle C\delta, A^{2^{m-1}}\delta, B^{2^{m-1}}\delta \rangle$ has order 2^{3m-1}.

We deduce from Proposition 5.43 that $|\mathrm{Inn}(H)\mathrm{Aut}_2(H)| = 2^{8m-6}$. On the other hand, it is obvious that $\mathrm{Aut}_2(K)$ is included in $\mathrm{Aut}_3(K)$. As $B^A = BC^{-1}$, $A^B = AC$, with $C \in Z_3(H)$, it follows that $\mathrm{Inn}(K)$ is also included in $\mathrm{Aut}_3(H)$. □

Proposition 5.46. *The assignment* $A \mapsto A^{1+s}$, $B \mapsto BA^s$ *extends to an automorphism, say* Γ, *of* H *that belongs to* $\mathrm{Aut}_3(H)$.

Proof. By Corollary 5.38, $[B, A^s] = (A^uB^0C^s)^{-1} = A^uC^{-s}$ and $[B, A^u] = (A^0B^0C^u)^{-1} = C^u$, so

$$BA^s = A^sB^{A^s} = A^sBA^uC^{-s} = A^{s+u}BC^{-s+u}.$$

By Corollary 5.40, $[A^{1+s}, BA^s] = [A^{1+s}, A^{s+u}BC^{-s+u}] = A^uB^0C^{1+s} = A^uC^{1+s}$, and by Corollary 5.38, $[A^{1+s}, C^{1+s}] = A^{2s\ell}$. Then

$$(A^{1+s})^{[A^{1+s},BA^s]} = (A^{1+s})^{A^uC^{1+s}} = A^{\alpha+s}.$$

On the other hand, $(A^{1+s})^\alpha = A^{\alpha+s}$. Thus $(A^{1+s})^{[A^{1+s},BA^s]} = (A^{1+s})^\alpha$.

As for the second relation, Corollary 5.38 and (2.1) give, $[BA^s, A^{1+s}] = A^uC^{-1-s}$, $[B, A^u] = C^u$, and $[A^{u+s}, C^{-1}] = 1$, so

$$(BA^s)^{[BA^s,A^{1+s}]} = (A^{s+u}BC^{-s+u})^{A^uC^{-1}} = (A^{s+u}B)^{C^{-1}}C^{-s} = A^{s+u}B^\alpha C^{-s}.$$

On the other hand, Note 5.42 gives

$$(BA^s)^\alpha = (A^{s+u}BC^{-s+u})^\alpha = (A^{s+u}B)^\alpha C^{-s+u} = A^{\alpha(s+u)}B^\alpha C^u C^{-s+u} = A^{s+u}B^\alpha C^{-s}.$$

Also, by Note 5.42, $(A^{1+s})^{2u} = 1$ and $(BA^s)^{2u} = (A^{s+u}BC^{-s+u})^{2u} = C^{u(s+u)} = 1$. Then the given assignment extends to an endomorphism Γ of H.

Since $[C, A^u] = 1$, then $(C^s)\Gamma = [A^{1+s}, BA^s]^s = (A^u C^{1+s})^s = A^{us}C^{(1+s)s} = C^{(1+s)s}$, so the restriction of Γ to $Z_1(H)$ is an automorphism, whence Γ is an automorphism, clearly in $\mathrm{Aut}_3(H)$. □

Proposition 5.47. *Let T be a group, and set $Y = T/Z_1(T)$. Let $\lambda : T \to Y$ be the canonical projection, and consider the associated map $\Lambda : \mathrm{Aut}(T) \to \mathrm{Aut}(Y)$. Then for any $i \geq 0$, Λ maps $\mathrm{Aut}_{i+2}(T)$ into $\mathrm{Aut}_{i+1}(Y)$, and the kernels of the induced maps $\mathrm{Aut}_{i+2}(T) \to \mathrm{Aut}_{i+1}(Y)/\mathrm{Aut}_i(Y)$ and $\mathrm{Inn}(T)\mathrm{Aut}_{i+2}(T) \to \mathrm{Inn}(Y)\mathrm{Aut}_{i+1}(Y)/\mathrm{Inn}(Y)\mathrm{Aut}_i(Y)$ are, respectively, $\mathrm{Aut}_{i+1}(T)$ and $\mathrm{Inn}(T)\mathrm{Aut}_{i+1}(T)$. Thus, $\mathrm{Aut}_{i+2}(T)/\mathrm{Aut}_{i+1}(T)$ is isomorphic to a subgroup of $\mathrm{Aut}_{i+1}(Y)/\mathrm{Aut}_i(Y)$, and the group $\mathrm{Inn}(T)\mathrm{Aut}_{i+2}(T)/\mathrm{Inn}(T)\mathrm{Aut}_{i+1}(T)$ imbeds into $\mathrm{Inn}(Y)\mathrm{Aut}_{i+1}(Y)/\mathrm{Inn}(Y)\mathrm{Aut}_i(Y)$.*

Proof. We first show by induction that λ sends $Z_{i+1}(T)$ onto $Z_i(Y)$ for any $i \geq 0$. The base case $i = 0$ holds by the very definition of λ. Suppose that λ maps $Z_{i+1}(T)$ onto $Z_i(Y)$ for some $i \geq 0$. Let $t \in Z_{i+2}(T)$. Then $[t, \sigma] \in Z_{i+1}(T)$, so $[t^\lambda, \sigma^\lambda] = [t, \sigma]^\lambda \in Z_i(Y)$ for every $\sigma \in T$, whence $t^\lambda \in Z_{i+1}(Y)$. Conversely, if $y \in Z_{i+1}(Y)$, then $y = t^\lambda$ for some $t \in T$. Let $\sigma \in T$. Then $[t, \sigma]^\lambda = [t^\lambda, \sigma^\lambda] \in Z_i(Y)$, so $[t, \sigma]^\lambda = w^\lambda$ for some $w \in Z_{i+1}(T)$, hence $[t, \sigma]w^{-1} \in \ker(\lambda) = Z_1(T)$, and therefore $[t, \sigma] \in Z_1(T)Z_{i+1}(T) = Z_{i+1}(T)$, which implies $t \in Z_{i+2}(T)$. This shows that λ maps $Z_{i+2}(T)$ onto $Z_i(Y)$.

For $t \in T$, we set $\overline{t} = t^\lambda$, and if $g \in \mathrm{Aut}(T)$, then $\overline{g} = g^\Lambda$ is defined by $\overline{t}^{\overline{g}} = \overline{t^g}$. This is well defined, as $Z_1(T)$ is a characteristic subgroup of T.

Let $i \geq 0$. We claim that Λ sends $\mathrm{Aut}_{i+2}(T)$ into $\mathrm{Aut}_{i+1}(Y)$. Indeed, let $g \in \mathrm{Aut}_{i+2}(T)$ and $t \in T$. Then $t^g t^{-1} \in Z_{i+2}(T)$, so $\overline{t^g t^{-1}} \in Z_{i+1}(Y)$ by the above, which means $\overline{t}^{\overline{g}}\overline{t}^{-1} Z_{i+1}(Y)$, so $g^\Lambda \in \mathrm{Aut}_{i+1}(Y)$, as claimed.

By the above, we have a group homomorphism $\eta : \mathrm{Aut}_{i+2}(T) \to \mathrm{Aut}_{i+1}(Y)/\mathrm{Aut}_i(Y)$ with $\mathrm{Aut}_{i+1}(T)$ contained in $\ker(\eta)$, and we claim equality holds. Let $g \in \ker(\eta)$. Then $g^\Lambda \in \mathrm{Aut}_i(Y)$. Let $t \in T$. Then $\overline{t}^{\overline{g}}\overline{t}^{-1} \in Z_i(Y)$, so $\overline{t^g t^{-1}} \in Z_i(Y)$. As λ maps $Z_{i+1}(T)$ onto $Z_i(Y)$, there is some $\sigma \in Z_{i+1}(T)$ such that $\overline{t^g t^{-1}} = \overline{\sigma}$, whence $t^g t^{-1}\sigma^{-1} \in Z_1(T)$, so $t^g t^{-1} \in Z_1(T)Z_{i+1}(T) = Z_{i+1}(T)$, and therefore $g \in \mathrm{Aut}_{i+1}(T)$. Thus $\ker(\eta) = \mathrm{Aut}_{i+1}(T)$, as claimed.

Now, we see that Λ maps $\mathrm{Inn}(T)\mathrm{Aut}_{i+2}(T)$ into $\mathrm{Inn}(Y)\mathrm{Aut}_{i+1}(Y)$, and $\mathrm{Inn}(T)\mathrm{Aut}_{i+1}(T)$ into $\mathrm{Inn}(Y)\mathrm{Aut}_i(Y)$, producing a map $\phi : \mathrm{Inn}(T)\mathrm{Aut}_{i+2}(T) \to \mathrm{Inn}(Y)\mathrm{Aut}_{i+1}(Y)/\mathrm{Inn}(Y)\mathrm{Aut}_i(Y)$ whose kernel contains $\mathrm{Inn}(T)\mathrm{Aut}_{i+1}(T)$, and we claim that $\ker(\phi) = \mathrm{Inn}(T)\mathrm{Aut}_{i+1}(T)$. Indeed, if $g \in \ker(\phi)$, then $g^\Lambda \in \mathrm{Inn}(Y)\mathrm{Aut}_i(Y)$, so that $g^\Lambda = hk$, with $h \in \mathrm{Inn}(Y)$ and $k \in \mathrm{Aut}_i(Y)$. But Λ maps $\mathrm{Inn}(T)$ onto $\mathrm{Inn}(Y)$, so $h = w^\Lambda$ for some $w \in \mathrm{Inn}(T)$, whence $k = (w^{-1}g)^\Lambda$, so by the above $w^{-1}g \in \mathrm{Aut}_{i+1}(T)$ and therefore $g \in \mathrm{Inn}(T)\mathrm{Aut}_{i+1}(T)$, as claimed. □

We apply Proposition 5.47 to the case $T = H$ and $Y = K = H/Z_1(H)$, which has presentation

$$K = \langle\, \rho, \eta \mid \rho^{[\rho,\eta]} = \rho^\alpha,\ \eta^{[\eta,\rho]} = \eta^\alpha,\ \rho^{2^{2m-1}} = 1,\ \eta^{2^{2m-1}} = 1,\ [\rho,\eta]^{2^{m-1}} = 1 \,\rangle.$$

Theorem 5.48. *Let $\lambda : H \to K$ be the projection $A \mapsto \rho$, $B \mapsto \eta$, $\Lambda : \mathrm{Aut}(H) \to \mathrm{Aut}(K)$ the corresponding homomorphism, and*

$$\widehat{\Lambda} : \mathrm{Aut}_3(H)/(\mathrm{Inn}(H)\mathrm{Aut}_2(H)) \hookrightarrow \mathrm{Aut}_2(K)/(\mathrm{Inn}(K)\mathrm{Aut}_1(K))$$

the imbedding associated to Λ, as indicated in Proposition 5.47. Then $\mathrm{Im}(\widehat{\Lambda}) = \langle \overline{\Gamma}, \overline{\Gamma^\nu}\rangle^{\widehat{\Lambda}}$ is isomorphic to the Klein 4-group. Therefore, $\mathrm{Aut}_3(H)$ has order 2^{8m-4} and $\mathrm{Aut}_3(H) = \mathrm{Inn}(H)\mathrm{Aut}_2(H)\langle\Gamma, \Gamma^\nu\rangle$, where Γ is as defined in Proposition 5.46, and ν is the automorphism $A \leftrightarrow B$ of H.

Proof. As $\mathrm{Inn}(H) \subseteq \mathrm{Aut}_3(H)$ and $\mathrm{Inn}(K) \subseteq \mathrm{Aut}_2(K)$, Proposition 5.47 yields the imbedding $\widehat{\Lambda}$.

We claim that $\mathrm{Im}(\widehat{\Lambda}) = \langle \overline{\Gamma}, \overline{\Gamma^\nu}\rangle^{\widehat{\Lambda}}$ is isomorphic to the Klein 4-group. It will then follow that $\mathrm{Aut}_3(H) = \mathrm{Inn}(H)\mathrm{Aut}_2(H)\langle\Gamma, \Gamma^\nu\rangle$, with $|\mathrm{Aut}_3(H)| = 2^{8m-4}$, as $|\mathrm{Inn}(H)\mathrm{Aut}_2(H)| = 2^{8m-6}$ by Corollary 5.45.

We know from Proposition 5.35 that $\mathrm{Aut}_2(K)/\mathrm{Inn}(K)\mathrm{Aut}_1(K)$ is generated by $\overline{\psi_1}, \overline{\psi_2}, \overline{\psi_3}, \overline{\psi_4}$. Setting $T = \langle \overline{\psi_1\psi_4}, \overline{\psi_2\psi_3}\rangle$, we proceed to show that $\mathrm{Im}(\widehat{\Lambda}) = T$. By Proposition 5.46, we have $\Gamma^\Lambda = \psi_1\psi_4$, and therefore $(\nu^{-1}\Gamma\nu)^\Lambda = \psi_2\psi_3$. Thus $T \subseteq \mathrm{Im}(\widehat{\Lambda})$. We readily see that $1, \overline{\psi_1}, \overline{\psi_2}, \overline{\psi_1\psi_2}$ is a system of representatives for the cosets of T in $\overline{\mathrm{Aut}_2(K)}$. Thus, it suffices to show that none of $\overline{\psi_1}, \overline{\psi_2}, \overline{\psi_1\psi_2}$ are in $\mathrm{Im}(\widehat{\Lambda})$. As $\mathrm{Inn}(H)\mathrm{Aut}_2(H)$ maps onto $\mathrm{Inn}(K)\mathrm{Aut}_1(K)$ by Proposition 5.43, this translates as follows: none of $\psi_1, \psi_2, \psi_1\psi_2$ lift to an automorphism of H. Note that we may replace any of $\psi_1, \psi_2, \psi_1\psi_2$ by itself multiplied by any element of $\mathrm{Inn}(K)\mathrm{Aut}_1(K)$ in this statement.

Suppose, if possible, that ψ_1 lifts to an automorphism, say τ, of H. Then there are $x, y \in Z_1(H)$ such that

$$A^\tau = A^{1+s}x,\ B^\tau = By.$$

Now by Corollary 5.38 and (2.1), we have $[A^{1+s}x, By] = [A^{1+s}, B] = A^u C^{1+s}$, and $[A^u, B] = C^u$, so

$$(By)^{[By, A^{1+s}x]} = B^{C^{-s}C^{-1}A^u}y = (B^\alpha)^{A^u}y = (BC^u)^\alpha y = B^\alpha C^u y.$$

Since $(By)^\alpha = B^\alpha y$, the second defining relation of H is not preserved by τ. This proves that ψ_1 does not lift to an automorphism of H. Since $\psi_2^\mu = \psi_1$, it follows that ψ_2 does not lift to an automorphism of H either.

Let $\psi_5 \in \mathrm{Aut}_2(K)$ be given by $a \mapsto a^{1+s}b^s$, $b \mapsto b$. Then $\overline{\psi_1\psi_2} \equiv \overline{\psi_1\psi_3} \mod T$ and $\psi_1\psi_3 \equiv \psi_5 \mod \mathrm{Inn}(K)\mathrm{Aut}_1(K)$. Suppose, if possible, that ψ_5 lifts to an automorphism, say σ, of H. Then there are $w, z \in Z_1(H)$ such that

$$A^\sigma = A^{1+s}B^s w, \ B^\sigma = Bz.$$

Since $[A^{1+s}B^s w, Bz] = [A^{1+s}, B]^{B^s} = A^u C^{1+s}$, we see, as in the previous case, that the second defining relation of H is not preserved by σ. □

We set $\overline{r} = r/2$ whenever $m > 2$ for the remainder of this section.

Proposition 5.49. *Suppose that $m > 2$. Let $x = rd$, $y = re$, with $d, e \in \{0, 1\}$, and further let $a, b \in \mathbb{Z}$, with $ab \equiv 1 \mod s$, as well as $z, z' \in Z_1(H)$. Then the assignment*

$$A \mapsto A^a B^x z, \quad B \mapsto B^b A^y z', \tag{5.50}$$

extends to an automorphism of H if and only if $x = y = 0$ and $a \equiv b \equiv 1 \mod 2s$, or $x = y = r$ and $a \equiv 1 + r \equiv b \mod 2s$.

Proof. By Corollary 5.39,

$$B^b A^y = (A^0 B^b C^0)(A^y B^0 C^0) = A^{y+2s\ell b\phi(y)} B^{b-2s\ell\phi(b)y} C^{-by-2s\ell\phi(b+1)\phi(y)}.$$

Since $z, z' \in Z_1(H) = \langle C^s \rangle$, then

$$[A^a B^x z, B^b A^y z'] = [A^a B^x, B^b A^y] = [A^a B^x, A^{y+2s\ell b\phi(y)} B^{b-2s\ell\phi(b)y} C^{-by}]. \tag{5.51}$$

Applying Corollary 5.40 to (5.51), using the fact that $\phi(n + 2st) \equiv \phi(n) \mod s$ for $n, t \in \mathbb{Z}$, and recalling that $ab \equiv 1 \mod s$ produces

$$\begin{aligned}
\exp A &\equiv 2s\ell\{x\phi(y) - \phi(a)b - aby\} \equiv -s\ell(xy + 2y + a - 1) \mod 2u, \\
\exp B &\equiv 2s\ell\{a\phi(b) - \phi(x)y + xab\} \equiv s\ell(xy + 2x + b - 1) \mod 2u, \\
\exp C &\equiv ab - xy + 2s\ell\{\phi(y)\phi(x) - \phi(a)(\phi(b) + xb) - ay\phi(b)\} \mod 2u,
\end{aligned}$$

where $\exp C \equiv 1 \mod s$, so

$$\begin{aligned}
&[A^aB^x, B^bA^y] \\
&\quad = A^{2s\ell\{x\phi(y)-\phi(a)b-aby\}}B^{2s\ell\{a\phi(b)-\phi(x)y+xab\}}C^{ab-xy+2s\ell\{\phi(y)\phi(x)-\phi(a)(\phi(b)+xb)-ay\phi(b)\}} \qquad (5.52)\\
&\quad \equiv A^{-s\ell(xy+2y+a-1)}B^{s\ell(xy+2x+b-1)}C \mod Z_1(H).
\end{aligned}$$

By Corollary 5.38, $[B^x, A^{-s\ell(xy+2y+a-1)}] = C^{sx(a-1)}$, $[A^a, B^{s\ell(xy+2x+b-1)}] = C^{sxa(y+2)+sa\ell(b-1)}$, and $[B^x, C] = B^{-2s\ell x} = B^{2s\ell x}$, so

$$\begin{aligned}
(A^aB^x)^{[A^aB^xz, B^bA^yz']} &= (A^aB^x)^{A^{-s\ell(xy+2y+a-1)}B^{s\ell(xy+2x+b-1)}C}\\
&= (A^aB^x)^{B^{s\ell(xy+2x+b-1)}C}C^{sx(a-1)}\\
&= (A^aB^x)^{C}C^{sx(3a+ya-1)+s\ell a(b-1)}\\
&= A^{\alpha a}B^{\alpha x}C^{sx(3a+ya-1)+s\ell a(b-1)}.
\end{aligned}$$

On the other hand, by Note 5.42, $(A^aB^x)^\alpha = A^{\alpha a}B^{\alpha x}C^{-sxa\ell}$ and $(A^aB^x)^{2u} = 1$.

Applying the automorphism $A \leftrightarrow B$ we get,

$$\begin{aligned}
(B^bA^y)^{[B^bA^yz', A^aB^xz]} &= B^{\alpha b}A^{\alpha y}C^{-sy(3b+xb-1)+s\ell b(a-1)},\\
(B^bA^y)^{\alpha} &= B^{\alpha b}A^{\alpha y}C^{syb\ell},\\
(B^bA^y)^{2u} &= 1.
\end{aligned}$$

Thus, the assignment (5.50) extends to an endomorphism of H if and only if $(A^aB^x)^{[A^aB^x, B^bA^y]} = (A^aB^x)^\alpha$ and $(B^bA^y)^{[B^bA^y, A^aB^x]} = (B^bA^y)^\alpha$ if and only if $C^{sx(3a+ya-1)+s\ell a(b-1)} = C^{-sxa\ell}$ and $C^{-sy(3b+xb+b\ell-1)+s\ell b(a-1)} = C^{syb\ell}$ if and only if

$$x(3a + ya + a\ell - 1) + \ell a(b-1) \equiv 0 \mod 2s, \qquad (5.53)$$

$$y(3b + xb + b\ell - 1) + \ell b(a-1) \equiv 0 \mod 2s. \qquad (5.54)$$

Assume that (5.53) and (5.54) hold. We claim that $d = 0 = e$ and $a \equiv 1 \equiv b \mod 2s$, or $d = 1 = e$ and $a \equiv 1 + r \equiv b \mod 2s$.

Suppose first that $d = 0$. From (5.53), we obtain $\ell a(b-1) \equiv 0 \mod 2s$. As ℓ and a are odd, we deduce $b - 1 \equiv 0 \mod 2s$. Since $ab \equiv 1 \mod s$, we infer $a \equiv 1 \mod s$. Now, suppose, if possible, that $e = 1$. From (5.54), we obtain $s + \ell(r + a - 1) \equiv 0 \mod 2s$, and from this, $s \mid \ell(r + a - 1)$. Since ℓ is odd and $a \equiv 1 \mod s$, this yields $s \mid r$ which is a contradiction. This proves that $e = 0$. But then (5.54) gives $\ell b(a-1) \equiv 0 \mod 2s$. Since ℓ and b are odd, we derive $a - 1 \equiv 0 \mod 2s$.

Suppose next that $e = 0$. Then, as indicated above, (5.54) gives $a \equiv 1 \mod 2s$, and as $ab \equiv 1 \mod s$, we deduce $b \equiv 1 \mod s$. If $d = 1$ then (5.53) yields the contradiction $s \mid r$. This forces $d = 0$, which then implies $b \equiv 1 \mod 2s$, as shown above.

Thus $d = 0$ if and only if $e = 0$, in which case $a \equiv 1 \equiv b \mod 2s$.

Suppose next that $d = 1 = e$. Then (5.53) and (5.54) imply $a \equiv 1 \equiv b \mod r$. Let $t_1, t_2 \in \mathbb{Z}$ be such that $a = 1 + rt_1$, $b = 1 + rt_2$. Replacing in (5.53) and (5.54) and dividing by r produces

$$r(3t_1 + t_1\ell + rt_1 + t_2t_1\ell + 1) + \ell(t_2 + 1) + 2 \equiv 0 \mod 4, \tag{5.55}$$

$$r(3t_2 + t_2\ell + rt_2 + t_1t_2\ell + 1) + \ell(t_1 + 1) + 2 \equiv 0 \mod 4, \tag{5.56}$$

which imply $t_1 + 1 \equiv 0 \equiv t_2 + 1 \mod 2$. Let $q_1, q_2 \in \mathbb{Z}$ be such that $t_1 = 2q_1 + 1$ and $t_2 = 2q_2 + 1$. Replacing this in (5.55) and (5.56) and dividing by 2 gives

$$\overline{r}(2q_1(3 + r + 2\ell) + 2q_2\ell + 4q_1q_2\ell + r + 2\ell + 4) + \ell(q_2 + 1) + 1 \equiv 0 \mod 2,$$

$$\overline{r}(2q_2(3 + r + 2\ell) + 2q_1\ell + 4q_1q_2\ell + r + 2\ell + 4) + \ell(q_1 + 1) + 1 \equiv 0 \mod 2.$$

From this we get $\ell(q_2 + 1) + 1 \equiv 0 \equiv \ell(q_1 + 1) + 1 \mod 2$, which imply $q_1 \equiv 0 \equiv q_2 \mod 2$. Thus $a \equiv 1 + r \equiv b \mod 2s$. This proves the claim.

Suppose, conversely, that $d = 0 = e$ and $a \equiv 1 \equiv b \mod 2s$, or $d = 1 = e$ and $a \equiv 1 + r \equiv b \mod 2s$. We claim that (5.53) and (5.54) are true. Indeed, if $d = 0 = e$ and $a \equiv 1 \equiv b \mod 2s$, we see directly that (5.53) and (5.54) hold. If $d = 1 = e$ and $a \equiv 1 + r \equiv b \mod 2s$, then $a = 1 + r + sq_1$ and $b = 1 + r + sq_2$ for some even $q_1, q_2 \in \mathbb{Z}$. After replacing a and b we readily see that (5.53) and (5.54) hold, as claimed.

We finally claim that if $d = 0 = e$ and $a \equiv 1 \equiv b \mod 2s$, or $d = 1 = e$ and $a \equiv 1 + r \equiv b \mod 2s$, then the endomorphism of H, say T, extending (5.50) is actually an automorphism. As H is a finite nilpotent group, it suffices to show that the restriction of T to $Z_1(H) = \langle C^s \rangle$ is a monomorphism. Now, from (5.51), (5.52), and Corollary 5.41, we have

$$(C^s)T = [A^aB^xz, B^bA^yz']^s = [A^aB^x, B^bA^y]^s = C^{s(ab-xy)}.$$

As $ab - xy$ is odd, the restriction of T to $Z_1(H)$ is a monomorphism, which completes the proof. □

Corollary 5.57. *Suppose $m > 2$. Then the assignment $A \mapsto A^{1+r}B^r$, $B \mapsto B^{1+r}A^r$ extends to an automorphism, say Σ, of H, which clearly commutes with ν.*

Lemma 5.58. *Suppose that $m = 2$. Then H is a group of order 512, with presentation*

$$\langle\, A, B, C \mid C = [A, B],\ A^C = A^5,\ B^C = B^5,\ A^8 = B^8 = C^8 = 1 \,\rangle,$$

where $Z_1(H) = \langle C^2 \rangle$, $[A^2, C] = 1 = [B^2, C]$, and $[A^2, B^2] = 1$. Moreover, if $z, w \in Z_1(H)$, then the assignment $A \mapsto ABz$, $B \mapsto Bw$ does not extend to an automorphism of H.

Proof. The first statement follows by specializing general facts about H to the case $m = 2$ (e.g. the relation $[A^2, B^2] = 1$ follows from Corollary 5.38). The given presentation shows, in particular, that the isomorphism type of J is independent of ℓ, and we take $\ell = 1$ and $\alpha = 5$.

As for the second statement, we claim that $(ABz)^{[ABz,Bw]} \neq (ABz)^5$. Now $(ABz)^{[ABz,Bw]} = (AB)^{[AB,B]}z$ and $(ABz)^5 = (AB)^5 z$, so it suffices to show that $(AB)^{[AB,B]} \neq (AB)^5$.

Using (2.1) and Corollary 5.38, we see that $[AB, B] = C^B = B^4C$, so

$$(AB)^{[AB,B]} = (AB)^{B^4C} = (A^{B^4}B)^C = (AC^4B)^C = A^5B^5C^4.$$

On the other hand, using Note 5.42 gives

$$(AB)^5 = A^5B^5C^{-\phi(5)+4\sigma_2(1,5)} = A^5B^5C^2.$$

Thus, the normal form of the elements of H yields that $(AB)^{[AB,B]} \neq (AB)^5$ (with equality modulo $Z_1(H)$, in agreement with Proposition 5.28). □

Set $\Sigma_1 \in \mathrm{Aut}(H)$ to be Σ if $m > 2$ and 1_H if $m = 2$.

Theorem 5.59. *The canonical map $\zeta : \mathrm{Aut}(H) \to \mathrm{Aut}(H/Z_3(H))$ has kernel $\mathrm{Aut}_3(H)$ and image $\langle \Sigma_1, \nu \rangle^\zeta$, so that $\mathrm{Aut}(H) = \mathrm{Aut}_3(H)\langle \Sigma_1, \nu \rangle = \mathrm{Aut}_2(H)\mathrm{Inn}(H)\langle \Gamma, \Sigma_1, \nu \rangle$. Moreover, we have $\mathrm{Aut}(H)/\mathrm{Aut}_3(H) \cong (\mathbb{Z}/2\mathbb{Z})^2$ if $m > 2$ and $\mathrm{Aut}(H)/\mathrm{Aut}_3(H) \cong \mathbb{Z}/2\mathbb{Z}$ if $m = 2$. Thus the order of $\mathrm{Aut}(H)$ is 2^{8m-2} if $m > 2$ and 2^{13} if $m = 2$.*

Proof. As J is nilpotent of class 5, the nilpotency classes of H and K are 4 and 3, respectively. Thus, Proposition 5.47 gives an imbedding $\widetilde{\Lambda} : \mathrm{Aut}(H)/\mathrm{Aut}_3(H) \to \mathrm{Aut}(K)/\mathrm{Aut}_2(K)$. We appeal to Theorem 5.29, its proof, and notation therein.

We have an imbedding $\eta : \mathrm{Aut}(K)/\mathrm{Aut}_2(K) \to \mathrm{GL}_2(\mathbb{Z}/2^{m-1}\mathbb{Z})$, which yields an imbedding $\widetilde{\Lambda}\eta : \mathrm{Aut}(H)/\mathrm{Aut}_3(H) \to \mathrm{GL}_2(\mathbb{Z}/2^{m-1}\mathbb{Z})$. Set $\chi = \zeta\widetilde{\Lambda}\eta$ and $I = \mathrm{Im}(\chi)$. As $\widetilde{\Lambda}\eta$ is injective, $\mathrm{Im}(\zeta) = \langle \Sigma_1, \nu \rangle^\zeta$ if and only if $I = \langle \Sigma_1, \nu \rangle^\chi$. Note also that $\nu^\chi = Q$.

Suppose first $m > 2$ and set $Z = M_{1+2^{m-2}}RT$. Then $\Sigma^\chi = Z$, and we must show that $I = \langle Q, Z \rangle$. Now $W = V\langle Q \rangle$, with $Q \in I$, so it suffices to show that $I \cap V = \langle Z \rangle$. Here V is

an abelian group of order 2^m. By Proposition 5.49, $I \cap \langle U \rangle$ is trivial. It remains to analyze the cosets $\langle U \rangle R$, $\langle U \rangle T$, and $\langle U \rangle RT$, inside of V.

We claim that none of the elements in $\langle U \rangle R$ is in I, which translates as follows: none of the assignments $A \mapsto A^q B^{2^{m-2}} z$, $B \mapsto B^t w$, where $z, w \in Z_1(H)$, $qt \equiv 1 \mod 2^{m-1}$, $1 \leq q, t \leq 2^{m-1}$, extends to an automorphism of H. This follows from Proposition 5.49.

Since $R = T^Q$ and $U = U^Q$, it follows that none of the elements in $\langle U \rangle T$ is in I either.

We next claim that if $M_q RT \in I$ for any odd q such that $1 \leq q \leq 2^{m-1}$, then $q = 1 + 2^{m-2}$. This translates as follows: if the assignment $A \mapsto A^q B^{2^{m-2}} z$, $B \mapsto B^t A^{2^{m-2}} w$, where $z, w \in Z_1(H)$, $qt \equiv 1 \mod 2^{m-1}$, and $1 \leq q, t \leq 2^{m-1}$, extends to an automorphism of H then $q = 1 + 2^{m-2}$. This follows from Proposition 5.49.

Clearly, $\langle Z, Q \rangle$ is isomorphic to the Klein 4-group, so $|\mathrm{Aut}(H)| = |\mathrm{Aut}_3(H)| \times |\langle Z, Q \rangle| = 2^{8m-2}$ by Theorem 5.48.

Suppose next $m = 2$. Since $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ is the disjoint union of $\langle Q \rangle$, $\langle Q \rangle R$, and $\langle Q \rangle T$, we must show that no element of the last 2 cosets is in I. Since Q conjugates R and T into each other, it suffices to show that R is not in I, which means that the assignment $A \mapsto ABz$, $B \mapsto Bw$, where $z, w \in Z_1(H)$, does not extend to an automorphism of H. This follows from Lemma 5.58.

Thus Theorem 5.48 gives $|\mathrm{Aut}(H)| = 2|\mathrm{Aut}_3(H)| = 2^{8m-3} = 2^{13}$. □

We next obtain a description of $\mathrm{Aut}(H)$ in terms of group extensions.

Theorem 5.60. *We have the following series of normal subgroups of* $\mathrm{Aut}(H)$*:*

$$1 \subseteq \mathrm{Aut}_2(H) \subseteq \mathrm{Inn}(H)\mathrm{Aut}_2(H) \subseteq \mathrm{Aut}_3(H) \subseteq \mathrm{Aut}(H),$$

with factors $\mathrm{Aut}_2(H) \cong (\mathbb{Z}/2^{m-1}\mathbb{Z})^4 \times (\mathbb{Z}/2^m\mathbb{Z})^2$, $\mathrm{Inn}(H)\mathrm{Aut}_2(H)/\mathrm{Aut}_2(H) \cong (\mathbb{Z}/2^{m-1}\mathbb{Z})^2$, $\mathrm{Aut}_3(H)/\mathrm{Inn}(H)\mathrm{Aut}_2(H) \cong (\mathbb{Z}/2\mathbb{Z})^2$, *and* $\mathrm{Aut}(H)/\mathrm{Aut}_3(H)$ *is isomorphic to* $(\mathbb{Z}/2\mathbb{Z})^2$ *if* $m > 2$ *and* $\mathbb{Z}/2\mathbb{Z}$ *if* $m = 2$.

Proof. We know that $Z_2(H)$ is abelian. Moreover, by Proposition 5.43, $\mathrm{Aut}_2(H) \cong Z_2(H) \times Z_2(H)$, where $Z_2(H) = \langle A^{2^m}, B^{2^m}, C^{2^{m-1}} \rangle \cong (\mathbb{Z}/2^{m-1}\mathbb{Z})^2 \times \mathbb{Z}/2^m\mathbb{Z}$ by the normal form of the elements of H and the orders of A, B, C. Thus $\mathrm{Aut}_2(H) \cong (\mathbb{Z}/2^{m-1}\mathbb{Z})^4 \times (\mathbb{Z}/2^m\mathbb{Z})^2$. Next, we have

$$\begin{aligned}&\mathrm{Inn}(H)\mathrm{Aut}_2(H)/\mathrm{Aut}_2(H)\\ &\quad\cong \mathrm{Inn}(H)/\mathrm{Aut}_2(H) \cap \mathrm{Inn}(H) \cong H\delta/Z_3(H)\delta \cong H/Z_3(H) \cong (\mathbb{Z}/2^{m-1}\mathbb{Z})^2.\end{aligned}$$

That $\mathrm{Aut}_3(H)/\mathrm{Inn}(H)\mathrm{Aut}_2(H) \cong (\mathbb{Z}/2\mathbb{Z})^2$ was shown in Theorem 5.48. Finally, Theorem 5.59 gives the structure of $\mathrm{Aut}(H)/\mathrm{Aut}_3(H)$. □

5.5 The automorphism group of J

Throughout this section we maintain the notation introduced in the beginning of the chapter and in Section 5.1 and recall the numerical information given in Section 5.2. Also, recall that the exponent of J is $4us$, which implies that if $x, y \in J$, then the assignment $A \mapsto x$, $B \mapsto y$ extends to an endomorphism of J if and only if it preserves the first and second defining relations of J.

Proposition 5.61. *For every $x, y \in Z_1(J)$ the assignment $A \mapsto Ax$, $B \mapsto By$ extends to a central automorphism $\Omega_{(x,y)}$ of J that fixes $Z_2(J)$ pointwise. Moreover, the corresponding map $\Omega : Z_1(J) \times Z_1(J) \to \mathrm{Aut}(J)$ is a group monomorphism whose image is $\mathrm{Aut}_1(J)$. In particular, $|\mathrm{Aut}_1(J)| = 2^{2m}$.*

Proof. This follows as in the proof of Proposition 5.14. □

Proposition 5.62. *For every $x, y \in Z_2(J)$ the assignment $A \mapsto Ax$, $B \mapsto By$ extends to a 2-central automorphism $\Psi_{(x,y)}$ of J that fixes $Z_1(J)$ and $Z_2(J)/Z_1(J)$ pointwise. Thus, $|\mathrm{Aut}_2(J)| = 2^{4m}$ and the map $g : Z_2(J) \times Z_2(J) \to \mathrm{Aut}_2(J)/\mathrm{Aut}_1(J)$, given by $(x, y) \mapsto \Psi_{(x,y)}\mathrm{Aut}_1(J)$ is a group epimorphism with kernel $Z_1(J)^2$, so we have that $\mathrm{Aut}_2(J)/\mathrm{Aut}_1(J) \cong (Z_2(J)/Z_1(J))^2$.*

Proof. Let $x \in Z_2(J)$. Then $x = A^{2ui}C^{sk}$ for some $i, k \in \mathbb{Z}$. Let us first show that

$$(Ax)^{[A,B]} = (Ax)^{\alpha},\ (Bx)^{[B,A]} = (Bx)^{\alpha}. \tag{5.63}$$

Applying Theorem 5.10 to $(Ax)^{\alpha} = (A^{1+2ui}C^{sk})^{\alpha} = A^{\exp A+\xi_4}B^{\exp B}C^{\exp C}$ yields $\exp A \equiv \alpha + 2ui + 2usk \mod 4us$, $\exp B \equiv 0 \mod 4us$, $\exp C \equiv sk + 2uk \mod 4u$, $\xi_4 \equiv 0 \mod 4us$, so

$$(Ax)^{\alpha} = A^{\alpha+2ui+2usk}C^{sk+2uk} = A^{\alpha+2ui}C^{sk}.$$

On the other hand,

$$(Ax)^{C} = (A^{1+2ui}C^{sk})^{C} = A^{\alpha(1+2ui)}C^{sk} = A^{\alpha+2ui}C^{sk}.$$

Thus $(Ax)^{[A,B]} = (Ax)^{\alpha}$ and, by the automorphism $A \leftrightarrow B$, $(Bx)^{[B,A]} = (Bx)^{\alpha}$.

Now, taking $x, y \in Z_2(J)$ and working modulo $Z_1(J)$, we obtain

$$[Ax, By] = [A, B]z$$

for a unique $z \in Z_1(J)$. Then

$$(Ax)^{[Ax,By]} = (Ax)^{[A,B]z} = (Ax)^{[A,B]},\ (By)^{[By,Ax]} = (By)^{[B,A]z} = (By)^{[B,A]}. \tag{5.64}$$

By (5.63) and (5.64), it follows that the defining relations of J are preserved. Thus the above assignment extends to an endomorphism $\Psi_{(x,y)}$ of J.

Applying Theorem 5.10 to the expression $(A^{1+2ui}C^{sk})^{2u} = A^{\exp A+\xi_4}B^{\exp B}C^{\exp C}$ produces, $\exp A \equiv 2u \mod 4us$, $\exp B \equiv 0 \mod 4us$, $\exp C \equiv 0 \mod 4u$, $\xi_4 \equiv 0 \mod 4us$, so

$$(A^{2u})\Psi_{(x,y)} = (Ax)^{2u} = (A^{1+2ui}C^{sk})^{2u} = A^{2u}$$

and $\Psi_{(x,y)}$ restricts to the identity map on $Z_1(J)$. As J is a finite nilpotent group, it follows that $\Psi_{(x,y)}$ is an automorphism of J that fixes $Z_1(J)$ pointwise. Moreover, since $\Psi_{(x,y)}$ sends C to Cz, with $z \in Z_1(J)$, we see that $\Psi_{(x,y)}$ fixes $C^{2^{m-1}}$ modulo $Z_1(J)$, whence $\Psi_{(x,y)}$ fixes $Z_2(J)/Z_1(J)$ pointwise. This implies that g is a group homomorphism, whose kernel clearly contains $Z_1(J)^2$.

On the other hand, by definition, every element of $\mathrm{Aut}_2(J)$ has the form $\Psi_{(x,y)}$ for a unique $(x, y) \in Z_2(J) \times Z_2(J)$, so g is an epimorphism, $|\mathrm{Aut}_2(J)| = 2^{4m}$, and $|\mathrm{Aut}_2(J)/\mathrm{Aut}_1(J)| = |Z_2(J)/Z_1(J)|^2$, which implies that $\ker(g) = Z_1(J) \times Z_1(J)$. □

We have the following series of normal subgroups of $\mathrm{Aut}(J)$:

$$1 \subseteq \mathrm{Aut}_1(J) \subseteq \mathrm{Aut}_2(J) \subseteq \mathrm{Aut}_3(J) \subseteq \mathrm{Inn}(J)\mathrm{Aut}_3(J) \subseteq \mathrm{Aut}_4(J) \subseteq \mathrm{Aut}(J). \tag{5.65}$$

Here $\mathrm{Aut}_1(J) \cong (\mathbb{Z}/2^m\mathbb{Z})^2$ and $\mathrm{Aut}_2(J)/\mathrm{Aut}_1(J) \cong (\mathbb{Z}/2^m\mathbb{Z})^2$ by Propositions 5.61 and 5.62. Regarding $\mathrm{Aut}_3(J)/\mathrm{Aut}_2(J)$, by Proposition 5.47, we have imbeddings

$$\mathrm{Aut}_3(J)/\mathrm{Aut}_2(J) \hookrightarrow \mathrm{Aut}_2(H)/\mathrm{Aut}_1(H) \hookrightarrow \mathrm{Aut}_1(K) \cong Z_1(K) \times Z_1(K).$$

We proceed to find the image of this composite imbedding and the structure of the quotient $\mathrm{Inn}(J)\mathrm{Aut}_3(J)/\mathrm{Aut}_3(J)$.

Theorem 5.66. *The assignments $A \mapsto AB^{2s}$, $B \mapsto B^{1-4s}A^{2s}$ and $A \mapsto A$, $B \mapsto BA^u$ extend to automorphisms, say Δ_1 and Δ_2, of J. Moreover,*

$$\mathrm{Inn}(J)\mathrm{Aut}_3(J) = \langle \Delta_1, \Delta_2 \rangle \mathrm{Inn}(J)\mathrm{Aut}_2(J),\ \mathrm{Aut}_3(J) = \langle \Delta_1, \Delta_2, C\delta \rangle \mathrm{Aut}_2(J),$$

$$\mathrm{Aut}_3(J)/\mathrm{Aut}_2(J) \cong (\mathbb{Z}/2^{m-1}\mathbb{Z})^2 \times \mathbb{Z}/2\mathbb{Z},\ \mathrm{Inn}(J)\mathrm{Aut}_3(J)/\mathrm{Aut}_3(J) \cong (\mathbb{Z}/2^{m-1}\mathbb{Z})^2,$$

$$|\mathrm{Aut}_3(J)| = 2^{6m-1},\ |\mathrm{Inn}(J)\mathrm{Aut}_3(J)| = 2^{8m-3}.$$

Proof. Applying Proposition 5.47 twice, we obtain

$$\mathrm{Aut}_3(J)/\mathrm{Aut}_2(J) \hookrightarrow \mathrm{Aut}_2(H)/\mathrm{Aut}_1(H) \hookrightarrow \mathrm{Aut}_1(K),$$

where $\mathrm{Aut}_1(K) \cong Z_1(K) \times Z_1(K)$ by Proposition 5.14. In this way we obtain a homomorphism $\psi : \mathrm{Aut}_3(J) \to Z_1(K)^2$ such that $\ker(\psi) = \mathrm{Aut}_2(J)$. We proceed to show that

$$\mathrm{Im}(\psi) = \langle (a^{2s}, b^{-2s}), (b^{2s}, a^{2s}b^{-4s}), (1, a^u) \rangle. \tag{5.67}$$

Let $i, j, g, h \in \mathbb{Z}$ and $w, z \in Z_2(J)$. We need to determine under what conditions the assignment

$$A \mapsto AA^{2si}B^{2sj}w, \ B \mapsto BA^{2sg}B^{2sh}z$$

extends to an automorphism of J. Skillfully using Propositions 5.61 and 5.62, we see that this is the case if and only if

$$A \mapsto A^{1+2si}B^{2sj}, \ B \mapsto BA^{2sg}B^{2sh} \tag{5.68}$$

extends to an automorphism of J. We will implicitly use in what follows that $Z_3(J)$ is abelian, as indicated in the beginning of the chapter.

By Theorem 5.3, $[B, A^{2sg}] = (A^{2u\ell g}C^{2sg})^{-1} = A^{2u\ell g}C^{-2sg}$. Then

$$BA^{2sg}B^{2sh} = A^{2sg}BA^{2u\ell g}C^{-2sg}B^{2sh} = A^{2sg}B^{1+2sh}C^{-2sg}A^{2u\ell g}$$

and

$$[A^{1+2si}B^{2sj}, BA^{2sg}B^{2sh}] = [A^{1+2si}B^{2sj}, A^{2sg}B^{1+2sh}C^{-2sg}].$$

Applying Proposition 5.9 to the above commutator produces, $\exp A \equiv 0 \mod 2u$, $\exp B \equiv 0 \mod 2u$, $\exp C \equiv 1 + 2s(i+h) \mod 2u$, so

$$[A^{1+2si}B^{2sj}, BA^{2sg}B^{2sh}] \equiv A^{\exp A}B^{\exp B}C^{\exp C} \equiv C^{1+2s(i+h)} \mod Z_1(J).$$

Thus

$$(A^{1+2si}B^{2sj})^{[A^{1+2si}B^{2sj}, BA^{2sg}B^{2sh}]} = (A^{1+2si}B^{2sj})^{C^{1+2s(i+h)}}.$$

As $[A^{1+2si}, C^{1+2s(i+h)}] = A^{2s\ell+4u\ell h+8u\ell i}$ and $[B^{2sj}, C^{1+2s(i+h)}] = B^{-4u\ell j}$, then

$$(A^{1+2si}B^{2sj})^{[A^{1+2si}B^{2sj}, BA^{2sg}B^{2sh}]} = A^{1+2s(i+\ell)+4u\ell h+8u\ell i}B^{2sj-4u\ell j} = A^{1+2s(i+\ell)+4u\ell(h+j+2i)}B^{2sj}.$$

On the other hand, applying Theorem 5.10 to $(A^{1+2si}B^{2sj})^\alpha = A^{\exp A+\xi_4}B^{\exp B}C^{\exp C}$ gives, $\exp A \equiv 1 + 2s(i+\ell) + 4u\ell i \mod 4us$, $\exp B \equiv 2sj + 4u\ell j + 2usj \mod 4us$, $\exp C \equiv 2uj \mod 4u$, and $\xi_4 \equiv 0 \mod 4us$, so

$$(A^{1+2si}B^{2sj})^\alpha = A^{1+2s(i+\ell)+4u\ell i}B^{2sj+4u\ell j+2usj}C^{2uj} = A^{1+2s(i+\ell)+4u\ell(i-j)}B^{2sj}.$$

Thus $(A^{1+2si}B^{2sj})^{[A^{1+2si}B^{2sj},BA^{2sg}B^{2sh}]} = (A^{1+2si}B^{2sj})^{\alpha}$ is equivalent to

$$A^{4u\ell(2j+h+i)} = 1. \tag{5.69}$$

By the automorphism $A \leftrightarrow B$ we have that $(BA^{2sg}B^{2sh})^{[BA^{2sg}B^{2sh},A^{1+2si}B^{2sj}]} = (BA^{2sg}B^{2sh})^{\alpha}$ is equivalent to

$$B^{4u\ell(2g+h+i)} = 1. \tag{5.70}$$

Note that (5.69) and (5.70) hold if and only if

$$2j + h + i \equiv 0 \mod s, \quad 2g + h + i \equiv 0 \mod s. \tag{5.71}$$

Thus, (5.68) extends to an endomorphism, say Υ, of J if and only if (5.71) holds, in which case Υ is an automorphism. Indeed, applying Theorem 5.10 to $(A^{1+2si}B^{2sj})^{2u} = A^{\exp A+\xi_4}B^{\exp B}C^{\exp C}$ yields, $\exp A \equiv 2u \mod 4us$, $\exp B \equiv 0 \mod 4us$, $\exp C \equiv 0 \mod 4u$, $\xi_4 \equiv 0 \mod 4us$, so

$$(A^{2u})\Upsilon = (A^{1+2si}B^{2sj})^{2u} = A^{2u},$$

which ensures that the restriction of Υ to $Z_1(J)$ is the identity map and, since J is nilpotent, this guarantees that $\ker(\Upsilon)$ is trivial.

Now (5.71) implies $g \equiv j \mod 2^{m-2}$ and $h \equiv -i-2j \mod 2^{m-1}$, so that $g = j + t2^{m-2}$ and $h = -i - 2j + q2^{m-1}$ with $t, q \in \mathbb{Z}$. Thus, the image of ψ consists of all

$$(a^{2^m}, b^{-2^m})^i\,(b^{2^m}, a^{2^m}b^{-2^{m+1}})^j\,(1, a^{2m-2})^t, \quad i, j, t.$$

Here $(a^{2^m}, b^{-2^m}), (b^{2^m}, a^{2^m}b^{-2^{m+1}}), (1, a^{2m-2})$ generate a subgroup of $Z_1(K)^2$ isomorphic to $(\mathbb{Z}/2^{m-1}\mathbb{Z})^2 \times \mathbb{Z}/2\mathbb{Z}$. Thus the image of ψ, and hence $\mathrm{Aut}_3(J)/\mathrm{Aut}_2(J)$, is as required. We also see that Δ_1 and Δ_2 are automorphisms, and that $(C\delta)^{\psi}$ and (a^{2^m}, b^{-2^m}) generate the same subgroup of $Z_1(K)^2$. We conclude that $|\mathrm{Aut}_3(J)| = |\mathrm{Aut}_2(J)| \times 2^{2m-1} = 2^{6m-1}$, by Proposition 5.62. Finally,

$$\mathrm{Inn}(J)\mathrm{Aut}_3(J)/\mathrm{Aut}_3(J) \cong \mathrm{Inn}(J)/\mathrm{Aut}_3(J)\cap\mathrm{Inn}(J) \cong J\delta/Z_4(J)\delta \cong J/Z_4(J) \cong (\mathbb{Z}/2^{m-1}\mathbb{Z})^2,$$

so $|\mathrm{Inn}(J)\mathrm{Aut}_3(J)| = 2^{6m-1} \times 2^{2m-2} = 2^{8m-3}$. □

We next determine the last two factors of (5.65). It turns out that $\mathrm{Aut}_4(J)/\mathrm{Inn}(J)\mathrm{Aut}_3(J) \cong \mathbb{Z}/2\mathbb{Z}$ and $\mathrm{Aut}(J)/\mathrm{Aut}_4(J)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$ if $m > 2$ and to $\mathbb{Z}/2\mathbb{Z}$ if $m = 2$. This will take considerable effort.

Proposition 5.72. *The assignment $A \mapsto A^{1+s}u_1$, $B \mapsto A^sBu_2$, where $u_1, u_2 \in Z_3(J)$, does not extend to an endomorphism of J.*

Proof. Suppose, if possible, that the given assignment extends to an endomorphism, say Γ, of J. We first consider the case when $u_1 = A^{2si}B^{2sj}$, $u_2 = A^{2sa}B^{2sb}$. Applying Theorem 5.7 to $(A^0BC^0)(A^{2sa}B^{2sb}C^0) = A^{\exp A+\xi}B^{\exp B}C^{\exp C}$, gives $\exp A \equiv 2sa \mod 2u$, $\exp B \equiv 1+2sb \mod 2u$, $\exp C \equiv -2sa \mod 2u$, and $\xi \equiv 0 \mod 2u$, so

$$B\Gamma \equiv A^{s+2sa}B^{1+2sb}C^{-2sa} \mod Z_1(J),$$

$$[A\Gamma, B\Gamma] = [A^{1+s+2si}B^{2sj}, A^{s+2sa}B^{1+2sb}C^{-2sa}].$$

By Proposition 5.9 applied to $[A\Gamma, B\Gamma] = A^{\exp A}B^{\exp B}C^{\exp C}$, we get $\exp A \equiv u \mod 2u$, $\exp B \equiv 0 \mod 2u$, $\exp C \equiv 1+s+2s(i+b) \mod 2u$, so

$$[A\Gamma, B\Gamma] \equiv A^uC^{1+s+2s(i+b)} \mod Z_1(J).$$

Thus, using that $Z_3(J)$ is abelian, we obtain

$$(A\Gamma)^{[A\Gamma,B\Gamma]} = (A^{1+s+2si}B^{2sj})^{A^uC^{1+s+2s(i+b)}} = (A^{1+s+2si}B^{2sj})^{C^{1+s+2s(i+b)}}.$$

A careful application of Theorem 5.3 gives

$$(A\Gamma)^{[A\Gamma,B\Gamma]} = A^{1+s+2si+2s\ell+4u\ell(2i+b+1)}B^{2sj-4u\ell j} = A^{\alpha+s+2si+4u\ell(2i+b+j+1)}B^{2sj}.$$

On the other hand, applying Theorem 5.10 to $(A^{1+s+2si}B^{2sj})^\alpha = A^{\exp A+\xi}B^{\exp B}C^{\exp C}$ gives $\exp A \equiv 1+2s\ell+s+2si+2u\ell+4u\ell i \mod 4us$, $\exp B \equiv 2sj+4u\ell j+2usj \mod 4us$, $\exp C \equiv 2uj \mod 4u$, $\xi \equiv 0 \mod 4us$, so

$$(A\Gamma)^\alpha = (A^{1+s+2si}B^{2sj})^\alpha = A^{\alpha+s+2si+2u\ell+4u\ell i}B^{2sj+4u\ell j+2usj}C^{2uj} = A^{\alpha+s+2si+2u\ell+4u\ell(i-j)}B^{2sj}$$

Since $2u\ell \not\equiv 0 \mod 4u$, $(A\Gamma)^{[A\Gamma,B\Gamma]} \neq (A\Gamma)^\alpha$, so Γ does not extend to an endomorphism of J in this case.

In general, we have $u_1 = v_1z_1$ and $u_2 = v_2z_2$, where $v_1 = A^{2se_1}B^{2sf_1}$, $v_2 = A^{2se_2}B^{2sf_2}$, and $z_1, z_2 \in Z_2(J)$. For any odd t, the map $x \mapsto x^t$ defines an automorphism of $Z_2(J)$ and $Z_1(J)$. Thus, we can find $x_1, x_2 \in Z_2(J)$ such that $x_1^{1+s+2sh_1+2sk_1} = z_1^{-1}$, $x_2^{1+s+2sh_2+2sk_2} = z_2^{-1}$. It follows from Proposition 5.62 that $\Gamma\Psi_{(x_1,x_2)}$ sends A to $A^{1+s}v_1y_1$ and B to $A^sBv_2y_2$, where $y_1, y_2 \in Z_1(J)$. Next we find $q_1, q_2 \in Z_1(J)$ such that $q_1^{1+s+2sh_1+2sk_1} = y_1^{-1}$ and $q_2^{1+s+2sh_2+2sk_2} = y_2^{-1}$. We deduce from Proposition 5.61 that $\Gamma\Psi_{(x_1,x_2)}\Omega_{(q_1,q_2)}$ sends A to $A^{1+s}v_1$ and B to A^sBv_2, which contradicts the previous case. □

Proposition 5.73. *The assignment $A \mapsto A^{1+s}B^s$, $B \mapsto B^{1+s(2\delta_{2,m}+s-3)}A^s$, where $\delta_{i,j}$ is the Kronecker delta function, extends to an automorphism, say Δ_3, of J.*

Proof. Applying Theorem 5.7 to $B\Delta_3 = (A^0B^{1+s(2\delta_{2,m}+s-3)}C^0)(A^sB^0C^0)$, we obtain

$$B\Delta_3 \equiv A^{s+u}B^{1-3s+2s\delta_{2,m}+u}C^{-s+ur} \mod Z_1(J), \tag{5.74}$$

where the exponents of A, B, C were reduced modulo $2u$. Thus

$$[A\Delta_3, B\Delta_3] = [A^{1+s}B^s, A^{s+u}B^{1-3s+2s\delta_{2,m}+u}C^{-s+ur}].$$

By Proposition 5.9 applied to $[A\Delta_3, B\Delta_3]$, we get

$$[A\Delta_3, B\Delta_3] \equiv A^uB^uC^{1+2s(\delta_{2,m}-1)+u} \mod Z_1(J).$$

By Theorem 5.3, $[B^s, A^u] = A^{u^2}$ and $[B, A^u] = A^{-us\ell}C^{-u}$, so $[B^{1+s}, A^u] = A^{-us\ell+u^2}C^{-u}$ by (2.1), whence $[A^{1+s}, B^u] = B^{-us\ell+u^2}C^u = A^{us\ell+u^2}C^u$ using θ, $B^{2u}A^{2u} = 1$ and $A^{4us} = 1$. Theorem 5.3 also gives $[B^s, C^{2s}] = 1$, which implies $[B^s, C^u] = 1$ and $[B^s, C^{1+2s(\delta_{2,m}-1)+u}] = [B^s, C] = B^{-2u\ell} = A^{2u\ell}$. Another application of Theorem 5.3 yields $[A^{1+s}, C^{1+2s(\delta_{2,m}-1)+u}] = A^{2s\ell+2u\ell+4u\ell(\delta_{2,m}-1)+2us}$. Using these commutators yields

$$\begin{aligned}(A\Delta_3)^{[A\Delta_3,B\Delta_3]} &= (A^{1+s}B^s)^{A^uB^uC^{1+2s(\delta_{2,m}-1)+u}} \\ &= (A^{1+s}B^s)^{B^uC^{1+2s(\delta_{2,m}-1)+u}}A^{u^2} \\ &= (A^{1+s}C^uB^s)^{C^{1+2s(\delta_{2,m}-1)+u}}A^{us\ell} \\ &= A^{\alpha+s}B^sC^uA^{4u\ell\delta_{2,m}+us\ell+2us}.\end{aligned}$$

On the other hand, applying Theorem 5.10 to $(A\Delta_3)^\alpha = (A^{1+s}B^s)^\alpha = A^{\exp A+\xi_4}B^{\exp B}C^{\exp C}$ gives $\exp A \equiv \alpha + s + 2u\ell + 2us + u^2 \mod 4us$, $\exp B \equiv s + 2u\ell + us\ell^2 \mod 4us$, $\exp C \equiv -u\ell + us \mod 4u$, and $\xi_4 \equiv u^2 \mod 4us$, so

$$(A\Delta_3)^\alpha = A^{\alpha+s+2u\ell+2us+u^2}B^{s+2u\ell+us\ell^2}C^{-u\ell+us}A^{u^2} = A^{\alpha+s}B^sC^{-u\ell}A^{-us\ell^2+2us+u^2}.$$

As $-u\ell \equiv 4u - u\ell \equiv u + u(3-\ell) \mod 4u$, then $(A\Delta_3)^\alpha = A^{\alpha+s}B^sC^uA^{us(3-\ell^2-\ell)+2us+u^2}$. Therefore $(A\Delta_3)^{[A\Delta_3,B\Delta_3]} = (A\Delta_3)^\alpha$ if and only if $A^{4u\ell\delta_{2,m}+us(\ell^2-1)+u^2} = 1$ if and only if $4s \mid 4\ell\delta_{2,m}+s(\ell^2-1)+u$. If $m = 2$, then $s = 2$ and $4s$ is a factor of $2(\ell+1)^2 = 4\ell\delta_{2,m}+s(\ell^2-1)+u$. If $m \geq 3$, then $s \geq 4$ and $4s$ is a factor of $s\{(\ell-1)(\ell+1)+s\} = 4\ell\delta_{2,m} + s(\ell^2-1) + u$. Thus $(A\Delta_3)^{[A\Delta_3,B\Delta_3]} = (A\Delta_3)^\alpha$.

As for the second relation, we have

$$[B\Delta_3, A\Delta_3] \equiv (A^uB^uC^{1+2s(\delta_{2,m}-1)+u})^{-1} \equiv C^{-1-2s(\delta_{2,m}-1)-u}B^{-u}A^{-u} \mod Z_1(J). \tag{5.75}$$

To conjugate $B\Delta_3$ by $[B\Delta_3, A\Delta_3]$ we need a sharpening of (5.74) and information on how each factor of (5.75) conjugates $B\Delta_3$.

Applying Theorem 5.7 to $B\Delta_3 = (A^0B^{1+s(2\delta_{2,m}+s-3)}C^0)(A^sB^0C^0)$, we obtain

$$\begin{aligned} B\Delta_3 &= A^{s-u\ell+2us\delta_{2,m}}B^{1-3s+2s\delta_{2,m}+u+3us\ell+2us\delta_{2,m}}C^{-s-3ur\ell+u(\ell+1)+2u(\delta_{2,m}+1)+us(\delta_{2,m}+r+1)} \\ &\qquad A^{us\ell^2(r+1)+2us+u^2(\delta_{2,m}+r+1)}. \\ &= A^{s-u\ell}B^{1-3s+2s\delta_{2,m}+u}C^{-s+ur\ell}A^{us(r\ell^2+\ell^2+1)+2us(\delta_{2,m}+1)}, \end{aligned}$$

where the exponents of A, B, C were reduced modulo $4us, 4us, 4u$ to produce the first equality, and we used $A^{2u} \in Z_1(J)$, $A^{2u}B^{2u} = 1$, and $A^{2us} = C^{2u}$ to obtain the second equality.

By (2.1) and Theorem 5.3, we have $[A^{s-u\ell}, C^{-1-2s(\delta_{2,m}-1)-u}] = [A^{s-u\ell}, C^{-1}] = A^{-2u\ell+2us}$, $[B^{1-3s+2s\delta_{2,m}+u}, C^{-1-2s(\delta_{2,m}-1)-u}] = B^{2s\ell-2u\ell(5-4\delta_{2,m})}$, $[C^{-s+ur\ell}, B^{-u}] = 1$, $[C^{-s+ur\ell}, A^{-u}] = 1$, $[A^{s-u\ell}, B^{-u}] = [A^s, B^{-u}] = A^{u^2}$, and $[B^{\alpha-3s+2s\delta_{2,m}+u}, A^{-u}] = [B^{1+s}, A^{-u}] = A^{us\ell+u^2}C^u$.

Using the above commutators to compute $(B\Delta_3)^{[B\Delta_3, A\Delta_3]}$ yields

$$\begin{aligned} (B\Delta_3)^{[B\Delta_3,A\Delta_3]} &= (A^{s-u\ell}B^{1-3s+2s\delta_{2,m}+u}C^{-s+ur\ell})^{C^{-1-2s(\delta_{2,m}-1)-u}B^{-u}A^{-u}}A^{us(r\ell^2+\ell^2+1)+2us(\delta_{2,m}+1)} \\ &= (A^{s-u\ell}B^{\alpha-3s+2s\delta_{2,m}+u}C^{-s+ur\ell})^{B^{-u}A^{-u}}A^{8u\ell(1-\delta_{2,m})+us(r\ell^2+\ell^2+1)+2us\delta_{2,m}} \\ &= (A^{s-u\ell}B^{\alpha-3s+2s\delta_{2,m}+u}C^{-s+ur\ell})^{A^{-u}}A^{8u\ell(1-\delta_{2,m})+us(r\ell^2+\ell^2+1)+2us\delta_{2,m}+u^2} \\ &= A^{s-u\ell}B^{\alpha-3s+2s\delta_{2,m}+u}C^{-s+u+ur\ell}A^{8u\ell(1-\delta_{2,m})+us\ell(r\ell-1)+2us\delta_{2,m}}. \end{aligned}$$

On the other hand, applying Theorem 5.10 to

$$(A^{s-u\ell}B^{1-3s+2s\delta_{2,m}+u}C^{-s+ur\ell})^\alpha = A^{\exp A+\xi_4}B^{\exp B}C^{\exp C}$$

yields, $\exp A \equiv s - u\ell + 2u\ell - us\ell^2 + 2us + u^2 \mod 4us$, $\exp B \equiv \alpha - 3s + 2s\delta_{2,m} + u - 6u\ell + 4u\ell\delta_{2,m} + 2us + u^2 \mod 4us$, $\exp C \equiv -s - u + ur\ell + u(3-\ell) + usr \mod 4u$, and $\xi_4 \equiv u^2(r+1) \mod 4us$, so

$$\begin{aligned} &(A^{s-u\ell}B^{1-3s+2s\delta_{2,m}+u}C^{-s+ur\ell})^\alpha \\ &= A^{s-u\ell+2u\ell-us\ell^2+2us+u^2}B^{\alpha-3s+2s\delta_{2,m}+u-6u\ell+4u\ell\delta_{2,m}+2us+u^2}C^{-s-u+ur\ell+u(3-\ell)+usr}A^{u^2(r+1)} \\ &= A^{s-u\ell}B^{\alpha-3s+2s\delta_{2,m}+u}C^{-s-u+ur\ell}A^{4u\ell(2-\delta_{2,m})+us\ell+u^2}. \end{aligned}$$

This and $C^{2u} = A^{2us}$ yield

$$\begin{aligned} (B\Delta_3)^\alpha &= (A^{s-u\ell}B^{1-3s+2s\delta_{2,m}+u}C^{-s+ur\ell})^\alpha A^{us(r\ell^2+\ell^2+1)+2us(\delta_{2,m}+1)} \\ &= A^{s-u\ell}B^{\alpha-3s+2s\delta_{2,m}+u}C^{-s+u+ur\ell}A^{4u\ell(2-\delta_{2,m})+us\ell(r\ell-1)+2us\delta_{2,m}+u^2}. \end{aligned}$$

Then $(B\Delta_3)^{[B\Delta_3,A\Delta_3]} = (B\Delta_3)^\alpha$ if and only if $A^{4u\ell\delta_{2,m}+u^2} = 1$ if and only if $s \mid \ell\delta_{2,m} + r^2$. If $m = 2$, then $s = 2$ is a factor of $\ell + 1 = \ell\delta_{2,m} + r^2$. If $m > 2$, then $s \geq 4$ is a factor of $s\frac{r}{2} = \ell\delta_{2,m} + r^2$. Thus $(B\Delta_3)^{[B\Delta_3,A\Delta_3]} = (B\Delta_3)^\alpha$ and Δ_3 extends to an endomorphism of J.

Let's see that Δ_3 fixes $Z_1(J)$. By Theorem 5.10 applied to $(A^{1+s}B^s)^{2u} = A^{\exp A+\xi_4}B^{\exp B}C^{\exp C}$, we get $\exp A \equiv 2u + 2us \mod 4us$, $\exp B \equiv 2us + u^2 \mod 4us$, $\exp C \equiv us \mod 4u$, and $\xi_4 \equiv 0 \mod 4us$, so

$$(A^{2u})\Delta_3 = (A\Delta_3)^{2u} = (A^{1+s}B^s)^{2u} = A^{2u+2us}B^{2us+u^2}C^{us} = A^{2u}.$$

Then Δ_3 is an automorphism of J. □

Once again, we set $\overline{r} = r/2$ whenever $m > 2$.

Proposition 5.76. *Suppose that $m > 2$. Then the assignment*

$$A \mapsto A^{1+r}B^rA^{s(sk+r\ell-2)},\ B \mapsto B^{1+r}A^r,$$

where k is even if $m > 3$ and odd if $m = 3$, extends to an automorphism, say Σ, of J.

Proof. Let $i = sk + r\ell - 2$. Applying Theorem 5.7 to

$$A\Sigma = (A^{1+r}B^rC^0)(A^{si}B^0C^0) = A^{\exp A+\xi_2}B^{\exp B}C^{\exp C}$$

yields $\exp A \equiv 1+r+si-uri\ell \mod 4us$, $\exp B \equiv r+uri\ell+usi\overline{r} \mod 4us$, $\exp C \equiv -sri+ui\overline{r} \mod 4u$, and $\xi_2 \equiv usi\overline{r} \mod 4us$, so

$$\begin{aligned} A\Sigma &= A^{1+r+si-uri\ell}B^{r+uri\ell+usi\overline{r}}C^{-sri+ui\overline{r}}A^{usi\overline{r}} \\ &= A^{1+r+si}B^rC^{-sri}A^{usi(\overline{r}+1)}. \end{aligned}$$

Also, applying the same theorem to $B\Sigma = (A^0B^{1+r}C^0)(A^rB^0C^0) = A^{\exp A+\xi_2}B^{\exp B}C^{\exp C}$ yields $\exp A \equiv r - sr\ell + ur\overline{r}\ell \mod 4us$, $\exp B \equiv 1 + r - u\overline{r}\ell - ur\overline{r}\ell \mod 4us$, $\exp C \equiv -r - s\overline{r} + sr\ell(\overline{r}+1) \mod 4u$, and $\xi_2 \equiv ur\ell^2(1-\overline{r}) + 4u\ell^2(\overline{r}-1)\varphi(r+1) - us\overline{r} + 2us(\overline{r}-1)\varphi(r+1) + usr \equiv ur\ell^2(1-\overline{r}) + 4u(\overline{r}-1)\varphi(r+1) - us\overline{r} + usr\overline{r} \mod 4us$, so

$$\begin{aligned} B\Sigma &= A^{r-sr\ell+ur\overline{r}\ell}B^{1+r-u\overline{r}\ell-ur\overline{r}\ell}C^{-r-s\overline{r}+sr\ell(\overline{r}+1)} \\ &\quad A^{ur\ell^2(1-\overline{r})+4u\ell^2(\overline{r}-1)\varphi(r+1)-us\overline{r}+2us(\overline{r}-1)\varphi(r+1)+usr} \\ &= A^{r-sr\ell}B^{1+r-u\overline{r}\ell}C^{-r-s\overline{r}+sr\ell(\overline{r}+1)}A^{ur\ell^2(1-\overline{r})+4u(\overline{r}-1)\varphi(r+1)+us\overline{r}(\ell-1)+usr\overline{r}}. \end{aligned}$$

Then $[A\Sigma, B\Sigma] = [A^{1+r+si}B^rC^{-sri}, A^{r-sr\ell}B^{1+r-u\overline{r}\ell}C^{-r-s\overline{r}+sr\ell(\overline{r}+1)}]$.
Applying Proposition 5.9 to $[A\Sigma, B\Sigma]$ produces $\exp A \equiv -sr\ell + u(\overline{r}+1) \mod 2u$, $\exp B \equiv sr\ell + u(\overline{r}+1) \mod 2u$, and $\exp C \equiv 1 + s + si + sri \mod 2u$, so

$$[A\Sigma, B\Sigma] \equiv A^{\exp A}B^{\exp B}C^{\exp C} \equiv A^{-sr\ell+u(\overline{r}+1)}B^{sr\ell+u(\overline{r}+1)}C^{1+s+si+sri} \mod Z_1(J).$$

Thus

$$(A\Sigma)^{[A\Sigma,B\Sigma]} = (A^{1+r+si}B^rC^{-sri})^{A^{-sr\ell+u(\overline{r}+1)}B^{sr\ell+u(\overline{r}+1)}C^{1+s+si+sri}}A^{usi(\overline{r}+1)}.$$

By Theorem 5.3 applied to $[B^r, A^{-sr\ell+u(\overline{r}+1)}] = (A^{\exp A+\xi_1}B^{\exp B}C^{\exp C})^{-1}$ we get $\exp A \equiv -us\overline{r}+usr(\overline{r}+1) \mod 4us$, $\exp B \equiv us\overline{r}+usr \mod 4us$, $\exp C \equiv -u\overline{r}\ell+ur \mod 4u$, and $\xi_1 \equiv usr\overline{r} \mod 4us$, so

$$[B^r, A^{-sr\ell+u(\overline{r}+1)}] = (A^{-us\overline{r}+usr(\overline{r}+1)}B^{us\overline{r}+usr}C^{-u\overline{r}\ell+ur}A^{usr\overline{r}})^{-1} = C^{u\overline{r}\ell}.$$

By Theorem 5.3, $[C^{-sri}, A^{-sr\ell+u(\overline{r}+1)}] = 1$.
Applying the same theorem to $[A^{1+r+si}, B^{sr\ell+u(\overline{r}+1)}] = A^{\exp A+\xi_1}B^{\exp B}C^{\exp C}$ gives $\exp A \equiv -us\overline{r}+usr \mod 4us$, $\exp B \equiv -ur\ell^2-us(\overline{r}\ell+\overline{r}+\ell)+usr(\overline{r}+1) \mod 4us$, and $\exp C \equiv sr\ell+u(\overline{r}\ell+\overline{r}+1)+ur \mod 4u$, $\xi_1 \equiv usr\overline{r} \mod 4us$, so

$$\begin{aligned}[A^{1+r+si}, B^{sr\ell+u(\overline{r}+1)}] &= A^{-us\overline{r}+usr}B^{-ur\ell^2-us(\overline{r}\ell+\overline{r}+\ell)+usr(\overline{r}+1)}C^{sr\ell+u(\overline{r}\ell+\overline{r}+1)+ur}A^{usr\overline{r}} \\ &= A^{ur\ell^2+us(\overline{r}+\ell)}C^{sr\ell+u}.\end{aligned}$$

Also, $[C^{-sri+u\overline{r}\ell}, B^{sr\ell+u(\overline{r}+1)}] = 1$, $[C^{sr\ell+u}, B^r] = B^{usr}$,
$[A^{1+r+si}, C^{1+s+si+sri}] = A^{2s\ell+2u\ell+4ui\ell+u\ell+us\ell+2us}$, and $[B^r, C^{1+s+si+sri}] = B^{-u\ell-us\ell+usi+2us}$.
Gathering the above commutators produces

$$\begin{aligned}(A\Sigma)^{[A\Sigma,B\Sigma]} &= (A^{1+r+si}B^rC^{-sri+u\overline{r}\ell})^{B^{sr\ell+u(\overline{r}+1)}C^{1+s+si+sri}}A^{usi(\overline{r}+1)} \\ &= (A^{1+r+si}C^{sr\ell+u}B^rC^{-sri+u\overline{r}\ell})^{C^{1+s+si+sri}}A^{ur\ell^2+us(\overline{r}+\ell)+usi(\overline{r}+1)} \\ &= (A^{1+r+si}B^rC^{sr\ell+u-sri+u\overline{r}\ell})^{C^{1+s+si+sri}}A^{ur\ell^2+us(\overline{r}+\ell)+usi(\overline{r}+1)+usr} \\ &= A^{\alpha+r+si+u\ell}B^{r-u\ell}C^{sr\ell+u-sri+u\overline{r}\ell}A^{2u\ell+4ui\ell+ur\ell^2+us(\overline{r}+\ell)+usi\overline{r}+usr+2us}.\end{aligned}$$

On the other hand, applying Theorem 5.10 to $(A^{1+r+si}B^rC^{-sri})^\alpha = A^{\exp A+\xi_4}B^{\exp B}C^{\exp C}$ gives $\exp A \equiv \alpha+r+si+u\ell+2ui\ell+u\ell\varphi(\alpha)+us\overline{r}+usr\overline{r} \mod 4us$, $\exp B \equiv r+u\ell+ur\ell^2 \mod 4us$, $\exp C \equiv -sr\ell-sri-u\overline{r}\ell+sr\varphi(\alpha)+ur\overline{r} \equiv -sr\ell-sri-u\overline{r}\ell+ur(\overline{r}+1) \mod 4u$, and $\xi_4 \equiv ur\varphi(\alpha)+usr(\overline{r}+1) \equiv usr\overline{r} \mod 4us$, so

$$\begin{aligned}&(A^{1+r+si}B^rC^{-sri})^\alpha \\ &= A^{\alpha+r+si+u\ell+2ui\ell+u\ell\varphi(\alpha)+us\overline{r}+usr\overline{r}}B^{r+u\ell+ur\ell^2}C^{-sr\ell-sri-u\overline{r}\ell+ur(\overline{r}+1)}A^{usr\overline{r}} \\ &= A^{\alpha+r+si+u\ell}B^{r+u\ell}C^{-sr\ell-sri-u\overline{r}\ell}A^{2ui\ell+u\ell\varphi(\alpha)-ur\ell^2+us\overline{r}+usr(\overline{r}+1)},\end{aligned}$$

and from this,

$$\begin{aligned}(A\Sigma)^\alpha &= (A^{1+r+si}B^rC^{-sri})^\alpha A^{usi(\overline{r}+1)} \\ &= A^{\alpha+r+si+u\ell}B^{r+u\ell}C^{-sr\ell-sri-u\overline{r}\ell}A^{2ui\ell+u\ell\varphi(\alpha)-ur\ell^2+us\overline{r}+usi(\overline{r}+1)+usr(\overline{r}+1)}.\end{aligned}$$

Then $(A\Sigma)^{[A\Sigma,B\Sigma]} = (A\Sigma)^{\alpha}$ if and only if $A^{4u\ell+2ui\ell-u\ell\varphi(\alpha)+2us+usi+usr(\overline{r}+1)} = 1$. Replacing $i = sk + r\ell - 2$, the last expression is equivalent to $A^{us-u\ell\varphi(\alpha)+usr\overline{r}+2usk} = 1$, which is true whenever $1 - \frac{\varphi(\alpha)}{s}\ell + r\overline{r} + 2k \equiv 0 \mod 4$. This congruence can be immediately verified.
As for the second relation, we have

$$\begin{aligned}[B\Sigma, A\Sigma] &\equiv (A^{-sr\ell+u(\overline{r}+1)}B^{sr\ell+u(\overline{r}+1)}C^{1+s+si+sri})^{-1} \\ &\equiv C^{-1-s-si-sri}B^{-sr\ell-u(\overline{r}+1)}A^{sr\ell-u(\overline{r}+1)} \mod Z_1(J).\end{aligned}$$

Thus

$$\begin{aligned}(B\Sigma)^{[B\Sigma,A\Sigma]} = (A^{r-sr\ell}B^{1+r-u\overline{r}\ell}C^{-r-s\overline{r}+sr\ell(\overline{r}+1)})^{C^{-1-s-si-sri}B^{-sr\ell-u(\overline{r}+1)}A^{sr\ell-u(\overline{r}+1)}} \\ A^{ur\ell^2(1-\overline{r})+4u(\overline{r}-1)\varphi(r+1)+us\overline{r}(\ell-1)+usr\overline{r}}.\end{aligned}$$

From Theorem 5.3 we obtain $[A^{r-sr\ell}, C^{-1-s-si-sri}] = A^{-u\ell+us(\ell-1)+2us+usi}$ and $[B^{1+r-u\overline{r}\ell}, C^{-1-s-si-sri}] = B^{2s\ell+3u\ell+2ui\ell+us\ell+2us+usr}$.
Applying Theorem 5.3 to $[A^{r-sr\ell-u\ell}, B^{-sr\ell-u(\overline{r}+1)}] = A^{\exp A+\xi_1}B^{\exp B}C^{\exp C}$ gives, $\exp A \equiv -us\overline{r} + usr \mod 4us$, $\exp B \equiv us\overline{r} + usr(\overline{r}+1) \mod 4us$, $\exp C \equiv -u\overline{r}\ell + ur \mod 4u$, and $\xi_1 \equiv usr\overline{r} \mod 4us$, so

$$[A^{r-sr\ell-u\ell}, B^{-sr\ell-u(\overline{r}+1)}] = A^{-us\overline{r}+usr}B^{us\overline{r}+usr(\overline{r}+1)}C^{-u\overline{r}\ell+ur}A^{usr\overline{r}} = C^{-u\overline{r}\ell}.$$

By Theorem 5.3, $[C^{-r-s\overline{r}+sr\ell(\overline{r}-1)}, B^{-sr\ell-u(\overline{r}+1)}] = B^{usr}$, $[C^{-u\overline{r}\ell}, B^{\alpha+r+u\ell(1-\overline{r})}] = B^{usr}$, and $[C^{-r-s\overline{r}-sr\ell(\overline{r}-1)-u\overline{r}\ell}, A^{sr\ell-u(\overline{r}+1)}] = A^{usr}$. Also, applying the same theorem to $[A^{sr\ell-u(\overline{r}+1)}, B^{\alpha+r+u\ell(1-\overline{r})}] = A^{\exp A+\xi_1}B^{\exp B}C^{\exp C}$ gives, $\exp A \equiv ur\ell^2+us(\overline{r}-\overline{r}\ell-\ell)+usr(\overline{r}+1) \mod 4us$, $\exp B \equiv us\overline{r}+usr \mod 4us$, $\exp C \equiv sr\ell-u+u\overline{r}(\ell-1)+ur \mod 4u$, and $\xi_1 \equiv usr\overline{r} \mod 4us$, so

$$\begin{aligned}&[B^{\alpha+r+u\ell(1-\overline{r})}, A^{sr\ell-u(\overline{r}+1)}] \\ &= (A^{ur\ell^2+us(\overline{r}-\overline{r}\ell-\ell)+usr(\overline{r}+1)}B^{us\overline{r}+usr}C^{sr\ell-u+u\overline{r}(\ell-1)+ur}A^{usr\overline{r}})^{-1} \\ &= A^{-ur\ell^2+us(\overline{r}+\ell)+usr}C^{-sr\ell+u}.\end{aligned}$$

Gathering all the above commutators produces

$$\begin{aligned}(B\Sigma)^{[B\Sigma,A\Sigma]} &= (A^{r-sr\ell-u\ell}B^{\alpha+r+u\ell(1-\overline{r})}C^{-r-s\overline{r}+sr\ell(\overline{r}+1)})^{B^{-sr\ell-u(\overline{r}+1)}A^{sr\ell-u(\overline{r}+1)}}\\ &\quad A^{ur\ell^2(1-\overline{r})+4u(\overline{r}-1)\varphi(r+1)-2u\ell-us-2ui\ell+us\overline{r}(\ell-1)+usr(\overline{r}+1)+usi}\\ &= (A^{r-sr\ell-u\ell}C^{-u\overline{r}\ell}B^{\alpha+r+u\ell(1-\overline{r})}C^{-r-s\overline{r}+sr\ell(\overline{r}+1)})^{A^{sr\ell-u(\overline{r}+1)}}\\ &\quad A^{ur\ell^2(1-\overline{r})+4u(\overline{r}-1)\varphi(r+1)-2u\ell-us-2ui\ell+us\overline{r}(\ell-1)+usr\overline{r}+usi}\\ &= (A^{r-sr\ell-u\ell}B^{\alpha+r+u\ell(1-\overline{r})}C^{-r-s\overline{r}+sr\ell(\overline{r}+1)-u\overline{r}\ell})^{A^{sr\ell-u(\overline{r}+1)}}\\ &\quad A^{ur\ell^2(1-\overline{r})+4u(\overline{r}-1)\varphi(r+1)-2u\ell-us-2ui\ell+us\overline{r}(\ell-1)+usr(\overline{r}+1)+usi}\\ &= A^{r-sr\ell-u\ell}B^{\alpha+r+u\ell(1-\overline{r})}C^{-r-s\overline{r}+sr\overline{r}\ell+u(1-\overline{r}\ell)}\\ &\quad A^{-ur\overline{r}\ell^2+4u(\overline{r}-1)\varphi(r+1)-2u\ell-2ui\ell+us\overline{r}\ell+us(\ell-1)+usi+usr(\overline{r}+1)}.\end{aligned}$$

On the other hand, applying Theorem 5.10 to

$$(A^{r-sr\ell}B^{1+r-u\overline{r}\ell}C^{-r-s\overline{r}+sr\ell(\overline{r}+1)})^{\alpha} = A^{\exp A+\xi_4}B^{\exp B}C^{\exp C},$$

we get $\exp A \equiv r-sr\ell+u\ell-ur\ell^2-us+ur\varphi(\alpha)+usr\overline{r} \equiv r-sr\ell+u\ell-ur\ell^2-us+usr(\overline{r}+1) \mod 4us$, $\exp B \equiv \alpha+r+u\ell(1-\overline{r})-us\overline{r}+usr(\overline{r}+1)+2us+2u\varphi(\alpha) \equiv \alpha+r+u\ell(1-\overline{r})-us\overline{r}+usr(\overline{r}+1) \mod 4us$, $\exp C \equiv -r-s\overline{r}+sr\overline{r}\ell-u\ell(\overline{r}+1)+ur\overline{r} \mod 4u$, and $\xi_4 \equiv usr(\overline{r}+1) \mod 4us$, so

$$\begin{aligned}&(A^{r-sr\ell}B^{1+r-u\overline{r}\ell}C^{-r-s\overline{r}+sr\ell(\overline{r}+1)})^{\alpha}\\ &= A^{r-sr\ell+u\ell-ur\ell^2-us+usr(\overline{r}+1)}B^{\alpha+r+u\ell(1-\overline{r})-us\overline{r}+usr(\overline{r}+1)}C^{-r-s\overline{r}+sr\overline{r}\ell-u\ell(\overline{r}+1)+ur\overline{r}}A^{usr(\overline{r}+1)}\\ &= A^{r-sr\ell+u\ell}B^{\alpha+r+u\ell(1-\overline{r})}C^{-r-s\overline{r}+sr\overline{r}\ell-u\ell(\overline{r}+1)}A^{-ur\ell^2+us(\overline{r}-1)+usr},\end{aligned}$$

and from this,

$$\begin{aligned}&(B\Sigma)^{\alpha}\\ &= (A^{r-sr\ell}B^{1+r-u\overline{r}\ell}C^{-r-s\overline{r}+sr\ell(\overline{r}+1)})^{\alpha}A^{ur\ell^2(1-\overline{r})+4u(\overline{r}-1)\varphi(r+1)+us\overline{r}(\ell-1)+usr\overline{r}}\\ &= A^{r-sr\ell+u\ell}B^{\alpha+r+u\ell(1-\overline{r})}C^{-r-s\overline{r}+sr\overline{r}\ell-u\ell(\overline{r}+1)}A^{-ur\overline{r}\ell^2+4u(\overline{r}-1)\varphi(r+1)+us(\overline{r}-1)+us\overline{r}(\ell-1)+usr(\overline{r}+1)}.\end{aligned}$$

Then $(B\Sigma)^{[B\Sigma,A\Sigma]} = (B\Sigma)^{\alpha}$ if and only if $A^{4u\ell+2ui\ell-us+2us+usi} = 1$. Replacing $i = sk+r\ell-2$, the last expression is equivalent to $A^{2usk+usr} = 1$, which happens to be true whenever $k+\overline{r}$ is even. The conditions on k confirm that this is the case. Thus the equality $(B\Sigma)^{[B\Sigma,A\Sigma]} = (B\Sigma)^{\alpha}$ holds and the given assignment extends to an endomorphism of J.
Let us see that Σ is an automorphism. We have

$$(A^{2u})\Sigma = (A\Sigma)^{2u} = (A^{1+r+si}B^{r}C^{-sri})^{2u}.$$

Applying Theorem 5.10 to $(A^{1+r+si}B^rC^{-sri})^{2u} = A^{\exp A+\xi_4}B^{\exp B}C^{\exp C}$ gives $\exp A \equiv 2u + us \mod 4us$, $\exp B \equiv us + usr \mod 4us$, $\exp C \equiv ur \mod 4u$, $\xi_4 \equiv 0 \mod 4us$, so

$$(A^{2u})\Sigma = A^{2u+us}B^{us+usr}C^{ur} = A^{2u}.$$

Thus Σ fixes $Z_1(J)$ pointwise and it is an automorphism. □

Theorem 5.77. *The factors of the series* (5.65) *are as follows:*

$$\mathrm{Aut}_1(J) \cong (\mathbb{Z}/2^m\mathbb{Z})^2,\ \mathrm{Aut}_2(J)/\mathrm{Aut}_1(J) \cong (\mathbb{Z}/2^m\mathbb{Z})^2,$$

$$\mathrm{Aut}_3(J)/\mathrm{Aut}_2(J) \cong (\mathbb{Z}/2^{m-1}\mathbb{Z})^2 \times (\mathbb{Z}/2\mathbb{Z}),\ \mathrm{Inn}(J)\mathrm{Aut}_3(J)/\mathrm{Aut}_3(J) \cong (\mathbb{Z}/2^{m-1}\mathbb{Z})^2,$$

$$\mathrm{Aut}_4(J)/\mathrm{Inn}(J)\mathrm{Aut}_3(J) \cong \mathbb{Z}/2\mathbb{Z},\ \mathrm{Aut}(J)/\mathrm{Aut}_4(J) \cong \begin{cases} (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } m > 2, \\ \mathbb{Z}/2\mathbb{Z} & \text{if } m = 2. \end{cases}$$

Thus $|\mathrm{Aut}(J)| = 2^{8m}$ *if* $m > 2$ *and* $|\mathrm{Aut}(J)| = 2^{15}$ *if* $m = 2$. *Moreover,* $\mathrm{Aut}(J)$ *is generated by* $\Omega_{(1,A^{2^{2m-1}})}, \Psi_{(1,C^{2^{m-1}})}, \Delta_1, \Delta_2, A\delta, \Delta_3, \theta$, *and, if* $m > 2$, *also* Σ, *where:* $\Omega_{(1,A^{2^{2m-1}})}$ *is defined in Proposition 5.61;* $\Psi_{(1,C^{2^{m-1}})}$ *is given in Proposition 5.62;* Δ_1 *and* Δ_2 *are defined in Theorem 5.66;* $A\delta$ *is conjugation by* A; Δ_3 *is given in Proposition 5.73;* θ *is the automorphism* $A \leftrightarrow B$; *and* Σ *is defined in Proposition 5.76.*

Proof. The descriptions of the first 4 factors follow from Propositions 5.61, 5.62, and Theorem 5.66.

As indicated in Sections 5.3 and 5.4, we have presentations

$$K = \langle\, a, b \mid a^{[a,b]} = a^\alpha,\ b^{[b,a]} = b^\alpha,\ a^{2^{2m-1}} = 1,\ b^{2^{2m-1}} = 1,\ [a,b]^{2^{m-1}} = 1 \,\rangle,$$

$$H = \langle\, A_0, B_0 \mid A_0^{[A_0,B_0]} = A_0^\alpha,\ B_0^{[B_0,A_0]} = B_0^\alpha,\ A_0^{2^{2m-1}} = 1,\ B_0^{2^{2m-1}} = 1 \,\rangle.$$

Let $\pi_1 : J \to H$ and $\pi_2 : H \to K$ be the projection maps, given by $A \mapsto A_0, B \mapsto B_0$ and $A_0 \mapsto a, B_0 \mapsto b$, respectively.
Consider $\mathrm{Aut}(J)/\mathrm{Aut}_4(J)$, by Proposition 5.47, we have an imbedding

$$f : \mathrm{Aut}(J)/\mathrm{Aut}_4(J) \hookrightarrow \mathrm{Aut}(H)/\mathrm{Aut}_3(H).$$

If $m = 2$, then $\langle\overline{\nu}\rangle = \mathrm{Aut}(H)/\mathrm{Aut}_3(H) \cong \mathbb{Z}/2\mathbb{Z}$ by Theorem 5.59, where ν is the automorphism $A_0 \leftrightarrow B_0$; As $\langle\overline{\theta}\rangle^f = \langle\overline{\nu}\rangle$, it follows that $\mathrm{Aut}(J)/\mathrm{Aut}_4(J) \cong \mathbb{Z}/2\mathbb{Z}$. If $m > 2$, Theorem 5.59 gives $\langle\overline{\nu}, \overline{\Sigma_0}\rangle = \mathrm{Aut}(H)/\mathrm{Aut}_3(H) \cong (\mathbb{Z}/2\mathbb{Z})^2$, where Σ_0 is as defined in Corollary 5.57; since $\overline{\Sigma}^f = \overline{\Sigma_0}$, we deduce that $\mathrm{Aut}(J)/\mathrm{Aut}_4(J) \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Next consider $\mathrm{Aut}_4(J)/\mathrm{Inn}(J)\mathrm{Aut}_3(J)$. By Proposition 5.47, we likewise have an imbedding

$$\eta_1 : \mathrm{Aut}_4(J)/\mathrm{Inn}(J)\mathrm{Aut}_3(J) \hookrightarrow \mathrm{Aut}_3(H)/\mathrm{Inn}(H)\mathrm{Aut}_2(H). \tag{5.78}$$

By Theorem 4.16, $\Delta_3 \in \mathrm{Aut}_4(J)$, and we show below that the image of η_1 has order 2 and is generated by $\overline{\Delta_3}$. The order of $\mathrm{Aut}(J)$ follows immediately from the structure of the above factors. Moreover, by Propositions 5.61, 5.62, and Theorem 5.66, we have

$$\mathrm{Inn}(J)\mathrm{Aut}_3(J) = \langle \Omega_{(1,A^{2^{2m-1}})}, \Omega_{(A^{2^{2m-1}},1)}, \Psi_{(1,C^{2^{m-1}})}, \Psi_{(C^{2^{m-1}},1)}, \Delta_1, \Delta_2, A\delta, B\delta \rangle. \tag{5.79}$$

It follows from (5.79) and the above considerations that $\mathrm{Aut}(J)$ is generated by the right-hand side of (5.79) together with Δ_3, θ as well as Σ if $m > 2$. The use of θ allows us to reduce these generators to the stated list.

We proceed to compute the required image of η_1. By Theorem 5.48, the image of η_1 is contained in $\overline{\langle \Gamma_0, \Gamma_0^\nu \rangle}$, where Γ_0 is as defined in Proposition 5.46, namely by $A_0 \mapsto A_0^{1+s}$, $B_0 \mapsto B_0 A_0^s$, and $\overline{\langle \Gamma_0, \Gamma_0^\nu \rangle}$ is the Klein 4-group.

By Propositions 5.35 and 5.47, we have maps

$$\eta_2 : \mathrm{Aut}_3(H)/\mathrm{Inn}(H)\mathrm{Aut}_2(H) \to \mathrm{Aut}_2(K)/\mathrm{Inn}(K)\mathrm{Aut}_1(K),$$

$$\eta_3 : \mathrm{Aut}_2(K)/\mathrm{Inn}(K)\mathrm{Aut}_1(K) \to Z_2(K)^2/(Z_1(K) \times \langle c \rangle)^2,$$

where η_2 is injective and η_3 is a bijection between two copies of $(\mathbb{Z}/2\mathbb{Z})^4$. In this notation, we have

$$\overline{\Delta_3}\eta_1\eta_2\eta_3 = \overline{(a^s b^s, a^s b^{s(2\delta_{2,m}+s-3)})}.$$

As $Z_1(K) = \langle a^{2s}, b^{2s} \rangle$, it follows that $\overline{\Delta_3}\eta_1\eta_2\eta_3$ is nontrivial, whence $\overline{\Delta_3}\eta_1$ is a nontrivial element of the Klein 4-group $\overline{\langle \Gamma_0, \Gamma_0^\nu \rangle}$. Thus, either $\mathrm{Im}(\eta_1) = \langle \overline{\Delta_3}\eta_1 \rangle$ has order 2, or else $\mathrm{Im}(\eta_1) = \langle \overline{\Gamma_0}, \overline{\Gamma_0^\nu} \rangle$ is the Klein 4-group. Suppose, if possible, that the latter case occurs. Then necessarily $\overline{\Gamma_0} \in \mathrm{Im}(\eta_1)$. Since $\mathrm{Inn}(J)$ maps onto $\mathrm{Inn}(H)$, we infer the existence of $\gamma \in \mathrm{Aut}_2(H)$ such that $\Gamma_0\gamma$ lifts to an automorphism, say β, of J. Here $\Gamma_0\gamma$ is given by $A_0 \mapsto A_0^{1+s}w_1$, $B_0 \mapsto B_0 A_0^s w_2$, with w_1, w_2 in $Z_2(H)$, so β is given by $A \mapsto A^{1+s}u_1$, $B \mapsto BA^s u_2$, with $u_1, u_2 \in Z_3(J)$. As $A^s \in Z_4(J)$, we can write this in the form $A \mapsto A^{1+s}u_1$, $B \mapsto A^s B v_2$, with $u_1, v_2 \in Z_3(J)$, against Proposition 5.72. □

5.6 Appendix 2

We assume in this section that $m \geq 1$ and recall the definitions of ϕ and φ given in Section 5.1.

Given $n, k \in \mathbb{Z}$, we readily verify that ϕ and φ satisfy the following properties:

$$\phi(n + 8usk) \equiv \phi(n) \mod 4us, \tag{5.80}$$

$$\varphi(n + 24usk) \equiv \varphi(n) \mod 4us, \tag{5.81}$$

$$\phi(-n) = \phi(n + 1), \tag{5.82}$$

$$\phi(n + 1) + \phi(n) = n^2, \tag{5.83}$$

$$\phi(nt) = \phi(n)\phi(t + 1) + \phi(n + 1)\phi(t), \tag{5.84}$$

$$\phi(n + k) = \phi(n) + \phi(k) + nk, \tag{5.85}$$

$$\varphi(n + k) = \varphi(n) + \varphi(k) + n\phi(k) + \phi(n)k. \tag{5.86}$$

Proof of Theorem 5.3: Suppose first that $n \in \mathbb{N}$ and $t \in \mathbb{Z}$. Since $\alpha^n \equiv (1 + 2s\ell)^n \equiv 1 + 2s\ell n + 4u\ell^2\phi(n) \mod 4us$, then

$$[C^n, A^t] = C^{-n}A^{-t}C^nA^t = (A^{-t})^{C^n}A^t = A^{t-t\alpha^n} = A^{-2s\ell nt-4u\ell^2\phi(n)t}.$$

If $n \in \mathbb{Z}$, let $k \in \mathbb{N}$ be such that $n + 8usk > 0$. Then, by the above and (5.80),

$$[C^n, A^t] = [C^{n+8usk}, A^t] = A^{-2s\ell nt-4u\ell^2\phi(n)t}.$$

This proves that (5.4) is true for all $n, t \in \mathbb{Z}$.

To prove (5.5) just apply the automorphism $A \leftrightarrow B$ to $[C^{-n}, A^t] = A^{2s\ell nt-4u\ell^2\phi(-n)t}$ and use the identity (5.82) to get $[C^n, B^t] = B^{2s\ell nt-4u\ell^2\phi(n+1)t}$ for every $n, t \in \mathbb{Z}$.

To prove (5.6) let us first see that for every $n \in \mathbb{Z}$,

$$[A^n, B] = A^{-2s\ell\phi(n)+4u\ell^2\varphi(n+1)}C^n. \tag{5.87}$$

It is clear that (5.87) holds for $n = 1$. Suppose it is true for some $n \geq 1$. Then

$$[A^{n+1}, B] = [A^n, B]^A [A, B] = (A^{-2s\ell\phi(n)+4u\ell^2\varphi(n+1)}C^n)^A C = A^{-2s\ell\phi(n)+4u\ell^2\varphi(n+1)}(C^n)^A C.$$

As $[C^n, A] = A^{-2s\ell n-4u\ell^2\phi(n)}$, then

$$[A^{n+1}, B] = A^{-2s\ell\phi(n)+4u\ell^2\varphi(n+1)}C^nA^{-2s\ell n-4u\ell^2\phi(n)}C.$$

Since $[C, A^{4u}] = 1$ and $[C^n, A^{-2s\ell n}] = A^{4u\ell^2n^2}$, using (5.83), (5.85), and (5.86), we get

$$[A^{n+1}, B] = A^{-2s\ell(\phi(n)+n)+4u\ell^2(\varphi(n+1)-\phi(n)+n^2)}C^{n+1} = A^{-2s\ell\phi(n+1)+4u\ell^2\varphi(n+2)}C^{n+1}.$$

By induction, it follows that (5.87) holds for all $n \in \mathbb{N}$. If $n \in \mathbb{Z}$, let $k \in \mathbb{N}$ be such that $n + 24usk > 0$. Then, by the above, (5.80), and (5.81),

$$[A^n, B] = [A^{n+24usk}, B] = A^{-2s\ell\phi(n)+4u\ell^2\varphi(n+1)}C^n,$$

so (5.87) holds for every $n \in \mathbb{Z}$.

Next fix $n \in \mathbb{Z}$. Let us see that (5.6) is true for every $t \in \mathbb{N}$ by induction on t. By (5.87), we have that (5.6) is true for $t = 1$. Suppose it is true for some $t \geq 1$ and set $\eta_{(x,y)} = A^{-2s\ell\phi(x)y}B^{2s\ell x\phi(y)}C^{xy-2s\ell\phi(x)\phi(y)}$. Then, by (5.87) and the inductive hypothesis,

$$[A^n, B^{t+1}] = [A^n, B][A^n, B^t]^B = (A^{-2s\ell\phi(n)+4u\ell^2\varphi(n+1)}C^n)(\eta_{(n,t)}A^{\xi_1(n,t)})^B.$$

Since $A^{\xi_1(n,t)} \in Z_1(J)$, then

$$[A^n, B^{t+1}] = A^{-2s\ell\phi(n)+4u\ell^2\varphi(n+1)}C^n\eta_{(n,t)}^B A^{\xi_1(n,t)}, \tag{5.88}$$

where

$$\eta_{(n,t)}^B = (A^{-2s\ell\phi(n)t}B^{2s\ell n\phi(t)}C^{nt-2s\ell\phi(n)\phi(t)})^B = (A^{-2s\ell\phi(n)t})^B B^{2s\ell n\phi(t)}(C^{nt-2s\ell\phi(n)\phi(t)})^B.$$

As $[A^{-2s\ell\phi(n)t}, B] = A^{-2u\ell^2\phi(n)t}C^{-2s\ell\phi(n)t}$, $[C^{nt-2s\ell\phi(n)\phi(t)}, B] = B^{2s\ell nt-4u\ell^2(\phi(n)\phi(t)+\phi(nt+1))}$, and $[C^{2s}, B^{2s}] = 1$, $[C, B^{4u}] = 1$ then

$$\begin{aligned}\eta_{(n,t)}^B &= A^{-2s\ell\phi(n)t-2u\ell^2\phi(n)t}C^{-2s\ell\phi(n)t}B^{2s\ell n\phi(t)}C^{nt-2s\ell\phi(n)\phi(t)}B^{2s\ell nt-4u\ell^2(\phi(n)\phi(t)+\phi(nt+1))}\\ &= A^{-2s\ell\phi(n)t-2u\ell^2\phi(n)t}B^{2s\ell n\phi(t)-4u\ell^2(\phi(n)\phi(t)+\phi(nt+1))}C^{nt}B^{2s\ell nt}C^{-2s\ell\phi(n)(t+\phi(t))}.\end{aligned}$$

Using that $[C^{nt}, B^{2s\ell nt}] = B^{4u\ell^2n^2t^2}$, $[C, B^{4u}] = 1$, and by (5.85), we have that

$$\eta_{(n,t)}^B = A^{-2s\ell\phi(n)t-2u\ell^2\phi(n)t}B^{2s\ell n\phi(t+1)-4u\ell^2(\phi(n)\phi(t)+\phi(nt+1)-n^2t^2)}C^{nt-2s\ell\phi(n)\phi(t+1)}.$$

Now, as $[C^n, A^{-2s\ell\phi(n)t}] = A^{4u\ell^2n\phi(n)t}$, $[C^n, B^{2s\ell n\phi(t+1)}] = B^{4u\ell^2n^2\phi(t+1)}$, and $[C, A^{2u}] = [C, B^{4u}] = 1$, then

$$\begin{aligned}C^n\eta_{(n,t)}^B = A^{-2s\ell\phi(n)t+2u\ell^2(2n-1)\phi(n)t}&B^{2s\ell n\phi(t+1)+4u\ell^2(n^2\phi(t+1)-\phi(n)\phi(t)-\phi(nt+1)+n^2t^2)}\\ &C^{n(t+1)-2s\ell\phi(n)\phi(t+1)}.\end{aligned} \tag{5.89}$$

Replacing (5.89) in (5.88) yields

$$\begin{aligned}[A^n, B^{t+1}] &= A^{-2s\ell\phi(n)(t+1)+2u\ell^2(2\varphi(n+1)+(2n-1)\phi(n)t)}B^{2s\ell n\phi(t+1)+4u\ell^2(n^2\phi(t+1)-\phi(n)\phi(t)-\phi(nt+1)+n^2t^2)}\\ &\quad C^{n(t+1)-2s\ell\phi(n)\phi(t+1)}A^{\xi_1(n,t)}\\ &= \eta_{(n,t+1)}A^{2u\ell^2(2\varphi(n+1)+(2n-1)\phi(n)t)}B^{4u\ell^2(n^2\phi(t+1)-\phi(n)\phi(t)-\phi(nt+1)+n^2t^2)}A^{\xi_1(n,t)}.\end{aligned}$$

By (5.2),

$$[A^n, B^{t+1}] = \eta_{(n,t+1)} A^{2u\ell^2\{2\varphi(n+1)+(2n-1)\phi(n)t-2n^2\phi(t+1)+2\phi(n)\phi(t)+2\phi(nt+1)-2n^2t^2\}} A^{\xi_1(n,t)}. \quad (5.90)$$

Successive applications of (5.83), (5.84), and (5.85) produce

$$2n^2\phi(t+1) = 4\phi(n)\phi(t) + 4\phi(n)t + 2n\phi(t) + 2nt, \quad (5.91)$$

$$2\phi(nt+1) = 4\phi(n)\phi(t) + 2\phi(n)t + 2n\phi(t) + 2nt, \quad (5.92)$$

$$2n^2t^2 = 8\phi(n)\phi(t) + 4\phi(n)t + 4n\phi(t) + 2nt. \quad (5.93)$$

Replacing (5.91), (5.92), and (5.93) in (5.90) yields

$$[A^n, B^{t+1}] = \eta_{(n,t+1)} A^{2u\ell^2\{2\varphi(n+1)+(2n-7)\phi(n)t-2nt-(3n+1)n\phi(t)\}} A^{\xi_1(n,t)},$$

where, by (5.85) and (5.86),

$$A^{2u\ell^2\{2\varphi(n+1)+(2n-7)\phi(n)t-2nt-(3n+1)n\phi(t)\}} A^{\xi_1(n,t)} = A^{\xi_1(n,t+1)}.$$

Thus $[A^n, B^{t+1}] = \eta_{(n,t+1)} A^{\xi_1(n,t+1)}$. This shows that (5.6) holds for every $n \in \mathbb{Z}$ and $t \in \mathbb{N}$.

Finally, if $t \in \mathbb{Z}$, let $k \in \mathbb{N}$ be such that $t + 24usk > 0$. Then, by the above, (5.80), and (5.81), we get $[A^n, B^t] = [A^n, B^{t+24usk}] = \eta_{(n,t+24usk)} A^{\xi_1(n,t+24usk)} = \eta_{(n,t)} A^{\xi_1(n,t)}$, and the result follows. □

Proof of Theorem 5.7: Let $\Delta = (A^i B^j C^k)(A^a B^b C^c)$ and set

$$\eta_{(x,y)} = A^{-2s\ell\phi(x)y} B^{2s\ell x\phi(y)} C^{xy-2s\ell\phi(x)\phi(y)}$$

as in the proof of Theorem 5.3. Let us first work with Δ modulo $Z_1(J)$.

From Theorem 5.3, we obtain $[C^k, A^a] = A^{-2s\ell ka} A^{-4u\ell^2\phi(k)a}$, $[B^j, A^a] = \eta^{-1}_{(a,j)} A^{-\xi_1(a,j)}$, and $\eta^{-1}_{(a,j)} = C^{2s\ell\phi(j)\phi(a)-ja} B^{-2s\ell\phi(j)a} A^{2s\ell j\phi(a)}$. Then

$$\Delta \equiv A^{i+a} B^j C^{2s\ell\phi(j)\phi(a)-ja} B^{-2s\ell\phi(j)a} A^{2s\ell j\phi(a)} C^k A^{-2s\ell ka} B^b C^c \mod Z_1(J).$$

Since $[C^{2s}, B^{2s}] = 1$, $[C^{-ja}, B^{-2s\ell\phi(j)a}] = B^{4u\ell^2 j\phi(j)a^2}$, $[C^k, A^{-2s\ell ka}] = A^{4u\ell^2k^2a}$, then

$$\Delta \equiv A^{i+a} B^{j-2s\ell\phi(j)a} C^{2s\ell\phi(j)\phi(a)-ja} A^{2s\ell(j\phi(a)-ka)} C^k B^b C^c \mod Z_1(J).$$

As $[C^{2s}, A^{2s}] = 1$, $[C^{-ja}, A^{2s\ell(j\phi(a)-ka)}] = A^{4u\ell^2 ja(j\phi(a)-ka)}$, $[C^k, B^b] = B^{2s\ell kb} B^{-4u\ell^2\phi(k+1)b}$, then

$$\Delta \equiv A^{i+a} B^{j-2s\ell\phi(j)a} A^{2s\ell(j\phi(a)-ka)} C^{2s\ell\phi(j)\phi(a)-ja} B^b C^k B^{2s\ell kb} C^c \mod Z_1(J).$$

Seeing that

$$[B^{j-2s\ell\phi(j)a}, A^{2s\ell(j\phi(a)-ka)}] = \eta^{-1}_{(2s\ell(j\phi(a)-ka),\, j-2s\ell\phi(j)a)} A^{-\xi_1(2s\ell(j\phi(a)-ka),\, j-2s\ell\phi(j)a)},$$

where

$$\begin{aligned}\eta^{-1}_{(2s\ell(j\phi(a)-ka),\, j-2s\ell\phi(j)a)} &= C^{2us\phi(j)a(ka-j\phi(a))} C^{2u\ell^2\phi(j)(ka-j\phi(a))} C^{2s\ell j(ka-j\phi(a))} \\ &\quad B^{4u\ell^2\phi(j)(ka-j\phi(a))} A^{2u\ell^2 j(ka-j\phi(a))},\end{aligned}$$

$[C^{2s\ell\phi(j)\phi(a)-ja}, B^b] = B^{-2s\ell jab} B^{4u\ell^2(\phi(j)\phi(a)b-\phi(1-ja)b)}$, and $[C^k, B^{2s\ell kb}] = B^{4u\ell^2k^2b}$, then

$$\Delta \equiv A^{i+a+2s\ell(j\phi(a)-ka)} B^{j-2s\ell\phi(j)a} C^{2s\ell j(ka-j\phi(a))} B^b C^{2s\ell\phi(j)\phi(a)-ja} B^{2s\ell(kb-jab)} C^{k+c} \mod Z_1(J).$$

As $[C^{2s\ell j(ka-j\phi(a))}, B^b] = B^{4u\ell^2 jb(ka-j\phi(a))}$, $[C^{2s}, B^{2s}] = 1$, $[C^{-ja}, B^{2s\ell(kb-jab)}] = B^{4u\ell^2 jab(ja-k)}$, then

$$\Delta \equiv A^{i+a+2s\ell(j\phi(a)-ka)} B^{j+b+2s\ell(kb-jab-\phi(j)a)} C^{k+c-ja+2s\ell(\phi(j)\phi(a)+j(ka-j\phi(a)))} \mod Z_1(J).$$

Using (5.83) and (5.85) in the exponent of C and collecting the above central elements, we obtain

$$\Delta = A^{i+a+2s\ell(j\phi(a)-ka)} B^{j+b+2s\ell(kb-jab-\phi(j)a)} C^{k+c-ja+2s\ell(jka-\phi(j+1)\phi(a))} \Delta',$$

where

$$\begin{aligned}\Delta' = A^{&4u\ell^2(-\phi(k)a+k^2a+j^2a\phi(a)-jka^2)+2u\ell^2j(ka-j\phi(a))} \\ &B^{4u\ell^2(j\phi(j)a^2-\phi(k+1)b-j\phi(j)\phi(a)+\phi(j)ka+\phi(j)\phi(a)b-\phi(1-ja)b+k^2b-j^2\phi(a)b+j^2a^2b)} \\ &C^{2us\phi(j)a(ka-j\phi(a))+2u\ell^2\phi(j)(ka-j\phi(a))} A^{-\xi_1(a,j)} A^{-\xi_1(2s\ell(j\phi(a)-ka),\, j-2s\ell\phi(j)a)}.\end{aligned}$$

It remains to show that $\Delta' = A^{\xi_2(j,k,a,b)}$. For this purpose, note that

$$\begin{aligned}&\xi_1(2s\ell(j\phi(a)-ka), j-2s\ell\phi(j)a) \\ &\quad = 2u\ell^2\{2\varphi(2s\ell(j\phi(a)-ka)+1)(j-2s\ell\phi(j)a) \\ &\quad + (4s\ell(j\phi(a)-ka)-7)\phi(2s\ell(j\phi(a)-ka))\phi(j-2s\ell\phi(j)a) \\ &\quad - 4s\ell(j\phi(a)-ka)\phi(j-2s\ell\phi(j)a) \\ &\quad - (6s\ell(j\phi(a)-ka)+1)(2s\ell(j\phi(a)-ka))\varphi(j-2s\ell\phi(j)a)\}.\end{aligned}$$

Since $s \mid \varphi(2s\ell(j\phi(a)-ka)+1)$ then

$$\begin{aligned}&\xi_1(2s\ell(j\phi(a)-ka), j-2s\ell\phi(j)a) \\ &\quad \equiv 2u\ell^2(-7)\phi(2s\ell(j\phi(a)-ka))\phi(j-2s\ell\phi(j)a) \\ &\quad \equiv 2us(j\phi(a)-ka)\phi(j-2s\ell\phi(j)a) \mod 4us.\end{aligned}$$

By (5.82) and (5.85), $\phi(j-2s\ell\phi(j)a)=\phi(j)+\phi(2s\ell\phi(j)a+1)-2s\ell j\phi(j)a$, so

$$\begin{aligned}
&\xi_1(2s\ell(j\phi(a)-ka),j-2s\ell\phi(j)a)\\
&\quad\equiv 2us(j\phi(a)-ka)(\phi(j)+\phi(2s\ell\phi(j)a+1))\\
&\quad\equiv 2us(j\phi(a)-ka)\phi(j)+2us(j\phi(a)-ka)\phi(2s\ell\phi(j)a+1))\\
&\quad\equiv 2us(j\phi(a)-ka)\phi(j)+2u^2(j\phi(a)-ka)\phi(j)a \mod 4us.
\end{aligned}$$

Since $C^{2u}=A^{2us}$, then $C^{2us\phi(j)a(j\phi(a)-ka)+2u\phi(j)(j\phi(a)-ka)}A^{-\xi_1(2s\ell(j\phi(a)-ka),j-2s\ell\phi(j)a)}=1$.

Now, if $n\in\mathbb{Z}$, then the use of (5.83) and (5.85) yields $n^2=2\phi(n)+n$.

Also by (5.82), (5.84), and (5.85), $\phi(1-ja)=\phi(-1+ja+1)=\phi(ja)=\phi(j)\phi(a+1)+\phi(j+1)\phi(a)=2\phi(j)\phi(a)+\phi(j)a+j\phi(a)$. By (5.2) Δ' is a power of A whose exponent is

$$\begin{aligned}
&2u\ell^2\{-2\varphi(a+1)j-(2a-7)\phi(a)\phi(j)+2a\phi(j)+(3a+1)a\varphi(j)-2\phi(k)a+2k^2a\\
&\quad+2j^2a\phi(a)-2jka^2+jka-j^2\phi(a)-2j\phi(j)a^2+2\phi(k+1)b+2j\phi(j)\phi(a)\\
&\quad-2\phi(j)ka-2\phi(j)\phi(a)b+2\phi(1-ja)b-2k^2b+2j^2\phi(a)b-2j^2a^2b\}\\
&=2u\ell^2\{-2\varphi(a+1)j-2a\phi(a)\phi(j)+7\phi(a)\phi(j)+2a\phi(j)+(3a+1)a\varphi(j)-2\phi(k)a\\
&\quad+4\phi(k)a+2ka+4\phi(j)a\phi(a)+2ja\phi(a)-4jk\phi(a)-2jka+jka-2\phi(j)\phi(a)\\
&\quad-j\phi(a)-4j\phi(j)\phi(a)-2j\phi(j)a+2\phi(k)b+2kb+2j\phi(j)\phi(a)-2\phi(j)ka\\
&\quad-2\phi(j)\phi(a)b+4\phi(j)\phi(a)b+2\phi(j)ab+2j\phi(a)b-4\phi(k)b-2kb+4\phi(j)\phi(a)b\\
&\quad+2j\phi(a)b-8\phi(j)\phi(a)b-4\phi(j)ab-4j\phi(a)b-2jab\}\\
&=2u\ell^2\{\phi(a)\phi(j)(-2a+7+4a-2-4j+2j-2b+4b+4b-8b)\\
&\quad+\phi(j)a(2-2j-2k+2b-4b)+j\phi(a)(2a-4k+2b+2b-4b-1)\\
&\quad+\phi(k)(-2a+4a+2b-4b)+ka(-2j+j+2)-2j(ab+\varphi(a+1))+(3a+1)a\varphi(j)\}\\
&=2u\ell^2\{\phi(a)\phi(j)(-2j+2a-2b+5)-2\phi(j)a(j+k+b-1)-j\phi(a)(-2a+4k+1)\\
&\quad+2\phi(k)(a-b)-ka(j-2)-2j(ab+\varphi(a+1))+(3a+1)a\varphi(j)\}.
\end{aligned}$$

Thus $\Delta'=A^{\xi_2(j,k,a,b)}$ as stated. □

Proof of Corollary 5.8: A direct application of Theorem 5.7 and the use of (5.82) and (5.85) give

$$\begin{aligned}
B^{-b}A^{-a}&=(A^0B^{-b}C^0)(A^{-a}B^0C^0)\\
&=A^{-a-2s\ell\phi(a+1)b}B^{-b+2s\ell a\phi(b+1)}C^{-ab-2s\ell\phi(a+1)\phi(b)}A^{\xi_2(-b,0,-a,0)},
\end{aligned}$$

so

$$\begin{aligned}(A^aB^bC^c)^{-1} &= C^{-c}B^{-b}A^{-a}\\ &= (A^0B^0C^{-c})(A^{-a-2s\ell\phi(a+1)b}B^{-b+2s\ell a\phi(b+1)}C^{-ab-2s\ell\phi(a+1)\phi(b)})A^{\xi_2(-b,0,-a,0)}\\ &= A^{-a-2s\ell(\phi(a+1)b+ac)-4u\ell^2\phi(a+1)bc}B^{-b+2s\ell(a\phi(b+1)+bc)-4u\ell^2a\phi(b+1)c}C^{-c-ab-2s\ell\phi(a+1)\phi(b)}\\ &\quad A^{\xi_2(-b,0,-a,0)+\xi_2(0,-c,-a-2s\ell\phi(a+1)b,-b+2s\ell a\phi(b+1))}.\end{aligned}$$

□

Proof of Proposition 5.9: By Corollary 5.8,

$$\begin{aligned}(A^iB^jC^k)^{-1} &\equiv A^{-i-2s\ell(\phi(i+1)j+ik)}B^{-j+2s\ell(i\phi(j+1)+jk)}C^{-k-ij-2s\ell\phi(i+1)\phi(j)} \mod Z_1(J),\\ (A^aB^bC^c)^{-1} &\equiv A^{-a-2s\ell(\phi(a+1)b+ac)}B^{-b+2s\ell(a\phi(b+1)+bc)}C^{-c-ab-2s\ell\phi(a+1)\phi(b)} \mod Z_1(J).\end{aligned}$$

It is easy to see that $\phi(n+2sk)\equiv\phi(n) \mod s$ for all $n,k\in\mathbb{Z}$, so Theorem 5.7 and the use of (5.82), (5.83), and (5.85), if necessary, implies,

$$(A^iB^jC^k)^{-1}(A^aB^bC^c)^{-1}\equiv A^{\delta_1}B^{\delta_2}C^{\delta_3} \mod Z_1(J),$$

where

$$\begin{aligned}\delta_1 &\equiv -i-a-2s\ell\{\phi(i+1)j+\phi(a+1)b+j\phi(a+1)+ik+ac+(k+ij)a\} \mod 2u,\\ \delta_2 &\equiv -j-b+2s\ell\{i\phi(j+1)+a\phi(b+1)+\phi(j+1)a+jk+bc+(k+ij)b+jab\} \mod 2u,\\ \delta_3 &\equiv -k-c-ij-ab-ja-2s\ell\{j\phi(a+1)b+jac-i\phi(j+1)a+\phi(i+1)\phi(j)\\ &\qquad +\phi(a+1)\phi(b)+ij^2a+\phi(j)\phi(a+1)\}\\ &\equiv -k-c-ij-ab-ja-2s\ell\{j\phi(a+1)b+i\phi(j)a+\phi(i+1)\phi(j)+\phi(a+1)\phi(b)\\ &\qquad +\phi(j)\phi(a+1)+jac\} \mod 2u,\end{aligned}$$

and

$$\begin{aligned}&(A^iB^jC^k)(A^aB^bC^c)\\ &\quad\equiv A^{i+a+2s\ell(j\phi(a)-ka)}B^{j+b+2s\ell(kb-jab-\phi(j)a)}C^{k+c-ja+2s\ell(jka-\phi(j+1)\phi(a))} \mod Z_1(J).\end{aligned}$$

Then, applying Theorem 5.7, and using (5.82), (5.83), and (5.85), shows that

$$\begin{aligned}[A^iB^jC^k,A^aB^bC^c] &= (A^iB^jC^k)^{-1}(A^aB^bC^c)^{-1}(A^iB^jC^k)(A^aB^bC^c)\\ &\equiv A^{\exp A}B^{\exp B}C^{\exp C} \mod Z_1(J),\end{aligned}$$

where

$$\begin{aligned}
\exp A &\equiv 2s\ell\{j\phi(a) - 2ka - \phi(i+1)j - \phi(a+1)b - j\phi(a+1) - ik - ac - ija \\
&\qquad - (j+b)\phi(i+a) + (k+c+ij+ab+ja)(i+a)\} \\
&\equiv 2s\ell\{j\phi(a) - \phi(i)b + ic - ka\} \mod 2u, \\
\exp B &\equiv 2s\ell\{kb - jab - \phi(j)a + i\phi(j+1) + a\phi(b+1) + \phi(j+1)a + jk + bc + (k+ij)b \\
&\qquad + jab - (k+c+ij+ab+ja)(j+b) + (j+b)^2(i+a) - \phi(j+b+1)(i+a)\} \\
&\equiv 2s\ell\{i\phi(b) - \phi(j)a + kb + j(ib - ab - c)\} \mod 2u, \\
\exp C &\equiv \delta_3 + k + c - ja + 2s\ell(jka - \phi(j+1)\phi(a)) - \delta_2(i + a + 2s\ell(j\phi(a) - ka)) \\
&\qquad + 2s\ell\{(j+b)(i+a)(k+c+ij+ab+ja) - \phi(j+b)\phi(i+a)\} \\
&\equiv ib - ja + 2s\ell\{\phi(a)(\phi(j) + jb) - \phi(i)(\phi(b) + jb) + ijc - kab\} \mod 2u. \qquad \square
\end{aligned}$$

Lemma 5.94. *Let $a \in \mathbb{Z}$ and $t \in \mathbb{N}$. Then*

$\sum_{k=0}^{t} k = \frac{t(t+1)}{2} = \phi(t+1)$,
$\sum_{k=0}^{t} k^2 = \frac{t(t+1)(2t+1)}{6} = 2\varphi(t+1) + \phi(t+1)$,
$\sum_{k=0}^{t} k^3 = (\frac{t(t+1)}{2})^2 = \phi(t+1)^2$,
$\sum_{k=0}^{t} \phi(ak) = \sum_{k=0}^{t} \frac{ak(ak-1)}{2} = a^2\varphi(t+1) + \phi(a)\phi(t+1)$,
$\sum_{k=0}^{t} \phi(ak)k = \sum_{k=0}^{t} \frac{ak^2(ak-1)}{2} = \frac{a\phi(t+1)(a\phi(t+1)-1)}{2} - a\varphi(t+1)$,
$\sum_{k=0}^{t} \varphi(ak+1) = \sum_{k=0}^{t} \frac{(ak+1)(ak)(ak-1)}{6} = \frac{a\phi(t+1)(a^2\phi(t+1)-1)}{6}$,
$\sum_{k=0}^{t} \varphi(k) = \sum_{k=0}^{t} \frac{k(k-1)(k-2)}{6} = \frac{\phi(t+1)(\phi(t+1)-1)}{6} - \varphi(t+1)$,
$\sum_{k=0}^{t} \varphi(k)k = \sum_{k=0}^{t} \frac{k^2(k-1)(k-2)}{6} = \frac{1}{6}\left(\frac{t(t+1)(6t^3+9t^2+t-1)}{30} - 3\phi(t+1)^2 + 4\varphi(t+1) + 2\phi(t+1)\right)$.

Proof. In each case use of the distributive law in the sum's general term, properties of finite sums, and the definitions of ϕ and φ give the desired results. $\square$

Proof of Theorem 5.10: Fix $a, b, c \in \mathbb{Z}$. Suppose that $n \geq 2$, let $k, t \in \mathbb{N}$, and set $\Delta = (A^a B^b C^c)^n$. Let us first work with Δ modulo $Z_1(J)$. By definition,

$$\begin{aligned}
\Delta &= (A^a B^b C^c)(A^a B^b C^c) \cdots (A^a B^b C^c)(A^a B^b C^c)(A^a B^b C^c) \\
&= A^{na}(B^b C^c)^{A^{(n-1)a}}(B^b C^c)^{A^{(n-2)a}} \cdots (B^b C^c)^{A^{2a}}(B^b C^c)^{A^a}(B^b C^c).
\end{aligned}$$

As

$$\begin{aligned}
[B^b, A^{ka}] &= [A^{ka}, B^b]^{-1} \\
&= (A^{-2s\ell b\phi(ak)} B^{2s\ell a\phi(b)k} C^{abk - 2s\ell\phi(b)\phi(ak)} A^{\xi_1(ak,b)})^{-1} \\
&= C^{2s\ell\phi(b)\phi(ak) - abk} B^{-2s\ell a\phi(b)k} A^{2s\ell b\phi(ak)} A^{-\xi_1(ak,b)}
\end{aligned}$$

and $[C^c, A^{ka}] = A^{-2s\ell ack-4u\ell^2 a\phi(c)k}$, we infer

$$\Delta \equiv A^{na}(B^bC^{2s\ell\phi(b)\phi((n-1)a)-ab(n-1)}B^{-2s\ell a\phi(b)(n-1)}A^{2s\ell b\phi((n-1)a)}C^cA^{-2s\ell ac(n-1)})\cdots$$
$$(B^bC^{2s\ell\phi(b)\phi((1)a)-ab(1)}B^{-2s\ell a\phi(b)(1)}A^{2s\ell b\phi((1)a)}C^cA^{-2s\ell ac(1)})(B^bC^c).$$

Since $[C^{2s\ell\phi(b)\phi(ka)-abk}, B^{-2s\ell a\phi(b)k}] = B^{4u\ell^2a^2\phi(b)bk^2}$ and $[A^{2s\ell b\phi(ka)}, C^c] = A^{4u\ell^2bc\phi(ka)}$, then

$$\Delta \equiv A^{na}(B^{b-2s\ell a\phi(b)(n-1)}C^{2s\ell\phi(b)\phi((n-1)a)-ab(n-1)+c}A^{2s\ell(b\phi((n-1)a)-ac(n-1))})\cdots$$
$$(B^{b-2s\ell a\phi(b)(1)}C^{2s\ell\phi(b)\phi((1)a)-ab(1)+c}A^{2s\ell(b\phi((1)a)-ac(1))})(B^bC^c).$$

Set $g_1(t) = \sum_{k=0}^{t}(b\phi(ka) - ack)$. By Lemma 5.94, $g_1(t) = a^2b\varphi(t+1) + (\phi(a)b - ac)\phi(t+1)$. Then

$$\Delta \equiv A^{na}A^{2s\ell g_1(n-1)}(B^{b-2s\ell a\phi(b)(n-1)}C^{2s\ell\phi(b)\phi((n-1)a)-ab(n-1)+c})^{A^{2s\ell g_1(n-1)}}\cdots$$
$$(B^{b-2s\ell a\phi(b)(1)}C^{2s\ell\phi(b)\phi((1)a)-ab(1)+c})^{A^{2s\ell g_1(1)}}(B^bC^c).$$

As

$$\begin{aligned}
&[B^{b-2s\ell a\phi(b)k}, A^{2s\ell g_1(k)}]\\
&\quad= [A^{2s\ell g_1(k)}, B^{b-2s\ell a\phi(b)k}]^{-1}\\
&\quad= (A^{2u\ell^2bg_1(k)}B^{4u\ell^2\phi(b)g_1(k)}C^{2s\ell bg_1(k)+2u\ell^2\phi(b)g_1(k)+2us\ell^3a\phi(b)g_1(k)k}A^{\xi_1(2s\ell g_1(k),b-2s\ell a\phi(b)k)})^{-1}\\
&\quad= C^{-2s\ell bg_1(k)}A^{-2u\ell^2bg_1(k)}B^{-4u\ell^2\phi(b)g_1(k)}C^{-2u\ell^2\phi(b)g_1(k)-2us\ell^3a\phi(b)g_1(k)k}A^{-\xi_1(2s\ell g_1(k),b-2s\ell a\phi(b)k)}
\end{aligned}$$

and $[C^{2s\ell\phi(b)\phi(ka)-abk+c}, A^{2s\ell g_1(k)}] = A^{-4u\ell^2g_1(k)(-abk+c)}$, we deduce

$$\Delta \equiv A^{na+2s\ell g_1(n-1)}(B^{b-2s\ell a\phi(b)(n-1)}C^{-2s\ell bg_1(n-1)+2s\ell\phi(b)\phi((n-1)a)-ab(n-1)+c})\cdots$$
$$(B^{b-2s\ell a\phi(b)(2)}C^{-2s\ell bg_1(2)+2s\ell\phi(b)\phi((2)a)-ab(2)+c})(B^{b-2s\ell a\phi(b)(1)}C^{-2s\ell bg_1(1)+2s\ell\phi(b)\phi((1)a)-ab(1)+c})$$
$$(B^bC^c).$$

Set $g_2(t) = \sum_{k=0}^{t}(b - 2s\ell a\phi(b)k)$ and $g_3(t) = 2s\ell\{\phi(b)\phi(ta) - bg_1(t)\} - abt + c$. By Lemma 5.94, $g_2(t) = b(t+1) - 2s\ell a\phi(b)\phi(t+1)$. Therefore

$$\Delta \equiv A^{na+2s\ell g_1(n-1)}B^{g_2(n-1)}(C^{g_3(n-1)})^{B^{g_2(n-2)}}\cdots(C^{g_3(2)})^{B^{g_2(1)}}(C^{g_3(1)})^{B^{g_2(0)}}(C^{g_3(0)}).$$

As $[C^{g_3(k)}, B^{g_2(k-1)}] = B^{2s\ell(bck-ab^2k^2)}B^{4u\ell^2(\phi(b)b\phi(ka)k-b^2g_1(k)k+a^2\phi(b)b\phi(k)k-a\phi(b)c\phi(k)-b\phi(-abk+c+1)k)}$, we deduce

$$\Delta \equiv A^{na+2s\ell g_1(n-1)}B^{g_2(n-1)}(C^{g_3(n-1)}B^{2s\ell(bc(n-1)-ab^2(n-1)^2)})\cdots(C^{g_3(2)}B^{2s\ell(bc(2)-ab^2 2^2)})$$
$$(C^{g_3(1)}B^{2s\ell(bc(1)-ab^2 1^2)})(C^{g_3(0)}).$$

Set $g_4(t)=\sum_{k=0}^{t}(bck-ab^2k^2)$. By Lemma 5.94, $g_4(t)=b(c-ab)\phi(t+1)-2ab^2\varphi(t+1)$. As $[C^{g_3(k)},B^{2s\ell g_4(k)}]=B^{4u\ell^2 g_4(k)(-abk+c)}$, then

$$\begin{aligned}\Delta &\equiv A^{na+2s\ell g_1(n-1)}B^{g_2(n-1)+2s\ell g_4(n-1)}(C^{g_3(n-1)})^{B^{2s\ell g_4(n-1)}}\cdots(C^{g_3(2)})^{B^{2s\ell g_4(2)}}(C^{g_3(1)})^{B^{2s\ell g_4(1)}}(C^{g_3(0)})\\ &\equiv A^{na+2s\ell g_1(n-1)}B^{g_2(n-1)+2s\ell g_4(n-1)}C^{g_5(n-1)} \mod Z_1(J),\end{aligned}$$

where $g_5(n-1)=\sum_{k=0}^{n-1}g_3(k)$. As $g_3(k)=2s\ell\{\phi(b)\phi(ak)-a^2b^2\varphi(k+1)-(\phi(a)b-ac)b\phi(k+1)\}-abk+c$, then Lemma 5.94 produces

$$g_5(n-1)=2s\ell\{a^2\phi(b)\varphi(n)+\phi(a)\phi(b)\phi(n)-a^2b^2\sigma_2(1,n)-(\phi(a)b-ac)b\varphi(n+1)\}-ab\phi(n)+cn.$$

Thus

$$\Delta=A^{na+2s\ell g_1(n-1)}B^{g_2(n-1)+2s\ell g_4(n-1)}C^{g_5(n-1)}A^{\xi_4},$$

were A^{ξ_4} is the central element obtained by gathering all the above central commutators, i.e,

$$\begin{aligned}&A^{\xi_4}=\\ &A^{4u\ell^2\sum_{k=0}^{n-1}\{bc\phi(ka)-a\phi(c)k-g_1(k)(-abk+c)\}-2u\ell^2\sum_{k=0}^{n-1}bg_1(k)-\sum_{k=0}^{n-1}\{\xi_1(ka,b)+\xi_1(2s\ell g_1(k),b-2s\ell a\phi(b)k)\}}\\ &B^{4u\ell^2\sum_{k=0}^{n-1}\{a^2\phi(b)bk^2-\phi(b)g_1(k)+\phi(b)b\phi(ka)k-b^2g_1(k)k+a^2\phi(b)b\phi(k)k-a\phi(b)c\phi(k)-b\phi(-abk+c+1)k+g_4(k)(-abk+c)\}}\\ &C^{\sum_{k=0}^{n-1}\{-2u\ell^2\phi(b)g_1(k)-2us\ell^3a\phi(b)g_1(k)k\}}.\end{aligned}$$

Using properties of ϕ and φ, and applying Lemma 5.94, gives
$\xi_1(2s\ell g_1(k),b-2s\ell a\phi(b)k)\equiv 2us\phi(b)g_1(k)+2u^2a\phi(b)g_1(k)k \mod 4us$,
$\xi_1(ak,b)=4u\ell^2\{b\varphi(ak+1)+a\phi(b)\phi(ak)k-a\phi(b)k\}-2u\ell^2\{7\phi(b)\phi(ak)+3a^2\varphi(b)k^2+a\varphi(b)k\}$.
Using the above and $A^{2u}B^{2u}=1$, $A^{2us}=C^{2u}$, produces

$$\begin{aligned}\xi_4=2u\ell^2\sum_{k=0}^{n-1}\{&a(\varphi(b)+2\phi(b)-2\phi(c))k+a^2(3\varphi(b)-2b\phi(b))k^2+2a\phi(b)c\phi(k)\\ &-2a^2b\phi(b)\phi(k)k+(2bc+7\phi(b))\phi(ak)-2\phi(b)(a+b)\phi(ak)k-2b\varphi(ak+1)\\ &+2b\phi(-abk+c+1)k+(2\phi(b)-2c-b)g_1(k)+2b(a+b)g_1(k)k-2cg_4(k)\\ &+2abg_4(k)k\}.\end{aligned}$$

Appealing to Lemma 5.94 again, it is easy to see that
$\sum_{k=0}^{t}g_1(k)=a^2b\sigma_2(1,t+1)+(\phi(a)b-ac)\varphi(t+2)$,
$\sum_{k=0}^{t}g_1(k)k=a^2b(\sigma_3(t+1)+\sigma_1(1,t+1)-\varphi(t+1))+(\phi(a)b-ac)(\sigma_1(1,t+1)+\varphi(t+2))$,
$\sum_{k=0}^{t}g_4(k)=b(c-ab)\varphi(t+2)-2ab^2\sigma_2(1,t+1)$,

$\sum_{k=0}^{t} g_4(k)k = b(c-ab)(\sigma_1(1,t+1)+\varphi(t+2)) - 2ab^2(\sigma_3(t+1)+\sigma_1(1,t+1)-\varphi(t+1))$,
$\sum_{k=0}^{t} \phi(-abk+c+1)k = \sigma_1(ab,t+1) + (\phi(c+1)-abc)\phi(t+1) - ab(2c+1)\varphi(t+1)$.

Thus

$$\begin{aligned}\xi_4 = 2u\ell^2\{&a(\varphi(b)+2\phi(b)-2\phi(c))\phi(n) + a^2(3\varphi(b)-2b\phi(b))(2\varphi(n)+\phi(n)) + 2a\phi(b)c\varphi(n)\\
&- 2a^2b\phi(b)(\sigma_1(1,n)-\varphi(n)) + (2bc+7\phi(b))(a^2\varphi(n)+\phi(a)\phi(n))\\
&- 2\phi(b)(a+b)(\sigma_1(a,n)-a\varphi(n)) - 2b\sigma_2(a,n)\\
&+ (2\phi(b)-2c-b)(a^2b\sigma_2(1,n)+(\phi(a)b-ac)\varphi(n+1))\\
&+ 2b(a(\phi(a)b-ac)+b^2(\phi(a)-a^2))(\sigma_1(1,n)+\varphi(n+1))\\
&+ 2a^2b^2(a-b)(\sigma_3(n)+\sigma_1(1,n)-\varphi(n))\\
&- 2c((c-ab)b\varphi(n+1)-2ab^2\sigma_2(1,n))\\
&+ 2b(\sigma_1(ab,n)+(\phi(c+1)-abc)\phi(n)-ab(2c+1)\varphi(n))\}.\end{aligned}$$

This completes the proof for the case $n \geq 2$. We readily see that the result is valid when $n \in \{0,1\}$. Now, if $n < 0$, as the exponent of J is $4us$ in the case $m > 1$ and 8 in the case $m = 1$, and letting $q \in \mathbb{N}$ be such that $n + 30 \cdot 6 \cdot 4usq > 0$, we have that $(A^aB^bC^c)^n = (A^aB^bC^c)^{n+30\cdot 6\cdot 4usq}$. Then from (5.80), (5.81), the fact that $\sigma_3(n+30\cdot 6\cdot 4usq) \equiv \sigma_3(n) \mod 4us$, and the above, it follows that the result is also valid for $n < 0$. □

Chapter 6

On the isomorphism problem for the Sylow 2-subgroup of G

Let $\alpha = 1 + 2^m\ell$ and $\alpha' = 1 + 2^m\ell'$ with ℓ and ℓ' odd integers and $m \geq 1$. By (5.1),

$$J(\alpha) = \langle\, A, B \mid A^{[A,B]} = A^{\alpha},\ B^{[B,A]} = B^{\alpha},\ A^{2^{3m-1}} = 1 = B^{2^{3m-1}} \,\rangle$$

and

$$J(\alpha') = \langle\, X, Y \mid X^{[X,Y]} = X^{\alpha'},\ Y^{[Y,X]} = Y^{\alpha'},\ X^{2^{3m-1}} = 1 = Y^{2^{3m-1}} \,\rangle.$$

By Theorem 4.13, $|J(\alpha)| = 2^{7m-3} = |J(\alpha')|$, so the following isomorphism problem arises: When are $J(\alpha)$ and $J(\alpha')$ isomorphic?

In this chapter we find necessary and sufficient conditions for the existence of such an isomorphism.

Set $C = [A, B]$ and let θ be the automorphism of $J(\alpha')$ given by $X \leftrightarrow Y$.

6.1 Sufficiency

Theorem 6.1. *Suppose that* $\ell' \equiv \ell \mod 2^m$, *that is,* $\alpha' \equiv \alpha \mod 2^{2m}$. *Then* $J(\alpha') \cong J(\alpha)$.

Proof. We have $\ell' = \ell + r2^m$ for some $r \in \mathbb{Z}$, so that $\alpha' = \alpha + r2^{2m}$. Let $f = 1 + k2^m$, with $k \in \mathbb{N}$. Then $\alpha^{k2^m} \equiv 1 + k\ell 2^{2m} \mod 2^{3m-1}$, so $\alpha^f \equiv \alpha + k\ell 2^{2m} \mod 2^{3m-1}$. As ℓ is odd, we can find k such that $k\ell \equiv r \mod 2^{m-1}$, whence $\alpha' \equiv \alpha^f \mod 2^{3m-1}$.

We claim that the assignment

$$X \mapsto A,\ Y \mapsto B^f,$$

extends to an isomorphism $J(\alpha') \to J(\alpha)$. We must verify that

$$A^{[A,B^f]} = A^{\alpha'} = A^{\alpha^f} = A^{C^f}, \ B^{[B^f,A]} = B^{\alpha'} = B^{\alpha^f} = B^{C^{-f}}.$$

By Proposition 4.15, we have $C_J(A) = \langle A \rangle$ and $C_J(B) = \langle B \rangle$, so the above conditions become

$$[A, B^f]C^{-f} \in \langle A \rangle, \ [B^f, A]C^f \in \langle B \rangle.$$

From $A^C = A^\alpha$ and $B^{C^{-1}} = B^\alpha$ we readily see that

$$[A, B^f] = B^{(\alpha-1)(\alpha+2\alpha^2+\cdots+(f-1)\alpha^{f-1})}C^f.$$

Thus $[B^f, A]C^f \in \langle B \rangle$ is equivalent to $C^{-f}B^{-(\alpha-1)(\alpha+2\alpha^2+\cdots+(f-1)\alpha^{f-1})}C^f \in \langle B \rangle$, which is automatically true since C normalizes $\langle B \rangle$, while $[A, B^f]C^{-f} \in \langle A \rangle$ is equivalent to

$$B^{(\alpha-1)(\alpha+2\alpha^2+\cdots+(f-1)\alpha^{f-1})} \in \langle A \rangle. \tag{6.2}$$

We are reduced to verify (6.2). In this case, from (5.2), we have the fundamental relation $A^{2^{2m-1}}B^{2^{2m-1}} = 1$. In particular, $B^{2^{2m-1}} \in \langle A \rangle$. In fact, Proposition 4.14 ensures that $\langle A \rangle \cap \langle B \rangle = \langle B^{2^{2m-1}} \rangle$. Thus, (6.2) is actually equivalent to

$$\alpha + 2\alpha^2 + \cdots + (f-1)\alpha^{f-1} \equiv 0 \mod 2^{m-1}. \tag{6.3}$$

Here $\alpha \equiv 1 \mod 2^m$, so (6.3) translates into $(f-1)f/2 \equiv 1+2+\cdots+(f-1) \equiv 0 \mod 2^{m-1}$, which is certainly true since $f \equiv 1 \mod 2^m$. □

6.2 Searching for isomorphisms

Let G_1 and G_2 be groups with characteristic subgroups N_1 and N_2, respectively, and write $L_1 = G_1/N_1$ and $L_2 = G_2/N_2$, with canonical projections $\pi_1 : G_1 \to L_1$ and $\pi_2 : G_2 \to L_2$.

As N_1 is a characteristic subgroup of G_1, we have a homomorphism $\Lambda : \mathrm{Aut}(G_1) \to \mathrm{Aut}(L_1)$ such that for all $\beta \in \mathrm{Aut}(G_1)$, β^Λ is the only automorphism of L_1 satisfying $\pi_1\beta^\Lambda = \beta\pi_1$.

Likewise, to every isomorphism $\Omega : G_1 \to G_2$ such that $N_1^\Omega = N_2$ there corresponds a unique isomorphism $\Omega^* : L_1 \to L_2$ satisfying $\pi_1\Omega^* = \Omega\pi_2$. Note that

$$(\beta\Omega)^* = \beta^\Lambda\Omega^*, \quad \beta \in \mathrm{Aut}(G_1), \tag{6.4}$$

as $\beta^\Lambda\Omega^* : L_1 \to L_2$ is an isomorphism and $\pi_1\beta^\Lambda\Omega^* = \beta\pi_1\Omega^* = \beta\Omega\pi_2 = \pi_1(\beta\Omega)^*$.

We say that an isomorphism $\delta : L_1 \to L_2$ lifts if there is an isomorphism $\Omega : G_1 \to G_2$ such that $N_1^\Omega = N_2$ and $\Omega^* = \delta$.

Proposition 6.5. *Let $\gamma : L_1 \to L_2$ be an isomorphism and U a subset of $\mathrm{Aut}(L_1)$ such that $\mathrm{Aut}(L_1) = \mathrm{Aut}(G_1)^\Lambda U$. Then, there is an isomorphism $\Omega : G_1 \to G_2$ such that $N_1^\Omega = N_2$ if and only if there is some $u \in U$ such that $u\gamma$ lifts.*

Proof. Sufficiency is clear. As for necessity, $\Omega^*\gamma^{-1} \in \mathrm{Aut}(L_1)$, so $\Omega^* = \beta^\Lambda u\gamma$ for some $\beta \in \mathrm{Aut}(G_1)$ and $u \in U$. It then follows from (6.4) that $(\beta^{-1}\Omega)^* = u\gamma$. □

Proposition 6.6. *Let $\gamma : L_1 \to L_2$ be an isomorphism, U a subset of $\mathrm{Aut}(L_1)$ such that $\mathrm{Aut}(L_1) = \mathrm{Aut}(G_1)^\Lambda U$, and E a generating subset of G_1. For $e \in E$ and $u \in U$, let $h_{e,u}$ be any element of G_2 satisfying $e\pi_1 u\gamma = h_{e,u}\pi_2$. Suppose that given any $(f_e)_{e\in E}$, with $f_e \in N_1$, there exists $\beta \in \mathrm{Aut}(G_1)$ such that $e^\beta = ef_e$ for all $e \in E$. Then, there is an isomorphism $\Omega : G_1 \to G_2$ such that $N_1^\Omega = N_2$ if and only if there is some $u \in U$ such that the assignment*

$$e \mapsto h_{e,u}, \quad e \in E,$$

extends to an isomorphism $\Delta : G_1 \to G_2$ satisfying $N_1^\Delta = N_2$.

Proof. Sufficiency is clear. As for necessity, by Proposition 6.5, there is some $u \in U$ and an isomorphism $\Delta : G_1 \to G_2$ such that $N_1^\Delta = N_2$ and $\Delta^* = u\gamma$. Then

$$h_{e,u}\pi_2 = e\pi_1 u\gamma = e\Delta\pi_2, \quad e \in E,$$

so there exist $(k_e)_{e\in E}$, with $k_e \in N_2$, such that $h_{e,u}k_e = e\Delta$ for all $e \in E$. Since $N_1^\Delta = N_2$, there exist $(f_e)_{e\in E}$, with $f_e \in N_1$, such that $f_e^\Delta = k_e^{-1}$ for all $e \in E$. By assumption, there exists $\beta \in \mathrm{Aut}(G_1)$ such that $e^\beta = ef_e$. Then $e^{\beta\Delta} = h_{e,u}$ for all $e \in E$. □

The above will be applied when N_1 and N_2 are the centers of G_1 and G_2, respectively, in which case N_1 and N_2 are characteristic subgroups of G_1 and G_2, and any isomorphism $\Omega : G_1 \to G_2$ satisfies $N_1^\Omega = N_2$.

6.3 Necessity for $J(\alpha)$ Part I

We assume in this section that $m > 1$.

As seen in (5.37),

$$H(\alpha) = \langle\, A_0, B_0 \mid A_0^{[A_0,B_0]} = A_0^\alpha,\ B_0^{[B_0,A_0]} = B_0^\alpha,\ A_0^{2^{2m-1}} = 1 = B_0^{2^{2m-1}} \,\rangle,$$

and

$$H(\alpha') = \langle\, X_0, Y_0 \mid X_0^{[X_0,Y_0]} = X_0^{\alpha'},\ Y_0^{[Y_0,X_0]} = Y_0^{\alpha'},\ X_0^{2^{2m-1}} = 1 = Y_0^{2^{2m-1}} \,\rangle.$$

Let ν be the automorphism of $H(\alpha')$ given by $X_0 \leftrightarrow Y_0$.

We set $s = 2^{m-1}$, $u = s^2$, and $r = s/2$. Under this notation we have the following results:

Proposition 6.7. *The terms of the upper central series of $J(\alpha)$ are:*

$$Z_1(J(\alpha)) = \langle A^{2u} \rangle,\ Z_2(J(\alpha)) = \langle A^{2u}, C^s \rangle,\ Z_3(J(\alpha)) = \langle A^{2s}, B^{2s}, C^s \rangle,$$

$$Z_4(J(\alpha)) = \langle A^s, B^s, C \rangle,\ Z_5(J(\alpha)) = J(\alpha)$$

with $Z_3(J(\alpha))$ abelian.

Proof. See Theorem 4.16 and Proposition 4.20. □

Proposition 6.8. *For every $x, y \in Z_2(H(\alpha'))$ the assignment $X_0 \mapsto X_0 x,\ Y_0 \mapsto Y_0 y$ extends to an automorphism $\Pi_{(x,y)}$ of $H(\alpha')$.*

Proof. See Proposition 5.43. □

Proposition 6.9. *The assignment $X_0 \mapsto X_0^{1+s},\ Y_0 \mapsto Y_0 X_0^s$ extends to an automorphism Γ of $H(\alpha')$ that belongs to $\mathrm{Aut}_3(H(\alpha'))$.*

Proof. See Proposition 5.46. □

Proposition 6.10. *For every $z_1, z_2 \in Z_2(J(\alpha'))$ the assignment $X \mapsto X z_1,\ Y \mapsto Y z_2$ extends to an automorphism of $J(\alpha')$.*

Proof. See Proposition 5.62. □

Consider the projection homomorphisms $\pi_\alpha : J(\alpha) \to H(\alpha)$, given by $A \mapsto A_0$ and $B \mapsto B_0$, and $\pi_{\alpha'} : J(\alpha') \to H(\alpha')$, given by $X \mapsto X_0$ and $Y \mapsto Y_0$.

We have the natural homomorphism $\Lambda : \mathrm{Aut}(J(\alpha')) \to \mathrm{Aut}(H(\alpha'))$ such that $\pi_{\alpha'} \beta^\Lambda = \beta \pi_{\alpha'}$ for all $\beta \in \mathrm{Aut}(J(\alpha'))$.

Lemma 6.11. *Let G be a group with a characteristic subgroup N and let $\mathrm{Aut}_N(G)$ be the kernel of $\mathrm{Aut}(G) \to \mathrm{Aut}(G/N)$. Given a generating subset T of G, suppose that $f, g \in \mathrm{Aut}(G)$ satisfy $t^f \equiv t^g \mod N$ for all $t \in T$. Then $f \equiv g \mod \mathrm{Aut}_N(G)$.*

Proof. Since N is a characteristic subgroup of G, from $t^f \equiv t^g \mod N$ for all $t \in T$, we deduce $t^{fg^{-1}} \equiv t \mod N$ for all $t \in T$, which implies $fg^{-1} \in \mathrm{Aut}_N(G)$. □

Theorem 6.12. *Set $V = \{\Pi_{(x,y)} \mid x, y \in \langle X_0^{2s}, Y_0^{2s} \rangle\}$ where $\Pi_{(x,y)}$ is like in Proposition 6.8 and set $U = V\{1, \Gamma\}$. Then $H(\alpha') = J(\alpha')^\Lambda U$.*

Proof. Set $J = J(\alpha')$ and $H = H(\alpha')$. Note that $\theta^\Lambda = \nu$.

We claim that if $m = 2$ then

$$\mathrm{Aut}(H) = \langle\theta\rangle^\Lambda \mathrm{Aut}_3(H), \tag{6.13}$$

while if $m > 2$ then

$$\mathrm{Aut}(H) = \langle\Sigma_1, \theta\rangle^\Lambda \mathrm{Aut}_3(H), \tag{6.14}$$

where $\Sigma_1 \in \mathrm{Aut}(J)$ is given by $X \mapsto X^{1+r}Y^rX^{s(sk+r\ell-2)}$, $Y \mapsto Y^{1+r}X^r$, where k is even if $m > 3$ and odd if $m = 3$, according to Proposition 5.76. Indeed, if $m = 2$, we have $\mathrm{Aut}(H) = \langle\nu\rangle\mathrm{Aut}_3(H)$ by Theorem 5.59, and the claim follows in this case. Suppose $m > 2$. Then Theorem 5.59 ensures that $\mathrm{Aut}(H) = \langle\Sigma, \nu\rangle\mathrm{Aut}_3(H)$, where Σ is defined in Corollary 5.57 by $X_0 \mapsto X_0^{1+r}Y_0^r$, $Y_0 \mapsto Y_0^{1+r}X_0^r$. Since $X_0^s \in Z_3(H)$ by Proposition 6.7, it follows from Lemma 6.11 that $\Sigma_1^\Lambda \equiv \Sigma \mod \mathrm{Aut}_3(H)$, which proves the claim in this case.

Let $\Gamma \in \mathrm{Aut}_3(H)$ be as defined in Proposition 6.9, and let $\Gamma_1 \in \mathrm{Aut}_4(J)$ be as defined in Proposition 5.73 by $X \mapsto X^{1+s}Y^s$, $Y \mapsto Y^{1+s(2\delta_{2,m}+s-3)}X^s$, where $\delta_{i,j}$ is the Kronecker delta function. By Theorem 5.48, we have

$$\langle\overline{\Gamma}, \overline{\Gamma^\nu}\rangle = \mathrm{Aut}_3(H)/\mathrm{Inn}(H)\mathrm{Aut}_2(H) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}),$$

which implies

$$\mathrm{Aut}_3(H) = \mathrm{Inn}(H)\mathrm{Aut}_2(H)\langle\Gamma, \Gamma^\nu\rangle = \mathrm{Inn}(H)\mathrm{Aut}_2(H)\{1, \Gamma\Gamma^\nu\}\{1, \Gamma\}.$$

Set $Z = [X, Y]$. Then $X^Y = XZ$ and $Y^X = YZ^{-1}$, with $Z \in Z_4(J)$ by Proposition 6.7. Thus, $\mathrm{Inn}(J) \subseteq \mathrm{Aut}_4(J)$ and $\mathrm{Inn}(H) \subseteq \mathrm{Aut}_3(H)$, so, by Proposition 5.47, Λ induces an imbedding

$$\overline{\Lambda} : \mathrm{Aut}_4(J)/\mathrm{Inn}(J)\mathrm{Aut}_3(J) \to \mathrm{Aut}_3(H)/\mathrm{Inn}(H)\mathrm{Aut}_2(H).$$

In this regard, the proof of Theorem 5.77 shows that $\overline{\mathrm{Aut}_4(J)} = \langle\overline{\Gamma_1}\rangle$ has order 2 and that $\overline{\Gamma_1}^{\overline{\Lambda}} \neq \overline{\Gamma}$, this is, $\Gamma_1^\Lambda \not\equiv \Gamma \mod \mathrm{Inn}(H)\mathrm{Aut}_2(H)$. But then $(\Gamma_1^\theta)^\Lambda \equiv (\Gamma_1^\Lambda)^\nu \not\equiv \Gamma^\nu \mod \mathrm{Inn}(H)\mathrm{Aut}_2(H)$, this is, $\overline{\Gamma_1}^{\overline{\Lambda}} \neq \overline{\Gamma^\nu}$. This forces $\overline{\Gamma_1}^{\overline{\Lambda}} = \overline{\Gamma\Gamma^\nu}$, this is, $\Gamma_1^\Lambda \equiv \Gamma\Gamma^\nu \mod \mathrm{Inn}(H)\mathrm{Aut}_2(H)$. Therefore,

$$\mathrm{Aut}_3(H) = \{1, \Gamma_1\}^\Lambda \mathrm{Inn}(H)\mathrm{Aut}_2(H)\{1, \Gamma\}. \tag{6.15}$$

It follows from Proposition 6.7 that $Z_2(H) = \langle X_0^{2s}, Y_0^{2s}, [X_0, Y_0]^s\rangle$ and $Z_1(H) = \langle[X_0, Y_0]^s\rangle$. We deduce from Proposition 5.43 that

$$\mathrm{Aut}_2(H) = \mathrm{Aut}_1(H)V. \tag{6.16}$$

Here

$$\mathrm{Aut}_1(H) = \mathrm{Aut}_2(J)^\Lambda \tag{6.17}$$

by Proposition 5.62. On other hand, it is clear that

$$\mathrm{Inn}(H) = \mathrm{Inn}(J)^\Lambda. \tag{6.18}$$

Combining (6.13)-(6.18) proves that $\mathrm{Aut}(H) = \mathrm{Aut}(J)^\Lambda U$. □

The fundamental relations $A^{2u}B^{2u} = 1$ and $A^{2us} = C^{2u} = B^{2us}$, shown in (5.2), will be used without comment, as well as $Z_1(J(\alpha)) = \langle A^{2u}\rangle$, as indicated in Proposition 6.7.

Theorem 6.19. *Suppose that $\alpha' \equiv \alpha \mod 2^{2m-1}$ but $\alpha' \not\equiv \alpha \mod 2^{2m}$. Then $J(\alpha') \cong J(\alpha)$ if and only if $m = 2$. In particular, $J(1+4\ell) \cong J(5)$ for all $\ell \in \mathbb{Z}$ odd.*

Proof. As $\alpha' \equiv \alpha \mod 2^{2m-1}$, it is clear that the assignment $X_0 \mapsto A_0$ and $Y_0 \mapsto B_0$ extends to an isomorphism $\gamma : H(\alpha') \to H(\alpha)$. We next apply Proposition 6.6 with $G_1 = J(\alpha')$, $G_2 = J(\alpha)$, $E = \{X, Y\}$, and U as in Theorem 6.12. This is a valid application thanks to Proposition 6.10.

By Proposition 6.7, $A_0^s \in Z_3(H(\alpha))$, and $Z_2(H(\alpha)) = \langle A_0^{2s}, B_0^{2s}, C_0^s\rangle$ is abelian with $C_0^s \in Z(H(\alpha))$. It follows that for $x, y \in \langle A_0^{2s}, B_0^{2s}\rangle$, we have

$$A_0\Pi_{(x,y)}\Gamma \equiv A_0^{1+s+2si}B_0^{2sj} \mod Z(H(\alpha)),\ B_0\Pi_{(x,y)}\Gamma \equiv A_0^sBA_0^{2sa}B_0^{2sb} \mod Z(H(\alpha))$$

for some $i, j, a, b \in \mathbb{Z}$. Thus, for $u = \Pi_{(x,y)}\Gamma$, we can take $h_{X,u} = A^{1+s+2si}B^{2sj}z_1$ and $h_{Y,u} = A^sBA^{2sa}B^{2sb}z_2$, where $z_1, z_2 \in Z_2(J(\alpha))$. By Proposition 6.6, $J(\alpha') \cong J(\alpha)$ if and only the assignment

$$X \mapsto A^{1+s+2si}B^{2sj}z_1,\ Y \mapsto A^sBA^{2sa}B^{2sb}z_2$$

extends to an isomorphism $J(\alpha') \to J(\alpha)$ for some choice of i, j, a, b and $z_1, z_2 \in Z_2(J(\alpha))$. In view of Proposition 6.10 and the fact that any isomorphism $J(\alpha') \to J(\alpha)$ restricts to an isomorphism between their second centers, we deduce that $J(\alpha') \cong J(\alpha)$ if and only the assignment

$$X \mapsto A^{1+s+2si}B^{2sj},\ Y \mapsto A^sBA^{2sa}B^{2sb} \tag{6.20}$$

extends to an isomorphism $J(\alpha') \to J(\alpha)$ for some choice of i, j, a, b.

Suppose that (6.20) extends to a homomorphism, say Ω, for some i, j, a, b. According to Proposition 6.7, the centers of $J(\alpha')$ and $J(\alpha)$ are generated by X^{2u} and A^{2u}, respectively. Since Ω maps X^{2u} into $A^{(1+s)2u}$, with $1 + s$ odd, we see that Ω restricts an isomorphism

between the centers of $J(\alpha')$ and $J(\alpha)$. As these are nilpotent groups, it follows that Ω is injective. But $J(\alpha')$ and $J(\alpha)$ have order 2^{7m-3}, so Ω is an isomorphism.

Now (6.20) extends to a homomorphism $J(\alpha') \to J(\alpha)$ if and only if there exist $i, j, a, b \in \mathbb{Z}$ such that the following relations hold in $J(\alpha)$:

$$(A^{1+s+2si}B^{2sj})^{[A^{1+s+2si}B^{2sj}, A^sBA^{2sa}B^{2sb}]} = (A^{(1+s+2si)}B^{2sj})^{\alpha'}, \tag{6.21}$$

$$(A^sBA^{2sa}B^{2sb})^{[A^sBA^{2sa}B^{2sb}, A^{1+s+2si}B^{2sj}]} = (A^sBA^{2sa}B^{2sb})^{\alpha'}. \tag{6.22}$$

We proceed to compute the left and right hand sides of (6.21) and (6.22).

Applying Theorem 5.7 to $(A^0BC^0)(A^{2sa}B^{2sb}C^0) = A^{\exp A+\xi_2}B^{\exp B}C^{\exp C}$ gives $\exp A \equiv 2sa - 2u\ell a \mod 4us$, $\exp B \equiv 1 + 2sb \mod 4us$, $\exp C \equiv -2sa + 2ua \mod 4u$, and $\xi_2 \equiv 2usa \mod 4us$. Thus

$$A^sBA^{2sa}B^{2sb} = A^{s+2sa}B^{1+2sb}C^{-2sa+2ua}A^{2usa-2u\ell a} = A^{s+2sa}B^{1+2sb}C^{-2sa}A^{-2u\ell a}. \tag{6.23}$$

Therefore

$$A^sBA^{2sa}B^{2sb} \equiv A^{s+2sa}B^{2sb}C^{-2sa} \mod Z(J(\alpha)),$$

$$[A^{1+s+2si}B^{2sj}, A^sBA^{2sa}B^{2sb}] = [A^{1+s+2si}B^{2sj}, A^{s+2sa}B^{2sb}C^{-2sa}].$$

Applying Proposition 5.9 to $[A^{1+s+2si}B^{2sj}, A^{s+2sa}BC^{-2sa}] = A^{\exp A}B^{\exp B}C^{\exp C}$ we obtain $\exp A \equiv u \mod 2u$, $\exp B \equiv 0 \mod 2u$, $\exp C \equiv 1 + s + 2s(i + b) \mod 2u$, so

$$[A^{1+s+2si}B^{2sj}, A^{s+2sa}B^{2sb}C^{-2sa}] \equiv A^uC^{1+s+2s(i+b)} \mod Z(J(\alpha)). \tag{6.24}$$

By Proposition 6.7, $Z_3(J(\alpha)) = \langle A^{2s}, B^{2s}, C^{2^s}\rangle$ is abelian, so

$$\begin{aligned}(A^{1+s+2si}B^{2sj})^{[A^{1+s+2si}B^{2sj}, A^sBA^{2sa}B^{2sb}]} &= (A^{1+s+2si}B^{2sj})^{A^uC^{1+s+2s(i+b)}} \\ &= (A^{1+s+2si}B^{2sj})^{C^{1+s+2s(i+b)}}.\end{aligned}$$

By means of Theorem 5.3, we may now derive

$$(A^{1+s+2si}B^{2sj})^{[A^{1+s+2si}B^{2sj}, A^sBA^{2sa}B^{2sb}]} = A^{\alpha+s+2si+4u\ell(2i+b+j+1)}. \tag{6.25}$$

On the other hand, applying Theorem 5.10 to $(A^{1+s+2si}B^{2sj})^{\alpha'} = A^{\exp A+\xi_4}B^{\exp B}C^{\exp C}$ gives $\exp A \equiv 1 + 2s\ell' + s + 2si + 2u\ell' + 4u\ell' i \mod 4us$, $\exp B \equiv 2sj + 4u\ell' j + 2usj \mod 4us$, $\exp C \equiv 2sj \mod 4u$, $\xi_4 \equiv 0 \mod 4us$, so

$$(A^{1+s+2si}B^{2sj})^{\alpha'} = A^{\alpha'+s+2si+2u\ell'+4u\ell' i}B^{2sj+4u\ell' j+2usj}C^{2sj} = A^{\alpha'+s+2si+2u\ell'+4u\ell'(i-j)}B^{2sj}. \tag{6.26}$$

Thus (6.21) holds if and only if (6.25) equals (6.26). The order of A is 2^{3m-1} by Proposition 4.14. Thus (6.21) is true if and only if

$$2s\ell + 4u\ell(2i+b+j+1) \equiv 2s\ell' + 2u\ell' + 4u\ell'(i-j) \mod 4us. \tag{6.27}$$

By hypothesis $\ell' = \ell + qs$ with q odd, so $q+\ell$ is even. Hence, recalling that $r = s/2$, (6.27) becomes

$$4u\ell(i+b+j+1) \equiv 4u(r + (q+\ell)/2) \mod 4us,$$

that is,

$$\ell(i+b+2j) \equiv -\ell + r + (q+\ell)/2 \mod s. \tag{6.28}$$

As for (6.22), by Theorem 5.3, Corollary 5.8, and (6.24), we have

$$\begin{aligned}[A^sBA^{2sa}B^{2sb}, A^{1+s+2si}B^{2sj}] &\equiv [A^{1+s+2si}B^{2sj}, A^sBA^{2sa}B^{2sb}]^{-1} \\ &\equiv A^{-u}C^{-1-s-2s(i+b)} \mod Z(J(\alpha)).\end{aligned}$$

Thus

$$(A^sBA^{2sa}B^{2sb})^{[A^sBA^{2sa}B^{2sb}, A^{1+s+2si}B^{2sj}]} = (A^sBA^{2sa}B^{2sa})^{A^{-u}C^{-1-s-2s(i+b)}}.$$

Appealing to Theorem 5.3, we obtain

$$\begin{aligned}&(A^sBA^{2sa}B^{2sb})^{[A^sBA^{2sa}B^{2sb}, A^{1+s+2si}B^{2sj}]} \\ &\quad = A^{s+2sa}B^{1+2s\ell+2sb}C^{-2sa+u}A^{-4u\ell-6u\ell a-4u\ell(i+2b)+us\ell}.\end{aligned} \tag{6.29}$$

Due to (6.23), $A^sBA^{2sa}B^{2sb} = A^{s+2sa}B^{1+2sb}C^{-2sa}A^{-2u\ell a}$, where $A^{-2u\ell a}$ is central and we have $(A^{-2u\ell a})^{1+2s\ell'} = A^{-2u\ell a}$. Applying Theorem 5.10 to

$$(A^{s+2sa}B^{1+2sb}C^{-2sa})^{1+2s\ell'} = A^{\exp A + \xi_4}B^{\exp B}C^{\exp C}$$

gives $\exp A \equiv s + 2sa + 2u\ell' + 4u\ell' a + u^2 - us\ell'\ell - 2usa \mod 4us$, $\exp B \equiv 1 + 2s\ell' + 2sb + 4u\ell' b + 2us \mod 4us$, $\exp C \equiv -2sa - u\ell' - 2u\ell' a \mod 4u$, $\xi_4 \equiv u^2 \mod 4us$, so

$$(A^sBA^{2sa}B^{2sb})^{1+2s\ell'} = A^{s+2sa}B^{1+2s\ell'+2sb}C^{-2sa-u\ell'}A^{2u(\ell'-s)+4u\ell'(a-b)-us\ell'\ell-2u\ell a}. \tag{6.30}$$

Thus (6.22) holds if and only if (6.29) equals (6.30). Here $B^{2s\ell'} = B^{2s\ell}B^{2uq} = B^{2s\ell}A^{-2uq}$, with A^{2u} central. As $B^{2sb} \in Z_3(J(\alpha))$, which is abelian, we see that (6.22) holds if and only if

$$C^uA^{-4u\ell-6u\ell a-4u\ell(i+2b)+us\ell} = C^{-u\ell'}A^{-2uq+2u(\ell'-s)+4u\ell'(a-b)-us\ell'\ell-2u\ell a}.$$

Here $C^{u(1+\ell')} = A^{us(1+\ell')}$. As A has order $4us$, the above condition becomes

$$s(1+\ell') - 4\ell - 6\ell a - 4\ell(i+2b) + s\ell \equiv -2q + 2(\ell'-s) + 4\ell'(a-b) - s\ell'\ell - 2\ell a \mod 4s,$$

which simplifies to

$$\ell(i+b+2a) \equiv (q-3\ell)/2 \mod s, \tag{6.31}$$

where $q-3\ell$ is even. Subtracting (6.31) from (6.28), we obtain

$$2\ell(j-a) \equiv r+\ell \mod s. \tag{6.32}$$

This has a solution if and only if $m=2$.

If $m=2$, once j and a are chosen so that (6.32) holds, the equations (6.28) and (6.31) become identical and they can be solved for i and b. □

6.4 Necessity for $H(\alpha)$

We assume in this section that $m>2$.

Note that α and α' have the same order modulo 2^{2m-1}, namely 2^{m-1}. It is well-known that $[\mathbb{Z}/2^{2m-1}\mathbb{Z}]^\times$ is the internal direct product of the cyclic subgroups generated by the classes of 5 and -1. Since α and α' are congruent to 1 modulo 4, their classes must belong to the subgroup generated by the class of 5. In a finite cyclic group there is at most one subgroup of any given order, so α and α' generate the same subgroup modulo 2^{2m-1}, which means that there is an odd integer t such that $\alpha' \equiv \alpha^t \mod 2^{2m-1}$. We may take t to be positive and we do so.

By (5.12), we have

$$K(\alpha) = \langle\, a,b \mid a^{[a,b]} = a^\alpha,\ b^{[b,a]} = b^\alpha,\ a^{2^{2m-1}} = 1 = b^{2^{2m-1}},\ [a,b]^{2^{m-1}} = 1 \,\rangle$$

and

$$K(\alpha') = \langle\, x,y \mid x^{[x,y]} = x^{\alpha'},\ y^{[y,x]} = y^{\alpha'},\ x^{2^{2m-1}} = 1 = y^{2^{2m-1}},\ [x,y]^{2^{m-1}} = 1 \,\rangle.$$

Let μ be the automorphism of $K(\alpha')$ given by $x \leftrightarrow y$.

Consider the projection homomorphisms $\pi_\alpha : H(\alpha) \to K(\alpha)$, given by $A \mapsto a$ and $B \mapsto b$, and $\pi_{\alpha'} : H(\alpha') \to K(\alpha')$, given by $X \mapsto x$ and $Y \mapsto y$.

We have the natural homomorphism $\Lambda : \mathrm{Aut}(H(\alpha')) \to \mathrm{Aut}(K(\alpha'))$ such that $\pi_{\alpha'}\beta^\Lambda = \beta\pi_{\alpha'}$ for all $\beta \in \mathrm{Aut}(H(\alpha'))$.

Proposition 6.33. *For any $u,v \in Z_2(K(\alpha'))$, the assignment $x \mapsto xu,\ y \mapsto yv$ extends to an automorphism of $K(\alpha')$. In particular, the assignments*

$$x \mapsto x^{1+s},\ y \mapsto y;\ x \mapsto x,\ y \mapsto y^{1+s};\ x \mapsto xy^s,\ y \mapsto y;\ x \mapsto x,\ y \mapsto yx^s$$

extend to automorphisms ψ_1, ψ_2, ψ_3, and ψ_4, respectively, of $K(\alpha')$.

Proof. See Proposition 5.22. □

Proposition 6.34. *The assignment* $x \mapsto xy^r,\ y \mapsto y$ *extends to an automorphism* Φ *of* $K(\alpha')$.

Proof. See Proposition 5.28. □

Recall the automorphism f_n of $K(\alpha')$ defined in Proposition 5.24.

Theorem 6.35. *Let* $U = \{\psi_1^d \psi_2^e f_n \Phi^g \mid 1 \le n \le m-1,\ n \equiv 1 \mod 2,\ 0 \le d, e, g \le 1\}$. *Then* $K(\alpha') = H(\alpha')^\Lambda U$.

Proof. Set $K = K(\alpha')$ and $H = H(\alpha')$. By Theorem 5.29 and its proof, we have

$$\mathrm{Aut}(K)/\mathrm{Aut}_2(K) = \langle \overline{\mu} \rangle \ltimes T,$$

where $T \cong (\mathbb{Z}/2^{m-1}\mathbb{Z})^\times \times (\mathbb{Z}/2\mathbb{Z})^2$ is given by

$$T = \{\overline{f_n} \,|\, 1 \le n \le m-1, n \equiv 1 \mod 2\} \times \{1, \overline{\Phi}\} \times \{1, \overline{\Phi^\mu}\}.$$

Here $\overline{f_{r+1}}$ has order 2, so

$$T = \{1, \overline{f_{r+1}\Phi\Phi^\mu}\} \times \{\overline{f_n} \,|\, 1 \le n \le m-1, n \equiv 1 \mod 2\} \times \{1, \overline{\Phi}\}.$$

Thus,

$$\mathrm{Aut}(K) = \{1, \mu\}\{1, f_{r+1}\Phi\Phi^\mu\}\mathrm{Aut}_2(K)\{f_n \,|\, 1 \le n \le m-1, n \equiv 1 \mod 2\}\{1, \Phi\}.$$

Let $\Sigma \in \mathrm{Aut}(H)$ be defined by $X \mapsto X^{1+r}Y^r$, $Y \mapsto Y^{1+r}X^r$, as in Corollary 5.57. Then $\overline{\Sigma^\Lambda} = \overline{f_{r+1}\Phi\Phi^\mu}$, that is, $\Sigma^\Lambda \equiv f_{r+1}\Phi\Phi^\mu \mod \mathrm{Aut}_2(K)$, so

$$\mathrm{Aut}(K) = (\{1, \nu\}\{1, \Sigma\})^\Lambda \mathrm{Aut}_2(K)\{f_n \,|\, 1 \le n \le m-1, n \equiv 1 \mod 2\}\{1, \Phi\}. \tag{6.36}$$

On the other hand, by Proposition 5.35, we have

$$\overline{\langle \psi_1, \psi_2, \psi_3, \psi_4 \rangle} = \mathrm{Aut}_2(K)/\mathrm{Inn}(K)\mathrm{Aut}_1(K) \cong (\mathbb{Z}/2\mathbb{Z})^4,$$

so

$$\mathrm{Aut}_2(K) = \mathrm{Inn}(K)\mathrm{Aut}_1(K)\{1, \psi_1\}\{1, \psi_2\}\{1, \psi_3\}\{1, \psi_4\}.$$

Here

$$(\mathrm{Inn}(H)\mathrm{Aut}_2(H))^\Lambda = \mathrm{Inn}(K)\mathrm{Aut}_1(K)$$

by Proposition 5.62. Moreover, if $\Gamma \in \mathrm{Aut}(H)$ is defined by $X \mapsto X^{1+s}$, $Y \mapsto YX^s$, as in Proposition 5.46, we readily see that $\Gamma^\Lambda = \psi_1\psi_4$ and $(\Gamma^\nu)^\Lambda = \psi_2\psi_3$. Therefore,

$$\mathrm{Aut}_2(K) = (\mathrm{Inn}(H)\mathrm{Aut}_2(H)\langle \Gamma, \Gamma^\nu \rangle)^\Lambda \{1, \psi_1\}\{1, \psi_2\}. \tag{6.37}$$

Combining (6.36) and (6.37) we obtain $K(\alpha') = H(\alpha')^\Lambda U$. □

Proposition 6.38. *We have* $K(\alpha') \cong K(\alpha)$.

Proof. Consider the assignment

$$x \mapsto a,\ y \mapsto b^t. \tag{6.39}$$

We claim that (6.39) extends to an isomorphism $K(\alpha') \to K(\alpha)$.

We have $[a,b] \in Z_2(K(\alpha))$ by Proposition 6.7, so $[a,b^t] \equiv [a,b]^t \mod Z(K(\alpha))$, that is, $[a,b^t] = [a,b]^t z, z \in Z(K(\alpha))$. Hence

$$a^{[a,b^t]} = a^{[a,b]^t z} = a^{[a,b]^t} = a^{\alpha^t} = a^{\alpha'},\ b^{[b^t,a]} = b^{[b,a]^t z^{-1}} = b^{[b,a]^t} = b^{\alpha^t} = b^{\alpha'}.$$

This shows that the first two defining relations of $K(\alpha')$ are preserved. The next two defining relations of $K(\alpha')$ are obviously preserved. As for the fifth, we have $Z(K(\alpha)) = \langle a^{2s}, b^{2s} \rangle$ by Proposition 6.7, so

$$[a,b^t]^{2^{m-1}} = ([a,b]^t z)^{2^{m-1}} = [a,b]^{2^{m-1}t} z^{2^{m-1}} = 1.$$

Thus (6.39) extends to an homomorphism $K(\alpha') \to K(\alpha)$. Likewise, if $q \in \mathbb{Z}$ is the inverse of t modulo 2^{2m-1}, we have a homomorphism $K(\alpha) \to K(\alpha')$ such that $a \mapsto x, b \mapsto y^q$. As these are inverse of each other, we deduce $K(\alpha) \cong K(\alpha')$. □

Recall that for $i \in \mathbb{Z}$, $\phi(i) = i(i-1)/2$.

Theorem 6.40. *We have* $H(\alpha') \cong H(\alpha)$ *if and only if* $\alpha' \equiv \alpha \mod 2^{2m-2}$.

Proof. Let $\gamma : K(\alpha') \to K(\alpha)$ be the isomorphism (6.39). For $u = \psi_1^d \psi_2^e f_n \Phi^g$, if $g = 0$, then

$$xu\gamma = a^i, yu\gamma = b^j,$$

for some odd integers i and j, while if $g = 1$, then

$$xu\gamma = (ab^r)^i,\ yu\gamma = b^j,$$

for some odd integers i and j. We next apply Proposition 6.6 with $G_1 = H(\alpha')$, $G_2 = H(\alpha)$, $E = \{X, Y\}$, and U as in Theorem 6.35. This is a valid application thanks to Proposition 6.33. For $g = 0$, we take $h_{U,X} = A^i$ and $h_{U,Y} = B^j$, and for $g = 1$, we take $h_{U,X} = (AB^r)^i$ and $h_{U,Y} = B^j$. By Proposition 6.6, $H(\alpha') \cong H(\alpha)$ if and only if at least one of the assignments

$$X \mapsto A^i,\ Y \mapsto B^j, \tag{6.41}$$

$$X \mapsto (AB^r)^i,\ Y \mapsto B^j, \tag{6.42}$$

extends to an isomorphism $H(\alpha') \to H(\alpha)$, where i and j are odd.

We proceed to prove that (6.41) extends to an isomorphism $H(\alpha') \to H(\alpha)$ if and only if $i \equiv 1 \mod 2s$, $j \equiv 1 \mod 2s$, and $\ell' \equiv \ell \mod s$, while (6.42) extends to an isomorphism $H(\alpha') \to H(\alpha)$ if and only if $\ell' \equiv \ell \mod r$, $\ell' \not\equiv \ell \mod s$, $i \equiv 1 \mod 2s$, and $j = 1 + kr$ with $k \equiv 1 \mod 4$. In particular, $H(1+8\ell) \cong H(9)$, where all integers $1+8\ell$ are congruent to 9 modulo 16.

We observe from the proof of Theorem 4.16 that every element of $H(\alpha)$ can be written in one and only one way as product of elements taken from $\langle A \rangle$, $\langle B \rangle$, and $\langle C \rangle$, in any fixed order.

Note that (6.41) extends to an isomorphism if and only if

$$A^{[A^i,B^j]} = A^{\alpha'}, B^{[B^j,A^i]} = B^{\alpha'}. \tag{6.43}$$

By Corollary 5.38,

$$[A^i, B^j] = A^{-2s\ell j\phi(i)} B^{2s\ell i\phi(j)} C^{ij-2s\ell\phi(i)\phi(j)}. \tag{6.44}$$

Using (6.44) and Corollary 5.38, we see that

$$A^{[A^i,B^j]} = A^{1+2s\ell ij} C^{2s\ell i\phi(j))}. \tag{6.45}$$

On the other hand,

$$A^{\alpha'} = A^{1+2s\ell'}. \tag{6.46}$$

Thus (6.45) is equal to (6.46) if and only if $\ell ij \equiv \ell' \mod s$ and $j \equiv 1 \mod 2s$.

Applying the automorphism $A \leftrightarrow B$ to (6.45) and then making the substitution $i \leftrightarrow j$ yields

$$B^{[B^j,A^i]} = B^{1+2s\ell ij} C^{-2s\ell j\phi(i))}. \tag{6.47}$$

On the other hand,

$$B^{\alpha'} = B^{1+2s\ell'}. \tag{6.48}$$

Thus (6.47) is equal to (6.48) if and only if $\ell ij \equiv \ell' \mod s$ and $i \equiv 1 \mod 2s$.

We deduce that (6.43) holds if and only if $i \equiv 1 \mod 2s$, $j \equiv 1 \mod 2s$, and $\ell \equiv \ell' \mod s$.

Moving now to (6.42), note that this assignment extends to an isomorphism if and only if

$$((AB^r)^i)^{[(AB^r)^i,B^j]} = (AB^r)^{i\alpha'} \tag{6.49}$$

and

$$B^{[B^j,(AB^r)^i]} = B^{\alpha'}. \tag{6.50}$$

Indeed, the conditions are clearly necessary. Using Corollary 5.41, we see that

$$(AB^r)^i = A^{i+u\phi(i)}B^{ir+\ell(r+1)\phi(i)u/2}C^{-r\phi(i)+\ell(r-1)\phi(i)u/2}. \tag{6.51}$$

By Note 5.42, it follows that $((AB^r)^i)^u = 1$. Thus if (6.49) and (6.50) hold, all 4 defining relations of $H(\alpha)$ are preserved, so (6.42) extends to an homomorphism. Using (6.51) and Corollary 5.40, we find that

$$[(AB^r)^i, B^j] = A^{-2s\ell\phi(i)j}B^{2s\ell i\phi(j)+u(1-\phi(i))}C^{ij+u\phi(i)j}, \tag{6.52}$$

where C^s is central in $H(\alpha)$ by Proposition 6.7. The given homomorphism will then map $[X,Y]^s$ to C^{ijs}. As i and j are odd, the given homomorphism will restrict to an isomorphism between the corresponding centers, and it will then be an isomorphism.

By means of (6.51) and (6.52), a careful use of Corollary 5.38 yields

$$\begin{aligned}&((AB^r)^i)^{[(AB^r)^i,B^j]}\\ &\quad = A^{i+u\phi(i)+2s\ell i^2 j}B^{u+ir+\ell(r+1)\phi(i)u/2}C^{-r\phi(i)+\ell(r-1)\phi(i)u/2+u\phi(i)+2s\ell i^2\phi(j)+u(1-\phi(i))}.\end{aligned} \tag{6.53}$$

On the other hand, Corollary 5.41 gives

$$(AB^r)^{i\alpha'} = A^{i+u\phi(i)+2s\ell' i}B^{u+ir+u+\ell(r+1)\phi(i)u/2}C^{-r\phi(i)+\ell(r-1)\phi(i)u/2-u\ell'\phi(i)-i^2\ell' u/2}. \tag{6.54}$$

By Corollary 5.38 all factors appearing in (6.52) commute with each other, so

$$[B^j, (AB^r)^i] = A^{2s\ell\phi(i)j}B^{-2s\ell i\phi(j)+u(1-\phi(i))}C^{-ij-u\phi(i)j}. \tag{6.55}$$

It follows from (6.55) and Corollary 5.38 that

$$B^{[B^j,(AB^r)^i]} = B^{1-2s\ell ij}C^{-2s\ell\phi(i)j}. \tag{6.56}$$

On the other hand, we have

$$B^{\alpha'} = B^{1+2s\ell'}. \tag{6.57}$$

We readily see that (6.56) is equal to (6.57) if and only if $i \equiv 1 \mod 2s$ and $\ell j \equiv \ell' \mod s$. On the other hand, (6.53) is equal to (6.54) if and only if $\ell ij \equiv \ell' \mod s$ and

$$2s\ell i^2\phi(j) + u \equiv u\phi(i) - i^2\ell' u/2 \mod 2u.$$

Thus (6.56) is equal to (6.57) and (6.53) is equal to (6.54) if and only if

$$i \equiv 1 \mod 2s,\ \ell j \equiv \ell' \mod s,\ 2s\ell\phi(j) + u \equiv -\ell' u/2 \mod 2u. \tag{6.58}$$

Suppose first that (6.58) holds. Then

$$2s\ell\phi(j) \equiv 0 \mod u/2,$$

which is equivalent to

$$j \equiv 1 \mod r.$$

Thus $\ell \equiv \ell' \mod r$, so that $\ell' = \ell + qr$ for some $q \in \mathbb{Z}$. Writing $j = 1 + rk$, with $k \in \mathbb{Z}$, and replacing this in (6.58) yields

$$\ell jku/2 + u \equiv -\ell' u/2 \mod 2u. \tag{6.59}$$

Note that (6.59) implies $\ell jk \equiv \ell' \mod 2$, so k must be odd. Also, from $\ell j \equiv \ell' \mod s$, we obtain

$$\ell(1 + rk) \equiv \ell + qr \mod s.$$

As ℓ is odd, this implies $rk \equiv qr \mod s$, or $k \equiv q \mod 2$, so q must be odd too. Going back to (6.59), we may write it in the form $\ell jk + 2 \equiv -\ell' \mod 4$, or $\ell jk + 2 \equiv -\ell - rq \mod 4$, that is $\ell(1 + jk) \equiv 2 - rq \mod 4$. Here j, k, and ℓ are odd, so the last condition becomes $1 + jk \equiv 2 - rq \mod 4$. If $m > 3$ this translates into

$$1 + (1 + rk)k \equiv 1 + k \equiv 2 \mod 4,$$

so $k \equiv 1 \mod 4$. If $m = 3$, the fact that q is odd implies $1 + (1 + 2k)k \equiv 0 \mod 4$. As $k^2 \equiv 1 \mod 4$, we deduce $1 + k + 2 \equiv 0 \mod 4$, so $k \equiv 1 \mod 4$. Retracing our steps we see that the conditions $\ell' \equiv \ell \mod r$, $\ell' \not\equiv \ell \mod s$, $i \equiv 1 \mod 2s$, and $j = 1 + kr$ with $k \equiv 1 \mod 4$, are sufficient. □

6.5 Necessity for $J(\alpha)$ Part II

We assume in this section that $m > 2$. Also we maintain the notation introduced in Section 6.3 and set $\overline{r} = r/2$.

Theorem 6.60. *Suppose* $\alpha' \equiv \alpha \mod 2^{2m-2}$ *but* $\alpha' \not\equiv \alpha \mod 2^{2m-1}$. *Then* $J(\alpha') \ncong J(\alpha)$.

Proof. Suppose, if possible, that $J(\alpha') \cong J(\alpha)$. The proof of Theorem 6.40 provides an explicit isomorphism $\gamma : H(\alpha') \to H(\alpha)$, given by

$$X_0 \mapsto A_0 B_0^r,\ Y_0 \mapsto B_0^{1+r}.$$

We next apply Proposition 6.6 with $G_1 = J(\alpha')$, $G_2 = J(\alpha)$, $E = \{X, Y\}$, and U as in Theorem 6.12. This is a valid application thanks to Proposition 6.10. Arguing as in the proof of Theorem 6.19, we see that for some choice of integers i, j, a, b, the assignment

$$X \mapsto (AB^r)^{1+s}A^{2si}B^{2sj},\ Y \mapsto B^{1+r}(AB^r)^sA^{2sa}B^{2sb}$$

extends to an isomorphism $J(\alpha') \to J(\alpha)$. This implies that the following equations hold:

$$((AB^r)^{1+s}A^{2si}B^{2sj})^{[(AB^r)^{1+s}A^{2si}B^{2sj},B^{1+r}(AB^r)^sA^{2sa}B^{2sb}]} = ((AB^r)^{1+s}A^{2si}B^{2sj})^{\alpha'}, \tag{6.61}$$

$$(B^{1+r}(AB^r)^sA^{2sa}B^{2sb})^{[B^{1+r}(AB^r)^sA^{2sa}B^{2sb},(AB^r)^{1+s}A^{2si}B^{2sj}]} = (B^{1+r}(AB^r)^sA^{2sa}B^{2sb})^{\alpha'}. \tag{6.62}$$

The calculation of both sides of (6.61) and (6.62) are tedious and they appear in Appendix 3 located in Section 6.8.

From (6.79) and (6.80) in Appendix 3, we get that (6.61) is equivalent to

$$\begin{aligned} &A^{2s(\ell-\ell')+u\ell}B^{r+sr+2sj+u\ell(\overline{r}-1)}C^{sr(\ell+\ell')+u(\overline{r}+1)}B^{-r-sr-2sj-u(\overline{r}\ell+\ell')} \\ &\quad = A^{2u(2i\ell'-2j\ell'+\ell'-4i\ell-2j\ell-2b\ell-2\ell)-ur\ell(\ell'+\ell+1)+us\overline{r}(\ell'+1)+u\varphi(2s\ell')+2us(i+j+a+b+1)}. \end{aligned}$$

By Theorem 5.3 we have $[C^{sr(\ell+\ell')+u(\overline{r}+1)}, B^{-r-sr-2sj-u(\overline{r}\ell+\ell')}] = 1$, so

$$\begin{aligned} &A^{2s(\ell-\ell')+u\ell}B^{-u(\ell+\ell')}C^{sr(\ell+\ell')+u(\overline{r}+1)} \\ &\quad = A^{2u(2i\ell'-2j\ell'+\ell'-4i\ell-2j\ell-2b\ell-2\ell)-ur\ell(\ell'+\ell+1)+us\overline{r}(\ell'+1)+u\varphi(2s\ell')+2us(i+j+a+b+1)}, \end{aligned}$$

and from this

$$\begin{aligned} &A^{2s(\ell-\ell')+u\ell}C^{sr(\ell+\ell')+u(\overline{r}+1)} \\ &= A^{-u(\ell+\ell')+2u(2i\ell'-2j\ell'+\ell'-4i\ell-2j\ell-2b\ell-2\ell)-ur\ell(\ell'+\ell+1)+us\overline{r}(\ell'+1)+u\varphi(2s\ell')+2us(i+j+a+b+1)}. \end{aligned} \tag{6.63}$$

From (6.81) and (6.82) in Appendix 3, we get that (6.62) is equivalent to

$$B^{2s(\ell-\ell')-u\ell'} = A^{2u(2a\ell'+2a\ell-2b\ell'+4b\ell+2i\ell+3\ell+\ell')+ur\ell-us\ell(\ell'-1)+2us}. \tag{6.64}$$

Since $\alpha \equiv \alpha' \mod u$ and $\alpha \not\equiv \alpha' \mod 2u$, this is, $\ell \equiv \ell' \mod r$ and $\ell \not\equiv \ell' \mod s$, then $\ell' = \ell - r - s\ell'_1$ for some $\ell'_1 \in \mathbb{Z}$ and

$$B^{2s(\ell-\ell')-u\ell'} = B^{u(1-\ell)+2u\ell'_1+ur+us\ell'_1} = A^{u(\ell-1)-2u\ell'_1-ur-us\ell'_1}.$$

Replacing the above in (6.64) produces

$$A^{u(1-\ell)+4u\ell(i+2a+b+2)+2u\ell'_1+ur(\ell+1)+us(\ell+\ell'_1)+usr+2us(a+b+\ell'_1)} = 1,$$

and from this

$$\begin{aligned} u(1-\ell)+4u\ell(i+2a+b+2)+2u\ell_1'+ur(\ell+1)+us(\ell+\ell_1')+usr \\ +2us(a+b+\ell_1')\equiv 0 \mod 4us. \end{aligned} \tag{6.65}$$

In the other hand,

$$A^{2s(\ell-\ell')+u\ell}C^{sr(\ell+\ell')+u(\overline{r}+1)}=A^{u(\ell+1)+2u\ell_1'}C^{u(\ell+1)+ur\ell_1'}=A^{u(\ell+1)+2u\ell_1'+us(\ell+1)+usr\ell_1'}.$$

Replacing the above in (6.63) produces

$$A^{-u(\ell+1)-2u\ell_1'-4u\ell(i+2j+b+1)-ur(\ell-1)+us(\overline{r}-\ell+\ell_1'+1)+usr(\overline{r}+1)+u\varphi(2s\ell')+2us(a+b+\ell_1'+1)}=1,$$

and from this

$$\begin{aligned} -u(\ell+1)-2u\ell_1'-4u\ell(i+2j+b+1)-ur(\ell-1)+us(\overline{r}-\ell+\ell_1'+1) \\ +usr(\overline{r}+1)+u\varphi(2s\ell')+2us(a+b+\ell_1'+1)\equiv 0 \mod 4us. \end{aligned} \tag{6.66}$$

Subtracting (6.66) from (6.65) produces

$$2u+4u\ell(2i+2j+2a+2b+3)+4u\ell_1'+us(\ell-\overline{r}-1)+usr\overline{r}+u\varphi(2s\ell')\equiv 0 \mod 4us.$$

Dividing this by $2u$ and reducing module 2 yields

$$1+2\ell(2i+2j+2a+2b+3)+2\ell_1'+r(\ell-\overline{r}-1)+s\overline{r}^2+\varphi(2s\ell')/2\equiv 0 \mod 2,$$

which is impossible. □

6.6 Common structural features of $J(\alpha)$ and $J(\alpha')$

Theorem 6.67. *The derived subgroups and all factors of the upper central series of $J(\alpha)$ and $J(\alpha')$ are isomorphic.*

Proof. If $m=1$ then $J(\alpha)\cong J(\alpha')$ by Theorem 6.1, so we assume $m>1$.

Set $J=J(\alpha)$, so that $J=\langle\, A,B \mid A^{[A,B]}=A^{\alpha},\ B^{[B,A]}=B^{\alpha},\ A^{2^{2m-1}}=1=B^{2^{2m-1}}\,\rangle$.

The terms of the upper central series of J are given in Proposition 6.7. Here $Z_1(J)\cong\mathbb{Z}/2^m\mathbb{Z}$ by Proposition 4.14. Since $Z_3(J)$ is abelian by Proposition 4.20, we infer $Z_2(J)\cong\mathbb{Z}/2^m\mathbb{Z}\times\mathbb{Z}/2^m\mathbb{Z}$ and $Z_2(J)/Z_1(J)\cong\mathbb{Z}/2^m\mathbb{Z}$ by Theorem 4.13, Proposition 4.14, and the fundamental relation $A^{2^{3m-2}}=C^{2^{m-1}}$. In Theorem 4.12 one constructs a group $\langle x_0,y_0\rangle$ isomorphic to J

via $A \mapsto x_0$, $B \mapsto y_0$. Under this isomorphism $Z_3(J)$ corresponds to a subgroup of order 2^{4m-2} generated by elements x, y, z subject to the defining relations

$$xy = yx,\ xz = zx,\ yz = zx,\ z^{2^m} = x^{2^{2m-2}},\ x^{2^{m-1}} y^{2^{m-1}} = 1,\ x^{2^{2m-1}} = 1.$$

In particular, the isomorphism type of $Z_3(J)$ is independent of ℓ. In view of the fundamental relation $A^{2^{2m-1}} B^{2^{2m-1}} = 1$, it follows that $Z_3(J)/Z_2(J)$ is a quotient of $\mathbb{Z}/2^{m-1}\mathbb{Z} \times \mathbb{Z}/2^{m-1}\mathbb{Z}$. But $Z_3(J)/Z_2(J)$ has order $2^{2(m-1)}$, so $Z_3(J)/Z_2(J) \cong \mathbb{Z}/2^{m-1}\mathbb{Z} \times \mathbb{Z}/2^{m-1}\mathbb{Z}$.

It is clear that $J/Z_4(J)$ and $\mathbb{Z}/2^{m-1}\mathbb{Z} \times \mathbb{Z}/2^{m-1}\mathbb{Z}$ are quotients of each other, so $J/Z_4(J) \cong \mathbb{Z}/2^{m-1}\mathbb{Z} \times \mathbb{Z}/2^{m-1}\mathbb{Z}$. Since $|J| = 2^{7m-3}$, it follows that $|Z_4(J)| = 2^{5m-1}$. It is also clear that $Z_4(J)/Z_3(J)$ is a quotient of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^m\mathbb{Z}$. But $Z_4(J)/Z_3(J)$ has order 2^{m+1}, so $Z_4(J)/Z_3(J) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^m\mathbb{Z}$.

By Theorem 4.16, we have $[J, J] = \langle A^{2s}, B^{2s}, C \rangle$. Here $J/[J, J]$ and $\mathbb{Z}/2^m\mathbb{Z} \times \mathbb{Z}/2^m\mathbb{Z}$ are quotients of each other, so $J/[J, J] \cong \mathbb{Z}/2^m\mathbb{Z} \times \mathbb{Z}/2^m\mathbb{Z}$, whence $[J, J]$ has order 2^{5m-3}.

Consider the group

$$U = \langle\, X, Y, Z \mid [X, Y] = 1,\ X^Z = X^\alpha,\ Y^Z = Y^\beta,\ Z^{2u} = X^u,\ X^s Y^s = 1,\ X^{2u} = 1 \,\rangle,$$

where $\beta = 2 - \alpha$ is the inverse of α modulo $2u$. It is not difficult to see that $|U| \leq 2^{5m-3}$.

Since $Z_3(J)$ is abelian, we have $[A^{2s}, B^{2s}] = 1$. It follows that the map $X \mapsto A^{2s}$, $Y \mapsto B^{2s}$, $Z \mapsto C$ extends to an isomorphism $U \to [J, J]$. Likewise, $Z_4(J(\alpha'))$ is isomorphic to

$$V = \langle\, a, b, c \mid [a, b] = 1,\ a^c = a^{\alpha'},\ b^c = b^{\beta'},\ c^{2u} = a^u,\ a^s b^s = 1,\ a^{2u} = 1 \,\rangle,$$

where $\beta' = 2 - \alpha'$ is the inverse of α' modulo $2u$. Now α and α' have the same order s modulo $2u$, so as explained at the beginning of Section 6.4, $\alpha \equiv (\alpha')^i \mod 2u$ for some odd $i > 0$. It follows that the assignment $X \mapsto a$, $Y \mapsto b$, $Y \mapsto c^i$ extends to a group isomorphism $U \to V$, so $[J(\alpha), J(\alpha)] \cong [J(\alpha'), J(\alpha')]$. □

6.7 Solution to the isomorphism problem

We summarize our findings in the following results:

Theorem 6.68.

1. *$J(1+2\ell) \cong J(3)$ and $J(1+4\ell) \cong J(5)$ for all $\ell \in \mathbb{Z}$ odd.*
2. *If $m > 2$, then $J(\alpha) \cong J(\alpha')$ if and only if $\alpha \equiv \alpha' \mod 2^{2m}$. In particular, for fixed m, there are exactly $\varphi(2^m)$ isomorphism classes of groups $J(\alpha)$.*
3. *For any $m \geq 1$ the derived subgroups as well as all factors of the upper central series of $J(\alpha)$ and $J(\alpha')$ are isomorphic. In addition, $K(1+2^m\ell) \cong K(1+2^m)$ for all $\ell \in \mathbb{Z}$ odd.*

Proof. Consequence of Theorems 6.1, 6.19, 6.40, 6.60, 6.67, and Proposition 6.38. □

Theorem 6.69.

1. *$H(1+2\ell) \cong H(3)$, $H(1+4\ell) \cong H(5)$, and $H(1+8\ell) \cong H(9)$ for all $\ell \in \mathbb{Z}$ odd.*
2. *If $m > 2$, then $H(\alpha') \cong H(\alpha)$ if and only if $\alpha' \equiv \alpha \mod 2^{2m-2}$. In particular, for fixed m, there are exactly $\varphi(2^{m-2})$ isomorphism classes of groups $H(\alpha)$.*

Proof. If $m = 1$ or $m = 2$ we appeal to Theorem 6.68, while if $m > 2$, we resort to Theorem 6.40. □

6.8 Appendix 3

We proceed to calculate both sides of (6.61) and (6.62). Recall the notation introduced in Sections 6.3 and 6.5.

Applying Theorem 5.10 to $(AB^r)^{1+s} = A^{\exp A}B^{\exp B}C^{\exp C}A^{\xi_4}$ produces $\exp A \equiv 1+s+u\varphi(s)\ell+usr-ur\ell \mod 4us$, $\exp B \equiv r+sr+u\overline{r}\ell-ur\overline{r}\ell \mod 4us$, $\exp C \equiv -s\overline{r}+sr\varphi(s)+u\overline{r}(\ell-1) \mod 4u$, $\xi_4 \equiv ur\varphi(s)+usr \mod 4us$, so

$$(AB^r)^{1+s} = A^{1+s}B^{r+sr+u\overline{r}\ell}C^{-s\overline{r}}A^{u\varphi(s)\ell+ur\ell(\overline{r}-1)+us\overline{r}(\ell-1)}. \tag{6.70}$$

Applying Theorem 5.7 to $(A^{1+s}B^{r+sr+u\overline{r}\ell}C^{-s\overline{r}})(A^{2si}B^{2sj}C^0) = A^{\exp A}B^{\exp B}C^{\exp C}A^{\xi_2}$ produces $\exp A \equiv 1+s+2si-us\ell i \mod 4us$, $\exp B \equiv r+sr+2sj+u\overline{r}\ell+usri+us\ell i \mod 4us$, $\exp C \equiv -s\overline{r}-ui+uri \mod 4u$, $\xi_2 \equiv usri \mod 4us$, so

$$(A^{1+s}B^{r+sr+u\overline{r}\ell}C^{-s\overline{r}})(A^{2si}B^{2sj}C^0) = A^{1+s+2si}B^{r+sr+2sj+u\overline{r}\ell}C^{-s\overline{r}-ui}A^{2usi+usri}. \tag{6.71}$$

By (6.70) and (6.71),

$$\begin{aligned}(AB^r)^{1+s}A^{2si}B^{2sj} &= (A^{1+s}B^{r+sr+u\overline{r}\ell}C^{-s\overline{r}})(A^{2si}B^{2sj}C^0)A^{u\varphi(s)\ell+ur\ell(\overline{r}-1)+us\overline{r}(\ell-1)} \\ &= A^{1+s+2si}B^{r+sr+2sj+u\overline{r}\ell}C^{-s\overline{r}-ui}A^{ur\ell(\overline{r}-1)+u\varphi(s)\ell+us\overline{r}(\ell-1)+usri+2usi}.\end{aligned} \tag{6.72}$$

Applying Theorem 5.10 to $(AB^r)^s = A^{\exp A}B^{\exp B}C^{\exp C}A^{\xi_4}$ produces $\exp A \equiv s + u\varphi(s)\ell \mod 4us$, $\exp B \equiv sr + ur\overline{r}\ell - u\overline{r}\ell \mod 4us$, $\exp C \equiv -u\overline{r} + s\overline{r} + sr\varphi(s) + ur\overline{r} \mod 4u$, $\xi_4 \equiv ur\varphi(s) + us\overline{r}\ell^2 \mod 4us$, so

$$(AB^r)^s = A^sB^{sr-u\overline{r}\ell}C^{-u\overline{r}+s\overline{r}}A^{u\varphi(s)\ell-ur\overline{r}\ell+usr\overline{r}+us\overline{r}\ell^2}. \tag{6.73}$$

Applying Theorem 5.7 to $(A^0B^{1+r}C^0)(A^sB^{sr-u\overline{r}\ell}C^{-u\overline{r}+s\overline{r}}) = A^{\exp A}B^{\exp B}C^{\exp C}A^{\xi_2}$ produces $\exp A \equiv s - u\ell - ur\ell + us\ell + usr \mod 4us$, $\exp B \equiv 1 + r + sr - u\overline{r}\ell - ur\ell - us\overline{r}\ell \mod 4us$, $\exp C \equiv s(\overline{r}-1) - sr + u(\overline{r}\ell + \ell - \overline{r}) + ur(\overline{r}+1) \mod 4u$, $\xi_2 \equiv us\ell^2(\overline{r}+1) + usr\overline{r} + 2us \mod 4us$, so

$$\begin{aligned}&(A^0B^{1+r}C^0)(A^sB^{sr-u\overline{r}\ell}C^{-u\overline{r}+s\overline{r}}) \\ &\quad = A^{s-u\ell}B^{1+r+sr-u\overline{r}\ell}C^{s(\overline{r}-1)-sr+u(\overline{r}\ell+\ell-\overline{r})}A^{us(\overline{r}\ell+\overline{r}+\ell+1)+2us}.\end{aligned} \tag{6.74}$$

By (6.73) and (6.74),

$$\begin{aligned}&B^{1+r}(AB^r)^s \\ &\quad = (A^0B^{1+r}C^0)(A^sB^{sr-u\overline{r}\ell}C^{-u\overline{r}+s\overline{r}})A^{u\varphi(s)\ell-ur\overline{r}\ell+usr\overline{r}+us\overline{r}\ell^2} \\ &\quad = A^{s-u\ell}B^{1+r+sr-u\overline{r}\ell}C^{s(\overline{r}-1)-sr+u(\overline{r}\ell+\ell-\overline{r})}A^{-ur\overline{r}\ell+us(\overline{r}\ell+\ell+1)+usr(\overline{r}+1)+u\varphi(s)\ell+2us}.\end{aligned} \tag{6.75}$$

Applying Theorem 5.7 to

$$(A^{s-u\ell}B^{1+r+sr-u\overline{r}\ell}C^{s(\overline{r}-1)-sr+u(\overline{r}\ell+\ell-\overline{r})})(A^{2sa}B^{2sb}C^0) = A^{\exp A}B^{\exp B}C^{\exp C}A^{\xi_2}$$

produces $\exp A \equiv s+2sa-u\ell-2u\ell a-us\ell a \mod 4us$, $\exp B \equiv 1+r+sr+2sb-u\overline{r}\ell-us\ell a+usra \mod 4us$, $\exp C \equiv s(\overline{r}-1)-2sa-sr+u(\overline{r}\ell+\ell-\overline{r}-a)+2ua+ura \mod 4u$, $\xi_2 \equiv usra+2usa \mod 4us$, so

$$\begin{aligned}&(A^{s-u\ell}B^{1+r+sr-u\overline{r}\ell}C^{s(\overline{r}-1)-sr+u(\overline{r}\ell+\ell-\overline{r})})(A^{2sa}B^{2sb}C^0) \\ &\quad = A^{s+2sa-u\ell}B^{1+r+sr+2sb-u\overline{r}\ell}C^{s(\overline{r}-1)-2sa-sr+u(\ell-a)}A^{-2u\ell a+us\overline{r}(\ell-1)+usra}.\end{aligned} \tag{6.76}$$

By (6.75) and (6.76),

$$\begin{aligned}B^{1+r}(AB^r)^sA^{2sa}B^{2sb} &= (A^{s-u\ell}B^{1+r+sr-u\overline{r}\ell}C^{s(\overline{r}-1)-sr+u(\overline{r}\ell+\ell-\overline{r})})(A^{2sa}B^{2sb}C^0) \\ &\quad A^{-ur\overline{r}\ell+us(\overline{r}\ell+\ell+1)+usr(\overline{r}+1)+u\varphi(s)\ell+2us} \\ &= A^{s+2sa-u\ell}B^{1+r+2sb+sr-u\overline{r}\ell}C^{s(\overline{r}-1)-2sa-sr+u(\ell-a)} \\ &\quad A^{-2u\ell a-ur\overline{r}\ell+us(\ell-\overline{r}+1)+u\varphi(s)\ell+usr(\overline{r}+a)+2us}.\end{aligned} \tag{6.77}$$

Applying Theorem 5.9 to

$$\begin{aligned}&[(AB^r)^{1+s}A^{2si}B^{2sj}, B^{1+r}(AB^r)^sA^{2sa}B^{2sb}]\\&\quad= [A^{1+s+2si}B^{r+sr+2sj+u\overline{r}\ell}C^{-s\overline{r}-ui}, A^{s+2sa-u\ell}B^{1+r+2sb+sr-u\overline{r}\ell}C^{s(\overline{r}-1)-2sa-sr+u(\ell-a)}]\end{aligned}$$

produces $\exp A \equiv u \mod 2u$, $\exp B \equiv sr\ell + u(\overline{r}+1) \mod 2u$, $\exp C \equiv 1+r+s+2s(i+b) - sr + u(\overline{r}+i+a+1) \mod 2u$, so

$$\begin{aligned}&[(AB^r)^{1+s}A^{2si}B^{2sj}, B^{1+r}(AB^r)^sA^{2sa}B^{2sb}]\\&\quad\equiv A^uB^{sr\ell+u(\overline{r}+1)}C^{1+r+s-sr+2s(i+b)+u(\overline{r}+i+a+1)} \mod Z_1(J).\end{aligned} \tag{6.78}$$

Repeated applications of Theorem 5.3 produce
$[A^u, B^{r+sr+2sj+u\overline{r}\ell}] = A^{usr}$,
$[C^{-s\overline{r}-ui}, A^u] = 1$,
$[A^{1+s+2si}, B^{sr\ell+u(\overline{r}+1)}] = C^{sr\ell+u(\overline{r}+1)}A^{ur\ell^2+us\ell(\overline{r}+1)+usr}$,
$[C^{-s\overline{r}-ui}, B^{sr\ell+u(\overline{r}+1)}] = 1$,
$[C^{sr\ell+u(\overline{r}+1)}, B^{r+sr+2sj+u\overline{r}\ell}] = B^{usr}$,
$[C^{1+r+s-sr+2s(i+b)+u(\overline{r}+i+a+1)}, A^{1+s+2si}] = A^{-2s\ell-u\ell}A^{-4u\ell(2i+b+1)-us\ell^2+2us(\overline{r}+a+1)+usr}$,
$[C^{1+r+s-sr+2s(i+b)+u(\overline{r}+i+a+1)}, B^{r+sr+2sj+u\overline{r}\ell}] = B^{u\ell}B^{4u\ell j+ur\ell+2us(\overline{r}+i+j+b)+usr}$,
which all together yield

$$\begin{aligned}&((AB^r)^{1+s}A^{2si}B^{2sj})^{[(AB^r)^{1+s}A^{2si}B^{2sj}, B^{1+r}(AB^r)^sA^{2sa}B^{2sb}]}\\&\quad\equiv (A^{1+s+2si}B^{r+sr+2sj+u\overline{r}\ell}C^{-s\overline{r}-ui})^{A^uB^{sr\ell+u(\overline{r}+1)}C^{1+r+s-sr+2s(i+b)+u(\overline{r}+i+a+1)}}\\&\quad\equiv (A^{1+s+2si}C^{sr\ell+u(\overline{r}+1)}B^{r+sr+2sj+u\overline{r}\ell}C^{-s\overline{r}-ui})^{C^{1+r+s-sr+2s(i+b)+u(\overline{r}+i+a+1)}}\\&\quad\equiv (A^{1+s+2si}B^{r+sr+2sj+u\overline{r}\ell}C^{-s\overline{r}+sr\ell+u(\overline{r}-i+1)})^{C^{1+r+s-sr+2s(i+b)+u(\overline{r}+i+a+1)}}\\&\quad\equiv A^{1+s+2s(i+\ell)+u\ell}B^{r+sr+2sj+u\ell(\overline{r}-1)}C^{-s\overline{r}+sr\ell+u(\overline{r}-i+1)} \mod Z_1(J),\end{aligned}$$

where the central element is $A^{4u\ell(2i+j+b+1)+ur\ell(\overline{r}+\ell)+u\varphi(s)\ell+us(\ell-\overline{r}+1)+usri+2us(j+a+b+1)}$. Then

$$\begin{aligned}&((AB^r)^{1+s}A^{2si}B^{2sj})^{[(AB^r)^{1+s}A^{2si}B^{2sj}, B^{1+r}(AB^r)^sA^{2sa}B^{2sb}]}\\&\quad= A^{1+s+2s(i+\ell)+u\ell}B^{r+sr+2sj+u\ell(\overline{r}-1)}C^{-s\overline{r}+sr\ell+u(\overline{r}-i+1)}\\&\qquad A^{4u\ell(2i+j+b+1)+ur\ell(\overline{r}+\ell)+u\varphi(s)\ell+us(\ell-\overline{r}+1)+usri+2us(j+a+b+1)}.\end{aligned} \tag{6.79}$$

Applying Theorem 5.10 to $(A^{1+s+2si}B^{r+sr+2sj+u\overline{r}\ell}C^{-s\overline{r}-ui})^{1+2s\ell'} = A^{\exp A}B^{\exp B}C^{\exp C}A^{\xi_4}$ produces $\exp A \equiv 1+s+2s(i+\ell')+2u\ell'(2i+1)+u\varphi(2s\ell')-us\ell\ell' \mod 4us$, $\exp B \equiv r+sr+2sj+4uj\ell'+u(\ell'+\overline{r}\ell)+ur\ell\ell'+us\ell'(1-\overline{r}\ell)+2usj\ell' \mod 4us$, $\exp C \equiv -s\overline{r}-sr\ell'-ui+2uj\ell'$

mod $4u$, $\xi_4 \equiv 0 \mod 4us$, so

$$\begin{aligned}
&((AB^r)^{1+s}A^{2si}B^{2sj})^{1+2s\ell'} \\
&= (A^{1+s+2si}B^{r+sr+2sj+u\overline{r}\ell}C^{-s\overline{r}-ui})^{1+2s\ell'}A^{(ur\ell(\overline{r}-1)+u\varphi(s)\ell+us\overline{r}(\ell-1)+usri+2usi)(1+2s\ell')} \\
&= A^{1+s+2s(i+\ell')}B^{r+sr+2sj+u(\overline{r}\ell+\ell')}C^{-s\overline{r}-sr\ell'-ui} \\
&\quad A^{2u\ell'(2i-2j+1)+ur\ell(\overline{r}-\ell'-1)+u\varphi(s)\ell+us(\overline{r}\ell+\overline{r}\ell\ell'-\overline{r}-\ell\ell'-\ell')+2usi+u\varphi(2s\ell')+usri}.
\end{aligned} \tag{6.80}$$

Repeated applications of Theorem 5.3 produce

$$[C^{-1-r-s+sr-2s(i+b)-u(\overline{r}+i+a+1)}, A^{s+2sa-u\ell}] = A^{2u\ell(2a+1)+us\ell+2usa},$$
$$[C^{-1-r-s+sr-2s(i+b)-u(\overline{r}+i+a+1)}, B^{1+r+2sb+sr-u\overline{r}\ell}] = B^{-2s\ell}B^{-4u\ell(i+2b+1)-ur\ell+us(\ell+1)+2usa},$$
$$[A^{s+2sa-u\ell}, B^{-sr\ell-u(\overline{r}+1)}] = A^{usr},$$
$$[C^{s(\overline{r}-1)-2sa-sr+u(\ell-a)}, B^{-sr\ell-u(\overline{r}+1)}] = 1,$$
$$[A^{-u}, B^{1+r+2s(b+\ell)+sr-u\overline{r}\ell}] = C^{-u}A^{-us\ell+usr},$$
$$[C^{s(\overline{r}-1)-2sa-sr+u(\ell-a)}, A^{-u}] = 1,$$

which all together yield

$$\begin{aligned}
&(B^{1+r}(AB^r)^sA^{2sa}B^{2sb})^{[B^{1+r}(AB^r)^sA^{2sa}B^{2sb},(AB^r)^{1+s}A^{2si}B^{2sj}]} \\
&\equiv (A^{s+2sa-u\ell}B^{1+r+2sb+sr-u\overline{r}\ell}C^{s(\overline{r}-1)-2sa-sr+u(\ell-a)})^{C^{-1-r-s+sr-2s(i+b)-u(\overline{r}+i+a+1)}B^{-sr\ell-u(\overline{r}+1)}A^{-u}} \\
&\equiv (A^{s+2sa-u\ell}B^{1+r+2s(b+\ell)+sr-u\overline{r}\ell}C^{s(\overline{r}-1)-2sa-sr+u(\ell-a)})^{B^{-sr\ell-u(\overline{r}+1)}A^{-u}} \\
&\equiv A^{s+2sa-u\ell}B^{1+r+2s(b+\ell)+sr-u\overline{r}\ell}C^{s(\overline{r}-1)-2sa-sr+u(\ell-a+1)} \mod Z_1(J),
\end{aligned}$$

where the central element is $A^{-2u\ell(2i+3a+4b+3)-ur\ell(\overline{r}+1)-us\overline{r}+u\varphi(s)\ell+usr(\overline{r}+a)+2us}$. Then

$$\begin{aligned}
&(B^{1+r}(AB^r)^sA^{2sa}B^{2sb})^{[B^{1+r}(AB^r)^sA^{2sa}B^{2sb},(AB^r)^{1+s}A^{2si}B^{2sj}]} \\
&\quad = A^{s+2sa-u\ell}B^{1+r+2s(b+\ell)+sr-u\overline{r}\ell}C^{s(\overline{r}-1)-2sa-sr+u(\ell-a+1)} \\
&\qquad A^{-2u\ell(2i+3a+4b+3)-ur\ell(\overline{r}+1)-us\overline{r}+u\varphi(s)\ell+usr(\overline{r}+a)+2us}.
\end{aligned} \tag{6.81}$$

Finally, applying Theorem 5.10 to

$$(A^{s+2sa-u\ell}B^{1+r+2sb+sr-u\overline{r}\ell}C^{s(\overline{r}-1)-2sa-sr+u(\ell-a)})^{1+2s\ell'} = A^{\exp A}B^{\exp B}C^{\exp C}A^{\xi_4}$$

produces $\exp A \equiv s+2sa-u\ell+2u\ell'(2a+1)-us\ell\ell'+2us\ell'(a+1) \mod 4us$, $\exp B \equiv 1+r+2s(b+\ell')+sr+4ub\ell'+u(\ell'-\overline{r}\ell)+us\ell' \mod 4us$, $\exp C \equiv s(\overline{r}-1)-2sa-sr+u(\ell-a+\ell')+2ua\ell'$ mod $4u$, $\xi_4 \equiv 0 \mod 4us$, so

$$\begin{aligned}
&(B^{1+r}(AB^r)^sA^{2sa}B^{2sb})^{1+2s\ell'} \\
&\quad = (A^{s+2sa-u\ell}B^{1+r+2sb+sr-u\overline{r}\ell}C^{s(\overline{r}-1)-2sa-sr+u(\ell-a)})^{1+2s\ell'} \\
&\qquad A^{(-2u\ell a-ur\overline{r}\ell+us(\ell-\overline{r}+1)+u\varphi(s)\ell+usr(\overline{r}+a)+2us)(1+2s\ell')} \\
&\quad = A^{s+2sa-u\ell}B^{1+r+2s(b+\ell')+sr+u(\ell'-\overline{r}\ell)}C^{s(\overline{r}-1)-2sa-sr+u(\ell-a+\ell')} \\
&\qquad A^{2u(2a\ell'-\ell a-2b\ell'+\ell')-ur\overline{r}\ell+us(\ell-\overline{r}+1-\ell\ell'-\ell')+u\varphi(s)\ell+usr(\overline{r}+a)+2us(\ell'+1)}.
\end{aligned} \tag{6.82}$$

This completes the calculation of both sides of (6.61) and (6.62).

References

[1] I. D. Macdonald *On a class of finitely presented groups*, Canad. J. Math 14 (1962) 602–613.

[2] I. D. Macdonald *A computer application to finite p-groups*, J. Aust. Math. Soc. 17 (1974) 102–112.

[3] A. Montoya Ocampo and F. Szechtman *Structure of the Macdonald groups in one parameter*, J. Group Theory (2023). https://doi.org/10.1515/jgth-2023-0036

[4] A. Montoya Ocampo and F. Szechtman *The automorphism group of finite 2-groups associated to the Macdonald group*, arXiv:2308.03510

[5] A. Montoya Ocampo and F. Szechtman *The automorphism group of finite p-groups associated to the Macdonald group*, arXiv:2303.06385

[6] A. Montoya Ocampo and F. Szechtman *On the isomorphism problem for certain p-groups*, Commun. Algebra (2024). https://doi.org/10.1080/00927872.2024.2311847

[7] D. J. S. Robinson *A course in the theory of groups*, Graduate Texts in Mathematics, 80. Springer- Verlag, New York, 1980.

[8] D. L. Johnson *Presentations of groups. 2nd ed.*, London Mathematical Society Student Texts. 15. Cambridge University Press, Cambridge, 1997.

[9] D. S. Dummit and R. M. Foote *Abstract algebra. 3rd ed.*, John Wiley & Sons, Inc., United States of America, 2004.

[10] T. W. Hungerford *Algebra*, Springer-Verlag New York, Inc., 1974.

[11] I. M. Isaacs *Cyclic extensions. Class notes*, accessed 20 August 2023, https://people.math.wisc.edu/~nboston/notes4.pdf, Fall 2002.

[12] H. J. Zassenhaus *The theory of groups*, Dover, New York, 1999.

[13] J. Mennicke *Einige endliche Gruppen mit drei Erzeugenden und drei Relationen*, Arch. Math. (Basel) 10 (1959) 409–418.

[14] J. W. Wamsley *The deficiency of finite groups*, Ph.D. thesis, Univ. of Queensland (1969).

[15] E. Schenkman *A factorization theorem for groups and Lie algebras*, Proc. Am. Math. Soc. 68 (1978) 149–152.

[16] E. Jabara *Gruppi fattorizzati da sottogruppi ciclici*, Rend. Semin. Mat. Univ. Padova 122 (2009) 65–84.

[17] D. L. Johnson and E. F. Robertson *Finite groups of deficiency zero*, in Homological Group Theory (ed. C.T.C. Wall), Cambridge University Press, 1979.

[18] M. A. Albar *On Mennicke groups of deficiency zero I*, Internati. J. Math. & Math. Sci. 8 (1985) 821–824.

[19] M. A. Albar and A.-A. A. Al-Shuaibi *On Mennicke groups of deficiency zero II*, Can. Math. Bull. 34 (1991) 289–293.

[20] J. W. Wamsley *A class of three-generator, three-relation, finite groups*, Canad. J. Math. 22 (1070) 36–40.

[21] A. Previtali and F. Szechtman *A study of the Wamsley group and its Sylow subgroups*, preprint.

[22] J. W. Wamsley *A class of finite groups with zero deficiency*, Proc. Edinb. Math. Soc., II. Ser. 19 (1974) 25–29.

[23] M. L. Lewis and J. B. Wilson *Isomorphism in expanding families of indistinguishable groups*, Groups Complex. Cryptol. 4 (2012) 73–110.

[24] Y. Berkovich *Groups of prime power order, vol. 1*, Walter de Gruyter, 2008.

[25] Y. Berkovich and Z. Janko *Groups of prime power order, vol. 2*, Walter de Gruyter, 2008.

[26] Y. Berkovich and Z. Janko *Groups of prime power order, vol. 3*, Walter de Gruyter, 2011.

[27] Y. Berkovich and Z. Janko *On subgroups of finite p-groups*, Israel J. Math. 171 (2009) 29–49.

[28] C. R. Leedham-Green and S. McKay *The structure of groups of prime power order*, London Mathematical Society Monographs, 27. Oxford, Oxford University Press, 2002.

[29] R. M. Davitt *The automorphism group of a finite metacyclic p-group*, Proc. Amer. Math. Soc. 25 (1970) 876–879.

[30] J. Dietz *Automorphisms of p-groups given as cyclic-by-elementary Abelian central extensions*, J. Algebra 242 (2001) 417–432.

[31] M. Golasiński and D. Gonçalves *On automorphisms of split metacyclic groups*, Manuscripta Math. 128 (2009) 251–273.

[32] J. N. S. Bidwell and M. J. Curran *The automorphism group of a split metacyclic p-group*, Arch. Math. (Basel) 87 (2006) 488–497.

[33] M. J. Curran *The automorphism group of a split metacyclic 2-group*, Arch. Math. (Basel) 89 (2007) 10–23.

[34] M. J. Curran *The automorphism group of a nonsplit metacyclic p-group*, Arch. Math. (Basel) 90 (2008) 483–489.

[35] I. Malinowska *The automorphism group of a split metacyclic 2-group and some groups of crossed homomorphisms*, Arch. Math. (Basel) 93 (2009) 99–109.

[36] I. Malinowska *On the structure of the automorphism group of a minimal nonabelian p-group (metacyclic case)*, Glas. Mat. 47(67) (2012) 153–164.