APPROVAL PAGE FOR GRADUATE THESIS OR PROJECT

GS-13

SUBMITTED IN PARTIAL FULFILLMENT OF REQUIREMENTS FOR DEGREE OF MASTER OF SCIENCE AT CALIFORNIA STATE UNIVERSITY, LOS ANGELES BY

Ahmed Al Fares
Candidate

Mathematics
Department

TITLE: **SEMIDIRECT PRODUCT OF THE INTEGERS MODULO TWO**

APPROVED:

Dr. Mike Krebs Committee Chairperson	Signature
Dr. Gary Brookfield Faculty Member	Signature
Dr. Anthony Shaheen Faculty Member	Signature
Dr. Grant Fraser Department Chairperson	Signature

DATE: **June 05, 2014**

SEMIDIRECT PRODUCT OF THE INTEGERS MODULO TWO

A Thesis

Presented to

The Faculty of the Department of Mathematics

California State University, Los Angeles

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

in

Mathematics

By

Ahmed Al Fares

June 2014

ABSTRACT

Semidirect Product of

The Integers Modulo Two

By

Ahmed Al Fares

This thesis concerns the existence of 2-groups with certain derived length, with a specified order of the quotient subgroups. Let a, b, c be positive integers. We will show that there exists a finite 2-group G of derived length 3 such that $|G/G'| = 2^a$ and $|G'/G''| = 2^b$ and $|G''/G'''| = 2^c$ if

(1) $a \geq 3$ and $b = 3$, or

(2) $a \geq 5$ and $b \geq 4$.

In another thesis E. Golvin is showing a statement stronger than the converse the theorem in the above paragraph. More specifically, he shows that: "If G is a finite 2-group with derived length 3, then a_G and b_G are both at least 3." The integers a_G and b_G are defined to be $a_G = \log_2 |G/G'|$ and $b_G = \log_2 |G'/G''|$.

TABLE OF CONTENTS

Abstract iii

Chapter

1. Introduction 1

2. Background 4

3. Case One of the Main Theorem 15

4. The Even Case 27

5. Higher Order Quotient Groups 40

References 50

CHAPTER 1

Introduction

Group theory is a subfield of abstract algebra that deals with the structure of certain objects called groups. In mathematics, a group could be described as a complete collection of symmetries of some object. For example, if we take an equilateral triangle to be this object, then some of the things in that collection will be a reflection of that triangle and a one hundred and twenty degree rotation of it in addition to other things. Different groups have different elements and have different sizes. They also differ in the way they are constructed. Group theory is vastly used in mathematics to answer many different questions, some directly related to group theory, others from other fields of mathematics. One big question is, what are the possible structures of groups of a given order?

This thesis centers around the following question: For a finite 2-group G of derived length 3, what are the possible orders of G/G', G'/G'', and G''/G'''? The meanings of the technical terms are going to be introduced later on in chapter 2.

The main theorems, Theorems 5.9 and 5.10, of this paper are the following:

For a finite group G, define:

$$a_G = \log_2 |G/G'|$$

$$b_G = \log_2 |G'/G''|$$

$$c_G = \log_2 |G''/G'''|$$

Let a, b, c be positive integers.

(1) If $a \geq 3$ and $b = 3$, then there exists a finite 2-group G with derived length 3 such that $a_G = a$ and $b_G = b$ and $c_G = c$. (Theorem 5.9)

(2) If $a \geq 5$ and $b \geq 4$, then there exists a finite 2-group G with derived length 3 such that $a_G = a$ and $b_G = b$ and $c_G = c$. (Theorem 5.10)

This theorem is an existence theorem, so it will be proved by construction. The construction involves semidirect products and wreath products. One of the tools or tricks that we'll be using to quickly find elements in the commutator subgroup is a theorem by Miller [6] from 1977. This theorem allows us to find elements in the commutator subgroup of a semidirect product.

There is other work that has been done in this area. In a companion thesis, Golvin gives a proof of the following theorem: If G is a finite 2-group with derived length 3, then a_G and b_G are both at least 3 ([8]). P. Hall proves that $a_G \geq 2$ and $b_G \geq 3$, and a proof that $a_G \neq 2$ can be found in Gorenstein ([5], [7]).

The question remains open in the cases where $a = 3, 4$ and $b \geq 4$. More effort will have to be made to prove or disprove the following conjecture:

Let a, b, c be positive integers. Then there exists a finite 2-group G with derived length 3 such that $a_G = a$ and $b_G = b$ and $c_G = c$ if and only if a and b are both at least 3.

An interesting thing about groups is: "There is a folklore conjecture asserting that almost all finite groups are 2-groups: the fraction of isomorphism classes of 2-groups among isomorphism classes of groups of order at most n is thought to tend to 1 as n tends to infinity. For instance, of the $49,910,529,484$ different groups of order

at most 2000, 49, 487, 365, 422, or just over 99%, are 2-groups of order 1024" (Besche, Eick & O'Brien 2002) ([9], [10]).

The papers [2], [3], [4], and [5] all contain results relevant to the derived series of finite p-groups.

CHAPTER 2

Background

This chapter will give a brief background about the basic facts and definitions that we'll need throughout this thesis. The reader is assumed to have some basic knowledge from abstract algebra and group theory. A good reference is the Dummit and Foote, Abstract Algebra textbook [1].

Definition 2.1. *Let G be a set with a binary operation $*$ that combines any two elements $a, b \in G$ to form another element $a * b$. Then $(G, *)$ is a* **group** *if it satisfies the following four axioms:*

(1) *If $a, b \in G$, then $a * b \in G$. (Closure)*

(2) *For any $a, b, c \in G, (a * b) * c = a * (b * c)$. (Associativity)*

(3) *There is an element $e \in G$ such that for any $a \in G, e * a = a * e = a$. (Identity element)*

(4) *For each $a \in G$, there exists an element $b \in G$ such that $a * b = b * a = e$. (Inverse element)*

Definition 2.2. *A subset H of a group G is said to be a* **subgroup** *if H forms a group with the same operation. We write $H \leq G$ to mean that H is a subgroup of G.*

Definition 2.3. *A subgroup H of a group G is said to be a* **normal subgroup** *in G if for any $g \in G$ we have $gH = Hg$. We write $H \trianglelefteq G$ to mean H is a normal subgroup of G.*

Definition 2.4. *If G and H are groups, the* **direct product** *$G \times H$ is defined as follows:*

(1) $G \times H = \{(a, b) \ : \ a \in G, b \in H\}$.

(2) *The binary operation on $G \times H, *$, is defined as*

$$(g_1, h_1) * (g_2, h_2) = (g_1 * g_2, h_1 * h_2).$$

Definition 2.5. *If $(G, *)$ and $(H, \square)$ are two groups and $f : (G, *) \to (H, \square)$ is a function, we say that f is a* **homomorphism** *if*

$$f(g_1 * g_2) = f(g_1) \square f(g_2) \text{ for all } g_1, g_2 \in G.$$

If the homomorphism f is bijective (one-to-one and onto), we say that f is an **isomorphism** *from G to H.*

Definition 2.6. *An isomorphism from a group G into itself is called* **automorphism**. *The set of all automorphisms from G into G is denoted as $Aut(G)$.*

Remark 2.7. *The set of automorphisms from G into itself, $Aut(G)$, under composition forms a group.*

Definition 2.8. *Take two groups, G and H. Let $\phi : H \to Aut(G)$ be a group homomorphism. The* **semidirect product** *of the groups G and H with respect to ϕ is the set $(G \times H, *)$ where the binary operation $*$ is defined as follows:*

$$(g_1, k_1) * (g_2, k_2) = (g_1[\phi(k_1)](g_2), k_1k_2) \text{ for any } (g_1, k_1), (g_2, k_2) \in G \times H.$$

It is denoted as $G \rtimes_\phi H$.

Theorem 2.9. *The semidirect product of two groups* $G \rtimes H$*, defined in Definition 2.8, is a group.*

Proof. We'll show that the four group properties, from Definition 2.1, are true for the set $G \rtimes H$. First, recall that

$$G \rtimes_\phi H = \{(g, h) \colon g \in G \text{ and } h \in H\}, \text{ where}$$

$$\phi \colon H \to Aut(G) \text{ is a group homomorphism.}$$

Also, recall that the binary operation is $*$ which is defined by,

$$(g_1, h_1) * (g_2, h_2) = (g_1[\phi(h_1)](g_2), h_1h_2) \text{ for any } (g_1, h_1), (g_2, h_2) \in G \times H.$$

(1) Let $(g_1, h_1), (g_2, h_2) \in G \rtimes_\phi H$. We want to show that $(g_1, h_1) * (g_2, h_2) \in G \times H$.

$$\begin{aligned}(g_1, h_1) * (g_2, h_2) &= (g_1[\phi(h_1)](g_2), h_1h_2) \\ &= (g_1k, h_1h_2)\end{aligned}$$

for some $k \in G$ such that $k = \phi(h_1)(g_2)$. This is an element of G because $\phi(h_1)$ is an element of $Aut(G)$ and it sends elements of G to elements of G. Therefore it will send g_2 to an element of G, which means that $k \in G$. This means that $(g_1, h_1) * (g_2, h_2) \in G \times H$.

(2) Let $(g_1, h_1), (g_2, h_2), (g_3, h_3) \in G \times H$. Then

$$\begin{aligned}(g_1, h_1) * [(g_2, h_2) * (g_3, h_3)] &= (g_1, h_1) * (g_2[\phi(h_2)](g_3), h_2h_3) \\ &= (g_1[\phi(h_1)](g_2[\phi(h_2)](g_3)), h_1h_2h_3) \\ &= (g_1[\phi(h_1)](g_2)[\phi(h_1h_2)](g_3), h_1h_2h_3) \\ &= (g_1[\phi(h_1)](g_2), h_1h_2) * (g_3, h_3) \\ &= [(g_1, h_1) * (g_2, h_2)] * (g_3, h_3)\end{aligned}$$

This shows that $G \times H$ is associative.

(3) The identity element of $G \times H$ is $(1_G, 1_H)$ where 1_G is the identity element of the group G, and 1_H is the identity element of the group H. For any $(g, h) \in G \times H$ we have:

$$\begin{aligned}(g, h) * (1_G, 1_H) &= (g[\phi(h)](1_G), h1_H) \\ &= (g1_G, h1_H) \\ &= (g, h);\end{aligned}$$

and also

$$\begin{aligned}(1_G, 1_H) * (g, h) &= (1_G[\phi(1_H)](g), 1_Hh) \\ &= (1_Gg, 1_Hh) \\ &= (g, h).\end{aligned}$$

This gives us the equation $(g, h)(1_G, 1_H) = (1_G, 1_H)(g, h) = (g, h)$. Hence, $(1_G, 1_H)$ is the identity element of $G \times H$.

(4) We claim that the inverse element of $(g, h) \in G \times H$ is the element $([\phi(h^{-1})](g^{-1}), h^{-1})$.

To see this, we follow the equation

$$\begin{aligned}(g,h)*([\phi(h^{-1})](g^{-1}),h^{-1}) &= (g[\phi(h)]([\phi(h^{-1})](g^{-1})),hh^{-1}) \\ &= (gg^{-1},hh^{-1}) \\ &= (1_G,1_H).\end{aligned}$$

Conversely,

$$\begin{aligned}([\phi(h^{-1})](g^{-1}),h^{-1})*(g,h) &= ([\phi(h^{-1})](g^{-1})[\phi((h^{-1})](g),h^{-1}h) \\ &= (1_G,1_H).\end{aligned}$$

This latter equation is saying that if the map $\phi(h^{-1})$ sends g to an element, it will send g^{-1} to the inverse of that element. This is true because $\phi(h^{-1}]$ is a group homomorphism. Therefore, the inverse of an element $(g,h) \in G \times H$ is $([\phi(h^{-1})](g^{-1}),h^{-1})$.

Hence, we conclude the proof; and so, $G \rtimes_\phi H = (G \times H, *)$ is a group. □

Definition 2.10. *Let G and H be two groups and let $\phi : G \to H$ be a homomorphism. Then the* **kernel** *of ϕ is the set $Ker(\phi) = \{g \in G : \phi(g) = 1_H\}$, where 1_H is the identity element of H.*

Definition 2.11. *Let n be a positive integer, and take two groups G and H. Let $\psi : H \to S_n$ be a homomorphism, where S_n is the symmetric group of n letters. Let G^n denote the direct product of n copies of G. We'll denote $\psi(h)(1)$ by $h \cdot 1$, $\psi(h)(2)$ by $h \cdot 2$, etc. Define $\phi : H \to Aut(G^n)$ by*

$$\phi(h)(g_1,\ldots,g_n) = (g_{(h\cdot 1)},\ldots,g_{(h\cdot n)}).$$

Then $G^n \rtimes H$ is a **wreath product**. *We denote the wreath product $G^n \rtimes_\phi H$ by $G \wr_\psi H$.*

Remark 2.12. *For the semidirect product, if the group homomorphism is clear from the context then we can write $G \rtimes_\phi H$ simply as $G \rtimes H$. The special case of the wreath product is no different, i.e. it could also be simply denoted by $G \wr H$.*

Remark 2.13. *The map from Definition 2.11, $\phi : H \to Aut(G)$ defined by*

$$\phi(h)(g_1, \ldots, g_n) = (g_{(h\cdot 1)}, \ldots, g_{(h\cdot n)})$$

is a homomorphism.

Proof. We'll use the same names of the functions as defined in Definition 2.11. So, let $\psi\colon H \to S_n$ be a homomorphism, and, as in the definition, $\psi(h)(j)$ will be denoted by $h \cdot j$ for all j such that $1 \leq j \leq n$. As above, ϕ will be defined from H to $Aut(G^n)$ by

$$\phi(h)(g_1, \ldots, g_n) = (g_{(h\cdot 1)}, \ldots, g_{(h\cdot n)}).$$

We also want to recall that the group law in S_n is function composition. That is, if $h, k \in S_n$, then $hk = h \circ k$. Now, we want to show that for $h, k \in H$, we have $\phi(hk)(g_1, \ldots, g_n) = \phi(h) \circ \phi(k)(g_1, \ldots, g_n)$.

$$\begin{aligned}
\phi(hk)(g_1, \ldots, g_n) &= (g_{(hk)\cdot 1}, \ldots, g_{(hk)\cdot n}) \\
&= (g_{h\cdot(k\cdot 1)}, \ldots, g_{h\cdot(k\cdot n)}) \\
&= \phi(h)(g_{k\cdot 1}, \ldots, g_{k\cdot n}) \\
&= \phi(h)(\phi(k)(g_1, \ldots, g_n)) \\
&= \phi(h) \circ \phi(k)(g_1, \ldots, g_n)
\end{aligned}$$

Therefore, the map $\phi(h)$ is a homomorphism. □

Theorem 2.14. *Let G and H be groups, and let $\phi : G \to H$ be a group homomor-*

phism. If the kernel of ϕ is K, then $K \leq G$, and further, we can conclude that $K \trianglelefteq G$.

Proof. First, we'll show that K is a subgroup of G. Since ϕ is an isomorphism, then we know that it will send the identity element of G, that is, 1_G to 1_H, the identity element of H. Suppose that $g_1, g_2 \in K$, then $\phi(g_1 g_2) = 1_H 1_H = 1_H$, hence K is closed under the operation of G. We also know that for any $g \in G$, we have that $gg^{-1} = 1_G$, and so $1_H = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$ and hence, this implies that if $g \in K$, then so is g^{-1}.

To see that K is also normal in G, it is enough to show that for any arbitrary $g \in G$ we have $g^{-1}Kg \subset K$. That is, for any $k \in K$, the element $g^{-1}kg$ is also an element of K. So let $k \in K$. We'll show that $\phi(g^{-1}kg) = 1_H$. Since ϕ is a homomorphism, we have $\phi(g^{-1}kg) = \phi(g^{-1})\phi(k)\phi(g) = \phi(g^{-1})1_H\phi(g) = \phi(g)^{-1}\phi(g) = 1_H$. That shows $g^{-1}kg \in K$ which means $g^{-1}Kg \subset K$ and therefore $K \trianglelefteq G$. □

Definition 2.15. *Let G be a group and let $N \leq G$ be a subgroup. The quotient G/N is defined as follows:*

$$G/N = \{gN : g \in G\}.$$

The elements of the set G/N are called **cosets** *of N.*

Theorem 2.16. *Let G be a group, and let N be a normal subgroup of G. Equip G/N with a binary operation *, defined as follows:*

$$\textit{For any } g, h \in G, \textit{ we have } gN * hN = (gh)N.$$

Then $(G/N, *)$ is a group.

Proof. To prove this theorem, we need to check the four properties of groups mentioned in Definition 2.1.

(1) Showing that G/N is well-defined: Suppose $g_1N = g_2N$ and $h_1N = h_2N$, we'll show that $g_1h_1N = g_2h_2N$.

$$\begin{aligned} g_1h_1N &= g_1Nh_1N \\ &= g_2Nh_2N \\ &= g_2h_2N \end{aligned}$$

(2) Closure: Take two elements gN and hN in the set G/N. It is clear that $ghN \in G/N$, so the set is closed under the operation $*$.

(3) Associativity: Let $gN, hN, kN \in G/N$, then

$$\begin{aligned} (gN * hN) * kN &= (gh)N * kN \\ &= (gh)kN \\ &= g(hk)N \\ &= gN * (hk)N \\ &= gN * (hN * kN). \end{aligned}$$

So G/N is associative.

(4) Identity element: The identity element of G/N is simply $eN = N$, where e is the identity of G. To verify that, take any arbitrary element $gN \in G/N$. Then $gN * N = gN * eN = (ge)N = gN$ and similarly $N * gN = gN$. Therefore $gN * N = N * gN = gN$ and this shows that N is the identity element of G/N.

(5) Inverse: It is clear that an arbitrary element $gN \in G/N$ will have $g^{-1}N$ as its inverse, where g^{-1} is the inverse of g in the group G.

By 1-5, we can conclude that G/N is a group under the operation $*$ defined as above. □

Definition 2.17. *From a group G, take two elements g and h. Then $[g,h]$ is a called a* **commutator** *and it is defined as $[g,h] = g^{-1}h^{-1}gh$.*

Definition 2.18. *Let G be a group. The* **commutator subgroup**, *G', is defined to be the subgroup generated by the commutators $[g,h]$ where $g,h \in G$.*

Theorem 2.19. *If the group G/N is abelian, then the commutator subgroup G' is a subgroup of N.*

Proof. We want to show that $G' \leq N$. Since G/N is abelian we know that for any elements $g,h \in G$

$$hgN = ghN$$

$$N = g^{-1}h^{-1}ghN$$

From the above equation, we get that $g^{-1}h^{-1}gh \in N$. Since g and h were arbitrary, any commutator is an element of N. Since G' is generated by the commutator elements, we conclude $G' \leq N$. □

Theorem 2.20. *Let G and H be groups, and $\phi : G \to H$ be a homomorphism. Let $\phi(G)$ denote the image of G under ϕ, then $\phi(G) \leq H$.*

Proof. It suffices to show that $\phi(G)$ is not empty and that if $h_1, h_2 \in \phi(G)$, then $h_1 h_2^{-1} \in \phi(G)$. Let 1_G, 1_H denote the identities of G and H respectively.

(1) Since ϕ is a homomorphism, then $\phi(1_G) = 1_H$. Therefore $1_G \in \phi(G)$ and so $\phi(G) \neq \emptyset$

(2) Let $h_1, h_2 \in \phi(G)$, then there exist $g_1, g_2 \in G$ such that $\phi(g_1) = h_1$, $\phi(g_2) = h_2$.

Then $\phi(g_1 g_2^{-1}) = \phi(g_1)\phi(g_2)^{-1} = h_1 h_2^{-1}$ and so $h_1 h_2^{-1} \in \phi(G)$. □

Theorem 2.21 (First Isomorphism Theorem)**.** *Take two groups G and H, and let $\phi : G \to H$ be a group homomorphism. Then the quotient group $G/Ker(\phi)$, where $Ker(\phi)$ is the kernel of ϕ, is isomorphic to the image of G under ϕ.*

Proof. In the proof of this theorem, we'll assume without loss of generality that ϕ is surjective (otherwise, replace H by the image of ϕ). Let K denote $Ker(\phi)$. Define $\psi\colon G/K \to H$ by

$$\psi(gK) = \phi(g)$$

We'll first show that ψ is well defined. Let $g_1K, g_2K \in G/K$, we'll show that $\psi(g_1K) = \psi(g_2K)$. Then

$$\psi(g_1K) = \phi(g_1) = \phi(g_2) = \psi(g_2K)$$

Also, ψ is surjective. So, it remains to prove that ψ is injective. To show this note that

$$\begin{aligned} Ker(\psi) &= \{gK \in G/K\colon \psi(gK) = 1_H\} \\ &= \{gK \in G/K\colon \phi(g) = 1_H\} \\ &= \{K\} \end{aligned}$$

Therefore, ψ is also injective. Hence, ψ defines an isomorphism from G/K to the image of G under ϕ. □

Theorem 2.22. *Let G be a group and let H be a subgroup of G. Then $H' \leq G'$.*

Proof. The proof of this theorem is really straightforward. We know that H' is generated by elements of the form

$$hkh^{-1}k^{-1} \text{ such that } h, k \in H.$$

We also know that $H < G$, i.e. the elements h and k are also in G. This means any generator of H' is an element of G'. Since H' is generated by elements of the form $hkh^{-1}k^{-1}$ such that $h, k \in H$, we can conclude that $H' \leq G'$. □

Theorem 2.23. *Let G be a group. Let $\phi \in Aut(G)$ such that ϕ has order 2. Define $\psi : \mathbb{Z}_2 \to Aut(G)$ by $\psi(1) = \phi$. Let $g \in G$. Then $(g^{-1}\phi(g), 0) \in (G \rtimes_\psi \mathbb{Z}_2)'$.*

Proof. Pick the two elements $(g, 0)$ and $(e, 1)$ in the group $G \times_\psi \mathbb{Z}_2$. Then

$$\begin{aligned}
[(g,0),(e,1)] &= (g,0)^{-1}(e,1)^{-1}(g,0)(e,1) \\
&= (g^{-1},0)(e,1)(g,0)(e,1) \\
&= (g^{-1},0)([\psi(1)](g),1)(e,1) \\
&= (g^{-1},0)(\phi(g),1)(e,1) \\
&= (g^{-1},0)(\phi(g)[\psi(1)](e),0) \\
&= (g^{-1},0)(\phi(g),0) \\
&= (g^{-1}[\psi(0)](\phi(g)),0) \\
&= (g^{-1}\phi(g),0).
\end{aligned}$$

Therefore, $(g^{-1}\phi(g), 0) \in (G \rtimes_\psi \mathbb{Z}_2)'$. □

CHAPTER 3

Case One of the Main Theorem

This chapter and the next two will be the heart of this paper. In this chapter, we will prove the main theorem in the case where $a = b = 3$ and c is odd. We'll also compute the order of all the terms of the derived series (Definition 3.1) of the the group that will be constructed during the proof of Theorem 3.4.

Definition 3.1. *Let G be a group. Then the* **derived series** *of G is defined as follows:*

$G^{(0)} = G$, $G^{(1)} = [G, G]$, $G^{(2)} = [G^{(1)}, G^{(1)}]$, $\ldots$ *and further*

$$G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \ldots$$

Throughout this thesis we'll use the notation:

$$G' = G^{(1)}, G'' = G^{(2)}, G''' = G^{(3)}, \ldots$$

Definition 3.2. *Let G be a group with commutator subgroups G', G'', $\ldots$, $G^{(n)}$ such that*

$$G^{(n)} \leq G^{(n-1)} \leq \cdots \leq G'' \leq G'.$$

Then we say that G is of derived length n if and only if $G^{(n)} = \{1_G\}$ and $G^{(k)}$ is nontrivial for all $k \leq n$.

Definition 3.3. *Let G be a finite group. If the order of G is a power of 2, we say that G is a* **2-group**.

In this thesis we are using D_{2^n} to refer to the dihedral group of order 2^n. D_{2^n} is defined to be the group of symmetries of a regular polygon with 2^n sides. Consider

the polygon in the complex plane whose vertices are the 2^{n-1}th roots of unity. We refer to rotation about the origin by an angle of $2\pi/2^{n-1}$ by the letter r, and we refer to reflection across the real axis by the letter s. Then

$$D_{2^n} = \langle r, s : r^{2^{n-1}} = e, s^2 = e, rs = sr^{-1} \rangle.$$

$$= \quad \{r^a s^b : 0 \leq a \leq 2^{n-1}, b = 0, 1\}.$$

The group D_{2^n} is a group of order 2^n, i.e. a 2-group (see Definition 3.3).

For the remainder of this chapter, take G to be $D_{2^n} \wr \mathbb{Z}_2$, where the wreath product is given by the map ϕ_1 which we define by

$$\phi_1 : \mathbb{Z}_2 \to S_2 \text{ by } \phi_1(1) = (1\ 2),$$

where (1 2) is cycle notation for the element of S_2 that interchanges 1 and 2.

Now, using this map, ϕ_1, we'll compute the commutator subgroups G', G'' and G'''. Then we'll also compute the quotient groups G/G', G'/G'' and G''/G''' and their orders.

Theorem 3.4. *Let n be an integer with $n \geq 3$. Then the group G defined above is a 2-group that has order 2^{2n+1} and derived length 3. Also, we have that $|G/G'| = 8$ and $|G'/G''| = 8$ and $|G''/G'''| = 2^{2n-5}$.*

Proof. We'll start by claiming that the commutator subgroup G' is as follows:

$$G' = \{((r^a s^b, r^c s^d), 0) : a + c \text{ and } b + d \text{ are even}\}$$

Lemma 3.5. *$G' = \{(r^a s^b, r^c s^d, e) : a + c$ is even and $b + d$ is even, $e = 0\}$.*

Proof. Let's start by letting

$$K = \{(r^a s^b, r^c s^d, e) : a + c \text{ is even and } b + d \text{ is even}, e = 0\}.$$

Define $f\colon G \to \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ by

$$f((r^a s^b, r^c s^d), e) = (a + c, b + d, e) \ (mod\ 2).$$

First, note that a and c are defined mod 2^{n-1}, and b and d are defined mod 2. So, f is a well-defined function. Now we'll show that f is a homomorphism. Let $((r^a s^b, r^c s^d), e), ((r^m s^n, r^u s^v), w) \in G$, then we have

$$\begin{aligned}(1)\ f((r^a s^b, r^c s^d), e) f((r^m s^n, r^u s^v), w) &= (a + c, b + d, e) + (m + u, n + v, e + w) \\ &= (a + c + m + u, b + d + n + v, e + w).\end{aligned}$$

$$\begin{aligned}(2)\ f((r^a s^b, r^c s^d), e)(r^m s^n, r^u s^v), w)) &= f((r^a s^b r^m s^n, r^c s^d r^u s^v), w + e) \\ &= f((r^{a+(-1)^b m} s^{b+n}, r^{c+(-1)^d u} s^{d+v}), e + w) \\ &= (a + (-1)^b m + c + (-1)^d u, b + n + d + v, e + w).\end{aligned}$$

To see that the element from (1) is the same as the one from (2) note that the second and the third components of $(a + c + m + u, b + d + n + v, e + w)$ and $(a + (-1)^b m + c + (-1)^d u, b + n + d + v, e + w)$ are the same. To see that $a + c + m + u$ is the same as $a + (-1)^b m + c + (-1)^d u \ mod\ 2$ we check the 4 cases:

(1) If $b = d = 0$, then $a + (-1)^b m + c + (-1)^d u = a + m + c + u = a + c + m + u$.

(2) If $b = 0$, $d = 1$, then $a + (-1)^b m + c + (-1)^d u = a + m + c - u \equiv a + c + m + u \ mod\ 2$.

(3) If $b = 1$, $d = 0$, then $a + (-1)^b m + c + (-1)^d u = a - m + c + u \equiv a + c + m + u \ mod\ 2$.

(4) Id $b = d = 1$, then $a + (-1)^b m + c + (-1)^d u = a - m + c - u \equiv a + c + m + u \ mod\ 2$.

So f is a homomorphism. Now the kernel of the function f will be

$$\begin{aligned} Ker(f) &= \{((r^a s^b, r^c s^d), e) \colon a + c \equiv 0 \ (mod\ 2) \text{ and } b + d \equiv 0 \ (mod\ 2), e = 0\} \\ &= \{((r^a s^d, r^c s^d), 0) \colon a + c \text{ and } b + d \text{ are even}\} \\ &= K. \end{aligned}$$

We'll show that $G' = K$.

(1) Showing $K \leq G'$.

Let's first compute several of the elements of the the group G'.

$$\begin{aligned} ((r^{-1}, e), 0) \cdot ((e, e), 1) \cdot ((r^{-1}, e), 0)^{-1} \cdot ((e, e), 1)^{-1} &= (r^{-1}, e) \cdot 1 \cdot (r, e) \cdot 1 \\ &= (r^{-1}, e) \cdot (e, r) \\ &= (r^{-1}, r) \\ &= ((r^{-1}, r), 0) \in G' \end{aligned}$$

Therefore, $((r^{-1}, r), 0)^{-1} = ((r, r^{-1}), 0) \in G'$. Another element

$$\begin{aligned} ((s, e), 0)((e, e), 1)((s, e), 0)((e, e), 1) &= (s, e) \cdot 1 \cdot (s, e) \cdot 1 \\ &= (s, e) \cdot (e, s) \\ &= (s, s) \\ &= ((s, s), 0) \in G'; \end{aligned}$$

Another element of G' is $((rs, rs), 0)$ as

$$\begin{aligned}((r,s),0)\cdot 1\cdot((r^{-1},s),0)\cdot 1 &= (r,s)(s,r^{-1})\\ &= (rs, sr^{-1})\\ &= (rs, rs)\\ &= ((rs,rs),0).\end{aligned}$$

Here, we are using 1 to mean $((e, e), 1)$.

Multiplying the two elements $((rs, rs), 0)$ and $((s, s), 0)$ we get,

$$((rs,rs),0)((s,s),0) = ((r,r),0) \in G' \text{ and so } ((r^{-1},r^{-1}),0) \in G'.$$

One can notice that all the elements that we computed so far are already elements of the group we called K at the beginning of this proof. Therefore, we'll use these facts to show that $K \leq G'$.

Now, we want to show show that if $a + c$ is even then we have $((r^a, r^c), 0)$ is in G'. Let give some of the elements we computed above names. Let

$$x = ((r, r^{-1}), 0),$$

$$y = ((r, r), 0),$$

$$z = ((s, s), 0).$$

Because $a + c$ is even, it follows that $a - c$ is also even. Let $k = (a + c)/2$ and

$j = (a - c)/2$. Then we get the following:

$$\begin{aligned}((r^a, r^c), 0) &= ((r^{k+j}, r^{k-j}), 0) \\ &= ((r^k r^j, r^k (r^{-1})^j), 0) \\ &= ((r^j, (r^{-1})^j), 0)((r^k, r^k), 0) \\ &= ((r, r^{-1}), 0)^j ((r, r), 0)^k \\ &= x^j \cdot y^k.\end{aligned}$$

So, this shows that any element of the form $((r^a, r^c), 0)$, with $a + c$ being even is an element of G'. For elements of the form $((r^a s, r^c s), 0)$, where $a + c$ is even, we can easily see that

$$\begin{aligned}((r^a s, r^c s), 0) &= ((r^a, r^c), 0)((s, s), 0) \\ &= x^j \cdot y^k \cdot z,\end{aligned}$$

where k and j are as defined in the equation of $((r^a, r^c), 0)$. This shows any element of the form $((r^a s, r^c s), 0)$ is an element of G'. Hence $K \leq G'$.

(2) Showing $G' \leq K$

By the first isomorphism theorem, Theorem 2.21, we know that G/K is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. This implies that G/K is abelian. Hence, by Theorem 2.19 and Theorem 2.21, we conclude that $G' \leq K$.

From (1) and (2) we, therefore, get that $G' = K$. □

Getting back to the proof of Theorem 3.4, we'll now use the first isomorphism theorem, Theorem 2.21, to compute $|G/G'|$. First, we note that $f(G)$, the image of G

under f, is $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Second, by the first isomorphism theorem, we know that $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ is isomorphic to the group G/G', since G' is the kernel of f. Therefore, $|G/G'| = 8$.

Now, we'll compute a couple of elements of G'', which is the commutator subgroup of G'. Before doing that, and since the elements of G' always have the form $((r^a s^b, r^c s^d), 0)$ with $a + c$ and $b + d$ both even, we'll use the shortcut $(r^a s^b, r^c s^d)$ to refer to $((r^a s^b, r^c s^d), 0)$ in the following computations.

$$\begin{aligned}(r,r)(s,s)(r^{-1},r^{-1})(s,s) &= (rsr^{-1}s, rsr^{-1}s)\\ &= (r^2, r^2).\end{aligned}$$

We also get $(r^{-2}, r^{-2}) \in G''$, as $G'' \leq G'$ by Theorem 2.17, so it is closed under taking inverses. Another element of G'' is

$$\begin{aligned}(e,r^{-2})(s,s)(e,r^2)(s,s) &= (eses, r^{-2}sr^2s)\\ &= (ss, r^{-2}r^{-2}ss)\\ &= (e, r^{-4}) \in G''.\end{aligned}$$

From these two elements we can get

$$\begin{aligned}(e,r^{-4})(r^2,r^2) &= (er^2, r^{-4}r^2)\\ &= (r^2, r^{-2}) \in G''.\end{aligned}$$

Lemma 3.6. *We claim that*

$$G'' = \{(r^a, r^c) \colon a \text{ and } c \text{ are both even and } a + c \equiv 0 (mod\ 4)\}.$$

Proof. Let $H = \{(r^a, r^c) \colon a \text{ and } c \text{ are both even and } a + c \equiv 0 (mod\ 4)\}$. Then we

want to show that $G'' = H$. We'll prove this theorem by showing that $H \subset G''$ first, and then that $G'' \subset H$.

(1) First, we'll show that $H \subset G''$.

From the work that was done just before the statement of this lemma, we can see that many of the elements of H are also in G''. We, specifically, showed that the two elements

$$x = (r^2, r^{-2}) \text{ and } y = (r^2, r^2)$$

are elements of G''. This means that it is enough to show that any element of the form (r^a, r^c), satisfying (1) a and c are both even, and (2) $a + c \equiv 0 \ (mod\ 4)$, can be generated by the elements x and y, as defined above. So, pick an element $(r^a, r^c) \in H$. Then, since both a and c are even, we can find two integers n and m such that

$$a = 2j \text{ and } c = 2m.$$

We also know that $a + b \equiv 0 \ (mod\ 4)$. This means that we can find an element $k \in \mathbb{Z}$ such that

$$a + c = 4k$$

$$2j + 2m = 4k$$

$$2(j + m) = 4k$$

$$j + m = 2k.$$

Let

$$q = k - m$$

Using this information, we get the following

$$\begin{aligned}(r^a, r^c) &= (r^{2j}, r^{2m}) \\ &= (r^j, r^m)^2 \\ &= (r^{k+q}, r^{k-q})^2 \\ &= (r^k r^q, r^k (r^{-1})^q)^2 \\ &= (r^k, r^k)^2 (r^q, (r^{-1})^q)^2 \\ &= (r, r)^{2k} (r, r^{-1})^{2q} \\ &= (r^2, r^2)^k (r^2, r^{-2})^q \\ &= x^k y^q \end{aligned} \tag{3.1}$$

This last equation, Equation 3.1, shows that any element of H can be generated using only the two elements x and y. This implies that x and y generate H. Since we know by the work done right above Lemma 3.6 that $x \in G''$ and $y \in G''$, we know that the whole set H is contained in G'', i.e. $H \subset G''$.

(2) Showing $G'' \subset H$.

Define $g\colon G' \to \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ by

$$g(r^a s^b, r^c s^d) = (a, (a+c)/2, b) \ mod\ 2.$$

We'll first show that g is a homomorphism. Let $(r^a s^b, r^c s^d), (r^m s^n, r^u s^v) \in G'$, then

$$\begin{aligned}(1)\ g(r^a s^b, r^c s^d) g(r^m s^n, r^u s^v) &= (a, (a+c)/2, b) + (m, (m+u)/2, n) \\ &= (a+m, (a+c+m+u)/2, b+n).\end{aligned}$$

(2) $g((r^a s^b, r^c s^d) \cdot (r^m s^n, r^u s^v)) = g(r^a s^b r^m s^n, r^c s^d r^u s^v)$

$$= g(r^{a+(-1)^b m} s^{b+n}, r^{c+(-1)^d u} s^{d+v})$$

$$= (a + (-1)^b m, (a + (-1)^b m + c + (-1)^d u)/2, b + n)$$

Then, going through the same cases when proving that f (from Lemma 3.5), we can conclude that g is a homomorphism. Now, the kernel of g is

$$Ker(g) = \{(r^a s^b, r^c s^d) \in G' \colon b = d = 0, a \text{ is even}, (a + c)/2 \text{ is even}\}$$

$$= \{(r^a, r^c) \in G' \colon a \equiv 0 \ (mod\ 2), (a + c)/2 \equiv 0 \ (mod\ 2)\}$$

$$= \{(r^a, r^c) \in G' \colon a = 2k \text{ for some integer } k \text{ and } (a + c)/2 = 2n \text{ for some integer } n\}$$

$$= \{(r^a, r^c) \in G' \colon a = 2k \text{ for some integer } k \text{ and } a + c = 4n \text{ for some integer } n\}$$

$$= \{(r^a, r^c) \in G' \colon a \text{ and } c \text{ are even, and } a + c = 4n \text{ for some integer } n\}$$

$$= \{((r^a, r^c), 0) \colon a \text{ and } c \text{ are even, and } a + c \equiv 0 \ (mod\ 4)\}$$

$$= H.$$

In the first equation, we know that $b = d = 0$ because $b+d$ has to be even. Therefore, by Theorems 2.19 and 2.21, we know that the commutator subgroup of the domain of g is a subset of $Ker(g) = H$. Hence $G'' \subset H$. From (1) and (2) we get that $G'' = H = Ker(g)$. □

By Lemma 3.6 above we know that

$$G'' = \{((r^a, r^c), 0) \colon a \text{ and } c \text{ are even, and } a + c \equiv 0 \ (mod\ 4)\}.$$

We also know that G'' is the kernel of the function g defined in the second part of the above proof. Then by the first isomorphism theorem, Theorem 2.21, we can

conclude that the image of G' under g is isomorphic to the quotient group G'/G''. The function g is onto, which means that $g(G') = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Therefore, we get that $|G'/G''| = 8$.

Before jumping to computing G''', here is a remark

Remark 3.7. *The fact that n has to be at least three was necessary for g, above, to be well-defined. This is because that both a and c are defined mod $2^{(n-1)}$, which means that $(a+c)/2$ is well-defined mod 2 if and only if $n \geq 3$.*

Back to computing G''', we want to show that $|G''/G'''| = 2^{2n-5}$. Pick any two elements of G'', say (r^a, r^c) and (r^k, r^n). Then by commutating these two elements we get the following:

$$\begin{aligned}(r^a, r^c)(r^k, r^n)(r^a, r^c)^{-1}(r^k, r^n)^{-1} &= (r^a, r^c)(r^k, r^n)(r^{-a}, r^{-c})(r^{-k}, r^{-n}) \\ &= (r^a r^k r^{-a} r^{-k}, r^c r^n r^{-c} r^{-n}) \\ &= (r^a r^{-a} r^k r^{-k}, r^c r^{-c} r^n r^{-n}) \\ &= (e, e).\end{aligned}$$

This is true for any two arbitrary elements of G'', which means that $G''' = \{((e,e),0)\}$ is the trivial subgroup of G. To see what the order of G''/G''' is, we'll compute the order of the subgroups G', G'' and G''' first. For the commutator subgroup of G, that is G', we have that

(1) The order of G/G' is 8, as shown in Lemma 3.5.

(2) The order of the group $G = D_{2^n} \wr \mathbb{Z}_2$ is 2^{2n+1}.

(3) By (1) and (2), we get

$8 = |G/G'| = |G|/|G'| \Rightarrow |G'| = |G|/8 = (2^{2n+1})/8 = 2^{2n-2}$.

To find the order of G'', we note that

(1) The order of G'/G'' is 8, as shown in Lemma 3.6.

(2) The order of G' is, as shown above, 2^{2n-2}.

(3) By (1) and (2), we get

$8 = |G'/G''| = |G'|/|G''| \Rightarrow |G''| = (2^{2n-2})/8 = 2^{2n-5}$.

Now, we know that G''' is the trivial group. This means that $|G''/G'''| = |G''| = 2^{2n-5}$.

□

CHAPTER 4

The Even Case

So far we have proved Theorem 3.4 (one case of the two main theorems 5.9 and 5.10), which is the case where $a = b = 3$ and c is odd. This chapter will be dealing with the other case, where c is even.

Theorem 4.1. *Let a, b, c be positive integers where a=b=3 and c is even. Then there exists a finite 2-group G with derived length 3 such that $|G/G'| = 2^a$ and $|G'/G''| = 2^b$ and $|G''/G'''| = 2^c$.*

Proof. Let $n \geq 3$ be an integer. To prove this theorem, let $H = D_{2^n} \wr \mathbb{Z}_2$ (the group G constructed in Theorem 3.4) and

$$x_1 = ((r, e), 0)$$

$$x_2 = ((s, e), 0)$$

$$x_3 = ((e, r), 0)$$

$$x_4 = ((e, s), 0)$$

$$x_5 = ((e, e), 1)$$

Then H is given as follows:

$$\begin{aligned} H = \langle x_1, x_2, x_3, x_4, x_5 | \ & x_1^{2^{n-1}} = x_2^2 = x_3^{2^{n-1}} = x_4^2 = x_5^2 = 1_H, \\ & x_2 x_1 = x_1^{-1} x_2, \\ & x_3 x_1 = x_1 x_3, \ x_3 x_2 = x_2 x_3, \\ & x_4 x_1 = x_1 x_4, \ x_4 x_2 = x_2 x_4, \ x_4 x_3 = x_3^{-1} x_4, \\ & x_5 x_1 = x_3 x_5, \ x_5 x_2 = x_4 x_5, \ x_5 x_3 = x_1 x_5, \ x_5 x_4 = x_2 x_5 \rangle \end{aligned}$$

Let $\psi\colon H \to H$ be defined by:

$$\psi(x_1) = x_1^{-1},$$

$$\psi(x_2) = x_1x_2,$$

$$\psi(x_3) = x_3^{-1},$$

$$\psi(x_4) = x_3x_4, \text{ and}$$

$$\psi(x_5) = x_5$$

We'll show that this gives a well-defined homomorphism. To show this, we'll need to verify that ψ respects all the relations listed above.

(1) Checking the relations $x_1^{2^{n-1}} = 1_H, x_2^2 = 1_H, x_3^{2^{n-1}} = 1_H, x_4^2 = 1_H, x_5^2 = 1_H$:

$$(\psi(x_1))^{2^{n-1}} = ((x_1)^{-1})^{2^{n-1}} = ((x_1^{2^{n-1}})^{-1} = (1_H)^{-1} = 1_H.$$

$$(\psi(x_2))^2 = (x_1x_2)^2 = x_1x_2x_1x_2 = x_1x_1^{-1}x_2x_2 = (x_2)^2 = 1_H.$$

$$(\psi(x_3))^{2^{n-1}} = ((x_3)^{-1})^{2^{n-1}} = (x_3^{-1})^{2^{n-1}} = (1_H)^{-1} = 1_H.$$

$$(\psi(x_4))^2 = (x_3x_4)^2 = x_3x_4x_3x_4 = x_3x_3^{-1}x_4x_4 = (x_4)^2 = 1_H.$$

$$(\psi(x_5))^2 = (x_5)^2 = 1_H.$$

(2) Checking the relation $x_2x_1 = x_1^{-1}x_2$:

$$\psi(x_2)\psi(x_1) = (x_1x_2)(x_1^{-1}) = x_1x_2x_1^{-1} = x_1x_1x_2 = x_1^2x_2.$$

$$(\psi(x_1))^{-1}\psi(x_2) = (x_1^{-1})^{-1}x_1x_2 = x_1x_1x_2 = x_1^2x_2.$$

(3) The relation $x_3x_1 = x_1x_3$:

$$\psi(x_3)\psi(x_1) = x_3^{-1}x_1^{-1} = (x_1x_3)^{-1}$$

$$\psi(x_1)\psi(x_3) = x_1^{-1}x_3^{-1} = (x_3x_1)^{-1} = (x_1x_3)^{-1} \text{ (since } x_3x_1 = x_1x_3).$$

(4) The relation $x_3x_2 = x_2x_3$:

$$\psi(x_3)\psi(x_2) = x_3^{-1}x_1x_2 = x_1x_3^{-1}x_2 = x_1x_2x_3^{-1}.$$

$$\psi(x_2)\psi(x_3) = x_1x_2x_3^{-1}.$$

(5) The relation $x_4x_1 = x_1x_4$:

$$\psi(x_4)\psi(x_1) = x_3x_4x_1^{-1} = x_3x_1^{-1}x_4 = x_1^{-1}x_3x_4.$$

$$\psi(x_1)\psi(x_4) = x_1^{-1}x_3x_4.$$

(6) The relation $x_4x_2 = x_2x_4$:

$$\psi(x_4)\psi(x_2) = x_3x_4x_1x_2 = x_3x_1x_4x_2 = x_1x_3x_2x_4 = x_1x_2x_3x_4.$$

$$\psi(x_2)\psi(x_4) = x_1x_2x_3x_4.$$

(7) The relation $x_4x_3 = x_3^{-1}x_4$:

$$\psi(x_4)\psi(x_3) = x_3x_4x_3^{-1} = x_3(x_3^{-1})^{-1}x_4 = x_3^2x_4.$$

$$(\psi(x_3))^{-1}\psi(x_4) = (x_3^{-1})^{-1}x_3x_4 = x_3^2x_4.$$

(8) The relation $x_5x_1 = x_3x_5$:

$$\psi(x_5)\psi(x_1) = x_5x_1^{-1} = x_3^{-1}x_5.$$

$$\psi(x_3)\psi(x_5) = x_3^{-1}x_5.$$

(9) The relation $x_5x_2 = x_4x_5$:

$$\psi(x_5)\psi(x_2) = x_5x_1x_2 = x_3x_5x_2 = x_3x_4x_5.$$

$$\psi(x_4)\psi(x_5) = x_3x_4x_5.$$

(10) The relation $x_5x_3 = x_1x_5$:

$$\psi(x_5)\psi(x_3) = x_5x_3^{-1} = x_1^{-1}x_5.$$

$$\psi(x_1)\psi(x_5) = x_1^{-1}x_5.$$

(11) The relation $x_5x_4 = x_2x_5$:

$$\psi(x_5)\psi(x_4) = x_5x_3x_4 = x_1x_5x_4 = x_1x_2x_5.$$

$$\psi(x_2)\psi(x_5) = x_1x_2x_5.$$

ψ respects all the relations, so ψ is a homomorphism.

Now, we'll show that ψ is bijective, i.e. that ψ is both injective and surjective. It suffices to show that ψ is its own inverse, i.e. it has order 2. So, we need to verify that $\psi(\psi(x_i)) = x_i$ for all $i = 1, 2, ..., 5$. We'll be using the fact that ψ is a homomorphism, since we already established that fact.

(1) $\psi(\psi(x_1)) = \psi(x_1^{-1}) = \psi(x_1)^{-1} = (x_1^{-1})^{-1} = x_1$.

(2) $\psi(\psi(x_2)) = \psi(x_1x_2) = \psi(x_1)\psi(x_2) = x_1^{-1}x_1x_2 = x_2$.

(3) $\psi(\psi(x_3)) = \psi(x_3^{-1}) = \psi(x_3)^{-1} = (x_3^{-1})^{-1} = x_3$.

(4) $\psi(\psi(x_4)) = \psi(x_3x_4) = \psi(x_3)\psi(x_4) = x_3^{-1}x_3x_4 = x_4$.

(5) $\psi(\psi(x_5)) = \psi(x_5) = x_5$.

With this being confirmed, now we know that ψ is an automorphism of order two from the group H to itself.

Now, we get back to the proof of the theorem. Let $G = H \rtimes_\psi \mathbb{Z}_2$. Then,

$$|G| = |H| \cdot |\mathbb{Z}_2| = 2^{2n+1} \cdot 2 = 2^{2n+2}$$

Obviously, G is a 2-group. We'll show that it has derived length three and that $|G/G'| = 8$ and $|G'/G''| = 8$ and $|G''/G'''|$ is an arbitrary even number.

Lemma 4.2. *Let* $K = \{(r^m s^n, r^u s^v, x, y) \in G \colon b + d \text{ is even}, \ e = 0, f = 0\}$. *Then,*

$K = G'$.

Proof. We want to show that $K = G'$. We'll show this in two steps.

(1) Showing $K \leq G'$.

The group H defined in the beginning of Theorem 4.1 above could be written as:

$$H = \{(r^a s^b, r^c s^d, e, f) \colon a, b, c, d, e, f \text{ are integers and } f = 0\}.$$

Then, by Lemma 3.5 we get that

$$H' = \{(r^a s^b, r^c s^d, 0, 0) \colon a + c \text{ is even and } c + d \text{ is even}\}. \tag{4.1}$$

One thing to note is that we need $n \geq 3$ to apply Theorem 3.4, because that is one of the hypotheses of Theorem 3.4.

Since $G = H \rtimes_\psi \mathbb{Z}_2$, we get that $H' \subset G'$ by Theorem 2.22. Let $x_6 = (e, e, 0, 1)$, the generator that comes from the map ψ. Then from the map ψ we get the new relations:

$$x_6 x_1 = x_1^{-1} x_6$$

$$x_6 x_2 = x_1 x_2 x_6$$

$$x_6 x_3 = x_3^{-1} x_6$$

$$x_6 x_4 = x_3 x_4 x_6$$

$$x_6 x_5 = x_5 x_6$$

From the second relation of this list of relations, we get

$$x_6 x_2 x_6 x_2 = x_1$$

and so $x_1 \in G'$. This is essentially the Miller trick—in a semidirect product of A by a cyclic group defined by a homomorphism ψ, any element of the form $\psi(a)a^{-1}$ is in

the commutator subgroup ([6]). Now the claim is that x_1 and H' generate K. If we show this, we can conclude that $K \leq G'$ using the two facts (i) $x_1 \in G'$, (ii) $H' \leq G'$. Let $(r^a s^b, r^c s^d, 0, 0)$ be an element of K, so we know that $b + d$ is an even number. Then, we have $a + c$ is either even or odd. If it is even then clearly it is an element of H' by (4.1). If $a + c$ is odd, however, then we get the following:

$$\begin{aligned}(r^a s^b, r^c s^d, 0, 0) &= (r^a, r^b, 0, 0) \text{ (if } b = d = 0) \\ &= (r, e, 0, 0)(r^{a-1}, r^c, 0, 0) \\ &= x_1(r^{a-1}, r^c, 0, 0)\end{aligned}$$

Obviously if $a + c$ is odd then $a - 1 + c = a + c - 1$ will be even which means that the element $(r^{a-1}, r^c, 0, 0)$ is an element of H'. Therefore, if $a + c$ is odd the element $(r^a s^b, r^c s^d, 0, 0)$ could be expressed as a product of x_1 and an element of H'. If we consider the case where $b = d = 1$, then we'll have

$$(r^a s^b, r^c s^d, 0, 0) = x_1(r^{a-1}, r^c, 0, 0)x_2 x_4$$

Therefore x_1, x_2, x_4 and H' generate the group K. So knowing that $H' \leq G'$ and $x_1 \in G'$, we conclude that $K \leq G'$.

(2) Showing $G' \leq K$.

Define the map $h \colon G \to \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ by

$$h(r^a s^b, r^c s^d, x, y) = (b + d, x, y) \; mod \; 2.$$

To see that h is onto, let $(\ell_1, \ell_2, \ell_3) \in \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Then $h(s^{\ell_1}, e, \ell_2, \ell_3) = (\ell_1, \ell_2, \ell_3)$. So h is surjective.

Now, we want to show that h is a homomorphism. To do this, we'll need to check

that h respects all the relations of G, which could be written as

$$\begin{aligned} G = \ \langle x_1, x_2, x_3, x_4, x_5, x_6 | \ & x_1^{2^{n-1}} = x_2^2 = x_3^{2^{n-1}} = x_4^2 = x_5^2 = x_6^2 = 1_G, \\ & x_2 x_1 = x_1^{-1} x_2, \\ & x_3 x_1 = x_1 x_3, \ x_3 x_2 = x_2 x_3, \\ & x_4 x_1 = x_1 x_4, \ x_4 x_2 = x_2 x_4, \ x_4 x_3 = x_3^{-1} x_4, \\ & x_5 x_1 = x_3 x_5, \ x_5 x_2 = x_4 x_5, \ x_5 x_3 = x_1 x_5, \ x_5 x_4 = x_2 x_5 \\ & x_6 x_1 = x_1^{-1} x_6, \ x_6 x_2 = x_1 x_2 x_6, \ x_6 x_3 = x_3^{-1} x_6, \\ & x_6 x_4 = x_3 x_4 x_6, \ x_6 x_5 = x_5 x_6 \rangle. \end{aligned}$$

(1) The relations $x_1^{2^{n-1}} = x_2^2 = x_3^{2^{n-1}} = x_4^2 = x_5^2 = x_6^2 = 1_G$.

$h(x_1)^{2^{n-1}} = 2^{n-1} \cdot (0,0,0) = (0,0,0)$.

$h(x_2)^2 = 2 \cdot (1,0,0) = (0,0,0)$.

$h(x_3)^{2^{n-1}} = 2^{n-1} \cdot (0,0,0) = (0,0,0)$.

$h(x_4)^2 = 2 \cdot (1,0,0) = (0,0,0)$.

$h(x_5)^2 = 2 \cdot (0,1,0) = (0,0,0)$.

$h(x_6)^2 = 2 \cdot (0,0,1) = (0,0,0)$.

(2) The relation $x_2 x_1 = x_1^{-1} x_2$.

$h(x_2)h(x_1) = (1,0,0) + (0,0,0) = (1,0,0)$.

$h(x_1)^{-1}h(x_2) = -(0,0,0) + (1,0,0) = (1,0,0)$.

(3) The relation $x_3 x_1 = x_1 x_3$.

$h(x_3)h(x_1) = (0,0,0) + (0,0,0) = (0,0,0)$.

$$h(x_1)h(x_3) = (0,0,0) + (0,0,0) = (0,0,0).$$

(4) The relation $x_3x_2 = x_2x_3$.

$$h(x_3)h(x_2) = (0,0,0) + (1,0,0) = (1,0,0).$$

$$h(x_2)h(x_3) = (1,0,0) + (0,0,0) = (1,0,0).$$

(5) The relation $x_4x_1 = x_1x_4$.

$$h(x_4)h(x_1) = (1,0,0) + (0,0,0) = (1,0,0).$$

$$h(x_1)h(x_4) = (0,0,0) + (1,0,0) = (1,0,0).$$

(6) The relation $x_4x_2 = x_2x_4$.

$$h(x_4)h(x_2) = (1,0,0) + (1,0,0) = (0,0,0).$$

$$h(x_2)h(x_4) = (1,0,0) + (1,0,0) = (0,0,0).$$

(7) The relation $x_4x_3 = x_3^{-1}x_4$.

$$h(x_4)h(x_3) = (1,0,0) + (0,0,0) = (1,0,0).$$

$$h(x_3)^{-1}h(x_4) = -(0,0,0) + (1,0,0) = (1,0,0).$$

(8) The relation $x_5x_1 = x_3x_5$.

$$h(x_5)h(x_1) = (0,1,0) + (0,0,0) = (0,1,0).$$

$$h(x_3)h(x_5) = (0,0,0) + (0,1,0) = (0,1,0).$$

(9) The relation $x_5x_2 = x_4x_5$.

$$h(x_5)h(x_2) = (0,1,0) + (1,0,0) = (1,1,0).$$

$$h(x_4)h(x_5) = (1,0,0) + (0,1,0) = (1,1,0).$$

(10) The relation $x_5x_3 = x_1x_5$.

$$h(x_5)h(x_3) = (0,1,0) + (0,0,0) = (0,1,0).$$

$$h(x_1)h(x_5) = (0,0,0) + (0,1,0) = (0,1,0).$$

(11) The relation $x_5x_4 = x_2x_5$.

$$h(x_5)h(x_4) = (0,1,0) + (1,0,0) = (1,1,0).$$

$$h(x_2)h(x_5) = (1,0,0) + (0,1,0) = (1,1,0).$$

(12) The relation $x_6x_1 = x_1^{-1}x_6$.

$$h(x_6)h(x_1) = (0,0,1) + (0,0,0) = (0,0,1).$$

$$h(x_1)^{-1}h(x_6) = -(0,0,0) + (0,0,1) = (0,0,1).$$

(13) The relation $x_6x_2 = x_1x_2x_6$.

$$h(x_6)h(x_2) = (0,0,1) + (1,0,0) = (1,0,1).$$

$$h(x_1)h(x_2)h(x_6) = (0,0,0) + (1,0,0) + (0,0,1) = (1,0,1).$$

(14) The relation $x_6x_3 = x_3^{-1}x_6$.

$$h(x_6)h(x_3) = (0,0,1) + (0,0,0) = (0,0,1).$$

$$h(x_3)^{-1}h(x_6) = -(0,0,0) + (0,0,1) = (0,0,1).$$

(15) The relation $x_6x_4 = x_3x_4x_6$.

$$h(x_6)h(x_4) = (0,0,1) + (1,0,0) = (1,0,1).$$

$$h(x_3)h(x_4)h(x_6) = (0,0,0) + (1,0,0) + (0,0,1) = (1,0,1).$$

(16) The relation $x_6x_5 = x_5x_6$.

$$h(x_6)h(x_5) = (0,0,1) + (0,1,0) = (0,1,1).$$

$$h(x_5)h(x_6) = (0,1,0) + (0,0,1) = (0,1,1).$$

This shows that h is also a homomorphism. The kernel of the function h defined above is:

$$\begin{aligned} Ker(h) &= \{(r^a s^d, r^c s^d, e, f) \in G \colon b + d \equiv 0 \ (mod\ 2), e = 0, f = 0\} \\ &= \{(r^a s^b, r^c s^d, 0, 0) \colon b + d \text{ is even } \} \\ &= K \end{aligned}$$

Therefore, we get that the quotient group G/K is abelian, and by Theorem 2.19 we get that $G' \leq K$.

By (1) and (2) we get that $G' = K = \{(r^a s^b, r^c s^d, e, f) \colon b + d \text{ is even}, e = 0, f = 0\}$. Further, from the function h and using the first isomorphism theorem, Theorem 2.21, we get that G/G' is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Hence $|G/G'| = 8$. □

Getting back to Theorem 4.1, we are now ready to compute the second group of the derived series of G, namely G''. We'll also start this by a claim, which will be the next lemma.

Lemma 4.3. *Let $L = \{(r^a, r^c, 0, 0) \colon a$ and c are both even$\}$. Then $L = G''$.*

Proof. We'll first show that $L < G''$. We'll first compute the following:

$$\begin{aligned}
[(r,e,0,0),(s,s,0,0)] &= (r,e,0,0)(s,s,0,0)(r^{-1},e,0,0)(s,s,0,0) \\
&= (rsr^{-1}s, eses, 0, 0) \\
&= (r^2, e, 0, 0) \\
[(e,r,0,0),(s,s,0,0)] &= (e,r,0,0)(s,s,0,0)(e,r^{-1},0,0)(s,s,0,0) \\
&= (eses, rsr^{-1}s, 0, 0) \\
&= (e, r^2, 0, 0)
\end{aligned}$$

This shows that $(r^2, e, 0, 0)$ and $(e, r^2, 0, 0)$ are elements of G'' as they are obtained from commutating elements of G'.

Now pick an element $(r^a, r^c, 0, 0)$ from L, then clearly we can write this element as

$$(r^a, r^c, 0, 0) = (r^2, e, 0, 0)^{a/2}(e, r^2, 0, 0)^{c/2}.$$

We know that this is possible as a and c are both even. Hence, $(r^a, r^c, 0, 0) \in G''$, and so $L < G''$.

To show that $G'' < L$, define the function $j\colon G' \to \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ by

$$j(r^a s^b, r^c s^d, 0, 0) = (a, b, c)\ mod\ 2 \quad .$$

Then j is a surjective homomorphism. To see that it is surjective we must prove that any element of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ will be the image of at least one element of G'. This is because that a, b, c are integers, so they are even or odd and the odd ones will map to 1 and the even ones will map to 0. This will cover all of the eight cases (as $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ has 8 elements).

To see that j is a homomorphism, pick two elements from G', say $(r^a s^b, r^c s^d, 0, 0)$ and

$(r^m s^n, r^u s^v, 0, 0)$. Then we know that $b+d, n+v$ are both even, and since

$$\begin{aligned}(r^a s^b, r^c s^d, 0, 0)(r^m s^n, r^u s^v, 0, 0) &= (r^a s^b r^m s^n, r^c s^d r^u s^v, 0, 0) \\ &= (r^{a+(-1)^b m} s^{b+n}, r^{c+(-1)^d u} s^{d+v}, 0, 0).\end{aligned}$$

We need to show

$$j(r^{a+(-1)^b m} s^{b+n}, r^{c+(-1)^d u} s^{d+v}, 0, 0) = j(r^a s^b, r^c s^d, 0, 0) \ + \ j(r^m s^n, r^u s^v, 0, 0).$$

On one hand we get

$$\begin{aligned}j(r^a s^b, r^c s^d, 0, 0) \ + \ j(r^m s^n, r^u s^v, 0, 0) &= (a, b, c) + (m, n, u) \\ &= (a+m, b+n, c+u).\end{aligned}$$

On the other hand, we have

$$\begin{aligned}j(r^{a+(-1)^b m} s^{b+n}, r^{c+(-1)^d u} s^{d+v}, 0, 0) &= (a+(-1)^b m, b+n, c+(-1)^d u) \\ &= (a \pm m, b+n, c \pm u).\end{aligned}$$

Since we are dealing with $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, then $a+m \equiv a-m \ (mod\ 2)$ and similarly for $c+u$ and $c-u$. This allows us to conclude that the function j is a homomorphism.

The kernel of j is the set L defined in the beginning of this proof, and therefore, by Theorem 2.19, we get $G'' < L$. From (1) and (2) we get $G'' = L$. □

From this lemma we get

$$G'' = \{(r^a, r^c, 0, 0) : \text{ both } a \text{ and } c \text{ are even}\}.$$

Also, from the function j and by using the first isomorphism theorem, Theorem 2.21, we get G'/G'' is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, and this tells us that $|G'/G''| = 8$. One

thing to note here that G'' is an abelian group, which means that its commutator subgroup G''' is trivial and this implies

$$\begin{aligned} 2^{2n+2} &= |G| \\ &= |G/G'||G'| \\ &= |G/G'||G'/G''||G''| \\ &= |G/G'||G'/G''||G''/G'''||G'''|. \end{aligned}$$

and so $|G''/G'''| = \frac{2^{2n+2}}{64} = 2^{2n-4}$. For c even, let $n = \frac{c+4}{2}$, and so a group of derived length 3, G, exists with $|G/G'| = 8$, $|G'/G''| = 8$ and $|G''/G'''| = 2^{2n-4}$ and clearly 2^{2n-4} is even. □

CHAPTER 5

Higher Order Quotient Groups

This last chapter of this thesis will discuss the case when we increase the values of a_G and b_G, where $a_G = \log_2 |G/G'|$ and $b_G = \log_2 |G'/G''|$ and $c_G = \log_2 |G''/G'''|$, as in the previous chapter. Specifically, we will prove that:

(1) Let a, b, and c be positive integers. If $a \geq 3$ and $b = 3$, then there exists a finite 2-group G with derived length 3 such that $a_G = a$ and $b_G = b$ and $c_G = c$. (Theorem 5.9).

(2) If a is at least 5 and b is at least 4, then there exists a finite 2-group G with derived length 3 such that $a_G = a$ and $b_G = b$ and $c_G = c$ (Theorem 5.10).

Theorem 5.1. *If G and H are two groups, then $(G \times H)' = G' \times H'$.*

Proof. The two groups $(G \times H)'$ and $G' \times H'$ are defined, in set notation, as follows:

$(G \times H)' = \langle [(g_1, h_1), (g_2, h_2)] \colon (g_1, h_1), (g_2, h_2) \in G \times H \rangle$

$G' \times H' = \langle ([g_1, g_2], [h_1, h_2]) \colon g_1, g_2 \in G, h_1, h_2 \in H \rangle$

We'll show that $(G \times H)' = G' \times H'$.

(1) Showing $(G \times H)' \subset G' \times H'$

Pick an arbitrary generator $[(g_1, h_1), (g_2, h_2)]$ from $(G \times H)'$, we'll show that it is also an element of $G' \times H'$.

$$[(g_1, h_1), (g_2, h_2)] = (g_1, h_1)(g_2, h_2)(g_1, h_1)^{-1}(g_2, h_2)^{-1}$$

$$= (g_1, h_1)(g_2, h_2)(g_1^{-1}, h_1^{-1})(g_2^{-1}, h_2^{-1})$$

$$= (g_1 g_2 g_1^{-1} g_2^{-1}, h_1 h_2 h_1^{-1} h_2^{-1}).$$

Since $g_1 g_2 g_1^{-1} g_2^{-1} \in G'$ and $h_1 h_2 h_1^{-1} h_2^{-1} \in H'$, then $(g_1 g_2 g_1^{-1} g_2^{-1}, h_1 h_2 h_1^{-1} h_2^{-1}) \in G' \times H'$. Hence $(G \times H)' \subset G' \times H'$.

(2) Showing $G' \times H' \subset (G \times H)'$

The converse follows from the above equation. If we have an element $(g_1 g_2 g_1^{-1} g_2^{-1}, h_1 h_2 h_1^{-1} h_2^{-1}) \in G' \times H'$, then this element is equal to $[(g_1, h_1), (g_2, h_2)]$ which is an element of $(G \times H)'$. Therefore, $G' \times H' \subset (G \times H)'$. From (1) and (2), we can conclude $(G \times H)' = G' \times H'$. □

Remark 5.2. *Note that the previous remark can be generalized. That is if $H^{(n)}$ denotes the nth element of the derived series of a group H, then it follows by induction on n that*

$$(G \times H)^{(n)} = G^{(n)} \times H^{(n)}.$$

Theorem 5.3. *For any finite group J, let $a_J = \log_2 |J/J'|, b_J = \log_2 |J'/J''|$, and $c_J = \log_2 |J''/J'''|$. Then a_J, b_J, and c_J are "additive," in the sense that if G and H are finite groups, then $a_{G\times H} = a_G + a_H$ and $b_{G\times H} = b_G + b_H$ and $c_{G\times H} = c_G + c_H$.*

Proof. To prove this theorem, let G and H be two finite groups. Define $J = G \times H$, then

$$a_G = \log_2 |G/G'|, b_G = \log_2 |G'/G''| \text{ and } c_G = \log_2 |G''/G'''|, \text{ and}$$

$$a_H = \log_2 |H/H'|, b_G = \log_2 |H'/H''| \text{ and } c_H = \log_2 |H''/H'''|$$

Referring back to Remarks 5.1 and 5.2, we know that $(G \times H)' = G' \times H'$ and $(G \times H)'' = G'' \times H''$.

By Theorem 5.1,

$$\begin{aligned} a_J &= a_{G\times H} \\ &= \log_2 |(G \times H)/((G \times H)')| \\ &= \log_2 |(G \times H)/(G' \times H')| \\ &= \log_2((|G| \cdot |H|)/(|G'| \cdot |H'|)) \\ &= \log_2(|G|/|G'|) + \log_2(|H|/|H'|) = a_G + a_H. \end{aligned}$$

By Remark 5.2,

$$\begin{aligned} b_J &= b_{G\times H} \\ &= \log_2 |(G \times H)'/((G \times H)'')| \\ &= \log_2 |(G' \times H')/(G'' \times H'')| \\ &= \log_2((|G'| \cdot |H'|)/(|G''| \cdot |H''|)) \\ &= \log_2(|G'|/|G''|) + \log_2(|H'|/|H''|) = b_G + b_H. \end{aligned}$$

Also by Remark 5.2,

$$\begin{aligned} c_J &= c_{G\times H} \\ &= \log_2 |(G \times H)''/((G \times H)''')| \end{aligned}$$

$$= \log_2 |(G'' \times H'')/(G''' \times H''')|$$

$$= \log_2((|G''| \cdot |H''|)/(|G'''| \cdot |H'''|))$$

$$= \log_2(|G''|/|G'''|) + \log_2(|H''|/|H'''|) = c_G + c_H. \qquad \square$$

Definition 5.4. *A* **cyclic group** *is a group that is generated by a single element. For example, $\mathbb{Z}_n$, where n is an integer is a cyclic group generated by* 1.

Theorem 5.5. *Let $Z = \mathbb{Z}_{2^n}$ denote the cyclic group of order 2^n. Then*

$$a_Z = n, b_Z = c_Z = 0.$$

Proof. We know that for an abelian group, the commutator subgroup is trivial. The claim here is that Z is abelian.

Lemma 5.6. *Let G be a cyclic group. Then G is abelian.*

Proof. As assumed, let G be a cyclic group and pick two elements $g_1, g_2 \in G$. We'll show that $g_1 g_2 = g_2 g_1$. Using the fact that G is cyclic, then there exists a $g \in G$ that generates the whole group. That is to say

$$G = \langle g \rangle$$

This also means that there exists n and k, integers, such that $g_1 = g^n$ and $g_2 = g^k$.

$$g_1 g_2 = g^n g^k$$

$$= g^{n+k}$$

$$= g^{k+n}$$

$$= g^k g^n$$

$$= g_2 g_1 \qquad \square$$

By this lemma, we know that $Z = \mathbb{Z}_{2^n}$ is abelian. We also know that for an abelian group, the commutator subgroup is trivial. This means that Z' is trivial, and so is Z''.

Therefore, the order the quotient groups are $|Z/Z'| = 2^n$, $|Z'/Z''| = 1$ and $|Z''/Z'''| = 1$, i.e. $a_Z = \log_2(2^n) = n, b_Z = \log_2 1 = 0$ and $c_Z = \log_2 1 = 0$. $\square$

Now, let D_{2^n} denote the dihedral group of order 2^n.

Theorem 5.7. *Let $D = D_{2^n}$, with $n \geq 3$. Then*

$$a_D = 2, b_D = n - 2 \text{ and } c_D = 0.$$

Proof. We first want to recall that

$$D = \langle r, s : r^{2^{n-1}} = e, s^2 = e, sr = r^{-1}s \rangle.$$

We now want to compute some of the elements of the group D'.

$$[r, s] = rsr^{-1}s$$

$$= rrss$$

$$= r^2 \in D'.$$

Then, we can claim the following:

Lemma 5.8. *The commutator subgroup of D is given by*

$$D' = \{r^a : a \text{ is even}\}$$

Proof. Let $A = \{r^a : a \text{ is even}\}$. Then, we'll prove that (1) $A \subset D'$ and (2) $D' \subset A$. We'll first do (1).

(1) Showing $A \subset D'$.

Pick an element $r^a \in A$, and we'll show that $r^a \in D'$. Since $r^a \in A$, then a is an even number; and so we can find an integer k such that $a = 2k$. Then

$$r^a = r^{2k}$$

$$= (r^2)^k.$$

Then, since $r^2 \in D'$, by the computation done above in Lemma 5.8, we also get that $r^a \in D'$. Therefore, we proved that $A \subset D'$.

(2) Showing $D' \subset A$.

Let $f\colon D \to \mathbb{Z}_2 \times \mathbb{Z}_2$ be defined by

$$f(r^a s^b) = (a, b)\ mod\ 2.$$

To see that f is well defined suppose that $r^a s^b = r^c s^d$. We'll show that $f(r^a s^b) = f(r^c s^d)$. Clearly, if a is even, then c has to be even otherwise we could have $r = r^2$ which is not true. This means that a and c are the same mod 2. Similarly for b and d, so $(a, b) = (c, d)$ and f is well defined.

We still need to show that f is a homomorphism. Pick two elements $r^a s^b, r^c s^d \in$

D. Then

$$\begin{aligned} f(r^a s^b r^c s^d) &= f(r^a r^{(-1)^b c} s^b s^d) \\ &= f(r^{a+(-1)^b c} s^{b+d}) \\ &= (a + (-1)^b c, b + d) \\ &= (a + c, b + d) \ (mod\ 2) \\ &= (a, b) + (c, d) \\ &= f(r^a s^b) f(r^c s^d) \end{aligned}$$

So f is a homomorphism. To see what the kernel of f is, follow:

$$\begin{aligned} Ker(f) &= \{r^a s^b \in D \colon a \equiv 0 \ (mod\ 2) \text{ and } b \equiv 0 \ (mod\ 2)\} \\ &= \{r^a s^b \in D \colon a \text{ and } b \text{ are both even}\} \\ &= \{r^a \colon a \text{ is even}\} \\ &= A. \end{aligned}$$

So the set A is the kernel of the function f. Therefore, by Theorem 2.19 we get $D' \subset A$. Hence, $D' = A$. □

Now, by the first isomorphism theorem, Theorem 2.21, the image of D, under f, is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. So,

$$|D'| = \frac{|D|}{|\mathbb{Z}_2 \times \mathbb{Z}_2|} = \frac{2^n}{4} = 2^{n-2}$$

This implies that $|D/D'| = 4$, and hence $a_D = \log_2 4 = 2$.

Now, we want to compute the second commutator subgroup, D''. Pick up any two elements $r^a, r^b \in D'$, then

$$r^a r^b (r^a)^{-1} (r^b)^{-1} = r^a r^b r^{-a} r^{-b}$$

$$= r^{a+b-a-b}$$

$$= e.$$

This shows that, the commutator of any two arbitrary elements of D' is the identity element e. That is to say that D'' is the trivial subgroup, $D'' = \{e\}$.

From this last paragraph, we can conclude that

$$|D'/D''| = \frac{|D'|}{|D''|} = \frac{2^{n-2}}{1} = 2^{n-2}.$$

This means that $b_D = \log_2(2^{n-2}) = n-2$. Further, $c_D = 0$ because D''' will be trivial, since D'' is. Therefore, we showed that

$$a_D = 2, b_D = n-2 \text{ and } c_D = 0. \quad \square$$

It is time now to prove another theorem about the existence of certain groups with certain values of the constants a, b and c.

Theorem 5.9. *Let a, b, and c be positive integers. If $a \geq 3$ and $b = 3$, then there exists a finite 2-group G with derived length 3 such that $a_G = a$ and $b_G = b$ and $c_G = c$.*

Proof. Let c be an odd integer. Let H be a 2-group of derived length 3 with

$$a_H = 3,\ b_H = 3, \text{ and } c_H = c,$$

which exists by Theorem 3.4 (if c is odd) or Theorem 4.1 (if c is even). Let $Z = \mathbb{Z}_{2^k}$. Then, by Theorem 5.5, we get:

$$a_Z = k, \text{ and}$$

$$b_Z = c_Z = 0.$$

Then define G to be the direct product of H and Z:

$$G = H \times Z.$$

Using Theorem 5.3 we get

$$a_G = a_H + a_Z = 3 + k = k + 3,$$

$$b_G = b_H + b_Z = 3 + 0 = 3, \text{ and}$$

$$c_G = c_H + c_Z = c + 0 = c.$$

Let $k = a - 3$, then $a \geq 3$. Therefore, this first case shows the existence of a 2-group G of derived length 3 with $a_G \geq 3$, $b_G = 3$ and c_G. □

Theorem 5.10. *Let a, b, and c be integers. If $a \geq 5$ and $b \geq 4$, then there exists a finite 2-group G with derived length 3 such that $a_G = a$ and $b_G = b$ and $c_G = c$.*

Proof. As in Theorem 5.9, let H be a 2-group of derived length 3 with

$$a_H = 3,\ b_H = 3, \text{ and } c_H = c,$$

with c being odd. Such a group exists by Theorem 3.4 (if c is odd) or Theorem 4.1 (if c is even). Let $D = D_{2^k}$, then by Theorem 5.7 we get

$$a_D = 2,\ b_D = k - 2, \text{ and } c_D = 0.$$

Let $Z = \mathbb{Z}_{2^m}$, then by Theorem 5.5 we have

$$a_Z = m, \text{ and}$$

$$b_Z = c_Z = 0.$$

Define G to be the direct product of the three groups H, Z and D, i.e.

$$G = H \times Z \times D,$$

then by Theorem 5.3 we have

$$a_G = a_H + a_Z + a_D = 3 + m + 2 = m + 5,$$

$$b_G = b_H + b_Z + b_D = 3 + 0 + (k - 2) = k + 1, \text{ and}$$

$$c_G = c_H + c_Z + c_D = c + 0 + 0 = c.$$

Now, if we pick $m = a - 5$ and $k = b - 1$. With c being odd, then G is a 2-group of derived length 3, with

$$a_G = a,\ b_G = b, \text{ and } c_G = c,$$

with c is odd.

This shows the existence of a 2-group G with derived length 3 and $a_G \geq 5$, $b_G = 4$, and $c_G = c$, with c being even or odd. □

REFERENCES

[1] D. S. Dummit and R. M. Foote, *Abstract Algebra,* Graduate Texts in Mathematics, John Wiley & Sons, Inc., Hoboken, NJ, 2004.

[2] C. Schneider, *The derived series of a finite p-group,* J. Algebra, **307**, No 1, (2007), 136–152.

[3] C. Schneider, *Small derived quotients in finite p-groups,* Publ. Math. Debrecen, **69**, No 3, (2006), 373–378.

[4] J. P. Serre, *Sur une question d'Olga Taussky*, J. Number Theory, **2**, (1970), 235–236.

[5] P. Maclachlan, *A Contribution to the Theory of Groups of Prime-Power Order,* Proc. London Math. Soc **S2-36**, No 1, 29.

[6] M. D. Miller, *Existence of finite groups with classical commutator subgroup,* J. Austral. Math. Soc. Set. A **25**, (1978), No 1, 41-44

[7] D. Gorenstein, *Finite Groups, Second Edition,* A Book in Mathematics, Chelsea Publishing Co., New York, 1980

[8] E. Golvin, *Ezekiel's Thesis Title,* Master's Thesis, California State University, Los Angeles United States, 2014

[9] H. U. Besche, B. Eick and E. A. O'Brien, *A millennium project: constructing small groups,* Internat. J. Algebra Comput, **12**, No 5, (2002), 623–644

[10] *P-Group,* Internet Page, ttp://en.wikipedia.org/wiki/P-primary_group#CITEREFBesceEickO.27Brien2002