

https://dspace.org/

Conjugacy classes of the automorphism group of a finite group

Motsisi, Rosina

2021
https://hdl.handle.net/10539/32471

Downloaded from a DSpace repository. https://dspace.org/



Masters Dissertation

Conjugacy classes of the automorphism group of a finite group

Author :

Motsisi Rosina

Supervisors :

Dr. R. Kwashira

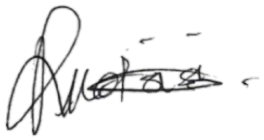
Dr. J. Mba

March 24, 2021

DECLARATION

I, Rosina Katlego Motsisi, (Student number: **867062**) am a student registered for MSc(Mathematics) in the year 2020. I hereby declare the following:

- I am aware that plagiarism (the use of someone else's work without their permission and/or without acknowledging the original source) is wrong.
- I confirm that ALL the work on the dissertation titled "Conjugacy classes of the automorphism group of a finite group" is my own work except where I have explicitly indicated otherwise.
- I have followed the required conventions in acknowledging all the main sources.
- I understand that the university may take disciplinary action against me if there is a belief that this in not my own work or that I have failed to acknowledge and reference the thoughts and ideas of others.



24/03/2021

Signature Date

Abstract

Let $\mathcal{K}$ denote the class of semi-direct products of the form $R = T \rtimes_\lambda \mathbb{Z}^k$, where $k \in \mathbb{Z}^+$, T is a finite abelian group and $\lambda : \mathbb{Z}^k \to Aut(T)$ is a group action. The non-cancellation set of R, denoted by $\chi(R)$ is the set of all isomorphism classes of groups Q such that $Q \times \mathbb{Z} \cong R \times \mathbb{Z}$. Various authors have studied the non-cancellation in the class of $\mathcal{K}$-groups. They have described the non-cancellation through conjugacy classes of $Aut(T)$ where T is a finite abelian group. We extend the study of the non-cancellation phenomena in the class of $\mathcal{K}$-group to the groups of the form $R = T \rtimes_\lambda \mathbb{Z}^k$ where T is a finite group but not necessarily abelian. We establish a link between the Nielsen equivalence classes and the conjugacy classes of $Aut(T)$. We then discuss the description of the non-cancellation set $\chi(R)$ through Nielsen equivalence classes.

Acknowledgements

I would like to express my earnest gratitude to my supervisors, Dr. R. Kwashira (University of the Witwatersrand) and Dr. J. Mba (University of Johannesburg), for their encouragement, guidance, contributions of time and ideas and for constantly reviewing my work.
I would also like to thank my parents, Ms. W. Motsisi and Mr. Z. Tembu, for their continued support throughout my study.

Contents

1 Introduction **5**

2 Preliminaries **8**

2.1 Groups and subgroups 8

2.2 Normal Subgroups 12

2.3 Homomorphisms 13

2.4 Conjugacy 16

2.5 Automorphisms 19

2.6 Group actions and Sylow theory 20

2.7 Direct and Semi-direct products 22

2.8 Finite abelian groups 23

2.9 Nilpotent groups 24

2.10 Rings 26

2.11 The automorphism group of finite groups 27

2.12 Subgroups of the automorphism group 31

3 Non-cancellation in the class of $\mathcal{K}$-groups **34**

3.1 The Nielsen equivalence relation 34

3.2 Isomorphisms in the class of $\mathcal{K}$-groups 41

3.3 Miller p-groups 53

4 Description of the non-cancellation set through Nielsen equivalence classes 59

4.1 The set of Nielsen equivalent classes 59

4.2 A link between the non-cancellation set and the set of Nielsen equivalence classes 68

5 Conclusion and further work 74

Chapter 1

Introduction

Let P be a finitely generated nilpotent group. In [20], G. Mislin introduced the notion of the genus set of a group P, denoted by $\mathcal{G}(P)$. He defined the Mislin genus set of P to be the set comprising of all isomorphism classes of finitely generated nilpotent groups M such that P and M have isomorphic p-localizations for all primes p. The author also presented the computation of the order of $\mathcal{G}(P)$, where P is a nilpotent group with a finite commutator subgroup.

Let $\mathcal{N}_0$ denote the class of finitely generated nilpotent groups with finite commutator subgroups. The notion of a genus set, applied to $\mathcal{N}_0$-groups was studied further in [10] and [11]. For a group P belonging to the $\mathcal{N}_0$-class, the authors in [10] defined an abelian group structure on the set $\mathcal{G}(P)$. In [11], Hilton constructed the genus set of $P \in \mathcal{N}_0$ and showed that $\mathcal{G}(P)$ is a cyclic group of finite order.

For any group R, the non-cancellation set of R, denoted by $\chi(R)$ is the set of all isomorphism classes $[Q]$ of groups Q such that $Q \times \mathbb{Z} \cong R \times \mathbb{Z}$ [29]. That is, the non-cancellation set measures the extent to which the infinite cyclic group $\mathbb{Z}$ cannot be cancelled as a direct factor in the isomorphism $R \times \mathbb{Z} \cong Q \times \mathbb{Z}$.

In [24], R. Warfield presented a result that relates the non-cancellation set and the Mislin genus sets of a finitely generated nilpotent group with finite commutator subgroup. The result states that for any $P \in \mathcal{N}_0$, the Mislin genus set of P coincides with the non-cancellation

set of P. That is $\chi(P) = \mathcal{G}(P)$.

Let $\mathcal{K}$ denote the class of semi-direct products of the form $T \rtimes_\lambda \mathbb{Z}^k$, where $k \in \mathbb{Z}^+$, T is a finite abelian group and $\lambda : \mathbb{Z}^k \to Aut(T)$ is a group action.
Motivated by Warfield's result, the non-cancellation phenomena was further studied in [26], [28], [22] and [29]. In [26], Witbooi studied isomorphisms in the class of $\mathcal{K}$-groups. He provided a sufficient condition that has to be satisfied in order for two $\mathcal{K}$-groups to be isomorphic [26, Theorem 2.3]. In [28], the author generalizes the Hilton-Mislin genus group and defines a group structure on the non-cancellation set of a finitely generated group with a finite commutator subgroup. Let $R = T \rtimes_\lambda \mathbb{Z}^k$. In [22], the authors describe the group structure on $\chi(R)$ through the notion of Nielsen equivalence classes, and the non-cancellation set through conjugate subgroups of $Aut(T)$. Two epimorphisms $f, g : \mathbb{Z}^k \to Aut(T)$ are said to be Nielsen equivalent if there exist $\alpha \in Aut(T)$ such that $f = g \circ \alpha$.

In this work, we extend the study of the non-cancellation phenomena in the class of $\mathcal{K}$-group to the groups of the form $R = T \rtimes_\lambda \mathbb{Z}^k$ where T is a finite group but not necessarily abelian. We study the notion of Nielsen equivalence relation since this is important when describing the non-cancellation set of a $\mathcal{K}$-group. Inspired by the work of [22], we investigate subgroups of the automorphism and determine the ones which have conjugates in $Aut(T)$. From our observation, the non-cancellation set cannot be trivial whenever the automorphism group of T is abelian. This result prompts us to investigate various cases of T which result in $Aut(T)$ being abelian. Lastly, we construct the elements of the set of Nielsen equivalence classes, denoted by $RE_k^{\sim_n}(B)$ where $B = Aut(T)$. We prove that $RE_k^{\sim_n}(B)$ is a cyclic group. We then establish an isomorphism between the non-cancellation set and the set of Nielsen equivalence classes.

The main purpose of Chapter 2 is to discuss basic results of group theory and lay a foundation of the work to be done in the later chapters.

In Chapter 3, we discuss some results contributed by the authors in [26], [28], [22] and [29] on the non-cancellation phenomena in the class of $\mathcal{K}$-groups.

We note that the results obtained on the non-cancellation phenomena in the class of $\mathcal{K}$-groups are restricted by the condition that T is a finite abelian group. Hence, in Chapter 4 we study the non-cancellation set of groups of the form $R = T \rtimes_\lambda \mathbb{Z}^k$, where T is a finite group but not necessarily abelian.

Chapter 2

Preliminaries

In this chapter, we recall basic concepts of group theory [5]. We will omit the proofs to most of the basic results as this can easily be found in any basic text on group theory.

2.1 Groups and subgroups

Definition 2.1.1.

Let R be a non empty set with a binary operation $*$. The set R is a **grou**p under the binary operation $*$ if the following conditions are satisfied:

1. $a * b \in R$ for every $a, b \in R$,
2. $a * (b * c) = (a * b) * c$ for every $a, b, c \in R$,
3. there exists an element e_R called the identity element such that $a * e_R = e_R * a = a$ for all $a \in R$,
4. for every element a in R there exists an element called the inverse of a, denoted by a^{-1} such that $a^{-1} * a = a * a^{-1} = e_R$.

We use $\langle R, * \rangle$ to denote a group under a binary operation $*$. If the binary operation $*$ is understood, we use R to denote the group. We assume that groups are **multiplicative** unless stated otherwise. That is, if we are told that R is a group but the binary operation is not explained, we assume that R is group under multiplication.

Definition 2.1.2.

Let R be a group. If $a * b = b * a$ for every $a, b \in R$ then R is called an **abelian** group.

Proposition 2.1.3. *Let R be a group under a binary operation *. The identity element $e_R \in R$ such that $a * e_R = e_R * a = a$ for all $a \in R$ is unique.*

Proposition 2.1.4. *Let R be a group under a binary operation *. For each $a \in R$ there is a unique $a^{-1} \in R$ such that $a^{-1} * a = a * a^{-1} = e_R$.*

Theorem 2.1.5. *If R is a group under the binary operation $*$, then $a * b = a * c \implies b = c$ and $b * a = c * a \implies b = c$ for all $a, b, c \in R$.*

Theorem 2.1.6. *Let R be a group with $a, b \in R$, then the linear equations $a * x = b$ and $x * a = b$ have unique solutions in R. That is $a * x = b \implies x = a^{-1} * b$ and $x * a = b \implies x = b * a^{-1}$.*

Definition 2.1.7.

Let R be a group and let $a \in R$. The **order** of R, denoted by $|R|$ is the number of elements in R. A group is called **finite** if it has a finite number of elements. If the number of elements in R is not finite, then R is called an **infinite group**. The order of a in R, denoted by $o(a)$ is the smallest positive integer n such that $a^n = e_R$. If no such integer exists then a is said to have an infinite order.

Definition 2.1.8.

A group R is called **cyclic** if $R = \{a^n \mid n \in \mathbb{Z}\} = \langle a \rangle$ for some $a \in R$. The element a is called the generator of R. We denote a cyclic group of order n by C_n.

Definition 2.1.9.

Let R be a group and let X be a non empty subset of R. The intersection of all subgroups of R which contain X is called the subgroup of R generated by X. A group R is called **finitely generated** if it has a finite generating subset.

Proposition 2.1.10. ***Properties of cyclic groups***

1. *Let R be a group and let a be an element of R. The order of a is equal to the order of a cyclic subgroup generated by a. That is $o(a) = |\langle a \rangle|$.*

2. *Every subgroup of a cyclic group is cyclic.*

3. *Every cyclic group is abelian.*

Example 2.1.11.

The set of integers modulo n, denoted by $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ is a group under addition modulo n and $|\mathbb{Z}_n| = n$.

Proof. Let $a, b \in \mathbb{Z}_n$, then we have that $(a+b) mod\ n \in \mathbb{Z}_n$.
Suppose that $a, b, c \in \mathbb{Z}_n$, then

$$\begin{aligned} ((a+b)+c) mod\ n &\equiv (a+b) mod\ n + c\ mod\ n \\ &\equiv a\ mod\ n + b\ mod\ n + c\ mod\ n \\ &\equiv a\ mod\ n + (b+c) mod\ n \\ &\equiv (a+(b+c)) mod\ n. \end{aligned}$$

The element $0 \in \mathbb{Z}_n$ is the identity element since $(a+0) mod\ n \equiv a mod\ n$ for every $a \in \mathbb{Z}_n$.
For every element a of $\mathbb{Z}_n$, there exists an element $n - a \in \mathbb{Z}_n$ such that
$(a + (n-a)) mod\ n \equiv 0$.

Moreover, every element a of $\mathbb{Z}_n$ can be expressed as $a = 1 + 1 + \ldots + 1$. Thus, we say that $\mathbb{Z}_n$ is a cylic group generated by 1. □

Example 2.1.12.

The set of units denoted by $\mathbb{Z}_n^* = \{k : k \in \mathbb{Z}_n, (k, n) = 1\}$ is a group under multiplication modulo n.

Theorem 2.1.13. *An element k of $\mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ if and only if $(k, n) = 1$.*

Definition 2.1.14.

Let R be a group and let x be an element of R. The **center** of R is the set

$$Z(R) = \{x \in R \mid ax = xa,\ \forall a \in R\}.$$

Definition 2.1.15.

Let R be a group and let $x \in R$. The **centralizer** of x in R is the set

$$C_R(x) = \{a \in R \mid ax = xa\}.$$

Definition 2.1.16.

Let R be group and let Q be a non-empty subset of R. The subset Q is called a **subgroup** of R if it is a group under the same binary operation as R. We write this as $Q \leq R$.

Proposition 2.1.17. *Let R be a group and let Q be a non-empty subset of Q. The subset Q is a subgroup of R if and only if the following three conditions are satisfied:*

1. *The identity element e_R, is contained in Q.*
2. *If $a, b \in Q$, then $ab \in Q$.*
3. *If $a \in Q$, then $a^{-1} \in Q$.*

Example 2.1.18.

Let R be a group. The center $Z(R)$ and the centralizer $C_R(x)$ are subgroups of R.

Proof. Let R be a group and let $C_R(x) = \{a \in R \mid ax = xa\}$. Then $C_R(x) \subset R$ and $e \in Z(R)$ since $ex = xe$.
Let $a \in C_R(x)$, then $ax = xa \implies xa^{-1} = a^{-1}x \implies a^{-1} \in C_R(x)$. Lastly, suppose that $a, b \in C_R(x)$, then

$$\begin{aligned}(ab^{-1})x &= a(b^{-1}x)\\ &= a(xb^{-1})\\ &= (ax)b^{-1}\\ &= (xa)b^{-1}\\ &= x(ab^{-1}).\end{aligned}$$

Thus, $ab^{-1} \in C_R(x)$. □

Definition 2.1.19.

Let R be a group and let Q be a subgroup of R with $a \in R$. The set $Qa = \{qa : q \in Q\}$ (or $aQ = \{aq : q \in Q\}$) is called the **right coset of Q generated by a** (or **left coset of Q generated by a**).

Definition 2.1.20.

Let R be a group and let $Q \leq R$. The number of distinct left (or right) cosets of Q is called the **index of Q in R** and it is denoted by $[R : Q]$.

Theorem 2.1.21. ***Lagrange's Theorem***

If R is a finite group and Q is a subgroup R then $|Q|$ divides $|R|$.

Corollary 2.1.22. *Let R be a finite group with $Q \leq R$, then $|R| = |Q|[R : Q]$.*

2.2 Normal Subgroups

Definition 2.2.1.

Let R be a group. A subgroup Q of R is called a **normal subgroup** of R if $aQ = Qa$ for all $a \in R$. We write this as $Q \trianglelefteq R$.

Theorem 2.2.2. *Let R be group and let Q be a subgroup of R. The following conditions are equivalent.*

1. $Q \trianglelefteq R$,
2. $aQa^{-1} \subseteq Q$ *for every* $a \in R$,
3. $aQa^{-1} = Q$ *for every* $a \in R$.

Proposition 2.2.3. *If R is an abelian group then every subgroup Q of R is normal in R.*

Proof. Let Q be a subgroup of an abelian group R and let $a \in R$. Then $Qa = \{qa : \ q \in Q\}$ and $aQ = \{aq : \ q \in Q\}$ by definitions of left and right cosets. Since R is abelian, it follows that $aq = qa$ for all $q \in R$. Hence, we have that $aQ = Qa$ for all $a \in R$. □

Definition 2.2.4.

Let R be a group and let Q be a subgroup of R. We define the multiplication of right cosets by $Qa \cdot Qb = Qab$ for all $a, b \in R$.

Lemma 2.2.5. *A subgroup N of R is normal if and only if $Qa \cdot Qb = Qab$ is well defined $\forall a, b \in R$.*

Theorem 2.2.6. *Let Q be a normal subgroup of R. The set of all cosets of Q, denoted by $R/Q = \{qa \mid a \in R\}$ form a group under the operation $Qa \cdot Qb = Qab$. This group is called the* ***quotient group of*** *R* ***by*** *Q.*

Definition 2.2.7.

Let Q be a subgroup of R. The set $N_R(Q) = \{a \in R \mid Qa = aQ\}$ is called **normalizer** of Q.

Theorem 2.2.8. *Let Q be a subgroup of R. The normalizer of Q is a subgroup of R.*

2.3 Homomorphisms

Definition 2.3.1.

Let R_1 be a group under a binary operation $*$ and let R_2 be a group under a binary operation $\bullet$. A **homomorphism** from R_1 to R_2 is a mapping $\theta : R_1 \to R_2$ that preserves the group operations:

$$\theta(a * b) = \theta(a) \bullet \theta(b) \ for\ all\ a, b\ in\ R_1.$$

Proposition 2.3.2. ***Properties of group homomorphisms***

Let R_1 and R_2 be groups such that $\theta : R_1 \to R_2$ is a homomorphism. Then,

1. *$\theta(e_{R_1}) = e_{R_2}$ and*
2. *$\theta(g^k) = \{\theta(g)\}^k$ for all integers k.*

Definition 2.3.3.

Let $\theta : R_1 \to R_2$ be a homomorphism.

1. The **kernel** of θ are defined to be the set $\text{Ker}(\theta) = \{a \in R_1 \mid \theta(a) = e_{R_2}\}$.

2. The **image** of θ is the set $Im(\theta)$=$\{\theta(a) \mid a \in R_1\}$.

3. The **cokernel** of θ, denoted by $coker(\theta)$ is the quotient group $R_2/Im(\theta)$.

Proposition 2.3.4. *Let $\theta : R_1 \to R_2$ be a homomorphism. Then,*

1. *the kernel of θ is a subgroup of R_1 and*

2. *the image of θ is a subgroup of R_2.*

Proposition 2.3.5. *Let R_1 and R_2 be groups and let $\theta : R_1 \to R_2$ be a homomorphism. If R_1 is abelian, then $\theta(R_1)$, the image of R_1 under the homomorphism θ is also abelian.*

Definition 2.3.6.

Let R_1 and R_2 be groups such that the mapping $\theta : R_1 \to R_2$ is group homomorphism. Then θ is called:

1. a **momorphism** if it is one-to-one,

2. an **epimorphism** if it is onto,

3. an **isomorphism** if it is bijection,

4. an **endomorphism** if $R_1 = R_2$.

Proposition 2.3.7. ***Properties of isomorphisms***

Let R_1, R_2 and R_3 be groups.

1. *If $\theta : R_1 \to R_2$ is an isomorphism, then the inverse $\theta^{-1} : R_2 \to R_1$ is also an isomorphism.*

2. *If $\theta : R_1 \to R_2$ and $\tau : R_2 \to R_3$ are isomorphisms, then the composite $\tau\theta : R_1 \to R_3$ is also an isomorphism.*

Proposition 2.3.8. *Let R be a cyclic group.*

1. *If $|R| = n$, then $R \cong \mathbb{Z}_n$ under addition.*

2. *If $|R| = \infty$, then $R \cong \mathbb{Z}$ under addition.*

Proof. 1. Let R be a cyclic group of order n. Define $\theta : R \to \mathbb{Z}_n$ by $\theta(a^r) = \bar{r}$ for some $a \in R$ and $r, s \in \mathbb{Z}$. Suppose that $a^r = a^s$, then $a^{r-s} = e_R \iff r - s = qn$ for some some integer q. Hence, $r = s \ (mod\ n) \iff \bar{r} = \bar{s} \iff \theta(a^r) = \theta(a^s)$. Thus, θ is well defined and one to one.

The mapping $\theta : R \to \mathbb{Z}_n$ is onto since for every $\bar{r} \in \mathbb{Z}_n$, there exists $a \in R$ such that $\bar{r} = \theta(a^r)$.

Lastly, $\theta(a^r a^s) = \theta(a^{r+s}) = \overline{r+s} = \bar{r} + \bar{s} = \theta(r) + \theta(s)$. Thus, $\theta : R \to \mathbb{Z}_n$ is an isomorphism.

□

Definition 2.3.9.

Let R be a group. The **isomorphism class** of R is the set of all groups that are isomorphic to R.

Theorem 2.3.10. ***The First Isomorphism Theorem***

Let $\theta : R \to Q$ be a homomorphism and let $Ker(\theta) = K$. Then $K \trianglelefteq R$ and $R/K \cong Im(\theta)$. In particular if θ is onto, then $R/K \cong Q$.

Theorem 2.3.11. ***The Second Isomorphism Theorem***

Let $Q \leq R$ and $K \trianglelefteq R$, then $Q \cap K$ is normal in Q and $Q/Q \cap K = QK/K$.

Theorem 2.3.12. ***The Third Isomorphism Theorem***

Let Q and K be normal subgroups of R such that $K \subseteq Q$. Then Q/K is a normal subgroup of Q/K and $(R/K)/(Q/K) \cong R/Q$.

2.4 Conjugacy

Definition 2.4.1.

Let R be a group. The elements a and b of R are called **conjugate** if $b = xax^{-1}$ for some $x \in R$. We write this as $a \sim b$.

Theorem 2.4.2. *Conjugacy is an equivalence relation.*

Proof. Let R be a group.

1. Reflexive: for every $a \in R$ we have $a = eae^{-1}$. Thus, $a \sim a$.

2. Symmetric: let $a, b \in R$ such that $a = xbx^{-1}$ for some $x \in R$. Then $b = x^{-1}ax$. Hence, $a \sim b$ implies $b \sim a$.

3. Transitive: suppose $a \sim b$ and $b \sim c$. Then $a = xbx^{-1}$ and $b = ycy^{-1}$ for some elements $x, y \in R$. Hence, $a = (xy)c(xy)^{-1}$.

□

Definition 2.4.3. Let R be a group and let $a, b \in R$ such that $b = xax^{-1}$. We say that a and b are equivalent since there is an equivalence relation between the two elements. A subset Q of R is called an **equivalence class** if it contains all the elements of R that are equivalent to each other.

Proposition 2.4.4. *Let R be a finite group and let $a, b \in R$. If $b = xax^{-1}$ for some $x \in R$ then a and b have the same order.*

Definition 2.4.5.

Let R be group. An element a of R is said to be **self-conjugate** if $a = xax^{-1}$ for some $x \in R$.

Lemma 2.4.6. *Every element of an abelian group R is self-conjugate.*

Proposition 2.4.7. *Let R be an abelian group. Then $a \sim b$ if and only if $a = b$.*

Proof. $\implies$) Let R be an abelian group and let $a \sim b$ for $a, b \in R$. Then for some $x \in R$ we have that $a = xbx^{-1} \implies a = xx^{-1}b = eb = b$.
$\impliedby$) If R is an abelian group and $a, b \in R$ such that $a = b$, then $a = ea = eb = xx^{-1}b = xbx^{-1} \implies a \sim b$. □

Lemma 2.4.8. *Let R be a group. The centre $Z(R)$ of R comprises of all self-conjugate elements of R.*

The following result presents a connection between the centre of an abelian group and the group itself.

Proposition 2.4.9. *If R is an abelian group then $R = Z(R)$.*

Definition 2.4.10.
Let R be a group. The **conjugacy class** of $g \in R$ is the set of all elements of R that are conjugate to it. We denote this set by $g^R = \{xgx^{-1} \mid x \in R\}$.

Lemma 2.4.11. *Let R be a group and let $g, h \in R$. The two conjuagacy classes g^R and h^R are equal if g and h are conjugate in R. Otherwise conjugacy classes are disjoint.*

Proposition 2.4.12. *Let R be a group and let $e \in R$ be the identity element of R. Then*

1. *the conjugacy class of e is the set $e^R = \{b \in R \mid b = xex^{-1} \text{ for some } x \in R\} = \{e\}$.*
2. *the conjugacy class of $a \in R$ is the set $\{xax^{-1} \mid x \in R\} = \{a\}$ if a commutes with all the elements of R.*

Proposition 2.4.13. *Let conjugacy relation be defined on a group R. Then,*

1. *every element a is contained in its own conjugacy class, that is $a \in a^R$.*
2. *the conjugacy classes of a and b are equal if and only if $b \in a^R$.*

The number of conjugates of an element is determined by the size of its conjugacy class. Consider an abelian group R with $g \in R$, then $|g^R| = 1$. However, if a group is non-abelian, then it is not easy to compute the carninalities of distinct conjugacy classes.

The next result presents a method for computing the number of conjugates of an element for any group R.

Lemma 2.4.14. *Let R be a group and let g be an element of R. The order of the conjugacy class of g is equal to the index of its centralizer in R:*

$$|g^R| = [R : C_R(g)].$$

If R is a finite group then $|g^R| < \infty$ for all $g \in R$.

Consider a finite group R with different conjugacy classes given by $g_1^R,\ g_2^R, \ldots, g_k^R$. Then

$$\begin{aligned}
|R| &= |g_1^R| + |g_2^R| + \ \ldots + \ |g_k^R| \\
&= [R : C_R(g_1)] + [R : C_R(g_2)] \ + \ldots + [R : C_R(g_k)] \\
&= \sum_{i=1}^{k} [R : C_R(g_i)] \\
&= \sum_{i=1}^{k} \frac{|R|}{|C_R(g_i)|} \\
&= |Z(R)| + \sum_{g_i \notin Z(R)} \frac{|R|}{|C_R(g_i)|}
\end{aligned}$$

This is called the **class equation**.

Corollary 2.4.15. *Let R be a finite group and let $a \in R$. The order of the conjugacy class of a divides the order of R.*

The notion of conjugacy can also be applied to subgroups.

Definition 2.4.16.

Let R be a group and let $Q, K \leq R$. Then Q is called a **conjugate subgroup** of K if $Q = xKx^{-1}$ for some $x \in R$. A subgroup Q of R is said to be self-conjugate if $Q = xQx^{-1}$.

Distinct conjugate subgroups are not disjoint since they all contain the identity element e_R. The next results highlights the connection between conjugacy classes and conjugate subgroups.

Theorem 2.4.17. *Every normal subgroup is the union of conjugacy classes.*

Proof. Let Q be a normal subgroup of R and let $q \in Q$. Then $gqg^{-1} \in gQg^{-1} = Q$. Thus, if $q \in Q$ then its conjugacy class is also contained in Q. □

2.5 Automorphisms

Definition 2.5.1.

Let R_1 and R_2 be groups such that $\theta : R_1 \to R_2$ is a group homomorphism. Then θ is said to be an **automorphism** if $R_1 = R_2$ and θ is an isomorphism. The set of all automorphisms θ of R_1 is the set $Aut(R_1) = \{\theta \ : R_1 \to R_1 |\ \theta \text{ is an isomorphism}\}$.

Proposition 2.5.2. *A set of automorphisms of R forms a group under composition of mappings.*

Proof. $Aut(R)$ is associative since function composition is associative. By Proposition 2.3.7, the composite of isomorphisms is again an isomorphism. Hence, if τ, $\theta \in Aut(R)$ then $\tau\theta \in Aut(R)$. The inverse of an isomorphism is an isomorphism. Thus, $Aut(R)$ contains inverses. Lastly, if $\theta \in Aut(R)$, then $\theta\theta^{-1} = \theta^{-1}\theta = 1_R$. □

Proposition 2.5.3. *Let R be a group generated by $a \in R$,*

1. *If $\theta : R \to R$ is an automorphism, then $\theta(a)$ is a generator of R.*
2. *If b is a generator of R, there is a unique automorphism $\theta : R \to R$ such that $\theta(a) = b$.*

Example 2.5.4.

Let R be a group with $a \in R$ and define $\pi_a : R \to R$ by $\pi_a(x) = axa^{-1}$. Then $\pi_a : R \to R$ is an automorphism.

Definition 2.5.5.

Let R be a group and $g \in R$, then the mapping $\pi_a : R \to R$ defined by $\pi_a(x) = axa^{-1}$ is called the **inner automorphism of** R. The set of all inner automorphisms of R form a group known as the **inner automorphism group of** R, denoted by $Inn(R)$.

Proposition 2.5.6. *Let R be a group, then $Inn(R)$ is a subgroup of $Aut(R)$.*

Lemma 2.5.7. *Let R be a group and let $Z(R)$ be the centre of R, then $R/Z(R) \cong Inn(R)$.*

Proof. Define $\tau : G \to Inn(R)$ by $\tau(gh) = \tau_{gh} = \tau_g\tau_h = \tau(g)\tau(h)$, then τ is a group homomorphism.
Let $z \in Ker(\tau)$, then $\tau_z = \tau(z) = i_d : R \to R \iff \tau_z(x) = x \ \forall x \in$R $\iff zxz^{-1} = x \iff zx = xz$. Thus, z commutes with all the elements in R, that is $z \in Z(R)$. So we have that $Ker(\tau) = Z(R)$. It follows from Theorem 2.3.10 that $R/Z(R) \cong Inn(R)$. □

2.6 Group actions and Sylow theory

Definition 2.6.1.

Let R be a group, X a non-empty set and consider the set $R \times X = \{(a, x) \ | a \in$R, $\ x \in X\}$. The function $\mu : R \times X \to X$ defined by $\mu(a, x) \mapsto ax$ is called a **group action** if

1. $\mu(e_R, x) = x$ and
2. $\mu(ab, x) = \mu(a, \mu(b, x))$ for $a, b \in R$.

Example 2.6.2.

Suppose $R = X$, then $\mu(a, x) = axa^{-1}$ is a group action.

Proof. Let $\mu : X \times X \to X$ be defined by $\mu(a, x) \mapsto axa^{-1}$. Then

$$\begin{aligned} \mu(e_R, x) &= e_R x (e_R)^{-1} \\ &= x. \end{aligned}$$

For every $a, b \in R$ we have that:

$$\begin{aligned}
\mu(ab, x) &= (ab)x(ab)^{-1} \\
&= (ab)x(b^{-1}a^{-1}) \\
&= a(bxb^{-1})a^{-1} \\
&= a(\mu(b, x))a^{-1} \\
&= \mu(a, \mu(b, x)).
\end{aligned}$$

□

Example 2.6.3.

Let R be a group and $X = \{Q \mid Q \leq R\}$, then $\mu(a, Q) = aQa^{-1}$ is a group action.

Definition 2.6.4.

Let R be group with $X \subseteq R$ and let $\mu : R \times X \to X$ be a group action on X. For every $x \in X$ we define the **Orbit** and the **Stabilizer** of x as $Orb(x) = \{\mu(a, x) \mid a \in R\}$ and $Stab_R(x) = \{a \in \mathrm{R} \mid \mu(a, x) = x\}$.

Theorem 2.6.5. ***The Orbit-Stabilizer Theorem***

Let $\mu : R \times X \to X$ be a group action, then for any $x \in X$ we have $|Orb(x)| = [R : Stab_R(x)]$.

Definition 2.6.6.

Let p be a prime number, a group R is called a **p-group** if the order of R is some power of p. If R is a p-group then a subgroup of a R is called a **p-subgroup** of R.

Definition 2.6.7.

Let R be a finite group and let p be a prime that divides $|R|$. A subgroup P of R is called a **Sylow p-subgroup of** R if $|P|$ is a power of p and $[R : P]$ is not divisible by p.

Theorem 2.6.8. ***The First Sylow theorem***

Let R be a group and let p be a prime that divides $|R|$, then R has a Sylow p-subgroup.

Theorem 2.6.9. ***The Second Sylow theorem***

Let R be a finite group with $|R| = mp^k$ where p is a prime dividing $|R|$. Then,

1. *If P and Q are the only two Sylow p-subgroups, then $Q = aPa^{-1}$ for some $a \in R$.*

2. *If n_p is the number of Sylow p-subgroups , then $n_p = 1 + kp$ for some $k \geq 0$ and $n_p | m$.*

2.7 Direct and Semi-direct products

Since we are investigating the cancellation of $\mathbb{Z}$ as a direct factor in the isomorphism $R \times \mathbb{Z} \cong Q \times \mathbb{Z}$, it is thus important to look at direct products. The cartesian product of the sets X and Y forms another set $X \times Y$, which is the set of all ordered pairs (x, y) with $x \in X$ and $y \in Y$. If H and K are groups, then $H \times K$ is also a group with the operation on $H \times K$ defined by $(h, k)(h', k') = (hh', kk')$ for $h, h' \in H$ and $k, k' \in K$.

Definition 2.7.1.
Let $H, K \trianglelefteq R$ with $H \cap K = \{e_R\}$. The **internal direct product** of H and K is the set $HK = \{hk : \ h \in H, \ k \in K\}$ and the **external direct product** of H and K is the set $H \times K = \{(h, k) : \ h \in H, \ k \in K\}$.

Proposition 2.7.2. *Let H and K be subgroups of R such that $HK = \{hk |\ h \in H$ and $k \in K\}$.*

1. *If $H \leq R$ and $K \trianglelefteq R$, then $HK \leq R$.*

2. *If $H \trianglelefteq R$ and $K \trianglelefteq R$, then $HK = KH \trianglelefteq R$.*

3. *Subgroups H and K are normal in R such that $R = HK$ and $H \cap K = \{e_R\}$ if and only if $R \cong H \times K$.*

4. *The direct product $H \times K$ is abelian if and only if H and K are abelian.*

Definition 2.7.3.
Let $n \in \mathbb{N}$ and let $R_1, R_2, \ldots, R_n$ be any n groups. The direct product of $R_1, R_2, \ldots, R_n$, denoted by $R_1 \times R_2 \times \ldots \times R_n$ is the set of all ordered n-tuples $(r_1, r_2, \ldots, r_n)$ with $r_i \in R_i$ for all $i = 1, \ldots, n$.

Definition 2.7.4.

Let R be a group and let H and K be subgroups of R. Then R is an **internal semi-direct product** of N by H if

1. $R = HK$,
2. $K \trianglelefteq R$ and
3. $H \cap K = \{e_R\}$.

Definition 2.7.5.

Let H and K be groups and let $\theta : H \to Aut(K)$ be a group homomorphism. The **external semi-direct** product of K by H via θ is the set $K \rtimes_\theta H = \{(k,h)|\ k \in K,\ h \in H\}$ with the binary operation $*$ defined by $(k,h) * (k',h') = (k\theta(h)(k'), hh')$.

Proposition 2.7.6. *Let H and K be groups and let i_H and i_K be the identity elements of H and K respectively. The semi-direct product, $K \rtimes_\theta H$ is a group under * with $e = (i_K, i_H)$ and the inverse $(k,h)^{-1} = (\theta(h^{-1})(k^{-1}), h^{-1})$.*

Theorem 2.7.7. *Let R be group and let $H,\ K \leq R$, then $K \rtimes_\theta H$ is the external direct product if and only if $\theta : H \to Aut(K)$ is trivial.*

Proof. Let (k,h)*(k′,h′)=(kk′,hh′). Then from the definition of $\theta : H \to Aut(K)$ we get that $(k\theta(h)(k'), hh') = (kk', hh') \iff k\theta(h)(k') = kk' \iff \theta(h)(k') = k' \iff \theta(h) = i_K : K \to K \iff \theta$ is a trivial map. □

2.8 Finite abelian groups

The following result presents classification of finite abelian groups and will be essential in the later chapters. It uses direct products and the application of Sylow theory to describe the structure of finite abelian groups.

Theorem 2.8.1. ***The fundamental theorem of finite abelian groups***

Let R be a finite abelian group. Then $R \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$ where $n_i > 2$ for all i and $n_{i+1} \mid n_i$ for $1 \leq i \leq k-1$.

Definition 2.8.2.

Let R be a finite abelian group such that $R \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$. The integers $n_1, \ldots, n_k$ are called the **invariant factors** of R.

Proposition 2.8.3. *Let R and Q be finite abelian groups, then $R \cong Q$ if R and Q have the same list of invariant factors.*

Proposition 2.8.4. *Let R be a finite abelian group with invariant factors $n_1, \ldots, n_k$, then* $|R| = \prod_{i=1}^{k} n_i$.

Definition 2.8.5.

Let $n_1, \ldots, n_k$ be the invariant factors of a finite abelian group R, we say that R is of type $(n_1, n_2, \ldots, n_k)$.

Example 2.8.6.

Let R be an abelian group with $|R| = 20 = 2^2 \times 5$. Then we can write R as a direct product of Q and K where $|Q| = 4$ and $|K| = 5$.

Elementary divisors	Finite abelian groups	Invariant factors	Factorization of R
$2^2,\ 5$	$\mathbb{Z}_4 \times \mathbb{Z}_5$	20	$R \cong \mathbb{Z}_{20}$
$2,\ 2,\ 5$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$	$10,\ 2$	$R \cong \mathbb{Z}_{10} \times \mathbb{Z}_2$

Definition 2.8.7. Let R be an abelian group and let Q be a subgroup of R. Then Q is called a **torsion subgroup** of R if all its elements have finite order. A **torsion-free abelian group** is an abelian group in which the identity element is the only element with finite order.

2.9 Nilpotent groups

Definition 2.9.1.

Let R be a group with $a, b \in R$, then the **commutator** of a and b, denoted by $[a, b]$ is the element $aba^{-1}b^{-1}$. The **commutator subgroup of** R, denoted by $[R, R]$ is the subgroup of R generated by all the commutators of R.

Lemma 2.9.2. *Let R be a group with $a, b \in R$, then $[a,b]^{-1} = [b,a]$ and $[a,b] = e_R$ if and only if R is abelian.*

Definition 2.9.3.

Let H and K be subgroups of R. The **commutator subgroup** of H and K is the defined as $[H,K] = \langle\ [h,k]\ \mid h \in H,\ k \in K \rangle$.

Definition 2.9.4.

Let $Z(R) = \{x \in R \mid ax = xa,\ \forall a \in R\}$ be the center of a group R and let $\pi : R \to R/Z(R)$ be a canonical epimorphism. Then $\pi^{-1}(Z(R/Z(R))) \trianglelefteq R$. We define

$$\begin{aligned} Z_1(R) &= Z(R) \text{ and} \\ Z_i(R) &= \pi_i^{-1}(Z(R/Z_{i-1}(R))) \end{aligned}$$

where $i > 1$ and $\pi_i^{-1} : R \to R/Z_{i-1}(R)$. The **upper central series** of R is the sequence of normal subgroups of R:

$$\{e_R\} = Z_0(R) \ \subseteq\ Z_1(R) \ \subseteq\ Z_2(R) \ \subseteq Z_3(R) \ \subseteq \ldots$$

Definition 2.9.5.

Let R be a non-trivial group. Then R is said to be **nilpotent** if $Z_i(R) = R$ for some i. The **nilpotency class** of a nilpotent group R is the smallest non-negative integer k such that $Z_k(R) = R$.

Proposition 2.9.6. *Let R be a finite p-group, then R is nilpotent.*

Proof. Let R be a group, then we have that $Z_i(R) \trianglelefteq R$ for all i. Let R be a finite p-group, then it follows that $R/Z_i(R)$ is also a p-group. The centre $Z(R/Z_i(R))$ is non-trivial if $R/Z_i(R)$ is non-trivial. Hence, $Z_i(R) \neq R$ implies that $Z_i(R) \ \subseteq Z_{i+1}(R)$ and $Z_i(R) \neq Z_{i+1}(R)$. Hence, $Z_n(R) = R$ for some $n \geq 0$ since R is finite. □

Definition 2.9.7. Let R be a group and let Q be a subgroup of R. We say that Q is a **characteristic subgroup of** R if for every automorphism θ of R, $\theta(Q) = Q$.

2.10 Rings

Definition 2.10.1.

A **Ring** R is a non empty set on which addition and multiplication operations are defined, satisfying the following axioms for all $a, b, c \in R$:

1. $a + b \in R$ and $ab \in R$,
2. $(a + b) + c \ = \ a + (b + c) \in R$ and $(ab)c = a(bc)$,
3. $a + b = b + a$,
4. There is a additive identity $0 \in R$, with $0 + a = a + 0 = a, \ \forall a \in R$,
5. There is an additive inverse for each element in R that is, $\forall a \in R$ there is $(-a) \in R$ such that $a + (-a) = (-a) + a = 0$,
6. The distributive laws hold.

Definition 2.10.2.

The ring is said to have unity if in addition to the above properties there is a **unity** $1 \in R$ such that $a.1 = 1.a = a$.

Definition 2.10.3.

Let R be a ring. An abelian group M is called an R**-module** if there is a multiplication $R \times M \to M$ such that $a(x + y) = ax + ay$, $(a + b)x = ax + bx$, $a(bx) = (ab)x$ and $1x = x$.

Definition 2.10.4.

An **ideal** I of a ring R with unity is a non empty subset of R closed under addition and multiplication.

Definition 2.10.5.

A commutative ring with unity and no zero divisor is called an **integral domain**, denoted by D. Let X be a subset of a ring R, the ideal generated by X, denoted by $\langle X \rangle$ is the smallest ideal of R containing X. If X is a singleton then $\langle X \rangle$ is the **principal ideal**. An integral domain D is called a **principal ideal domain**(or ***PID***) if all ideals in D are principal.

Definition 2.10.6. Let R be a ring. A left (right) **annihilator** of a subset Q of R is defined by $l_R(Q) = \{a \in R |\ aQ = 0\}$ $(r_R(Q) = \{a \in R |\ Qa = 0\})$.

2.11 The automorphism group of finite groups

In this section we investigate the structure of the automorphism group $Aut(T)$, given that T is a finite abelian group. We also provide properties of this group. Motivated by the Fundamental Theorem of Finite Abelian groups, we discuss the automorphism group of direct products, referring to C. J. Hillar and D. L. Rhea's work in [8].

The group of integers $\mathbb{Z}$ under addition is a cyclic group generated by 1 and -1. Hence, an isomorphism from $\mathbb{Z}$ to $\mathbb{Z}$ has to map a generator to a generator. Automorphisms preserve the group structure, so we have the following maps, $1 \mapsto 1$ and $1 \mapsto -1$. Thus, there are only two automorphisms of $\mathbb{Z}$: the identity map $i_d : \mathbb{Z} \to \mathbb{Z}$ and $\mu : \mathbb{Z} \to \mathbb{Z}$ defined by $\mu(x) = -x$ for all $x \in \mathbb{Z}$. We write $Aut(\mathbb{Z}) = \{\mu(x) = x\ ;\ \mu(x) = -x\}$ and $|Aut(\mathbb{Z})| = 2$. The group of integers modulo 2 is the only unique group of order 2, hence $Aut(\mathbb{Z}) \cong \mathbb{Z}_2$.

The description of $Aut(\mathbb{Z}_n)$ also depends on the number of generators of $\mathbb{Z}_n$. According to Theorem 2.1.13, an element of $\mathbb{Z}_n$ is a generator if it is relatively prime to n. We use the notion of Euler-phi function to compute the number of generators of $\mathbb{Z}_n$.

Definition 2.11.1.
Let $n \geq 1$ be an integer. The Euler phi-function, denoted by $\phi(n)$ is the number of elements in the set $\{1, 2, \ldots, n-1\}$ which are co-prime with n.

Proposition 2.11.2. *Let p be a prime and let α be a positive integer. Then $\phi(p) = p - 1$ and $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$.*

For cases whereby n can be factorized using more than one prime number, we have the following result.

Proposition 2.11.3. *Let n be a natural number greater than 1. If $n = pq$ where p and q are prime numbers, then $\phi(n) = \phi(p)\phi(q)$.*

Definition 2.11.4.

The automorphism group of $\mathbb{Z}_n$ is the set:

$$Aut(\mathbb{Z}_n) = \{\sigma_a(x) = ax \bmod n \mid \sigma_a : \mathbb{Z}_n \to \mathbb{Z}_n \text{ is an isomorphism, } 1 \leq a \leq n \text{ and } (a, n) = 1\}.$$

Proposition 2.11.5. *Let $n \in \mathbb{Z}^+$ and let $Aut(\mathbb{Z}_n) = \{\sigma_a : \mathbb{Z}_n \to \mathbb{Z}_n \mid \sigma_a$ is an isomorphism, $1 \leq a \leq n$ and $(a, n) = 1\}$. Then the order of $Aut(\mathbb{Z}_n)$ is equal to $\phi(n)$.*

Proof. An element $a \in \mathbb{Z}_n$ generates $\mathbb{Z}_n$ if and only if it is relatively prime to n. Hence, it follows from the definition of ϕ that the number of generators of $\mathbb{Z}_n$ is equal to $\phi(n)$. Proposition 2.5.3 states that for every generator a of $\mathbb{Z}_n$ there is a unique automorphism. Hence, we have that $|Aut(\mathbb{Z}_n)| = \phi(n)$.

□

Next, we study groups that are isomorphic to $Aut(\mathbb{Z}_n)$.

Proposition 2.11.6. *The automorphism group of $\mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_n^*$.*

Proof. Let $\theta : Aut(\mathbb{Z}_n) \to \mathbb{Z}_n^*$ be defined by $\alpha \mapsto \alpha(1)$ where $\alpha \in Aut(\mathbb{Z}_n)$. Then,

$$\begin{aligned}
\alpha(i) &= \alpha(\underbrace{1 + 1 + \ldots + 1}_{i \text{ times}}) \\
&= \underbrace{\alpha(1) + \alpha(1) + \ldots + \alpha(1)}_{i \text{ times}} \\
&= i \cdot \alpha(1)
\end{aligned}$$

Since α is onto, then there exists an element m of $\mathbb{Z}_n$ such that $\alpha(m) = 1 \in \mathbb{Z}_n$. So inverse of $\alpha(1)$ is m modulo n since $\alpha(m) = m \cdot \alpha(1) = 1$ and $\alpha(1) \in \mathbb{Z}_n^*$.
Let $\alpha, \beta \in Aut(\mathbb{Z}_n)$ and suppose that $\alpha(1) = \beta(1)$, then

$$\begin{aligned}
\alpha(i) &= i \cdot \alpha(1) \\
&= i \cdot \beta(1) \\
&= \beta(i)
\end{aligned}$$

for all $i \in \mathbb{Z}_n$. Thus, θ is one-to-one.

Let $r \in \mathbb{Z}_n^*$ and define $\alpha : \mathbb{Z}_n \to \mathbb{Z}_n$ by $s \mapsto rs \ mod \ n$. From the definition of θ we have that $\theta(\alpha) = \alpha(1) = r$. Hence, there is a pre-image for r and θ is onto.

Suppose that $\alpha, \beta \in Aut(\mathbb{Z}_n)$, then

$$\begin{aligned} \theta(\alpha \circ \beta) &= (\alpha \circ \beta)(1) \\ &= \alpha(\beta(1)) \\ &= \alpha(1)\beta(1) \qquad since\ \alpha(i) = \alpha(1) \cdot i \\ &= \theta(\alpha)\theta(\beta) \qquad since\ \alpha(1) = \theta(\alpha). \end{aligned}$$

Thus, θ is a group isomorphism.

□

Proposition 2.11.7. *For any prime number p, let C_p be a cyclic group of order p. Then $Aut(C_p) \cong C_{p-1}$.*

The Fundamental Theorem of Finite Abelian groups states that every finite abelian group is equal to the direct product of its cyclic subgroups. Motivated by this result, we investigate the automorphism group of direct products.

Lemma 2.11.8. *[8, 2.1] Let P and Q be finite groups with relatively prime orders. Then*

$$Aut(P \times Q) \cong Aut(P) \times Aut(Q).$$

Proof. We show that there is a homomorphism ϕ from $Aut(P) \times Aut(Q)$ onto $Aut(P \times Q)$. Consider an automorphism α of P and an automorphism β of Q. Then $\phi(\alpha, \beta) \in Aut(P \times Q)$ is given by

$$\phi(\alpha, \beta)(p, q) = (\alpha(p), \beta(q)).$$

Let $i_P \in Aut(P)$ and $i_Q \in Aut(Q)$ be the identity automorphisms of Q and P. Then $\phi(i_P, i_Q) = i_{P \times Q}$ and

$$\phi(\alpha_1\alpha_2,\ \beta_1\beta_2)(p, q) = (\alpha_1\alpha_2(p), \beta_1\beta_2(q)) = \phi(\alpha_1, \beta_1)\phi(\alpha_2, \beta_2)(p, q),$$

for all $\alpha_1,\ \alpha_2 \in Aut(P)$, $\beta_1,\ \beta_2 \in Aut(Q)$ and $q \in Q,\ p \in P$. Thus, ϕ is a homomorphism.
To show that ϕ is onto, let $|P| = n$, $|Q| = m$ and $\pi_P : P \times Q \to P$ and $\pi_Q : P \times Q \to Q$ be standard projection homomorphisms. Fix $\lambda \in Aut(P \times Q)$ and let $\gamma : Q \to P$ be a homomorphism defined by $\gamma(q) = \pi_P(\lambda(i_P, q))$, where i_P is the identity element of $Aut(P)$. We have that $L = \{q^n : q \in Q\} \subset Ker(\gamma)$.
The set L consists of m elements since m and n are relatively prime. Hence it follows that $Ker(\gamma) = Q$ and γ is a trivial homomorphism. Similarly, $\delta : P \to Q$ given by $\delta(p) = \pi_Q(\lambda(p, i_Q))$ is trivial.
Finally, define endomorphisms of P and Q as follows:

$$\lambda_P(p) = \pi_P(\lambda(p, i_Q) \text{ and } \lambda_Q(q) = \pi_Q(\lambda(i_P, q)).$$

From this construction and the above arguments, we have

$$\lambda(p, q) = \lambda(p, i_Q) \cdot \lambda(i_P, q) = (\lambda_P(p), \lambda_Q(q)) = \phi(\lambda_P, \lambda_Q)(p, q)$$

for all $p \in P$ and $q \in Q$. It remains to prove that $\lambda_P \in Aut(P)$ and $\lambda_Q \in Aut(Q)$. It suffices that λ_P and λ_Q are injective (since P and Q are both finite).
Let $\lambda_P(p) = i_P$ for some $p \in P$. Then $\lambda(p, i_Q) = (\lambda_P(p), \lambda_Q(i_Q)) = (i_P, i_Q)$, so $p = i_P$ by injectivity of λ. A similar argument shows that $\lambda_Q \in Aut(Q)$. □

Applying the above lemma to a finite abelian group yields the following result.

Proposition 2.11.9. *Let R be a finite abelian group of type $(p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_r^{\alpha_r})$ where $p_1, p_2, \ldots$ and p_r are distinct primes. Then*

$$Aut(R) \cong Aut(\mathbb{Z}_{{p_1}^{\alpha_1}}) \times Aut(\mathbb{Z}_{{p_2}^{\alpha_2}}) \times \ldots \times Aut(\mathbb{Z}_{{p_r}^{\alpha_r}}).$$

Proof. Let R be a finite abelian group. Suppose that $p_1, p_2, \ldots$ and p_r are distinct primes such that $\mathbb{Z}_{{p_1}^{\alpha_1}},\ \mathbb{Z}_{{p_2}^{\alpha_2}},\ \ldots, \mathbb{Z}_{{p_r}^{\alpha_r}}$ are cyclic subgroups of R. Then it follows from the fundamental theorem of finite abelian groups that $R \cong \mathbb{Z}_{{p_1}^{\alpha_1}} \times \mathbb{Z}{p_2}^{\alpha_2} \times \ldots \times \mathbb{Z}_{{p_r}^{\alpha_r}}$. Applying Lemma 2.11.8 yields:

$$Aut(\mathbb{Z}_{{p_1}^{\alpha_1}} \times \mathbb{Z}_{{p_2}^{\alpha_2}} \times \ldots \times \mathbb{Z}_{{p_r}^{\alpha_r}}) \cong Aut(\mathbb{Z}_{{p_1}^{\alpha_1}}) \times Aut(\mathbb{Z}_{{p_2}^{\alpha_2}}) \times \ldots \times Aut(\mathbb{Z}_{{p_r}^{\alpha_r}}).$$

□

2.12 Subgroups of the automorphism group

In this section we discuss normal subgroups of the automorphism group.
Every non-trivial group R has at least two normal subgroups, the improper subgroup R and the trivial subgroup $\{e_R\}$.

Proposition 2.12.1. *Let R be a finite abelian group and let $1_R : R \to R$ be the identity automorphism. Then $\{1_R\}$ is a normal subgroup of $Aut(R)$.*

Proof. Let $\alpha \in Aut(R)$. The only element of $\{1_R\}$ is 1_R and $\alpha 1_R \alpha^{-1} = 1_R \in \{1_R\}$. Hence, $\{1_R\}$ is normal in $Aut(R)$. □

The centre $Z(R)$ of R always forms a normal subgroup of R since it comprises self-conjugate elements.

Proposition 2.12.2. *Let R be a finite abelian group. Then the centre $Z(Aut(R))$ is a normal subgroup of $Aut(R)$.*

Proof. Let $Z = Z(Aut(R))$ and let $\alpha \in Aut(R),\ \beta \in Z$. Then $\alpha\beta = \beta\alpha$ by definition of Z. Thus, $\alpha Z \subseteq Z\alpha$ and $Z\alpha \subseteq \alpha Z$ since α is chosen arbitrarily. Hence, Z is a normal subgroup of $Aut(R)$. □

Proposition 2.12.3. *Let R be a group. If H is a subset of $Z(Aut(R)) = Z$ then H is a normal subgroup of Z. Furthermore H is not necessarily normal in $Aut(R)$.*

Proof. We have that $H \subseteq Z \trianglelefteq Aut(R)$ and $H \leq Aut(R)$. The centre forms a group under the same operation as $Aut(R)$. Also, $H \subseteq Z(Aut(R))$ and H forms a group under same operation as $Aut(R)$, hence as $Z(Aut(R))$. Thus, $H \leq Z(Aut(R))$.
The centre of $Aut(R)$ is abelian and $H \leq Z \trianglelefteq Aut(R)$, hence H is normal in Z since subgroups of an abelian group are normal.
However, the relation of normality is not an equivalence relation. So we do not have enough information to conclude that H is normal in $Aut(R)$. □

Theorem 2.12.4. *The inner automorphism group is a normal subgroup of $Aut(R)$.*

Proof. Let $\psi \in Aut(R)$ and $\phi_g \in Inn(R)$. Then

$$\psi\phi_g\psi^{-1}(x) = \psi(g\psi^{-1}(x)g^{-1}) = \psi(g)x\psi(g^{-1}) = \phi_{\psi(g)}(x).$$

Thus, $\psi\phi_g\psi^{-1} = \phi_{\psi(g)} \in Inn(R)$. It follows that $Inn(R)$ is normal in $Aut(R)$. □

Definition 2.12.5.

The automorphisms of R which are not inner automorphisms are called **outer automorphisms**. Outer automorphisms of R form the outer automorphism group, denoted by

$$Out(R) = Aut(R)/Inn(R).$$

The identity map, $1_R : R \to R$ is an element of $Inn(R)$. Thus, $Out(R)$ is not a subgroup of $Aut(R)$ since it does not contain the identity element.

Definition 2.12.6.

An automorphism ϕ of R is called **class preserving** if for all $g \in R, \phi(g)$ is in the conjugacy class of R. We denote the set of all class preserving automorphisms of R by $Aut_c(R)$.

Theorem 2.12.7. *The set of all class preserving automorphisms of G forms a normal subgroup of $Aut(R)$.*

Definition 2.12.8.

Let H be a subgroup of R and let

$$Aut_H(R) = \{\alpha \in Aut(R) \mid \forall x \in H,\ \alpha(x) = x\}.$$

For a normal subgroup N of $Aut(R)$, define $F(N) = \{x \in R \mid \beta(x) = x\ \forall \beta \in N\}$.

The next result highlights the connection between the characteristic subgroups of R and the normal subgroups of $Aut(R)$.

Lemma 2.12.9. *[17] Let $H \leq R$ and let $N \trianglelefteq Aut(R)$ with $Aut_H(R)$ and $F(N)$ as defined above. The following statements are true.*

1. *If H is a characteristic subgroup of R, then $Aut_H(R)$ is normal in $Aut(R)$.*

2. *If N is normal in $Aut(R)$, then $F(N)$ is a characteristic subgroup of R.*

3. *If H_1 and H_2 are characteristic subgroups of R and $H_1 \leq H_2$, then $Aut_{H_2}(R) \subset Aut_{H_1}(R)$.*

Proof. 1. Let $\alpha \in Aut_H(R)$, $\beta \in Aut(R)$ and $x \in H$. Then $\beta^{-1}\alpha\beta(x) = \beta^{-1}\alpha(\beta x) = \beta^{-1}(\beta x) = x$. Thus, $Aut_H(R)$ is a normal subgroup of $Aut(R)$.

2. Let N be a normal subgroup of $Aut(R)$, $\alpha \in N$, $x \in F(N)$ with $\beta \in Aut(R)$. Then $\alpha(\beta x) = \beta(\beta^{-1}\alpha\beta)(x) = \beta(x)$.

□

Proposition 2.12.10. *If H_1 and H_2 are characteristic subgroups of R, then $Aut_{H_1}(R)$ and $Aut_{H_2}(R)$ are normal subgroups of $Aut(R)$. These groups form two different isomorphisms classes, thus giving a non trivial non-cancellation set.*

Definition 2.12.11.

An automorphism α of R is called **central** if $x^{-1}\alpha(x) \in Z(R)$ for all $x \in R$.

Proposition 2.12.12. *The set of all central automorphisms of R, denoted by $Aut_{cent}(R)$ is a normal subgroup of $Aut(R)$ and $Aut_{cent}(R)$ is equal to the centralizer of $Inn(R)$ in $Aut(R)$.*

Chapter 3

Non-cancellation in the class of $\mathcal{K}$-groups

3.1 The Nielsen equivalence relation

In [22] and [28], the authors described a group structure on the non-cancellation set of semi-direct products of the form $R = T \rtimes_\lambda \mathbb{Z}^k$ using the Nielsen equivalence classes of epimorphisms from a finite rank free abelian group onto a finite abelian group. They dealt with presentations of modules over a principal ideal domain.

In this work, we consider a commutative ring $\mathbb{Z}$ and $\mathbb{Z}-$modules. We investigate epimorphisms from $\mathbb{Z}^k$ onto a finite abelian group B. We denote the set of all this epimorphisms by $RE_k(B)$.

According to P. Witbooi [28], the description of Nielsen equivalence classes depends on the rank of the automorphism group of T.

Definition 3.1.1. [28]

Let B be a non-trivial finite abelian group. The ***Prüfer rank*** of B, denoted by $r(B)$ is the smallest of the cardinalities of the generating subsets of B.

Theorem 3.1.2. *[1] Let B be a group. Then*

1. *$r(B) = 0$ if B is a trivial group and*
2. *$r(B) = 1$ if B is a cyclic group.*

Notation 3.1.3.

Let T be a finite abelian group and denote the automorphism group $Aut(T)$ of T by B. Following the notation from [28], we denote by $m(T) = m$ the number of prime divisors (including repetitions) of $|T|$ and $d(T)$ denotes the minimum number of generators of T. The next theorem presents a result on the number of minimum number of elements in the generating subset of $Aut(T)$.

Theorem 3.1.4. *[25, Theorem 1] Let T be a finite group and let m be the number of prime divisors (including repetitions) of $|T|$. Then,*

$$r(Aut(T)) \leq m + \left(\frac{m^2}{2}\right) \leq m^2. \tag{3.1}$$

Proof. Suppose that $m \leq 1$, then we have that $|T| = p$, where $p \geq$ is a prime number. It follows from Proposition 2.11.7 that $Aut(T)$ is isomorphic to a cyclic group of order $p-1$. Lastly, by Theorem 4.1.1, we have that $r(AutT) = 1$. Thus, 3.1 holds.

Assume $m \geq 2$, we want to show that $r(Aut(T)) \leq m + \left(\frac{m^2}{2}\right)$.

Consider a characteristic subgroup N of T such that $\langle 1\rangle \leq N \leq T$. Then there exists a homomorphism of $Aut(T)$ into $Aut(N) \times Aut(T/N)$ with kernel K. Also, K is isomorphic to a section of $N^{m(T/N)}$, [see [15, Proposition 1.C.3]].

Thus, $m(K) \leq m(N)m(T/N)$ and $m = m(N) + m(T/N)$. By induction on m we have

$$\begin{aligned}
r(Aut(T)) &\leq m(N) + \frac{[m(N)]^2}{2} + m(T/N) + \frac{[m(T/N)]^2}{2} + m(N)m(T/N) \\
&= m + \frac{[m(N)]^2}{2} + \frac{[m(T/N)]^2}{2} + m(N)m(T/N) \\
&= m + \frac{1}{2}\left[[m(N)]^2 + [m(T/N)]^2 + 2m(N)m(T/N)\right] \\
&= m + \frac{1}{2}[m(N) + m(T/N)]^2 \\
&= m + \frac{m^2}{2}
\end{aligned}$$

□

Let d be the lowest common multiple of invariant factors of B and let $k \in \mathbb{N}$. The following result gives a link between the group of endomorphisms of B and the group of enedomorphisms of is $\mathbb{Z}_d^k$.

Proposition 3.1.5. *[21] Let B be a finite abelian group and let $\rho : B \to B$ be defined by $b \mapsto db$ and let $J = Im(\rho)$. Then $h(J) \subseteq J$ for all endomorphisms h of B. Suppose that $\beta : B \to B/J$ is a canonical epimorphism, then B/J is isomorphic to $\mathbb{Z}_d^k$.*

For every endomorphism h of B there exists a unique $h_J \in End\ (\mathbb{Z}_d^k)$ such that $\beta \circ h = h_J \circ \beta$.

Definition 3.1.6. [21]
Let R and Q be groups such that α is an endomorphism of R^k and β is an automorphism of Q^k. Then the determinant of α is an element of R and the determinant of β is a unit of Q.

Proposition 3.1.7. *[21] Let B be a finite abelian group. Consider a natural number k such that $k \geq r(B)$. Suppose that h is an endomorphism of B. Then the determinant $det(h)$ of h is an element $det(h_J)$in $\mathbb{Z}_d$.*

Lemma 3.1.8. *[22, 2.1] Let B be a finite abelian group and d be the lowest common multiple of invariant factors of B. Consider homomorphisms $f, h : \mathbb{Z}^k \to \mathbb{Z}_d^k$ and $\alpha : \mathbb{Z}_d^k \to \mathbb{Z}_d^k$ such that $\alpha \circ h = f \circ \beta$ for some $\beta \in Aut(\mathbb{Z}^k)$. Then*

$$det(\alpha)det(h_J) \ = \pm\ det(f_J)\ mod\ d.$$

Proof. The units of $\mathbb{Z}$ are 1 and -1, thus $det(\beta) = \pm 1$ because β is an automorphism of $\mathbb{Z}^k$. Let $\alpha : \mathbb{Z}_d^k \to \mathbb{Z}_d^k$ and $f, h : \mathbb{Z}^k \to \mathbb{Z}_d^k$ be homomorphisms such that $\alpha \circ h = f \circ \beta$ for some β automorphism of $\mathbb{Z}^k$, then we have the following commutative diagram:

$$\begin{array}{ccc} \mathbb{Z}^k & \xrightarrow{h} & \mathbb{Z}_d^k \\ \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \alpha} \\ \mathbb{Z}^k & \xrightarrow{f} & \mathbb{Z}_d^k \ . \end{array}$$

The determinant of α is a unit of $\mathbb{Z}_d$.

For each $f, h : \mathbb{Z}^k \to \mathbb{Z}_d^k$ there exists $f_J,\ h_J : \mathbb{Z}_d^k \to \mathbb{Z}_d^k$. It follows by Proposition 3.1.7 that $det(f) = det(f_J)$ and $det(h) = det(h_J)$. Thus,

$$\begin{aligned} det(\alpha \circ h) &= det(f \circ \beta) \\ det(\alpha)det(h) &= det(f)det(\beta) \\ det(\alpha)det(h) &= \pm det(f) \\ det(\alpha)det(h_J) &= \pm det(f_J)\ in\ \mathbb{Z}_d. \end{aligned}$$

□

Let B be a finite abelian group, $k \in \mathbb{N}$ such that $k \geq r(B)$. The following definitions and results present basic results that are essential to the study of the Nielsen equivalence relation.

Definition 3.1.9. [22, 2.2]

Let B be a finite abelian group and let $b = (b_1, b_2 \ldots, b_k)$ be an ordered k-tuple of elements of B. For every b_j, let $d_j \in \mathbb{Z}$ such that $\langle d_j \rangle \leq \mathbb{Z}$ and $\langle d_j \rangle$ is the innihilator of $\langle b_j \rangle$. The ordered k-tuple $b = (b_1, b_2 \ldots, b_k)$ is said to be **good** if the following conditions hold true:

1. There exists a natural number q, $q \leq k$ such that $B = \langle b_1 \rangle \bigoplus \langle b_2 \rangle \bigoplus \ldots \bigoplus \langle b_q \rangle$ and $b_j = 0$ if and only if $q < j \leq k$.

2. For all $j < k$ we have that $d_{j+1} \mid d_j$.

The definition above is closely related to the fundamental theorem of finite abelian group, hence we say that b is good if B is a direct sum of cyclic groups $\langle b_1 \rangle$, $\langle b_2 \rangle$, $\ldots$, $\langle b_k \rangle$ and $d_{j+1} \mid d_j$ where $d_j = |\langle b_j \rangle|$.

Definition 3.1.10. [22, 2.3]

For a finite abelian group B, let $b = (b_1, \ldots, b_k)$ be a good ordered k-tuple of elements of B. For every integer n we define a unique homomorphism $f_{(b,n)} : \mathbb{Z}^k \to B$ as follows:

$$f_{(b,n)}(e_j) = \begin{cases} b_j & \text{if } j < k \\ nb_k & \text{if } j = k \end{cases}$$

where $e_1, \ldots, e_k$ is the standard basis of $\mathbb{Z}^k$. For simplicity we write f_n instead of $f(b, n)$.

The next lemma presents a condition under which a homorphism $f_n : \mathbb{Z}^k \to B$ is an epimorphism.

Lemma 3.1.11. *[22, 2.4] Let $b = (b_1, \ldots, b_k)$ be a good ordered k-tuple of elements of a finite abelian group B. Let $d_k \in \mathbb{Z}$ such that $d_k = |b_k|$, then f_n is an epimorphism if n is relatively prime to d_k.*

The set of all epimorphisms $f : \mathbb{Z}^k \to B$ will be denoted by $RE_k(B)$.

Definition 3.1.12. [28]
Let $f, g \in RE_k(B)$. Then f and g are said to be **Nielsen equivalent** if and only if there exists an automorphism α of $\mathbb{Z}^k$ such that $f = g \circ \alpha$. We write this as $f \sim_n g$, the subscript n on $\sim_n$ helps distinguish the Nielsen equivalence relation from the conjugacy relation. The set of Nielsen equivalent classes of epimorphisms is denoted by $RE_k^{\sim_n}(B)$ and the class of all epimorphisms that are Nielsen equivalent to f is denoted by $[f]$.

Proposition 3.1.13. *Let B be a finite abelian group. The Nielsen equivalence is an equivalence relation.*

Proof. 1. Let $f \in RE_k(B)$, then $f = f \circ 1_{\mathbb{Z}^k}$. Thus, $f \sim_n f$, giving that $\sim_n$ is reflexive.

2. Suppose $f, g \in RE_k(B)$, then $f \sim_n g$ implies that $f = g \circ \alpha$ for $\alpha \in Aut(\mathbb{Z}^k)$. It follows that $g = f \circ \alpha^{-1} \implies g \sim_n f$ since $\alpha^{-1} \in Aut(\mathbb{Z}^k)$. Thus, $\sim_n$ is symmetric.

3. Let $f, g, h \in RE_k(B)$ such that $f \sim_n g$ and $g \sim_n h$. Then there exist $\alpha, \beta \in Aut(\mathbb{Z}^k)$ such that $f = g \circ \alpha$ and $g = h \circ \beta$. This gives $f = (h \circ \beta) \circ \alpha = h \circ (\beta \circ \alpha)$. Then $\beta \circ \alpha \in Aut(\mathbb{Z}^k)$ since the automorphism group is closed under composition of maps. Hence, $f \sim_n h$.

□

The following result presents a condition under which the epimorphisms in $RE_k(B)$ are Nielsen equivalent to the unique homomorphism f_n.

Lemma 3.1.14. *[22, 2.4] Let B be a finite abelian group and let $b = (b_1, \ldots, b_k)$ be a good ordered k-tuple of elements of B. Let $d_k = |b_k|$. We have that every epimorphism in $RE_k(B)$ is Nielsen equivalent to some f_n where $(n, d_k) = 1$.*

Proof. An automorphism of $\mathbb{Z}^k$ has a determinant ± 1. Let $m, n \in \mathbb{Z}$ be relatively prime to d_k, then $m = \pm n \ mod \ d_k$ implies $f_n \sim_n f_m$. So for n relatively prime to d_k, the functions f_n represent all the Nielsen equivalence classes. □

The next result gives some conditions for which two epimorphisms f_n and f_m are Nielsen equivalent.

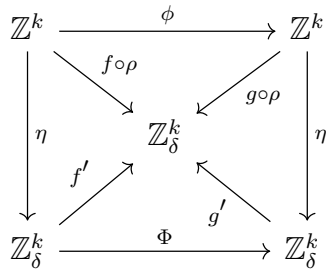
Lemma 3.1.15. *[22, 2.6] Let B be a finite abelian group and let $b = (b_1, \ldots, b_k)$ be a good ordered k-tuple of elements of B. Suppose that d_k is the order of b_k and let $m, n \in \mathbb{Z}$ such that $(m, d_k) = (n, d_k) = 1$. Then $f_n \sim_n f_m$ if and only if there exists $r \in \mathbb{Z}^*$ such that $m = \pm n + r d_k$.*

The following theorem gives sufficient conditions that have to be satisfied in order for any two epimorphisms $f, g : \mathbb{Z}^k \to B$ to be Nielsen equivalent.

Theorem 3.1.16. *[26, 3.4] Let B be a finite abelian group and let $f, g : \mathbb{Z}^k \to B$ be epimorphisms. If $f(\mathbb{Z}^k) = g(\mathbb{Z}^k)$ and $Im(f)$ is generated by a subset of fewer elements than k, then there exists $\alpha \in \mathbb{Z}^k$ such that $f = g \circ \alpha$.*

Proposition 3.1.17. *[28, 3.1] Let B be a finite abelian group such that $r(B) = k$ and let δ be the greatest common divisor of the orders of the invariant factors of B. Let $f, g \in RE_k(B)$ and let $\phi \in End(\mathbb{Z}^k)$ such that $f = g \circ \phi$. Then $coker(\phi)$ is a finite group and $|coker(\phi)|$ is relatively prime to δ.*

Proof. For a finite abelian group B, let $f, g \in RE_k(B)$. Let $\phi : \mathbb{Z}^k \to \mathbb{Z}^k$ be an endomorphism such that $f = g \circ \phi$. Then there exists an epimorphism $\rho : B \to \mathbb{Z}_\delta^k$. Let $y = (y_1, y_2, \ldots, y_k)$ be an element of $\mathbb{Z}^k$ and define a homomorphism $\eta : \mathbb{Z}^k \to \mathbb{Z}_\delta^k$ by $\eta((y_1, y_2, y_3 \ldots, y_k)) = (\overline{y_1}, \overline{y_2}, \overline{y_3} \ldots, \overline{y_k})$. By definition of η, there exists homomorphisms $f', g' : \mathbb{Z}_\delta^k \to \mathbb{Z}_\delta^k$ such that the following diagram is commutative.



Then it follows that f' and g' are isomorphisms since $\mathbb{Z}_\delta^k$ is finite and f' and g' are epimorphisms. Hence, $\Phi = (g')^{-1} \circ f'$ is also an isomorphism. The determinant $det(\Phi)$ of Φ is a unit of $\mathbb{Z}_\delta$.

The determinant of Φ is the residue class of $det(\phi)$. That is $det(\Phi) = det(\phi)\ mod\ \delta$. Then $det(\phi)$ is relatively prime to δ. Also, $|coker(\phi)| = |det(\phi)|$. □

3.2 Isomorphisms in the class of $\mathcal{K}$-groups

In this section we study the non-cancellation phenomena in the class of $\mathcal{K}$-groups. We refer to the work done by the authors in [22], [26], [28] and [29]. We give simplified proofs for isomorphisms for $\mathcal{K}$-groups.

We recall that a mapping $\mu : R \times X \to X$ is called a group action if the following conditions are satisfied:

1. $\mu(e_R, x) = x$ and
2. $\mu(ab, x) = \mu(a, \mu(b, x))$ for $a, b \in R$.

Definition 3.2.1. [22]
Let $k \in \mathbb{Z}$ and let T be a finite abelian group. We denote by $\mathcal{K}$ the class of semi-direct products of the form $R = T \rtimes_\lambda \mathbb{Z}^k$, where $\lambda : \mathbb{Z}^k \to Aut(T)$ is a group action.

Definition 3.2.2. [28]
Let R be a $\mathcal{K}$-group, the **non-cancellation** set of R, denoted by $\chi(R)$ is the set of all isomorphism classes $[Q]$ of groups Q such that $Q \times \mathbb{Z} \cong R \times \mathbb{Z}$.

Lemma 3.2.3. *[29] Let $R = T \rtimes_\lambda \mathbb{Z}^k$ be a $\mathcal{K}$-group, with a torsion subgroup T and a torsion-free quotient $\mathbb{Z}^k$. Consider another $\mathcal{K}$-group, $Q = S \rtimes_v \mathbb{Z}^l$ and let $f : R \to Q$ be a group homomorphism. Then f induces a homomorphisms $h_0 : T \to S$ and $h_1 : \mathbb{Z}^k \to \mathbb{Z}^l$.*

Theorem 3.2.4. *[29, 2.2] Let $R = T \rtimes_\lambda \mathbb{Z}^k$ and let $Q = T \rtimes_v \mathbb{Z}^k$ for some $k \in \mathbb{N}$. Then $Q \cong R$ if and only if there exist automorphisms $f : T \to T$ and $h : \mathbb{Z}^k \to \mathbb{Z}^k$ such that the following identity holds for every $t \in T$ and every $z \in \mathbb{Z}^k$,*

$$[f \circ \lambda(z)](t) = [v(h(z))](f(t)). \tag{3.2}$$

Proof. Suppose that $R = T \rtimes_\lambda \mathbb{Z}^k$ and $Q = T \rtimes_v \mathbb{Z}^k$ such that $R \cong Q$. Then $\phi : R \to Q$ induces homomorphisms $f : T \to T$ and $h : \mathbb{Z}^k \to \mathbb{Z}^k$. Also, f and h are bijective, thus giving $f \in Aut(T)$ and $h \in Aut(\mathbb{Z}^k)$. It remains to show that (3.2) holds for all $t \in T$ and

$z \in \mathbb{Z}^k$.

Let $(x, q),\ (y, r)$ denote elements of R and let $(x', q'),\ (y', r')$ denote elements of Q. We define the binary operations in these groups by $(x, q)(y, r) = (x\lambda(q)y, q + r)$ for R and $(x', q')(y', r') = (x'v(q')y', q' + r')$ for Q.

For any $t \in T$ and $z \in \mathbb{Z}^k$, let $\phi : R \to Q$ be defined by $\phi(t, z) = (f(t), h(z))$. Then it follows that

$$\begin{aligned} \phi(t, 0) &= (f(t), h(0)) \\ &= (f(t), 0) \end{aligned}$$

and

$$\phi(1, z) = (u, h(z)) \ where\ u = f(1)$$

By the definition of multiplication, we have that $(1, z)(t, 0) = ([\lambda(z)](t), z)$ and $([\lambda(z)](t), 0)(1, z) = ([\lambda(z)](t), z)$. Thus,

$$\begin{aligned} \phi[(1, z)(t, 0)] &= \phi\left[([\lambda(z)](t), 0)(1, z)\right] \\ &= \phi[[\lambda(z)](t), 0)] \cdot \phi[(1, z)] \qquad \text{since } \phi \text{ is a homomorphism} \\ &= (f([\lambda(z)](t)), h(0)) \cdot (f(1), h(z)) \\ &= (f([\lambda(z)](t), 0)(u, h(z)) \qquad \text{where } u = f(1) \\ &= ([f \circ \lambda(z)](t) \cdot u, h(z)) \end{aligned}$$

and

$$\begin{aligned} \phi[(1, z)(t, 0)] &= \phi(1, z) \cdot \phi(t, 0) \qquad \phi \text{ is a homomorphism} \\ &= (f(1), h(z)) \cdot (f(t), 0) \\ &= (u \cdot [v(h(z))(f(t))], h(z)) \qquad \text{where } u = f(1) \\ &= (u \cdot [v(h(z)) \circ f](t), h(z)). \end{aligned}$$

Hence,

$$\begin{aligned}([f \circ \lambda(z)](t) \cdot u, h(z)) &= (u \cdot [v(h(z)) \circ f](t), h(z)) \\ [f \circ \lambda(z)](t) \cdot u &= u \cdot [v(h(z)) \circ f](t) \\ [f \circ \lambda(z)](t) &= [v(h(z)) \circ f](t) \text{ since } T \text{ is abelian} \\ [f \circ \lambda(z)](t) &= [v(h(z))](f(t)).\end{aligned}$$

Conversely, suppose that there exist $f \in Aut(T)$ and $h \in Aut(\mathbb{Z}^k)$ and define the function $\phi : R \to Q$ by $\phi(t, z) = (f(t), h(z))$. We have to show that ϕ is a homomorphism.

Let $(x, q),\ (y, r)$ be elements of R. Then

$$\begin{aligned}\phi((x, q)(y, r)) &= \phi((x\lambda(q)y, q + r)) \\ &= (f(x\lambda(q)y), h(q + r)).\end{aligned}$$

It follows that $f(x\lambda(q)y) = f(x)f(\lambda(q))f(y)$ and $h(q + r) = h(q) + h(r)$ since f and h are defined to be homomorphisms.

Also,

$$\begin{aligned}f(\lambda(q)) &= f \circ \lambda(q) \\ &= v(h(q)) \textit{ since } [f \circ \lambda(z)](t) = [v(h(z))](f(t))\end{aligned}$$

Hence,

$$\begin{aligned}\phi((x, q)(y, r)) &= (f(x\lambda(q)y), h(q + r)) \\ &= (f(x)f(\lambda(q))f(y), h(q) + h(r)) \\ &= (f(x)v(h(q))f(y), h(q) + h(r)) \\ &= (f(x), h(q))(f(y), h(r)) \\ &= \phi(x, q)\phi(y, r).\end{aligned}$$

Then ϕ is a group homomorphism.

Finally, ϕ is an isomorphism since f and h are isomorphisms. □

The next two results from literature are direct consequences of Theorem 3.2.4.

Theorem 3.2.5. *[29, 2.3] Let T be a finite abelian group and let $k \in \mathbb{N}$. Let $R = T \rtimes_\lambda \mathbb{Z}^k$ and let $Q = T \rtimes_v \mathbb{Z}^k$. If $Q \cong R$, then $\lambda(\mathbb{Z}^k) = \alpha v(\mathbb{Z}^k)\alpha^{-1}$ for some automorphism α of T.*

Proof. Let $\theta : R \to Q$ be an isomorphism. By Theorem 3.2.4 it follows that there exist $f \in Aut(T)$ and $h \in Aut(\mathbb{Z}^k)$ such that

$$f \circ \lambda(z) = [v(h(z))](f)$$

for every $z \in \mathbb{Z}^k$.
Hence, $\lambda(z) = f^{-1}[v(h(z))]f \in f^{-1}v(\mathbb{Z}^k)f$ for all $z \in \mathbb{Z}^k$. This implies that $\lambda(\mathbb{Z}^k) \subseteq fv(\mathbb{Z}^k)f^{-1}$.
The image of v coincides with the image of $v \circ h$ since $h : \mathbb{Z}^k \to \mathbb{Z}^k$ is an epimorphism. Hence, $f^{-1}v(h(z))f = \lambda(\mathbb{Z}^k) \implies f^{-1}v(\mathbb{Z}^k)f \subseteq \lambda(\mathbb{Z}^k)$. Therefore, $\lambda(\mathbb{Z}^k) = f^{-1}v(\mathbb{Z}^k)f$. □

Theorem 3.2.6. *[22, 3.2] Characterization of isomorphic $\mathcal{K}$-groups*
Let $R = T \times_u \mathbb{Z}^k$ and let $Q = T \rtimes_v \mathbb{Z}^k$ be $\mathcal{K}$-groups. Then $R \cong Q$ if and only if there exists an automorphism α of T such that $u \sim_n \lambda$, where $\lambda : \mathbb{Z}^k \to Aut(T)$ is defined by $\lambda(z) \mapsto \alpha v(z)\alpha^{-1}$.

We deduce the following results from Theorem 3.2.4.

Corollary 3.2.7. *Let $h : \mathbb{Z}^k \to \mathbb{Z}^k$ be an automorphism and let $v : \mathbb{Z}^k \to Aut(T)$ be a group homomorphism. Then $Im(v \circ h) = Im(v)$.*

Proof. Let $h : \mathbb{Z}^k \to \mathbb{Z}^k$ and let $v : \mathbb{Z}^k \to Aut(T)$, then $v \circ h : \mathbb{Z}^k \to Aut(T)$. Also,

$$Im(v) = \{v(z_1) \mid z_1 \in \mathbb{Z}^k\} \subset Aut(T) \text{ and}$$

$$Im(v \circ h) = \{(v \circ h)(z_2) \mid z_2 \in \mathbb{Z}^k\} \subset Aut(T).$$

Since h is an automorphism, then it is surjective. So for any $z \in \mathbb{Z}^k$ there exists z_1 in $\mathbb{Z}^k$ such that $z = h(z_1)$. Hence, $v(z_1) = v(h(z_2))$, that is

$$\{v(z_1) \mid z_1 \in \mathbb{Z}^k\} \;=\; \{(v \circ h)(z_2) \mid z_2 \in \mathbb{Z}^k\}.$$

□

For subgroups Q and P of Q, were call that Q is conjugate to P if $Q = xPx^{-1}$ for every element $x \in R$.

Corollary 3.2.8. *Let $f : T \to T$ and $h : \mathbb{Z}^k \to \mathbb{Z}^k$ be automorphisms and let $\lambda, v : \mathbb{Z}^k \to Aut(T)$. Then $Im(\lambda)$ is conjugate to $Im(v)$ if and only if $[f \circ \lambda(z)](t) = [v(h(z))]\,(f(t))$.*

Proof. Suppose that $[f \circ \lambda(z)](t) = [v(h(z))]\,(f(t))$, then

$$\begin{aligned} [f \circ \lambda(z)](t) \;&=\; [v(h(z)) \circ f]\,(t) \\ \implies f \circ \lambda(z) \;&=\; v(h(z)) \circ f \end{aligned}$$

Then for any $z \in \mathbb{Z}^k$, it follows that

$$\begin{aligned} \lambda(z) \;&=\; f^{-1}\,[v(h(z))]\,f \\ &=\; f^{-1}\,[v(z)]\,f \;\in\; f^{-1}\left[v(\mathbb{Z}^k)\right] f. \end{aligned}$$

Hence, $\lambda(\mathbb{Z}^k) \subseteq f^{-1}\left[v(\mathbb{Z}^k)\right] f$.
Similarly, $f^{-1}\left[v(\mathbb{Z}^k)\right] f \subseteq \lambda(\mathbb{Z}^k)$. Then $v(\mathbb{Z}^k)$ is conjugate to $\lambda(\mathbb{Z}^k)$.
Conversely, let $Im(\lambda) \sim Im(v)$. Then $\lambda(\mathbb{Z}^k) \;=\; f^{-1}\left[v(\mathbb{Z}^k)\right] f$, where $f \in Aut(T)$. This implies that $f \circ \left[\lambda(\mathbb{Z}^k)\right] \;=\; \left[v(\mathbb{Z}^k)\right] \circ f$. For some $z \in \mathbb{Z}^k$ and $f : T \to T$, we have that

$$\begin{aligned} f \circ [\lambda(z)] \;&=\; [v(z)] \circ f \\ &= [v(h(z))] \circ f \qquad \textit{since } Im(v) = \; Im(v \circ h). \end{aligned}$$

□

Let $R = T \rtimes_\lambda \mathbb{Z}^k$ be a $\mathcal{K}$-class group. Let $B = Aut(T)$ and let $RE_k^{\sim_n}(B)$ be the set of Nielsen equivalent classes. Our next task is to establish a link between the Nielsen equivalence classes and the conjugacy classes of B. In [22] and [26], the authors described the

non-cancellation set of $\mathcal{K}$-groups through Nielsen equivalence classes. Also, in [22], P. Witbooi presented a result which describes the non-cancellation set through conjugacy classes of B. Inspired by this, we shall use the results on the non-cancellation phenomena to prove that there is a link between the Nielsen equivalence relation and the conjugacy relation.

The following result is important for proving the link between the Nielsen equivalence classes and the conjugacy classes.

Lemma 3.2.9. *Let N and H be groups and let $\rho : H \to Aut(N)$ be a homomorphism. If $\beta \in Aut(H)$, then the groups $N \rtimes_\rho H$ and $N \rtimes_{\rho\circ\beta} H$ are isomorphic.*

Proof. Consider groups N and H and let $\rho : H \to Aut(N)$. For an automorphism β of H, we define the mapping $\theta : N \rtimes_\rho H \to N \rtimes_{\rho\circ\beta} H$ by $(n, h) \mapsto (n, \beta^{-1}(h))$.
Suppose that $(n_1, h_1) = (n_2, h_2)$, then $n_1 = n_2$ and $h_1 = h_2$. It follows that $\beta^{-1}(h_1) = \beta^{-1}(h_2)$ since β is well-defined. Hence, $(n_1, \beta^{-1}(h_1)) = (n_2, \beta^{-1}(h_2))$.
Recall that the binary operation in $N \rtimes_\rho H$ is defined by $(n_1, h_1)*(n_2, h_2) = (n_1\rho(h_1)(n_2), h_1h_2)$. Then θ is a homomorphism since

$$\begin{aligned}
\theta\Big((n_1, h_1) * (n_2, h_2)\Big) &= \theta\Big((n_1\rho(h_1)(n_2),\ h_1h_2)\Big) \\
&= \Big((n_1\rho(h_1)(n_2),\ \beta^{-1}(h_1h_2)\Big) \\
&= \Big((n_1\rho(h_1)(n_2),\ \beta^{-1}(h_1)\beta^{-1}(h_2)\Big) \text{ since } \beta \text{ is a homomorphism}
\end{aligned}$$

and

$$\begin{aligned}
\theta(n_1, h_1)\theta(n_2, h_2) &= (n_1,\ \beta^{-1}(h_1)) * (n_2,\ \beta^{-1}(h_2)) \\
&= (n_1(\rho \circ \beta)(\beta^{-1}(h_1))(n_2),\ \beta^{-1}(h_1)\beta^{-1}(h_2)) \\
&= (n_1\rho(h_1)(n_2),\ \beta^{-1}(h_1)\beta^{-1}(h_2)).
\end{aligned}$$

The mapping θ is onto since for every $(n, \beta^{-1}(h))$ in $N \rtimes_{\rho\circ\beta} H$ there exists (n, h) $N \rtimes_\rho H$. Finally, we show that $\theta : N \rtimes_\rho H \to N \rtimes_{\rho\circ\beta} H$ is one-to-one. Suppose that $\theta(n_1, h_1) =$

$\theta(n_2, h_2)$, then

$$\begin{aligned}(n_1, \beta^{-1}(h_1)) = (n_2, \beta^{-1}(h_2)) &\implies n_1 = n_2 \text{ and } \beta^{-1}(h_1) = \beta^{-1}(h_2) \\ &\implies (n_1, h_1) = (n_2, h_2).\end{aligned}$$

Thus, $N \rtimes_\rho H \cong N \rtimes_{\rho\circ\beta} H$. □

Proposition 3.2.10. *Let $R = T \rtimes_\lambda \mathbb{Z}^k$ and $Q = T \rtimes_v \mathbb{Z}^k$ where $\lambda, v : \mathbb{Z}^k \to Aut(T)$ are group actions. If the images $Im(\lambda)$ and $Im(v)$ are conjugate in $Aut(T)$ then λ is Nielsen equivalent to v.*

Proof. Let $R = T \rtimes_\lambda \mathbb{Z}^k$ and $Q = T \rtimes_v \mathbb{Z}^k$ where $\lambda, v : \mathbb{Z}^k \to Aut(T)$ are group actions. Suppose that $Im(\lambda)$ is conjugate to $Im(v)$ in $Aut(T)$. It follows by Corollary 3.2.8 that $[f \circ \lambda(z)](t) = [v(h(z))]\,(f(t))$ for some automorphisms $f \in Aut(T)$ and $h \in Aut(\mathbb{Z}^k)$. Then by Theorem 3.2.4 we have that $R \cong Q$, that is $T \rtimes_\lambda \mathbb{Z}^k \cong T \rtimes_v \mathbb{Z}^k$.
Applying Lemma 3.2.9, we get $T \rtimes_v \mathbb{Z}^k \cong T \rtimes_{v\circ h} \mathbb{Z}^k$. Thus, $T \rtimes_\lambda \mathbb{Z}^k \cong T \rtimes_{v\circ h} \mathbb{Z}^k$ since $\cong$ is an equivalence relation.
Applying Theorem 3.2.4 and Corollary 3.2.8 to these the isomorphisms gives:

1. $Im(\lambda)$ is conjugate to $Im(v)$,
2. $Im(v)$ is conjugate to $Im(v \circ h)$ and
3. $Im(\lambda)$ is conjugate to $Im(v \circ h)$.

Hence, $Im(v)$ is self-conjugate since $Im(v) = Im(v \circ h)$. Also,

$$\begin{aligned} Im(\lambda) &= \alpha^{-1} Im(v) \alpha \quad \text{for some } \alpha \in Aut(T) \\ &= Im(v) \quad \text{since Im(v) commutes with every element of } Aut(T) \\ &= Im(v \circ h). \end{aligned}$$

Hence $\lambda = v \circ h$.

□

Following the notation in [26], we present another notation of groups in the $\mathcal{K}$-class. Let T be a finite abelian group and let q be the exponent of T. For any positive integer k, suppose that $u_1,\ u_2,\ ,\ldots,\ u_k$ is a sequence of integers which are relatively prime to q, then we denote a $\mathcal{K}$-group $R = T \rtimes_\lambda \mathbb{Z}^k$ by $R(T; u_1, u_2, , \ldots, u_k)$. For simplicity, we adopt the short-hand notation and write $R(q; u_1, u_2, , \ldots, u_k)$ instead of $R(\mathbb{Z}_q; u_1, u_2, , \ldots, u_k)$ where q is relatively prime to each u_i. Thus, a group $R = \mathbb{Z}_n \rtimes_\lambda \mathbb{Z}$ is simply denoted by $R(n, u)$ for $n, u \in \mathbb{Z}^+$ with $gcd(n, u) = 1$.

The following results present conditions under which two $\mathcal{K}$-groups are isomorphic to each other.

Theorem 3.2.11. *[26, 0.3] Let $u_1,\ u_2,\ ,\ldots,\ u_k$ be a sequence of integers all of which are relatively prime to q. Then $R(q; u_1, u_2, , \ldots, u_k, 1) \cong R(q; u_1, u_2, , \ldots, u_k) \times \mathbb{Z}$.*

Proof. Let $R = R(q; u_1, u_2, , \ldots, u_k) = \mathbb{Z}_q \rtimes_\lambda \mathbb{Z}^k$ and let $Q = R(q; u_1, u_2, , \ldots, u_k, 1) = \mathbb{Z}_q \rtimes_v \mathbb{Z}^{k+1}$ where $\lambda : \mathbb{Z}^k \to Aut(\mathbb{Z}_q)$ and $v : \mathbb{Z}^{k+1} \to Aut(\mathbb{Z}_q)$ are group actions. It follows that $\lambda(\mathbb{Z}^k) = v(\mathbb{Z}^{k+1})$ and $Im(\lambda)$ is generated by a subset of fewer than $k+1$ elements. Theorem 3.1.16 states that if $Im(\lambda) = Im(v)$, then there exists an automorphism α of $\mathbb{Z}^{k+1}$ such that $\lambda = v \circ \alpha$. Hence, we shall write $v \sim_n \lambda$, where n in the notation $\sim_n$ distinguishes the Nielsen equivalence relation from the conjugacy relation.
Consider another $\mathcal{K}$-group $F = \mathbb{Z}_q \rtimes_\epsilon \mathbb{Z}^{k+1}$, where $\epsilon : \mathbb{Z}^{k+1} \to Aut(\mathbb{Z}_q)$ is a group action. Then $v \sim_n \epsilon$. Let T_R, T_Q and T_F denote torsion subgroups of R, Q and F respectively and suppose $Q \cong F$. Then $T_Q \cong T_F$ and their respective torsion free quotients are also isomorphic. However, R and F have equal torsion free quotients and $\mathbb{Z}^{k+1} \cong \mathbb{Z}^k \times \mathbb{Z}$. Thus, $\lambda \sim_n \epsilon$ and $F \cong R \times \mathbb{Z}$. This implies that $Q \cong$R$\times\mathbb{Z}$. □

Theorem 3.2.12. *[27, 3.1] Let T be a finite abelian group of exponent n and let u_1 and u_2 be integers such that $(n, u_1) = (n, u_2) = 1$. Then the following statements are equivalent.*

1. *$R(T; u_1) \cong R(T; u_2)$,*
2. *$u_1 \equiv u_2$ mod n or $u_1 u_2 \equiv 1$ mod n.*

Proof. For each $i \in \{1, 2\}$, consider an automorphism λ_i of T defined by $t \mapsto u_i t$. Suppose that λ_1 and λ_2 are the only elements of $Z(Aut(T))$. Let $R(T; u_1) \cong R(T; u_2)$. Applying Theorem 3.2.4 gives $\lambda_1 = \lambda_2$ or $\lambda_1 = \lambda_2^{-1}$. Hence, $R(T; u_1) \cong R(T; u_2)$ implies $u_1 \equiv u_2 \; mod \; n$ or $u_1 u_2 \equiv 1 \; mod \; n$. □

Next, we discuss some results on the non-cancellation phenomena in the class of $\mathcal{K}$-groups.

Theorem 3.2.13. *[27, 2.4] Let T be a finite abelian group. Let $\lambda, v : \mathbb{Z}^k \to Aut(T)$ be group actions such that $R = T \rtimes_\lambda \mathbb{Z}^k$ and $Q = T \rtimes_v \mathbb{Z}^k$. If $\lambda(\mathbb{Z}^k) = v(\mathbb{Z}^k)$, then $R \times \mathbb{Z} \cong Q \times \mathbb{Z}$.*

Theorem 3.2.14. *[22, 3.1] Let $R = T \rtimes_\lambda \mathbb{Z}^k$ and $Q = T \rtimes_v \mathbb{Z}^k$ where T is a finite abelian group. The following two statements are equivalent:*

1. *$R \times \mathbb{Z} \cong Q \times \mathbb{Z}$,*
2. *$\lambda(\mathbb{Z}^k) = \alpha v(\mathbb{Z}^k)\alpha^{-1}$ for some $\alpha \in Aut(T)$.*

Proof. Let $R = T \rtimes_\lambda \mathbb{Z}^k$ and $Q = T \rtimes_v \mathbb{Z}^k$ such that $R \times \mathbb{Z} \cong Q \times \mathbb{Z}$. Define a projection $f : \mathbb{Z}^{k+1} \to \mathbb{Z}^k$ by $f(e_{k+1}) = 0$, where $e_1, \ldots, e_k$ is the standard basis of $\mathbb{Z}^k$. Suppose $\lambda = \lambda_1 \circ f$ and $v = v_1 \circ f$, then $R \times \mathbb{Z} \cong T \rtimes_{\lambda_1} \mathbb{Z}^{k+1}$ and $Q \times \mathbb{Z} \cong T \rtimes_{v_1} \mathbb{Z}^{k+1}$. By Theorem 3.2.5, $\lambda_1(\mathbb{Z}^{k+1}) = \alpha^{-1} v_1(\mathbb{Z}^{k+1})\alpha$ for some $\alpha \in Aut(T)$. Finally, $\lambda(\mathbb{Z}^k) = \lambda_1(\mathbb{Z}^{k+1})$ and $v(\mathbb{Z}^k) = v(\mathbb{Z}^{k+1})$ since f is onto. Hence, $\lambda(\mathbb{Z}^k) = \alpha v(\mathbb{Z}^k)\alpha^{-1}$.
Suppose that $\lambda(\mathbb{Z}^k) = \alpha v(\mathbb{Z}^k)\alpha^{-1}$ for some $\alpha \in Aut(T)$. Let $K = T \rtimes_h \mathbb{Z}^k$ where $h : \mathbb{Z}^k \to Aut(T)$ is a homomorphism defined by $h(z) = \alpha\lambda(z)\alpha^{-1}$. Fix $\alpha = h_0 : T \to T$ and let $h_1 : \mathbb{Z}^k \to \mathbb{Z}^k$ be an identity automorphism. Then $Im(h)$ is conjugate to $Im(\lambda)$ which implies that $h(\mathbb{Z}^k) = v(\mathbb{Z}^k)$. Therefore, $K \times \mathbb{Z} \cong Q \times \mathbb{Z} \implies R \times \mathbb{Z} \cong Q \times \mathbb{Z}$ since $K \cong R$. □

From the two preceding results, we can conclude that two $\mathcal{K}$-groups, $T \rtimes_\lambda \mathbb{Z}^k$ and $T \rtimes_v \mathbb{Z}^k$ are in the same non-cancellation set if and only if the images $Im(\lambda)$ and $Im(v)$ coincide or are conjugate in $Aut(T)$.

Recall that the non-cancellation set measures the extent to which an infinite cyclic group

$\mathbb{Z}$ can be cancelled as a direct factor. Thus, before we look at the trivial case of the non-cancellation set, we shall state a result that allows cancellation.

Lemma 3.2.15. *[12] Suppose that R and Q are any groups such that $R \times \mathbb{Z} \cong Q \times \mathbb{Z} \times \mathbb{Z}$. Then $R \cong Q \times \mathbb{Z}$.*

Theorem 3.2.16. *[26, 4.2] Let $R = T \rtimes_\lambda \mathbb{Z}^k$ where $k \in \mathbb{Z}^+$, T is a finite abelian group and $\lambda : \mathbb{Z}^k \to Aut(T)$ is a group action. If the image of λ in $Aut(T)$ can be generated by a set of fewer elements than k then the non-cancellation set $\chi(R)$ is trivial.*

Proof. Let H be a $\mathcal{K}-$group such that $Q \times \mathbb{Z} \cong R \times \mathbb{Z}$. Suppose that $\lambda(\mathbb{Z}^{k+1})$ is generated by a subset of k elements and let $v : \mathbb{Z}^k \to \lambda(\mathbb{Z}^{k+1})$ be a homomorphism. Then $v(\mathbb{Z}^k) = \lambda(\mathbb{Z}^{k+1})$ and $R \cong (T \rtimes_v \mathbb{Z}^k) \times \mathbb{Z}$.
By our assumption we have that $Q \times \mathbb{Z} \cong R \times \mathbb{Z}$ and $R \times \mathbb{Z} \cong (T \rtimes_v \mathbb{Z}^k) \times \mathbb{Z} \times \mathbb{Z}$. By Lemma 3.2.15 we get that $Q \cong (T \rtimes_v \mathbb{Z}^k) \times \mathbb{Z}$ and $(T \rtimes_v \mathbb{Z}^k) \times \mathbb{Z} \cong R$. Hence, $R \cong Q$. □

The following result follows from the description of the non-cancellation set through the notion of Nielsen equivalence classes and the notion of conjugacy classes.

Proposition 3.2.17. *Let $R = T \rtimes_\lambda \mathbb{Z}^k$ and $Q = T \rtimes_v \mathbb{Z}^k$ where $\lambda, v : \mathbb{Z}^k \to Aut(T)$ are group actions. If λ is Nielsen equivalent to v, then $Im(\lambda)$ and $Im(v)$ are conjugate in $Aut(T)$.*

Proof. Suppose that λ is Nielsen equivalent to v, then $\lambda = v \circ h$, where h is an automorphism of $\mathbb{Z}^k$. So it follows that

$$\begin{aligned}
\lambda(z) &= (v \circ h)(z) \quad \forall z \in \mathbb{Z}^k \\
\implies Im(\lambda) &= Im(v \circ h) \\
\implies Im(\lambda) &= Im(v) \quad \text{by Corollary 3.2.7} \\
\implies R \times \mathbb{Z} &\cong Q \times \mathbb{Z} \quad \text{by Theorem 3.2.13} \\
\implies Im(\lambda) &= \alpha Im(v) \alpha^{-1} \quad \text{by Theorem 3.2.14}
\end{aligned}$$

□

In this section, we studied the non-cancellation phenomena in the class of $\mathcal{K}$-groups. We deduced some results that follow from Theorem 3.2.4 which states that two $\mathcal{K}$-groups, $R = T \rtimes_\lambda \mathbb{Z}^k$ and $Q = T \rtimes_v \mathbb{Z}^k$ are isomorphic if and only if there exist automorphisms $f : T \to T$ and $h : \mathbb{Z}^k \to \mathbb{Z}^k$ such that $[f \circ \lambda(z)](t) = [v(h(z))](f(t))$ for every $t \in T$ and every $z \in \mathbb{Z}^k$. We also established a link between the Nielsen equivalence classes and the conjugacy classes.

The next section is motivated by Theorem 3.2.14 which states that two $\mathcal{K}$-groups $R = T \rtimes_\lambda \mathbb{Z}^k$ and $Q = T \rtimes_v \mathbb{Z}^k$ are in the same non cancellation set if and only if the images $Im(\lambda)$ and $Im(v)$ are conjugate in $Aut(T)$.

Suppose that $R_i = T \rtimes_{\lambda_i} \mathbb{Z}^k$ where $\lambda_i : \mathbb{Z}^k \to Aut(T)$ is a group action and denote by Q_i the image of λ_i. Recall that $Im(\lambda_i)$ is a subgroup of $Aut(T)$, hence for a certain group T we want to study its conjugate subgroups.

Consider automorphisms α and β of a finite abelian group T and let $Q_1 = \alpha Q_2 \alpha^{-1}$ and $Q_2 = \beta Q_3 \beta^{-1}$. Then R_1, R_2 and R_3 are in the same isomorphism class since $Q_1 = (\alpha\beta)Q_3(\alpha\beta)^{-1}$ and $\alpha\beta \in Aut(T)$. Conjugate subgroups can be represented by one isomorphism class in the non-cancellation set, thus if all subgroups of $Aut(T)$ are conjugate to each other then the non cancellation set has only one isomorphism class.

Other subgroups of $Aut(T)$ which do not have conjugates form distinct isomorphism classes in the non-cancellation set. Thus, investigating conjugate subgroups of $Aut(T)$ gives an insight on the order of the non-cancellation set. In Chapter 2 we discussed the normal subgroups of the automorphism group. Recall that these subgroups are self conjugate. Thus, if $Im(\lambda)$ and $Im(v)$ are normal subgroups of $Aut(T)$ then $T \rtimes_\lambda \mathbb{Z}^k$ and $T \rtimes_v \mathbb{Z}^k$ are not in the same isomorphism class. This implies that the non-cancellation set is not trivial.

An interesting questions would then be:

"What properties should a group satisfy to ensure that all its subgroups are normal?"

We know that all subgroups of an abelian group are normal. Hence, we have that if the

automorphism group of T is abelian then the non-cancellation set is not trivial.

The non-cancellation phenomena has already been studied for the case where T is a finite abelian group ([22], [26], [28] and [29]). Our interest is to expand this and study the non cancellation of groups of the form $R = T \rtimes_\lambda \mathbb{Z}^k$ where T is a finite group that is not necessarily abelian. We shall begin by studying non-abelian groups with abelian automorphism groups.

3.3 Miller p-groups

The main results of this section are based on the following papers; G. Miller[18], D. Jonah and M. Konvisser[14], C. Hopkins[13] and B. Earnley[4]. We discuss specific cases of T that result in every automorphism group of T being abelian. That is, we want to answer the question "When is the automorphism group abelian?"

There isn't any known general condition that can ensure that the automorphism group is abelian but various authors have studied the structures of different groups and identified groups that have an abelian automorphism group. We shall begin by discussing the case when T is an abelian group.

Lemma 3.3.1. *[19, Lemma 6]*

Let T be a cyclic group, then $Aut(T)$ is abelian.

Proof. Let $T = \langle t \rangle$. Consider automorphisms α and β of T. We want to show that $\alpha \circ \beta = \beta \circ \alpha$.

For positive integers a and b, we have that $t^a, t^b \in T$. Define the automorphisms of T by: $\alpha(t) = t^a$ and $\beta(t) = t^b$. Thus,

$$\begin{aligned}
(\alpha \circ \beta)(t) &= \alpha(\beta(t)) \\
&= \alpha(t^b) \\
&= (t^b)^a \\
&= t^{ba} \\
&= t^{ab} \qquad a \text{ and } b \text{ commute since } \mathbb{Z} \textit{ is} \text{ abelian} \\
&= (t^a)^b \\
&= \alpha(t^b) \\
&= \alpha(\beta(t)).
\end{aligned}$$

Thus, $\beta \circ \alpha = \alpha \circ \beta$.

□

Abelian groups can either be cyclic or non-cyclic. So our next task is to discuss commutativity in the automorphism group of a non-cyclic group T.

Proposition 3.3.2. *Let T be an abelian group that is not cyclic. Then $Aut(T)$ is non-abelian.*

Proof. Suppose that $T = \mathbb{Z}_m \times \mathbb{Z}_{md}$ for some positive integers m and d. We first show that $\mathbb{Z}_m \times \mathbb{Z}_{md}$ is not cyclic.
In our case we have that $gcd(m, md) = m \neq 1$. Thus, $\dfrac{m * md}{gcd(m, md)} = md$ is divisible by both m and md. Therefore, for any element $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_{md}$ the sum of l copies of (a, b) is given by $(la \ mod \ m, \ lb \ mod \ md)$. Then

$$\Big(\frac{m * md}{gcd(m, md)} a \ mod \ m, \ \frac{m * md}{gcd(m, md)} b \ mod \ md\Big) = (0, 0).$$

A cyclic subgroup generated by (a, b) has an order less than $\dfrac{m * md}{gcd(m, md)} < |\mathbb{Z}_m \times \mathbb{Z}_{md}|$. Therefore, $\mathbb{Z}_m \times \mathbb{Z}_{md}$ cannot be generated by any of its elements. This implies that $\mathbb{Z}_m \times \mathbb{Z}_{md}$ is not cyclic.

Next, we show that $Aut(\mathbb{Z}_m \times \mathbb{Z}_{md})$ is not abelian.
We define automorphisms α, β of $\mathbb{Z}_m \times \mathbb{Z}_{md}$ by:

$$\alpha : (x + m\mathbb{Z}, \ y + md\mathbb{Z}) \mapsto (x + y + m\mathbb{Z}, \ y + md\mathbb{Z}) \ and$$

$$\beta : (x + m\mathbb{Z}, \ y + md\mathbb{Z}) \mapsto (x + m\mathbb{Z}, \ y + dx + md\mathbb{Z}).$$

Thus,

$$\begin{aligned} (\alpha \circ \beta)(m\mathbb{Z}, \ 1 + md\mathbb{Z}) &= \alpha(\beta(m\mathbb{Z}, \ 1 + md\mathbb{Z})) \\ &= \alpha(m\mathbb{Z}, \ 1 + md\mathbb{Z}) \\ &= (1 + m\mathbb{Z}, \ 1 + md\mathbb{Z}) \end{aligned}$$

Also

$$\begin{aligned}(\beta \circ \alpha)(m\mathbb{Z},\ 1+md\mathbb{Z}) &= \beta(\alpha(m\mathbb{Z},\ 1+md\mathbb{Z})) \\ &= \beta(1+m\mathbb{Z},\ 1+md\mathbb{Z}) \\ &= (1+m\mathbb{Z},\ 1+d+md\mathbb{Z}) \\ &\neq (\alpha \circ \beta)(m\mathbb{Z},\ 1+md\mathbb{Z})\end{aligned}$$

Hence $Aut(T)$ is not an abelian group. □

Next, we discuss the case where a non-abelian group T has an abelian automorphism group. In [9], H. Hilton posed the question: "Can a non-abelian group have an abelian group of automorphisms?"
An affirmative answer to this question was first presented by G. Miller in [18]. The author constructed a non-abelian p-group T with $|T|= 64$, $|Aut(T)|= 2^7$ and $Aut(T)$ abelian.

Definition 3.3.3.
Following [4], we call a non-abelian group with an abelian automorphism group a **Miller group**.

The next theorems present the relationship between automorphisms of a Miller p-group T and the commutator subgroup of T.

Theorem 3.3.4. *[13] Let T be a Miller group, then every automorphism α of T is an identity automorphism on $[T, T]$.*

Definition 3.3.5.
A group T is called **purely non-abelian** if it does not have any non-trivial abelian factors.

Theorem 3.3.6. *[13] Let T be a Miller p-group, then T is purely non-abelian.*

Every finite abelian group has a minimal generating set $\{y_1, y_2, \ldots y_m\}$ such that $\langle y_i\rangle \cap \langle y_j\rangle = \{e_T\}$ for all $i \neq j$. Hopkins[13] discovered that the generating set of a Miller p-group also has this property.

Theorem 3.3.7. *[13] Let T be a Miller p-group, then there exists a generating set $\{y_1, y_2, \ldots y_m\}$ of T such that*

1. *if $p > 2$, then $\langle y_i \rangle \cap \langle y_j \rangle = \{e_T\}$ for all $i \neq j$;*

2. *if $p = 2$, then the order of $\langle y_i \rangle \cap \langle y_j \rangle$ is at most 2 for all $i \neq j$.*

Definition 3.3.8.
A group T is called **special** if $Z(T) = [T, T]$ is abelian.

The next result presents the properties of the direct factors of a Miller p-group.

Theorem 3.3.9. *[3] Let $H \neq \{e\}$ be an abelian group and let K be a purely non-abelian group. Let $T = H \times K$ be a finite p-group. Then T is a Miller group if and only if $p = 2$ and H and K satisfy the following conditions:*

1. *H is cyclic with order $2^n > 2$,*

2. *K is a special Miller 2-group.*

The automorphisms of a Miller p-group form a p-group.

Theorem 3.3.10. *[13] Let T be a Miller p-group, then $Aut(T)$ is a p-group.*

Theorem 3.3.11. *[13] Let T be a Miller group, then the centre of T is non-cyclic.*

The commutator subgroup of a Miller p-group has the following restriction.

Theorem 3.3.12. *Let $p \geq 2$ be a prime number and let T be a Miller p-group. Then the direct product decomposition of $[T, T]$ has at least two cyclic factors of maximum order.*

The next theorem gives the order of the generating set of a Miller p-group, depending on the value of p.

Theorem 3.3.13. *[3] Let T be a Miller p-group.*

1. *If $p = 2$, then T is generated by at least 3 elements.*

2. *If $p > 2$ is a prime, then T is generated by at least 4 elements.*

The smallest Miller p-group has an order equal to 2^6.

Theorem 3.3.14. *Let T be a Miller p-group.*

1. *If $p \geq 2$ is a prime, then $|T| \geq p^6$.*

2. *If p is an odd prime, then $|T| \geq p^7$.*

The first non-abelian group whose automorphism group is abelian was constructed by G. Miller[18]. The author presented this group as:

$$\begin{aligned} G_m &= C_8 \rtimes D_8 \\ &= \langle u, v, w \mid u^8 = v^4 = w^2 = e, wvw^{-1} = v^{-1}, vuv^{-1} = u^5, wuw^{-1} = u \rangle \end{aligned}$$

where C_8 is a cyclic group of order 8 and D_8 is a dihedral group of order 8. (A group R of order n is called a **dihedral group** if it is generated by two elements a, b such that $|a| = n$, $|b| = 2$ and $ba = a^{-1}b$.)

In [16], Macdonald investigated the generalization of G_m[16, see exercise 46, page 237]. For an integer n such that $n \geq 3$, the author presented this generalization by:

$$G_{m,n} = \langle u, v, w \mid u^{2^n} = v^4 = w^2 = e,\ v^{-1}uv = u^{1+2^{n-1}},\ z^{-1}vw = v^{-1},\ wuw^{-1}u^{-1} = e \rangle.$$

He proved that $G_{m,n}$ has order 2^{n+3} and $Aut(G_{mn})$ is a finite abelian group of type $(2^{n-2}, 2, 2, 2, 2, 2, 2)$.

In [4], B. Earnley investigated other non-abelian groups of order 64 to determine which ones have an abelian automorphism group. The author found two more Miller p-groups of order 2^6. Following the notation of authors in [3], we present these groups by:

$$\begin{aligned} G_1 &= (C_4 \rtimes C_4) \rtimes C_4 \\ &= \langle u, v, w \mid vuv^{-1} = u^{-1}, wuw^{-1} = uv^2, wvw^{-1} = v \rangle \end{aligned}$$

and

$$G_2 = (C_4 \times C_4 \times C_2) \rtimes C_2$$
$$= \langle u, v, w, t \mid u^4 = v^4 = w^2 = t^2 = e, uv = vu, uw = wu, vw = wv, txt^{-1} = uv^2, tyt^{-1} = tw \text{ and } t^{-2}wt = w \rangle.$$

These groups have a centre of order 8 and the commutator subgroup of order 4. The automorphism groups of G_1 and G_2 are abelian with order 2^9. The generalization of G_1 and G_2 was investigated by Glasby[7].

In the next chapter we discuss the non-cancellation phenomena of groups of the form $R = T \rtimes_\lambda \mathbb{Z}^k$ where T is a finite non-abelian group. We shall take T to be the Miller 2-group that was presented by Macdonald in [3]. That is, for $n \geq 3$ we assume that;

$$T = \langle u, v, w \mid u^{2^n} = v^4 = w^2 = e,\ v^{-1}uv = u^{1+2^{n-1}},\ z^{-1}vw = v^{-1},\ wuw^{-1}u^{-1} = e \rangle \text{ and}$$
$$Aut(T) = C_{n-2} \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2.$$

Chapter 4

Description of the non-cancellation set through Nielsen equivalence classes

This chapter is a continuation of the work done in Chapter 3. We extend the study of the non-cancellation phenomena in the class of $\mathcal{K}$-group to the study of non-cancellation of groups of the form $R = T \rtimes_\lambda \mathbb{Z}^k$ where T is a Miller p-group.
In the first section we determine the number of Nielsen equivalence classes of epimorphisms $f : \mathbb{Z}^k \to Aut(T)$. The main focus of Section 4.2 is to present results that support the link between the non-cancellation set and Nielsen equivalence classes.

4.1 The set of Nielsen equivalent classes

For this section, we consider T to be a Miller p-group whose automorphism group is a finite abelian group of type $(2^{n-2}, 2, 2, 2, 2, 2, 2)$. We denote $Aut(T)$ by B.
According to P. Witbooi[28], the description of Nielsen equivalence classes depends on the Prüfer rank of the automorphism group of T. The Prüfer rank of a group B, denoted by $r(B)$ is the smallest of the cardinalities of the generating subsets of B.

It is essential to study the computation of the rank of direct products since B is a finite abelian group. This is because the Fundamental Theorem of finite abelian groups states that every finite abelian group can be expressed as a direct product of its cyclic subgroups.

Before compute the rank of B we shall recall some important terminology on the classification of finite abelian groups.

1. For a finite abelian group B we have that $B \cong C_{n_1} \times C_{n_2} \times \ldots \times C_{n_k}$ where $n_i > 2$ for all i and $n_{i+1} \mid n_i$ for $1 \leq i \leq k-1$.

2. If B is a finite abelian group such that $B \cong C_{n_1} \times C_{n_2} \times \ldots \times C_{n_k}$ then the integers $n_1, \ldots, n_k$ are called the invariant factors of B. Also, we say that B is a finite abelian group of type $(n_1, n_2, \ldots, n_k)$ and $|B| = \prod_{i=1}^{k} n_i$.

Proposition 4.1.1. *Let B be a direct product of $\mathbb{Z}_{n_1}, \mathbb{Z}_{n_2}, \ldots, \mathbb{Z}_{n_k}$ where n_i is an integer greater than 1. Let p be a prime divisor of each n_i. If $d_p = |\{i \leq k \ : \ p \mid n_i\}|$ then $r(B) = max\{d_p \ : \ p \ prime\}$.*

In the following example we compute the Prüfer rank of B.

Example 4.1.2. The rank of B.

1. Suppose $B = \mathbb{Z}_6 \times \mathbb{Z}_{50} \times \mathbb{Z}_{45} \times \mathbb{Z}_{54}$, then $d_2 = 3$, $d_3 = 3$ and $d_5 = 2$. Thus, the rank of B is 3.

2. Suppose that B is a finite abelian group of type $(2^{n-2}, 2, 2, 2, 2, 2, 2)$ where $n \geq 3$ is an integer. Applying Proposition 4.1.1 yields $r(B) = d_2 = 7$ since 2 is the only prime divisor of the invariant factors.

Let B be the automorphism group of T and let m be the number of prime divisors of $|Aut(T)|$. Theorem 3.1.4 states that $r(B)$ is less than or equal to m^2. We provide the following result to compute the number of prime divisors of $|B|$.

Lemma 4.1.3. *Let $B \cong C_{2^{n-2}} \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2$, then $m = n + 4$.*

Proof. Let $B \cong C_{2^{n-2}} \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2$. The order of B is equal to the product of its invariant factors, hence $|B| = 2^{n+4}$. From the definition of m, it follows that $m = n + 4$. □

We recall the following definitions and notation from the previous chapter:

1. Two epimorphisms $f, g : \mathbb{Z}^k \to B$ are said to be in Nielsen equivalent if there exists an automorphism α of $\mathbb{Z}^k$ such that $f = g \circ \alpha$.

2. We denote the set of all Nielsen equivalent epimorphisms by $RE_k^{\sim n}(B)$.

3. Let $b = (b_1, \ldots, b_k)$ be a good ordered k-tuple of elements of B and let n be an integer. We define $f_n : \mathbb{Z}^k \to B$ by:

$$f_n(e_j) = \begin{cases} b_j & \text{if } j < k \\ nb_k & \text{if } j = k \end{cases}$$

where $e_1, \ldots, e_k$ is the standard basis of $\mathbb{Z}^k$.

Let $B \cong C_{2^{n-2}} \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2$ and let $b = (b_1, \ldots, b_k)$ be a good ordered k-tuple of elements of B. Let d be the order of b_k. The maximum order of elements of $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \ldots \times \mathbb{Z}_{n_j}$ is equal to $lcm(n_1, n_2, \ldots, n_j)$. Thus, we redefine d to be the lowest common multiple of the invariant factors of B.
Theorem 3.1.15 states that for integers s and t, two epimorphisms $f_s, f_t : \mathbb{Z}^k \to B$ are Nielsen equivalent if s and t are coprime with d and $t = \pm s \ mod \ d$. Motivated by this result we want to compute the following for the abelian group B:

1. The lowest common multiple of the invariant factors of B.

2. Integers s and t such that $(s, d) = (t, d) = 1$ and $t = \pm s \ mod \ d$.

3. The number of Nielsen equivalence classes.

To compute d, we first have to determine the order of each b_i.

Lemma 4.1.4. *Let $B \cong C_{2^{n-2}} \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2$ and let $b = (\beta_1, \beta_2, \ldots, \beta_7)$ be an element of B. Then $\beta_1 \in \{0, 1, 2, \ldots, 2^{n-2} - 1\}$ and $\beta_i \in \{0, 1\}$ for $2 \leq i \leq 7$. Furthermore, $o(\beta_1) = \dfrac{2^{n-2}}{gcd(\beta_1, 2^{n-2})}$ in $C_{2^{n-2}}$ and $o(0) = 1$, $o(1) = 2$ in C_2.*

Proof. Let $B \cong C_{2^{n-2}} \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2$ and let $(\beta_1, \beta_2, \beta_3, \beta_4, \beta_5, \beta_6, \beta_7) \in B$. Then $\beta_1 \in \{0, 1, 2, \ldots, 2^{n-2} - 1\}$ and $\beta_i \in \{0, 1\}$ for $2 \leq i \leq 7$.
For any integer n such that β_i is an element of $\mathbb{Z}_n$ we have that $o(\beta_i) = \dfrac{|\mathbb{Z}_n|}{gcd(\beta_i, |\mathbb{Z}_n|)}$. Thus, it follows that $o(\beta_1) = \dfrac{2^{n-2}}{gcd(\beta_1, 2^{n-2})}$ in $C_{2^{n-2}}$. In $\mathbb{Z}_2$ we have that $o(1) = \dfrac{2}{gcd(1,2)} = 2$ and $o(0) = 1$ since 0 is an identity in $\mathbb{Z}_2$. □

In the next example, we calculate d for various values of n and then we determine the relationship between d and the number of Nielsen equivalence classes.

Example 4.1.5. The lowest common multiple of the invariant factors of B.

1. If $n = 3$, then $B \cong C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2$. Thus, the lowest common multiple of the invariant factors of B is 2.

2. If $n = 4$ then B is a finite abelian group of type $(4, 2, 2, 2, 2, 2, 2)$. Hence, $d = 4$.

3. If $n = 5$ then the invariant factors of B are $8, 2, 2, 2, 2, 2$ and 2. Hence, $d = 8$.

Proposition 4.1.6. *If B is a finite abelian group of type $(2^{n-2}, 2, 2, 2, 2, 2, 2)$, then $d = 2^{n-2}$.*

Proof. Let $B \cong C_{2^{n-2}} \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2$. The invariant factors of B are powers of 2, hence the lowest common multiple of the invariant factors is equal 2^{n-2}. □

In the following examples we compute pairs of integers s and t such that $(s, d) = (t, d) = 1$ and $t \equiv \pm s \ mod \ d$.

Example 4.1.7.
Let $d = 4$, then $s,\ t \in \{1, 3\}$ since $(1, 4) = (3, 4) = 1$. Also $3 \equiv -1 \ mod \ 4$ and $1 \equiv -3 \ mod \ 4$, hence $f_1 \sim_n f_3$. Thus, we have one Nielsen equivalence class.

Example 4.1.8.
Let $d = 16$, then we have that $s, t \in \{1, 3, 5, 7, 9, 11, 13, 15\}$ and $15 \equiv -1 \ mod \ 16$, $13 \equiv -3 \ mod \ 16$, $11 \equiv -5 \ mod \ 16$ and $9 \equiv -7 \ mod \ 16$. So $f_1 \sim_n f_{15}$, $f_3 \sim_n f_{13}$, $f_5 \sim_n f_{11}$ and $f_7 \sim_n f_9$. Thus, we have four Nielsen equivalence classes.

Motivated by the examples above, we propose the following results about the number of Nielsen equivalence classes.

Lemma 4.1.9. *Let T be a Miller 2-group and let $B \cong C_4 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2$ be a finite abelian group. Then $d = 4$ and the number of Nielsen equivalence classes is equal to* 1.

Proof. Let $B \cong C_4 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2$. Then $|B| = 2^8$ and B has 1 element of order 1, 127 elements of order 2 and 128 elements of order 4. Hence, $d = 4$ and $f_1 \sim_n f_3$ since $(1,4) = (3,4) = 1$ and $3 \equiv -1 \ mod\ 4$. So there is only one Nielsen equivalence class. □

Lemma 4.1.10. *For a Miller p-groups T, let $B \cong C_{16} \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2$. Then $d = 16$ and $|RE_k^{\sim_n}(B)| = 4$.*

Proof. Let T be a Miller p-group and let $B \cong C_{16} \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2$. Then $|B| = 2^9$ and elements of B have orders 1, 2, 4, 8 and 16. By Lemma 3.1.15 we have the following pairs of Nielsen equivalent epimorphisms: (f_1, f_{15}), (f_3, f_{13}), (f_5, f_{11}) and (f_7, f_9). Hence, there are 4 Nielsen equivalence classes. □

Next, we compute the number of Nielsen equivalence classes for $d = 2^{n-2}$.

Proposition 4.1.11. *Let T be a Miller p-group and let $B \cong C_{2^{n-2}} \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2$. Then $d = 2^{n-2}$ and $|RE_k^{\sim_n}(B)| = 2^{n-4}$.*

Proof. Let $B = Aut(T)$ be a finite abelian group of type $(2^{n-2}, 2, 2, 2, 2, 2, 2)$, then by Proposition 4.1.6 we have that $d = 2^{n-2}$.

Let $s, t \in \mathbb{Z}^+$ such that $(t, d) = (s, d) = 1$ and $t \equiv \pm s \ mod\ d$, then $f_t \sim_n f_s$. By definition of the Euler-Phi function we have that the number of integers in $\{1, 2, \ldots, d-1\}$ which are relatively prime to d is equal to $\phi(d)$. Hence, $|RE_k^{\sim_n}(B)| = \dfrac{\phi(d)}{2}$ since any $f_t \in RE_k^{\sim_n}(B)$ is Nielsen equivalent to some $f_s \in RE_k^{\sim_n}(B)$. Finally, $|RE_k^{\sim_n}(B)| = 2^{n-4}$ since

$$\begin{aligned} \phi(d) &= \phi(2^{n-2}) \\ &= 2^{n-3} \end{aligned}$$

□

Our next task is to discuss the Nielsen equivalence classes of a Miller p-group, where p is a prime number greater than 2.

Proposition 4.1.12. *Let T be a Miller p-group and let $B = Aut(T)$ be a finite abelian group of type $(p^\alpha, p, p, \ldots, p)$. Then the following statements hold:*

1. *The lowest common multiple of invariant factors of B is $d = p^\alpha$.*
2. *The number of Nielsen equivalence classes is $|RE_k^{\sim_n}(B)| = \dfrac{p^{\alpha-1}(p-1)}{2}$.*

Proof.

1. Let T be a Miller p-group and let B be a finite abelian group of type $(p^\alpha, p, p, \ldots, p)$. Then invariant factors of B are $p^\alpha, p, p, \ldots$ and p, which implies that the lowest common multiple of these factors is p^α. Hence, $d = p^\alpha$.

2. Let t and s be positive integers such that $(t, d) = (s, d) = 1$ and $s \equiv \pm t \ mod \ d$. Then $f_s \sim_n f_t$. So,

$$\begin{aligned} |RE_k^{\sim_n}(B)| &= \frac{\phi(d)}{2} \\ &= \frac{p^{\alpha-1}(p-1)}{2} \end{aligned}$$

□

The above result provides a relationship between the lowest common multiple of invariant factors of B and the number of Nielsen equivalence classes. We will prove that the set of Nielsen equivalence classes is a group.

Proposition 4.1.13. *Let T be a Miller p-group. Define the binary operation $*$ on the set of Nielsen equivalence classes by $[f_t] * [f_s] = [f_{ts}]$. Then $RE_k^{\sim_n}(B)$ is a group under $*$.*

Proof. Let T be a Miller p-group and let $B = Aut(T)$. Suppose that s and t are integers which are relatively prime to d and let $t \equiv \pm s \ mod \ d$.

We first show that $*$ is a well-defined binary operation. By definition of t and s it follows that $(ts, d) = 1$ and $ts \equiv \pm k \ mod \ d$ for some $k \in \mathbb{Z}_d^*$. Hence, $*$ is well-defined since $[f_{ts}] \in RE_k^{\sim_n}(B)$. This also implies that the set of Nielsen equivalence classes is closed under $*$.

The identity element of $RE_k^{\sim_n}(B)$ is f_1 since $[f_t] * [f_1] = [f_1] * [f_t] = [f_t]$. Every element in $\mathbb{Z}_d^*$ has an inverse, so for each $f_t \in RE_k^{\sim_n}(B)$ there exists an epimorphism f_s such that $[f_t] * [f_s] = [f_s] * [f_t] = [f_1]$.

Hence $RE_k^{\sim_n}(B)$ is a group. □

In the following example we explore some properties of elements of the group $RE_k^{\sim_n}(B)$.

Example 4.1.14.

1. Let $n = 5$ and let $d = 8$. Then we have the following:

$$f_1 \sim_n f_7 \ and \ f_3 \sim_n f_5.$$

Consider a set $\{[f_1], [f_3]\}$, then every element of this set can be expressed as a power of $[f_3]$ since $3^2 \equiv 1 \ mod \ 8$. We have that

$$\begin{aligned} [f_3]^2 &= [f_3] * [f_3] \\ &= [f_1]. \end{aligned}$$

We also have that

$$\begin{aligned} [f_3]^3 &= [f_{27}] \\ &= [f_3] \ since \ 3^3 \equiv 3 \ mod \ 8. \end{aligned}$$

2. If $n = 6$, then $d = 16$. Following Example 4.1.8, we have the following pairs of Nielsen equivalent epimorphisms: (f_1, f_{15}), (f_3, f_{13}), (f_5, f_{11}) and (f_7, f_9).

Hence, $RE_k^{\sim_n}(B) = \Big\{[f_1], [f_3], [f_5], [f_7]\Big\}$.

We also observe the following:

$[f_3]^2 = [f_9] = [f_7]$, $[f_3]^3 = [f_{11}] = [f_5]$, $[f_3]^4 = [f_1]$ and $[f_3]^5 = [f_{243}] = [f_3]$.

Hence, we conclude that every element in $\Big\{[f_1], [f_3], [f_5], [f_7]\Big\}$ can be expressed as powers of $[f_3]$. That is, for any positive integer α, we have that $([f_3])^\alpha$ is always in $RE_k^{\sim_n}(B)$.

The above computation prompted us to investigate whether or not $RE_k^{\sim_n}(B)$ is a cyclic group. We propose the following results.

Proposition 4.1.15. *If B is a finite abelian group of type $(2^4, 2, 2, 2, 2, 2, 2)$, then $RE_k^{\sim_n}(B)$ is a cyclic group.*

Proof. Let B be a finite abelian group of type $(2^4, 2, 2, 2, 2, 2, 2)$. It follows from Example 4.1.7 that we have one Nielsen equivalence class. That is $f_1 \sim_n f_3$. Thus, $RE_k^{\sim_n}(B)$ is cyclic since it has order 1. □

For a case whereby B is a finite abelian group of type $(2^{16}, 2, 2, 2, 2, 2, 2)$, we shall prove that $RE_k^{\sim_n}(B)$ is a cyclic of order 4.

Proposition 4.1.16. *If B is a finite abelian group of type $(2^{16}, 2, 2, 2, 2, 2, 2)$, then the set Nielsen equivalence classes is a cyclic group of order 4.*

Proof. Consider the set $\Big\{[f_1], [f_3], [f_5], [f_7]\Big\}$. We first establish an isomorphism between this set and $\mathbb{Z}_4$.

In $\{[f_1], [f_3], [f_5], [f_7]\}$ we have the following:

$$\begin{aligned}
[f_1]^1 &= [f_1] \implies o([f_1]) = 1 \\
[f_3]^4 &= [f_1] \implies o([f_3]) = 4 \\
[f_5]^4 &= [f_1] \implies o([f_5]) = 4 \\
[f_7]^2 &= [f_1] \implies o([f_7]) = 2.
\end{aligned}$$

We show that $RE_k^{\sim n}(B)$ is isomorphic to $\mathbb{Z}_4$. In $\mathbb{Z}_4$, we have that $o(0) = 1$, $o(1) = 4$, $o(2) = 2$ and $o(3) = 4$.

The set $\{[f_1], [f_3], [f_5], [f_7]\}$ has one element of order 1, one element of order 2 and two elements of order 4. We note that the elements of $\mathbb{Z}_4$ also have same orders. That is, in $\mathbb{Z}_4$ there is one element of order 1, one element of order 2 and two elements of order 4.

Thus, we have an isomorphism $\alpha : \{[f_1], [f_3], [f_5], [f_7]\} \to \mathbb{Z}_4$ defined by:

$$\alpha([f_1]) = 0,\ \alpha([f_3]) = 1,\ \alpha([f_5]) = 3,\ \textit{and}\ \alpha([f_7]) = 2.$$

Hence, $\{[f_1], [f_3], [f_5], [f_7]\}$ is cyclic as $\mathbb{Z}_4$.

Also;

$$[f_3]^2 = [f_7],\ [f_3]^3 = [f_5],\ [f_5]^2 = [f_7]\ \textit{and}\ [f_5]^3 = [f_3].$$

The elements of $\{[f_1], [f_3], [f_5], [f_7]\}$ can be expressed as powers $[f_3]$ and $[f_5]$ and $o([f_3]) = o([f_5]) = \Big|\{[f_1], [f_3], [f_5], [f_7]\}\Big|$. Hence, $[f_3]$ and $[f_5]$ are generators of $\{[f_1], [f_3], [f_5], [f_7]\}$. $\square$

4.2 A link between the non-cancellation set and the set of Nielsen equivalence classes

Let $R = T \rtimes_\lambda \mathbb{Z}^k$ and let $B = Aut(T)$ where T is a Miller p-group. In the previous section we computed the following for a finite abelian group B: the rank, number of prime divisors of $|B|$, the lowest common multiple of invariant factors of B and the number of Nielsen equivalence classes. We also proved that the set of all Nielsen equivalence classes is a cyclic group. The focus of this section is to use these computations to describe the non-cancellation set of R through the Nielsen equivalence classes. That is, we want to establish an isomorphism between $\chi(R)$ and $RE_k^{\sim_n}(B)$.

Consider a Miller group T and let d be the lowest common multiple of the invariant factors of B. In the previous section we computed the elements of the set of Nielsen equivalence classes. Recall that two epimorphisms f_t and f_s are in the same Nielsen equivalence class if s and t are integers such that $t \equiv \pm s \ mod \ d$. This results in $\dfrac{\phi(d)}{2}$ Nielsen equivalence classes in each $RE_k^{\sim_n}(B)$, where $\phi(d)$ is the number of elements in the set of $\{1, 2, \ldots, d-1\}$ that are relatively prime to d.

We shall begin by comparing $RE_k^{\sim_n}(B)$ with $\mathbb{Z}_d^*/\{1, -1\}$. Before we give the relationship between these two groups, we shall compute the elements of $\mathbb{Z}_d^*/\{1, \ -1\}$ for various values of d. We will then use the structure of $\mathbb{Z}_d^*/\{1, \ -1\}$ to explain the relationship between $\mathbb{Z}_d^*/\{1, \ -1\}$ and $RE_k^{\sim_n}(B)$.

Example 4.2.1.
Let T be a Miller 2-group and let B be a finite abelian group of type $(2^{n-2}, 2, 2, 2, 2, 2, 2)$ where $n \geq 3$.

1. If $n = 4$, then $d = 4$. Thus,

$$\begin{aligned}\mathbb{Z}_4^*/\{1,\ -1\} &= \{a\{1,\ -1\} \mid a \in \mathbb{Z}_4^*\} \\ &= \{\{1,\ -1\}, \{3,\ -3\}\} \\ &= \{\{1,\ 3\}\}\end{aligned}$$

2. Let $d = 16$, then

$$\begin{aligned}\mathbb{Z}_{16}^*/\{1,\ -1\} &= \{a\{1,\ -1\} \mid a \in \mathbb{Z}_{16}^*\} \\ &= \{\{1,\ -1\}, \{3,\ -3\}, \{5,\ -5\}, \{7,\ -7\}, \{9,\ -9\}, \{11,\ -11\}, \{13,\ -13\}, \{15,\ -15\}\} \\ &= \{\{1,\ 15\}, \{3,\ 13\}, \{5,\ 11\}, \{7,\ 9\}, \{9,\ 7\}, \{11,\ 5\}, \{13,\ 3\}, \{15,\ 1\}\} \\ &= \{\{1,\ 15\}, \{3,\ 13\}, \{5,\ 11\}, \{7,\ 9\}\}.\end{aligned}$$

From the previous section we know that if $d = 4$, then we have one pair of Nielsen equivalence epimorphisms, (f_1, f_3). We note from the example above that $\{1, 3\} \in \mathbb{Z}_4^*/\{1,\ -1\}$. Also, if $d = 16$ then $\mathbb{Z}_{16}^*/\{1,\ -1\} = \{\{1,\ 15\}, \{3,\ 13\}, \{5,\ 11\}, \{7,\ 9\}\}$ and we have the following pairs of Nielsen equivalence epimorphisms: (f_1, f_{15}), (f_3, f_{13}), (f_5, f_{11}) and (f_7, f_9). We observe that the elements of $\mathbb{Z}_d^*/\{1,\ -1\}$ correspond with the elements of $RE_k^{\sim n}(B)$. That is for every $\{t, s\}$ in $\mathbb{Z}_d^*/\{1,\ -1\}$ we have a corresponding pair of (f_t, f_s) of Nielsen equivalent epimorphisms in $RE_k^{\sim n}(B)$. Thus, we give the following result.

Proposition 4.2.2. *Let B be a finite abelian group and let d be the lowest common multiple of the invariant factors of B. Then the function which sends an element $n \in \mathbb{Z}_d^*$ to f_n induces an epimorphism $\theta : \mathbb{Z}_d^* \to RE_k^{\sim n}(B)$. Furthermore, $Ker(\theta) = \{1, -1\}$ and $\mathbb{Z}_d^*/\{1,\ -1\}$ is isomorphic to $RE_k^{\sim n}(B)$.*

Proof. Let $\theta : \mathbb{Z}_d^* \to RE_k^{\sim n}(B)$ be defined by $\theta(t) = [f_t]$. We apply the definition of Nielsen equivalent epimorphisms to show that θ is well-defined. The definition states that if s and t are integers such that $(t, d) = (s, d) = 1$ and $t \equiv \pm s \ mod\ d$, then f_t is Nielsen equivalent to f_s, [see Lemma 3.1.15].

Suppose that $t \equiv s \ mod \ d$, then if follows from Lemma 3.1.15 that $f_t \sim_n f_s$. Thus, θ is well-defined.

The mapping $\theta : \mathbb{Z}_d^* \to RE_k^{\sim_n}(B)$ is onto since for every Nielsen equivalence class $[f_t]$ in $RE_k^{\sim_n}(B)$ there exists an element t of $\mathbb{Z}_d^*$.

The identity element of $\mathbb{Z}_d^*$ is 1 and the identity element of $RE_k^{\sim_n}(B)$ is $[f_1]$. Thus, $Ker(\theta) = \{t \in \mathbb{Z}_d^* \mid \theta(t) = [f_1]\}$.

By the definition of θ, we have that $\theta(1) = [f_1]$. Hence, $1 \in Ker(\theta)$.

Also,

$$\begin{aligned} 1 &\equiv d+1 \ mod \ d \\ &\equiv -(d-1) \ mod \ d. \end{aligned}$$

Following the definition of Nielsen equivalent epimorphisms we have that $[f_1] = [f_{d-1}]$. Thus, $[f_1] = [f_{-1}]$ since $-1 \equiv (d-1) \ mod \ d$. This implies that -1 is also in $Ker(\theta)$ since $\theta(-1) = [f_1]$.

Hence, $Ker(\theta) = \{1, -1\}$.

We have established that $\theta : \mathbb{Z}_d^* \to RE_k^{\sim_n}(B)$ is onto and $Ker(\theta) = \{1, -1\}$. We recall that the First Isomorphism Theorem states that for a homomorphism $\theta : R \to Q$ such that $Ker(\theta) = K$, we have that$R/K \cong Q$. Thus, by $\mathbb{Z}_d^*/\{1, -1\} \cong RE_k^{\sim_n}(B)$. □

Our interest is to establish an isomorphism $\theta : RE_k^{\sim_n}(B) \to \chi(R)$. To achieve that, we will show that there is a relationship between $\chi(R)$ and $\mathbb{Z}_d^*/\{1, -1\}$ and use this relationship to prove that $\chi(R) \cong RE_k^{\sim_n}(B)$.

For an abelian group T, this relation has already been studied in [22]. The authors presented a condition under which $\chi(R) \cong \mathbb{Z}_d^*/\{1, -1\}$.

Theorem 4.2.3. *[22, 3.8] Let T be a finite abelian group and let $R = T \rtimes_\lambda \mathbb{Z}^k$ be a $\mathcal{K}$-group such that the image $Im(\lambda)$ of λ belongs to the centre of $Aut(T)$.*

1. *If $k > rank(Im(\lambda)$, then the non-cancellation set is trivial.*

2. *If $k = rank(Im(\lambda))$, then $\chi(R) \cong \mathbb{Z}_d^*/\{1, -1\}$ where d is the least positive integer n such that the rank of $nIm(\lambda)$ is strictly less that the rank of $Im(\lambda)$.*

We note that the above result is restricted by the condition that T is a finite abelian group. We shall investigate the relationship between $\chi(R)$ and $\mathbb{Z}_d^*/\{1, -1\}$ when T is a Miller p-group. Our work focuses on the non-cancellation set $\chi(R)$ when T is not necessarily abelian.

Proposition 4.2.4. *Let T be a Miller p-group and let R be a semi-direct product of the form $R = T \rtimes_\lambda \mathbb{Z}^k$. If d is the lowest common multiple of orders of the invariant factors of $Aut(T)$, then $\psi : \mathbb{Z}_d^* \to \chi(R)$ is surjective and $\chi(R) \cong \mathbb{Z}_d^*/\{1, -1\}$.*

Proof. Let T be a Miller-p group let $H_t = T \rtimes_{f_t} \mathbb{Z}^k$ where $f_t : \mathbb{Z}^k \to Aut(T)$ is an epimorphism. Let $[H_t]$ denote the isomorphism class of H_t, we define $\chi(H_t)$ to be the set of all isomorphism classes of groups Q such that $Q \times \mathbb{Z} \cong H_t \times \mathbb{Z}$.
Let the mapping $\psi : \mathbb{Z}_d^* \to \chi(H_t)$ be defined by $t \mapsto [H_t]$. We begin by showing that $\psi : \mathbb{Z}_d^* \to \chi(H_t)$ is a well defined map, that is, for $s, t \in \mathbb{Z}_d^*$ then $t \equiv s \ mod \ d \implies \psi(t) = \psi(s)$.

If $t, s \in \mathbb{Z}_d^*$ such that $t \equiv s \ mod \ d$ then it follows by the definition of Nielsen equivalent epimorphisms that $[f_t] = [f_s]$.
We recall that two epimorphisms f_t and f_s are said to be Nielsen equivalent if $f_t = f_s \circ h$ for some automorphism h of $\mathbb{Z}^k$. Thus, we have that $T \rtimes_{f_t} \mathbb{Z}^k \cong T \rtimes_{f_s \circ h} \mathbb{Z}^k$.
Also, Lemma 3.2.9 states that for groups N and H and a homomorphism $\rho : H \to Aut(N)$, if $h \in Aut(H)$, then the groups $N \rtimes_\rho H$ and $N \rtimes_{\rho \circ h} H$ are isomorphic. This gives $T \rtimes_{f_s} \mathbb{Z}^k \cong T \rtimes_{f_s \circ h} \mathbb{Z}^k$.
We then conclude that $T \rtimes_{f_t} \mathbb{Z}^k \cong T \rtimes_{f_s} \mathbb{Z}^k$, which implies that $[H_t] = [H_s]$. Hence, ψ is a well defined function.
The function ψ is onto since for every $[H_t] \in \chi(H_t)$ there is a corresponding $t \in \mathbb{Z}_d^*$.

Next, we compute the kernel $ker(\psi) = \{t \in \mathbb{Z}_d^* \mid \psi(t) = [H_1]\}$.

Clearly $1 \in Ker(\psi)$ since $1 \mapsto [H_1]$. Also, f_t is Nielsen equivalent to f_s if $t \equiv \pm s$. Hence,

$$\begin{aligned} 1 &\equiv -d+1 \ mod\ d \\ &\equiv -(d-1) \ mod\ d. \end{aligned}$$

Thus, $[f_1] = [f_{d-1}]$ which implies that $[f_1] = [f_{-1}]$ since $-1 \equiv (d-1) \ mod\ d$. Since f_1 and f_{-1} are Nielsen equivalent we have that $f_1 = f_{-1} \circ h$ for some $h \in Aut(\mathbb{Z}^k)$. Thus, $T \rtimes_{f_1} \mathbb{Z}^k \cong T \rtimes_{f_{-1}\circ h} \mathbb{Z}^k$ and $T \rtimes_{f_{-1}} \mathbb{Z}^k \cong T \rtimes_{f_{-1}\circ h} \mathbb{Z}^k$. This implies that $[H_1] = [H_{-1}]$ and $-1 \mapsto [H_1]$.
Hence, $-1 \in Ker(\psi)$.

The function $\psi : \mathbb{Z}_d^* \to \chi(R)$ is onto and $Ker(\psi) = \{1, -1\}$. Thus, by the First Isomorphism Theorem it follows that $\mathbb{Z}_d^*/\{1, -1\} \cong \chi(R)$.

□

We give the following result.

Theorem 4.2.5. *Let $R = T \rtimes_\lambda \mathbb{Z}^k$ where $w : \mathbb{Z}^k \to Aut(T)$ is a group action. Denote $Aut(T)$ by B and let d be the lowest common multiple of invariant factors of B. Then $RE_k^{\sim n}(B) \cong \chi(R)$.*

Proof. Let $Aut(T) = B$ be a finite abelian group. Let $b = (a_1, \ldots, a_k)$ be a good ordered k-tuple of elements of B. It follows by Proposition 4.2.2 and Lemma 4.2.4 that $\mathbb{Z}_d^*/\{1, -1\} \cong RE_k^{\sim n}(B)$ and $\chi(R) \cong \mathbb{Z}_d^*/\{1, -1\}$. Thus, $\chi(R) \cong RE_k^{\sim n}(B)$. □

The following proposition presents a result on the order of the non-cancellation set of $R = T \rtimes_\lambda \mathbb{Z}_k$ when the automorphism group of T is a finite abelian group of type $(2^{n-2}, 2, 2, 2, 2, 2, 2)$.

Proposition 4.2.6. *Let T be a Miller 2-group and let $B \cong C_{2^{n-2}} \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2$.*

1. *If $n = 4$, then the non-cancellation set is trivial.*
2. *If $n > 4$, then $|\chi(R)| = \dfrac{\phi(d)}{2}$.*

Proof.

1. Suppose that $n = 4$, then $|\chi(R)| = 1$. This implies that the non-cancellation set is trivial.

2. Suppose that $n > 4$, and let d be the lowest common multiple of invariant factors of B. By Proposition 4.2.5 we have that $RE_k^{\sim n}(B) \cong \chi(R)$. Thus, it follows by Proposition 4.1.11 that the order of $\chi(R)$ is equalt to $\dfrac{\phi(d)}{2}$.

□

Chapter 5

Conclusion and further work

Let $R = T \rtimes_\lambda \mathbb{Z}^k$ T, where $\lambda : \mathbb{Z}^k \to Aut(T)$ is a group action. Various authors have studied the non-cancellation set of R when T is a finite abelian group([22], [26], [28] and [29]). The basis of this work is to extend the study of the non-cancellation set to groups of the form $R = T \rtimes_\lambda \mathbb{Z}^k$, where T is a finite group but not necessarily abelian.

In [22] and [28], the authors described a group structure on the non-cancellation set of R using the Nielsen equivalence classes of epimorphisms from a finite rank free abelian group onto a finite abelian group. We discuss the non-cancellation phenomena in the class of $\mathcal{K}$-groups in Section 3.2. According to Witbooi's result [Theorem 3.2.4], two groups $R = T \rtimes_\lambda \mathbb{Z}^k$ and $Q = T \rtimes_v \mathbb{Z}^k$ are isomorphic if and only if there exist automorphisms $f : T \to T$ and $h : \mathbb{Z}^k \to \mathbb{Z}^k$ such that the following identity holds for every $t \in T$ and every $z \in \mathbb{Z}^k$,

$$[f \circ \lambda(z)](t) = [v(h(z))](f(t)).$$

The authors show that R and H are in the same non-cancellation class if $Im(\lambda)$ and $Im(v)$ are conjugate in $Aut(T)$. We made the following contributions:

- We give a link between the Nielsen equivalence classes and the congugacy classes of subgroups of $Aut(T)$ in Proposition 3.2.10. We showed that if the two images $Im(\lambda)$ and $Im(v)$ are conjugate in $Aut(T)$ then λ is Nielsen equivalent to v.

In Section 3.2, the non-cancellation set is described through congugacy classes of subgroups of $Aut(T)$. Witbooi's result in [22] states that $Q \times \mathbb{Z} \cong G \times \mathbb{Z}$ if and only if

$\lambda(\mathbb{Z}^k) = \alpha^{-1}v(\mathbb{Z}^k)\alpha$ for some $\alpha \in Aut(T)$, [see Theorem 3.2.14]. Recall that for any homomorphism $\lambda : \mathbb{Z}^k \to Aut(T)$, the image $Im(\lambda)$ of λ is subgroup of $Aut(T)$. This prompted us to investigate subgroups of $Aut(T)$ in Section 2.12.

Conjugate subgroups are represented by one isomorphism class in the non-cancellation set. Thus, if all subgroups of $Aut(T)$ are conjugate to each other, then the non-cancellation set is trivial since it has only one isomorphism class. If $Aut(T)$ has other subgroups which do not have conjugates, then the non-cancellation set is not trivial since these subgroups form distinct isomorphism classes.

Our interest is to discuss the case where the non-cancellation $\chi(R)$ is non-trivial. This condition is met if there is at least one subgroup of $Aut(T)$ which does not have any conjugate other than itself in $Aut(T)$, that is if at least one subgroup of $Aut(T)$ is normal. Suppose that $Im(\lambda)$ is normal and $Im(v) = \alpha^{-1}Im(u)\alpha$, then $T \rtimes_\lambda \mathbb{Z}^k$ is not in the same non-cancellation set as $T \rtimes_v \mathbb{Z}^k$ and $T \rtimes_u \mathbb{Z}^k$.

Another case that can result distinct isomorphism classes is when all subgroups of $Aut(T)$ are normal. To explore this case, we answer the question "What condition(s) should a group satisfy to ensure that all its subgroups are normal?"
All subgroups of an abelian group are normal. Hence, we conclude that if $Aut(T)$ is an abelian group, then the non-cancellation set of R is not trivial. We then investigate various cases of T which result in $Aut(T)$ being abelian.

For an abelian group T, we look at the case where T is cyclic and the case where T is not cyclic. A non-abelian group with an abelian automorphism group is called a Miller group. In Section 3.3, we discussed the structure and the properties of Miller groups. We have that the non-cancellation set of $R = T \rtimes_\lambda \mathbb{Z}^k$ is non-trivial if T is a cyclic group or T is a Miller-p group.

We go on to study the non-cancellation of $R = T \rtimes_\lambda \mathbb{Z}^k$ when T is a finite non-abelian group.

Consider the automorphism group of T to be a finite abelian group of type $(2^{n-2}, 2, 2, 2, 2, 2, 2)$ and denote the lowest common multiple of the invariant factors of B by d. In Section 4.1 we constructed set of Nielsen equivalence classes for various values of $n \geq 3$.

We began by computing the various values of d. We then establish a relationship between d and $n \geq 3$ in Proposition 4.1.6 which states that if B is a finite abelian group of type $(2^{n-2}, 2, 2, 2, 2, 2, 2)$, then $d = 2^{n-2}$.

According to Lemma 3.1.15, two epimorphisms f_t and f_s are Nielsen equivalent if s and t are integers such that $(s, d) = (t, d) = 1$ and $t \equiv \pm s \ mod \ d$. We used the different values of d that we computed to determine integers s and t that satisfy these conditions. That is we identified various pairs of Nielsen equivalent epimorphisms for each d, hence determining the order of $RE_k^{\sim n}(B)$.

We made the following contributions:

- In Proposition 4.1.11 we showed that $|RE_k^{\sim n}(B)| = \dfrac{\phi(d)}{2}$.
- We then generalized this result to discuss the order of the set $RE_k^{\sim n}(B)$ when T is a Miller-p group for any prime number p such that $p > 2$.

For a finite abelian group $B = Aut(T)$, we define a binary operation $*$ on $RE_k^{\sim n}(B)$ by $[f_t] * [f_s] = [f_{ts}]$. In Proposition 4.1.13 we proved that $RE_k^{\sim n}(B)$ is a group under $*$. Using the binary operation $*$, we explored some properties of elements of $RE_k^{\sim n}(B)$. We then made the following contribution:

- We showed in Proposition 4.1.16 that $RE_k^{\sim n}(B)$ is a cyclic group. For a finite abelian group B of type $(2^{16}, 2, 2, 2, 2, 2, 2)$ we showed that $RE_k^{\sim n}(B)$ is a cyclic group of order 4. Thus, $RE_k^{\sim n}(B) \cong \mathbb{Z}_4$.

We established an isomorphism $\theta : \chi(R) \to RE_k^{\sim_n}(B)$ and made the following contribution:

- In Proposition 4.2.2 we constructed a surjection $\theta : \mathbb{Z}_d^* \to RE_k^{\sim_n}(B)$. We also established that $\mathbb{Z}_d^*/Ker(\theta) \cong RE_k^{\sim_n}(B)$.
- We proved in Proposition 4.2.5 that $\chi(R) \cong RE_k^{\sim_n}(B)$.

For further work we would refer to the work done by P. Witbooi in [28] where he defined an abelian group structure on the non-cancellations set. Following the author's notation, for a group $R = T \rtimes_\lambda \mathbb{Z}^k$, let n_1 be the exponent of T, let n_2 be the exponent of the group $Aut(T)$, and let n_3 be the exponent of the torsion subgroup of the centre of R. The author defined the natural number $n(R) = n_1 n_2 n_3$. He presented a result which states that the function $\theta : \mathbb{Z}_n^*/\{1, -1\} \to \chi(R)$ induces a group structure on the non-cancellation set. It would be interesting to investigate if there is a relationship between the natural number n and the lowest common multiple of the invariant factors of $B = Aut(T)$ where T is a Miller group.

Bibliography

[1] https://en.wikipedia.org/wiki/Rank_of_a_group

[2] J. Curran, R. Heffernan and D. Machale, *On the order of the Automorphism group of a finite group*, Comm. in Algebra **39**(10), (2011), 3616-3624.

[3] R. Dattatraya and M. Yadav, *Finite groups with abelian automorphism groups: A survey*, Group Theory and Computation, (2018), 119-140.

[4] B. E. Earnley, *On finite groups whose group of automorphisms is abelian* Ph.D. Thesis, Wayne State University, (1975).

[5] J. B. Fraleigh, *First Course In Abstract Algebra*, Seventh edition, Boston: Pearson Education, (2003).

[6] A. Fransman, *Non-cancellation sets of direct powers of certain metacyclic groups*, Kyungpook Math. J. **41** (2001), 191-197.

[7] S. P. Glasby, *2-groups with every automorphisms central*, J. Austral. Math. Soc. (Series A), **41** (1986), 233-236.

[8] C. J. Hillar and D. L. Rhea, *Automorphisms of finite abelian groups*, The Amer. Math. Monthly, **114**(10) (2007), 917-923.

[9] H. Hilton, *An Introduction to the theory of groups of finite order*, Oxford at the Clarendon Press, (1908).

[10] P. Hilton and G. Mislin, *On the genus of a nilpotent group with finite commutator subgroup*, Math Z. **146** (1976), 201-211.

[11] P. Hilton, *On the genus of nilpotent groups and spaces*, Israel J. Math. **54**(1) (1986), 1-13.

[12] R. Hirshon, *Some cancellation theorems with applications to nilpotent groups*, J. Austral. Math. Soc. Ser A, **23** (1997), 147-165.

[13] C. Hopkins, *Non-abelian groups whose groups of isomorphisms are abelian*, Ann. Math. **9**(1) (1927), 508-520.

[14] D. Jonah and M. Konvisser, *Some non-abelian p-groups with abelian automorphism groups*, Arch. Math. **26** (1975), 131-133.

[15] O. H. Kegel and B.A. F. Wehrfritz, *Locally Finite Groups*, North-Holland, Amsterdam (1967).

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

[17] A. Mader, *The Automorphism group of finite abelian p-groups*, Ann. Sci. Math. **36**(2) (2012), 559-575.

[18] G. A. Miller, *A non-abelian group whose group of isomorphisms is abelian*, The Messenger of Math. **XVIII** (1913-1914), 124-125.

[19] K. Mincheva, *Automorphism group of non-abelian p-groups*, MSc Dissertation, Central European University, (2010).

[20] G. Mislin, Nilpotent groups with finite commutator subgroups, in: P. Hilton (Ed.), *Localization in Group Theory and Homotopy Theory*, Lecture Notes in Mathematics **418**, Springer-Verlag Berlin (1974), 103-120.

[21] L.T. Mkiva, *The non-cancellation groups of certain groups which are split extensions of a finite abelian group by a finite rank free abelian group*, MSc Dissertation, University of the Western Cape, (2008).

[22] D. Scevenels and P. Witbooi, *Non-cancellation and Mislin Genus of certain groups and $H_0 - spaces$*, J. Pure and Applied Algebra, **170**(2-3) (2002), 309-320.

[23] I. Stewart and D. Tall, *Algebraic Number Theory*, Chapman and Hall London, (1979).

[24] R. Warfield, *Genus and cancellation for groups with finite commutator subgroup*, J. Pure Appl. Algebra, **6** (1975), 125-132.

[25] B. A. F. Wehrfritz, *The rank of the automorphism group of a finite group*, Ricerchedi Matematica, (2018).

[26] P. Witbooi, *Non-cancellation for certain classes of groups*, Comm. in Algebra, **27**(8) (1999), 3639-3646.

[27] P. Witbooi, *Non-unique direct product decompositions of direct powers of certain meta-cyclic groups*, Comm. in Algebra, **28**(5) (2000), 2565-2576.

[28] P. Witbooi, *Generalizing the Hilton-Mislin genus group*, J. Algebra, **239** (2001), 327-339.

[29] P. Witbooi, *Non-cancellation for groups with non-abelian torsion*, J. Group Theory **6**(4) (2003), 505-515.

[30] P. Witbooi, *The non-cancellation group of a direct power of a (finite cyclic)-by-cyclic group*, J. Manuscripta Math. **114** (2004), 469-475.