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

Matthew Aivazian
Candidate

Mathematics
Department

TITLE: **ITERATED SEMI-DIRECT PRODUCT OF THE INTEGERS MODULO TWO**

APPROVED: **Michael Krebs PhD**
Committee Chairperson
Signature

Gary Brookfield PhD
Faculty Member
Signature

Michael Hoffman PhD
Faculty Member
Signature

Grant Fraser PhD
Department Chairperson
Signature

DATE: **June 6, 2012**

ITERATED SEMI-DIRECT 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

By

Matthew Aivazian

June 2012

ACKNOWLEDGMENTS

First, I would like to express my deep gratitude to my advisor, Dr. Michael Krebs, for months of patient guidance. Also, I would like to extend heartfelt thanks to the faculty at the Department of Mathematics, California State University, Los Angeles who have assisted in large ways and small throughout this process: Dr. Gary Brookfield, Dr. Grant Fraser, Dr. Michael Hoffman, Dr. Daphne Liu and many others. I dedicate this thesis to my dearest wife Jacqueline, without whose unwavering love and support it would never have been completed.

ABSTRACT

Iterated Semi-Direct Product of the Integers of Modulo Two

By

Matthew Aivazian

A topic in graph theory, namely the construction of certain sequences of graphs called expander families, leads to a question about iterated semi-direct products of the integers modulo two and the abelianization of their derived subgroups. Specifically, the question is, “Can we construct these semi-direct products so that the resulting sequences of abelianizations are bounded?” In this thesis, we will discuss but not answer this question.

TABLE OF CONTENTS

Chapter

LIST OF TABLES

Table

LIST OF FIGURES

Figure

CHAPTER 1

Introduction

A sequence of finite groups is said to be "potentially expanding" if the groups become arbitrarily large but all the corresponding sequences of abelianizations are bounded. (See Definition 2.12 for details.)

One method for constructing a sequence of groups is the following. Begin with the simplest non-trivial group, namely, the integers modulo two. Then at each step, take a semi-direct product of the previous group with the integers modulo two. Now, the main question is, "Using this method, can we construct a potentially expanding sequence of groups?"

The motivation for the definition of "potentially expanding" comes from graph theory. Certain sequences of graphs are called "expander families." A necessary condition for a sequence of groups to yield an expander family, via the Cayley graph construction, is that it be potentially expanding. It is an open problem to find conditions that are both necessary and sufficient.

All infinite families of finite non-abelian simple groups are potentially expanding. In fact, it was recently proven that all infinite families of finite non-abelian simple groups yield expander families. This result is the culmination of many years' work by several mathematicians. The last case was completed by Emmanuel Breuillard, Ben Green, and Terence Tao in 2011 (see [1]).

However, in the second stage of this research project, namely the graph theory phase, we want to have particularly nice groups. Therefore, we prefer to work with groups constructed recursively in the manner described above.

In this thesis, we will:

- Prove that if a potentially expanding sequence is constructed in this manner, then infinitely many automorphisms used to induce the semi-direct products must be outer. (Corollary 4.9)
- Show, by means of an example, that the converse of the previous item will fail. (Theorem 5.9)

In addition, we will discuss many other examples of this construction in our attempt to answer the (as yet) unresolved main question.

CHAPTER 2

Basic Information About Commutator Subgroups and Semi-Direct Products

In this chapter we will present some basic definitions and theorems concerning the parts of group theory we will need in order to state our main objectives. We refer the reader to [2] for general background on group theory.

Definition 2.1. *Let G be a group and $a, b \in G$. Then $[a,b] = a^{-1}b^{-1}ab$ is called the* ***commutator of*** *a* ***and*** *b.*

Note: We denote the identity element of a group G by e_G, or simply by e, when the group is understood.

Theorem 2.2. *Let G be a group and $a, b, c \in G$. Then $c^{-1}[a,b]c = [c^{-1}ac, c^{-1}bc]$.*

Proof.

$$\begin{aligned}
[c^{-1}ac, c^{-1}bc] &= (c^{-1}ac)^{-1}(c^{-1}bc)^{-1}(c^{-1}ac)(c^{-1}bc) \\
&= c^{-1}a^{-1}(c^{-1})^{-1}c^{-1}b^{-1}(c^{-1})^{-1}c^{-1}acc^{-1}bc \\
&= c^{-1}a^{-1}cc^{-1}b^{-1}cc^{-1}acc^{-1}bc \\
&= c^{-1}a^{-1}eb^{-1}eaebc \\
&= c^{-1}a^{-1}b^{-1}abc \\
&= c^{-1}[a,b]c,
\end{aligned}$$

as claimed. □

Definition 2.3. *Let G be a group. Then $G' = [G,G] = \langle [a,b] \mid a, b \in G \rangle$ is called the* ***commutator subgroup of*** *G.*

Theorem 2.4. *Let G be a group. Then $G' \trianglelefteq G$.*

Proof. Let $g \in G$ and $x \in G'$. Then there exist elements $a_1, b_1, a_2, b_2, \ldots, a_n, b_n \in G$ such that $x = [a_1, b_1][a_2, b_2] \cdots [a_n, b_n]$. Hence

$$\begin{aligned} g^{-1}xg &= g^{-1}[a_1, b_1][a_2, b_2] \cdots [a_n, b_n]g \\ &= g^{-1}[a_1, b_1]e[a_2, b_2]e \cdots e[a_n, b_n]g \\ &= g^{-1}[a_1, b_1]gg^{-1}[a_2, b_2]gg^{-1} \cdots gg^{-1}[a_n, b_n]g \\ &= [g^{-1}a_1g, g^{-1}b_1g][g^{-1}a_2g, g^{-1}b_2g] \cdots [g^{-1}a_ng, g^{-1}b_ng] \in G'. \end{aligned}$$

Since $g \in G$ and $x \in G'$ are arbitrarily chosen elements, $G' \trianglelefteq G$, as claimed. □

Theorem 2.5. *Let G be a group. Then G/G' is an abelian group.*

Proof. Let $x, y \in G/G'$. Then there exist $a, b \in G$ such that $x = aG'$ and $y = bG'$. Since $a, b \in G$, $a^{-1}b^{-1}ab = [a, b] \in G'$ and consequently

$$\begin{aligned} yx &= bG'aG' \\ &= baG' \\ &= baa^{-1}b^{-1}abG' \\ &= beb^{-1}abG' \\ &= bb^{-1}abG' \\ &= eabG' \\ &= abG' \\ &= aG'bG' \\ &= xy. \end{aligned}$$

Since $x, y \in G/G'$ are arbitrarily chosen elements, G/G' is an abelian group, as claimed. $\square$

Definition 2.6. *Let G be a group and $N \trianglelefteq G$. Then the function $\pi : G \longrightarrow G/N$ defined by $\pi(x) = xN$ is called the **natural projection of** G **on** N.*

Theorem 2.7. *Let G be a group and $N \trianglelefteq G$. Then the natural projection of G on N is a group homomorphism with $ker(\pi) = N$.*

Proof. Let $x, y \in G$. Then $\pi(xy) = xyN = xNyN = \pi(x)\pi(y)$. This shows that π is a group homomorphism, as claimed. On the other hand, since N is the identity element of the quotient group G/N and $xN = N$ if and only if $x \in N$ for all $x \in G$, we have

$$\begin{aligned} ker(\pi) &= \{x \in G \mid \pi(x) = N\} \\ &= \{x \in G \mid xN = N\} \\ &= \{x \in G \mid x \in N\} \\ &= G \cap N \\ &= N, \end{aligned}$$

as claimed. $\square$

Theorem 2.8. *Let G be a group and $N \trianglelefteq G$ such that G/N is an abelian group. Then $G' \subseteq N$.*

Proof. Let $\pi : G \longrightarrow G/N$ defined by $\pi(x) = xN$ be the natural projection of G on N and let $x \in G'$. Then there exist elements $a_1, b_1, a_2, b_2, \ldots, a_n, b_n \in G$ such that $x = [a_1, b_1][a_2, b_2] \cdots [a_n, b_n]$. Now, let i be an integer satisfying $0 \leq i \leq n$. Then since $a_i, b_i \in G$ and G/N is an abelian group, we have

$$\pi([a_i, b_i]) = \pi([a_i^{-1} b_i^{-1} a_i b_i])$$

$$
\begin{aligned}
&= \pi(a_i^{-1})\pi(b_i^{-1})\pi(a_i)\pi(b_i) \\
&= (\pi(a_i))^{-1}(\pi(b_i))^{-1}\pi(a_i)\pi(b_i) \\
&= (\pi(a_i))^{-1}(\pi(b_i))^{-1}\pi(b_i)\pi(a_i) \\
&= (\pi(a_i))^{-1}N\pi(a_i) \\
&= (\pi(a_i))^{-1}\pi(a_i) \\
&= N.
\end{aligned}
$$

Therefore $[a_i, b_i] \in ker(\pi) = N$, by Theorem 2.7. Since i is an arbitrarily chosen integer satisfying $0 \leq i \leq n$, it follows that for every integer i satisfying $0 \leq i \leq n$, $[a_i, b_i] \in N$. Since for every integer i satisfying $0 \leq i \leq n$, $[a_i, b_i] \in N$ and $N \leq G$, $x = [a_1, b_1][a_2, b_2] \cdots [a_n, b_n] \in N$. Since $x \in G'$ is an arbitrarily chosen element, $G' \subseteq N$, as claimed. □

Definition 2.9. *Suppose that G is a group and m is a positive integer. We define $G^{(0)} = G$. Then $G^{(m)} = [G^{(m-1)}, G^{(m-1)}]$ is called the m^{th}* ***derived subgroup of*** *G and $G^{(m-1)}/G^{(m)}$ is called the m^{th}* ***abelianization of*** *G.*

Theorem 2.10. *Let G be an abelian group. Then $G' = \{e\}$.*

Proof. Since G is an abelian group, for every $a, b \in G$,

$$
\begin{aligned}
[a, b] &= a^{-1}b^{-1}ab \\
&= a^{-1}b^{-1}ba \\
&= a^{-1}ea \\
&= a^{-1}a \\
&= e
\end{aligned}
$$

and consequently $G' = [G, G] = \langle [a, b] \mid a, b \in G \rangle = \{e\}$, as claimed. $\square$

Theorem 2.11. *Suppose that G and H are groups and θ is a group homomorphism defined from H to $Aut(G)$. Then the Cartesian product $G \times H$ under the binary operation defined by $(g_1, h_1)(g_2, h_2) = (g_1\theta(h_1)(g_2), h_1h_2)$ forms a group, called the semi-direct product of G and H induced by θ, that will be denoted by $G \rtimes_\theta H$.*

Proof. First, we will prove that the binary operation is associative. In order to do so, let $(g_1, h_1), (g_2, h_2), (g_3, h_3) \in G \rtimes_\theta H$. Since the binary operations defined on G and H are associative, θ is a group homomorphism defined from H to $Aut(G)$, and $\theta(h_1), \theta(h_2) \in Aut(G)$,

$$\begin{aligned}
((g_1, h_1)(g_2, h_2))(g_3, h_3) &= (g_1\theta(h_1)(g_2), h_1h_2)(g_3, h_3) \\
&= ((g_1\theta(h_1)(g_2))\theta(h_1h_2)(g_3), (h_1h_2)h_3) \\
&= ((g_1\theta(h_1)(g_2))\theta(h_1)\theta(h_2)(g_3), (h_1h_2)h_3)) \\
&= (g_1(\theta(h_1)(g_2)\theta(h_1)\theta(h_2)(g_3)), h_1(h_2h_3)) \\
&= (g_1\theta(h_1)(g_2\theta(h_2)(g_3)), h_1(h_2h_3)) \\
&= (g_1, h_1)(g_2\theta(h_2)(g_3), h_2h_3) \\
&= (g_1, h_1)((g_2, h_2)(g_3, h_3)).
\end{aligned}$$

This shows that the binary operation defined on $G \rtimes_\theta H$ is associative, as claimed.

Second, we will prove that (e_G, e_H) is the identity element of $G \rtimes_\theta H$. To do so, let $(g, h) \in G \rtimes_\theta H$. Then $g \in G$ and $h \in H$. We know that $\theta(h) \in Aut(G)$, and consequently $\theta(h)(e_G) = e_G$. Since $\theta(h)(e_G) = e_G$ and e_G and e_H are the identity elements of G and H, respectively,

$$\begin{aligned}(g,h)(e_G,e_H) &= (g\theta(h)(e_G), he_H)\\ &= (ge_G, h)\\ &= (g,h).\end{aligned}$$

On the other hand, since θ is a group homomorphism defined from H to $Aut(G)$ and e_H is the identity element of H, $\theta(e_H)$ is the identity element of $Aut(G)$ and consequently $\theta(e_H)(g) = g$. Since $\theta(e_H)(g) = g$ and e_G and e_H are the identity elements of G and H, respectively,

$$\begin{aligned}(e_G,e_H)(g,h) &= (e_G\theta(e_H)(g), e_Hh)\\ &= (e_Gg, h)\\ &= (g,h).\end{aligned}$$

This shows that (e_G, e_H) is the identity element of $G \rtimes_\theta H$, as claimed.

Third, we will prove that each element of $G \rtimes_\theta H$ has an inverse. To do so, let $(g,h) \in G \rtimes_\theta H$. Then $g \in G$ and $h \in H$. Since $g \in G$, $h \in H$, and G and H are groups, g^{-1} and h^{-1} exist. Since θ is a group homomorphism defined from H to $Aut(G)$ and $h \in H$, $\theta(h) \in Aut(G)$. Since $\theta(h) \in Aut(G)$ and $Aut(G)$ is a group, $\theta(h)^{-1}$ exists and $\theta(h)^{-1} = \theta(h^{-1})$. Moreover, since θ is a group homomorphism defined from H to $Aut(G)$ and e_H is the identity element of H, $\theta(e_H)$ is the identity element of $Aut(G)$. Since $\theta(e_H)$ is the identity element of $Aut(G)$, for every $x \in G$, $\theta(e_H)(x) = x$. Specifically, since $g^{-1} \in G$, $\theta(e_H)(g^{-1}) = g^{-1}$. Thus

$$(g,h)(\theta(h^{-1})(g^{-1}), h^{-1}) = (g\theta(h)(\theta(h^{-1})(g^{-1})), hh^{-1})$$

$$\begin{aligned}
&= (g\theta(h)\theta(h^{-1})(g^{-1}), e_H) \\
&= (g\theta(hh^{-1})(g^{-1}), e_H) \\
&= (g\theta(e_H)(g^{-1}), e_H) \\
&= (gg^{-1}, e_H) \\
&= (e_G, e_H).
\end{aligned}$$

On the other hand, Since θ is a group homomorphism defined from H to $Aut(G)$ and $h^{-1} \in H$, $\theta(h^{-1}) \in Aut(G)$. Since $\theta(h^{-1}) \in Aut(G)$ and e_G is the identity element of G, $\theta(h^{-1})(e_G) = e_G$. Thus

$$\begin{aligned}
(\theta(h^{-1})(g^{-1}), h^{-1})(g, h) &= (\theta(h^{-1})(g^{-1})\theta(h^{-1})(g), h^{-1}h) \\
&= (\theta(h^{-1})(g^{-1}g), e_H) \\
&= (\theta(h^{-1})(e_G), e_H) \\
&= (e_G, e_H).
\end{aligned}$$

This shows that each element of $G \rtimes_\theta H$ has an inverse, as claimed. Hence the Cartesian product $G \times H$ under the given binary operation forms a group, as claimed.

□

Definition 2.12. *A sequence of finite groups* $\{G_n\}_{n=1}^{\infty}$ *is said to be* ***potentially expanding*** *if it satisfies both conditions below:*

a) $|G_n| \to \infty$ *as* $n \to \infty$

b) *For every non-negative integer* m, $\{|G_n^{(m)}/G_n^{(m+1)}|\}_{n=1}^{\infty}$ *is a bounded sequence.*

The motivation for the definition above comes from the theory of expander families. For more on expander families, we refer the reader to [4]. If a sequence of finite groups yields an expander family, via the Cayley graph construction, then the sequence is necessarily potentially expanding. However, this condition is not sufficient. A counterexample (referring to [3]) is the sequence of n-fold direct products of the alternating group A_5. No one has found conditions that are both necessary and sufficient under which a sequence of finite groups yields an expander family.

We know that for every positive integer $n \geq 5$, we have $A_n^{(1)} = A_n' = A_n$ where $A_n = \{\sigma \in S_n \mid \sigma \text{ is an even permutation}\}$ is the alternating group on n letters and S_n is the symmetric group on n letters. So, if for every positive integer n, $G_n = A_{n+4}$, then $\{G_n\}_{n=1}^{\infty}$ will satisfy both conditions above. So $\{G_n\}_{n=1}^{\infty}$ is potentially expanding. More generally, for the same reason all infinite families of finite non-abelian simple groups are potentially expanding.

CHAPTER 3

General Properties of Semi-Direct Products

In this chapter we will present general properties of semi-direct products. We begin our discussion by showing that a semi-direct product induced by the trivial homomorphism and the corresponding direct product are the same. At the end of the chapter we will present a sequence of finite groups that is not potentially expanding.

Theorem 3.1. *Suppose that G and H are groups. Then the semi-direct product of G and H induced by the trivial homomorphism defined from H to $Aut(G)$ and the direct product of G and H are the same.*

Proof. Let θ be the trivial homomorphism defined from H to $Aut(G)$ that maps every $h \in H$ to the identity element of $Aut(G)$ and $(g_1, h_1), (g_2, h_2) \in G \times H$. Moreover, let $\star_1 : (G \times H) \times (G \times H) \longrightarrow G \times H$ and $\star_2 : (G \times H) \times (G \times H) \longrightarrow G \times H$ be the binary operations defined on $G \times H$ by $\star_1((x_1, y_1), (x_2, y_2)) = (x_1, y_1) \star_1 (x_2, y_2) = (x_1x_2, y_1y_2)$ and $\star_2((x_1, y_1), (x_2, y_2)) = (x_1, y_1) \star_2 (x_2, y_2) = (x_1\theta(y_1)(x_2), y_1y_2)$, respectively. Since θ maps every $h \in H$ to the identity element of $Aut(G)$, for every $g \in G$ and every $h \in H$, $\theta(h)(g) = g$. Therefore

$$\begin{aligned}(g_1, h_1) \star_2 (g_2, h_2) &= (g_1\theta(h_1)(g_2), h_1h_2) \\ &= (g_1g_2, h_1h_2) \\ &= (g_1, h_1) \star_1 (g_2, h_2).\end{aligned}$$

Hence the semi-direct product of G and H induced by the trivial homomorphism defined from H to $Aut(G)$ and the direct product of G and H are the same, as claimed. □

Definition 3.2. *Let G be a group and $g \in G$. If there exists a positive integer m such that $g^m = e$, then the well-ordering principle guarantees the existence of the least positive integer n with $g^n = e$. Such a positive integer n is called the* ***order*** *of g and is denoted by $|g|$.*

Theorem 3.3. *Suppose that G_1 and G_2 are groups and θ is a group homomorphism defined from G_1 to G_2. Let $g \in G_1$. If $|g|$ is finite, then $|\theta(g)|$ is also finite and divides $|g|$.*

Proof. Let $|g| = n$ where n is a positive integer. Then $g^n = e$ where e_1 is the identity element of G_1. Since θ is a group homomorphism, $\theta(e_1) = e_2$ where e_2 is the identity element of G_2. Hence $\theta(g)^n = \theta(g^n) = \theta(e_1) = e_2$ and consequently $|\theta(g)|$ is finite and $|\theta(g)| \leq n$, by the definition of the order of an element of a group. Now, assume to the contrary that $|\theta(g)| = m$ does not divide $|g|$. Hence by the division theorem, there exist unique integers q and r such that $n = mq + r$ and $0 < r < m$. Since $|\theta(g)| = m$ and $n = mq + r$, $\theta(g)^m = e_2$ and $r = n - mq$. Therefore

$$\begin{aligned}
\theta(g)^r &= \theta(g)^{n-mq} \\
&= \theta(g)^n \theta(g)^{-mq} \\
&= \theta(g^n)(\theta(g)^m)^{-q} \\
&= \theta(e_1)e_2^{-q} \\
&= e_2 e_2
\end{aligned}$$

$$= e_2$$

which is a contradiction, because m is the least positive integer satisfying $\theta(g)^m = e_2$. Hence $|\theta(g)|$ divides $|g|$, as claimed. □

Corollary 3.4. *Suppose that G is a group and $\theta \in Aut(G)$. Let $g \in G$. Then $|g|$ is finite if and only if $|\theta(g)|$ is finite. Furthermore $|\theta(g)| = |g|$.*

Proof. Since θ is a group homomorphism defined from G to G and $|g|$ is finite, $|\theta(g)|$ is also finite and divides $|g|$, by Theorem 3.3. On the other hand, since θ^{-1} is a group homomorphism defined from G to G and $|\theta(g)|$ is finite, $|g| = |\theta^{-1}(\theta(g))|$ is also finite and divides $|\theta(g)|$, by Theorem 3.3. Since $|g|$ and $|\theta(g)|$ are positive integers, $|\theta(g)|$ divides $|g|$, and $|g|$ divides $|\theta(g)|$, we have $|\theta(g)| = |g|$, as claimed. □

Corollary 3.5. *Suppose G is a group and θ is a group homomorphism defined from $\mathbb{Z}_2$ to $Aut(G)$. Then $\theta(1)$ is either the trivial automorphism or an automorphism of order two.*

Proof. Since $1 \in \mathbb{Z}_2$ is of order two and the only positive divisors of 2 are 1 and 2, either $|\theta(1)| = 1$ or $|\theta(1)| = 2$, by Theorem 3.3. If $|\theta(1)| = 1$, then $\theta(1)$ is the trivial automorphism. If $|\theta(1)| = 2$, then $\theta(1)$ is an automorphism of order two, as claimed. □

Theorem 3.6. *Let G and H be abelian groups. Then $G \times H$ is also an abelian group.*

Proof. Let $x, y \in G \times H$. Then there exist $g_1, g_2 \in G$ and $h_1, h_2 \in H$ such that $x = (g_1, h_1)$ and $y = (g_2, h_2)$. Since $g_1, g_2 \in G$, $h_1, h_2 \in H$, and G and H are abelian groups, $g_1g_2 = g_2g_1$ and $h_1h_2 = h_2h_1$ and consequently

$$xy = (g_1, h_1)(g_2, h_2)$$

$$\begin{aligned} &= (g_1g_2, h_1h_2) \\ &= (g_2g_1, h_2h_1) \\ &= (g_2, h_2)(g_1, h_1) \\ &= yx. \end{aligned}$$

Since $x, y \in G \times H$ are arbitrarily chosen elements, this shows that the direct product of G and H is an abelian group, as claimed. □

Corollary 3.7. *Let $n > 1$ be a positive integer and let $G_1, \ldots, G_n$ be abelian groups. Then the direct product $G_1 \times \ldots \times G_n$ is also an abelian group.*

Proof. This follows immediately from Theorem 3.6 and mathematical induction on n.

□

Corollary 3.8. *For every positive integer n, $\mathbb{Z}_2^n$ is an abelian group.*

Proof. This follows immediately from Corollary 3.7 and the fact that $\mathbb{Z}_2$ is an abelian group. □

Corollary 3.9. *For every positive integer n, $(\mathbb{Z}_2^n)'$ is the proper trivial subgroup.*

Proof. This follows immediately from Theorem 2.10 and Corollary 3.8. □

Corollary 3.10. *For every positive integer n, $|\mathbb{Z}_2^n/(\mathbb{Z}_2^n)'| = 2^n$.*

Proof. Since for every positive integer n, $|\mathbb{Z}_2^n| = 2^n$ and $|(\mathbb{Z}_2^n)'| = |\{e\}| = 1$,

$$\begin{aligned} |\mathbb{Z}_2^n/(\mathbb{Z}_2^n)'| &= \frac{|\mathbb{Z}_2^n|}{|(\mathbb{Z}_2^n)'|} \\ &= \frac{2^n}{1} \\ &= 2^n, \end{aligned}$$

as claimed. □

Corollary 3.11. *Since for every positive integer n, the semi-direct product of $\mathbb{Z}_2^n$ and $\mathbb{Z}_2$ induced by the trivial homomorphism defined from $\mathbb{Z}_2$ to $Aut(\mathbb{Z}_2^n)$ is $\mathbb{Z}_2^n \times \mathbb{Z}_2 \cong \mathbb{Z}_2^{n+1}$, the sequence $\{\mathbb{Z}_2^n\}_{n=1}^{\infty}$ obtained in this manner is not potentially expanding.*

Proof. This follows immediately from Corollary 3.10 and Definition 2.12. □

Remark. This is why we look at semi-direct products instead of direct products.

CHAPTER 4

Inner Automorphisms and Related Semi-Direct Products

In this chapter we will present general properties of inner automorphisms of a group induced by elements of order two. At the end of the chapter we will prove a general theorem showing that certain sequences of finite groups are not potentially expanding.

Theorem 4.1. *Let G be a group and $a \in G$. Then the function $\varphi_a : G \longrightarrow G$ defined by $\varphi_a(x) = axa^{-1}$ is an automorphism of G, called the* ***inner automorphism of*** G ***induced by*** a.

Proof. First, we will prove that φ_a is a group homomorphism. To do so, let $x, y \in G$. Then

$$\begin{aligned} \varphi_a(xy) &= axya^{-1} \\ &= axeya^{-1} \\ &= axa^{-1}aya^{-1} \\ &= \varphi_a(x)\varphi_a(y). \end{aligned}$$

This shows that φ_a is a group homomorphism, as claimed.

Next, we will prove that φ_a is a bijection by showing that $\varphi_{a^{-1}}$ is the inverse function of φ_a. To do so, let $x \in G$. Then

$$\begin{aligned} (\varphi_a\varphi_{a^{-1}})(x) &= \varphi_a(\varphi_{a^{-1}}(x)) \\ &= \varphi_a(a^{-1}x(a^{-1})^{-1}) \end{aligned}$$

$$
\begin{aligned}
&= aa^{-1}x(a^{-1})^{-1}a^{-1} \\
&= exe \\
&= x
\end{aligned}
$$

and

$$
\begin{aligned}
(\varphi_{a^{-1}}\varphi_a)(x) &= \varphi_{a^{-1}}(\varphi_a(x)) \\
&= \varphi_{a^{-1}}(axa^{-1}) \\
&= a^{-1}axa^{-1}(a^{-1})^{-1} \\
&= exe \\
&= x.
\end{aligned}
$$

This shows that φ_a is a bijection, as claimed. □

Theorem 4.2. *Let G be a group and $a, b \in G$. Then $\varphi_{ab} = \varphi_a\varphi_b$ where φ_{ab}, φ_a, and φ_b are the inner automorphisms of G induced by ab, a, and b, respectively.*

Proof. Let $x \in G$. Then

$$
\begin{aligned}
\varphi_{ab}(x) &= abx(ab)^{-1} \\
&= abxb^{-1}a^{-1} \\
&= a\varphi_b(x)a^{-1} \\
&= \varphi_a(\varphi_b(x)) \\
&= (\varphi_a\varphi_b)(x).
\end{aligned}
$$

Since $x \in G$ is an arbitrarily chosen element, this shows that $\varphi_{ab} = \varphi_a\varphi_b$, as claimed.

□

Corollary 4.3. *Let G be a group. Then the function $\psi : G \longrightarrow Aut(G)$ defined by $\psi(a) = \varphi_a$ is a group homomorphism.*

Proof. By corollary 4.1, ψ is a well-defined function. Now, let $a, b \in G$. Then $\varphi_{ab} = \varphi_a\varphi_b$, by Theorem 4.2 and consequently

$$\begin{aligned} \psi(ab) &= \varphi_{ab} \\ &= \varphi_a\varphi_b \\ &= \psi(a)\psi(b). \end{aligned}$$

This shows that ψ is a group homomorphism, as claimed. □

Theorem 4.4. *Let G be a group and $a \in G$ with $a^2 = e$. Then the inner automorphism φ_a of G induced by a is an automorphism of order either one or two.*

Proof. Since $a^2 = e$, either $|a| = 1$ or $|a| = 2$. Now, let $\psi : G \longrightarrow Aut(G)$ be defined by $\psi(a) = \varphi_a$. Then by Corollary 4.3 ψ is a group homomorphism and consequently $|\varphi_a| = |\psi(a)|$ is finite and divides $|a|$, by Theorem 3.3. Since either $|a| = 1$ or $|a| = 2$, $|\varphi_a| = 1$ or $|\varphi_a| = 2$ and therefore φ_a is an automorphism of order either one or two, as claimed. □

Now, we fix a group G, an element $a \in G$ with $a^2 = e$, and let $G \rtimes_{\theta_a} \mathbb{Z}_2$ be the semi-direct product induced by the homomorphism θ_a defined from $\mathbb{Z}_2$ to $Aut(G)$ that maps 1 to the inner automorphism φ_a of G induced by a.

Theorem 4.5. *For every $g \in G$, $(g, 0)^{-1} = (g^{-1}, 0)$ and $(g, 1)^{-1} = (ag^{-1}a, 1)$.*

Proof. Let $g \in G$. Then since $a^2 = e$, $a^{-1} = a$ and consequently for every $x \in G$, $\theta_a(1)(x) = \varphi_a(x) = axa^{-1} = axa$. Moreover, since the additive inverses of the elements $0 \in \mathbb{Z}_2$ and $1 \in \mathbb{Z}_2$ are 0 and 1, respectively and $\theta_a(0) \in Aut(G)$ is the trivial automorphism of G, we have

$$\begin{aligned}(g,0)^{-1} &= (\theta_a(0)(g^{-1}),0)\\ &= (g^{-1},0)\end{aligned}$$

and

$$\begin{aligned}(g,1)^{-1} &= (\theta_a(1)(g^{-1}),1)\\ &= (ag^{-1}a,1),\end{aligned}$$

by Theorem 2.11. Since $g \in G$ is an arbitrarily chosen element, this shows that for every $g \in G$, $(g,0)^{-1} = (g^{-1},0)$ and $(g,1)^{-1} = (ag^{-1}a,1)$, as claimed. □

Theorem 4.6. *Let G and H be groups and $G \rtimes_\theta H$ be the semi-direct product induced by a homomorphism θ defined from H to $Aut(G)$. Then for every $a, b \in G$ we have $[(a,e_H),(b,e_H)] = ([a,b],e_H)$.*

Proof. Let $a, b \in G$. Then since $e_H^{-1} = e_H$ and $\theta(e_H)$ is the trivial automorphism of G, we have

$$\begin{aligned}(a,e_H)^{-1} &= (\theta(e_H^{-1})(a^{-1}),e_H^{-1})\\ &= (\theta(e_H)(a^{-1}),e_H)\\ &= (a^{-1},e_H)\end{aligned}$$

and

$$\begin{aligned}(b,e_H)^{-1} &= (\theta(e_H^{-1})(b^{-1}),e_H^{-1})\\ &= (\theta(e_H)(b^{-1}),e_H)\\ &= (b^{-1},e_H),\end{aligned}$$

by Theorem 2.11 and consequently

$$\begin{aligned}[(a,e_H),(b,e_H)] &= (a,e_H)^{-1}(b,e_H)^{-1}(a,e_H)(b,e_H)\\ &= (a^{-1},e_H)(b^{-1},e_H)(a,e_H)(b,e_H)\\ &= (a^{-1}\theta(e_H)(b^{-1}),e_He_H)(a\theta(e_H)(b),e_He_H)\\ &= (a^{-1}b^{-1},e_H)(ab,e_H)\\ &= (a^{-1}b^{-1}\theta(e_H)(ab),e_He_H)\\ &= (a^{-1}b^{-1}ab,e_H)\\ &= ([a,b],e_H),\end{aligned}$$

as claimed. □

Theorem 4.7. *We have that* $(G \rtimes_{\theta_a} \mathbb{Z}_2)' = \{(g',0) \mid g' \in G'\}$.

Proof. First, we will prove that $(G \rtimes_{\theta_a} \mathbb{Z}_2)' \subseteq \{(g',0) \mid g' \in G'\}$. In order to do so, let $x, y \in G \rtimes_{\theta_a} \mathbb{Z}_2$. Then there exist $g, h \in G$ and $m, n \in \mathbb{Z}_2$ such that $x = (g,m)$ and $y = (h,n)$.

If $m = 0$ and $n = 0$, then since 0 is the identity element of $\mathbb{Z}_2$ we have

$$[x,y] = [(g,m),(h,n)] = [(g,0),(h,0)] = ([g,h],0) \in \{(g',0) \mid g' \in G'\},$$

by Theorem 4.6.

If $m = 0$ and $n = 1$, then

$$\begin{aligned}[x,y] = x^{-1}y^{-1}xy &= (g,m)^{-1}(h,n)^{-1}(g,m)(h,n)\\ &= (g,0)^{-1}(h,1)^{-1}(g,0)(h,1)\\ &= (g^{-1},0)(ah^{-1}a,1)(g,0)(h,1)\end{aligned}$$

$$\begin{aligned}
&= (g^{-1}\theta_a(0)(ah^{-1}a), 0+1)(g\theta_a(0)(h), 0+1) \\
&= (g^{-1}ah^{-1}a, 1)(gh, 1) \\
&= (g^{-1}ah^{-1}a\theta_a(1)(gh), 1+1) \\
&= (g^{-1}ah^{-1}aagha, 0) \\
&= (g^{-1}ah^{-1}gha, 0) \\
&= ([g, ha], 0) \in \{(g', 0) \mid g' \in G'\}.
\end{aligned}$$

If $m = 1$ and $n = 0$, then

$$\begin{aligned}
[x, y] = x^{-1}y^{-1}xy &= (g, m)^{-1}(h, n)^{-1}(g, m)(h, n) \\
&= (g, 1)^{-1}(h, 0)^{-1}(g, 1)(h, 0) \\
&= (ag^{-1}a, 1)(h^{-1}, 0)(g, 1)(h, 0) \\
&= (ag^{-1}a\theta_a(1)(h^{-1}), 1+0)(g\theta_a(1)(h), 1+0) \\
&= (ag^{-1}aah^{-1}a, 1)(gaha, 1) \\
&= (ag^{-1}h^{-1}a, 1)(gaha, 1) \\
&= (ag^{-1}h^{-1}a\theta_a(1)(gaha), 1+1) \\
&= (ag^{-1}h^{-1}aagahaa, 0) \\
&= (ag^{-1}h^{-1}gah, 0) \\
&= ([ga, h], 0) \in \{(g', 0) \mid g' \in G'\}.
\end{aligned}$$

If $m = 1$ and $n = 1$, then

$$\begin{aligned}
[x, y] = x^{-1}y^{-1}xy &= (g, m)^{-1}(h, n)^{-1}(g, m)(h, n) \\
&= (g, 1)^{-1}(h, 1)^{-1}(g, 1)(h, 1)
\end{aligned}$$

$$\begin{aligned}
&= (ag^{-1}a, 1)(ah^{-1}a, 1)(g, 1)(h, 1) \\
&= (ag^{-1}a\theta_a(1)(ah^{-1}a), 1+1)(g\theta_a(1)(h), 1+1) \\
&= (ag^{-1}aaah^{-1}aa, 0)(gaha, 0) \\
&= (ag^{-1}ah^{-1}, 0)(gaha, 0) \\
&= (ag^{-1}ah^{-1}\theta_a(0)(gaha), 0+0) \\
&= (ag^{-1}ah^{-1}gaha, 0) \\
&= ([ga, ha], 0) \in \{(g', 0) \mid g' \in G'\}.
\end{aligned}$$

Since $x, y \in G \rtimes_{\theta_a} \mathbb{Z}_2$ are arbitrarily chosen elements, for every $x, y \in G \rtimes_{\theta_a} \mathbb{Z}_2$, $[x, y] \in \{(g', 0) \mid g' \in G'\}$ and consequently

$$(G \rtimes_{\theta_a} \mathbb{Z}_2)' = \langle [x, y] \mid x, y \in G \rtimes_{\theta_a} \mathbb{Z}_2 \rangle \subseteq \{(g', 0) \mid g' \in G'\},$$

as claimed.

Second, we will prove that $\{(g', 0) \mid g' \in G'\} \subseteq (G \rtimes_{\theta_a} \mathbb{Z}_2)'$. In order to do so, let $x \in \{(g', 0) \mid g' \in G'\}$. Then there exits $g' \in G'$ such that $x = (g', 0)$. Since $g' \in G'$, there exist $a_1, b_1, a_2, b_2, \ldots, a_n, b_n \in G$ such that $g' = [a_1, b_1][a_2, b_2] \cdots [a_n, b_n]$. Hence

$$\begin{aligned}
x &= (g', 0) \\
&= ([a_1, b_1][a_2, b_2] \cdots [a_n, b_n], 0) \\
&= ([a_1, b_1], 0)([a_2, b_2], 0) \cdots ([a_n, b_n], 0) \\
&= [(a_1, 0), (b_1, 0)][(a_2, 0), (b_2, 0)] \cdots [(a_n, 0), (b_n, 0)] \in (G \rtimes_{\theta_a} \mathbb{Z}_2)'.
\end{aligned}$$

Since $x \in \{(g', 0) \mid g' \in G'\}$ is arbitrarily chosen, for every $x \in \{(g', 0) \mid g' \in G'\}$, $x \in (G \rtimes_{\theta_a} \mathbb{Z}_2)'$ and consequently $\{(g', 0) \mid g' \in G'\} \subseteq (G \rtimes_{\theta_a} \mathbb{Z}_2)'$, as claimed. Thus $(G \rtimes_{\theta_a} \mathbb{Z}_2)' = \{(g', 0) \mid g' \in G'\}$, as claimed. □

Corollary 4.8. *Let G be a finite group. Then $|(G \rtimes_{\theta_a} \mathbb{Z}_2)/(G \rtimes_{\theta_a} \mathbb{Z}_2)'| = 2|G/G'|$.*

Proof. Since $(G \rtimes_{\theta_a} \mathbb{Z}_2)' = \{(g', 0) \mid g' \in G'\}$,

$$\begin{aligned}
|(G \rtimes_{\theta_a} \mathbb{Z}_2)/(G \rtimes_{\theta_a} \mathbb{Z}_2)'| &= \frac{|G \rtimes_{\theta_a} \mathbb{Z}_2|}{|(G \rtimes_{\theta_a} \mathbb{Z}_2)'|} \\
&= \frac{|G \rtimes_{\theta_a} \mathbb{Z}_2|}{|\{(g', 0) \mid g' \in G'\}|} \\
&= \frac{|G||\mathbb{Z}_2|}{|G'|} \\
&= \frac{2|G|}{|G'|} \\
&= 2\frac{|G|}{|G'|} \\
&= 2|G/G'|,
\end{aligned}$$

as claimed. □

Corollary 4.9. *Let G_1 be an arbitrary finite group and for every positive integer n, let $G_{n+1} = G_n \rtimes_{\theta_n} \mathbb{Z}_2$ where $G_n \rtimes_{\theta_n} \mathbb{Z}_2$ is the semi-direct product induced by the homomorphism θ_n defined from $\mathbb{Z}_2$ to $Aut(G_n)$ that maps 1 to the inner automorphism φ_n of G_n induced by an element $a_n \in G_n$ of order one or two. Then $\{G_n\}_{n=1}^{\infty}$ is not potentially expanding.*

Proof. This follows immediately from Corollary 4.8 and Definition 2.12. □

Hence, in order to construct a potentially expanding sequence of finite groups the way we want to, infinitely many of the semi-direct products must be induced by outer automorphisms.

CHAPTER 5

Dihedral Groups as Semi-Direct Products

In this chapter we will show that dihedral groups of order 2^n can be constructed by iterating semi-direct products with $\mathbb{Z}_2$. Then, we will show that the sequence $\{D_{2^n}\}_{n=2}^{\infty}$ so constructed is not potentially expanding.

Theorem 5.1. *Suppose that $D_n = \langle r, s \mid r^n = s^2 = e$ and $rs = sr^{-1}\rangle$ is the dihedral group of order $2n$ where n is a positive integer no less than three. Then we have $D_n \rtimes_\theta \mathbb{Z}_2 = \langle (r,0),(s,0),(e,1)\rangle$ where the semi-direct product $D_n \rtimes_\theta \mathbb{Z}_2$ is induced by a non-trivial homomorphism θ defined from $\mathbb{Z}_2$ to $Aut(D_n)$.*

Proof. Since $(r,0),(s,0),(e,1) \in D_n \rtimes_\theta \mathbb{Z}_2$, $\langle (r,0),(s,0),(e,1)\rangle \subseteq D_n \rtimes_\theta \mathbb{Z}_2$. Now, we will prove that $D_n \rtimes_\theta \mathbb{Z}_2 \subseteq \langle (r,0),(s,0),(e,1)\rangle$. To do so, let $x \in D_n \rtimes_\theta \mathbb{Z}_2$. Then there exist integers i, j, and k such that $0 \leq i \leq n-1$, $0 \leq j \leq 1$, and $0 \leq k \leq 1$ such that $x = (r^i s^j, k)$. On the other hand, $(r^i s^j, k) = (r,0)^i(s,0)^j(e,1)^k$ and $(r,0)^i(s,0)^j(e,1)^k \in \langle (r,0),(s,0),(e,1)\rangle$. Therefore

$$x = (r^i s^j, k) = (r,0)^i(s,0)^j(e,1)^k \in \langle (r,0),(s,0),(e,1)\rangle$$

and consequently $D_n \rtimes_\theta \mathbb{Z}_2 \subseteq \langle (r,0),(s,0),(e,1)\rangle$. So $D_n \rtimes_\theta \mathbb{Z}_2 = \langle (r,0),(s,0),(e,1)\rangle$, as claimed. □

Now, we will show that a sequence of dihedral groups of order 2^n can be constructed by iterating semi-direct products.

Theorem 5.2. *Let G and H be groups and let $\varphi : G \longrightarrow H$ be a group homomor-*

phism. Then φ is injective if and only if $ker(\varphi) = \{e_H\}$.

Proof. For a proof, we refer the reader to [2]. □

Theorem 5.3. *Suppose that n is a positive integer no less than three. Let $a, b \in D_n$ such that $|a| = n$, $|b| = 2$, and $ab = ba^{-1}$. Moreover, let $\varphi_{a,b} : D_n \longrightarrow D_n$ be the homomorphism that maps r to a and s to b. Then $\varphi_{a,b} \in Aut(D_n)$.*

Proof. First, observe that $\varphi_{a,b}$ is a well-defined homomorphism, because it maps r to a and s to b where $a, b \in D_n$ satisfying $|a| = n$, $|b| = 2$, and $ab = ba^{-1}$. Since D_n is a finite group, to prove that $\varphi_{a,b}$ is bijective, it suffices to prove that it is injective. To do so, let $x \in D_n$ such that $\varphi_{a,b}(x) = e$. Then since $x \in D_n$, there exist integers i and j satisfying $0 \leq i \leq n-1$ and $0 \leq j \leq 1$ such that $x = r^i s^j$. Hence

$$\begin{aligned} a^i b^j &= (\varphi_{a,b}(r))^i (\varphi_{a,b}(s))^j \\ &= \varphi_{a,b}(r^i)\varphi_{a,b}(s^j) \\ &= \varphi_{a,b}(r^i s^j) \\ &= \varphi_{a,b}(x) = e. \end{aligned}$$

Thus, if $j = 1$, then $a^i = a^i e = a^i bb = a^i b^j b = eb = b$ and consequently

$$a^{1+i} = aa^i = ab = ba^{-1} = a^i a^{-1} = a^{i-1}.$$

Since $a^{1+i} = a^{i-1}$, we have

$$a^2 = a^{1+i-i+1} = a^{1+i}a^{-i+1} = a^{i-1}(a^{i-1})^{-1} = e$$

which is a contradiction, because $|a| = n \geq 3$.

So $j = 0$ and therefore $a^i = a^i e = a^i b^0 = a^i b^j = e$. Since $a^i = e$ and $|a| = n$, we have $i \equiv 0 \ (modn)$ which implies $i = 0$, because $0 \leq i \leq n-1$. Therefore

$x = r^i s^j = r^0 s^0 = ee = e$. Since $x \in D_n$ is an arbitrarily chosen element, this shows that $\varphi_{a,b}$ is injective, by Theorem 5.2. Hence $\varphi_{a,b} \in Aut(D_n)$, as claimed. □

Theorem 5.4. *Suppose that n is a positive integer no less than two. Then we have $D_{2^n} \rtimes_{\varphi_{r^{-1},rs}} \mathbb{Z}_2 \cong D_{2^{n+1}}$ where $\varphi_{r^{-1},rs} \in Aut(D_{2^n})$ maps r to r^{-1} and s to rs, and the semi-direct product $D_{2^n} \rtimes_{\varphi_{r^{-1},rs}} \mathbb{Z}_2$ is induced by the non-trivial homomorphism defined from $\mathbb{Z}_2$ to $Aut(D_{2^n})$ that maps 1 to $\varphi_{r^{-1},rs}$.*

Proof. First, observe that since $r^{-1}, rs \in D_{2^n}$ such that $|r^{-1}| = 2^n$, $|rs| = 2$, and $r^{-1}(rs) = (rs)(r^{-1})^{-1}$, we have $\varphi_{r^{-1},rs} \in Aut(D_{2^n})$, by Theorem 5.3. Now, suppose that $\psi : D_{2^{n+1}} \longrightarrow D_{2^n} \rtimes_{\varphi_{r^{-1},rs}} \mathbb{Z}_2$ is the group homomorphism that maps r to $(rs, 1)$ and s to $(s, 0)$. Observe that ψ is a well-defined homomorphism, because it maps r to $(rs, 1)$ and s to $(s, 0)$ where $(rs, 1), (s, 0) \in D_{2^n} \rtimes_{\varphi_{r^{-1},rs}} \mathbb{Z}_2$ satisfying $|(rs, 1)| = 2^{n+1}$, $|(s, 0)| = 2$, and $(rs, 1)(s, 0) = (s, 0)(rs, 1)^{-1}$. Since $D_{2^{n+1}}$ is a finite group, to prove that ψ is bijective, it suffices to prove that it is surjective. Since

$$\begin{aligned}
(r, 0) &= (rs, 1)(rs, 1) \\
&= \psi(r)\psi(r) \\
&= \psi(rr) \\
&= \psi(r^2) \in \psi(D_{2^{n+1}}), \\
(s, 0) &= \psi(s) \in \psi(D_{2^{n+1}}), and \\
(e, 1) &= (rs, 1)(rs, 1)(s, 0)(rs, 1) \\
&= \psi(r)\psi(r)\psi(s)\psi(r) \\
&= \psi(rrsr) \\
&= \psi(r^2 sr) \in \psi(D_{2^{n+1}}),
\end{aligned}$$

it can be concluded that $\langle (r,0),(s,0)(e,1)\rangle \subseteq \psi(D_{2^{n+1}})$. On the other hand,

$$D_{2^n} \rtimes_{\varphi_{r^{-1},rs}} \mathbb{Z}_2 = \langle (r,0),(s,0)(e,1)\rangle$$

and consequently

$$D_{2^n} \rtimes_{\varphi_{r^{-1},rs}} \mathbb{Z}_2 = \langle (r,0),(s,0)(e,1)\rangle \subseteq \psi(D_{2^{n+1}}) \subseteq D_{2^n} \rtimes_{\varphi_{r^{-1},rs}} \mathbb{Z}_2.$$

Hence $\psi(D_{2^{n+1}}) = D_{2^n} \rtimes_{\varphi_{r^{-1},rs}} \mathbb{Z}_2$. So ψ is surjective and therefore bijective. Thus $D_{2^n} \rtimes_{\varphi_{r^{-1},rs}} \mathbb{Z}_2 \cong D_{2^{n+1}}$, as claimed. □

Now, we will show, though, that $\{D_{2^n}\}_{n=1}^{\infty}$ gives a negative answer to our main question.

Lemma 5.5. *For every even positive integer $n > 2$, $(D_n)' = \langle r^2\rangle$.*

Proof. Let $\psi : D_n \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ be the group homomorphism that maps r to $(1,0)$ and s to $(0,1)$. First, observe that ψ is a well-defined homomorphism, because it maps r to $(1,0)$ and s to $(0,1)$ where $(1,0),(0,1) \in \mathbb{Z}_2 \times \mathbb{Z}_2$ satisfying $|(1,0)| = 2$, $|(0,1)| = 2$, and $(1,0)+(0,1) = (0,1)+(1,0)$. Since

$$\begin{aligned}
\psi(r^2) &= \psi(rr)\\
&= \psi(r)+\psi(r)\\
&= (1,0)+(1,0)\\
&= (1+1,0+0)\\
&= (0,0),\\
\psi(r) &= (1,0),\\
\psi(s) &= (0,1), and
\end{aligned}$$

$$\begin{aligned}\psi(rs) &= \psi(r)+\psi(s)\\ &= (1,0)+(0,1)\\ &= (1+0,0+1)\\ &= (1,1),\end{aligned}$$

ψ is surjective. Hence $D_n/ker(\psi) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ by the First Isomorphism Theorem. Since $D_n/ker(\psi) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ is an abelian group, $D_n/ker(\psi)$ is also an abelian group. Hence $D_n' \subseteq ker(\psi)$. Now, we will prove that $ker(\psi) = \langle r^2 \rangle$. To do so, let $x \in ker(\psi) \subseteq D_n$. Then $\psi(x) = (0,0)$ and $x = r^i s^j$ where i and j are integers with $0 \leq i \leq n-1$ and $0 \leq j \leq 1$. Since ψ is a homomorphism,

$$\begin{aligned}(0,0) &= \psi(x)\\ &= \psi(r^i s^j)\\ &= \psi(r^i)+\psi(s^j)\\ &= i\psi(r)+j\psi(s)\\ &= i(1,0)+j(0,1)\\ &= (i,j)\end{aligned}$$

which implies $i \equiv 0(mod\ 2)$ and $j \equiv 0(mod\ 2)$. Hence there exists an integer k with $0 \leq k \leq \frac{n-1}{2}$ such that $i = 2k$ and $j = 0$. Thus $x = r^i s^j = r^{2k} s^0 = (r^2)^k \in \langle r^2 \rangle$ and consequently $ker(\psi) \subseteq \langle r^2 \rangle$. Conversely, since $\psi(r^2) = (0,0)$, $r^2 \in ker(\psi)$ and consequently $\langle r^2 \rangle \subseteq ker(\psi)$. So $ker(\psi) = \langle r^2 \rangle$. Since $D_n' \subseteq ker(\psi)$ and $ker(\psi) = \langle r^2 \rangle$,

$D_n' \subseteq \langle r^2 \rangle$. On the other hand, since

$$\begin{aligned} r^2 &= rr \\ &= rer \\ &= rs^2r \\ &= rssr \\ &= sr^{-1}sr \\ &= s^{-1}r^{-1}sr \\ &= [s,r] \in D_n', \end{aligned}$$

$\langle r^2 \rangle \subseteq D_n'$. Therefore $D_n' = \langle r^2 \rangle$, as claimed. □

Lemma 5.6. *For every even positive integer $n > 2$, $(D_n)'$ is an abelian group.*

Proof. By Lemma 5.5, $D_n' = \langle r^2 \rangle$. On the other hand, $\langle r^2 \rangle$ is a cyclic group and every cyclic group is an abelian group. Therefore $(D_n)'$ is an abelian group, as claimed. □

Remark. Corollary 4.8 and Lemma 5.5 show that the automorphisms $\varphi_{r^{-1},rs}$ are outer.

Lemma 5.7. *For every positive integer $n > 1$, $|(D_{2^n})'| = 2^{n-1}$ and $|D_{2^n}/(D_{2^n})'| = 4$.*

Proof. Since $D_{2^n}' = \langle r^2 \rangle$ and $|r| = 2^n$,

$$\begin{aligned} |D_{2^n}'| &= |\langle r^2 \rangle| \\ &= |r^2| \\ &= \frac{|r|}{gcd(2,|r|)} \\ &= \frac{2^n}{gcd(2,2^n)} \\ &= \frac{2^n}{2} \end{aligned}$$

$$= \quad 2^{n-1}$$

and consequently

$$\begin{aligned} |D_{2^n}/(D_{2^n})'| &= \frac{|D_{2^n}|}{|(D_{2^n})'|} \\ &= \frac{2^{n+1}}{2^{n-1}} \\ &= 4, \end{aligned}$$

as claimed. □

Lemma 5.8. *For every positive integer $n > 1$, $|(D_{2^n})'/(D_{2^n})''| = 2^{n-1}$.*

Proof. Since $(D_n)'$ is an abelian group, $(D_n)'' = ((D_n)')' = \{e\}$ and consequently $|(D_n)''| = |\{e\}| = 1$. On the other hand, $|(D_{2^n})'| = 2^{n-1}$. So

$$\begin{aligned} |(D_{2^n})'/(D_{2^n})''| &= \frac{|(D_{2^n})'|}{|(D_{2^n})''|} \\ &= \frac{2^{n-1}}{1} \\ &= 2^{n-1}, \end{aligned}$$

as claimed. □

Theorem 5.9. *The sequence $\{D_{2^n}\}_{n=1}^{\infty}$ is not potentially expanding.*

Proof. This follows immediately from Lemma 5.8 and Definition 2.12. □

CHAPTER 6

A Non-Potentially Expanding Sequence of Finite Groups

In this chapter we will present some specific semi-direct products of D_{2^n} and $\mathbb{Z}_2$. Using these specific semi-direct products, at the end of the chapter, we will present a sequence of finite groups that is not potentially expanding.

Lemma 6.1. *Let m and n be positive integers such that $0 < 2m+1 < 2^n$. Let $\varphi_{r^{2m+1},s}$ be the automorphism of D_{2^n} that maps r to r^{2m+1} and s to s. Then $\varphi_{r^{2m+1},s}$ is of order one or two if and only if $m(m+1) \equiv 0(mod\ 2^{n-2})$.*

Proof. First, observe that

$$\begin{aligned} |r^{2m+1}| &= \frac{|r|}{gcd(2m+1, |r|)} \\ &= \frac{2^n}{gcd(2m+1, 2^n)} \\ &= \frac{2^n}{1} \\ &= 2^n. \end{aligned}$$

Hence $\varphi_{r^{2m+1},s}$ is a well-defined homomorphism, because it maps r to r^{2m+1} and s to s where $r^{2m+1}, s \in D_{2^n}$ satisfying $|r^{2m+1}| = 2^n$, $|s| = 2$, and $r^{2m+1}s = s(r^{2m+1})^{-1}$. Also, notice that $m(m+1) \equiv 0(mod\ 2^{n-2})$ if and only if $4m(m+1) \equiv 0(mod\ 2^n)$ if and only if $4m^2 + 4m \equiv 0(mod\ 2^n)$ if and only if $4m^2 + 4m + 1 \equiv 1(mod\ 2^n)$ if and only if $(2m+1)^2 \equiv 1(mod\ 2^n)$. Now, observe that $\varphi_{r^{2m+1},s}$ has order less than or equal to two if and only if

$$r = \varphi^2_{r^{2m+1},s}(r)$$

$$
\begin{aligned}
&= (\varphi_{r^{2m+1},s}\varphi_{r^{2m+1},s})(r) \\
&= \varphi_{r^{2m+1},s}(\varphi_{r^{2m+1},s}(r)) \\
&= \varphi_{r^{2m+1},s}(r^{2m+1}) \\
&= (\varphi_{r^{2m+1},s}(r))^{2m+1} \\
&= (r^{2m+1})^{2m+1} \\
&= r^{(2m+1)^2}
\end{aligned}
$$

if and only if

$$(2m+1)^2 \equiv 1(mod\ 2^n)$$

if and only if

$$m(m+1) \equiv 0(mod\ 2^{n-2}).$$

□

Lemma 6.2. *Let m and n be positive integers such that $0 < 2m+1 < 2^n$ and $m(m+1) \equiv 0(mod\ 2^{n-2})$. Let $\varphi_{r^{2m+1},s} \in Aut(D_{2^n})$ be the automorphism that maps r to r^{2m+1} and s to s. Then $(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)' = \langle (r^2, 0)\rangle$ where the semi-direct product $D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2$ is induced by the non-trivial homomorphism θ defined from $\mathbb{Z}_2$ to $Aut(D_{2^n})$ that maps 1 to $\varphi_{r^{2m+1},s}$.*

Proof. By Theorem 5.1, $D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2 = \langle (r,0), (s,0), (e,1)\rangle$. Now, suppose that $\psi : D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ is the group homomorphism that maps $(r,0)$ to $(1,0,0)$, $(s,0)$ to $(0,1,0)$, and $(e,1)$ to $(0,0,1)$.

First, we will prove that ψ is a group homomorphism. In order to do so, let $x, y \in D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2$. Then $x = (r^{i_1}s^{j_1}, k_1)$ and $y = (r^{i_2}s^{j_2}, k_2)$ where i_1, i_2, j_1, j_2,

k_1, and k_2 are integers with $0 \leq i_1 \leq 2^n - 1$, $0 \leq i_2 \leq 2^n - 1$, $0 \leq j_1 \leq 1$, $0 \leq j_2 \leq 1$, $0 \leq k_1 \leq 1$, and $0 \leq k_2 \leq 1$.

If $j_1 = 0$ and $k_1 = 0$, then

$$\begin{aligned}
\psi(xy) &= \psi((r^{i_1}s^{j_1}, k_1)(r^{i_2}s^{j_2}, k_2)) \\
&= \psi((r^{i_1}, 0)(r^{i_2}s^{j_2}, k_2)) \\
&= \psi((r^{i_1}\theta(0)(r^{i_2}s^{j_2}), 0 + k_2)) \\
&= \psi((r^{i_1}r^{i_2}s^{j_2}, k_2)) \\
&= \psi((r^{i_1+i_2}s^{j_2}, k_2)) \\
&= \psi((r^{i_1+i_2}, 0)(s^{j_2}, 0)(e, k_2)) \\
&= \psi((r, 0)^{i_1+i_2}(s, 0)^{j_2}(e, 1)^{k_2}) \\
&= \psi((r, 0)^{i_1+i_2}) + \psi((s, 0)^{j_2}) + \psi((e, 1)^{k_2}) \\
&= (i_1 + i_2)\psi((r, 0)) + j_2\psi((s, 0)) + k_2\psi((e, 1)) \\
&= i_1\psi((r, 0)) + i_2\psi((r, 0)) + j_2\psi((s, 0)) + k_2\psi((e, 1)) \\
&= \psi((r, 0)^{i_1}) + \psi((r, 0)^{i_2}) + \psi((s, 0)^{j_2}) + \psi((e, 1)^{k_2}) \\
&= \psi((r, 0)^{i_1}) + \psi((r, 0)^{i_2}(s, 0)^{j_2}(e, 1)^{k_2}) \\
&= \psi((r^{i_1}, 0)) + \psi((r^{i_2}, 0)(s^{j_2}, 0)(e, k_2)) \\
&= \psi((r^{i_1}s^{j_1}, k_1)) + \psi((r^{i_2}s^{j_2}, k_2)) \\
&= \psi(x) + \psi(y).
\end{aligned}$$

If $j_1 = 1$ and $k_1 = 0$, then

$$\psi(xy) = \psi((r^{i_1}s^{j_1}, k_1)(r^{i_2}s^{j_2}, k_2))$$

$$
\begin{aligned}
&= \psi((r^{i_1}s,0)(r^{i_2}s^{j_2},k_2)) \\
&= \psi((r^{i_1}s\theta(0)(r^{i_2}s^{j_2}),0+k_2)) \\
&= \psi((r^{i_1}sr^{i_2}s^{j_2},k_2)) \\
&= \psi((r^{i_1}r^{-i_2}ss^{j_2},k_2)) \\
&= \psi((r^{i_1-i_2}s^{1+j_2},k_2)) \\
&= \psi((r^{i_1-i_2},0)(s^{1+j_2},0)(e,k_2)) \\
&= \psi((r,0)^{i_1-i_2}(s,0)^{1+j_2}(e,1)^{k_2}) \\
&= \psi((r,0)^{i_1-i_2})+\psi((s,0)^{1+j_2})+\psi((e,1)^{k_2}) \\
&= (i_1-i_2)\psi((r,0))+(1+j_2)\psi((s,0))+k_2\psi((e,1)) \\
&= (i_1+i_2)\psi((r,0))+(1+j_2)\psi((s,0))+k_2\psi((e,1)) \\
&= i_1\psi((r,0))+i_2\psi((r,0))+\psi((s,0))+j_2\psi((s,0))+k_2\psi((e,1)) \\
&= i_1\psi((r,0))+\psi((s,0))+i_2\psi((r,0))+j_2\psi((s,0))+k_2\psi((e,1)) \\
&= \psi((r,0)^{i_1})+\psi((s,0))+\psi((r,0)^{i_2})+\psi((s,0)^{j_2})+\psi((e,1)^{k_2}) \\
&= \psi((r,0)^{i_1}(s,0))+\psi((r,0)^{i_2}(s,0)^{j_2}(e,1)^{k_2}) \\
&= \psi((r^{i_1},0)(s,0))+\psi((r^{i_2},0)(s^{j_2},0)(e,k_2)) \\
&= \psi((r^{i_1}s,k_1))+\psi((r^{i_2}s^{j_2},k_2)) \\
&= \psi((r^{i_1}s^{j_1},k_1))+\psi((r^{i_2}s^{j_2},k_2)) \\
&= \psi(x)+\psi(y).
\end{aligned}
$$

If $j_1 = 0$ and $k_1 = 1$, then

$$
\psi(xy) = \psi((r^{i_1}s^{j_1},k_1)(r^{i_2}s^{j_2},k_2))
$$

$$\begin{aligned}
&= \psi((r^{i_1},1)(r^{i_2}s^{j_2},k_2)) \\
&= \psi((r^{i_1}\theta(1)(r^{i_2}s^{j_2}),1+k_2)) \\
&= \psi((r^{i_1}(r^{2m+1})^{i_2}s^{j_2},1+k_2)) \\
&= \psi((r^{i_1}r^{(2m+1)i_2}s^{j_2},1+k_2)) \\
&= \psi((r^{i_1+(2m+1)i_2}s^{j_2},1+k_2)) \\
&= \psi((r^{i_1+(2m+1)i_2},0)(s^{j_2},0)(e,1+k_2)) \\
&= \psi((r,0)^{i_1+(2m+1)i_2}(s,0)^{j_2}(e,1)^{1+k_2}) \\
&= \psi((r,0)^{i_1+(2m+1)i_2})+\psi((s,0)^{j_2})+\psi((e,1)^{1+k_2}) \\
&= (i_1+(2m+1)i_2)\psi((r,0))+j_2\psi((s,0))+(1+k_2)\psi((e,1)) \\
&= (i_1+i_2)\psi((r,0))+j_2\psi((s,0))+(1+k_2)\psi((e,1)) \\
&= i_1\psi((r,0))+i_2\psi((r,0))+j_2\psi((s,0))+\psi((e,1))+k_2\psi((e,1)) \\
&= i_1\psi((r,0))+\psi((e,1))+i_2\psi((r,0))+j_2\psi((s,0))+k_2\psi((e,1)) \\
&= \psi((r,0)^{i_1})+\psi((e,1))+\psi((r,0)^{i_2})+\psi((s,0)^{j_2})+\psi((e,1)^{k_2}) \\
&= \psi((r,0)^{i_1}(e,1))+\psi((r,0)^{i_2}(s,0)^{j_2}(e,1)^{k_2}) \\
&= \psi((r^{i_1},0)(e,1))+\psi((r^{i_2},0)(s^{j_2},0)(e,k_2)) \\
&= \psi((r^{i_1},1))+\psi((r^{i_2}s^{j_2},k_2)) \\
&= \psi((r^{i_1}s^{j_1},k_1))+\psi((r^{i_2}s^{j_2},k_2)) \\
&= \psi(x)+\psi(y).
\end{aligned}$$

If $j_1 = 1$ and $k_1 = 1$, then

$$\psi(xy) = \psi((r^{i_1}s^{j_1},k_1)(r^{i_2}s^{j_2},k_2))$$

$$
\begin{aligned}
&= \psi((r^{i_1}s,1)(r^{i_2}s^{j_2},k_2)) \\
&= \psi((r^{i_1}s\theta(1)(r^{i_2}s^{j_2}),1+k_2)) \\
&= \psi((r^{i_1}s(r^{2m+1})^{i_2}s^{j_2},1+k_2)) \\
&= \psi((r^{i_1}sr^{(2m+1)i_2}s^{j_2},1+k_2)) \\
&= \psi((r^{i_1}r^{-(2m+1)i_2}ss^{j_2},1+k_2)) \\
&= \psi((r^{i_1-(2m+1)i_2}s^{1+j_2},1+k_2)) \\
&= \psi((r^{i_1-(2m+1)i_2},0)(s^{1+j_2},0)(e,1+k_2)) \\
&= \psi((r,0)^{i_1-(2m+1)i_2}(s,0)^{1+j_2}(e,1)^{1+k_2}) \\
&= \psi((r,0)^{i_1-(2m+1)i_2})+\psi((s,0)^{1+j_2})+\psi((e,1)^{1+k_2}) \\
&= (i_1-(2m+1)i_2)\psi((r,0))+(1+j_2)\psi((s,0))+(1+k_2)\psi((e,1)) \\
&= (i_1-i_2)\psi((r,0))+(1+j_2)\psi((s,0))+(1+k_2)\psi((e,1)) \\
&= (i_1+i_2)\psi((r,0))+(1+j_2)\psi((s,0))+(1+k_2)\psi((e,1)) \\
&= i_1\psi((r,0))+i_2\psi((r,0))+\psi((s,0))+j_2\psi((s,0))+\psi((e,1))+k_2\psi((e,1)) \\
&= i_1\psi((r,0))+\psi((s,0))+\psi((e,1))+i_2\psi((r,0))+j_2\psi((s,0))+k_2\psi((e,1)) \\
&= \psi((r,0)^{i_1})+\psi((s,0))+\psi((e,1))+\psi((r,0)^{i_2})+\psi((s,0)^{j_2})+\psi((e,1)^{k_2}) \\
&= \psi((r,0)^{i_1}(s,0)(e,1))+\psi((r,0)^{i_2}(s,0)^{j_2}(e,1)^{k_2}) \\
&= \psi((r^{i_1},0)(s,0)(e,1))+\psi((r^{i_2},0)(s^{j_2},0)(e,k_2)) \\
&= \psi((r^{i_1}s,1))+\psi((r^{i_2}s^{j_2},k_2)) \\
&= \psi((r^{i_1}s^{j_1},k_1))+\psi((r^{i_2}s^{j_2},k_2)) \\
&= \psi(x)+\psi(y).
\end{aligned}
$$

This shows that ψ is a group homomorphism, as claimed.

Second, we will prove that ψ is surjective. In order to do so, observe that since $\psi((r,0)) = (1,0,0)$, $\psi((s,0)) = (0,1,0)$, and $\psi((e,1)) = (0,0,1)$, we have

$$\langle (1,0,0),(0,1,0),(0,0,1)\rangle \leq \psi(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)$$

and consequently $\langle (1,0,0),(0,1,0),(0,0,1)\rangle = \psi(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)$, because obviously $\psi(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2) \leq \langle (1,0,0),(0,1,0),(0,0,1)\rangle$. Hence ψ is surjective, as claimed. So $(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)/ker(\psi) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ by the First Isomorphism Theorem. Since $(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)/ker(\psi) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ is an abelian group, $(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)/ker(\psi)$ is also an abelian group.

Hence $(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)' \subseteq ker(\psi)$. Now, we will prove that $ker(\psi) = \langle (r^2,0)\rangle$. To do so, let $x \in ker(\psi) \subseteq (D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)'$. Then $\psi(x) = (0,0,0)$ and $x = (r^i s^j, k)$ where i, j, and k are integers with $0 \leq i \leq n-1$, $0 \leq j \leq 1$, and $0 \leq k \leq 1$. Since ψ is a homomorphism,

$$\begin{aligned}
(0,0,0) &= \psi(x) \\
&= \psi((r^i s^j, k)) \\
&= \psi((r^i,0)(s^j,0)(e,k)) \\
&= \psi((r,0)^i (s,0)^j (e,1)^k) \\
&= \psi((r,0)^i) + \psi((s,0)^j) + \psi((e,1)^k) \\
&= i\psi((r,0)) + j\psi((s,0)) + k\psi((e,1)) \\
&= i(1,0,0) + j(0,1,0) + k(0,0,1) \\
&= (i,j,k)
\end{aligned}$$

which implies $i \equiv 0(mod\, 2)$, $j \equiv 0(mod\, 2)$, and $k \equiv 0(mod\, 2)$. Hence there exists an integer k with $0 \leq k \leq \frac{n-1}{2}$ such that $i = 2k$, $j = 0$, and $k = 0$. Thus

$$x = (r^i s^j, k) = (r^{2k} s^0, 0) = (r^2, 0)^k \in \langle (r^2, 0) \rangle$$

and consequently $ker(\psi) \subseteq \langle (r^2, 0) \rangle$.

Conversely, since $\psi((r^2, 0)) = (0, 0, 0)$, we have $(r^2, 0) \in ker(\psi)$ and consequently $\langle (r^2, 0) \rangle \subseteq ker(\psi)$. So $ker(\psi) = \langle (r^2, 0) \rangle$. Since $(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)' \subseteq ker(\psi)$ and $ker(\psi) = \langle (r^2, 0) \rangle$, $(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)' \subseteq \langle (r^2, 0) \rangle$. On the other hand, since

$$\begin{aligned}
(r^2, 0) &= (r, 0)(r, 0) \\
&= (r, 0)(e, 0)(r, 0) \\
&= (r, 0)(s^2, 0)(r, 0) \\
&= (r, 0)(s, 0)(s, 0)(r, 0) \\
&= (rs, 0)(s, 0)(r, 0) \\
&= (sr^{-1}, 0)(s, 0)(r, 0) \\
&= (s, 0)(r^{-1}, 0)(s, 0)(r, 0) \\
&= (s, 0)^{-1}(r, 0)^{-1}(s, 0)(r, 0) \\
&= [(s, 0), (r, 0)] \in (D_n \rtimes_\theta \mathbb{Z}_2)',
\end{aligned}$$

$\langle (r^2, 0) \rangle \subseteq (D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)'$. Therefore $(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)' = \langle (r^2, 0) \rangle$, as claimed. □

Now, suppose that m and n are positive integers satisfying $0 < 2m + 1 < 2^n$ and $\varphi_{r^{2m+1},s} \in Aut(D_{2^n})$ is the automorphism that maps r to r^{2m+1} and s to s, and the semi-direct product $D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2$ be induced by the non-trivial homomorphism defined from $\mathbb{Z}_2$ to $Aut(D_{2^n})$ that maps 1 to $\varphi_{r^{2m+1},s}$.

Lemma 6.3. *$(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)'$ is an abelian group.*

Proof. By Lemma 6.2, $(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)' = \langle (r^2, 0) \rangle$. On the other hand, $\langle (r^2, 0) \rangle$ is a cyclic group and every cyclic group is an abelian group. Therefore $(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)'$ is an abelian group, as claimed. □

Lemma 6.4. *$|(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)'| = 2^n$ and*

$$|(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)/(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)'| = 8.$$

Proof. Since $(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)' = \langle (r^2, 0) \rangle$ and $|(r, 0)| = 2^n$,

$$\begin{aligned} |(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)'| &= |\langle (r^2, 0) \rangle| \\ &= |(r^2, 0)| \\ &= \frac{|(r,0)|}{gcd(2, |(r,0)|)} \\ &= \frac{2^n}{gcd(2, 2^n)} \\ &= \frac{2^n}{2} \\ &= 2^{n-1} \end{aligned}$$

and consequently

$$\begin{aligned} |(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)/(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)'| &= \frac{|D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2|}{|(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)'|} \\ &= \frac{2^{n+2}}{2^{n-1}} \\ &= 8, \end{aligned}$$

as claimed. □

Corollary 6.5. $|(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)'/(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)''| = 2^{n-1}$.

Proof. Since $(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)'$ is an abelian group, we have

$$(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)'' = ((D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)')' = \{e\}$$

and consequently $|(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)''| = |\{e\}| = 1$. On the other hand, we have $|(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)'| = 2^{n-1}$. So

$$\begin{aligned} |(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)'/(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)''| &= \frac{|(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)'|}{|(D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2)''|} \\ &= \frac{2^{n-1}}{1} \\ &= 2^{n-1}, \end{aligned}$$

as claimed. □

Theorem 6.6. *The sequence* $\{D_{2^n} \rtimes_{\varphi_{r^{2m+1},s}} \mathbb{Z}_2\}_{n=1}^{\infty}$ *is not potentially expanding.*

Proof. This follows immediately from Corollary 6.5 and Definition 2.12. □

CHAPTER 7

Miscellaneous Computations

In this chapter we will start iterating semi-direct products of the integers modulo two. But, first we will present some important facts about some useful isomorphisms that will be used in the iteration process.

Definition 7.1. *Let G be a group and $x, y \in G$. Then x is said to be conjugate to y if there exists an element $g \in G$ such that $x = g^{-1}yg$.*

Theorem 7.2. *Let G be a group and $\sim$ be a relation on G defined as follows:*

$$x \sim y \text{ if and only if } x \text{ is conjugate to } y.$$

Then $\sim$ is an equivalence relation that partitions G into equivalence classes, called the conjugacy classes of G.

Proof. For a proof, we refer the reader to [2]. □

Theorem 7.3. *Let G be a group and θ_1 and θ_2 be group homomorphisms defined from $\mathbb{Z}_2$ to $Aut(G)$ with $(\theta_1(1))^{\theta} = \theta_2(1)$ where $\theta \in Aut(G)$ and $(\theta_1(1))^{\theta} = \theta^{-1}\theta_1(1)\theta$ is the conjugate of $\theta_1(1)$ by θ. Then $G \rtimes_{\theta_1} \mathbb{Z}_2 \cong G \rtimes_{\theta_2} \mathbb{Z}_2$. In other words, if θ_1 and θ_2 are two homomorphisms defined from $\mathbb{Z}_2$ to $Aut(G)$ such that $\theta_1(1)$ and $\theta_2(1)$ are two conjugate elements of $Aut(G)$, then θ_1 and θ_2 will induce isomorphic semi-direct products of G and $\mathbb{Z}_2$.*

Proof. Define $\varphi : G \rtimes_{\theta_1} \mathbb{Z}_2 \longrightarrow G \rtimes_{\theta_2} \mathbb{Z}_2$ by $\varphi(g, m) = (\theta^{-1}(g), m)$. We will prove that φ is a group isomorphism. First, we will prove that φ is a group homomorphism. To do so, let $(g,m),(h,n) \in G \rtimes_{\theta_1} \mathbb{Z}_2$. If $m=0$, then

$$\begin{aligned}
\varphi((g,m)(h,n)) &= \varphi((g,0)(h,n)) \\
&= \varphi(g\theta_1(0)(h), 0+n) \\
&= \varphi(gh,n) \\
&= (\theta^{-1}(gh),n) \\
&= (\theta^{-1}(g)\theta^{-1}(h),n) \\
&= (\theta^{-1}(g)\theta_2(0)(\theta^{-1}(h)),0+n) \\
&= (\theta^{-1}(g),0)(\theta^{-1}(h),n) \\
&= \varphi(g,0)\varphi(h,n) \\
&= \varphi(g,m)\varphi(h,n).
\end{aligned}$$

If $m=1$, then

$$\begin{aligned}
\varphi((g,m)(h,n)) &= \varphi((g,1)(h,n)) \\
&= \varphi(g\theta_1(1)(h), 1+n) \\
&= (\theta^{-1}(g\theta_1(1)(h)),1+n) \\
&= (\theta^{-1}(g)\theta^{-1}(\theta_1(1)(h)),1+n) \\
&= (\theta^{-1}(g)(\theta^{-1}\theta_1(1))(h),1+n) \\
&= (\theta^{-1}(g)(\theta^{-1}\theta_1(1)\theta\theta^{-1})(h),1+n) \\
&= (\theta^{-1}(g)(\theta^{-1}\theta_1(1)\theta)(\theta^{-1}(h)),1+n) \\
&= (\theta^{-1}(g)\theta_2(1)(\theta^{-1}(h)),1+n) \\
&= (\theta^{-1}(g),1)(\theta^{-1}(h),n)
\end{aligned}$$

$$
\begin{aligned}
&= \varphi(g,1)\varphi(h,n) \\
&= \varphi(g,m)\varphi(h,n).
\end{aligned}
$$

This shows that φ is a group homomorphism.

Next, we will prove that φ is injective. To do so, let $\varphi(g,m) = \varphi(h,n)$ with $(g,m),(h,n) \in G \rtimes_{\theta_1} \mathbb{Z}_2$. Then $(\theta^{-1}(g),m) = \varphi(g,m) = \varphi(h,n) = (\theta^{-1}(h),n)$ and so $\theta^{-1}(g) = \theta^{-1}(h)$ and $m = n$. Since $\theta \in Aut(G)$ and $\theta^{-1}(g) = \theta^{-1}(h)$, $g = h$. Hence $(g,m) = (h,n)$. This shows that φ is injective.

Finally, we will prove that φ is surjective. In order to do so, let $(h,n) \in G \rtimes_{\theta_2} \mathbb{Z}_2$. Then $(\theta(h),n) \in G \rtimes_{\theta_1} \mathbb{Z}_2$ and $\varphi(\theta(h),n) = (\theta^{-1}(\theta(h)),n) = ((\theta^{-1}\theta)(h),n) = (h,n)$. This shows that φ is surjective. Hence φ is a group isomorphism and therefore $G \rtimes_{\theta_1} \mathbb{Z}_2 \cong G \rtimes_{\theta_2} \mathbb{Z}_2$, as claimed. □

Theorem 7.4. *Let $\phi_{a,b} : D_4 \longrightarrow D_4$ be the group homomorphism that maps r to $a \in \{r, r^3\}$ and s to $b \in \{s, rs, r^2s, r^3s\}$. Then we have $\phi_{a,b} \in Aut(D_4)$. Moreover, $Aut(D_4) = \{\phi_{r,s}, \phi_{r,rs}, \phi_{r,r^2s}, \phi_{r,r^3s}, \phi_{r^3,s}, \phi_{r^3,rs}, \phi_{r^3,r^2s}, \phi_{r^3,r^3s}\}$.*

Proof. A straight forward computation shows that for every $a \in \{r, r^3\}$ and for every $b \in \{s, rs, r^2s, r^3s\}$, we have $|a| = 4$, $|b| = 2$, and $ab = ba^{-1}$. Hence $\phi_{a,b}$ is a well-defined homomorphism, because it maps r to a and s to b where $a \in \{r, r^3\}$ and $b \in \{s, rs, r^2s, r^3s\}$ satisfying $|a| = 4$, $|b| = 2$, and $ab = ba^{-1}$. Table 7.1 shows that each element of $\{\phi_{r,s}, \phi_{r,rs}, \phi_{r,r^2s}, \phi_{r,r^3s}, \phi_{r^3,s}, \phi_{r^3,rs}, \phi_{r^3,r^2s}, \phi_{r^3,r^3s}\}$ is bijective. So $\{\phi_{r,s}, \phi_{r,rs}, \phi_{r,r^2s}, \phi_{r,r^3s}, \phi_{r^3,s}, \phi_{r^3,rs}, \phi_{r^3,r^2s}, \phi_{r^3,r^3s}\} \subseteq Aut(D_4)$. On the other hand, since $D_4 = \langle r, s \mid r^4 = s^2 = e \textit{ and } rs = sr^{-1}\rangle$, each $\phi \in Aut(D_4)$ can be completely determined by its values at r and s. Moreover, since $s \notin Z(D_4)$ and $r^2 \in Z(D_4)$, for every $\phi \in Aut(D_4)$, $\phi(s) \neq r^2$. Furthermore, since for every $\phi \in Aut(D_4)$, $|\phi(r)| = |r| = 4$ and $|\phi(s)| = |s| = 2$, for every $\phi \in Aut(D_4)$, $\phi(r) \in \{r, r^3\}$ and $\phi(s) \in \{s, rs, r^2s, r^3s\}$.

Thus $|Aut(D_4)| \leq 8$ and consequently $|Aut(D_4)| = 8$. Since $|Aut(D_4)| = 8$ and $\{\phi_{r,s}, \phi_{r,rs}, \phi_{r,r^2s}, \phi_{r,r^3s}, \phi_{r^3,s}, \phi_{r^3,rs}, \phi_{r^3,r^2s}, \phi_{r^3,r^3s}\} \subseteq Aut(D_4)$, we have

$$Aut(D_4) = \{\phi_{r,s}, \phi_{r,rs}, \phi_{r,r^2s}, \phi_{r,r^3s}, \phi_{r^3,s}, \phi_{r^3,rs}, \phi_{r^3,r^2s}, \phi_{r^3,r^3s}\},$$

as claimed.

Table 7.1: *The elements of* $\{\phi_{r,s}, \phi_{r,rs}, \phi_{r,r^2s}, \phi_{r,r^3s}, \phi_{r^3,s}, \phi_{r^3,rs}, \phi_{r^3,r^2s}, \phi_{r^3,r^3s}\}$

x	e	r	r^2	r^3	s	rs	r^2s	r^3s
$\phi_{r,s}(x)$	e	r	r^2	r^3	s	rs	r^2s	r^3s
$\phi_{r,rs}(x)$	e	r	r^2	r^3	rs	r^2s	r^3s	s
$\phi_{r,r^2s}(x)$	e	r	r^2	r^3	r^2s	r^3s	s	rs
$\phi_{r,r^3s}(x)$	e	r	r^2	r^3	r^3s	s	rs	r^2s
$\phi_{r^3,s}(x)$	e	r^3	r^2	r	s	r^3s	r^2s	rs
$\phi_{r^3,rs}(x)$	e	r^3	r^2	r	rs	s	r^3s	r^2s
$\phi_{r^3,r^2s}(x)$	e	r^3	r^2	r	r^2s	rs	s	r^3s
$\phi_{r^3,r^3s}(x)$	e	r^3	r^2	r	r^3s	r^2s	rs	s

□

Theorem 7.5. *$D_4 \cong Aut(D_4)$.*

Proof. A straightforward computation shows that

$$\phi_{r,rs}^4 = \phi_{r^3,s}^2 = id$$

and

$$\phi_{r,rs}\phi_{r^3,s} = \phi_{r^3,s}\phi_{r,rs}^{-1}.$$

So there exists a well-defined homomorphism $\psi : D_4 \longrightarrow Aut(D_4)$ that maps r to $\phi_{r,rs}$ and s to $\phi_{r^3,s}$. By Theorem 7.4, ψ is surjective. Hence ψ is an isomorphism, by the Pigeon-Hole Principle. Therefore $D_4 \cong Aut(D_4)$, as claimed. □

Theorem 7.6. *Let $\phi_{a,b} : \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ be the group homomorphism that maps $(0,1)$ to a and $(1,0)$ to b where $a, b \in \{(0,1),(1,0),(1,1)\}$ and $a \neq b$. Then $Aut(\mathbb{Z}_2 \times \mathbb{Z}_2) = \{\phi_{a,b} \mid a, b \in \{(0,1),(1,0),(1,1)\} \text{ and } a \neq b\}$.*

Proof. Table 7.2 shows that each element of

$$\{\phi_{a,b} \mid a, b \in \{(0,1),(1,0),(1,1)\} \textit{ and } a \neq b\}$$

is bijective. So $\{\phi_{a,b} \mid a, b \in \{(0,1),(1,0),(1,1)\} \textit{ and } a \neq b\} \subseteq Aut(\mathbb{Z}_2 \times \mathbb{Z}_2)$.

On the other hand, since $\mathbb{Z}_2 \times \mathbb{Z}_2 = \langle (0,1),(1,0) \rangle$, each $\phi \in Aut(\mathbb{Z}_2 \times \mathbb{Z}_2)$ can be completely determined by its values at $(0,1)$ and $(1,0)$. Moreover, since for every $\phi \in Aut(\mathbb{Z}_2 \times \mathbb{Z}_2)$, $|\phi((0,1))| = |(0,1)| = 2$ and $|\phi((1,0))| = |(1,0)| = 2$, for every $\phi \in Aut(\mathbb{Z}_2 \times \mathbb{Z}_2)$, $\phi((0,1)), \phi((1,0)) \in \{(0,1),(1,0),(1,1)\}$. Thus $|Aut(\mathbb{Z}_2 \times \mathbb{Z}_2)| \leq 6$ and consequently $|Aut(\mathbb{Z}_2 \times \mathbb{Z}_2)| = 6$.

Since $|Aut(\mathbb{Z}_2 \times \mathbb{Z}_2)| = 6$ and

$$\{\phi_{a,b} \mid a, b \in \{(0,1),(1,0),(1,1)\} \textit{ and } a \neq b\} \subseteq Aut(\mathbb{Z}_2 \times \mathbb{Z}_2),$$

we have

$$Aut(\mathbb{Z}_2 \times \mathbb{Z}_2) = \{\phi_{a,b} \mid a, b \in \{(0,1),(1,0),(1,1)\} \textit{ and } a \neq b\},$$

as claimed.

Table 7.2: *The elements of* $\{\phi_{a,b} \mid a, b \in \{(0,1),(1,0),(1,1)\}$ *and* $a \neq b\}$

x	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$\phi_{(0,1),(1,0)}(x)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$\phi_{(1,0),(0,1)}(x)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$\phi_{(1,1),(1,0)}(x)$	$(0,0)$	$(1,1)$	$(1,0)$	$(0,1)$
$\phi_{(0,1),(1,1)}(x)$	$(0,0)$	$(0,1)$	$(1,1)$	$(1,0)$
$\phi_{(1,0),(1,1)}(x)$	$(0,0)$	$(1,0)$	$(1,1)$	$(0,1)$
$\phi_{(1,1),(0,1)}(x)$	$(0,0)$	$(1,1)$	$(0,1)$	$(1,0)$

□

Theorem 7.7. $S_3 \cong Aut(\mathbb{Z}_2 \times \mathbb{Z}_2)$

Proof. Table 7.3 shows that $\psi : S_3 \longrightarrow Aut(\mathbb{Z}_2 \times \mathbb{Z}_2)$ is a well-defined bijective function and Table 7.4 shows that ψ is a homomorphism.

Table 7.3: ψ *is a bijection*

x	(1)	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
$\psi(x)$	$\phi_{(0,1),(1,0)}$	$\phi_{(1,0),(0,1)}$	$\phi_{(1,1),(1,0)}$	$\phi_{(0,1),(1,1)}$	$\phi_{(1,0),(1,1)}$	$\phi_{(1,1),(0,1)}$

Table 7.4: ψ *is a homomorphism*

	$\phi_{(0,1),(1,0)}$	$\phi_{(1,0),(0,1)}$	$\phi_{(1,1),(1,0)}$	$\phi_{(0,1),(1,1)}$	$\phi_{(1,0),(1,1)}$	$\phi_{(1,1),(0,1)}$
$\phi_{(0,1),(1,0)}$	$\phi_{(0,1),(1,0)}$	$\phi_{(1,0),(0,1)}$	$\phi_{(1,1),(1,0)}$	$\phi_{(0,1),(1,1)}$	$\phi_{(1,0),(1,1)}$	$\phi_{(1,1),(0,1)}$
$\phi_{(1,0),(0,1)}$	$\phi_{(1,0),(0,1)}$	$\phi_{(0,1),(1,0)}$	$\phi_{(1,1),(0,1)}$	$\phi_{(1,0),(1,1)}$	$\phi_{(0,1),(1,1)}$	$\phi_{(1,1),(1,0)}$
$\phi_{(1,1),(1,0)}$	$\phi_{(1,1),(1,0)}$	$\phi_{(1,0),(1,1)}$	$\phi_{(0,1),(1,0)}$	$\phi_{(1,1),(0,1)}$	$\phi_{(1,0),(0,1)}$	$\phi_{(0,1),(1,1)}$

	$\phi_{(0,1),(1,0)}$	$\phi_{(1,0),(0,1)}$	$\phi_{(1,1),(1,0)}$	$\phi_{(0,1),(1,1)}$	$\phi_{(1,0),(1,1)}$	$\phi_{(1,1),(0,1)}$
$\phi_{(0,1),(1,1)}$	$\phi_{(0,1),(1,1)}$	$\phi_{(1,1),(0,1)}$	$\phi_{(1,0),(1,1)}$	$\phi_{(0,1),(1,0)}$	$\phi_{(1,1),(1,0)}$	$\phi_{(1,0),(0,1)}$
$\phi_{(1,0),(1,1)}$	$\phi_{(1,0),(1,1)}$	$\phi_{(1,1),(1,0)}$	$\phi_{(0,1),(1,1)}$	$\phi_{(1,0),(0,1)}$	$\phi_{(1,1),(0,1)}$	$\phi_{(0,1),(1,0)}$
$\phi_{(1,1),(0,1)}$	$\phi_{(1,1),(0,1)}$	$\phi_{(0,1),(1,1)}$	$\phi_{(1,0),(0,1)}$	$\phi_{(1,1),(1,0)}$	$\phi_{(0,1),(1,0)}$	$\phi_{(1,0),(1,1)}$

Hence $S_3 \cong Aut(\mathbb{Z}_2 \times \mathbb{Z}_2)$, as claimed. □

Now, we begin constructing groups in a recursive manner by starting with $\mathbb{Z}_2$, the additive group of the integers modulo two, and by forming a semi-direct product with $\mathbb{Z}_2$ at each step.

First Step:

Let $G_1 = \mathbb{Z}_2$. Since $Aut(G_1)$ is the trivial group, the only possible semi-direct product of G_1 and $\mathbb{Z}_2$ is their direct product.

Second Step:

Let $G_2 = G_1 \rtimes_{\theta_1} \mathbb{Z}_2$ where θ_1 is the trivial homomorphism defined from $\mathbb{Z}_2$ to $Aut(G_1)$. Since $G_2 = G_1 \rtimes_{\theta_1} \mathbb{Z}_2 = \mathbb{Z}_2 \times \mathbb{Z}_2$ and $Aut(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$, $Aut(G_2) \cong S_3$ and consequently the collection of all conjugacy classes of $Aut(G_2)$ whose elements are automorphisms of order two is $\{\{\phi_{(1,0),(0,1)}, \phi_{(1,1),(1,0)}, \phi_{(0,1),(1,1)}\}\}$. The elements of the conjugacy class $\{\phi_{(1,0),(0,1)}, \phi_{(1,1),(1,0)}, \phi_{(0,1),(1,1)}\}$ are defined in Table 7.5.

Table 7.5: *The elements of the conjugacy class* $\{\phi_{(1,0),(0,1)}, \phi_{(1,1),(1,0)}, \phi_{(0,1),(1,1)}\}$

x	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$\phi_{(1,0),(0,1)}(x)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$\phi_{(1,1),(1,0)}(x)$	$(0,0)$	$(1,1)$	$(1,0)$	$(0,1)$
$\phi_{(0,1),(1,1)}(x)$	$(0,0)$	$(0,1)$	$(1,1)$	$(1,0)$

Therefore, all non-trivial homomorphisms defined from $\mathbb{Z}_2$ to $Aut(G_2)$ induce isomorphic semi-direct products of G_2 and $\mathbb{Z}_2$.

Third Step:

Let $G_3 = G_2 \rtimes_{\theta_2} \mathbb{Z}_2$ where θ_2 is a non-trivial homomorphism defined from $\mathbb{Z}_2$ to $Aut(G_2)$. Since $G_3 \cong D_4 \cong Aut(D_4)$, the conjugacy classes of $Aut(G_3)$ whose elements are automorphisms of order two are as follows:

The conjugacy class $\{\phi_{r,r^2s}\}$ whose element is defined in Table 7.6.

Table 7.6: *The definitions of* ϕ_{r,r^2s}

x	e	r	r^2	r^3	s	rs	r^2s	r^3s
$\phi_{r,r^2s}(x)$	e	r	r^2	r^3	r^2s	r^3s	s	rs

The conjugacy class $\{\phi_{r^3,s}, \phi_{r^3,r^2s}\}$ whose elements are defined in Table 7.7.

Table 7.7: *The definitions of* $\phi_{r^3,s}$ *and* ϕ_{r^3,r^2s}

x	e	r	r^2	r^3	s	rs	r^2s	r^3s
$\phi_{r^3,s}(x)$	e	r^3	r^2	r	s	r^3s	r^2s	rs
$\phi_{r^3,r^2s}(x)$	e	r^3	r^2	r	r^2s	rs	s	r^3s

The conjugacy class $\{\phi_{r^3,rs}, \phi_{r^3,r^3s}\}$ whose elements are defined in Table 7.8.

Table 7.8: *The definitions of* $\phi_{r^3,rs}$ *and* ϕ_{r^3,r^3s}

x	e	r	r^2	r^3	s	rs	r^2s	r^3s
$\phi_{r^3,rs}(x)$	e	r^3	r^2	r	rs	s	r^3s	r^2s
$\phi_{r^3,r^3s}(x)$	e	r^3	r^2	r	r^3s	r^2s	rs	s

Using cycle graphs, we can show that no two of the semi-direct products induced by ϕ_{r,r^2s}, $\phi_{r^3,s}$, and $\phi_{r^3,rs}$ are isomorphic (see Figures 7.1, 7.2, and 7.3). Therefore, there exist at most four non-isomorphic semi-direct products of G_3 and $\mathbb{Z}_2$ that are listed below:

1) The semi-direct product $G_3 \rtimes_{\phi_{r,r^2s}} \mathbb{Z}_2$ induced by the non-trivial homomorphism defined from $\mathbb{Z}_2$ to $Aut(G_3)$ that maps 1 to ϕ_{r,r^2s}. This group of order sixteen is isomorphic to the group of Pauli matrices that was used by, then named after, the Austrian-born physicist Wolfgang Pauli in his 1925 study of spin in quantum mechanics (see Figure 7.1).

2) The semi-direct product $G_3 \rtimes_{\phi_{r^3,s}} \mathbb{Z}_2$ induced by the non-trivial homomorphism defined from $\mathbb{Z}_2$ to $Aut(G_3)$ that maps 1 to $\phi_{r^3,s}$ (see Figure 7.2).

3) The semi-direct product $G_3 \rtimes_{\phi_{r^3,rs}} \mathbb{Z}_2 \cong D_8$ induced by the non-trivial homomorphism defined from $\mathbb{Z}_2$ to $Aut(G_3)$ that maps 1 to $\phi_{r^3,rs}$ (see Figure 7.3).

4) $G_3 \times \mathbb{Z}_2$.

Fourth Step:

Let $G_4 = G_3 \rtimes_{\theta_3} \mathbb{Z}_2$ where θ_3 is the non-trivial homomorphism defined from $\mathbb{Z}_2$ to $Aut(G_3)$ that maps 1 to $\phi_{r^3,rs}$. Since $G_4 \cong D_8$, the conjugacy classes of $Aut(G_4)$ whose elements are automorphisms of order two are as follows:

The conjugacy class $\{\phi_{r,r^4s}\}$ whose element is defined in Table 7.9.

Table 7.9: *The definition of* ϕ_{r,r^4s}

x	e	r	r^2	r^3	r^4	r^5	r^6	r^7
$\phi_{r,r^4s}(x)$	e	r	r^2	r^3	r^4	r^5	r^6	r^7
x	s	rs	r^2s	r^3s	r^4s	r^5s	r^6s	r^7s
$\phi_{r,r^4s}(x)$	r^4s	r^5s	r^6s	r^7s	s	rs	r^2s	r^3s

The conjugacy class $\{\phi_{r^3,s}, \phi_{r^3,r^2s}, \phi_{r^3,r^4s}, \phi_{r^3,r^6s}\}$ whose elements are defined in tables 7.10, 7.11, 7.12, and 7.13:

Table 7.10: *The definition of* $\phi_{r^3,s}$

x	e	r	r^2	r^3	r^4	r^5	r^6	r^7
$\phi_{r^3,s}(x)$	e	r^3	r^6	r	r^4	r^7	r^2	r^5
x	s	rs	r^2s	r^3s	r^4s	r^5s	r^6s	r^7s
$\phi_{r^3,s}(x)$	s	r^3s	r^6s	rs	r^4s	r^7s	r^2s	r^5s

Table 7.11: *The definition of* ϕ_{r^3,r^2s}

x	e	r	r^2	r^3	r^4	r^5	r^6	r^7
$\phi_{r^3,r^2s}(x)$	e	r^3	r^6	r	r^4	r^7	r^2	r^5
x	s	rs	r^2s	r^3s	r^4s	r^5s	r^6s	r^7s
$\phi_{r^3,r^2s}(x)$	r^2s	r^5s	s	r^3s	r^6s	rs	r^4s	r^7s

Table 7.12: *The definition of* ϕ_{r^3,r^4s}

x	e	r	r^2	r^3	r^4	r^5	r^6	r^7
$\phi_{r^3,r^4s}(x)$	e	r^3	r^6	r	r^4	r^7	r^2	r^5
x	s	rs	r^2s	r^3s	r^4s	r^5s	r^6s	r^7s
$\phi_{r^3,r^4s}(x)$	r^4s	r^7s	r^2s	r^5s	s	r^3s	r^6s	rs

Table 7.13: *The definition of* ϕ_{r^3,r^6s}

x	e	r	r^2	r^3	r^4	r^5	r^6	r^7
$\phi_{r^3,r^6s}(x)$	e	r^3	r^6	r	r^4	r^7	r^2	r^5
x	s	rs	r^2s	r^3s	r^4s	r^5s	r^6s	r^7s
$\phi_{r^3,r^6s}(x)$	r^6s	rs	r^4s	r^7s	r^2s	r^5s	s	r^3s

The conjugacy class $\{\phi_{r^5,s}, \phi_{r^5,r^4s}\}$ whose elements are defined in Tables 7.14 and 7.15.

Table 7.14: *The definition of* $\phi_{r^5,s}$

x	e	r	r^2	r^3	r^4	r^5	r^6	r^7
$\phi_{r^5,s}(x)$	e	r^5	r^2	r^7	r^4	r	r^6	r^3
x	s	rs	r^2s	r^3s	r^4s	r^5s	r^6s	r^7s
$\phi_{r^5,s}(x)$	s	r^5s	r^2s	r^7s	r^4s	rs	r^6s	r^3s

Table 7.15: *The definition of* ϕ_{r^5,r^4s}

x	e	r	r^2	r^3	r^4	r^5	r^6	r^7
$\phi_{r^5,r^4s}(x)$	e	r^5	r^2	r^7	r^4	r	r^6	r^3
x	s	rs	r^2s	r^3s	r^4s	r^5s	r^6s	r^7s
$\phi_{r^5,r^4s}(x)$	r^4s	rs	r^6s	r^3s	s	r^5s	r^2s	r^7s

The conjugacy class $\{\phi_{r^7,s}, \phi_{r^7,r^2s}, \phi_{r^7,r^4s}, \phi_{r^7,r^6s}\}$ whose elements are defined in Tables 7.16, 7.17, 7.18, and 7.19.

Table 7.16: *The definition of* $\phi_{r^7,s}$

x	e	r	r^2	r^3	r^4	r^5	r^6	r^7
$\phi_{r^7,s}(x)$	e	r^7	r^6	r^5	r^4	r^3	r^2	r
x	s	rs	r^2s	r^3s	r^4s	r^5s	r^6s	r^7s
$\phi_{r^7,s}(x)$	s	r^7s	r^6s	r^5s	r^4s	r^3s	r^2s	rs

Table 7.17: *The definition of* ϕ_{r^7,r^2s}

x	e	r	r^2	r^3	r^4	r^5	r^6	r^7
$\phi_{r^7,r^2s}(x)$	e	r^7	r^6	r^5	r^4	r^3	r^2	r
x	s	rs	r^2s	r^3s	r^4s	r^5s	r^6s	r^7s
$\phi_{r^7,r^2s}(x)$	r^2s	rs	s	r^7s	r^6s	r^5s	r^4s	r^3s

Table 7.18: *The definition of* ϕ_{r^7,r^4s}

x	e	r	r^2	r^3	r^4	r^5	r^6	r^7
$\phi_{r^7,r^4s}(x)$	e	r^7	r^6	r^5	r^4	r^3	r^2	r
x	s	rs	r^2s	r^3s	r^4s	r^5s	r^6s	r^7s
$\phi_{r^7,r^4s}(x)$	r^4s	r^3s	r^2s	rs	s	r^7s	r^6s	r^5s

Table 7.19: *The definition of* ϕ_{r^7,r^6s}

x	e	r	r^2	r^3	r^4	r^5	r^6	r^7
$\phi_{r^7,r^6s}(x)$	e	r^7	r^6	r^5	r^4	r^3	r^2	r
x	s	rs	r^2s	r^3s	r^4s	r^5s	r^6s	r^7s
$\phi_{r^7,r^6s}(x)$	r^6s	r^5s	r^4s	r^3s	r^2s	rs	s	r^7s

The conjugacy class $\{\phi_{r^7,rs}, \phi_{r^7,r^3s}, \phi_{r^7,r^5s}, \phi_{r^7,r^7s}\}$ whose elements are defined in Tables 7.20, 7.21, 7.22, and 7.23.

Table 7.20: *The definition of* $\phi_{r^7,rs}$

x	e	r	r^2	r^3	r^4	r^5	r^6	r^7
$\phi_{r^7,rs}(x)$	e	r^7	r^6	r^5	r^4	r^3	r^2	r
x	s	rs	r^2s	r^3s	r^4s	r^5s	r^6s	r^7s
$\phi_{r^7,rs}(x)$	rs	s	r^7s	r^6s	r^5s	r^4s	r^3s	r^2s

Table 7.21: *The definition of* ϕ_{r^7,r^3s}

x	e	r	r^2	r^3	r^4	r^5	r^6	r^7
$\phi_{r^7,r^3s}(x)$	e	r^7	r^6	r^5	r^4	r^3	r^2	r
x	s	rs	r^2s	r^3s	r^4s	r^5s	r^6s	r^7s
$\phi_{r^7,r^3s}(x)$	r^3s	r^2s	rs	s	r^7s	r^6s	r^5s	r^4s

Table 7.22: *The definition of* ϕ_{r^7,r^5s}

x	e	r	r^2	r^3	r^4	r^5	r^6	r^7
$\phi_{r^7,r^5s}(x)$	e	r^7	r^6	r^5	r^4	r^3	r^2	r
x	s	rs	r^2s	r^3s	r^4s	r^5s	r^6s	r^7s
$\phi_{r^7,r^5s}(x)$	r^5s	r^4s	r^3s	r^2s	rs	s	r^7s	r^6s

In each one of the conjugacy classes above, $\phi_{a,b} \in Aut(D_8)$ maps r to

$$a \in \{r, r^3, r^5, r^7\} \subset D_8$$

and s to

$$b \in \{s, rs, r^2s, r^3s, r^4s, r^5s, r^6s, r^7s\} \subset D_8.$$

Therefore there exist at most six non-isomorphic semi-direct products of G_4 and $\mathbb{Z}_2$ that are listed below:

1) The semi-direct product $G_4 \rtimes_{\phi_{r,r^4s}} \mathbb{Z}_2$ induced by the non-trivial homomorphism defined from $\mathbb{Z}_2$ to $Aut(G_4)$ that maps 1 to ϕ_{r,r^4s} (see Figure 7.4).

2) The semi-direct product $G_4 \rtimes_{\phi_{r^3,s}} \mathbb{Z}_2$ induced by the non-trivial homomorphism defined from $\mathbb{Z}_2$ to $Aut(G_3)$ that maps 1 to $\phi_{r^3,s}$ (see Figure 7.5).

Table 7.23: *The definition of* ϕ_{r^7,r^7s}

x	e	r	r^2	r^3	r^4	r^5	r^6	r^7
$\phi_{r^7,r^7s}(x)$	e	r^7	r^6	r^5	r^4	r^3	r^2	r
x	s	rs	r^2s	r^3s	r^4s	r^5s	r^6s	r^7s
$\phi_{r^7,r^7s}(x)$	r^7s	r^6s	r^5s	r^4s	r^3s	r^2s	rs	s

3) The semi-direct product $G_4 \rtimes_{\phi_{r^5,s}} \mathbb{Z}_2$ induced by the non-trivial homomorphism defined from $\mathbb{Z}_2$ to $Aut(G_3)$ that maps 1 to $\phi_{r^5,s}$ (see Figure 7.5).

4) The semi-direct product $G_4 \rtimes_{\phi_{r^7,s}} \mathbb{Z}_2$ induced by the non-trivial homomorphism defined from $\mathbb{Z}_2$ to $Aut(G_3)$ that maps 1 to $\phi_{r^7,s}$ (see Figure 7.6).

5) The semi-direct product $G_4 \rtimes_{\phi_{r^7,rs}} \mathbb{Z}_2$ induced by the non-trivial homomorphism defined from $\mathbb{Z}_2$ to $Aut(G_3)$ that maps 1 to $\phi_{r^7,rs}$ (see Figure 7.7).

6) $G_4 \times \mathbb{Z}_2$.

Fifth Step:

Let $G_5 = G_4 \rtimes_{\theta_4} \mathbb{Z}_2$ where θ_4 is the non-trivial homomorphism defined from $\mathbb{Z}_2$ to $Aut(G_4)$ that maps 1 to $\phi_{r^3,s}$. Then $G_5' = \langle (r^2, 0) \rangle$ where $r \in D_8$, by Lemma 6.2 when $m = 1$ and $n = 3$ (see Figure 7.8).

Sixth Step:

Let $G_6 = G_5 \rtimes_{\theta_5} \mathbb{Z}_2 = \langle a, b, c, d \rangle$ where $a = (r, 0, 0)$, $b = (s, 0, 0)$, $c = (e, 1, 0)$, and $d = (e, 0, 1)$ and θ_5 is the non-trivial homomorphism defined from $\mathbb{Z}_2$ to $Aut(G_5)$ that maps 1 to $\phi_{abc,c,b}$. Then $G_6' = \langle (a^2, bc) \rangle$ (see Figure 7.9).

LIST OF FIGURES

We can use cycle graphs (graphs that show relationships between powers of elements of a finite group) to distinguish the corresponding isomorphism classes. The following figures are the relevant cycle graphs.

Figure 7.1: The Cycle Graph of $G_3 \rtimes_{\phi_{r,r^2s}} \mathbb{Z}_2$

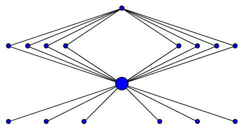


Figure 7.2: The Cycle Graph of $G_3 \rtimes_{\phi_{r^3,s}} \mathbb{Z}_2 \cong D_4 \times \mathbb{Z}_2$

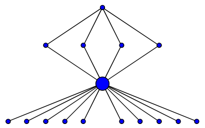


Figure 7.3: The Cycle Graph of $G_3 \rtimes_{\phi_{r^3,rs}} \mathbb{Z}_2 \cong D_8$

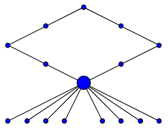


Figure 7.4: The Cycle Graph of $G_4 \rtimes_{\phi_{r,r^4s}} \mathbb{Z}_2$

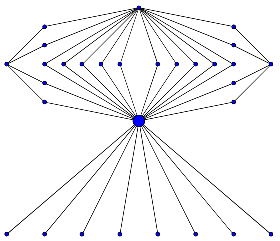


Figure 7.5: The Cycle Graph of $G_4 \rtimes_{\phi_{r^3,s}} \mathbb{Z}_2$ and $G_4 \rtimes_{\phi_{r^5,s}} \mathbb{Z}_2$

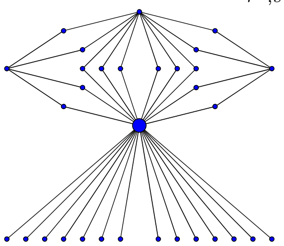


Figure 7.6: The Cycle Graph of $G_4 \rtimes_{\phi_{r^7,s}} \mathbb{Z}_2$

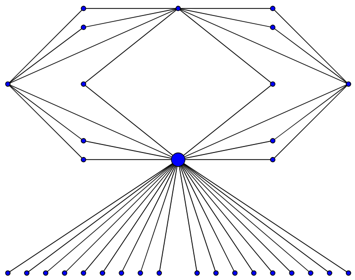


Figure 7.7: The Cycle Graph of $G_4 \rtimes_{\phi_{r^7,rs}} \mathbb{Z}_2$

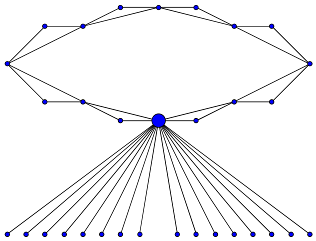


Figure 7.8: The Cycle Graph of $D_4 \times \mathbb{Z}_2^2$

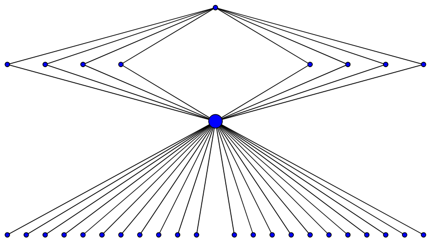
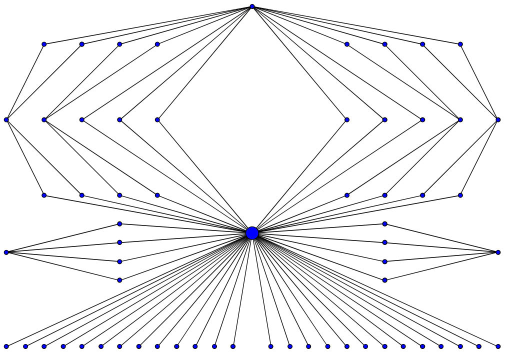


Figure 7.9: The Cycle Graph of $G_5 \rtimes_{\phi_{abc,c,b}} \mathbb{Z}_2$



REFERENCES

[1] Emmanuel Breuillard, Ben Green, and Terence Tao, *Suzuki groups as expanders*, Groups Geom. Dyn. **5** (2011), no. 2, 281–299. MR 2782174 (2012c:20066)

[2] David Dummit, *Abstract algebra*, Wiley, Hoboken, NJ, 2004.

[3] M. Krebs, private communication, 2012.

[4] M. Krebs and A. Shaheen, *Expander families and Cayley graphs: A beginner's guide*, Oxford University Press, USA, 2011.