MASTERS DISSERTATION

The effect of the group structure of a group Q on its non-cancellation set

Author:
Elliot LUBISI

Supervisor:
Dr. R KWASHIRA and
Dr. J. MBA

A dissertation submitted in fulfillment of the requirements for the degree of Master of Science

in the

School of Mathematics

March 14, 2018

Declaration of Authorship

I, Elliot LUBISI, declare that this dissertation titled, "The effect of the group structure of a group Q on its non-cancellation set" and the work presented in it are my own. I confirm that:

- This work was mainly done while I was a candidate for a research degree at this University.
- Where any part of this dissertation has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- This dissertation is entirely my own work. With an exception of results I have quoted from the work of others, in which case the source of the result is always given.
- All main sources which I have used have being acknowledged.
- In this dissertation I have clearly stated my contributions and acknowledged the work done by others if there were collaborations.

Signed: ELubisi.

Date: 20/03/2018

"Pure mathematics is, in its way, the poetry of logical ideas."

Albert Einstein

"God used beautiful mathematics in creating the world."

Paul Dirac

Abstract

Let Q be any group. The non-cancellation set $\chi(Q)$ is the set of all isomorphism classes of groups U such that $U \times \mathbb{Z} \cong Q \times \mathbb{Z}$. Let Q be a finitely generated group with finite commutator subgroup, there is a group structure on its non-cancellation set $\chi(Q)$. If Q is a nilpotent group then the group structure of $\chi(Q)$ coincides with the Hilton-Mislin genus group. For a finitely generated group Q with a finite commutator subgroup, we investigate the effect of the group structure of Q on its non-cancellation set $\chi(Q)$.

Acknowledgements

My supervisors Dr. R. Kwashira (University of the Witwatersrand) and Dr. J. Mba (University of Johannesburg) for their support and constantly reviewing my work. Mostly, I would like to thank my supervisors for allowing this paper to be my own work, but steering me in the right direction whenever needed.

Professor Peter Witbooi for writing the paper "*Generalizing the Hilton-Mislin Genus Group*" which is the main source of information for this work.

Contents

Dedicated to my family for their continued support throughout my academic career.

Chapter 1

Introduction

Let R be a finitely generated nilpotent group with a finite commutator subgroup. The ***Mislin genus***, denoted by $\mathcal{G}(R)$, is the set of all isomorphism classes of finitely generated nilpotent groups S such that for each prime p we have $S_p \cong R_p$, that is, the groups S and R have isomorphic p-localizations, see [7]. In [2], Hilton and Mislin defined an abelian group structure on $\mathcal{G}(R)$. Let Q be a finitely generated group with a finite commutator subgroup, the non-cancellation set, denoted by $\chi(Q)$, is the set of all isomorphism classes of groups V such that $V \times \mathbb{Z} \cong Q \times \mathbb{Z}$. Note that the non-cancellation set is a measure of non-cancellation of $\mathbb{Z}$ as a direct factor of $Q \times \mathbb{Z}$. For a finitely generated nilpotent group R with a finite commutator subgroup, Warfield in [10] showed that $\mathcal{G}(R)$ coincides with $\chi(R)$, that is, $\chi(R) = \mathcal{G}(R)$. (For further studies regarding the genus see ([10], [3], [2], [4])). This relation and the group structure deduced by Hilton and Mislin on the genus sparked an interest in the study of the group structure of $\chi(Q)$. The author in [12] showed that some results obtained for non-cancellation sets of nilpotent groups do not simply generalize to the non-nilpotent groups. That is, the result $\chi(Q) = \mathcal{G}(Q)$ does not hold for every group Q.

Denote by χ_0 the class of all finitely generated groups with a finite commutator subgroup. The author in [11] showed that for any χ_0-group Q such that Q has subgroups of finite index the non-cancellation set $\chi(Q)$ has a group structure which coincides with the Hilton-Mislin genus group if Q is nilpotent. Let A be a finite abelian group and let m be a positive integer. The class $\mathcal{K}$ of groups of the form $A \rtimes \mathbb{Z}^m$ is a subclass of χ_0-groups. This subclass was studied in [9] for groups with an abelian torsion subgroup. The authors in [9] gave an alternative description of the group structure of the non-cancellation set of a $\mathcal{K}$-group. In this work we focus on χ_0-groups. We study the effect of the group structure of a χ_0-group on its non-cancellation set. We consider χ_0-groups with some additional properties and check whether the additional properties on the χ_0-group have an effect on the group structure of its non-cancellation set.

In Chapter 2 we give basic definitions and results from Group Theory. We define the key terms needed in later chapters such as torsion subgroup, automorphism group, commutator subgroup etc. A formal definition of a finitely generated group is given. There is a construction of direct products of groups as well as a construction of semi-direct products. Lagrange's Theorem (Theorem 2.22) allows us to compute the size of the non-cancellation sets of certain χ_0-groups in Chapter 3. Also, the size of the non-cancellation set depends on the Euler-phi function, we discuss the Euler-phi function to complete this chapter.

In Chapter 3 we follow the notation introduced by the author in [11] and consider the group structure of non-cancellation sets of χ_0-groups. We formally define a χ_0-group and we give basic properties of these groups. Results which consider subgroups of finite index of χ_0-groups are given in this chapter since subgroups of finite index play an important role in constructing the non-cancellation set of χ_0-groups. As in [11] we show that the non-cancellation set of a χ_0-group has an abelian group structure.

In Chapter 4 we discuss χ_0-groups with additional properties and check whether these properties have an effect on the non-cancellation set of the χ_0-group. In Chapter 5 we conclude our work.

Chapter 2

Preliminaries

2.1 Groups and subgroups

Definition 2.1.

A non-empty set Q is called a ***group*** if under the binary operation $\bullet$ the following are satisfied:

1. $v \bullet w \in Q$ for any $v, w \in Q$.

2. $(v \bullet w) \bullet k = v \bullet (w \bullet k)$ for any $v, w, k \in Q$.

3. There is a unique element $i_Q \in Q$ called the *identity* such that $v \bullet i_Q = i_Q \bullet v = v$ for any $v \in Q$.

4. There exist a unique element $v^{-1} \in Q$ such that $v \bullet v^{-1} = v^{-1} \bullet v = i_Q$, v^{-1} is called the *inverse* of v.

Instead $v \bullet w$ we write vw for notational convenience.

Definition 2.2.

A group Q is said to be ***abelian*** if for any $v, w \in Q$ we have that $vw = wv$.

Example 2.3.

1. Let $A = \{v \in \mathbb{Z} : v \text{ is even}\}$ define the binary operation on A to be addition. We show that A is a group under this operation. If $v, w \in A$ then $v + w$ is even so $v + w \in A$ hence A is closed. Also $(v + w) + k = v + (w + k)$ for any $v, w, k \in A$ so A is associative. We know that $0 \in A$ and $0 + v = v + 0 = v$ for any $v \in A$, that is, 0 is the identity in A. Finally $v + (-v) = (-v) + v = 0$ hence $-v \in A$ is the inverse of v. Therefore A is a group. Also $v + w = w + v$ for any $v, w \in A$, that is, A is abelian.

2. $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ are all groups under addition.

3. $\mathbb{C} - \{0\}, \mathbb{R} - \{0\}, \mathbb{Q} - \{0\}$ are all groups under multiplication.

4. Consider the set of integers $\mathbb{Z}$ under multiplication. We show that $\mathbb{Z}$ under multiplication is not a group. For any $v, w \in \mathbb{Z}$ we have that $vw \in \mathbb{Z}$ so $\mathbb{Z}$ is closed under multiplication. Also for any $v, w, k \in \mathbb{Z}$ we have that $(vw)k = v(wk)$, that is, associativity holds. The multiplicative identity is 1 since $1v = v1 = v$ for any $v \in \mathbb{Z}$. Let $v \in \mathbb{Z}$ and suppose that there is a unique element $x \in \mathbb{Z}$ such that $xv = vx = 1$ then $xv = 1$ implies that $x = \frac{1}{v} \notin \mathbb{Z}$ contradicting our assumption that $x \in \mathbb{Z}$. Hence for any $v \in \mathbb{Z}$ the multiplicative inverse of v is not contained in $\mathbb{Z}$ therefore under multiplication $\mathbb{Z}$ is not a group.

5. The set of integers modulo n, denoted by $\mathbb{Z}_n$, is a group under addition modulo n, but $\mathbb{Z}_n$ is not a group under multiplication modulo n.

6. The set of integers relatively prime to n, denoted by $\mathbb{Z}_n^*$, is a group under multiplication modulo n.

Definition 2.4.

Let Q be a group and let $v \in Q$. We define the ***order*** of v, denoted by $|v|$, to be the least positive integer m such that $v^m = i_Q$. If no such positive integer exist the order of v is said to be infinite.

Definition 2.5.

The ***order*** of a group Q, denoted by $|Q|$, is the number of elements in Q. We say that Q is a *finite group* if Q has finite order otherwise Q is said to be an *infinite group*, that is, $|Q| = \infty$.

Example 2.6.

1. The group $Q = \{i_Q\}$ is called the ***trivial group*** and it is the only group of order 1.

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

Definition 2.7.

A group Q is said to have ***exponent*** m if m is the least positive integer such that $v^m = i_Q$ for each $v \in Q$.

Definition 2.8.

Let U be a non-empty subset of a group Q. We say that U is a ***subgroup*** of Q if U is a group under the same binary operation as Q. We write $U \leq Q$.

Example 2.9.

Consider the group of integers $\mathbb{Z}$ under addition. We know that the set of even integers $2\mathbb{Z}$ is a non-empty subset of $\mathbb{Z}$. In Example 2.3 we have shown that $2\mathbb{Z}$ is a group under addition hence $2\mathbb{Z} \leq \mathbb{Z}$. Note that for any $m \in \mathbb{Z}$ we have that $m\mathbb{Z} \leq \mathbb{Z}$.

Theorem 2.10. *Let U be a non-empty subset of a group Q. Then $U \leq Q$ if and only if $vw^{-1} \in U$ for each $v, w \in U$.*

Proof. Assume that $U \leq Q$ so U is a group under the same binary operation as Q. Let $v, w \in U$ then as $w \in U$ we have that $w^{-1} \in U$ since U is a group. Thus $vw^{-1} \in U$ since U is closed under the binary operation.

Conversely, suppose that U is a non-empty subset of Q with $vw^{-1} \in U$ for each $v, w \in U$. Let $x \in U$ then $i_Q = xx^{-1} \in U$. Now if $i_Q, x \in U$ then $i_Q x^{-1} = x^{-1} i_Q = x^{-1} \in U$. For $w \in U$ we have that $w^{-1} \in U$ hence $vw \in U$. Since the associativity condition is inherited by $U \subseteq Q$ we have shown that $U \leq Q$. $\square$

Definition 2.11.

The set of all elements of finite order in a group Q form a subgroup of Q called the ***torsion subgroup***, denoted by T_Q. A group with a trivial torsion subgroup is called a ***torsionfree group***.

Definition 2.12.

A set Y of elements of a group Q is said to ***generate*** the group Q if all the elements of Q can be presented as a product of elements of Y and inverses of elements of Y.

That is, for any $v \in Q$ there exists $y_i \in Y$ and $\epsilon_i \in \{1, -1\}$ and some integer m such that

$$v = y_1^{\epsilon_1} \dots y_m^{\epsilon_m}.$$

Note 2.13.

If a finite set Y generates a group Q we say that Q is *finitely generated.*

Definition 2.14.

A group Q is said to be ***cyclic*** if Q is generated by a single element. We denote a cyclic group of order m by C_m.

2.2 Cosets and Lagrange's theorem

Definition 2.15.

Let v be an element of a group Q and let $U \leq Q$. The set $vU = \{vu : u \in U\}$ is said to be the ***left coset*** of U generated by v. In a similar manner, the set $Uv = \{uv : u \in U\}$ is said to be the ***right coset*** of U generated by v.

Example 2.16.

Let $Q = \{0, 1, 2, 3\}$, that is, Q is the group of integers modulo 4. Let $U = \{0, 2\}$, note that U is a subgroup of Q. Thus U has the following left cosets in Q

$$0 + U = U, 1 + U = \{1, 3\}, 2 + U = U, 3 + U = \{1, 3\}.$$

Hence $0 + U = 2 + U$ and $1 + U = 3 + U$. Therefore U has only two left cosets in Q, that is, $0 + U = U$ and $1 + U$.

Note 2.17.

Let Q be a group and let $U \leq Q$.

1. $Ui_Q = i_Q U = U$ then U is both a left and a right coset of itself.

2. For an abelian group Q we have $Uv = vU$ for any $v \in Q$, that is, there is no distinction between the left and right cosets.

Proposition 2.18. *Let U be a subgroup of a group Q and let $v \in Q$. Then $vU = U$ if and only if $v \in U$.*

Proof. Suppose that $vU = U$ then $vu = u_1$ where $u_1 \in U$ then $v = u^{-1}u_1 \in U$ therefore $v \in U$.

Conversely, suppose that $v \in U$ we show that $vU = U$. First we show that $vU \subseteq U$. Let $vu \in vU$ where $v \in U$ then $vu \in U$ since $v, u \in U$ and $U \leq Q$ so $vU \subseteq U$. Now we show that $U \subseteq vU$. Let $u \in U$ then $vu \in U$ since $v, u \in U$ and $U \leq Q$. As $vu \in U$ and $vu \in vU$ we have that $U \subseteq vU$ giving that $U = vU$. □

Theorem 2.19. *Let Q be a group and let $v, w \in Q$. Suppose that U is a subgroup of Q. Then $vU = wU$ if and only if $v^{-1}w \in U$.*

Proof. Suppose that $vU = wU$ then as $i_Q \in U$ we have that $vu = w$ for some $u \in U$ giving that $u = v^{-1}w$, that is, $v^{-1}w = u \in U$.

Conversely, suppose that $v^{-1}w \in U$ then $v^{-1}w = u$ for some $u \in U$ so $w = vu$ therefore

$$wU = vuU = vU$$

since U is a subgroup. □

A similar result holds for right cosets.

Note 2.20.

Suppose that Q is a group and let $U \leq Q$. If $v \in Q$ then $\vartheta : U \to vU$ defined by $\vartheta(U) = vu$ is a bijection then $|vU| = |U|$ which holds for all $v \in Q$.

Definition 2.21.

Let U be a subgroup of a group Q. The number of distinct left (or right) cosets of U in Q is said to be the ***index*** of U in Q, denoted by $[Q : U]$.

Theorem 2.22 (Lagrange's Theorem). *Let Q be a group and let $U \leq Q$. Then $|Q| = |U|[Q : U]$. Furthermore , if Q is a finite group then $|U|$ divides $|Q|$ and $[Q : U] = \frac{|Q|}{|U|}$.*

Proof. A partition of Q is formed by the left cosets of U hence

$$Q = \bigcup_{v \in Q} vU.$$

Note that for $v, w \in Q$ with $v \neq w$ we have $vU \cap wU = \emptyset$ hence the above union is a union of disjoint cosets. Thus

$$|Q| = |\bigcup_{v \in Q} vU| = \sum_{v \in Q} |vU|.$$

As we know that $|U| = |vU|$ for all cosets of U then

$$\sum_{v \in Q} |vU| = \sum_{v \in Q} |U|.$$

Therefore

$$|Q| = \sum_{v \in Q} |U| = [Q : U]|U|.$$

□

Corollary 2.23. *Suppose that Q is a finite group.*

1. *If $v \in Q$ then $|v|$ divides $|Q|$. Furthermore $v^{|Q|} = i_Q$.*

2. *If Q has prime order then Q is a cyclic group.*

Proof. 1. Suppose that v is an element of Q of order m then $U = \{i_Q, v, ..., v^{m-1}\}$ is a subgroup of Q of order m. Thus m divides $|Q|$ by Theorem 2.22. In particular since $|v|$ divides $|Q|$ we have that $v^{|Q|} = i_Q$.
2. Suppose that $|Q|$ is prime. Then we may take $v \neq i_Q$ in Q, given that $|v|$ divides $|Q|$ we have that $|v| = |Q|$. Then Q coincides with the cyclic group generated by v. □

2.3 Normal subgroups and quotient groups

Definition 2.24.

Let v be an element of a group Q. The element xvx^{-1} where $x \in Q$ is said to be the ***conjugate*** of v in Q.

Definition 2.25.

Let Q be a group and let $U \leq Q$. Then U is called a ***normal subgroup*** of Q if $vU = Uv$ for each $v \in Q$. We write $U \trianglelefteq Q$.

Example 2.26.

1. Let Q be a group. Then the trivial subgroup $\{i_Q\} \trianglelefteq Q$ and $Q \trianglelefteq Q$.

2. Let $Q = \mathbb{Z}_n^*$ and $U = \{1, -1\}$, then for any $v \in \mathbb{Z}_n^*$ we have that

$$v1v^{-1} = vv^{-1} = 1 \in U$$

$$v(-1)v^{-1} = -(v1v^{-1}) = -(vv^{-1}) = -1 \in U$$

hence $U \trianglelefteq Q$.

Note 2.27.

Suppose that Q is an abelian group and let $U \leq Q$. Then for all $v \in Q$ with $v \notin U$ we have $vu = uv$ for all $u \in U$ hence $vU = Uv$. Which implies that $U \trianglelefteq Q$. This holds for any subgroup U of Q. Hence all subgroups of an abelian group Q are normal subgroups of Q.

Theorem 2.28. *Suppose that Q is a group. Then the following conditions are equivalent:*

1. $U \trianglelefteq Q$.

2. $vUv^{-1} \subseteq U$ *for each* $v \in Q$.

3. $vUv^{-1} = U$ *for each* $v \in Q$.

Proof. 1. $\Rightarrow$ 2. Let $v \in Q$ and assume that $U \trianglelefteq Q$. We show that $vU = Uv$ implies that $vUv^{-1} \subseteq U$. Let $u \in U$ then

$$vuv^{-1} \in vUv^{-1} \Rightarrow vu \in vU = Uv \Rightarrow vu \in Uv \Rightarrow vuv^{-1} \in U$$

thus $vUv^{-1} \subseteq U$.
2. $\Rightarrow$ 3. Suppose that $vUv^{-1} \subseteq U$ for each $v \in Q$ it follows that $v^{-1}Uv \subseteq U$. Let $u \in U$ then

$$u = vv^{-1}uvv^{-1} \in vUv^{-1}.$$

Since $v^{-1}uv \in U$ as $v^{-1}Uv \subseteq U$ so $u \in vUv^{-1}$ giving that $U \subseteq vUv^{-1}$ hence $vUv^{-1} = U$.
3. $\Rightarrow$ 1. Suppose $vUv^{-1} = U$ for all $v \in U$. We show that $vUv^{-1} = U$ implies that

$vU = Uv$ for all $v \in Q$. Let $w \in vU \Rightarrow wv^{-1} \in U \Rightarrow w \in Uv$ giving that $vU \subseteq Uv$. Now let $k \in Uv \Rightarrow v^{-1}k \in U \Rightarrow k \in vU$ giving that $Uv \subseteq vU$ hence $vU = Uv$. □

Example 2.29.

Suppose that Q is an abelian group. We show that $T_Q \trianglelefteq Q$. It is enough to show that $T_Q \leq Q$. Since for any integer m we have that $i_Q^m = i_Q$ so $i_Q \in T_Q$ giving that $T_Q \neq \emptyset$. Let $v, w \in T_Q$ so there are finite integers n_1 and n_2 such that $a^{n_1} = b^{n_2} = i_Q$ then

$$(vw)^{n_1 n_2} = v^{n_1} w^{n_2} = i_Q$$

since Q is abelian therefore T_Q is closed. For any $v \in T_Q$ with $v^n = i_Q$ we have that $(v^{-1})^n = v^{-n} = (v^n)^{-1} = i_Q$ so T_Q contains inverses of its elements and the identity is i_Q. Associativity is inherited from Q. Normality follows as Q is abelian.

Proposition 2.30. *Let Q be a group and let $U \trianglelefteq Q$. Then the set of cosets of U in Q form a group under the binary operation*

$$vU \bullet wU = vwU \text{ for } v, w \in Q$$

Proof. Let $\bar{Q} = \{vU : v \in Q\}$. Clearly $\bar{Q}$ is closed since if $vU, wU \in \bar{Q}$ then $vU \bullet wU = vwU \in \bar{Q}$ as $vw \in Q$, that is, Q is a group. Now $i_Q \in Q$ so $i_Q U = U \in \bar{Q}$ and for any $vU \in \bar{Q}$ we have that $vU \bullet i_Q U = i_Q U \bullet vU = vU$ hence U is the identity element in $\bar{Q}$. Since Q is a group for any $v \in Q$ there is $v^{-1} \in Q$ hence $v^{-1}U \in \bar{Q}$ and $vU \bullet v^{-1}U = vv^{-1}U = i_Q U = U$, similarly $v^{-1}U \bullet vU = U$ so $v^{-1}U$ is the inverse of vU in $\bar{Q}$. Let $vU, vU, kU \in \bar{Q}$ now

$$(vU \bullet wU) \bullet kU = (vw)U \bullet kU = (vw)kU = v(wk)U = vU \bullet (wk)U = vU \bullet (wU \bullet kU)$$

therefore $\bar{Q}$ is associative. We have shown that $\bar{Q}$ is a group. □

Definition 2.31.

Let Q be a group and let $R \trianglelefteq Q$. The set of cosets of R in Q form a group called the ***quotient group*** of Q by R, denoted by Q/R.

Example 2.32.

Let $Q = \mathbb{Z}_n^*$ and let $U = \{1, -1\}$. In Example 2.26 we have shown that $U \trianglelefteq Q$

therefore Q/U is a group. Note that Q/U is an abelian group, to justify this claim let $vU, wU \in Q/U$ then

$$vU \bullet wU = vwU = wvU = wU \bullet vU.$$

Since $v, w \in Q$ and the binary operation in Q is commutative hence Q/U is abelian.

Definition 2.33.

Let Q_1 and Q_2 be groups.

1. A map $\kappa : Q_1 \to Q_2$ is said to be a ***group homomorphism*** if for each $v, w \in Q_1$

$$\kappa(vw) = \kappa(v)\kappa(w).$$

2. Suppose that $\kappa : Q_1 \to Q_2$ is a group homomorphism. The set

$$Ker\,\kappa = \{v \in Q_1 \,:\, \kappa(v) = i_{Q_2}\}$$

is said to be the ***kernel*** of κ, denoted by $Ker\,\kappa$. Moreover, $Ker\,\kappa \trianglelefteq Q_1$.

3. Let $\kappa : Q_1 \to Q_2$ be a group homomorphism. The ***image*** of κ, denoted by $Im\,\kappa$, is defined by

$$Im\,\kappa = \{\kappa(v) \,:\, v \in Q_1\}.$$

Furthermore $Im\,\kappa \leq Q_2$.

Remark 2.34.

Suppose that Q_1 and Q_2 are groups and $\kappa : Q_1 \to Q_2$ is a group homomorphism. Then $Ker\,\kappa \leq Q_1$. We prove this result. Clearly $Ker\,\kappa \neq \emptyset$ since $\kappa(i_{Q_1}) = i_{Q_2}$ so $i_{Q_1} \in Ker\,\kappa$. Let $v, w \in Ker\,\kappa$ then $\kappa(vw) = \kappa(v)\kappa(w) = i_{Q_2}i_{Q_2} = i_{Q_2}$ so $vw \in Ker\,\kappa$ giving that $Ker\,\kappa$ is closed. We know that if $v \in Ker\,\kappa$ then $\kappa(v) = i_{Q_2}$ so $\kappa(vv^{-1}) = \kappa(v)\kappa(v^{-1}) = i_{Q_2}\kappa(v^{-1}) = \kappa(v^{-1})$ but $\kappa(vv^{-1}) = \kappa(i_{Q_1}) = i_{Q_2}$ so $\kappa(v^{-1}) = i_{Q_2}$ hence $v^{-1} \in Ker\,\kappa$. Furthermore, $Ker\,\kappa \trianglelefteq Q$ to show this result let $v \in Q_1$ and $w \in Ker\,\kappa$ then

$$\kappa(vwv^{-1}) = \kappa(v)\kappa(w)\kappa(v^{-1}) = \kappa(v)i_{Q_2}\kappa(v^{-1}) = \kappa(v)\kappa(v^{-1}) = \kappa(vv^{-1}) = \kappa(i_{Q_1}) = i_{Q_2}.$$

Then $vwv^{-1} \in Ker\,\kappa$, thus $Ker\,\kappa \trianglelefteq Q_1$.

Proposition 2.35. *Suppose that Q is a group. Then every normal subgroup of Q is a kernel of some homomorphism.*

Proof. Let $R \trianglelefteq Q$. Define a map $\pi : Q \to Q/R$ by $\pi(v) = vR$. We show that π is a group homomorphism with $Ker\,\pi = R$. Let $v, w \in Q$ then $\pi(vw) = vwN$
$= vN \bullet wN = \pi(v)\pi(w)$ so π is a group homomorphism and

$$Ker\,\pi = \{v \in Q : \pi(v) = i_{Q/R}\} = \{v \in Q : vR = R\} = \{v \in R : a \in R\} = R.$$

□

Definition 2.36.

Let Q be a group and let $R \trianglelefteq Q$. Then group homomorphism

$$\pi : Q \to Q/R$$

is said be ***canonical homomorphism***.

Note 2.37.

A group homomorphism is one-to-one if and only if the kernel is trivial.

Definition 2.38.

Let Q_1 and Q_2 be groups and $\kappa : Q_1 \to Q_2$ is a group homomorphism.

1. κ is said to be a ***monomorphism*** if κ is one-to-one.
2. κ is said to be an ***epimorphism*** if κ is onto.
3. κ is said to be an ***isomorphism*** if κ is a bijection.
4. κ is said to be an ***endomorphism*** if $Q_1 = Q_2$.
5. κ is said to be an ***automorphism*** if $Q_1 = Q_2$ and κ is an isomorphism.

Definition 2.39.

An ***automorphism group***, denoted by $Aut(Q)$, is the set of automorphisms of Q under the composition of maps.

Lemma 2.40. *Let v be an element of a group Q. Define $\phi_v : Q \to Q$ by $\phi_v(x) = vxv^{-1}$. Then ϕ_v is an automorphism.*

Proof. Let $x, y \in Q$ then

$$x = y \Leftrightarrow vxv^{-1} = vyv^{-1} \Leftrightarrow \phi_v(x) = \phi_v(y).$$

Hence ϕ_v is well-defined and one-to-one. Also for $y \in Q$ we have that $y = vv^{-1}yvv^{-1}$ $= \phi_v(v^{-1}yv)$ thus ϕ_v is onto. Let $x, y \in Q$ then

$$\phi_v(xy) = vxyv^{-1} = vxv^{-1}vyv^{-1} = \phi_v(x)\phi_v(y).$$

Thus ϕ_v is a group homomorphism. Therefore ϕ_v is an automorphism. □

Definition 2.41.

Let v be an element of a group Q. The automorphism $\phi_v : Q \to Q$ defined by $\phi_v(x) = vxv^{-1}$ is said to be the ***inner automorphism***. The set of inner automorphisms is denoted by $Inn(Q)$.

Definition 2.42.

Let x and y be elements of a group Q. Then x and y are said to be ***conjugate*** if there is $v \in Q$ such that $\phi_v(x) = y$.

Proposition 2.43. *Suppose that Q is a group. Then the set of inner automorphisms $Inn(Q)$ is a subgroup of $Aut(Q)$. Moreover, $Inn(Q) \trianglelefteq Aut(Q)$.*

Proof. Since $\phi_{i_Q}(x) = i_Q x i_Q^{-1} = x$ for any $x \in Q$ thus $\phi_{i_Q} \in Inn(Q)$, that is, $Inn(Q) \neq \emptyset$. Let $\phi_v, \phi_w \in Inn(Q)$ then

$$(\phi_v\phi_w)(x) = \phi_v(\phi_w(x)) = \phi_v(wxw^{-1}) = vwxw^{-1}v^{-1} = vwx(vw)^{-1} = \phi_{vw}(x)$$

where $vw \in Q$ as Q is a group then $\phi_{vw} \in Inn(Q)$, that is, $\phi_v\phi_w \in Inn(Q)$ therefore $Inn(Q)$ is closed. Also for $v \in Q$ we have that

$$(\phi_{v^{-1}}\phi_v)(x) = \phi_{v^{-1}}(\phi_v(x)) = \phi_{v^{-1}}(vxv^{-1}) = v^{-1}vxv^{-1}v = i_Q x i_Q^{-1} = \phi_{i_Q}(x).$$

Similarly $\phi_v\phi_{v^{-1}} = \phi_{i_Q}$ so all elements of $Inn(Q)$ have inverses contained in $Inn(Q)$. Associativity is inherited from $Aut(Q)$ thus $Inn(Q) \leq Aut(Q)$. Moreover, let

$\kappa \in Aut(Q)$ and $\phi_v \in Inn(Q)$ then

$$(\kappa\phi_v\kappa^{-1})(x) = \kappa(\phi_v(\kappa^{-1}(x))) = \kappa(v\kappa^{-1}(x)v^{-1}) = \kappa(v)\kappa(\kappa^{-1}(x))(\kappa(v)^{-1})$$

$$= \kappa(v)x\kappa(v)^{-1} = \phi_{\kappa(v)}(x) \in Inn(Q).$$

Thus $Inn(Q) \trianglelefteq Aut(Q)$. □

Proposition 2.44. *Let Q_1 and Q_2 be groups and let $\kappa : Q_1 \to Q_2$ be a group homomorphism.*

1. *If $K \leq Q_1$ then $\kappa(K) \leq Q_2$. Moreover, if κ is an epimorphism and $K \trianglelefteq Q_1$ then $\kappa(K) \trianglelefteq Q_2$.*

2. *If $K \leq Q_2$ then $\kappa^{-1}(K) = \{v \in Q_1 : \kappa(v) \in K\} \leq Q_1$. If $K \trianglelefteq Q_2$ then $\kappa^{-1}(K) \trianglelefteq Q_1$.*

Proof. 1. Let $v, w \in K$. We show that $\kappa(v)\kappa(w)^{-1} \in \kappa(K)$. That is,

$$\kappa(v)\kappa(w^{-1}) = \kappa(vw^{-1}) \in \kappa(K)$$

since $K \leq Q_1$. Suppose that K is a normal subgroup of Q_1. We show that $x\kappa(K)x^{-1} = \kappa(K)$ for all $x \in Q_2$. Given that κ is an epimorphism then there is $y \in Q_1$ with $\kappa(y) = x$ so that

$$x\kappa(K)x^{-1} = \kappa(y)\kappa(K)\kappa(y^{-1}) = \kappa(yKy^{-1}) = \kappa(K)$$

since K is normal in Q_1.
2. We show that $vw^{-1} \in \kappa^{-1}(K)$ for $v, w \in \kappa^{-1}(K)$ which is the same as showing that $\kappa(vw^{-1}) \in K$. As $K \leq Q_2$ then $\kappa(vw^{-1}) = \kappa(v)\kappa(w^{-1}) \in K$ where $v, w \in \kappa^{-1}(K)$ thus $\kappa^{-1}(K) \leq Q_1$. Suppose that $K \trianglelefteq Q_2$ we show that for all $x \in Q_1$ we have $x\kappa^{-1}(K)x^{-1} = \kappa^{-1}(K)$ which is the same as showing that $\kappa(x\kappa^{-1}(K)x^{-1}) = K$ for $x \in Q_1$. Let $x \in Q_1$ and $v \in \kappa^{-1}(K)$ it follows that

$$\kappa(xvx^{-1}) = \kappa(x)\kappa(v)\kappa(x)^{-1} \in K$$

since $K \trianglelefteq Q_2$. □

Definition 2.45.

Let v and w be elements of a group Q. The element $vwv^{-1}w^{-1}$ is said to be the ***commutator*** of v and w, denoted by $[v, w]$.

Definition 2.46.

A ***commutator subgroup*** of a group Q, denoted by Q' or $[Q, Q]$, is the subgroup of Q which is generated by all the commutators of Q.

Note 2.47.

Suppose that Q is a group. The commutator subgroup Q' of Q is also called the *derived subgroup*. The commutator subgroup measures the abelianiarity of Q. That is, if Q is abelian then $Q' = \{i_Q\}$. If Q is not abelian then Q/Q' is an abelian group.

Definition 2.48.

Let Q be a group. Then the ***centre*** of a group Q, denoted by Z_Q, is defined by

$$Z_Q = \{v \in Q : vw = wv \text{ for any } w \in Q\}.$$

Proposition 2.49. *Suppose that Q is a group. Then $Z_Q \trianglelefteq Q$.*

Proof. We know that $i_Q v = v i_Q$ for any $v \in Q$ so $i_Q \in Z_Q$ thus $Z_Q \neq \emptyset$. Let $v, w \in Z_Q$ and $x \in Q$ then

$$(vw)x = v(wx) = v(xw) = (vx)w = (xv)w = x(vw)$$

giving that $vw \in Z_Q$. Let $v \in Z_Q$ we need to show that $v^{-1} \in Z_Q$. For any $x \in Q$ we have that

$$v^{-1}x = v^{-1}x(vv^{-1}) = v^{-1}(xv)v^{-1} = (v^{-1}v)xv^{-1} = xv^{-1}$$

hence $v^{-1} \in Z_Q$. Associativity is inherited from Q hence $Z_Q \leq Q$. Let $v \in Z_Q$ and $w \in Q$ then

$$wvw^{-1} = vww^{-1} = v \in Z_Q$$

therefore for any $v \in Z_Q$ and $w \in Q$ we have that $wvw^{-1} \in Z_Q$ thus $Z_Q \trianglelefteq Q$. $\square$

2.4 Direct products and isomorphism theorems

Theorem 2.50. *Suppose that Q_1 and Q_2 are groups. Then the set*

$$Q = \{(v, w) : v \in Q_1,\ w \in Q_2\}$$

form a group with binary operation

$$(v_1, w_1) \bullet (v_2, w_2) = (v_1v_2, w_1w_2)$$

where $v_1, v_2 \in Q_1$ and $w_1, w_2 \in Q_2$.

Proof. Let $v_1, v_2 \in Q_1$ and $w_1, w_2 \in Q_2$ then $(v_1, w_1) \bullet (v_2, w_2) = (v_1v_2, w_1w_2) \in Q$ so Q is closed under this binary operation. Also for $(v_1, w_1), (v_2, w_2), (v_3, w_3) \in Q$ we have that

$$[(v_1, w_1) \bullet (v_2, w_2)] \bullet (v_3, w_3) = (v_1v_2, w_1w_2) \bullet (v_3, w_3) = (v_1v_2v_3, w_1w_2w_3)$$

$$= (v_1, w_1) \bullet (v_2v_3, w_2w_3) = (v_1, w_1) \bullet [(v_2, w_2) \bullet (v_3, w_3)]$$

hence associativity holds in Q. Now let $(v, w) \in Q$ then

$$(i_{Q_1}, i_{Q_2}) \bullet (v, w) = (i_{Q_1}v, i_{Q_2}w) = (v, w)$$

similarly $(v, w) \bullet (i_{Q_1}, i_{Q_2}) = (v, w)$. Hence (i_{Q_1}, i_{Q_2}) is the identity in Q. Now $(v, w)^{-1} = (v^{-1}, w^{-1})$, that is,

$$(v^{-1}, w^{-1}) \bullet (v, w) = (v^{-1}v, w^{-1}w) = (i_{Q_1}, i_{Q_2})$$

similarly $(v, w) \bullet (v^{-1}, w^{-1}) = (i_{Q_1}, i_{Q_2})$. Therefore Q is a group. □

Definition 2.51.

Let Q_1 and Q_2 be groups. We define the ***external direct product*** to be the group $Q_1 \times Q_2$ under the binary operation

$$(v_1, w_1) \bullet (v_2, w_2) = (v_1v_2, w_1w_2)$$

where $v_1, v_2 \in Q_1$ and $w_1, w_2 \in Q_2$.

Example 2.52.

Consider the group of integers modulo 2, $\mathbb{Z}_2$. Let $Q_1 = \mathbb{Z}_2$ and $Q_2 = \mathbb{Z}_2$ then $Q = Q_1 \times Q_2$ is a group under component-wise addition.

Note 2.53.

Suppose that Q_1 and Q_2 are groups and $Q = Q_1 \times Q_2$. Then $\bar{Q_1} = \{(v, i_{Q_2}) : v \in Q_1\}$ and $\bar{Q_2} = \{(i_{Q_1}, w) : w \in Q_2\}$ are isomorphic copies contained in Q. Moreover, $\bar{Q_1}$ and $\bar{Q_2}$ are normal subgroups of Q. We show that $\bar{Q_2} \trianglelefteq Q$, a similar proof can be done to show that $\bar{Q_1} \trianglelefteq Q$. Clearly $\bar{Q_2} \neq \emptyset$ since $(i_{Q_1}, i_{Q_2}) \in \bar{Q_2}$, that is, $i_{Q_2} \in Q_2$. Now let $(i_{Q_1}, w_1), (i_{Q_1}, w_2) \in \bar{Q_2}$ then $(i_{Q_1}, w_1) \bullet (i_{Q_1}, w_2) = (i_{Q_1}, w_1 w_2) \in \bar{Q_2}$ since $w_1 w_2 \in Q_2$. As Q_2 is a group so $w^{-1} \in Q_2$ for any $w \in Q_2$ hence $(i_{Q_1}, w^{-1}) \in \bar{Q_2}$ also (i_{Q_1}, i_{Q_2}) is the identity in $\bar{Q_2}$ therefore $\bar{Q_2} \leq Q$. Finally, let $(v, w) \in Q$ and $(i_{Q_1}, w') \in \bar{Q_2}$ then

$$(v, w) \bullet (i_{Q_1}, w') \bullet (v^{-1}, w^{-1}) = (v i_{Q_1} v^{-1}, w w' w^{-1}) = (v v^{-1}, w w' w^{-1}) = (i_{Q_1}, w w' w^{-1}) \in \bar{Q_2}$$

since $w w' w^{-1} \in Q_2$ hence $\bar{Q_2} \trianglelefteq Q$. Note that $Q = \bar{Q_1} \bar{Q_2}$ with $\bar{Q_1} \cap \bar{Q_2} = \{(i_{Q_1}, i_{Q_2})\}$.

Remark 2.54.

Let $U_1, ..., U_n$ be groups then $Q = U_1 \times \cdots \times U_n$ is a group with respect to component-wise multiplication. That is, the definition of the external direct product is not restricted to two groups.

Theorem 2.55 (Factor theorem). *Suppose that Q_1 and Q_2 are groups with $R \trianglelefteq Q_1$. Suppose that $\pi : Q_1 \to Q_1/R$ is the canonical homomorphism and let $\kappa : Q_1 \to Q_2$ be a group homomorphism. Then any group homomorphism with a kernel containing R can be factored through Q_1/R. That is, there exist a unique homomorphism $\bar{\kappa} : Q_1/R \to Q_2$ so that $\bar{\kappa} \circ \pi = \kappa$. Moreover,*

1. *$\bar{\kappa}$ is an epimorphism if and only if κ is an epimorphism.*

2. *$\bar{\kappa}$ is a monomorphism if and only if $Ker\, \kappa = R$.*

3. *$\bar{\kappa}$ is an isomorphism if and only if κ is an epimorphism and $Ker\, \kappa = R$.*

Proof. First we show that if there exist $\bar{\kappa}$ so that $\bar{\kappa} \circ \pi = \kappa$ then it is unique. Suppose that there is another homomorphism $\hat{\kappa}$ such that $\hat{\kappa} \circ \pi = \kappa$. Hence

$$(\bar{\kappa} \circ \pi)(v) = (\hat{\kappa} \circ \pi)(v) = \kappa(v)$$

for each $v \in Q$, giving that

$$\bar{\kappa}(vR) = \hat{\kappa}(vR) = \kappa(v).$$

Therefore for all $wR \in Q_1/R$ there is $w \in Q_1$ such that $\pi(w) = wR$, then the image is given by either $\bar{\kappa}$ or $\hat{\kappa}$ which is determined by κ. Therefore $\bar{\kappa} = \hat{\kappa}$ since π is onto hence $\bar{\kappa}$ is unique. Now we show that such a $\bar{\kappa}$ exists. Suppose that $vR \in Q_1/R$ such that $\pi(v) = vR$ for $v \in Q_1$. Define a mapping $\bar{\kappa} : Q_1/R \to Q_2$ by $\bar{\kappa}(vR) = \kappa(v)$. We show that $\bar{\kappa}$ is well-defined. Let $w \in vR$ as v and w are in the same coset we have that $v^{-1}w \in R \subseteq Ker\, \kappa$ by assumption. As $v^{-1}w \in Ker\, \kappa$ then $\kappa(v^{-1}w) = i_{Q_2}$ so $\kappa(v) = \kappa(w)$, thus $\bar{\kappa}$ is well-defined. Now we show that $\bar{\kappa}$ is a group homomorphism. Let $vR, wR \in Q_1/R$ then

$$\bar{\kappa}(vRwR) = \bar{\kappa}(vwR) = \kappa(vw) = \kappa(v)\kappa(w) = \bar{\kappa}(vR)\bar{\kappa}(wR)$$

so $\bar{\kappa}$ is a group homomorphsism.

1. The fact that $\bar{\kappa}$ is an epimorphism if and only if κ is an epimorphism follows from that $Im(\bar{\kappa}) = Im(\kappa)$.

2. The statement that $\bar{\kappa}$ is a monomorphism if and only if $Ker\, \kappa = R$ is true since $Ker\, \kappa$ is a normal subgroup of Q_1. We show that $\bar{\kappa}$ is a monomorphism by showing that $Ker\, \bar{\kappa}$ is trivial. As

$$Ker\, \bar{\kappa} = \{vR \in Q_1/R : \bar{\kappa}(vR) = i_{Q_2}\} = \{vR \in Q_1/R : \bar{\kappa}(\pi(v)) = \kappa(v) = i_{Q_2}\}$$

$$= \{vR \in Q_1/R : v \in Ker\, \kappa\}.$$

hence $Ker\, \bar{\kappa}$ contains elements of the form vR with $v \in Ker\, \kappa$ but $Ker\, \bar{\kappa}$ is trivial if $Ker\, \kappa = R$.

3. From 1. and 2. we get this result.

□

Theorem 2.56 (The First Isomorphism Theorem). *Suppose that Q_1 and Q_2 are groups and $\kappa : Q_1 \to Q_2$ is a group homomorphism. Then $Q_1/Ker\,\kappa \cong Im\,\kappa$.*

Proof. We know that $Ker\,\kappa \trianglelefteq Q_1$ so $Q_1/Ker\,\kappa$ is a group. Define a map $\bar{\kappa} : Q_1/Ker\,\kappa \to Im\,\kappa$ by $\bar{\kappa}(v\,Ker\,\kappa) = \kappa(v)$. Let $vKer\,\kappa, wKer\,\kappa \in Q_1/Ker\,\kappa$ then

$$v\,Ker\,\kappa = w\,Ker\,\kappa \Leftrightarrow v^{-1}w \in Ker\,\kappa \Leftrightarrow \kappa(v^{-1}w) = i_{Q_2} \Leftrightarrow \kappa(v)^{-1}\kappa(w) = i_{Q_2}$$

$$\Leftrightarrow \kappa(v) = \kappa(w) \Leftrightarrow \bar{\kappa}(v\,Ker\,\kappa) = \bar{\kappa}(w\,Ker\,\kappa)$$

thus $\bar{\kappa}$ is well-defined and one-to-one. In order to show that $\bar{\kappa}$ is onto we show that $Im\,\bar{\kappa} = Im\,\kappa$, that is,

$$\kappa(v) \in Im\,\kappa \Leftrightarrow \bar{\kappa}(v\,Ker\,\kappa) = \kappa(v) \in Im\,\bar{\kappa}$$

therfore $\bar{\kappa}$ is onto. We show that $\bar{\kappa}$ is a group homomorphism.

$$\bar{\kappa}((v\,Ker\,\kappa)\,(w\,Ker\,\kappa)) = \bar{\kappa}(vw\,Ker\,\kappa) = \kappa(vw) = \kappa(v)\kappa(w) = \bar{\kappa}(v\,Ker\,\kappa)\bar{\kappa}(w\,Ker\,\kappa)$$

hence $Q/Ker\,\kappa \cong Im\,\kappa$. □

2.5 Permutations and group actions

Definition 2.57.

Let v be an element of a group Q and let $U \leq Q$. The set $\{vuv^{-1} : u \in U\}$ is said to be the ***conjugate*** of U, denoted by U^v or vUv^{-1}.

Proposition 2.58. *Let Q be a group and let $U \leq Q$. Then the conjugate of U is a subgroup of Q.*

Proof. Since $i_Q = vi_Qv^{-1} \in U^v$ we have that $U^v \neq \emptyset$. Let $vu_1v^{-1}, vu_2v^{-1} \in U^v$ then

$$(vu_1v^{-1})(vu_2v^{-1})^{-1} = (vu_1v^{-1})(vu_2^{-1}v^{-1}) = vu_1(v^{-1}v)u_2^{-1}v^{-1} = vu_1u_2^{-1}v^{-1} \in U^v$$

since $u_1u_2^{-1} \in U$ as $U \leq Q$. Associativity is inherited from Q. Thus $U^v \leq Q$. □

Lemma 2.59. *Let Q be a group and let $U \leq Q$. If $v \in Q$ then vUv^{-1} is isomorphic to U.*

Proof. For $v \in Q$ we have $vUv^{-1} \leq Q$. Define $\phi : U \to vUv^{-1}$ by $\phi(u) = vuv^{-1}$. We show that ϕ is an isomorphism. Let $u_1, u_2 \in U$ then

$$u_1 = u_2 \Leftrightarrow vu_1v^{-1} = vu_2v^{-1} \Leftrightarrow \phi(u_1) = \phi(u_2)$$

hence ϕ is well-defined and one-to-one.
For any $vuv^{-1} \in vUv^{-1}$ there is $u \in U$ such that $\phi(u) = vuv^{-1}$ so ϕ is onto. Finally we show that ϕ is a homomorphism, let $u_1, u_2 \in U$ then

$$\phi(u_1u_2) = vu_1u_2v^{-1} = vu_1v^{-1}vu_2v^{-1} = \phi(u_1)\phi(u_2)$$

so ϕ is a homomorphism. Therefore ϕ is an isomorphism giving that $U \cong vUv^{-1}$. □

Definition 2.60.

Let Y be a set with m elements. We define a ***permutation*** of Y to be a bijection on Y. The set of permutations on Y(with respect to function composition) form a group called the ***symmetric group*** on Y, denoted by S_m.

Definition 2.61.

Let Y be a set with m elements. The ***alternating group***, denoted by A_m, is the set of all even permutations of S_m, $A_m \leq S_m$.

Theorem 2.62 (Cayley's Theorem). *Every group Q is isomorphic to a subgroup of the group of permutations.*

Proof. Denote by S_Q the set of permutations of a group Q. We show that every group is isomorphic to a subgroup of S_Q. Define a map $\mu : Q \to S_Q$ by $\mu(v) = \mu_v$ where $\mu_v : Q \to Q$ is a bijection on Q defined by $\mu_v(x) = vx$. We need to show that μ is one-to-one. Since Q is a group we have that $\mu_v(x) = \mu_w(x) \Rightarrow vx = wx$ if $x = i_Q$ so μ is one-to-one. Finally,

$$(\mu(v) \circ \mu(w))(x) = (\mu_v \circ \mu_w)(x) = v(wx) = vwx = \mu_{vw}(x) = \mu(vw)(x)$$

for any x, giving that $\mu(v) \circ \mu(w) = \mu(vw)$. Thus μ is a group homomorphism. Which completes the proof. □

Definition 2.63.

Let Y be a non-empty set and Q be a group. A mapping $* : Q \times Y \to Y$, defined by $v * y = vy$, is called an ***left action*** of Q on Y if it satisfies:

1. $v * y \in Y$ for any $v \in Q$ and any $y \in Y$.
2. $i_Q * y = y$ for $i_Q \in Q$ and any $y \in Y$.
3. $(v_1 v_2) * y = v_1 * (v_2 * y)$ for any $v_1, v_2 \in Q$ and any $y \in Y$.

The set Y is said to be a Q-set or we say that Q acts on Y.

Definition 2.64.

Let Q be a group and let Y be a Q-set. Then the set $\{v \in Q : v * y = y\}$ where $y \in Y$ is called the ***stabilizer*** of y, denoted by $Stab_Q(y)$.

Proposition 2.65. *Let Q be a group and let Y be a Q-set. Then the stabilizer of $y \in Y$ is a subgroup of Q. This subgroup is called an **isotropy subgroup**.*

Proof. As $i_Q * y = y$ so $i_Q \in Stab_Q(y)$, that is, $Stab_Q(y) \neq \emptyset$. Let $v_1, v_2 \in Stab_Q(y)$ then $v_1 * y = y$ and $v_2 * y = y$ then

$$(v_1 v_2) * y = v_1 * (v_2 * y) = v_1 * y = y$$

so $v_1 v_2 \in Stab_Q(y)$. If $v \in Stab_Q(y)$ then $v * y = y$ so $y = v^{-1} * y$ giving that $v^{-1} \in Stab_Q(y)$. Associativity is inherited from Q hence $Stab_Q(y) \leq Q$. □

Definition 2.66.

Let a group Q act on a set Y. Then the ***orbit*** of $y \in Y$, denoted by $Orb(y)$, is defined by

$$Orb(y) = \{v * y : v \in Q\}.$$

Example 2.67.

(a) For a group Q define $* : Q \times Q \to Q$ by $v * y = vy$. We show that $*$ is an action.

1. Let $v \in Q$, clearly $v * y = vy \in Q$ since Q is a group, that is, Q is closed.
2. $i_Q * y = i_Q y = y$ since i_Q is the identity in Q.

3. Let $v_1, v_2, y \in Q$ then

$$(v_1 v_2) * y = v_1 v_2 y = v_1(v_2 * y) = v_1 * (v_2 * y).$$

Thus $*$ is an action.

(b) Suppose that Q is a group and $Y = \{U : U \leq Q\}$. Then Q acts on Y by conjugation. We justify this claim. Define $* : Q \times Y \to Y$ by $v * U = vUv^{-1} = U^v$.

1. $v * U = vUv^{-1} = U^v \in Y$ for any $v \in Q$ and $U \in Y$.
2. $i_Q * U = i_Q H i_Q^{-1} = U^{i_Q} = U$ for $i_Q \in Q$ and $U \in Y$.
3. $(v_1 v_2) * U = (v_1 v_2) U (v_1 v_2)^{-1} = v_1(v_2 U v_2^{-1}) v_1^{-1} = v_1 * (v_2 * U)$ for any $v_1, v_2 \in Q$ and $U \in Y$.

Therefore Q acts on Y by conjugation. Also

$$Stab_Q(U) = \{v \in Q : v * U = U\} = \{v \in Q : vUv^{-1} = U\} = \{v \in Q : U^v = U\}.$$

(c) Let $C_2 = (x)$ and let $C_n = (y)$. Define $* : C_2 \times Aut(C_n) \to Aut(C_n)$ by $x * f = f_x$ with $f_x : C_n \to C_n$ defined by $f_x(y) = y^{-1}$. Also $i_{C_2} * f = f_{i_{C_2}}$ where $f_{i_{C_2}} : C_n \to C_n$ is defined by $f_{i_{C_2}}(y) = y$, note that $f_{i_{C_2}}$ is the identity map.
We will show that $*$ is an action.

1. For $x \in C_2$ we have $x * f = f_x$ where $f_x : C_n \to C_n$ is defined by $f_x(y) = y^{-1}$ hence $f_x \in Aut(C_n)$. We now verify the claim $f_x \in Aut(C_n)$. Since $f_x : C_n \to C_n$, it is enough to show that f_x is an isomorphism. Let $a, b \in C_n$ then $a = y^n$ and $b = y^m$ for some $n, m \in \mathbb{Z}$.

$$f_x(ab) = f_x(y^n y^m) = f_x(y^{n+m}) = y^{-n-m} = y^{-n} y^{-m} = (y^n)^{-1}(y^m)^{-1} = a^{-1}b^{-1}$$

$$= f_x(a) f_x(b)$$

hence f_x is a homomorphism.
For any $y^{-1} \in C_n$ there is $y \in C_n$ such that $f_x(y) = y^{-1}$ so f_x is onto.
Since C_n is a group then the inverse of $y \in C_n$ is unique giving that f_x is one-to-one and well defined. Thus f_x is an isomorphism.

2. $i_{C_2} * f = f_{i_{C_2}}$ then $f_{i_{C_2}} : C_n \to C_n$ is defined by $f_{i_{C_2}}(y) = y$. That is, $f_{i_{C_2}}$ is equivalent to the identity map in $Aut(C_n)$.

3. Since $|C_2| = 2$ so $i_{C_2}, x \in C_2$ hence

$$(xi_{C_2}) * f = f_{xi_{C_2}} = f_x.$$

Thus

$$(xi_{C_2}) * f = x * (i_{C_2} * f).$$

Example 2.68.

Suppose that Q is a group and let $Y = \{U : U \leq Q\}$. From Example 2.67(b) we know that Q acts on Y by conjugation. Now we have that for $U \in Y$.

$$Orb(U) = \{v * U : v \in Q\} = \{vUv^{-1} : v \in Q\} = \{U^v : v \in Q\}.$$

Definition 2.69.

Let a group Q act on a set Y. An action $* : Q \times Y \to Y$ is said to be ***transitive*** if $*$ has exactly one orbit.

Theorem 2.70 (Orbit-Stabilizer Theorem). *Suppose that a group Q acts on a set Y and $y \in Y$. Then*

$$|Orb(y)| = [Q : Stab_Q(y)].$$

Proof. Since $Stab_Q(y) \leq Q$ then by Theorem 2.22 $[Q : Stab_Q(y)]$ is the number of left cosets of $Stab_Q(y)$ in Q. Define a map $\vartheta : Orb(y) \to \{v\, Stab_Q(y) : v \in Q\}$ by $\vartheta(v * y) = v\, Stab_Q(y)$. Let $v_1, v_2 \in Q$ then

$$v_1 * y = v_2 * y \Leftrightarrow (v_2^{-1}v_1) * y = y \Leftrightarrow v_2^{-1}v_1 \in Stab_Q(y)$$

$$\Leftrightarrow v_1\, Stab_Q(y) = v_2\, Stab_Q(y) \Leftrightarrow \vartheta(v_1 * y) = \vartheta(v_2 * y)$$

thus ϑ is well-defined and one-to-one. For any $v\, Stab_Q(y)$ we have $v * y \in Orb(y)$ such that $\vartheta(v * y) = v\, Stab_Q(y)$ hence ϑ is onto. Thus ϑ is a bijection therefore $|Orb(y)| = [Q : Stab_Q(y)]$. □

Definition 2.71.

Let Q be a group and let $U \leq Q$. We say that U is ***conjugate*** to a subgroup V of Q if there is $z \in Q$ such that $U = zVz^{-1} = V^z$. We say that U is ***self-conjugate*** if U is a normal subgroup of Q.

Lemma 2.72. *Let Q be a group and $U \leq Q$. Then $[Q : U] = [Q : U^v]$ for any $v \in Q$.*

Proof. Let $\mathcal{F} = \{xU : x \in Q\}$ and $\mathcal{F}' = \{xU^v : x \in Q,\ \text{for a fixed } v \in U\}$. Note that $|\mathcal{F}| = [Q : U]$ and $|\mathcal{F}'| = [Q : U^v]$. We show that there is a bijection between $\mathcal{F}$ and $\mathcal{F}'$. Define $\psi : \mathcal{F} \to \mathcal{F}'$ by $\psi(xU) = x^v U^v$, let $xU, yU \in \mathcal{F}$ then

$$\psi(xU) = \psi(yU) \Rightarrow x^v U^v = y^v U^v \Rightarrow (y^{-1})^v x^v U^v = U^v \Rightarrow (y^{-1})^v x^v \in U^v$$

$$\Rightarrow vy^{-1}v^{-1}vxv^{-1} \in vUv^{-1} \Rightarrow vy^{-1}xv^{-1} \in vUv^{-1} \Rightarrow y^{-1}x \in U \Rightarrow y^{-1}xU = U$$

$$\Rightarrow xU = yU.$$

Thus ψ is one-to-one. For any $xU^v \in \mathcal{F}'$ there is $x^{v^{-1}}U \in \mathcal{F}$ such that $\psi(x^{v^{-1}}U) = xU^v$, therefore ψ is onto. Hence ψ is a bijection giving that $|\mathcal{F}| = |\mathcal{F}'|$ so $[Q : U] = [Q : U^v]$. □

Note 2.73.

Let U and V be conjugate subgroups of a group Q, that is, there is $z \in Q$ such that $V = U^z$. From Lemma 2.72 we have that $[Q : U] = [Q : U^z]$ hence $[Q : U] = [Q : U^z] = [Q : V]$. That is, U and V have the same index.

Theorem 2.74. *Let U and V be subgroups of a group Q. If U and V are conjugate then $U \cong V$.*

Proof. Since U and V are conjugate there is $c \in Q$ such that $U = cVc^{-1}$. As V is a subgroup of Q it follows from Lemma 2.59 that $V \cong cVc^{-1} = U$ giving that $U \cong V$. □

Example 2.75.

Suppose that $Q = \mathbb{Z} \times \mathbb{Z}$ and $U = \{0\} \times \mathbb{Z}$ and $V = \mathbb{Z} \times \{0\}$, note that $U \leq Q$ and $V \leq Q$. Then the map $\kappa : U \to V$ defined by $\kappa(0, y) = (y, 0)$ is an isomorphism, we justify this claim. Let $(0, y), (0, z) \in U$ then

$$(0, y) = (0, z) \Leftrightarrow y = z\ ,\ y, z \in \mathbb{Z} \Leftrightarrow (y, 0) = (z, 0) \Leftrightarrow \kappa(0, y) = \kappa(0, z)$$

so κ is well-defined and one-to-one. For any $(y,0) \in V$ there is $(0,y) \in U$ such that $\kappa(0,y) = (y,0)$ hence κ is onto. Let $(0,y),(0,z) \in U$ then

$$\kappa((0,y)(0,z)) = \kappa(0,yz) = (yz,0) = (y,0)(z,0) = \kappa(0,y)\kappa(0,z)$$

therefore κ is a homomorphism thus κ is an isomorphism. It follows that $U \cong V$. Let $k \in Q$ and let $(y,0) \in V$ then

$$k(y,0)k^{-1} = (kyk^{-1},0) \notin U$$

this is true for any $k \in Q$ giving that U is not conjugate to V. Hence $U \cong V$ does not imply that U is conjugate to V.

Remark 2.76.

Let U and V be subgroups of a group Q. Suppose that $U = aVa^{-1}$ for some $a \in Q$. Let Y be the set of all subgroups of Q. Define an action $\kappa : Q \times Y \to Y$ by $\kappa(a,V) = aVa^{-1} \in Y$. Then the orbit of V is given by

$$Orb(V) = \{\kappa(a,V) \mid a \in Q\} = \{aVa^{-1} \mid a \in Q\}.$$

thus $U \in Orb(V)$, similarly $V \in Orb(U)$. Hence under this action $Orb(V) = Orb(U)$ if U and V are conjugate.

Definition 2.77.

A group Q can be ***presented*** in the form $\langle X \mid Y \rangle$, that is, $Q = \langle X \mid Y \rangle$ where X is the set of generators and Y is the set of relations between the elements of X.

Example 2.78.

Consider the cyclic group with m elements C_m. Since C_m has one generator, say a, then $a^m = i_{C_m}$ so $X = \{a\}$ and $Y = \{a^m = i_{C_m}\}$ so

$$C_m = \langle a \mid a^m = i_{C_m} \rangle.$$

Since C_m is generated by single element a we write $C_m = (a)$.

Example 2.79.

A $\mathcal{K}$-*group* Q is a group which is presented as follows

$$G = \langle a, b \mid a^m = i_G, bab^{-1} = a^u \rangle$$

where $gcd(m, u) = 1$.

2.6 Euler phi function

Definition 2.80.

A function is called an ***arithmetic function*** if it is a real-valued or complex-valued function defined on the set of natural numbers $\mathbb{N}$.

The function defined below is an example of an arithmetic function.

Definition 2.81.

Let n be a positive integer. The ***Euler phi function***, denoted by $\varphi(n)$, is defined to be the number of positive integers relatively prime to n.

Note 2.82.

Since $\mathbb{Z}_n^*$ contains all the positive integers which are relatively prime to n we have that $|\mathbb{Z}_n^*| = \varphi(n)$. Thus $|\mathbb{Z}_n^*| = \varphi(n)$ is even for $n \geq 3$.

Definition 2.83.

An arithmetic function η is said to be ***multiplicative*** if for any $m, n \in \mathbb{N}$ we have that $\eta(mn) = \eta(m)\eta(n)$.

Remark 2.84.

From Number Theory we know that φ is *multiplicative* also for any prime p we have that $\varphi(p) = p - 1$, that is, all positive integers less than p are relatively prime to p. Now for $p = 2$ we have that $\varphi(2) = 2 - 1 = 1$. If p is an odd prime then $\varphi(p) = p - 1$ is even. Let m be any positive integer. It follows that

$$\varphi(p^m) = p^m - p^{m-1} = p^{m-1}(p - 1)$$

so $\varphi(p^m)$ is a multiple of an even number hence $\varphi(p^m)$ is even. Let k be any positive integer such that $k \geq 3$. Let $k = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$ where $p_1, \ldots, p_t$ are primes and

$m_1, \ldots, m_t$ are positive integers. Then

$$\varphi(k) = \varphi(p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}) = \varphi(p_1^{m_1})\varphi(p_2^{m_2}) \cdots \varphi(p_t^{m_t})$$

where each $\varphi(p_i^{m_i})$, $1 \leq i \leq t$, is even hence $\varphi(k)$ is even for any $k \geq 3$.

In Chapter 3, we will show that for certain χ_0-groups the size of the non-cancellation set is $\frac{\varphi(m)}{2}$, for some positive integer m which will be defined in the next chapter.

Chapter 3

Non-cancellation sets of χ_0-groups

In this chapter we discuss some results obtained by the author in [11]. In the first section we discuss basic properties of χ_0-groups. In Section 2 we study subgroups U of a χ_0-group Q such that U is of finite index in Q. We discuss the classes in the non-cancellation set of a χ_0-group Q. We conclude the chapter by investigating the group structure of the non-cancellation set of a χ_0-group.

3.1 Basic properties of χ_0-groups

In this section we introduce some basic properties of χ_0-groups, for a χ_0-group Q we define the number $m(Q)$ as in [11] and prove certain properties of this number. Note that for a χ_0-group Q the torsion subgroup is a finite normal subgroup. We begin the section by defining a χ_0-group.

Definition 3.1.

We say that a group Q is a χ_0***-group*** if Q is a finitely generated group with a finite commutator subgroup.

Theorem 3.2. *Let Q be a group and let $U \leq Q$ with $[Q : U]$ finite. Then Q is finitely generated if and only if U is finitely generated.*

Corollary 3.3. *Suppose that Q is any χ_0-group and let $U \leq Q$ with $[Q : U]$ finite. Then U is finitely generated.*

Proof. Given that Q is a χ_0-group then Q is finitely generated. It follows from Theorem 3.2 that U is finitely generated. □

From [11] we have the following two properties of χ_0-groups.

Lemma 3.4. *Suppose that Q is a χ_0-group. Then $Q \times \mathbb{Z}$ is a χ_0-group.*

Proof. Given that Q is a χ_0-group then Q is finitely generated, say $Y = \{v_1, \ldots, v_t\}$ is the generating set of Q, and $\mathbb{Z}$ is generated by 1, that is, $\mathbb{Z}$ is also finitely generated so $Q \times \mathbb{Z}$ is generated by elements of the form $(v, 1)$ where $v \in Y$. As the set Y is finite we have that there are finitely many elements of the form $(v, 1)$ where $v \in Y$ therefore $Q \times \mathbb{Z}$ is finitely generated. Since Q is a χ_0-group then Q has a finite commutator subgroup, as $\mathbb{Z}$ is an abelian group then the commutator subgroup of $\mathbb{Z}$ is trivial, that is, $[\mathbb{Z}, \mathbb{Z}] = \{i_{\mathbb{Z}}\}$. We show that the commutator subgroup of $Q \times \mathbb{Z}$ is finite. The commutator subgroup of $Q \times \mathbb{Z}$ is given by elements of the form $(v, i_{\mathbb{Z}})$ where v is a commutator of Q. Since there are finitely many commutators in Q it follows that the commutator subgroup of $Q \times \mathbb{Z}$ is finite thus $Q \times \mathbb{Z}$ is a χ_0-group. □

Lemma 3.5. *Suppose that Q is a group. Then $Q \times \mathbb{Z}$ is a χ_0-group if Q is a χ_0-group.*

Proof. Suppose that Q is not a χ_0-group. Then Q is not finitely generated and Q has an infinite commutator subgroup. As $Q \times \mathbb{Z}$ is a χ_0-group so the commutator subgroup of $Q \times \mathbb{Z}$ is finite. Since the commutator subgroup of $Q \times \mathbb{Z}$ has elements of the form $(v, i_{\mathbb{Z}})$ where v is a commutator of Q, there are infinitely many commutators of Q by assumption. Hence there are infinitely many elements of the form $(v, i_{\mathbb{Z}})$ where v is a commutator of Q, thus the commutator subgroup of $Q \times \mathbb{Z}$ is infinite, a contradiction. Also Q has infinitely many generators, let Y be the set of generators of Q then Y has infinitely many elements, as $\mathbb{Z}$ is generated by 1 it follows that the generators of $Q \times \mathbb{Z}$ are of the form $(v, 1)$ where $v \in Y$. Therefore there are infinitely many generators of $Q \times \mathbb{Z}$ since Q has infinitely many generators, contradicting that $Q \times \mathbb{Z}$ is a χ_0-group. Therefore Q is a χ_0-group. □

Theorem 3.6. *Suppose that Q is a group. Then $Q \times \mathbb{Z}$ is a χ_0-group if and only if Q is a χ_0-group.*

Proof. If $Q \times \mathbb{Z}$ is a χ_0-group then by Lemma 3.5 we have that Q is a χ_0-group.

Conversely, suppose that Q is a χ_0-group then $Q \times \mathbb{Z}$ is a χ_0-group by Lemma 3.4. □

The following property of χ_0-groups was given in [11].

Proposition 3.7. *Suppose that Q is a χ_0-group. If U is a group satisfying $U \times \mathbb{Z} \cong Q \times \mathbb{Z}$ then U is a χ_0-group.*

Proof. As Q is a χ_0-group we have $Q \times \mathbb{Z}$ is a χ_0-group by Lemma 3.4, since $U \times \mathbb{Z} \cong Q \times \mathbb{Z}$ then $U \times \mathbb{Z}$ is a χ_0-group thus by Lemma 3.5 we have that U is a χ_0-group. □

The notation presented below was introduced in [11].

Notation 3.8.

Let Q be a group and let $m(Q) = m_1 m_2 m_3$ where:

- $m_1 =$ exponent of T_Q,
- $m_2 =$ exponent of $Aut(T_Q)$,
- $m_3 =$ exponent of T_{Z_Q}.

Theorem 3.9. *Suppose that Q is a group.*

1. *If Q is trivial then $Aut(Q)$ is trivial.*
2. *If Q is a cyclic with $|Q| = 2$ then $Aut(Q)$ is trivial.*

Proof. 1. If Q is trivial then $Aut(Q)$ contains only the trivial automorphism hence $Aut(Q)$ is trivial.
2. Suppose that Q is cyclic with $|Q| = 2$. Let x be a generator of Q, that is, $Q = (x)$ so $x^2 = i_Q$ since the order of Q is 2. Let $\phi : Q \to Q$ be an automorphism, it follows that $\phi(x)$ is a generator of Q so $(\phi(x))^2 = i_Q$. Assume that $\phi(x) \neq x$. Then Q is generated by two elements x and $\phi(x)$ contradicting the assumption that Q is a cyclic group of order 2. Therefore $\phi(x) = x$, that is, ϕ is the identity map. Thus $Aut(Q)$ is trivial. □

Proposition 3.10. *Suppose that Q is any χ_0-group with $Z_Q = \{i_Q\}$ and $m = m(Q)$. If T_Q is cyclic with $|T_Q| = 2$ then $m = 2$.*

Proof. Since $Z_Q = \{i_Q\}$ then $T_{Z_Q} = \{i_Q\}$ thus the exponent of T_{Z_Q} is 1 so $m_3 = 1$. As T_Q is a cyclic with $|T_Q| = 2$ by Theorem 3.9 we have that $Aut(T_Q)$ is trivial so the exponent of $Aut(T_Q)$ is 1 hence $m_2 = 1$. Also as T_Q is a cyclic with $|T_Q| = 2$ we have that the exponent of T_Q is 2 so $m_1 = 2$. Therefore

$$m = m(Q) = m_1 m_2 m_3 = 2 \times 1 \times 1 = 2.$$

□

Lemma 3.11. *Suppose that a group Q is non-abelian. If Q is not trivial then $Aut(Q)$ is not trivial.*

Proof. Since Q is not trivial and non-abelian thus there exist $v \in Q$ with $v \neq i_Q$. We define $\phi_v : Q \to Q$ by $\phi_v(x) = vxv^{-1}$, that is, ϕ_v is the inner automorphism hence $\phi_v \in Inn(Q)$ giving that $|Inn(Q)| \geq 2$. As $Inn(Q) \leq Aut(Q)$ then $|Aut(Q)| \geq |Inn(Q)| \geq 2$ therefore $Aut(Q)$ is not trivial. □

Theorem 3.12. *If Q is a group with $|Q| \geq 3$ then $Aut(Q)$ is not trivial.*

Proof. If Q is not an abelian group and Q has order at least three then the result follows from Lemma 3.11. Assume that Q is abelian with $|Q| \geq 3$. Define a map $\phi : Q \to Q$ by $\phi(v) = v^{-1}$. We show that ϕ is an automorphism. Let $v, w \in Q$ then

$$v = w \Rightarrow vw^{-1} = i_Q \Rightarrow w^{-1} = v^{-1} \Rightarrow \phi(w) = \phi(v) \Rightarrow \phi(v) = \phi(w).$$

Therefore ϕ is well-defined. Now

$$Ker\,\phi = \{v \in Q : \phi(v) = i_Q\} = \{v \in Q : v^{-1} = i_Q\} = \{v \in Q : i_Q = v\} = \{i_Q\}$$

hence ϕ is one-to-one. Since Q is a group we have that for any $v^{-1} \in Q$ there is $v \in Q$ such that $\phi(v) = v^{-1}$ so ϕ is onto. Let $v, w \in Q$ then

$$\phi(vw) = (vw)^{-1} = w^{-1}v^{-1} = \phi(w)\phi(v) = \phi(v)\phi(w)$$

since Q is abelian, hence ϕ is a group homomorphism. Thus ϕ is an automorphism so $|Aut(Q)| \geq 2$, that is, $Aut(Q)$ is not trivial. □

Proposition 3.13. *Suppose that Q is a χ_0-group. If $m(Q)$ is prime then $m(Q) = 2$.*

Proof. Suppose that p is is an odd prime and $m(Q) = p$. We consider three cases:

Case 1

Assume that $m_1 = p$ and $m_2 = m_3 = 1$. Since T_Q is not trivial it follows that $Aut(T_Q)$ is not trivial by Theorem 3.12, therefore $m_2 \neq 1$ contradicting the assumption that $m_2 = 1$ so $m(Q) \neq p$. *Case 2*

Assume that $m_3 = p$ and $m_1 = m_2 = 1$. Since $m_3 = p$ we have that T_{z_Q} is not trivial therefore there exist $z \in T_{z_Q}$ such that $|z|$ is finite thus $z \in T_Q$ which implies that T_Q is not trivial so $m_1 \neq 1$ contradicting the assumption that $m_1 = 1$ thus $m(Q) \neq p$.

Case 3

Assume that $m_2 = p$ and $m_1 = m_3 = 1$. Since $m_1 = 1$ so T_Q is trivial then $Aut(T_Q)$ is trivial. Therefore the exponent of $Aut(T_Q)$ is 1, that is, $m_2 = 1$ contradicting the assuption that $m_2 = p$ thus $m(Q) \neq p$. □

For any infinite χ_0-group Q, the following proposition guarantees existence of a subgroup W of Q of index n for any natural number n.

Proposition 3.14 ([11], Proposition 2.5). *Let $n \in \mathbb{N}$. If Q is any infinite χ_0-group then there exist $W \leq Q$ with $[Q : W] = n$.*

3.2 Subgroups of finite index

The author in [11] showed that for any χ_0-group Q the classes in $\chi(Q)$ are represented by the subgroups U of Q with $[Q : U]$ finite and $gcd([Q : U], m) = 1$ where $m = m(Q)$. In this section we study these subgroups in detail. First we give a formal definition of a non-cancellation set.

Definition 3.15.

We define the ***non-cancellation set*** of a group Q, denoted by $\chi(Q)$, to be the set of all isomorphism classes of groups U satisfying $U \times \mathbb{Z} \cong Q \times \mathbb{Z}$. A non-cancellation set is said to be trivial if it contains a single isomorphism class.

Note 3.16.

For a finite group Q we have that $\chi(Q)$ is trivial, hence in our study we consider infinite χ_0-groups.

For any χ_0-group Q, the following result guarantees that if $U \leq Q$ with $[Q : U]$ finite and $gcd([Q : U], m) = 1$ where $m = m(Q)$ satisfies $U \times \mathbb{Z} \cong Q \times \mathbb{Z}$.

Theorem 3.17 ([11], Theorem 4.1). *Suppose that Q is any χ_0-group. If U is a subgroup of Q with $[Q : U]$ finite and $gcd([Q : U], m) = 1$ where $m = m(Q)$. Then $U \times \mathbb{Z} \cong Q \times \mathbb{Z}$.*

For any χ_0-group Q, the next result shows that any group U satisfying $U \times \mathbb{Z} \cong Q \times \mathbb{Z}$ is isomorphic to some subgroup of Q of finite index.

Theorem 3.18 ([11], Theorem 4.2). *Suppose that Q is any χ_0-group and $m = m(Q)$. If U is any group satisfying $U \times \mathbb{Z} \cong Q \times \mathbb{Z}$, then $U \cong W$ where $W \leq G$ with $[Q : W]$ finite and $gcd([Q : W], m) = 1$.*

Let U and W be subgroups of a χ_0-group Q of finite index. The next result gives the isomorphism classes of subgroups U of Q such that $Q \times \mathbb{Z} \cong U \times \mathbb{Z}$.

Theorem 3.19 ([11], Theorem 4.3). *Suppose that Q is any χ_0-group and $m = m(Q)$. Let $U \leq Q$ and $W \leq Q$ such that $[Q : U]$ and $[Q : W]$ are both finite. If $gcd([Q : U], m) = 1$ and $[Q : W] \equiv \pm[Q : U] \, mod \, m$ then $U \cong W$.*

Theorem 3.20 ([11], Theorem 4.4). *Suppose that Q is any χ_0-group and $m = m(Q)$. Let U be a subgroup of Q such that $[Q : U]$ is finite. If $gcd([Q : U], m) = 1$ then there is a mapping $\kappa : Q \to U$ such that $[Q : U][U : Im\,\kappa] = \pm 1 \, mod \, m$.*

3.3 Group structure of non-cancellation sets

Let Q be a χ_0-group and let $m = m(Q)$. The author in [11] deduced that the group structure on $\mathbb{Z}_m^*/\{1, -1\}$ induces a group structure on the non-cancellation set $\chi(Q)$. We study these results and give the order of $\chi(Q)$ for certain χ_0-groups in this section. First we consider non-cancellation sets of abelian χ_0-groups.

Let A be an abelian χ_0-group. In Theorem 3.29 we show that $\chi(A)$ is trivial. We first give results which are needed in the proof of Theorem 3.29.

Note 3.21.

The direct product $\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ is a finitely generated group with a finite commutator subgroup. That is, $\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ is a χ_0-group, we write $\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z} = \mathbb{Z}^t$ if we have t copies of $\mathbb{Z}$.

Lemma 3.22 ([6], Lemma 1). *Suppose that R and S are any groups. If $R \times \mathbb{Z} \cong S \times \mathbb{Z} \times \mathbb{Z}$ then $R \cong S \times \mathbb{Z}$.*

Theorem 3.23. *Let $Q = \mathbb{Z}^r$ for some $r \geq 0$. Suppose that V is a group satisfying $Q \times \mathbb{Z} \cong V \times \mathbb{Z}$. Then $Q \cong V$.*

Proof. We have that $V \times \mathbb{Z} \cong Q \times \mathbb{Z}$ then

$$V \times \mathbb{Z} \cong \mathbb{Z}^r \times \mathbb{Z} \Rightarrow V \times \mathbb{Z} \cong \mathbb{Z}^{r-1} \times \mathbb{Z} \times \mathbb{Z}$$

thus $V \cong \mathbb{Z}^{r-1} \times \mathbb{Z}$ by Lemma 3.22. Hence $V \cong \mathbb{Z}^r = Q$ giving that $V \cong Q$. □

Remark 3.24.

Let $Q = \mathbb{Z}^r$ for some $r \geq 0$. From Theorem 3.23 we have that any group U satisfying $Q \times \mathbb{Z} \cong U \times \mathbb{Z}$ is isomorphic to Q. Hence all isomorphism classes in $\chi(Q)$ are represented by $[Q]$, that is, $\chi(Q)$ contains a single element therefore $\chi(Q)$ is trivial.

Theorem 3.25 ([1], Theorem 11.1). **(Fundamental Theorem of Finite Abelian Groups).** Suppose that A is a finite abelian group. Then

$$A \cong \mathbb{Z}_{p^{n_1}} \times \cdots \times \mathbb{Z}_{p^{n_s}}$$

where p is prime and $n_i \in \mathbb{Z}$, $i = 1, \ldots, s$. Furthermore, the group A uniquely determines the number of terms and orders of the cyclic groups.

Theorem 3.26 ([8], Theorem 9.27). **(Fundamental Theorem of Finitely Generated Abelian Groups).** Suppose that A is a finitely generated abelian group. Then

$$A \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s}$$

where r is a positive integer and $n_1 \geq n_2 \geq \cdots \geq n_s \geq 2$ with $r \geq 2$ and $n_{i+1}|n_1$. Furthermore, this expression is unique.

Corollary 3.27. *Suppose that A is a finitely generated abelian group then $A \cong \mathbb{Z}^r \times T_A$ for some $r \geq 0$. Moreover, T_A is a finite abelian group and it is isomorphic to a direct product of cyclic groups.*

Corollary 3.28 ([11], Corollary 6.3). *If R and S are any χ_0-groups with R infinite and $\chi(R)$ trivial, then $\chi(R \times S)$ is trivial.*

Theorem 3.29. *If A is an abelian χ_0-group then $\chi(A)$ is trivial.*

Proof. Since A is an abelian χ_0-group, we have that A is a finitely generated abelian group. Then $A \cong \mathbb{Z}^r \times T_A$ for some $r \geq 0$ by Corollary 3.27. Now $\mathbb{Z}^r$ is an infinite χ_0-group and $\chi(\mathbb{Z}^r)$ is trivial. From Corollary 3.28 it follows that $\chi(\mathbb{Z}^r \times T_A)$ is trivial therefore $\chi(A)$ is trivial which completes the proof. □

The next result shows that any χ_0-group with a trivial torsion subgroup has a trivial non-cancellation set.

Theorem 3.30. *Suppose that Q is any χ_0-group and $m = m(Q)$. If T_Q is trivial then $\chi(Q)$ is trivial.*

Proof. Given that T_Q is trivial then the exponent of T_Q is 1, that is, $m_1 = 1$. As T_Q is trivial it follows that $Aut(T_Q)$ is trivial so the exponent of $Aut(T_Q)$ is 1 hence $m_2 = 1$. We know that $Z_Q \leq Q$, since Q is torsionfree it follows that Z_Q is also torsionfree hence T_{Z_Q} is trivial, giving that the exponent of T_{Z_Q} is 1 thus $m_3 = 1$. Now

$$m = m(Q) = m_1 m_2 m_3 = 1 \times 1 \times 1 = 1.$$

From Theorem 3.17, 3.18 and 3.19 we have that each class in $\chi(Q)$ is represented by $U \leq Q$ such that $gcd([Q : U], m) = 1$. Since $m = 1$ we get that $gcd([Q : U], 1) = 1$ so $[Q : U] = 1$ hence $Q = U$ for any $U \leq Q$ satisfying $gcd([Q : U], m) = 1$. Thus $\chi(Q) = \{[Q]\}$, that is, $\chi(Q)$ is trivial. □

In Theorem 3.30 we have shown that any χ_0-group Q with a trivial torsion subgroup has a trivial non-cancellation set $\chi(Q)$, that is, torsionfree groups have a trivial non-cancellation set. Going forward we assume that the torsion subgroup is non-trivial.

Note 3.31.

Recall that $\mathbb{Z}_m \cong \mathbb{Z}/m\mathbb{Z}$ for some $m \in \mathbb{Z}$. If $m = 1$ then $\mathbb{Z}_1 \cong \mathbb{Z}/\mathbb{Z}$ which implies that $\mathbb{Z}_1 \cong \mathbb{Z}$. Hence we denote by $\mathbb{Z}_m$ the group of integers modulo m with $m \geq 2$.

Let $[\bullet]$ denote an isomorphism class and denote by Y the set of positive integers n such that $gcd(n, m) = 1$ where $m = m(Q)$. A well-defined surjective mapping $\nu : Y \to \chi(Q)$ defined by $\nu(x) = [U]$ where $U \leq Q$ with $[Q : U] = |x|$ can be defined from Theorem 3.17, 3.18 and 3.19. Using the "reduction mod m"-function the map ν can be factorized to

$$\psi : Y \to \mathbb{Z}_m^*/\{1, -1\}.$$

Define $\phi : \mathbb{Z}_m^*/\{1, -1\} \to \chi(Q)$ to be the unique mapping such that $\psi \circ \phi = \nu$.

Theorem 3.32 ([11], Theorem 5.1). *(a) Let $\phi^{-1}[Q]$ denote the fibre of ϕ over $[Q]$. Then $\phi^{-1}[Q] \leq \mathbb{Z}_m^*/\{1, -1\}$.*
(b) If $[U]$ is any element of $\chi(Q)$ then $\phi^{-1}[U]$ is a coset of $\phi^{-1}[Q]$.

Proof. (a) From Theorem 3.20 we have that for $y \in \phi^{-1}[Q]$ there is $v^{-1} \in \phi^{-1}[Q]$. Hence the fibre contains all the inverses of its elements. Suppose that $y, z \in Y$ and $\delta_1 : Q \to Q$ and $\delta_2 : Q \to Q$ so that $[Q : \delta_1(Q)] = y$ and $[Q : \delta_2(Q)] = z$ thus $[Q : \delta_2 \circ \delta_1(Q)] = yz$ which gives that $\phi^{-1}[Q]$ is closed. As $y, y^{-1} \in \phi^{-1}[Q]$ we have that $1 = yy^{-1} \in \phi^{-1}[Q]$ so $\phi^{-1}[Q]$ has an identity element. Associativity is inherited from $\mathbb{Z}^*_m/\{1,-1\}$ therefore $\phi^{-1}[Q]$ is a subgroup of $\mathbb{Z}^*_m/\{1,-1\}$.
(b) Let $y, z, c \in Y$ such that $\nu(z) = \nu(c)$ and let $W \leq Q$ with $[Q : W] = z$. Then there is a mapping $\alpha : W \to Q$ so that $[Q : \alpha(W)] = c$. Let $V \leq W$ so that $[W : V] = y$ then $[Q : V] = [W : V][Q : W] = yz$ giving that $[V] = \nu(yz)$. Since $\alpha(V) \leq \alpha(W)$ we have that $[Q : \alpha(V)] = [\alpha(W) : \alpha(V)][Q : \alpha(W)] = yc$ giving that $[V] = \nu(yc)$. Hence $\nu(z) = \nu(c)$ implies that $\nu(yz) = \nu(yc)$. The result follows from the latter part. □

Note 3.33.

As a consequence of Theorem 3.32 we have the following bijection

$$\Phi : (\mathbb{Z}^*_m/\{1,-1\})/(\phi^{-1}[Q]) \to \chi(Q)$$

so that we have a canonical epimorphism of semigroups

$$\beta : \mathbb{Z}^*_m/\{1,-1\} \to (\mathbb{Z}^*_m/\{1,-1\})/(\phi^{-1}[Q])$$

such that $\phi = \Phi \circ \beta$.
In order for us to impose a group structure on $\chi(Q)$ we use Φ.

Theorem 3.34 ([11], Theorem 5.2). *Suppose that Q is any χ_0-group. Then a group structure on $\chi(Q)$ is induced by the map $\phi : \mathbb{Z}^*_m/\{1,-1\} \to \chi(Q)$ where $m = m(Q)$. If Q is nilpotent then $\chi(Q)$ is the same as the Hilton-Mislin genus group.*

Note 3.35.

In the group $\mathbb{Z}^*_m/\{1,-1\}$ we have that $a \in \mathbb{Z}^*_m$ and its additive inverse $-a$ belong to the same class in $\mathbb{Z}^*_m/\{1,-1\}$, that is, $a\{1,-1\} = \{a,-a\} \in \mathbb{Z}^*_m/\{1,-1\}$.

Remark 3.36.

Suppose that Q is any χ_0-group and $m = m(Q)$. Define a map $\mu : \mathbb{Z}^*_m \to \chi(Q)$ by $\mu(v) = [U]$ where $U \leq Q$ such that $[Q : U] = v$. We show that μ is a well-defined surjective map. Suppose that $b, b_1 \in \mathbb{Z}^*_m$ such that $b = b_1$ then there are subgroups

B and B_1 with $[Q : B] = b$ and $[Q : B_1] = b_1$. Hence $[Q : B] = [Q : B_1]$ as $[Q : B] \equiv [Q : B] \bmod m$ then $[Q : B] \equiv [Q : B_1] \bmod m$ giving that $B \cong B_1$ by Theorem 3.19. It follows that $[B] = [B_1]$ since B and B_1 belong to the same isomorphism class thus $b = b_1$ implies $\mu(b) = \mu(b_1)$. Thus μ is well-defined. Also for any $[U]$ where $U \leq Q$ there is $v \in \mathbb{Z}_m^*$ such that $\mu(v) = [U]$ with $[Q : U] = a$. Therefore μ is a well-defined surjective map.

Moreover, if $y, z \in \mathbb{Z}_m^*$ then $\mu(yz) = [V]$ where $V \leq Q$ such that $[Q : V] = yz$. Note that $gcd(yz, m) = 1$ then $gcd(y, m) = 1$ and $gcd(z, m) = 1$. Then the are subgroups U_1 and U_2 such that $[Q : U_1] = y$ and $[Q : U_2] = z$ respectively. Giving that $[Q : V] = [Q : U_1][Q : U_2]$ therefore

$$\mu(yz) = [V] = [U_1][U_2] = \mu(y)\mu(z).$$

Thus μ is a homomorphism.

Suppose that Q is any χ_0-group and $m = m(Q)$. The group structure on $\chi(Q)$ is imposed by the map

$$\Phi : (\mathbb{Z}_m^*/\{1, -1\})/\phi^{-1}[Q] \to \chi(Q).$$

Note that $\mathbb{Z}_m^*/\{1, -1\}$ is not isomorphic to $\chi(Q)$ in general, that is, the map $\phi : \mathbb{Z}_m^*/\{1, -1\} \to \chi(Q)$ is not an isomorphism in general. In the next result we show that $\phi : \mathbb{Z}_m^*/\{1, -1\} \to \chi(Q)$ is an isomorphism if isomorphic subgroups of Q are conjugate.

Proposition 3.37. *Let Q be any χ_0-group and let $m = m(Q)$. If isomorphic subgroups of Q are conjugate then the mapping*

$$\phi : \mathbb{Z}_m^*/\{1, -1\} \to \chi(Q)$$

is an isomorphism.

Proof. In order to show that $\phi : \mathbb{Z}_m^*/\{1, -1\} \to \chi(Q)$ is an isomorphism, we show that $\mathbb{Z}_m^*/\{1, -1\} \cong \chi(Q)$. We know that there exist a surjective group homomorphism $\mu : \mathbb{Z}_m^* \to \chi(Q)$ defined by $\mu(v) = [U]$ where $U \leq Q$ with $[Q : U] = v$. Now

$$Ker\,\mu = \{v \in \mathbb{Z}_m^* \mid \mu(v) = i_{\chi(Q)}\} = \{v \in \mathbb{Z}_m^* \mid [U] = [Q]\}.$$

As $U \leq Q$ such that $[Q : U] = v$ and we have that $[U] = [Q]$ hence U and Q belong to the same isomorphism class giving that $U \cong Q$. Since isomorphic subgroups of Q are conjugate, it follows that U is conjugate to Q. Therefore $[Q : U] = [Q : Q] = 1$ then $1 = [Q : U] = v$ thus $v = 1$. From Theorem 3.19 we get that U is isomorphic to any subgroup W of Q with $[Q : W] \equiv \pm[Q : U] \bmod m$ so $[Q : W] \equiv \pm 1 \bmod m$. Giving that $Ker\, \mu$ contains 1 and -1, that is, $Ker\, \mu = \{1, -1\}$. Hence $\mathbb{Z}^*_m/\{1, -1\} \cong \chi(Q)$ by the First Isomorphism Theorem, since ϕ is a unique map hence

$$\phi : \mathbb{Z}^*_m/\{1, -1\} \to \chi(Q)$$

is an isomorphism. □

Recall that the map

$$\Phi : (\mathbb{Z}^*_m/\{1, -1\})/\phi^{-1}[Q] \to \chi(Q)$$

induces a group structure on $\chi(Q)$. In the next result we show that for a χ_0-group Q such that isomorphic subgroups of Q are conjugate then $\phi^{-1}[Q]$ is trivial, that is, $\phi^{-1}[Q] = \{\{1, -1\}\}$.

Corollary 3.38. *Suppose that Q is any χ_0-group and $m = m(Q)$. If isomorphic subgroups of Q are conjugate then $\phi^{-1}[Q] = \{\{1, -1\}\}$.*

Proof. Note that $\phi^{-1}[Q] \leq \mathbb{Z}^*_m/\{1, -1\}$. We need to show that $\phi^{-1}[Q] \subseteq \{\{1, -1\}\}$ and $\{\{1, -1\}\} \subseteq \phi^{-1}[Q]$. First we show that $\phi^{-1}[G] \subseteq \{\{1, -1\}\}$. Let $a\{1, -1\}$ be an arbitrary element of $\phi^{-1}[Q]$ and $a \in \mathbb{Z}^*_m$. We show that $a = 1$. As $a \in \mathbb{Z}^*_m$ there is $U \leq Q$ such that $[Q : U] = a$ but $a\{1, -1\} \in \phi^{-1}[Q]$ hence $U \cong Q$. Since isomorphic subgroups of Q are conjugate, then U is conjugate to Q therefore $a = [Q : U] = [Q : Q] = 1$ so $a = 1$. As $a\{1, -1\}$ was an arbitrary element of $\phi^{-1}[Q]$ we have that $\{a\{1, -1\}\} = \{\{1, -1\}\}$. Therefore $\phi^{-1}[Q] \subseteq \{\{1, -1\}\}$. Now we show that $\{\{1, -1\}\} \subseteq \phi^{-1}[Q]$. We know that $\phi : \mathbb{Z}^*_m/\{1, -1\} \to \chi(Q)$ is an isomorphism hence $\phi(\{1, -1\}) = [Q]$ also $[Q : Q] = 1$. Hence $\{1, -1\} \in \phi^{-1}[Q]$ giving that $\{\{1, -1\}\} \subseteq \phi^{-1}[Q]$. Thus $\phi^{-1}[Q] = \{\{1, -1\}\}$. □

Remark 3.39.

Suppose that Q is any χ_0-group and $m = m(Q)$. From Theorems 3.17, 3.18 and

3.19 we have that the non-cancellation set of Q is given by

$$\chi(Q) = \{[U] : [Q : U] < \infty,\ gcd([Q : U], m) = 1\}.$$

From Theorem 3.34 we have that $\chi(Q)$ has an abelian group structure.

Suppose that Q is a χ_0-group such that any isomorphic subgroups of Q are conjugate. In the following result we show that, if T_Q is cyclic with $|T_Q| = 2$ and the centre of Q is trivial then $\chi(Q)$ is trivial.

Corollary 3.40. *Suppose that Q is any χ_0-group with $Z_Q = \{i_Q\}$ and $m = m(Q)$. If isomorphic subgroups of Q are conjugate and T_Q is cyclic with $|T_Q| = 2$, then $\chi(Q)$ is trivial.*

Proof. Given that $Z_Q = \{i_Q\}$ and T_Q is cyclic with $|T_Q| = 2$ then $m = m(G) = 2$ by Proposition 3.10. From Proposition 3.37 we get that $\phi : \mathbb{Z}_2^*/\{1, -1\} \to \chi(Q)$ is an isomorphism. Now $\mathbb{Z}_2^* = \{1\}$ and $\{1, -1\} = \{1\}$. Hence

$$\mathbb{Z}_2^*/\{1, -1\} = \{1\}/\{1\} = \{1\}$$

thus

$$\{1\} \cong \chi(Q)$$

so $\chi(Q)$ is trivial. □

Suppose that Q is a χ_0-groups such that isomorphic subgroups of Q are conjugate. In Corollary 3.40 we have shown that if Q has a trivial centre and T_Q is cyclic with $|T_Q| = 2$ then the non-cancellation set is trivial. The following result determines the order of $\chi(Q)$ of a χ_0-group Q such that isomorphic subgroups of Q are conjugate with $m(Q) \geq 3$.

Proposition 3.41. *Suppose that Q is any χ_0-group. If isomorphic subgroups of Q are conjugate then*

$$|\chi(Q)| = \frac{\varphi(m)}{2}$$

where $m = m(Q) \geq 3$.

Proof. We know that there is an isomorphism $\phi : \mathbb{Z}^*_m/\{1,-1\} \to \chi(Q)$ then $|\mathbb{Z}^*_m/\{1,-1\}| = |\chi(Q)|$ since ϕ is a bijection. Now $\mathbb{Z}^*_m$ is finite so we apply Theorem 2.22 to get

$$|\mathbb{Z}^*_m/\{1,-1\}| = [\mathbb{Z}^*_m : \{1,-1\}] = \frac{|\mathbb{Z}^*_m|}{|\{1,-1\}|} = \frac{\varphi(m)}{2}$$

so

$$|\chi(Q)| = |\mathbb{Z}^*_m/\{1,-1\}| = \frac{\varphi(m)}{2}.$$

□

In Theorem 3.42 we generalize Corollary 3.40.

Theorem 3.42. *Suppose that Q is any χ_0-group and $m = m(Q)$. If isomorphic subgroups of Q are conjugate and T_Q is cyclic with $|T_Q| = 2$ then $\chi(Q)$ is trivial.*

Proof. Note that $|T_Q| = 2$ implies that T_Q contains two elements, that is, the identity i_Q and an element, say x, such that $x^2 = i_Q$. If $Z_Q = \{i_Q\}$ and we are given that T_Q is cyclic with $|T_Q| = 2$ then $\chi(Q)$ is trivial by Corollary 3.40. Suppose that Z_Q is not trivial. We consider two cases:

Case 1

If Z_Q is torsionfree then Z_Q contains only the trivial torsion element so T_{Z_Q} is trivial giving that the exponent of T_{Z_Q} is 1 so $m_3 = 1$. Also T_Q is cyclic with $|T_Q| = 2$ then $Aut(T_Q)$ is trivial so the exponent of $Aut(T_Q)$ is 1 so $m_2 = 1$. Since T_Q is cyclic with $|T_Q| = 2$ then the exponent of T_Q is 2 so $m_1 = 2$ giving that

$$m = m(Q) = m_1 m_2 m_3 = 2 \times 1 \times 1 = 2.$$

It follows from Proposition 3.37 that $\phi : \mathbb{Z}^*_2/\{1,-1\} \to \chi(Q)$ is an isomorphism. Now $\mathbb{Z}^*_2 = \{1\}$ and $\{1,-1\} = \{1\}$ hence

$$\mathbb{Z}^*_2/\{1,-1\} = \{1\}/\{1\} = \{1\}$$

thus

$$\{1\} \cong \chi(Q)$$

so $\chi(Q)$ is trivial.

Case 2

If Z_Q contains a non-trivial torsion element then $T_{Z_Q} = T_Q$ since there are only two torsion elements. Hence T_{Z_Q} is a cyclic group of order 2 thus the exponent of T_{Z_Q} is 2 so $m_3 = 2$. Also T_Q is a cyclic group of order 2 so $Aut(T_Q)$ is trivial hence the exponent of $Aut(T_Q)$ is 1 so $m_2 = 1$ and $m_1 = 2$ since T_Q is cyclic with $|T_Q| = 2$ therefore

$$m = m(Q) = m_1 m_2 m_3 = 2 \times 1 \times 2 = 4.$$

From Proposition 3.41 we have

$$|\chi(Q)| = \frac{\varphi(m)}{2} = \frac{\varphi(4)}{2} = \frac{2}{2} = 1$$

therefore $\chi(Q)$ is trivial. $\square$

Chapter 4

χ_0-groups with additional properties

In this chapter we study χ_0-groups with additional properties and deduce whether these additional properties have an effect on the group structure of the non-cancellation set of a χ_0-group.

Property 4.1.

Let Q be any χ_0-group such that any subgroups of Q with the same index are conjugate.

Theorem 4.2. *Suppose that Q is any finitely generated group and $n \in \mathbb{N}$. Then there exists finitely many subgroups with finite index n.*

Proof. Suppose that U is a subgroup of Q with $[Q : U] = n$. Then there is an action of Q on Y where Y is the set of left cosets of U. This action corresponds to the homomorphism from Q to the permutation group S_n that is transitive. Furthermore, since $Stab_Q(U) = U$ so U is recovered as a subgroup of the coset U. There are only finitely many homomorphisms from Q to S_n which are transitive since Q is finitely generated. Hence there are finitely many possibilities for U. □

Corollary 4.3. *Suppose that Q is any χ_0-group with Property 4.1. Let $U \leq Q$ with $[Q : U] = m$ where $m \in \mathbb{N}$. Then there are finitely many subgroups of Q conjugate to U.*

Proof. Let U be a subgroup of Q such that $[Q : U] = m$. Then by Theorem 4.2, there are finitely many subgroups of finite index m. Since Q has Property 4.1 we have that all subgroups of Q of index m are conjugate to U. As there are finitely many subgroups of finite index m. It follows that Q has finitely many subgroups which are conjugate to U. □

Notation 4.4.

Denote by $\mathcal{F}$ the set of all isomorphism classes of subgroups of a group Q of the same finite index. That is, $\mathcal{F}$ contains all classes $[U]$ with$[Q : U]$ finite.

Theorem 4.5. *Suppose that Q is any χ_0-group with Property 4.1. If U and V are subgroups of Q of the same index. Then $U \cong V$.*

Proof. Since U and V have the same index and Q has Property 4.1 we have that U is conjugate to V so $U \cong V$. □

Remark 4.6.

Let Q be any χ_0-group with Property 4.1 and let $m = m(Q)$. From Theorem 3.17 we have that $\chi(Q)$ contains all classes $[U]$ where $U \leq Q$ with $gcd([Q : U], m) = 1$. From Theorem 3.18 we have that any group V satisfying $V \times \mathbb{Z} \cong Q \times \mathbb{Z}$ is isomorphic to some subgroup of Q with finite index relatively prime to m. Finally, from Theorem 4.5 we have that all subgroups of the same index are isomorphic. Each class in $\chi(Q)$ is represented by a subgroup U of Q with $[Q : U]$ finite and $gcd([Q : U], m) = 1$. Hence $\chi(Q) \subseteq \mathcal{F}$. However, we can define a map $\delta : \mathcal{F} \to \chi(Q)$ by

$$\begin{cases} \delta([U]) = [U] & \text{if } gcd([Q : U], m) = 1 \\ \delta([U]) = [Q] & \text{if } gcd([Q : U], m) \neq 1 \end{cases}$$

this is a surjective map between $\mathcal{F}$ and $\chi(Q)$.

Example 4.7.

Suppose that Q is an infinite χ_0-group and $m = m(Q)$. From Proposition 3.14 we have that for any $n \in \mathbb{N}$ there exist a subgroup V of Q with $[Q : V] = n$. Thus there is a bijection $\mu : \mathbb{N} \to \mathcal{F}$ giving that $|\mathcal{F}| = |\mathbb{N}|$. Consider $U \leq Q$ with $[Q : U]$ finite then $[U] \in \mathcal{F}$ but $[U] \in \chi(Q)$ if $gcd([Q : U], m) = 1$ then $|\chi(Q)| \leq |\mathcal{F}|$.

Property 4.8.

Let Q be a χ_0-group such that any isomorphic subgroups of Q are conjugate.

Proposition 4.9. *Suppose that Q is any χ_0-group with Property 4.8 and $m = m(Q)$. Let $U \leq Q$ with $[Q : U]$ finite. If there is $V \leq Q$ with $[Q : V]$ finite and $gcd([Q : V], M) = 1$ such that $[Q : U] = \pm[Q : V] \bmod m$ then U is conjugate to V.*

Proof. Let $U \leq Q$ with $[Q : U]$ finite. If we have a subgroup V of Q of finite index with $gcd([Q : V], m) = 1$ such that $[Q : U] \equiv \pm[Q : V] \bmod m$, then U is isomorphic to V by Theorem 3.19. As Q has Property 4.8 it follows that U is conjugate to V. $\square$

Note 4.10.

Suppose that Q is a χ_0-group with Property 4.8 and $m = m(Q)$. Since $\chi(Q)$ contains all isomorphism classes $[U]$ where $U \leq Q$ with $[Q : U]$ finite and $gcd([Q : U], m) = 1$. As all subgroups isomorphic to U are represented in the class $[U]$, it follows that all subgroups represented by the class $[U]$ are conjugate to U as Q has Property 4.8.

Remark 4.11.

Let Q be a χ_0-group with Property 4.8. Let

$$Y = \{U : U \leq Q,\ [Q : U] < \infty,\ gcd([Q : U], m) = 1\}$$

where $m = m(Q)$ and define an action $* : Q \times Y \to Y$ by $v * U = vUv^{-1}$. As Q has Property 4.8 we have that if U is isomorphic to V then U is conjugate to V hence $Orb(U) = Orb(V)$. Thus we have that

$$\{Orb(U) : [Q : U] < \infty,\ gcd([Q : U], m) = 1\} = \chi(Q).$$

Theorem 4.12. *Suppose that Q is a χ_0-group with Property 4.8. Let*

$$Y = \{U : U \leq Q,\ [Q : U],\ gcd([Q : U], m) = 1\}$$

where $m = m(Q)$ and define an action $* : Q \times Y \to Y$ by $v * U = vUv^{-1}$. If the action $*$ is transitive then $\chi(Q)$ is trivial.

Proof. Since the action $*$ is transitive we have that there is only one orbit. Hence the group

$$\chi(Q) = \{Orb(U) : [Q : U] < \infty,\ gcd([Q : U], m) = 1\}$$

contains a single element therefore $|\chi(Q)| = 1$ giving that $\chi(Q)$ is trivial. $\square$

Note 4.13.

Suppose that Q is any χ_0-group with Property 4.8. Let

$$Y = \{U : U \leq Q, [Q : U] < \infty,\ gcd([Q : U], m) = 1\}$$

where $m = m(Q)$ and define an action $* : Q \times Y \to Y$ by $v * U = vUv^{-1}$. If subgroups U of Q with $[Q : U]$ and $gcd([Q : U], m) = 1$ are conjugate, that is, all the elements of Y are conjugate then the action $*$ is transitive. It follows that the action $*$ has a single orbit therefore

$$\chi(Q) = \{Orb(U) : [Q : U] < \infty,\ gcd([Q : U], m) = 1\} = \{Orb(U)\}$$

thus $\chi(Q)$ is trivial.

Remark 4.14.

Suppose that Q is any χ_0-group with Property 4.8. Let

$$Y = \{U : U \leq Q, [Q : U] < \infty,\ gcd([Q : U], m) = 1\}$$

where $m = m(Q)$ and define an action $* : Q \times Y \to Y$ by $v * U = vUv^{-1}$. We have given an alternative description of the non-cancellation set $\chi(Q)$, in which the classes in $\chi(Q)$ are the orbits of the action described above. From Proposition 3.41 we have that for a χ_0-group Q with Property 4.8 we have $\frac{|\varphi(m)|}{2}$. Thus the number of orbits of the action $*$ described above is given by $\frac{|\varphi(m)|}{2}$.

Chapter 5

Conclusion and Further work

Suppose that Q is a χ_0-group with $m = m(Q)$. Then a group structure on the non-cancellation set $\chi(Q)$ is induced by the group $\mathbb{Z}_m^*/\{1, -1\}$, see [11]. We have studied these results in Chapter 3. In Chapter 3 we made the following contributions

- Theorem 3.29 in which we have shown that for any abelian χ_0-group the non-cancellation set is trivial.
- Theorem 3.30 where we have shown that the non-cancellation set of a torsion-free χ_0-group is trivial.

In Chapter 3 we also consider χ_0-group with the property that any isomorphic subgroups are conjugate, that is, Property 4.8. We obtained the following results:

- Proposition 3.37 we showed that if a χ_0-group has Property 4.8 then the map $\phi : \mathbb{Z}_m^*/\{1, -1\} \to \chi(Q)$ is an isomorphism.
- Corollary 3.40 we showed that any χ_0-group with Property 4.8 which has a trivial centre and a cyclic torsion subgroup of order 2 then the non-cancellation set is trivial. In Theorem 3.42 we gave a more general version of this result.
- Proposition 3.41 we give a computation of the order of non-cancellation sets of χ_0-groups with Property 4.8.

We have given two cases (Theorem 3.30 and Theorem 3.42) in which we considered the group structure of the torsion subgroup of a χ_0-group. Given more time we can attempt to generalize Theorem 3.42. That is, consider all χ_0-groups instead of concentrating only on χ_0-groups with Property 4.8. Then we can study the effect of the group structure of the torsion subgroup of a χ_0-group Q on the group structure of the non-cancellation set $\chi(Q)$.

Suppose that Q is any χ_0-group with Property 4.8, we have shown that $\chi(Q)$ is isomorphic to $\mathbb{Z}_m^*/\{1,-1\}$, that is, the group structure of $\chi(Q)$ is the same as the group structure of $\mathbb{Z}_m^*/\{1,-1\}$. From this result we have also deduced that for a χ_0-group Q with Property 4.8 has $|\chi(Q)| = \frac{\varphi(m)}{2}$ where $m = m(Q)$. Note that in this work we have only managed to compute the order of non-cancellation sets of χ_0-groups with Property 4.8. It would be interesting to determine the order of non-cancellation sets of any χ_0-group. That is, does Proposition 3.41 hold in general, if not then what is the order of non-cancellation sets of χ_0-groups without Property 4.8?

In Chapter 4 we considered χ_0-groups Q with additional properties. First we considered χ_0-groups with Property 4.1. From our study, we can conclude that the group structure of $\chi(Q)$ is exactly the same as the group structure of $\chi(Q)$ described by Witbooi in [11].

We also studied χ_0-groups with Property 4.8. Suppose that Q is any χ_0-group with Property 4.8 and $m = m(Q)$. Let

$$Y = \{U : U \leq Q, [Q : U] < \infty,\ gcd([Q : U], m) = 1\}$$

and define an action $* : Q \times Y \to Y$ by $v * U = vUv^{-1}$. We have given an alternative description of the classes in $\chi(Q)$, that is, for a χ_0-group Q with Property 4.8 the classes in $\chi(Q)$ are the orbits of the action $*$ described above. Therefore, $\frac{\varphi(m)}{2}$ is the number of orbits of the action $*$ described above. To take our work a step further we can consider a general χ_0-group then describe an action $*$ in which the classes in $\chi(Q)$ are the orbits of this action.

Bibliography

[1] J. Gallian, *Contemporary abstract algebra*, Ninth edition, Cengage Learning, United States of America, 2013, pg. 212.

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

[3] P. Hilton and D. Scevenels, *Calculating the genus of a direct product of certain nilpotent groups*, Publ. Mat. **39** (1995), 241–261.

[4] P. Hilton and C. Schuck, *Calculating the Mislin genus of nilpotent groups*, Bol. Soc. Mexicana (2) **37**, 263-269.

[5] P. Hilton and P. Witbooi, *Morphism of Mislin genera induced by finite normal subgroups*, Int. J. Math. Sci. **32** (2002) no. 5, 281-284.

[6] R. Hirshon, Some cancellation theorems with applications to nilpotent groups, J Austral . Ž. Math. Soc. Ser. A **23** (1977), 147-165.

[7] 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.

[8] J. Rotman, *The Theory of Groups*, Allyn and Bacon, Inc., Boston, 1973, pg. 193.

[9] D. Scevenels and P. Witbooi, *Non-cancellation and Mislin genus of certain groups and H_0-spaces*, Journal of Pure and Applied Algebra, **170**, (2002), 309-320.

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

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

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